

Ш. Х. МИХЕЛОВИЧ

ТЕОРИЯ ЧИСЕЛ

ИЗДАНИЕ ВТОРОЕ,
ПЕРЕРАБОТАННОЕ И ДОПОЛНЕННОЕ

Допущено
Министерством просвещения РСФСР
в качестве учебного пособия
для физико-математических факультетов
педагогических институтов



ИЗДАТЕЛЬСТВО
«ВЫСШАЯ ШКОЛА»
Москва 1967

Михелович Шефтель Хенехович

ТЕОРИЯ ЧИСЕЛ

Редактор *А. М. Суходский*

Технический редактор *Н. А. Битюкова*

Корректор *Л. П. Тарасова*

Т-06838 Слано в набор 1/XI-66 г. Подписано в печать 23/V-67 г
Формат $84 \times 108^{1/32}$. Объем 10,5 п. л. 17, 64 усл. п. л.
Уч.-изд. л. 16, 11. Изд. № ФМ-284. Тираж 20.000 экз.
Заказ Б-530 Цена 45 коп.

Тематический план изд-ва „Высшая школа“ (вузы и техникумы
на 1967 г. Позиция № 39

Москва, К-51, Неглинная ул., д. 29/14,
Издательство „Высшая школа“

Типография „Татполиграф“ Управления по печати
при Совете Министров ТАССР
г. Казань, ул. Миславского, 9.

ОГЛАВЛЕНИЕ

	<i>Стр.</i>
Предисловие ко второму изданию	9
Введение	
§ 1. Предмет и основные разделы теории чисел	11
1. Предмет теории чисел (11). 2. Основные разделы теории чисел (11).	
§ 2. Краткие сведения из истории развития теории чисел	13
1. От Пифагора до Ферма (13). 2. Ферма, Эйлер, Лагранж, Гаусс (15). 3. XIX век. Развитие теории чисел в России (18). 4. Развитие теории чисел в XX веке. Советская школа теории чисел (20)	
Глава I. Теория делимости	
§ 1. Делимость, деление с остатком	23
1. Понятие делимости; свойства делимости (23). 2. Деление с остатком (24). Упражнения 1—5 (24)	
§ 2. Наибольший общий делитель	25
1. Наибольший общий делитель двух чисел. Алгоритм Евклида (25). 2. Основные свойства Н.О.Д. двух и нескольких чисел (27). Упражнения 6—19 (28)	
§ 3. Наименьшее общее кратное	29
1. Наименьшее общее кратное двух чисел (29)	
2. Н.О.К. нескольких чисел (30). Упражнения 20—25 (31)	
§ 4. Простые числа. Разложение на простые множители	31
1. Простые и составные числа; их основные свойства (31). 2. Основная теорема арифметики (32). 3. Решето Эратосфена (34). Упражнения 26—40 (35)	

Глава II. Классы по данному модулю. Сравнения и классы

§ 1. Сравнения и их основные свойства	36
1. Понятие сравнимости и равносильные утверждения (36). 2. Основные свойства сравнений (38). Упражнения 41—50 (41)	
§ 2. Классы по данному модулю	43
1. Разбиение множества целых чисел на классы (43). 2. Сложение и умножение классов (44). 3. Кольцо классов (45). Упражнения 51—57 (46)	
§ 3. Системы вычетов	47
1. Полная система вычетов (47). 2. Признак полной системы вычетов (48). 3. Первая теорема о вычетах линейной формы (48). 4. Приведенная система вычетов. Функция Эйлера (49). 5. Признак приведенной системы вычетов (50). 6. Вторая теорема о вычетах линейной формы (50). Упражнения 58—66 (52)	
§ 4. Основные свойства функции Эйлера	52
1. Мультипликативность функции Эйлера (52). 2. Формула для вычисления $\varphi(m)$ (54). 3. Сумма значений функции Эйлера, распространенная по всем делителям данного числа (55). Упражнения 67—77 (56)	
§ 5. Теоремы Эйлера и Ферма	57
1. Теорема Эйлера (57). 2. Теорема Ферма (58). 3. Применение теорем Эйлера и Ферма (59). Упражнения 78—88 (60)	

Глава III. Сравнения с неизвестной величиной

§ 1. Классы решений сравнения произвольной степени . .	61
Упражнение 89 (63)	
§ 2. Сравнения первой степени	64
1. Критерий разрешимости и число решений. Решение методом подбора (64). 2. Решение сравнения первой степени методом преобразования коэффициентов (66). 3. Решение сравнения первой степени при помощи теоремы Эйлера (67). Упражнения 90—94 (68)	
§ 3. Правильные конечные цепные дроби	69
1. Выделение целой части (69). 2. Разложение в правильную цепную дробь (70). 3. Подходящие дроби; некоторые их свойства (75). Упражнения 95—102 (78)	
§ 4. Решение сравнений первой степени с помощью цепных дробей	79

1. Вывод формулы решения (79). 2. Применение сравнений первой степени к решению неопределенных уравнений первой степени с двумя неизвестными (81). Упражнения 103—115 (82)	
§ 5. Системы сравнений первой степени	82
1. Общий случай (82). 2. Случай попарно простых модулей (84). Упражнения 116—122 (87)	
§ 6. Сравнения n -ой степени по простому модулю	87
1. Сведение к наиболее простому виду (87). 2. О максимальном числе решений (90). 3. Теорема Вильсона (93). Упражнения 123—130 (94)	
§ 7. Сравнения n -ой степени по составному модулю	95
1. Приведение сравнения по составному модулю к системе сравнений по модулям попарно простым (95). 2. Приведение к сравнениям по модулю p^a и к сравнениям по модулю p (98). Упражнения 131—138 (101)	
§ 8. Сравнения второй степени общего вида	101
1. Сравнения второй степени и их связь с неопределенными уравнениями второй степени с двумя неизвестными (101). 2. Приведение сравнений второй степени к двучленным сравнениям (102). Упражнение 139 (105)	
§ 9. Общие сведения о двучленных сравнениях второй степени по нечетному простому модулю	105
1. Число решений. Нахождение решений методом подбора. Число квадратичных вычетов (105). 2. Критерий Эйлера (107). Упражнения 140—146 (109)	
§ 10. Символ Лежандра	110
1. Символ Лежандра и его свойства (110). 2. Лемма Гаусса (115). 3. Доказательство свойства V символа Лежандра (117). 4. Доказательство закона взаимности (120). 5. Символ Якоби и его свойства (123). Упражнения 147—159 (124)	

Глава IV. Степенные вычеты

§ 1. Показатели и их основные свойства	125
1. Число, принадлежащее показателю. Первообразный корень (125). 2. Классы, принадлежащие показателю (127). 3. Свойства системы чисел $a^0, a^1, \dots, a^{\delta-1}$ (127). 4. Необходимое и достаточное условие сравнимости a^{γ} и $a^{\gamma'}$ по модулю m , если a принадлежит показателю δ по модулю m (128). Упражнения 160—172 (130)	

§ 2. Существование и число классов, принадлежащих показателю	131
1. Лемма о числе классов, принадлежащих показателю (по простому модулю p) (131). 2. Теорема о существовании и числе классов, принадлежащих показателю по простому модулю (133). Упражнения 173—184 (135)	
§ 3. Индексы и их свойства	136
1. Понятие индекса. Основные свойства (136). 2. Таблицы индексов (139). Упражнения 185—190 (140)	
§ 4. Применение индексов к решению сравнений	141
1. Решение двучленных сравнений (141) 2. Критерий разрешимости сравнений $x^a \equiv 0 \pmod{p}$ (143). 3. Решение показательных сравнений (144). Упражнения 191—198 (145)	

Глава V. Арифметические приложения теории сравнений

§ 1. Вычисление остатков при делении на данное число. Установление признаков делимости с помощью сравнений. Упражнения 199—205 (150)	147
§ 2. Определение длины периода, получающегося при обращении обыкновенной дроби в десятичную	150
Упражнения 206—215 (157)	
§ 3. Проверка результатов арифметических действий	159
Упражнения 216—218 (160)	

Глава VI. Аппроксимация действительных чисел рациональными числами

§ 1. Представление иррациональных чисел правильными бесконечными цепными дробями	161
1. Разложение действительного иррационального числа в правильную бесконечную цепную дробь (161). 2. Сходимость правильных бесконечных цепных дробей (167). 3. Единственность представления действительного иррационального числа правильной бесконечной цепной дробью (169). Упражнения 219—223 (171)	
§ 2. Приближение действительного числа рациональными дробями с заданным ограничением для знаменателя . . .	172
1. Постановка задачи (172). 2. Оценка погрешности при замене действительного числа его подходящей дробью (172). 3. Приближение действительного числа подходящими дробями (173). 4. Теорема Дирихле (179). 5. Подходящие дроби как наилучшие приближения (183). Упражнения 224—233 (190)	

§ 3. Квадратические иррациональности и периодические цепные дроби	191
Упражнение 234 (196)	
§ 4. Решение уравнения Пелля	196
Упражнение 235 (199)	
§ 5. Представление действительных чисел цепными дробями общего вида	199

Глава VII. Алгебраические и трансцендентные числа

§ 1. Иррациональные числа	205
1. Некоторые признаки иррациональности (205). 2. Иррациональность чисел e и π (207)	
§ 2. Поле алгебраических чисел	210
1. Понятие алгебраического числа степени n (210). 2. Поле всех алгебраических чисел (211). 3. Целые алгебраические числа (213). 4. Значение законов взаимности. Общий закон взаимности (216). 5. Проблема Ферма (217). Упражнения 236—240 (221)	
§ 3. Теорема Лиувилля. Трансцендентные числа	221
1. Теорема Лиувилля (221). 2. Доказательство существования трансцендентных чисел (223). 3. Исследования трансцендентности. Результаты Гельфонда (225). 4. Усиление неравенства Лиувилля. Приложение к решению неопределенных уравнений (227). Упражнение 241 (228)	

Глава VIII. Числовые функции

§ 1. Число и сумма делителей данного числа	229
1. Формула для числа делителей данного числа (229). 2. Формула для суммы делителей данного числа (230). Упражнения 242—249 (231)	
§ 2. Совершенные числа. Специальные простые числа . . .	231
1. Определение совершенных и дружественных чисел (231). 2. Представление четных совершенных чисел. О нечетных совершенных числах (232). 3. Простые числа Мерсенна; их наибольшее известное значение (234). 4. Простые числа Ферма (235). 5. О числовых функциях, принимающих простые значения (237). 6. О критериях простых чисел и разложении на множители (239). Упражнения 250—254 (242)	
§ 3. Функции $[x]$ и $\{x\}$	242
1. Графики функций $[x]$ и $\{x\}$ (242). 2. Некоторые свойства функции $[x]$ (243). 3. Вычисление показателя α ,	

с которым простое число p входит в произведение $n!$ (244). Упражнения 255—269 (245)

§ 4. Распределение простых чисел.	246
1. Бесконечность множества простых чисел. Доказательство Евклида. Функция $\pi(x)$ и ее график (246).	
2. Оценка n -го простого числа, вытекающая из доказательства Евклида (248).	
3. Существование любых отрезков натурального ряда, не содержащих простых чисел. Проблема простых чисел — «близнецов» (249).	
4. Доказательство Эйлера бесконечности множества простых чисел (250).	
5. Расходимость ряда величин, обратных простым числам. О «средней плотности» простых чисел (252).	
6. Асимптотический закон распределения простых чисел (255).	
7. Основные результаты 1-го мемуара П. Л. Чебышева о простых числах (257).	
8. Основные результаты 2-го мемуара П. Л. Чебышева о простых числах. Неравенство Чебышева и его упрощенное доказательство (263).	
9. Оценка роста n -го простого числа на основании неравенства Чебышева (271).	
10. О доказательствах закона распределения простых чисел (272).	
11. Об оценках добавочного члена в приближенном представлении $\pi(x)$ (274).	
12. О распределении простых чисел в арифметической прогрессии (276). Упражнения 270—275 (277)	
§ 5. Аддитивные проблемы теории чисел	278
1. Примеры аддитивных задач: проблемы Гольдбаха — Эйлера, Варинга и Харди — Литлвуда (278).	
2. Разложения на сумму квадратов (282).	
3. О методе Л. Г. Шнирельмана (288).	
4. О методе И. М. Виноградова (294). Упражнения 276—280 (301)	
Указания и ответы к упражнениям	301
Таблицы индексов	327
Литература	334

ПРЕДИСЛОВИЕ

ко второму изданию

А. Из предисловия к первому изданию целесообразно напомнить, что книга написана в качестве учебного пособия по курсу теории чисел для физико-математических факультетов педагогических институтов и предназначена не только для студентов стационара, но и заочных факультетов. Поэтому изложение проводится по возможности в доступной форме, причем особое внимание уделяется разъяснению вводимых понятий.

Материал книги в основном излагается в объеме, предусмотренном программой, и в той же последовательности.

Несколько подробнее рассмотрены «Числовые функции». Это сделано потому, что эта область теории чисел, ярко свидетельствующая о большом вкладе в науку русской и советской математических школ теории чисел, очень богата интересными для учителя вопросами. В остальном материал, выходящий за рамки программы, дается, как правило, обзорно.

Б. Во второе издание книги наряду с довольно многочисленными мелкими исправлениями и уточнениями внесен ряд более значительных изменений и дополнений.

1. Чтобы придать книге большую полноту и расширить возможный круг читателей, в нее включена теория делимости (гл. I).

Добавлены некоторые сведения о сравнениях (гл. II, § 1, п. 2; гл. III, § 6, п. 2), степенных вычетах (гл. IV, § 1, п. 4), цепных дробях (гл. VI, § 2, п. 3 и п. 5Б), функции «целая часть» (гл. III, § 3, п. 2) и работах Л. Г. Шнирельмана (гл. VIII, § 4, п. 3).

Уточнена терминология цепных дробей. Дан краткий обзор цепных дробей общего вида (гл. VI, § 5).

Добавлен новый параграф об иррациональных числах (гл. VII, § 1) в соответствии с новой программой по теории чисел.

2. Переработано изложение некоторых вопросов (о максимальном числе решений сравнения (гл. III, § 6, п. 2), степенных вычетах (гл. IV, § 2), признаках делимости (гл. V, § 1), проблеме Варинга (гл. VIII, § 5, п. 1 Е)) и доказательств.

Отмечены достижения последних лет.

3. Книга дополнена 280 упражнениями, которые отнесены к соответствующим параграфам. Многие из них составлены за-

ново. Подчеркнута геометрическая интерпретация. Ко всем упражнениям даны ответы, а к более трудным также и указания.

Материал, изложенный в тексте книги, от задач не зависит; однако задачи в ряде случаев способствуют расширению кругозора читателя.

При работе над вторым изданием книги были использованы ценные советы и критические замечания доц. А. Н. Хованского.

Важные предложения по улучшению книги внесли рецензенты проф. А. М. Лопшиц, доц. В. И. Нечаев и доц. П. Н. Реморов.

Полезные замечания сделали студенты и преподаватели Даугавпилсского педагогического института, особенно доц. В. А. Юрик.

Всем указанным лицам приношу глубокую благодарность.

ВВЕДЕНИЕ ¹

§ 1. Предмет и основные разделы теории чисел

1. Предмет теории чисел

Теория чисел является наукой о числовых системах с их связями и законами. При этом в первую очередь уделяется внимание числам натурального ряда, которые являются основой для построения других числовых систем: целых, рациональных и иррациональных, действительных и комплексных.

Теория чисел изучает числа с точки зрения их строения и внутренних связей, рассматривает возможности представить одни числа через другие, более простые по своим свойствам, между тем строгое логическое обоснование понятия натурального числа и его обобщений, а также связанная с ним теория действий рассматриваются отдельно в основаниях арифметики.

Поскольку упомянутые вопросы изучаются в школьном курсе (или более подробно, например, на физико-математических факультетах педвузов в курсе элементарной математики), они объединяются под названием арифметики, хотя, как наука, арифметика отождествляется с теорией чисел.

Следует отметить, что в последнее время бурно развиваются новые области математики, требующие глубокого анализа дискретного, т. е. прерывного. В связи с этим возрастает интерес к теории чисел, большинство утверждений которой относятся к дискретной математике.

2. Основные разделы теории чисел

Проблемы и задачи, которые возникли в теории чисел, можно распределить на четыре основные группы:

1) решение диофантовых (или неопределенных) уравнений, т. е. решение в целых числах алгебраических уравнений с целыми коэффициентами или систем таких уравнений, у которых число неизвестных больше числа уравнений;

¹ Желательно, чтобы читатель после изучения основных глав еще раз вернулся к введению.

2) диофантовы приближения. В этом направлении теории чисел рассматриваются приближения действительных чисел рациональными числами, решение в целых числах разного рода неравенств (например, неравенства $|ax - y| < \frac{1}{x}$, где a — иррациональное число). К диофантовым приближениям относится

также теория трансцендентных чисел (см. гл. VII). В ней занимаются исследованием арифметической природы разных классов иррациональных чисел относительно их принадлежности к трансцендентным числам или к алгебраическим иррациональностям;

3) вопросы распределения простых чисел в натуральном ряду и других числовых последовательностях.

К этой части теории чисел, в частности, относят проблему нахождения n -го простого числа;

4) аддитивные проблемы. Это проблемы касаются разложения целых (обычно больших) чисел на слагаемые определенного вида.

В теории чисел развились различные методы исследования для решения упомянутых задач, которые также берутся за основу для классификации ее направлений.

С точки зрения методов различают 4 главных направления:

а) элементарные методы теории чисел. К элементарным методам относят такие, которые в основном используют сведения из элементарной математики и самое большое — элементы анализа бесконечно малых.

Элементарными считают методы теории сравнений (см. § 1, гл. II), творцом которых является великий немецкий математик К. Ф. Гаусс (1777—1855), методы цепных дробей (см. § 3, гл. III), которые развили великий петербургский математик Л. Эйлер (1707—1783) и французский математик Ж. Лагранж (1736—1813), и многие другие. Следует иметь в виду, что элементарность метода не говорит еще о его простоте.

По созданию важных элементарных методов в теории чисел большие заслуги принадлежат великому русскому математику П. Л. Чебышеву¹ (1821—1894), французским математикам Ж. Лиувиллю (1809—1882) и Ш. Эрмиту (1822—1901), норвежским математикам А. Туэ (1863—1922) и В. Бруну, а также датскому математику А. Сельбергу.

Фундаментальный метод в аддитивной теории чисел создан советским математиком Л. Г. Шнирельманом (1905—1938);

б) аналитическая теория чисел. Аналитическая теория чисел применяет средства математического анализа, теорию функций действительного и комплексного переменного, теорию рядов, теорию вероятностей и другие разделы математики.

Основоположителем этого направления является Л. Эйлер. Значительное влияние на развитие этой теории оказали работы Гаусса. В области действительного переменного аналитические методы были развиты немецким математиком Л. Дирихле (1805—

¹ По его собственному указанию, надо произносить: Чебышёв.

1859) и П. Л. Чебышевым. Большую роль в развитии аналитических методов, связанных с теорией функций комплексного переменного, сыграли работы немецкого математика Б. Римана (1826—1866). Очень важными оказались работы немецкого математика Г. Вейля (1885—1955) и русского математика Г. Ф. Вороного (1868—1908).

Больших успехов добились индийский математик С. Рамануджан (1887—1920), английские математики Г. Харди (1877—1947) и Дж. Литлвуд (род. в 1885 г.) и немецкий математик К. Зигель. Наиболее мощные методы созданы советскими математиками — академиком И. М. Виноградовым (род. в 1891 г.), а также чл.-корр. АН СССР А. О. Гельфондом (род. в 1906 г.) и академиком Ю. В. Линником (род. в 1915 г.);

в) алгебраическая теория чисел. Эта теория, исходящая из понятия алгебраического числа, создавалась в работах английского математика Дж. Валлиса (1616—1703), Ж. Лагранжа и Л. Эйлера. Особенно важны работы немецких ученых К. Гаусса, Э. Куммера (1810—1893), Р. Дедекинда (1831—1916), Л. Кронекера (1823—1891) и выдающихся русских ученых Е. И. Золотарева (1847—1878) и Г. Ф. Вороного.

Из современных зарубежных ученых необходимо отметить А. Вейля, Г. Хассе, К. Зигеля. Крупных успехов в этой области добились советские математики Н. Г. Чеботарев (1894—1947), Б. А. Венков (род. в 1900 г.), в особенности И. Р. Шафаревич (род. в 1923 г.);

г) геометрическая теория чисел. В этой теории применяются так называемые «пространственные решетки» или системы целочисленных точек, имеющих в качестве координат в заданной прямоугольной системе координат целые числа. Эта теория используется в геометрии и в кристаллографии, в теории чисел она связана с теорией квадратичных форм (т. е. однородных многочленов второй степени $ax^2 + bxy + cy^2$, где коэффициенты a, b, c — целые числа). При помощи сетки целых точек многим утверждениям теории чисел можно дать весьма наглядное толкование.

Основателями этой теории являются Г. Минковский (1864—1909), Г. Ф. Вороной и Ф. Клейн (1849—1925).

Геометрические методы успешно применяются советскими математиками, особенно Б. Н. Делоне (род. в 1890 г.) и Б. А. Венковым.

Отмеченные методы часто переплетаются между собой. Так, например, методы аналитической теории чисел применяются в алгебраической и геометрической теории чисел.

§ 2. Краткие сведения из истории развития теории чисел

1. От Пифагора до Ферма

Важные свойства целых чисел были установлены уже в древности. В Греции, в школе Пифагора (VI в. до н. э.), изучались вопросы делимости чисел, рассматривались различные категории

чисел, например простые, составные, совершенные (т. е. числа, сумма собственных делителей которых равна этому же числу, например $6 = 1 + 2 + 3$), квадратные. Было также известно, что взаимно простые целые числа x, y, z , удовлетворяющие уравнению $x^2 + y^2 = z^2$, так называемые *пифагоровы числа*, получаются по формулам:

$$x = 2m \cdot n, \quad y = m^2 - n^2, \quad z = m^2 + n^2,$$

где m и n — целые числа, $m > n > 0$, $(m, n) = 1$ ¹, $m \cdot n$ — четное (см. п. 5, § 1, гл. VII).

В своих «Началах» Евклид (III в. до н. э.) дает алгоритм (так называемый *алгоритм Евклида*) для определения Н. О. Д. двух чисел, являющийся основой теории делимости, излагает основные свойства делимости целых чисел, доказывает теорему о том, что простые числа образуют бесконечное множество.

Эратосфен (III в. до н. э.), давший способ для выделения простых чисел из ряда натуральных чисел (решето Эратосфена) сделал дальнейший шаг в теории простых чисел.

Эратосфен занимался также *многоугольными числами*². По-

¹ Знаком (m, n) мы будем обозначать наибольший общий делитель (сокращенно Н.О.Д.) m и n .

² Числами n -угольными называются числа вида S_1^n, S_2^n, \dots , где k — n -угольное число S_k^n , является суммой k членов арифметической прогрессии с первым членом $a_1 = 1$ и разностью $d = n - 2$. Таким образом, треугольные числа имеют вид

$$S_1^3 = 1, \quad S_2^3 = 1 + 2 = 3,$$

$$S_3^3 = 1 + 2 + 3 = 6, \dots, \quad S_k^3 = \frac{k(k+1)}{2}.$$

Им соответствуют треугольники, составленные из точек,

$$\begin{array}{c} \cdot \\ \cdot \cdot \cdot \\ \cdot \cdot \cdot \cdot \cdot \end{array}$$

и т. д.

(поэтому и название «треугольные числа»).

Аналогично для 4-угольных чисел имеем разность $d = n - 2 = 2$, так что

$$S_1^4 = 1, \quad S_2^4 = 1 + 3 = 4, \dots, \quad S_k^4 = 1 + 3 + \dots + (2k - 1) = k^2.$$

Им соответствуют квадраты, составленные из точек,

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}$$

и т. д.

Для $n > 2$ геометрическое истолкование несколько усложняется.

следним большое внимание уделено и в «Введении в арифметику» Никомаха. Эта книга является первым из известных систематических руководств по арифметике; она сыграла значительную роль в развитии математики в средние века.

Характерным для работы Никомаха является то, что в ней арифметика впервые излагается независимо от геометрических представлений.

Большое значение имели работы греческого математика Диофанта из Александрии (около III в. н. э.). Из его работ сохранились только часть «Арифметики» и книги о многоугольных числах. Значительную часть своей работы он посвятил решению неопределенных уравнений в рациональных числах. (В дальнейшем название диофантовых уравнений получили уравнения, решаемые в целых числах.) Диофант с большим мастерством решает различные неопределенные уравнения до 3-й и 4-й степени, однако общих методов у него нет. Работа Диофанта, переизданная французским математиком Баше де-Мезириаком в 1621 г., явилась отправной точкой для теоретико-числовых исследований французского математика П. Ферма (1601—1665), Эйлера, Гаусса и других математиков.

Необходимо отметить, что и в Китае со второго века занимались неопределенными уравнениями. Известна задача о нахождении наименьшего целого числа, которое при делении на заданные числа дает заданные остатки.

В дошедших до нас работах индийских математиков Ариабхата (V в.), Брамигупта (VII в.), Бхаскара (XII в.) имеются общие методы решения неопределенных уравнений 1-й степени с 2 неизвестными. Они с успехом занимались также уравнениями вида $ax^2 + b = cy^2$, $xu = ax + by + c$.

В отличие от Диофанта индусы решали неопределенные уравнения в целых числах.

Вопрос о взаимовлиянии греческой и индийской математики остается до сих пор невыясненным. Не подлежит сомнению влияние последней на развитие математики у арабов, которые, однако, в области теории чисел существенно не продвинулись, что вообще характерно для средних веков.

2. Ферма, Эйлер, Лагранж, Гаусс

а) Расцвет теории чисел начинается в новое время и связан в первую очередь с именем величайшего французского математика XVII в. П. Ферма. Ферма под влиянием работ Диофанта исследовал прежде всего решение многих уравнений в целых числах. Ферма, очевидно, владел решением уравнения $x^2 - ay^2 = 1$, где a — целое положительное число, не равное квадрату. В открытом письме в виде вызова современным ему математикам Ферма пред-

ложил доказать, что это уравнение всегда имеет решение в целых числах x, y ($y \neq 0$). Упомянутое утверждение имеет большое значение¹. Впервые оно было доказано Лангранжем², который использовал эту теорему для полного решения в целых числах любого неопределенного уравнения второй степени с двумя неизвестными:

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0.$$

Ферма высказал утверждение, что он владеет замечательным доказательством неразрешимости уравнения $x^n + y^n = z^n$ для $n > 2$ в целых числах (см. п. 5, § 2, гл. VII). Это утверждение, которое носит название *великой теоремы Ферма*, еще до сих пор не доказано и не опровергнуто. Попытки многих математиков решить проблему Ферма стимулировали развитие теории алгебраических чисел.

Ферма доказал, что простые числа вида $4n + 1$ единственным образом разлагаются в сумму двух квадратов. Эту теорему можно считать первым важным предложением о квадратичных формах.

Ферма высказал одну из важнейших теорем теории сравнений, а именно, что $a^{p-1} - 1$ всегда делится на p , если p — простое число и a не делится на p . Эта теорема называется теперь малой теоремой Ферма.

Из других теорем Ферма отметим утверждение, что всякое натуральное число является суммой n или меньшего числа n -угольных чисел. Это предложение можно считать одним из самых первых в аддитивной теории чисел. В общем виде оно было впервые доказано Коши (1815).

б) Большой вклад в развитие теории чисел внес член Петербургской Академии Наук великий Л. Эйлер, жизнь и научная деятельность которого тесно связаны с Россией.

По теории чисел Эйлер написал более 100 мемуаров. Он доказал почти все теоремы Ферма, которые последний оставил без доказательств, открыл также много новых законов и методов.

Стремясь исследовать природу натуральных чисел относительно их простоты и определить сколь угодно большое простое число, Эйлер, исходя из малой теоремы Ферма, обобщил ее в двух направлениях. Он доказал теорему, которая носит теперь его имя, а именно, что $a^{\varphi(m)} - 1$ делится на m , если a и m — числа взаимно

¹ Найти решение удалось Валлису и Броункеру, однако впоследствии Эйлер по недоразумению приписал это решение Дж. Пеллю, в связи с чем упомянутое уравнение вошло в математическую литературу под названием *уравнения Пелля*. Так называют и более общее уравнение $x^2 - ay^2 = c$.

² Необходимо отметить, что Ферма не оставил систематического изложения своих открытий и методов. Результаты, найденные им, записаны лишь без доказательств на полях его рабочего экземпляра Диофанта или имеются в письмах к современным ему математикам, но тоже без доказательств.

простые и $\varphi(m)$ (называется теперь *функцией Эйлера*) — число натуральных чисел, не превосходящих m и взаимно простых с ним. (Если $m = p$ число простое, то $\varphi(m) = p - 1$, и мы получаем малую теорему Ферма.) Кроме того Эйлер разработал основы так называемой теории степенных вычетов, связанной с понятием наименьшего числа $\gamma \neq 0$, для которого $a^\gamma - 1$ делится на простое p , если a на p не делится (см. § 1, гл. IV).

Исходя из теоремы Ферма о том, что простое число вида $4n + 1$ представляется единственным образом в виде суммы двух квадратов, Эйлер исследовал вопрос о делителях чисел вида $x^2 + dy^2$ для специальных значений d (Эйлер, между прочим, доказал, что число вида $4n + 1$ является простым, если оно имеет лишь одно представление в виде суммы двух квадратов и эти квадраты к тому еще взаимно просты).

В 1772 г. Эйлер эмпирически нашел *закон взаимности* (см. § 10, гл. III), который характеризует остатки, получающиеся от деления квадратов на простые числа. Этот закон имеет фундаментальное значение для решения неопределенных уравнений второй степени.

Эйлер исследовал ряд задач из диофантова анализа, доказал великую теорему Ферма для случаев, когда $n = 3, 4$.

Эйлер первый изложил теорию цепных дробей, поставил вопрос об их использовании для решения дифференциальных уравнений, применил их к разложению функций, представлению бесконечных произведений, дал важное их обобщение.

Работы Эйлера по теории цепных дробей были продолжены М. Софроновым (1729—1760), акад. В. М. Висковатым (1779—1812), Д. Бернулли (1700—1782) и др.

Эйлер дал новое доказательство бесконечности количества простых чисел, применив для этого аппарат математического анализа, и положил этим начало аналитической теории чисел (см. п. 4, § 4, гл. VIII).

Необходимо еще отметить, что в переписке Эйлера с петербургским академиком Х. Гольдбахом (1690—1764) в 1742 г. возникла сложнейшая аддитивная проблема, знаменитая «*проблема Гольдбаха*», а именно были выдвинуты две гипотезы: (1) всякое четное число > 2 есть сумма двух простых; (2) всякое нечетное число > 6 есть сумма трех простых (см. § 5, гл. VIII).

в) Ж. Лагранж (1736—1813) заложил основы общей теории бинарных (т. е. зависящих от двух переменных) квадратичных форм (которая впоследствии была развита Гауссом и для форм с большим количеством переменных) и решил, как об этом уже выше отмечалось, неоднородное уравнение второй степени с двумя неизвестными. При этом он воспользовался свойствами цепных дробей.

Лагранж значительно развил теорию цепных дробей и нашел метод приближенного решения с их помощью дифференциальных уравнений.

Лагранж доказал также частный случай утверждения Ферма о многоугольных числах, а именно, что каждое целое положительное N есть сумма не более 4 квадратов. (Это утверждение является также частным случаем *проблемы Варинга* (см. § 5, гл. VIII).)

г) В развитии теории чисел особенно велики заслуги Гаусса. В своих знаменитых «Арифметических исследованиях» (1801)¹ и других трудах он изложил все существенное, что было создано до него, причем во многом в более общей форме².

Кроме того, ему принадлежат крупные открытия, из которых отметим следующие: Гаусс создал аппарат сравнений и доказал основной закон в теории сравнений второй степени — так называемый закон взаимности. Он развил теорию квадратичных форм. Его арифметическая теория целых комплексных чисел имела большое значение для развития алгебраической теории чисел. Гаусс рассматривал также особые тригонометрические суммы, которые сыграли важную роль в аналитической теории чисел (см. § 5, гл. VIII).

3. XIX век. Развитие теории чисел в России

а) Для развития теории чисел в XIX в. характерны, во-первых, фундаментальные работы Гаусса (которые мы уже отмечали) и дальнейшая разработка глубоких идей, изложенных в его трудах; далее, значительное укрепление аналитических методов исследования и успешное решение различных проблем в теории распределения простых чисел, наконец, создание новых направлений, а именно геометрической теории чисел и теории трансцендентных чисел.

б) Работы Гаусса не были сразу поняты его современниками, однако в дальнейшем они нашли многих продолжателей, в первую очередь среди немецких математиков.

Важную роль в разработке идей Гаусса, изложенных в его «Арифметических исследованиях», сыграл Дирихле, в частности, его работы оказали большое влияние на развитие теории алгебраических чисел и аналитических методов в теории чисел.

В создании основ алгебраической теории чисел большие заслуги имеет Куммер, который пришел к ней, пытаясь доказать великую теорему Ферма. Куммер ввел так называемые идеальные числа и дал доказательство теоремы Ферма для целого ряда показателей, в том числе для всех $n < 100$. Идеи Куммера были дальше развиты в работах Кронекера и Дедекинда. Особенно глубокое развитие теория алгебраических чисел получила в работах русского математика Е. И. Золотарева.

Начатые Гауссом исследования, касающиеся законов взаимности, были обобщены математиками К. Якоби (1804—1851), Г. Эйзенштейном (1823—1852) и Д. Гильбертом (1862—1943).

¹ Написаны на латинском языке под названием «Disquisitiones arithmeticae». Имеется русский перевод в книге (5).

² Первую попытку систематически изложить современную ему теорию чисел сделал А. Лежандр (1752—1833) в своей работе «Опыт теории чисел» (1797—1798). Лежандр имеет и другие большие заслуги в истории развития теории чисел.

Дальнейшее развитие теории форм привело Г. Минковского и Г. Ф. Вороного к открытию геометрической теории чисел.

в) В развитии теории трансцендентных чисел важные результаты были получены французскими математиками.

Ж. Лиувилль открыл необходимый признак алгебраического числа и исходя из этого признака получил метод построения трансцендентных чисел (см. § 3, гл. VII).

Ш. Эрмит развил теорию квадратичных форм и нашел элементарный метод для доказательства трансцендентности числа e .

Этим же методом немецкий математик Ф. Линдеман (1852—1939) доказал трансцендентность числа π .

г) Существенная роль в развитии теории чисел XIX в. принадлежит русским математикам.

Интерес к теории чисел в России в XIX в. возродил В. Я. Буняковский (1804—1889); он посвятил теории чисел более 40 интересных работ (среди них имеются: доказательства закона взаимности, задачи диофантова анализа, исследования свойств числовых функций, вопросы Эратосфенова решета и др.), принял деятельное участие в издании арифметических работ Л. Эйлера и привлек к этому молодого П. Л. Чебышева, дальнейшие открытия и научная деятельность которого в области теории чисел создали целую школу, сыгравшую в развитии теории чисел XIX в. очень большую роль и известную под названием Петербургской школы теории чисел.

Глубокие исследования Чебышева в области теории чисел относятся к вопросу о распределении простых чисел (см. § 4, гл. VIII). В изучении этой важнейшей проблемы со времен Евклида до начала XIX в. были сделаны только лишь первые шаги. Лежандр и Гаусс нашли эмпирические формулы для количества простых чисел $\pi(x)$, не превосходящих данное число x .

Это были замечательные формулы, но подкрепить их теоретическими доводами эти ученые не сумели. Чебышев был первый, кто после Евклида достиг важных теоретических результатов в этом труднейшем вопросе теории чисел. В своих знаменитых работах 1849 и 1852 гг. он существенно продвинулся в теоретическом обосновании так называемого *асимптотического закона*

распределения простых чисел (т. е. доказательства того, что

$\lim_{x \rightarrow \infty} \left(\pi(x) : \frac{x}{\ln x} \right) = 1$), который средствами теории функций

комплексного переменного был полностью доказан пятьдесят лет спустя, в 1896 г., французским математиком Ж. Адамаром (1865—1963) и бельгийским математиком Ш. Ж. Валле-Пуссенем (1866—1962), а элементарным путем — сто лет спустя, в 1949 г., датским ученым А. Сельбергом и венгерским ученым П. Эрдешем.

Выдающиеся представители Петербургской школы теории чисел А. Н. Коркин (1837—1908), Е. И. Золотарев (1847—1878), А. А. Марков (1856—1922) и Г. Ф. Вороной нашли новые методы и направления в теории чисел.

Они провели глубокие исследования, касающиеся квадратичных форм, которые по сей день остаются предметом внимательного изучения.

Вороной сделал, кроме того, важные открытия в геометрии чисел и некоторыми своими работами стимулировал развитие современной аналитической теории чисел.

Работы Маркова имеют важное значение для решения задачи о приближении действительного числа рациональной дробью.

Работы Золотарева по теории алгебраических чисел, что уже отмечалось выше, оказались в этой области исключительными по своей глубине.

Последователями Чебышева в направлении исследований по вопросам распределения простых чисел были П. В. Преображенский (1846—1905), П. С. Порецкий (1846—1907) и др.

д) В развитие теории чисел в XIX в. значительный вклад внесли и другие русские ученые. Особенно следует отметить московского ученого Н. В. Бугаева (1837—1903), который посвятил многочисленные ценные труды изучению различных числовых функций и указал на большое значение прерывных функций в математике вообще.

В этом же направлении работали и его ученики Н. Я. Сонин (1849—1915), Д. Ф. Егоров (1869—1931), Н. В. Берви, И. И. Чистяков и др.

4. Развитие теории чисел в XX в. Советская школа теории чисел

а) В XX в. теория чисел интенсивно развивается во всех своих разветвлениях с применением всех основных методов исследования. Начиная с тридцатых годов в развитии теории чисел ведущее место занимает советская школа теории чисел во главе с академиком И. М. Виноградовым. Об этом убедительно свидетельствуют успехи советских ученых в решении наиболее сложных проблем теории чисел.

б) Важнейшее значение в современной теории чисел приобрели аналитические методы. В первых десятилетиях нашего века сильные методы в аналитической теории чисел для решения аддитивных задач и вопросов распределения простых чисел были развиты английскими математиками Харди и Литтлвудом, индийским математиком Рамануджаном, голландским математиком Ван дер Корпутом, американским математиком Диксоном, немецким математиком К. Зигелем и др.

В указанных методах применялась главным образом теория функций комплексного переменного.

Еще более сильный метод развит академиком И. М. Виноградовым, который успешно применяется как советскими математиками (Н. Г. Чудаков, Ю. В. Линник, К. К. Марджанишвили, Н. М. Коробов), так и зарубежными (Хейльброн, Ван дер Корпут, китайский математик Хуа Ло-кен, Диксон и др.).

Метод Виноградова касается оценки так называемых тригонометрических сумм, т. е. сумм вида $\sum e^{2\pi i f(x)}$, где $f(x)$ — некоторая функция от x , а x пробегает ту или иную числовую последовательность. Оказывается, что многие проблемы аналитической и аддитивной теории чисел сводятся к таким оценкам, например знаменитая проблема Э. Варинга (1770 г.): доказать, что для лю-

бого целого числа $n \geq 2$ существует такое натуральное число $r = r(n)$, что всякое натуральное число N можно представить как сумму r неотрицательных n -х степеней.

Впервые в 1909 г. эту проблему решил Д. Гильберт, но очень громоздким способом и с грубой оценкой числа слагаемых.

Методом тригонометрических сумм И. М. Виноградов в начале 30-х годов добился больших успехов в улучшении решения проблемы Варинга (см. § 5, гл. VIII). Тем же методом Виноградов в 1937 г. доказал справедливость гипотезы Гольдбаха для достаточно больших нечетных чисел, т. е. доказал, что все нечетные числа, начиная с некоторого, являются суммами трех простых (см. § 5, гл. VIII).

Первые успехи в решении проблемы Гольдбаха также принадлежат советскому математику, а именно Л. Г. Шнирельману, который в 1930 г. новым методом, имеющим фундаментальное значение в аддитивной теории чисел, установил, что всякое целое число является суммой ограниченного числа простых чисел (см. § 5, гл. VIII).

Необходимо еще отметить крупные успехи советского математика Ю. В. Линника, который методом Шнирельмана в 1943 г. дал элементарное решение проблемы Варинга, аналитическим методом теории функций комплексного переменного в 1946 г. доказал теорему Гольдбаха-Виноградова, а в 1959 г. — предположение Харди и Литлвуда о том, что каждое достаточно большое натуральное число есть сумма простого числа и двух квадратов целых чисел.

в) Крупные успехи достигнуты за последние три десятилетия в теории трансцендентных чисел.

Найдены методы для определения арифметической природы (относительно трансцендентности) довольно широких классов чисел.

В этой области важнейшую роль сыграл сильный аналитический метод, созданный советским математиком А. О. Гельфондом. В 1934 г. А. О. Гельфонд доказал, что α^β , где α — алгебраическое число, отличное от нуля и 1, а β — алгебраическое иррациональное число, является трансцендентным числом, и решил этим так называемую 7-ю проблему Гильберта, которая в течение 30 лет не поддавалась усилиям математиков (см. § 3, гл. VII).

Важные результаты в области теории трансцендентных чисел принадлежат также немецкому математику К. Зигелю.

г) В теории приближения алгебраических чисел при помощи рациональных большую роль сыграли исследования норвежского математика А. Туэ (1909), которые были продолжены в дальнейшем математиками Зигелем, Дайсоном, Гельфондом и Ротом.

При помощи теоремы Туэ впервые удалось получить сведения о числе решений неопределенного уравнения n -й степени с двумя неизвестными.

Советский математик Б. Н. Делоне достиг значительных успехов в области решения диофантовых уравнений третьей степени (см. § 3, гл. VII).

Важные результаты принадлежат Б. Н. Делоне и Б. А. Венкову в геометрической теории чисел и А. Я. Хинчину (1894—1959) в теории диофантовых приближений.

д) Успешно развивается алгебраическая теория чисел.

Крупный вклад внесли в эту область советский математик Н. Г. Чеботарев, немецкие математики Хассе и Хекке, французский математик А. Вейль.

Очень важным результатом является общий закон взаимности, открытый и доказанный в 1949 г. советским математиком И. Р. Шафаревичем (см. § 2, гл. VII).

е) Новыми сильными методами обогатилась в XX в. элементарная теория чисел. Кроме упомянутых выше методов Туэ и фундаментального метода Л. Г. Шнирельмана, необходимо указать на метод эратосфенова решета, созданный норвежским математиком В. Бруном в 1919 г. Этот метод, получивший дальнейшее развитие в работах А. Сельберга, советского математика А. А. Бухштаба (род. в 1905 г.) и других ученых, успешно применяется в решении аддитивных проблем.

Глава I

ТЕОРИЯ ДЕЛИМОСТИ

§ 1. Делимость, деление с остатком

1. Понятие делимости; свойства делимости

В области целых чисел из основных арифметических действий деление не всегда выполнимо. Возникающие в этой связи вопросы решаются теорией делимости.

Говорят, что целое число a делится на целое число b ($b \neq 0$), или что b делит a , если существует целое число q , такое, что $a = bq$. При этом q называется кратным числа b , а b — делителем числа a . То, что a делится на b , будем обозначать символом $a|b$, если a на b не делится, будем писать $a \nmid b$, например $15|5$, $17 \nmid 5^1$.

Из определения понятия делимости и свойств целых чисел вытекают некоторые простые свойства делимости, которые укажем без доказательства.

1. Отношение делимости рефлексивно и транзитивно, т. е.

а) $a|a$;

б) из $a|b$ и $b|c$ следует $a|c$.

2. Из $a|c$ следует $ab|c$ для любого целого b .

3. Из $a|c$ и $b|c$ следует $ax + by|c$ для любых целых чисел x и y (напр., $a \pm b|c$); это свойство можно распространить на несколько чисел.

4. Из $a|b$ и $b|a$ следует $a = \pm b$.

5. Из $a|b$, $a > 0$, $b > 0$ следует $b \leq a$.

¹ Символом $a|b$ чаще принято обозначать то, что « a делит b ».

2. Деление с остатком

Пусть a — целое, а b — целое положительное число. Не всегда a делится на b , но всегда возможно деление a на b с остатком, т. е. можно найти, причем единственным образом, такие целые q и r , что

$$a = bq + r, \quad 0 \leq r < b. \quad (1)$$

Число q называется *неполным частным*, а число r — *остатком* от деления a на b .

Примеры:

$$99 = 17 \cdot 5 + 14, \quad 0 < 14 < 17,$$

$$-99 = 17 \cdot (-6) + 3, \quad 0 < 3 < 17,$$

$$77 = 11 \cdot 7 + 0, \quad 0 = 0 < 11.$$

Доказательство возможности. Пусть bq — наибольшее кратное числа b , не превышающее a , тогда

$$bq \leq a < b(q+1)$$

и

$$0 \leq a - bq < b.$$

Полагая $a - bq = r$, получаем представление (1).

Доказательство единственности. Допустим, что, кроме (1), возможно представление

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b. \quad (1')$$

Из (1) и (1') следует

$$bq + r = bq_1 + r_1,$$

$$r - r_1 = b(q_1 - q),$$

$$r - r_1 \mid b.$$

Так как $|r - r_1| < b$, то $r - r_1 \mid b$ возможно лишь при $r - r_1 = 0$, т. е. при $r = r_1$. В таком случае и $q = q_1$. Единственность доказана.

Упражнения

1. При делении целого числа a на 13 получается неполное частное 17. Найти наибольшее значение делимого a .

2. Делимое равно 371, частное 14. Найти делители b и соответствующие им остатки r .

3. При делении a на b получается частное q и ненулевой остаток r . На какое натуральное число n нужно умножить a , чтобы при делении на b частное увеличилось в n раз?

4. Делимое 100, остаток 6. Найти делитель b и частное q .

5. Доказать, что 1) из трех последовательных натуральных чисел одно делится на 3, 2) из двух последовательных четных чисел одно делится на 4, 3) из пяти последовательных натуральных чисел одно делится на 5.

§ 2. Наибольший общий делитель

1. Наибольший общий делитель двух чисел.

Алгоритм Евклида

Всякое целое число, которое делит целые числа a и b , называется их общим делителем. Целесообразно ограничиться рассмотрением натуральных делителей, что и предполагается в дальнейшем.

Совокупность общих делителей a и b — будем ее обозначать символом $D_{a,b}$ — является конечной¹ в ней имеется поэтому наибольшее число — так называемый наибольший общий делитель (сокращенно — Н. О. Д.) данных чисел, который обычно обозначается символом (a, b) . Если $(a, b) = 1$, то a и b называются взаимно простыми.

Для нахождения Н. О. Д. двух целых чисел a и b можно составить совокупности D_a и D_b всех делителей каждого, отобрать из них общие, а из последних — наибольший.

Для чисел 24 и 30 имеем, например:

$$D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\},$$

$$D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\},$$

$$D_{24,30} = \{1, 2, 3, 6\}, \quad (24, 30) = 6.$$

Еще Евклид указал на более удобный способ нахождения Н. О. Д.

1. Если $a|b$, то $D_{a,b} = D_b$ и $(a, b) = b$. Действительно, каждый общий делитель чисел a и b делит b ; с другой стороны, всякий делитель числа b является делителем числа a (и b). Поэтому $D_{a,b} = D_b$. Так как из делителей b само число b является наибольшим, то $(a, b) = b$.

2. Если $a \nmid b$, то согласно теореме о делении с остатком получается система равенств

¹ Предполагается, что по меньшей мере одно из чисел a и b отлично от нуля.

$$(A) \quad \begin{cases} a = bq_1 + r_2, & 0 < r_2 < b, \\ b = r_2q_2 + r_3, & 0 < r_3 < r_2, \\ \dots & \dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_nq_n & \end{cases}$$

Система (А) не обрывается, пока получаемые остатки больше нуля. Но поскольку целые неотрицательные остатки r_2, r_3, \dots убывают, то для некоторого n получится $r_{n+1} = 0$, что и принято в (А) ($r_{n-1} = r_nq_n + r_{n+1}$, $r_{n+1} = 0$).

Первое из равенств (А) показывает, что всякий общий делитель a и b делит r_2 (и b), а всякий общий делитель b и r_2 делит a (и b); поэтому $D_{a,b} = D_{b,r_2}$, и вместе с тем $(a, b) = (b, r_2)$. Переходя к следующим строкам системы (А), получаем

$$D_{a,b} = D_{b,r_2} = \dots = D_{r_{n-1}}, \quad r_n = D_{r_n} \quad \text{и} \quad (a, b) = r_n.$$

Указанный способ нахождения Н. О. Д. носит название метода последовательного деления или алгоритма Евклида. Итак, установлено, что множество общих делителей чисел a и b совпадает с множеством делителей их Н. О. Д., который равен последнему отличному от нуля остатку алгоритма Евклида, т. е.

$$D_{a,b} = D_{(a,b)} \quad (1)$$

$$(a, b) = r_n. \quad (2)$$

Для практического определения Н. О. Д. двух чисел (например, для 259 и 119) алгоритмом Евклида обычно применяется схема следующего вида:

$$\begin{array}{r} 259 \overline{) 119} \\ \underline{238} \quad 2 \\ 119 \overline{) 21} \\ \underline{105} \quad 5 \\ 21 \overline{) 14} \\ \underline{14} \quad 1 \\ 14 \overline{) 7} \\ \underline{-} \quad 2 \end{array}$$

Более целесообразно (особенно в связи с цепными дробями, см. п. 3, § 3, гл. III) вспомогательные вычисления выполнять по возможности в уме и располагать схему в одну строку слева направо по следующему образцу:

$$259 \left| \frac{119}{2} \right| \frac{21}{5} \left| \frac{14}{1} \right| \frac{7}{2}$$

Итак, $(259, 119) = 7$.

2. Основные свойства Н. О. Д. двух и нескольких чисел

Применяя алгоритм Евклида к числам ak и bk , где k — натуральное число, вместо равенств системы (А) п. 1 получаем равенства, члены которых в k раз больше. Поэтому

$$(ak, bk) = (a, b)k. \quad (1)$$

Если d является общим делителем a и b , то можно согласно (1) писать

$$(a, b) = \left(\frac{a}{d} d, \frac{b}{d} d \right) = \left(\frac{a}{d}, \frac{b}{d} \right) \cdot d,$$

откуда следует

$$\left(\frac{a}{d}, \frac{b}{d} \right) = \frac{(a, b)}{d}. \quad (2)$$

В частном случае, когда $d = (a, b)$, из (2) получается

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1. \quad (3)$$

Из свойств (1) и (1) п. 1 вытекает важная теорема.

Если ab делится на c и $(a, c) = 1$, то b делится на c , т. е.

$$\text{из } ab|c, (a, c) = 1 \text{ следует } b|c. \quad (4)$$

Действительно, из $(a, c) = 1$ следует $(ab, cb) = b$. Далее, из $ab|c$ (по условию) и $cb|c$ (cb — кратное c) следует согласно (1) п. 1, что $(ab, cb)|c$. Но так как $(ab, cb) = b$, то и получается, что $b|c$.

Понятия общего делителя и Н. О. Д. можно отнести и к нескольким числам. Задача нахождения Н. О. Д. более чем двух чисел сводится к аналогичной задаче для двух чисел.

Пусть имеем числа

$$a_1, a_2, \dots, a_n \quad (A)$$

и пусть

$$(a_1, a_2) = d_2, (d_2, a_3) = d_3, \dots, (d_{n-1}, a_n) = d_n.$$

Известно, что множество D_{a_1, a_2} всех общих делителей a_1 и a_2 совпадает с множеством D_{d_2} делителей их Н. О. Д., аналогично D_{d_2, a_3} совпадает с D_{d_3} и т. д.

Поэтому

$$D_{a_1, a_2, \dots, a_n} = D_{d_2, a_3, \dots, a_n} = \dots = D_{d_{n-1}, a_n} = D_{d_n}$$

и

$$(a_1, a_2, \dots, a_n) = d_n, \quad (5)$$

где (a_1, a_2, \dots, a_n) означает Н. О. Д. чисел a_1, a_2, \dots, a_n . Нетрудно проверить, что и для более чем двух чисел остаются справедливыми соотношения (1) — (3).

Если $d_n = 1$, то числа ряда (A) называются взаимно простыми; если каждое из чисел этого ряда взаимно простое с каждым другим из них, то они называются попарно простыми. Если числа ряда (A) попарно простые, то они и взаимно простые. Обратное утверждать можно лишь для двух чисел.

Упражнения

6. Применяя алгоритм Евклида, найти 1) (247, 133); 2) (703, 481); 3) (3763, 3337).

7. Доказать, что $d = (a, b)$ при a и b , не равных одновременно нулю, можно представить как линейную форму $ax + by$, где x и y — целые.

8. Доказать, что соотношение $a_1x + b_1y = 1$, где x и y — целые числа, выражает необходимое и достаточное условие взаимной простоты целых чисел a_1 и b_1 .

9. Представить $3 = (51, 21)$ как линейную форму $51x + 21y$, где x и y — целые.

10. Найти 1) $d_1 = (819, 702, 689)$, 2) $d_2 = (3059, 2737, 943)$.

11. Доказать, что $(a, b) = (a, a \pm b)$.

12. Доказать, что числа $n, n+1, 2n+1$ — попарно взаимно простые.

13. Доказать, что из условия $(a, b) = 1$ следует, что $(a+b, a-b)$ равен 1 или 2.

14. Доказать, что из условий $(ab, c) = d$ и $(a, c) = 1$ следует $b \mid d$.

15. Показать, что соотношение (4) из п. 2 является следствием теоремы предыдущей задачи.

16. Доказать, что $(a, b) = (u_1a + v_1b, u_2a + v_2b)$, если $u_1v_2 - u_2v_1 = 1$.

17. Доказать, что из условий $(a, c) = 1$ и $(b, c) = 1$ следует $(ab, c) = 1$.

18. Доказать обобщение предыдущей теоремы: если для чисел систем

$$a_1, a_2, \dots, a_k,$$

$$b_1, b_2, \dots, b_e$$

$$(a_i, b_j) = 1 \text{ при любом } i \text{ и } j \text{ и } a_1a_2\dots a_k = A,$$

$$b_1b_2\dots b_e = B, \text{ то } (A, B) = 1.$$

19. Доказать, что $(ac, b) = (c, b)$, если $(a, b) = 1$.

§ 3. Наименьшее общее кратное

1. Наименьшее общее кратное двух чисел

Пусть a и b — целые (отличные от нуля) числа, их общим кратным называется любое число, кратное как a , так и b (т. е. делящееся на a и на b). Такое наименьшее натуральное число называется наименьшим общим кратным (сокращенно Н. О. К.) чисел a и b , мы будем его обозначать символом $[a, b]$.

Если M — какое-либо общее кратное a и b , то $M \mid a$ и $M \mid b$. Из $M \mid a$ следует, что $M = ak$, так что $ak \mid b$.

Пусть теперь $(a, b) = d$, $a = a_1d$, $b = b_1d$. Тогда в силу того, что $(a_1, b_1) = 1$, из $ak \mid b$ следует $a_1k \mid b_1$ и далее $k \mid b_1$. Поэтому $k = b_1t = \frac{b}{d}t$, где t — целое число.

Итак, если M — общее кратное a и b , то оно имеет вид

$$M = \frac{ab}{d}t. \quad (1)$$

С другой стороны, любое число вида (1) является кратным a и b , так как его можно записать в форме

$$M = a(b_1t) = b(a_1t).$$

Таким образом, формой (1) исчерпываются все возможные кратные чисел a и b .

Поскольку множества общих кратных целых положительных и целых отрицательных чисел совпадают и $[a, b] = [|a|, |b|]$, то ограничимся в дальнейшем рассмотрением общих кратных натуральных чисел. Тогда при $t = 1$ получаем из (1) Н. О. К. чисел a и b , так что

$$[a, b] = \frac{ab}{d}$$

и

$$M = [a, b] t.$$

Итак,

1) Н. О. К. двух чисел равно их произведению, деленному на их Н. О. Д.;

2) множество общих кратных двух чисел совпадает с множеством кратных их Н. О. К., или: всякое число M , которое делится на числа a и b , делится на их Н. О. К. $[a, b]$;

3) числа $\frac{[a, b]}{a}$ и $\frac{[a, b]}{b}$ взаимно простые, так как первое из них равно $\frac{b}{d} = b_1$, а второе $\frac{a}{d} = a_1$;

4) Н. О. К. двух взаимно простых чисел равно их произведению, т. е.

если $(a, b) = 1$, то $[a, b] = ab$;

5) если $k > 0$, то $[ak, bk] = [a, b] k$, и если $a | k$ и $b | k$, то $\left[\frac{a}{k}, \frac{b}{k} \right] = \frac{[a, b]}{k}$.

2. Н. О. К. нескольких чисел

Понятия общего кратного и Н. О. К. можно отнести к нескольким числам. При этом задача нахождения Н. О. К. более чем двух чисел сводится к аналогичной задаче для двух чисел. Покажем это.

Пусть дан ряд натуральных чисел

$$a_1, a_2, \dots, a_n \tag{A}$$

и пусть

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \dots, [m_{n-1}, a_n] = m_n.$$

Поскольку общие кратные чисел a_1 и a_2 совпадают с общими кратными их Н. О. К. m_2 , то общие кратные рядов (A) и

$$m_2, a_3, \dots, a_n$$

совпадают, а следовательно, совпадают и их Н. О. К., так что

$$[a_1, a_2, \dots, a_n] = [m_2, a_3, \dots, a_n],$$

где $[a_1, a_2, \dots, a_n]$ означает Н. О. К. чисел ряда (A).

Повторяя указанное рассуждение, находим

$$[a_1, a_2, \dots, a_n] = [m_2, a_3, \dots, a_n] = \dots = [m_{n-1}, a_n] = m_n,$$

значит,

$$[a_1, a_2, \dots, a_n] = m_n.$$

Из доказательства следует, что общие кратные более чем двух чисел совпадают с кратными их Н. О. К. и что для попарно простых натуральных чисел

$$[a_1, a_2, \dots, a_n] = a_1 a_2 \dots a_n.$$

Упражнения

20. Доказать, что 1) произведение трех последовательных натуральных чисел делится на 6, 2) произведение пяти последовательных натуральных чисел делится на 120.

21. Найти 1) $[299, 234]$, 2) $[493, 221]$, пользуясь соотношением

$$[a, b] = \frac{ab}{(a, b)}.$$

22. Найти натуральные числа a и b , если $(a, b) = 15$ и $[a, b] = 840$.

23. Найти Н. О. К. трех последовательных натуральных чисел.

24. Доказать, что для натуральных чисел a_1, a_2, \dots, a_n

$$m = [a_1, a_2, \dots, a_n] = \frac{A}{d}, \quad \text{где } A = a_1 \cdot a_2 \dots a_n,$$

$$d = (A_1, A_2, \dots, A_n), \quad A_1 = \frac{A}{a_1}, \quad A_2 = \frac{A}{a_2}, \quad \dots, \quad A_n = \frac{A}{a_n}.$$

25. Доказать, что для натуральных чисел a, b и c $abc = [a, b, c] \cdot (ab, ac, bc)$.

§ 4. Простые числа. Разложение на простые множители

1. Простые и составные числа; их основные свойства

Всякое натуральное число $p > 1$, не имеющее других натуральных делителей, кроме 1 и p , называется простым. Натуральные числа, отличные от 1 и не

являющиеся простыми, называются составными. Число 1 не считается ни простым, ни составным.

Рассмотрим некоторые теоремы, связанные с понятиями простых и составных чисел.

1. Если $p_1 > 1$ является наименьшим делителем целого числа $n > 1$, то оно простое.

Действительно, иначе p_1 имело бы такой делитель a , что $1 < a < p_1$, и из $n|p_1$ и $p_1|a$ следовало бы, что $n|a$, $a < p_1$, но это противоречит определению числа p_1 .

2. Натуральное число a и простое число p либо взаимно просты, либо a делится на p , т. е. либо $(a, p) = 1$, либо $a|p$.

В самом деле, единственные делители p —это 1 и p , поэтому Н. О. Д. a и p может равняться либо 1, либо p , т. е. либо $(a, p) = 1$, либо $(a, p) = p$. Но в последнем случае $a|p$.

3. Если произведение ab делится на простое число p , то по меньшей мере один из сомножителей делится на p .

Действительно, если $a \nmid p$, то согласно предыдущему свойству $(a, p) = 1$. Но в таком случае из делимости ab на p в силу (4) п. 2, § 2 следует, что b делится на p .

Эту теорему можно способом индукции распространить на произведения трех и более множителей. Так, например, если $abc|p$, а $a \nmid p$, то согласно доказанному $bc|p$, откуда следует, что либо $b|p$, либо $c|p$.

Следует отметить, что в случае, когда все сомножители произведения, делящегося на p , простые числа, то по меньшей мере один из сомножителей должен совпадать с p .

2. Основная теорема арифметики

Теперь мы можем перейти к рассмотрению основной теоремы арифметики: *Всякое натуральное число a , кроме 1, может быть представлено как произведение простых множителей*

$$a = p_1 p_2 \dots p_n, \quad n \geq 1, \quad (1)$$

причем единственным образом, если не обращать внимания на порядок сомножителей.

Представление (1) называется *разложением числа a на простые множители*.

Существование разложения доказывается без особого труда.

В силу 1) из п. 1 число a имеет в качестве наименьшего делителя, отличного от 1, простое число p_1 , так что $a = p_1 a_1$. Если $a_1 > 1$ и p_2 — его наименьший простой делитель, то $a_1 = p_2 a_2$, отсюда $a = p_1 p_2 a_2$. Этот процесс можно продолжить, пока не приходим к какому-либо $a_n = 1$. (То, что после конечного числа шагов такое a_n должно получиться, следует из того, что $a > a_1 > a_2 > \dots$, где a, a_1, \dots натуральные числа.) Итак,

$$a = p_1 p_2 \dots p_n.$$

Единственность разложения доказывается при помощи свойства 3) из п. 1.

Допустим, что существуют два разложения a на простые множители, а именно, что

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_s. \quad (1')$$

Поскольку каждое p_i делит произведение чисел q , то согласно свойству 3) из п. 1 можно утверждать, что p_i равно некоторому q_j и что, наоборот, каждое q равно некоторому p . Таким образом, обе части в (1') содержат одинаковые простые числа. Единственное их отличие может состоять лишь в том, что некоторое простое p встречается в одной части равенства большее число раз, чем в другой. Однако после сокращения на p достаточное количество раз получилось бы равенство с числом p в одной части равенства и без него в другой части, а это противоречило бы свойству 3) из п. 1. Теорема доказана.

Среди простых сомножителей представления (1) могут быть и равные.

Если обозначить различные из них через p_1, p_2, \dots, p_k и допустить, что они встречаются соответственно $\alpha_1, \alpha_2, \dots, \alpha_k$ раз, то получается представление

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad (2)$$

которое называется *каноническим*.

Каноническое разложение показывает, что все делители числа a исчерпываются числами вида

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \quad (3)$$

где

$$0 \leq \beta_1 \leq \alpha_1, \quad 0 \leq \beta_2 \leq \alpha_2, \dots, \quad 0 \leq \beta_k \leq \alpha_k. \quad (4)$$

Действительно, с одной стороны, всякое d такого вида делит a .

С другой стороны, всякое число d , которое делит a , имеет указанный вид, так как оно не может иметь других простых сомножителей, кроме p_1, p_2, \dots, p_k , а их показатели $\beta_1, \beta_2, \dots, \beta_k$ не могут противоречить условиям (4).

3. Решето Эратосфена

Евклид доказал бесконечность множества простых чисел (см. п. 1, § 4, гл. VIII), но вопрос о том, является ли данное число простым или составным, решается для больших чисел с значительным трудом (см. п. 6, § 2, гл. VIII). Важно учесть, что наименьший простой делитель числа a не может быть больше \sqrt{a} .

В самом деле, если p_1 — наименьший простой делитель a , то $a = p_1 a_1$, причем $a_1 \geq p_1$. Поэтому $a = p_1 a_1 \geq p_1^2$, откуда $p_1 \leq \sqrt{a}$.

Упомянутый факт используется при составлении таблицы простых чисел $\leq N$ способом, который был указан еще Эратосфеном и который носит название решета Эратосфена.

Выписывают все натуральные числа от 2 до N . Из них вычеркивают каждое второе число после простого числа 2. Первым незачеркнутым числом остается простое число 3; теперь вычеркивают каждое третье число после 3 (причем считают и те числа, которые зачеркнуты ранее) и т. д.

После вычеркивания всех чисел, кратных простому p_n , первое следующее за p_n незачеркнутое число p_{n+1} является простым, иначе оно имело бы простой делитель $\leq p_n$, но все кратные простым числам $\leq p_n$ уже зачеркнуты.

Простыми являются также незачеркнутые числа $< p_{n+1}^2$, так как составные числа $< p_{n+1}^2$ имеют простой

делитель $\leq p_n$ и уже ранее вычеркнуты из таблицы. Поэтому вычеркивание кратных простому p_{n+1} следует начинать с p_{n+1}^2 и составление таблицы простых чисел $\leq N$ считать законченным, как только найдено простое число $> \sqrt{N}$.

Пример. $N=60$

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60.

Упражнения

26. Доказать, что для простого числа p из условий $a + b \mid p$ и $ab \mid b$ следует, что $a \mid p$ и $b \mid p$.

27. Доказать, что для простого числа p из условий $a \mid p$ и $a^2 + b^2 \mid p$ следует $b \mid p$.

28. Найти (a, b) и $[a, b]$, зная канонические разложения натуральных чисел a и b .

29. Доказать, что при простом p из условий $(a, bp) = d$ и $(a, b) = 1$ следует: d равно 1 или p .

30. Доказать, что из условия $(a, b) = 1$ следует $(a + b, ab) = 1$, $(a - b, ab) = 1$.

31. Доказать, что $(a + b, abp)$ либо равен 1, либо p , если $(a, b) = 1$ и p — простое число.

32. Доказать, что при $(a, b) = 1$ $(a + b, a^2 - ab + b^2)$ равен либо 1, либо 3.

33. Доказать, что $(a, b) = (a + b, [a, b])$.

34. Доказать, что всякое простое число, большее 3, имеет форму $6k + 1$ или $6k + 5$.

35. Доказать, что квадрат любого простого числа, большего 3, имеет форму $12k + 1$.

36. Доказать, что простое число вида $3k + 1$ имеет форму $6n + 1$.

37. Найти все простые числа p , такие, чтобы $p + 10$ и $p + 20$ тоже были простыми.

38. Доказать, что при $n > 2$ числа $2^n - 1$ и $2^n + 1$ не могут одновременно быть простыми.

39. Числа p и $8p^2 + 1$ — простые; доказать, что $8p^2 + 2p + 1$ — также число простое.

40. Доказать, что целое положительное число a вида $3k + 2$ всегда имеет простой делитель такой же формы.

Глава II

КЛАССЫ ПО ДАННОМУ МОДУЛЮ. СРАВНЕНИЯ И КЛАССЫ

§ 1. Сравнения и их основные свойства

1. Понятие сравнимости и равносильные утверждения

Пусть m натуральное число. Тогда, по теореме о делении с остатком, для всякого целого числа a существует единственная пара целых чисел q и r — таких, что

$$a = mq + r, \quad 0 \leq r < m. \quad (1)$$

Упомянутая теорема является основой следующего определения: Если два целых числа a и b при делении на целое положительное m дают один и тот же остаток r , так что

$$a = mq + r \text{ и } b = mq_1 + r, \quad 0 \leq r < m, \quad (2)$$

то они называются равноостаточными, или сравнимыми по модулю m . Это записывается следующим образом:

$$a \equiv b \pmod{m} \quad (3)$$

и читается так: « a сравнимо с b по модулю m ». Соотношение (3) называется *сравнением*.

Пример. 57 и 37 при делении на 5 дают один и тот же остаток 2, следовательно, они сравнимы по модулю 5:

$$57 \equiv 37 \pmod{5}.$$

Введенное понятие сравнимости находит свое оправдание в том, что во многих арифметических вопросах основную роль играют не числа сами по себе, а те остатки, которые получаются при их делении на третье число. Сравнимые числа по данному модулю в неко-

тором смысле «равны» между собою, а сравнения во многом подобны равенствам.

Чтобы изучить свойства сравнений и научиться бегло ими пользоваться, необходимо установить удобную связь нового аппарата с обычными для нас соотношениями и понятиями.

Такая связь устанавливается при помощи формул (2).

Из них следует

$$a - b = m(q - q_1) = mt,$$

или

$$a = b + mt, \quad (4)$$

где t целое число.

Пусть теперь, наоборот, имеет место (4), а b при делении на m дает остаток r , т. е. $b = mq_1 + r$. Тогда и a при делении на m даст тот же остаток r . В самом деле, из (4) следует

$$a = mq_1 + r + mt = m(q_1 + t) + r,$$

где $q_1 + t$ целое число. Обозначая его через q , имеем

$$a = mq + r.$$

Итак, мы установили эквивалентность (3) и (4). Но (4) эквивалентно соотношению

$$a - b = mt,$$

или

$$a - b \mid m. \quad (5)$$

Поэтому соотношения (3), (4) и (5) между собою эквивалентны: (3) \leftrightarrow (4) \leftrightarrow (5).

В рассмотренном выше примере имеем

$$57 = 37 + 5 \cdot 4,$$

а также

$$57 - 37 \mid 5.$$

Отметим в заключение следующие очевидные, но тем не менее важные факты:

1) если a при делении на m дает остаток r , т. е.

$$a = mq + r,$$

то

$$a \equiv r \pmod{m};$$

2) если a делится на m , т. е. $a \mid m$,

$$a \equiv 0 \pmod{m},$$

то

или, другими словами, кратное модуля сравнимо с нулем по данному модулю:

$$mk \equiv 0 \pmod{m}.$$

2. Основные свойства сравнений

1. *Соотношение сравнимости: а) рефлексивно, б) симметрично и в) транзитивно:*

а) из $a = b$ следует $a \equiv b \pmod{m}$, т. е. равные числа сравнимы по любому модулю.

Рефлексивность можно выразить и так:

$$a \equiv a \pmod{m};$$

б) из $a \equiv b \pmod{m}$ следует $b \equiv a \pmod{m}$;

в) из $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ следует
 $a \equiv c \pmod{m}$.

Все перечисленные свойства непосредственно вытекают из определения сравнимости, или равноостаточности;

2. *Сравнения с одним и тем же модулем можно почленно складывать и вычитать,*

т. е. из $a_1 \equiv b_1 \pmod{m}$ и $a_2 \equiv b_2 \pmod{m}$ следует

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}.$$

В самом деле, из условий имеем

$$a_1 = b_1 + mt_1, \quad a_2 = b_2 + mt_2,$$

откуда

$$a_1 \pm a_2 = b_1 \pm b_2 + m(t_1 \pm t_2),$$

или, в силу (3) \leftrightarrow (4)

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}.$$

Доказанное свойство, очевидно, распространяется и на случай k сравнений.

Следствия: А. Слагаемое можно из одной части сравнения перенести в другую, если изменить его знак.

Действительно, из

$$a + b \equiv c \pmod{m} \text{ и}$$

$$-b \equiv -b \pmod{m}$$

следует

$$a \equiv c - b \pmod{m}.$$

Б. К любой части сравнения можно прибавить число, кратное модулю. Действительно, из

$$a \equiv b \pmod{m} \text{ и } 0 \equiv mk \pmod{m}$$

следует

$$a \equiv b + mk \pmod{m},$$

где $k = 0, \pm 1, \pm 2, \dots$

3. Сравнения с одним и тем же модулем можно почленно перемножать, т. е.

из

$$a_1 \equiv b_1 \pmod{m} \text{ и}$$

$$a_2 \equiv b_2 \pmod{m}$$

следует

$$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

Для доказательства выражаем данные условия в форме

$$a_1 = b_1 + mt_1, \quad a_2 = b_2 + mt_2,$$

тогда

$$a_1 \cdot a_2 = (b_1 + mt_1)(b_2 + mt_2).$$

В произведении этих сумм все члены, кроме $b_1 \cdot b_2$, содержат сомножитель m , поэтому

$$a_1 \cdot a_2 = b_1 \cdot b_2 + mt, \text{ где } t \text{ — целое,}$$

или

$$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

Очевидно, это свойство распространяется на случай k сравнений.

Следствия. А. Сравнение можно почленно возвышать в любую целую положительную степень, т. е. из

$$a \equiv b \pmod{m}$$

следует

$$a^n \equiv b^n \pmod{m}.$$

Б. Обе части сравнения можно умножать на одно и то же целое число k , т. е. из

$$a \equiv b \pmod{m}$$

следует

$$ak \equiv bk \pmod{m}.$$

Это свойство получается, если данное сравнение почленно умножить на сравнение $k \equiv k \pmod{m}$.

В. Сложение и умножение сравнений приводит к следующему, легко понятному обобщению: выражения, составленные сложением (алгебраическим) и умножением сравнимых по модулю m чисел, сравнимы по этому же модулю.

В частности, если

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$$

— многочлен с целыми коэффициентами, то из

$$x \equiv y \pmod{m} \text{ следует } f(x) \equiv f(y) \pmod{m};$$

если, кроме того,

$$a_i \equiv b_i \pmod{m}, \quad i = 0, 1, \dots, n,$$

то

$$a_0x^n + \dots + a_n \equiv b_0y^n + \dots + b_n \pmod{m}.$$

Рассматриваемое свойство показывает также, что в сравнении по модулю m можно слагаемые и множители заменить сравнимыми числами по тому же модулю.

Так, например, по модулю m из $a + b \equiv c$ и $b \equiv d$ следует $a + d \equiv c$, из $ac + b \equiv 0$ и $c \equiv e$ следует $ae + b \equiv 0$.

Однако необходимо обратить внимание на то, что встречающиеся в сравнении показатели указанным образом заменять нельзя.

Так, например, $3 \equiv 8 \pmod{5}$, однако $2^3 \not\equiv 2^8 \pmod{5}$, так как $2^3 \equiv 3 \pmod{5}$, а $2^8 \equiv 1 \pmod{5}$.

4. На общий делитель, взаимно простой с модулем, можно всегда разделить обе части сравнения, сохраняя при этом данный модуль.

Действительно, пусть

$$ad \equiv bd \pmod{m} \text{ и } (d, m) = 1,$$

тогда

$$ad - bd \mid m, \text{ или } (a - b)d \mid m,$$

откуда, ввиду того что $(d, m) = 1$, следует

$$a - b \mid m \text{ или } a \equiv b \pmod{m}.$$

Если условие взаимной простоты делителя с модулем не выполнено, то сокращение может привести

к числам, не сравнимым по данному модулю, но это не обязательно.

Так, например, $7 \cdot 5 \equiv 4 \cdot 5 \pmod{15}$, но $7 \not\equiv 4 \pmod{15}$, однако $17 \cdot 5 \equiv 2 \cdot 5 \pmod{15}$ и $17 \equiv 2 \pmod{15}$.

5. Обе части сравнения и модуль можно умножить на одно и то же целое положительное число, а также разделить на любой их общий положительный делитель: если целое $d > 0$, то из $a \equiv b \pmod{m}$ следует

$$ad \equiv bd \pmod{md}.$$

Справедливо также и обратное утверждение.

Доказательство. Пусть $a \equiv b \pmod{m}$, тогда

$$a - b \mid m,$$

следовательно, $(a - b) \cdot d \mid m \cdot d$ или $ad - bd \mid md$, т. е.

$$ad \equiv bd \pmod{md}.$$

Второе утверждение получается, если рассуждения провести в обратной последовательности.

Согласно свойствам 4 и 5 из

$$ad \equiv bd \pmod{m}$$

всегда следует $a \equiv b \pmod{\frac{m}{(d, m)}}$.

Действительно, пусть $(d, m) = k$, $d = d_1 k$, $m = m_1 k$.

Тогда первое сравнение можно записать в виде

$$ad_1 k \equiv bd_1 k \pmod{m_1 k},$$

откуда по 5-му свойству $ad_1 \equiv bd_1 \pmod{m_1}$

и далее по 4-му свойству $a \equiv b \pmod{m_1}$,

или $a \equiv b \pmod{\frac{m}{(d, m)}}$.

6. Если сравнение имеет место по нескольким модулям, то оно имеет место по модулю, равному общему наименьшему кратному этих модулей.

В самом деле, пусть

$$a \equiv b \pmod{m_1} \text{ и } a \equiv b \pmod{m_2},$$

тогда

$$a - b \mid m_1 \text{ и } a - b \mid m_2,$$

откуда

$$a - b \mid M, \text{ где } M = [m_1, m_2],$$

или

$$a \equiv b \pmod{M}.$$

Очевидно, свойство остается верным и для нескольких модулей.

7. Если сравнение имеет место по модулю m , то оно имеет место и по модулю d , равному любому делителю числа m : если $m \mid d$, то из $a \equiv b \pmod{m}$ следует

$$a \equiv b \pmod{d}.$$

Действительно, из условия следует, что $a - b \mid m$, а так как $m \equiv m_1 \cdot d$, то $a - b \mid d$, т. е. $a \equiv b \pmod{d}$.

8. Общий делитель одной части сравнения и модуля является также делителем второй части.

Действительно, если

$$a \equiv b \pmod{m} \text{ и } a = a_1 \cdot d, \quad m = m_1 \cdot d,$$

то $a = b + mt$, или $a_1 d - m_1 d t = b$, откуда видно, что $b \mid d$.

Доказанное свойство показывает, что все делители пар чисел a и m , а также b и m являются общими. Это относится и к их общим наибольшим делителям. Таким образом, мы приходим к важному следствию.

Части сравнения и модуль имеют одинаковый общий наибольший делитель, т. е. $(a, m) = (b, m)$.

В частности, если $(a, m) = 1$, то и $(b, m) = 1$.

Другими словами, если одна часть сравнения и модуль числа взаимно простые, то и вторая часть сравнения и модуль числа взаимно простые.

Рассмотрим числовой пример на применение основных свойств сравнений.

Так как $10 \equiv 1 \pmod{3}$, то

$$N = a_0 + 10 \cdot a_1 + \dots + 10^n a_n \equiv a_0 + a_1 + \dots + a_n \pmod{3}.$$

Отсюда следует, что число делится на 3 тогда и только тогда, когда сумма цифр делится на 3.

Аналогично можно вывести и другие признаки делимости (см. § 1, гл. V).

Упражнения

41. Записать в виде сравнений условия:

1) -38 и -3 дают при делении на 7 одинаковые остатки (проверить!); 2) при делении на 8 число 53 дает остаток 5; 3) $a^2 - b^2$

делится на $a - b$ ($a \neq b$); 4) определить остаток r от деления -73 на 8 .

42. Охарактеризовать сравнениями числа N следующего вида:
1) четные; 2) нечетные; 3) $5k + 3$; 4) $7k - 2$.

43. Указать наименьшее натуральное n , чтобы выполнялось условие $n \equiv 0 \pmod{m}$.

44. От деления на m целые числа a_1 и a_2 дают соответственно остатки r_1 и r_2 . Какие остатки получаются от деления на m суммы, разности и произведения данных чисел?

45. Сохранится ли сравнение $abc + d - e + f \equiv g^2 \pmod{m}$, если заменить в нем b через b_1 , f через f_1 и g через g_1 при условии, что $b \equiv b_1 \pmod{m}$, $f \equiv f_1 + 3m$, $g \equiv -g_1 \pmod{m}$?

46. Какому необходимому условию должны удовлетворять целые t , чтобы выполнялось сравнение $5t \equiv 3b \pmod{6m}$?

47. Каков остаток, получаемый от деления целых чисел (в десятичной системе) на: 1) 9 ; 2) 11 ?

48. Доказать, что из условий $a \equiv b \pmod{m}$, $(a, b) = d$, $(a, m) = 1$ следует $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d_1}}$.

49. Доказать, что для простого p $C_{p-1}^k \equiv (-1)^k \pmod{p}$.

50. Доказать, что при нечетном m $(m-1)! \equiv (-1)^{\frac{m-1}{2}} \times \times \left[\left(\frac{m-1}{2} \right)! \right]^2 \pmod{m}$. Записать это соотношение для случаев $m = 4k + 1$, $m = 4k + 3$.

§ 2. Классы по данному модулю

1. Разбиение множества целых чисел на классы

Соотношение сравнимости по данному модулю m , которое мы начали изучать в § 1, можно выразить иным образом.

Для этого объединим все целые числа, которые при делении на m дают один и тот же остаток r , в один класс, обозначив его через C_r .

Тогда в зависимости от возможных m остатков

$$0, 1, 2, \dots, m-1$$

при делении на m все целые числа разбиваются на m классов

$$C_0, C_1, C_2, \dots, C_{m-1},$$

которые мы называем *классами вычетов по модулю m* .

Согласно теореме существования и единственности частного и остатка понятно, что разные классы вы-

четов по модулю m не имеют общих элементов, так что получается распределение на непересекающиеся классы.

Числа класса C_r имеют форму $mq + r$, и все их можно получить, если в этой форме q принимает все возможные целые значения.

Так, например, по модулю 10 все числа класса, дающие остаток 3, имеют вид $10q + 3$, где $q = 0, \pm 1, \pm 2, \dots$, т. е. представляются рядом чисел

$$\dots - 27, -17, -7, 3, 13, 23, \dots$$

Очевидно, числа сравнимы по модулю m тогда и только тогда, когда они принадлежат одному и тому же классу вычетов по модулю m .

Числа одного и того же класса называются *вычетами этого класса*.

2. Сложение и умножение классов

Если из двух классов C_k и C_l (необязательно разных) выбрать по вычету и сложить их или перемножить, то всегда получим вычеты вполне определенных классов.

Действительно, пусть выбранные представители $mq_1 + k$ и $mq_2 + l$. Тогда при сложении имеем

$$(mq_1 + k) + (mq_2 + l) = mq + k + l, \quad q = q_1 + q_2.$$

Если $k + l < m$, то полученное число принадлежит классу C_{k+l} ; если $k + l \geq m$, то полученное число можно представить в виде $m(q + 1) + k + l - m$ с условием $0 \leq k + l - m < m$, а это означает, что оно принадлежит классу C_{k+l-m} .

Чтобы узнать, к какому классу принадлежит произведение $(mq_1 + k) \cdot (mq_2 + l)$, надо найти остаток r при его делении на m . Этот остаток, очевидно, равен остатку от деления kl на m , так как остальные члены произведения делятся на m . Таким образом, r определяется условием

$$kl = mq + r,$$

а произведение принадлежит классу C_r .

Пример. По модулю 10 два любых вычета соответственно из классов C_3 и C_4 в сумме всегда дают

вычет из класса C_7 , а в качестве произведения — вычет из класса C_2 .

$$13 + 24 = 37, \quad -27 + 14 = -13 \text{ и}$$

$$13 \times 24 = 312, \quad -27 \times 14 = -378.$$

Указанный факт выражает в новой форме известные свойства сравнений, установленные ранее при их почленном сложении и умножении. В самом деле, в результате почленного сложения (умножения) сравнений сравнимые по модулю m числа переходят в сравнимые по тому же модулю, а это как раз означает, что произвольно выбранным представителям из двух классов сопоставляется представитель определенного класса в качестве их суммы (произведения).

Отмеченные выше равенства можно на языке сравнений выразить следующим образом:

$$\begin{array}{rcl} 13 & \equiv & -27 \pmod{10} \\ 24 & \equiv & 14 \pmod{10}, \end{array}$$

$$\begin{array}{rcl} \text{откуда при сложении} & 37 & \equiv -13 \pmod{10}, \\ \text{а при умножении} & 312 & \equiv -378 \pmod{10}. \end{array}$$

На основании полученных результатов можно естественным образом ввести операции сложения и умножения для классов вычетов, а именно:

$$C_k + C_l = \begin{cases} C_{k+l}, & \text{если } k+l < m, \\ C_{k+l-m}, & \text{если } k+l \geq m \end{cases}$$

и $C_k \cdot C_l = C_r$ с условием $k \cdot l = m \cdot q + r$, $0 \leq r < m$.

Определенные таким образом суммы и произведения классов существуют и единственны.

3. Кольцо классов

Во множестве классов вычетов по модулю m , которое обозначим через M , нами определены две операции сложения и умножения.

При этом сложение и умножение коммутативны и ассоциативны, выполняется также дистрибутивный закон умножения относительно сложения, так как все эти свойства имеют место при сложении и умножении вычетов.

Кроме того, в M существует нулевой элемент, а именно $-C_0$, так как $C_k + C_0 = C_k$ и, наконец, для

каждого элемента C_k из M существует противоположный элемент $C_{-k} = C_{m-k}$, так как $C_k + C_{m-k} = C_0$.

Таким образом, M удовлетворяет условиям коммутативного кольца.

Если модуль m число составное, то M обладает одной особенностью, которой числовые кольца не имеют, а именно: в M существуют тогда ненулевые элементы, произведение которых равно нулевому элементу. Их называют делителями нуля.

