ВОЛОГОДСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
им. В. М. МОЛОТОВА

К. С. ЛАЗАРЕВ

КУРС ТЕОРЕТИЧЕСКОЙ АРИФМЕТИКИ

ЧАСТЬ ВТОРАЯ

ВОЛОГДА • 1941

ВОЛОГОДСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
им. В. М. МОЛОТОВА

К. С. ЛАЗАРЕВ

КУРС ТЕОРЕТИЧЕСКОЙ АРИФМЕТИКИ

ЧАСТЬ ВТОРАЯ

ВОЛОГДА • 1941

ПРЕДИСЛОВИЕ

Настоящая вторая часть „Курса теоретической арифметики" составлена по плану, изложенному в предисловии к первой части.

Мои книги представляют собою лишь попытку облегчить студентам усвоение теории чисел. Насколько удовлетворительны мои книги, судить не мне. Надеюсь, что преподаватели вузов не сочтут за труд прислать мне свои указания на замеченные недостатки. Мой адрес: Вологда, ул. Маяковского, 8, кв. 60, *Константину Семеновичу Лазареву*.

К. С. Лазарев.

Вологда.
12 февраля 1941 г.

ГЛАВА ЧЕТВЕРТАЯ

Простые числа

65. Натуральные числа, отличные от единицы, распадаются на два класса: *составные (сложные) числа* (4, 6, 8, 9, ...) и *простые числа* (2, 3, 5, 7, 11, ...). Наименьшее простое число есть 2; оно одно между простыми числами есть четное. Единица не причисляется ни к простым числам, ни к составным: она остается в стороне. *Таким образом, приходится отличать три категории натуральных чисел: единицу, простые числа и составные числа.* Относительно простых чисел имеется следующая теорема:

66. Теорема. *Простых чисел бесконечное множество.*

Доказательство. Эта теорема была доказана еще Евклидом.[1] Предположим, что существует конечное число простых чисел, и пусть наибольшее из них есть p.

Составим произведение всех простых чисел от 2 до p включительно, к этому произведению прибавим единицу и полученную сумму обозначим через s. Тогда:

$$s = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \ldots p + 1.$$

Число s больше p. Если s есть простое число, то теорема доказана; если же s есть составное число, то оно должно делиться на простое число, большее p. В самом деле, s не делится ни на одно из чисел нашего ряда 2, 3, 5, ..., p, так как s есть сумма двух слагаемых $2 \cdot 3 \cdot 5 \cdot 7 \ldots p$ и 1, из которых первое слагаемое делится на любое из чисел ряда 2, 3, 5, 7, 11, ..., p, а второе слагаемое 1 ни на одно из них не делится. Отсюда следует заключить, что s либо само должно быть простым числом, либо должно делиться на простое число, большее p. В действительности может иметь место как то, так и другое. Следовательно, во всяком случае, как бы велико ни было простое число p, имеется еще другое простое число, большее p, что и требовалось доказать. Примеры:

$$2 \cdot 3 + 1 = 7, \text{ простое число}$$
$$2 \cdot 3 \cdot 5 + 1 = 31, \text{ простое число}$$
$$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211, \text{ простое число}$$
$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311, \text{ простое число}$$
$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509, \text{ составное число.}$$

[1] О жизни греческого геометра Евклида мы имеем скудные сведения. Свои бессмертные „Начала" он написал в Александрии около 300 г. до н. э. „Начала" состоят из 13 книг; из них книги VII, VIII и IX посвящены учению о натуральных числах. 20-я теорема IX книги трактует о бесконечном множестве простых чисел.

Мы видим, что, давая p значения 3, 5, 7, 11, получаем пр
стые числа, а при $p=13$ получаем составное число.

67. Составление таблицы простых чисел. Положим, что нуж
составить таблицу простых чисел от 2 до n.

Способ составления такой таблицы состоит в следующе
пишем ряд натуральных чисел от 2 до n включительно:

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, . . .,

Зачеркиваем в этом ряду все четные числа, исключая
Первое после 2 не вычеркнутое простое число есть 3. Оставл
3, вычеркиваем после него каждое третье число, считая п
этом как зачеркнутые числа, так и не зачеркнутые.

Первое после 3 не вычеркнутое простое число есть 5. Ос
вляя 5, вычеркиваем после него каждое пятое число (некотор
из них повторно уже вычеркнуты).

Продолжаем поступать и дальше так, т.-е. начинаем с бл
жайшего не зачеркнутого числа, оставляем его, а после не
зачеркиваем числа (некоторые уже вычеркнуты) через столь
мест, сколько единиц в том числе, с которого мы начали.

По окончании этой операции в нашем ряду останутся од
простые числа.

Этот способ составления таблицы простых чисел называет
Эратосфеновым решетом, потому что александрийск
математик Эратосфен (275—194) писал числа на дощечке, иокр
той воском, и прокалывал дырочки над составными числа
От этого дощечка уподоблялась решету, через которое как
просеивались составные числа.

68. В настоящее время имеются таблицы простых чисел, ме
ших 9 000 000; таблицы, простирающиеся за 9 000 000, еще
напечатаны. „Правда, в архивах Венской Академии Наук х
нится рукопись Кулика, в которой таблица простых чисел
разложений на множителей доведена до 100 000 000". (В. Ли
ман. Великаны и карлики в мире чисел. М.—Л. 1935, стр.

Нужно отметить, что закон, по которому простые числа с
дуют одно за другим, остается до сих пор неразгаданным. В ви
этого распознавание простых чисел представляет собою о
из труднейших задач математики.

Эйлер дал три формулы x^2+x+17, x^2+x+41, $2x^2+2$
которые при подстановке в них вместо x чисел ряда 0, 1, 2
4, . . . дают большое число простых чисел, но он же показал,
полином с целыми коэффициентами $a_0x^n+a_1x^{n-1}+a_2x^{n-2}$
$+a_3x^{n-3}+\ldots+a_n$ при подстановке в него вместо x чисел р
0, 1, 2, 3, 4, . . . дает и составные числа.

В самом деле, многочлен x^2+x+17 при $x=0$ дает прос
число 17, а при $x=17$ уже дает составное число $17\cdot 19=3$
кратное 17. Тот же многочлен при $x=1$ дает простое число
а при $x=1+19=20$ дает составное число $437=19\cdot 23$, крат
19; тот же многочлен при $x=2$ дает простое число 23, при
$2+23=25$ дает составное число $667=23\cdot 29$, кратное

[1] Наименьшие значения x, для которых получаются составные числа, соответственно x 16, x 40, $x=29$.

Вообще, если какой-нибудь многочлен с целыми коэффициентами при $x=a$ дает простое число p, то уже при $x=a+p$ он даст составное число, кратное p.

В самом деле, пусть многочлен $f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+a_3x^{n-3}+\ldots+a_n$ *при* $x=a$ дает простое число p:

$$f(a)=a_0a^n+a_1a^{n-1}+a_2a^{n-2}+a_3a^{n-3}+\ldots+a_n=p. \quad (1)$$

$$f(a+p)=a_0(a+p)^n+a_1(a+p)^{n-1}+a_2(a+p)^{n-2}+a_3(a+p)^{n-3}+\ldots+a_{n-1}(a+p)+a_n.$$

Разлагая $(a+p)^n$ по формуле бинома Ньютона, получим в разложении $n+1$ членов, из которых один только первый член a^n не будет содержать p, а остальные n членов разложения, начиная со второго, будут содержать p соответственно в степенях 1, 2, 3, . . ., n, а потому $(a+p)^n$ можно представить в виде суммы двух слагаемых, одно из которых будет кратно p, а другое слагаемое будет a^n:

$$(a+p)^n=kp\cdot p+a^n.$$

Получаем ряд равенств:

$$\begin{aligned}
a_0(a+p)^n &= kp\cdot p+a_0a^n\\
a_1(a+p)^{n-1} &= kp\cdot p+a_1a^{n-1}\\
a_2(a+p)^{n-2} &= kp\cdot p+a_2a^{n-2}\\
a_3(a+p)^{n-3} &= kp\cdot p+a_3a^{n-3}\\
&\ldots\ldots\ldots\quad\ldots\ldots\\
a_{n-1}(a+p) &= kp\cdot p+a_{n-1}a\\
a_n &= a_n.
\end{aligned}$$

Складывая эти равенства почленно и имея в виду равенство (1), получим: $f(a+p)=kp\cdot p+p=kp\cdot p$, что и требовалось доказать.

69. *Функция $\pi(n)$ обозначает число простых чисел, не превышающих n.* Так, напр., $\pi(25)=9$, $\pi(100)=25$, $\pi(229)=50$. Эйлеру было известно, что дробь $\frac{\pi(n)}{n}$ стремится к нулю при безграничном возрастании n; это можно истолковать так: число простых чисел бесконечно мало в сравнении со множеством всех целых положительных чисел. При изучении простых чисел возникает вопрос: существует ли точная формула для числа простых чисел между 1 и n? Теперь доказано, что такой формулы не существует, но зато доказано, что $\pi(n)$ приблизительно равно $\frac{n}{\ln n}$, где $\ln n$ есть натуральный логарифм числа n. Эту замечательную теорему доказали в 1896 году почти одновременно и независимо друг от друга бельгийский математик Шарль-Жан де ла Валле-Пуссен и французский математик Жак Адамар. Две такие функции, как $\pi(n)$ и $\frac{n}{\ln n}$, отношение которых $\pi(n):\frac{n}{\ln n}$ стремится к единице при

безграничном возрастании n, называются эквивалентными или асимптотическими. Первыми теоретическими результатами, устанавливающими связь функции $\pi(n)$ с отношением $\frac{n}{\ln n}$, мы обязаны нашему русскому математику академику Пафнутию Львовичу Чебышеву (1821—1894).

Не все вопросы, возникающие при изучении простых чисел легко разрешаются. Многие из них до сих пор еще не получили ответа. Нам известны пары простых чисел, отличающиеся друг от друга на 2: 3 и 5, 5 и 7, 11 и 13, 17 и 19 и т. д. Такие числа называются близнецами. Установлено, что между 1 и 100000 таких пар имеется всего 1125; между 1000000 и 1100000—только 725; между 8000000 и 8100000 еще меньше, именно 518. Словом, их становится все меньше и меньше. Спрашивается теперь, перестают ли потом встречаться вовсе такие пары или нет? Ответа на этот вопрос до сих пор еще не получено. Не решенной остается также проблема Гольдбаха.

Академик Петербургской Академии Наук Гольдбах в письме от 7 июня 1742 года к знаменитому Эйлеру выдвинул следующую проблему: *„Доказать, что всякое целое число $n \geqq 6$ есть сумма трех простых чисел“*.

В своем ответном письме от 30 июня 1742 года Эйлер пишет: *„Но что каждое четное число есть сумма двух простых чисел, я считаю совершенно справедливой теоремой, несмотря на то, что я ее доказать не могу“*.

Советский академик Иван Матвеевич Виноградов видоизменил теорему Гольдбаха и в мае 1937 года доказал такую теорему: *„Всякое достаточно большое нечетное число есть сумма трех простых чисел“*. Что же касается четных чисел, то из работы академика Виноградова следует, что они, начиная с некоторого места, являются суммами четырех простых чисел. Доказательство академика Виноградова является выдающимся открытием, однако полного решения проблемы Гольдбаха мы до сих пор еще не имеем.

70. Как узнать, есть ли данное число n простое или составное?

Чтобы узнать, есть ли данное число простое или составное, нужно делить его на простые числа, начиная с 2; если n ни на одно из простых чисел 2, 3, 5, 7, 11, 13, 17, ... не разделится, то, значит, оно есть число простое. Надо сказать, что нет необходимости делить его на все простые числа, меньшие данного числа n; достаточно пробы производить до тех пор, пока не получится в частном число, меньшее делителя. Если при этом получится остаток, то заключаем, что данное число есть простое. В самом деле, если бы данное число разделилось на какое-либо из следующих простых чисел, то оно разделилось бы и на частное от этого деления. Между тем деление на числа, меньшие делителя, уже испробовано и оказалось невозможным. Поэтому можно, не продолжая испытаний, сказать, что данное число n есть простое. Таким образом, мы приходим к следующему правилу:

Правило. *Чтобы узнать, есть ли данное число простое или составное, достаточно делить его на простые числа 2, 3, 5, 7, 11, 13, . . . в том порядке, в котором эти числа следуют одно за другим, и продолжать эти пробы до тех пор, пока в частном не получится число, меньшее делителя; если ни одно из этих делений не совершается без остатка, то данное число есть простое.*

Примеры. 1) Возьмем число 883. На основании признаков делимости мы заключаем, что это число не делится ни на 2, ни на 3, ни на 5, ни на 7, ни на 11. Деления на 13, на 17, на 19, на 23, на 29, на 31 дают остатки. Деление на 31 дает в частном 28, число меньшее делителя. Следовательно, 883 есть простое число.

2) Возьмем число 667. На основании признаков делимости мы заключаем, что данное число не делится ни на 2, ни на 3, ни на 5, ни на 7, ни на 11. Деления на 13, на 17 и на 19 дают остатки. Деление на 23 совершается без остатка и дает в частном 29. Следовательно, 667 есть составное число:

$$667 = 23 \cdot 29.$$

71. Основная теорема арифметики. *Всякое составное число всегда может быть представлено и притом одним только способом в виде произведения простых чисел.*

Доказательство. Докажем сначала первую часть теоремы: всякое составное число всегда может быть представлено в виде произведения простых чисел.

Пусть m будет составное число. В таком случае оно непременно должно делиться на какое-нибудь число a, большее 1 и меньшее m, иначе m не было бы составным числом. Если a число составное, то оно имеет отличного от 1 и a некоторого делителя b. Если и b есть составное число, то оно должно иметь некоторого делителя c, отличного от 1 и b. Продолжая итти таким образом далее, мы дойдем, наконец, до какого-нибудь простого числа. В самом деле, делители a, b, c, . . . идут убывая, все члены этого ряда суть натуральные числа, число которых меньше m. Таким образом, последний член ряда a, b, c, . . . будет простым числом. Обозначим его через p_1. Обозначим частное от деления m на p_1 через m_1. Тогда мы получим:

$$m = p_1 m_1,$$

где m_1 меньше m.

Если m_1 простое число, то m уже представлено в виде произведения простых чисел; если же m_1 число составное, то, применяя к нему предыдущее рассуждение, мы придем к некоторому простому делителю p_2; обозначив частное от деления m_1 на p_2 через m_2, будем иметь: $m_1 = p_2 m_2$. Таким образом, получим:

$$m = p_1 p_2 m_2,$$

где m_2 меньше m_1. Если m_2 будет простое число, то m уже представлено в виде произведения простых чисел; если же m_2 будет составное число, то оно должно иметь некоторого про-

стого делителя p_2; обозначив частное от деления m_2 на через m_3, получим:

$$m_2 = p_3 m_3.$$

Тогда

$$m = p_1 p_2 p_3 m_3.$$

Это рассуждение мы можем продолжить, и, так как числа $m_1, m_2, m_3, \ldots$ постоянно убывают и отличны от 1, то мы должны в конце концов притти к числу m_n, которое представляет собой простое число. Таким образом, мы получим разложение числа на простых делителей, число которых обозначим через n:

$$m = p_1 p_2 p_3 \ldots p_n.$$

Таким образом, первая часть теоремы доказана.

Докажем теперь вторую часть теоремы.

Всякое составное число m может быть представлено в виде произведения простых чисел только одним способом. Допустим, что существуют два различных разложения m на простых множителей: одно разложение

$$m = p_1 p_2 p_3 p_4 \ldots p_n, \tag{1}$$

а другое

$$m = q_1 q_2 q_3 q_4 \ldots q_S. \tag{2}$$

Тогда

$$p_1 p_2 p_3 p_4 \ldots p_n = q_1 q_2 q_3 q_4 \ldots q_S. \tag{3}$$

Левая часть последнего равенства делится на простое число p_1. Значит, и правая его часть должна делиться на p_1. Но произведение $q_1 q_2 q_3 \ldots q_S$ простых чисел только тогда разделится на простое число p_1, когда одно из этих чисел будет равно p_1 (п. 43). Пусть $q_1 = p_1$. Разделив обе части равенства (3) на p_1, получим:

$$p_2 p_3 p_4 \ldots p_n = q_2 q_3 q_4 \ldots q_S. \tag{4}$$

Число p_2 простое и делит произведение $q_2 q_3 q_4 \ldots q_S$ простых чисел, а потому оно должно быть равно одному из чисел $q_2, q_3, q_4, \ldots, q_S$ (п. 43). Пусть $q_2 = p_2$. Разделив обе части равенства (4) на p_2, получим

$$p_3 p_4 \ldots p_n = q_3 q_4 \ldots q_S. \tag{5}$$

Применяя те же самые рассуждения как к равенству (5), так и к каждому следующему, мы придем к заключению, что все n сомножителей произведения $a_1 a_2 a_3 \ldots a_n$ должны быть равны n сомножителям произведения $q_1 q_2 q_3 q_4 \ldots q_S$. Имеем:

$$p_1 = q_1,\ p_2 = q_2,\ p_3 = q_3, \ldots, p_n = q_n.$$

Всякий раз, когда идет речь о разложении числа на простые сомножители, подразумевается, что между этими сомножителями нет числа 1. Отсюда следует, что

$$s = n.$$

Таким образом, и вторая часть теоремы доказана.

72. Укажем другой прием разложения составного числа на простых сомножителей. Возьмем составное число m. Пусть будет p_1 его наименьший простой делитель. Делим m на p_1, получаем в частном m_1, так что

$$m = p_1 m_1. \qquad (1)$$

Если m_1 есть составное число, то разложение окончено, ибо m представит тогда произведение двух простых чисел p_1 и m_1. Если m_1 есть составное число, то делим его на его наименьшего простого делителя p_2. Получаем в частном m_2, так что

$$m_1 = p_2 m_2.$$

Подставляя это значение m_1 в равенство (1), найдем:

$$m = p_1 p_2 m_2. \qquad (2)$$

Если m_2 есть число простое, то теорема доказана, ибо m представит тогда произведение трех простых чисел p_1, p_2 и m_2; если же m_2 есть составное число, то делим его на его наименьшего простого делителя p_3, получаем в частном m_3, так что

$$m_2 = p_3 m_3.$$

Подставляя это значение $p_3 m_3$ в равенство (2), найдем:

$$m = p_1 p_2 p_3 m_3.$$

Продолжаем этот прием до тех пор, пока какое-нибудь частное само не будет простым числом. Этот процесс не может продолжаться бесконечно, так как целые положительные числа $m_1, m_2, m_3, \ldots$ следуют друг за другом уменьшаясь, а число их в несколько раз меньше m.

73. Пусть составное число m представлено в виде

$$m = a_1 a_2 a_3 \ldots a_n. \qquad (3)$$

Среди простых множителей $a_1, a_2, a_3, \ldots, a_n$ могут быть и равные между собою. Пусть между простыми множителями имеется α множителей, равных a, β множителей, равных b, γ множителей, равных c, и т. д., и, наконец, λ множителей, равных l. Тогда разложение (3) представится так:

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots l^{\lambda},$$

где $\alpha + \beta + \gamma + \ldots + \lambda = n$.

Такое разложение числа m на сомножителей называется каноническим.

Примеры. Каноническое разложение числа 100 будет:

$$100 = 2^2 \cdot 5^2.$$

Каноническое разложение числа 90 будет:

$$90 = 2 \cdot 5 \cdot 3^2.$$

Каноническое разложение числа 360 будет:

$$360 = 2^3 \cdot 3^2 \cdot 5.$$

74. Теперь покажем на примере, как выполняется разложение числа на простых сомножителей.