Так, например, по модулю 10

$$C_2 \cdot C_5 = C_0, \quad C_8 \cdot C_5 = C_0.$$

Делителями нуля в M по составному модулю m являются те элементы $C_{\bar{k}}$, для которых $(\bar{k}, m) = d > 1$, так как для них можно найти такой элемент $C_{\bar{l}}$, $\bar{l} \neq 0$, что $C_{\bar{k}} \cdot C_{\bar{l}} = C_0$.

Действительно, если возьмем $\bar{l} = \frac{m}{d}$, то $\bar{k} \cdot \bar{l} = \frac{\bar{k} \cdot m}{d} = [\bar{k}, m]$, т. е. равно общему наименьшему кратному \bar{k} и m , которое, конечно, делится на m . Рассмотренные примеры подтверждают полученный результат.

Заметим в заключение, что кольцо классов M по составному модулю не может образовать поля. Дело в том, что в поле не могут существовать делители нуля. В самом деле, в поле для каждого ненулевого элемента a существует обратный элемент a^{-1} с условием $a \cdot a^{-1} = 1$ (единичный элемент). Поэтому при $a \neq 0$ из условия $ab = 0$ умножением обеих сторон на a^{-1} получаем

$$(a^{-1} \cdot a) \cdot b = a^{-1} \cdot 0,$$

откуда следует, ввиду $a^{-1} \cdot a = 1$, $1 \cdot b = b$ и $a^{-1} \cdot 0 = 0$,
 $b = 0$.

Упражнения

51. Каким классам вычетов по модулю 6 принадлежат все простые числа $p > 3$? Охарактеризовать вычеты этих классов формами и сравнениями.

52. Доказать, что произведения вычетов одного класса по модулю m на одно и то же целое число принадлежат одному классу вычетов по модулю m .

53. Принадлежат ли в предыдущей задаче произведения тому же самому классу, что и данные вычеты?

54. Пусть два вычета из одного класса по модулю m нацело делятся на n . Принадлежат ли частные также одному классу вычетов по модулю m ?

55. Скольким классам вычетов по модулю 20 ($M = dm$) принадлежат вычеты из одного класса по модулю 10 (m)?

56. Найти: 1) сумму и произведение классов C_7 и C_9 по модулю 13; 2) класс, противоположный классу C_{19} по модулю 27.

57. Какие классы по модулю 10 являются делителями нуля?

§ 3. Системы вычетов

1. Полная система вычетов

Если из каждого класса по модулю m взять по одному представителю, то полученную систему чисел называют *полной системой вычетов по модулю m* .

Так, например, чтобы составить полную систему вычетов по модулю 10, мы должны взять по одному представителю из классов, числа которых характеризуются следующими формами:

$$10q + 0, 10q + 1, 10q + 2, \dots, 10q + 9,$$

например, вычеты

$$20, 31, 112, \dots - 31.$$

Чаще всего пользуются наименьшими неотрицательными вычетами, которые получаются, когда в форме $mq + r$ число q принимает значение 0. В таком случае вычеты равны остаткам r , так что полная система наименьших неотрицательных вычетов по модулю m имеет вид

$$0, 1, 2, \dots, m - 1;$$

по модулю 10 это будут числа

$$0, 1, 2, \dots, 9.$$

Иногда удобно рассматривать полную систему наименьших положительных вычетов по модулю m

$$1, 2, 3, \dots, m.$$

Часто применяется также полная система абсолютно наименьших вычетов по модулю m . По четному модулю 10 она имеет вид

$$0, 1, 2, 3, 4, 5, -4, -3, -2, -1,$$

или

$$0, \pm 1, \pm 2, \pm 3, \pm 4, 5,$$

а по нечетному модулю 13

$$0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6,$$

в общем случае по четному модулю m имеем

$$0, \pm 1, \pm 2, \dots, \pm \left(\frac{m}{2} - 1\right), \frac{m}{2},$$

а по нечетному

$$0, \pm 1, \pm 2, \dots, \pm \frac{m-1}{2}.$$

2. Признак полной системы вычетов

Возникает вопрос, когда можно о некоторой системе чисел утверждать, что она образует полную систему вычетов по модулю m ? Легко понять, что система из m несравнимых между собой по модулю m чисел образует такую систему.

В самом деле: 1) поскольку эти числа несравнимы по модулю m , они должны принадлежать разным классам по этому модулю, 2) поскольку их число равно m , они должны принадлежать m разным классам. Но вообще-то классов имеется всего m , следовательно, из каждого класса имеется по одному представителю, что и требуется для полной системы вычетов.

3. Первая теорема о вычетах линейной формы

Установленный признак для полной системы вычетов дает нам возможность доказать важную теорему, которую будем называть первой теоремой о вычетах линейной формы.

Если в линейной форме $ax + b$ число x пробегает все значения из полной системы вычетов по модулю m при $(a, m) = 1$ и произвольном b , то и $ax + b$ пробегает все значения полной системы вычетов по модулю m .

Действительно, полученная система чисел состоит: 1) из m чисел, так как вместо x мы подставляем m значений; остается еще доказать, что 2) полученные числа будут принадлежать разным классам, другими словами, что они несравнимы по модулю m .

Предположим противное, а именно, что для двух значений x_1 и x_2 из разных классов получаются сравнимые значения для $ax + b$ по модулю m , т. е., что

$$ax_1 + b \equiv ax_2 + b \pmod{m}.$$

Тогда

$$ax_1 \equiv ax_2 \pmod{m}$$

и в силу

$$(a, m) = 1, \quad x_1 \equiv x_2 \pmod{m}.$$

Получается противоречие с условием, что и доказывает нашу теорему.

4. Приведенная система вычетов. Функция Эйлера

Из 8-го свойства сравнений нам известно, что сравнимые числа по модулю m , т. е. вычеты одного класса по модулю m — имеют с ним один и тот же общий наибольший делитель. Следовательно, если один вычет класса взаимно прост с модулем, то такими же будут все вычеты этого класса. Поэтому можно говорить о классах вычетов по модулю m , взаимно простых с этим модулем. Их совокупность играет большую роль в теории чисел.

Если из каждого класса упомянутой совокупности взять по одному представителю, то получается так называемая *приведенная система вычетов по модулю m* .

Из определения следует, что приведенную систему вычетов можно составить, исходя из полной системы вычетов (взятой в какой-либо форме), выделяя из нее те вычеты, которые взаимно просты с модулем.

При этом из полной системы наименьших неотрицательных или наименьших положительных вычетов получается приведенная система наименьших положительных вычетов, а из полной системы абсолютно наименьших вычетов — приведенная система абсолютно наименьших вычетов. По модулю 10, например, указанные приведенные системы имеют соответственно следующий вид:

$$\begin{aligned} &1, 3, 7, 9, \\ &1, 3, -3, -1. \end{aligned}$$

Важный вопрос о числе вычетов в приведенной системе по модулю m решается при помощи функции Эйлера $\varphi(m)$, с которой мы уже ознакомились в введении.

Функция Эйлера $\varphi(m)$ определяется для всех целых положительных m как число целых положительных чисел, не превосходящих m и взаимно простых с m , или как число чисел ряда

$$0, 1, 2, \dots, m-1$$

взаимно простых с m .

Из определения видно, что в приведенной системе вычетов по модулю m имеется как раз $\varphi(m)$ чисел.

Заметим, что значение $\varphi(m)$ характеризует также число классов вычетов по модулю m , взаимно простых с этим модулем.

5. Признак приведенной системы вычетов

Мы сейчас убедимся в справедливости следующего признака: Система 1) из $\varphi(m)$ чисел,

2) несравнимых между собой по модулю m , (т. е. принадлежащих разным классам по этому модулю) и

3) взаимно простых с модулем m , образует приведенную систему вычетов по модулю m .

В самом деле, поскольку эти числа взаимно просты с модулем, они принадлежат классам вычетов, взаимно простым с модулем, причем, согласно второму условию, разным таким классам. Наконец, поскольку имеется $\varphi(m)$ чисел, т. е. столько же, сколько классов вычетов, взаимно простых с модулем, то в нашей системе чисел должен быть представлен каждый из этих классов, причем единственным образом, что и доказывает наше утверждение.

6. Вторая теорема о вычетах линейной формы

Признак приведенной системы вычетов дает нам возможность доказать теорему, которую будем называть второй теоремой о вычетах линейной формы.

Если в линейной форме ax число x пробегает все значения из приведенной системы вычетов по модулю m при $(a, m) = 1$, то и ax принимает все значения из приведенной системы вычетов по модулю m .

Действительно, мы получаем:

1) $\varphi(m)$ чисел, так как вместо x подставляем $\varphi(m)$ чисел;

2) эти числа принадлежат по модулю m разным классам, так как вместо x берутся числа из разных классов, а в таком случае (как это было показано в доказательстве первой теоремы о вычетах линейной формы) числа ax (даже $ax + b$) должны быть по модулю m несравнимыми;

3) наконец, числа ax взаимно просты с m , так как сомножители в отдельности взаимно просты с m , а именно, по условию $(a, m) = 1$, кроме того, $(x, m) = 1$, так как x — вычет из приведенной системы.

Таким образом, система чисел ax , как это установлено в признаке, образует приведенную систему вычетов по модулю m .

Важно обратить внимание на то, что, хотя вместе взятые вычеты x , а также числа ax , образуют приведенные системы по одному и тому же модулю, тем не менее отдельные значения x и соответствующие им ax , вообще говоря, принадлежат различным классам. Действительно, так как здесь $(x, m) = 1$, то сравнение $ax \equiv x \pmod{m}$ может выполняться тогда и только тогда, когда $a \equiv 1 \pmod{m}$.

Если, в частности, вычеты чисел ax взять в той же форме, в которой даны вычеты x (например, в обоих случаях пользоваться наименьшими положительными вычетами), то в совокупности получатся одинаковые системы чисел, однако соответствующие их значения будут, вообще говоря, разные.

Пусть, например, $a = 5$, $m = 14$. Условие $(a, m) = 1$ выполняется. Выразим приведенную систему вычетов по модулю 14 через наименьшие положительные вычеты и найдем также наименьшие положительные вычеты чисел ax .

Тогда имеем

$$x = 1, 3, 5, 9, 11, 13$$

и далее по модулю 14

$$\begin{aligned}5 \cdot 1 &\equiv 5 \\5 \cdot 3 &= 15 \equiv 1 \\5 \cdot 5 &= 25 \equiv 11 \\5 \cdot 9 &= 45 \equiv 3 \\5 \cdot 11 &= 55 \equiv 13 \\5 \cdot 13 &= 65 \equiv 9.\end{aligned}$$

В этом примере x пробегает наименьшие положительные значения вычетов, взаимно простых с модулем 14, т. е. последовательность чисел 1, 3, 5, 9, 11 и 13, а наименьшие положительные вычеты соответствующих чисел ax принимают значения 5, 1, 11, 3, 13 и 9, т. е. те же значения, но расположенные по-иному.

Упражнения

58. Составить по модулям 14 и 15 полные и приведенные системы наименьших неотрицательных, наименьших положительных и абсолютно наименьших вычетов.

59. Записать приведенные системы наименьших положительных и абсолютно наименьших вычетов по простому модулю $p > 2$.

60. Чем отличается приведенная система вычетов по простому модулю p от полной системы вычетов по такому модулю?

61. Система чисел $3^1, 3^2, \dots, 3^6$ составляет приведенную систему вычетов по модулю 7. Проверить.

62. Составить наименьшие положительные вычеты линейных форм 1) $5x$ и 2) $5x + 7$ по модулю 9, когда x пробегает полную систему наименьших положительных вычетов по модулю 9. Сравнить полученные системы чисел с исходной.

63. Показать, что члены арифметической прогрессии $a, a + d, \dots, a + d(n-1)$ образуют полную систему вычетов по модулю n , если $(d, n) = 1$.

64. Показать, что числа $2, 4, \dots, 2m$ составляют полную систему вычетов по модулю m , если m нечетно.

65. Составить при помощи чисел, кратных 3, 1) полную систему вычетов по модулю 11 и 2) приведенную систему вычетов по модулю 8.

66. В линейной форме ax число x пробегает все значения из полной системы вычетов по модулю m , причем $(a, m) = d$. Сколько чисел полученной системы делится на m ?

§ 4. Основные свойства функции Эйлера

1. Мультипликативность функции Эйлера

Прежде чем заняться вычислением функции Эйлера $\varphi(m)$, определение которой дано в предыдущем параграфе, докажем одно важное ее свойство, а именно — мультипликативность.

Функция $f(m)$ называется мультипликативной, если:

- 1) она определена для всех натуральных n и хотя бы для одного такого n отлична от нуля;
- 2) для любых взаимно простых n_1 и n_2

$$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2).$$

Для функции Эйлера первое условие выполняется согласно определению. Таким образом, остается доказать, что

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n), \text{ если } (m, n) = 1.$$

Для доказательства расположим числа от 1 до mn в виде следующей таблицы:

$$\begin{array}{ccc} 1, \dots, & k, \dots, & m \\ m+1, \dots, & m+k, \dots, & 2m \\ \dots & \dots & \dots \\ (n-1)m+1, \dots, & (n-1)m+k, \dots, & (n-1)m+m=mn \end{array}$$

Чтобы найти $\varphi(m \cdot n)$, мы должны узнать сколько в этой таблице имеется чисел, взаимно простых с mn . Но взаимно простыми с произведением mn являются те и только те числа, которые взаимно просты как с m , так и с n . Поэтому отберем из этой таблицы сначала все числа, взаимно простые с m , а из них те, которые взаимно просты с n .

Числа одного столбца принадлежат одному классу вычетов по модулю m , поэтому все эти числа имеют с m одинаковый Н. О. Д.: если одно из них взаимно простое с m , то и все остальные тоже взаимно простые с m . Таким образом, можно говорить о «столбцах взаимно простых с m » и судить о количестве таких столбцов по количеству чисел взаимно простых с m одной строки, например первой. Очевидно, поэтому «столбцов взаимно простых с m », будет $\varphi(m)$.

Рассмотрим теперь любой столбец таблицы, например:

$$k, m+k, 2m+k, \dots, (n-1)m+k.$$

Числа этого столбца можно рассматривать как значения линейной функции $mx + k$, когда x пробегает полную систему вычетов $0, 1, 2, \dots, n-1$ по модулю n .

Так как по условию $(m, n) = 1$, то получается такая совокупность чисел, которая независимо от k образует полную систему вычетов по модулю n и содержит поэтому $\varphi(n)$ чисел, взаимно простых с n .

Итак, любой столбец нашей таблицы содержит $\varphi(n)$ чисел, взаимно простых с n .

Таким образом, всего в таблице имеется $\varphi(m) \cdot \varphi(n)$ чисел, взаимно простых как с m , так и с n , а следовательно, и с mn , так что

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Полученное свойство остается, очевидно, справедливым для любого числа попарно простых сомножителей.

2. Формула для вычисления $\varphi(m)$

Пусть, во-первых, $m = p$ число простое.

Тогда, очевидно, $\varphi(p) = p - 1$.

Пусть, далее, $m = p^a$. Для определения $\varphi(p^a)$ мы должны рассмотреть ряд чисел от 1 до p^a , который запишем в следующем виде:

$$1, 2, \dots, p, \dots, 2p, \dots, 3p, \dots, p \cdot p, \dots, p^{a-1} \cdot p = p^a.$$

Ясно, что этот ряд содержит p^{a-1} чисел, которые делятся на p и, таким образом, не являются взаимно простыми с p^a ; остальные числа этого ряда взаимно простые с p^a .

Их число, следовательно:

$$\varphi(p^a) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right).$$

Пусть, наконец, m — произвольное натуральное число и его каноническое разложение

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Тогда, по свойству мультипликативности,

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}).$$

Следовательно,

$$\varphi(m) = p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right),$$

$$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right),$$

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

или

$$\varphi(m) = p_1^{\alpha_1-1} (p_1 - 1) p_2^{\alpha_2-1} (p_2 - 1) \dots p_k^{\alpha_k-1} (p_k - 1).$$

На практике удобно пользоваться последней формулой.

Пример: $m = 360 = 2^3 \cdot 3^2 \cdot 5$.

$$\varphi(360) = 2^2 \cdot (2 - 1) \cdot 3(3 - 1) \cdot (5 - 1) = 96.$$

3. Сумма значений функции Эйлера, распространенная по всем делителям данного числа

Рассмотрим теперь сумму значений функции Эйлера, распространенную по всем делителям d данного числа m , и запишем ее в виде $\sum_m \varphi(d)$.

Докажем, что $\sum_m \varphi(d) = m$.

Так, например, для $m = 12$ имеем

$$\begin{aligned} \sum_{12} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12. \end{aligned}$$

Доказательство. Пусть каноническое разложение m имеет вид

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad (1)$$

где p_1, p_2, \dots, p_k разные простые делители m .

Тогда можно утверждать, что все делители числа m исчерпываются всеми числами вида

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \quad (2)$$

где

$$0 \leq \beta_1 \leq \alpha_1, \quad 0 \leq \beta_2 \leq \alpha_2, \quad \dots, \quad 0 \leq \beta_k \leq \alpha_k \quad (3)$$

(см. п. 2, § 4, гл. I).

Поэтому имеет место следующее тождество:

$$\sum_m \varphi(d) = (1 + \varphi(p_1) + \dots + \varphi(p_1^{\alpha_1})) (1 + \varphi(p_2) + \dots + \varphi(p_2^{\alpha_2})) \dots (1 + \varphi(p_k) + \dots + \varphi(p_k^{\alpha_k})),$$

так как в качестве слагаемых произведения мы получаем все числа вида

$$\varphi(p_1^{\beta_1}) \cdot \varphi(p_2^{\beta_2}) \dots \varphi(p_k^{\beta_k}) = \varphi(p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_k^{\beta_k}),$$

где

$$0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_k \leq \alpha_k,$$

т. е. значения функции Эйлера для всех делителей числа m . Но

$$1 + \varphi(p_k) + \varphi(p_k^2) + \dots + \varphi(p_k^{\alpha_k}) = \\ = 1 + (p_k - 1) + (p_k^2 - p_k) + \dots + (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = p_k^{\alpha_k}.$$

Следовательно:

$$\sum_m \varphi(d) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k} = m. \text{ Теорема доказана.}$$

Упражнения

67. Сколько имеется правильных несократимых дробей $\frac{a}{b} > 0$: 1) при фиксированном знаменателе b , 2) если $1 < b \leq n$?

68. Найти число вычетов приведенной системы по модулям: 1) 540, 2) 2240, 3) 13·17, 4) 9·15·42.

69. Найти n : 1) вида 5^α , если $\varphi(n) = 100$; 2) вида $3^\alpha \cdot 5^\beta$, если $\varphi(n) = 600$.

70. Представить выражение $\frac{\varphi(m)}{m}$, где $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, в виде суммы, пользуясь формулой

$$\frac{\varphi(m)}{m} = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

71. Сколько имеется натуральных чисел: 1) ≤ 385 , взаимно простых с 77, 2) $\leq mk$, взаимно простых с m ?

72. Сколько имеется чисел, взаимно простых 1) с 24 среди чисел 301, 302, ..., 540, 2) с 35 среди чисел 436, 437, ..., 750?

73. Сколько имеется чисел, взаимно простых с n , в арифметической прогрессии $a, a + d, \dots, a + (2n - 1)d$, если $(d, n) = 1$?

74. Для каких n $\varphi(2n) = \varphi(n)$?

75. Доказать: 1) что $\varphi(m)$ четно, если $m > 2$; 2) что для $m > 1$ сумма натуральных чисел, меньших m и взаимно простых с m , равна $\frac{1}{2} m \cdot \varphi(m)$.

76. Найти: 1) количество натуральных чисел $\leq n$, имеющих с n Н. О. Д. d ; 2) применить полученную формулу к случаям, когда n и d соответственно равны: а) 624 и 12; б) 580 и 20; в) 595 и 17.

77. Пусть n имеет делители d_1, d_2, \dots, d_k ; в совокупности они совпадают с соответствующими им дополнительными делителями d'_1, d'_2, \dots, d'_k для которых $d_i \cdot d'_i = n$ и $d_i = \frac{n}{d'_i}$.

Согласно решению предыдущей задачи $\varphi(d_i) = \varphi\left(\frac{n}{d'_i}\right) = \varphi_{d'_i}(n)$. Пользуясь соотношением $\varphi(d_i) = \varphi_{d'_i}(n)$, дать другое доказательство для $\sum_n \varphi(d_i) = n$.

§ 5. Теоремы Эйлера и Ферма

1. Теорема Эйлера

Если a и m числа взаимно простые, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Эту теорему мы докажем, пользуясь 2-й теоремой о вычетах линейной формы.

Возьмем линейную форму ax и подставим в нее вместо x вычеты приведенной системы по модулю m , взятые в форме наименьших положительных вычетов.

Если x пробегает значения

$$r_1, r_2, \dots, r_k, \quad k = \varphi(m),$$

то, как это подробно показано в конце § 3-го, наименьшие положительные вычеты соответствующих чисел ax

$$r'_1, r'_2, \dots, r'_k$$

образуют в совокупности такую же систему чисел. Итак,

$$ar_1 \equiv r'_1 \pmod{m},$$

$$ar_2 \equiv r'_2 \pmod{m},$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

$$ar_k \equiv r'_k \pmod{m},$$

откуда

$$a^k(r_1 r_2 \dots r_k) \equiv (r'_1 \cdot r'_2 \dots r'_k) \pmod{m}.$$

Но так как произведения $r_1 \cdot r_2 \dots r_k$ и $r'_1 \cdot r'_2 \dots r'_k$ по предыдущему равны и, кроме того, взаимно просты с модулем, ибо каждый их сомножитель взаимно прост с модулем, то можно обе части сравнения разделить на них, после чего получаем утверждение теоремы Эйлера $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Пример. Пусть $m = 9$, $a = 14$.

Тогда $\varphi(m) = \varphi(3^2) = 3^2 - 3 = 6$. Далее, так как $14 \equiv 5 \pmod{9}$, имеем $14^6 \equiv 5^6 \pmod{9}$. Но по модулю 9:

$$5^1 = 5, 5^2 = 25 \equiv -2, 5^4 \equiv 4, 5^6 \equiv -8 \equiv 1.$$

Итак,

$$14^{\varphi(9)} \equiv 1 \pmod{9}.$$

2. Теорема Ферма

Для частного случая, когда $m = p$ число простое, из теоремы Эйлера следует теорема Ферма: *если p число простое и $(a, p) = 1$, то $a^{p-1} \equiv 1 \pmod{p}$.*

Пример: пусть $p = 11$, $a = 8$. В силу того, что $8 \equiv -3 \pmod{11}$, имеем $8^{10} \equiv (-3)^{10} \pmod{11}$.

Но по модулю 11

$$(-3)^2 = 9 \equiv -2, (-3)^{10} \equiv (-2)^5 \equiv -32 \equiv 1.$$

Следовательно,

$$8^{10} \equiv 1 \pmod{11}.$$

Часто применяется следующее следствие из теоремы Ферма: для простого p и любого a

$$a^p \equiv a \pmod{p}.$$

В самом деле, по теореме Ферма

$$a^{p-1} - 1 \mid p \text{ при } (a, p) = 1.$$

С другой стороны,

$$a \mid p \text{ при } (a, p) \neq 1;$$

поэтому при любом a произведение

$$a(a^{p-1} - 1) \mid p,$$

или

$$a^p - a \mid p,$$

т. е.

$$a^p \equiv a \pmod{p}.$$

В заключение заметим, что предложение, обратное теореме Ферма, не имеет места, т. е. в случае, когда при $(a, n) = 1$

$$a^{n-1} \equiv 1 \pmod{n},$$

нельзя еще утверждать, что n число простое.

Так, например, $2^{341-1} \equiv 1 \pmod{341}$, однако $341 = 31 \cdot 11$.

Действительно,

$$2^{10} = 1024 \equiv 1 \pmod{341},$$

поэтому

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}.$$

3. Применение теорем Эйлера и Ферма

Теоремы Эйлера и Ферма имеют многочисленные применения. Рассмотрим примеры вычисления остатков при делении степеней на данное число.

Пример 1. Найти остаток при делении 2^{30} на 13. По теореме Ферма $2^{12} \equiv 1 \pmod{13}$, поэтому $2^{24} \equiv 1 \pmod{13}$; кроме того, $2^6 = 64 \equiv -1 \pmod{13}$. Следовательно,

$$2^{30} \equiv -1 \equiv 12 \pmod{13}.$$

Итак, искомый остаток равен 12.

Пример 2. Найти остаток при делении 3^{40} на 83.

Теорему Ферма для данного случая нельзя применить, так как $\varphi(83) = 82 > 40$. Поэтому следует найти такие 3^k , чтобы при возможно больших значениях k , $k \leq 40$, получались бы при делении на 83 по возможности меньшие остатки

$$3^4 = 81 \equiv -2 \pmod{83}; \quad 3^{40} \equiv (-2)^{10} \equiv 1024 \equiv \\ \equiv 28 \pmod{83}.$$

Итак, искомый остаток равен 28.

Пример 3. Найти остаток от деления 317^{259} на 15. Так как

$$317 \equiv 2 \pmod{15}, \text{ то } 317^{259} \equiv 2^{259} \pmod{15}.$$

По теореме Эйлера

$$2^{\varphi(15)} \equiv 1 \pmod{15},$$

но $\varphi(15) = 8$, поэтому $2^8 \equiv 1 \pmod{15}$.

Далее, $259 = 32 \cdot 8 + 3$,

$$2^{259} = (2^8)^{32} \cdot 2^3 \equiv 8 \pmod{15}.$$

Итак, 317^{259} при делении на 15 дает остаток 8.

Упражнения

78. Найти остаток от деления: 1) 3^{59} на 17; 2) 7^{67} на 12; 3) 317^{273} на 39; 4) 4^{50} на 67; 5) 267^{311} на 37; 6) 197^{157} на 35.

79. Найти остаток от деления: 1) 4^{113} на 92; 2) 6^{76} на 26; 3) 21^{83} на 24; 4) 35^{150} на 425.

80. Найти остаток от деления: 1) $3^{100} + 4^{100}$ на 7; 2) $5^{50} + 7^{70}$ на 9; 3) $3 \cdot 5^{75} + 4 \cdot 7^{100}$ на 132.

81. Найти последние две цифры в десятичном представлении: 1) 2^{153} , 2) 3^{219} .

82. Доказать, что 1) $a^{12} - 1$ делится на 7, если $(a, 7) = 1$; 2) $a^{12} - b^{12}$ делится на 65, если $(a, 65) = 1$ и $(b, 65) = 1$.

83. Доказать, что для простого p : 1) $(a + b)^p \equiv a^p + b^p \pmod{p}$; 2) $(c_1 + c_2 + \dots + c_n)^p \equiv c_1^p + c_2^p + \dots + c_n^p \pmod{p}$.

84. Соотношение 2) из предыдущей задачи получено при помощи малой теоремы Ферма; из 2), наоборот, следует малая теорема Ферма, если положить $c_1 = c_2 = \dots = c_n = 1$. Поэтому спрашивается, как получить 2) без помощи малой теоремы Ферма.

85. Показать, что $2^{n-1} \equiv 1 \pmod{n}$ для $n = 73 \cdot 37$.

86. Доказать, что 1) $1^{30} + 2^{30} + \dots + 10^{30} \equiv -1 \pmod{11}$; 2) $1^{k(p-1)} + 2^{k(p-1)} + \dots + (p-1)^{k(p-1)} \equiv -1 \pmod{p}$.

87. Доказать, что при нечетном простом p и $(a, p) = 1$ одно и только одно из выражений

$$a^{1+2+\dots+(p-1)} + 1, a^{1+2+\dots+(p-1)} - 1$$

делится на p , а при $p = 2$, $(a, 2) = 1$ оба выражения делятся на p .

88. Доказать, что для любого простого p из $a^p \equiv b^p \pmod{p}$ следует $a^p \equiv b^p \pmod{p^2}$.

Глава III

СРАВНЕНИЯ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ

§ 1. Классы решений сравнения произвольной степени

Если неизвестное целое x подчинено условию

$$f(x) \equiv 0 \pmod{m}, \quad (1)$$

где $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ многочлен с целыми коэффициентами, причем a_0 не делится на m , т. е. $a_0 \not\equiv 0 \pmod{m}$, то (1) называется *сравнением с неизвестной величиной степени n* .

Решить сравнение (1) — значит найти все целые значения x , которые ему удовлетворяют. Но если x_1 одно такое число, т. е. $f(x_1) \equiv 0 \pmod{m}$, то по третьему свойству сравнений (следствие В) этому сравнению будут также удовлетворять все числа

$$x \equiv x_1 \pmod{m},$$

т. е. все вычеты, принадлежащие к тому же классу, что и x_1 по модулю m . Поэтому *решением принято считать не отдельное число, а целый класс чисел по модулю m , удовлетворяющих данному сравнению*¹. Таких классов решений сравнение (1) имеет, очевидно, столько, сколько вычетов полной системы ему удовлетворяют.

Непосредственным испытанием всех вычетов полной системы по модулю m можно установить, какие из них данному сравнению удовлетворяют. Соответ-

¹ Иногда мы и отдельные числа называем решениями, но при этом они считаются разными только в том случае, когда они несравнимы друг с другом по данному модулю, т. е. принадлежат разным классам.

ствующие им классы по модулю m являются решениями сравнения.

Описанный способ нахождения решений называется методом подбора.

Пример 1. Решить сравнение

$$2x^3 + 3x - 5 \equiv 0 \pmod{7}.$$

Чтобы упростить вычисления, берем полную систему вычетов по модулю 7 в форме абсолютно наименьших вычетов

$$0, \pm 1, \pm 2, \pm 3.$$

Проверка показывает, что из этих чисел сравнению удовлетворяет только число $x=1$. Поэтому рассматриваемое сравнение имеет одно решение $x \equiv 1 \pmod{7}$.

Пример 2. Решить сравнение

$$x^2 + x - 2 \equiv 0 \pmod{5}.$$

Среди вычетов полной системы $0, \pm 1, \pm 2$ по модулю 5 этому сравнению удовлетворяют два числа $x=1$ и $x=-2$, следовательно, оно имеет два решения: $x \equiv 1 \pmod{5}$ и $x \equiv -2 \pmod{5}$.

Пример. Решить сравнение

$$x^3 - x + 1 \equiv 0 \pmod{3}.$$

Испытывая вычеты полной системы $0, \pm 1$ по модулю 3, видим, что ни один из них сравнению не удовлетворяет. Таким образом, данное сравнение не имеет решений.

Если сравнению удовлетворяет любое целое число, то такое сравнение называют *тождественным*.

Пример тождественного сравнения дает следствие из малой теоремы Ферма, согласно которому

$$x^p - x \equiv 0 \pmod{p}$$

для любого целого x .

Другим примером тождественного сравнения является каждое сравнение $f(x) \equiv 0 \pmod{m}$, все коэффициенты которого делятся на m .

Такое сравнение можно рассматривать как сравнение степени n только в том случае, если отказаться от предварительного требования, чтобы $a_0 \not\equiv 0 \pmod{m}$.

Указанное условие ставится в связи с тем, что прибавление к выражению $f(x)$ или вычитание из него члена a_0x^n , где a_0 делится на m , приводит к *равносильному* сравнению, т. е. к такому, которому удовлетворяют точно такие же значения x , как и исходному.

Из пятого свойства сравнений следует, что если обе части сравнения и модуль умножить на одно и то же целое положительное число или разделить на любой их общий положительный делитель, то также получится равносильное сравнение.

Из третьего и четвертого свойств сравнений далее следует, что и умножение обеих частей сравнения на число d , взаимно простое с модулем m , приводит к равносильному сравнению. Однако этого не будет, если d и m не являются числами взаимно простыми. В частности, при умножении обеих частей сравнения на $d = m$, всегда получится тождественное сравнение, так как все коэффициенты нового сравнения будут делиться на модуль m . Так, например, сравнение $x^3 - x + 1 \equiv 0 \pmod{3}$, которое (как мы это выше установили) не имеет решений, перейдет в тождественное сравнение

$$3x^3 - 3x + 3 \equiv 0 \pmod{3}.$$

Заметим в заключение, что сравнение (1) можно записать в виде уравнения $f(x) = my$. Таким образом, мы видим, что сравнение n -ой степени представляет собой частный случай неопределенного уравнения с двумя неизвестными, в котором одно неизвестное встречается в первой степени.

Если и второе неизвестное, входящее в уравнение, имеет первую степень, то имеем неопределенное уравнение первой степени с двумя неизвестными, решение которого сводится к решению сравнения 1-ой степени.

Упражнение

89. Решить методом подбора сравнения:

- 1) $x^2 - x + 2 \equiv 0 \pmod{7}$; 2) $3x^4 + 2x^2 - 1 \equiv 0 \pmod{5}$; 3) $7x^2 - 5x + 1 \equiv 0 \pmod{13}$; 4) $4x^3 - 7x^2 + 10 \equiv 0 \pmod{11}$; 5) $2x^2 + 5x + 3 \equiv 0 \pmod{6}$; 6) $3x^2 + x - 1 \equiv 0 \pmod{5}$.

§ 2. Сравнения первой степени

1. Критерий разрешимости и число решений. Решение методом подбора

Общий вид сравнения первой степени с одним неизвестным следующий:

$$ax \equiv b \pmod{m}. \quad (1)$$

1. Рассмотрим сначала наиболее важный случай, когда a и m числа взаимно простые, т. е. $(a, m) = 1$.

Если в (1) вместо x подставить все вычеты из полной системы вычетов по модулю m , то по первой теореме о вычетах линейной формы ax также примет все значения из полной системы вычетов, поэтому для одного и только одного значения x_1 число ax попадет в тот класс, к которому принадлежит b ; для него будем иметь

$$ax_1 \equiv b \pmod{m}.$$

Таким образом, мы приходим к выводу, что в случае, когда $(a, m) = 1$, для сравнения (1) существует решение, притом единственное

$$x \equiv x_1 \pmod{m},$$

или

$$x = x_1 + mt, \text{ где } t = 0, \pm 1, \pm 2, \dots$$

Это решение можно найти методом подбора.

Пример:

$$5x \equiv 7 \pmod{8}.$$

Испытывая вычеты из полной системы вычетов по модулю 8, т. е. числа $0, \pm 1, \pm 2, \pm 3, 4$, находим решение

$$x \equiv 3 \pmod{8}.$$

2. Пусть теперь $(a, m) = d > 1$.

Тогда представляются два случая.

1. Число b в правой части на d не делится.

В этом случае сравнение (1) решения иметь не может, так как это противоречило бы (восьмому) свойству сравнений, которое говорит о том, что части сравнения имеют с модулем один и тот же общий наибольший делитель.

Пример. Сравнение $6x \equiv 7 \pmod{15}$ неразрешимо, так как $(6, 15) = 3$, между тем $7 \nmid 3$.

Следует отметить, что если $(b, m) = d > 1$, но $a \not\equiv d$, то это еще не значит, что сравнение неразрешимо, а только лишь то, что решение, если оно существует должно удовлетворять условию $ax \not\equiv d$.

Если, например, $7x \equiv 6 \pmod{15}$, то мы, ввиду $(7, 15) = 1$, заключаем, что сравнение разрешимо, а на основании того, что $(6, 15) = 3$, можем утверждать, что $7x \equiv 3$. Но так как $7 \not\equiv 3$, то отсюда вытекает, что, $x \not\equiv 3$. Это можно использовать для упрощения решения, о чем еще будет речь в дальнейшем.

II. Число b в правой части делится на d . Тогда имеем

$$a = a_1 d, \quad b = b_1 d, \quad m = m_1 d.$$

Поэтому по пятому свойству сравнений обе части и модуль сравнения можно разделить на d , после чего получаем сравнение

$$a_1 x \equiv b_1 \pmod{m_1}, \text{ где } (a_1, m_1) = 1, \quad (2)$$

которое равносильно (1).

Сравнение (2) по основному случаю имеет по модулю m_1 единственное решение

$$x \equiv x_1 \pmod{m_1}.$$

Однако на этом решение сравнения (1) еще не заканчивается, так как, согласно определению, следует указать классы решений по исходному модулю m , а мы пока имеем решения по модулю m_1 . Чтобы найти классы решений по исходному модулю m , заметим следующее. Все вычеты

$$\dots, x_1 - m_1, x_1, x_1 + m_1, \dots, x_1 + (d-1)m_1, x_1 + dm_1, \dots \quad (3)$$

сравнимые с x_1 по модулю m_1 , принадлежат по модулю $m_1 d = m$ к d различным классам, представителями которых являются вычеты:

$$x_1, x_1 + m_1, x_1 + 2m_1, \dots, x_1 + (d-1)m_1. \quad (4)$$

Действительно, разность любых двух вычетов из (4) не делится на m (поэтому все они принадлежат различным классам по модулю m), а для каждого другого вычета из (3) найдется среди вычетов (4) такой, что их разность будет кратна m (поэтому такие вычеты принадлежат одному классу по модулю m).

Таким образом, в данном случае имеем по исходному модулю m d решений:

$$x \equiv x_1, x + m_1, \dots, x_1 + (d - 1)m_1 \pmod{m}.$$

Пример:

$$15x \equiv 35 \pmod{55}.$$

Здесь, после деления обеих частей сравнения и модуля на 5, получаем

$$3x \equiv 7 \pmod{11}.$$

Методом подбора можем найти

$$x \equiv 6 \pmod{11} \text{ или } x = 6 + 11t, \text{ где } t = 0, \pm 1, \dots$$

Исходное сравнение имеет 5 решений

$$x \equiv 6, 6 + 11, 6 + 2 \cdot 11, 6 + 3 \cdot 11, 6 + 4 \cdot 11 \pmod{55}, \\ \text{т. е. } x \equiv 6, 17, 28, 39, 50 \pmod{55}.$$

Резюмируя, приходим к следующему критерию разрешимости и заключению о числе решений сравнения (1):

1) если $(a, m) = 1$, то решение существует, причем единственное:

2) если $(a, m) = d > 1$, то

I) при $b \not\equiv d$ решений нет, а

II) при $b \equiv d$ существует d решений.

Заметим, что решение сравнения надо начинать с определения $d = (a, m)$ и проверки того, делится ли b на d или нет.

2. Решение сравнения первой степени методом преобразования коэффициентов

Решение сравнения 1-ой степени методом подбора не является эффективным. На практике для небольших модулей m целесообразнее, используя общие свойства сравнений, попытаться преобразовать коэффициенты так, чтобы правую часть можно было бы разделить на коэффициент у неизвестного x .

Преобразования, о которых идет речь, следующие: замена коэффициентов абсолютно наименьшими вычетами, замена b (прибавлением кратного модулю) сравнимым по модулю m числом с тем, чтобы последнее делилось на a , переход от a и b к другим, сравнимым с ними по модулю m числам, у которых оказался бы общий делитель и т. п.

Преобразованиям можно подвергать a или b , а также a и b сразу.

Отметим еще, что в случае, когда $(b, m) = d > 1$, бывает полезным перейти к новому неизвестному.

Хотя этот метод, который мы будем называть методом преобразования коэффициентов, не выражен в виде определенного предписания, все же для небольших модулей он является (при соответствующем навыке) довольно эффективным.

Примеры:

$$1) 5x \equiv 7 \pmod{8},$$

$$5x \equiv 7 + 8 = 15 \pmod{8}, x \equiv 3 \pmod{8};$$

$$2) 7x \equiv 6 \pmod{15}.$$

$$\text{Решение 1-е. } 7x \equiv 6 + 15 = 21 \pmod{15}, \\ x \equiv 3 \pmod{15}.$$

Решение 2-е. Так как $(6, 15) = 3$, делаем подстановку $x = 3y$, тогда $7 \cdot 3y \equiv 6 \pmod{15}$, $7y \equiv 2 \pmod{5}$,

$$2y \equiv 2 \pmod{5}, y \equiv 1 \pmod{5},$$

$$3y \equiv 3 \pmod{15}; x = 3y \equiv 3 \pmod{15}.$$

$$3) 17x \equiv 25 \pmod{28},$$

$$45x \equiv 25 \pmod{28}, 9x \equiv 5 \pmod{28},$$

$$9x \equiv 5 - 140 = -135 \pmod{28}, x \equiv -15 \equiv 13 \pmod{28}$$

3. Решение сравнения первой степени при помощи теоремы Эйлера

Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$,
откуда

$$a^{\varphi(m)} b \equiv b \pmod{m}.$$

При сопоставлении этого сравнения с $ax \equiv b \pmod{m}$ видно, что

$$x \equiv a^{\varphi(m)-1} \cdot b \pmod{m} \quad (1)$$

является его решением.

Мы получили решение в виде готовой формулы. Однако задачу можно считать эффективно решенной лишь тогда, когда для $a^{\varphi(m)-1} b$ будет найден наименьший неотрицательный или абсолютно наименьший вычет по модулю m .

Примеры:

$$1) 3x \equiv 7 \pmod{11}.$$

$$x \equiv 3^{\varphi(11)-1} \cdot 7 \pmod{11},$$

$\varphi(11) = 10$; далее находим абсолютно наименьший вычет для $3^9 \pmod{11}$:

$$3^2 = 9 \equiv -2, \quad 3^4 \equiv 4, \quad 3^5 \equiv 12 \equiv 1, \quad 3^9 \equiv 4 \pmod{11}.$$

Теперь

$$3^9 \cdot 7 \equiv 28 \equiv 6 \pmod{11}.$$

Итак,

$$x \equiv 6 \pmod{11}.$$

$$2) \quad 17x \equiv 25 \pmod{28}.$$

$$x \equiv 17^{-(28)-1} \cdot 25 \pmod{28},$$

$$\varphi(28) = \varphi(4) \cdot \varphi(7) = 2 \cdot 6 = 12.$$

Переходим к вычислению абсолютно наименьшего вычета $17^{11} \cdot 25 \pmod{28}$.

$$17 \equiv -11, \quad 17^2 \equiv 121 \equiv 9, \quad 17^4 \equiv 81 \equiv -3 \pmod{28},$$

$$17^8 \equiv 9, \quad 17^{10} \equiv 81 \equiv -3, \quad 17^{11} \equiv 33 \equiv 5 \pmod{28}.$$

$$17^{11} \cdot 25 \equiv 125 \equiv 13 \pmod{28}.$$

Итак,

$$x \equiv 13 \pmod{28}.$$

Примеры показывают, что применение формулы (1) для решения сравнения первой степени не является практичным.

Подводя итоги всем рассмотренным методам решения сравнений первой степени, становится ясным, что для больших модулей (исключая легко обозримые случаи) ни один из них не является подходящим.

Эффективный способ получается при помощи конечных непрерывных дробей, с которыми мы ознакомимся в следующем параграфе.

Упражнения

90. Решить методом подбора сравнения: 1) $3x \equiv 1 \pmod{7}$; 2) $5x \equiv -2 \pmod{11}$; 3) $4x \equiv 7 \pmod{17}$; 4) $7x \equiv 5 \pmod{8}$; 5) $15x \equiv 25 \pmod{35}$; 6) $15x \equiv 11 \pmod{36}$; 7) $11x \equiv 15 \pmod{36}$; 8) $13x \equiv 1 \pmod{15}$; 9) $21x \equiv 4 \pmod{35}$; 10) $4x \equiv 21 \pmod{35}$.

91. Решить методом преобразования коэффициентов сравнения: 1) $27x \equiv 14 \pmod{25}$; 2) $13x \equiv 10 \pmod{11}$; 3) $5x \equiv 3 \pmod{11}$; 4) $7x \equiv 5 \pmod{24}$; 5) $16x \equiv 19 \pmod{31}$; 6) $19x \equiv 12 \pmod{35}$.

92. Решить сравнения, используя теорему Эйлера: 1) $7x \equiv 5 \pmod{17}$; 2) $13x \equiv 3 \pmod{19}$; 3) $27x \equiv 7 \pmod{58}$.

93. Решить сравнения предыдущей задачи методом преобразования коэффициентов.

94. Доказать, что кольцо классов по простому модулю p образует поле.

§ 3. Правильные конечные цепные дроби

1. Выделение целой части

Если a — целое, а m — натуральное число, то существует единственное представление

$$a = mq + r, \quad 0 \leq r < m, \quad (1)$$

где q — неполное частное, а r — остаток от деления a на m . Формула (1) равносильна соотношению

$$\frac{a}{m} = q + \frac{r}{m} \text{ с } 0 \leq \frac{r}{m} < 1. \quad (2)$$

Примеры:

$$\frac{147}{17} = 8 + \frac{11}{17}, \quad -\frac{79}{17} = -5 + \frac{6}{17},$$

$$\frac{68}{17} = 4 + \frac{0}{17}, \quad \frac{13}{17} = 0 + \frac{13}{17}.$$

Из (2) видно, что $q \leq \frac{a}{m} < q + 1$.

Таким образом, q можно рассматривать как наибольшее целое число, не превосходящее рациональное число $\frac{a}{m}$. Так определенное целое число q на-

зывается *целой частью рационального числа* $\frac{a}{m}$ и

обозначается $q = \left[\frac{a}{m} \right]$.

Разность $\frac{a}{m} - q = \frac{r}{m}$ называется *дробной частью* числа $\frac{a}{m}$ и обозначается $\frac{r}{m} = \left\{ \frac{a}{m} \right\}$.

Примеры:

$$\left[\frac{147}{17} \right] = 8, \quad \left[-\frac{79}{17} \right] = -5, \quad [-7,25] = -8,$$

$$[4] = 4, \quad \left[\frac{13}{17} \right] = 0;$$

$$\left\{ \frac{147}{17} \right\} = \frac{11}{17}, \quad \left\{ -\frac{79}{17} \right\} = \frac{6}{17}.$$

$$\{-7,25\} = 0,75, \quad \{4\} = 0, \quad \left\{ \frac{13}{17} \right\} = \frac{13}{17}.$$

Определение целой части q согласно (2) называется *выделением целой части*.

Поскольку это понадобится нам в дальнейшем, отметим, что понятия целой и дробной части можно отнести к любому действительному числу α .

Целой частью действительного числа α называется наибольшее целое число k , не превосходящее α , т. е. удовлетворяющее соотношению

$$k \leq \alpha < k + 1.$$

Целая часть действительного числа α существует в единственном виде и обозначается $[\alpha]$. Итак, $[\alpha] = k$, так что $[\alpha] \leq \alpha < [\alpha] + 1$.

Дробной частью действительного числа α называется разность $\alpha - [\alpha]$; она тоже существует в единственном виде и обозначается $\{\alpha\}$.

Таким образом,

$$\{\alpha\} = \alpha - [\alpha],$$

откуда

$$\alpha = [\alpha] + \{\alpha\}, \text{ где } 0 \leq \{\alpha\} < 1.$$

2. Разложение в правильную цепную дробь

Пусть $\frac{a}{b}$ рациональное число, причем $b > 0$. Применяя к a и b алгоритм Евклида для определения их общего наибольшего делителя, получаем конечную систему равенств:

$$\left. \begin{aligned} a &= bq_1 + r_2, \\ b &= r_2q_2 + r_3, \\ r_2 &= r_3q_3 + r_4, \\ &\dots \dots \dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\ r_{n-1} &= r_nq_n, \end{aligned} \right\} \quad (1)$$

где неполным частным последовательных делений q_1, q_2, \dots, q_{n-1} соответствуют остатки r_2, r_3, \dots, r_n с условием $b > r_2 > r_3 > \dots > r_n > 0$, а q_n соответствует остаток 0.

Системе равенств (1) соответствует равносильная система

$$\left. \begin{aligned} \frac{a}{b} &= q_1 + \frac{r_2}{b} = q_1 + \frac{1}{b/r_2}, \\ \frac{b}{r_2} &= q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{r_2/r_3}, \\ &\dots\dots\dots \\ \frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n}, \\ \frac{r_{n-1}}{r_n} &= q_n, \end{aligned} \right\} \quad (2)$$

из которой последовательной заменой каждой из дробей $\frac{b}{r_2}$, $\frac{r_2}{r_3}$ и т. д. ее соответствующим выражением из следующей строки получается представление дроби $\frac{a}{b}$ в виде

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}.$$

Такое выражение называется *правильной (конечной) цепной* или *правильной непрерывной дробью*; при этом предполагается, что q_1 — целое число, а q_2, \dots, q_n — натуральные числа.

Правильные цепные дроби являются частным случаем цепных дробей более общего вида, с которыми ознакомимся в гл. VI, § 5. До этого речь будет идти только о правильных цепных дробях и мы будем их просто называть цепными, или непрерывными дробями.

Имеются различные формы записи цепных дробей:

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}}$$

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_n}}}$$

$$\frac{a}{b} = (q_1, q_2, \dots, q_n)^1$$

и др.

Согласно последнему обозначению имеем

$$(q_1, q_2, \dots, q_n) = q_1 + \frac{1}{(q_2, \dots, q_n)}.$$

Числа q_1, q_2, \dots, q_n называются *элементами цепной дроби*.

Алгоритм Евклида дает возможность найти представление (или разложение) любого рационального числа $\frac{a}{b}$ в виде цепной дроби. В качестве элементов цепной дроби получаются неполные частные последовательных делений в системе равенств (1), поэтому элементы цепной дроби называются также неполными частными.

Кроме того, равенства системы (2) показывают, что процесс разложения в цепную дробь состоит в последовательном выделении целой части и перевертывании дробной части.

Последняя точка зрения является более общей по сравнению с первой, так как она применима к разложению в непрерывную дробь не только рационального, но и (см. гл. VI) любого действительного числа.

Разложение рационального числа $\frac{a}{b}$ имеет, очевидно, конечное число элементов, так как алгоритм Евклида последовательного деления a на b является конечным.

Рассмотрим в качестве примера разложение $\frac{95}{42}$ в непрерывную дробь.

$$\begin{aligned} \frac{95}{42} &= 2 + \frac{11}{42} = 2 + \frac{1}{42/11}, \\ \frac{42}{11} &= 3 + \frac{9}{11} = 3 + \frac{1}{11/9}, \end{aligned}$$

¹ Хотя для Н. О. Д. введен такой же символ, это не приведет читателя к каким-либо недоразумениям.

$$\frac{11}{9} = 1 + \frac{2}{9} = 1 + \frac{1}{9/2},$$

$$\frac{9}{2} = 4 + \frac{1}{2}.$$

Подставляя по цепочке, получаем

$$\frac{95}{42} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}}} = (2, 3, 1, 4, 2).$$

Практически неполные частные определяются по той же схеме, по которой находится Н.О.Д. двух чисел алгоритмом Евклида

$$95 \overline{) 42} \quad \overline{) 11} \quad \overline{) 9} \quad \overline{) 2} \quad \overline{) 1}$$

$$2 \quad 3 \quad 1 \quad 4 \quad 2$$

Понятно, что каждая цепная дробь представляет определенное рациональное число, т. е. равна определенному рациональному числу. Но возникает вопрос, не имеются ли различные представления одного и того же рационального числа цепной дробью (т. е. не могут ли различные цепные дроби быть равны между собой)? Оказывается, что не имеются, если потребовать, чтобы было $q_n > 1$.

Заметим прежде всего, что при отказе от указанного условия единственность представимости отпадает. В самом деле, при $q_n > 1$

$$q_n = (q_n - 1) + \frac{1}{1},$$

так что представление можно удлинить:

$$(q_1, q_2, \dots, q_n) = (q_1, q_2, \dots, q_n - 1, 1),$$

например $(2, 3, 1, 4, 2) = (2, 3, 1, 4, 1, 1)$.

Отметим далее, что принимая условие $q_n > 1$, можно утверждать, что целая часть цепной дроби (q_1, q_2, \dots, q_n) равна ее первому неполному частному q_1 .

В самом деле:

1) если $n = 1$, то это очевидно;

2) если $n = 2$, то $(q_1, q_2) = q_1 + \frac{1}{q_2}$, $q_2 > 1$; поэтому

$$[(q_1, q_2)] = q_1;$$

3) если $n > 2$, то

$$(q_1, q_2, \dots, q_n) = q_1 + \frac{1}{q_2 + \frac{1}{q_n}}, \quad \text{где } q_2 + \frac{1}{q_n} > 1,$$

так как $q_2 \geq 1$. Поэтому и здесь $[(q_1, q_2, \dots, q_n)] = q_1$.

Перейдем к доказательству того, что рациональное число $\frac{a}{b}$ однозначно представляется цепной дробью (q_1, q_2, \dots, q_n) , если $q_n > 1$.

Пусть $\frac{a}{b} = (q_1, q_2, \dots, q_n) = (q'_1, q'_2, \dots, q'_{n'})$ с условием $q_n > 1, q'_{n'} > 1$.

Тогда, как выше показано,

$$\left[\frac{a}{b} \right] = q_1 = q'_1,$$

так что $(q_2, \dots, q_n) = (q'_2, \dots, q'_{n'})$.

Повторным сравнением целых частей получаем $q_2 = q'_2$, а следовательно, $(q_3, \dots, q_n) = (q'_3, \dots, q'_{n'})$ и т. д.

Если $n \neq n'$, то в продолжении указанного процесса получим также $q_n = q'_{n'}$.

Если же $n \neq n'$, например $n' > n$, то получим

$$0 = \frac{1}{(q'_{n+1}, \dots, q'_{n'})}, \quad \text{что невозможно.}$$

Теорема доказана. Вместе с тем установлено, что при соблюдении условия $q_n > 1$ между рациональными числами и конечными цепными дробями существует взаимнооднозначное соответствие.

В заключение сделаем несколько замечаний:

1. В случае разложения правильной положительной дроби первый элемент $q_1 = 0$, например:

$$\frac{42}{95} = 0 + \frac{1}{95/42} = (0, 2, 3, 1, 4, 2).$$

2. При разложении отрицательной дроби (условимся отрицательный знак дроби всегда относить к числителю) первый элемент будет отрицательным, остальные положительными.

Это следует из того, что целая часть отрицательной дроби является целым отрицательным числом, а ее дробная часть, как всегда, положительна.

Пример:

$$-\frac{95}{42} = -3 + \frac{31}{42} = -3 + \frac{1}{42/31},$$

а так как $\frac{42}{31} = (1, 2, 1, 4, 2)$, то $-\frac{95}{42} = (-3, 1, 2, 1, 4, 2)$.

3. Всякое целое число можно рассматривать как непрерывную дробь, состоящую из одного элемента, например $5 = (5)$; дробь $\frac{1}{m}$ можно рассматривать как цепную дробь $(0, m)$.

3. Подходящие дроби; некоторые их свойства

Задаче разложения обыкновенной дроби в непрерывную дробь естественно противостоит обратная задача — обращения или свертывания цепной дроби (q_1, q_2, \dots, q_n) в простую дробь $\frac{a}{b}$.

При этом, а также и в других вопросах теории непрерывных дробей, основную роль играют дроби вида

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \dots, {}^1$$

или

$\delta_1 = q_1, \delta_2 = (q_1, q_2), \delta_3 = (q_1, q_2, q_3), \dots$, которые называются *подходящими дробями* данной непрерывной дроби или соответствующего ей числа $\frac{a}{b}$.

Заметим, что

$$\frac{a}{b} = (q_1, q_2, \dots, q_n) = \delta_n.$$

Считается, что подходящая дробь δ_k имеет порядок k .

¹ Здесь, а также в аналогичных случаях точки будут означать возможное продолжение, «пока не обрывается».

Приступая к вычислению подходящих дробей, предварительно заметим, что δ_k переходит в δ_{k+1} , если в первой заменить q_k выражением $q_k + \frac{1}{q_{k+1}}$.

Имеем

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1},$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_2 q_1 + 1}{q_2} = \frac{q_2 q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_3 (q_2 P_1 + P_0) + P_1}{q_3 (q_2 Q_1 + Q_0) + Q_1} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}, \dots,$$

при этом принимается, что $P_0=1$, $Q_0=0$, $P_1=q_1$, $Q_1=1$, $P_2=q_2 P_1 + P_0$, $Q_2=q_2 Q_1 + Q_0$ и т. д.

Закономерность, которую мы замечаем в построении формулы для δ_2 (ее числителя P_2 и знаменателя Q_2), сохраняется при переходе к δ_3 и сохранится также при переходе от k к $k+1$.

Поэтому на основании принципа математической индукции для любого k , где $2 \leq k \leq n$, имеем

$$\delta_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}, \quad (1)$$

причем

$$P_k = q_k \cdot P_{k-1} + P_{k-2}$$

и

$$Q_k = q_k \cdot Q_{k-1} + Q_{k-2}.$$

Впредь, говоря о подходящих дробях δ_k (в свернутом виде), мы будем иметь в виду их форму $\frac{P_k}{Q_k}$.

Соотношения (1) являются рекуррентными формулами для вычисления подходящих дробей, а также их числителей и знаменателей. Из формул для числителя и знаменателя сразу же видно, что при увеличении k они возрастают.

Применяется следующая схема, в которую последовательно записываются значения P_k , Q_k от P_1 , Q_1 до P_n , Q_n по формулам (1)

		q_1	q_2	$\cdot \cdot$	q_{k-2}	q_{k-1}	q_k	$\cdot \cdot \cdot$	q_n
P_k	$P_0=1$	$P_1=q_1$	P_2	$\cdot \cdot \cdot$	P_{k-2}	P_{k-1}	P_k	$\cdot \cdot \cdot$	P_n
Q_k	$Q_0=0$	$Q_1=1$	Q_2	$\cdot \cdot \cdot$	Q_{k-2}	Q_{k-1}	Q_k	$\cdot \cdot \cdot$	Q_n

В качестве иллюстрации найдем все подходящие дроби δ_k цепной дроби $\frac{95}{42} = (2, 3, 1, 4, 2)$.

		2	3	1	4	2
P_k	1	2	$3 \cdot 2 + 1 = 7$	$1 \cdot 7 + 2 = 9$	$4 \cdot 9 + 7 = 43$	$2 \cdot 43 + 9 = 95$
Q_k	0	1	$3 \cdot 1 + 0 = 3$	$1 \cdot 3 + 1 = 4$	$4 \cdot 4 + 3 = 19$	$2 \cdot 19 + 4 = 42$

Итак, для данной непрерывной дроби

$$\delta_1 = \frac{2}{1}, \quad \delta_2 = \frac{7}{3}, \quad \delta_3 = \frac{9}{4}, \quad \delta_4 = \frac{43}{19}, \quad \delta_5 = \frac{95}{42}.$$

Практически нахождение неполных частных и подходящих дробей удобно объединить в одну краткую схему, которую приведем для $\frac{95}{42}$:

$$\begin{array}{rccccc} 95 & | 42 & | 11 & | 9 & | 2 & | 1, \\ q_k & 2 & 3 & 1 & 4 & 2 \\ \delta_k & 1 & \frac{2}{3} & \frac{7}{4} & \frac{43}{19} & \frac{95}{42}. \\ & 0 & 1 & 3 & 4 & 19 \end{array}$$

В заключение отметим некоторые свойства подходящих дробей, которые используются в следующем параграфе (к другим их свойствам мы вернемся в гл. VI).

1. Пусть

$$P_k Q_{k-1} - P_{k-1} Q_k = \Delta_k.$$

Так как по формулам (1)

$$\begin{aligned} P_k \cdot Q_{k-1} - P_{k-1} \cdot Q_k &= (q_k \cdot P_{k-1} + P_{k-2}) \cdot Q_{k-1} - P_{k-1} (q_k \cdot Q_{k-1} + \\ &+ Q_{k-2}) = -(P_{k-1} \cdot Q_{k-2} - P_{k-2} \cdot Q_{k-1}), \end{aligned}$$

то

$$\Delta_k = -\Delta_{k-1},$$

откуда видно, что все Δ_k имеют одинаковое абсолютное значение, а знаки их чередуются.

Но

$$\Delta_1 = P_1 \cdot Q_0 - P_0 \cdot Q_1 = q_1 \cdot 0 - 1 \cdot 1 = -1,$$

поэтому для любого k ($1 \leq k \leq n$)

$$\Delta_k = P_k \cdot Q_{k-1} - P_{k-1} \cdot Q_k = (-1)^k. \quad (2)$$

Формула (2) показывает, что $(P_k, Q_k) = 1$. В самом деле, если предположить, что $(P_k, Q_k) = d > 1$, то получится противоречие, так как из этого следовало бы, что $(-1)^k$ делится на d , что, однако, невозможно.

Таким образом, мы приходим к выводу, что все подходящие дроби $\frac{P_k}{Q_k}$ являются несократимыми.

Отсюда, кроме того, следует, что если $\frac{a}{b}$ несократимая дробь, а $\frac{P_n}{Q_n}$ последняя ее подходящая дробь, то $a = P_n$ и $b = Q_n$. Заметим, что в этом суждении учитывается, что b и Q_n имеют одинаковый (положительный) анак.

2. При помощи формулы (2) легко установить разность двух соседних подходящих дробей. Действительно, так как

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k \cdot Q_{k-1} - P_{k-1} \cdot Q_k}{Q_k \cdot Q_{k-1}},$$

то

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k \cdot Q_{k-1}}. \quad (3)$$

Отсюда расстояние между двумя соседними подходящими дробями

$$|\delta_k - \delta_{k-1}| = \frac{1}{Q_k \cdot Q_{k-1}}. \quad (4)$$

Упражнения

95. Найти целую и дробную части от 1) $\frac{317}{45}$; 2) $-47,3$; 3) $0,73$;
4) $-\frac{15}{23}$; 5) $\sqrt{19}$; 6) $5 + \sqrt{17}$; 7) $3 + \sin \frac{\pi}{4}$; 8) $-2 - \sin \frac{\pi}{3}$;
9) $2,7 + \sqrt{2}$; 10) $\sqrt{8} + \sqrt{23}$; 11) $3 - \lg 0,7$; 12) $\sqrt[3]{20}$.

96. Доказать, что остаток r от деления целого a на модуль m совпадает с абсолютно наименьшим вычетом a по модулю m , если $\left\{\frac{a}{m}\right\} \leq \frac{1}{2}$, и не совпадает с ним, если $\left\{\frac{a}{m}\right\} > \frac{1}{2}$.

97. Найти число целых точек, имеющих абсциссы: 1) 17, 2) -33 и расположенных между осью абсцисс и прямой $3x + 5y - 4 = 0$ (сделать чертеж).

98. Найти число целых точек, имеющих ординату; 1) 23, 2) -28 и расположенных между осью ординат и прямой $5x + 3y - 8 = 0$ (сделать чертеж).

99. Доказать, что для действительного α и целого n $[\alpha + n] = [\alpha] + n$.

100. Разложить простую дробь $\frac{a}{b}$ в правильную цепную дробь и найти ее подходящие дроби; $\frac{a}{b}$ равно: 1) $\frac{137}{31}$; 2) $\frac{521}{143}$; 3) $\frac{247}{74}$, 4) $-\frac{313}{57}$, 5) $\frac{77}{187}$, 6) $-\frac{53}{217}$.

101. Сократить следующие дроби, пользуясь их разложением в цепную дробь. 1) $\frac{871}{3953}$, 2) $\frac{1241}{6059}$, 3) $\frac{6821}{2147}$, 4) $\frac{32671}{10027}$.

102. Представить Н. О. Д. чисел 285 и 786 как линейную форму этих чисел.

§ 4. Решение сравнений первой степени с помощью цепных дробей

1. Вывод формулы решения

Пусть дано сравнение

$$ax \equiv b \pmod{m}, \text{ где } (a, m) = 1, a > 0^1 \quad (1)$$

Разложим $\frac{m}{a}$ в непрерывную дробь и обозначим ее подходящие дроби через $\frac{P_k}{Q_k}$, где $k = 1, 2, \dots, n$.

Тогда согласно свойству несократимости подходящих дробей имеем

$$P_n = m, \quad Q_n = a.$$

Поэтому вместо соотношения

$$P_n \cdot Q_{n-1} - P_{n-1} \cdot Q_n = (-1)^n$$

¹ Случай $a < 0$ приводится к данному.

имеем

$$m \cdot Q_{n-1} - P_{n-1} \cdot a = (-1)^n.$$

Отсюда

$$a \cdot P_{n-1} = -(-1)^n + m \cdot Q_{n-1},$$

или (так как Q_{n-1} целое число)

$$a \cdot P_{n-1} \equiv (-1)^{n-1} \pmod{m}.$$

Умножая обе части этого сравнения на $(-1)^{n-1}b$, получим

$$a((-1)^{n-1} \cdot P_{n-1} \cdot b) \equiv b \pmod{m}.$$

Сравнивая это сравнение с исходным (1), приходим к выводу, что оно имеет решение

$$x \equiv (-1)^{n-1} \cdot P_{n-1} \cdot b \pmod{m}, \quad (2)$$

где P_{n-1} — числитель предпоследней подходящей дроби в разложении $\frac{m}{a}$. Так как (1) имеет только одно решение, то (2) совпадает с единственным решением.

Пример. Решить сравнение $285x \equiv 177 \pmod{924}$.

Находим $(285, 924) = 3$, $177 = 59 \cdot 3$; далее, после деления обеих частей сравнения и модуля на 3 получаем

$$95x \equiv 59 \pmod{308}.$$

По схеме определяем теперь неполные частные разложения $\frac{308}{95}$ в цепную дробь, а затем P_{n-1} и (для проверки правильности вычисления) P_n . Имеем

	$308 \overline{) 95}$	$\overline{) 23}$	$\overline{) 3}$	$\overline{) 2}$	$\overline{) 1}$
q_k	3	4	7	1	2
P_k	1 3	13 94	107 308.		

Итак, $P_{n-1} = P_4 = 107$, следовательно,

$$x \equiv (-1)^4 \cdot 107 \cdot 59 \pmod{308},$$

$$x \equiv 153 \pmod{308}.$$

Исходное сравнение имеет решения

$$x \equiv 153, 461, 769 \pmod{924}.$$

2. Применение сравнений первой степени к решению неопределенных уравнений первой степени с двумя неизвестными

Пусть требуется решить неопределенное уравнение

$$ax + by = c, \quad (a, b) = 1. \quad (1)$$

Это уравнение можно переписать в следующем виде:

$$ax = c - by;$$

но так как y должно быть целым числом, то

$$ax \equiv c \pmod{b}^1.$$

Решая это сравнение (оно разрешимо, так как $(a, b) = 1$), получаем $x \equiv x_1 \pmod{b}$,
или

$$x = x_1 + bt, \text{ где } t = 0, \pm 1, \pm 2, \dots$$

Для определения соответствующих значений y имеем уравнение

$$a(x_1 + bt) + by = c,$$

откуда $by = c - ax_1 - a \cdot bt$,

$$y = \frac{c - ax_1}{b} - at, \text{ где } t = 0, \pm 1, \pm 2, \dots$$

Следовательно, $y_1 = \frac{c - ax_1}{b}$ должно быть целым числом, при этом оно является частным значением неизвестного y , соответствующим x_1 (получается, как и x_1 , при $t = 0$). Поэтому общее решение уравнения (1) примет вид

$$\left. \begin{aligned} x &= x_1 + bt \\ y &= y_1 - at \end{aligned} \right\}, \text{ где } t \text{ любое целое число.} \quad (2)$$

Пример. Решить неопределенное уравнение

$$53x + 17y = 25.$$

Решая сравнение $53x \equiv 25 \pmod{17}$, получаем $x \equiv 4 \pmod{17}$ или $x = 4 + 17t$, где $t = 0, \pm 1, \dots$. Если $t = 0$, то $x_1 = 4$, а из уравнения $53 \cdot 4 + 17y_1 = 25$ следует $y_1 = -11$. Поэтому, согласно (2) общее решение данного уравнения имеет вид $x = 4 + 17t$, $y = -11 - 53t$, где $t = 0, \pm 1, \dots$

¹ Без ограничения общности можно считать, что $b > 0$.

Упражнения

103. Решить сравнения: 1) $67x \equiv 64 \pmod{183}$; 2) $89x \equiv 86 \pmod{241}$; 3) $213x \equiv 137 \pmod{516}$.

104. Решить сравнения: 1) $111x \equiv 81 \pmod{447}$; 2) $186x \equiv 374 \pmod{422}$; 3) $129x \equiv 321 \pmod{471}$.

105. Решить сравнения: 1) $-50x \equiv 67 \pmod{177}$; 2) $-73x \equiv 60 \pmod{311}$; 3) $-53x \equiv 84 \pmod{219}$.

106. Решить неопределенные уравнения: 1) $17x - 16y = 31$; 2) $23x + 15y = 19$; 3) $12x - 37y = -3$; 4) $18x - 33y = 26$; 5) $11x + 16y = 156$.

107. Определить день рождения, зная сумму S произведений числа месяца на 12 и номера месяца на 31, например для $S = 436$.

108. Сколько решений имеет неопределенное уравнение $ax + by = c$, если $(a, b) = 1$ и $0 < x \leq b$ (или $0 < y \leq a$)?

109. Чем объяснить возможность отгадывания дня рождения в задаче 107?

110. При каких наименьших целых положительных значениях a и b неопределенное уравнение $ax - by = 31$ имеет решение $(5, 9)$?

111. На прямой $ax + by = c$ найти количество целых точек, лежащих между точками с абсциссами a_1 и a_2 . 1) $8x - 13y + 6 = 0$, $a_1 = -100$, $a_2 = 150$; 2) $7x + 29y = 584$, $a_1 = -20$, $a_2 = 160$; 3) $90x - 74y = 50$, $a_1 = -100$, $a_2 = 200$.

112. Доказать, что число внутренних целых точек отрезка с целыми концами $A(x_1, y_1)$, $B(x_2, y_2)$ равно $d - 1$, где $d = (y_1 - y_2, x_1 - x_2)$.

113. Через сколько целых точек проходит треугольник с вершинами $A(2, 1)$, $B(20, 7)$ и $C(8, 15)$?

114. Найти расстояние r между соседними целыми точками прямой $ax + by = c$, $(a, b) = 1$.

115. При каком условии можно дробь $\frac{c}{ab}$ представить в виде суммы двух дробей с знаменателями a и b (с целыми числителями)?

§ 5. Система сравнений первой степени

1. Общий случай

Пусть имеем систему сравнений первой степени с одним неизвестным

$$\left. \begin{aligned} A_1x &\equiv B_1 \pmod{m_1}, & A_2x &\equiv B_2 \pmod{m_2}, & \dots, & \\ A_kx &\equiv B_k \pmod{m_k}. \end{aligned} \right\}$$

Решить эту систему — значит найти все целые значения x , которые ей удовлетворяют. Ясно, что для существования таких чисел необходимо (но недостаточно), чтобы каждое сравнение в отдельности было разрешимым.

Поэтому достаточно ограничиться рассмотрением системы

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \dots, x \equiv b_k \pmod{m_k}. \quad (1)$$

В общем случае на модули отдельных сравнений никаких требований накладывать не будем.

Перейдем теперь к решению системы (1). Покажем, что в случае разрешимости системы (1) числа, ей удовлетворяющие, всегда образуют класс вычетов по модулю M , равному Н. О. К. модулей m_1, m_2, \dots, m_k .

Первому сравнению системы (1) удовлетворяют числа вида

$$x = b_1 + m_1 t_1, \quad (2)$$

где t_1 любое целое число.

Из них одновременно удовлетворяют второму сравнению системы (1) только те, для которых

$$b_1 + m_1 t_1 \equiv b_2 \pmod{m_2}. \quad (3)$$

Отсюда $m_1 t_1 \equiv b_2 - b_1 \pmod{m_2}$.

Пусть $(m_1, m_2) = d$. Если $b_2 - b_1 \not\equiv 0 \pmod{d}$, то сравнение (3) не имеет решения, если $b_2 - b_1 \equiv 0 \pmod{d}$, то

$$\frac{m_1}{d} t_1 \equiv \frac{b_2 - b_1}{d} \pmod{\frac{m_2}{d}};$$

так как в этом сравнении $\left(\frac{m_1}{d}, \frac{m_2}{d}\right) = 1$, то оно имеет решение

$$t_1 \equiv t' \pmod{\frac{m_2}{d}},$$

или $t_1 = t' + \frac{m_2}{d} t_2$, где t_2 любое целое число.

Следовательно, первым двум сравнениям удовлетворяют значения

$$x = b_1 + m_1 \left(t' + \frac{m_2}{d} t_2 \right),$$

или

$$x = b_1 + m_1 t' + \frac{m_1 m_2}{d} t_2.$$

Но частное от деления произведения двух чисел на их Н. О. Д. равно Н. О. К. этих чисел, т. е.

¹ Дроби, обозначенные в сравнении, фактически являются целыми числами.

$\frac{m_1 m_2}{d} = [m_1, m_2]$. Обозначим далее $b_1 + m_1 t' = x_2$, так как это число является частным значением, удовлетворяющим первым двум сравнениям (если положим $t_2 = 0$).

Тогда

$$x = x_2 + [m_1, m_2]t, \text{ или } x \equiv x_2 \pmod{[m_1, m_2]}.$$

Начатое рассуждение можно продолжить при переходе к третьему и т. д. к k -тому сравнению.

В случае разрешимости системы, ей удовлетворяет класс вычетов по модулю $M = [m_1, m_2, \dots, m_k]$, который называют *решением системы* (1).

Если модули m_1, m_2, \dots, m_k попарно простые, то система (1) обязательно имеет решение (сравнение (3) разрешимо, так как коэффициент m_1 у неизвестного и модуль m_2 взаимно простые; то же будет и в продолжении решения системы), причем решением будет класс вычетов по модулю M , равному произведению всех модулей сравнений данной системы, т. е. $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$.

Пример. Решить систему $x \equiv 5 \pmod{18}$, $x \equiv 8 \pmod{21}$. Из первого сравнения вытекает $x = 5 + 18t_1$, где $t_1 = 0, \pm 1, \dots$. Затем, из $5 + 18t_1 \equiv 8 \pmod{21}$ следует $t_1 \equiv -1 \pmod{7}$, или $t_1 = -1 + 7t_2$, где $t_2 = 0, \pm 1, \dots$

Поэтому $x = 5 + 18(-1 + 7t_2) = -13 + 126t_2$, где $t_2 = 0, \pm 1, \dots$ или $x \equiv -13 \pmod{126}$.

2. Случай попарно простых модулей

Случай системы сравнений первой степени с попарно простыми модулями играет, как мы это в дальнейшем увидим, особую роль, причем для выполнения этой роли весьма подходящим является нижеследующий метод ее решения.

Итак, пусть имеется система сравнений

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \dots, x \equiv b_k \pmod{m_k} \quad (1)$$

с условием, что $(m_i, m_j) = 1$.

В том случае, когда все правые части в сравнениях системы (1) равны одному и тому же числу x_0 , решение системы получается сразу как класс вычетов, сравнимых с x_0 по модулю $M = m_1 \cdot m_2 \dots m_k$.

Действительно, в силу известных свойств сравнений (см. свойства 6 и 7 в § 1, гл. II), сравнение $x \equiv x_0 \pmod{m_1 \cdot m_2 \dots m_k}$ равносильно системе (1) с одинаковыми правыми частями x_0 .

Поэтому возникает идея выразить правые части отдельных сравнений системы (1) единым образом через некоторое x_0 , т. е. найти такое x_0 , чтобы оно по модулю m_1 было сравнимо с b_1 , по модулю m_2 с b_2 и т. д., по модулю m_k с b_k .

Оказывается, что в данном случае, когда все $(m_i, m_j) = 1$, это всегда возможно, и мы сейчас увидим, как это делается.

Представим M в следующих видах:

$$M = (m_1) \cdot m_2 \dots m_k = m_1 (m_2) m_3 \dots m_k = \dots = \\ = m_1 \dots m_{k-1} (m_k),$$

или

$$M = m_1 \cdot M_1 = m_2 \cdot M_2 = \dots = m_k \cdot M_k.$$

Так как M_1 содержит все модули, кроме m_1 , M_2 — все модули, кроме m_2 , и т. д., то ясно, что $(M_1, m_1) = 1$, $(M_2, m_2) = 1, \dots, (M_k, m_k) = 1$. Поэтому можно найти такие числа M'_1, M'_2, \dots, M'_k (они нам пока неизвестны), чтобы выполнялись сравнения:

$$M_1 \cdot M'_1 \equiv 1 \pmod{m_1}, \quad M_2 \cdot M'_2 \equiv 1 \pmod{m_2}, \quad \dots, \quad M_k \cdot M'_k \equiv \\ \equiv 1 \pmod{m_k},$$

после чего можно составить число x_0 (обладающее вышеуказанными свойствами) по следующей формуле

$$x_0 = M_1 \cdot M'_1 \cdot b_1 + M_2 \cdot M'_2 \cdot b_2 + \dots + M_k \cdot M'_k \cdot b_k. \quad (2)$$

В самом деле, по модулю m_1 : $M_1 \cdot M'_1 \equiv 1$, а $M_2 \equiv 0$, $M_3 \equiv 0, \dots, M_k \equiv 0$; по модулю m_2 : $M_2 \cdot M'_2 \equiv 1$, а $M_1 \equiv 0$, $M_3 \equiv 0, \dots, M_k \equiv 0$ и т. д.

Поэтому

$$x_0 \equiv b_1 \pmod{m_1}, \quad x_0 \equiv b_2 \pmod{m_2}, \quad \dots, \quad x_0 \equiv b_k \pmod{m_k}. \quad (3)$$

Посредством этих сравнений система (1) переходит в равносильную

$$x \equiv x_0 \pmod{m_1}, \quad x \equiv x_0 \pmod{m_2}, \quad \dots, \quad x \equiv x_0 \pmod{m_k}, \quad (4)$$

откуда, как уже об этом говорилось, сразу получается

решение системы (4) и вместе с тем равносильной ей системы (1):

$$x \equiv x_0 \pmod{M}. \quad (5)$$

Важно обратить внимание на то, что числа M_i и M'_i от b_i совершенно не зависят. Поэтому при изменении правых частей в сравнениях системы (1) соответствующие выражения для x_0 в равенстве (2) легко найти, если b_i заменить их новыми значениями.

Как раз в этом удобство метода, так как в дальнейшем нам придется иметь дело с системами вида (1), которые, имея одинаковые модули, будут отличаться своими правыми частями.

Пример. Решить систему сравнений:

$$x \equiv 20 \pmod{21}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 5 \pmod{8}.$$

Здесь $M = 21 \cdot 5 \cdot 8 = (21) \cdot 5 \cdot 8 = 21(5) \cdot 8 = 21 \cdot 5(8)$,

или $M = 21 \cdot M_1 = 5 \cdot M_2 = 8 \cdot M_3$,

где $M = 840$, $M_1 = 40$, $M_2 = 168$, $M_3 = 105$.

Найдем теперь M'_1 , M'_2 , M'_3 из сравнений:

$$40M'_1 \equiv 1 \pmod{21}, \quad 168M'_2 \equiv 1 \pmod{5}, \quad 105M'_3 \equiv 1 \pmod{8},$$

$$2M'_1 \equiv 20 \pmod{21}, \quad 3M'_2 \equiv 6 \pmod{5}, \quad M'_3 \equiv 1 \pmod{8}.$$

$$M'_1 \equiv 10 \pmod{21}, \quad M'_2 \equiv 2 \pmod{5}.$$

Составляем x_0 :

$$x_0 = 40 \cdot 10 \cdot 20 + 168 \cdot 2 \cdot 3 + 105 \cdot 1 \cdot 5.$$

Тогда

$$x \equiv x_0 \pmod{M},$$

т. е.

$$x \equiv 800 \cdot 10 + 1008 + 525 \pmod{840},$$

$$x \equiv -40 \cdot 10 + 168 + 525 \pmod{840},$$

$$x \equiv 293 \pmod{840}.$$

Для других значений правых частей рассматриваемой системы решение имело бы вид

$$x \equiv 400b_1 + 336b_2 + 105b_3 \pmod{840}.$$

В заключение заметим, что системы вида (1) выражают условие известной старинной китайской задачи, а именно: *найти число, которое при делении на m_1 дает остаток b_1 , при делении на m_2 — остаток b_2 и так далее, при делении на m_k — остаток b_k .*

Упражнения

116. Установить, совместны ли системы сравнений, не решая их: 1) $x \equiv 17 \pmod{81}$; $x \equiv 23 \pmod{63}$; 2) $x \equiv 33 \pmod{77}$; $x \equiv 47 \pmod{91}$.

117. Решить системы сравнений: 1) $x \equiv 19 \pmod{24}$, $x \equiv 10 \pmod{21}$; 2) $x \equiv 23 \pmod{35}$, $x \equiv 13 \pmod{20}$; 3) $x \equiv 12 \pmod{15}$, $x \equiv 3 \pmod{33}$; 4) $x \equiv 32 \pmod{40}$, $x \equiv 23 \pmod{72}$.

118. Решить системы сравнений: 1) $x \equiv 6 \pmod{15}$, $x \equiv 18 \pmod{21}$, $x \equiv 3 \pmod{12}$; 2) $x \equiv 13 \pmod{14}$, $x \equiv 6 \pmod{35}$, $x \equiv 26 \pmod{45}$; 3) $x \equiv 19 \pmod{56}$, $x \equiv 3 \pmod{24}$, $x \equiv 7 \pmod{20}$; 4) $x \equiv 19 \pmod{22}$, $x \equiv 8 \pmod{33}$, $x \equiv 14 \pmod{21}$.

119. В каких целых точках оси абсцисс перпендикуляры к ней пересекают данные прямые одновременно в целых точках? Уравнения прямых: 1) $x = 2 + 5y$, $x = 1 + 8y$, $x = 3 + 11y$; 2) $4x - 7y = 9$, $2x + 9y = 15$, $5x - 13y = 12$.

120. Найти натуральные числа ≤ 1000 , которые при делении на: 1) 3, 5, 8, 2) 5, 7, 9, 3) 15, 14, 11, 4) 13, 21, 23 дают соответственно остатки: 1) 2, 4, 1; 2) 4, 6, 1; 3) 11, 3, 5; 4) 9, 1, 13.

121. Между 200 и 500 найти все числа, которые при делении на 4, 5, 7 дают соответственно остатки 3, 4, 5.

122. Найти общий вид решения системы сравнений: $x \equiv b_1 \pmod{8}$, $x \equiv b_2 \pmod{9}$, $x \equiv b_3 \pmod{13}$.

§ 6. Сравнения n -ой степени по простому модулю

1. Сведение к наиболее простому виду

А. Сравнения по простому модулю представляют собой наиболее простой случай сравнений. Вместе с тем это и наиболее важный случай, так как решение сравнения по составному модулю можно свести к решению сравнения по простому модулю. Поэтому изучение сравнений n -ой степени мы начнем с рассмотрения некоторых их общих свойств по простому модулю. Итак, пусть дано сравнение

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{p}, \quad a_0 \not\equiv 0 \pmod{p}. \quad (1)$$

Приступая к решению такого сравнения, можно, во-первых, заменить коэффициенты a_0, a_1, \dots, a_n их абсолютно наименьшими вычетами, что уже дает некоторое упрощение сравнения¹.

Таким образом, можно, например, сравнение

$$25x^3 + 17x^2 - 13 \equiv 0 \pmod{11} \quad (1')$$

¹ Это, между прочим, надо сделать при любом модуле.

свести к сравнению

$$3x^3 - 5x^2 - 2 \equiv 0 \pmod{11}. \quad (2')$$

Кроме того, заметим, что можно всегда добиться того, чтобы старший коэффициент был равен 1. В самом деле, так как $(a_0, p) = 1$, то можно всегда найти такое a , чтобы

$$a_0 \cdot a \equiv 1 \pmod{p}.$$

Умножая теперь обе части (1) на a (здесь модуль сравнения не надо умножать на a , чтобы получить сравнение, равносильное с исходным, так как a , очевидно, не делится на p), получим сравнение с коэффициентом $a_0 \cdot a$ у x^n , который можно заменить сравнимым с ним вычетом 1 по модулю p .

Так, например, для (2') имеем

$$3a \equiv 1 \pmod{11},$$

откуда

$$3a \equiv 12 \pmod{11}, \quad a \equiv 4 \pmod{11}.$$

Поэтому, умножая обе части (2') на 4, получаем

$$12x^3 - 20x^2 - 8 \equiv 0 \pmod{11},$$

откуда

$$x^3 + 2x^2 + 3 \equiv 0 \pmod{11}.$$

Более существенное упрощение сравнения достигается на основании следующей теоремы: *сравнение n -ой степени по простому модулю p равносильно сравнению степени не выше $p - 1$.*

Чтобы это доказать, разделим $f(x)$ на $x^p - x$.

На основании теоремы о делении с остатком для многочленов мы можем утверждать, что в остатке получится многочлен $R(x)$ степени не выше $p - 1$.

Если частное равно $Q(x)$, то имеем тождественное равенство

$$f(x) = (x^p - x) \cdot Q(x) + R(x),$$

где все коэффициенты в $Q(x)$ и $R(x)$, конечно, целые.

Сравнение (1) можно теперь представить в виде

$$(x^p - x) \cdot Q(x) + R(x) \equiv 0 \pmod{p}. \quad (2)$$

Но так как $x^p - x \equiv 0 \pmod{p}$ для любого x , то сравнение (2), а вместе с тем и (1) равносильно сравнению

$$R(x) \equiv 0 \pmod{p}. \quad (3)$$

Теорема доказана.

Б. Для практического применения этой теоремы нет необходимости делить $f(x)$ на $x^p - x$, проще пользоваться следующим приемом сведения x^m к степени x не выше $p - 1$.

Разделим m на $p - 1$ и определим остаток r в пределах от 1 до $p - 1$ ¹, так что $m = (p - 1) \cdot k + r$, $1 \leq r \leq p - 1$.

Умножая далее обе части тождественного сравнения

$$x \equiv x^p \pmod{p}$$

на x^{r-1} , $x^{(p-1) \cdot 1 + r-1}$, ..., $x^{(p-1) \cdot (k-1) + (r-1)}$, по цепочке получим

$$x^r \equiv x^{(p-1) \cdot 1 + r} \equiv x^{(p-1) \cdot 2 + r} \equiv \dots \equiv x^{(p-1) \cdot (k-1) + r} \equiv x^{(p-1) \cdot k + r},$$

где $k = 0, 1, 2, \dots$

(Заметим, что здесь нельзя брать $r = 0$, так как умножение на x^{r-1} означало бы умножение на x^{-1} .)

Таким образом,

$$x^m = x^{(p-1) \cdot k + r} \equiv x^r \pmod{p}, \quad 1 \leq r \leq p - 1. \quad (4)$$

Вместе с тем мы получили новое доказательство теоремы.

Пример. Привести сравнение

$$x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0 \pmod{5}$$

к сравнению степени не выше 4.

Заменяя степени числа x согласно формуле (4), получаем сравнение

$$x^4 + 2x^3 + x - x^4 - x + 3 \equiv 0 \pmod{5},$$

или

$$2x^3 + 3 \equiv 0 \pmod{5}.$$

¹ Т. е. в отличие от остатков в обычном смысле этого слова, которые при делении на $p - 1$ берутся в пределах от 0 до $p - 2$, возьмем здесь вместо остатка 0 число $p - 1$.

2. О максимальном числе решений

А. В теории сравнений большое значение имеет следующая теорема о максимальном числе решений сравнения: *сравнение степени n по простому модулю имеет не более n решений.*

Доказательство этой теоремы аналогично доказательству теоремы Безу в алгебре.

Пусть сравнение

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{p}, \quad a_1 \not\equiv 0 \pmod{p} \quad (1)$$

имеет решение x_1 , т. е. $f(x_1) \equiv 0 \pmod{p}$. Тогда по теореме Безу имеем тождество

$$f(x) = (x - x_1) f_1(x) + f(x_1),$$

где $f_1(x)$ — многочлен с целыми коэффициентами степени $n-1$ с неизменным старшим коэффициентом a_0 , а $f(x_1)$ делится на p .

По модулю p это тождество переходит в тождественное сравнение

$$f(x) \equiv (x - x_1) f_1(x) \pmod{p}, \quad (2)$$

т. е. в сравнение, верное для любого целого x , так что сравнение (1) эквивалентно сравнению

$$(x - x_1) f_1(x) \equiv 0 \pmod{p}.$$

Подобным же образом можем получить тождественное сравнение $f_1(x) \equiv (x - x_2) f_2(x) \pmod{p}$, если $f_1(x) \equiv 0 \pmod{p}$ имеет решение x_2 и т. д., пока не натолкнемся на неразрешимое сравнение $f_k(x) \equiv 0 \pmod{p}$ степени $n-k > 1$ или не дойдем до разрешимого сравнения 1-й степени $a_0(x - x_n) \equiv 0 \pmod{p}$.

Подстановкой по обратной цепочке получаем в 1-м случае тождественное сравнение

$$f(x) \equiv (x - x_1)(x - x_2) \dots (x - x_k) f_k(x) \pmod{p}, \quad (3)$$

которое показывает, что все найденные решения x_2, x_3, \dots для $f_1(x) \equiv 0 \pmod{p}$, $f_2(x) \equiv 0 \pmod{p}$, ... являются также решениями сравнения (1). (Все сказанное выше справедливо даже при составном модуле.) Других решений (1) иметь не может. Действительно, если $f(x_{k+1}) \equiv 0 \pmod{p}$ и $x_{k+1} \not\equiv x_1, x_2, \dots, x_k \pmod{p}$, то должно выполняться сравнение $f_k(x_{k+1}) \equiv 0 \pmod{p}$ (так как остальные множители не делятся на p), но

это противоречит принятому условию о неразрешимости $f_k(x) \equiv 0 \pmod{p}$.

В случае n решений x_1, x_2, \dots, x_n получается тождественное сравнение

$$f(x) \equiv a_0(x - x_1)(x - x_2) \dots (x - x_n) \pmod{p}, \quad (4)$$

которое аналогичным образом свидетельствует о том, что (1) не может иметь более n решений. Теорема доказана¹.

Заметим, что в случае тождественного сравнения вида (2) говорят, что $f(x)$ делится на $x - x_1$ и $f_1(x)$ по модулю p , а правую часть (2) называют разложением $f(x)$ на множители по модулю p^2 .

Таким образом, в ходе доказательства теоремы нами попутно в сравнении (4) установлено, что если сравнение (1) имеет n решений, то левая его часть раскладывается на n линейных множителей по модулю p .

При решении сравнения $f_2(x) \equiv 0 \pmod{p}$ может оказаться, что его решение $x_2 \equiv x_1 \pmod{p}$. В таком случае из $f(x)$ вторично выделяется линейный множитель $x - x_1$, а корень x_1 считается для (1) кратным. Подобные явления могут встретиться и в дальнейшем.

Заметим еще, что при отказе от предварительного условия $a_0 \not\equiv 0 \pmod{p}$ из доказанной теоремы вытекает следствие: если сравнение n -й степени по простому модулю имеет более чем n решений, то все коэффициенты $f(x)$ делятся на p . В самом деле, так как в (4) скобки не делятся на p , то $a_0 \equiv 0 \pmod{p}$ и вместе с тем все коэффициенты $f(x)$.

Результаты, полученные при доказательстве теоремы, показывают, что выделением из $f(x)$ линейных множителей по модулю p можно упростить нахождение решений сравнения (1).

Пример. Решить сравнение

$$f(x) = x^4 + 15x^3 + 4x^2 + 4x - 15 \equiv 0 \pmod{29}.$$

¹ По составному модулю последние суждения несправедливы и как раз поэтому по составному модулю доказанная теорема не имеет места. Так, например, сравнение $x^2 - 5x + 6 \equiv 0 \pmod{6}$ имеет четыре решения $x \equiv 0, 2, 3, 5 \pmod{6}$.

² Необходимо учесть, что алгебраическое разложение всегда влечет за собой разложимость по модулю (даже любому), но не наоборот.

Устанавливаем, что $f(-1) \equiv 0 \pmod{29}$, делением $f(x)$ на $x+1$ по модулю 29 находим

$$f(x) \equiv (x+1)(x^3 + 14x^2 - 10x + 14) \pmod{29}$$

и решаем

$$f_1(x) = x^3 + 14x^2 - 10x + 14 \equiv 0 \pmod{29}.$$

Это сравнение имеет решение 2. После деления $f_1(x)$ на $x-2$ по модулю 29 из $f(x)$ вторично выделяется линейный множитель $x-2$ и получается частное $x+18$, так что $f(x)$ по модулю 29 разлагается на линейные множители:

$$f(x) \equiv (x+1)(x-2)^2(x+18) \pmod{29}.$$

Таким образом, исходное сравнение имеет решения $x \equiv -1, 2, 11 \pmod{29}$, из которых второе является двойным. Нахождение последнего корня методом подбора было бы, конечно, затруднительно.

Б. На естественный вопрос о том, когда сравнение степени $n < p$ (где простое p — модуль сравнения) имеет точно n решений, отвечает теорема.

Сравнение $f(x) \equiv 0 \pmod{p}$ степени $n < p$ с коэффициентом 1 при старшем члене¹ имеет n решений тогда и только тогда, когда все коэффициенты остатка от деления $x^p - x$ на $f(x)$ кратны p .

Доказательство. Пусть при делении $x^p - x$ на $f(x)$ получились частное $q(x)$ и остаток $r(x)$.

Тогда имеем тождество

$$x^p - x = f(x) \cdot q(x) + r(x),$$

или

$$r(x) = x^p - x - f(x) \cdot q(x),$$

причем $q(x)$ и $r(x)$ имеют целые коэффициенты, степень $q(x)$ равна $p-n$, а степень $r(x)$ не превосходит $n-1$.

Пусть теперь $f(x) \equiv 0 \pmod{p}$ имеет n решений, тогда и $r(x) \equiv 0 \pmod{p}$ имеет этих же n решений, так как $x^p - x \equiv 0 \pmod{p}$ выполняется тождественно. Но так как $r(x)$ имеет степень $\leq n-1$, то из этого следует, что все коэффициенты $r(x)$ делятся на p .

¹ Этим случаем можно ограничиться.

Если, наоборот, все коэффициенты $r(x)$ делятся на p , то сравнение

$$f(x) \cdot q(x) \equiv 0 \pmod{p}$$

выполняется тождественно, т. е. имеет p решений. Но любое решение этого сравнения удовлетворяет по крайней мере одному из сравнений

$$f(x) \equiv 0 \pmod{p}, \quad q(x) \equiv 0 \pmod{p},$$

поэтому общее число решений этих двух сравнений не может быть меньше p , т. е. если число решений этих двух сравнений соответственно n_1 и n_2 , то $n_1 + n_2 \geq p$. Учитывая, что $n_2 \leq p - n$, получаем $n_1 \geq n$, но так как $n_1 \leq n$, то $n_1 = n$ и теорема доказана.

Пример. Выяснить, имеет ли сравнение $x^3 + x - 3 \equiv 0 \pmod{5}$ 3 решения.

Так как $x^5 - x = (x^3 + x - 3)(x^2 - 1) + 3x^2 - 3$, то этого не может быть.

3. Теорема Вильсона

При помощи теоремы о максимальном числе решений легко доказать известную теорему Вильсона: *если p простое число, то*

$$(p-1)! + 1 \equiv 0 \pmod{p}. \quad (1)$$

Для доказательства заметим, что сравнение

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

имеет $p-1$ (значит максимальное число) решений, наименьшие положительные вычеты которых по модулю p равны $1, 2, \dots, p-1$. Поэтому, согласно (4) из предыдущего пункта, имеет место тождественное сравнение

$$x^{p-1} - 1 \equiv (x-1)(x-2) \dots (x-(p-1)) \pmod{p}.$$

Подставляя здесь $x=0$, находим

$$-1 \equiv (-1)^{p-1} \cdot (p-1)! \pmod{p}.$$

Если p число нечетное, то получаем отсюда

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Это же соотношение имеет место для $p=2$, поэтому оно справедливо для любого простого p . Теорема доказана.

Легко понять, что для составного p (1) не может иметь места. Действительно, если $p = p_1 d$, $1 < d < p$, то $(p-1)!$ делится на d , поэтому $(p-1)! + 1$ на d делиться не может. Но если $(p-1)! + 1$ не делится на d , то оно не может также делиться на p .

Отсюда вытекает, что справедлива обратная теорема: *если для целого положительного p имеет место соотношение (1), то p число простое.*

Таким образом, мы приобрели критерий простого числа, однако легко понять, что непосредственного применения на практике он не имеет.

Дело в том, что даже для небольших чисел p $(p-1)!$ очень большое число.

Если бы мы при помощи указанного критерия захотели узнать, является ли, например, 11 простым числом, то надо было бы проверить делимость числа $10! + 1 = 3\,628\,801$ на 11.

Упражнения

123. Сравнения упростить (понижить степень, коэффициенты по абсолютному значению уменьшить, а коэффициент у старшего члена сделать равным 1) и решить методом подбора: 1) $28x^9 + 29x^8 - 26x^7 + 20x^4 - 17x + 23 \equiv 0 \pmod{3}$; 2) $34x^{10} - 29x^7 + 43x^4 - 19x + 37 \equiv 0 \pmod{5}$; 3) $75x^{13} - 62x^{12} - 53x^{11} - 24x^6 + 13x - 27 \equiv 0 \pmod{7}$.

124. Разложить многочлен на множители по данному модулю: 1) $x^3 + 3x^2 - 3$ по модулю 17; 2) $x^3 + 11x^2 + 8x + 3$ по модулю 23; 3) $x^3 - 13x^2 - 3x + 11$ по модулю 31.

125. Найти простейший вид сравнения 3-й степени, имеющего решения 1, -7 и 19 по модулю: 1) 23, 2) 29, 3) 31.

126. Многочлен $f(x)$ имеет по модулю m разложение $f(x) \equiv (x-3)(x-5) \pmod{m}$; 1) $m = 15$, 2) $m = 17$, 3) $m = 20$. Единственное ли оно? Если нет, указать другие разложения.

127. Выяснить, имеют ли сравнения максимальное число решений: 1) $x^5 + x^3 + 2 \equiv 0 \pmod{7}$, 2) $x^5 - 3x^4 + 2x^3 + x^2 - 3x + 2 \equiv 0 \pmod{7}$.

128. Доказать, что для простых $p = 4n + 1$ $\left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0 \pmod{p}$, а для простых $p = 4n + 3$ $\left[\left(\frac{p-1}{2}\right)!\right]^2 - 1 \equiv 0 \pmod{p}$.

129. Доказать, что для простого p и любого целого a $a^p + (p-1)!a \equiv 0 \pmod{p}$.

130. Доказать критерий Лейбница для простого числа: для того, чтобы натуральное число $p > 2$ было простым, необходимо и достаточно, чтобы $(p-2)! - 1 \equiv 0 \pmod{p}$.

§ 7. Сравнения n -ой степени по составному модулю

1. Приведение сравнения по составному модулю к системе сравнений по модулям попарно простым

В настоящем параграфе покажем, что решение сравнения по составному модулю можно свести к решению сравнения по простому модулю. Предварительно докажем следующую теорему.

Пусть составной модуль M сравнения

$$f(x) \equiv 0 \pmod{M} \quad (1)$$

представлен в виде произведения попарно простых множителей

$$M = m_1 \cdot m_2 \dots m_k, \text{ где } (m_i, m_j) = 1.$$

Тогда: 1) сравнение (1) равносильно системе сравнений

$$f(x) \equiv 0 \pmod{m_1}, f(x) \equiv 0 \pmod{m_2}, \dots, f(x) \equiv 0 \pmod{m_k}; \quad (2)$$

2) если (1) имеет N решений по модулю M , а отдельные сравнения системы (2) имеют по соответственным модулям n_1, n_2, \dots, n_k решений, то $N = n_1 \cdot n_2 \dots n_k$.

Доказательство. 1. Известно, что если сравнение имеет место по некоторому модулю M , то оно имеет также место по модулю, равному любому его делителю. Отсюда видно, что каждое значение x , удовлетворяющее (1), удовлетворяет системе (2).

С другой стороны, известно, что если сравнение имеет место по нескольким модулям, то оно справедливо также по модулю, равному Н. О. К. данных модулей (в случае попарно простых чисел их Н. О. К. равно произведению данных чисел). Это показывает, что всякое значение x , удовлетворяющее системе (2), удовлетворяет сравнению (1).

Таким образом, сравнение (1) и система сравнений (2) эквивалентны, причем даже в том случае, когда $(m_i, m_j) \neq 1$.

2. В силу эквивалентности сравнения (1) и системы (2) (даже в том случае, когда $(m_i, m_j) \neq 1$) естественно считать решением системы (2) класс чисел по модулю $M = [m_1, m_2, \dots, m_k]$, удовлетворяющих всем сравнениям системы (2).

Принимая такое определение для решений системы (2)¹, можем сказать, что сравнение (1) и система (2) имеют одни и те же решения.

Таким образом, чтобы найти число N решений сравнения (1), достаточно подсчитать число решений системы (2).

Сделаем это для случая, когда $(m_i, m_j) = 1$, который рассматривается в теореме.

Полезно заметить, что если хотя бы одно из сравнений системы (2) неразрешимо, то неразрешима также вся система, а следовательно, и сравнение (1).

Пусть b_1 одно из решений 1-го сравнения, b_2 — одно из решений 2-го сравнения, ..., b_k — одно из решений k -го сравнения. Тогда система сравнений

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \dots, x \equiv b_k \pmod{m_k} \quad (3)$$

имеет единственное решение

$$x \equiv x_0 = M_1 \cdot M'_1 b'_1 + M_2 \cdot M'_2 b_2 + \dots + M_k \cdot M'_k b_k \pmod{M}, \quad (4)$$

которое является также решением системы (2) и сравнения (1).

(M_i, M'_i) имеют в сравнении (4) такие же значения, как и в § 5 настоящей главы). Но 1-е сравнение имеет n_1 , 2-е — n_2 , ..., k -ое — n_k решений, следовательно, получается $n_1 \cdot n_2 \dots n_k$ систем вида (3), которым соответствуют столько же значений x_0 .

Для утверждения, что им соответствуют разные решения системы (2), необходимо еще показать, что они принадлежат разным классам по модулю M .

В справедливости последнего мы убеждаемся, рассматривая, какие числа x_0 и x'_0 получаются, когда заменяем решение хотя бы одного сравнения другим его решением, например b_1 на b'_1 .

Вопрос сводится, очевидно, к тому, могут ли быть сравнимыми по модулю M числа $M_1 \cdot M'_1 b_1$ и $M_1 \cdot M'_1 b'_1$, так как остальные слагаемые в x_0 и x'_0 равны между собой. Но если предположить, что

$$M_1 \cdot M'_1 b_1 \equiv M_1 \cdot M'_1 b'_1 \pmod{M},$$

¹ Этому определению отвечает принятое в п. 1, § 5, наст. гл. понятие решения линейной системы.

то должно также быть

$$M_1 \cdot M'_1 b_1 \equiv M_1 \cdot M'_1 b'_1 \pmod{m_1},$$

а так как

$$M_1 M'_1 \equiv 1 \pmod{m_1},$$

то и

$$b_1 \equiv b'_1 \pmod{m_1},$$

однако это невозможно, так как b_1 и b'_1 принадлежат разным классам по модулю m_1 .

Итак, мы получаем несравнимые числа по модулю M , а поэтому $N = n_1 \cdot n_2 \dots n_k$.

Теорема доказана.

Пример. Решить сравнение

$$f(x) = 3x^3 + 6x^2 + x + 10 \equiv 0 \pmod{15}. \quad (1')$$

(1') заменяем системой

$$f(x) \equiv 0 \pmod{3}, \quad f(x) \equiv 0 \pmod{5}. \quad (2')$$

Легко найти, что 1-ое сравнение имеет одно решение $x \equiv -1 \pmod{3}$, а второе — три решения $x \equiv 0, 1, 2 \pmod{5}$. Переходим к решению системы

$$x \equiv b_1 \pmod{3}, \quad x \equiv b_2 \pmod{5}. \quad (3')$$

Здесь $M = 5 \cdot 3 = 3 \cdot 5$, поэтому имеем

$$5M'_1 \equiv 1 \pmod{3}, \quad M'_1 \equiv -1 \pmod{3};$$

$$3M'_2 \equiv 1 \pmod{5}, \quad M'_2 \equiv 2 \pmod{5};$$

$$x_0 = 5 \cdot (-1) \cdot b_1 + 3 \cdot 2 \cdot b_2 = -5b_1 + 6b_2.$$

Таким образом, сравнение (1') имеет решения

$$x_1 = -5 \cdot (-1) + 6 \cdot 0 \equiv 5 \pmod{15},$$

$$x_2 = 5 + 6 \cdot 1 \equiv 11 \pmod{15},$$

$$x_3 = 5 + 6 \cdot 2 \equiv 17 \equiv 2 \pmod{15}.$$

Приведение сравнений по составному модулю к системе сравнений по модулям попарно простым можно также применить к решению сравнений 1-й степени.

Пример. Вместо сравнения $37x \equiv 17 \pmod{180}$ можно рассмотреть систему: $37x \equiv 17 \pmod{36}$, $37x \equiv 17 \pmod{5}$, или

$$x \equiv 17 \pmod{36}, \quad x \equiv 1 \pmod{5}.$$

Решая последнюю систему, находим: $x \equiv -19 \pmod{180}$.

2. Приведение к сравнениям по модулю p^α и к сравнениям по модулю p

Согласно теореме, доказанной в предыдущем пункте, решение сравнения $f(x) \equiv 0$ по составному модулю M сводится к решению сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}, \quad (1)$$

так как в качестве попарно простых множителей модуля M можно брать числа вида p^α , где p — простое число.

Решать (1) непосредственно методом подбора, очевидно, очень неудобно, так как даже для небольших p и α число p^α может оказаться большим. Поэтому весьма примечательно то, что решение сравнения (1) можно свести к решению сравнения

$$f(x) \equiv 0 \pmod{p}. \quad (2)$$

Действительно, так как всякое число x_1 , удовлетворяющее сравнению (1), удовлетворяет также сравнению (2) (если $f(x_1) \mid p^\alpha$, то тем более $f(x_1) \mid p$), то надо такие числа, которые удовлетворяют сравнению (1), искать среди множества значений, удовлетворяющих (2). Сделаем это постепенно, переходя сначала от (2) к такому же сравнению по модулю p^2 , затем по модулю p^3 и т. д., пока не дойдем до (1).

Итак, пусть нами найдено одно решение сравнения (2):

$$x \equiv x_1 \pmod{p},$$

или

$$x_1 = x + pt_1, \text{ где } t_1 = 0, \pm 1, \dots \quad (3)$$

Рассуждение, которым мы здесь воспользуемся, вполне аналогично тому, которое мы применяли при решении линейной системы.

Если t_1 — любое целое число, то по формуле (3) получаются числа, которые все удовлетворяют сравнению (2). Чтобы выделить из них те числа, которые удовлетворяют сравнению

$$f(x) \equiv 0 \pmod{p^2}, \quad (4)$$

мы не можем для t_1 брать любые целые значения, а должны брать такие, для которых

$$f(x_1 + pt_1) \equiv 0 \pmod{p^2}.$$

Для вычисления левой части и упрощения ее вида удобно заменить многочлен $f(x_1 + pt_1)$ его разложением по формуле Тейлора

$$f(x_1) + pt_1 f'(x_1) + \frac{(pt_1)^2}{2!} f''(x_1) + \dots + \frac{(pt_1)^k}{k!} f^{(k)}(x_1),$$

где, как известно, $\frac{1}{k!} f^{(k)}(x_1)$ — число целое.

За исключением первых двух слагаемых, все остальные содержат p в степени ≥ 2 и делятся, таким образом, на p^2 . Поэтому по модулю p^2 предыдущее сравнение равносильно следующему:

$$f(x_1) + pt_1 \cdot f'(x_1) \equiv 0 \pmod{p^2}. \quad (5)$$

Отсюда, в силу того, что $f(x_1) \not\equiv 0 \pmod{p}$, получаем сравнение

$$\frac{f(x_1)}{p} + f'(x_1) \cdot t_1 \equiv 0 \pmod{p},$$

или

$$f'(x_1) t_1 \equiv -\frac{f(x_1)}{p} \pmod{p}. \quad (6)$$

А. В наиболее общем случае, когда $f'(x_1) \not\equiv 0 \pmod{p}$, т. е. $f'(x_1) \not\equiv 0 \pmod{p}$, из (6) находим

$$t_1 \equiv t' \pmod{p}, \quad t_1 = t' + pt_2, \quad \text{где } t_2 = 0, \pm 1, \dots$$

Подставляя значение t_1 в (3), получаем решение сравнения (4)

$$x = x_1 + p(t' + pt_2) = x_1 + pt' + p^2 t_2.$$

При $t_2 = 0$ эта формула дает одно из значений, удовлетворяющих (4); обозначим его через x_2 . Тогда

$$x = x_2 + p^2 \cdot t_2, \quad \text{где } t_2 = 0, \pm 1, \dots,$$

или

$$x \equiv x_2 \pmod{p^2}.$$

Переходя к решению

$$f(x) \equiv 0 \pmod{p^3}, \quad (7)$$

на t_2 накладываем требование

$$f(x_2 + p^2 t_2) \equiv 0 \pmod{p^3}.$$

Применяя формулу Тейлора, легко находим

$$f(x_2) + p^2 \cdot t_2 \cdot f'(x_2) \equiv 0 \pmod{p^3}.$$

а так как $f(x_2) \not\equiv 0 \pmod{p^2}$, то отсюда следует

$$\frac{f(x_2)}{p^2} + f'(x_2) \cdot t_2 \equiv 0 \pmod{p}. \quad (8)$$

Так как $x_1 \equiv x_2 \pmod{p}$,

то $f'(x_1) \equiv f'(x_2) \pmod{p}$.

Но $f'(x_1) \not\equiv 0 \pmod{p}$, следовательно, и $f'(x_2) \not\equiv 0 \pmod{p}$.

Таким образом, (8) дает одно решение

$$t_2 \equiv t'_2 \pmod{p}, \text{ или } t_2 = t'_2 + pt_3, \text{ где } t_3 = 0, \pm 1, \dots,$$

при помощи которого составляем решение сравнения (7):

$$x = x_2 + p^2(t'_2 + pt_3) = x_2 + p^2t'_2 + p^3t_3,$$

или

$$x = x_3 + p^3t_3, \quad t_3 = 0, \pm 1, \dots,$$

или

$$x \equiv x_3 \pmod{p^3}.$$

Повторяя примененный процесс, приходим к решению сравнения (1)

$$x \equiv x_a \pmod{p^a}.$$

Итак, в случае, когда $f'(x_1) \not\equiv 0 \pmod{p}$, каждое решение сравнения (2) приводит к одному решению сравнения (1).

Пример. Решить сравнение

$$f(x) \equiv 0 \pmod{27}, \text{ где } f(x) = 2x^4 + 5x - 1.$$

Сравнение $f(x) \equiv 0 \pmod{3}$ имеет одно решение $x \equiv 1 \pmod{3}$. Здесь $f'(x) = 8x^3 + 5$, следовательно, $f'(1) = 13 \not\equiv 0 \pmod{3}$, что соответствует рассмотренному выше случаю.

Следуя далее общему приему решения, находим:

$$x = 1 + 3t_1;$$

$$f(1) + 3t_1 \cdot f'(1) \equiv 0 \pmod{9}, \quad 6 + 3 \cdot t_1 \cdot 13 \equiv 0 \pmod{9},$$

$$13t_1 \equiv -2 \pmod{3}, \quad t_1 \equiv -2 \pmod{3}, \quad t_1 = -2 + 3t_2;$$

$$x = -5 + 9t_2;$$

$$f(-5) + 9t_2 \cdot f'(-5) \equiv 0 \pmod{27},$$

$$1224 + 9t_2 \cdot (-995) \equiv 0 \pmod{27},$$

$$-995t_2 \equiv -136 \pmod{3}, \quad t_2 \equiv -1 \pmod{3}, \quad t_2 = -1 + 3t_3;$$

$$x = -14 + 27t_3,$$

или

$$x \equiv 13 \pmod{27}.$$

Б. Если в сравнении (6) $f'(x_1) \mid p$, а правая часть на p не делится, то оно неразрешимо; вместе с тем неразрешимы будут также (4) и (1).

В. Если при $f'(x_1) \mid p$ правая часть тоже делится на p , то сравнение (6) является тождественным и ему будут удовлетворять все целые числа t_1 .

Таким образом, сравнению (4) будут удовлетворять все числа, получаемые по формуле (3), т. е. те же числа, которые удовлетворяли сравнению (2). Однако по модулю p^2 они не будут больше принадлежать одному классу вычетов, а p классам, так что сравнение (4) будет иметь p решений.

Из этих решений будем далее общим приемом выделять те числа, которые удовлетворяют сравнению по модулю p^3 и т. д.

Упражнения

131. Решить сравнения: 1) $5x^4 + 2x^3 - x + 17 \equiv 0 \pmod{21}$; 2) $5x^3 - 7x^2 + 3x + 11 \equiv 0 \pmod{33}$; 3) $2x^2 - 7x + 6 \equiv 0 \pmod{55}$; 4) $4x^3 - 5x^2 + 7x + 21 \equiv 0 \pmod{105}$; 5) $3x^2 + 7x + 5 \equiv 0 \pmod{34}$.

132. Через какие целые точки проходят линии: 1) $15y = 2x^3 - 5x^2 + 4x + 11$, если $-2 < x < 8$; 2) $14y = 3x^3 - 4x^2 + 11x + 4$, если $-7 < x < 7$?

133. Решить сравнения 1-й степени, рассматривая эквивалентные им системы: 1) $43x \equiv 59 \pmod{112}$; 2) $37x \equiv 162 \pmod{245}$; 3) $23x \equiv 11 \pmod{153}$.

134. Решить сравнения: 1) $x^2 \equiv 19 \pmod{25}$; 2) $x^2 \equiv 29 \pmod{49}$; 3) $x^2 \equiv 31 \pmod{121}$; 4) $x^2 \equiv 82 \pmod{169}$.

135. Доказать, что ни при каком целом значении x выражение $x^2 + 3x + 5$ не делится на 121.

136. Решить сравнения: 1) $5x^3 + 3x + 1 \equiv 0 \pmod{25}$; 2) $3x^3 - 5x^2 - 15 \equiv 0 \pmod{49}$; 3) $3x^4 - 2x^2 + 3x + 1 \equiv 0 \pmod{49}$; 4) $4x^3 - 5x^2 + 7x - 10 \equiv 0 \pmod{27}$; 5) $3x^3 - 7x - 69 \equiv 0 \pmod{125}$.

137. Решить сравнения: 1) $2x^3 + x + 12 \equiv 0 \pmod{25}$; 2) $4x^3 + 7x + 1 \equiv 0 \pmod{25}$; 3) $3x^3 - 2x^2 - 2x - 21 \equiv 0 \pmod{49}$; 4) $5x^3 + 4x^2 - 6x + 5 \equiv 0 \pmod{49}$.

138. Решить сравнение $2x^3 - 5x - 32 \equiv 0 \pmod{175}$.

§ 8. Сравнения второй степени общего вида

1. Сравнения второй степени и их связь с неопределенными уравнениями второй степени с двумя неизвестными

Теория сравнений второй степени, к изучению которой мы переходим, связана с решением в целых числах уравнений второй степени с двумя неизвестными.

Сравнение второй степени общего вида

$$Ax^2 + Bx + C \equiv 0 \pmod{M} \quad (1)$$

равносильно неопределенному уравнению второй степени частного вида

$$Ax^2 + Bx + C = My. \quad (2)$$

К сравнениям (1) приводят нас также неопределенные уравнения второй степени общего вида:

$$ax^2 + 2bx + cy^2 + 2dx + 2ey + f = 0, \quad (3)$$

решение которых связано также с решением уравнения Пелля $x^2 - ay^2 = c$ (см. § 4, гл. VI).

2. Приведение сравнений второй степени к двучленным сравнениям

А. Сравнение второй степени общего вида

$$Ax^2 + Bx + C \equiv 0 \pmod{M} \quad (1)$$

можно привести к более простому двучленному сравнению:

$$x^2 \equiv a \pmod{m}. \quad (2)$$

Это достигается следующим образом.

Умножим обе части и модуль сравнения (1) на $4A$; тогда имеем

$$4A^2x^2 + 4ABx + 4AC \equiv 0 \pmod{4AM}. \quad (3)$$

Напомним здесь, что модуль тоже умножается на $4A$ для того, чтобы сравнение (3) было равносильным с (1). В самом деле, если бы мы этого не сделали, то в случае, когда $(4A, M) = d > 1$, нельзя было бы перейти обратно от (3) к (1), так как известно, что обе части сравнения можно всегда делить только на множитель, взаимно простой с модулем. Вместе с тем понятно, что в случае, когда $4A$ и M взаимно просты (если M — число простое, это всегда будет так), то и без умножения модуля на $4A$ получается сравнение, равносильное исходному.

Дальнейшие преобразования следующие:

$$4A^2x^2 + 4ABx + B^2 - B^2 + 4AC \equiv 0 \pmod{4AM}.$$

$$(2Ax + B)^2 \equiv B^2 - 4AC \pmod{4AM}:$$

обозначив здесь $2Ax + B = y$, $B^2 - 4AC = D$,
получаем двучленное сравнение

$$y^2 \equiv D \pmod{4AM}. \quad (4)$$

Ясно, что каждое число, удовлетворяющее (1), будет также удовлетворять (4), поэтому из неразрешимости (4) сразу же следует неразрешимость (1). Однако из разрешимости (4) относительно y еще не следует разрешимость (1) относительно x . В самом деле, каждое решение (4)

$$y \equiv y_1 \pmod{4AM}$$

приводит нас к сравнению относительно x

$$2Ax \equiv y_1 - B \pmod{4AM},$$

которое может оказаться неразрешимым, если $y_1 - B \not\vdash 2A$.

В случае разрешимости надо еще иметь в виду, что решения последнего сравнения получатся по модулю $2M$, в то время как мы должны указать решения по исходному модулю M сравнения (1). Переходя к модулю M , количество классов решений может уменьшиться.

Отметим в заключение, что при переходе от (1) к (4) в конкретной задаче не следует обязательно придерживаться общей схемы, а надо стараться упростить процесс выделения полного квадрата, для чего имеются различные возможности, однако мы на них останавливаться не станем.

Рассмотрим примеры приведения к двучленному сравнению.

Примеры: 1) $4x^2 - 11x - 3 \equiv 0 \pmod{13}$.

Имеем: $4x^2 - 24x - 16 \equiv 0 \pmod{13}$, $x^2 - 6x - 4 \equiv 0 \pmod{13}$,

$$(x - 3)^2 - 13 \equiv 0 \pmod{13}, \quad (x - 3)^2 \equiv 0 \pmod{13}, \\ x \equiv 3 \pmod{13}.$$

2) $3x^2 + 7x + 8 \equiv 0 \pmod{17}$.

Имеем: $3x^2 + 24x - 9 \equiv 0 \pmod{17}$, $x^2 + 8x - 3 \equiv 0 \pmod{17}$,

$$(x + 4)^2 \equiv 19 \pmod{17}, \quad (x + 4)^2 \equiv 2 \pmod{17}, \\ x + 4 \equiv \pm 6 \pmod{17}.$$

Отсюда: 1) $x + 4 \equiv 6 \pmod{17}$, $x \equiv 2 \pmod{17}$;

2) $x + 4 \equiv -6 \pmod{17}$, $x \equiv -10 \equiv 7 \pmod{17}$.

3) $x^2 - 5x + 6 \equiv 0 \pmod{24}$.

Имеем: $4x^2 - 20x + 64 \equiv 0 \pmod{96}$,

$(2x - 5)^2 \equiv -39 \pmod{96}$, $y^2 \equiv -39 \pmod{96}$,

где $y = 2x - 5$.

Не останавливаясь здесь на самом решении этого сравнения, отметим, что оно имеет решения $y \equiv \pm 21$, $\pm 27 \pmod{96}$. Отсюда легко получить значения $x \equiv 13$, -8 , 16 , $-11 \pmod{48}$.

Но по модулю 24: $13 \equiv -11$, $16 \equiv -8$. Итак, имеем по модулю 24 два решения

$$x \equiv 13, 16 \pmod{24}.$$

Подстановкой легко проверить правильность решений.

Б. Мы установили, что сравнение (1) можно привести к сравнению вида (2).

Если сравнение (2) разрешимо при a , взаимно простом с модулем m , то a называется *квадратичным вычетом* по модулю m ; если неразрешимо, то *квадратичным невычетом*.

Аналогичные понятия вводятся, кстати, и для двучленных сравнений высших степеней, а именно: в зависимости от разрешимости или неразрешимости сравнения $x^3 \equiv a \pmod{m}$, где $(a, m) = 1$, мы говорим о кубических вычетах и невычетах, а относительно сравнения $x^n \equiv a \pmod{m}$, где $(a, m) = 1$, — о вычетах и невычетах степени n .

Решение сравнения вида (2) по составному модулю сводится (согласно общей теории) к решению следующих сравнений:

1) $x^2 \equiv a \pmod{p}$, где p — нечетное простое число;

2) $x^2 \equiv a \pmod{p^\alpha}$, а $\alpha \geq 1$

и

3) $x^2 \equiv a \pmod{2^\alpha}$, $\alpha \geq 1$.

Наиболее важным является случай нечетного простого модуля; с ним ознакомимся в следующих параграфах (остальные случаи рассмотрены в задачах).

Заметим в заключение, что приведение сравнений второй степени общего вида по составному модулю

к более простому виду можно также выполнить, переходя сначала к простому модулю, а затем уже к двучленному сравнению. Иногда как раз этот путь может оказаться более удобным.

Упражнение

139. Привести к двучленным сравнениям и решить:

- 1) $5x^2 - 9x + 13 \equiv 0 \pmod{17}$; 2) $7x^2 + 15x - 11 \equiv 0 \pmod{23}$;
 3) $3x^2 + 13x - 10 \equiv 0 \pmod{19}$; 4) $6x^2 + 3x + 1 \equiv 0 \pmod{17}$;
 5) $12x^2 - 6x - 7 \equiv 0 \pmod{19}$.

§ 9. Общие сведения о двучленных сравнениях второй степени по нечетному простому модулю

1. Число решений. Нахождение решений методом подбора. Число квадратичных вычетов

Пусть дано двучленное сравнение второй степени по нечетному простому модулю p :

$$x^2 \equiv a \pmod{p}, \quad (2, p) = 1. \quad (1)$$

Случай, когда $a|p$, является тривиальным, так как в этом и только в этом случае, очевидно, $x \equiv 0 \pmod{p}$. Поэтому исключим этот случай из дальнейшего рассмотрения и будем считать, что $(a, p) = 1$.

Тогда решения сравнения (1) следует искать только среди классов вычетов приведенной системы по модулю p .

Легко понять, что если (1) имеет в качестве одного решения $x \equiv x_1 \pmod{p}$, то оно должно также иметь и второе $x \equiv -x_1 \pmod{p}$. То, что $-x_1$ удовлетворяет (1), является очевидным, поэтому остается доказать, что $-x_1$ является представителем другого класса.

Предположим противное, т. е. что x_1 и $-x_1$ принадлежат к одному классу. Тогда

$$x_1 \equiv -x_1 \pmod{p}, \quad 2x_1 \equiv 0 \pmod{p};$$

но $(2, p) = 1$, поэтому имеем

$$x_1 \equiv 0 \pmod{p},$$

однако это исключается ввиду условия, что $(a, p) = 1$.

Итак, если (1) разрешимо, то имеются по крайней мере 2 решения. Но больше решений и быть не может, так как число решений сравнения по простому

модулю не может превысить степень сравнения. Мы приходим к окончательному выводу, что если (1) разрешимо, то оно имеет точно два решения. При этом, если одно решение $x \equiv x_1 \pmod{p}$ найдено, то второе можно записать автоматически:

$$x \equiv -x_1 \pmod{p}.$$

Процесс нахождения решения методом подбора является для сравнения (1) более простым, по сравнению с общим случаем. Дело в том, что записывая приведенную систему вычетов по модулю p абсолютно наименьшими вычетами

$$\pm 1, \pm 2, \dots, \pm \frac{p-1}{2},$$

мы можем пригодность их положительных и отрицательных значений проверять одновременно.

Итак, для отыскания решения достаточно подставить в (1) вместо x значения

$$1, 2, 3, \dots, \frac{p-1}{2}. \quad (2)$$

При этом в левой части получаются числа

$$1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2. \quad (3)$$

В случае сравнимости (по модулю p) одного из них, например k^2 с a (заметим, что больше чем в одном случае это, согласно предыдущему, быть не может), мы получаем решения

$$x \equiv \pm k \pmod{p}.$$

Одновременно видно, что по модулю p разрешимыми будут только такие сравнения (1), в которых a сравнимо по модулю p с числами ряда (3). Другими словами, в ряде (3) записаны квадратичные вычеты по модулю p .

Все они принадлежат различным классам. Действительно, если предположить противное, т. е. что для

$$1 \leq k < l \leq \frac{p-1}{2} \\ k^2 \equiv l^2 \pmod{p}.$$

то оказалось бы, что (1) имеет 4 решения

$$x \equiv \pm k \pmod{p} \text{ и } x \equiv \pm l \pmod{p},$$

что невозможно.

Итак, можно утверждать, что количество квадратичных вычетов из разных классов (или среди вычетов приведенной системы) по модулю p равно $\frac{p-1}{2}$.

Таково же, следовательно, количество квадратичных невычетов. При помощи ряда (3) можно найти наименьшие положительные квадратичные вычеты.

Пример. Найти наименьшие положительные квадратичные вычеты по модулю 17. Их число должно быть $\frac{17-1}{2} = 8$. Они находятся нижеследующим вычислением по модулю 17:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 \equiv 16, \quad 5^2 = 25 \equiv 8, \\ 6^2 = 36 \equiv 2, \quad 7^2 = 49 \equiv 15, \quad 8^2 = 64 \equiv 13.$$

Итак, наименьшие положительные квадратичные вычеты по модулю 17 суть следующие:

$$1, 2, 4, 8, 9, 13, 15, 16; \quad (3')$$

отсюда сразу же следует, что наименьшими положительными квадратичными невычетами по модулю 17 являются числа

$$3, 5, 6, 7, 10, 11, 12, 14.$$

Только в том случае, если a сравнимо с одним из чисел ряда (3') по модулю 17, сравнение $x^2 \equiv a \pmod{17}$ является разрешимым.

2. Критерий Эйлера

Вполне естественно, что в первую очередь нас интересует, разрешимо ли сравнение $x^2 \equiv a \pmod{p}$, $(2, p) = 1$, $(a, p) = 1$, т. е. является ли a квадратичным вычетом.

В первом пункте этого параграфа установлен способ решения этого вопроса; в случае положительного ответа он дает даже решение сравнения. Однако ясно, что этот способ не является эффективным.

Очень важным является критерий, установленный Эйлером: число a , которое не делится на нечетное

простое p , является квадратичным вычетом по модулю p тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, и квадратичным невычетом тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Доказательство. По теореме Ферма имеем для $(a, p) = 1$ и $(2, p) = 1$

$$a^{p-1} \equiv 1 \pmod{p},$$

или

$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \pmod{p},$$

или

$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \nmid p.$$

Отсюда видно, что, по крайней мере, одна из скобок должна делиться на p . Но обе скобки не могут делиться на p , так как в этом случае на p делилась бы и их разность 2, что невозможно, ибо $(2, p) = 1$.

Если a является квадратичным вычетом, то

$$a^{\frac{p-1}{2}} - 1 \mid p, \text{ т. е. } a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \quad (1)$$

Действительно, в этом случае существует такое значение x , $(x, p) = 1$, что

$$a \equiv x^2 \pmod{p},$$

откуда

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Так как по модулю p имеется $\frac{p-1}{2}$ квадратичных вычетов, то полученный результат означает, что сравнение (1) имеет $\geq \frac{p-1}{2}$ решений, если будем в нем a рассматривать как неизвестное. Но сравнение (1), как сравнение по простому модулю, не может иметь большее число решений, чем степень сравнения, т. е. больше чем $\frac{p-1}{2}$.

Итак, для всех квадратичных вычетов и только для них выполняется (1). Но тогда для остальных a ,

$(a, p) = 1$, т. е. для квадратичных невычетов и только для них

$$a^{\frac{p-1}{2}} + 1 \mid p,$$

или

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (2)$$

Критерий Эйлера доказан.

Пример. Установить, сколько решений имеет сравнение

$$x^2 \equiv 7 \pmod{19}.$$

Пользуясь критерием Эйлера, необходимо исследовать, с чем сравнимо

$$7^{\frac{19-1}{2}} \equiv 7^9 \pmod{19}.$$

По модулю 19 имеем

$$7^2 = 49 \equiv 11, \quad 7^3 \equiv 77 \equiv 1, \quad 7^9 \equiv 1.$$

Итак, сравнение разрешимо и имеет, следовательно, два решения.

Упражнения

140. Найти наименьшие положительные квадратичные вычеты и невычеты среди вычетов приведенной системы по модулям: 1) 11, 2) 13, 3) 19, 4) 23.

141. Пользуясь критерием Эйлера, установить, разрешимо ли сравнение: 1) $x^2 \equiv 7 \pmod{29}$; 2) $x^2 \equiv 5 \pmod{31}$; 3) $x^2 \equiv 8 \pmod{37}$; 4) $x^2 \equiv 37 \pmod{43}$.

142. Доказать, что сравнение $x^2 \equiv a \pmod{p^\alpha}$, $\alpha > 1$, $(a, p) = 1$, $(2, p) = 1$ разрешимо и имеет в таком случае 2 решения тогда и только тогда, когда разрешимо соответствующее сравнение для $\alpha = 1$.

143. Найти необходимые условия разрешимости сравнения $x^2 \equiv a \pmod{2^\alpha}$, $\alpha > 0$, $(a, 2) = 1$.

144. Найти достаточные условия разрешимости сравнения $x^2 \equiv a \pmod{2^\alpha}$, $(a, 2) = 1$, $\alpha = 1, 2, 3$ и соответствующие решения.

145. Доказать, что сравнение $x^2 \equiv a \pmod{16}$, $a \equiv 1 \pmod{8}$ имеет решения $x \equiv \pm x_4$, $\pm (x_4 + 8) \pmod{16}$, где x_4 — одно из решений данного сравнения. (Примечание. По модулю 2^α , $\alpha > 4$, аналогично $x \equiv \pm x_\alpha$, $\pm (x_\alpha + 2^{\alpha-1}) \pmod{2^\alpha}$).

146. Решить сравнение $x^2 \equiv 9 \pmod{16}$.

§ 10. Символ Лежандра

1. Символ Лежандра и его свойства

При больших значениях модуля p критерием Эйлера неудобно выяснять, является ли a квадратичным вычетом или нет. Эффективный способ получается, если применить символ, который ввел Лежандр. Этот символ $\left(\frac{a}{p}\right)$ (читается так: «символ Лежандра a по отношению к p ») определяется для нечетных простых p и чисел a , которые не делятся на p ; при этом a называется *числителем*, а p *знаменателем* символа.

Если a квадратичный вычет по модулю p , то символу $\left(\frac{a}{p}\right)$ сопоставляется число $+1$, т. е. $\left(\frac{a}{p}\right) = +1$; если a квадратичный невычет по модулю p , то символу $\left(\frac{a}{p}\right)$ сопоставляется число -1 , т. е. $\left(\frac{a}{p}\right) = -1$.

Пример. В примерах § 9 мы видели, что 7 является квадратичным вычетом по модулю 19, а 5—квадратичным невычетом по модулю 17, следовательно,

$$\left(\frac{7}{19}\right) = +1, \quad \left(\frac{5}{17}\right) = -1.$$

В силу критерия Эйлера получается следующее основное соотношение

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \quad (1)$$

Действительно, для всякого квадратичного вычета имеем одновременно

$$\left(\frac{a}{p}\right) = +1, \quad a^{\frac{p-1}{2}} \equiv +1 \pmod{p},$$

а для квадратичного невычета

$$\left(\frac{a}{p}\right) = -1, \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

откуда и вытекает соотношение (1).

Исследуем свойства символа Лежандра.

Свойство 1. Если $a \equiv a_1 \pmod{p}$, то

$$\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right). \quad (I)$$

Это свойство вытекает просто из того, что числа одного класса являются одновременно или квадратичными вычетами, или невычетами.

Воспользовавшись этим свойством, можно записать

$$\left(\frac{a}{p}\right) = \left(\frac{a + kp}{p}\right), \text{ где } k = 0, \pm 1, \pm 2, \dots$$

Свойство II. Символ

$$\left(\frac{1}{p}\right) = 1, \quad (II)$$

иными словами, 1 является квадратичным вычетом для любого нечетного простого p , или сравнение

$$x^2 \equiv 1 \pmod{p}, \quad (2, p) = 1,$$

всегда разрешимо.

Это действительно имеет место, так как указанное сравнение имеет решения

$$x \equiv \pm 1 \pmod{p}.$$

Свойство III. Символ

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \quad (III)$$

В самом деле, в силу сравнения (1) имеем

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Символ $\left(\frac{-1}{p}\right)$ может иметь значение $+1$ или -1 ; то

же можно сказать о выражении $(-1)^{\frac{p-1}{2}}$. Но так как по нечетному простому модулю p $(+1)$ и (-1) несравнимы, то мы должны иметь в обеих частях сравнения одновременно $+1$, или -1 .

Поэтому здесь

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Из этого свойства следует, что для простых чисел $p = 4m + 1$

$$\left(\frac{-1}{p}\right) = 1,$$

а для простых чисел $p = 4m + 3$

$$\left(\frac{-1}{p}\right) = -1.$$

Другими словами, для простых чисел вида $4m + 1$ число (-1) является квадратичным вычетом, а для простых чисел вида $4m + 3$ — квадратичным невычетом.

Пример. Сравнение

$$x^2 \equiv -1 \pmod{433},$$

разрешимо, так как простое число $433 \equiv 1 \pmod{4}$.
Сравнение

$$x^2 \equiv -1 \pmod{587},$$

неразрешимо, так как простое число

$$587 \equiv -1 \pmod{4}.$$

Свойство IV.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right). \quad (\text{IV})$$

В самом деле, в силу сравнения (1) имеем

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}.$$

Итак,

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p};$$

рассуждая далее так же, как при доказательстве свойства III, приходим к выводу, что имеет место равенство

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

Это свойство, очевидно, распространяется на случай k множителей.

В частности, из этого свойства следует

$$\left(\frac{a^2}{p}\right) = +1, \quad \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right),$$

а также и то, что произведение двух квадратичных вычетов или невычетов является квадратичным вычетом, произведение квадратичного вычета на квадратичный невычет — квадратичным невычетом.

Свойство V.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \quad (V)$$

Это важное свойство, доказательство которого приведем отдельно в третьем пункте, выразим для практического применения иным образом.

Если $p = 8m \pm 1$, то

$$\begin{aligned} \frac{p^2-1}{8} &= \frac{(8m \pm 1)^2 - 1}{8} = \frac{64m^2 \pm 16m}{8} = 8m^2 \pm 2m \equiv \\ &\equiv 0 \pmod{2}, \end{aligned}$$

т. е. число четное.

Если $p = 8m \pm 3$, то

$$\begin{aligned} \frac{p^2-1}{8} &= \frac{(8m \pm 3)^2 - 1}{8} = \frac{64m^2 \pm 48m + 8}{8} = \\ &= 8m^2 \pm 6m + 1 \equiv 1 \pmod{2}, \end{aligned}$$

т. е. число нечетное.

Поэтому имеем:

$$\text{для } p = 8m \pm 1 \text{ (или } 8m + 1, 8m + 7) \quad \left(\frac{2}{p}\right) = +1;$$

$$\text{для } p = 8m \pm 3 \text{ (или } 8m + 3, 8m + 5) \quad \left(\frac{2}{p}\right) = -1,$$

т. е. для простых чисел вида $8m \pm 1$ число 2 является квадратичным вычетом, а для простых чисел вида $8m \pm 3$ оно является квадратичным невычетом.

Примеры: 1) Установить, является ли 2 квадратичным вычетом по простому модулю 1097.

Так как $1097 \equiv 1 \pmod{8}$, то 2 является квадратичным вычетом;

2) разрешимо ли сравнение $x^2 \equiv 2 \pmod{1709}$?

Простое число $1709 \equiv 5 \pmod{8}$, поэтому сравнение неразрешимо.

Свойство VI. Закон взаимности нечетных простых чисел.

Если p и q нечетные простые числа, то

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \quad (\text{VI})$$

Доказательство этого важнейшего утверждения о квадратичных вычетах мы тоже дадим отдельно в четвертом пункте, здесь же отметим другое его выражение, удобное для практики.

Умножим предварительно обе части (VI) на $\left(\frac{p}{q}\right)$

Тогда

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right).$$

Отсюда: если хотя бы одно из чисел p или q имеет форму $4m+1$, то показатель в правой части равенства четный, поэтому

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

если же как p , так и q имеют форму $4m+3$, то показатель степени числа (-1) окажется числом нечетным и мы будем иметь

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Пример. Установить, разрешимо ли сравнение $x^2 \equiv 426 \pmod{491}$. 491 — простое число, поэтому можно дать ответ на поставленный вопрос, вычислив символ Лежандра $\left(\frac{426}{491}\right)$.

Во-первых, разлагаем 426 на множители:

$$426 = 2 \cdot 3 \cdot 71.$$

Поэтому, согласно (IV),

$$\left(\frac{426}{491}\right) = \left(\frac{2}{491}\right) \cdot \left(\frac{3}{491}\right) \cdot \left(\frac{71}{491}\right).$$

Далее имеем:

$$1) \left(\frac{2}{491}\right) = -1, \text{ так как } 491 \equiv 3 \pmod{8};$$

$$2) \left(\frac{3}{491}\right) = -\left(\frac{491}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1,$$

так как $491 \equiv 3 \pmod{4}$, а $3 \equiv 3 \pmod{8}$;

$$\begin{aligned} 3) \left(\frac{71}{491}\right) &= -\left(\frac{491}{71}\right) = -\left(\frac{65}{71}\right) = -\left(\frac{5}{71}\right) \cdot \left(\frac{13}{71}\right) = \\ &= -\left(\frac{71}{5}\right) \cdot \left(\frac{71}{13}\right) = -\left(\frac{1}{5}\right) \cdot \left(\frac{6}{13}\right) = -\left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) = \\ &= -(-1) \cdot \left(\frac{13}{3}\right) = 1 \cdot \left(\frac{1}{3}\right) = 1, \end{aligned}$$

так как $491 \equiv 71 \equiv 3 \pmod{4}$, $491 \equiv 65 \pmod{71}$, $5 \equiv 1 \pmod{4}$, $13 \equiv 1 \pmod{4}$, $13 \equiv 5 \pmod{8}$.

Следовательно, $\left(\frac{426}{491}\right) = (-1) \cdot 1 \cdot 1 = -1$, другими словами, данное сравнение неразрешимо.

2. Лемма Гаусса

Для доказательства свойства V найдем предварительно новое соотношение для символа Лежандра.

Пусть $(a, p) = 1$ и $(2, p) = 1$.

Обозначим абсолютно наименьший вычет произведения ax по модулю p через $\varepsilon_x \cdot r_x$, где $\varepsilon_x = +1$ или -1 , а r_x — абсолютное значение этого вычета. Подставим затем в выражение ax вместо x значения

$$1, 2, \dots, p_1 = \frac{p-1}{2}$$

и найдем соответствующие абсолютно наименьшие вычеты.

Пример. Для $a=5$, $p=19$ имеем по модулю 19:

$$\begin{array}{lll} 5 \cdot 1 = 5 \equiv +1.5 & 5 \cdot 4 = 20 \equiv +1.1 & 5 \cdot 7 = 35 \equiv -1.3 \\ 5 \cdot 2 = 10 \equiv -1.9 & 5 \cdot 5 = 25 \equiv +1.6 & 5 \cdot 8 = 40 \equiv +1.2 \\ 5 \cdot 3 = 15 \equiv -1.4 & 5 \cdot 6 = 30 \equiv -1.8 & 5 \cdot 9 = 45 \equiv +1.7 \end{array}$$

В общем случае имеем:

$$\left. \begin{aligned} \alpha \cdot 1 &\equiv \varepsilon_1 \cdot r_1 \pmod{p}, \\ \alpha \cdot 2 &\equiv \varepsilon_2 \cdot r_2 \pmod{p}, \\ &\vdots \\ \alpha \cdot p_1 &\equiv \varepsilon_{p_1} \cdot r_{p_1} \pmod{p}, \end{aligned} \right\} \quad (1)$$

откуда почленным перемножением получаем

$$a^{p_1} \cdot 1 \cdot 2 \dots p_1 = \varepsilon_1 \cdot \varepsilon_2 \dots \varepsilon_{p_1} \cdot r_1 \cdot r_2 \dots r_{p_1} \pmod{p}. \quad (2)$$

Мы сейчас убедимся в том, что

$$1 \cdot 2 \dots p_1 = r_1 \cdot r_2 \dots r_{p_1}. \quad (3)$$

Для этого запишем сначала приведенную систему вычетов по модулю p при помощи абсолютно наименьших вычетов

$$1, -1, 2, -2, \dots, p_1, -p_1. \quad (4)$$

Тогда по 2-й теореме о вычетах линейной формы система чисел

$$a \cdot 1, -a \cdot 1, a \cdot 2, -a \cdot 2, \dots, a p_1, -a p_1 \quad (5)$$

тоже составляет приведенную систему вычетов.

Заметим теперь, что если абсолютно наименьший вычет ax равен $\varepsilon_x r_x$, то абсолютно наименьший вычет $-ax$ равен $-\varepsilon_x r_x$.

Поэтому, в силу системы (1), абсолютно наименьшие вычеты приведенной системы (5) имеют вид

$$\varepsilon_1 \cdot r_1, -\varepsilon_1 \cdot r_1, \varepsilon_2 \cdot r_2, -\varepsilon_2 \cdot r_2, \dots, \varepsilon_{p_1} \cdot r_{p_1}, -\varepsilon_{p_1} \cdot r_{p_1}. \quad (6)$$

Таким образом, в (6) имеются те же числа, что и в системе (4), только возможно расположенные в ином порядке. Отсюда следует, что в совокупности положительные вычеты системы чисел (4), т. е. числа $1, 2, \dots, p_1$ должны совпасть с положительными вычетами системы (6), т. е. с числами r_1, r_2, \dots, r_{p_1} . Это и доказывает справедливость упомянутого равенства (3).

Так как, кроме того, каждое из чисел $1, 2, \dots, p_1$ взаимно просто с p , то можно обе части (2) разделить на их произведение, после чего получим соотношение

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \varepsilon_2 \dots \varepsilon_{p_1} \pmod{p}. \quad (7)$$

Отсюда, в силу $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, легко находим новое соотношение для символа Лежандра

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \varepsilon_2 \dots \varepsilon_{p_1}. \quad (8)$$

Последнее в несколько ином виде выражает знаменитую лемму Гаусса о том, что

$$\left(\frac{a}{p}\right) = (-1)^u,$$

где μ — число отрицательных вычетов среди абсолютно наименьших вычетов произведений $a \cdot 1, a \cdot 2, \dots, a \cdot p_1$ по модулю p .

Действительно, если в формуле (8) отбросить положительные ε_x , то из нее получается лемма Гаусса.

Из леммы Гаусса следует, что a является квадратичным вычетом, или невычетом по модулю p в зависимости от того, четно ли число μ или нечетно.

В рассмотренном выше примере $\mu = 4$, так что

$$\left(\frac{5}{19}\right) = (-1)^4 = 1,$$

поэтому 5 является квадратичным вычетом по модулю 19.

3. Доказательство свойства V символа Лежандра

Чтобы доказать свойство V, воспользуемся полученной формулой

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \varepsilon_2 \dots \varepsilon_{p_1} \quad (1)$$

для символа Лежандра, отыскав предварительно выражение для каждого ε_x в отдельности.

Проанализируем с этой целью, в каком случае $\varepsilon_x = +1$ и в каком -1 .

Начнем с примера.

Для $a = 5$ и $x = 9$ имеем: $5 \cdot 9 = 45 \equiv 7 \equiv +1 \cdot 7 \pmod{19}$; здесь остаток 7 от деления 45 на 19 совпадает с абсолютно наименьшим вычетом 45 по модулю 19, так как $7 < \frac{1}{2} \cdot 19$, поэтому

$$\varepsilon_9 = +1, \quad r_9 = 7.$$

Одновременно замечаем, что

$$\left\{\frac{45}{19}\right\} = \frac{7}{19} < \frac{1}{2}.$$

Для $a = 5$ и $x = 6$ имеем: $5 \cdot 6 = 30 \equiv 11 \equiv -1 \cdot 8 \pmod{19}$; здесь остаток 11 от деления 30 на 19 не совпадает с абсолютно наименьшим вычетом 30 по модулю 19, так как $11 > \frac{1}{2} \cdot 19$, абсолютно наимень-

ший вычет равен -8 , так что $\varepsilon_6 = -1$. $r_6 = 8$, одновременно

$$\left\{ \frac{30}{19} \right\} = \frac{11}{19} > \frac{1}{2}.$$

Очевидно, вообще $\varepsilon_x = +1$ в том и только в том случае, когда при делении ax на p получается остаток $< \frac{1}{2}p$ (т. е. когда по модулю p наименьший положительный вычет для ax меньше $\frac{1}{2}p$ и вместе с тем дробная часть $\left\{ \frac{ax}{p} \right\} < \frac{1}{2}$), и $\varepsilon_x = -1$ тогда и только тогда, когда указанный остаток $> \frac{1}{2}p$ (а дробная часть $\left\{ \frac{ax}{p} \right\} > \frac{1}{2}$).

Итак, имеем одновременно

$$1) \quad 0 < \left\{ \frac{ax}{p} \right\} < \frac{1}{2}, \text{ или } 0 < 2 \left\{ \frac{ax}{p} \right\} < 1 \text{ или} \\ \left[2 \left\{ \frac{ax}{p} \right\} \right] = 0 \text{ и } \varepsilon_x = +1;$$

$$2) \quad \frac{1}{2} < \left\{ \frac{ax}{p} \right\} < 1, \text{ или } 1 < 2 \left\{ \frac{ax}{p} \right\} < 2, \text{ или} \\ \left[2 \left\{ \frac{ax}{p} \right\} \right] = 1, \text{ и } \varepsilon_x = -1.$$

Для дальнейшего воспользуемся ещё равенством

$$\frac{ax}{p} = \left[\frac{ax}{p} \right] + \left\{ \frac{ax}{p} \right\},$$

из которого следует

$$\frac{2ax}{p} = 2 \left[\frac{ax}{p} \right] + 2 \left\{ \frac{ax}{p} \right\}, \\ \left[\frac{2ax}{p} \right] = 2 \left[\frac{ax}{p} \right] + \left[2 \left\{ \frac{ax}{p} \right\} \right]. \quad (2)$$

Заметим, например, что $\left[13\frac{3}{4} \right] = 10 + \left[3\frac{3}{4} \right]$; подробнее см. задачу 99.

Последнее соотношение дает возможность отмеченные в 1) и 2) факты выразить следующим образом. Имеем одновременно:

- 1) $\left[\frac{2ax}{p} \right]$ число четное и $\varepsilon_x = +1$;
- 2) $\left[\frac{2ax}{p} \right]$ число нечетное и $\varepsilon_x = -1$.

Таким образом, имеем возможность представить ε_x в следующем виде:

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p} \right]}. \quad (3)$$

При помощи этого выражения соотношение (1) переходит в формулу

$$\left(\frac{a}{p} \right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{2ax}{p} \right]} \quad (4)$$

Используя (4), запишем теперь $\left(\frac{2a}{p} \right)$, предполагая при этом, что a — нечетное.

Имеем

$$\begin{aligned} \left(\frac{2a}{p} \right) &= \left(\frac{2a + 2p}{p} \right) = \left(\frac{4}{p} \right) \cdot \left(\frac{1/2(a + p)}{p} \right) = \\ &= \left(\frac{1/2(a + p)}{p} \right)^{\left[\frac{(a+p) \cdot 1}{p} \right]} = \\ &= (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p} \right] + \sum_{x=1}^{p_1} x} = \\ &= (-1)^{\sum_{x=1}^{p_1} x} \end{aligned}$$

но так как

$$\sum_{x=1}^{p_1} x = 1 + 2 + \dots + p_1 = \frac{(1 + p_1)p_1}{2} = \frac{p^2 - 1}{8}.$$

то из предыдущего следует

$$\left(\frac{2}{p}\right) \left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}} \quad (5)$$

Если теперь в (5) подставить $a = 1$, то

$$\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] = \left[\frac{1}{p}\right] + \left[\frac{2}{p}\right] + \dots + \left[\frac{p_1}{p}\right] = 0,$$

и мы получаем

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

т. е. свойство V символа Лежандра.

4. Доказательство закона взаимности

В силу свойства V соотношение (5) предыдущего пункта принимает вид

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]} \quad (1)$$

где a — нечетное число, а $p_1 = \frac{p-1}{2}$.

Поэтому для нечетных простых p и q можем написать

$$\left(\frac{q}{p}\right) = (-1)^\alpha, \quad \alpha = \sum_{x=1}^{p_1} \left[\frac{qx}{p}\right], \quad p_1 = \frac{p-1}{2},$$

$$\left(\frac{p}{q}\right) = (-1)^\beta, \quad \beta = \sum_{y=1}^{q_1} \left[\frac{py}{q}\right], \quad q_1 = \frac{q-1}{2},$$

откуда

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\alpha+\beta}. \quad (2)$$

Так как числа, сравнимые по модулю 2, имеют одинаковую четность, то остается доказать, что

$$\alpha + \beta \equiv p_1 \cdot q_1 \pmod{2}.$$

Покажем, что имеет место даже равенство указанных выражений. Для этого построим в прямоугольной

системе координат прямоугольник с вершинами $O(0, 0)$, $A\left(\frac{p}{2}, 0\right)$, $B\left(\frac{p}{2}, \frac{q}{2}\right)$ и $C\left(0, \frac{q}{2}\right)$ (см. рис. 1) и, отметив на сторонах этого прямоугольника OA и OC соответственно точки с абсциссами $x = 1, 2, \dots, p_1 = \frac{p-1}{2}$ и ординатами $y = 1, 2, \dots, q_1 = \frac{q-1}{2}$, найдем число его внутренних целочисленных точек¹. Сопоставление результатов двух таких подсчетов приводит нас к искомому соотношению.

С одной стороны, считая по рядам и по столбцам, мы сразу же видим, что число внутренних целочисленных точек равно произведению $p_1 \cdot q_1$.

Перейдем теперь к другому подсчету.

Предварительно заметим, что внутри отрезка OB нет целочисленных точек. В самом деле, уравнение прямой OB имеет вид $y = \frac{q}{p}x$ и, когда x пробегает значения

$$1, 2, \dots, \frac{p-1}{2},$$

y не может стать целым числом.

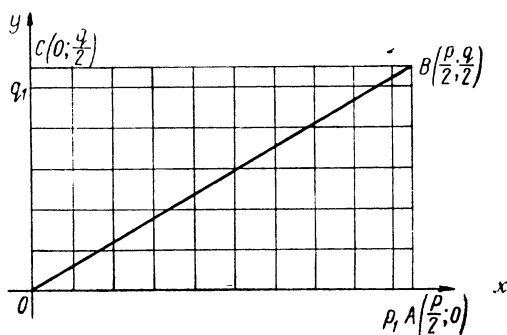


Рис. 1.

Таким образом, остается подсчитать количество целочисленных точек внутри треугольников OAB и OBC .

¹ Целочисленные или целые точки — точки, координаты которых целые числа.

Целые точки внутри треугольника OAB имеются только на прямых $x = k$, где $k = 1, 2, \dots, p_1$. Каждая из них пересекает OB в точке $\left(k, \frac{qk}{p}\right)$ и количество целых точек такой прямой, расположенных между осью Ox и OB , равно $\left[\frac{qk}{p}\right]$.

Поэтому число целых точек внутри треугольника OAB равно сумме

$$\left[\frac{q \cdot 1}{p}\right] + \left[\frac{q \cdot 2}{p}\right] + \dots + \left[\frac{q \cdot p_1}{p}\right] = \sum_{x=1}^{p_1} \left[\frac{qx}{p}\right] = \alpha.$$

Рассматривая аналогично прямые $y = l$, где $l = 1, 2, \dots, q_1$, найдем, что число целых точек внутри треугольника OBC равно сумме

$$\left[\frac{p \cdot 1}{q}\right] + \left[\frac{p \cdot 2}{q}\right] + \dots + \left[\frac{p \cdot q_1}{q}\right] = \sum_{y=1}^{q_1} \left[\frac{py}{q}\right] = \beta.$$

Таким образом, второй подсчет показывает, что число целых точек в прямоугольнике $OABC$ равно

$$\alpha + \beta = p_1 \cdot q_1.$$

В силу этого соотношения из формулы (2) получается закон взаимности

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Этот закон, который Гаусс справедливо называет «фундаментальной теоремой» о квадратичных вычетах, впервые эмпирически был найден Эйлером в 1772 г. и опубликован им в 1783 г. Независимо от Эйлера к этому закону в 1785 г. пришел Лежандр, но и он не сумел еще дать строгого его доказательства.

Впервые закон взаимности был доказан Гауссом в 1796 г. В дальнейшем ему удалось найти еще 6 других доказательств этого закона. После Гаусса можно насчитать около 150 доказательств, данных другими учеными. Изложенное доказательство дано Эйзенштейном.

5. Символ Якоби и его свойства

Еще более эффективным, чем символ Лежандра, является символ Якоби $\left(\frac{a}{P}\right)$ (читается «символ Якоби a по отношению к P »). Он определяется для любых нечетных положительных чисел $P > 1$ и чисел a , взаимно простых с P , равенством

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right),$$

где $P = p_1 p_2 \cdots p_k$ является разложением P на простые множители (среди них могут быть и равные), т. е. как произведение символов Лежандра.

Символ Лежандра является, таким образом, частным случаем символа Якоби. Для него сохраняются формулы I—VI символа Лежандра с той лишь разницей, что в случае символа Якоби речь идет не о нечетных простых числах p , а о нечетных числах P .

Поэтому при вычислении символа Лежандра (для определения квадратичности вычета по простому нечетному модулю) удобно рассматривать его как символ Якоби. Тогда отпадает необходимость выделять из числителя символа его нечетные простые множители.

Так, например, символ Лежандра (ср. с п. 1 этого параграфа)

$$\begin{aligned} \left(\frac{426}{491}\right) &= \left(\frac{2}{491}\right) \cdot \left(\frac{213}{491}\right) = - \left(\frac{213}{491}\right) = - \left(\frac{491}{213}\right) = \\ &= - \left(\frac{65}{213}\right) = - \left(\frac{213}{65}\right) = - \left(\frac{18}{65}\right) = - \left(\frac{2}{65}\right) \cdot \left(\frac{9}{65}\right) = -1. \end{aligned}$$

Заметим, что по значению символа Якоби можно о квадратичности вычета a по модулю P сказать следующее: если $\left(\frac{a}{P}\right) = -1$, то a является квадратичным невычетом по модулю P ; если же $\left(\frac{a}{P}\right) = 1$, а P — число составное или неизвестно, простое ли оно, то о квадратичности вычета a по модулю P непосредственно судить нельзя.

Упражнения

147. Определить символы Лежандра: 1) $\left(\frac{19}{67}\right)$, 2) $\left(\frac{56}{73}\right)$, 3) $\left(\frac{54}{83}\right)$,
 4) $\left(\frac{297}{337}\right)$, 5) $\left(\frac{157}{401}\right)$, 6) $\left(\frac{165}{373}\right)$, 7) $\left(\frac{238}{593}\right)$, 8) $\left(\frac{114}{277}\right)$, 9) $\left(\frac{1015}{1621}\right)$,
 10) $\left(\frac{230}{457}\right)$.

148. Определить символы Лежандра, пользуясь свойствами символа Якоби: 1) $\left(\frac{323}{607}\right)$, 2) $\left(\frac{283}{563}\right)$, 3) $\left(\frac{374}{523}\right)$, 4) $\left(\frac{237}{499}\right)$,
 5) $\left(\frac{346}{643}\right)$.

149. Установить, проходят ли следующие параболы через целые точки:

- 1) $73y = x^2 - 37$; 2) $83y = x^2 - 34$;
 3) $443y = x^2 - 152$; 4) $43y = x^2 - 42$.

150. Установить, разрешимо ли сравнение:

- 1) $x^2 \equiv 37 \pmod{93}$; 2) $x^2 \equiv 29 \pmod{105}$;
 3) $x^2 \equiv 31 \pmod{77}$; 4) $x^2 \equiv 51 \pmod{175}$;
 5) $x^2 \equiv 54 \pmod{143}$; 6) $x^2 \equiv 20 \pmod{171}$;
 7) $x^2 \equiv 23 \pmod{1189}$.

151. Для каких целых значений a : 1) $3a^2 - 5$ делится на 17;
 2) $7a^2 + 13$ делится на 23; 3) $13a^2 - 11$ делится на 29?

152. Доказать свойства символа Якоби.

153. Для каких нечетных простых p число 3 является квадратичным вычетом?

154. Для каких нечетных простых p число -3 является квадратичным вычетом?

155. Для квадратичного вычета a по простому модулю $p=4k+3$ найти решение сравнения $x^2 \equiv a \pmod{p}$.

156. Для квадратичного вычета a по простому модулю $p=8k+5$ доказать, что либо $a^{2k+2} \equiv a \pmod{p}$, либо $a^{2k+2} \equiv -a \pmod{p}$.

157. Для квадратичного вычета a по простому модулю $p=8k+5$ найти решение сравнения $x^2 \equiv a \pmod{p}$.

158. Применить результаты задач 155 и 157 к решению сравнений:

- 1) $x^2 \equiv 7 \pmod{19}$; 2) $x^2 \equiv 6 \pmod{29}$.

159. Найти: 1) условия разрешимости сравнения

$$x^2 \equiv a \pmod{m}, \quad (a, m) = 1, \quad m = 2^a \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k};$$

2) в случае разрешимости число решений.

Глава IV

СТЕПЕННЫЕ ВЫЧЕТЫ

§ 1. Показатели и их основные свойства

1. Число, принадлежащее показателю. Первообразный корень

Пусть $(a, m) = 1$; тогда по теореме Эйлера

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \quad (1)$$

Здесь содержится, очевидно, следующее более слабое утверждение: если $(a, m) = 1$, то существуют такие натуральные числа γ , что

$$a^{\gamma} \equiv 1 \pmod{m}^1. \quad (2)$$

В самом деле, по крайней мере одно такое число нам известно по теореме Эйлера, а именно $\varphi(m)$. Кроме того, ясно, что и кратные $\varphi(m)$ будут такими же числами.

Наименьшее из чисел γ , обозначаемое в дальнейшем через δ (такое обязательно существует, так как числа γ натуральные),² мы будем называть показателем, которому a принадлежит по модулю m , или показателем a по модулю m .

Итак, натуральное число δ является по модулю m показателем для числа a , взаимно простого с m , если

$$a^{\delta} \equiv 1 \pmod{m} \quad (3)$$

¹ Заметим, что если $(a, m) = d > 1$, то $a^{\gamma} \equiv 1 \pmod{m}$ невозможно, так как правая часть сравнения (1) не делится на d .

² Мы применяем здесь одну из эквивалентных форм аксиомы математической индукции, так называемый принцип наименьшего числа: любое непустое множество натуральных чисел содержит наименьшее число.

и $\delta \leq \gamma$, коль скоро $a^\gamma \equiv 1 \pmod{m}$, или $a^x \not\equiv 1 \pmod{m}$, коль скоро $1 \leq x < \delta$.

Ясно, что δ не превосходит $\varphi(m)$, т. е. $\delta \leq \varphi(m)$. В частном случае, когда a по модулю m принадлежит показателю $\varphi(m)$, т. е. $\delta = \varphi(m)$, a называют *первообразным корнем* по модулю m . Отсюда следует, что если a является первообразным корнем по простому модулю p , то a принадлежит показателю $\varphi(p) = p-1$.

Рассмотрим примеры нахождения показателя, которому a принадлежит по модулю m .

Составим для этого ряд чисел a^1, a^2, a^3 и т. д., пока впервые не натолкнемся на такое δ , что $a^\delta \equiv 1 \pmod{m}$.

1. Найдем показатель, которому принадлежит 2 по модулю 7.

Имеем по модулю 7

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8 \equiv 1 \pmod{7}.$$

Итак, 2 принадлежит показателю 3 по модулю 7, первообразным корнем по модулю 7 число 2 не является.

2. Найдем показатель, которому 3 принадлежит по модулю 7.

По модулю 7

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv -1, \quad 3^4 \equiv -3, \quad 3^5 \equiv -2, \quad 3^6 \equiv 1.$$

Итак, 3 принадлежит показателю 6, вместе с тем 3 является первообразным корнем по модулю 7.

3. Найдем показатель, которому 5 принадлежит по модулю 7.

По модулю 7

$$5^1 \equiv -2, \quad 5^2 \equiv -3, \quad 5^3 \equiv -1, \quad 5^4 \equiv 2, \quad 5^5 \equiv 3, \quad 5^6 \equiv 1.$$

Итак, 5 принадлежит показателю 6 по модулю 7, значит тоже является первообразным корнем по модулю 7.

Примеры 2 и 3 показывают, что по одному и тому же модулю бывают разные первообразные корни.

Перейдем теперь к изучению свойств показателей

2. Классы, принадлежащие показателю

Покажем, что сравнимые числа, т. е. числа одного класса по модулю m , принадлежат по этому модулю одному и тому же показателю.

Пример. В предыдущем пункте мы видели, что 2 принадлежит показателю 3 по модулю 7. Этому же показателю принадлежит $9 \equiv 2 \pmod{7}$.

Действительно,

$$9^1 \equiv 2, \quad 9^2 \equiv 4, \quad 9^3 \equiv 8 \equiv 1 \pmod{7}.$$

Доказательство. Допустим противное, а именно, что $a \equiv a_1 \pmod{m}$ и при этом $\delta < \delta_1$ или $\delta > \delta_1$ (где δ и δ_1 показатели, которым соответственно принадлежат a и a_1 по модулю m). Первое предположение исключается, так как из $a^\delta \equiv 1 \pmod{m}$ и $a \equiv a_1 \pmod{m}$ следует, что $a_1^\delta \equiv 1 \pmod{m}$, и если a_1 принадлежит показателю δ_1 , то должно быть $\delta_1 \leq \delta$, а по условию $\delta < \delta_1$.

Аналогично можно также показать невозможность второго предположения. Таким образом, остается принять, что $\delta = \delta_1$.

Доказанное свойство показывает, что имеет смысл говорить о *классах, принадлежащих показателю по модулю m* (подразумеваются классы вычетов, взаимно простых с модулем, так как, согласно подстрочному замечанию на стр. 125, о других классах не может быть речи) и о классах первообразных корней по модулю m .

3. Свойства системы чисел $a^0, a^1, \dots, a^{\delta-1}$

Система чисел

$$1 = a^0, a^1, \dots, a^{\delta-1}, \quad (1)$$

где δ — показатель, которому a принадлежит по модулю m , обладает очень важным свойством, а именно — ее члены несравнимы по модулю m . Это утверждение следует из того, что противное предположение

$$a^l \equiv a^k \pmod{m}, \quad \delta - 1 \geq l > k \geq 0$$

приводит к противоречию. Действительно, из условия, что $(a, m) = 1$, получаем

$$a^{l-k} \equiv 1 \pmod{m}, \quad 0 < l - k < \delta,$$

но это невозможно, так как a принадлежит показателю δ по модулю m (см. (3) п. 1).

Из указанного свойства следует, что в случае первообразного корня, т. е. когда $\delta = \varphi(m)$, (1) переходит в ряд чисел

$$1 = a^0, a^1, \dots, a^{\varphi(m)-1}, \quad (2)$$

образующий приведенную систему вычетов по модулю m .

В самом деле, ряд чисел (2) удовлетворяет признаку приведенной системы вычетов:

- 1) (2) содержит $\varphi(m)$ чисел;
- 2) последние взаимно просты с m , так как $(a, m)=1$;
- 3) они, как мы это только что показали, принадлежат различным классам.

По простому модулю p ряд (2) принимает вид

$$1 = a^0, a^1, \dots, a^{p-2}. \quad (3)$$

Пример. Составим ряд чисел (3) для первообразного корня 3 по модулю 7.

Получаем систему чисел

$$1 = 3^0, 3^1, 3^2, 3^3, 3^4, 3^5;$$

их наименьшие положительные вычеты (см. 2-й пример 1-го пункта)

$$1, 3, 2, 6, 4, 5$$

очевидно, образуют приведенную систему вычетов по модулю 7.

4. Необходимое и достаточное условие сравнимости a^γ и $a^{\gamma'}$ по модулю m , если a принадлежит показателю δ по модулю m

В дальнейшем мы часто будем пользоваться следующей важной теоремой: *при a , принадлежащем показателю δ по модулю m , $a^\gamma \equiv a^{\gamma'} \pmod{m}$ тогда и только тогда, когда $\gamma \equiv \gamma' \pmod{\delta}$, т. е. когда γ и γ' принадлежат одному классу по модулю δ .*

В частности, $a^\gamma \equiv 1 \pmod{m}$ тогда и только тогда, когда $\gamma \equiv 0 \pmod{\delta}$, т. е. когда γ делится на δ .

Доказательство: 1) пусть a принадлежит показателю δ по модулю m и $a^\gamma \equiv a^{\gamma'} \pmod{m}$. Тогда, представив γ и γ' в виде

$$\gamma = \delta q + r \quad \text{и} \quad \gamma' = \delta q' + r', \quad 0 \leq r < \delta, \quad 0 \leq r' < \delta,$$

получим $a^{\delta q+r} \equiv a^{\delta q'+r'} \pmod{m}$, или

$$(a^\delta)^q a^r \equiv (a^\delta)^{q'} a^{r'} \pmod{m}.$$

Но $a^\delta \equiv 1 \pmod{m}$, поэтому из предыдущего следует

$$a^r \equiv a^{r'} \pmod{m}, \quad 0 \leq r < \delta, \quad 0 \leq r' < \delta.$$

Числа a^r и $a^{r'}$ принадлежат ряду (1) п. 3, который содержит вычеты лишь из разных классов. Поэтому их сравнимость означает, что они равны, т. е. $a^r = a^{r'}$, откуда вытекает, что $r = r'$, или

$$\gamma \equiv \gamma' \pmod{\delta};$$

2) если, наоборот, $\gamma \equiv \gamma' \pmod{\delta}$, или

$$\gamma = \delta q + r, \quad \gamma' = \delta q' + r, \quad 0 \leq r < \delta$$

и a принадлежит показателю δ по модулю m , ввиду чего $a^\delta \equiv 1 \pmod{m}$, то имеем

$$(a^\delta)^q \equiv (a^\delta)^{q'} \pmod{m},$$

$$a^{\delta q} \cdot a^r \equiv a^{\delta q'} \cdot a^r \pmod{m},$$

или $a^{\delta q+r} \equiv a^{\delta q'+r} \pmod{m}$, или $a^\gamma \equiv a^{\gamma'} \pmod{m}$. Теорема доказана.

Указанный в теореме частный случай получается, если берем $\gamma' = 0$. Из частного случая вытекают важные следствия.

Следствие 1. Показатель δ , которому a принадлежит по модулю m , является делителем $\varphi(m)$ (а по простому модулю p — делителем $\varphi(p) = p - 1$), так как $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Это следствие дает возможность следующим образом упростить нахождение δ : проверяются не все степени от a , начиная с a^1, a^2, \dots , а только те, показатели которых делят $\varphi(m)$.

Так, например, для нахождения показателя, которому 3 принадлежит по модулю 7 (см. 2-й пример 1-го пункта), достаточно испытать подряд: $3^1, 3^2, 3^3, 3^6$, потому что $\varphi(7) = 6$ имеет делители 1, 2, 3 и 6.

Рассмотрим следующий пример: найти показатель, которому 5 принадлежит по модулю 17.

Имеем $\varphi(17) = 16$, делители 16 суть: 1, 2, 4, 8, 16.

Находим по модулю 17

$$5^1 \equiv 5, \quad 5^2 = 25 \equiv 8, \quad 5^4 \equiv 64 \equiv -4, \\ 5^8 \equiv 16 \equiv -1, \quad 5^{16} \equiv 1.$$

Итак, 5 является первообразным корнем по модулю 17.

Следствие 2. Если a принадлежит показателю δ по модулю m , то a^k принадлежит показателю $\frac{\delta}{(\delta, k)}$ по модулю m .

В самом деле, пусть a^k принадлежит показателю γ по модулю m , так что γ — наименьшее натуральное число, для которого $(a^k)^\gamma \equiv 1 \pmod{m}$, или $a^{k\gamma} \equiv 1 \pmod{m}$. Согласно доказанной теореме последнее выполняется тогда и только тогда, когда $k\gamma \equiv 0 \pmod{\delta}$, или $\gamma \equiv 0 \pmod{\frac{\delta}{(\delta, k)}}$. Наименьшее γ , удовлетворяющее этому условию, равно $\frac{\delta}{(\delta, k)}$, что и утверждалось.

Если, в частности, $(\delta, k) = 1$, то a^k принадлежит тому же самому показателю δ по модулю m , что и число a , а если $(\delta, k) > 1$, то меньшему.

Примеры. 1). 2 принадлежит показателю 3 по модулю 7, $2^2 = 4$ также принадлежит показателю 3 по модулю 7, так как $(2, 3) = 1$; действительно, по модулю 7 имеем: $4 \equiv -3, 4^2 \equiv 2, 4^3 \equiv 1$.

2). 3 принадлежит показателю 6 по модулю 7, $3^4 = 81$ принадлежит показателю 3 по модулю 7, так как $\frac{6}{(6, 4)} = 3$; действительно, по модулю 7 имеем: $81 \equiv -3, 81^2 \equiv 2, 81^3 \equiv 1$.

Упражнения

160. Число 5 является показателем 4 по модулю 11; может ли существовать натуральное число $n < 5$, удовлетворяющее условию $4^n \equiv 1 \pmod{11}$? Обосновать ответ.

161. $9^3 \equiv 1 \pmod{28}$; может ли 9 принадлежать показателю 6 по модулю 28? Обосновать ответ.

162. 1). Зная, что 5 является первообразным корнем по модулю 18, составить приведенную систему вычетов по модулю 18 при помощи степеней числа 5. Найти наименьшие положительные вычеты указанных степеней по модулю 18; 2) то же для первообразного корня 3 по модулю 19.