Пусть требуется 630 разложить на простых сомножителей. Делим 630 на 2, в частном получаем 315, так что

$$630 = 2 \cdot 315. \qquad (1)$$

315 больше не делится на 2, но делится на 3. Делим 315 на 3, получаем в частном 105, так что:

$$315 = 3 \cdot 105.$$

Заменив в равенстве (1) число 315 равным ему произведением $3 \cdot 105$, получим:

$$630 = 2 \cdot 3 \cdot 105. \qquad (2)$$

105 делится на 3; делим 105 на 3, получаем в частном 35, так что:

$$105 = 3 \cdot 35.$$

Заменив в равенстве (2) число 105 равным ему произведением $3 \cdot 35$, получим:

$$630 = 2 \cdot 3 \cdot 3 \cdot 35.$$

35 не делится на 3, но делится на 5; делим 35 на 5, получаем в частном 7, а 7 есть простое число; имеем:

$$35 = 5 \cdot 7.$$

Заменив в равенстве (3) число 35 равным ему произведением $5 \cdot 7$, получаем окончательно:

$$630 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 = 2 \cdot 3^2 \cdot 5 \cdot 7.$$

Каноническое разложение числа 630 будет:

$$630 = 2 \cdot 3^2 \cdot 5 \cdot 7.$$

Чтобы избежать при разложении числа на простых множителей лишнего письма, вычисления расположим так: пишем данное число 630 и проводим справа от него вертикальную черту; наименьший из простых делителей 630 есть 2; против 630 справа от черты пишем 2, делим 630 на 2, под 630 пишем частное 315. Наименьший из простых делителей 315 есть 3; против 315 справа от черты пишем 3, делим 315 на 3, под 315 пишем частное 105. С данным частным 105 поступаем так же, как с частным 315. Действия продолжаем до тех пор, пока в частном не получится единица. Тогда все числа, стоящие направо от черты, будут простыми сомножителями данного числа 630. Таким образом, мы пришли к следующему практическому правилу:

630	2
315	3
105	3
35	5
7	7
1	

Правило. *Чтобы разложить какое-нибудь число на простых сомножителей, мы проводим справа от этого числа вертикальную черту, делим данное число на наименьшего из его простых делителей, пишем этого делителя против данного числа справа от черты, а частное пишем под данным числом. Затем делим полученное частное на его наименьшего делителя*

и пишем этого делителя вслед за предыдущим, а полученное новое частное пишем под первым частным. Этот прием мы повторяем до тех пор, пока не получим частное, равное единице. Полученные все последовательные делители будут представлять простых сомножителей данного числа.

75. Способ представлять составные числа в каноническом виде бывает весьма полезен во многих случаях: он облегчает различные действия и обнаруживает различные свойства чисел.

1. *Когда числа представлены в каноническом виде, то произведение их получается так: складывают показателей одинаковых чисел, а те числа, которые входят только в одного сомножителя, переносят в произведение с их показателями.*

Пример. Пусть $a = 2^2 \cdot 3^3 \cdot 5 \cdot 11$; $b = 2^3 \cdot 3 \cdot 5^2 \cdot 7$.

Тогда:

$$ab = 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 2^5 \cdot 3^4 \cdot 5^3 \cdot 7 \cdot 11.$$

2. Посмотрим, когда деление числа a на число b возможно. Числа a и b представлены в каноническом виде. Пусть a делится на b. *Разделить число a на число b значит найти такое число c, которое, будучи умножено на делителя b, дает в произведении делимое a; имеем:*

$$a = bc. \qquad (1)$$

Мы имеем тождество. Но при умножении двух чисел показатели одинаковых чисел складываются, а те числа, которые входят только в одного сомножителя, переносятся в произведение с их показателями.

Из равенства (1) следует, что число a и число bc состоят из одних и тех же простых чисел с одними и теми же показателями. Следовательно, в делимое a входят все простые множители делителя b с показателями, не меньшими тех, с какими они входят в делителя b. Это условие необходимо, но оно и достаточно. В самом деле, в делимом a можно переставить вперед всех простых сомножителей делителя b и притом так, чтобы каждый из них имел показателя, равного тому, которого он имеет в делителе. Тогда становится очевидным, что a делится на b, и что частное c есть произведение других сомножителей a. Можно поэтому высказать следующую теорему:

Теорема. *Для того, чтобы одно из двух чисел, представленных в каноническом виде, делилось на другое, необходимо и достаточно, чтобы все простые сомножители делителя входили в делимое с показателями, не меньшими тех, с какими они входят в делителя.*

Следствия. *Деление числа a на число b невозможно в следующих случаях:*

1) когда в делителе есть числа, каких нет в делимом;

2) когда показатель какого-нибудь числа делимого меньше показателя того же числа в делителе.

Примечание. *Когда число разложено на простых сомножителей, то всякий из этих сомножителей есть делитель данного*

числа; произведение, составленное из нескольких сомножителей данного числа, также есть делитель этого числа. Если на него разделить данное число, то в частном получится произведение остальных сомножителей числа.

76. Теперь покажем, как находится общий наибольший делитель нескольких чисел, представленных в каноническом виде.

Обозначим данные числа через A, B, C, ... Пусть простые числа a, b, c, ... входят множителями во все данные числа. Пусть a входит в одно из данных чисел множителем α раз, во все же остальные числа—не менее α раз. Тогда каждое из данных чисел разделится на a^α. Точно так же пусть b входит в одно из данных чисел множителем β раз, во все же остальные числа—не менее β раз, и т. д.

Любое из данных чисел A, B, C, ... делится на каждое из попарно простых чисел a^α, b^β, c^γ, ..., следовательно, разделится и на их произведение $a^\alpha b^\beta c^\gamma \ldots$ (п. 52). Таким образом, произведение $a^\alpha b^\beta c^\gamma \ldots$ есть общий делитель всех данных чисел A, B, C, ... Но если этого общего делителя всех данных чисел мы умножим на какое угодно простое число, скажем, на a, то на полученное произведение $a^{\alpha+1} b^\beta c^\gamma \ldots$ уже не будет делиться, по крайней мере, одно из данных чисел. Отсюда следует, что $a^\alpha b^\beta c^\gamma \ldots$ есть искомый общий наибольший делитель всех данных чисел.

Итак,

$$(A, B, C, \ldots) = a^\alpha b^\beta c^\gamma \ldots \qquad (1)$$

Таким образом, мы приходим к следующему правилу:

Правило. *Чтобы найти общего наибольшего делителя нескольких чисел, представленных в каноническом виде, нужно взять простых множителей, общих всем данным числам, и каждого из них с его наименьшим показателем, с которым он входит во все данные числа. Произведение полученных таким образом степеней простых чисел и будет искомым общим наибольшим делителем всех данных чисел.*

Примечание. Если у чисел A, B, C, ... нет общих простых сомножителей, то эти числа взаимно простые.

Примеры 1. Найти общего наибольшего делителя чисел 504 и 840.

Решение. $504 = 2^3 \cdot 3^2 \cdot 7$; $840 = 2^3 \cdot 3 \cdot 5 \cdot 7$. Их общий наибольший делитель будет: $(504, 840) = 2^3 \cdot 3 \cdot 7 = 168$.

2. Найти общего наибольшего делителя чисел 180, 270 и 630.

Решение. $180 = 2^2 \cdot 3^2 \cdot 5$; $270 = 2 \cdot 3^3 \cdot 5$; $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$.

Их общий наибольший делитель будет:

$$(180, 270, 630) = 2 \cdot 3^2 \cdot 5 = 90.$$

77. Теперь покажем, как находится *общее наименьшее кратное* нескольких чисел, представленных в каноническом виде.

Обозначим данные числа через $A, B, C, \ldots$. Возьмем различные между собой простые числа $a, b, c, \ldots$. Пусть простое число a входит множителем по крайней мере в одно из данных чисел α_1 раз, во все же прочие числа не более α_1 раз (в состав некоторых чисел a может вовсе не входить).

Точно так же пусть простое число b входит множителем по крайней мере в одно из данных чисел β_1 раз, во все же прочие числа не более β_1 раз и т. д. Таким образом, $\alpha_1, \beta_1, \gamma_1, \ldots$ суть наибольшие из показателей, с какими простые числа $a, b, c \ldots$ встречаются в разложениях данных чисел $A, B, C, \ldots$. Но, чтобы одно число делилось на другое, необходимо и достаточно, чтобы каждый из простых сомножителей делителя входил в делимое с показателем, не меньшим того, которого он имеет в делителе. А чтобы число делилось на каждое из данных чисел, необходимо, чтобы в его состав вошли все простые числа, входящие в состав данных чисел, и притом с наибольшими показателями.

Такое число у нас выразится формулой $a^{\alpha_1} b^{\beta_1} c^{\gamma_1} \ldots$. Но если составленное таким образом число мы разделим на какое-нибудь простое число, скажем, на a, то $a^{\alpha_1 - 1} b^{\beta_1} c^{\gamma_1} \ldots$ уже не будет делиться по крайней мере на одно из данных чисел. Следовательно, число $a^{\alpha_1} b^{\beta_1} c^{\gamma_1} \ldots$ и есть искомое общее наименьшее кратное всех данных чисел $A, B, C, \ldots$. Итак,

$$m\,(A, B, C, \ldots) = a^{\alpha_1} b^{\beta_1} c^{\gamma_1} \ldots$$

Таким образом, мы приходим к такому правилу:

Правило. *Чтобы найти общее наименьшее кратное нескольких чисел, берем каждого простого множителя, входящего хотя бы в одно из данных чисел, и пишем его с наибольшим показателем, встречающимся при этом множителе в разложениях. Произведение полученных таким образом степеней простых чисел и будет искомым общим наименьшим кратным всех данных чисел.*

Примечание. *Если данные числа попарно простые, то общее наименьшее кратное этих чисел равно произведению их.*

Примеры. 1) Найти общее наименьшее кратное чисел 180 и 225.