163. Может ли существовать число, принадлежащее показателю 5 по модулю 26? Обосновать ответ.

164. Проверить, сравнимы ли 2^{23} и 2^6 по модулю 11.

165. Какому показателю принадлежит a по модулю m для следующих значений a и m (соответственно): 1) 3, 17; 2) 3, 19; 3) 4, 21; 4) 5, 18; 5) 5, 23; 6) 7, 24? Является ли a первообразным корнем по модулю m ?

166. Доказать, что для целого положительного a и натурального n $\varphi(a^n - 1)$ делится на n .

167. 1) Зная, что 12 принадлежит показателю 6 по модулю 19, найти показатели для 12^3 , 12^4 и 12^5 по этому модулю; 2) зная, что 6 есть первообразный корень по модулю 41, найти показатели для 6^{12} , 6^{15} , 6^{16} по этому модулю.

168. Доказать, что если a принадлежит четному показателю δ по нечетному простому модулю p , то $a^{\delta/2} \equiv -1 \pmod{p}$.

169. Зная, что по взаимно простым модулям m_1 и m_2 число a принадлежит соответственно показателям δ_1 и δ_2 , найти показатель δ для a по модулю $m_1 m_2$.

170. Найти показатели для: 1) 2 по модулю 35 и 2) 3 по модулю 55, пользуясь свойством, вытекающим из предыдущей задачи, и независимо от него.

171. Доказать, что если по модулю m показатель для $a_1 - \delta_1$, для $a_2 - \delta_2$, а для $a_1 a_2 - \delta$, то $\delta_1 \delta_2 \mid \delta$; в частности, когда $(\delta_1, \delta_2) = 1$, $\delta = \delta_1 \delta_2$.

172. Зная, что по модулю 37 число 10 принадлежит показателю 3, а 31 показателю 4, найти, к какому показателю по этому же модулю принадлежит 14. (Воспользоваться результатом предыдущей задачи.)

§ 2. Существование и число классов, принадлежащих показателю

1. Лемма о числе классов, принадлежащих показателю (по простому модулю p)

В предыдущем параграфе мы установили, что каждый класс вычетов по модулю m , взаимно простых с модулем, принадлежит некоторому показателю δ , который обязательно является делителем $\varphi(m)$.

Возникает вопрос, можно ли утверждать обратное, т. е. что по модулю m каждый делитель $\varphi(m)$ является показателем некоторого класса, в частности, что само число $\varphi(m)$ всегда является показателем некоторого класса, или что для любого m существует класс первообразных корней. Этот вопрос можно выразить и так: исчерпывают ли показатели классов вычетов по модулю m все делители $\varphi(m)$?

Оказывается, что не для любого модуля m поставленный вопрос имеет положительный ответ, а только для простого модуля $m = p$ и некоторых других категорий чисел.

Наиболее важным в практическом отношении является случай, когда $m = p$. Он будет подробно рассмотрен в этом параграфе. Будет также показано, сколько указанных классов вычетов существует.

В выяснении этих вопросов имеет значение лемма: *по простому модулю p делитель δ числа $p - 1$ либо не является показателем какого-либо класса вычетов либо является для $\varphi(\delta)$ таких классов.*

Эту лемму можно выразить и так: если по простому модулю p существует хотя бы один класс, принадлежащий показателю δ (где δ делитель числа $p - 1$), то таких классов имеется $\varphi(\delta)$.

Доказательство. Отметим, во-первых, что утверждение леммы можно отнести к числу вычетов приведенной системы по модулю p , так как каждому вычету из приведенной системы, принадлежащему показателю δ , соответствует класс, принадлежащий этому же показателю, и наоборот.

Обозначив через $\psi(\delta)$ число вычетов приведенной системы по модулю p , принадлежащих по этому модулю показателю δ , можно утверждать: $\psi(\delta)$ либо равно нулю, либо не меньше единицы.

Если $\psi(\delta) = 0$, то нечего доказывать.

Предположим поэтому, что $\psi(\delta)$ равно хотя бы единице, т. е. что δ является показателем некоторого a , и постараемся найти все вычеты приведенной системы по модулю p , принадлежащие этому показателю.

Так как все числа, принадлежащие показателю δ по модулю p , должны удовлетворять сравнению

$$x^\delta \equiv 1 \pmod{p}, \quad (1)$$

то ясно, что указанные вычеты следует искать среди решений этого сравнения.

Но решения сравнения (1) исчерпываются классами по модулю p , которые имеют вычеты

$$a^0, a^1, \dots, a^k, \dots, a^{\delta-1}. \quad (2)$$

Действительно, все числа этого ряда

1) удовлетворяют (1), ибо $(a^k)^\delta = (a^\delta)^k \equiv 1 \pmod{p}$,

2) принадлежат разным классам по модулю p (см. п. 3, § 1) и 3) их число равно δ , т. е. максимально возможному количеству решений (1) (сравнение (1), имея простой модуль p и степень δ , не может иметь больше чем δ решений).

Поэтому остается разыскать среди чисел ряда (2) те, которые принадлежат показателю δ по модулю p .

Согласно второму следствию п. 4 § 1 такими числами являются те и только те числа a^k , для которых $(\delta, k) = 1$; но таких чисел в ряде (2) имеется $\varphi(\delta)$ (поскольку k пробегает в (2) все значения из полной системы вычетов по модулю δ , а в последней содержится $\varphi(\delta)$ вычетов, взаимно простых с δ). Итак, в данном случае $\psi(\delta) = \varphi(\delta)$, чем и завершается доказательство леммы.

Пример. По модулю 19 число 4 принадлежит показателю 9 (предлагается проверить это). Найти все вычеты приведенной системы по модулю 19, принадлежащие этому же показателю по модулю 19.

Искомými числами являются

$$4^1, 4^2, 4^4, 4^5, 4^7, 4^8,$$

так как числа 1, 2, 4, 5, 7, 8 образуют приведенную систему вычетов по модулю 9.

Их количество равно $\varphi(9) = 6$; располагая их наименьшие положительные вычеты по модулю 19 в порядке возрастания, получаем, как это легко проверить, числа 4, 5, 6, 9, 16, 17.

2. Теорема о существовании и числе классов, принадлежащих показателю по простому модулю

Доказанная лемма, которую можно записать в форме

$$\psi(\delta) = \begin{cases} 0 \\ \varphi(\delta) \neq 0, \end{cases} \quad (1)$$

не дает еще определенного ответа на вопрос о числе классов $\psi(\delta)$, принадлежащих показателю δ по простому модулю p .

Между тем, справедлива следующая совершенно определенная и очень важная теорема: *по простому*

модулю p каждый делитель δ числа $p - 1$ является показателем для $\varphi(\delta)$ классов (или вычетов приведенной системы); в частности, существует $\varphi(p - 1)$ классов первообразных корней.

Проверим сначала справедливость теоремы на числовом примере.

Пусть, например, $p = 13$; тогда $p - 1 = 12$, а делители $p - 1$ суть числа: 1, 2, 3, 4, 6, 12.

Числа приведенной системы по модулю 13

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

распределяются по принадлежности к своим показателям согласно (вычисления опущены) следующей таблице:

Делители δ	Числа, принадлежащие показателю δ	$\psi(\delta)$	$\varphi(\delta)$
1	1	1	1
2	12	1	1
3	3, 9	2	2
4	5, 8	2	2
6	4, 10	2	2
12	2, 6, 7, 11	4	4
	Количество распределенных чисел: $p - 1 = 12$	$\sum \psi(\delta) = 12$	$\sum \varphi(\delta) = 12$

Доказательство теоремы. Пусть $\delta_1 = 1, \delta_2, \dots, \delta_k = p - 1$ все делители числа $p - 1$. Распределяя числа 1, 2, ..., $p - 1$, т. е. вычеты приведенной системы по модулю p , в отдельные группы по принадлежности к своему показателю, мы должны, конечно, во всех группах вместе получить число распределенных чисел, т. е. $p - 1$.

Таким образом,

$$\psi(\delta_1) + \psi(\delta_2) + \dots + \psi(\delta_k) = p - 1. \quad (2)$$

С другой стороны, нам известно, что сумма значений функций Эйлера, распространенная по всем делителям данного числа, равна этому числу, так что

$$\varphi(\delta_1) + \varphi(\delta_2) + \dots + \varphi(\delta_k) = p - 1. \quad (3)$$

Итак,

$$\psi(\delta_1) + \psi(\delta_2) + \dots + \psi(\delta_k) = \varphi(\delta_1) + \varphi(\delta_2) + \dots + \varphi(\delta_k), \quad (4)$$

откуда в силу (1) легко обнаружить, что всегда $\psi(\delta_i) = \varphi(\delta_i)$. Действительно, если хотя бы в одном случае допустить, что $\psi(\delta_i)$ равно нулю, в правой части равенства (4) останется лишний положительный член и равенство нарушится. Итак, теорема доказана.

Применяя доказанную теорему к делителю $\delta_k = p - 1$, мы получаем теорему о числе классов первообразных корней: *по простому модулю p существует $\varphi(p - 1)$ классов первообразных корней.*

Доказательство, которое мы привели, принадлежит Гауссу и считается одним из самых блестящих арифметических рассуждений.

В заключение заметим, что первообразные корни существуют только по модулям $m = 2, 4, p^\alpha$ и $2p^\alpha$, где p — простое нечетное число, а $\alpha \geq 1$.

В 1918 г. И. М. Виноградов доказал, что для простого числа p всегда существует первообразный корень, меньший, чем $2^{2^k} \sqrt[p]{\ln p}$, где k — число различных простых делителей $p - 1$.

Что касается самого нахождения первообразного корня, то до сих пор эффективный алгоритм для этого еще не найден.

Упражнения

173. Зная, что a принадлежит показателю δ по модулю p , найти в приведенной системе наименьших положительных вычетов по этому модулю все вычеты, принадлежащие показателю δ ; значения a , δ и p (соответственно): 1) 7, 7, 29, 2) 9, 9, 37.

174. Зная, что a является первообразным корнем по простому модулю p , найти в приведенной системе наименьших положительных вычетов по этому модулю все первообразные корни; значения a и p (соответственно): 1) 2, 11; 2) 5, 23.

175. Зная, что a принадлежит показателю δ по простому модулю p , найти все решения сравнения $x^\delta \equiv 1 \pmod{p}$; значения a , δ и p (соответственно): 1) 3, 5, 11; 2) 4, 6, 13.

176. Найти число классов первообразных корней по модулям: 1) 17, 2) 43, 3) 73, 4) 89.

177. Найти число классов, принадлежащих показателю 1) 7 по модулю 29, 2) 9 по модулю 37.

178. Путем испытаний найти наименьший положительный первообразный корень по модулю 23.

179. Доказать, что первообразный корень по модулю $m > 2$ всегда является квадратичным невычетом по модулю m .

180. Доказать существование первообразных корней по модулям 2 и 4; найти их наименьшие положительные значения.

181. Доказать, что по нечетному модулю m , имеющему не менее двух различных простых множителей, первообразных корней не существует.

182. Доказать, что по четному модулю $2m$, где нечетное m имеет не менее двух различных простых множителей, а также по модулю $2^\alpha \cdot m'$, где $(2, m') = 1$, $\alpha > 1$, первообразных корней не существует.

183. Доказать, что по четному модулю 2^α , $\alpha > 2$, первообразных корней не существует.

184. Для каких модулей существование первообразных корней не исключается, если учесть результаты предыдущих трех задач?

§ 3. Индексы и их свойства

1. Понятие индекса. Основные свойства

Свойства первообразных корней дают возможность ввести в теорию чисел важное понятие, которое аналогично понятию логарифма.

Пусть g первообразный корень по простому модулю p . Тогда по свойствам показателей ряд чисел

$$g^0, g^1, \dots, g^{p-2} \quad (1)$$

представляет собой приведенную систему вычетов по модулю p .

Так как известно, что для каждого простого p существуют первообразные корни, то, очевидно, приведенную систему вычетов по любому простому модулю p можно составить, пользуясь системой чисел в форме (1).

Отсюда вытекает, что для каждого числа a , взаимно простого с p , в ряде (1) найдется единственное число g^{γ_1} , которое принадлежит к тому же классу по модулю p , что и a , т. е. такое, что

$$a \equiv g^{\gamma_1} \pmod{p}, \quad 0 \leq \gamma_1 \leq p-2. \quad (2)$$

Ясно, что числам, сравнимым с a по модулю p , соответствует то же самое число g^{γ_1} . Таким образом, числам одного класса по модулю p сопоставляется единственное число γ_1 с условием (2).

Введем следующее определение: *если g первообразный корень по модулю p и для a , взаимно простого с p , имеет место сравнение*

$$a \equiv g^{\gamma} \pmod{p}, \quad (3)$$

где $\gamma \geq 0$, то каждое такое γ называется *индексом числа a по модулю p при основании g* и обозначается символом $\text{ind}_g a$, или (если нет опасности ошибиться или нет надобности подчеркивать основание) более кратко, через $\text{ind } a$. Поэтому имеем

$$a \equiv g^{\text{ind } a} \pmod{p}. \quad (4)$$

Из предыдущего ясно, что любое a , взаимно простое с p , имеет при данном основании g единственный индекс γ_1 среди чисел

$$0, 1, \dots, p-2. \quad (5)$$

Числа, сравнимые с a по модулю p , имеют один и тот же индекс среди чисел (5).

При переходе к другому основанию индекс γ_1 , вообще говоря, меняется.

Так, например, по модулю 7 числа

$$1, 2, 3, 4, 5, 6$$

и сравнимые с ними по модулю 7 имеют при основании 3 (см. 2-й пример 1 п. § 1 настоящей главы) среди чисел ряда (5) соответственно индексы γ_1 :

$$0, 2, 1, 4, 5, 3,$$

а при основании 5 (см. 3-й пример 1 п. § 1 настоящей главы):

$$0, 4, 5, 2, 1, 3.$$

С другой стороны, легко понять, что при данном основании g каждое число a имеет бесконечное множество индексов γ . Из (2) и (3) видно, что это неотрицательные числа, удовлетворяющие условию

$$g^{\gamma} \equiv g^{\gamma_1} \pmod{p}.$$

Но так как g по модулю p является первообразным корнем, т. е. принадлежит показателю $p-1$, то в силу известных свойств показателей последнее сравнение имеет место тогда и только тогда, когда

$$\gamma \equiv \gamma_1 \pmod{p-1}.$$

Таким образом, каждому классу вычетов по модулю p , взаимно простых с модулем, взаимно однозначно сопоставляется множество индексов, которое состоит из неотрицательных вычетов некоторого класса вычетов по модулю $p - 1$:

Если $a \equiv b \pmod{p}$, то

$$\text{ind } a \equiv \text{ind } b \pmod{p - 1}.$$

В силу сравнения (4), соотношение между γ и a в (3) можно выражать следующим образом:

$$\gamma \equiv \text{ind } a \pmod{p - 1}. \quad (6)$$

Пример. Мы выше нашли, что по модулю 7 $\text{ind}_3 6$ равен 3, если взять его среди чисел 0, 1, ..., 5. Поэтому из

$$55 \equiv 27 \equiv 6 \pmod{7}$$

следует

$$\text{ind}_3 55 \equiv \text{ind}_3 27 \equiv \text{ind}_3 6 \equiv 3 \pmod{6}.$$

Индексы обладают следующими свойствами, которые аналогичны свойствам логарифмов.

1. Индекс произведения сравним по модулю $p - 1$ с суммой индексов сомножителей:

$$\text{ind } ab \dots l \equiv \text{ind } a + \text{ind } b + \dots + \text{ind } l \pmod{p - 1}.$$

Действительно,

$$a \equiv g^{\text{ind } a} \pmod{p},$$

$$b \equiv g^{\text{ind } b} \pmod{p},$$

$$\dots$$

$$l \equiv g^{\text{ind } l} \pmod{p};$$

поэтому $ab \dots l \equiv g^{\text{ind } a + \text{ind } b + \dots + \text{ind } l} \pmod{p}$, откуда, в силу сравнений (3) и (6), получаем

$$\text{ind } ab \dots l \equiv \text{ind } a + \text{ind } b + \dots + \text{ind } l \pmod{p - 1}.$$

Если все множители равны, то имеем:

2. Индекс степени (с натуральным показателем) сравним по модулю $p - 1$ с произведением показателя степени на индекс основания степени:

$$\text{ind } a^n \equiv n \text{ ind } a \pmod{p - 1}.$$

Заметим, что при любом простом p индекс единицы сравним по модулю $p - 1$ с нулем, а индекс основания с единицей.

$$\text{ind } 1 \equiv 0 \pmod{p - 1}, \text{ind } g \equiv 1 \pmod{p - 1}.$$

Это следует из того, что

$$g^0 \equiv 1 \pmod{p} \text{ и } g^1 \equiv g \pmod{p}.$$

2. Таблицы индексов

Составленные таблицы индексов для простых модулей p дают возможность по числу находить его индекс и, наоборот, по индексу — число. В качестве основания выбирается один из первообразных корней числа p .

Первые таблицы индексов для простых модулей до 200 составил в 1837 г. знаменитый русский математик М. В. Остроградский (1801—1862), немецким математиком К. Якоби эти таблицы были доведены до 1000, а в настоящее время существуют таблицы индексов для простых модулей до 10 000; в конце этой книги имеются таблицы индексов для простых модулей до 97. Хотя для данного p обе задачи — нахождение индекса по числу и числа по индексу — можно выполнить при помощи одной таблицы, все же, для большего удобства, она разделена на две части:

- 1) для нахождения индекса I по числу N ,
- 2) для нахождения числа N по индексу I .

В таблицах сопоставлены наименьшие неотрицательные вычеты чисел по модулю p и их наименьшие индексы по модулю $p - 1$. Чтобы составить таблицу индексов для модуля p , надо для какого-нибудь его первообразного корня g найти наименьшие неотрицательные вычеты степеней

$$g^0, g^1, \dots, g^{p-2}.$$

Пользование таблицами весьма простое.

Для примера рассмотрим таблицу индексов для простого модуля 37 при основании 2.

Простое число 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

В таблицах выделены номера строк и столбцов, которые соответственно указывают число десятков и единиц числа (индекса). На пересечении строки и столбца помещается соответствующий индекс (число).

Примеры: 1) найти индекс числа 23 для модуля 37.

По табличке слева на пересечении 2-й строки и третьего столбца находим число 15, поэтому $\text{ind } 23 \equiv 15 \pmod{36}$;

2) Найти число, если его индекс равен 18 по модулю 37.

Имеем $\text{ind } N \equiv 18 \pmod{36}$. По табличке справа на пересечении 1-й строки и 8-го столбца находим число 36, следовательно, $N \equiv 36 \pmod{37}$.

Если значения чисел или индексов выходят за пределы таблицы, то переходим к наименьшим неотрицательным вычетам: для чисел—по модулю p , для индексов—по модулю $p-1$.

Отметим, что основание, по которому таблица составлена, видно из таблицы, так как $\text{ind } g \equiv 1 \pmod{p-1}$; в нашей табличке, таким образом, $g = 2$.

В заключение заметим, что можно рассматривать индексы не только по простым модулям, но и по другим модулям m , для которых существуют первообразные корни, так как в таких случаях вычеты степеней первообразного корня также образуют приведенную систему вычетов по модулю m (см. 3-й пункт § 1 настоящей главы).

Упражнения

185. Зная, что 6 является первообразным корнем по модулю 13, составить при основании 6 таблицу индексов по модулю 13.

186. Зная, что 5 является первообразным корнем по модулю 18, составить при основании 5 таблицу индексов по модулю 18.

187. Доказать, что по нечетному простому модулю p

$$\text{ind}(-1) \equiv \text{ind}(p-1) \equiv \frac{p-1}{2} \pmod{p-1}.$$

188. Пользуясь свойствами индексов, доказать теорему Вильсона.

189. Зная, что по модулю 73 $\text{ind}_5 54 \equiv 26 \pmod{72}$, найти по этому же модулю $\text{ind}_{11} 54$ (11—первообразный корень по модулю 73).

190. Зная, что по модулю 71 $\text{ind}_7 66 \equiv 63 \pmod{70}$ найти по этому же модулю $\text{ind}_{13} 66$ (13—первообразный корень по модулю 71).

§ 4. Применение индексов к решению сравнений

1. Решение двучленных сравнений

Двучленные сравнения с одним неизвестным имеют вид:

$$ax^n \equiv b \pmod{m}, \quad a \nmid m. \quad (1)$$

Мы ограничимся рассмотрением случая, когда $m = p$ число нечетное простое, так как решение сравнения (1) сводится, как известно, к решению сравнений по простым модулям, а что касается случая четного простого модуля 2, то он легко решается испытанием чисел 0 и 1.

Итак, пусть дано сравнение

$$ax^n \equiv b \pmod{p}, \quad a \nmid p. \quad (2)$$

Пользуясь таблицами индексов, переходим к равносильному сравнению

$$\text{ind } a + n \text{ ind } x \equiv \text{ind } b \pmod{p-1},$$

откуда

$$n \text{ ind } x \equiv \text{ind } b - \text{ind } a \pmod{p-1}. \quad (3)$$

Рассмотрим в этом сравнении $\text{ind } x$ как неизвестное. Решив сравнение (3) относительно $\text{ind } x$ (если оно разрешимо), в таблицах индексов по модулю p находим решение исходного сравнения (2).

Представляются следующие случаи:

$$1) (n, p-1) = 1.$$

Тогда сравнение (3) относительно $\text{ind } x$ имеет единственное решение, следовательно, и (2) будет иметь единственное решение для x ;

$$2) (n, p-1) = d > 1.$$

В этом случае, как это известно из теории решения сравнений 1-й степени, имеем два подслучая:

1 подслучай: правая часть сравнения (3) не делится на d , то есть $\text{ind } b - \text{ind } a \not\equiv d$.

Тогда сравнение (3) не имеет решений относительно $\text{ind } x$, поэтому и (2) не имеет решений;

II подслучай: $\text{ind } b - \text{ind } a \equiv d$.

Тогда получаем из (3)

$$\frac{n}{d} \text{ind } x \equiv \frac{\text{ind } b - \text{ind } a}{d} \left(\text{mod } \frac{p-1}{d} \right).$$

Это сравнение имеет относительно $\text{ind } x$ одно решение по модулю $\frac{p-1}{d}$, а по модулю $p-1$ d решений.

После их определения можно с помощью таблиц индексов найти d соответствующих решений для x по модулю p .

Здесь особенно важно учесть требование, что решения сравнения необходимо указать по первоначальному модулю, так как переход от индексов к соответствующим числам означает (см. § 3, п. 1 настоящей главы) переход от сравнения вида

$$\text{ind } x \equiv \gamma \pmod{p-1}$$

к сравнению

$$x \equiv g^{\gamma} \pmod{p},$$

при условии, что под $\text{ind } x$ подразумевается « $\text{ind } x$ по модулю p при основании g »¹.

¹ Если для такого индекса имеем

$$\text{ind } x \equiv \gamma_1 \left(\text{mod } \frac{p-1}{d} \right),$$

то при переходе к

$$x \equiv g^{\gamma_1} \pmod{p}$$

мы не охватываем всех возможных значений x , удовлетворяющих исходному сравнению, а только часть.

Заметим, что если $\frac{p-1}{d} = p_1 - 1$, где p_1 — простое число,

например $\frac{19-1}{3} = 6 = 7-1$, то уже неверно будет в качестве решения находить в таблицах индексов по модулю p_1 , при первообразном корне g_1 как основания, число, соответствующее индексу γ_1 , так как это означало бы, что

$$x \equiv g_1^{\gamma_1} \pmod{p_1}.$$

Рассмотрим несколько примеров:

1. Решить сравнение $17x \equiv 8 \pmod{73}$.

Имеем $\text{ind } 17 + \text{ind } x \equiv \text{ind } 8 \pmod{72}$,

$$\text{ind } x \equiv \text{ind } 8 - \text{ind } 17 \pmod{72},$$

$$\text{ind } x \equiv 24 - 21 \pmod{72},$$

$$\text{ind } x \equiv 3 \pmod{72},$$

$$x \equiv 52 \pmod{73}.$$

Этот пример показывает, что с помощью таблицы индексов получаем удобный способ решения сравнений первой степени по простому модулю p .

2. Решить сравнение $x^3 \equiv 34 \pmod{41}$.

Имеем

$$3 \text{ ind } x \equiv \text{ind } 34 \pmod{40},$$

$$3 \text{ ind } x \equiv 19 \pmod{40},$$

$$3 \text{ ind } x \equiv -21 \pmod{40},$$

$$\text{ind } x \equiv -7 \pmod{40},$$

$$\text{ind } x \equiv 33 \pmod{40},$$

$$x \equiv 17 \pmod{41}.$$

3. Решить сравнение

$$39x^{21} \equiv 53 \pmod{73}.$$

Имеем

$$\text{ind } 39 + 21 \text{ ind } x \equiv \text{ind } 53 \pmod{72},$$

$$21 \text{ ind } x \equiv \text{ind } 53 - \text{ind } 39 \pmod{72},$$

$$21 \text{ ind } x \equiv 53 - 65 \pmod{72},$$

$$21 \text{ ind } x \equiv -12 \pmod{72},$$

$$7 \text{ ind } x \equiv -4 \pmod{24},$$

$$7 \text{ ind } x \equiv -28 \pmod{24},$$

$$\text{ind } x \equiv -4 \pmod{24},$$

$$\text{ind } x \equiv 20, 44, 68 \pmod{72},$$

$$x \equiv 18, 71, 57 \pmod{73}.$$

В последнем примере особенно ярко сказывается мощность примененного метода.

2. Критерий разрешимости сравнения $x^n \equiv a \pmod{p}$

При помощи теории индексов легко найти критерий разрешимости сравнения

$$x^n \equiv a \pmod{p}. \quad (1)$$

Действительно, перейдем к равносильному сравнению

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}. \quad (2)$$

Тогда становится очевидным, что при $(n, p-1)=d$ необходимое и достаточное условие разрешимости (2) заключается в том, чтобы $\operatorname{ind} a$ делился на d , или

$$\operatorname{ind} a \equiv 0 \pmod{d}. \quad (3)$$

Выразим это условие в зависимости от p и d . Умножим для этого обе части и модуль сравнения (3) на $\frac{p-1}{d}$. Получается сравнение, равносильное с (3):

$$\frac{p-1}{d} \operatorname{ind} a \equiv 0 \pmod{p-1},$$

или

$$\operatorname{ind} a^{\frac{p-1}{d}} \equiv 0 \pmod{p-1};$$

отсюда следует

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}. \quad (4)$$

Итак, необходимое и достаточное условие разрешимости сравнения (1) заключается в том, чтобы выполнялось сравнение (4).

Для случая, когда $n=2$, получаем известный критерий Эйлера для разрешимости двучленных сравнений 2-й степени по нечетному простому модулю. Действительно, для сравнения $x^2 \equiv a \pmod{p}$ условие (4) принимает вид

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \text{ так как здесь } d=(2, p-1)=2.$$

3. Решение показательных сравнений

Рассмотрим еще решение показательных сравнений по простому модулю, т. е. сравнений

$$a^x \equiv b \pmod{p} \quad (1)$$

с помощью индексов. Переходя к индексам, получаем из (1) равносильное сравнение относительно x

$$x \operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1},$$

которое легко решается.

Примеры. 1) Решить сравнение $5^x \equiv 17 \pmod{31}$.
Имеем

$$x \operatorname{ind} 5 \equiv \operatorname{ind} 17 \pmod{30},$$

$$20x \equiv 7 \pmod{30};$$

так как $(20, 30) = 10$, а 7 на 10 не делится, то сравнение не имеет решения.

2) Решить сравнение $11^x \equiv 17 \pmod{31}$.
Имеем

$$x \operatorname{ind} 11 \equiv \operatorname{ind} 17 \pmod{30}.$$

$$23x \equiv 7 \pmod{30},$$

$$23x \equiv -23 \pmod{30},$$

$$x \equiv -1 \pmod{30},$$

$$x \equiv 29 \pmod{30}.$$

3) Найти показатель, к которому 6 принадлежит по модулю 23. Для решения поставленной задачи мы должны найти наименьшее целое неотрицательное решение сравнения $6^x \equiv 1 \pmod{23}$.

Имеем $x \operatorname{ind} 6 \equiv 0 \pmod{22}$, $18x \equiv 0 \pmod{22}$,

$$9x \equiv 0 \pmod{11}, \quad x \equiv 0 \pmod{11},$$

или x делится на 11. Наименьшее значение x , которое этому условию удовлетворяет, равно 11. Итак, 6 принадлежит показателю 11 по модулю 23.

Упражнения

191. Решить двучленные сравнения, пользуясь таблицами индексов: 1) $x^5 \equiv 37 \pmod{43}$; 2) $x^8 \equiv 27 \pmod{37}$; 3) $x^{10} \equiv 33 \pmod{37}$; 4) $x^{12} \equiv 27 \pmod{83}$; 5) $x^2 \equiv 61 \pmod{73^2}$; 6) $x^2 \equiv 29 \pmod{59^2}$.

192. Решить сравнения первой степени, пользуясь таблицами индексов: 1) $23x \equiv 9 \pmod{97}$; 2) $47x \equiv 23 \pmod{73}$; 3) $53x \equiv 37 \pmod{79}$; 4) $65x \equiv 38 \pmod{83}$.

193. Решить двучленные сравнения, пользуясь таблицами индексов: 1) $43x^{17} \equiv 35 \pmod{71}$; 2) $45x^{12} \equiv 28 \pmod{67}$; 3) $53x^{21} \equiv 38 \pmod{61}$; 4) $27x^{30} \equiv 41 \pmod{79}$.

194. Найти остаток от деления, пользуясь таблицами индексов: 1) 341^{245} на 89; 2) 244^{408} на 73; 3) 749^{193} на 79; 4) $53^{29} \cdot 43^{17}$ на 37; 5) 175^{411} на 629.

195. Какому необходимому и достаточному условию должен удовлетворять $\text{ind } a \pmod{p}$, где $p > 2$, чтобы a было квадратичным вычетом по модулю p ?

196. Пользуясь результатом предыдущей задачи, найти при помощи таблицы индексов квадратичные вычеты по модулю 23.

197. Пользуясь таблицами индексов, найти показатель: 1) 7 по модулю 29; 2) 13 по модулю 53; 3) 27 по модулю 47; 4) 18 по модулю 41; 5) 10 по модулю $1739 = 37 \cdot 47$; 6) 32 по модулю $4331 = 61 \cdot 71$.

198. Найти наименьшие целые положительные решения показательных сравнений: 1) $13^x \equiv 42 \pmod{53}$; 2) $18^x \equiv 53 \pmod{79}$; 3) $44^x \equiv 19 \pmod{71}$.

Глава V

АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

§ 1. Вычисление остатков при делении на данное число. Установление признаков делимости с помощью сравнений

А. Впервые знаменитый французский математик Б. Паскаль (1623—1662) указал на довольно общий способ, как заменить данное число N другим так, чтобы вычисление остатка от деления на m значительно упростилось. Мы рассмотрим этот способ для чисел, данных в десятичной системе счисления, а также в системах счисления с основаниями 10^2 , 10^3 и т. д. Получаемые при этом признаки равноостаточности и делимости легко обобщить на случай любой g -ичной системы счисления.

Пусть в десятичной системе счисления натуральное число N имеет вид

$$N = a_0 + a_1 \cdot 10^1 + \dots + a_n \cdot 10^n.$$

Обозначим абсолютно наименьший вычет числа 10^k по модулю m через r_k , так что

$$10^k \equiv r_k \pmod{m}, \quad k = 0, 1, \dots, n, \text{ и } r_0 = 1.$$

Тогда

$$N \equiv a_0 r_0 + a_1 r_1 + \dots + a_n r_n \pmod{m} \quad (1)$$

или

$$N \equiv R_m \pmod{m},$$

где $R_m = a_0 r_0 + \dots + a_n r_n$ представляет собой выше упомянутую замену.

Сравнение (1) выражает признак делимости (а также равноостаточности) Паскаля: 1) при делении на m R_m

дает такой же остаток, как и N ; 2) N делится на m тогда и только тогда, когда R_m делится на m .

Рассмотрим некоторые частные случаи.

1) Если $m=3$, то $10 \equiv 1 \pmod{3}$ и $10^k \equiv 1 \pmod{3}$; таким образом, здесь все $r_k = 1$, а

$$R_3 = a_0 + a_1 + \dots + a_n.$$

Итак, при делении на 3 сумма цифр числа дает такой же остаток, как само число; число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

2) Для $m=9$ получается аналогичная картина, так как $10 \equiv 1 \pmod{9}$ и $10^k \equiv 1 \pmod{9}$, вследствие чего все $r_k = 1$ и

$$R_9 = a_0 + a_1 + \dots + a_n.$$

Так, например, для $N=285\,976$ имеем

$$N \equiv 2 + 8 + 5 + 9 + 7 + 6 \equiv 1 \pmod{9},$$

т. е. указанное число при делении на 9 дает остаток 1.

Заметим, что при суммировании цифр кратные 9 следует сразу же отбросить, так как в конечном итоге нас интересует остаток от деления R_9 на 9.

3) Если $m=11$, то $10^k \equiv (-1)^k \pmod{11}$ и

$$R_{11} = a_0 - a_1 + a_2 - \dots$$

или

$$R_{11} = (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots).$$

Так, например, для $N=3\,758\,396$

$N \equiv 6 - 9 + 3 - 8 + 5 - 7 + 3 \equiv 4 \pmod{11}$, т. е. дает при делении на 11 остаток 4.

4) По модулю $m=7$: $10^0 \equiv 1, 10^1 \equiv 3, 10^2 \equiv 2, 10^3 \equiv -1, 10^4 \equiv -3, 10^5 \equiv -2$; начиная с 10^6 , остатки будут повторяться в такой же последовательности, так как $10^6 \equiv 1 \pmod{7}$. Итак,

$$R_7 = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + \dots$$

Здесь уже замена более громоздкая.

Б. Остановимся несколько подробнее на случае, когда 10 принадлежит показателю δ по модулю m . Здесь $r_\delta = 1$, так как $10^\delta \equiv 1 \pmod{m}$, поэтому начиная с r_δ , все остатки r_k повторяются и

$$R_m = a_0 + a_1 r_1 + \dots + a_{\delta-1} r_{\delta-1} + a_\delta + a_{\delta+1} r_1 + \dots$$

По модулям 3, 7, 9 и 11 число 10 принадлежит соответственно показателям 1, 6, 1 и 2, поэтому и при указанных модулях остатки начинают соответственно повторяться с r_1 , r_6 , r_1 и r_2 (как мы это видели в примерах 1—4).

Если по модулю m число 10 принадлежит показателю δ , то в системе счисления с основанием 10^δ имеем

$$N = d_0 + d_1 \cdot 10^\delta + \dots + d_n \cdot (10^\delta)^n,$$

а так как $(10^\delta)^k \equiv 1 \pmod{m}$, условие (1) принимает вид

$$N \equiv d_0 + d_1 + \dots + d_n \pmod{m},$$

т. е. признаки равноостаточности и делимости по модулю m здесь такие же, как для 3 в десятичной системе. Однако «цифрами» в данном случае следует считать δ -значные числа, получающиеся при разбиении N справа налево на грани по δ цифр в каждой.

Примеры. 1) Представляя N в виде

$$N = b_0 + b_1 \cdot 100 + \dots + b_n \cdot 100^n,$$

имеем $100 \equiv 1 \pmod{11}$, $100^k \equiv 1 \pmod{11}$ и

$$N \equiv b_0 + b_1 + \dots + b_n \pmod{11},$$

т. е. остаток от деления числа N на 11 равен остатку от деления на 11 суммы двузначных граней числа N , считая справа налево.

Для рассмотренного выше примера $N = 3758396$ получается

$$N = 96 + 83 + 75 + 3 = 257 \equiv 57 + 2 = 59 \equiv 4 \pmod{11}$$

(вычисления удобно расположить в «столбик»).

2) По модулю $m = 37$ число 10 принадлежит показателю 3, поэтому при основании счисления 1000 для $m = 37$ получается признак делимости, аналогичный признаку делимости для 3 в десятичной системе, т. е. если представим N в виде

$$N = c_0 + c_1 \cdot 1000 + \dots + c_n \cdot 1000^n,$$

то

$$N \equiv c_0 + c_1 + \dots + c_n \pmod{37}.$$

Для $N = 83576289$ имеем $N \equiv 289 + 576 + 83 \equiv \equiv 23 \pmod{37}$.

В случае когда по нечетному простому модулю p 10 принадлежит четному показателю δ , тогда при основании счисления $10^{\frac{\delta}{2}}$ для p получается признак делимости, аналогичный признаку делимости на 11 в десятичной системе, так как $10^{\frac{\delta}{2}} \equiv -1 \pmod{p}$. (см. задачу 168). Таковы, например, признаки делимости на 7 и 13 в системе счисления с основанием $1000=10^3$, поскольку по указанным модулям 10 принадлежит показателю 6.

В заключение заметим, что признаки делимости можно рассматривать как алгоритмы, перерабатывающие каждое число в ответ, делится ли оно на данное число или нет. С таких позиций вопрос излагается в (39).

Упражнения

199. Найти признаки равноостаточности и делимости Паскаля для числа N на m в g -ичной системе счисления.

200. В g -ичной системе счисления найти признаки равноостаточности и делимости для N на $g-1$ и делитель d этого числа.

201. Найти в g -ичной системе счисления признаки равноостаточности и делимости для N на $g+1$.

202. Найти остаток от деления на 37 чисел: 1) 3 989 713; 2) 27 877 165; 3) 31 127 567.

203. Найти остаток от деления 34521, на 6.

204. Для каких чисел в системах счисления с основаниями 1) 13 и 2) 25 признаки делимости аналогичны признакам делимости на 3 в десятичной системе счисления?

205. В какой системе счисления признаки делимости на числа 2, 3, 4, ..., n аналогичны признакам делимости на 3 в десятичной системе?

§ 2. Определение длины периода, получающегося при обращении обыкновенной дроби в десятичную

1. Как известно, при обращении обыкновенной несократимой дроби $\frac{a}{b}$, содержащей в знаменателе отличные от чисел 2 и 5 множители, в десятичную получается бесконечная периодическая дробь.

Чтобы найти число цифр в периоде, рассмотрим сначала случай, когда знаменатель b несократимой дроби $\frac{a}{b}$ не содержит множителей 2 и 5, т. е. когда

$(b, 10) = 1$. При этом можно ограничиться правильной дробью ($a < b$) (так как при обращении неправильной дроби ($a > b$) в десятичную из нее предварительно выделяется целая часть). Ясно, что в такой дроби числитель a может принимать одно из $\varphi(b)$ значений, меньших b и взаимно простых с b .

Поступая так, как это обычно делается при обращении обыкновенной дроби в десятичную, мы, после m шагов последовательных делений, получим:

$$\left. \begin{aligned} 10a &= bq_1 + r_1 \\ 10r_1 &= bq_2 + r_2 \\ \vdots &\vdots \\ 10r_{m-1} &= bq_m + r_m \end{aligned} \right\}, \quad (1)$$

где все остатки r_i удовлетворяют условию $0 < r_i < b$. При этом $q_1 < 10$, так как $b > a$; аналогично $q_2 < 10$, так как $b > r_1$ и т. д. Таким образом, все q_i являются цифрами.

Пример: $\frac{a}{b} = \frac{5}{13}$. Здесь

$$\left. \begin{aligned} 10 \cdot 5 &= 13 \cdot 3 + 11 \\ 10 \cdot 11 &= 13 \cdot 8 + 6 \\ 10 \cdot 6 &= 13 \cdot 4 + 8 \\ 10 \cdot 8 &= 13 \cdot 6 + 2 \\ 10 \cdot 2 &= 13 \cdot 1 + 7 \\ 10 \cdot 7 &= 13 \cdot 5 + 5 \end{aligned} \right\}. \quad (1')$$

Заметим, что получаемые остатки r_i взаимно просты с b . Действительно, так как $(10, b) = 1$, $(a, b) = 1$, то $(10a, b) = 1$, откуда и $(r_1, b) = 1$; аналогично из второй строчки (1) следует, что $(r_2, b) = 1$ и так далее.

Таким образом, различные остатки r_i принадлежат приведенной системе вычетов по модулю b и их число не может быть $> \varphi(b)$.

Поэтому не позже, чем через $\varphi(b)$ шагов, остатки начнут повторяться и вместе с тем цифры в частном, так что в периоде не может быть более $\varphi(b)$ цифр.

2. Чтобы получить более определенные сведения о числе цифр в периоде, а также о самом периоде, рассмотрим равенства (1) по модулю b .

Тогда имеем

$$\left. \begin{aligned} 10a &\equiv r_1 \pmod{b} \\ 10r_1 &\equiv r_2 \pmod{b} \\ &\vdots \\ 10 \cdot r_{m-1} &\equiv r_m \pmod{b} \end{aligned} \right\}, \quad (2)$$

откуда (в силу того, что произведение $r_1 \cdot r_2 \dots r_{m-1}$ взаимно просто с b) после умножения следует

$$10^m \cdot a \equiv r_m \pmod{b}. \quad (3)$$

Пусть теперь m не какое-либо число, а показатель, которому 10 принадлежит по модулю b , т. е. наименьший показатель степени для которого

$$10^m \equiv 1 \pmod{b}.$$

Для такого m из (3) получаем $a \equiv r_m \pmod{b}$. Но так как $0 < a < b$ и $0 < r_m < b$, то из сравнимости a и r_m по модулю b следует, что они обязательно равны, т. е. что

$$a = r_m.$$

Итак, мы получили остаток, который равен числителю данной дроби. Отсюда вытекает, что с этого момента остатки начнут повторяться:

$$r_{m+1} = r_1, r_{m+2} = r_2 \text{ и т. д.}$$

Очевидно, m соответствует наименьшему периоду, так как если для $m' < m$ возможно было бы $a = r_{m'}$, то из (3) следовало бы $10^{m'} \equiv 1 \pmod{b}$, а это противоречит условию, что m является показателем числа 10 по модулю b .

Итак, получается чисто периодическая дробь, причем число цифр в периоде зависит только от знаменателя b , а от числителя a не зависит¹.

¹ Результат о числе цифр в периоде можно также получить следующим, более кратким рассуждением. После того как при последовательных делениях $10^1 a, 10^2 a, \dots, 10^m a$ на b впервые получится остаток a , в частном определится наименьший период дроби. Таким образом, число цифр в периоде дроби $\frac{a}{b}$ равно наименьшему показателю m , для которого $10^m a \equiv a \pmod{b}$, или так как $(a, b) = 1$, $10^m \equiv 1 \pmod{b}$, т. е. число цифр в периоде равно показателю, которому принадлежит 10 по модулю b .

Мы предпочли в тексте иное изложение, так как оно дает более обзримую картину относительно особенностей самого периода, о чем будет речь впереди.

3. Равенства (1) показывают, что дробь

$$\frac{a}{b} = \frac{r_0}{b} \text{ имеет период } q_1 q_2 \dots q_m,$$

$$\frac{r_1}{b} \quad \gg \quad q_2 q_3 \dots q_m q_1 \text{ и т. д.,}$$

$$\text{а вообще } \frac{r_k}{b} \quad \gg \quad q_{k+1} \dots q_k.$$

Таким образом, периоды дробей

$$\frac{r_0}{b}, \frac{r_1}{b}, \dots, \frac{r_{m-1}}{b}$$

отличаются друг от друга только лишь круговой перестановкой цифр. При этом период дроби $\frac{r_k}{b}$ получается круговой перестановкой цифр периода дроби $\frac{r_0}{b}$ на k знаков вправо, где k определяется из сравнения

$$10^k \cdot r_0 \equiv r_k \pmod{b},$$

которое следует из (2), если перемножить k первых сравнений.

Пример. Пусть $\frac{a}{b} = \frac{5}{13}$. Так как 10 принадлежит показателю 6 по модулю 13, то в периоде должно быть 6 цифр. Это подтверждают равенства (1'), из которых видно, что

$$\begin{aligned} \frac{5}{13} &= 0,(384\ 615), & \frac{11}{13} &= 0,(846\ 153), & \frac{6}{13} &= 0,(461\ 538), \\ \frac{8}{13} &= 0,(615\ 384), & \frac{2}{13} &= 0,(153\ 846), & \frac{7}{13} &= 0,(538\ 461). \end{aligned}$$

По этим значениям можно также проверить правила о смещении знаков периода, так как по модулю 13

$$10^1 \cdot 5 \equiv 11, \quad 10^2 \cdot 5 \equiv 6, \quad 10^3 \cdot 5 \equiv 8, \quad 10^4 \cdot 5 \equiv 2, \quad 10^5 \cdot 5 \equiv 7.$$

4. Если 10 не является первообразным корнем по модулю b (для $b \neq p^\alpha$, где $\alpha \geq 1$, это всегда будет так, ибо по таким модулям b , взаимно простым с 10, пер-

вообразные корни вообще не существуют), а принадлежит показателю $m < \varphi(b)$, который, как известно, должен быть делителем $\varphi(b)$, так что $\varphi(b) = m \cdot d$, то несократимые правильные $\varphi(b)$ дробей со знаменателем b распадаются на d систем дробей

$$\left[\begin{array}{c} \frac{r_0}{b}, \frac{r_1}{b}, \dots, \frac{r_{m-1}}{b} \\ \frac{s_0}{b}, \frac{s_1}{b}, \dots, \frac{s_{m-1}}{b} \\ \vdots \\ \frac{t_0}{h}, \frac{t_1}{h}, \dots, \frac{t_{m-1}}{h} \end{array} \right],$$

из которых каждая имеет периоды (с одинаковым числом t цифр в периоде), отличающиеся друг от друга только круговой перестановкой одних и тех же цифр (причем, согласно установленному выше правилу о смещении знаков).

Действительно, если 10 принадлежит показателю m по модулю b ($0 < m < \varphi(b)$), то в периоде каждой несократимой дроби со знаменателем b содержится m цифр. Пусть дробь $\frac{r_0}{b}$ имеет период $(q_1 q_2 \dots q_m)$, тогда

такой же период с точностью до круговой перестановки имеют дроби с числителями r_1, r_2, \dots, r_{m-1} , которые определяются по равенствам (1).

Этими дробями не исчерпываются все правильные несократимые дроби со знаменателем b .

Пусть s_0 — числитель, отличный от всех r_i .

Тогда $\frac{s_0}{h}$ порождает согласно равенствам вида (1)

дроби с числителями s_1, s_2, \dots, s_{m-1} (отличными от всех r_i , так как дроби с числителями r_i порождают дроби только с такими же числителями), имеющие с точностью до круговой перестановки период $(p_1 p_2 \dots p_m)$. Продолжая начатые рассуждения, мы и придем к указанным d системам дробей.

Периоды в разных системах не могут быть получены друга из друга круговой перестановкой.

Допустим противное. Не ограничивая общности, можно предположить, что период $(p_1 p_2 \dots p_m)$ совпадает с периодом $(q_1 q_2 \dots q_m)$. Тогда имеем системы

$$\left. \begin{aligned} 10r_0 &= bq_1 + r_1 \\ 10r_1 &= bq_2 + r_2 \\ \dots &\dots \dots \dots \dots \dots \dots \\ 10r_{m-1} &= b \cdot q_m + r_m \end{aligned} \right\}, \quad \left. \begin{aligned} 10s_0 &= bq_1 + s_1 \\ 10s_1 &= b \cdot q_2 + s_2 \\ \dots &\dots \dots \dots \dots \dots \dots \\ 10 \cdot s_{m-1} &= b \cdot q_m + s_m \end{aligned} \right\},$$

где $r_0 = r_m$ и $s_0 = s_m$.

Из этих систем следует

$$\begin{aligned} 10(r_0 - s_0) &= r_1 - s_1 \\ 10(r_1 - s_1) &= r_2 - s_2 \\ \dots &\dots \dots \dots \dots \dots \dots \\ 10(r_{m-1} - s_{m-1}) &= r_0 - s_0, \end{aligned}$$

откуда, в силу того, что $r_i - s_i \neq 0$, умножением получим

$$10^m = 1,$$

что невозможно, так как $m \geq 1$.

Пример. По модулю 13 число 10 не является первообразным корнем, а принадлежит показателю 6. Поэтому правильные дроби со знаменателем 13 распадаются на $\frac{\varphi(13)}{6} = 2$ системы дробей с только что указанными свойствами. С одной из них мы ознакомились в предыдущем примере.

Если же исходить, например, из дроби $\frac{1}{13}$ (ее числитель отличен от числителей со знаменателем 13 в предыдущем примере), то получим вторую систему дробей со знаменателем 13, а именно:

$$\begin{aligned} \frac{1}{13} &= 0,(076923), \quad \frac{10}{13} = 0,(769\ 230), \quad \frac{9}{13} = 0,(692307), \\ \frac{12}{13} &= 0,(923076), \quad \frac{3}{13} = 0,(230769), \quad \frac{41}{13} = 0,(307692). \end{aligned}$$

Если 10 является первообразным корнем по модулю b , то в системе (2) остатки r_i исчерпывают приведенную систему вычетов по модулю b , а поэтому получается одна система дробей со знаменателем b ,

периоды которых содержат по $\varphi(b)$ цифр и получаются друг из друга круговой перестановкой цифр. Если b к тому же еще является простым числом, то в периоде имеем $b-1$ цифру, т. е. максимально возможное количество со знаменателем b .

Пример. По модулю 7 число 10 является первообразным корнем. Поэтому правильные дроби со знаменателем 7 имеют 6 цифр в периоде. Легко убедиться, что

$$\begin{aligned}\frac{1}{7} &= 0,(142\ 857), & \frac{2}{7} &= 0,(285\ 714), & \frac{3}{7} &= 0,(428\ 571), \\ \frac{4}{7} &= 0,(571\ 428), & \frac{5}{7} &= 0,(714\ 285), & \frac{6}{7} &= 0,(857\ 142).\end{aligned}$$

5. В заключение рассмотрим пример на определение числа цифр в периоде: найти число цифр в периоде при обращении несократимой дроби со знаменателем $b=41$ в десятичную.

Решение 1. Показатель числа 10 по модулю 41 является делителем $\varphi(41)=40$, т. е. одним из чисел

$$1, 2, 4, 5, 8, 10, 20, 40.$$

Выясним, какое это число, последовательными вычислениями по модулю 41:

$$10^1 \equiv 10, \quad 10^2 \equiv 18, \quad 10^4 \equiv 324 \equiv -4, \quad 10^5 \equiv -40 \equiv 1.$$

Итак, в периоде со знаменателем 41 имеется 5 цифр.

Решение 2. Число цифр в периоде является наименьшим значением x , которое удовлетворяет сравнению $10^x \equiv 1 \pmod{41}$.

Отсюда

$$\begin{aligned}x \cdot \text{ind } 10 &\equiv \text{ind } 1 \pmod{40}, \\ 8x &\equiv 0 \pmod{40}, \\ x &\equiv 0 \pmod{5}, \\ \text{или } x &\neq 5.\end{aligned}$$

Наименьшее значение для x равно 5.

Решение 3. Так как число цифр в периоде не зависит от числителя, то можно в качестве числителя выбрать 1. Приписывая к ней нули и производя последовательные деления, мы должны этот процесс продолжать до тех пор, пока в остатке опять не появится

ся 1. Этому процессу равнозначно последовательное деление чисел $10^1 - 1 = 9$, $10^2 - 1 = 99$ и так далее на b , пока не получится деление без остатка. Очевидно, при этом находится и сам период дроби $\frac{1}{b}$.

Для $b = 41$ таким делением обнаруживаем, что $0,99999 : 41 = 0,02439$, так что $\frac{1}{41} = 0, (02439)$.

6. Рассмотрим теперь обращение несократимой дроби $\frac{a}{b}$ в десятичную, когда b и 10 не взаимно простые. Пусть при этом $b = 2^\alpha \cdot 5^\beta \cdot b_1$, где $(b_1, 10) = 1$, а наибольшее из чисел α и β обозначено через n . Тогда число

$$\frac{10^n \cdot a}{b} = \frac{2^{n-\alpha} \cdot 5^{n-\beta} \cdot a}{b_1} = \frac{a_1}{b_1}.$$

Обращая несократимую дробь $\frac{a_1}{b_1}$, $(b_1, 10) = 1$ в десятичную обычным способом, получим

$$\frac{10^n \cdot a}{b} = \frac{a_1}{b_1} = K, (q_1 q_2 \dots q_m).$$

Чтобы найти отсюда $\frac{a}{b}$, надо число $K, (q_1 q_2 \dots q_m)$ разделить на 10^n , т. е. перенести запятую на n знаков влево.

Тогда получится смешанная периодическая дробь с n цифрами между запятой и началом периода:

$$\frac{a}{b} = k, k_1, k_2 \dots k_n (q_1 q_2 \dots q_m).$$

Итак, при обращении несократимой дроби $\frac{a}{b}$ в десятичную, где $b = 2^\alpha \cdot 5^\beta \cdot b_1$, $(b_1, 10) = 1$, получается смешанная периодическая дробь. При этом число цифр в периоде равно показателю m , которому принадлежит 10 по модулю b_1 , а число цифр вправо от запятой до первого периода равно n — наибольшему из чисел α и β .

Упражнения

206. Найти число цифр в периоде при обращении несократимой дроби со знаменателем b в десятичную; значения b следующие:

1) 19, 29, 37, 43, 59, 67, 73, 89, 97; 2) 21, 33, 39, 49, 51, 77, 91; 3) 220, 1150, 2380, 26500 (в 3) указать также число цифр вправо от запятой до первого периода).

207. Сколько имеется систем несократимых дробей со знаменателем b , из которых каждая имеет периоды, отличающиеся только циклической перестановкой; значения b — как в задаче 206—1) и 206—2).

208. В каждой из систем несократимых дробей со знаменателем b (о которых говорилось в задаче 207) указать по одному представителю, а также его десятичное выражение, если $b = 39$.

209. Найти числитель a правильных дробей

$$1) \frac{a}{73} = 0, (86\ 301\ 369) \quad \text{и} \quad 2) \frac{a}{73} = 0, (30\ 136\ 986), \quad \text{если} \quad \frac{1}{73} = 0, (01\ 369\ 863).$$

210. 1) Зная, что $\frac{1}{17} = 0, (0\ 588\ 235\ 294\ 117\ 647)$, найти период $\frac{6}{17}$; 2) зная, что $\frac{1}{41} = 0, (02\ 439)$ и что $\frac{16}{41}$ имеет период, отличающийся от периода $\frac{1}{41}$ только циклической перестановкой, найти этот период.

211. Пользуясь результатами задачи 208, охарактеризовать произведения числа 025641, т. е. периода дроби $\frac{1}{39}$: 1) на некоторое k , где $1 \leq k \leq 38$, $(k, 39) = 1$ (например, $k = 37$) 2) на 39; 3) на некоторое $K = 39n + k$, где n — натуральное число, например 2.

212. Доказать, что если по модулю b число 10 является первообразным корнем и $\frac{1}{b} = 0, (q_1 \dots q_m)$, то тогда произведения $Q_m = \overline{q_1 \dots q_m}$: 1) на k , где $(k, b) = 1, 1 \leq k < b$, отличаются от Q_m только циклической перестановкой; 2) на b равны числу, состоящему из m девяток, т. е. $10^m - 1$; 3) на $K = nb + k$, где n — натуральное число и $1 \leq k < b$, имеют слева число n , а после отбрасывания этого числа слева и прибавления его к оставшемуся числу, получается одно из чисел, указанных в 1).

213. Сформулировать свойства, отмеченные в предыдущей задаче, для случая, когда 10 принадлежит показателю m по модулю b и $\varphi(b) = m \cdot d$.

214. Доказать, что для простого знаменателя p , отличного от 2 и 5, с четным числом цифр в периоде сумма полупериодов состоит только из девяток.

215. Найти вид периодической дроби для: 1) $\frac{107}{143}$, зная, что $\frac{1}{11} = 0, (09)$, $\frac{1}{13} = 0, (076\ 923)$; 2) $\frac{123}{133}$, зная, что $\frac{1}{7} = 0, (142\ 857)$; $\frac{1}{19} = 0, (052\ 631\ 578\ 947\ 368\ 421)$.

§ 3. Проверка результатов арифметических действий

Пусть при сложении целых чисел N_1 и N_2 получено число N . Если сложение выполнено правильно, то

$$N_1 + N_2 = N. \quad (1)$$

Если по модулю m

$$N_1 \equiv r_1, \quad N_2 \equiv r_2, \quad N \equiv r \pmod{m},$$

то в силу равенства (1) должно быть

$$r_1 + r_2 \equiv r \pmod{m}. \quad (1')$$

Таким же образом (пользуясь при этом аналогичными обозначениями), получаем: если

$$N_1 - N_2 = N, \quad (2)$$

то

$$r_1 - r_2 \equiv r \pmod{m}; \quad (2')$$

если

$$N_1 \cdot N_2 = N, \quad (3)$$

то

$$r_1 \cdot r_2 \equiv r \pmod{m}; \quad (3')$$

если

$$N_1 \cdot N_2 + N_3 = N \quad (4)$$

(последнее соотношение имеем, если N при делении на N_1 дает частное N_2 и остаток N_3), то

$$r_1 \cdot r_2 + r_3 \equiv r \pmod{m}. \quad (4')$$

Соотношения, аналогичные отмеченным, можно, очевидно, распространить на все случаи, когда над числами производятся в какой-либо последовательности действия сложения, вычитания и умножения.

Соотношения (1') — (4') являются необходимыми условиями правильности выполненных действий в (1) — (4), но, очевидно, еще недостаточными.

Чтобы проверка была по возможности более надежной и одновременно простой, в качестве модуля целесообразно выбрать число 9, так как остаток чисел при их делении на 9 равен остатку при делении суммы цифр на 9, вследствие чего в проверке участвуют все цифры, причем сама проверка является легкой. Конечно, если в качестве модуля выбрать число 10, то остатки можно найти еще проще, но такую про-

верку нельзя считать достаточно надежной, так как в ней участвует только последняя цифра (справа) данного числа. Надежность проверки значительно увеличивается, если она выполняется не только по модулю 9, но и по модулю 11.

Примеры: 1) Проверить правильность сложения
 $375819 + 726345 + 807611 = 1909775$.

Абсолютно наименьшие вычеты чисел по модулю 9 в данном соотношении соответственно равны: $-3, 0 - 4, 2$; таким образом, условие проверки $-3 + 0 - 4 \equiv 2 \pmod{9}$ здесь выполняется.

Легко понять, что при изменении порядка следования двух последних цифр «суммы» или в случае пропуска в ней нуля или цифры 9, условие проверки не нарушается, между тем результат будет неправильным.

2) Проверить правильность умножения

$$732 \cdot 421 = 308172.$$

Здесь по модулю 9

$$732 \equiv 3, 421 \equiv -2, 308172 \equiv 3 \pmod{9},$$

далее

$$3 \cdot (-2) \equiv -6 \equiv 3 \pmod{9},$$

так что условие проверки выполнено.

Упражнения

216. Проверить результаты арифметических действий, пользуясь модулями 9 и 11:

1) $208\,973 + 163\,786 = 372\,759$; 2) $387\,912 - 203\,756 = 185\,146$;
3) $2\,543 \cdot 783 = 1\,984\,122$; 4) $783\,897 : 3\,914 = 200$ (ост. 1097).

217. Указать способ проверки арифметического действия, если $\sqrt[k]{S} = Q$ с остатком R .

218. Проверить по модулю 9 следующий результат: $\sqrt{73\,818} = -271$ с остатком 377.

Глава VI

§ 1. Представление иррациональных чисел правильными бесконечными цепными дробями

1. Разложение действительного иррационального числа в правильную бесконечную цепную дробь

В § 3, гл. III рассмотрено, как процессом последовательного выделения целой части и перевортывания дробной рациональная дробь $\alpha = \frac{a}{b}$ разлагается в конечную непрерывную дробь

$$\alpha = q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}} = (q_1, q_2, \dots, q_n) \quad (1)$$

и, наоборот, свертывание такой конечной непрерывной дроби приводит к рациональной дроби.

Процесс выделения целой части и перевертывания дробной можно применить к любому действительному числу.

Для иррационального числа α указанный процесс должен быть бесконечным, так как конечная цепная дробь равна рациональному числу.

Выражение

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots}} \quad (2)$$

(где все q_i целые и, начиная с q_2 , положительные), возникающее в таком процессе или заданное фор-

мально (т. е. безотносительно к тому, откуда взялись числа q_1, q_2 и т. д.), мы будем называть *правильной бесконечной цепной* или *непрерывной дробью*¹ (и обозначать кратко через (q_1, q_2, q_3, \dots)), а числа q_1, q_2 и т. д. — ее *элементами* или *неполными частными*.

Если выражение (2) возникло в процессе последовательного выделения целой части из действительного числа α , то будем также говорить, что оно является *разложением α* .

Отметим, что разложение α возможно только в единственном виде, так как процесс выделения целой части — процесс однозначный².

Рассмотрим пример разложения иррационального числа α .

Пусть имеем $\alpha = \sqrt{11}$. Выделим из $\sqrt{11}$ его целую часть $[\sqrt{11}] = 3$, а дробную часть $\sqrt{11} - 3$, которая < 1 , представим в виде $\frac{1}{\alpha_2}$, где $\alpha_2 = \frac{1}{\sqrt{11} - 3} > 1$. Повторя операцию выделения целой части и перевертывания дробной, мы получаем:

$$\alpha = \alpha_1 = \sqrt{11} = 3 + \frac{1}{\alpha_2}, \quad \alpha_2 > 1.$$

$$\alpha_2 = \frac{1}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{2} = 3 + \frac{1}{\alpha_3}, \quad \alpha_3 > 1,$$

$$\alpha_3 = \frac{2}{\sqrt{11} - 3} = \frac{2(\sqrt{11} + 3)}{2} = 6 + \frac{1}{\alpha_4}, \quad \alpha_4 > 1.$$

¹ До § 5 настоящей главы, как об этом уже отмечалось на стр. 71, мы будем рассматривать только правильные цепные дроби и называть их просто цепными дробями.

² Заметим, однако, тот факт, что иррациональное число α можно разложить в цепную дробь единственным образом, еще не означает, что α представимо цепной дробью единственным образом, е ли понимать под этим то, что существует единственная цепная дробь, имеющая значение α . Дело в том, что мы пока даже не знаем, как сопоставить произвольно заданной цепной дроби число. Естественно хотелось бы определить понятие числового значения бесконечной цепной дроби так, чтобы α оказалось равным своему разложению.

В дальнейшем мы выясним, как можно найти α , исходя из элементов его разложения, и это подскажет нам, как ввести понятие значения любой бесконечной цепной дроби.

так что

$$\alpha = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{1}{\ddots + \frac{1}{q_k + \frac{1}{\alpha_{k+1}}}}}}} \quad (4)$$

Числа α_k называются остаточными числами порядка k разложения α . В формуле (4) имеем кусок разложения до остаточного числа α_{k+1} . (Заметим, что представление (4) можно также отнести к рациональной дроби $\frac{a}{b} = \delta_n$, при этом, конечно, $k < n$, а α_{k+1} может быть и целое.)

Для бесконечной цепной дроби (2) можно построить бесконечную последовательность конечных непрерывных дробей

$$\delta_1 = q_1, \delta_2 = (q_1, q_2), \dots, \delta_k = (q_1, q_2, \dots, q_k), \dots$$

Эти дроби называют *подходящими дробями*.

Ясно, что закон образования соответствующих им простых дробей будет такой же, как и для подходящих дробей в случае конечных непрерывных дробей, так как этот закон зависит только от неполных частей q_1, q_2, \dots, q_k и совершенно не зависит от того, является ли q_k последним элементом или за ним следует еще элемент q_{k+1} . Поэтому для них сохранятся также остальные свойства, которые выводятся из закона образования числителей и знаменателей подходящих дробей. В частности, мы имеем здесь, как и в § 3, гл. III

1)

$$\delta_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}},$$

причем

$$P_k = q_k P_{k-1} + P_{k-2}, \quad Q_k = q_k Q_{k-1} + Q_{k-2};$$

2)

$$\Delta_k = P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k,$$

откуда следует несократимость подходящих дробей

$$\delta_k = \frac{P_k}{Q_k};$$

$$3) \quad \delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}}.$$

Сравним теперь подходящую дробь δ_{k+1} и кусок разложения α до остаточного числа α_{k+1} .
Имеем

$$\delta_{k+1} = q_1 + \frac{1}{q_2 + \frac{1}{q_k + \frac{1}{q_{k+1}}}} \quad \alpha = q_1 + \frac{1}{q_2 + \frac{1}{q_k + \frac{1}{\alpha_{k+1}}}},$$

откуда видно, что вычисление δ_{k+1} по δ_k формально производится таким же образом, как вычисление α по δ_k с тем лишь отличием, что в первом случае q_k заменяется на $q_k + \frac{1}{q_{k+1}}$, а во втором q_k заменяется на

$q_k + \frac{1}{\alpha_{k+1}}$. Поэтому на основании формулы

$$\delta_{k+1} = \frac{q_{k+1} \cdot P_k + P_{k-1}}{q_{k+1} Q_k + Q_{k-1}}$$

можно сделать вывод о справедливости следующего важного соотношения

$$\alpha = \frac{\alpha_{k+1} P_k + P_{k-1}}{\alpha_{k+1} Q_k + Q_{k-1}}. \quad (5)$$

По этой причине мы пишем также

$$\alpha = (q_1, q_2, \dots, q_k, \alpha_{k+1}),$$

хотя α_{k+1} не является здесь целым положительным числом. При помощи формулы (5) можно вывести следующую теорему о расположении подходящих дробей разложения действительного α .

*Действительное число α всегда находится между двумя соседними подходящими дробями своего разложения, причем оно ближе к последующей, чем к предыдущей подходящей дроби*¹.

Действительно, из (5) следует

¹ Рациональное число α совпадает со своей последней подходящей дробью δ_{k+1} и находится между любыми двумя подходящими дробями меньшего порядка.

$$\begin{aligned}\alpha \cdot \alpha_{k+1} Q_k + \alpha Q_{k-1} &= \alpha_{k+1} P_k + P_{k-1}, \\ \alpha_{k+1} (\alpha Q_k - P_k) &= P_{k-1} - \alpha Q_{k-1}, \\ \alpha_{k+1} Q_k \left(\alpha - \frac{P_k}{Q_k} \right) &= Q_{k-1} \left(\frac{P_{k-1}}{Q_{k-1}} - \alpha \right), \\ \alpha_{k+1} Q_k (\alpha - \delta_k) &= Q_{k-1} (\delta_{k-1} - \alpha).\end{aligned}$$

Но

$\alpha_{k+1} > 1$, $Q_k > Q_{k-1} > 0$, так что $\alpha_{k+1} Q_k > Q_{k-1} > 0$.

Из этого следует:

1) $\alpha - \delta_k$ и $\delta_{k-1} - \alpha$ имеют одинаковый знак, а это значит, что α находится между δ_{k-1} и δ_k ;

2) $|\alpha - \delta_k| < |\delta_{k-1} - \alpha|$, т. е. α ближе к δ_k , чем к δ_{k-1} .
Теорема доказана.

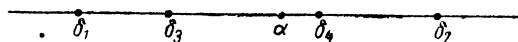
Так как, $\alpha > \delta_1 = q_1$, то $\alpha < \delta_2$, $\alpha > \delta_3$ и так далее; отсюда приходим к следующему заключению о взаимном расположении подходящих дробей:

1) α больше всех подходящих дробей нечетного порядка и меньше всех подходящих дробей четного порядка;

2) подходящие дроби нечетного порядка образуют возрастающую последовательность, а четного порядка — убывающую (в случае иррационального α указанные последовательности — бесконечные), т. е.

$$\delta_1 < \delta_3 < \dots < \alpha < \dots < \delta_4 < \delta_2$$

(в случае рационального α $\delta_n = \alpha$).



Учитывая, наконец, то, что при $k \rightarrow \infty$ $Q_k \rightarrow \infty$, вследствие чего

$$\lim_{k \rightarrow \infty} |\delta_k - \delta_{k-1}| = \lim_{k \rightarrow \infty} \frac{1}{Q_k \cdot Q_{k-1}} = 0,$$

приходим к дальнейшему выводу, что в случае иррационального α сегменты $[\delta_1, \delta_2]$, $[\delta_3, \delta_4]$, ... образуют стягивающуюся последовательность, которая, как известно, должна иметь единственную общую точку, являющуюся общим пределом последовательностей $\delta_1, \delta_3, \dots$ и $\delta_2, \delta_4, \dots$

Но так как α принадлежит всем сегментам последовательности, то α и совпадает с указанной точкой, так что

$$\alpha = \lim_{k \rightarrow \infty} \delta_k.$$

Итак, мы имеем следующий важный результат: *бесконечная последовательность подходящих дробей δ_k , которая возникает при разложении иррационального α , сходится к α , колеблясь около него.* Или: иррациональное действительное α равно пределу последовательности подходящих дробей своего разложения в бесконечную непрерывную дробь (процессом выделения целой части).

2. Сходимость правильных бесконечных цепных дробей

Покажем, что сходящейся является последовательность подходящих дробей не только такой бесконечной непрерывной дроби, которая возникает при разложении иррационального α , но и любой бесконечной непрерывной дроби (q_1, q_2, \dots) , где q_1 целое, а q_2, q_3, \dots произвольно выбранные целые положительные числа.

Однако для этого нам предварительно придется заново исследовать взаимное расположение подходящих дробей, так как соответствующие результаты предыдущего пункта выведены в связи с разложением α .

С этой целью рассмотрим формулы

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \quad (1) \quad \text{и} \quad |\delta_k - \delta_{k-1}| = \frac{1}{Q_k Q_{k-1}}, \quad (2)$$

которые справедливы для любой бесконечной непрерывной дроби.

1) формула (1) показывает, что всякая подходящая дробь четного порядка больше двух соседних подходящих дробей, у которых порядок на единицу меньше или больше, чем у нее, т. е.

$$\delta_{2k} > \delta_{2k-1} \quad \text{и} \quad \delta_{2k} > \delta_{2k+1}.$$

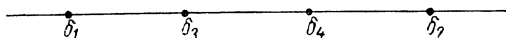
Согласно этому δ_1 и δ_3 расположены слева от δ_2 , δ_5 и δ_7 — слева от δ_4 и так далее.

2) формула (2) показывает, что расстояние между соседними подходящими дробями при увеличении k

убывает. Действительно, в силу того, что $Q_{k+1} > Q_{k-1}$, имеем

$$|\delta_{k+1} - \delta_k| = \frac{1}{Q_{k+1} Q_k} < \frac{1}{Q_k Q_{k-1}} = |\delta_k - \delta_{k-1}|;$$

3) согласно этому свойству δ_3 ближе к δ_2 , чем δ_1 , а так как δ_1 и δ_3 находятся слева от δ_2 , то $\delta_1 < \delta_3$ (см. рис.). Из этого далее следует, что подходящая дробь δ_4 , которая, как и δ_2 , расположена справа от δ_3 , ближе к δ_3 , чем δ_2 . Итак, $\delta_4 < \delta_2$.



Подходящие дроби дальнейших порядков располагаются подобным же образом.

Итак, подходящие дроби нечетного порядка увеличиваются с ростом порядка, а подходящие дроби четного порядка убывают с ростом порядка; при этом все подходящие дроби нечетного порядка меньше всех подходящих дробей четного порядка, т. е.

$$\delta_1 < \delta_3 < \dots < \delta_{2k+1} < \dots < \delta_{2l} < \dots < \delta_4 < \delta_2$$

при любых k и l .

И так как $\lim_{k \rightarrow \infty} (\delta_k - \delta_{k-1}) = 0$, то пары подходящих дробей $[\delta_1, \delta_2]$, $[\delta_3, \delta_4]$, ... образуют стягивающуюся последовательность отрезков, которая должна иметь единственную общую точку, являющуюся общим пределом последовательностей $\delta_1, \delta_3, \dots$ и $\delta_2, \delta_4, \dots$. Обозначая этот предел через α , имеем $\lim_{k \rightarrow \infty} \delta_k = \alpha$, причем,

очевидно, $\delta_{2k-1} < \alpha < \delta_{2k}$ для любых k , т. е. α находится между любыми двумя соседними подходящими дробями.

Следовательно, подходящие дроби любой бесконечной непрерывной дроби имеют некоторый предел α . Этот предел α принимается в качестве значения бесконечной непрерывной дроби. Говорят, что бесконечная непрерывная дробь сходится к α или представляет число α .

Теперь можно записать

$$\alpha = (q_1, q_2, q_3 \dots),$$

подразумевая при этом, что

$$\alpha = \lim_{k \rightarrow \infty} (q_1, q_2, \dots, q_k).$$

3. Единственность представления действительного иррационального числа правильной бесконечной цепной дробью

Учитывая результаты предыдущих пунктов, можно утверждать, что для каждого действительного иррационального α существует представление в виде бесконечной непрерывной дроби. Таким представлением является разложение α в бесконечную непрерывную дробь, так как предел подходящих дробей последней равен как раз α .

Возникает вопрос, сколько представлений действительного иррационального α в виде бесконечных непрерывных дробей существует вообще. Покажем, что только одно. Другими словами: представление действительного иррационального α в виде бесконечной непрерывной дроби всегда является разложением α с помощью выделения целой части¹.

Докажем это важное утверждение.

Пусть действительное иррациональное α представлено бесконечной непрерывной дробью $(q_1, q_2, \dots, q_k, q_{k+1}, \dots)$,

$$\text{т. е. } \alpha = \lim_{k \rightarrow \infty} (q_1, q_2, \dots, q_k).$$

Назовем теперь бесконечную непрерывную дробь (q_k, q_{k+1}, \dots) *остатком* данной дроби *порядка* k . Так как любая бесконечная непрерывная дробь представляет некоторое действительное число, то это утверждение относится также и к остатку (q_k, q_{k+1}, \dots) .

Обозначая его через α'_k , имеем

$$\alpha'_k = (q_k, q_{k+1}, \dots), \text{ т. е. } \alpha'_k = \lim_{r \rightarrow \infty} (q_k, q_{k+1}, \dots, q_{k+r}).$$

Аналогично

$$\alpha'_{k+1} = (q_{k+1}, q_{k+2}, \dots), \text{ т. е. } \alpha'_{k+1} = \lim_{r \rightarrow \infty} (q_{k+1}, \dots, q_{k+r}).$$

¹ Можно сказать: разложения иррациональных чисел исчерпывают все возможные бесконечные непрерывные дроби.

В силу этого из соотношения

$$(q_k, q_{k+1}, \dots, q_{k+r}) = q_k + \frac{1}{(q_{k+1}, q_{k+2}, \dots, q_{k+r})}$$

предельным переходом получаем

$$\alpha'_k = q_k + \frac{1}{\alpha'_{k+1}}. \quad (1)$$

Так как при

$$k \geq 1 \quad q_k \geq 1, \text{ то все } \alpha'_k > 1, \text{ а } \frac{1}{\alpha'_{k+1}} < 1;$$

следовательно,

$$q_k < \alpha'_k < q_k + 1,$$

т. е.

$$q_k = [\alpha'_k]. \quad (2)$$

Но так как $\alpha'_1 = \alpha$, то $q_1 = [\alpha]$ и, ввиду равенства (1), α'_2 равно остаточному числу 2-го порядка для α , т. е. (согласно обозначению в 1 п. настоящего §) α_2 .

Тогда далее

$$q_2 = [\alpha'_2] = [\alpha_2], \text{ а } \alpha'_3 = \alpha_3 \text{ и т. д.};$$

вообще в силу того что $\alpha'_k = \alpha_k$,

$$q_k = [\alpha'_k] = [\alpha_k], \text{ а } \alpha'_{k+1} = \alpha_{k+1}.$$

Элементы данной бесконечной непрерывной дроби получаются, таким образом, из его значения α последовательным выделением целой части; это и требовалось доказать.

Вместе с тем установлено, что остаток бесконечной непрерывной дроби $\alpha = (q_1, q_2, q_3, \dots)$ порядка $k+1$ α'_{k+1} совпадает с ее остаточным числом порядка $k+1$ α_{k+1} .

Поэтому формула (5) 1-го пункта остается действительной, если под α_{k+1} будем понимать остаток бесконечной непрерывной дроби порядка $k+1$.

Исследования настоящего параграфа приводят нас к следующему основному результату: *каждое иррациональное действительное число α единственным образом представляется бесконечной непрерывной дробью вида (q_1, q_2, \dots) и, наоборот, каждой бесконечной цепной дроби соответствует единственное ирра-*

циональное действительное число, которое она представляет.

Можно поэтому утверждать: множество всех действительных чисел взаимно однозначно отображается на множестве всех непрерывных дробей (если условиться, что для конечных непрерывных дробей берется последнее $q_n > 1$). При этом рациональным числам соответствуют конечные непрерывные дроби, а иррациональным — бесконечные дроби.

Упражнения

219. Найти разложение и подходящие дроби для $\alpha = \frac{\sqrt{5} + 1}{2}$

Отметить свойство последовательности знаменателей (а также числителей) этого разложения (получаемый ряд носит имя Фибоначчи, см. (40)).

220. Найти действительное число α , имеющее подходящую дробь δ_k и остаточное число α_{k+1} . Значения δ_k и α_{k+1} :

$$1) \frac{10}{3}, \sqrt{2}; \quad 2) \frac{43}{17}, \sqrt{5}.$$

221. Найти разложение действительного числа α в цепную дробь, если α имеет подходящую дробь δ_k и остаточное число α_{k+1} . Значения δ_k и α_{k+1} : 1) $\frac{10}{7}, \sqrt{3}$; 2) $\frac{37}{13}, \frac{1 + \sqrt{3}}{2}$.

222. Не разлагая действительное число α в цепную дробь, установить, может ли оно иметь подходящую дробь δ ?

$$\text{Значения } \alpha \text{ и } \delta: 1) \sqrt{10}, \frac{19}{6}; \quad 2) \sqrt{7}, \frac{37}{14}.$$

223. Теореме о расположении подходящих дробей разложения действительного α дать наглядное истолкование Ф. Клейна, приняв (ограничиваясь положительными числами) следующие условия: рациональной дроби $\frac{y}{x}$ (сократимой или несократимой) с положительными x и y сопоставим точку $M(x, y)$, так что $\frac{y}{x} = \operatorname{tg} MOx$, а иррациональному α — иррациональный луч OM_α (M_α — любая точка этого луча), для которого $\operatorname{tg} M_\alpha Ox = \alpha$. (Если $\frac{y}{x}$ — несократимая дробь, то на отрезке OM нет целых точек; на иррациональном луче OM_α нет целых точек, кроме O ; $\frac{y_1}{x_1} > \frac{y}{x}$ означает, что $\angle M_1 Ox > \angle MOx$; если луч OM лежит между лучами OM_1 и OM_2 , то будем это записывать символически

$OM_1, OM, OM_2 | \cdot$) В частности, пусть подходящим дробям δ_k и δ_{k-1} сопоставлены точки M_k и M_{k-1} , а действительному числу α — луч OM_α , если α иррационально, и точка M_α , если α дробь. Сделать чертеж.

§ 2. Приближение действительного числа рациональными дробями с заданным ограничением для знаменателя

1. Постановка задачи

Рассматривая задачу приближения действительного числа α (рационального или иррационального) рациональной дробью $\frac{p}{q}$, надо иметь в виду, что так как множество рациональных чисел всюду плотно, то существуют, конечно, рациональные дроби, сколь угодно близкие к любому α .

Если даны α и положительное число ε , то всегда существует рациональная дробь $\frac{p}{q}$ такая, что

$$\left| \alpha - \frac{p}{q} \right| < \varepsilon,$$

т. е. любое действительное α может быть аппроксимировано рациональной дробью с любой степенью точности.

Основные проблемы, которые здесь возникают, заключаются в следующем:

1) Если даны α и ε , найти, как велико необходимо взять q , чтобы добиться приближения с точностью до ε ?

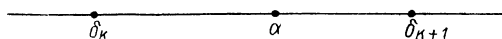
2) Если же даны α и q или некоторое ограничение сверху для q , установить, сколь малым можно сделать ε ?

2. Оценка погрешности при замене действительного числа его подходящей дробью

В вопросах приближенного представления действительных чисел (рациональных и иррациональных) рациональными дробями очень большое значение имеет аппарат непрерывных дробей.

Раньше, чем его практически применить, найдем оценку погрешности, возникающей от приближения действительного числа α его подходящей дробью.

Как уже известно, точное значение непрерывной дроби (конечной или бесконечной) находится между двумя соседними подходящими дробями.



Это дает нам возможность оценить погрешность, возникающую при замене точного значения непрерывной дроби ее подходящей дробью, а именно:

$$|\alpha - \delta_k| \leq |\delta_{k+1} - \delta_k| = \frac{1}{Q_k \cdot Q_{k+1}},$$

причем знак равенства следует брать только в том случае, когда $\alpha = \delta_{k+1}$. Но так как

$$Q_{k+1} = q_{k+1}Q_k + Q_{k-1},$$

где $q_{k+1} \geq 1$, а Q_k и Q_{k-1} целые положительные, то

$$Q_{k+1} \geq Q_k + Q_{k-1} > Q_k.$$

Поэтому

$$\frac{1}{Q_k Q_{k+1}} \leq \frac{1}{Q_k (Q_k + Q_{k-1})} < \frac{1}{Q_k^2}.$$

Таким образом, получаем следующие оценки погрешности $|\alpha - \delta_k|$:

$$|\alpha - \delta_k| \leq \frac{1}{Q_k Q_{k+1}}, \quad |\alpha - \delta_k| \leq \frac{1}{Q_k (Q_k + Q_{k-1})}, \quad (1)$$

$$|\alpha - \delta_k| < \frac{1}{Q_k^2},$$

из которых первая является наиболее точной, а последняя — наиболее грубой.

3. Приближение действительного числа подходящими дробями

Решение поставленной в заголовке задачи начнем с рассмотрения нескольких примеров.

Пример 1. Рассмотрим задачу, аналогичную той, с которой встретился голландский математик Х. Гюйгенс (1629 — 1695) при построении модели солнечной системы с помощью набора зубчатых колес и кото-

рая привела его к открытию ряда важных свойств непрерывных дробей.

Пусть требуется, чтобы отношение угловых скоростей двух зацепляющихся зубчатых колес II и I было равно α .

Так как угловые скорости колес обратно пропорциональны числам зубцов, то отношение чисел зубцов колес I и II должно быть равно α . Если α несократимая дробь $\frac{N}{n}$ с большими числителем и знаменате-

лем, например $\frac{1261}{881}$, то для точного решения задачи возникает техническая трудность изготовления колес с большим количеством зубцов.

Задачу можно технически упростить при помощи колес с меньшим числом зубцов. При этом важно, чтобы отношение этих чисел было, по возможности, ближе к заданному отношению. Хорошего удовлетворения поставленных требований можно добиться, если воспользоваться непрерывными дробями.

Пусть, например, поставлено требование заменить N и n меньшими числами N_1 и n_1 так, чтобы $n_1 \leq 100$ и чтобы отношение $\frac{N_1}{n_1}$ было, по возможности, ближе к $\frac{N}{n}$.

Применяя аппарат цепных дробей, можем дать следующее решение этой задачи: разлагаем $\frac{1261}{881}$ в непрерывную дробь и берем ее подходящую дробь с наибольшим знаменателем, не превышающим 100. Легко проверить, что

$$\frac{1261}{881} = (1, 2, 3, 7, 8, 2).$$

Составляя схему, находим

q_k		1	2	3	7	8	2
P_k	1	1	3	10	73	594	1261
Q_k	0	1	2	7	51	415	881

Поставленному условию удовлетворяет подходящая дробь

$$\delta_4 = \frac{73}{51}.$$

При этом допущенная погрешность

$$\left| \frac{N}{n} - \delta_4 \right| = \left| \frac{1261}{881} - \frac{73}{51} \right| < \frac{1}{51 \cdot 415} < 0,0001,$$

т. е. весьма незначительна.

Задачу можно было бы иначе поставить: заменить $\frac{N}{n}$ рациональной дробью с возможно меньшим знаменателем так, чтобы отклонение от данного отношения не превосходило бы 0,0001. При такой постановке задачи надо, пользуясь непрерывными дробями, отыскать подходящую дробь $\delta_k = \frac{P_k}{Q_k}$ с наименьшим знаменателем Q_k так, чтобы $Q_k \cdot Q_{k+1} > 10\,000$.

Ответом и здесь является подходящая дробь $\frac{73}{51}$.

Заметим, что для иррационального α по существу возможно лишь приближенное решение задачи.

Пример 2. Как нам уже известно, $\sqrt{11} = (3, (3, 6))$. Поставим перед собой задачу вычислить $\sqrt{11}$ с точностью до 0,001.

Для ее решения, как уже на это указывалось в конце предыдущей задачи, придется найти такую подходящую дробь $\delta_k = \frac{P_k}{Q_k}$ разложения $\sqrt{11}$, чтобы $Q_k \times Q_{k+1} > \frac{1}{0,001} = 1000$. Сделаем это, используя схему

q_k		3	3	6	3
P_k	1	3	10	63	199
Q_k	0	1	3	19	60

Очевидно, нам достаточно взять $\delta_3 = \frac{63}{19}$, так как $19 \cdot 60 > 1000$. Это значение будет равно $\sqrt{11}$ с точностью до 0,001, причем с недостатком, так как δ_3 — подходящая дробь нечетного порядка.