Решение. $180 = 2^2 \cdot 3^2 \cdot 5$; $225 = 3^2 \cdot 5^2$, откуда получаем:

$$m\,(180, 225) = 2^2 \cdot 3^2 \cdot 5^2 = 900.$$

2) Найти общее наименьшее кратное чисел 72, 225 и 70.

Решение. $72 = 2^3 \cdot 3^2$; $225 = 3^2 \cdot 5^2$; $70 = 2 \cdot 5 \cdot 7$.

Откуда

$$m\,(72, 225, 70) = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 = 12600.$$

ГЛАВА ПЯТАЯ

Числовые функции

78. В математике встречаются два рода величин: *1) постоянные и 2) переменные. Постоянной величиной называется такая величина, которая сохраняет всегда или только в данном вопросе одно определенное значение. Переменной величиной называется такая величина, которая в данном вопросе может принимать различные значения.* Если две переменные величины x и y, из которых каждая имеет определенную совокупность значений (или область изменения), связаны между собою по определенному закону так, что каждому значению x из его области изменения соответствует определенное значение y из его области, то x называется независимой переменной или аргументом, а y — зависимой переменной или фукцией от x, и пишут $y=f(x)$. Вместо f можно употреблять и другие буквы. В математическом анализе изучаются такие функции, аргумент которых может принимать не только вещественные значения, но и комплексные. *Мы же будем изучать только такие функции, аргумент которых может принимать только целые положительные значения. Функция, аргумент которой может принимать только целые положительные значения, называется числовой.*

79. Всякое число делится на единицу и на самого себя. Эти делители называются *несобственными делителями* числа в отличие от других его делителей (если таковые существуют), которые называются *собственными.* Собственных делителей может иметь только составное число.

80. Число делителей числа. Число делителей данного числа легко мы найдем, если нам известно каноническое разложение этого числа. Пусть

$$n=a^{\alpha}b^{\beta}c^{\gamma}\ldots l^{\lambda},$$

где $a, b, c, \ldots, l$ суть различные между собою простые числа, а $a^{\alpha}, b^{\beta}, c^{\gamma}, \ldots, l^{\lambda}$ — наивысшие степени, в которых эти простые числа входят в состав n. Возьмем многочлены:

$$\begin{aligned} A&=1+a+a^2+\ldots+a^{\alpha}\\ B&=1+b+b^2+\ldots+b^{\beta}\\ C&=1+c+c^2+\ldots+c^{\gamma}\\ &\ldots\ldots\ldots\ldots\\ L&=1+l+l^2+\ldots+l^{\lambda}. \end{aligned} \qquad (1)$$

Определим число членов произведения $ABC\ldots L$. Сколько членов в каждом из многочленов (1), нам известно: в многочлене A членов $\alpha+1$, в многочлене B членов $\beta+1$, в многочлене C членов $\gamma+1$, и т. д., и, наконец, в многочлене L членов $\lambda+1$.

Раскрывая скобки в правой части равенства

$$AB=(1+a+a^2+\ldots+a^{\alpha})\,(1+b+b^2+\ldots+b^{\beta}),$$

мы получим $(\alpha+1)(\beta+1)$ членов. Раскрывая скобки в правой части равенства

$$ABC=(1+a+a^2+\ldots+a^\alpha)(1+b+b^2+\ldots+b^\beta)(1+c+c^2+\\+\ldots+c^\gamma),$$

мы получим $(\alpha+1)(\beta+1)(\gamma+1)$ членов, и т. д. Наконец, раскрывая скобки в правой части равенства

$$ABC\ldots L=(1+a+a^2+\ldots+a^\alpha)\ (1+b+b^2+\ldots+\\+b^\beta)(1+c+c^2+\ldots+c^\gamma)\ldots(1+l+l^2+\ldots+l^\lambda),$$

мы получим $(\alpha+1)\ (\beta+1)\ (\gamma+1)\ \ldots\ (\lambda+1)$ членов.

Старший (или высший) член этого произведения есть $a^\alpha\ b^\beta\ c^\gamma\ldots l^\lambda$, а младший (или низший) член есть **1**. Каждый член произведения представляет собою произведение, причем в состав каждого такого произведения входит по одному члену из каждого многочлена. Все эти произведения различны между собою. Число n делится на любой член каждого из многочленов (1), оно также разделится и на любое произведение, в состав которого входит по одному члену из каждого многочлена. Но n не разделится ни на одно число, отличное от членов произведения $ABC\ldots L$. Поэтому все $(\alpha+1)\ (\beta+1)\ (\gamma+1)\ \ldots(\lambda+1)$ членов произведения $ABC\ldots L$ представляют собою всех делителей числа n. Итак, число всех делителей числа n равно

$$(\alpha+1)\ (\beta+1)\ (\gamma+1)\ldots(\lambda+1).$$

Таким образом, мы доказали следующее важное предложение:

Теорема. *Число всех делителей числа* $n\ (=a^\alpha b^\beta c^\gamma\ldots l^\lambda)$ *равно произведению увеличенных на единицу показателей различных простых чисел, входящих в каноническое разложение числа* n.

Обозначив число всех делителей числа n символом $\tau(n)$, получим следующую формулу:

$$\tau(n)=\tau(a^\alpha b^\beta c^\gamma\ldots l^\lambda)=(\alpha+1)\ (\beta+1)\ (\gamma+1)\ldots(\lambda+1).$$

Из этой формулы видно, что число всех делителей числа $n=a^\alpha b^\beta c^\gamma\ldots l^\lambda$ зависит от показателей α, β, γ, . . ., λ, но не от простых множителей a, b, c, . . ., l. Так, например, числа $12=2^2\cdot 3$ и $931=7^2\cdot 19$ имеют одинаковое число делителей: $\tau(12)=\tau(931)=(2+1)\ (1+1)=6$.

Для каждого данного числа n число его делителей имеет определенное численное значение; следовательно, число делителей числа n есть функция числа n, изменяющаяся с изменением n.

81. Теперь покажем, как найти всех делителей числа 180.

Имеем: $180=2^2\cdot 3^2\cdot 5$; $A=1+2+4$; $B=1+3+9$; $C=1+5$.

Члены произведения ABC и будут делителями числа 180.

Действия располагаем так:

$$\begin{array}{r} \times \begin{matrix} 1+2+4 \\ 1+3+9 \end{matrix} \\ \hline 1+2+4+3+6+12+9+18+36 \\ \times 1+5 \\ \hline 1+2+4+3+6+12+9+18+36+5+10+20+15+30+60+45+90+180 \end{array}$$

Следовательно, делителями 180 являются 18 чисел:

1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.

Покажем другой прием нахождения всех делителей числа $180 = 2^2 \cdot 3^2 \cdot 5$. Составляем три ряда:

$$\begin{matrix} 1, 2, 4 \\ 1, 3, 9 \\ 1, 5. \end{matrix}$$

Первая строка содержит всех делителей 2^2, вторая строка — всех делителей 3^2, а третья строка — всех делителей 5. Умножаем каждое число первой строки на каждое число второй строки и все полученные произведения умножаем на каждое число третьей строки. Получаем

$$\begin{array}{r} \times \begin{matrix} 1, 2, 4 \\ 1, 3, 9 \end{matrix} \\ \hline 1, 2, 4, 3, 6, 12, 9, 18, 36 \\ \times 1, 5 \\ \hline 1, 2, 4, 3, 6, 12, 9, 18, 36, 5, 10, 20, 15, 30, 60, 45, 90, 180. \end{array}$$

Полученные числа будут представлять собою всех делителей числа 180.

82. Определим сумму делителей числа

$$n = a^\alpha b^\beta c^\gamma \ldots l^\lambda.$$

Возьмем многочлены:

$$\begin{aligned} A &= 1 + a + a^2 + \ldots + a^\alpha \\ B &= 1 + b + b^2 + \ldots + b^\beta \\ C &= 1 + c + c^2 + \ldots + c^\gamma \\ &\cdots\cdots\cdots \\ L &= 1 + l + l^2 + \ldots + l^\lambda \end{aligned}$$

Было доказано (п. 80), что число делителей числа n равно числу членов произведения

$$ABC \ldots L = (1 + a + a^2 + \ldots + a^\alpha)(1 + b + b^2 + \ldots + b^\beta)(1 + c + c^2 + \ldots + c^\gamma) \ldots (1 + l + l^2 + \ldots + l^\lambda) \quad (1)$$

и выражается формулой

$$\tau(a^\alpha b^\beta c^\gamma \ldots l^\lambda) = (\alpha + 1)(\beta + 1)(\gamma + 1) \ldots (\lambda + 1).$$

Тогда сумма делителей числа n будет равна сумме членов произведения (1), или, что одно и то же, самому произведению (1). Но так как

$$1+a+a^2+\ldots+a^\alpha=\frac{a^{\alpha+1}-1}{a-1},$$

$$1+b+b^2+\ldots+b^\beta=\frac{b^{\beta+1}-1}{b-1},$$

$$1+c+c^2+\ldots+c^\gamma=\frac{c^{\gamma+1}-1}{c-1},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$1+l+l^2+\ldots+l^\lambda=\frac{l^{\lambda+1}-1}{l-1},$$

то, обозначив сумму всех делителей числа n символом $S(n)$, получим следующую формулу:

$$S(n)=S(a^\alpha b^\beta c^\gamma\ldots l^\lambda)=\frac{a^{\alpha+1}-1}{a-1}\cdot\frac{b^{\beta+1}-1}{b-1}\cdot\frac{c^{\gamma+1}-1}{c-1}\cdots\frac{l^{\lambda+1}-1}{l-1}.$$

Для каждого данного числа n сумма всех его делителей имеет определенное численное значение; следовательно, сумма всех делителей числа n есть функция числа n, изменяющаяся с изменением n.

Пример. Найти сумму всех делителей числа 12600.

Решение. $12600=2^3\cdot 3^2\cdot 5^2\cdot 7$; $S(2^3\cdot 3^2\cdot 5^2\cdot 7)=$

$$=\frac{2^4-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^3-1}{5-1}\cdot\frac{7^2-1}{7-1}=15\cdot 13\cdot 31\cdot 8=48360.$$

83. Свойства чисел еще в глубокой древности привлекали внимание греков. Так, например, пифагорейцы (последователи учения древнегреческого философа Пифагора) поставили вопрос о нахождении чисел, равных сумме своих настоящих (правильных) делителей (настоящим делителем или правильным делителем числа n называется всякий его делитель, отличный от самого числа n). Такие числа называются совершенными. Итак, совершенным числом называется всякое число, которое равно сумме своих правильных делителей. Обозначая через $S(n)$ сумму всех делителей числа n, совершенное число выразим тогда формулой:

$$S(n)-n=n, \text{ или формулой } S(n)=2n.$$

Таковы, например, числа:

$$6=1+2+3;\ 28=1+2+4+7+14.$$

С совершенными числами имеют сходство дружественные числа. Два числа m и n называются дружественными, если каждое из них равно сумме правильных делителей другого.

Получаем:

$$m = S(n) - n, \text{ или } S(n) = m + n,$$
$$n = S(m) - m, \text{ или } S(m) = m + n,$$

Следовательно,

$$S(m) = S(n) = m + n.$$

Таковы, например, числа

$$m = 2^2 \cdot 5 \cdot 11 = 220 \text{ и } n = 2^2 \cdot 71 = 284,$$
$$m + n = 504.$$

В самом деле,

$$S(2^2 \cdot 5 \cdot 11) = \frac{2^3 - 1}{2 - 1} \cdot \frac{5^2 - 1}{5 - 1} \cdot \frac{11^2 - 1}{11 - 1} = 504;$$
$$S(2^2 \cdot 71) = \frac{2^3 - 1}{2 - 1} \cdot \frac{71^2 - 1}{71 - 1} = 7 \cdot 72 = 504;$$
$$S(2^2 \cdot 5 \cdot 11) = S(2^2 \cdot 71) = 504.$$

84. Функция Эйлера. *Обозначим через $\varphi(n)$ число целых положительных чисел, меньших данного числа n и вместе с ним простых относительно n.*

Эта функция введена Эйлером и называется функцией Эйлера.

Непосредственная проверка дает:

Число n	Числа, взаимно простые с n	Значение $\varphi(n)$	Число n	Числа, взаимно простые с n	Значение $\varphi(n)$
$n = 2$	1	$\varphi(2) = 1$	$n = 5$	1, 2, 3, 4	$\varphi(5) =$
$n = 3$	1, 2	$\varphi(3) = 2$	$n = 6$	1, 5	$\varphi(6) =$
$n = 4$	1, 3	$\varphi(4) = 2$	$n = 7$	1, 2, 3, 4, 5, 6	$\varphi(7) =$

Чтобы не исключить случая, когда $n = 1$, принято говорить еще так: „$\varphi(n)$ *означает число чисел, взаимно простых с n не больших, чем n*“. Так как единица есть число взаимно простое с единицей и не больше единицы, то $\varphi(1) = 1$.

Теперь нам надо найти общее выражение для функции $\varphi(n)$. Рассмотрим для этого следующие три случая:

Первый случай. n есть простое число. В этом случае каждое из $n - 1$ чисел ряда 1, 2, 3, 4, . . ., $n - 1$ будет меньше n и простым относительно n; следовательно, в этом случае

$$\varphi(n) = n - 1. \qquad (1)$$

Второй случай. n есть степень простого числа p: $n = p^\alpha$. Числа, простые относительно p и меньшие, чем p, суть те из чисел ряда

$$1, 2, 3, 4, 5, \ldots, p^\alpha - 1, p^\alpha, \qquad (2)$$

которые не делятся на p. Числа, кратные p, суть следующие

$$1 \cdot p, 2 \cdot p, 3 \cdot p, 4 \cdot p, 5 \cdot p, \ldots, p^{\alpha-1} \cdot p. \qquad (3)$$

В ряду (2) всего p^α чисел; в ряду (3) всего $p^{\alpha-1}$ чисел, кратных p. Вычитая из p^α чисел ряда (2) $p^{\alpha-1}$ чисел ряда (3), мы получим число членов ряда (2), взаимно простых с p:

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

Стало быть,

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha\left(1-\frac{1}{p}\right). \qquad (4)$$

Примеры. 1. $\varphi(5^2) = 5\,(5-1) = 20.$

2. $\varphi(2^4) = 2^3(2-1) = 8.$

Третий случай. В состав числа n входят различные простые множители a, b, c, d, ... Требуется определить число тех чисел ряда

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ \ldots,\ n, \qquad (5)$$

которые не делятся ни на одно из простых чисел a, b, c, d, ...

Поступаем так: исключаем из ряда (5) все числа, которые делятся на a.

Установить количество таких чисел легко: выпишем из ряда (5) все числа, кратные a; получим такой ряд:

$$1\cdot a,\ 2\cdot a,\ 3\cdot a,\ 4\cdot a,\ 5\cdot a,\ \ldots,\ \frac{n}{a}\cdot a.$$

В полученном ряду всего $\frac{n}{a}$ чисел, кратных a. Следовательно, в ряду (5) также всего $\frac{n}{a}$ чисел, кратных a.

Разность

$$n - \frac{n}{a} = n\left(1-\frac{1}{a}\right) \qquad (6)$$

есть число членов ряда (5), взаимно простых с a. Таким образом, мы доказали следующее предложение:

Теорема. *Число чисел ряда (5), которые не делятся на простое число a, входящее в состав n, равно произведению*

$$n\left(1-\frac{1}{a}\right).$$

Исключив из ряда (5) $\frac{n}{a}$ чисел, кратных a, получим новый ряд, в котором всего будет $n\left(1-\frac{1}{a}\right)$ чисел.

Пусть этот ряд будет такой:

$$a_1,\ a_2,\ a_3,\ a_4,\ \ldots,\ a_\alpha, \qquad (7)$$

где $\alpha = n\left(1-\frac{1}{a}\right)$.

Из ряда (7) нужно исключить все числа, кратные b. Но исключить из ряда (7) все числа, кратные b, значит исключить из

ряда (5) все те числа, которые одновременно удовлетворяют двум условиям, а именно: они не делятся на a, но делятся на b.

Выпишем из ряда (5) все числа, кратные b; получим такой ряд:

$$1 \cdot b,\ 2 \cdot b,\ 3 \cdot b,\ 4 \cdot b,\ \ldots,\ \frac{n}{b} \cdot b.$$

Среди чисел этого ряда находятся и такие числа, которые не делятся на a. Для того, чтобы какое-нибудь из этих чисел, например, rb, не делилось на a, необходимо и достаточно, чтобы коэффициент его r не делился на a (a и b взаимно простые числа). Поэтому из ряда (7) придется исключить столько чисел, сколько чисел ряда

$$1,\ 2,\ 3,\ 4,\ 5,\ \ldots,\ \frac{n}{b}$$

не делится на a.

Применив к данному ряду предыдущую теорему, получим

$$\frac{n}{b}\left(1 - \frac{1}{a}\right)$$

чисел. Мы нашли, что количество чисел ряда (7), которые делятся на b, выражается произведением

$$\frac{n}{b}\left(1 - \frac{1}{a}\right).$$

При исключении из ряда (7) $\frac{n}{b}\left(1 - \frac{1}{a}\right)$ чисел в ряду всего останется

$$n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$$

чисел, которые не делятся на b. Но в то же время $n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$ есть количество тех чисел ряда (5), которые не делятся ни на a, ни на b.

В самом деле, исключив из ряда (5) сначала $\frac{n}{a}$ чисел, кратных a, мы получим ряд, в котором будет всего $n\left(1 - \frac{1}{a}\right)$ чисел. Из этих оставшихся $n\left(1 - \frac{a}{1}\right)$ чисел мы выбросили еще $\frac{n}{b}\left(1 - \frac{1}{a}\right)$ чисел, кратных b. После этих двух операций в ряду осталось всего $n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$ чисел, которые не делятся ни на a, ни на b.

Таким образом, мы пришли к такой теореме:

Теорема. *Число членов ряда (5), которые не делятся ни на одно из простых чисел a и b, входящих в состав n, равно произведению*

$$n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right).$$

Исключив из ряда (7) $\frac{n}{b}\left(1-\frac{1}{a}\right)$ чисел, кратных b, мы получим новый ряд, в котором всего будет $n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$ чисел.

Пусть этот новый ряд будет такой:

$$b_1,\ b_2,\ b_3,\ \ldots,\ b_\beta, \tag{8}$$

где $\beta = n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{a}\right)$. Из ряда (8) исключим все числа, кратные c. Но исключить из ряда (8) все числа, кратные c, значит из ряда (5) исключить все те числа, которые одновременно удовлетворяют двум условиям, а именно: они не делятся ни на a, ни на b, но зато делятся на c. Выпишем из ряда (5) все числа, кратные c. Получим такой ряд:

$$1\cdot c,\ 2\cdot c,\ 3\cdot c,\ 4\cdot c,\ \ldots,\ \frac{n}{c}\cdot c. \tag{9}$$

Среди этих чисел находятся и такие числа, которые не делятся ни на a, ни на b. Но для того, чтобы какое-нибудь число ряда (9), например, rc, не делилось ни на a, ни на b, необходимо и достаточно, чтобы его коэффициент r не делился ни на a, ни на b. Поэтому из ряда (8) придется удалить столько чисел, сколько в ряду

$$1,\ 2,\ 3,\ 4,\ \ldots,\ \frac{n}{c} \tag{10}$$

есть чисел, не делящихся ни на a, ни на b.