Мы можем $\frac{63}{19}$ представить в виде десятичной дроби, причем имеем право взять 3 знака после запятой, так как $\frac{63}{19}$ является приближенным значением для $\sqrt[3]{11}$ с точностью до 0,001. Получаем $\frac{63}{19} \approx 3,316$. (Мы округляем по избытку, так как $\frac{63}{19}$ является приближенным значением с недостатком, однако уже не можем теперь сказать, будет ли 3,316 приближенным значением $\sqrt[3]{11}$ с недостатком или избытком.)

Задачи, рассмотренные нами в примерах, в более общем виде формулируются так:

1). Найти рациональное приближение к действительному числу α со знаменателем $\leq n$ в виде наиболее близкой к α подходящей дроби.

Для этого надо взять подходящую дробь для α с наибольшим знаменателем $\leq n$.

2). Найти рациональное приближение к действительному числу α с возможно меньшим знаменателем так, чтобы погрешность не превосходила ε (т. е. с точностью до ε). Для этого, пользуясь аппаратом цепных дробей, находим подходящую дробь $\delta_k = \frac{P_k}{Q_k}$ с наи-

меньшим знаменателем Q_k так, чтобы $Q_k \cdot Q_{k+1} > \frac{1}{\varepsilon}$.

Заметим, что приближение подходящими дробями иррациональностей степени выше второй представляет значительные трудности. Рассмотрим соответствующий пример.

Пример 3. Найти подходящую дробь к $\sqrt[3]{2}$ с точностью до 0,01.

Решение 1. Имеем $\alpha = \sqrt[3]{2} = 1 + \frac{1}{\alpha_2}$. Для оценки целой части α_2 можно исходить из того уравнения, которому α_2 удовлетворяет. Чтобы его найти, заменим в левой части уравнения $\alpha^3 - 2 = 0$ число α выражением $1 + \frac{1}{\alpha_2}$. Практически уравнение относительно α_2 находят, разлагая левую часть данного уравнения

по степеням разности $\alpha - 1 = \frac{1}{\alpha_2}$, применяя для этого формулу Тейлора и схему Горнера¹.

Последовательно имеем тогда для α_2 , α_3 и α_4 следующие схемы, уравнения и оценки:

1.

	1	0	0	-2
1	1	1	1	-1
1	1	2	3	
1	1	3		

$$\alpha_2^3 - 3\alpha_2^2 - 3\alpha_2 - 1 = 0,$$

$$3 < \alpha_2 < 4, \quad \alpha_2 = 3 + \frac{1}{\alpha_3};$$

2.

	1	-3	-3	-1
3	1	0	-3	-10
3	1	3	6	
3	1	6		

$$10\alpha_3^3 - 6\alpha_3^2 - 6\alpha_3 - 1 = 0,$$

$$1 < \alpha_3 < 2, \quad \alpha_3 = 1 + \frac{1}{\alpha_4};$$

3.

	10	-6	-6	-1
1	10	4	-2	-3
1	10	14	12	
1	10	24		

$$3\alpha_4^3 - 12\alpha_4^2 - 24\alpha_4 - 10 = 0,$$

$$5 < \alpha_4 < 6, \quad \alpha_4 = 5 + \frac{1}{\alpha_5}.$$

Таким образом,

$$\sqrt[3]{2} = (1, 3, 1, 5, \dots),$$

¹ См., например: Л. Я. Окунев, Высшая алгебра, Учпедгиз, 1958, § 28 и 41.

так что

$$\delta_k = \frac{1}{0}, \frac{1}{1}, \frac{4}{3}, \frac{5}{4}, \frac{29}{23} \approx 1,26$$

и

$$\left| \sqrt[3]{2} - \frac{29}{23} \right| < \frac{1}{23^2} < 0,01.$$

Указанный способ решения можно применить для нахождения подходящих дробей иррациональности, определенной некоторым уравнением.

Решение 2. Можно выделять целую часть из $\alpha_2, \alpha_3, \alpha_4$ непосредственно.

$$\alpha_2 = \frac{1}{\sqrt[3]{2}-1} = \frac{\sqrt[3]{4} + \sqrt[3]{2} + 1}{1} = 3 + \frac{1}{\alpha_3},$$

так как $1,5 < \sqrt[3]{4} < 1,6$, $1,2 < \sqrt[3]{2} < 1,3$, что легко найти; далее

$$\alpha_3 = \frac{1}{\sqrt[3]{4} + \sqrt[3]{2} - 2} = 1 + \frac{1}{\alpha_4},$$

если учесть, что при указанных границах для $\sqrt[3]{4}$ и $\sqrt[3]{2}$ имеем $\frac{10}{7} > \alpha_3 > \frac{10}{9}$.

Определим теперь $\delta_3 = (1, 3, 1)$ к α и α_4 по формуле $\alpha_{k+1} = \frac{P_{k-1} - \alpha Q_{k-1}}{\alpha Q_k - P_k}$, вытекающей из (5), стр. 165,

так как из такого выражения для α_4 легче выделить его целую часть, чем из полученного выше соотношения для α_4 . Имеем

$$\delta_k = \begin{array}{c|ccc} q_k & 1 & 3 & 1 \\ \hline & 1 & 1 & 4 & 5 \\ & 0 & 1 & 3 & 4 \end{array}$$

поэтому

$$\begin{aligned} \alpha_4 &= \frac{4 - 3\sqrt[3]{2}}{4\sqrt[3]{2} - 5} = \frac{(4 - 3\sqrt[3]{2})(16\sqrt[3]{4} + 20\sqrt[3]{2} + 25)}{3} = \\ &= \frac{4 \cdot \sqrt[3]{4} + 5 \cdot \sqrt[3]{2} + 4}{3}, \end{aligned}$$

или

$$\alpha_4 = 5 + \frac{1}{\alpha_5},$$

если учесть хотя бы вышеуказанные границы для $\sqrt[3]{4}$ и $\sqrt[3]{2}$.

Таким образом, так же как и в решении 1, находим $\sqrt[3]{2} = (1, 3, 1, 5, \dots)$ и т. д.

4. Теорема Дирихле

А. Во 2-м пункте настоящего параграфа мы нашли оценку погрешности, возникающей при замене любого действительного числа α рациональными дробями определенного типа, а именно: подходящими дробями.

Закономерность возможного приближения любого действительного числа α рациональной дробью, независимо от того или иного ее вида, выражает следующая важная теорема, которая носит имя Дирихле.

Теорема Дирихле. Пусть α и $\tau \geq 1$ действительные числа; существует несократимая дробь $\frac{a}{b}$, для которой

$$\left| \alpha - \frac{a}{b} \right| < \frac{1}{b\tau}, \quad 0 < b \leq \tau^1$$

(или: существует такая пара взаимно простых целых чисел a и b , что $|b\alpha - a| < \frac{1}{\tau}$, $0 < b \leq \tau$).

Содержание теоремы Дирихле можно выразить и так: для любого действительного α и произвольного $\tau \geq 1$ существует рациональное приближение $\frac{a}{b}$ с точностью до $\frac{1}{b\tau}$, где $0 < b \leq \tau$, например для $\sqrt{19}$ существует рациональное приближение $\frac{a}{b}$ с точностью до $\frac{1}{1000b}$, причем b не больше 1000.

Теорему легко доказать с помощью аппарата цепных дробей.

¹ Если τ отлично от натурального числа, то знак равенства отпадает.

Пусть $\frac{P_k}{Q_k}$ подходящая дробь числа α ; выберем наибольший из знаменателей Q_k , не превышающий τ , т. е. наибольшее k , чтобы $Q_k \leq \tau$ и положим $\frac{a}{b} = \frac{P_k}{Q_k}$.

Не останавливаясь на тривиальном случае, когда

$$\alpha = \frac{P_k}{Q_k}, \text{ имеем } Q_k \leq \tau < Q_{k+1},$$

поэтому

$$\left| \alpha - \frac{a}{b} \right| = \left| \alpha - \frac{P_k}{Q_k} \right| \leq \frac{1}{Q_k \cdot Q_{k+1}} < \frac{1}{b\tau}.$$

Теорема доказана.

Б. Сам Дирихле дал другое доказательство, используя в нем принцип, который носит теперь имя Дирихле: при распределении N объектов между $N-1$ ящиками хотя бы в одном ящике должно находиться 2 объекта.

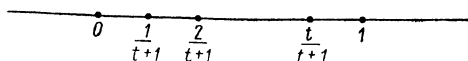
Ввиду общей значимости принципа Дирихле, приведем упомянутое доказательство.

Пусть $t = [\tau]$. Рассмотрим совокупность $t+2$ чисел, состоящую из 1 и значений дробных частей $\{x\alpha\}$ для $x = 0, 1, \dots, t$ (причем, как известно, $\{x\alpha\} = x\alpha - [x\alpha]$, $0 \leq \{x\alpha\} < 1$).

Очевидно, каждое из чисел этой совокупности принадлежит точно одному из $t+1$ промежутков

$$\left[0, \frac{1}{t+1}\right), \left[\frac{1}{t+1}, \frac{2}{t+1}\right), \dots, \left[\frac{t}{t+1}, 1\right],$$

из которых первые t являются полусегментами, а последний — сегментом.



Так как чисел у нас $t+2$, то (согласно принципу Дирихле) обязательно найдется такой промежуток, который содержит 2 числа из совокупности $\{x\alpha\}$ и 1. Разность этих двух чисел не превосходит длину содержащего их промежутка, т. е. $\leq \frac{1}{t+1} < \frac{1}{\tau}$.

1. Если такими числами являются $\{x_1\alpha\}$ и $\{x_2\alpha\}$, то
- $$|\{x_2\alpha\} - \{x_1\alpha\}| = |(x_2 - x_1)\alpha - ([x_2\alpha] - [x_1\alpha])|.$$

Пусть

$$x_2 > x_1 \text{ и } x_2 - x_1 = b, [x_2\alpha] - [x_1\alpha] = a.$$

Так как $0 < b \leq t \leq \tau$, то

$$|b\alpha - a| < \frac{1}{\tau}, \quad 0 < b \leq \tau.$$

2. Если $\{x_3\alpha\}$ и 1 принадлежат одному промежутку, то

$$|1 - \{x_3\alpha\}| = |1 - x_3\alpha + [x_3\alpha]| = |x_3\alpha - (1 + [x_3\alpha])|.$$

Пусть в таком случае

$$x_3 = b, \quad 1 + [x_3\alpha] = a.$$

Очевидно, и здесь $0 < b \leq t \leq \tau$, так что

$$|b\alpha - a| < \frac{1}{\tau}, \quad 0 < b \leq \tau.$$

Теорема доказана.

Заметим, не останавливаясь на этом подробно, что главное преимущество применения принципа Дирихле заключается в том, что его легко применить для обобщения рассматриваемой задачи (приближения действительного α к рациональному $\frac{a}{b}$) на случай нескольких действительных чисел. Кроме того, метод Дирихле имеет огромное значение в учении о приближенном решении уравнений в целых числах, т. е. в теории диофантовых приближений.

В. Примеры применения теоремы Дирихле.

1. Найти приближение $\frac{a}{b}$ к $\sqrt{19}$ с точностью до $\frac{1}{100b}$.

Разлагая $\sqrt{19}$ (вычисления опускаем), находим

$$\sqrt{19} = (4, (2, 1, 3, 1, 2, 8)).$$

Из схемы

	4	2	1	3	1	2	8
1	4	9	13	48	61	170	
0	1	2	3	11	14	39	326

видно, что наибольший знаменатель $Q_k \leq 100$ равен 39. Поэтому в качестве решения можно взять дробь $\frac{170}{39}$;

$$\left| \sqrt{19} - \frac{170}{39} \right| < \frac{1}{100 \cdot 39}.$$

2. Доказать, что каждое простое число $p = 4n + 1$ есть сумма двух квадратов.

Так как (-1) является квадратичным вычетом такого p (см. свойство III символа Лежандра), то существует такое k , что

$$k^2 \equiv -1 \pmod{p}.$$

Возьмем $a = \frac{k}{p}$ и $\tau = \sqrt{p}$; тогда согласно теореме Дирихле существуют такие целые числа z и x , что

$$\left| \frac{k}{p} - \frac{z}{x} \right| < \frac{1}{x\sqrt{p}}, \quad 0 < x < \sqrt{p}.$$

Введем обозначение

$$y = kx - pz, \text{ так что } |y| < \sqrt{p}.$$

Так как

$$y \equiv kx \pmod{p},$$

то

$$y^2 \equiv k^2 x^2 \equiv -x^2 \pmod{p},$$

откуда

$$x^2 + y^2 \equiv 0 \pmod{p},$$

а так как

$$x^2 < p, \quad y^2 < p,$$

то должно быть

$$x^2 + y^2 = p. \quad (1)$$

Заметим, что $(x, y) = 1$, так как из $(x, y) = d \neq 1$ следовало бы, что $x^2 | d^2$, $y^2 | d^2$ и $p | d^2$, а это невозможно.

Полученный результат можно выразить так: уравнение (1), где $p = 4n + 1$ нечетное простое число, всегда имеет решение во взаимно простых целых числах x, y (в п. 2, § 5, гл. VIII будет показано, что в натуральных числах — только единственное).

Доказательство указывает путь, как найти решение. Практически целесообразнее вычислять разности $p - 1^2, p - 2^2, \dots$, пока не получится квадрат.

5. Подходящие дроби, как наилучшие приближения

А. В рассмотренных примерах мы видели, что подходящие дроби хорошо аппроксимируют действительные числа. Они дают в общем куда лучшие приближения, чем приближающие десятичные дроби с примерно такими же знаменателями, что у подходящих дробей.

В самом деле, округляя десятичное выражение действительного α до n -го знака после запятой, мы тем самым представляем α приближенно дробью $\frac{p}{q}$ со знаменателем $q = 10^n$, причем погрешность

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q};$$

если же $\frac{p}{q}$ подходящая дробь к α , то, как известно,

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2},$$

так что при сколько-нибудь значительном q величина $\frac{1}{q^2}$ во много раз меньше, чем $\frac{1}{2q}$.

Так, например, десятичное выражение числа $\pi = 3,1415926 \dots$ в виде рациональной дроби со знаменателем ≤ 100 имеет вид $3,14 = \frac{314}{100}$ откуда $|\pi - 3,14| < 0,0016$. Если же π разложить в цепную дробь, получается

$$\pi = (3, \quad 7, \quad 15, \dots),$$

$$\delta_k = 0, \quad \frac{3}{1}, \quad \frac{22}{7}, \quad \frac{333}{106}.$$

Наибольшей подходящей дробью для π со знаменателем ≤ 100 является число $\frac{22}{7}$, известное уже Архимеду, причем

$$\left| \pi - \frac{22}{7} \right| < \frac{1}{7 \cdot 106} < 0,0014.$$

Итак, приближение подходящей дробью дает большую точность при значительно меньшем знаменателе, чем приближение десятичной дробью.

Основой рассматриваемого факта является большая гибкость аппарата цепных дробей по сравнению с аппаратом десятичных дробей: в то время как знаменатели подходящих дробей полностью определяются арифметической природой изображаемого числа, знаменатели приближающих десятичных дробей не могут быть иными, как только 10^n .

Естественно возникает теперь вопрос, нельзя ли при том же или меньшем знаменателе, что у подходящей дроби, найти такое рациональное число, которое дало бы еще лучшее приближение, чем выбранная подходящая дробь. Оказывается, что это невозможно. Имеет место следующая замечательная теорема: *если рациональное число $\delta = \frac{P}{Q}$ ближе к действительному числу α , чем его подходящая дробь $\delta_k = \frac{P_k}{Q_k}$, где $k > 1$, то $Q > Q_k$, т. е., если $|\alpha - \delta| < |\alpha - \delta_k|$, то $Q > Q_k$.*

Доказательство. Рассмотрим случай, когда $\alpha \neq \delta_k$ (так как иначе теорема теряет смысл). Тогда α всегда лежит между любыми двумя последующими подходящими дробями, так что для $k > 1$ α всегда лежит между δ_{k-1} и δ_k , причем α ближе к δ_k , чем к δ_{k-1} .

Поэтому, если δ ближе к α , чем δ_k , то оно находится между δ_{k-1} и δ_k .

В случае четного k можно записать

$$\delta_{k-1} < \delta < \delta_k$$

(в случае нечетного k доказательство существенно не изменяется), откуда

$$0 < \delta - \delta_{k-1} < \delta_k - \delta_{k-1} = \frac{1}{Q_k Q_{k-1}},$$

или

$$0 < \frac{P}{Q} - \frac{P_{k-1}}{Q_{k-1}} < \frac{1}{Q_k \cdot Q_{k-1}},$$
$$0 < \frac{PQ_{k-1} - QP_{k-1}}{QQ_{k-1}} < \frac{1}{Q_k \cdot Q_{k-1}},$$

откуда

$$Q_k(PQ_{k-1} - QP_{k-1}) < Q.$$

Так как $PQ_{k-1} - QP_{k-1}$ число целое и положительное, то из предыдущего неравенства следует $Q_k < Q$, что и утверждается в теореме.

Попутно нами еще установлено, что любая рациональная дробь $\delta = \frac{P}{Q}$, принадлежащая интервалу (δ_{k-1}, δ_k) , $k > 1$, имеет знаменатель $Q > Q_k > Q_{k-1}$.

Заметим, что для $k=1$ теорема неверна:

$\delta = \frac{P}{Q}$ может оказаться ближе к α , чем его подходящая дробь $\delta_1 = \frac{P_1}{Q_1} = \frac{q_1}{1} = q_1$, хотя $Q = Q_1 = 1$. Так, например, для $\alpha = \sqrt{15}$ $\delta_1 = \frac{3}{1}$, однако $\frac{4}{1}$ ближе к α .

Доказанная теорема приводит нас к определению понятия *наилучшего приближения*: рациональную дробь $\frac{a}{b}$ называют наилучшим приближением действительного α , если любая более близкая к α рациональная дробь $\frac{c}{d}$ имеет больший знаменатель, чем $\frac{a}{b}$, т. е. если из

$$\left| \alpha - \frac{c}{d} \right| < \left| \alpha - \frac{a}{b} \right| \text{ следует } d > b.$$

Таким образом, подходящие дроби являются наилучшими приближениями, например Архимедово число $\frac{22}{7}$ для π является наилучшим приближением.

Заметим в заключение, не останавливаясь на этом подробно, что подходящие дроби не являются единственными наилучшими приближениями в указанном смысле.

Б. Во 2-м пункте настоящего параграфа мы доказали, что для оценки погрешности $|\alpha - \delta_k|$, возникающей при замене любого действительного числа α его подходящей дробью $\delta_k = \frac{P_k}{Q_k}$, можно пользоваться неравенством

$$|\alpha - \delta_k| < \frac{1}{Q_k^2}.$$

Выразим этот результат по отношению к действительным иррациональным числам α , имеющим бесконечное множество подходящих дробей, следующим образом: для любого действительного иррационального α существует при $c=1$ бесконечное множество несократимых дробей $\frac{P}{Q}$, таких, что

$$\left| \alpha - \frac{P}{Q} \right| < \frac{c}{Q^2}. \quad (1)$$

Таковыми дробями являются, например, все подходящие дроби для α

$$\delta_k = \frac{P_k}{Q_k}.$$

Возникает вопрос о существовании меньших значений c (чем $c=1$), для которых неравенство (1) допускает для любого действительного иррационального α бесконечное множество решений в виде несократимых дробей $\frac{P}{Q}$.

(Указанный вопрос можно поставить и так: при каких меньших значениях c (чем $c=1$) существует для любого действительного иррационального α бесконечное множество (несократимых) рациональных приближений $\frac{P}{Q}$, погрешность которых $< \frac{c}{Q^2}$.) Оказывается, что такие числа c существуют.

Теорема. Для любого действительного иррационального числа α существует при $c = \frac{1}{2}$ бесконечное множество несократимых рациональных дробей

бей $\frac{P}{Q}$, таких, что выполняется неравенство (1), т. е. неравенство

$$\left| \alpha - \frac{P}{Q} \right| < \frac{1}{2 \cdot Q^2}. \quad (1')$$

Таковыми рациональными дробями могут быть только подходящие дроби к α .

Справедливость первой части утверждения следует из того, что из двух последующих подходящих дробей

$$\delta_k = \frac{P_k}{Q_k} \text{ и } \delta_{k+1} = \frac{P_{k+1}}{Q_{k+1}} \text{ к } \alpha$$

при $k > 1$ по крайней мере одна удовлетворяет неравенству (1').

Действительно, если допустить противное, то мы имели бы

$$|\alpha - \delta_k| \geq \frac{1}{2Q_k^2}, \quad |\alpha - \delta_{k+1}| \geq \frac{1}{2 \cdot Q_{k+1}^2},$$

откуда

$$|\alpha - \delta_k| + |\alpha - \delta_{k+1}| \geq \frac{1}{2} \left(\frac{1}{Q_k^2} + \frac{1}{Q_{k+1}^2} \right).$$

Но так как α лежит между δ_k и δ_{k+1} , то

$$|\alpha - \delta_k| + |\alpha - \delta_{k+1}| = |\delta_k - \delta_{k+1}| = \frac{1}{Q_k Q_{k+1}},$$

вследствие чего

$$\frac{1}{2} \left(\frac{1}{Q_k^2} + \frac{1}{Q_{k+1}^2} \right) \leq \frac{1}{Q_k Q_{k+1}}, \text{ или } \left(\frac{1}{Q_k} - \frac{1}{Q_{k+1}} \right)^2 \leq 0,$$

а это для $k > 1$ невозможно.

Вторая часть теоремы вытекает из достаточного признака подходящей дроби к действительному числу α : если $\frac{P}{Q}$, где $Q > 0$, несократимая дробь и для действительного α имеет место неравенство (1'), то $\frac{P}{Q}$ является подходящей дробью к α .

Для доказательства этого признака достаточно показать, что, принимая $\frac{P}{Q} = (q_1, q_2, \dots, q_k) = \frac{P_k}{Q_k}$, удов-

летворяющее условию теоремы, в качестве подходящей дроби к α , соответствующее остаточное число α_{k+1} разложения данного α в цепную дробь окажется > 1 . Но это действительно так, ибо из

$$\left| \alpha - \frac{P_k}{Q_k} \right| = \left| \frac{\alpha_{k+1} P_k + P_{k-1}}{\alpha_{k+1} Q_k + Q_{k-1}} - \frac{P_k}{Q_k} \right| = \\ = \frac{1}{Q_k (\alpha_{k+1} Q_k + Q_{k-1})} < \frac{1}{2Q_k^2}$$

следует $\alpha_{k+1} Q_k - Q_{k-1} > 2Q_k$, откуда

$$\alpha_{k+1} > 2 - \frac{Q_{k-1}}{Q_k} > 1,$$

в силу того, что $\frac{Q_{k-1}}{Q_k} < 1$.

Достаточное условие подходящей дроби имеет важное значение: с его помощью можно, например, решить уравнение Пелля $x^2 - ay^2 = 1$, где $a > 0$ и \sqrt{a} — иррациональное число (см. § 4 настоящей гл.).

Заметим, что достаточный признак подходящей дроби не является ее необходимым признаком; могут существовать подходящие дроби для α (их может даже быть бесконечно много), которые ему не удовлетворяют.

Крайнюю возможность уменьшения c в указанном раньше смысле выражает теорема Гурвица — Бореля: для любого действительного иррационального числа α существует при $c = \frac{1}{\sqrt{5}}$ бесконечное множество несократимых рациональных дробей $\frac{P}{Q}$, таких, что выполняется неравенство (1), т. е. неравенство

$$\left| \alpha - \frac{P}{Q} \right| < \frac{1}{\sqrt{5}Q^2}, \quad (1'')$$

если же $c < \frac{1}{\sqrt{5}}$, то существуют такие действительные иррациональные α , для которых неравенство (1) имеет не более конечного числа рациональных решений $\frac{P}{Q}$ (о последних мы говорим, что они «плохо»

приближаются рациональными дробями; такими, например, являются все квадратические иррациональности, т. е. иррациональные корни квадратных уравнений с целыми коэффициентами (см. § 3, настоящей гл.).

Справедливость первой части теоремы вытекает из того, что из трех соседних подходящих дробей $\delta_i = \frac{P_i}{Q_i}$, $i = k, k+1, k+2$ действительного α по крайней мере одна удовлетворяет условию $|\alpha - \delta_i| < \frac{1}{\sqrt{5}Q_i^2}$. Это утверждение оставим без доказатель-

ства. По второй части теоремы ограничимся замечанием относительно того, что достаточно доказать существование таких действительных иррациональных α , для которых при $c < \frac{1}{\sqrt{5}}$ неравенству (1) удовлет-

воряют не более конечного числа подходящих дробей к α , так как согласно предыдущей теореме других рациональных дробей (кроме подходящих), удовлетворяющих (1) при $c \leq \frac{1}{2}$, вообще быть не может.

Заметим в заключение, что последним теоремам можно дать и другое очень важное истолкование. Рассмотрим для этого уравнение

$$\alpha x - y = 0, \quad (2)$$

где α — любое действительное иррациональное число. Исключая тривиальное решение $x = y = 0$, уравнение (2) не может иметь решений в целых числах. Однако можно поставить задачу о приближенном его решении в целых числах, т. е. о нахождении таких пар чисел x ($x > 0$) и y , чтобы

$$|\alpha x - y| < \frac{c}{x},$$

или

$$\left| \alpha - \frac{y}{x} \right| < \frac{c}{x^2}.$$

Теорема Гурвица — Бореля показывает, что для $c \geq \frac{1}{\sqrt{5}}$ всегда существует бесконечное множество

таких пар; если же $c < \frac{1}{\sqrt{5}}$, то существуют такие действительные числа, для которых таких пар имеется лишь конечное множество.

Новая точка зрения получает в содружестве с методом Дирихле весьма значительное применение в теории диофантовых приближений.

Упражнения

224. Пользуясь аппаратом цепных дробей, заменить дробь $\frac{N}{n}$ дробью $\frac{N_1}{n_1}$ так, чтобы $n_1 \leq 100$ и чтобы $\frac{N_1}{n_1}$ было по возможности ближе к $\frac{N}{n}$; оценить допущенную погрешность ϵ ;

$$\frac{N}{n} = 1) \frac{1847}{379}, 2) \frac{857}{149}, 3) \frac{1499}{647}, 4) \frac{2099}{593}.$$

225. Пользуясь аппаратом цепных дробей, заменить дробь $\frac{N}{n}$ дробью $\frac{N_1}{n_1}$ с возможно меньшим знаменателем n_1 так, чтобы допущенная при этом погрешность не превышала ϵ . Значения $\frac{N}{n}$ и ϵ : 1) из примеров предыдущей задачи с $\epsilon = 0,01$; 2) $\frac{1741}{293}$, $\epsilon = 0,01$; 3) $\frac{1327}{383}$, $\epsilon = 0,001$; 4) $\frac{1609}{239}$, $\epsilon = 0,01$.

226. Пользуясь аппаратом цепных дробей, найти для \sqrt{a} рациональное приближение с наибольшим знаменателем $n_1 \leq b$ и оценить допущенную погрешность ϵ : 1) $a = 15$, $n_1 \leq 10$; 2) $a = 17$, $n_1 \leq 10$; 3) $a = 23$, $n_1 \leq 50$; 4) $a = 31$, $n_1 \leq 100$.

227. Среди подходящих дробей разложения α найти приближение к α с возможно меньшим знаменателем так, чтобы допущенная погрешность не превышала ϵ : 1) $\alpha = \sqrt{26}$, $\epsilon = 0,001$; 2) $\alpha = \sqrt{37}$, $\epsilon = 0,001$; 3) $\alpha = \sqrt{29}$, $\epsilon = 0,001$; 4) $\alpha = \sqrt{19}$, $\epsilon = 0,01$.

228. То же, что в предыдущей задаче, для

$$1) \alpha = \frac{\sqrt{5} + 2}{2}, \epsilon = 0,01; 2) \alpha = \frac{\sqrt{401} + 18}{11}, \epsilon = 0,01;$$

$$3) \alpha = \frac{2\sqrt{39} + 11}{7}, \epsilon = 0,01; 4) \alpha = \frac{\sqrt{101} + 9}{5}, \epsilon = 0,01;$$

$$5) \alpha = \frac{\sqrt{7} + 2}{4}, \epsilon = 0,01; 6) \alpha = \frac{\sqrt{21} + 9}{6}, \epsilon = 0,01.$$

229. Найти для разложения $e = 2,718\ 281\ 828 \dots$ в цепную дробь ее неполные частные до q_6 и подходящие дроби до δ_6 ; оценить погрешность для δ_6 и выразить эту подходящую дробь в виде десятичной дроби.

230. Найти подходящую дробь к $\sqrt[3]{10}$ с точностью до 0,01.

231. Среди подходящих дробей разложения α найти наилучшее приближение \bar{a} со знаменателем $n_1 \leq b$ и оценить допущенную погрешность ϵ :

$$1) \alpha = \frac{\sqrt{77} - 3}{2}, n_1 \leq 100; 2) \alpha = \frac{\sqrt{35} + 1}{2}, n_1 \leq 100;$$

$$3) \alpha = \frac{22 + \sqrt{15}}{7}, n_1 \leq 100; 4) \alpha = \frac{\sqrt{21} + 1}{2}, n_1 \leq 50.$$

232. Сформулировать теорему о том, что любая рациональная дробь $\delta = \frac{P}{Q}$, принадлежащая интервалу (δ_{k-1}, δ_k) , $k > 1$, имеет знаменатель $Q > Q_k > Q_{k-1}$, пользуясь интерпретацией Ф. Клейна (см. задачу 223).

233. Найти разложение простого числа p на сумму двух квадратов; значения p : 97, 137, 157, 173, 181, 193, 197, 281, 317.

§ 3. Квадратические иррациональности и периодические цепные дроби

Иррациональный корень квадратного уравнения с целыми коэффициентами называется *квадратической иррациональностью*. Общий вид действительной квадратической иррациональности следующий

$$\frac{a + \sqrt{b}}{c},$$

где a, b, c — целые числа, $a, b > 0$, но не является квадратом целого числа.

Раскладывая квадратическую иррациональность \sqrt{b} в непрерывную дробь, мы заметили, что получается периодическая непрерывная дробь (см. § 1, настоящей гл.). Оказывается, что это не единичное и частное явление, а общая закономерность.

Справедлива также обратная теорема, с рассмотрения которой, как более легкой, мы и начнем настоящий параграф.

Теорема: *всякая периодическая непрерывная дробь изображает квадратическую иррациональность.*

Доказательство. Пусть α смешанная периодическая цепная дробь, т. е.

$$\alpha = (q_1, q_2, \dots, q_k, \alpha'),$$

где

$$\alpha' = ((q'_1, q'_2, \dots, q'_l))$$

чисто периодическая цепная дробь.

Обозначим подходящие дроби к α и α' соответственно через $\frac{P_i}{Q_i}$ и $\frac{P'_i}{Q'_i}$.

Так как

$$\alpha' = (q'_1, q'_2, \dots, q'_l, \alpha'),$$

то согласно формуле (5) из 1-го пункта § 1 настоящей главы

$$\alpha' = \frac{P'_l \alpha' + P'_{l-1}}{Q'_l \alpha' + Q'_{l-1}}.$$

Из этой формулы видно, что α' удовлетворяет квадратному уравнению с целыми коэффициентами. Кроме того, α' — число иррациональное, так как оно представляет бесконечную непрерывную дробь.

Таким образом, α' является квадратической иррациональностью.

Но по той же формуле

$$\alpha = \frac{P_k \alpha' + P_{k-1}}{Q_k \alpha' + Q_{k-1}},$$

поэтому и α является, очевидно, квадратической иррациональностью.

Труднее доказать обратную теорему, которая носит имя Лагранжа.

Теорема Лагранжа: *всякая действительная квадратическая иррациональность изображается периодической непрерывной дробью.*

Доказательство: пусть α действительный иррациональный корень квадратного уравнения

$$a\alpha^2 + b\alpha + c = 0 \tag{1}$$

с целыми коэффициентами a, b, c .

При разложении α в непрерывную дробь получаем

$$\alpha = \frac{P_k x' + P_{k-1}}{Q_k x' + Q_{k-1}}, \quad (2)$$

где α' — остаток α порядка $k + 1$.

Подставляя выражение для α из (2) в (1), получаем после преобразований (которые ввиду их тривиальности опускаем)

$$A_k \cdot \alpha'^2 + B_k \alpha' + C_k = 0, \quad (3)$$

где

$$\begin{cases} A_k = aP_k^2 + bP_k \cdot Q_k + cQ_k^2, \\ B_k = 2aP_k P_{k-1} + b(P_k Q_{k-1} + P_{k-1} Q_k) + 2cQ_k Q_{k-1}, \\ C_k = aP_{k-1}^2 + bP_{k-1} Q_{k-1} + cQ_{k-1}^2. \end{cases} \quad (4)$$

Отсюда во-первых, видно, что

$$C_k = A_{k-1}; \quad (5)$$

во-вторых, можно непосредственным вычислением установить, что

$$B_k^2 - 4A_k C_k = (b^2 - 4ac) (P_k Q_{k-1} - Q_k P_{k-1})^2 = b^2 - 4ac. \quad (6)$$

Таким образом, дискриминант уравнения (3) такой же, как и дискриминант уравнения (1), откуда следует, что он от k не зависит.

Идея доказательства в дальнейшем заключается в том, чтобы показать, что при данном α коэффициенты A_k , B_k и C_k ограничены по своей абсолютной величине.

Если этот факт на самом деле имел бы место, то это означало бы, что коэффициенты, будучи целыми числами, могут принимать только конечное число различных значений. Вместе с тем и число возможных уравнений (3) было бы конечным, хотя k пробегает бесконечное множество значений.

Но в таком случае и остатки α' (которые определяются из (3)), число которых бесконечно, могли бы принять только конечное число различных значений. Поэтому должны были бы существовать остатки α' с одинаковыми значениями, а это уже означает, что непрерывная дробь — периодическая.

Итак, попытаемся доказать, что A_k , B_k и C_k ограничены по абсолютной величине. Достаточно сделать это для A_k , так как, в силу соотношения (5), из ограниченности A_k уже как следствие вытекает ограниченность C_k и далее, в силу равенства (6), ограниченность B_k .

Как известно из свойств подходящих дробей,

$$\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k^2},$$

или

$$\alpha - \frac{P_k}{Q_k} = \frac{\varepsilon}{Q_k^2}, \text{ где } |\varepsilon| < 1,$$

откуда

$$\frac{P_k}{Q_k} = \alpha - \frac{\varepsilon}{Q_k^2}.$$

Поэтому из первого равенства (4) имеем

$$\begin{aligned} \frac{A_k}{Q_k^2} &= a \left(\frac{P_k}{Q_k} \right)^2 + b \left(\frac{P_k}{Q_k} \right) + c = a \left(\alpha - \frac{\varepsilon}{Q_k^2} \right)^2 + \\ &+ b \left(\alpha - \frac{\varepsilon}{Q_k^2} \right) + c = a\alpha^2 + b\alpha + c - \\ &- 2a\alpha \cdot \varepsilon \frac{1}{Q_k^2} + a\varepsilon^2 \frac{1}{Q_k^4} - b\varepsilon \frac{1}{Q_k^2}. \end{aligned}$$

Так как $a\alpha^2 + b\alpha + c = 0$, то из предыдущего далее следует

$$|A_k| = \left| -2a\alpha\varepsilon + a\varepsilon^2 \frac{1}{Q_k^4} - b\varepsilon \frac{1}{Q_k^2} \right|$$

и

$$|A_k| \leq |2a\alpha| + |a| + |b|,$$

а это и доказывает ограниченность $|A_k|$.

Согласно вышеизложенному, этим завершается также и доказательство теоремы Лагранжа.

Отметим еще без доказательства следующие свойства разложений квадратических иррациональностей;

1) при разложении квадратного корня из целого положительного числа, не являющегося полным квадратом, период начинается со второго звена;

2) чисто периодическая цепная дробь получается тогда и только тогда, когда квадратическая иррациональность

$$\alpha = \frac{a + \sqrt{b}}{c} > 1,$$

а сопряженная иррациональность α' , т. е.

$$\alpha' = \frac{a - \sqrt{b}}{c}$$

лежит в интервале $(-1, 0)$.

Примеры. 1. Составить уравнение, один из корней которого разлагается в периодическую непрерывную дробь $((2, 3, 1))$, и найти значение этой дроби.

Решение: $x = (2, 3, 1, x)$.

Составляем схему вычисления числителей и знаменателей подходящих дробей:

	1	2	3	1	x
1	2	7	9	$9x + 7$	
0	1	3	4	$4x + 3$	

Итак, $x = \frac{9x + 7}{4x + 3},$

откуда получаем

$$4x^2 - 6x - 7 = 0.$$

Положительное решение этого уравнения дает искомую периодическую дробь $((2, 3, 1)) = \frac{3 + \sqrt{37}}{4}.$

Заметим, что $\frac{3 + \sqrt{37}}{4} > 1$, а $\frac{3 - \sqrt{37}}{4}$ лежит в интервале $(-1, 0)$.

2. Составить уравнение, один из корней которого разлагается в смешанную периодическую дробь $(4, (2, 1))$, и найти значение этой дроби.

Решение: $x = (4, y)$, где $y = (2, 1, y)$.

Составляем схему для вычисления числителей и знаменателей подходящих дробей y :

	2	1	y
1	2	3	$3y + 2$
0	1	1	$y + 1$

Следовательно,

$$y = \frac{3y+2}{y+1}, \quad x = 4 + \frac{1}{y}.$$

Определим y из $y^2 - 2y - 2 = 0$.

Так как $y > 0$, то мы должны взять положительный корень этого уравнения $y = 1 + \sqrt{3}$. Поэтому для x имеем

$$x = 4 + \frac{1}{1 + \sqrt{3}} = 4 + \frac{\sqrt{3}-1}{2} = \frac{7 + \sqrt{3}}{2}.$$

Таким образом, искомая дробь $(4, (2,1)) = \frac{7 + \sqrt{3}}{2}$.

Для соответствующего квадратного уравнения имеем

$$2x - 7 = \sqrt{3},$$

откуда получаем $2x^2 - 14x + 23 = 0$.

Заметим, что при решении данной задачи можно было сначала из $x = 4 + \frac{1}{y}$ найти $y = \frac{1}{x-4}$ и это выражение подставить в уравнение $y^2 - 2y - 2 = 0$. В тех случаях, когда нас интересует лишь уравнение, которому данная цепная дробь удовлетворяет, так поступать иногда удобнее, потому что не приходится иметь дело с преобразованиями иррациональностей.

Упражнение

234. Составить уравнение, один из корней которого разлагается в периодическую цепную дробь α , и найти соответствующую иррациональность:

- 1) $\alpha = ((3, 2));$ 2) $\alpha = ((1, 7));$
3) $\alpha = ((2, 6, 1));$ 4) $\alpha = ((5, 4, 3));$ 5) $\alpha = (3, (2, 1));$
6) $\alpha = (4, (3, 2));$ 7) $\alpha = (1, 2, (3, 4)).$

§ 4. Решение уравнения Пелля

Теорема Лагранжа и достаточный признак подходящей дроби (см. п. 5Б § 2, настоящей гл.) дают возможность решить уравнение Пелля

$$x^2 - ay^2 = 1, \tag{1}$$

где целое $a > 0$ и \sqrt{a} — число иррациональное. (Случай, когда $a = a_1^2$ или $a < 0$, решаются очень просто, и мы на этом не останавливаемся.)

Уравнение (1) имеет решение $x_0 = 1, y_0 = 0$, которое называется тривиальным. Из остальных решений важно найти лишь положительные, т. е. те, для которых $x > 0$ и $y > 0$.

Для таких пар чисел x, y из уравнения (1) получаем

$$\frac{x^2}{y^2} - a = \frac{1}{y^2},$$

$$\frac{x}{y} - \sqrt{a} = \frac{1}{y^2 \left(\frac{x}{y} + \sqrt{a} \right)}.$$

Отсюда видно, что $\frac{x}{y} > \sqrt{a}$; следовательно,

$$\frac{x}{y} + \sqrt{a} > 2\sqrt{a} > 2 \text{ и } 0 < \frac{x}{y} - \sqrt{a} < \frac{1}{2y^2}.$$

Таким образом, $\frac{x}{y}$ удовлетворяет достаточному условию подходящей дроби \sqrt{a} (причем, очевидно, четного порядка, так как $\frac{x}{y} > \sqrt{a}$), вследствие чего все возможные положительные решения x, y следует искать среди числителей и соответствующих знаменателей подходящих дробей $\frac{P_k}{Q_k}$ четного порядка разложения

$$\sqrt{a} = (q_1, q_2, \dots, q_k, q_{k+1}, \dots).$$

Сделаем это.

Согласно формуле (5) п. 1, § 1, настоящей гл., имеем

$$\sqrt{a} = \frac{\alpha_{k+1}P_k + P_{k-1}}{\alpha_{k+1}Q_k + Q_{k-1}}, \quad (2)$$

где через $\alpha_{k+1} = (q_{k+1}, \dots)$ обозначен остаток разложения \sqrt{a} порядка $k+1$.

Отсюда при k четном получаем

$$\alpha_{k+1}(P_k - Q_k \sqrt{a}) = Q_{k-1} \sqrt{a} - P_{k-1},$$

откуда

$$\alpha_{k+1} (P_k^2 - aQ_k^2) = (P_k + \sqrt{a}Q_k) (Q_{k-1}\sqrt{a} - P_{k-1}) = \\ = (P_k Q_{k-1} - Q_k P_{k-1}) \sqrt{a} + Q_k Q_{k-1} a - P_k P_{k-1},$$

или

$$\alpha_{k+1} (P_k^2 - aQ_k^2) = \sqrt{a} + b,$$

если обозначим $Q_k Q_{k-1} a - P_k P_{k-1} = b$ и вспомним, что $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^k = 1$ при четном k .

Полученное соотношение показывает: если $x = P_k$, $y = Q_k$ является решением, так что $P_k^2 - aQ_k^2 = 1$, то должно быть

$$\alpha_{k+1} = \sqrt{a} + b; \quad (3)$$

наоборот, из выполнения последнего соотношения следует, что $P_k^2 - aQ_k^2 = 1$, а отсюда вытекает, что $x = P_k$, $y = Q_k$ является решением.

Итак, $x = P_k$, $y = Q_k$ является решением тогда и только тогда, когда при четном k выполняется (3).

Так как согласно (2)

$$\sqrt{a} = (q_1, q_2, \dots, q_k, \alpha_{k+1}),$$

то условие (3) переходит в условие

$$\alpha_{k+1} = b + \sqrt{a} = (b + q_1, q_2, \dots, q_k, \alpha_{k+1}) = \\ = (q_{k+1}, q_2, \dots, q_k, \alpha_{k+1}),$$

или

$$\alpha_{k+1} = ((q_{k+1}, q_2, \dots, q_k)), \quad (4)$$

так что

$$\sqrt{a} = (q_1, q_2, \dots, q_k, q_{k+1}, q_2, \dots, q_k, q_{k+1}, \dots),$$

или

$$\sqrt{a} = (q_1, (q_2, \dots, q_{k+1})). \quad (5)$$

Итак, пары чисел (P_k, Q_k) будут нам давать решения в том и только в том случае, если (согласно (5)) \sqrt{a} раскладывается в периодическую непрерывную дробь, период которой начинается со второго звена, и если мы в таком разложении возьмем такие *четные* подходящие дроби, чтобы (согласно (4)) остаток начинался с последнего члена периода.

Так как период разложения квадратного корня из целого числа на самом деле начинается со второго звена, то можно вышеуказанным способом получить все целые положительные решения уравнения (1): если

при этом число чисел в периоде равно k и k четное, то решениями уравнения (1) являются пары чисел (P_k, Q_k) , (P_{2k}, Q_{2k}) и т. д., а при нечетном k — пары чисел (P_{2k}, Q_{2k}) , (P_{4k}, Q_{4k}) и т. д.

Наименьшее положительное решение в первом случае равно (P_k, Q_k) , а во втором — (P_{2k}, Q_{2k}) .

Примеры. 1. Решить уравнение $x^2 - 11y^2 = 1$.

Как нам уже известно, $\sqrt{11} = (3, (3,6))$.

Поэтому имеем наименьшее положительное решение

$$x = P_2 = 10 \text{ и } y = Q_2 = 3.$$

2. Решить уравнения $x^2 - 41y^2 = 1$. Здесь (вычисления опускаем) $\sqrt{41} = (6, (2, 2, 12))$, так что количество чисел в периоде — нечетное. Поэтому для определения наименьшего положительного решения надо взять $\frac{P_6}{Q_6} = (6, 2, 2, 12, 2, 2) = \frac{2049}{320}$, наименьшее положительное решение будет $x = P_6 = 2049$, $y = Q_6 = 320$.

Заметим в заключение, что, зная наименьшее нетривиальное решение уравнения (1), можно всю совокупность решений (x_n, y_n) этого уравнения получить из формулы

$$x_n + y_n \sqrt{a} = (x_1 + y_1 \sqrt{a})^n,$$

где $n = 0, 1, 2, \dots$ (см., например, (42)).

Упражнение

235. Найти наименьшее положительное решение уравнений:

1) $x^2 - 26y^2 = 1$; 2) $x^2 - 37y^2 = 1$; 3) $x^2 - 19y^2 = 1$; 4) $x^2 - 29y^2 = 1$.

§ 5. Представление действительных чисел цепными дробями общего вида

А. Рассмотренные до сих пор правильные бесконечные (конечные) цепные дроби являются частным случаем бесконечных (конечных) цепных дробей общего вида

$$b_1 + \frac{a_1}{b_2 + \frac{a_2}{b_3 + \frac{a_3}{\ddots}}} \quad , \quad (1)$$

когда в них принимается, что все $a_k = 1$, b_1 — целое число, а все остальные b_k — натуральные числа.

В общем случае элементы цепной дроби a_k и b_k , $k > 1$ могут принимать произвольные, отличные от нуля рациональные значения, а b_1 может также быть равно нулю¹.

При помощи цепных дробей общего вида одно и то же рациональное число можно представить различными способами. Так, например, легко проверить, что

$$\frac{95}{42} = 2 + \frac{3}{10 + \frac{4}{2 + \frac{3}{4}}} = 3 - \frac{5}{7 - \frac{2}{8 + \frac{2}{3 - \frac{2}{3}}}} = 5/2 - \frac{2/3}{2/5 + \frac{3}{5/4}}.$$

В цепной дроби (1), которую записывают также иначе, например,

$$b_1 + \frac{a_2}{b_2 + \frac{a_3}{b_3 + \dots + \frac{a_n}{b_n} + \dots}} \quad (1')$$

или

$$\left(b_1; \frac{a_2}{b_2}, \frac{a_3}{b_3}, \dots \right), \quad (1'')$$

числа b_1 и $\frac{a_k}{b_k}$ ($k = 2, 3, \dots$) называют звеньями, a_k и b_k — членами k -го звена, из них a_k — частным числителем, а b_k — частным знаменателем.

Чтобы получить разложение рационального числа $\frac{a}{b}$ в конечную цепную дробь (1), можно все a_k и b_k за исключением одного, выбрать произвольно. Можно, например, найти разложение

$$\frac{95}{42} = 1 + \frac{2}{3 + \frac{4}{5 + \frac{6}{x}}};$$

для этого (что легко проверить) следует положить $x = 450/587$.

¹ Рассматриваются даже цепные дроби, где a_k и b_k — любые действительные или комплексные числа, или функции одной или нескольких переменных.

Можно цепную дробь преобразовать так, чтобы все частные числители a_k были равны 1, т. е., чтобы (1) приняло вид

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_n + \dots}}} \quad (2)$$

Так, например,

$$\frac{95}{42} = 2 + \frac{3}{10 + \frac{4}{2 + \frac{3}{4}}} = 2 + \frac{1}{10/3 + \frac{1}{3/2 + \frac{1}{16/9}}}.$$

Дроби вида (2) называют обыкновенными цепными дробями, а q_1, q_2, \dots, q_n — их неполными частными. Правильные цепные дроби можно поэтому определить как обыкновенные цепные дроби с целыми положительными неполными частными, начиная с q_2 , причем q_1 может быть любым целым числом.

Правильные цепные дроби являются наиболее простыми и наиболее изученными среди цепных дробей общего вида, однако и другие цепные дроби играют большую роль и имеют важные применения, например, в приближенном анализе, где при их помощи без сложных выкладок получают дробно-рациональные приближения функций.

Б. Рассмотрим обзорно некоторые свойства цепных дробей общего вида.

Происхождение таких цепных дробей связано с обобщенным алгоритмом Евклида.

Если мы имеем систему равенств

$$a = b_1 b + a_2 c, \quad b = b_2 c + a_3 d, \quad c = b_3 d + a_4 e, \dots$$

с произвольными рациональными числами, то при b, c, d , отличных от нуля, из них следуют равенства

$$\frac{a}{b} = b_1 + \frac{a_2}{b/c}, \quad \frac{b}{c} = b_2 + \frac{a_3}{c/d}, \quad \frac{c}{d} = b_3 + \frac{a_4}{d/e}, \dots,$$

так что, подставляя по цепочке, получаем

$$\frac{a}{b} = b_1 + \frac{a_2}{b_2 + \frac{a_3}{b_3 + \dots}}.$$

Нетрудно доказать, что k -я подходящая дробь

$\delta_k = \left(b_1; \frac{a_2}{b_2}, \dots, \frac{a_k}{b_k} \right)$ определяется для $k \geq 2$ по формуле

$$\delta_k = \frac{P_k}{Q_k} = \frac{b_k P_{k-1} + a_k P_{k-2}}{b_k Q_{k-1} + a_k Q_{k-2}}$$

при условии, что $P_0 = 1$, $Q_0 = 0$, $P_1 = b_1$, $Q_1 = 1$.

Пользуясь ею, найдем, например, подходящие дроби для разложения

$$\frac{95}{42} = 3 - \frac{5}{7} - \frac{2}{8} + \frac{2}{3} - \frac{2}{3}.$$

Имеем

$$\delta_k = \frac{1}{0}, \frac{3}{1}, \frac{16}{7}, \frac{122}{54}, \frac{398}{176}, \frac{950}{420}.$$

Заметим, что получаемые в процессе рекуррентного вычисления подходящие дроби могут быть сократимыми, но сокращать их можно лишь при определенных условиях.

Свойства подходящих дробей цепных дробей общего вида с положительными элементами и правильных цепных дробей вполне аналогичны.

Бесконечная цепная дробь (1) называется *сходящейся*, если существует конечный предел $\alpha = \lim_{k \rightarrow \infty} \frac{P_k}{Q_k}$; в таком случае α принимается за значение этой дроби. Не всегда общие бесконечные цепные дроби являются сходящимися, даже тогда, когда они имеют лишь положительные элементы.

Интересной особенностью цепных дробей общего вида является то, что даже рациональные числа могут ими разлагаться в бесконечные цепные дроби. Так, например, имеется разложение

$$\frac{1}{2} = \frac{1}{3} - \frac{3}{5} - \frac{8}{7} - \frac{15}{9} - \dots - \frac{n^2 - 1}{2n + 1} - \dots$$

$$\delta_k = \frac{1}{0}, \frac{0}{1}, \frac{1}{3}, \frac{5}{12}, \frac{27}{60}, \frac{168}{360}, \dots$$

$$0,3; 0,42; 0,45; 0,467; \dots$$

Примечательно далее то, что квадратические иррациональности разлагаются и в непериодические цепные дроби общего вида. Так, например, имеется разложение

$$\sqrt{2} = \frac{1}{1} - \frac{1}{3} + \frac{2}{3} + \frac{12}{3} + \frac{30}{3} + \dots + \frac{2n(2n-1)}{3} + \dots$$

$$\delta_1 = \frac{1}{0}, \frac{0}{1}, \frac{1}{1}, \frac{3}{2}, \frac{11}{8}, \frac{49}{8}, \frac{537}{384}, \dots$$

$$1; 1,5; 1,38; 1,44; 1,40; \dots$$

Но самое интересное и важное это то, что в то время как до настоящего времени неизвестно разложение в правильную цепную дробь ни одной алгебраической иррациональности степени выше второй (другими словами, неизвестны общие свойства неполных частных таких разложений, разложения сами по себе со сколь угодно точностью можно практически найти — см., например, стр. 177), при помощи общих цепных дробей такие разложения находятся довольно легко. Отметим, например, некоторые разложения и соответствующие подходящие дроби для $\sqrt[3]{2}$;

$$\sqrt[3]{2} = \frac{1}{1} - \frac{1}{4} + \frac{6}{4} + \frac{30}{4} + \dots + \frac{3n(3n-1)}{4} + \dots$$

$$\delta_k = \frac{1}{0}, \frac{0}{1}, \frac{1}{1}, \frac{4}{3}, \frac{22}{18}; \frac{208}{162}, \dots$$

$$1,33; 1,22; 1,284; \dots$$

$$\sqrt[3]{2} = 1 + \frac{1}{6} - \frac{4}{2} - \frac{2}{18} - \frac{7}{2} - \dots - \frac{3n+1}{2} - \frac{3n-1}{6(2n+1)} - \dots$$

$$\delta_k = \frac{0}{1}, \frac{1}{1}, \frac{7}{6}, \frac{10}{8}, \frac{166}{132}, \frac{262}{208}, \dots$$

$$1,17; 1,25; 1,258; 1,2596; \dots$$

В заключение приведем еще несколько примеров разложений других иррациональностей в цепные дроби

общего вида:

$$\frac{\pi}{4} = \frac{1}{1} + \frac{1}{2} + \frac{3^2}{2} + \frac{5^2}{2} + \dots + \frac{(2n-1)^2}{2} + \dots,$$

$$\delta_k = \frac{1}{0}, \frac{0}{1}, \frac{1}{1}, \frac{2}{3}, \frac{13}{15}, \frac{76}{105}, \dots$$

$$e = \frac{1}{1} - \frac{1}{1} + \frac{1}{2} - \frac{1}{3} + \frac{1}{2} - \frac{1}{5} + \dots + \frac{1}{2} - \frac{1}{2n+1} + \dots,$$

$$\delta_k = \frac{1}{0}, \frac{0}{1}, \frac{1}{1}, \frac{1}{0}, \frac{1}{1}, \frac{2}{3}, \frac{3}{5}, \frac{13}{22}, \dots$$

Более подробно о цепных дробях общего вида см. (17).

Глава VII

АЛГЕБРАИЧЕСКИЕ И ТРАНСЦЕНДЕНТНЫЕ ЧИСЛА

§ 1. Иррациональные числа

В предыдущих главах мы встречались как с рациональными, так и с иррациональными числами. В этой главе остановимся сначала на том, как можно в некоторых простейших случаях судить о том, является ли данное число рациональным или иррациональным, как доказывается иррациональность чисел e и π .

В дальнейшем ознакомимся с различными видами иррациональных чисел.

1. Некоторые признаки иррациональности

1. Понятия рациональности и иррациональности весьма существенно характеризуют строение числа.

Так, например, рациональные числа и только они представимы в виде периодических десятичных дробей (конечные десятичные дроби рассматриваются при этом как периодические десятичные дроби с периодом 0) и в виде правильных конечных цепных дробей, иррациональные числа и только они представимы в виде бесконечных непериодических десятичных дробей и в виде правильных бесконечных цепных дробей.

Указанные факты могут, очевидно, служить критериями рациональных и иррациональных чисел, но не всегда имеется возможность непосредственно их применить.

2. Еще в школе Пифагора была доказана иррациональность числа $\sqrt{2}$, что равносильно утверждению: уравнение $x^2 = 2y^2$ неразрешимо в целых числах. Для выяснения этого факта можно воспользоваться рассуж-

дением, которое применимо для доказательства более общей теоремы: *если N и k — натуральные числа, причем N не является k -ой степенью целого числа, то $\sqrt[k]{N}$ — число иррациональное.*

Допустим, что $\sqrt[k]{N} = \frac{a}{b}$ — число рациональное, (a, b) = 1 и $b > 1$ (иначе N было бы k -й степенью целого числа). Тогда

$$a^k = b^k N,$$

откуда следует, что $a^k | b$ и $a^k | p$, где p простой делитель числа b . В таком случае a также должно делиться на p , и получается противоречие с условием $(a, b) = 1$.

Итак, $\sqrt[k]{N}$ не может при данном условии быть рациональным числом, следовательно, оно иррационально. Теорема доказана.

Доказанная теорема является частным случаем более общей теоремы: *если α — действительный корень уравнения*

$$x^n + c_1 x^{n-1} + \dots + c_n = 0 \quad (1)$$

с целыми коэффициентами, то α — либо целое, либо иррациональное число.

В доказательстве ограничимся случаем, когда $c_n \neq 0$. Если допустим, что α не является иррациональным числом, а рациональной дробью, т. е. $\alpha = \frac{a}{b}$, $(a, b) = 1$ и $b > 1$, то

$$a^n + c_1 a^{n-1} b + \dots + c_n b^n = 0,$$

или

$$a^n = -(c_1 a^{n-1} b + \dots + c_n b^n);$$

поэтому $a^n | b$, откуда, как и в предыдущей теореме, получается противоречие, из которого и вытекает справедливость данной теоремы.

На основании последней можно утверждать, что число α , неявно определенное уравнением (1) и не являющееся целым, иррационально, причем, как известно из алгебры, целые решения (1) следует искать среди делителей c_n .

3. Для некоторых действительных чисел вопрос об их иррациональности выясняется при помощи следующих двух теорем.

Теорема 1. Для всякого рационального числа α существует такое положительное постоянное число c , что неравенство

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q} \quad (2)$$

выполняется для любой рациональной дроби $\frac{p}{q} \neq \alpha$.

Доказательство. Пусть $\alpha = \frac{a}{b} \neq \frac{p}{q}$ (так что $aq - bp \neq 0$) и $b \geq 1$. Тогда

$$\left| \alpha - \frac{p}{q} \right| = \left| \frac{a}{b} - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq} = \frac{1/b}{q}.$$

Принимая поэтому $\frac{1}{b} = c$, получаем

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q},$$

что и утверждалось.

В этой теореме содержится необходимый признак рационального числа. Число, которое этому признаку не удовлетворяет, не может быть рациональным и должно быть иррациональным. Таким образом, приходим к теореме 2.

Теорема 2. Если для любого положительного c можно найти хотя бы одну пару целых чисел p и q , таких, что

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q}, \quad (3)$$

то α иррационально.

Действительно, если α было бы рациональным, то существовало бы такое c , что для указанной дроби $\frac{p}{q}$ выполнялось бы (2), и тогда для этого c не могло бы выполняться (3). Итак, α иррационально и теорема доказана.

2. Иррациональность чисел e и π

1. Полученный в конце предыдущего пункта признак иррациональности можно, например, применить для доказательства иррациональности числа e . Но еще проще воспользоваться следующим рассуждением.

Допустим, что e — рациональное число, т. е. $e = \frac{a}{b}$, где a и b целые, и рассмотрим при $k \geq b$ выражение

$$c = k! \left(e - 1 - \frac{1}{1!} - \frac{1}{2!} - \dots - \frac{1}{k!} \right).$$

Поскольку при $k \geq b$ произведение $k!$ делится на b , ясно, что c должно быть целым числом (так как $k!e$ целое, а остальные слагаемые в скобке при умножении на $k!$ также дают целые числа).

Но с другой стороны,

$$0 < c = \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \dots < \frac{1}{k+1} + \frac{1}{(k+1)^2} + \dots = \frac{1}{k},$$

т. е. c — дробное число. Полученное противоречие свидетельствует о справедливости утверждения об иррациональности числа e .

2. Доказать иррациональность π куда сложнее. Впервые это удалось в 1761 г. Ламберту при помощи цепных дробей общего вида. Доказательство Ламберта, уточненное Лежандром, сводится к следующему. Находят разложение $\operatorname{tg} x$ в цепную дробь

$$\operatorname{tg} x = \frac{x}{1 - \frac{x^2}{3 - \frac{x^2}{5 - \frac{x^2}{7 - \dots}}}};$$

далее, с одной стороны, $\operatorname{tg} \frac{\pi}{4} = 1$, а с другой стороны, из предположения рациональности $\frac{\pi}{4}$ следует иррациональность правой части в указанном равенстве¹.

Мы рассмотрим доказательство иррациональности π , данное американским математиком И. Нивеном в 1947 г.

Допустим, что π рационально, а именно, что $\pi = \frac{a}{b}$, где a и b — целые, и рассмотрим функции

$$f(x) = \frac{x^n (a - bx)^n}{n!} \quad (1)$$

¹ Доказательства Ламберта и Лежандра можно найти в книге акад. С. Н. Бернштейна. «О квадратуре круга», с приложением истории вопроса, составленной Ф. Рудио (изд. 3, М.—Л., 1936).

и

$$F(x) = f(x) - f^{(n)}(x) + f^{(IV)}(x) - \dots + (-1)^n f^{(2n)}(x). \quad (2)$$

Так как x входит в числитель $f(x)$ с показателями от n до $2n$, то можно $f(x)$ записать в следующем виде:

$$f(x) = \frac{1}{n!} \sum_{i=n}^{2n} a_{i-n} \cdot x^i,$$

откуда видно, что

$$f(0) = f'(0) = \dots = f^{(n-1)}(0) = 0$$

и что в производной $f^{(k)}(x)$, $n \leq k \leq 2n$ при $x=0$ сохранится лишь слагаемое, порожденное членом $f(x)$ с x^k , так что

$$f^{(k)}(0) = \frac{k!}{n!} a_{k-n}.$$

Итак, для $0 \leq j \leq 2n$ $f^{(j)}(0)$ — целое число. Но так как согласно (1) $f(x) = f(\pi - x)$, то при любом j $f^{(j)}(x) = f^{(j)}(\pi - x)$ и $f^{(j)}(\pi) = f^{(j)}(0)$ — также целое число. Поэтому и $F(0)$ и $F(\pi)$ — целые числа.

Учитывая теперь, что из

$$\begin{aligned} \frac{d}{dx} (F'(x) \sin x - F(x) \cos x) &= F''(x) \sin x + F(x) \sin x = \\ &= f(x) \sin x \end{aligned}$$

следует

$$\begin{aligned} I &= \int_0^{\pi} f(x) \sin x \, dx = [F'(x) \sin x - F(x) \cos x]_0^{\pi} = \\ &= F(\pi) + F(0), \end{aligned}$$

приходим к выводу, что I — число целое, притом положительное, так как в интервале $(0, \pi)$ подынтегральная функция положительна.

Но это противоречит тому, что (как это видно из (1) для $0 < x < \pi$ $f(x) \sin x < \frac{\pi^n a^n}{n!}$ и вследствие этого для достаточно больших n подынтегральная функция, а вместе с тем и сам интеграл I могут стать произвольно малыми. Обнаруженное противоречие показывает, что π не может быть рациональным числом, поэтому π — иррациональное число.

§ 2. Поле алгебраических чисел

1. Понятие алгебраического числа степени n

Алгебраическим числом называется корень какого-либо алгебраического уравнения

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad (1)$$

коэффициенты которого a_0, a_1, \dots, a_n суть целые рациональные числа, не все равные нулю.

Если предположить, что коэффициенты в (1) — числа рациональные, то от этого класс определяемых чисел не изменится, так как и в таком случае можно (1) преобразовать в уравнение с целыми коэффициентами.

Если число α удовлетворяет алгебраическому уравнению с целыми коэффициентами степени n , но не удовлетворяет такому же уравнению степени $< n$, то α называют алгебраическим числом степени n .

Из этого определения вытекает, что уравнение (1) степени n , корнем которого является алгебраическое число α степени n , является неприводимым в поле рациональных чисел, т. е. что многочлен $f(x)$ нельзя разложить в произведение двух многочленов с рациональными коэффициентами степени не ниже первой.

В самом деле, если бы это было возможно, то мы имели бы

$$f(x) = f_1(x) \cdot f_2(x) = 0,$$

и тогда оказалось бы, что α удовлетворяет по крайней мере одному из уравнений

$$f_1(x) = 0, \quad f_2(x) = 0$$

степени $< n$ с рациональными коэффициентами и не может поэтому быть алгебраическим числом степени n .

К алгебраическим числам, очевидно, относятся все рациональные числа $\frac{a}{b}$, так как последние удовлетворяют уравнению $bx - a = 0$. (При этом ясно, что они будут алгебраическими числами степени 1, так как уравнению с меньшей степенью они удовлетворять не могут.) Алгебраическими числами будут также числа вида a^m , где a — целое, а m — любое рациональ-

ное число, например число $\sqrt[3]{5}$, которое удовлетворяет уравнению $x^3 - 5 = 0$.

Неприводимый целочисленный многочлен $f(x)$, корнем которого является α , определен с точностью до постоянного множителя.

Действительно, если α было бы корнем двух неприводимых многочленов $f(x)$ и $\varphi(x)$, отличающихся не только постоянным множителем, то Н. О. Д. этих многочленов был бы отличен от многочлена нулевой степени (так как он должен делиться на $x - \alpha$), а это невозможно, в силу неприводимости $f(x)$ и $\varphi(x)$.

Алгебраические числа, являющиеся корнями одного и того же неприводимого (над полем рациональных чисел) многочлена, называются *сопряженными*.

2. Поле всех алгебраических чисел

Покажем, что алгебраические числа образуют поле, т. е. что сумма, разность, произведение и частное алгебраических чисел тоже является алгебраическим числом.

Действительно, пусть даны алгебраические числа $\alpha = \alpha_1$ степени n и $\beta = \beta_1$ степени m . Сопряженные с ними числа обозначим соответственно через $\alpha_2, \alpha_3, \dots, \alpha_n$ и $\beta_2, \beta_3, \dots, \beta_m$.

Согласно теореме Виета понятно, что элементарные симметричные функции σ_i от $(\alpha_1, \alpha_2, \dots, \alpha_n)^1$ и τ_j от $(\beta_1, \beta_2, \dots, \beta_m)$ являются рациональными числами.

Составим теперь элементарные симметрические функции от $m \cdot n$ чисел

$$\alpha_i + \beta_j, \text{ где } i = 1, 2, \dots, n, j = 1, 2, \dots, m.$$

Легко понять, что они не меняются при перестановках всех α_i между собою, а также всех β_j между собою. Таким образом, они являются симметричными по двум системам неизвестных, а поэтому (согласно теореме о многочленах, симметричных по двум системам неизвестных)² они представимы в виде многочле-

¹ $\sigma_1 = \alpha_1 + \alpha_2 + \dots + \alpha_n$, $\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n$, ..., $\sigma_n = \alpha_1\alpha_2\dots\alpha_n$.

² См., например, А. Г. Курош. Курс высшей алгебры, М.—Л., 1949, § 37.

нов от элементарных симметрических функций σ_i и τ_j . Значит, они являются рациональными числами. Но тогда все эти числа, и среди них число $\alpha + \beta$, будут корнями уравнения m -й степени с рациональными коэффициентами, т. е. алгебраическими.

Аналогичным образом можно показать, что и числа $\alpha - \beta$, $\alpha \cdot \beta$ и $\frac{\alpha}{\beta}$ — алгебраические (для последнего случая надо учесть, что если β — алгебраическое число $\neq 0$, то и β^{-1} — число алгебраическое). Таким образом, алгебраические числа образуют поле.

Из доказанного следует, что сумма (а также разность, произведение и частное) рационального числа и радикала, например $3 + \sqrt{2}$, или любых двух радикалов, например $\sqrt{2} + \sqrt[3]{5}$, являются алгебраическими числами, так как каждое из слагаемых является алгебраическим числом. То что и радикалы из радикалов являются алгебраическими числами, вытекает из следующей теоремы (доказательство которой опускаем): если α корень уравнения

$$\beta_0 x^n + \beta_1 x^{n-1} + \dots + \beta_n = 0,$$

где все β_i — алгебраические числа, то α — число алгебраическое. (Иными словами, поле алгебраических чисел алгебраически замкнуто.)

Действительно, если, например, $\alpha = \sqrt[3]{3 + \sqrt{2}}$, то α является корнем уравнения $x^3 - \beta = 0$ (где $\beta = 3 + \sqrt{2}$ — число алгебраическое), т. е. алгебраического уравнения с алгебраическими коэффициентами, поэтому, согласно вышеуказанной теореме, α — алгебраическое число. Очевидно, вообще любое число, выраженное через комбинацию радикалов над полем рациональных чисел, является алгебраическим числом. Однако такими числами нельзя еще исчерпать все множество алгебраических чисел, так как известно, что корни уравнений степени выше 4-й, а значит, и алгебраические числа степени выше 4-й, не всегда выражаются через радикалы (т. е. явно в виде алгебраических выражений, составленных из коэффициентов уравнения при помощи алгебраических действий сложения,

вычитания, умножения, деления, возведения в целую степень и извлечения корня целой степени).

3. Целые алгебраические числа

А. Среди алгебраических чисел особенно важны те, которые являются решениями уравнения вида

$$f(x) = x^n + b_1 x^{n-1} + \dots + b_n = 0 \quad (1)$$

с целыми коэффициентами b_1, b_2, \dots, b_n . Такие числа называются целыми алгебраическими числами.

Из предыдущего легко понять, что они образуют кольцо, т. е. сумма, разность и произведение двух целых алгебраических чисел α и β снова будут алгебраическими числами.¹ Но не всегда частное $\frac{\alpha}{\beta}$ является целым алгебраическим числом. В связи с этим возникает вопрос о делимости целых алгебраических чисел.

Как известно из арифметики обычных целых чисел, вопрос делимости тесно связан с вопросом об однозначном разложении целого числа на простые множители. Поэтому и для целых алгебраических чисел возникает вопрос об их однозначном разложении на «простые» множители. Если бы это оказалось возможным, то теория делимости и вместе с тем вся арифметика в кольце целых алгебраических чисел была бы аналогична обычной арифметике.

Б. Если говорить о всех целых алгебраических числах, то здесь на первых порах понятие неразложимости теряет смысл, так как, например, $\alpha = \sqrt{\alpha} \sqrt{\alpha} = \sqrt[3]{\alpha} \sqrt[3]{\alpha} \sqrt[3]{\alpha}$ и так далее, причем $\sqrt{\alpha}$ и $\sqrt[3]{\alpha}$ также являются целыми алгебраическими числами. Не так плохо обстоит дело, если рассматривать целые алгебраические числа так называемого простого расширения поля рациональных чисел с помощью присоединения целого алгебраического числа α степени n , т. е. все числа вида

$$A = c_0 + c_1 \alpha + \dots + c_{n-1} \alpha^{n-1}, \quad (2)$$

¹ Заметим еще, что если коэффициенты в (1) — целые алгебраические числа, то и корни этого уравнения также являются целыми алгебраическими числами.

где c_0, c_1, \dots, c_{n-1} — целые числа, а α — решение уравнения вида (1). Совокупность этих чисел, которую будем обозначать через $P(\alpha)$, образует кольцо.

В. Впервые такие числа рассматривал Гаусс, а именно — целые комплексные числа, т. е. числа вида $a + bi$, где $i = \sqrt{-1}$, а a и b — все возможные целые рациональные числа.

В этом так называемом гауссовом кольце, имеется бесконечно много «простых» чисел, и всякое число этого кольца может быть разложено в произведение конечного числа таких «простых» чисел (и еще одной из четырех так называемых единиц $\sqrt[4]{1} = 1, i, -1, -i$ кольца $a + bi$), причем однозначно (если не обращать внимание на порядок их следования и на множители «единицы»).

Г. Однако такое однозначное разложение на простые множители (т. е. на множители, которые уже не могут быть представлены в виде произведения сомножителей такого же вида) не всегда возможно. Так, например, в кольце $P(\sqrt{-5})$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

причем числа

$$2 = 2 + 0 \cdot \sqrt{-5}, \quad 3 = 3 + 0 \cdot \sqrt{-5}, \quad 1 + \sqrt{-5}, \quad 1 - \sqrt{-5}$$

являются в нем «простыми», так как оказывается, что они не разложимы на другие числа такого же вида.

С такими трудностями как раз впервые встретился Куммер, пытаясь доказать великую теорему Ферма.

Рассматривая целые числа поля деления круга (т. е. числа вида (2), где α корень неприводимого уравнения $\frac{x^n - 1}{x - 1} = 0$) для простых значений n , он обнаружил, что для некоторых n возможно однозначное разложение любого числа кольца, а для других n этого нет.

После многолетних усилий Куммеру удалось преодолеть возникшие трудности. Он ввел в поле алгебраических чисел новые элементы, так называемые идеальные числа. С их помощью ему удалось восстановить однозначность разложения на простые мно-

жители и решить проблему Ферма для целого класса значений n .

Д. Идея, которая лежит в основе введения идеальных множителей, аналогична той, с которой встречаемся в проективной геометрии, когда вводим несобственные элементы.

Поясним эту идею следующим примером. Предположим, что нам известно только множество D_2 четных чисел 2, 4, 6, 8, 10, 12 и так далее. В этом множестве числа 2, 6, 10, 14, 18 и другие будут неразложимы. Если будем их считать «простыми», то закон однозначного разложения на множители в D_2 нарушится, например

$$60 = 6 \cdot 10 = 2 \cdot 30.$$

Если же дополнить множество D_2 нечетными числами, которые играют здесь роль идеальных элементов, и определить «простые» числа в расширенной области, то однозначность разложения восстановится. Для числа 60 мы получим

$$60 = 2 \cdot 3 \cdot 2 \cdot 5,$$

причем $6 = 2 \cdot 3$, $10 = 2 \cdot 5$, $30 = 2 \cdot 3 \cdot 5$ (здесь 2 — «неидеальный» простой множитель, а 3 и 5 — «идеальные» простые множители).

Причину неоднозначности разложения числа множества D_2 на неразложимые числа этого множества можно объяснить тем, что различные группировки идеальных множителей в одном и том же произведении могут давать различные произведения неразложимых чисел множества D_2 .

Е. Теория Куммера получила широкое признание. Однако при попытке распространить метод Куммера на кольца алгебраических чисел, зависящих от корня α произвольного неприводимого уравнения

$$f(x) = x^n + b_1 x^{n-1} + \dots + b_n = 0,$$

где b_1, b_2, \dots, b_n — целые рациональные числа, возникли принципиально новые трудности.

Эту сложную задачу одновременно и независимо друг от друга решили в самой общей форме Дедекин и Е. М. Золотарев в 70-х годах прошлого столетия.

При этом решение, данное Золотаревым, оказалось во многих отношениях более глубоким, благодаря применению им новых методов.

4. Значение законов взаимности. Общий закон взаимности

В развитии алгебраической теории чисел крупных успехов добились советские ученые.

Особенно важным достижением является открытие и доказательство в 1949 г. И. Р. Шафаревичем общего закона взаимности.

Прежде чем характеризовать закон взаимности Шафаревича, остановимся на связи, которая существует между вопросами разложимости на простые множители (идеальные и неидеальные) и законами взаимности.

Во-первых, отметим, что при помощи квадратичного закона взаимности для нечетных простых чисел можно не только по данному a и простому p определить, является ли a по модулю p квадратичным вычетом или нет, но и решить более сложную обратную задачу, как найти те простые числа p , для которых заданное число a является квадратичным вычетом по модулю p .

Для случая, когда $a = -1$ и 2 , это непосредственно вытекает из свойств III и V символа Лежандра, а именно: -1 является квадратичным вычетом всех простых чисел вида $4n + 1$, а 2 — для простых чисел вида $8n \pm 1$.

В общем случае, когда a — любое целое число, не делящееся ни на какой квадрат, оказывается, что a является квадратичным вычетом тех и только тех простых чисел p , которые имеют одну из форм $4ak + r_1$, $4ak + r_2$, $4ak + r_3, \dots$ (т. е. $p \equiv r_1, r_2, r_3 \dots \pmod{4a}$), где r_1, r_2, r_3, \dots — вполне определенные числа, удовлетворяющие условиям

$$1 \leq r_i < 4a, (r_i, 4a) = 1.$$

(Условие, что a не делится на квадрат, принято потому, что если $a = b^2 \cdot a'$, то a и a' являются одновременно квадратичными вычетами и невычетами.)

Одновременно оказывается, что как раз те простые числа p , по которым a является квадратичным вычетом (т. е. числа указанных прогрессий), разлагаются в квадратичном поле $K = R(\sqrt{a})$ (т. е. в поле чисел,

получаемых путем присоединения к полю рациональных чисел иррационального числа \sqrt{a} на простые множители¹ (идеальные и неидеальные), а те, по которым a является квадратичным невычетом, — не разлагаются, т. е. являются простыми и в поле K .

Таким образом, квадратичный закон взаимности показывает, какова зависимость арифметики квадратичного поля от арифметики рационального поля. Как раз в этом фундаментальность закона взаимности.

Аналогичные вопросы возникают при переходах к более сложным полям. Несмотря на большие усилия таких виднейших ученых, как Гаусс, Эйзенштейн, Куммер, Гильберт и др., в течение 150 лет эти вопросы удалось решить только для разных частных случаев.

Общий закон взаимности Шафаревича решает указанную проблему в наиболее общем виде: он устанавливает зависимость арифметики поля K от арифметики поля k , где k — произвольное поле алгебраических чисел m -й степени, а K — его расширение, полученное присоединением к нему $\sqrt[n]{a}$ (где a — число поля k).

5. Проблема Ферма

А. Знаменитое утверждение Ферма (известно под названиями «Великая теорема Ферма», «Проблема Ферма») о том, что уравнение $x^n + y^n = z^n$, где $n > 2$, не имеет решений в целых положительных числах, до сих пор в общем случае не доказано и не опровергнуто.

¹ Заметим, что это равносильно представимости числа p формой $x^2 - ay^2$, т. е. разрешимости уравнения Пелля $x^2 - ay^2 = p$. Аналогично представимость простого p формой $x^2 + y^2 =$ $=(x + y\sqrt{-1})(x - y\sqrt{-1})$ решается арифметикой в гауссовом кольце целых комплексных чисел поля $R(\sqrt{-1})$. Так как число (-1) является квадратичным вычетом для всех p вида $4k + 1$ и квадратичным невычетом для всех p вида $4k + 3$, то первые и только они всегда представимы формой $x^2 + y^2$, причем единственным образом, ввиду того что в гауссовом кольце имеет место однозначность разложения на простые множители (с точностью до порядка следования сомножителей и множителей «единиц»).

Так с точки зрения арифметической теории алгебраических чисел знаменитые теоремы Ферма и Эйлера относительно простых чисел p вида $4k + 1$ получают совершенно прозрачное доказательство.

Если утверждение верно для n , то и для $k \cdot n$ (так как уравнению $x^{kn} + y^{kn} = z^{kn}$ можно придать вид $(x^k)^n + (y^k)^n = (z^k)^n$), поэтому теорему достаточно доказать для простых показателей $p \geq 3$ и для $n = 4$.

Эйлер доказал теорему Ферма для $n = 3$ и 4, Дирхле и Лежандр — для $n = 5$, Ламэ — для $n = 7$. Начиная с Куммера, для решения проблемы Ферма применяется алгебраическая теория чисел. Куммер доказал теорему Ферма для всех значений $n \leq 100$.

До 1956 года доказана справедливость теоремы Ферма для всех простых показателей $n < 4003$. (Для численной обработки критериев разрешимости уравнения $x^n + y^n = z^n$ в последние годы применяются электронные вычислительные машины.)

Для случая $n = 4$ теорема Ферма доказывается элементарно и приводится ниже.

Б. Прежде чем доказать неразрешимость проблемы Ферма для $n = 4$, целесообразно рассмотреть решение уравнения

$$x^2 + y^2 = z^2 \quad (1)$$

во взаимно простых натуральных числах x, y, z .

Мы принимаем условие $(x, y, z) = 1$ потому, что в случае $(x, y, z) = d > 1$ обе части (1) можно разделить на d^2 . Отметим еще, что в отношении к тройкам чисел, удовлетворяющим (1), условие взаимной простоты означает даже попарно взаимную простоту, ибо если бы, например,

$$(x, y) = d > 1, \text{ то } z | d \text{ и } (x, y, z) \neq 1.$$

Теорема: уравнению (1) удовлетворяют такие и только такие тройки взаимно простых натуральных чисел x, y, z , что

- 1) одно из чисел x и y четно, а другое нечетно;
- 2) при четном x и нечетном y

$$x = 2m \cdot n, \quad y = m^2 - n^2, \quad z = m^2 + n^2,$$

где $m > n > 0$, $(m, n) = 1$ и одно из чисел m и n четно, а другое нечетно.

Доказательство необходимости условий. Если (1) выполняется для натуральных чисел x, y, z и $(x, y, z) = 1$, то x и y не могут быть оба ни четными, ни нечетными. Первый случай отпадает в силу отмеченной попарной взаимной простоты чисел x, y, z ;

во втором случае мы имели бы $x^2 \equiv y^2 \equiv 1 \pmod{4}$, а $z^2 \equiv 2 \pmod{4}$, но это невозможно, так как квадрат при делении на 4 не может давать остатка 2.

Итак, одно из чисел x и y должно быть четным, а другое — нечетным.

Пусть x будет четным; тогда из (1) вследствие нечетности y и z следует

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2},$$

где $\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$, так как иначе $(y, z) \neq 1$ вопреки условию. Но если произведение двух взаимно простых чисел равно квадрату, то каждый из этих сомножителей в отдельности равен квадрату, поэтому существуют натуральные числа m, n , такие, что

$$\frac{x}{2} = m \cdot n, \quad \frac{z+y}{2} = m^2, \quad \frac{z-y}{2} = n^2, \quad (2)$$

так что

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2. \quad (3)$$

При этом $(m, n) = 1$, где одно из чисел m и n четное, а другое — нечетное, иначе y и z были бы оба четными и $(x, y, z) \neq 1$.

Доказательство достаточности условий.

Если натуральные числа x, y, z составлены по формулам (3), то при любых натуральных m и n выполняется (1), так как

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2.$$

Если $(m, n) = 1$ и при этом m и n имеют разную четность, то y и z — нечетные, а, кроме того, $(y, z) = 1$, иначе из $(y, z) = d > 1$ следовало бы

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = d > 1,$$

или $(m^2, n^2) = d > 1$, а это несовместимо с $(m, n) = 1$.

Итак, $(y, z) = 1$, а вместе с тем $(x, y, z) = 1$.

Так как x — число четное и нами установлено также, что y — нечетное, то достаточность условий доказана. Вместе с тем доказана вся теорема.

Пример. Для $m = 7, n = 4$ получаем: $x = 56, y = 33, z = 65$.

В. Докажем теперь теорему: *уравнение*

$$x^4 + y^4 = z^4 \quad (4)$$

не имеет решений в натуральных числах. Для доказательства покажем, что даже

$$x^4 + y^4 = z^2 \quad (5)$$

не имеет решений в натуральных числах.

Доказательство. Так же, как в теореме п. Б, достаточно доказать утверждение при условии $(x, y, z) = 1$, которое, как и в п. Б, означает даже попарно взаимную простоту чисел x, y, z .

Допустим, что существуют тройки взаимно простых натуральных чисел x, y, z , удовлетворяющие уравнению (5), и выберем из них тройку с наименьшим значением z^1 . Как и в доказательстве теоремы п. Б, можно убедиться в том, что одно из чисел x и y четно, другое нечетно.

Пусть x — четное (а y , следовательно, нечетное), тогда согласно формулам (3)

$$x^2 = 2mn, \quad y^2 = m^2 - n^2, \quad z = m^2 + n^2,$$

где $m > n \geq 1$, $(m, n) = 1$ и одно из чисел m и n четно, а другое нечетно.

Не может быть, чтобы m было четным, а n — нечетным, ибо тогда $m^2 \equiv 0 \pmod{4}$, $n^2 \equiv 1 \pmod{4}$ и $y^2 = m^2 - n^2 \equiv -1 \equiv 3 \pmod{4}$, что невозможно, так как квадрат нечетного числа имеет вид $4k + 1$. Поэтому m должно быть нечетным, а n четным, т. е. $n = 2n'$.

Тогда $x^2 = 4m \cdot n'$, $\left(\frac{x}{2}\right)^2 = m \cdot n'$ с условием $(m, n') = 1$,

отсюда, как и в п. Б, заключаем, что

$$m = z_1^2, \quad n' = n_1^2,$$

где $(z_1, n_1) = 1$, а z_1 — нечетное (ввиду нечетности m). Из $y^2 = m^2 - n^2$ получаем теперь

$$(2n_1^2)^2 + y^2 = z_1^4,$$

где $(2n_1^2, y) = 1$, ибо в противном случае мы имели бы

$$(2n_1^2, z_1^2) = (2n', m) = d > 1,$$

¹ См. по этому поводу подстрочное замечание на стр. 125.

что невозможно, так как

$$(2, m) = 1 \text{ и } (n', m) = 1.$$

Согласно формулам (3) снова имеем

$$2n_1^2 = 2u \cdot v, \quad z_1^2 = u^2 + v^2, \text{ где } (u, v) = 1.$$

Первое из этих равенств приводит нас, как и выше, к выводу, что

$$u = x_1^2, \quad v = y_1^2,$$

вследствие чего по второму из указанных равенств

$$x_1^4 + y_1^4 = z_1^2, \quad (5)$$

где $z_1 < z$ (так как $z > m^2 > m = z_1^2 > z_1$).

Итак, предположение о существовании наименьшего значения z привело нас к противоречию, значит уравнение (5) не имеет решений в натуральных числах. Теорема доказана.

Упражнения

236. Указать решения уравнения $x^2 + y^2 = z^2$ (по формулам (3) на стр. 219) при 1) $m = 5, n = 4$; 2) $m = 6, n = 5$; 3) $m = 9, n = 8$; 4) $m = 12, n = 7$; 5) $m = 12, n = 5$.

237. Пользуясь результатами задачи 233, указать разложения (с точностью до множителей единиц) в квадратичном поле $R(i)$ для: 1) 97, 2) 137, 3) 181, 4) 281, 5) 317.

238. Доказать, что при пересечении окружности $x^2 + y^2 = 1$ (1) с прямыми $y = kx - 1$ (2), где k рационально, получаются все рациональные точки окружности. Сделать чертеж.

239. Найти решения уравнения $x^2 + y^2 = z^2$ в натуральных и взаимнопростых числах, пользуясь предыдущей задачей.

240. Великая теорема Ферма эквивалентна утверждению: уравнение $X^n + Y^n = 1$ не имеет решений в положительных рациональных числах, если $n > 2$. Дать геометрическое истолкование теоремы, сделать чертеж.

§ 3. Теорема Лиувилля. Трансцендентные числа

1. Теорема Лиувилля

Продолжительное время считали, что все числа являются алгебраическими. Только в 1844 г. французский математик Ж. Лиувиль показал, что существуют такие числа, которые не являются алгебраическими, т. е. не могут удовлетворять ни одному алгебраическому

уравнению с целыми коэффициентами. Такие числа называются *трансцендентными*.

Идея доказательства Лиувилля заключается в следующем. Он сперва показывает, что алгебраические числа приближаются рациональными числами по определенному закону, а затем показывает, что существуют такие числа, которые этой закономерности не подчиняются.

Теорема Лиувилля: Для всякого действительного алгебраического числа α степени n (≥ 2) существует такое положительное постоянное число c , что неравенство

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^n} \quad (1)$$

выполняется для любой рациональной дроби $\frac{p}{q}$.

Доказательство. Пусть α — действительный корень неприводимого алгебраического уравнения n -й степени

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0,$$

где все a_i целые и $n \geq 2$.

Согласно теореме Безу $f(x)$ делится на $x - \alpha$, значит,

$$f(x) = (x - \alpha) \varphi(x),$$

где $\varphi(x)$ — многочлен степени $n - 1$ с действительными коэффициентами. Полагая $x = \frac{p}{q}$, имеем

$$\left| f\left(\frac{p}{q}\right) \right| = \left| \alpha - \frac{p}{q} \right| \cdot \left| \varphi\left(\frac{p}{q}\right) \right|. \quad (2)$$

Ввиду неприводимости многочлена $f(x)$, число $f\left(\frac{p}{q}\right)$ не может быть равно нулю, иначе многочлен $f(x)$ делился бы на $x - \frac{p}{q}$. Поэтому

$$\left| f\left(\frac{p}{q}\right) \right| = \frac{|a_0 p^n + a_1 p^{n-1} \cdot q + \dots + a_n q^n|}{q^n} \geq \frac{1}{q^n}, \quad (3)$$

так как $|a_0 p^n + \dots + a_n q^n|$ — целое число, которое отлично от нуля.

Пусть теперь $\frac{p}{q}$ принадлежит сегменту $[\alpha - 1, \alpha + 1]$ и $\frac{1}{c_1}$ — наибольшее значение многочлена $|\varphi(x)|$ на этом сегменте. Тогда $\left| \varphi\left(\frac{p}{q}\right) \right| \leq \frac{1}{c_1}$ и согласно (2) и (3)

$$\frac{1}{q^n} \leq \left| f\left(\frac{p}{q}\right) \right| \leq \frac{1}{c_1} \left| \alpha - \frac{p}{q} \right|,$$

откуда

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c_1}{q^n}. \quad (4)$$

Если взять $\frac{p}{q}$ вне сегмента $[\alpha - 1, \alpha + 1]$, то $\left| \alpha - \frac{p}{q} \right| > 1$, а так как q — целое число, то имеем также

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{q^n}. \quad (5)$$

Обозначим теперь наименьшее из чисел 1 и c_1 через c ; тогда ввиду соотношений (4) и (5) имеем для любых рациональных $\frac{p}{q}$

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^n},$$

где постоянная c от p и q не зависит. Теорема доказана.

Теорема Лиувилля показывает, что приближение алгебраического иррационального числа рациональными дробями ограничено снизу.

2. Доказательство существования трансцендентных чисел

Теорема Лиувилля дает необходимый признак алгебраического числа. Лиувилль показал, что можно строить бесконечно много таких чисел, которые этому признаку не подчиняются и поэтому должны быть трансцендентными. Для этого он воспользовался аппаратом непрерывных дробей.

Пусть неполные частные строящейся бесконечной цепной дроби удовлетворяют следующему рекуррент-

ному правилу: после того как неполные частные q_1, q_2, \dots, q_k уже определены (а следовательно, определена и подходящая дробь $\frac{P_k}{Q_k}$), следующее неполное частное выбирается так, чтобы выполнялось условие $q_{k+1} > Q_k^k$.

Определенная таким образом непрерывная дробь представляет некоторое иррациональное число α . Покажем, что α трансцендентно. Действительно, в силу известных свойств непрерывных дробей и условия $Q_k^k < q_{k+1}$ имеем

$$\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k \cdot q_{k+1}} = \frac{1}{Q_k (q_{k+1} Q_k + Q_{k-1})} < \\ < \frac{1}{Q_k^2 \cdot q_{k+1}} < \frac{1}{Q_k^2 \cdot Q_k^k},$$

или

$$\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1/Q_k^2}{Q_k^k}.$$

Пусть теперь дано любое $c > 0$ и произвольно задано натуральное $n (\geq 2)$. Если мы возьмем $k \geq n$ такое большое, что

$$\frac{1}{Q_k^2} < c$$

(это всегда возможно, так как Q_k неограниченно возрастает), то будем иметь $\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{c}{Q_k^k}$, а так как

при таком k $Q_k^k \geq Q_k^n$, то тем более $\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{c}{Q_k^n}$.

Таким образом, число α не удовлетворяет необходимому признаку алгебраического числа степени n , данному в теореме Лиувилля. Поэтому α не может быть алгебраическим числом степени n . Но так как n выбрано произвольно, то α вообще не может быть алгебраическим числом, следовательно, оно трансцендентно.

Заметим, что можно также строить трансцендентные числа, не прибегая к помощи непрерывных дробей.

Заметим также, что в 1874 г. немецкий математик Г. Кантор, исходя из развитой им теории множеств, дал новое замечательное доказательство существования трансцендентных чисел. Он показал, что множество действительных алгебраических чисел счетно, тогда как множество действительных чисел — несчетно. Отсюда сразу же следует, что должны существовать трансцендентные числа, причем даже в «большем» количестве, чем алгебраические числа, так как множество трансцендентных чисел — несчетно.

3. Исследования трансцендентности. Результаты Гельфонда

В предыдущем пункте мы видели, что не представляет теперь особого труда строить трансцендентные числа. Несравненно труднее исследовать арифметическую природу каких-либо конкретно заданных чисел, в особенности выяснить, являются ли эти числа алгебраическими или трансцендентными.

Как раз в этом — важнейшая задача теории трансцендентных чисел.

Задачи такого рода принадлежат к труднейшим задачам современной математики.

Только в 1873 г. французский математик Ш. Эрмит доказал трансцендентность e , а в 1882 г. немецкий математик Ф. Линдеман (аналогичным методом) — трансцендентность числа π .

Доказательства этих фактов довольно сложные (см., например, (8) или (23)).

Доказательством трансцендентности π были наконец решены вопросы о квадратуре круга и о спрямлении окружности, которые равносильны задаче о построении отрезка длиной π . Действительно, при помощи циркуля и линейки можно строить только корни алгебраического уравнения с целыми коэффициентами, разрешимого в квадратных радикалах, а π , будучи трансцендентным числом, не может быть корнем такого уравнения.

После результатов, полученных Эрмитом и Линдеманом, долгое время не удавалось добиться новых значительных успехов в рассматриваемой области. На международном математическом конгрессе в 1900 г.

Д. Гильберт в качестве одной из актуальных 23 математических проблем выдвинул задачу исследовать, являются ли трансцендентными числа вида α^β , где α и β — алгебраические числа, причем α отлично от нуля и единицы, а β — иррационально¹, и, в частности, являются ли трансцендентными числа $2^{\sqrt{2}}$, e^π .

Несмотря на усилия многих ученых, эта проблема долгое время не поддавалась решению. Только в 1929 г. советскому математику А. О. Гельфонду удалось при помощи открытого им весьма сильного метода (основанного на теории функций комплексного переменного) найти частичное решение проблемы Гильберта. Углубив свой метод введением в него новых идей, А. О. Гельфонд дал в 1934 г. полное ее решение. Он доказал, что все числа, о которых идет речь в этой проблеме, являются трансцендентными.

Из результата Гельфонда непосредственно следует, что трансцендентными будут, например, все десятичные логарифмы рациональных чисел, если сами они не являются рациональными числами. Действительно, если бы $\lg r$, где r — рациональное число, было числом алгебраически иррациональным, то число $10^{\lg r}$, согласно результату Гельфонда, должно было бы быть трансцендентным, между тем $10^{\lg r} = r$ — число рациональное. Трансцендентным является также число e^π , так как из $e^{\pi i} = -1 = i^2$ следует $e^\pi = i^{-2i}$.

В последние десятилетия А. О. Гельфонд, все более совершенствуя свои прежние методы, получил возможность указать на ряд новых классов трансцендентных чисел.

Метод Гельфонда успешно использован также другими авторами, как советскими, так и зарубежными (например, Зигель, Малер, Риччи, Шнейдер).

В заключение отметим, что большие заслуги в развитии теории трансцендентных чисел имеет также немецкий математик К. Зигель. В 1930 г. ему удалось найти естественное обобщение того метода, которым

¹ Проблема трансцендентности чисел вида α^β была впервые в частной форме поставлена Л. Эйлером.

пользовались Эрмит и Линдеман в своих доказательствах трансцендентности чисел e и π .

С помощью метода Зигеля стало возможным исследовать арифметическую природу значений довольно широкого класса целых функций, степенные ряды которых имеют алгебраические коэффициенты, например функций типа e^{x^1} .

Советскому математику А. Б. Шидловскому удалось усилить метод Зигеля и получить важные результаты в теории трансцендентных чисел.

4. Усиление неравенства Лиувилля.

Приложение к решению неопределенных уравнений

Легко понять, что теорему Лиувилля, которую мы изучали в п. 1, можно выразить также следующим образом: для всякой действительной алгебраической иррациональности α степени n (≥ 2) существует такое положительное постоянное c' , что неравенство

$$\left| \alpha - \frac{p}{q} \right| < \frac{c'}{q^n} \quad (1)$$

имеет лишь конечное число решений в целых числах p и q . (Если взять $c' = c$ из формулы (1) п. 1, согласно первой формулировке теоремы Лиувилля, то надо сказать, что решений вообще не существует.)

Неравенство Лиувилля через 50 лет удалось усилить. Это сделал в 1909 г. норвежский математик А. Туэ, который доказал следующую теорему:

Если α — любое алгебраическое число степени n , то неравенство

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^s} \quad (2)$$

может иметь только конечное число решений в целых числах p и q при любом $s > \frac{n}{2} + 1$.

Метод Туэ был 10 лет спустя усовершенствован немецким математиком К. Зигелем, а в сороковых годах усилен советским математиком А. О. Гельфондом и английским математиком Д. Дайсоном.

¹ Методом Зигеля — Шнейдера Малер в 1937 г. доказал трансцендентность числа $\eta = 0,123456789101112...$

Наконец, в 1955 г. английский математик К. Рот, пользуясь методом Туэ — Зигеля, еще более усилил неравенство Лиувилля (1), доказав, что неравенство (2) имеет только конечное число решений при $s > 2$. Этот результат, свидетельствующий об определенной близости алгебраических чисел к квадратическим иррациональностям, является большим успехом в теории чисел.

Упомянутые результаты имеют многочисленные приложения в теории решения уравнений в целых числах, в теории трансцендентных чисел, а также в других разделах теории чисел.

Уже сам Туэ при помощи теоремы, носящей его имя, доказал, что неопределенное уравнение

$$a_0x^n + a_1x^{n-1} \cdot y + \dots + a_ny^n = c, \quad (3)$$

где a_0, a_1, \dots, a_n, c — целые и многочлен $a_0t^n + a_1t^{n-1} + \dots + a_n$ неприводим в поле рациональных чисел, имеет только конечное число целых решений при $n \geq 3$.

Заметим в заключение, что метод Туэ не дает возможности судить о том, в каких границах находятся решения и каково их число.

Пользуясь другим методом, советский математик Б. Н. Делоне для более узкого класса неопределенных уравнений установил границы числа решений. Он доказал, что кубическое уравнение Пелля $ax^3 + y^3 = 1$, где a — целое, может иметь, кроме тривиального решения $(0, 1)$, не более одного решения в целых числах. Он показал также, что для каждого заданного значения a можно установить, существует ли нетривиальное решение и как найти его. Делоне доказал также, что уравнение $ax^3 + bx^2y + cxy^2 + dy^3 = 1$ имеет не более 5, а иногда ровно 5 решений в целых числах, и указал алгоритм решения.

Упражнение

241. Доказать, что: 1) $\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \dots = 0,11000100 \dots$ — число трансцендентное, 2) то же для $\alpha = \frac{1}{2^{1!}} + \frac{1}{2^{2!}} + \dots$

Глава VIII

ЧИСЛОВЫЕ ФУНКЦИИ

§ 1. Число и сумма делителей данного числа

Под *числовой функцией* $f(x)$ понимают функцию, определенную для любого натурального аргумента.

С некоторыми числовыми функциями мы уже познакомились: с функцией Эйлера, а также с функциями «целая часть от x » и «дробная часть от x ».

В этой главе продолжим изучение числовых функций.

1. Формула для числа делителей данного числа

Обозначим число натуральных делителей натурального числа n (включая тривиальные делители 1 и n) через $\tau(n)$. Если в каноническом разложении n имеет вид

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad (1)$$

где p_1, p_2, \dots, p_k — простые делители n , то, как это показано в п. 2, § 4, гл. 1, все делители d этого числа суть все числа вида

$$d = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_k^{\beta_k}, \quad (2)$$

где

$$0 \leq \beta_1 \leq \alpha_1, \quad 0 \leq \beta_2 \leq \alpha_2, \quad \dots, \quad 0 \leq \beta_k \leq \alpha_k. \quad (3)$$

Чтобы найти число делителей, необходимо подсчитать число возможных различных комбинаций для $\beta_1, \beta_2, \dots, \beta_k$, отвечающих условиям (3), так как различным комбинациям значений $\beta_1, \beta_2, \dots, \beta_k$ соответствуют различные числа d . Поскольку $\beta_1, \beta_2, \dots, \beta_k$ независимо

друг от друга принимают соответственно $\alpha_1 + 1, \alpha_2 + 1, \dots, \alpha_k + 1$ различных значений, общее число таких комбинаций будет

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

Таким образом, получаем:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1). \quad (4)$$

Пример. Пусть $n = 504 = 2^3 \cdot 3^2 \cdot 7$; тогда $\tau(504) = 4 \cdot 3 \cdot 2 = 24$.

Формула (4), как и ее вывод, показывает, что $\tau(n)$ не зависит от простых множителей p_1, p_2, \dots, p_k канонического разложения числа n , а только от их показателей.

2. Формула для суммы делителей данного числа

Пусть $S(n)$ или $\sum_n d$ — сумма всех натуральных делителей d натурального числа n ¹, имеющего каноническое разложение (1) п. 1.

Легко понять, что

$$S(n) = (1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + \dots + p_2^{\alpha_2}) \dots \dots (1 + p_k + \dots + p_k^{\alpha_k}), \quad (1)$$

так как слагаемые произведения совпадают с делителями числа n (см. (2) и (3) п. 1).

Суммируя каждый сомножитель по формуле для суммы членов геометрической прогрессии, получаем

$$S(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \quad (2)$$

Пример:

$$S(504) = S(2^3 \cdot 3^2 \cdot 7^1) = \frac{2^{3+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{7^{1+1} - 1}{7 - 1} = 1560.$$

Если в каноническом разложении числа n прибавить сомножитель $p_l^{\alpha_l}$, взаимно простой с остальными, то в правой части (1) появится дополнительный сомножитель $(1 + p + \dots + p_l^{\alpha_l})$, а в правой части (2) —

¹ Обозначается также знаком $\int(n)$ — числовой интеграл от n , взятый по делителям (Эйлер).

сомножитель $\frac{p_l^{a_l+1} - 1}{p_l - 1}$, равный сумме делителей числа $p_l^{a_l}$.

Итак, если $(n, p_l^{a_l}) = 1$, то $S(n \cdot p_l^{a_l}) = S(n) \cdot S(p_l^{a_l})$.

Вообще для взаимно простых n_1 и n_2 $S(n) = S(n_1 n_2) = S(n_1) \cdot S(n_2)$, откуда видно, что функция $S(n)$ мультипликативная.

Упражнения

242. Найти число делителей для n : 1) 378, 2) 2205, 3) 5775, 4) 36 000, 6) 31 652.

243. Найти число решений сравнений: 1) $59 \equiv 23 \pmod{x}$; 2) $173 \equiv 47 \pmod{x}$; 3) $159 \equiv 75 \pmod{2x}$; 4) $319 \equiv 39 \pmod{3x}$.

244. Найти решения сравнений: 1) $127 \equiv 87 \pmod{x}$; 2) $127 \equiv 87 \pmod{2x}$; 3) $167 \equiv 68 \pmod{5x}$.

245. Доказать, что $\tau(n)$ равно количеству целых точек на гиперболе $xy = n$ в 1-м квадранте.

246. Найти наименьшее натуральное число с 10 делителями.

247. Найти сумму делителей числа n : 1) 210, 2) 756, 3) 495, 4) 18 375.

248. Найти $S_r(n)$ — сумму r -х степеней делителей данного числа n .

249. Пользуясь результатом предыдущей задачи, найти

$$S_2(12), S_2(14), S_3(30).$$

§ 2. Совершенные числа. Специальные простые числа

1. Определение совершенных и дружественных чисел

Делители числа n (имеются в виду натуральные делители), за исключением самого числа, называются его собственными делителями; их сумма равна $S(n) - n$.

Если для двух чисел a , b сумма собственных делителей каждого из них равна другому, то такие числа называются *дружественными*; для них

$$S(a) - a = b, S(b) - b = a, \text{ откуда } S(a) = S(b) = a + b.$$

Натуральное число называется *совершенным*, если оно равно сумме своих собственных делителей (или если оно дружественно самому себе), т. е. удовлетворяет условию

$$S(n) - n = n,$$

или

$$S(n) = 2n.$$

Определения совершенных и дружественных чисел имеются уже в «Началах» Евклида, они упоминаются и Платоном. Греки видели в них некую совершенную гармонию и приписывали им мистический характер.

Древним грекам была известна пара дружественных чисел 220 и 284 и четыре совершенных числа: 6, 28, 495, 8128.

2. Представление четных совершенных чисел. О нечетных совершенных числах

Евклид нашел достаточное условие для четных совершенных чисел.

Теорема Евклида: *если число имеет вид $n = 2^{k-1}(2^k - 1)$, где натуральное $k > 1$ и при этом $2^k - 1 = p$ число простое, то n совершенно.*

В самом деле, для такого $n = 2^{k-1} \cdot p$ по формуле для суммы делителей данного числа находим

$$\begin{aligned} S(n) &= \frac{2^k - 1}{2 - 1} \cdot \frac{p^{1+1} - 1}{p - 1} = (2^k - 1) \cdot (p + 1) = p \cdot 2^k = \\ &= 2 \cdot 2^{k-1} \cdot p = 2n. \end{aligned}$$

Среди чисел $k \leq 7$ условие теоремы, чтобы $2^k - 1$ было простым числом, выполняется для $k = 2, 3, 5$ и 7 . Мы получаем простые числа 3, 7, 31 и 127, которым соответствуют упомянутые выше четыре совершенных числа.

После Евклида дальнейший крупный успех в исследовании совершенных чисел был достигнут только через 2 тысячи лет Эйлером.

Эйлер доказал, что достаточное условие Евклида для четных совершенных чисел является для них также необходимым.

Теорема Эйлера: *четные совершенные числа имеют вид $n = 2^{k-1} \cdot (2^k - 1)$, где натуральное $k > 1$ и $2^k - 1$ — число простое.*

Доказательство. Из условия четности числа n следует, что оно имеет вид

$$n = 2^{k-1} \cdot u,$$

где натуральное $k > 1$, а u — нечетное натуральное число, так что $(2^{k-1}, u) = 1$ и

$$S(n) = S(2^{k-1}) \cdot S(u) = (2^k - 1) \cdot S(u).$$

Если n к тому же число совершенное, то

$$S(n) = 2n = 2^k \cdot u,$$

поэтому

$$(2^k - 1) \cdot S(u) = 2^k \cdot u,$$

что дает нам возможность найти вид числа u .

Действительно, в силу того, что $(2^k, 2^k - 1) = 1$, из этого равенства следует, что $u = (2^k - 1) \cdot t$ (где t — натуральное число), а вместе с тем, что

$$S(u) = 2^k \cdot t.$$

Число u заведомо имеет два различных делителя: t и $u = (2^k - 1) \cdot t > t$ (так как при $k > 1$ $2^k - 1 > 1$).

Но так как их сумма равна $2^k \cdot t$, т. е. $S(u)$, то этими числами исчерпываются все натуральные делители u .

Поскольку лишь простые числа p имеют точно два различных натуральных делителя, именно 1 и p , то ясно, что $t = 1$ и $u = (2^k - 1) \cdot t = (2^k - 1) \cdot 1 = 2^k - 1 = p$ — число простое. Следовательно, n на самом деле имеет вид, указанный в теореме Евклида.

Теоремы Евклида и Эйлера показывают, что формулой

$$n = 2^{k-1} (2^k - 1),$$

где $k > 1$ и $2^k - 1$ — простое число, представимы все четные совершенные числа.

В заключение отметим, что в 50-е годы нашего столетия сведения о совершенных числах обогатились новыми интересными данными. Найдены, например, верхние оценки плотностей числа совершенных чисел:

$$\lim_{x \rightarrow \infty} \frac{V(x)}{\sqrt{x}} \leq \frac{1}{2\sqrt{5}},$$

где $V(x)$ — число совершенных чисел $< x$.

Что касается нечетных совершенных чисел, то до сих пор неизвестно, существуют ли такие или нет.

Во всяком случае твердо установлено, что если нечетные совершенные числа и существуют, то они чрезвычайно велики; ни одно из них не может быть, например, меньше e^{52729} . Известно также, что они могут быть только формы $p^{4k+1} \cdot N^2$, где простое $p = 4m + 1$, $(N, p) = 1$, и не могут иметь менее 2800 различных

простых множителей. Один из первых результатов о простых делителях совершенных чисел получен советским математиком И. С. Градштейном в 1925 г.

3. Простые числа Мерсенна; их наибольшее известное значение

До сих пор неизвестно, имеется ли бесконечно много четных совершенных чисел, так как неизвестно, существует ли бесконечно много простых чисел вида $2^k - 1$.

Необходимым условием простоты числа такого вида является простота его показателя k .

В самом деле, если $k = k_1 \cdot k_2$ — число составное, то можно $2^k - 1 = (2^{k_1})^{k_2} - 1$ разложить на нетривиальные множители (т. е. такие, которые отличны от самого числа и от единицы), из которых один будет $2^{k_1} - 1$.

Полученное условие не является однако достаточным. Так, например, при $k = 11$ имеем $2^{11} - 1 = 2047 = 23 \cdot 89$.

О простых числах вида $M_p = 2^p - 1$ (где p — простое число) французский математик Мерсенн вел переписку с Ферма; эти числа получили название *простых чисел Мерсенна*.

До Эйлера было известно 7 совершенных чисел, соответствующих простым числам Мерсенна при $p = 2, 3, 5, 7, 13, 17$ и 19 , Эйлер доказал, что $2^{31} - 1$ есть простое число.

Число Эйлера считалось наибольшим известным простым числом до 1883 г., когда талантливый русский вычислитель И. М. Первушин (1827—1900) доказал, что $2^{61} - 1$ есть простое число (см. (49)).

К настоящему времени установлена еще простота чисел вида $2^p - 1$ для показателей:

$p = 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213$.

Начиная с показателя $p = 521$, простота чисел M_p была установлена при помощи электронных вычислительных машин (1952).

Простота числа $2^{11213} - 1$ (имеет 3375 цифр) была установлена в 1963 г. Это вообще наибольшее из известных до 1963 г. простое число.

Основой для указанных вычислений является критерий простоты чисел M_p , найденный в основном уже в 1878 г. французским математиком Э. Люка:

Число $M_p = 2^p - 1$ (где p — нечетное простое число) тогда и только тогда простое, когда $(p-1)$ -й член рекуррентной последовательности.

$$c_1 = 4, c_2 = 4^2 - 2 = 14, \dots, c_k = c_{k-1}^2 - 2$$

делится на M_p , т. е. когда $c_{p-1} \equiv 0 \pmod{M_p}$.

Пример. Применим критерий Люка к $M_7 = 127$. Имеем по модулю 127

$$c_3 = 14^2 - 2 = 194 \equiv 67, c_4 = 194^2 - 2 \equiv 67^2 - 2 \equiv 42,$$

$$c_5 = 42^2 - 2 \equiv -16, c_6 = 16^2 - 2 = 254 \equiv 0 \pmod{127}.$$

Условие теоремы выполнено, следовательно, можно утверждать, что $2^7 - 1 = 127$ — число простое.

Отметим в заключение без доказательства один признак делимости чисел Мерсенна, на который уже указал Эйлер: если $p = 4n + 3$ и $q = 2p + 1 = 8n + 7$ оба простые, то $M_p \equiv 0 \pmod{q}$ (некоторые другие признаки делимости чисел M_p указаны, например, в (45)).

4. Простые числа Ферма

Ферма высказал предположение, что все числа вида $2^k + 1$, где $k = 2^n$, являются простыми. Для $k > 0$ условие $k = 2^n$ является необходимой предпосылкой, так как в противном случае, когда $k = k_1 \cdot k_2$ содержит нечетный множитель $k_1 > 1$, $2^k + 1 \equiv (2^{k_1})^{k_2} + 1$, очевидно, делится на $2^{k_1} + 1$.

Однако указанное условие не является достаточным: в то время как для $n = 0, 1, 2, 3, 4$ получаются простые числа, так называемые *простые числа Ферма*,

$$3, 5, 17, 257, 65537,$$

для $n > 4$ до сих пор не найдено ни одного простого числа¹. Неизвестно также, обрывается ли последова-

¹ Интересно отметить, что простые числа Ферма играют важную роль в геометрии. А именно, Гаусс доказал, что правильный p -угольник для простого $p > 2$ можно построить циркулем и линейкой тогда и только тогда, когда p — простое число Ферма.

тельность простых чисел Ферма или их существует бесконечно много.

До 1952 г. было известно, что числа Ферма $F_n = 2^{2^n} + 1$ являются составными для показателей $n = 5, 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73$. (Для $n = 5$ этот факт впервые доказал Эйлер, для $n = 12, 23$ — И. М. Первушин.)

При помощи электронных вычислительных машин до 1964 г. установлено, что и для показателей 10, 13, 14, 15, 16, 19, 21, 25, 26, 27, 30, 32, 39, 42, 52, 55, 58, 63, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945 получаются составные числа.

Отметим без доказательства критерий простоты чисел F_n : число $F_n = 2^{2^n} + 1$ в том и только в том случае простое, когда

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Нахождение простых делителей составных F_n значительно облегчается теоремой: для $n > 1$ *каждый простой делитель $F_n = 2^{2^n} + 1$ имеет вид $p = k \cdot 2^{n+2} + 1$.*

Доказательство. Если $F_n | p$, то $2^{2^n} \equiv -1 \pmod{p}$ и $2^{2^{n+1}} \equiv 1 \pmod{p}$, откуда следует, что по модулю p число 2 принадлежит показателю 2^k , где $k \leq n + 1$ (так как $2^{2^{n+1}}$ имеет в качестве делителей только числа указанного вида).

Но k не равно n , так как в противном случае получилось бы, что $2^{2^n} + 1 | p$, $2^{2^n} - 1 | p$ и вместе с тем $2 | p$, т. е. $p = 2$, что невозможно ввиду того что F_n — нечетное; k не может также быть меньше n , так как если бы 2 принадлежало показателю 2^{n_1} , где $n_1 < n$, то 2^n делилось бы на 2^{n_1} и из $2^{2^{n_1}} \equiv 1 \pmod{p}$ следовало бы $2^{2^n} \equiv 1 \pmod{p}$, что, как мы в этом убедились, невозможно.

Итак, 2 принадлежит по модулю p показателю 2^{n+1} и этот показатель должен быть делителем $p - 1$, так что $p \equiv 1 \pmod{2^{n+1}}$, для $n > 1$, поэтому $p \equiv 1 \pmod{8}$, откуда следует, что символ Лежандра $\left(\frac{2}{p}\right) = 1$ и

$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) = 1 \pmod{p}$. Из этого следует далее, что $\frac{p-1}{2}$ делится на 2^{n+1} , т. е. $p = k \cdot 2^{n+2} + 1$.

На основании доказанной теоремы можно, например, утверждать, что возможные простые делители F_5 имеют вид $128k + 1$. На самом деле оказывается, что $641 = 5 \cdot 128 + 1$ является делителем F_5 , так как, с одной стороны, $641 = 5 \cdot 2^7 + 1$, $5 \cdot 2^7 \equiv -1 \pmod{641}$ и $5^4 \cdot 2^{28} \equiv 1 \pmod{641}$, (1)

а, с другой стороны, $641 = 16 + 625 = 2^4 + 5^4$ и $2^4 \equiv -5^4 \pmod{641}$, (2)

откуда (почленным перемножением (1) и (2)) получается

$$2^{32} \equiv -1 \pmod{641}, \text{ или } 2^{32} + 1 \equiv 0 \pmod{641}.$$

Наибольшее из известных составных чисел Ферма F_{1945} имеет $> 10^{582}$ цифр. О том, как можно убедиться, что число $5 \cdot 2^{1947} + 1$, насчитывающее 587 цифр, является его наименьшим простым делителем, интересно почитать в (53).

5. О числовых функциях, принимающих простые значения

Многие математики старались найти такую элементарную функцию $f(x)$, которая для всех целых x (или по крайней мере для бесконечной последовательности таких x) давала бы различные простые числа. При помощи такой функции можно было бы вычислить сколь угодно много простых чисел и сколь угодно большие простые числа, если только имеется возможность найти $f(x)$ для каждого x .

Эйлер нашел сравнительно длинные последовательности простых чисел, пользуясь квадратичными функциями. Так, например, выражение $x^2 + x + 17$ при $x = 0, 1, \dots, 15$, а $x^2 - x + 41$ при $x = 0, 1, 2, \dots, 40$ дают только простые числа. Аналогичным свойством обладают многочлены $2x^2 + 29$ при $x = 0, 1, \dots, 28$, $x^2 + x + 41$ при $x = 0, 1, \dots, 39$, $x^2 - 79x + 1601$ при $x = 0, 1, \dots, 79$.

Найдены также другие многочлены $f(x)$, которые при $x = 0, 1, 2, \dots, k$ принимают значения простых чисел.

В то же время легко доказать теорему, которую впервые высказал петербургский академик Х. Гольдбах: *никакая целая рациональная функция от x с целыми коэффициентами не может для всякого натурального значения x равняться простому числу.*

Доказательство. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ и $f(a) = p$, где p — простое число. Тогда для любого целого t имеем по формуле Тейлора

$$f(a+pt) = f(a) + pt f'(a) + (pt)^2 \cdot \frac{f''(a)}{2!} + \dots + (pt)^n \cdot \frac{f^{(n)}(a)}{n!},$$

откуда видно, что $f(a+pt)$ делится на p , так как каждое слагаемое в правой части равенства делится на p .

Поэтому, если и $f(a+pt)$ — число простое, то должно быть $f(a+pt) = p$ для всех целых t , в том числе и при $t \rightarrow \infty$.

Исключая тривиальный случай, когда $f(x) = f(a)$ тождественно, это противоречит теореме о неограниченном возрастании модуля многочлена, согласно которой при $t \rightarrow \infty$ $f(a+pt) \rightarrow \infty$.

Таким образом, не для всякого натурального значения аргумента x $f(x)$ может равняться простому числу. Теорема доказана.

Попытка построить функцию, охарактеризованную в начале настоящего пункта, в виде показательной функции $f(x) = a^x \pm b^x$, где a и b — целые, приводит в простейшем случае, когда $a=2$, $b=1$, к простым числам Мерсенна и Ферма, которые мы рассматривали в третьем и четвертом пунктах настоящего параграфа.

В заключение отметим, что хотя американский математик Миллс в 1947 году доказал существование действительного числа α , такого, что $[\alpha^{3^n}]$ простое число для любого натурального n , все же задача нахождения простого числа, большего любого заданного числа, остается до сих пор практически нерешенной.

Дело в том, что известны лишь немногие знаки α , так что по указанной формуле действительно вычислить можно лишь немногие простые числа. Результат

английского математика Е. М. Райта, что существует такое действительное число α , при котором числа $[2^\alpha]$, $[2^{\alpha_1}]$, $[2^{\alpha_2}]$, ..., где $\alpha_1 = 2^\alpha$, $\alpha_2 = 2^{\alpha_1}$ и так далее, все являются простыми, и еще более интересный результат польского математика В. Серпинского, что существует такое действительное число α , при помощи которого по формуле

$$p_n = [\alpha \cdot 10^{2^n}] - 10^{2^{n-1}} [\alpha \cdot 10^{2^{n-1}}]$$

можно вычислить n -ое простое число в натуральном ряду, имеют аналогичный недостаток.

6. О критериях простых чисел и разложении на множители

Прежде всего отметим, что каждое составное число N содержит простой множитель $\leq \sqrt{N}$; если N не делится ни на одно простое число $p \leq \sqrt{N}$, то оно простое.

Существуют таблицы простых чисел и разложений на множители (основой для их составления является метод решета Эратосфена). Наилучшие таблицы простых чисел составлены Д. Н. Лемером (1914), в них содержатся простые числа до 10006721¹.

Таблица разложений на множители того же автора (1909) дает самый меньший делитель всех чисел до 10017000, не делящихся на 2, 3, 5 или 7. После нахождения наименьшего делителя некоторого составного числа задача разложения на множители сводится к меньшему числу.

Для исследования больших чисел, выходящих за пределы таблиц, найдены различные критерии простоты (см. (13)), однако многие из них (например, критерий Вильсона) не имеют непосредственной практической ценности. Некоторые критерии приобрели практическое значение благодаря применению электронных вычислительных машин.

Разложение на множители очень больших чисел, не делящихся на малые простые числа, представляет собой задачу очень трудоемкую, для решения которой общий метод не найден.

¹ В 1959 г. Бэкер и Грюнбергер закончили работу по созданию микроарт, содержащих простые числа, меньше чем 104 395 301.

Некоторые критерии простоты и методы разложения на множители связаны с представлением чисел квадратичными формами и употреблялись еще Ферма и Эйлером. Эти эффективные методы и сейчас сохраняли свое значение. Рассмотрим их кратко.

1. Из тождества $N = 2n + 1 = (n + 1)^2 - n^2$ (1) видно, что каждое нечетное число представимо в виде разности квадратов. Нечетное простое число другого представления в виде разности двух квадратов иметь не может.

В самом деле, если $N = p$ число простое, то из

$$p = 2n + 1 = x^2 - y^2 = (x + y)(x - y)$$

следует

$$x + y = 2n + 1, \quad x - y = 1,$$

откуда

$$x = n + 1, \quad y = n.$$

Если нечетное N составное и $N = a \cdot b$, $a > b > 1$ (или $a = b \neq 1$), то имеем для N и другое представление в виде разности двух квадратов: полагая

$$x + y = a, \quad x - y = b,$$

находим

$$x = \frac{a + b}{2}, \quad y = \frac{a - b}{2},$$

где x и y целые числа, ибо a и b нечетные.

Таким образом, $N = x^2 - y^2$ является представлением, отличным от (1).

Если, наоборот, для нечетного N имеется больше чем одно представление в виде разности двух квадратов, то N составное (так как простое N не может иметь более одного представления) и представление, отличное от (1) дает возможность найти разложение N на нетривиальные множители.

Практически нахождение нетривиального разложения осуществляется следующим образом: прибавляем последовательно к $N = 2n + 1$ квадраты y^2 . Если при $y < n$ получается квадрат, то сразу находим нетривиальное разложение, например

$$493 + 6^2 = 23^2, \text{ поэтому } 493 = 29 \cdot 17.$$

2. Эйлер указал 65 чисел $d \geq 1$ (он называл их удобными), для которых имеет место теорема: *если нечетное число N имеет лишь одно представление в форме $x^2 + dy^2$, причем с условием $(x, dy) = 1$, то оно простое* (к числам d , в частности, принадлежат все натуральные числа от 1 до 10, а самое большое из них 1848; из новых исследований вытекает, что количество чисел d конечно, однако неизвестно, является ли 1848 наибольшим из них).

Представления некоторых простых чисел даны в нижеприведенной таблице.

Простые числа N	Формы, которыми N представляются лишь однозначно, причем с условием $(x, dy) = 1$
$4n + 1$	$x^2 + y^2$
$8n + 1, 8n + 3$	$x^2 + 2y^2$
$6n + 1$	$x^2 + 3y^2$
$14n + 1, 14n + 9, \}$ $14n + 11 \}$	$x^2 + 7y^2$

Если существует более одного представления N формой $x^2 + dy^2$, то N можно разложить на множители.

Примеры:

1) Пусть

$$N = x_1^2 + y_1^2 = x_2^2 + y_2^2,$$

тогда

$$x_1^2 - x_2^2 = y_2^2 - y_1^2, \quad \frac{x_1 - x_2}{y_2 - y_1} = \frac{y_2 + y_1}{x_1 + x_2} = \frac{u}{v}, \quad (u, v) = 1,$$

откуда

$$\begin{aligned} x_1 - x_2 &= ut, & y_2 - y_1 &= vt, \\ y_2 + y_1 &= us, & x_1 + x_2 &= vs, \\ x_1 &= \frac{1}{2}(ut + vs), & y_1 &= \frac{1}{2}(us - vt), \\ N &= x_1^2 + y_1^2 = \frac{1}{4}(u^2 + v^2)(s^2 + t^2). \end{aligned}$$

Пусть

$$N = 254137 = 504^2 + 11^2 = 484^2 + 141^2.$$

Здесь

$$u = 2, \quad v = 13, \quad t = 10, \quad s = 76,$$

поэтому

$$N = (2^2 + 13^2) \cdot (5^2 + 38^2) = 173 \cdot 1469;$$

2) Из тождества

$$p^4 + 4 = (p^2)^2 + 2^2 = (p - 2)^2 + (2p)^2$$

следует, что все числа вида $p^4 + 4$, кроме 5, являются составными (теорема Софьи Жермен). К тому же результату приводит и алгебраическое разложение

$$p^4 + 4 = (p^2 + 2p + 2)(p^2 - 2p + 2).$$

Заметим, что вообще разложения на множители, которые арифметическим методам поддаются лишь с большим трудом, иногда легко осуществляются с помощью алгебраической формулы. Так, например, с большим трудом удалось разложить на множители $2^{58} + 1$, однако впоследствии оказалось, что

$$2^{4n+2} + 1 = [(2^n - 1)^2 + 2^{2n}][2^{2n} + (2^n + 1)^2],$$

откуда искомое разложение легко получается.

Упражнения

250. Какой вид имеет каждый натуральный делитель составного F_n ?

251. Если $F_5 = 4\,294\,967\,297$ разделить на наименьший его простой делитель 641, то получается число $m = 6\,700\,417$. Сколькими делениями можно подтвердить простоту этого числа?

252. Найти нетривиальные множители разложения $N = 2n + 1$ на сумму двух квадратов методом, указанным на стр. 240 (воспользоваться таблицей квадратов); $N = 2173, 1363, 7663, 4187$.

253. Разложить на множители число N : 1) $N = 32\,980 = 178^2 + 36^2 = 146^2 + 108^2$; 2) $N = 76\,082 = 269^2 + 61^2 = 199^2 + 191^2$.

254. Найти простые числа, которые являются суммами двух кубов натуральных чисел.

§ 3. Функции $[x]$ и $\{x\}$.

1. Графики функций $[x]$ и $\{x\}$

В настоящем параграфе продолжим изучение функций $[x]$ — «целая часть от x » и $\{x\}$ — «дробная часть от x », определения которых уже даны в § 3 гл. III. Наглядное представление об этих функциях дают их графики.

1. Если m — целое число, причем $m \leq x < m + 1$, то по определению $[x] = m$, так что $[x] \leq x < [x] + 1$.

Таким образом, график функции $y = [x]$ имеет вид как на рис. 2.

2. Из определения «дробной части от x » $\{x\} = x - [x]$ следует, что $0 \leq \{x\} < 1$. Поэтому график функции $y = \{x\}$, имеет вид как на рис. 3.

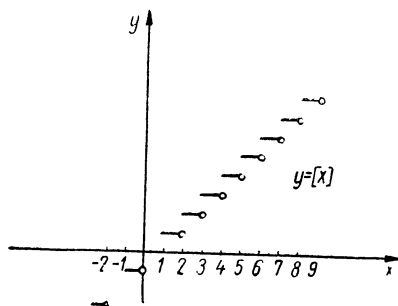


Рис. 2.

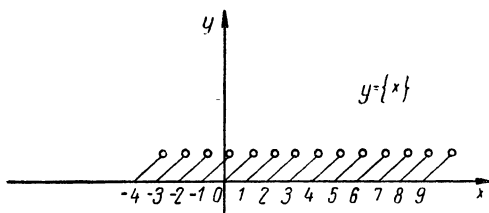


Рис. 3.

2. Некоторые свойства функции $[x]$

При помощи функции «целая часть» легко найти наибольшее целое a , n кратное которого не превосходит действительное число x . (Если $x > 0$, то a означает количество натуральных чисел, не превосходящих x и делящихся на n .) В самом деле, поскольку по условию $an \leq x < (a+1)n$, то $a \leq \frac{x}{n} < a+1$, а это означает, что $a = \left[\frac{x}{n} \right]$.

Используя указанное истолкование для $\left[\frac{x}{n} \right]$, можно без особого труда доказать, что $\left[\frac{[x]}{n} \right] = \left[\frac{x}{n} \right]$. Дейст-

вительно, так как между $[x]$ и x нет целых точек, то наибольшее целое a , n кратное которого $\leq [x]$, является также наибольшим целым, n кратное которого $\leq x$. Но последнее равно $\left[\frac{x}{n}\right]$, поэтому и $a = \left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$.

Из этого свойства следует, что для натуральных чисел a , b и n $\left[\frac{n}{ab}\right] = \left[\frac{[n/a]}{b}\right] = \left[\frac{[n/b]}{a}\right]$, потому что $\left[\frac{n}{ab}\right]$ можно записать также в видах $\left[\frac{n/a}{b}\right]$ и $\left[\frac{n/b}{a}\right]$.

3. Вычисление показателя α , с которым простое число p входит в произведение $n!$

Рассмотрим задачу, в решении которой функция $[x]$ имеет важное применение.

Задача: найти, с каким показателем α простое число p входит в произведение $n!$

Показатель простого числа p в произведении $n!$ зависит только от тех сомножителей, которые делятся на p .

По крайней мере, по единице в показатель числа p вносят те сомножители произведения $n!$, которые делятся на p , т. е. числа последовательности $1 \cdot p, 2 \cdot p, \dots, \left[\frac{n}{p}\right] \cdot p$; их число равняется $\left[\frac{n}{p}\right]$.

По крайней мере, по второй единице в показатель числа p вносят те числа указанной последовательности, которые делятся на p^2 : их число равняется $\left[\frac{n}{p^2}\right]$ и т. д.

Поэтому

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots, \quad (1)$$

пока ряд не обрывается.

При практическом вычислении α целесообразно учесть, что согласно доказанному в предыдущем пункте, $\left[\frac{n}{p^2}\right] = \left[\frac{[n/p]}{p}\right]$, $\left[\frac{n}{p^3}\right] = \left[\frac{[n/p^2]}{p}\right]$ и т. д.

Пример. Найти показатель α , с которым число 5 входит в $71!$

$$\alpha = \left[\frac{71}{5} \right] + \left[\frac{71}{5^2} \right] = 14 + 2 = 16.$$

В силу последнего замечания можно воспользоваться легко понятной схемой

$$\begin{array}{r} 71 \mid 5 \\ 14 \mid 5 \\ 2 \mid 5 \\ 0 \end{array}, \quad \alpha = 14 + 2 = 16.$$

Если p^t есть наибольшая степень p , не превосходящая n , то α можно записать в виде

$$\alpha = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \dots + \left[\frac{n}{p^t} \right] = \sum_{k=1}^t \left[\frac{n}{p^k} \right]. \quad (2)$$

Легко вычислить t :

$$\begin{aligned} p^t &\leq n, \\ t \ln p &\leq \ln n, \\ t &\leq \frac{\ln n}{\ln p}. \end{aligned}$$

Следовательно, $t = \left\lfloor \frac{\ln n}{\ln p} \right\rfloor$.

Впредь будем обозначать максимальное значение целого t , которое удовлетворяет условию $p^t \leq n$, через $t_{n,p}$.

Упражнения

255. Найти показатель α , с которым 1) 7 входит в $89!$, 2) 5 — в $313!$, 3) 11 — в $887!$ 4) 3 — в $569!$

256. 1) Определить сколькими нулями оканчивается $295!$ 2) Увеличится ли количество нулей, если взять $299!$?

257. Найти канонические разложения на множители для $10!$ и $20!$

258. Найти наибольшее натуральное значение x в сравнении $201 \cdot 202 \dots 700 \equiv 0 \pmod{13'}$.

259. Доказать, что $\tau(1) + \tau(2) + \dots + \tau(n) = \left[\frac{n}{1} \right] + \left[\frac{n}{2} \right] + \dots + \left[\frac{n}{n} \right]$, где $\tau(n)$ — число делителей n .

260. Доказать формулу предыдущей задачи, пользуясь геометрической интерпретацией, указанной в задаче 245. Сделать чертеж.

261. Доказать, что $s(1) + s(2) + \dots + s(n) = 1 \cdot \left[\frac{n}{1} \right] + 2 \left[\frac{n}{2} \right] + \dots + n \left[\frac{n}{n} \right]$, где $s(n)$ — сумма делителей n .

262. Доказать, что $[x + y] \geq [x] + [y]$ и вообще $[x + y + \dots + z] \geq [x] + [y] + \dots + [z]$.

263. Доказать, что $N = \frac{(a_1 + a_2 + \dots + a_k)!}{a_1! \cdot a_2! \dots a_k!}$ — целое число.

264. Доказать, что для действительных чисел α и β $[2\alpha] + [2\beta] \geq [\alpha] + [\beta] + [\alpha + \beta]$.

265. Доказать, что для натуральных m и n $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ является целым числом.

266. Доказать, что для любого действительного x и натурального n

$$[x] + \left[x + \frac{1}{n} \right] + \dots + \left[x + \frac{n-1}{n} \right] = [nx]. \quad (1)$$

267. Доказать, что $\varphi(x, N)$ — количество натуральных чисел $\leq x$ и взаимно простых с N (или, что равнозначно, с каждым его простым делителем p_1, p_2, \dots, p_n или произведением этих делителей) выражается формулой

$$\varphi(x, N) = [x] - \sum \left[\frac{x}{p_i} \right] + \sum \left[\frac{x}{p_i p_j} \right] - \dots + (-1)^n \left[\frac{x}{p_1 p_2 \dots p_n} \right],$$

на которую впервые указал Лежандр. Имея в виду замечание в скобках, пишут также $\varphi(x; p_1, p_2, \dots, p_n)$, $\varphi(x; p_1 p_2 \dots p_n)$.

268. Найти количество натуральных чисел: 1) ≤ 300 и взаимно простых с 30; 2) ≤ 713 и взаимно простых с 42.

269. Найти значение функции Эйлера $\varphi(m)$, пользуясь формулой Лежандра, указанной в задаче 267.

§ 4. Распределение простых чисел

1. Бесконечность множества простых чисел. Доказательство Евклида. Функция $\pi(x)$ и ее график

Вопросы распределения простых чисел 2, 3, 5, 7, ... в ряду натуральных чисел принадлежат к труднейшим вопросам теории чисел; ими интересовались математики уже с древнейших времен.

Еще Евклид в «Началах» доказал бесконечность множества простых чисел. Сущность его рассуждения состоит в следующем:

Допустим, что число простых чисел конечно, и пронумеруем их, например в порядке возрастания через p_1, p_2, \dots, p_n .

Число $Q_n = p_1 \cdot p_2 \dots p_n + 1$

должно обладать хотя бы одним простым делителем p_m . Этот простой делитель не может быть равен p_1 , или p_2, \dots , или p_n , так как в противном случае из делимости Q_n на p_m и делимости $p_1 \cdot p_2 \dots p_n$ на p_m , следовало бы, что и 1 делится на p_m , а это невозможно.

Таким образом, предположение, что числами p_1, p_2, \dots, p_n исчерпываются все простые числа, приводит к противоречию.

Обозначим, как это принято, через $\pi(x)$ число простых чисел, не превосходящих действительное число x . Тогда теорему Евклида можно выразить следующим образом:

При $x \rightarrow \infty$ $\pi(x) \rightarrow \infty$, или $\lim_{x \rightarrow \infty} \pi(x) = \infty$.

На рис. 4 дано графическое изображение функции $\pi(x)$. $\pi(2) = 1$, $\pi(3) = 2$, $\pi(5) = 3$, $\pi(7) = 4$, $\pi(11) = 5$, $\pi(13) = 6$ и т. д. Левые концы «ступеней» принадлежат графику $\pi(x)$, правые концы ему не принадлежат.

С переходом от одного простого числа к следующему значение функции $\pi(x)$ увеличивается на 1; чтобы

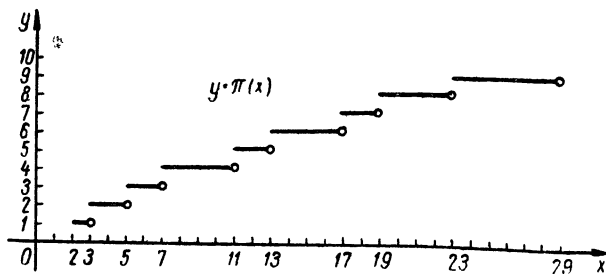


Рис. 4.

получить ее значение для x , нужно просуммировать эти единицы по всем простым числам, не превосходящим x . Поэтому пишут также

$$\pi(x) = \sum_{p \leq x} 1.$$

2. Оценка n -го простого числа, вытекающая из доказательства Евклида

Доказательство Евклида дает возможность найти оценку (правда, грубую) для n -го простого числа.

В самом деле, из доказательства следует, что Q_n делится на некоторое простое число p_m с индексом $m > n$.

Значит,

$$p_{n+1} \leq p_m \leq Q_n$$

и

$$p_{n+1} \leq p_1 \cdot p_2 \dots p_n + 1.$$

Отсюда методом математической индукции получаем оценку

$$p_{n+1} < 2^{2^n}.$$

Действительно,

$$1) \ p_{1+1} = p_2 < 2^{2^1};$$

2) предположим, что и

$$p_3 < 2^{2^2}, \quad p_4 < 2^{2^3}, \dots, p_n < 2^{2^{n-1}};$$

тогда из

$$p_{n+1} \leq p_1 \cdot p_2 \dots p_n + 1,$$

в силу того, что

$$p_1 = 2 \text{ и } 2p_1 \cdot p_2 \dots p_n > p_1 \cdot p_2 \dots p_n + 1,$$

следует

$$\begin{aligned} p_{n+1} &< 2 \cdot 2 \cdot 2^{2^1} \cdot 2^{2^2} \dots 2^{2^{n-1}} = 2^{1+(1+2^1+2^2+\dots+2^{n-1})} = \\ &= 2^{1+(2^n-1)} = 2^{2^n}, \end{aligned}$$

т. е.

$$p_{n+1} < 2^{2^n}.$$

Поэтому на основании аксиомы математической индукции¹ мы можем утверждать, что для любого натурального n

$$p_{n+1} < 2^{2^n}.$$

¹ Мы применили здесь аксиому математической индукции в следующей форме (которая равносильна обычной). Пусть: 1) число единица обладает свойством А; 2) из того, что свойством А обладают все натуральные числа, меньшие натурального числа n , вытекает, что и число n обладает свойством А. При этих условиях любое натуральное число обладает свойством А.

Отметим, что нетрудно получить более сильную оценку¹: $p_n < 2^n$, но еще более точная оценка вытекает, как это в дальнейшем будет показано, из результатов П. Л. Чебышева.

3. Существование любых отрезков натурального ряда, не содержащих простых чисел. Проблема простых чисел «близнецов»

В закономерности следования простых чисел в натуральном ряду на первый взгляд неожиданным фактом является тот, что в последовательности p_1, p_2, \dots всех простых чисел встречаются промежутки сколь угодно большой длины. Однако этот факт доказывается очень просто.

Действительно, если $n > 1$ какое-либо натуральное число, то среди $n - 1$ следующих друг за другом натуральных чисел

$$n! + 2, n! + 3, \dots, n! + n$$

ни одно не является простым, так как $n! + 2$ делится на 2, $n! + 3$ на 3 и так далее, наконец, $n! + n$ делится на n , причем во всех случаях делитель меньше делимого, т. е. является собственным.

С другой стороны, встречаются такие простые числа, как например, 11 и 13; 17 и 19, разность между которыми равна двум, так называемые «близнецы».

Таблица простых чисел (доведенная до одиннадцати миллионов) показывает наличие весьма больших пар простых чисел — близнецов p и $p + 2$ (например, для $p = 8\,004\,119, 10\,006\,427$), однако вопрос о бесконечности числа таких пар является до сих пор нерешенным (для наибольшей из известных пар $p = 1\,000\,000\,009\,649$).

Интересно отметить, что в 1919 году норвежский математик В. Брун доказал, что если даже число «близнецов» бесконечно, то все же ряд из обратных величин «близнецов» сходится. Он показал также, что для больших x число простых чисел «близнецов», не пре-

¹ См., например: Д. О. Шклярский и др. Избранные задачи и теоремы элементарной математики, ч. 1. Арифметика и алгебра, Гостехиздат, 1950, задача 206.

вышающих x , не превосходит $C \cdot \frac{x}{\ln^2 x}$, где C соответствующая постоянная¹.

4. Доказательство Эйлера бесконечности множества простых чисел

После Евклида крупных результатов в развитии теории простых чисел достиг Л. Эйлер.

Эйлер дал новое доказательство бесконечности числа простых чисел, основанное на идеях математического анализа и тем самым положил начало аналитической теории чисел.

Доказательство Эйлера можно изложить следующим образом: для простого числа p можно писать

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \dots \quad (1)$$

Предположим, что число простых чисел конечно, и пусть p_1, p_2, \dots, p_k вся их совокупность.

Напишем ряды (1) для всех этих простых чисел.

Так как правые части (1) — сходящиеся ряды положительных чисел и их число конечно, то их можно почленно перемножить, причем должен получиться сходящийся ряд. Получим

$$\prod_{i=1}^k \frac{1}{1 - \frac{1}{p_i}} = \sum \frac{1}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}}, \quad (2)$$

где суммирование распространено на все различные возможные комбинации неотрицательных показателей $\alpha_1, \alpha_2, \dots, \alpha_k$.

Таким образом, знаменатели представляют собой канонические разложения всех натуральных чисел, имеющих в качестве простых делителей числа p_1, p_2, \dots, p_k .

¹ Этому противостоит тот факт, что ряд $\sum_p \frac{1}{p}$, взятый по всем простым числам, является расходящимся (см. п. 5 наст. параграфа), а $\pi(x) < C \frac{x}{\ln x}$ (см. п. 8, наст. параграфа).

По предположению этими простыми числами исчерпываются все простые числа, поэтому знаменатели представляют собой совокупность всех натуральных чисел вообще. Располагая члены полученного сходящегося ряда по возрастающим знаменателям (на это имеем право, так как все члены этого ряда — числа

положительные), получаем гармонический ряд $\sum_{m=1}^{\infty} \frac{1}{m}$,

который, таким образом, должен быть сходящимся и

иметь сумму $\prod_{i=1}^k \frac{1}{1 - \frac{1}{p_i}}$.

Однако, как известно, гармонический ряд является расходящимся. Получается противоречие, доказывающее неверность предположения о конечности числа простых чисел.

Отметим, что в доказательстве бесконечности числа простых чисел Эйлер сам исходил из рассмотрения введенной им функции

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots + \frac{1}{n^s} + \dots = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

где $s > 1$. В настоящее время эту функцию называют дзета-функцией Эйлера (еще более широко она известна под именем дзета-функции Римана, поскольку Риман первый предпринял глубокие исследования этой функции для комплексных s).

Как известно, указанный ряд при $s > 1$ сходится. Эйлер нашел замечательное тождество, играющее очень важную роль в теории простых чисел, а именно:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

где произведение распространяется по всем простым числам.

Если s стремится к единице, левая сторона последнего равенства беспредельно растет. Это свидетельствует о том, что простых чисел p бесконечно много.

5. Расходимость ряда величин, обратных простым числам.
О «средней плотности» простых чисел

А. Метод Эйлера дает возможность доказать, что ряд величин, обратных простым числам, т. е. ряд

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots = \sum_p \frac{1}{p}$$

является расходящимся.

Это важное предложение, которое гораздо сильнее утверждения о расходимости гармонического ряда

$\sum_{m=1}^{\infty} \frac{1}{m}$, ибо здесь речь идет лишь о части его членов,

дает некоторую характеристику роста простых чисел. Оно показывает, что ряд простых чисел ведет себя в некотором отношении так же, как весь натуральный ряд, в противоположность, например, ряду «полных квадратов» $1^2, 2^2, 3^2, \dots$, обратные величины которого

образуют сходящийся ряд $\sum_{m=1}^{\infty} \frac{1}{m^2}$. Можно поэтому ска-

зать, что простые числа в некотором смысле расположены «гуще», чем полные квадраты.

Докажем расходимость $\sum_p \frac{1}{p}$.

В дальнейшем будем считать, что бесконечность числа простых чисел доказана. Умножая (см. предыдущий пункт) все ряды (1) для $p_i \leq N$, мы получим ряд (2). Произведения $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$ будут при этом содержать все натуральные числа до N включительно, а из натуральных чисел, больших N , только часть (так как среди натуральных чисел $> N$ имеются и такие, которые содержат простые делители, отличные от p_1, p_2, \dots, p_k).¹

¹ Если не сделать оговорку о том, что бесконечность числа простых чисел считается доказанной, то этого нельзя было бы утверждать (см. предыдущий пункт).

Поэтому

$$\prod_{p_i \leq N} \frac{1}{1 - \frac{1}{p_i}} > \sum_{n=1}^N \frac{1}{n}.$$

Но при $N \rightarrow \infty$ в правой части получается расходящийся гармонический ряд. Следовательно, и бесконечное произведение $\prod_{i=1}^{\infty} \frac{1}{1 - \frac{1}{p_i}}$ расходится и имеет зна-

чение $+\infty$. Но тогда расходится и ряд

$$-\sum_{i=1}^{\infty} \ln \left(1 - \frac{1}{p_i}\right),$$

причем его сумма тоже стремится к $+\infty$ ¹.

(Заметим, что $\ln \left(1 - \frac{1}{p_i}\right)$ сами по себе отрицательны.)

¹ Под значением бесконечного произведения

$$\prod_{v=1}^{\infty} a_v = a_1 a_2 a_3 \dots \quad (1)$$

понимают предел последовательности частичных произведений

$$a_1, a_1 \cdot a_2, a_1 \cdot a_2 \cdot a_3, a_1 \cdot a_2 \cdot a_3 \cdot a_4, \dots,$$

если этот предел существует. (В общей теории бесконечных произведений обычно исключают случай, когда один из множителей равен нулю или когда произведение $a_1 \cdot a_2 \dots a_n$ с возрастанием n стремится к нулю.)

В случае положительных сомножителей сходимость произведения (1), очевидно, равносильна сходимости ряда

$$\sum_{v=1}^{\infty} \ln a_v. \quad (II)$$

В самом деле, одновременно с частичными суммами этого ряда стремятся к пределу и частичные произведения $a_1 \cdot a_2 \dots a_n$, и наоборот. Согласно теории бесконечных рядов, впрочем, из того, что

$$\prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i}\right) = 0, \text{ непосредственно следует расходимость ряда } \sum_{i=1}^{\infty} \frac{1}{p_i}.$$

Далее, поскольку $\frac{1}{p_i} < 1$, имеем

$$\begin{aligned}
 -\ln\left(1 - \frac{1}{p_i}\right) &= \frac{1}{p_i} + \frac{1}{2}\left(\frac{1}{p_i}\right)^2 + \frac{1}{3}\left(\frac{1}{p_i}\right)^3 + \dots < \\
 &< \frac{1}{p_i} + \left(\frac{1}{p_i}\right)^2 + \left(\frac{1}{p_i}\right)^3 + \dots = \frac{\frac{1}{p_i}}{1 - \frac{1}{p_i}},
 \end{aligned}$$

причем для $p_i > 2$

$$1 - \frac{1}{p_i} > \frac{1}{2} \text{ и } \frac{\frac{1}{p_i}}{1 - \frac{1}{p_i}} < \frac{\frac{1}{p_i}}{\frac{1}{2}}, \text{ т. е. } \frac{\frac{1}{p_i}}{1 - \frac{1}{p_i}} < 2 \frac{1}{p_i}.$$

Таким образом мы видим, что члены ряда $2 \cdot \sum_{i=1}^{\infty} \frac{1}{p_i}$ (начиная со второго члена) больше соответствующих членов ряда $-\sum_{i=1}^{\infty} \ln\left(1 - \frac{1}{p_i}\right)$. Но последний ряд является расходящимся, следовательно, расходится и ряд $2 \cdot \sum_{i=1}^{\infty} \frac{1}{p_i}$, а также ряд

$$\sum_{i=1}^{\infty} \frac{1}{p_i}.$$

Б. Изучая имеющиеся таблицы простых чисел, легко заметить, что в среднем простые числа встречаются все реже и реже, точнее говоря, что отношение $\frac{\pi(x)}{x}$ — так называемая «средняя плотность» простых чисел в отрезке от 1 до x все время убывает. Эйлер впервые, хотя и не совсем строго, доказал, что при $x \rightarrow \infty$ $\frac{\pi(x)}{x} \rightarrow 0$ или

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0.$$

На доказательстве этого факта, который легко выводится из результатов Чебышева, мы здесь останавливаться не будем.

6. Асимптотический закон распределения простых чисел

Отмеченные факты о распределении простых чисел дают лишь смутное представление об этом сложнейшем вопросе теории чисел.

Ученые начала XIX века поставили перед собой задачу — найти для функции $\pi(x)$ простую, хорошо известную и как можно лучше приближающую ее функцию $f(x)$, такую, чтобы относительная погрешность была как можно меньше, т. е. чтобы отношение $\frac{\pi(x)}{f(x)}$ для беспредельно возрастающих значений x становилось все более и более близким к числу 1, другими словами, чтобы при $x \rightarrow \infty$ $\frac{\pi(x)}{f(x)} \rightarrow 1$, или $\lim_{x \rightarrow \infty} \frac{\pi(x)}{f(x)} = 1$.

Иначе говоря, проблема состояла в том, чтобы найти такую аналитическую функцию $f(x)$, которой $\pi(x)$ равнялась бы асимптотически, или с которой она была бы асимптотически эквивалентна. Употребляя символ асимптотического равенства, предыдущее соотношение записываем следующим образом:

$$\pi(x) \sim f(x).$$

Заметим, что из асимптотического равенства, например предыдущего, следует, что функция $f(x)$ должна быть главным членом в приближенной формуле для $\pi(x)$. Если при этом добавочный член («ошибка») в приближенной формуле равен $R(x)$, то можем писать $\pi(x) = f(x) + R(x)$, или

$$\pi(x) - f(x) = R(x), \text{ где } \frac{R(x)}{f(x)} \rightarrow 0 \text{ при } x \rightarrow \infty.$$

В 1808 году Лежандр на основании исследования таблицы простых чисел (таблица простых чисел к тому времени была составлена до числа 400 000) опубликовал замечательную эмпирическую формулу для приближенного представления функции $\pi(x)$. Лежандр утверждал

дал, что для больших значений x функция $\pi(x)$ приближенно равна

$$\frac{x}{\ln x - B},$$

где B — некоторое постоянное число, равное 1,08366.

Независимо от Лежандра Гаусс, подсчитывая число простых чисел последовательно на каждую тысячу чисел натурального ряда, высказал предположение, что $\pi(x)$ сравнительно мало отличается от

$$\int_2^x \frac{dt}{\ln t}.$$

В целях удобства обозначений этот интеграл, который нельзя выразить элементарными функциями, обычно заменяется «интегральным логарифмом»

$$\text{Li } x = \lim_{\eta \rightarrow +0} \left(\int_0^{1-\eta} + \int_{1+\eta}^x \right) \frac{dt}{\ln t},$$

от которого он отличается на постоянную $\text{Li}2 = 1,04$.

По правилу Лопиталя легко доказать, что

$$\lim_{x \rightarrow \infty} \left(\int_2^x \frac{dt}{\ln t} : \frac{x}{\ln x} \right) = 1.$$

В самом деле,

$$\lim_{x \rightarrow \infty} \left(\int_2^x \frac{dt}{\ln t} : \frac{x}{\ln x} \right) = \lim_{x \rightarrow \infty} \left(\frac{1}{\ln x} : \frac{\ln x - 1}{\ln^2 x} \right) = \lim_{x \rightarrow \infty} \left(\frac{\ln x}{\ln x - 1} \right) = 1.$$

Из доказанного факта следует, что предположения Лежандра и Гаусса приводят к одинаковым асимптотическим оценкам функции $\pi(x)$, а именно:

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \quad \text{и} \quad \lim_{x \rightarrow \infty} \frac{\pi(x)}{\int_2^x \frac{dt}{\ln t}} = 1,$$

или соответственно

$$\pi(x) \sim \frac{x}{\ln x} \quad \text{и} \quad \pi(x) \sim \int_2^x \frac{dt}{\ln t}.$$

Они выражают так называемый *асимптотический закон* распределения простых чисел, который на самом деле имеет место. Однако для теоретического обоснования этого закона Лежандр и Гаусс ничего сделать не сумели.

7. Основные результаты 1-го мемуара П. Л. Чебышева о простых числах

Первым, кто после Евклида добился существенного продвижения в труднейшем вопросе о распределении простых чисел при помощи теоретических исследований, был великий русский математик П. Л. Чебышев. Его результаты по этому вопросу изложены в двух мемуарах о простых числах: «Об определении числа простых чисел, не превосходящих данной величины» (1849) и «О простых числах» (1852).

А. В первом мемуаре Чебышев, исходя из рассмотрения функции Эйлера $\zeta(s)$ при действительных s , получил следующий основной результат: *если $n > 0$ сколь угодно велико и $\alpha > 0$ сколь угодно мало, то будут существовать сколь угодно большие x , для которых*

$$\pi(x) > \int_2^x \frac{dt}{\ln t} - \frac{\alpha x}{\ln^n x},$$

а также сколь угодно большие x (возможно отличающиеся от предыдущих), для которых

$$\pi(x) < \int_2^x \frac{dt}{\ln t} + \frac{\alpha x}{\ln^n x}.$$

Обозначая функции в правых частях этих неравенств соответственно через y_1 и y_2 , сформулированную важную теорему можем выразить также следующим образом: функция $\pi(x)$ растет не медленнее, чем функция y_1 и не быстрее, чем функция y_2 , или, другими словами, нет такого значения x , начиная с которого график функции $\pi(x)$ весь лежит под графиком функции y_1 или над графиком функции y_2 .

Для лучшего уяснения содержания этой теоремы полезно рассмотреть более подробно графическое ее истолкование.

Функция $\text{Li } x = \int_2^x \frac{dt}{\ln t}$, которая для достаточно больших значений x сравнительно мало отличается от функции $\frac{x}{\ln x}$, очевидно, монотонно и неограниченно возрастает; ее график своей вогнутостью направлен к оси x . Значения функции $\frac{\alpha x}{\ln^n x}$, которой определяются отклонения графиков y_1 и y_2 от графика $\int_2^x \frac{dt}{\ln t}$, при небольших значениях x сколь угодно малы, однако при неограниченно возрастающем x тоже неограниченно возрастают. Таким образом, y_1 и y_2 определяют сначала узкую, а затем все расширяющуюся кривую полосу около графика $\int_2^x \frac{dt}{\ln t}$.

Было отмечено, что нет такого значения x , начиная с которого график функции $\pi(x)$ весь лежит под графиком y_1 или над графиком y_2 . Вместе с тем можно также утверждать, что график $\pi(x)$, который состоит из отдельных ступеней, отделяющихся одинаковыми скачками в размере единицы, не может расположиться только вне указанной полосы.

Отсюда следует, что ступени графика $\pi(x)$ должны бесчисленное множество раз входить в полосу между y_1 и y_2 — в этом наглядный смысл теоремы Чебышева.

Графически все это можно иллюстрировать на рис. 5 (в котором мы пока чертим ступени $\pi(x)$, не превышающими график $\text{Li } x$, как это соответствует имеющимся таблицам простых чисел).

Б. При помощи указанной теоремы Чебышев в дальнейшем доказывает, что выражение $B(x) = \ln x - \frac{x}{\pi(x)}$ при $x \rightarrow \infty$ не может иметь предела, отличного от 1 (если таковой вообще существует).

Так как из эмпирической формулы Лежандра следует, что

$$\lim_{x \rightarrow \infty} \left\{ \ln x - \frac{x}{\pi(x)} \right\} = B,$$

то Чебышев и заключает, что формула Лежандра при $x \rightarrow \infty$ не может быть точной, и более подходящей константой является $B = 1$.

На первый взгляд может показаться странным тот факт, что в асимптотическом законе распределения

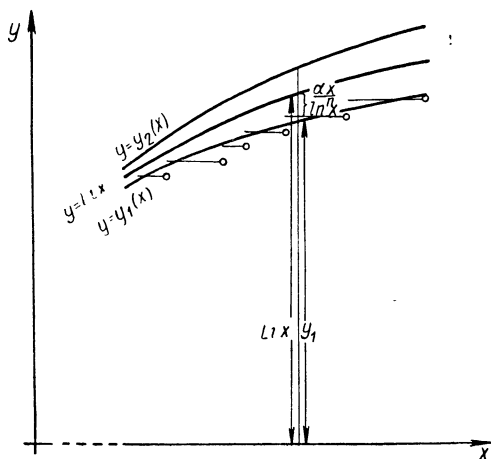


Рис. 5.

простых чисел утверждается, будто $\pi(x) \sim \frac{x}{\ln x}$, в то время как в формуле Лежандра наиболее подходящей константой оказывается $B = 1$, вместо возможного ожидаемого значения $B = 0$. Однако это недоумение необосновано, если учесть, что асимптотический закон распределения простых чисел может быть записан при помощи выражения Лежандра следующим образом:

$$\pi(x) \sim \frac{x}{\ln x - B}.$$

Асимптотический закон допускает различный выбор главного члена в приближенной формуле для $\pi(x)$. Какой из них является наилучшим, можно решить лишь дополнительным исследованием, которое Чебышев и предпринял.

Он доказал, что при выборе в качестве главного члена приближенной формулы для $\pi(x)$ выражения вида

$$\frac{x}{A \ln x - B}$$

«ошибка»

$$|R(x)| = \left| \pi(x) - \frac{x}{A \ln x - B} \right|$$

для достаточно больших x становится меньше $C \cdot \frac{x}{\ln^3 x}$ (где C — постоянное число) только в том случае, если $A = 1$ и $B = 1$.

При рассмотрении таблицы простых чисел, известной во времена Лежандра (т. е. до числа $x = 400\,000$), создается впечатление, что формула Лежандра

$\frac{x}{\ln x - 1,08366}$ в качестве главного члена приближенной

формулы для $\pi(x)$ лучше выражения $\text{Li } x = \int_2^x \frac{dt}{\ln t}$.

x	100	1 000	10 000	100 000
$\frac{x}{\ln x - 1,08366}$	28	171	1 230	9 587
$\pi(x)$	25	168	1 229	9 592
$\text{Li } x$	29	178	1 246	9 630

В действительности это не так: формула $\text{Li } x$ лучше формулы Лежандра и подобных ей.

Однако, как справедливо указал Чебышев, таблицы простых чисел, составленные к тому времени, были слишком малы, чтобы указанное преимущество заметить. В пределах этих таблиц оба выражения мало отличаются друг от друга; но разность их

$$\frac{x}{\ln x - 1,08366} - \int_2^x \frac{dt}{\ln t},$$

имея минимум при $x = e^{\frac{(2,08366)^2}{0,08366}} \approx 1\,247\,646$, после него постоянно возрастает до ∞ и уже при $x > 10\,000\,000$ принимает довольно большое значение. Для таких x

формула $\int_2^x \frac{dt}{\ln t}$ дает куда лучшие приближения к $\pi(x)$,

чем формула Лежандра.

Из отмеченного выше свойства константы B следует, что еще более грубые значения, чем при помощи формулы Лежандра, получаются при пользовании формулой

$$\pi(x) \approx \frac{x}{\ln x}.$$

Однако ею очень удобно пользоваться, в особенности для $x = 10^k$. Тогда

$$\pi(10^k) \approx \frac{10^k}{k \ln 10} = \frac{10^k}{2,303 \cdot k} = \frac{0,434}{k} \cdot 10^{k1}.$$

При $k = 1, 2, 3, 4, 5, 6$ соответственно легко находим следующие приближенные значения для $\pi(10^k)$:

$$4, 22, 145, 1090, 8680, 72300.$$

Их относительная погрешность убывает (сравните с правильными значениями $\pi(x)$ в таблице на стр. 274) и для достаточно большого k может быть сделана сколь угодно малой.

В. Установив, что эмпирическое приближение формулы Лежандра к функции $\pi(x)$ неудовлетворительно, Чебышев далее показал, что если только предел $\pi(x) : \frac{x}{\ln x}$ при $x \rightarrow \infty$ существует, то он должен быть равен 1.

Доказательство этого факта в основных чертах следующее: если взять в основной теореме Чебышева $n = 1$ и разделить в обоих неравенствах левые и правые части на $\frac{x}{\ln x}$, получаем неравенства

$$\frac{\pi(x)}{\frac{x}{\ln x}} > \frac{\int_2^x \frac{dt}{\ln t}}{\frac{x}{\ln x}} - \alpha \quad \text{и} \quad \frac{\pi(x)}{\frac{x}{\ln x}} < \frac{\int_2^x \frac{dt}{\ln t}}{\frac{x}{\ln x}} + \alpha.$$

¹ О вычислении точных значений $\pi(x)$ далеко за пределами таблиц см., например (13).

Можно утверждать, что существуют сколь угодно большие x , для которых

$$\left| \frac{\frac{\pi(x)}{x}}{\frac{1}{\ln x}} - \frac{\frac{\int_2^x \frac{dt}{\ln t}}{x}}{\frac{1}{\ln x}} \right| < \alpha.$$

Если далее учесть, что $\left(\int_2^x \frac{dt}{\ln t} : \frac{x}{\ln x} \right)$ стремится

к пределу 1, то из последнего неравенства явствует, что существуют сколь угодно большие x , для которых $\pi(x) : \frac{x}{\ln x}$ отличается от 1 на сколь угодно малое положительное α .

Из этого следует, что если предел существует, то он не может отличаться от единицы. (Мы не знаем, как дело обстоит для *всех* сколь угодно больших x . Если бы для всех сколь угодно больших x $\pi(x) : \frac{x}{\ln x}$

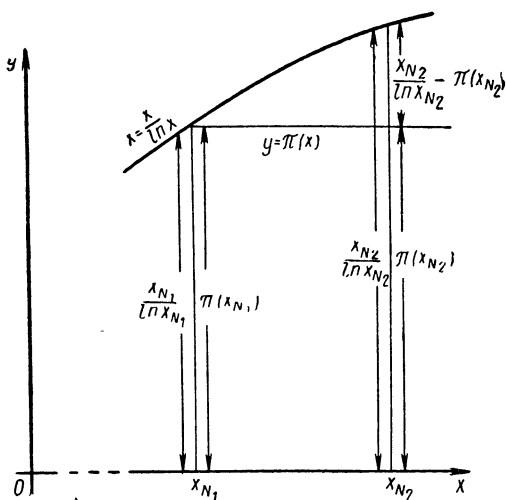


Рис. 6.

отличалось от 1 на сколь угодно малое положительное α , то мы могли бы утверждать, что предел $\pi(x) : \frac{x}{\ln x}$ существует и равен единице).

Графически картина этого примерно следующая: на «ступенях» $\pi(x)$ для сколь угодно больших x существуют точки, расположенные вблизи графика $\frac{x}{\ln x}$. Поскольку существуют сколь угодно большие интервалы натурального ряда, не содержащие простых чисел, «ступени» могут сделаться любой длины и значительно удалиться от графика $\frac{x}{\ln x}$. Вместе с тем надо иметь в виду, что такие очень длинные «ступени» появляются лишь тогда, когда само $\pi(x)$ очень велико. Поэтому не исключено, что несмотря на абсолютно значительное удаление «ступени» $\pi(x)$ от $\frac{x}{\ln x}$, отношение соответствующих ординат будет сравнительно мало отличаться от единицы, а в пределе при $x \rightarrow \infty$ будет равно единице. Иллюстрацией всего сказанного может служить схематический рис. 6, на котором изображена часть графика $\pi(x)$ и функций $\frac{x}{\ln x}$ для больших значений x .

8. Основные результаты 2-го мемуара П. Л. Чебышева о простых числах.

Неравенство Чебышева и его упрощенное доказательство

Переходим к рассмотрению основных результатов 2-го мемуара П. Л. Чебышева.

А. Поводом для написания второго мемуара явился так называемый *постулат Бертрана*. Незадолго до этого известный французский математик Бертран в своих исследованиях по теории групп встретился с необходимостью доказать эмпирически подтверждавшийся факт, что между n ($n > 3$) и $2n - 2$ всегда имеется хотя бы одно простое число. Все попытки Бертрана, а также других математиков, доказать это предложение оставались безуспешными.

В своей второй работе (1852) Чебышев доказал постулат Бертрана¹. Однако этим не исчерпывается значение выдающейся работы Чебышева. Главное значение мемуара «О простых числах» состоит в тех элементарных и вместе с тем сильных методах, которые в нем даны и использованы для оценок функции $\pi(x)$, а также других функций. Из оценок Чебышева вытекает, что для достаточно больших x выполняются неравенства

$$0,92129 < \frac{\pi(x)}{\frac{x}{\ln x}} < 1,10555,$$

или

$$0,92129 \frac{x}{\ln x} < \pi(x) < 1,10555 \frac{x}{\ln x},$$

которые впредь будем называть *неравенствами Чебышева*.

Графически неравенства означают, что для достаточно больших x график функции $\pi(x) : \frac{x}{\ln x}$ лежит между параллелями $y_1 = 0,92129$ и $y_2 = 1,10555$ (см. рис. 7).

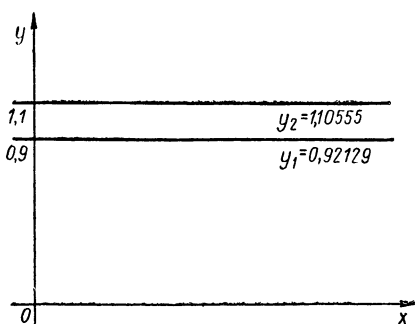


Рис. 7.

Неравенствами Чебышева впервые было строго доказано, что $\pi(x)$ при $x \rightarrow \infty$ растет как функция $\frac{x}{\ln x}$. На основании первого мемуара этого еще нельзя было утверждать.

¹ В настоящее время доказано, что для натуральных $n > 5$ между n и $2n$ содержатся по меньшей мере два простых числа.

Удовлетворяясь более грубыми результатами, чем у Чебышева, мы дадим упрощенное изложение метода Чебышева, а именно: докажем следующую теорему: *Для всякого действительного $x \geq 2$ имеют место неравенства*

$$c \cdot \frac{x}{\ln x} < \pi(x) < C \frac{x}{\ln x},$$

где $0 < c < 1 < C$.

Б. Для оценки $\pi(x)$ сверху введем функцию Чебышева $\theta(x)$, с которой $\pi(x)$ тесно связана. Эта функция определяется соотношением

$$\theta(x) = \sum_{p \leq x} \ln p,$$

где суммирование распространяется на все простые числа $\leq x$.

Из определения видно, что число слагаемых $\ln p$ в $\theta(x)$ равно

$$\sum_{p \leq x} 1 = \pi(x).$$

Пример. Пусть $x = 10$; запишем все натуральные числа до 10: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

Очевидно, $\theta(10) = \sum_{p \leq 10} \ln p = \ln 2 + \ln 3 + \ln 5 + \ln 7$.

Установим связь между $\pi(x)$ и $\theta(x)$.

При $x > 1$ $\theta(x) = \sum_{p \leq x} \ln p \geq \sum_{\substack{p \leq x \\ \sqrt{x} < p \leq x}} \ln p \geq (\pi(x) - \pi(\sqrt{x})) \cdot \ln \sqrt{x}$,

так как в $\sum_{p \leq x} \ln p$ при $x > 1$ наименьшее слагаемое $\ln \sqrt{x}$, а число слагаемых $\sum_{\substack{p \leq x \\ \sqrt{x} < p \leq x}} 1 = \pi(x) - \pi(\sqrt{x})$.

Но так как

$$\pi(x^{\frac{1}{2}}) < x^{\frac{1}{2}},$$

то

$$\theta(x) > \frac{1}{2} (\pi(x) - \sqrt{x}) \cdot \ln x,$$

откуда

$$\frac{2}{\ln x} \theta(x) > \pi(x) - \sqrt{x}$$

и

$$\pi(x) < \frac{2}{\ln x} \theta(x) + \sqrt{x}. \quad (1)$$

В. Оценим теперь $\theta(x)$ и используем результат для последующей оценки $\pi(x)$ сверху.

Рассмотрим число

$$N = C_{2n}^n = \frac{(n+1)(n+2)\dots 2n}{1 \cdot 2 \dots n} = \frac{(2n)!}{(n!)^2}.$$

Это число целое, а так как оно является членом биномиального разложения $(1+1)^{2n} = 2^{2n}$, то

$$N < 2^{2n}.$$

N делится на все простые числа p в интервале $n < p \leq 2n$, так как эти простые числа входят сомножителями в его числитель, но не могут входить в знаменатель, который содержит числа сегмента $[1, n]$. Поэтому N делится также на произведение указанных простых чисел.

Обозначим простые множители в интервале $n < p \leq 2n$ через p_1, p_2, \dots, p_k . Тогда имеем

$$p_1 \cdot p_2 \dots p_k = \prod_{n < p \leq 2n} p \leq N < 2^{2n}.$$

Следовательно,

$$\sum_{n < p \leq 2n} \ln p < 2n \ln 2.$$

Но так как

$$\sum_{n < p \leq 2n} \ln p = \sum_{p \leq 2n} \ln p - \sum_{p \leq n} \ln p = \theta(2n) - \theta(n),$$

то

$$\theta(2n) - \theta(n) < 2n \ln 2.$$

Это неравенство остается верным и в том случае, когда простых чисел p_1, p_2, \dots, p_k вовсе не существует, так как в этом случае $\theta(2n) - \theta(n) = 0$.

Полагая

$$n = 2^{k-1}, 2^{k-2}, \dots, 1, \text{ где } k = 1, 2, \dots,$$

имеем

$$\begin{aligned}\theta(2^k) - \theta(2^{k-1}) &< 2^k \ln 2, \\ \theta(2^{k-1}) - \theta(2^{k-2}) &< 2^{k-1} \ln 2, \\ &\vdots \\ \theta(2) - \theta(1) &< 2 \cdot \ln 2.\end{aligned}$$

Суммируя эти неравенства и учитывая, что $\theta(1) = 0$, получаем

$$\theta(2^k) < (2^k + 2^{k-1} + \dots + 2) \ln 2 = 2 \cdot (2^k - 1) \cdot \ln 2.$$

Следовательно,

$$\theta(2^k) < 2^{k+1} \cdot \ln 2. \quad (2)$$

Пусть теперь $x \geq 1$; тогда x удовлетворяет неравенствам

$$2^{k-1} \leq x < 2^k,$$

где k — некоторое целое ≥ 1 .