Как найти количество чисел ряда (10), которые не делятся ни на a, ни на b, мы знаем: надо $\frac{n}{c}$ помножить на $\left(1-\frac{1}{a}\right)\cdot\left(1-\frac{1}{b}\right)$.

Получаем

$$\frac{n}{c}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$$

чисел. Мы нашли, что в ряду (8) есть $\frac{n}{c}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$ чисел, кратных c. Если исключить из ряда (8) все числа, кратные c, в ряду всего останется

$$n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)$$

чисел, которые не делятся на c. Но в то же время

$$n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{a}\right)\left(1-\frac{1}{c}\right)$$

есть число тех чисел ряда (5), которые не делятся ни на a, ни на b, ни на c. Таким образом, мы пришли к такой теореме:

Теорема. *Число членов ряда (5), которые не делятся ни на одно из простых чисел a, b, c, входящих в состав числа n, равно произведению*

$$n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right).$$

Докажем, что эта теорема справедлива для любого числа простых чисел, входящих в состав n. С этой целью допустим, что она имеет место для m разных простых чисел $a, b, c, d, \ldots, k$, входящих в состав n. Имеем:

$$n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right). \qquad (11)$$

Получается такая теорема:

Теорема. *Число чисел ряда (5), которые не делятся ни на одно из простых чисел $a, b, c, \ldots, k$, входящих в состав n, равно произведению*

$$n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right). \qquad (12)$$

Сделав такое допущение, докажем, что теорема будет иметь место и для $m+1$ простых чисел, входящих в состав n.

Пусть

$$n = abc\ldots kl.$$

Нам нужно найти число членов ряда (5), которые не делятся ни на одно из простых чисел $a, b, c, d, \ldots, k, l$. Произведение (12) есть число тех чисел ряда (5), которые не делятся ни на одно из простых чисел $a, b, c, d, \ldots, k$. Из этих

$$n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right)$$

чисел ряда (5) составим новый ряд. Пусть этот новый ряд будет такой:

$$k_1, k_2, k_3, k_4 \ldots, k_x, \qquad (13)$$

где $x = n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots\left(1-\frac{1}{k}\right)$.

Из ряда (13) исключим все числа, кратные l. Но исключить из ряда (13) все числа, кратные l, значит из ряда (5) исключить все те числа, которые одновременно удовлетворяют двум условиям: они не делятся ни на одно из простых чисел $a, b, c, \ldots, k$, входящих в состав n, но делятся на l. Выпишем из ряда (5) все числа, кратные l. Получим такой ряд:

$$1\cdot l,\ 2\cdot l,\ 3\cdot l,\ 4\cdot l,\ \ldots,\ \frac{n}{l}\cdot l. \qquad (14)$$

Среди чисел этого ряда находятся и такие числа, которые не делятся ни на одно из простых чисел $a, b, c, d, \ldots, k$. Но для того, чтобы какое-нибудь число ряда (14), скажем, rl, не делилось ни на одно из простых чисел $a, b, c, d, \ldots, k$, необходимо и достаточно, чтобы коэффициент его r не делился ни на одно из простых чисел $a, b, c, \ldots, k$. Поэтому из ряда (13) придется удалить столько чисел, сколько в ряду

$$1, 2, 3, 4, \ldots, \frac{n}{l} \qquad (15)$$

есть чисел, которые не делятся ни на одно из простых чисел $a, b, c, \ldots, k$.

Как найти число членов ряда (15), которые не делятся ни на одно из простых чисел $a, b, c, \ldots, k$, мы знаем: надо $\frac{n}{l}$ умножить на $\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right)$.

Получаем

$$\frac{n}{l}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right)$$

чисел.

В ряду (13) всего $n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right)$ чисел. При исключении из этого ряда

$$\frac{n}{l}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right)$$

чисел, кратных l, в ряду (13) всего останется

$$n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{l}\right)$$

чисел, которые не делятся на l. В то же время полученное выражение означает число тех чисел ряда (5), которые не делятся ни на одно из простых чисел $a, b, c, d, \ldots, k, l$, входящих в состав n. Таким образом, теорема доказана в общем виде. Обозначив число чисел ряда (5), меньших n и взаимно простых с ним, через $\varphi(n)$, получим такую формулу:

$$\varphi(n)=n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{l}\right). \quad (16)$$

Пример. Найти $\varphi(30)$.

Решение. Имеем: $30=2\cdot 3\cdot 5$. Тогда

$$\varphi(2\cdot 3\cdot 5)=30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=8.$$

Действительно, в ряду 1, 2, 3, 4, 5, ..., 30 находятся следующие 8 чисел, меньших 30 и взаимно простых с 30: 1, 7, 11, 13, 17, 19, 23, 29.

85. Теорема. Если m и n числа взаимно простые, то имеет место равенство

$$\varphi(mn)=\varphi(m)\varphi(n). \quad (1)$$

Доказательство. Пусть отличные друг от друга простые числа $a_1, a_2, a_3, \ldots$ входят множителями в состав m; другие отличные друг от друга простые числа $b_1, b_2, b_3, \ldots$ входят множителями в состав n. Таким образом, в состав произведения mn входят множителями простые числа $a_1, a_3, a_2, \ldots, b_1, b_2, b_3, \ldots$

Тогда

$$\varphi(mn)=$$

$$mn\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\left(1-\frac{1}{a_3}\right)\ldots\left(1-\frac{1}{b_1}\right)\left(1-\frac{1}{b_2}\right)\left(1-\frac{1}{b_3}\right)\ldots=$$

$$m\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\left(1-\frac{1}{a_3}\right)\ldots n\left(1-\frac{1}{b_1}\right)\left(1-\frac{1}{b_2}\right)\left(1-\frac{1}{b_3}\right)\ldots$$

Так как

$$\varphi(m)=m\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\left(1-\frac{1}{a_3}\right)\ldots,$$

$$\varphi(n)=n\left(1-\frac{1}{b_1}\right)\left(1-\frac{1}{b_2}\right)\left(1-\frac{1}{b_3}\right)\ldots,$$

то формула принимает следующий вид:

$$\varphi(mn)=\varphi(m)\varphi(n), \qquad (2)$$

что и требовалось доказать.

Очевидно, что эта теорема имеет место для произведения какого угодно числа попарно простых сомножителей. В самом деле, пусть произведение содержит в себе трех попарно простых сомножителей n_1, n_2, n_3. Тогда

$$\varphi(n_1n_2n_3)=\varphi((n_1n_1)n_3)=\varphi(n_1n_2)\varphi(n_3)=\varphi(n_1)\varphi(n_2)\varphi(n_3).$$

Переходя от случая трех попарно простых сомножителей к случаю четырех, ... попарно простых сомножителей, получим

$$\varphi(n_1n_2n_3\ldots n_\kappa)=\varphi(n_1)\varphi(n_2)\varphi(n_3)\ldots\varphi(n_\kappa). \qquad (3)$$

Пусть данное число n представлено в каноническом виде:

$$n=a^\alpha b^\beta c^\gamma\ldots l^\lambda.$$

Тогда получим:

$$\varphi(n)=\varphi(a^\alpha)\varphi(b^\beta)\varphi(c^\gamma)\ldots\varphi(l^\lambda)=$$

$$=\begin{cases} a^\alpha\left(1-\frac{1}{a}\right)b^\beta\left(1-\frac{1}{b}\right)c^\gamma\left(1-\frac{1}{c}\right)\ldots l^\lambda\left(1-\frac{1}{l}\right). \\ a^{\alpha-1}(a-1)\cdot b^{\beta-1}(b-1)\cdot c^{\gamma-1}(c-1)\ldots l^{\lambda-1}(l-1). \\ a^\alpha b^\beta c^\gamma\ldots l^\lambda\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots\left(1-\frac{1}{c}\right)\ldots\left(1-\frac{1}{l}\right) \\ a^{\alpha-1}b^{\beta-1}c^{\gamma-1}\ldots l^{\lambda-1}(a-1)(b-1)(c-1)\ldots(l-1). \end{cases}$$

Пример. Найти $\varphi(60)$.

Решение. Имеем: $60=2^2\cdot 3\cdot 5$. Тогда

$$\varphi(2^2\cdot 3\cdot 5)=\varphi(2^2)\varphi(3)\varphi(5)=2(2-1)\cdot 2\cdot 4=$$
$$=2\cdot 2\cdot 4=16.$$

ГЛАВА ШЕСТАЯ

Сравнения и их свойства

86. Класс целых чисел содержит в себе класс положительных целых чисел (1, 2, 3, 4, ...), класс отрицательных целых чисел (—1, —2, —3, ...) и число 0. *Теория чисел занимается изучением свойств целых чисел.* Одни математики называют теорию чисел высшей арифметикой, а другие математики говорят: „теория чисел — это та же арифметика, но расширенная и углубленная".

Возьмем два целых числа a и b. Пусть их разность $a-b$ делится на целое положительное число k. Тогда говорят: *„a сравнимо с b по модулю p“* и пишут:

$$a \equiv b \pmod{k}, \text{ или короче } a \equiv b \ (k).$$

Такое соотношение между a и b называется сравнением. Знак сравнения $\equiv$ был введен Гауссом. *Числа a и b называются членами сравнения, а число k — модулем сравнения.* Слово „модуль“ заменяет здесь слово „делитель“. Числа a и b называются также сравнимыми по модулю k. (П. Чебышев. Теория сравнений. Изд. 3-е, стр. 20). Члены сравнения a и b могут быть какими угодно целыми числами, но модуль сравнения k всегда предполагается числом натуральным и большим единицы. Если же разность $a-b$ не делится на k, то говорят: *„a не сравнимо с b по модулю k“ и пишут*:

$$a \not\equiv b \pmod{k}$$

В частности, сказать, что a сравнимо с 0 по модулю k или написать сравнение $a \equiv 0 \pmod{k}$, значит сказать, что a делится на k. Так, например, для обозначения, что разность $19-4$ делится на 5, пишут $19 \equiv 4 \pmod{5}$.

Сравнение $21 \equiv 0 \pmod{7}$ означает, что 21 делится на 7.

Примечание. Если при вычислении модуль не меняется, то его часто опускают. Сравнения обладают многими свойствами; некоторые из них аналогичны свойствам равенств. Перечислим свойства сравнений.

87. Теорема. *Всякое число a сравнимо с самим собою по модулю k.*

$$a \equiv a \pmod{k}.$$

Доказательство. Действительно, $a-a=0$ делится не только на k, но и на любой модуль.

88. Теорема. *Всякое число сравнимо со своим остатком, если за модуль принять делителя.*

Доказательство. Обозначим частное от деления a на k через q, а остаток — через r. Зная, что делимое равно произведению делителя на частное, сложенному с остатком, имеем: $a = kq + r$. Это равенство можно записать в таком виде: $a - r = kq$; это равенство показывает, что разность $a-r$ делится на k, а делимость разности $a-r$ на k выражается сравнением $a \equiv b \pmod{k}$, что и требовалось доказать.

89. Теорема. *Два числа a и b, которые при делении на k дают один и тот же остаток r, сравнимы по модулю k.*

Доказательство. Пусть a и b при делении на k дают один и тот же остаток r.

Пусть при делении a и b на k получаются соответственно частные q_1 и q_2.

По свойству деления должно быть:

$$a = kq_1 + r, \ b = kq_2 + r.$$

Вычитая из первого равенства почленно второе, получим $a-b=(q_1-r_2)k$. Из этого равенства видно, что разность $a-b$ делится на k, а делимость разности $a-b$ на k выражается сравнением

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

Примечание. *Два числа, дающие при делении на одного того же делителя равные остатки, называются разноостаточными относительно этого делителя* (п. 9).

Поэтому эта теорема может быть сформулирована так: *Равноостаточные числа a и b сравнимы между собою по модулю k.*

90. Теорема. *Два числа a и b, сравнимые по модулю k с третьим числом c, сравнимы между собою по тому же модулю k.*

Доказательство. Пусть будут даны сравнения $a\equiv c$, $b\equiv c$. Требуется доказать, что в данном случае должно иметь место сравнение $a\equiv b \pmod{k}$.

Из делимости разностей $a-c$ и $b-c$ на k следует, что разность этих разностей должна делиться на k [если уменьшаемое и вычитаемое делятся на какое-нибудь число, то и разность разделится на это число (п. 6)]. Но разность этих разностей есть $a-b$, а делимость разности $a-b$ на k выражается сравнением

$$a\equiv b \pmod{k},$$

что и требовалось доказать.

Пример. $25\equiv 4 \pmod 3$, $13\equiv 4 \pmod 3$. Получаем

$$25\equiv 13 \pmod 3.$$

91. Теорема. *Любой член сравнения можно перенести из одной части в другую, меняя лишь при этом его знак на обратный.*

Доказательство. Пусть будет дано сравнение

$$a+b\equiv c-d \pmod{k}.$$

Требуется доказать, что $a+d\equiv c-b \pmod{k}$.

Из определения сравнения следует, что разность $(a+b)-(c-d)$ делится на k. Но эту разность можно записать так $(a+d)-(c-b)$, а делимость этой разности на k выражается сравнением:

$$a+d\equiv c-b \pmod{k},$$

что и требовалось доказать.

92. Теорема. *Сравнения с одним и тем же модулем можно почленно складывать и вычитать.*

Доказательство. Пусть будут даны сравнения

$$a\equiv b \pmod{k},\quad c\equiv d \pmod{k}.$$

Требуется доказать, что

$$a+c\equiv b+d \pmod{k},\quad a-c\equiv b-d \pmod{k}.$$

Из определения сравнения следует, что разности $a-b$ и $c-d$ делятся на k. Из делимости этих разностей на k следует, что сумма их разделится на k.

Но сумму этих разностей можно записать так:

$$(a+c)-(b+d),$$

а делимость этого выражения на k выражается сравнением

$$a+c\equiv b+d \pmod{k}.$$

Далее, из делимости разностей $a-b$ и $c-d$ на k следует, что разность этих разностей также делится на k. Но эта последняя разность есть $(a-c)-(b-d)$, а делимость ее на k выражается сравнением $a-c\equiv b-d \pmod{k}$.

Таким образом, теорема доказана полностью.

93. Теорема. *Члены сравнения могут быть умножены на одно и то же число.*

Доказательство. Дано сравнение $a\equiv b \pmod{k}$. Требуется доказать, что $mb\equiv mb \pmod{k}$. Из данного сравнения следует, что разность $a-b$ делится на k. Из делимости разности $a-b$ на k следует, что $ma-mb$ также делится на k (п. 13), а делимость разности $ma-mb$ на k выражается сравнением

$$ma\equiv mb \pmod{k},$$

что и требовалось доказать.

94. Теорема. *Можно изменить одновременно знаки у всех членов сравнения.*

Доказательство. Пусть дано сравнение

$$a-b\equiv c+d-e \pmod{k}. \qquad (1)$$

Требуется доказать, что $b-a\equiv e-c-d \pmod{k}$.

Вычитая почленно сравнение (1) из сравнения $0\equiv 0 \pmod{k}$, получим сравнение

$$b-a\equiv e-c-d \pmod{k},$$

что и требовалось доказать.

95. Теорема. *Сравнения с одним и тем же модулем можно почленно перемножать.*

Доказательство. Пусть даны сравнения

$$a\equiv b \pmod{k},\ c\equiv d \pmod{k}.$$

Требуется доказать, что $ac\equiv bd \pmod{k}$.

Из определения сравнения следует, что разность $a-b$ делится на k. Обозначим частное от деления $a-b$ на k через q_1. Получаем:

$$a-b=kq_1, \text{ или } a=b+kq_1. \qquad (1)$$

Разность $c-d$ также делится на p. Обозначив частное от деления $c-d$ на k через q_2, получим $c=d+kq_2$. (2)

Перемножая почленно равенства (1) и (2), получим:

$$ac = bd + (dq_1 + bq_2 + kq_1q_2)k,$$

или

$$ac - bd = (dq_1 + bq_2 + kq_1q_2)k.$$

Из этого равенства видно, что разность $ac - bd$ делится на k, а делимость этой разности на k выражается сравнением:

$$ac \equiv bk \pmod{k},$$

что и требовалось доказать.

96. Теорема. *Оба члена сравнения можно возвышать в одну и ту же целую положительную степень.*

Доказательство. Положим, что мы имеем сравнение $a \equiv b \pmod{k}$. Требуется доказать, что $a^n \equiv b^n \pmod{k}$. Для доказательства возьмем n сравнений по одному и тому же модулю k:

$$a_1 \equiv b_1 \pmod{k},\ a_2 \equiv b_2 \pmod{k},\ a_3 \equiv b_3 \pmod{k},\ \ldots,\ a_n \equiv b_n \pmod{k}.$$

Если мы перемножим почленно сравнения $a_1 \equiv b_1$ и $a_2 \equiv b_2$ между собою, полученное сравнение $a_1a_2 \equiv b_1b_2$ и сравнение $a_3 \equiv b_3$ и т. д., то мы получим сравнение

$$a_1a_2a_3 \ldots a_n \equiv b_1b_2b_3 \ldots b_n \pmod{k}.$$

Полагая в полученном сравнении

$$a_1 = a_2 = a_3 = \ldots = a_n = a,\ b_1 = b_2 = b_3 = \ldots = b_n = b,$$

найдем:

$$a^n \equiv b^n \pmod{p},$$

что и требовалось доказать.

97. Теорема. *Обе части сравнения можно разделить на их общего наибольшего делителя, если этот делитель взаимно прост с модулем сравнения.*

Доказательство. Пусть дано сравнение $a \equiv b \pmod{k}$. Обозначив через d общего наибольшего делителя членов сравнения a и b, а частные от деления a и b на d соответственно через a_1 и b_1, имеем:

$$a = da_1,\ b = db_1.$$

Заменив в нашем сравнении члены a и b соответственно через da_1 и db_1, получаем:

$$a_1d \equiv b_1d \pmod{k}.$$

Разность $da_1 - db_1 = (a_1 - b_1)d$ делится на число k, взаимно простое с d. В таком случае разность $a_1 - b_1$ должна делиться на k (п. 40), а делимость разности $a_1 - b_1$ на k выражается сравнением

$$a_1 \equiv b_1 \pmod{k},$$

что и требовалось доказать.

98. Теорема. *Обе части сравнения и модуль можно умножить на одно и то же целое положительное число m.*

Доказательство. Пусть нам дано сравнение $a \equiv b \pmod{k}$. Требуется доказать, что из этого сравнения можно получить сравнение $ma \equiv mb \pmod{mk}$, где m есть натуральное число.

Из определения сравнения следует, что разность $a - b$ делится на k. Обозначим частное от деления разности $a - b$ на k через q. Находим: $a - b = kq$. Умножив обе части этого равенства на m, получим: $ma - mb = (km)\, q$.

Это равенство показывает, что разность $ma - mb$ делится на km, а делимость разности $ma - mb$ на km выражается сравнением

$$ma \equiv mb \pmod{km},$$

что и требовалось доказать.

99. Теорема. *Обе части сравнения и модуль можно разделить на их общего наибольшего делителя.*

Доказательство. Пусть нам дано сравнение $a \equiv b \pmod{k}$ и пусть d будет общий наибольший делитель чисел a, b, k. Обозначим частные от деления a, b, k на d соответственно через a_1, b_1, k_1. Имеем: $a = a_1 d$, $b = b_1 d$, $k = k_1 d$. Из определения сравнения следует, что разность $a - b$ делится на k. Пусть будет q частное от деления $a - b$ на k. Находим:

$$a - b = kq, \text{ или } a_1 d - b_1 d = k_1 dq.$$

Разделив обе части этого равенства на d, получим: $a_1 - b_1 = k_1 q$. Это равенство показывает, что разность $a_1 - b_1$ делится на k_1, а делимость разности $a_1 - b_1$ на k_1 выражается сравнением

$$a_1 \equiv b_1 \pmod{k_1},$$

что и требовалось доказать.