Так как при $x_1 = x_2$ $\theta(x_1) = \theta(x_2)$, а при $x_1 < x_2$ $\theta(x_1) \leq \theta(x_2)$, то на основании (2) получаем

$$\theta(x) \leq \theta(2^k) < 2^{k+1} \cdot \ln 2.$$

Но

$$2^{k+1} = 4 \cdot 2^{k-1} \leq 4x;$$

следовательно, $\theta(x) < 4x \cdot \ln 2$.

При $0 < x < 1$ это неравенство тоже выполняется. Поэтому для $x > 0$ имеем

$$\theta(x) < C_1 \cdot x, \quad \text{где } C_1 = 4 \ln 2. \quad (3)$$

Теперь можно оценить $\pi(x)$ сверху.

Учитывая (3), находим из (1)

$$\begin{aligned}\pi(x) &< \frac{2}{\ln x} \cdot 4 \ln 2 \cdot x + \sqrt{x}, \\ \pi(x) &< \frac{x}{\ln x} \left(8 \ln 2 + \frac{\ln x}{\sqrt{x}} \right).\end{aligned}$$

Легко убедиться, что при $x \geq 2$ выражение $\frac{\ln x}{\sqrt{x}}$ имеет наибольшее значение при $x = e^2$, а именно $\frac{2}{e} \approx 0,7$.

Итак, при $x \geq 2$

$$\pi(x) < C \cdot \frac{x}{\ln x}, \quad (4)$$

где $C = 8 \ln 2 + 0,7 = 8 \cdot 0,69 + 0,7 \approx 6,2$;
этим часть теоремы доказана.

Г. Оценим теперь $\pi(x)$ снизу.

Число $N = \frac{(2n)!}{(n!)^2}$ можно представить в виде

$$N = \prod_{p \leq 2n} p^{\nu_p},$$

где по § 3 настоящей гл.

$$\nu_p = \left[\frac{2n}{p} \right] + \left[\frac{2n}{p^2} \right] + \dots - 2 \left(\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \dots \right)$$

и каждая из этих сумм обрывается на $t_{2n,p}$ -ом члене

$$\left(t_{2n,p} = \left[\frac{\ln 2n}{\ln p} \right] \geq t_{n,p} \right).$$

При этом мы имеем в виду, что при $p > n$, или $t > t_{n,p}$ справедливо соотношение $\left[\frac{n}{p^t} \right] = 0$.

Поэтому

$$\nu_p = \sum_{t=1}^{t_{2n,p}} \left(\left[\frac{2n}{p^t} \right] - 2 \left[\frac{n}{p^t} \right] \right).$$

Но $[2y] - 2[y]$ равно либо нулю, либо единице. На самом деле, пусть

$$m \leq y < m + 1.$$

Если при этом

$$1) \ y < m + \frac{1}{2}, \text{ то } [2y] - 2[y] = 2m - 2m = 0;$$

$$2) \ y \geq m + \frac{1}{2}, \text{ то } [2y] - 2[y] = (2m + 1) - 2m = 1.$$

Следовательно,

$$\nu_p \leq t_{2n,p}$$

и

$$N \leq \prod_{p \leq 2n} p^{t_{2n,p}}.$$

В правой части имеются $\pi(2n)$ сомножителей $p^{t_{2n,p}}$, из которых каждый $\leq 2n$, причем знак равенства может

выполняться лишь в одном случае (см. п. 3 § 3 настоящей главы); поэтому

$$(2n)^{\pi(2n)} > N,$$

откуда

$$\pi(2n) \ln 2n > \ln N.$$

Но число N можно представить также и в следующем виде:

$$N = \frac{2n \cdot (2n-1) \dots 2 \cdot 1}{n^2 \cdot (n-1)^2 \dots 2^2 \cdot 1^2} = \frac{2n(2n-1)}{n^2} \cdot \frac{(2n-2)(2n-3)}{(n-1)^2} \dots \frac{2 \cdot 1}{1^2},$$

$$\begin{aligned} N &= 4^n \left(1 - \frac{1}{2n}\right) \cdot \left(1 - \frac{1}{2(n-1)}\right) \dots \left(1 - \frac{1}{2}\right) = \\ &= 4^n \cdot \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \dots \frac{2n-1}{2n}, \end{aligned}$$

$$N > 4^n \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \frac{4}{5} \dots \frac{2n-1}{2n} = \frac{4^n}{2n} = \frac{2^{2n}}{2n}.$$

Итак,

$$N > \frac{2^{2n}}{2n},$$

$$\text{следовательно, } \ln N > 2n \ln 2 - \ln 2n \quad (5)$$

$$\text{и} \quad \pi(2n) \ln 2n > 2n \ln 2 - \ln 2n. \quad (6)$$

Пусть теперь

$$n = \left[\frac{1}{2} x \right], \quad x > 2,$$

так что

$$\left[\frac{1}{2} x \right] \leq \frac{1}{2} x < \left[\frac{1}{2} x \right] + 1,$$

$$n \leq \frac{1}{2} x < n + 1,$$

$$2n \leq x < 2n + 2,$$

$$x - 2 < 2n.$$

Тогда, учитывая, что при

$$x_1 \geq x_2 \quad \pi(x_1) \geq \pi(x_2) \quad \text{и} \quad \ln x_1 \geq \ln x_2,$$

получаем из (6)

$$\pi(x) \ln x > (x-2) \ln 2 - \ln x,$$

$$\begin{aligned}
\text{откуда } \pi(x) &> \frac{(x-2) \ln 2 - \ln x}{\ln x}, \\
\pi(x) &> \frac{x \ln 2 - \ln 4x}{\ln x}, \\
\pi(x) &> \frac{x}{\ln x} \left(\ln 2 - \frac{\ln 4x}{x} \right). \tag{7}
\end{aligned}$$

Если $x=8$, то

$$\begin{aligned}
\frac{\ln 4x}{x} &= \frac{\ln 2^5}{8} = \frac{5 \ln 2}{8}, \text{ а} \\
\ln 2 - \frac{\ln 4x}{x} &= \frac{3}{8} \ln 2.
\end{aligned}$$

При $x > 8$ значение $\frac{\ln 4x}{x}$ убывает, поэтому величина в скобках будет увеличиваться; тем не менее (7) остается в силе, так как оно имеет место для всех $x > 2$.

Таким образом, мы можем утверждать, что при $x \geq 8$

$$\pi(x) > \frac{3}{8} \ln 2 \cdot \frac{x}{\ln x}.$$

Но и для $2 \leq x < 8$ последнее неравенство остается в силе.

В самом деле, для таких x $\pi(x)$ принимает значения ≥ 1 (причем знак равенства имеем для $x=2$); с другой стороны, $\frac{x}{\ln x}$, достигая в интервале $[2, 8]$ для $x=e$ своего минимума, в остальных точках будет $\leq \frac{8}{3 \ln 2}$ (причем знак равенства имеем для $x=8$). Следовательно,

$$\frac{3}{8} \ln 2 \cdot \frac{x}{\ln x} \leq \frac{3}{8} \ln 2 \cdot \frac{8}{3 \ln 2} = 1 \leq \pi(x).$$

Учитывая замечания в скобках, имеем и для интервала $[2, 8]$

$$\pi(x) > \frac{3}{8} \ln 2 \cdot \frac{x}{\ln x}.$$

Поэтому имеем окончательно для $x \geq 2$

$$\pi(x) > c \cdot \frac{x}{\ln x}, \quad \text{где } c = \frac{3}{8} \ln 2 \approx 0,26. \tag{8}$$

Этим доказана вторая часть теоремы и вместе с тем вся теорема.

Заметим в заключение, что из теоремы Чебышева непосредственно вытекает теорема Эйлера о том, что $\frac{\pi(x)}{x} \rightarrow 0$, когда $x \rightarrow \infty$.

9. Оценка роста n -го простого числа на основании неравенства Чебышева

Из неравенства Чебышева для $\pi(x)$ вытекает оценка роста n -го простого числа p_n , а именно: пусть p_n — n -ое простое число и $n \geq 2$, тогда

$$c_1 \cdot n \ln n < p_n < C_1 n \cdot \ln n$$

(необходимо принять $n \geq 2$, так как $\ln 1 = 0$).

Доказательство. При $x = p_n$ $\pi(p_n) = n$, и неравенство Чебышева принимает следующий вид:

$$c \frac{p_n}{\ln p_n} < n < C \frac{p_n}{\ln p_n}. \quad (1)$$

Из правой части (1) следует

$$p_n > \frac{1}{C} n \ln p_n, \quad \text{но } \ln p_n > \ln n,$$

поэтому

$$p_n > \frac{1}{C} n \ln n. \quad (2)$$

Из левой части (1) следует

$$p_n < \frac{1}{c} n \ln p_n, \quad (3)$$

а также

$$\ln p_n - \ln \frac{\ln p_n}{c} < \ln n. \quad (4)$$

Но для достаточно больших n

$$\ln \frac{\ln p_n}{c} < \frac{1}{2} \ln p_n, \quad (5)$$

или $\frac{\ln p_n}{c} < \sqrt{\ln p_n}$, или $\frac{\ln p_n}{\sqrt{\ln p_n}} < c$, так как $\lim_{n \rightarrow \infty} \frac{\ln p_n}{\sqrt{\ln p_n}} = 0$.

Поэтому из (4) для достаточно больших n следует

$$\ln p_n - \frac{1}{2} \ln p_n < \ln n,$$

или

$$\frac{1}{2} \ln p_n < \ln n,$$

или

$$\ln p_n < 2 \ln n. \quad (6)$$

Учитывая (6), для достаточно больших n из (3) получаем

$$p_n < \frac{1}{c} n \cdot 2 \ln n,$$

или

$$p_n < \frac{2}{c} n \ln n. \quad (7)$$

При увеличении в достаточной мере постоянной $\frac{2}{c}$ (7) останется в силе для всех $n \geq 2$. Меняя обозначения для постоянных, из (2) и (7) получим

$$c_1 n \ln n < p_n < C_1 n \ln n. \quad (8)$$

Отметим еще: 1) для достаточно больших n из (6) следует оценка $p_n < n^2$;

2) из (8) легко доказать расходимость ряда величин, обратных простым числам.

10. О доказательствах закона распределения простых чисел

Выдающиеся результаты Чебышева в вопросе о распределении простых чисел произвели на современников очень сильное впечатление. Об этом, например, ярко свидетельствуют слова выдающегося английского математика Сильвестра, который в 1881 году предлагал для дальнейших успехов теории чисел ждать, пока родится некто настолько же превосходящий Чебышева своею проницательностью и вдумчивостью, насколько Чебышев превосходил этими умственными качествами обыкновенных людей, или слова выдающегося немецкого математика Э. Ландау (1877—1938), который в своей специальной работе, посвященной распределению простых чисел, в 1909 году писал: «Первый после Евклида, кто пошел правильным путем для решения проблемы о простых числах и достиг важных результатов, был Чебышев». Однако достижения Чебышева были еще недостаточны для того, чтобы сделать последний

шаг в доказательстве асимптотического закона распределения простых чисел, а именно: чтобы доказать существование $\lim_{x \rightarrow \infty} \left(\pi(x) : \frac{x}{\ln x} \right)$. И хотя после Чебышева были найдены еще более точные границы (так, например, Сильвестр нашел, что для достаточно больших x $0,95695 < \frac{\pi(x)}{\frac{x}{\ln x}} < 1,04423$) для отношения

$\pi(x) : \frac{x}{\ln x}$ при достаточно больших x , все же попытки доказать этим путем асимптотический закон оказались безуспешными.

Ключ к решению проблемы оказался заложенным в исследованиях знаменитого немецкого математика Б. Римана, который в своем мемуаре 1859 года указал на возможность получения глубоких результатов по распределению простых чисел при помощи исследования дзета-функции $\zeta(s)$ для комплексных значений переменной¹ $s = \sigma + \tau i$. (Чебышев в свое время исследовал эту функцию для действительных переменных.) Рيمان своим методом ни одного арифметического результата не получил, однако, воспользовавшись методом Римана, французский математик Ж. Адамар и бельгийский математик Валле-Пуссен в 1896 году, независимо друг от друга, доказали существование предела для $\pi(x) : \frac{x}{\ln x}$.

До недавнего времени все доказательства асимптотического закона базировались на более или менее глубоко изучении поведения функции $\zeta(s)$.

Только в 1949 году попытка элементарного доказательства увенчалась успехом. Эта заслуга принадлежит датскому математику А. Сельбергу и венгерскому математику П. Эрдешу. Доказательство было упрощено другими математиками. Наиболее простое доказатель-

¹ Рيمان высказал предположение, что все нетривиальные нули $\zeta(s)$ лежат на прямой $\sigma = \frac{1}{2}$. Эта так называемая гипотеза Римана до сих пор не доказана и не опровергнута. Однако известно, что из ее справедливости следовали бы многие замечательные теоремы о простых числах.

ство дано советскими математиками А. Г. Постниковым и Н. П. Романовым (см. (48)).

Отметим в заключение, что из асимптотического закона распределения простых чисел легко вывести асимптотическую оценку для n -го простого числа p_n :

$$p_n \sim n \ln n.$$

11. Об оценках добавочного члена в приближенном представлении $\pi(x)$

После открытия асимптотического закона распределения простых чисел стал актуальным вопрос об оценке добавочного члена

$$\pi(x) - \int_2^x \frac{dt}{\ln t}$$

как по абсолютной величине, так и по знаку.

Если посмотреть в таблицы для $\pi(x)$ и $\text{Li } x$, то замечаем, что для всех приведенных значений $\pi(x) < \text{Li } x$.

До 1914 года существовала уверенность, что такое соотношение имеет место для всех x . Но в 1914 году английский математик Литлвуд доказал, что при достаточном расширении таблиц в конце концов встре-

x	$\pi(x)$	$\text{Li } x$
1 000	168	178
10 000	1 229	1 246
50 000	5 133	5 167
100 000	9 592	9 630
500 000	41 538	41 606
1 000 000	78 498	78 628
2 000 000	148 933	149 055
5 000 000	348 513	348 638
10 000 000	664 579	664 918
20 000 000	1 270 607	1 270 905
90 000 000	5 216 954	5 217 810
100 000 000	5 761 455	5 762 209
1 000 000 000	50 847 534	50 849 235

тятся значения x , для которых $\pi(x) > \text{Li } x^1$, что вообще разность

$$\pi(x) - \text{Li } x$$

бесчисленное множество раз меняет свой знак в промежутке от $x=2$ до $x=\infty$. Этим факт колебания функции $\pi(x)$ около $\text{Li } x$, о котором идет речь в основной теореме Чебышева, получил свою окончательную формулировку. Вместе с тем отсюда следует, что, представляя себе мысленно графики функций $\pi(x)$ и $\text{Li } x$, нужно считать, что существуют сколь угодно большие x , для которых ступени $\pi(x)$ пересекают линию $y = \text{Li } x$.

Вопросом о том, с какой степенью точности функция $\int_2^x \frac{dt}{\ln t}$ представляет $\pi(x)$, занимались и сам Чебышев, а также Адамар, Валле-Пуссен, Харди и Литлвуд и другие ученые; этим вопросом занимаются и в настоящее время советские ученые. Наилучшие результаты в этом направлении были получены на основе применения созданного И. М. Виноградовым метода оценки тригонометрических сумм (см. § 5) Н. Г. Чудаковым (в 1936 г.), Е. Титчмаршем, Н. М. Коробовым и самим И. М. Виноградовым, который в 1958 г. доказал, что в равенстве

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + R(x)$$

добавочный член $|R(x)| < c_1 \cdot x \cdot e^{-c_2 (\ln x)^\mu}$, где c_1 и c_2 положительные постоянные, а $\mu = \frac{3}{5} + \varepsilon$.

Применяя тот же метод, Чудакову в 1936 г. удалось также значительно уменьшить те границы, в пределах которых можно утверждать наличие хотя бы одного простого числа. До этого немецким математиком Х. Хейльброном в 1933 г. было установлено, что в последовательности

$$1^{250}, 2^{250}, 3^{250}, \dots, n^{250}, (n+1)^{250}, \dots,$$

¹ Такое значение до сих пор неизвестно, однако Скъюз установил, что оно меньше, чем $10^{10} 10^{10^3}$.

начиная с некоторого $n = n_0$, между двумя ее соседними членами лежит хотя бы одно простое число. Чудакову удалось заменить эту последовательность более тесной:

$$1^4, 2^4, 3^4, \dots, n^4, (n+1)^4, \dots,$$

имеющей тем не менее аналогичное свойство.

Впоследствии английскому математику А. Е. Ингаму в 1937 г. удалось еще более уточнить этот результат, заменив четвертые степени кубами.

Из результатов Ингама следует даже, что число простых чисел между n^3 и $(n+1)^3$ стремится вместе с n к бесконечности.

12. О распределении простых чисел в арифметической прогрессии

Проблема о распределении простых чисел в натуральном ряду получает дальнейшее развитие в вопросе распределения простых чисел в арифметических прогрессиях и других числовых последовательностях.

Уже в 1788 г. Лежандр высказал предположение, что в каждой арифметической прогрессии

$$l, l+k, l+2k, \dots \quad (1)$$

с общим членом $kx+l$, где k и l — целые взаимно простые числа, а $x=0, 1, 2, \dots$, содержится бесконечное множество простых чисел (другими словами, при указанных условиях относительно k , x и l существует бесконечно много простых чисел вида $kx+l$).

Однако лишь в 1837 г. немецкий математик Лежен Дирихле сумел доказать эту теорему. Доказательство его для общего случая является весьма сложным. Элементарное доказательство дано А. Сельбергом в 1949 году, затем советским математиком А. О. Гельфондом. Наиболее простое доказательство дал швейцарский математик Е. Трост (см. (13)).

Для отдельных частных случаев теорема Дирихле доказывается просто. Докажем, например, что существует бесконечно много простых чисел вида $4n+1$.

Допустим противное, т. е. что простых чисел такого вида имеется лишь конечное множество, а имен-

но, q_1, q_2, \dots, q_k . Тогда число $x^2 + 1 = 4(q_1 \cdot q_2 \cdot \dots \cdot q_k)^2 + 1$, также имеющее вид $4n + 1$, должно быть составным, а так как оно не делится ни на одно из чисел q_i , оно должно иметь простой делитель $p = 4n + 3$, или $x^2 + 1 \equiv 0 \pmod{p}$, или $x^2 \equiv -1 \pmod{p}$, т. е. $\left(\frac{-1}{p}\right) = 1$,

что невозможно, когда $p = 4n + 3$.

Полученное противоречие доказывает наше утверждение.

Аналогично получается, что существует бесконечно много простых чисел вида $4n + 3$ и $6n + 5$.

Следует отметить, что уже много лет назад была поставлена проблема о наименьшем простом числе в арифметической прогрессии (1). Эту проблему качественно решил выдающийся ленинградский математик Ю. В. Линник. В 1944 г. он доказал, что в такой прогрессии (при $0 < l < k$) содержится простое число $p < k^c$, где c — абсолютная константа (не зависящая от k)¹.

Отметим в заключение, что исследования относительно содержания простых чисел в последовательности чисел, которая получается, когда в квадратичной функции $ax^2 + bx + c$ x пробегает все натуральные значения, даже для частного случая функции $x^2 + 1$, до сих пор не имели успеха.

Упражнения

270. Пользуясь приближенной формулой $\pi(x) \approx \frac{x}{\ln x}$, найти:

1) $\pi(10^7)$; 2) $\pi(10^8)$.

271. Доказать, что $\pi(x) = \pi(\sqrt{x}) - 1 + \varphi(x; p_1 p_2 \dots p_r)$, где p_1, p_2, \dots, p_r — последовательность простых чисел $\leq \sqrt{x}$, а $\varphi(x; p_1 p_2 \dots p_r)$ имеет значение, указанное в задаче 267.

272. Пользуясь формулой, установленной в предыдущей задаче, найти $\pi(120)$.

273. Доказать, что существует бесконечно много простых чисел вида $4n + 3$.

274. Доказать, что существует бесконечно много простых чисел вида $6n + 5$.

275. Доказать, что существует бесконечно много простых чисел вида $6n + 1$.

¹ В 1958 г. китайский математик Пан Чен-тонг, пользуясь методом Ю. В. Линника, показал, что $c \leq 5448$, а в 1965 г. Чен-ин-рун доказал, что $c \leq 777$

§ 5. Аддитивные проблемы теории чисел

1. Примеры аддитивных задач: проблемы Гольдбаха — Эйлера, Варинга и Харди — Литлвуда

1. Аддитивными проблемами теории чисел называют такие задачи, в которых рассматривается составление целых чисел из слагаемых определенного вида.

Требования, которые налагаются на слагаемые, часто связаны с их мультипликативным представлением, т. е. с их представлением в виде произведения простых сомножителей.

В таких аддитивных задачах исследуются связи, которые существуют между свойствами целых чисел относительно умножения (мультипликативные свойства) и их свойствами относительно сложения (аддитивные свойства). Эти связи имеют весьма сложный характер. Стремление установить их привело к ряду основных проблем теории чисел, которые объединяются в одно большое направление аддитивных проблем. Несмотря на простоту в формулировках, эти проблемы для своего решения очень часто требуют невероятных усилий.

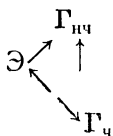
2. Одной из таких проблем является знаменитая проблема Гольдбаха. Она была поставлена в 1742 году Петербургским академиком Х. Гольдбахом в письме к Эйлеру и заключается в утверждении, что *всякое целое число, большее или равное 6, может быть представлено в виде суммы трех простых чисел*. Эйлер в ответе выразил уверенность в справедливости теоремы, что каждое четное число, превосходящее 2, есть сумма двух простых¹.

¹ Утверждения Гольдбаха и Эйлера даны в тексте с некоторыми уточнениями. Фактически в письме Гольдбаха к Эйлеру от 7 июня 1742 г. мы находим следующее замечание: «Кажется, по крайней мере, что каждое число, большее единицы, является суммой трех простых чисел».

В ответном письме от 30 июня 1742 г. Эйлер в этой связи писал: «Но что каждое число есть сумма двух простых чисел, я считаю совершенно справедливой теоремой, несмотря на то, что я ее доказать не могу».

Извлечения из писем цитируются в переводе по Д. А. Граве (8), стр. 18—19.

Если расчленить утверждение Гольдбаха на два отдельных утверждения для четных ($\Gamma_{\text{ч}}$) и нечетных чисел ($\Gamma_{\text{нч}}$), тогда зависимость между ними, а также между ними и гипотезой Эйлера (\mathcal{E}) представляется, очевидно, следующей схемой:



где стрелочка означает — «вытекает». В самом деле:

1) Если к каждому из четных чисел ≥ 4 прибавить простое число 2, то получатся все четные числа ≥ 6 . Отсюда видно, что гипотеза Эйлера о том, что всякое четное число ≥ 4 является суммой двух простых чисел, приводит нас к выводу, что всякое четное число ≥ 6 можно представить в виде суммы трех простых чисел, т. е. к утверждению Гольдбаха для четных чисел.

С другой стороны, исходя из гипотезы Гольдбаха для четных чисел, мы должны, очевидно, предположить, что одно из слагаемых является четным простым числом, т. е. равно 2. В таком случае мы можем утверждать, что всякое четное число ≥ 4 является суммой двух простых чисел.

Мы получили утверждение Эйлера. Итак, утверждения Гольдбаха для четных чисел и Эйлера эквивалентны.

2) Из гипотезы Эйлера (или эквивалентной ей гипотезы Гольдбаха для четных чисел), которая говорит о том, что всякое четное число ≥ 4 есть сумма двух простых чисел, можно сделать вывод, что всякое нечетное число > 6 представляется в виде суммы трех простых чисел.

Для этого достаточно к каждому из четных чисел ≥ 4 прибавить по тройке.

Мы получили утверждение Гольдбаха для нечетных чисел. Вместе с тем последний вывод показывает, что гипотеза Гольдбаха равносильна с гипотезой Гольдбаха для четных чисел (или с эквивалентной ей гипотезой Эйлера).

В то же время необходимо подчеркнуть, что из гипотезы Гольдбаха для нечетных чисел еще не следует гипотеза Эйлера; из нее лишь следует, что для любого четного числа ≥ 10 достаточно 4 простых слагаемых.

Отметим еще в заключение, что, ограничиваясь рассмотрением четных чисел ≥ 6 и нечетных ≥ 9 , утверждение Эйлера и утверждение Гольдбаха для нечетных чисел можно соответственно сформулировать следующим образом:

Утверждение Эйлера: всякое четное число ≥ 6 есть сумма двух нечетных простых чисел.

Утверждение Гольдбаха для нечетных чисел: всякое нечетное число ≥ 9 есть сумма трех нечетных простых чисел.

Легко заметить также, что гипотезу Гольдбаха можно выразить так: всякое целое число, превосходящее 1, есть сумма не более чем трех простых чисел.

В течение почти что двух столетий попытки решить проблему Гольдбаха оставались безуспешными. В 1912 году на международном конгрессе Э. Ландау сделал даже в связи с этой проблемой пессимистический вывод: «Проблема Гольдбаха превосходит силы современной математики».

3. Другой знаменитой аддитивной проблемой является проблема Варинга. Ее выдвинул английский математик Э. Варинг в 1770 г.: *для любого целого числа $n \geq 2$ существует такое натуральное $g = g(n)$, что всякое натуральное число N можно представить в виде*

$$N = x_1^n + x_2^n + \dots + x_r^n, \quad x_i \geq 0, \quad (1)$$

т. е. как сумму g целых неотрицательных (или не более чем g целых положительных) n -х степеней.

Надо обратить внимание на то, что число слагаемых зависит только от показателя n и не зависит от представляемого числа N . В противном случае утверждение теоремы становится совершенно тривиальным, так как любое натуральное число N можно, например, выразить как сумму N единиц и вместе с тем как сумму n -х степеней единицы, поскольку $1 = 1^n$.

С другой стороны, нетрудно понять, что проблему Варинга в принципе (т. е. как теорему существования) достаточно решить для всех достаточно больших N , так как если для представления натуральных $N > N_0$ (т. е. достаточно больших N) в форме (1) достаточно r слагаемых, то для любого N потребуется не более чем r' таких слагаемых, где r' не превосходит наибольшее из чисел r и N_0 . В самом деле, любое натуральное число $N \leq N_0$ можно, во всяком случае, представить как сумму N n -х степеней единицы.

Заметим, однако, с самого начала, что вопрос о том, каково наименьшее значение для числа r слагаемых в (1), является, конечно, в проблеме Варинга наиболее интересным. Если речь идет о представлении любого N , то оно обозначается через $g(n)$; если о достаточно больших N , то через $G(n)$.

Еще в XVIII в. частный случай проблемы Варинга для $n = 2$ был доказан Лагранжем. Для этого частного случая теорема Лагранжа формулируется так: всякое натуральное число представляется в виде суммы не более четырех квадратов, т. е. $g(2) = 4$.

Например,

$$\begin{aligned} 27 &= 4^2 + 3^2 + 1^2 + 1^2, \\ 250 &= 14^2 + 7^2 + 2^2 + 1^2. \end{aligned}$$

Теорема Лагранжа доказывается элементарно (см. следующий пункт). В дальнейшем разными математиками были даны доказательства также для $n = 3, 4, 5, 6, 7, 8, 10$. Однако в общем виде проблема оставалась нерешенной до начала XX в. Первое общее доказательство дал немецкий математик Д. Гильберт в 1909 г., но это доказательство очень сложно и громоздко, а значение верхней границы для $G(n)$, как это было показано позже, излишне велико.

4. Харди и Литлвуд высказали следующие аддитивные предположения: 1) каждое достаточно большое натуральное число, не являющееся квадратом, есть сумма квадрата целого числа и простого числа; 2) каждое достаточно большое натуральное число есть сумма двух квадратов целых чисел и простого числа. Из них второе было доказано Ю. В. Линником в 1959 г., первое же остается пока гипотезой.

2. Разложения на сумму квадратов

А. Прежде чем доказать теорему Лагранжа о разложении любых натуральных чисел на сумму 4 квадратов, рассмотрим разложение натуральных чисел специального вида на сумму двух квадратов.

Теорема: Необходимое и достаточное условие представимости натурального числа N формой $x^2 + y^2$ (т. е. разрешимости уравнения $x^2 + y^2 = N$, или того, что окружность $x^2 + y^2 = N$ проходит через целые точки) заключается в том, чтобы каноническое разложение N не содержало простых множителей вида $4n + 3$ в нечетных степенях

Доказательство. 1. Необходимость условия следует из того, что если

$$N = x^2 + y^2 \quad (1)$$

и $N|p = 4n + 3$, то $N|p^2$.

Действительно, если имеем равенство (1) и $N|p$, то

$$x^2 + y^2 \equiv 0 \pmod{p},$$

или

$$x^2 \equiv -y^2 \pmod{p}. \quad (2)$$

Так как $-y^2$ не может быть квадратичным вычетом по модулю $4n + 3$ (символ Лежандра $\left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right) = 1$ в том и только в том случае, когда $p = 4n + 1$), то из (2) следует

$$x \equiv 0 \pmod{p}, \quad y \equiv 0 \pmod{p}, \quad (3)$$

а тогда $N|p^2$.

Заметим, что согласно (3) в рассматриваемом случае $(x, y) \neq 1$. Числа x и y не могут так же быть взаимно простыми, когда N представимо в виде (1) и $N|4$, так как тогда x и y должны быть четными. Из этого замечания следует, что если N представимо в форме (1) и $(x, y) = 1$, то N имеет простые нечетные делители только вида $4n + 1$ и $N \nmid 4$.

С другой стороны ясно, что в представлении (1) простого числа $p = 4n + 1$ $(x, y) = 1$, так как иначе из $(x, y) = d > 1$ следовало бы $p|d^2$, что невозможно.

Представление (1), в котором $(x, y) = 1$, называется *собственным*; если $(x, y) \neq 1$, то оно называется *несобственным*.

2) Достаточность условия следует из того, что, с одной стороны, имеет место тождество

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 \mp b_1b_2)^2 + (a_1b_2 \pm a_2b_1)^2,$$

которое показывает, что произведение двух целых чисел, являющихся суммами квадратов, есть снова сумма квадратов, а с другой стороны, число N , каноническое разложение которого не содержит простых множителей вида $4n + 3$ в нечетных степенях, можно рассматривать как произведение множителей следующего вида: квадрата, двойки и простых множителей вида $4n + 1$, которые все разлагаются на сумму двух квадратов ($k^2 = k^2 + 0^2$, $2 = 1^2 + 1^2$, $p = 4n + 1 = x^2 + y^2$, согласно п. 4, § 2, гл. VI).

Б. Число представлений простого числа $4n + 1$ формой $x^2 + y^2$ определяется следующей теоремой: *простое число $p = 4n + 1$ представимо формой $x^2 + y^2$ не более, чем одним способом, если представления, отличающиеся порядком слагаемых, мы не будем считать различными.*

Теорему можно выразить и так (если учесть, что в представлении $p = 4n + 1 = x^2 + y^2$ $x \neq y$): для простого числа $p = 4n + 1$ при натуральных и попарно неравных x_1, y_1, x_2, y_2 представления

$$p = x_1^2 + y_1^2 = x_2^2 + y_2^2 \quad (1)$$

невозможны.

Доказательство. Допустим противное. Тогда из (1) следует

$$x_1^2 y_2^2 - y_1^2 x_2^2 = p(y_2^2 - y_1^2),$$

откуда

$$(x_1 y_2 - y_1 x_2)(x_1 y_2 + y_1 x_2) | p, \quad (2)$$

причем обе скобки не могут делиться на p , так как их сумма $2x_1 y_2 \nmid p$.

Перемножая оба представления (1), получим (учитывая тождество в А)

$$p^2 = (x_1 x_2 \pm y_1 y_2)^2 + (x_1 y_2 \mp y_1 x_2)^2, \quad (3)$$

где можно взять или верхние, или нижние знаки.

Если $x_1 y_2 - y_1 x_2 \mid p$, то $(x_1 y_2 - y_1 x_2)^2 \mid p^2$ и при верхних знаках в (3) также $(x_1 x_2 + y_1 y_2)^2 \mid p^2$. После деления на p^2 из (3) получается, что сумма двух квадратов равна 1, а это возможно лишь тогда, когда один из квадратов равен 0.

Так как для натуральных значений x_1, y_1, x_2, y_2 $x_1 x_2 + y_1 y_2 \neq 0$, то должно быть $x_1 y_2 - y_1 x_2 = 0$, или $x_1 y_2 = y_1 x_2$, откуда, в силу того, что $(x_1, y_1) = (x_2, y_2) = 1$ (см. замечание в А), следует $x_1 \mid x_2$ и $x_2 \mid x_1$, т. е. $x_1 = x_2$, $y_1 = y_2$, а это противоречит условию.

Если $x_1 y_2 + y_1 x_2 \mid p$, то при нижних знаках в (3) аналогично получаем $x_1 x_2 - y_1 y_2 = 0$, откуда вследствие $(x_1, y_1) = (x_2, y_2) = 1$ следует $x_1 \mid y_2$ и $y_2 \mid x_1$, т. е. $x_1 = y_2$, $y_1 = x_2$, но это также противоречит условию. Теорема доказана.

В. Представление числа $N = 4n + 1$ формой $x^2 + y^2$ дает возможность установить критерий простого числа такого вида. Мы видели, что *простые* числа вида $4n + 1$ имеют единственное, причем собственное представление формой $x^2 + y^2$.

Оказывается, что и наоборот, *если число вида $4n + 1$ имеет единственное, причем собственное представление формой $x^2 + y^2$, то оно простое.*

В самом деле, составные числа вида $4n + 1$, имеющие собственное представление, содержат, согласно замечанию в 1-й части доказательства теоремы п. А, только простые делители вида $4n + 1$, из которых каждый представим формой $x^2 + y^2$.

Произведение двух таких простых чисел, например $p_1 = x_1^2 + y_1^2$, $p_2 = x_2^2 + y_2^2$, где можно предположить $x_1 > y_1 > 0$, $x_2 > y_2 > 0$, имеет по крайней мере 2 представления формой $x^2 + y^2$, как это видно из тождества

$$p_1 p_2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 \pm y_1 y_2)^2 + (x_1 y_2 \mp y_1 x_2)^2,$$

если учесть, что все x_1, y_1, x_2, y_2 отличны от нуля и что $(x_1 x_2 + y_1 y_2)^2$ больше остальных трех квадратов в правой части тождества. (Достаточно убедиться в том, что $x_1 x_2 + y_1 y_2 > x_1 y_2 + y_1 x_2$, а это действительно имеет место, ибо $(x_1 x_2 + y_1 y_2) - (x_1 y_2 + y_1 x_2) = (x_1 - y_1)(x_2 - y_2) > 0$.)

Применяя указанное тождество повторно, можно убедиться, что любое составное $N = 4n + 1$, содержащее только простые множители вида $4n + 1$, представимо более чем одним способом.

Итак, имеем следующий критерий простого числа вида $4n + 1$: *нечетное число вида $4n + 1$ тогда и только тогда является простым, когда оно лишь единственным образом представимо в виде суммы двух квадратов, причем собственно.*

Этот критерий впервые установлен Эйлером.

Г. Теорема Лагранжа: *каждое натуральное число можно представить в виде суммы четырех квадратов целых чисел (или в виде суммы не более четырех квадратов натуральных чисел).*

1. Эйлер указал на тождество, согласно которому произведение сумм четырех квадратов тоже сумма четырех квадратов:

$$(a_1^2 + b_1^2 + c_1^2 + d_1^2) (a_2^2 + b_2^2 + c_2^2 + d_2^2) = A^2 + B^2 + C^2 + D^2, \quad (1)$$

где

$$A = a_1 a_2 + b_1 b_2 + c_1 c_2 + d_1 d_2,$$

$$B = -a_1 b_2 + b_1 a_2 - c_1 d_2 + d_1 c_2,$$

$$C = -a_1 c_2 + c_1 a_2 - d_1 b_2 + b_1 d_2,$$

$$D = -a_1 d_2 + d_1 a_2 - b_1 c_2 + c_1 b_2.$$

Это тождество проверяется непосредственно. Ввиду (1) для доказательства справедливости теоремы Лагранжа достаточно показать, что каждое простое число и единицу можно представить в виде суммы четырех квадратов. Так как 1, 2 и каждое простое число $4n + 1$ представимы даже в виде суммы двух квадратов, то тем более — в виде суммы четырех квадратов (достаточно прибавить $0^2 + 0^2$). Остается доказать, что каждое простое число формы $4n + 3$ представимо в виде суммы четырех квадратов. Мы все же будем, сохраняя независимость от предыдущих результатов, рассматривать представления любых простых чисел $p > 2$, так как доказательство от этого почти не усложняется.

Сначала покажем, что для простого числа $p > 2$ существует кратное mp , где $0 < m < p$, представимое

в виде суммы четырех квадратов, а затем — что само p также представимо, т. е. что можно положить $m = 1$.

2. Для первого шага рассмотрим числа вида x^2 и $-y^2 - 1$, где x и y пробегает значения $0, 1, \dots, \frac{p-1}{2}$.

Из теории квадратичных вычетов известно, что для таких чисел никакие два значения x^2 или два значения $-y^2 - 1$ не могут быть сравнимы по модулю p .

Так как всего получается $p + 1$ число, а по модулю p имеется p классов, то согласно принципу Дирихле по крайней мере два числа из этих разных совокупностей должны принадлежать одному классу по модулю p .

Поэтому существуют x и y , для которых

$$x^2 \equiv -y^2 - 1 \pmod{p},$$

или

$$mp = x^2 + y^2 + 1^2 + 0^2, \text{ где } 0 < m < p, \quad (2)$$

так как 1) $x^2 + y^2 + 1 > 0$; 2) вследствие того, что

$$x < \frac{p}{2}, \quad y < \frac{p}{2},$$

$$m = \frac{1}{p}(x^2 + y^2 + 1) < \frac{1}{p}\left(\frac{p^2}{2} + 1\right) < p.$$

Таким образом, первый шаг сделан: доказано, что при любом простом $p > 2$ существуют целые числа a_1, b_1, c_1, d_1 , для которых

$$mp = a_1^2 + b_1^2 + c_1^2 + d_1^2, \text{ где } 0 < m < p. \quad (3)$$

3. Чтобы доказать второе утверждение, отметим, во-первых, что из существования натурального $m < p$, такого, что mp разлагается на сумму четырех квадратов, вытекает также существование наименьшего натурального числа m , обладающего тем же свойством. Пусть в дальнейшем m и означает это наименьшее число. Нам надо показать, что $m = 1$.

Допустим, что $m > 1$.

Прежде всего можно утверждать, что m нечетно. Действительно, если $m = 2m_1$, то в равенстве (3) либо все a_1, b_1, c_1, d_1 — четные, либо все нечетные, либо два из них четные, а два нечетные. В каждом из этих

случаев можно числа a_1, b_1, c_1, d_1 так сгруппировать по два, чтобы их полусуммы, а значит и полуразности, были целыми числами. Без ограничения общности можно считать, что как раз $\frac{a_1 + b_1}{2}, \frac{a_1 - b_1}{2}, \frac{c_1 + d_1}{2}, \frac{c_1 - d_1}{2}$ являются целыми числами. Тогда имеем

$$m_1 p = \left(\frac{a_1 + b_1}{2}\right)^2 + \left(\frac{a_1 - b_1}{2}\right)^2 + \left(\frac{c_1 + d_1}{2}\right)^2 + \left(\frac{c_1 - d_1}{2}\right)^2,$$

т. е. $m_1 p = \frac{1}{2} m p$ уже разлагается на сумму четырех целых квадратов вопреки предположению, что $m p$ — наименьшее такое кратное p .

Итак, число m — нечетное.

Обозначим теперь соответственно через a_2, b_2, c_2, d_2 абсолютно наименьшие вычеты чисел a_1, b_1, c_1, d_1 , по модулю m , так что

$$a_1 \equiv a_2, b_1 \equiv b_2, c_1 \equiv c_2, d_1 \equiv d_2 \pmod{m}, \quad (4)$$

причем все $|a_2|, |b_2|, |c_2|, |d_2| < \frac{m}{2}$, так как m — нечетное. Тогда имеем

$$m p = a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a_2^2 + b_2^2 + c_2^2 + d_2^2 \equiv 0 \pmod{m}, \quad (5)$$

откуда

$$m k = a_2^2 + b_2^2 + c_2^2 + d_2^2 < 4 \left(\frac{m}{2}\right)^2 = m^2, \quad (6)$$

с условием $0 < k < m$, ибо $k \neq 0$ (в противном случае $a_2 = b_2 = c_2 = d_2 = 0$, все a_1, b_1, c_1, d_1 делились бы на m , а $m p$ делилось бы на m^2 , т. е. p делилось бы на m , что невозможно, так как $1 < m < p$).

Перемножая равенства в левых частях (5) и (6) и учитывая (1), получаем

$$m^2 k p = A^2 + B^2 + C^2 + D^2, \quad (7)$$

где в силу (4) и (5) $A \equiv B \equiv C \equiv D \equiv 0 \pmod{m}$.

Поэтому из (7) следует

$$k p = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2, \quad (8)$$

где $\frac{A}{m}, \frac{B}{m}, \frac{C}{m}$ и $\frac{D}{m}$ — целые числа.

Получается, что kp , где $0 < k < t$, можно представить в виде суммы четырех квадратов, но это несовместимо с определением минимальности числа t .

Итак, предположение, что натуральное $t > 1$ недопустимо, следовательно, $t = 1$. Теорема Лагранжа доказана.

3. О методе Л. Г. Шнирельмана

А. Как уже отмечалось во введении, первые успехи в решении проблемы Гольдбаха принадлежат выдающемуся советскому математику Л. Г. Шнирельману.

В 1930 г. Шнирельман открыл новый метод, имеющий очень важное значение в аддитивной теории чисел, так называемый *метод сложения числовых последовательностей*. При помощи этого метода Шнирельман доказал, что существует константа C (называется теперь константой Шнирельмана), такая, что всякое натуральное число $N > 1$ есть сумма не более C простых.

Для *достаточно больших* N Шнирельман установил, что наименьшее значение константы не превышает 800 000. Разные ученые, применившие метод Шнирельмана, скоро снизили указанную верхнюю грань до 67 (Риччи, 1936), в 1951 г. она была снижена до 20 (Шапиرو и Варга), а в 1958 г. даже до 18 (Ин).

Метод Шнирельмана дал решение проблемы Гольдбаха в ослабленной формулировке. Это был первый существенный сдвиг в этой, до тех пор в течение почти 200 лет казавшейся неприступной проблеме. Для своего времени результат Шнирельмана был фундаментальным и вызвал величайший интерес в математическом мире. Крупнейший специалист по теории чисел Э. Ландау, пессимистические высказывания которого в 1912 году мы упоминали, тогда писал: «Работа Л. Г. Шнирельмана содержит одно из величайших достижений в теории чисел, до которого мне удалось дожить».

После работы Шнирельмана исследования его методом вылились в самостоятельное направление.

Б. Метод Шнирельмана заключается в следующем: пусть нам дано некоторое число начинающих с нуля

возрастающих последовательностей целых чисел

$$a_0 (= 0), a_1, a_2, \dots, a_m, \dots, \quad (A)$$

$$b_0 (= 0), b_1, b_2, \dots, b_m, \dots, \quad (B)$$

$$\dots \dots \dots c_0 (= 0), c_1, c_2, \dots, c_m, \dots \quad (C)$$

Выберем по одному числу из каждой последовательности и сложим между собой эти числа. Совокупность всех полученных таким образом чисел, в которой равные между собою будем считать только по одному разу, можно расположить в виде некоторой новой возрастающей последовательности

$$n_0 (= 0), n_1, n_2, \dots, n_m, \dots \quad (N)$$

Последнюю последовательность мы назовем суммой данных последовательностей A, B, \dots, C .

$$N = A + B + \dots + C.$$

Последовательность N состоит из всех чисел вида

$$a_i + b_j + \dots + c_l$$

и содержит, в частности, все члены данных последовательностей (чтобы их получить, нужно складывать члены данной последовательности с нулевыми членами остальных последовательностей).

Обозначая через P последовательность

$$0, 2, 3, 5, 7, 11, 13, \dots, \quad (P)$$

состоящую из нуля и всех простых чисел, можно гипотезу Гольдбаха выразить следующим образом: сумма $P + P + P$ содержит все натуральные числа, превосходящие единицу. В самом деле, последовательность $P + P + P$ состоит из сумм вида $0 + 0 + 0$, $0 + 0 + p_1$, $0 + p_1 + p_2$, $p_1 + p_2 + p_3$, т. е. из сумм не более трех простых чисел. Если она содержит все натуральные числа больше единицы, то это значит, что всякое натуральное число > 1 можно представить в виде суммы не более чем трех простых чисел, а это как раз и утверждается в гипотезе Гольдбаха.

Если сумма k одинаковых последовательностей A охватывает все натуральные числа, то последовательность A называется базисом (натурального ряда) порядка k (она будет также базисом порядка $k_1 > k$).

Говорят также о базисе k -го порядка для достаточно больших чисел, если сумма k одинаковых последовательностей A охватывает все достаточно большие числа.

Не всякая последовательность является базисом. Так, например, последовательность четных чисел

$$0, 2, 4, \dots$$

не является базисом какого-либо порядка, так как при сложении чисел этой последовательности нельзя получить ни одного нечетного числа. Не является также базисом ранее упомянутая последовательность P , так как при сложении ее чисел нельзя получить 1.

Шнирельман ввел понятие *плотности* последовательности. Пусть

$$a_0 = 0, a_1, a_2, \dots, a_n, \dots \quad (A)$$

— возрастающая последовательность натуральных чисел. Обозначим через $A(n)$ число членов этой последовательности, не превосходящих n (при этом подсчете $a_0 = 0$ не считается). Очевидно, при любом n

$$0 \leq A(n) \leq n,$$

откуда

$$0 \leq \frac{A(n)}{n} \leq 1.$$

Так как множество всех значений отношения $\frac{A(n)}{n}$ ограничено снизу, то оно имеет нижнюю грань, т. е. существует такое наибольшее число α , которое не превосходит ни одного из значений отношения $\frac{A(n)}{n}$ при любом n .

Нижнюю грань α всех значений отношения $\frac{A(n)}{n}$ мы и называем плотностью последовательности A . Итак, $\alpha = \inf \frac{A(n)}{n}$, так что $\alpha \leq \frac{A(n)}{n}$ и $\alpha n \leq A(n)$ для любого n .

Очевидно, плотность последовательности может принимать только неотрицательные значения и не может быть больше 1.

Если $a_1 > 1$ (т. е. если последовательность A не содержит единицы), то $\alpha = 0$; если плотность последовательности равна 1, то последовательность содержит все натуральные числа.

Шнирельман показал, что *плотность суммы любых двух числовых последовательностей A и B с плотностями α и соответственно β не меньше, чем $\alpha + \beta - \alpha \cdot \beta$.*

Другими словами, если мы через γ обозначим плотность суммы $C = A + B$, то

$$\gamma \geq \alpha + \beta - \alpha\beta. \quad (1)$$

Для доказательства подсчитаем на отрезке натурального ряда $[1, n]$ некоторые категории чисел, принадлежащих C .

К таким можно, во-первых, отнести все числа a_k последовательности A на указанном отрезке: их количество равно $A(n)$.

Пусть далее между двумя соседними числами a_k и a_{k+1} из A расположено l натуральных чисел $a_k + r$, $1 \leq r \leq l$. Те из них, для которых r принадлежит B , по определению суммы последовательностей также принадлежат C .

Внутри $[a_k, a_{k+1}]$ таких чисел имеется $B(l)$, а на отрезке $[1, n]$ всего их $\sum_l B(l)$, где суммирование производится по всем отрезкам между a_k и a_{k+1} .

Указанными двумя категориями чисел, вообще говоря, не исчерпываются все члены последовательности C , так как внутренние точки отрезков $[a_k, a_{k+1}]$ могут оказаться принадлежащими к C в результате таких сочетаний членов последовательностей A и B , которые отличны от вышеуказанных. Пусть, например, имеем последовательности

$$0, 1^2, 2^2, 3^2, \dots \quad (A_1)$$

и

$$0, 1^3, 2^3, 3^3, \dots; \quad (B_1)$$

тогда указанным способом можно на отрезке $[25, 36]$ выявить лишь числа $25 + 1 = 26$ и $25 + 8 = 33$ из $C_1 = A_1 + B_1$, между тем этому отрезку принадлежат также следующие числа C_1 : $0 + 27 = 27$, $1 + 27 = 28$ и $4 + 27 = 31$.

Таким образом, имеем для всех $n \geq 1$

$$C(n) \geq A(n) + \sum_l B(l).$$

Но так как $B(l) \geq \beta l$, так что

$$\sum_l B(l) \geq \beta \sum_l l = \beta(n - A(n)) \quad \text{и} \quad A(n) \geq \alpha n,$$

то

$$C(n) \geq A(n) + \beta(n - A(n)) = A(n)(1 - \beta) + \beta n \geq \alpha(1 - \beta)n + \beta n,$$

откуда

$$\gamma = \inf \frac{C(n)}{n} \geq \alpha + \beta - \alpha\beta;$$

теорема доказана.

Теорема Шнирельмана допускает следующее важное усиление:

$$\gamma \geq \min(1, \alpha + \beta).$$

Оно было впервые доказано в 1942 г. Х. Манном. Заметим, что (1) можно заменить соотношением

$$1 - \gamma \leq 1 - \alpha - \beta + \alpha\beta,$$

или

$$1 - \gamma \leq (1 - \alpha)(1 - \beta), \quad (2)$$

распространяемое по индукции на любое конечное число последовательностей.

При помощи предыдущей теоремы Шнирельман доказал следующую основную теорему: *всякая последовательность положительной плотности есть базис натурального ряда.*

Другими словами, если для некоторой числовой последовательности A $\alpha > 0$, то сумма достаточного количества последовательностей A охватывает весь натуральный ряд.

Для доказательства допустим, что γ — плотность последовательности C , суммы k последовательностей A плотности α . Тогда согласно (2)

$$1 - \gamma \leq (1 - \alpha)^k.$$

Для достаточно большого k правая часть станет меньше $\frac{1}{2}$ и вместе с тем $\gamma > \frac{1}{2}$. Из этого следует, что на любом сегменте $[1, n]$ расположено $r > \frac{n}{2}$ членов C

$$c_1, c_2, \dots, c_r.$$

Если к ним присоединить 0 и числа

$$n - c_1, n - c_2, \dots, n - c_r,$$

то получится всего $2r + 1 > n + 1$ чисел, принадлежащих отрезку $[0, n]$. Поэтому (по принципу Дирихле) среди них должны быть равные, т. е.

$$n - c_i = c_j,$$

откуда

$$n = c_i + c_j.$$

Другими словами, любое натуральное число n можно получить как сумму двух чисел из C , а это значит, что A есть базис натурального ряда (при этом порядка $\leq 2k$), что и требовалось доказать.

Основную теорему Шнирельман постарался применить к решению проблемы Гольдбаха. Сделать это непосредственно не было возможности, так как плотность последовательности P'

$$0, 1, 2, 3, 5, 7, 11, 13, \dots \quad (P'),$$

состоящей из нуля, единицы и всех простых чисел, имеет плотность нуль. Однако Шнирельману удалось доказать знаменитую теорему о том, что последовательность $P' + P'$ имеет положительную плотность. Вместе с тем оказывается, что $P' + P'$, а следовательно, и P' является базисом натурального ряда. Из этого уже нетрудно заключить, что всякое натуральное число N , кроме 1, есть сумма ограниченного, не зависящего от N числа простых чисел.

Отметим в заключение, что, применяя метод Шнирельмана, Ю. В. Линник в 1943 г. дал элементарное решение проблемы Варинга в основном, доказав, что для любого натурального n последовательность

$$0, 1^n, 2^n, \dots, k^n, \dots$$

представляет собой базис натурального ряда (см. (7), (54)).

Порядок базиса, т. е. минимальное число слагаемых x^n в представлении N , методом Ю. В. Линника пока не установлен.

4. О методе И. М. Виноградова

1. В проблемах Варинга и Гольдбаха, а также в других аддитивных задачах И. М. Виноградов исходит из интеграла

$$I = \int_0^1 e^{2\pi i m \alpha} d\alpha,$$

где m — любое целое число.

Если $m = 0$,

$$I = \int_0^1 d\alpha = 1,$$

если же $m \neq 0$, то

$$I = \int_0^1 e^{2\pi i m \alpha} d\alpha = \frac{1}{2\pi i m} [e^{2\pi i m \alpha}]_0^1 = \frac{1}{2\pi i m} (e^{2\pi i m} - e^0) = 0,$$

так как

$$e^{2\pi i m} = \cos 2\pi m + i \sin 2\pi m = 1.$$

Рассмотрим применение этого интеграла к решению проблемы Варинга.

Предварительно заметим, что если целое число N представлено в виде

$$N = x_1^n + x_2^n + \dots + x_r^n$$

с целыми положительными x_i , то, очевидно, $x_i < P$, где P равно целой части от $\sqrt[n]{N}$, т. е. $[\sqrt[n]{N}]$.

Пусть дано некоторое целое число $N > 0$ и пусть x_1, x_2, \dots, x_r какие-либо r положительных целых чисел, удовлетворяющих условию $x_i < P$.

Возьмем

$$m = (x_1^n + x_2^n + \dots + x_r^n) - N$$

и подставим это число в интеграл I .

Всякий раз, когда

$$N = x_1^n + x_2^n + \dots + x_r^n,$$

m обращается в нуль и интеграл I принимает значение 1, в остальных случаях, т. е. когда

$$N \neq x_1^n + x_2^n + \dots + x_r^n,$$

$m \neq 0$ и интеграл равен нулю.

Суммируя поэтому указанный интеграл по всем x_1, x_2, \dots, x_r , пробегающим независимо друг от друга значения $1, 2, \dots, P$, мы получим столько единиц, сколько имеется различных представлений числа N в виде суммы r слагаемых n -ых степеней целых положительных чисел (при этом, очевидно, представления, отличающиеся только лишь порядком следования чисел x_i , считаются различными).

Обозначая через $W(N)$ число таких представлений, мы можем утверждать, что

$$W(N) = \sum_{x_1=1}^P \sum_{x_2=1}^P \dots \sum_{x_r=1}^P \int_0^1 e^{2\pi i (x_1^n + x_2^n + \dots + x_r^n - N)\alpha} d\alpha.$$

Так как сумма нескольких интегралов, взятых в одинаковых пределах, равна интегралу от суммы подинтегральных выражений, то из предыдущего равенства следует

$$\begin{aligned} W(N) &= \int_0^1 \sum_{x_1=1}^P \sum_{x_2=1}^P \dots \sum_{x_r=1}^P e^{2\pi i (x_1^n + x_2^n + \dots + x_r^n - N)\alpha} d\alpha, \\ W(N) &= \\ &= \int_0^1 \sum_{x_1=1}^P \sum_{x_2=1}^P \dots \sum_{x_r=1}^P (e^{2\pi i x_1^n \alpha} \cdot e^{2\pi i x_2^n \alpha} \dots e^{2\pi i x_r^n \alpha} \cdot e^{-2\pi i N \alpha}) d\alpha. \end{aligned}$$

Легко понять, что из всех слагаемых подинтегрального выражения можно взять за общую скобку сомножитель $e^{-2\pi i N \alpha}$ и что в скобке останется произведение

$$\sum_{x_1=1}^P e^{2\pi i x_1^n \alpha} \cdot \sum_{x_2=1}^P e^{2\pi i x_2^n \alpha} \dots \sum_{x_r=1}^P e^{2\pi i x_r^n \alpha},$$

но

$$\sum_{x_1=1}^P e^{2\pi i x_1^n \alpha} = \sum_{x_2=1}^P e^{2\pi i x_2^n \alpha} = \dots = \sum_{x_r=1}^P e^{2\pi i x_r^n \alpha} = \sum_{x=1}^P e^{2\pi i x^n \alpha}.$$

Обозначая поэтому

$$L_\alpha = \sum_{x=1}^P e^{2\pi i x^n \alpha},$$

мы можем писать

$$W(N) = \int_0^1 L_\alpha' \cdot e^{-2\pi i N \alpha} d\alpha.$$

Для решения проблемы Варинга надо, очевидно, при любом данном n установить существование такого $G(n)$, чтобы при $r \geq G(n)$ для достаточно больших N $W(N)$ было положительным.

2. В гипотезе Гольдбаха для нечетных чисел утверждается, что любое нечетное число $N \geq 9$ есть сумма трех нечетных простых чисел:

$$N = p_1 + p_2 + p_3,$$

где p_1, p_2 и p_3 — нечетные простые числа.

Рассуждая таким же образом, как при рассмотрении проблемы Варинга, мы легко найдем, что число $I(N)$ представлений нечетного числа N в виде суммы трех нечетных простых чисел выразится через

$$I(N) = \sum_{p_1 \leq N} \sum_{p_2 \leq N} \sum_{p_3 \leq N} \int_0^1 e^{2\pi i (p_1 + p_2 + p_3 - N) \alpha} d\alpha,$$

где суммирование ведется по нечетным простым числам, не превосходящим N .

Легко понять, что можно также писать

$$I(N) = \int_0^1 \sum_{p_1 \leq N} \sum_{p_2 \leq N} \sum_{p_3 \leq N} e^{2\pi i (p_1 + p_2 + p_3 - N) \alpha} d\alpha,$$

$$I(N) = \int_0^1 \left(\sum_{p_1 \leq N} e^{2\pi i p_1 \alpha} \cdot \sum_{p_2 \leq N} e^{2\pi i p_2 \alpha} \cdot \sum_{p_3 \leq N} e^{2\pi i p_3 \alpha} \right) e^{-2\pi i N \alpha} d\alpha,$$

$$I(N) = \int_0^1 \left(\sum_{p \leq N} e^{2\pi i p \alpha} \right)^3 \cdot e^{-2\pi i N \alpha} d\alpha,$$

или

$$I(N) = \int_0^1 T_\alpha^3 \cdot e^{-2\pi i N \alpha} d\alpha,$$

где

$$T_\alpha = \sum_{p \leq N} e^{2\pi i p \alpha}.$$

Проблема Гольдбаха для нечетных чисел будет решена, если удастся доказать, что для любого нечетного $N \geq 9$ $I(N) > 0$. Теоретически важно доказать это для достаточно больших N .

3. Как в проблеме Варинга, так и в проблеме Гольдбаха наиболее трудным вопросом является оценка сумм

$$L_\alpha \text{ и } T_\alpha.$$

Эти суммы являются частными случаями сумм вида

$$\sum_{A < x < B} e^{2\pi i f(x)},$$

где $f(x)$ — некоторая действительная функция от x и суммирование распространяется на все целые числа некоторого интервала (A, B) , или же на какую-либо часть этих целых чисел, например простые числа.

Такие суммы называются *тригонометрическими суммами*. Оценка тригонометрических сумм является чрезвычайно важным вопросом в аналитической теории чисел.

Впервые тригонометрическими суммами интересовался К. Ф. Гаусс. Гаусс изучил суммы вида

$$\sum_{x=0}^{q-1} e^{2\pi i \frac{ax^2}{q}}, \text{ где } (a, q) = 1,$$

получившие впоследствии название «суммы Гаусса».

Первый общий метод оценки сумм вида

$$\sum_{x=1}^P e^{2\pi i f(x)}, \quad f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x,$$

где $\alpha_n, \alpha_{n-1}, \dots, \alpha_1$ — заданные действительные числа, причем хотя бы одно из них иррациональное, дал Герман Вейль в 1914 г., поэтому эти суммы носят

название «суммы Вейля». Оценки, получаемые по методу Вейля, зависят от приближений посредством рациональных дробей к старшему коэффициенту многочлена $f(x)$.

Хотя оценка Вейля лишь немного лучше тривиальной, (тривиальной является оценка $\left| \sum_{x=1}^P e^{2\pi i f(x)} \right| \leq P$; это неравенство заведомо имеет место, так как модуль $e^{2\pi i f(x)}$ при действительных значениях $f(x)$ равен единице, а модуль суммы нескольких слагаемых не превосходит суммы модулей этих слагаемых), однако и она уже ведет к замечательным приложениям.

Используя ее, Харди и Литлвуд создали первый мощный аналитический метод для решения аддитивных задач теории чисел.

Этим методом им (с 1920 по 1925 гг.) удалось, в частности, дать более совершенное, чем у Гильберта, доказательство теоремы Варинга. Они снизили также верхнюю границу для $G(n)$ (т. е. для наименьшего числа слагаемых r , необходимых для представления достаточно большого числа N в виде суммы целых неотрицательных n -х степеней) до величины

$$(n-2) \cdot 2^{n-1} + 5.$$

В отношении проблемы Гольдбаха результаты Харди и Литлвуда имеют условный характер, так как в доказательстве использована обобщенная гипотеза Римана.

Существенное развитие теория тригонометрических сумм получила в работах И. М. Виноградова, начиная с 1934 г.

Характерной чертой этих работ является освобождение от условия, чтобы суммирование проводилось по всем натуральным числам некоторого отрезка подряд.

В отношении проблемы Варинга (которой И. М. Виноградов начал заниматься с 1924 г.) новый метод позволил резко снизить верхнюю границу для $G(n)$. И. М. Виноградов нашел оценку $G(n) < n(3 \ln n + 11)$, а в 1959 г. улучшил свой результат и показал, что

$$G(n) < n \ln n (2 + \varepsilon(n)), \text{ где } \varepsilon(n) \rightarrow 0 \text{ при } n \rightarrow \infty;$$

Методом И. М. Виноградова получены также наилучшие значения для $g(n)$ (т. е. для наименьшего числа слагаемых r , необходимых для представления любого натурального N в виде суммы целых неотрицательных n -х степеней).

Заметим, что для небольших значений n специальные исследования показали, что $G(3) \leq 7$ (Ю. В. Линник), $G(4) = 16$, $G(5) \leq 23$, $G(6) \leq 36$, $G(7) \leq 52$, $G(8) \leq 73$ (Давенпорт), а $g(3) = 9$ (Виферих), $g(4) \leq 35$ (Л. Диксон), $g(5) \leq 40$ (Чень Цзынь-жунь), $g(6) = 73$ (С. Пиллаи).

Необходимо также подчеркнуть, что в работах И. М. Виноградова проблема Варинга получила обобщимое решение.

Еще более усовершенствовав свой глубокий метод¹ (речь идет об оценке суммы $\sum_{P \leq N} e^{2\pi i a p}$, взятой по

всем простым числам $\leq N$ и отчасти о новых соображениях относительно способа применения Эратостенова решета, а также об использовании результатов, касающихся распределения простых чисел в арифметической прогрессии), И. М. Виноградов в 1937 г.

доказал, что для всякого достаточно большого нечетного положительного числа $N(N > N_0)$ число представлений N в виде суммы трех простых чисел > 0 , а это значит, что такие представления возможны. И. М. Виноградов нашел также приближенное значение для $I(N)$.

Относительно числа N_0 К. Г. Бороздкин в 1939 г. показал, что

$$N_0 \leq e^{e^{e^{41,96}}},$$

а позднее, что

$$N_0 \leq e^{e^{16,038}}.$$

¹ Систематическое изложение этого метода И. М. Виноградов дал в книгах «Новый метод в аналитической теории чисел». Труды математического института им. В. А. Стеклова, т. X, 1937 и «Метод тригонометрических сумм в теории чисел». Труды математического института им. В. А. Стеклова, т. XXIII, 1947 (см. (4)).

Таким образом, И. М. Виноградовым была, наконец, в принципе решена знаменитая проблема Гольдбаха для нечетных чисел.

Следует отметить, что сильный аналитический метод в классическом направлении аналитической и аддитивной теории чисел (использующий метод аналитических функций комплексного переменного, опирающийся в частности на свойства функции $\zeta(s)$) разработан Ю. В. Линником. Пользуясь этим методом, Ю. В. Линник в 1946 г. дал новое доказательство теоремы Гольдбаха — Виноградова о представлении нечетного числа суммой трех простых чисел.

Что касается предположения Эйлера о том, что всякое четное число представимо в виде суммы двух простых чисел, то этот вопрос до настоящего времени не решен.

Важнейшие результаты, полученные по данному вопросу, следующие.

Венгерским математиком А. Реньи (1948) методом «большого решета» Линника доказано, что всякое большое четное число представимо в виде суммы простого и произведения не более k простых, и А. И. Виноградовым (1946) применением свойств дзета-функции Римана к решету Сельберга, что всякое достаточно большое четное число является суммой двух целых, каждое из которых содержит не более трех простых множителей. Методом решета Бруно-Бухштаба китайскому математику Ван-Юаню (1958) удалось уменьшить максимальное число множителей одного из слагаемых до двух, не менее числа множителей во втором слагаемом. Наилучший результат получен А. А. Бухштабом в 1965 г.: он показал, что каждое достаточно большое число может быть представлено суммой простого числа и произведения не более трех простых чисел.

Отметим в заключение, что значение метода И. М. Виноградова не ограничивается одной теорией чисел.

Этот метод имеет также применение, выходящее за пределы области теории чисел, например в теории функций, теории вероятностей и приближенном анализе (в котором для некоторых классов функций, часто встречающихся в задачах математической физики,

классические квадратурные формулы практически непригодны, но в то же время квадратурные формулы на основе теоретикочисловых сеток обеспечивают весьма большую точность в вычислениях, причем оценка их погрешности зависит от оценки некоторых тригонометрических сумм; см. (11)).

Упражнения

276. Указать, какие из простых чисел p можно разложить на сумму двух квадратов; значения p : 1) 113, 2) 151, 3), 541, 4) 757, 5) 811, 6) 1091, 7) 1423.

277. Зная, что $317 = 11^2 + 14^2$, $281 = 5^2 + 16^2$, найти разложения на сумму двух квадратов числа $N = 317 \cdot 281 = 89\,077$; 2) зная, что $937 = 19^2 + 24^2$, $746 = 11^2 + 25^2$, найти разложения на сумму двух квадратов числа $N = 937 \cdot 746 = 699\,002$.

278. Доказать, что не существует различных целых точек на одинаковом расстоянии от точки $Q\left(\sqrt{2}, \frac{1}{3}\right)$.

279. Доказать, что для каждого натурального числа n существует такой круг с центром $Q\left(\sqrt{2}, \frac{1}{3}\right)$, что внутри него лежат точно n точек решетки.

280. Разложить на сумму 4 квадратов $5220 = (1^2 + 2^2 + 3^2 + 4^2) \times (5^2 + 6^2 + 7^2 + 8^2)$.

Указания и ответы к упражнениям

1. Имеем $a = 13 \cdot 17 + r$, $0 \leq r < 13$. Поэтому наибольшее значение для a равно $13 \cdot 17 + 12 = 233$.

2. Из $371 = b \cdot 14 + r$, $0 \leq r < b$ следует $14b < 371$, $b \leq 26$. С другой стороны, $15b > 371$, откуда $b > 24$. Итак, имеем $b = 25$, 26 и соответственно $r = 21, 7$.

3. Из $ap = b \cdot qp + rp$, $rp < b$ следует $p < \frac{b}{r}$.

4. Имеем $100 = b \cdot q + 6$, $0 \leq 6 < b$. Поэтому $bq = 94 = 94 \cdot 1$, $1 \cdot 94$, $47 \cdot 2$, $2 \cdot 47$. Так как делитель b больше 6, то b равно либо 94, либо 47. Соответствующие частные равны 1 и 2.

5. 1) Натуральное число имеет одну из форм: $3k$, $3k + 1$, $3k + 2$. Если $n = 3k$, то $n \mid 3$, если $n = 3k + 1$, то $n + 2 \mid 3$, если $n = 3k + 2$, то $n + 1 \mid 3$; задачи 2) и 3) решаются аналогично.

6. 1) 19, 2) 37, 3) 71.

7. Вытекает из алгоритма Евклида: $r_2 = a - bq_1$, $r_3 = b - r_2q_2 = a \cdot (-q_2) + b(1 + q_1q_2)$ и т. д.

8. Если $(a_1b_1) = d_1 = 1$, то (см. предыдущую задачу) существуют целые числа x и y , такие, что $a_1x + b_1y = 1$.

Если, наоборот, $a_1x + b_1y = 1$ и $(a_1, b_1) = d_1$, то $a_1 \mid d_1$, $b_1 \mid d_1$, откуда $a_1x + b_1y \mid d_1$, т. е. $1 \mid d_1$, так что $d_1 = 1$.

9. $51 = 21 \cdot 2 + 9$, $21 = 9 \cdot 2 + 3$. Поэтому $3 = 21 - 2 \cdot 9 = 21 - 2 \cdot (51 - 21 \cdot 2) = 21 \cdot 5 - 51 \cdot 2$.

10. 1) $d_1 = 13$; 2) $d_2 = 23$.

11. Следует из того, что $D_{a, b} = D_{a, a \pm b}$.

12. По теореме предыдущей задачи имеем: $(n, n+1) = (n, 1) = 1$; $(n, 2n+1) = (n, n+1) = 1$, $(n+1, 2n+1) = (n+1, n) = 1$.

13. Пусть $(a+b, a-b) = d$, тогда $2a \mid d$ и $2b \mid d$, так что $(2a, 2b) = 2(a, b) = 2$ делится на d . Следовательно, $d = 1$ или 2.

14. Из первого условия следует $ab \mid d$, $cb \mid d$, так что $(ab, cb) \mid d$. Но $(ab, cb) = b(a, c) = b$, поэтому $b \mid d$.

15. Пусть $ab \mid c$, тогда $(ab, c) = c$. Кроме того, имеем $(a, c) = 1$; поэтому согласно теореме предыдущей задачи получаем $b \mid c$.

16. Пусть $(a, b) = d$, $(u_1a + v_1b, u_2a + v_2b) = d_1$. Имеем $u_1a + v_1b \mid d_1$, $u_2a + v_2b \mid d_1$, откуда в силу $u_1v_2 - u_2v_1 = 1$ получается $a \mid d_1$, $b \mid d_1$, так что $(a, b) = d \mid d_1$. С другой стороны, $a \mid d$, $b \mid d$, откуда легко следует, что $d_1 \mid d$. Таким образом, $d = d_1$.

17. Пусть $(ab, c) = d > 1$. Тогда в силу того, что $(a, c) = 1$, имеем $b \mid d$. Так как, кроме того, $c \mid d$, то $(b, c) \mid d$, $d > 1$, но это противоречит условию $(b, c) = 1$.

18. По теореме предыдущей задачи имеем последовательно

$$(a_1, b_j) = 1, (a_1 \cdot a_2, b_j) = 1, \dots, (A, b_j) = 1,$$

так что

$$(A, b_1) = 1, (A, b_2) = 1, \dots, (A, b_l) = 1.$$

Отсюда, как и выше, следует

$$(A, b_1) = 1, (A, b_1 \cdot b_2) = 1, \dots, (A, B) = 1.$$

19. Пусть $(ac, b) = d$ и $(c, b) = d_1$. Согласно теореме задачи 14 из $(ac, b) = d$ и $(a, b) = 1$ имеем $c \mid d$. Так как, кроме того, $b \mid d$, то $(c, b) \mid d$, т. е. $d_1 \mid d$. С другой стороны, $ac \mid d_1$ и $b \mid d_1$, так что $(ac, b) \mid d_1$, т. е. $d \mid d_1$. Таким образом, $d = d_1$.

20. 1) Если $N = n(n+1)(n+2)$, то $N \mid 2$ и $N \mid 3$, поэтому $N \mid [2, 3] = 6$; 2) если $N = n(n+1)(n+2)(n+3)(n+4)$, то $N \mid 3$, $N \mid 5$, $N \mid 8$ (см. задачу 5), поэтому $N \mid [3, 5, 8] = 120$.

21. 1) 5382, 2) 6409.

22. Имеем $(a, b) = 15$, поэтому $a = 15a_1$, $b = 15b_1$, $(a_1, b_1) = 1$. Далее, из $[a, b] = 840$ следует $15[a_1, b_1] = 840$, $[a_1, b_1] = 56$. Итак, $a_1b_1 = 56$. Отсюда получаются такие пары значений (если на последовательность чисел в отдельных парах не будем обращать внимания):

$$a_1b_1 : 1, 56; 2, 28; 4, 14; 7, 8$$

$$a, b : 15, 840; 30, 420; 60, 210; 105, 120.$$

23. Пусть $m = [n, n+1, n+2] = [[n, n+1], n+2]$. Так как $(n, n+1) = 1$ (см. задачу 12), то $m = [n(n+1), n+2]$. Далее возможны 2 случая:

1) $n = 2k$; тогда $(n(n+1), n+2) = (2k(2k+1), 2(k+1)) = 2$, так как $(k, k+1) = 1$ и $(k+1, 2k+1) = 1$ (см. задачу 12). Поэтому $m = \frac{1}{2}n(n+1)(n+2)$.

2) $n = 2k+1$; тогда $(n(n+1), n+2) = ((2k+1) \cdot 2 \cdot (k+1), 2k+3) = 1$, так как $(2, 2k+3) = 1$, $(2k+1, 2k+3) = (2k+1, 2) = 1$, $(k+1, 2k+3) = (k+1, k+2) = 1$. Поэтому $m = n(n+1)(n+2)$.

24. Пусть $\frac{A}{d} = x$. Так как $x = a_1 \frac{A_1}{d} = a_2 \frac{A_2}{d} = \dots = a_n \frac{A_n}{d}$ то $x | a_1, x | a_2, \dots, x | a_n$, так что $x | m$ или $x = mq$, где $q \geq 1$.

Поэтому $\frac{A_1}{d} = \frac{m}{a_1} q, \frac{A_2}{d} = \frac{m}{a_2} q, \dots, \frac{A_n}{d} = \frac{m}{a_n} q$.

Левые части этих равенств представляют взаимно простые числа, а правые части имеют общий делитель q , следовательно, $q = 1$ и $\frac{A}{d} = m$.

25. Формула выражает частный случай соотношения из предыдущей задачи.

26. Из $ab | p$ следует, что по меньшей мере один из сомножителей делится на p . В силу условия $a + b | p$ тогда получается, что и второй сомножитель делится на p .

27. Из данных условий следует, что $a^2 | p$ и $b^2 | p$, но в таком случае и $b | p$ (в силу того, что p — простое число).

28. Числа a и b можно представить в виде $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, где $\alpha_i \geq 0, \beta_i \geq 0$.

Тогда ясно, что $(a, b) = \prod p_i^{\min(\alpha_i, \beta_i)}$, $[a, b] = \prod p_i^{\max(\alpha_i, \beta_i)}$ (Π — символ произведения).

29. Согласно задаче 14 $p | d$, но так как p — простое число, то d равно либо 1, либо p .

30. Пусть $a + b$ и ab имеют общий простой делитель p . Из того, что $ab | p$, следует, что по меньшей мере один из сомножителей делится на p . Пусть $a | p$. Так как, кроме того, $a + b | p$, то и $b | p$, так что $(a, b) | p$, но это противоречит условию $(a, b) = 1$.

Аналогично доказывается второе утверждение.

31. Следует непосредственно из теорем, установленных в задачах 29 и 30.

32. Пусть $(a+b, a^2 - ab + b^2) = d$, тогда $a + b | d$, а также $a^2 - ab + b^2 = (a+b)^2 - 3ab | d$, так что и $3ab | d$. Поэтому $(a+b, 3ab) | d$. Но согласно предыдущей задаче $(a+b, 3ab)$ равен либо 1, либо 3. Следовательно, и d равен либо 1, либо 3.

33. Пусть $(a, b) = d$, так что $a = a_1 d, b = b_1 d, (a_1, b_1) = 1$. Тогда (см. задачу 30) $(a_1 + b_1, a_1 b_1) = 1$, откуда $(a + b, d \cdot a_1 b_1) = d$. Но

$$d \cdot a_1 b_1 = \frac{ab}{d} = [a, b], \text{ поэтому } (a+b, [a, b]) = d.$$

34. Следует из того, что натуральные числа, большие 3, вида $6k, 6k+2, 6k+3$ и $6k+4$ составные.

35. Следует из положения предыдущей задачи.

36. Если $k = 2n + 1$, то число $3k + 1 = 6n + 4$ составное, поэтому для простого p вида $3k + 1, k = 2n$ и $p = 6n + 1$ (например, $31 = 3 \cdot 10 + 1 = 6 \cdot 5 + 1$).

37. Простое число p может иметь вид: 1) 3, 2) $3k + 1$, 3) $3k + 2$. Условия задачи выполняются только в первом случае ($p + 10 = 13, p + 20 = 23$); во втором случае $p + 20 = 3k + 21$ является составным, а в третьем случае $p + 10 = 3k + 12$ — число составное.

38. $2^n \times 3$, поэтому 2^n имеет вид $3k + 1$ или $3k + 2$. В первом случае $2^n - 1 \mid 3$, а во втором $-2^n + 1 \mid 3$; при этом указанные числа не равны 3, если $n > 2$.

39. Если p и $8p^2 + 1$ — простые числа, то $p = 3$ (так как при $p = 3k + 1$ или $3k + 2$ число $8p^2 + 1$ не является простым); вместе с тем $8p^2 + 2p + 1 = 79$ — также простое число.

40. Простое число может иметь вид: 1) 3 , 2) $3k + 1$, 3) $3k + 2$. Но $a = 3k + 2 \mid 3$ и не может (в силу своей положительности) иметь простых делителей только формы $3k + 1$, так как произведение таких чисел имеет ту же форму. Поэтому должны существовать простые делители числа a формы $3k + 2$.

41. 1) $-38 \equiv -3 \pmod{7}$; 2) $53 \equiv 5 \pmod{8}$; 3) $a^2 - b^2 \equiv 0 \pmod{a - b}$; 4) $-73 \equiv r \pmod{8}$, $0 \leq r < 8$.

42. 1) $N \equiv 0 \pmod{2}$; 2) $N \equiv 1 \pmod{2}$, или $N \equiv -1 \pmod{2}$; 3) $N \equiv 3 \pmod{5}$, или $N \equiv -2 \pmod{5}$; 4) $N \equiv -2 \pmod{7}$, или $N \equiv 5 \pmod{7}$.

43. m .

44. Искомые остатки равны остаткам от деления на m чисел $r_1 \pm r_2$ и $r_1 \cdot r_2$. Сказанное выражают также сравнения $a_1 \pm a_2 \equiv r_1 \pm r_2 \pmod{m}$, $a_1 \cdot a_2 \equiv r_1 \cdot r_2 \pmod{m}$.

45. Сохранится.

46. $t \equiv 0 \pmod{3}$.

47. Если $N = a_0 + a_1 10 + \dots + a_n 10^n$, то 1) $N \equiv a_0 + a_1 + \dots \pmod{9}$, 2) $N \equiv a_0 - a_1 + \dots + (-1)^n a_n \pmod{11}$.

48. Согласно следствию из свойства 5-го: $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{(d, m)}}$, но $(d, m) = d_1$.

49. $C_{p-1}^k = \frac{(p-1)(p-2)\dots(p-k)}{1 \cdot 2 \dots k}$, или $1 \cdot 2 \dots k \cdot C_{p-1}^k = (p-1)(p-2)\dots(p-k)$. Но $p - i \equiv -i \pmod{p}$, кроме того, $(i, p) = 1$, поэтому $C_{p-1}^k \equiv (-1)^k \pmod{p}$.

50. По нечетному модулю m вычеты систем чисел

$$1, 2, \dots, \frac{m-1}{2}, \frac{m+1}{2}, \dots, m-1$$

и

$$1, 2, \dots, \frac{m-1}{2}, -\frac{m-1}{2}, \dots, -1$$

попарно сравнимы. Поэтому

$$(m-1)! \equiv (-1)^{\frac{m-1}{2}} \left[\left(\frac{m-1}{2} \right)! \right]^2 \pmod{m}.$$

51. C_1 и C_5 ; $p = 6n \pm 1$; $p \equiv \pm 1 \pmod{6}$.

52. Следует из того, что $a \equiv b \pmod{m}$ влечет за собой

$$ak \equiv bk \pmod{m}.$$

53. Не всегда; ak и a принадлежат одному и тому же классу вычетов по модулю m в том и только в том случае, когда k при-

надлежит классу C_1 по модулю $\frac{m}{d}$, где $(a, m) = d$, потому что из $ak \equiv a \pmod{m}$ следует $k \equiv 1 \pmod{\frac{m}{d}}$.

54. Принадлежат всегда, если $(m, n) = 1$, принадлежат не всегда, если $(m, n) > 1$.

55. Двум, (d) .

56. 1) C_3, C_{11} ; 2) C_8 .

57. C_2, C_4, C_5, C_6, C_8 .

58. П. С. В. $1 \pmod{14}$: 0, 1, 2, ..., 13; 1, 2, ..., 14; 0, $\pm 1, \dots$, $\pm 6, 7$.

Пр. С. В. $\pmod{14}$: 1, 3, 5, 9, 11, 13; то же; $\pm 1, \pm 3, \pm 5$.

59. 1, 2, ..., $p-1$; $\pm 1 \pm 2, \dots, \pm \frac{p-1}{2}$.

60. Отсутствует представитель нулевого класса.

61. Составить наименьшие положительные вычеты указанных чисел по модулю 7.

62. Получаются полные системы наименьших положительных вычетов.

63. Указанная совокупность чисел получается, если в линейной форме $dx + a$ x пробегает полную систему вычетов по модулю n .

64. Числа указанной системы получаются, когда в линейной форме $2x$, где $(2, m) = 1$, x пробегает все значения из полной системы вычетов по модулю m : 1, 2, ..., m .

65. 1) 3·1, 3·2, ..., 3·10, 3·11; 2) 3·1, 3·3, 3·5, 3·7.

66. Пусть $a = a_1 d$, $m = m_1 d$, так что $(a_1, m_1) = 1$. Число $ax \mid m$, или $a_1 x \mid m_1$, тогда и только тогда, когда $x \mid m_1$; в полной системе вычетов 1, 2, ..., $m_1, \dots, 2m_1, \dots, dm_1 = m$ таких чисел имеется d .

67. 1) $\varphi(b)$; 2) $\varphi(2) + \varphi(3) + \dots + \varphi(n)$.

68. 1) 144, 2) 768, 3) $\varphi(13 \cdot 17) = 12 \cdot 16 = 192$. 4) $\varphi(9 \cdot 15 \cdot 42) = \varphi(2 \cdot 3^4 \cdot 5 \cdot 7) = 1296$.

69. 1) $\varphi(5^\alpha) = 5^{\alpha-1} \cdot 4 = 100$, $5^{\alpha-1} = 5^2$, $\alpha = 3$; $n = 125$;

2) $\varphi(3^\alpha \cdot 5^\beta) = 3^{\alpha-1} \cdot 2 \cdot 5^{\beta-1} \cdot 4 = 600$, $3^{\alpha-1} \cdot 5^{\beta-1} = 3^1 \cdot 5^2$, $\alpha = 2$, $\beta = 3$; $n = 1125$.

70.
$$\frac{\varphi(m)}{m} = 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_h} + \dots$$

$$\dots + (-1)^k \frac{1}{p_1 p_2 \dots p_k}.$$

71. 1) В сегменте [1, 385] содержится 5 П. С. В. по модулю 77, а в каждой из последних имеется $\varphi(77) = 60$ натуральных чисел, взаимно простых с 77. Итак, искомым чисел всего $5 \cdot \varphi(77) = 300$.

2) В общем случае получается аналогично $k \cdot \varphi(m)$.

72. 1) В сегменте [301, 540] содержится 10 П. С. В. по модулю 24, поэтому надо найти $10 \cdot \varphi(24) = 10 \cdot 8 = 80$;

1 П. С. В. — полная система вычетов, Пр. С. В. — приведенная система вычетов.

2) аналогично — $9 \cdot \varphi(35) = 216$.

73. Указанная система чисел содержит 2 полные системы вычетов по модулю n , поэтому искомое число равно $2\varphi(n)$.

74. Пусть n нечетно, тогда $(2, n) = 1$ и $\varphi(2n) = \varphi(2) \cdot \varphi(n) = \varphi(n)$. Если n нечетно, то $n = 2^a \cdot n_1$, $(2, n_1) = 1$, $\varphi(2n) = \varphi(2^{a+1} \cdot n_1) = 2^a \cdot \varphi(n_1)$, а $\varphi(n) = \varphi(2^a \cdot n_1) = 2^{a-1} \cdot \varphi(n_1)$, так что $\varphi(2n) = 2\varphi(n)$. Итак, $\varphi(2n) = \varphi(n)$ для нечетных n и только для них.

75. 1) Следует из того, что вычеты Пр. С. В. по модулю m можно сгруппировать в пары, а именно: если a принадлежит Пр. С. В. по модулю m то и $m - a$, потому что $(a, m) = (m - a, m)$ (см. задачу 11). При этом $a \neq m - a$, если $(a, m) = 1$ и $m > 2$. В самом деле, из $a = m - a$ следовало бы $2a = m$, $(a, m) = (a, 2a) = a = 1$, $m = 2$, что исключается.

2) При $m > 2$ вычеты каждой из указанных групп имеют сумму m , а таких групп имеется $\frac{1}{2} \varphi(m)$, поэтому их общая сумма равна $\frac{1}{2} m \varphi(m)$; случай, когда $m = 2$, проверяется непосредственно.

76. 1) Пусть искомое количество $\varphi_d(n)$ (так что $\varphi(n) = \varphi_1(n)$).

Для интересующих нас чисел $dx (\leq n)$ $(n, dx) = d$, а

$\left(\frac{n}{d}, x\right) = 1$ и $x \leq \frac{n}{d}$, поэтому $\varphi_d(n) = \varphi_1\left(\frac{n}{d}\right) = \varphi\left(\frac{n}{d}\right)$;

2) а) $\varphi_{12}(624) = \varphi(52) = 24$; б) $\varphi_{20}(580) = \varphi(59) = 58$; в) $\varphi_{17}(595) = \varphi(35) = 24$.

77. Имеем $\sum_n \varphi(d_i) = \sum_n \varphi_{d_i}(n)$; в правой части собраны все числа $\leq n$, которые имеют с n Н. О. Д. d_1, d_2, \dots, d_k ; таким образом, исчерпываются все числа от 1 до n , значит, и $\sum_n \varphi(d_i) = n$.

78. 1) 7; 2) 7; 3) 5; 4) 65; 5) 14; 6) 22.

79. 1) $4^{113} \equiv 4x \pmod{92}$. $4^{112} \equiv x \pmod{23}$, $4^{112} \equiv 16 \pmod{23}$, $4^{113} \equiv 64 \pmod{92}$;

2) $6^{76} \equiv 2x \pmod{26}$, $3 \cdot 6^{75} \equiv x \pmod{13}$, $6^{75} \equiv 8 \pmod{13}$, $3 \cdot 6^{75} \equiv 11 \pmod{13}$, $6^{75} \equiv 22 \pmod{26}$;

3) $21^{83} \equiv 3x \pmod{24}$, $7 \cdot 21^{82} \equiv x \pmod{8}$, $21^{82} \equiv 21 \pmod{24}$;

4) $35^{150} \equiv 25x \pmod{17 \cdot 25}$, $49 \cdot 35^{148} \equiv x \pmod{17}$, $35^{148} \equiv 1 \pmod{17}$, $49 \cdot 35^{148} \equiv -2 \pmod{17}$, $35^{150} \equiv 375 \pmod{425}$.

80. 1) 1; 2) 5; 3) $3 \cdot 5^{75} \equiv x \equiv 3 \pmod{132}$; $4 \cdot 7^{100} \equiv y \equiv 4 \pmod{132}$; $x + y \equiv 7 \pmod{132}$.

81. Надо найти остаток от деления на 100: 1) $2^{153} \equiv 4x \equiv 92 \pmod{100}$; 2) $3^{219} \equiv x \equiv 67 \pmod{100}$.

82. 1) если $(a, 7) = 1$, то $a^6 - 1 \mid 7$, поэтому и $a^{12} - 1 = (a^6 - 1)(a^6 + 1) \mid 7$;

2) если $(a, 65) = 1$ и $(b, 65) = 1$, то $a^{12} \equiv b^{12} \equiv 1 \pmod{13}$, $a^{12} - b^{12} \equiv 0 \pmod{13}$; $a^4 \equiv b^4 \equiv 1 \pmod{5}$, $a^{12} \equiv b^{12} \pmod{5}$, $a^{12} - b^{12} \equiv 0 \pmod{5}$.

Итак, $a^{12} - b^{12} \mid 5 \cdot 13 = 65$.

83. 1) По малой теореме Ферма $(a+b)^p \equiv a+b \pmod{p}$, $a^p \equiv a \pmod{p}$, $b^p \equiv b \pmod{p}$; $a^p + b^p \equiv a+b \pmod{p}$; итак, $(a+b)^p \equiv a^p + b^p \pmod{p}$.

2) Получается аналогично.

84. $(c_1 + c_2)^p = c_1^p + C_p^1 \cdot c_1^{p-1} \cdot c_2 + \dots + C_p^{p-1} \cdot c_1 \cdot c_2^{p-1} + c_2^p \equiv c_1^p + c_2^p \pmod{p}$, так как C_p^1, C_p^2 и т. д. делятся на p . На основании предыдущего $(c_1 + c_2 + c_3)^p \equiv (c_1 + c_2)^p + c_3^p \equiv c_1^p + c_2^p + c_3^p \pmod{p}$ и т. д.

85. Так как $n-1 = 2700 = 36 \cdot 75$, $2^{36} \equiv 1 \pmod{37}$, $2^9 \equiv 26 \cdot 2^3 \equiv -9 \cdot 8 \equiv 1 \pmod{73}$, так что $2^{36} \equiv 1 \pmod{73}$, имеем $2^{36} \equiv 1 \pmod{37 \cdot 73}$, $2^{36 \cdot 75} \equiv 1 \pmod{37 \cdot 73}$, т. е. $2^{n-1} \equiv 1 \pmod{n}$.

86. 1) $1^{10} \equiv 2^{10} \equiv \dots \equiv 10^{10} \equiv 1 \pmod{11}$, поэтому и $1^{30} \equiv 2^{30} \equiv \dots \equiv 10^{30} \equiv 1 \pmod{11}$, так что $1^{30} + 2^{30} + \dots + 10^{30} \equiv 10 \equiv -1 \pmod{11}$; 2) аналогично.

87. $1 + 2 + \dots + (p-1) = \frac{p(p-1)}{2}$; $a^{p-1} \equiv 1 \pmod{p}$,

$a^{p(p-1)} \equiv 1 \pmod{p}$, $(a^{\frac{p(p-1)}{2}} - 1)(a^{\frac{p(p-1)}{2}} + 1) | p$. Итак, одна из скобок должна делиться на p , а обе скобки делиться не могут, так как иначе на нечетное p делилась бы и их разность 2, что невозможно. Если $p=2$, $(a, 2)=1$, то $a+1$ и $a-1$ четны и делятся на 2.

88. Имеем $a^p - b^p = (a-b)M$, где $M = a^{p-1} + a^{p-2} \times \dots + b^{p-1}$. По малой теореме Ферма для любого простого p $a^p \equiv a \pmod{p}$, $b^p \equiv b \pmod{p}$, так что $a^p - b^p \equiv a - b \pmod{p}$. Из данного условия $a^p - b^p \equiv 0 \pmod{p}$ следует поэтому, что $a - b \equiv 0 \pmod{p}$, или $a \equiv b \pmod{p}$, так что $a^i \equiv b^i \pmod{p}$. Но тогда при $(a, p)=1$ $M \equiv a^{p-1} + \dots + a^{p-1} \equiv p \equiv 0 \pmod{p}$ и $a^p - b^p | p^2$; случай, когда $a | p$, ясен сам по себе.

89. 1) $x \equiv -3 \pmod{7}$; 2) $x_1 \equiv 2 \pmod{5}$; $x_2 \equiv -2 \pmod{5}$; 3) $x_1 \equiv -1 \pmod{13}$; $x_2 \equiv -2 \pmod{13}$; 4) $x_1 \equiv 3 \pmod{11}$, $x_2 \equiv 4 \pmod{11}$; 5) $x_1 \equiv -1 \pmod{6}$, $x_2 \equiv 3 \pmod{6}$; 6) неразрешимо.

90. 1) $x \equiv 5 \pmod{7}$; 2) $x \equiv 4 \pmod{11}$; 3) $x \equiv 6 \pmod{17}$; 4) $x \equiv 3 \pmod{8}$; 5) $x \equiv 4, 11, 18, 25, 32 \pmod{35}$; 6) неразрешимо; 7) $x \equiv 21 \pmod{36}$; указание: заменить $x = 3y$; 8) $x \equiv 7 \pmod{15}$; 9) неразрешимо; 10) $x \equiv 14 \pmod{35}$; указание: заменить $x = 7y$.

91. 1) $x \equiv 7 \pmod{25}$; 2) $x \equiv 5 \pmod{11}$; 3) $x \equiv 5 \pmod{11}$; 3) $x \equiv 11 \pmod{24}$; 5) $x \equiv 7 \pmod{31}$; 6) $x \equiv 8 \pmod{35}$.

92. 1) $x \equiv 8 \pmod{17}$; 2) $x \equiv 9 \pmod{19}$; 3) $x \equiv 11 \pmod{58}$.

93. 1) $-10x \equiv 5 \pmod{17}$, $-2x \equiv 1 \pmod{17}$, $-2x \equiv -16 \pmod{17}$, $x \equiv 8 \pmod{17}$; 2) $-6x \equiv 3 \pmod{19}$, $-2x \equiv 1 \pmod{19}$, $-2x \equiv -18 \pmod{19}$, $x \equiv 9 \pmod{19}$; 3) $27x \equiv -5 \pmod{58}$, $9x \equiv -17 \pmod{58}$, $9x \equiv -17 + 116 = 99 \pmod{58}$, $x \equiv 11 \pmod{58}$.

94. Вытекает из того, что сравнение $kx \equiv l \pmod{p}$, где $(k, p)=1$, всегда имеет единственное решение.

95. 1) $7, \frac{2}{45}$; 2) $-48, 0,7$; 3) $0, 0,73$; 4) $-1, \frac{8}{23}$; 5) $4, \sqrt{19}-4$; 6) $9, \sqrt{17}-4$; 7) $3, \sin \frac{\pi}{4}$; 8) $-3, 1-\sin \frac{\pi}{4}$; 9) $4, \sqrt{2}-1,3$; 10) $7, \sqrt{8}+\sqrt{23}-7$; 11) $3, -\lg 0,7$; 12) $2, \sqrt[3]{20}-2$.

96. Пусть $a = mq + r$, $0 \leq r < m$, тогда $\frac{a}{m} = q + \frac{r}{m}$, где $q = \left[\frac{a}{m} \right]$ и $\frac{r}{m} = \left\{ \frac{a}{m} \right\}$. Остаток r является абсолютно наименьшим вычетом по модулю m , если $r \leq \frac{1}{2}m$, или $\frac{r}{m} \leq \frac{1}{2}$, т. е. когда $\left\{ \frac{a}{m} \right\} \leq \frac{1}{2}$. Остаток r не является абсолютно наименьшим вычетом, когда $r > \frac{1}{2}m$, или $\frac{r}{m} > \frac{1}{2}$, т. е. когда $\left\{ \frac{a}{m} \right\} > \frac{1}{2}$.

97. 1) Уравнение прямой выражаем в форме $y = \frac{-3x+4}{5}$; искомое число равно $\left[\left| \frac{-47}{5} \right| \right] = \left[\frac{47}{5} \right] = 9$; 2) $\left[\frac{103}{5} \right] = 20$.

98. 1) Уравнение прямой выражаем в форме $x = \frac{-3y+8}{5}$; искомое число равно $\left[\left| \frac{-61}{5} \right| \right] = \left[\frac{61}{5} \right] = 12$; 2) $\left[\frac{92}{5} \right] = 18$.

99. $\alpha + n - 1 < [x + n] \leq \alpha + n$, откуда $\alpha - 1 < [x + n] - n \leq \alpha$, а так как $[x + n] - n$ — целое, то $[x + n] - n = [x]$ и $[x + n] = [x] + n$.

100. 1) $\frac{137}{31} = (4, 2, 2, 1, 1, 2)$, 2) $\frac{521}{143} = (3, 1, 1, 1, 4, 10)$
 $\delta_k = \frac{1}{0}, \frac{4}{1}, \frac{9}{2}, \frac{22}{5}, \frac{31}{7}, \frac{53}{12}, \frac{137}{31}$; $\delta_k = \frac{1}{0}, \frac{3}{1}, \frac{4}{1}, \frac{7}{2}, \frac{11}{3}, \frac{51}{14}, \frac{521}{143}$;
 3) $\frac{247}{74} = (3, 2, 1, 24)$; 4) $-\frac{313}{57} = (-6, 1, 1, 28)$;
 $\delta_k = \frac{1}{0}, \frac{3}{1}, \frac{7}{2}, \frac{10}{3}, \frac{247}{74}$; $\delta_k = \frac{1}{0}, \frac{-6}{1}, \frac{-5}{1}, \frac{-11}{2}, \frac{-33}{57}$;
 5) $\frac{77}{187} = (0, 2, 2, 3)$; 6) $\frac{-83}{217} = (-1, 1, 1, 1, 1, 1, 2, 6)$;
 $\delta_k = \frac{1}{0}, \frac{0}{1}, \frac{1}{2}, \frac{2}{5}, \frac{7}{17}$; $\delta_k = \frac{1}{0}, \frac{-1}{1}, \frac{0}{1}, \frac{-1}{2}, \frac{-1}{3}, \frac{-2}{5}, \frac{-3}{8}, \frac{-5}{13}, \frac{-13}{34}, \frac{-83}{217}$;

$$101. 1) \quad 3953 \mid \frac{871}{4} \mid \frac{469}{1} \mid \frac{402}{1} \mid \frac{67}{6}$$

$$\delta_k = \frac{1}{0}, \frac{4}{1}, \frac{5}{1}, \frac{9}{2}, \frac{59}{13}, \frac{871}{3953} = \frac{13}{59};$$

$$2) \quad 6059 \mid \frac{1241}{4} \mid \frac{1095}{1} \mid \frac{146}{7} \mid \frac{73}{2}$$

$$\delta_k = \frac{1}{0}, \frac{4}{1}, \frac{5}{1}, \frac{39}{8}, \frac{83}{17}, \frac{1241}{6059} = \frac{17}{83};$$

$$3) \quad 6821 \mid \frac{2147}{3} \mid \frac{380}{5} \mid \frac{247}{1} \mid \frac{133}{1} \mid \frac{114}{1} \mid \frac{19}{6}$$

$$\delta_k = \frac{1}{0}, \frac{3}{1}, \frac{16}{5}, \frac{19}{6}, \frac{35}{11}, \frac{54}{17}, \frac{359}{113} = \frac{6821}{2147};$$

$$4) \quad 32671 \mid \frac{10\ 027}{3} \mid \frac{2\ 590}{3} \mid \frac{2\ 257}{1} \mid \frac{333}{6} \mid \frac{259}{1} \mid \frac{74}{3} \mid \frac{37}{2}$$

$$\delta_k = \frac{1}{0}, \frac{3}{1}, \frac{10}{3}, \frac{13}{4}, \frac{88}{27}, \frac{101}{31}, \frac{391}{120}, \frac{883}{271} = \frac{32\ 671}{10\ 027}.$$

102. При решении пользуемся формулой $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k$; находим для $\frac{786}{285}$ предпоследнюю подходящую дробь

$$\frac{P_{k-1}}{Q_{k-1}} = \frac{91}{93} \text{ и несократимое значение } \frac{P_k}{Q_k} = \frac{262}{95}, \text{ обнаруживая}$$

попутно, что $k=6$ и $d=(786, 285)=3$. Поэтому по указанной формуле $(-1)^6 = 262 \cdot 33 - 91 \cdot 95$, откуда $3 = 786 \cdot 33 - 285 \cdot 91$.

Возможны и другие представления, так как неопределенное уравнение $786x + 285y = 3$ имеет (см. след. §) бесчисленное множество решений.

103. 1) $x \equiv 31 \pmod{183}$; 2) $x \equiv 47 \pmod{241}$; 3) неразрешимо.

104. 1) $x \equiv 41, 190, 339 \pmod{447}$; 2) $x \equiv 61, 248 \pmod{422}$; 3) $x \equiv 39, 196, 353 \pmod{471}$.

105. 1) $x \equiv 73 \pmod{177}$; 2) $x \equiv 29 \pmod{311}$; 3) $x \equiv 48 \pmod{219}$.

106. 1) $x \equiv -1 + 16t$, $y \equiv -8 + 17t$; 2) $x \equiv -7 + 15t$, $y \equiv 12 - 23t$; 3) $x \equiv 9 + 37t$, $y \equiv 3 + 12t$; 4) неразрешимо; 5) $x \equiv 4 + 16t$, $y \equiv 7 - 11t$.

107. 26 апреля.

108. Решение уравнения можно свести к решению сравнения $ax \equiv c \pmod{b}$. Когда x пробегает П. С. В. по модулю b , ax также пробегает П. С. В. по модулю b . Получается единственное число, удовлетворяющее сравнению, а также уравнению. Указанному x соответствует единственное y .

109. Решение задачи об отгадывании дня рождения сводится к решению неопределенного уравнения $12x + 31y = s$, $(12, 31) = 1$, $1 \leq x \leq 31$ (или $1 \leq y \leq 12$), которое согласно предыдущей задаче решается однозначно.

110. $a = 8, b = 1$.

111. 1) $x = -4 + 13t, -100 < -4 + 13t < 150, -7 \leq t \leq 11$; 19 точек; 2) 7 точек; 3) 8 точек.

112. Следует из того, что угловой коэффициент прямой AB , т. е. $\frac{y_1 - y_2}{x_1 - x_2}$, есть сократимая дробь; случай, когда $x_1 = x_2$, ясен сам по себе.

113. Согласно предыдущей задаче (учитывая еще вершины треугольника) искомое число целых точек равно $(18,6) + (12,8) + (6,14) + 3 = 12$.

114. Прямая $ax + by = c$ имеет угловой коэффициент $-\frac{a}{b}$,

причем $(a, b) = 1$, поэтому $r = \sqrt{a^2 + b^2}$.

115. Искомое условие определяется разрешимостью неопределенного уравнения $\frac{c}{ab} = \frac{y}{a} + \frac{x}{b}$, или $ax + by = c$, а последнее имеет решение тогда и только тогда, когда $c \mid (a, b)$.

116. 1) $(81, 63) = 9, 23 - 17 \nmid 9$, система несовместна; 2) $(77, 91) = 7, 47 - 33 \mid 7$; система совместна.

117. 1) $x \equiv 115 \pmod{168}$; 2) $x \equiv 93 \pmod{140}$; 3) $x \equiv 102 \pmod{165}$; 4) неразрешима.

118. 1) $x \equiv 291 \pmod{420}$; 2) $x \equiv 251 \pmod{630}$; 3) $x \equiv 747 \pmod{840}$; 4) $x \equiv 371 \pmod{462}$.

119. 1) Надо найти решение системы сравнений $x \equiv 2 \pmod{5}, x \equiv 1 \pmod{8}, x \equiv 3 \pmod{11}$; $x \equiv 377 \pmod{440}$; 2) решается аналогично; $x \equiv 291 \pmod{819}$.

120. 1) 89, 209, 329, 449, 569, 689, 809, 929; 2) 244, 559, 874; 3) 731; 4) 841.

121. 299 и 439.

122. $x \equiv -351b_1 + 208b_2 + 144b_3 \pmod{936}$.

123. 1) $x^2 - 1 \equiv 0 \pmod{3}$; $x \equiv \pm 1 \pmod{3}$; 2) $x^4 + 2x^3 - 2x^2 + 2x - 1 \equiv 0 \pmod{5}$, неразрешимо; 3) $x^6 + 2x^5 - 2x + 3 \equiv 0 \pmod{7}$; $x_1 \equiv -2 \pmod{7}$; $x_2 \equiv -3 \pmod{7}$.

124. 1) $x^3 + 3x^2 - 3 \equiv (x-2)(x-3)(x-9) \pmod{17}$; 2) $x^3 + 11x^2 + 8x + 3 \equiv (x-1)(x+2)(x-13) \pmod{23}$; 3) $x^3 - 13x^2 - 3x + 11 \equiv (x+1)(x+3)(x-17) \pmod{31}$.

125. 1) $x^3 + 10x^2 - 6x - 5 \equiv 0 \pmod{23}$; 2) $x^3 - 13x^2 - 5x - 12 \equiv 0 \pmod{29}$; 3) $x^3 - 13x^2 + 3x + 9 \equiv 0 \pmod{31}$.

126. 1) Имеется второе разложение $f(x) \equiv x(x-8) \pmod{15}$; 2) единственное; 3) имеется второе разложение $f(x) \equiv (x+5)(x+7) \pmod{20}$.

127. 1) Не имеет; 2) имеет.

128. Вытекает из теоремы Вильсона, если учесть результат задачи 50.

129. Получается почленным перемножением сравнений $a \equiv a^p \pmod{p}$ и $(p-1)! \equiv -1 \pmod{p}$.

130. Если $p > 2$ простое, то по теореме Вильсона $(p-1)! + 1 \equiv 0 \pmod{p}$, или $(p-2)!(p-1) + 1 \equiv 0 \pmod{p}$, или $(p-2)! - 1 \equiv 0 \pmod{p}$. Если, наоборот, выполняется последнее соотношение, то p не может быть составным. Допустим, что имеется составное $p \geq 4$. Тогда оно имеет простой делитель

$p_1 \leq p-2$. (В самом деле, из $p = p_1 \cdot d$ следует, что $p \geq 2p_1$, и если $p_1 > p-2$, то $p > 2p-4$, $p < 4$, что противоречит условию.) Но $(p-2)! - 1$ не может делиться на простое число $p_1 \leq p-2$, так как $(p-2)!$ делится на любое такое число, а -1 нет.

131. 1) $x \equiv 11, 20 \pmod{21}$; 2) $x \equiv 4, 22 \pmod{33}$; 3) $x \equiv 2, 7, 24, 29 \pmod{55}$; 4) $x \equiv 3, 26, 28, 49, 63, 73, 84, 94 \pmod{105}$; 5) неразрешимо.

132. 1) $(-1, 0), (2, 1), (4, 5), (7, 32)$; 2) $(-6, -61), (-1, -1), (1, 1), (6, 41)$.

133. 1) $x \equiv 17 \pmod{112}$; 2) $x \equiv 11 \pmod{245}$; 3) $x \equiv 67 \pmod{153}$.

134. 1) $x \equiv \pm 12 \pmod{25}$; 2) $x \equiv \pm 15 \pmod{49}$; 3) $x \equiv \pm 47 \pmod{121}$; 4) $x \equiv \pm 63 \pmod{169}$.

135. Сравнение $x^2 + 3x + 5 \equiv 0 \pmod{121}$ не имеет решений.

136. 1) $x \equiv 13 \pmod{25}$; 2) $x \equiv 17 \pmod{49}$; 3) $x \equiv 18, 33 \pmod{49}$; 4) $x \equiv 11 \pmod{27}$; 5) $x \equiv 19 \pmod{125}$.

137. 1) $x \equiv 6 \pmod{25}$; 2) $x \equiv 14 \pmod{25}$; 3) $x \equiv 14 \pmod{49}$; $x \equiv 5, 12, 19, 26, 33, 40, 47, \pmod{49}$; 4) $x \equiv 33 \pmod{49}$; $x \equiv 2, 9, 16, 23, 30, 37, 44 \pmod{49}$.

138. $x \equiv 36, 136 \pmod{175}$.

139. 1) $(5x+4)^2 \equiv 36 \pmod{17}$; $x \equiv -2, -3 \pmod{17}$; 2) $(x+6)^2 \equiv 8 \pmod{23}$; $x \equiv 4, 7 \pmod{23}$; 3) $(x-1)^2 \equiv 17 \pmod{19}$; $x \equiv -5, 7 \pmod{19}$; 4) $(x-4)^2 \equiv 13 \pmod{17}$; $x \equiv -4, -5 \pmod{17}$; 5) $(x-5)^2 \equiv 5 \pmod{19}$; $x \equiv -4, -5 \pmod{19}$.

140. 1) Квадратичные вычеты: 1, 3, 4, 5, 9;

2) квадратичные вычеты: 1, 3, 4, 9, 10, 12;

3) квадратичные вычеты: 1, 4, 5, 6, 7, 9, 11, 16, 17;

4) квадратичные вычеты: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.

141. 1) разрешимо; 2) разрешимо; 3) неразрешимо; 4) неразрешимо.

142. Вытекает из того, что для данного сравнения $f(x) = x^2 - a$ и $f'(x) = 2x \not\equiv p$.

143. Сравнению могут удовлетворять только нечетные числа $x = 2t + 1$. Из $(2t+1)^2 \equiv a \pmod{2^a}$ или $4t(t+1) \equiv a-1 \pmod{2^a}$ вытекают необходимые условия разрешимости сравнения: 1) при $a=1$ $a \equiv 1 \pmod{2}$, т. е. имеем данное условие ($a, 2) = 1$; 2) при $a=2$ $a \equiv 1 \pmod{4}$, 3) при $a \geq 3$ $a \equiv 1 \pmod{8}$.

144. Необходимые условия разрешимости, найденные в предыдущей задаче, являются также для $a=1, 2, 3$ достаточными, а так как при этих условиях сравнение $4t(t+1) \equiv a-1 \pmod{2^a}$ выполняется тождественно, то решениями являются: 1) при $a=1$ $x \equiv 1 \pmod{2}$, 2) при $a=2$ $x \equiv 1, 3 \pmod{4}$, 3) при $a=3$ $x \equiv 1, 3, 5, 7 \pmod{8}$.

145. По модулю 4 представим нечетные числа в форме $x \equiv \pm(4t_1+1)$, тогда $(4t_1+1)^2 \equiv a \pmod{16}$, $8t_1 \equiv a-1 \pmod{16}$,

$t_1 \equiv \frac{a-1}{8} \pmod{2}$, $t_1 = t' + 2t$, где t — любое целое. Поэтому

$x \equiv \pm(1+4t'+8t)$ и $x \equiv \pm(x_4+8t)$, или $x \equiv \pm x_4; \pm(x_4+8) \pmod{16}$; где x_4 — значение x для $t=0$.

146. Методом, указанным в предыдущей задаче, находим $x \equiv \pm 5, \pm 13 \pmod{16}$.

147. 1) 1; 2) -1; 3) -1; 4) -1; 5) 1; 6) 1; 7) -1; 8) -1; 9) -1; 10) 1.

148. 1) — 1; 2) — 1; 3) — 1; 4) 1; 5) — 1.

149. 1) Проходят; 2) не проходят; 3) проходят; 4) не проходят.

150. 1) разрешимо; 2) неразрешимо; 3) неразрешимо; 4) разрешимо; 5) неразрешимо; 6) неразрешимо; 7) разрешимо.

151. 1) Рассмотреть сравнение $3a^2 - 5 \equiv 0 \pmod{17}$, преобразовать левую часть, чтобы старший коэффициент был равен 1, с помощью символа Лежандра исследовать вопрос о разрешимости полученного сравнения; $3a^2 - 5 \mid 17$ для $a \equiv \pm 8 \pmod{17}$; 2) делится для $a \equiv \pm 10 \pmod{23}$; 3) таких целых a не существует.

152. Доказательство усматривается непосредственно из определения символа Якоби и свойств символа Лежандра, если учесть, что

$$\frac{P-1}{2} \equiv \sum \frac{p-1}{2} \pmod{2}, \quad \frac{P^2-1}{8} \equiv \sum \frac{p^2-1}{8} \pmod{2} \text{ и}$$

$$\sum_{p,q} \frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_p \frac{p-1}{2} \cdot \sum_q \frac{q-1}{2} \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}.$$

Чтобы упростить рассмотрение, можно ограничиться частным случаем, когда $P = p_1 \cdot p_2$.

$$153. \quad \left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right), & \text{если } p \equiv 1 \pmod{4} \\ -\left(\frac{p}{3}\right), & \text{если } p \equiv 3 \pmod{4}, \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, & \text{если } p \equiv 1 \pmod{3}, \\ \left(\frac{2}{3}\right) = -1, & \text{если } p \equiv 2 \pmod{3}. \end{cases}$$

Итак, $\left(\frac{3}{p}\right) = 1$ тогда и только тогда, когда 1) $3p \equiv 3 \pmod{12}$ и $4p \equiv 4 \pmod{12}$, откуда $p \equiv 1 \pmod{12}$, или 2) $3p \equiv 9 \pmod{12}$ и $4p \equiv 8 \pmod{12}$, откуда $p \equiv -1 \equiv 11 \pmod{12}$.

$$154. \quad \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right),$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod{4}, \\ -1, & \text{если } p \equiv 3 \pmod{4}; \end{cases}$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{если } p \equiv 1 \pmod{4}, \\ -1 & \text{если } p \equiv 3 \pmod{4}; \end{cases}$$

$$\text{итак, } \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right).$$

Но $\left(\frac{p}{3}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod{3}, \\ -1, & \text{если } p \equiv 2 \pmod{3} \end{cases}$ (см. предыдущую задачу).

Таким образом, $\left(\frac{-3}{p}\right) = 1$ тогда и только тогда, когда $p \equiv 1 \pmod{3}$, т. е. p имеет вид $6n + 1$.

155. В указанном случае согласно критерию Эйлера $a^{\frac{p-1}{2}} \equiv a^{2k+1} \equiv 1 \pmod{p}$, откуда $(a^{k+1})^2 \equiv a \pmod{p}$, так что $x \equiv \pm a^{k+1} \pmod{p}$.

156. В указанном случае согласно критерию Эйлера $a^{\frac{p-1}{2}} \equiv a^{4k+2} \equiv 1 \pmod{p}$, откуда $(a^{2k+1} - 1)(a^{2k+1} + 1) \equiv 0 \pmod{p}$. Так как один из множителей должен делиться на p , а оба не могут (иначе $2 \mid p$, что невозможно), то либо $a^{2k+1} \equiv 1 \pmod{p}$, либо $a^{2k+1} \equiv -1 \pmod{p}$. В первом случае $a^{2k+2} \equiv a \pmod{p}$, а во втором $a^{2k+2} \equiv -a \pmod{p}$.

157. Согласно предыдущей задаче, либо 1) $a^{2k+2} \equiv a \pmod{p}$, так что $(a^{k+1})^2 \equiv a \pmod{p}$, и тогда $x \equiv \pm a^{k+1} \pmod{p}$; либо 2) $a^{2k+2} \equiv -a \pmod{p}$; в этом случае учтем, что по данному

модулю $\left(\frac{2}{p}\right) = -1$, вследствие чего $2^{\frac{p-1}{2}} = 2^{4k+2} \equiv -1 \pmod{p}$, так что $(2^{k+1} \cdot a^{k+1})^2 \equiv a \pmod{p}$ и $x \equiv \pm 2^{k+1} \cdot a^{k+1} \pmod{p}$.

158. 1) $x \equiv \pm 8 \pmod{19}$; 2) $x \equiv \pm 8 \pmod{29}$.

159. 1) Согласно теореме гл. III, § 7, п. 1 сравнение эквивалентно системе $x^2 \equiv a \pmod{2^n}$, $x^2 \equiv a \pmod{p_1^{a_1}}$, ..., $x^2 \equiv a \pmod{p_k^{a_k}}$. В соответствии с п. 2 § 7 гл. III и результатами задач 143–145 необходимыми и достаточными условиями являются: $\left(\frac{a}{p_i}\right) = 1$, кроме того, при $\alpha = 1$ $a \equiv 1 \pmod{2}$, при $\alpha = 2$ $a \equiv 1 \pmod{4}$, при $\alpha \geq 3$ $a \equiv 1 \pmod{8}$. 2) Число решений при $\alpha = 0, 1$ 2^k , при $\alpha = 2$ 2^{k+1} , при $\alpha \geq 3$ 2^{k+2} .

160. Не может; вытекает из определения показателя по модулю.

161. Не может; вытекает из определения показателя по модулю.

162. 1) $5^0, 5^1, \dots, 5^5; 1, 5, 7, 11, 13, 17$; 2) $3^0, 3^1, 3^2, \dots, 3^{17}; 1, 3, 9, 8, 5, 15, 7, 2, 6, 18, 16, 10, 11, 14, 4, 12, 17, 13$.

163. Не может, так как показатель по модулю 26 является делителем $\varphi(26) = 12$.

164. Несравнимы; из сравнимости следовало бы, что 2^{17} сравнимо с 1 по модулю 11, а последнее невозможно, так как 1 не является показателем 2 по модулю 11, а остальные делители $\varphi(11)$ не делят 17.

165. 1) 16, является; 2) 18, является; 3) 3, не является; 4) 6, является; 5) 22, является; 6) 2, не является.

166. Наименьшее x , для которого $a^x \equiv 1 \pmod{a^n - 1}$, равно n , поэтому n является показателем для a по модулю $a^n - 1$, а $\varphi(a^n - 1) \mid n$.

$$167. 1) \frac{6}{(6,3)} = 2, \quad \frac{6}{(6,4)} = 3, \quad \frac{6}{(6,5)} = 6.$$

$$2) \frac{40}{(40,12)} = 10, \quad \frac{40}{(40,15)} = 8, \quad \frac{40}{(40,16)} = 5.$$

168. Из $a^{\delta} \equiv 1 \pmod{p}$ следует для четного δ , что $(a^{\delta/2} - 1)(a^{\delta/2} + 1) \mid p$. Одна из скобок должна делиться на p , первая не может (так как это противоречило бы тому, что a принадлежит показателю δ по модулю p), следовательно, на p делится вторая скобка, т. е. $a^{\delta/2} \equiv -1 \pmod{p}$.

169. Согласно свойствам показателей, установленным в гл. IV, § 1, п. 4, $a^{\gamma} - 1 \mid m_1$ только, если $\gamma \mid \delta_1$ и $a^{\gamma} - 1 \mid m_2$ только, если $\gamma \mid \delta_2$, поэтому (в силу того, что $(m_1, m_2) = 1$) $a^{\gamma} - 1 \mid m_1 \cdot m_2$ только в том случае, если $\gamma \mid [\delta_1, \delta_2]$. Наименьшее значение для γ , т. е. показатель δ для a по модулю $m_1 m_2$, равно, таким образом, $[\delta_1, \delta_2]$. Итак, $\delta = [\delta_1, \delta_2]$.

170. 1) 2 принадлежит показателям 4 (mod 5), 3 (mod 7) и 12 (mod 35). 2) 3 принадлежит показателям 4 (mod 5), 5 (mod 11) и 20 (mod 55).

171. 1) Из $(a_1 a_2)^{\delta_1 \delta_2} = (a_1^{\delta_1})^{\delta_2} \cdot (a_2^{\delta_2})^{\delta_1} \equiv 1 \pmod{m}$ следует, что $\delta_1 \delta_2 \mid \delta$; 2) по условию $a_1^{\delta \delta_2} \equiv a_1^{\delta \delta_2} \cdot (a_2^{\delta_2})^{\delta} \equiv (a_1 a_2)^{\delta \delta_2} \equiv 1 \pmod{m}$, поэтому $\delta \delta_2 \mid \delta_1$, откуда (в силу $(\delta_1, \delta_2) = 1$) $\delta \mid \delta_1$, аналогично $\delta \mid \delta_2$. Таким образом (в силу $(\delta_1, \delta_2) = 1$), $\delta \mid \delta_1 \delta_2$. Учитывая, что $\delta_1 \delta_2 \mid \delta$, получаем в данном случае $\delta = \delta_1 \delta_2$.

172. Так как $(3, 4) = 1$, то $14 \equiv 31 \cdot 10 \pmod{37}$ принадлежит показателю 12 по модулю 37.

173. 1) $7^1, 7^2, 7^3, 7^4, 7^5, 7^6$; 7, 20, 24, 23, 16, 25.

2) $9^1, 9^2, 9^4, 9^5, 9^7, 9^8$; 9, 7, 12, 34, 16, 33.

174. 1) 2, 6, 7, 8;

2) 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

175. 1) $x \equiv 3^0, 3^1, 3^2, 3^3, 3^4 \pmod{11}$, или $x \equiv 1, 3, 9, 5, 4 \pmod{11}$. 2) $x \equiv 4^0, 4^1, 4^2, 4^3, 4^4, 4^5 \pmod{13}$, или $x \equiv 1, 4, 3, 12, 9, 10 \pmod{13}$.

176. 1) $\varphi(16) = 8$; 2) $\varphi(42) = 12$; 3) $\varphi(72) = 32$; 4) $\varphi(88) = 40$.

177. 1) $\varphi(7) = 6$; 2) $\varphi(9) = 6$.

178. 5.

179. Для $m > 2$ $\varphi(m)$ четно (см. задачу 75), поэтому $\frac{1}{2} \varphi(m)$ — целое. Пусть a — квадратичный вычет по модулю m и $(a, m) = 1$;

тогда из $x^2 \equiv a \pmod{m}$ следует $x^{\varphi(m)} \equiv a^{\frac{1}{2} \varphi(m)} \equiv 1 \pmod{m}$.

Итак, a принадлежит показателю $\leq \frac{1}{2} \varphi(m)$ по модулю m , т. е.

не может быть первообразным корнем по этому модулю.

180. Первообразные корни x по модулю m удовлетворяют сравнению $x^{\varphi(m)} \equiv 1 \pmod{m}$, но не удовлетворяют такому сравнению с меньшей степенью. Для $m = 2$ $\varphi(2) = 1$, а для $m = 4$ $\varphi(4) = 2$. Итак, надо показать существование решений сравнений

$x^1 \equiv 1 \pmod{2}$ и $x^2 \equiv 1 \pmod{4}$, не удовлетворяющих таким же сравнениям с меньшей степенью. Такие решения имеются; их наименьшие положительные значения соответственно равны 1 и 3.

181. Можно представить $m = m_1 m_2$, $(m_1, m_2) = 1$, $m_1 > 2$, $m_2 > 2$. Если g — первообразный корень по модулю m , то он принадлежит показателю $\varphi(m_1)\varphi(m_2)$. Если, с другой стороны, g принадлежит показателю $\delta_1 \pmod{m_1}$ и $\delta_2 \pmod{m_2}$, то (см. 129 задачу) g принадлежит показателю $[\delta_1, \delta_2]$ по модулю $m_1 m_2$. Так как $\varphi(m_1) \mid \delta_1$, $\varphi(m_2) \mid \delta_2$, то $[\varphi(m_1), \varphi(m_2)] \mid [\delta_1, \delta_2]$, а поскольку m_1 и $m_2 > 2$, то $\varphi(m_1)$ и $\varphi(m_2)$ четны (см. задачу 35) и $[\varphi(m_1), \varphi(m_2)] < \varphi(m_1)\varphi(m_2)$; таким образом, $[\delta_1, \delta_2] < \varphi(m_1)\varphi(m_2)$ и g не может быть первообразным корнем по модулю m .

182. Доказывается аналогично тому, как это делалось в предыдущей задаче.

183. Первообразный корень g имел бы вид $g = 4k \pm 1$ и тогда $g^{2^{\alpha-2}} = (1 \pm 2^2 k)^{2^{\alpha-2}} = 1 \pm 2^{\alpha} \cdot k + 2^{\alpha+1} \cdot N$, где N — целое,

откуда $g^{2^{\alpha-2}} \equiv 1 \pmod{2^{\alpha}}$. Но $g^{2^{\alpha-2}} = g^{\frac{1}{2} \varphi(2^{\alpha})}$, если $\alpha > 2$, поэтому $g^{\frac{1}{2} \varphi(2^{\alpha})} \equiv 1 \pmod{2^{\alpha}}$, а это значит, что по модулю 2^{α} , где $\alpha > 2$, первообразных корней быть не может.

184. Для модулей $2, 4, p^{\alpha}, 2p^{\alpha}$, где p — нечетное простое, α — натуральное.

185. Приведенную систему вычетов по модулю 13 образуют числа

$$6^0, 6^1, 6^2, 6^3, 6^4, 6^5, 6^6, 6^7, 6^8, 6^9, 6^{10}, 6^{11};$$

их наименьшие положительные вычеты по модулю 13 равны соответственно:

$$1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11.$$

Поэтому искомая таблица имеет вид

N	0	1	2	3	4	5	6	7	8	9
0		0	5	8	10	9	1	7	3	4
1		2	11	6						

186. Приведенную систему вычетов по модулю 18 образуют числа

$$5^0, 5^1, 5^2, 5^3, 5^4, 5^5,$$

их наименьшие положительные вычеты по модулю 18 равны соответственно 1, 5, 7, 17, 13, 11.

Поэтому искомая таблица следующая

N	0	1	2	3	4	5	6	7	8	9
0		0	—	—	—	1	—	2	—	—
1		—	5	—	4	—	—	3		

Числа, не взаимно простые с модулем, не имеют индекса.

187. Первообразный корень g по нечетному простому p принадлежит четному показателю $p-1$, поэтому (см. задачу 128)

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \text{ откуда } \frac{p-1}{2} \equiv \text{ind}(-1) \equiv \text{ind}(p-1) \pmod{p-1}.$$

188. Для нечетного простого p $\text{ind}(p-1)! \equiv \text{ind} 1 + \text{ind} 2 + \dots + \text{ind}(p-1) \pmod{p-1}$. Так как совокупность индексов от 1 до $p-1$ составляет полную систему вычетов по модулю $p-1$, т. е. числа $1, 2, \dots, p-1$, то сумма правой части сравнения $\equiv \frac{p(p-1)}{2}$, или $\frac{(p-1)}{2}(p-1) + \frac{p-1}{2}$; но $\frac{p-1}{2}(p-1) \equiv 0 \pmod{p-1}$ и $\frac{p-1}{2} \equiv \text{ind}(-1) \pmod{p-1}$ (см. предыдущую задачу), поэтому $\text{ind}(p-1)! \equiv \text{ind}(-1) \pmod{p-1}$, откуда $(p-1)! \equiv -1 \pmod{p}$, или $(p-1)! + 1 \equiv 0 \pmod{p}$.

189. $54 \equiv 11^x \equiv 5^{26} \pmod{73}$; переходя к индексам при основании 5, имеем $x \text{ ind } 11 \equiv 26 \pmod{72}$, или $55x \equiv 26 \pmod{72}$, откуда $x \equiv \text{ind}_{11} 54 \equiv 62 \pmod{72}$.

190. $66 \equiv 13^x \equiv 7^{63} \pmod{71}$; переходя к индексам при основании 7, имеем $x \text{ ind } 13 \equiv 63 \pmod{70}$, или $39x \equiv 63 \pmod{70}$, откуда $13x \equiv 21 \pmod{70}$, $13x \equiv 91 \pmod{70}$ и окончательно $x \equiv \text{ind}_{13} 66 \equiv 7 \pmod{70}$.

191. 1) $x \equiv 7 \pmod{43}$; 2) неразрешимо; 3) $x \equiv 4,33 \pmod{37}$; 4) $x \equiv 30, 53 \pmod{83}$; 5) $x \equiv \pm 253 \pmod{73^2}$; 6) $x \equiv \pm 1634 \pmod{59^2}$.

192. 1) $x \equiv 51 \pmod{97}$; 2) $x \equiv 30 \pmod{73}$; 3) $x \equiv 32 \pmod{79}$; 4) $x \equiv 44 \pmod{83}$.

193. 1) $x \equiv 59 \pmod{71}$; 2) неразрешимо; 3) $x \equiv 36, 45, 41 \pmod{61}$; 4) $x \equiv 6, 65, 59, 73, 14, 20 \pmod{79}$.

194. 1) 60; 2) 8; 3) 8; 4) 19; 5) искомое число — наименьший положительный вычет решения сравнения $x \equiv 175^{411} \pmod{629}$. Это сравнение равносильно системе $x \equiv 175^{411} \pmod{17}$, $x \equiv 175^{411} \pmod{37}$; первое сравнение дает решение $x \equiv 11 \pmod{17}$, второе — $x \equiv 36 \pmod{37}$; система, составленная из последних двух сравнений, имеет решение $x \equiv 147 \pmod{629}$, так что искомый остаток 147.

195. $\text{ind } a$ 2.

196. 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.

197. 1) 7; 2) 13; 3) 23; 4) 5; 5) 10 принадлежит показателям 3 $\pmod{37}$ и 46 $\pmod{47}$, а поэтому (см. 129 задачу) показателю $[3, 46] = 138 \pmod{1739}$; 6) 32 принадлежит показателям 12 $\pmod{61}$ и 7 $\pmod{71}$, а поэтому показателю $[12, 7] = 84 \pmod{4331}$.

198. 1) 10; 2) неразрешимо; 3) 2.

199. Если $N = a_0 + a_1 g' + \dots + a_n g^n$, $g^k \equiv r'_k \pmod{m}$, то $N \equiv R'_m \pmod{m}$, где $R'_m = a_0 r'_0 + \dots + a_n r'_n$.

200. Аналогичны соответствующим признакам в десятичной системе счисления при делении N на 9 и 3.

201. Аналогичны соответствующим признакам в десятичной системе счисления при делении N на 11.

202. 1) 3; 2) 33; 3) 22.

203. $R'_6 = 3 + 4 + 5 + 2 + 1 \equiv 3 \pmod{6}$.

204. 1) 2, 3, 4, 6, 12; 2) 2, 3, 4, 6, 8, 12, 24.

205. В системе счисления с основанием $M+1$, где $M=[1, 2, 3, \dots, n]$ — Н. О. К. всех чисел от 1 до n .

206. 1) 18, 28, 3, 21, 58, 33, 8, 44, 96; 2) 6, 2, 6, 42, 16, 6, 6; 3) 2, 2; 2, 22; 4, 48; 3, 13.

207. 1) 1, 1, 12, 2, 1, 2, 9, 2, 1; 2) 2, 10, 4, 1, 2, 10, 12.

208. $\frac{1}{39} = 0, (025641)$, $\frac{2}{39} = 0, (051282)$, $\frac{7}{39} = 0, (179489)$,

$\frac{14}{39} = 0, (358974)$.

209. 1) Решая сравнение $a \equiv 10^5 \pmod{73}$, находим $a = 63$; 2) аналогично находим $a = 22$.

210. 1) Решая $10^x \equiv 6 \pmod{17}$ и учитывая, что $x < 16$, находим $x = 5$, так что $\frac{6}{17} = 0, (35294 \dots 5882)$; 2) 1-й способ: решая $10^x \equiv 16 \pmod{41}$ и учитывая, что $x < 5$, находим $x = 3$, так что $\frac{16}{41} = 0, (39024)$; 2-й способ: умножаем 02439 на 16 и получаем 39024; 2-й способ применяется независимо от дополнительного условия.

211. 1) 948717 — период дроби $\frac{37}{39}$; 2) 999999; 3) 2948715, если слева отбросить двойку и прибавить ее к полученному числу, то получается число из 1).

212. 1) Вытекает из того, что период Q'_m дроби $\frac{k}{b}$ отличается от периода Q_m дроби $\frac{1}{b}$ только циклической перестановкой;

2) $\frac{1}{b} \cdot b = \frac{Q_m b}{10^m} + \frac{Q_m b}{10^{2m}} + \dots = 1 = 0, (99 \dots 9)$, откуда $Q_m b = \overbrace{99 \dots 9}^m = 10^m - 1$; 3) $Q_m K = Q_m (nb + k) = \overbrace{Q_m b}^m n + Q_m k = (10^m - 1)n + Q'_m = 10^m \cdot n + Q'_m - n = \overbrace{n Q'_m}^m - n$.

213. Отличие от свойств, отмеченных в предыдущей задаче, только в 1): произведения распадаются на d групп чисел с m цифрами в каждой, отличающимися между собой в группе только циклической перестановкой.

214. Пусть 10 по модулю p принадлежит четному показателю $2n$, тогда $10^n \equiv -1 \equiv p-1 \pmod{p}$ (см. задачу 128), так что через n делений 1 на p должен появиться остаток $p-1$.

Если теперь

$10 \cdot 1 = pq_1 + r_1$, то $10(p-1) = p(9-q_1) + (p-r_1)$,
 $0 < p-r_1 < p$, если $10 \cdot r_1 = pq_2 + r_2$, то $10(p-r_1) = p(9-q_2) + (p-r_2)$, $0 < p-r_2 < p$ и т. д.

Итак, 1) среди остатков деления $1:p$ должен появиться остаток $p-1$ и тогда можно сказать, что первой полупериод завершен; 2) цифры второго полупериода дополняют цифры первого до девяти. Случай, когда a делят на p , $a < p$, доказывается аналогично.

215. 1) Решая $\frac{107}{143} = \frac{a}{11} + \frac{b}{13}$, находим $a = 4$, $b = 5$;

$$\frac{4}{11} = 0, (36), \frac{5}{13} = 0, (384615),$$

$$\frac{4}{11} = 0, 363\ 636 \dots$$

$$\frac{5}{13} = 0, 384\ 615 \dots$$

$$\frac{107}{143} = 0, 748\ 251 \dots$$

2) решая $\frac{123}{133} = \frac{a}{7} + \frac{b}{19}$, находим $a = 5$, $b = 4$; чтобы найти период $\frac{4}{19}$, решаем $10^x \equiv 1 \pmod{19}$, откуда $x = 17$, итак,

$$\frac{5}{7} = 0, 714\ 285\ 714\ 285\ 714\ 285 \dots$$

$$\frac{4}{19} = 0, 210\ 526\ 315\ 789\ 473\ 684 \dots$$

$$\frac{123}{133} = 0, 924\ 812\ 030\ 075\ 187\ 969 \dots$$

216. 2) Результат неверен, однако проверкой по модулям 9 и 11 этого обнаружить нельзя.

217. $Q^k + R = S$, поэтому если $Q \equiv q \pmod{m}$, $R \equiv r \pmod{m}$, $S \equiv s \pmod{m}$, то $q^k + r \equiv s \pmod{m}$.

218. Должно быть $271^2 + 377 = 73818$, по модулю 9 это подтверждается.

219. $\alpha = ((1)) = (1, 1, \dots)$

$$\begin{array}{c|ccccccc} q_k & 1 & 1 & 1 & 1 & 1 & 1 & 1 \dots \\ \hline \delta_k = \frac{1}{0} & \frac{1}{1}, & \frac{2}{1}, & \frac{3}{2}, & \frac{5}{3}, & \frac{8}{5}, & \frac{13}{8}, & \frac{21}{13}, \dots \end{array}$$

В ряде Фибоначчи $1, 1, 2, 3, 5, 8, 13, \dots$ $a_n = u_{n-1} + u_{n-2}$.

220. Разлагаем в цепную дробь δ_k , чтобы найти $\delta_{k-1} = \frac{P_{k-1}}{Q_{k-1}}$, затем используем формулу (5) на стр. 165.

$$\begin{aligned} 1) \quad \delta_k &= \frac{10}{3} = (3, 3), \quad \delta_{k-1} = \frac{3}{1}; \quad \alpha = \frac{\sqrt{2} \cdot 10 + 3}{\sqrt{2} \cdot 3 + 1} = \\ &= \frac{57 - \sqrt{2}}{17}; \end{aligned}$$

$$2) \delta_k = \frac{43}{17} = (2, 1, 1, 8), \delta_{k-1} = \frac{5}{2}; \alpha = \frac{\sqrt{5 \cdot 43 + 5}}{\sqrt{5 \cdot 17 + 2}} = \frac{3645 - \sqrt{5}}{1441}.$$

221. Находим разложения для δ_k и α_{k+1} и присоединяем к первому разложению второе.

$$1) \frac{10}{7} = (1, 2, 3); \sqrt{3} = (1, (1, 2)); \alpha = (1, 2, 3, 1, (1, 2));$$

$$2) \frac{37}{13} = (2, 1, 5, 2); \frac{1 + \sqrt{3}}{2} = (1, (2, 1));$$

$$\alpha = (2, 1, 5, 2, 1, (2, 1)).$$

222. Надо найти по формуле (5) стр. 165 остаточное число α_{k+1} и убедиться в том, что оно > 1 .

$$1) \frac{19}{6} = (3, 6); \sqrt{10} = \frac{19x + 3}{6x + 1}; \quad x = 3 + \sqrt{10} > 1;$$

$$1, \quad \frac{3}{1}, \quad \frac{19}{6}.$$

$$2) \frac{37}{14} = (2, 1, 1, 1, 4); \sqrt{7} = \frac{37x + 8}{14x + 3}; \quad x = \frac{2 + \sqrt{7}}{3} > 1;$$

$$1, \quad \frac{2}{1}, \quad \frac{3}{1}, \quad \frac{5}{2}, \quad \frac{8}{3}, \quad \frac{37}{14}.$$

$$223. 1) |OM_{k-1}, OM_\alpha, OM_k|; 2) \rhd M_\alpha OM_k < \rhd M_\alpha OM_{k-1}.$$

$$224. 1) \frac{N}{n} \approx \frac{N_1}{n_1} = \delta_6 = \frac{385}{79} \text{ (с избытком)}, \varepsilon < \frac{1}{79 \cdot 150} < 0,0001;$$

$$2) \frac{N}{n} \approx \frac{N_1}{n_1} = \delta_3 = \frac{23}{4} \text{ (с недостатком)}, \varepsilon < \frac{1}{4 \cdot 149} < 0,01;$$

$$3) \frac{N}{n} \approx \frac{N_1}{n_1} = \delta_6 = \frac{95}{41} \text{ (с избытком)}, \varepsilon < \frac{1}{41 \cdot 101} < 0,001;$$

$$4) \frac{N}{n} \approx \frac{N_1}{n_1} = \delta_6 = \frac{223}{63} \text{ (с избытком)}, \varepsilon < \frac{1}{63 \cdot 265} < 0,0001.$$

$$225. 1) \frac{N_1}{n_1} = \frac{39}{8}, \frac{23}{4}, \frac{44}{19}, \frac{39}{11}; \quad 2) \frac{N_1}{n_1} = \delta_4 = \frac{101}{17};$$

$$3) \frac{N_1}{n_1} = \delta_3 = \frac{97}{28}; \quad 4) \frac{N_1}{n_1} = \delta_5 = \frac{74}{11}.$$

$$226. 1) \sqrt{15} = (3, (1, 6)) \approx \delta_4 = \frac{31}{8} \text{ (с избытком)}, \varepsilon < \frac{1}{8 \cdot 55} < 0,01,$$

$\delta_1 \approx 3,87$ (при округлении с недостатком);

$$2) \sqrt{17} = (4, (8)) \approx \delta_2 = \frac{33}{8} \text{ (с избытком)}, \varepsilon < \frac{1}{8 \cdot 65} < 0,01, \delta_4 \approx 4,12; \text{ (при округлении с недостатком).}$$

3) $\sqrt{23} = (4, (1, 3, 1, 8)) \approx \delta_8 = \frac{235}{49}$ (с избытком), $\varepsilon < \frac{1}{49 \cdot 191} < 0,001$, $\delta_8 \approx 4,795$ (при округлении с недостатком);

4) $\sqrt{31} = (5, (1, 1, 3, 5, 3, 1, 1, 10)) \approx \delta_5 = \frac{206}{37}$ (с недостатком), $\varepsilon < \frac{1}{37 \cdot 118} < 0,001$, $\delta_5 \approx 5,568$ (при округлении с избытком).

227. 1) $\sqrt{26} = (5, (10)) \approx \delta_2 = \frac{51}{10}$ (с избытком), $\delta_2 = 5,100$;

2) $\sqrt{37} = (6, (12)) \approx \delta_2 = \frac{73}{12}$ (с избытком), $\delta_2 \approx 6,083$ (при округлении с недостатком);

3) $\sqrt{29} = (5, (2, 1, 1, 2, 10)) \approx \delta_5 = \frac{70}{13}$ (с недостатком), $\delta_5 \approx 5,385$ (при округлении с избытком);

4) $\sqrt{19} = (4, (2, 1, 3, 1, 2, 8)) \approx \delta_4 = \frac{48}{11}$ (с избытком), $\delta_4 \approx 4,36$ (при округлении с недостатком).

228. 1) $\alpha = ((2, 8)) \approx \delta_3 = \frac{36}{17}$ (с недостатком), $\delta_3 \approx 2,12$ (при округлении с избытком);

2) $\alpha = ((3, 2, 5)) \approx \delta_3 = \frac{38}{11}$ (с недостатком), $\delta_3 \approx 3,46$ (при округлении с избытком);

3) $\alpha = ((3, 2, 1, 4)) \approx \delta_4 = \frac{47}{14}$ (с избытком), $\delta_4 \approx 3,35$ (при округлении с недостатком);

4) $\alpha = ((3, 1, 4)) \approx \delta_4 = \frac{61}{16}$ (с избытком), $\delta_4 \approx 3,81$ (при округлении с недостатком);

5) $\alpha = ((1, 6, 5, 6)) \approx \delta_2 = \frac{7}{6}$ (с избытком), $\delta_2 \approx 1,16$ (при округлении с недостатком);

6) $\alpha = (2, (3, 1)) \approx \delta_4 = \frac{34}{15}$ (с избытком), $\delta_4 \approx 2,26$ (при округлении с недостатком).

229. $e = (2, 1, 2, 1, 1, 4, \dots)$

$$\delta_k = 0, \frac{2}{1}, \frac{3}{1}, \frac{8}{3}, \frac{11}{4}, \frac{19}{7}, \frac{32}{32}, \dots$$

$$e \approx \delta_8 = \frac{87}{32} \text{ (с избытком), } \varepsilon < \frac{1}{32^2} < 0,001,$$

$\delta_8 \approx 2,718$ (при округлении с недостатком).

$$230. \sqrt[3]{10} = (2, 6, 2, \dots)$$

$$\delta_k = 0, \frac{2}{1}, \frac{13}{6}, \frac{28}{13}, \dots$$

$$\sqrt[3]{10} \approx \delta_6 = \frac{28}{13} \text{ (с недостатком),}$$

$$\delta_3 \approx 2,16 \text{ (при округлении с избытком).}$$

$$231. 1) \alpha = (2, (1, 7)), \bar{\alpha} = \delta_6 = \frac{231}{80}, \varepsilon < \frac{1}{80 \cdot 631} < 0,0001;$$

$$2) \alpha = (3, (2, 5)), \bar{\alpha} = \delta_4 = \frac{83}{24}, \varepsilon < \frac{1}{24 \cdot 131} < 0,001;$$

$$3) \alpha = (3, 1, (2, 3)), \bar{\alpha} = \delta_6 = \frac{292}{79}, \varepsilon < \frac{1}{79 \cdot 181} < 0,0001;$$

$$4) \alpha = (2, 1, (3, 1)), \bar{\alpha} = \delta_6 = \frac{67}{24}, \varepsilon < \frac{1}{24 \cdot 91} < 0,001.$$

232. В треугольнике $OM_{k-1}M_k$ нет целых точек.

$$233. 97 = 4^2 + 9^2, 137 = 4^2 + 11^2, 157 = 6^2 + 11^2, 173 = 2^2 + 13^2, \\ 181 = 9^2 + 10^2, 193 = 7^2 + 12^2, 281 = 5^2 + 16^2, 317 = 11^2 + 14^2.$$

$$234. 1) 2\alpha^2 - 6\alpha - 3 = 0; \alpha = \frac{\sqrt{15} + 3}{2}; 2) 7\alpha^2 - 7\alpha - 1 = 0;$$

$$\alpha = \frac{\sqrt{77} + 7}{14}; 3) 7\alpha^2 - 9\alpha - 13 = 0; \alpha = \frac{9 + \sqrt{445}}{14};$$

$$4) 13x^2 - 64x - 21 = 0; \alpha = \frac{32 + \sqrt{1297}}{13};$$

$$5) \alpha^2 - 4x + 1 = 0; \alpha = \sqrt{3} + 2; 6) 3\alpha^2 - 18\alpha + 22 = 0; \\ \alpha = \frac{9 + \sqrt{15}}{3}; 7) 16x^2 - 32x + 13 = 0; \alpha = \frac{4 + \sqrt{3}}{4}.$$

$$235. 1) \sqrt{26} = (5, (10)), x = 51, y = 10; 2) \sqrt{37} = (6, (12)), \\ x = 73, y = 12; 3) \sqrt{19} = (4, (2, 1, 3, 1, 2, 8)), x = 170, y = 39;$$

$$4) \sqrt{29} = (5, (2, 1, 1, 2, 10)), x = 9801, y = 1820.$$

$$236. 1) x = 40, y = 9, z = 41; 2) x = 60, y = 11, z = 61; \\ 3) x = 144, y = 17, z = 145; 4) x = 168, y = 95, z = 193; 5) x = 120, \\ y = 119, z = 169.$$

$$237. 1) 97 = (4 + 9i)(4 - 9i); 2) 137 = (4 + 11i)(4 - 11i); \\ 3) 181 = (10 + 11i)(10 - 11i); 4) 281 = (5 + 16i)(5 - 16i); 5) 317 = \\ = (11 + 14i)(11 - 14i).$$

238. Окружность $x^2 + y^2 = 1$ (1) и прямая $y = kx - 1$ (2) имеют общую рациональную точку $Q(0, -1)$; если и вторая точка их пересечения рациональная, то $k = \frac{y+1}{x}$, т. е. рационально.

Если, наоборот, k — рациональное число, то координаты P , второй точки пересечения (1) и (2), удовлетворяют уравнениям $x^2 +$

$+ (kx - 1)^2 = 1$, или $x = \frac{2k}{k^2 + 1}$, и $y = \frac{k^2 - 1}{k^2 + 1}$, т. е. P — рациональная точка.

239. Вопрос о целых решениях уравнения $x^2 + y^2 = z^2$ (1) равносильен вопросу о рациональных точках единичной окружности $X^2 + Y^2 = 1$. Последние получаются по формулам $X = \frac{2k}{k^2 + 1}$,

$Y = \frac{k^2 - 1}{k^2 + 1}$ (см. предыдущую задачу). Если положить в них $X = \frac{x}{z}$,

$Y = \frac{y}{z}$, $k = \frac{m}{n}$, $(m, n) = 1$, $m > n > 0$, m — четное, n — нечетное (или наоборот), то получаются формулы $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, которые выражают натуральные и взаимно простые решения уравнения (1).

240. Геометрический смысл утверждения Ферма состоит в том, что при $n > 2$ дуга кривой $X^n + Y^n = 1$ (в первом квадранте) не проходит ни через одну рациональную точку, кроме (1,0) и (0,1). По сравнению с дугой единичной окружности для случая $n = 2$ дуга кривой для $n > 2$ все более прижимается к сторонам единичного квадрата.

241. 1) Пусть $\frac{p}{q} = \alpha_k = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \dots + \frac{1}{10^{k!}} = \frac{p}{10^{k!}}$, так что $\alpha - \alpha_k < \frac{1}{10^{(k+1)!}} \left(1 + \frac{1}{10} + \frac{1}{10^2} + \dots\right) < \frac{10}{10^{(k+1)!}}$ и, наоборот, $\frac{10}{10^{(k+1)!}} > \alpha - \alpha_k$. Если α — алгебраическое число степени n ,

то согласно теореме Лиувилля существует положительное c такое, что $|\alpha - \alpha_k| \geq \frac{c}{10^{k!n}}$. Пусть k так велико, что $10^{k!} > \frac{10}{c}$, а $c >$

$> \frac{10}{10^{k!}}$; тогда по предыдущим неравенствам $\frac{10}{10^{(k+1)!}} > \frac{10}{10^{k!(n+1)}}$

и $k!(n+1) > (k+1)!$ для достаточно больших k , но это неверно для значений $k > n$. Итак, α — трансцендентно; 2) аналогично.

242. 1) 16, 2) 18, 3) 24, 4) 72, 5) 60.

243. 1) $x = \tau(36) = 9$; 2) $x = \tau(126) = 12$; 3) $x = \tau(42) = 8$; 4) решений нет.

244. 1) Решениями являются все делители числа 40, их можно получить как слагаемые произведения $(1 + 2 + 2^2 + 2^3)(1 + 5)$: 1, 2, 2^2, 2^3, 5, 2·5, 2^2·5, 2^3·5; 2) 1, 2, 2^2, 5, 2·5, 2^2·5; 3) решений нет.

245. Целой точке (x, y) гиперболы $xy = n$ соответствует делитель x числа n и наоборот.

246. $10 = 10 \cdot 1 = 2 \cdot 5$, поэтому искомое число имеет либо один простой делитель, либо два простых делителя; в первом случае показатель степени единственного простого делителя равен 9 и наименьшее соответствующее число равно 2^9 , во втором случае показателями степеней простых делителей являются 1 и 4 и наи-

меньшее соответствующее число равно $2^4 \cdot 3^1 = 48$. Итак, искомое число равно 48, так как $48 < 2^9$.

247. 1) 576, 2) 2240, 3) 936, 4) 35568.

248. Все r -е степени делителей данного $n = p_1^{a_1} \dots p_k^{a_k}$ получаются как слагаемые произведения

$(1 + p_1^r + \dots + (p_1^r)^{a_1})(1 + p_2^r + \dots + (p_2^r)^{a_2}) \dots (1 + p_k^r + \dots + (p_k^r)^{a_k})$, поэтому $S_r(n)$ равно этому произведению, т. е.

$$S_r(n) = \frac{(p_1^r)^{a_1+1} - 1}{p_1^r - 1} \cdot \frac{(p_2^r)^{a_2+1} - 1}{p_2^r - 1} \dots \frac{(p_k^r)^{a_k+1} - 1}{p_k^r - 1},$$

или

$$S_r(n) = \frac{p_1^{(a_1+1)r} - 1}{p_1^r - 1} \cdot \frac{p_2^{(a_2+1)r} - 1}{p_2^r - 1} \dots \frac{p_k^{(a_k+1)r} - 1}{p_k^r - 1}.$$

249. $S_2(12) = 210$, $S_2(14) = 50$, $S_3(30) = 31752$.

250. Такой же, как и простой делитель.

251. Если число m составное, то его простые делители также имеют вид $128k + 1$ и наименьший из них $< \sqrt{m}$, т. е. < 2600 ; поэтому $k < 21$, с другой стороны, $k \geq 5$, таким образом, достаточно 16 делений.

252. $2173 + 6^2 = 47^2$, $2173 = (47 - 6)(47 + 6) = 41 \cdot 53$; $1363 + 9^2 = 38^2$, $1363 = 29 \cdot 47$; $7663 + 9^2 = 88^2$, $7663 = 79 \cdot 97$; $4187 + 13^2 = 66^2$, $4187 = 53 \cdot 79$.

253. 1) $N = 194 \cdot 170$; 2) $N = 349 \cdot 218$.

254. Только $2 = 1^3 + 1^3$; если $p = x^3 + y^3$ и хотя бы одно из чисел $x, y > 1$, то p делилось бы на сумму $x + y$, которая > 1 и $< p$, что невозможно для простого числа.

255. 1) $\alpha = 13$, 2) $\alpha = 76$, 3) $\alpha = 87$, 4) $\alpha = 282$.

256. 1) Достаточно определить показатель степени 5 в 295! (так как двойка входит в это произведение с большим показателем); он равен 70, так что число оканчивается 70 нулями. 2) Нет, так как между 295 и 300 нет чисел делящихся на 5.

257. Пользуясь $[x]$, находим показатель степени для каждого простого множителя в 10! и 20!

$$10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$$

$$20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$$

258. Находим показатель степени 13 в 700!: 200!; он равен 41.

259. Надо пересчитать совокупность чисел, состоящую из всех делителей каждого из чисел от 1 до n . В ней имеются числа, делящиеся на 1, на 2, ..., на n , общее количество которых равно

$$\left[\frac{n}{1} \right] + \left[\frac{n}{2} \right] + \dots + \left[\frac{n}{n} \right]; \text{ других чисел в ней нет, поэтому}$$

$$\tau(1) + \tau(2) + \dots + \tau(n) = \left[\frac{n}{1} \right] + \left[\frac{n}{2} \right] + \dots + \left[\frac{n}{n} \right].$$

260. В левой части формулы сосчитаны целые точки на гиперболах $xy = 1, 2, \dots, n$; их общее число равно количеству целых точек ниже гиперболы $xy = n$ и на ней. Пересчитывая те же точки по вертикалям через целые абсциссы между осью абсцисс и гиперболой $xy = n$ (включая ее), получаем сумму из правой части формулы.

261. Для чисел от 1 до n число k является делителем в $\left[\frac{n}{k} \right]$ случаях, а сумма их равна $k \cdot \left[\frac{n}{k} \right]$. Таким образом, сумма всех делителей чисел от 1 до n равна выражению в правой части формулы.

262. Так как $[x] \leq x, [y] \leq y$, то $[x] + [y] \leq x + y$. Итак, $[x] + [y]$ — целое, не превосходящее $x + y$, а $[x + y]$ — наибольшее целое $\leq x + y$, поэтому $[x] + [y] \leq [x + y]$.

263. Простое p входит в N с показателем $\sum a_i$, где

$$a_i = \left[\frac{a_1 + a_2 + \dots + a_k}{p^i} \right] - \left[\frac{a_1}{p^i} \right] - \left[\frac{a_2}{p^i} \right] - \dots - \left[\frac{a_k}{p^i} \right];$$

но $\left[\frac{a_1 + a_2 + \dots + a_k}{p^i} \right] \geq \left[\frac{a_1}{p^i} \right] + \left[\frac{a_2}{p^i} \right] + \dots + \left[\frac{a_k}{p^i} \right]$ (см. предыдущую задачу), поэтому N целое.

264. $[2\alpha] + [2\beta]$ и $[\alpha] + [\beta] + [\alpha + \beta]$ изменяются на равные числа, если α и β изменяются на какие либо целые числа (так как $[\alpha + n] = [\alpha] + n$ для целого n), поэтому соотношение достаточно доказать для случая $0 \leq \alpha < 1, 0 \leq \beta < 1$; тогда оно имеет вид $[2\alpha] + [2\beta] \geq [\alpha + \beta]$. Если $[\alpha + \beta] = 0$, оно очевидно; если же $[\alpha + \beta] = 1$, то $\alpha + \beta \geq 1$ и по крайней мере одно из обоих слагаемых, например, $\alpha \geq \frac{1}{2}$; тогда $[2\alpha] + [2\beta] \geq 1$, так что на самом деле $[2\alpha] + [2\beta] \geq [\alpha + \beta]$.

265. Записать показатели, с которыми p входит в числитель и знаменатель, и учесть формулу предыдущей задачи.

266. Справедливость равенства (1) вытекает из следующего:

1) Для $x = \alpha, 0 \leq \alpha < \frac{1}{n}$ (1) выполняется, так как в таком случае все слагаемые слева и выражение в правой части равны нулю.

2) Если (1) верно для некоторого x , то оно сохраняется, если к x прибавить $\frac{1}{n}$. Действительно, при этом каждое слагаемое слева, кроме последнего, переходит в соседнее справа, а последнее в $[x + 1] = [x] + 1$, так что левая часть увеличивается на 1. То же происходит с правой частью, так как $\left[n \left(x + \frac{1}{n} \right) \right] = [nx + 1] = [nx] + 1$.

3) Любое x можно получить, прибавляя к некоторому $\alpha, 0 \leq \alpha < \frac{1}{n}$, $\frac{1}{n} m$ раз, т. е. $\frac{m}{n}$. В самом деле, из $\alpha + \frac{m}{n} = x$,

$x - \frac{m}{n} = x, 0 \leq x - \frac{m}{n} < \frac{1}{n}$, или $0 \leq nx - m < 1$, или $0 \geq m - nx > -1$, следует неравенство $nx \geq m > nx - 1$, которое определяет m однозначно, а вместе с тем и x .

267. Искомое число получается, если сопоставить числам из 1, 2, ..., $[x]$ (1), взаимно простым с N , число 1, числам (1), имеющим k простых делителей из p_i , число $0 = (1-1)^k = 1 - C_k^1 + C_k^2 - \dots \pm C_k^k$ и сопоставленные числа сложить. Получится сумма $[x] - \sum C_k^1 + \sum C_k^2 - \dots \pm \sum C_k^k$, где суммирование производится по всем числам 1, 2, ..., $[x]$ (и в зависимости от числа простых делителей p_i каждого из них).

Но

$$\sum C_k^1 = \sum \left[\frac{x}{p_i} \right], \quad \sum C_k^2 = \sum \left[\frac{x}{p_i p_j} \right]$$

и т. д., поэтому

$$\varphi(x, N) = [x] - \sum \left[\frac{x}{p_i} \right] + \sum \left[\frac{x}{p_i p_j} \right] - \dots + (-1)^n \left[\frac{x}{p_1 p_2 \dots p_n} \right].$$

268. По формуле Лежандра из предыдущей задачи находим:

1) $30 = 2 \cdot 3 \cdot 5$,

$$\begin{aligned} \varphi(300, 30) &= [300] - \left[\frac{300}{2} \right] - \left[\frac{300}{3} \right] - \left[\frac{300}{5} \right] + \left[\frac{300}{2 \cdot 3} \right] + \\ &+ \left[\frac{300}{2 \cdot 5} \right] + \left[\frac{300}{3 \cdot 5} \right] - \left[\frac{300}{2 \cdot 3 \cdot 5} \right] = 80, \end{aligned}$$

2) аналогично $\varphi(713, 42) = 204$.

269. Функцию Эйлера $\varphi(m)$ можно истолковать как $\varphi(m, m)$, поэтому (если $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$)

$$\begin{aligned} \varphi(m) = \varphi(m, m) &= m - \frac{m}{p_1} - \frac{m}{p_2} - \dots - \frac{m}{p_k} + \frac{m}{p_1 p_2} + \dots + \\ &+ \frac{m}{p_{k-1} p_k} - \dots + (-1)^k \frac{m}{p_1 \dots p_k}, \end{aligned}$$

или

$$\varphi(m) = m \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_k} \right).$$

Здесь в $\varphi(m, m)$ знак «целой части» не нужен, так как m делится на p_1, p_2, \dots, p_k .

270. 1) $\pi(10^7) \approx 620000$, 2) $\pi(10^8) \approx 5425000$.

271. Если из множества простых чисел $\leq x$ исключить все простые числа $p_1, p_2, \dots, p_r \leq \sqrt{x}$ и прибавить к нему 1, то получится множество таких чисел $\leq x$, которые взаимно просты с $p_l \leq \sqrt{x}$; поэтому

$$\pi(x) - \pi(\sqrt{x}) + 1 = \varphi(x; p_1 p_2 \dots p_r).$$

272. $\pi(120) = \pi(\sqrt{120}) - 1 + \varphi(120; 2, 3, 5, 7) = 3 + \varphi(120; 2, 3, 5, 7) = 30$.

273. Допустим, что простых чисел вида $4n + 3$ имеется лишь конечное число, а именно q_1, q_2, \dots, q_k . Тогда число $4q_1 q_2 \dots q_k - 1$, также имеющее вид $4n + 3$, должно быть составным и иметь простой делитель вида $4n + 3$ (так как произведение чисел вида $4n + 1$ всегда имеет вид $4n + 1$), но ни одно из чисел q_1, q_2, \dots, q_k не подходит. Наше предположение привело к противоречию.

274. Допустим, что простых чисел вида $6n + 5$ имеется лишь конечное множество, а именно q_1, q_2, \dots, q_k . Тогда число $6q_1 q_2 \dots q_k - 1$, также имеющее вид $6n + 5$, должно быть составным и иметь простой делитель такого же вида (так как простые числа, больше 3, имеют вид $6n + 1$ или $6n + 5$, а произведение чисел вида $6n + 1$ имеет такой же вид), но ни одно из чисел q_1, q_2, \dots, q_k не подходит. Получается противоречие.

275. Допустим, что простых чисел вида $6n + 1$ имеется лишь конечное множество, а именно q_1, q_2, \dots, q_k . Тогда число $x^2 + 3 = 4(q_1 q_2 \dots q_k)^2 + 3$, также имеющее вид $6n + 1$, должно быть составным, а так как оно не делится ни на одно из чисел q_i (оно должно иметь простой делитель $p = 6n + 5$, или $x^2 + 3 \equiv 0 \pmod{p}$), т. е. $\left(\frac{-3}{p}\right) = 1$, что, однако, невозможно, когда $p = 6n + 5$ (см. 154 задачу).

276. 113, 541, 757 можно, остальные — нет.

277. 1) $N = 279^2 + 106^2 = 169^2 + 246^2$;

2) $N = 809^2 + 211^2 = 391^2 + 739^2$.

278. Если целые точки $P_1(x_1, y_1)$ и $P_2(x_2, y_2)$ имеют от $Q\left(\sqrt{2}, \frac{1}{3}\right)$ одинаковое расстояние, то должно быть

$$(x_1 - \sqrt{2})^2 + \left(y_1 - \frac{1}{3}\right)^2 = (x_2 - \sqrt{2})^2 + \left(y_2 - \frac{1}{3}\right)^2,$$

откуда $x_1^2 - x_2^2 + 2(x_1 - x_2)\sqrt{2} + y_1^2 - y_2^2 = \frac{2}{3}(y_1 - y_2)$, что влечет за собой необходимое условие $x_1 = x_2$. Но так как в таком случае $y_1 \neq y_2$, то получается $y_1 + y_2 = \frac{2}{3}$, что для целых y_1, y_2 невозможно.

279. Пусть K — круг с центром $Q\left(\sqrt{2}, \frac{1}{3}\right)$, который содержит более n целых точек (такой круг, конечно, существует). Вместе с тем он содержит лишь конечное число целых точек. Поскольку они имеют различное расстояние от Q (см. предыдущую задачу), то их можно расположить в конечную последовательность по увеличивающимся расстояниям

$$P_1, P_2, \dots, P_n, P_{n+1}, \dots$$

и тогда круг K_{n+1} с центром Q , проходящий через P_{n+1} , имеет как раз внутри себя точно n целых точек P_1, P_2, \dots, P_n .

280. $5220 = 0^2 + 8^2 + 16^2 + 70^2$.

ТАБЛИЦЫ ИНДЕКСОВ

Простое число 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Простое число 5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Простое число 7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Простое число 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Простое число 13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Простое число 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Простое число 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Простое число 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Простое число 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Простое число 31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Простое число 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Простое число 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Простое число 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Простое число 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Простое число 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Простое число 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Простое число 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Простое число 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Простое число 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	43	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Простое число 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Простое число 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Простое число 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Простое число 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Простое число 97

N	0	1	2	3	4	5	6	7	8	9	
0			0	34	70	68	1	8	31	6	44
1	35		6	42	25	65	71	40	89	78	81
2	69		5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95	
4	7	85	39	4	58	45	15	84	14	62	
5	36	63	93	10	52	87	37	55	47	67	
6	43	64	80	75	12	26	94	57	61	51	
7	66	11	50	28	29	72	53	21	33	30	
8	41	88	23	17	73	90	38	83	92	54	
9	79	56	49	20	22	82	48				

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	56	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

ЛИТЕРАТУРА

Монографии

1. Борович З. И. и Шафаревич И. Р. Теория чисел. М., изд-во «Наука», 1964 г.
2. Васильев А. В. Целое число. Научное изд-во, 1919.
3. Венков Б. А. Элементарная теория чисел. М. — Л., 1937.
4. Виноградов И. М. Избранные труды. М., изд-во АН СССР, 1952.
5. Гаусс К. Ф. Труды по теории чисел. Общая редакция акад. И. М. Виноградова. Перевод В. Б. Демьянова. М., изд-во АН СССР, 1959.
6. Гельфонд А. О. Трансцендентные и алгебраические числа. М., Гостехиздат, 1952.
7. Гельфонд А. О., Линник Ю. В. Элементарные методы в аналитической теории чисел. М., Гос. изд-во физ.-мат. литературы, 1962.
8. Граве Д. А. Трактат по алгебраическому анализу, т. II, Изд. АН УССР, 1939.
9. Делоне Б. Н. Петербургская школа теории чисел. Изд. АН СССР, 1947.
10. Ингам А. Е. Распределение простых чисел. Перевод с английского Райкова, ОНТИ, 1936.
11. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. М., Гос. изд-во физ.-мат. литературы, 1963.
12. Титчмарш Е. К. Теория дзета-функции Римана. Перевод с английского М. А. Евграфова. Под ред. А. О. Гельфонда. М., ИЛ, 1953.
13. Трост Э. Простые числа. Перевод с немецкого Н. И. Фельдмана. Под ред. А. О. Гельфонда. М., Гос. изд-во физ.-мат. литературы, 1959.
14. Хуа Ло-ген. Аддитивная теория простых чисел. Труды мат. ин-та АН СССР, 22, 1947.
15. Хуа Ло-ген. Метод тригонометрических сумм и его применения в теории чисел. Перевод с немецкого А. М. Полосуева. Под ред. Н. Г. Чудакова. М., изд-во «Мир», 1964.
16. Хинчин А. Я. Цепные дроби, изд. 3. М., Гос. Изд-во физ.-мат. литературы, 1961.
17. Хованский А. Н. Приложение цепных дробей и их обобщений к вопросам приближенного анализа. М., Гостехиздат, 1956.

18. Чебышев П. Л. Полное собрание сочинений, т. 1. Изд-во АН СССР, М. — Л., 1946.

19. Чудаков Н. Г. Введение в теорию L -функций Дирихле. М. — Л., Гостехиздат, 1947.

Учебники и учебные пособия

20. Арнольд И. В. Теория чисел. Учпедгиз, 1939.

21. Архангельская В. М. Элементарная теория чисел. Изд-во Саратовского ун-та, 1963.

22. Архангельская В. М. L — функции Дирихле. Изд-во Саратовского ун-та, 1962.

23. Бухштаб А. А. Теория чисел. Учпедгиз, 1960.

24. Виноградов И. М. Основы теории чисел, Изд. 7. Изд-во «Наука», 1965.

25. Гекке Э. Лекции по теории алгебраических чисел. ГТТИ, 1940.

26. Граве Д. А. Элементарный курс теории чисел. Киев, 1913.

27. Гребенча М. К. Теория чисел. Учебно-метод. пособие для заочников пед. ин-тов. М., 1949.

28. Грибанов В. У., Титов П. И. Сборник упражнений по теории чисел. М., изд-во «Просвещение», 1964.

29. Лежен-Дирихле П. Г. Лекции по теории чисел в обработке и с добавлениями Р. Дедекинда. Перевод с немецкого под ред. Б. И. Сегала, с приложением статьи Б. Н. Делоне «Геометрия бинарных квадратичных форм». ОНТИ, 1936.

30. Диксон Л. Е. Введение в теорию чисел. Тбилиси. Изд. АН Груз. ССР, 1941.

31. Егоров Д. Ф. Элементы теории чисел. ГМЗ, 1923.

32. Марчевский М. Н. Теория чисел. Изд. Харьковского гос. ун-та, 1958.

33. Окунев Л. Я. Краткий курс теории чисел. Учпедгиз, 1956.

34. Сушкевич А. К. Теория чисел, изд. 2. Изд. Харьковского ун-та, 1956.

35. Хассе Г. Лекции по теории чисел. Перевод с немецкого В. Б. Демьянова. Под ред. И. Р. Шафаревича. ИЛ, 1953.

36. Хинчин А. Я. Элементы теории чисел. Энциклопедия элементарной математики, т. 1, Гостехиздат, 1951.

Обзорные статьи и популярная литература

37. Вальфиш А. З. Уравнения Пелля. Тбилиси, Изд. Акад. наук Груз. ССР, 1952.

38. Виноградов И. М. Некоторые проблемы аналитической теории чисел. Статья в сборнике «Труды третьего Всесоюзного математического съезда», т. III, М., 1958.

39. Воробьев Н. Н. Признаки делимости. Гос. изд-во физ.-мат. литературы, М., 1963.

40. Воробьев Н. Н. Числа фибоначчи, М., изд-во «Наука», 1964.

41. Гельфонд А. О. О проблеме приближения алгебраических чисел рациональными. Статья во 2-м выпуске «Математическое просвещение». М., ГТТИ, 1957.
42. Гельфонд А. О. Решение уравнений в целых числах, вып. 8 популярных лекций по математике. М.-Л., ГТТИ, 1952.
43. Гельфонд А. О. Теория чисел. Статья в сборнике «Математика в СССР за тридцать лет». Гостехиздат, 1947.
44. Гельфонд А. О., Линник Ю. В. Чисел теория, Б. С. Э., изд. 2, т. 47, 1957.
45. Голубев В. А. Реферативный обзор современных работ по элементарной теории чисел. «Математика в школе», 1958, № 6, 1960, 5.
46. Линник Ю. В. Теория чисел. Статья в сборнике «Математика в СССР за сорок лет, 1917—1957», т. 1. М., Гос. изд-во физ.-мат. литературы, 1959.
47. Марджанишвили К. К. Простые числа. Статья в сборнике «Математика, ее содержание, методы и значение», т. II, Изд. Акад. наук СССР, 1956.
48. Постников А. Г. и Романов К. П. Упрощение элементарного доказательства А. Сельберга асимптотического закона распределения простых чисел. «Успехи математических наук», т. X, 1955, № 4.
49. Райк А. Е. Уральский математик Иван Михеевич Первушин «Истор. мат. иссл.», т. VI, Гостехиздат, 1953 г. стр. 535—572.
50. Серпинский В. Пифагоровы треугольники. Перевод с польского. Учпедгиз, 1959.
51. Серпинский В. О решении уравнений в целых числах. Перевод с польского. М., Гос. изд-во физ.-мат. литературы, 1961.
52. Серпинский В. Сто простых, но одновременно и трудных вопросов арифметики. Перевод с польского. Учпедгиз, 1961.
53. Серпинский В. Что мы знаем и чего мы не знаем о простых числах. Перевод с польского. М. — Л., Гос. изд-во физ.-мат., литературы, 1963.
54. Хинчин А. Я. Три жемчужины теории чисел. Гостехиздат, 1947.
55. Хинчин А. Я. Великая теорема Ферма, изд. 2. ГТТИ, 1932.
56. Шнирельман Л. Г. Простые числа. Гостехиздат, 1940.
57. Дэвенпорт Г. Высшая арифметика, введение в теорию чисел. Перевод с английского. М., изд-во «Наука», 1965.
-