100. Теорема. *Если одна часть сравнения и модуль делятся на какое-нибудь число, то и другая часть сравнения должна делиться на то же число.*

Доказательство. Пусть дано сравнение $a \equiv b \pmod{k}$ (1). Из определения сравнения следует, что разность $a - b$ делится на k. Обозначим частное от деления разности $a - b$ на k через q. Находим: $a - b = kq$ (2). Положим, что a и k делятся на d и при делении на d дают соответственно частные a_1 и k_1. Находим: $a = a_1 d$, $k = k_1 b$. Тогда равенство (2) может быть записано так:

$$b = a - kq = a_1 d - k_1 dq = (a_1 - k_1 q)\, d,$$

а это равенство показывает, что b делится на d, что и требовалось доказать.

Примечание. Если бы b не делилось на d, то сравнение (1) было бы невозможно.

101. Теорема. *Сравнение не нарушается, если модуль сравнения заменим каким-нибудь из его делителей.*

Доказательство. Пусть дано сравнение $a \equiv b \pmod{k}$. Из определения сравнения следует, что разность $a - b$ делится на p.

Модуль сравнения k есть составное число. Представим k в виде произведения простых чисел: $k = k_1 k_2 k_3 \ldots k_n$. Из делимости разности $a - b$ на произведение $k_1 k_2 k_3 \ldots k_n$ следует, что разность $a - b$ делится на каждого из сомножителей $k_1, k_2, k_3, \ldots, k_n$ (п. 14), а делимость разности $a - b$ на сомножителей $k_1, k_2, k_3, \ldots, k_n$ может быть написана в виде сравнений

$$a \equiv b \pmod{k_1},\ a \equiv b \pmod{k_2},\ a \equiv b \pmod{k_3},\ \ldots,\ a \equiv b \pmod{k_n},$$

что и требовалось доказать.

102. Теорема. *Два числа, сравнимые между собою по нескольким модулям, попарно простым между собою, сравнимы и по модулю, равному произведению этих модулей.*

Доказательство. Пусть даны сравнения $a \equiv b \pmod{k_1}$, $a \equiv b \pmod{k_2}$, $a \equiv b \pmod{k_3}$, $\ldots$, $a \equiv b \pmod{k_n}$, где $k_1, k_2, k_3, \ldots, k_n$ суть попарно простые числа.

Требуется доказать, что из этих сравнений следует сравнение

$$a \equiv b \pmod{k_1 k_2 k_3 \ldots k_n}.$$

Из определения сравнения следует, что разность $a - b$ делится на каждое из попарно простых чисел $k_1, k_2, k_3, \ldots, k_n$. Из делимости разности $a - b$ на каждое из этих попарно простых чисел следует, что $a - b$ разделится и на произведение их $k_1 k_2 k_3 \ldots k_n$ (п. 52), а делимость разности $a - b$ на произведение $k_1 k_2 k_3 \ldots k_n$ выражается сравнением $a \equiv b \pmod{k_1 k_2 k_3 \ldots k_n}$, что и требовалось доказать.

103. Теорема. Если числа a и b сравнимы между собою по модулю k, а $f(x)$ есть целая функция с целыми коэффициентами, то значения $f(a)$ и $f(b)$ функции $f(x)$ при $x = a$ и $x = b$ также сравнимы между собою по тому же модулю k.

Доказательство. Пусть дано сравнение $a \equiv b \pmod{k}$, а

$$f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + a_3 x^{n-3} + \ldots + a_n$$

есть целая функция с целыми коэффициентами. Требуется доказать, что

$$f(a) \equiv f(b) \pmod{k}.$$

Из сравнения $a \equiv b \pmod{b}$ следует ряд сравнений по модулю k:

$$a^n \equiv b^n,\ a^{n-1} \equiv b^{n-1},\ a^{n-2} \equiv b^{n-2},\ a^{n-3} \equiv b^{n-3},\ \ldots,\ 1 \equiv 1.$$

Умножая члены первого сравнения на a_0, второго — на a_1, третьего — на a_2, и т. д., получим следующий ряд сравнений по модулю k:

$$a_0 a^n \equiv a_0 b^n,\ a_1 a^{n-1} \equiv a_1 b^{n-1},\ a_2 a^{n-2} \equiv a_2 b^{n-2},\ a_3 a^{n-3} \equiv$$
$$\equiv a_3 b^{n-3},\ \ldots,\ a_n \equiv a_n.$$

Складывая найденные сравнения почленно, получим:

$$a_0 a^n + a_1 a^{n-1} + a_2 a^{n-2} + a_3 a^{n-3} + \ldots + a_n \equiv a_0 b^n + a_1 b^{n-1} +$$
$$+ a_2 b^{n-2} + a_3 b^{n-3} + \ldots + a_n \pmod{k}.$$

Замечая, что

$$a_0a^n + a_1a^{n-1} + a_2a^{n-2} + a_3a^{n-3} + \ldots + a_n = f(a),$$

$$a_0b^n + a_1b^{n-1} + a_2b^{n-2} + a_3b^{n-3} + \ldots + a_n = f(b),$$

имеем:

$$f(a) \equiv f(b) \pmod{k},$$

что и требовалось доказать.

ГЛАВА СЕДЬМАЯ

Признаки делимости чисел

104. Свойства сравнений применим к выводу признаков делимости чисел. Признаками делимости чисел называются признаки, по которым, не производя самого деления, можно узнать, делится ли одно число на другое или нет (п. 15). „Системой счисления называется собрание правил, которые показывают, как проще всего считать числа, как называть их и как обозначать". (Н. А. Шапошников и Н. К. Вальцев. Сборник арифметических задач, ч. I, стр. 3, 1918).

Наша система счисления называется десятичной, потому что по этой системе 10 единиц одного разряда составляют одну единицу следующего высшего разряда. Число 10 называется основанием десятичной системы счисления. Система цифр, которою мы пользуемся, ведет свое происхождение из Индии. Возникновение этой удивительно совершенной системы, превзойти которую представляется совершенно невозможным, теряется во мраке древности. Из всех математических открытий ни одно так не способствовало общему прогрессу умственного развития, как изобретение нынешней системы письменной нумерации.

Индусская система обозначений проникла в Европу около XI или XII века через посредство арабов,[1] откуда произошло и самое название „арабское обозначение". Справедливость требует отметить, что арабы всегда признавали это обозначение наследием индусов. За основание системы счисления можно взять любое натуральное число, отличное от 1, например, 5. Известно, что для десятичной системы нужно 10 цифр: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0. Для пятеричной же системы нужно 5 цифр: 1, 2, 3, 4, 0. В пятеричной системе счисления цифры 0, 1, 2, 3, 4 означают те же числа, как и в десятичной системе счисления; число 5 в новой системе изображается в виде 10, число 6 — в виде 11, число 7 — в виде 12, число 8 — в виде 13, число 9 — в виде 14, число 10 — в виде 20. Таким образом, первые десять чисел нашего натурального ряда изображаются по пятеричной системе так: 1, 2, 3, 4, 10, 11, 12, 13, 14, 20. В десятичной системе счисления 10 единиц одного разряда составляют одну единицу следующего высшего разряда; в пятеричной же системе счисления 5 единиц

[1] Арабские цифры появились в России впервые в 1703 г. в „Арифметике" Леонтия Магницкого.

одного разряда составляют одну единицу следующего высшего разряда. Таким образом, по пятеричной системе единицей 2-го разряда должна быть пятерка, единицей 3-го разряда 5 пятерок или 5^2, единицей 4-го разряда — пять раз по 5 пятерок или 5^3 и т. д. По этой системе любое число N представляется так:

$$N = a_0 + a_1 5 + a_2 5^2 + a_3 5^3 + \ldots + a_n 5^n,$$

где каждое из чисел a_0, a_1, a_2, a_3, ... означает либо какое-нибудь натуральное число, меньшее 5, либо 0. Если за основание системы принято число, большее 10, например, 12, то для обозначения чисел по двенадцатиричной системе нужно присоединить к 10 существующим цифрам 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 еще две новые цифры для обозначения чисел 10 и 11.

105. Теперь покажем, как число N, написанное по пятеричной системе счисления, написать по десятичной. Пусть число N состоит из a_0 единиц первого разряда, из a_1 единиц второго разряда, ..., из a_n единиц $n+1$ разряда. Тогда число N представится так:

$$N = a_n 5^n + a_{n-1} 5^{n-1} + a_{n-2} 5^{n-2} + \ldots + a_2 5^2 + a_1 5 + a_0. \quad (1)$$

Вычислив правую часть этого равенства, мы получим число, написанное по десятичной системе счисления.

Для нахождения искомого числа удобно пользоваться следующей таблицей:

	a_n	a_{n-1}	a_{n-2}	. . .	a_1	a_0
5	a_n	$5a_n + a_{n-1} = b_1$	$5b_1 + a_{n-2} = b_2$	. . .	$5b_{n-2} + a_1 = b_{n-1}$	$5b_{n-1} + a_0 = b_n$

Таблица строится так: в верхней строке выписываем числа a_n, a_{n-1}, a_{n-2}, a_{n-3}, ..., a_1, a_0, не исключая и тех, которые равны нулю. В первой клетке второй строки пишем число a_n, а слева от него число 5; 5 умножаем на a_n и к полученному произведению $5a_n$ прибавляем a_{n-1}. Полученную сумму $5a_n + a_{n-1}$ обозначаем через b_1; 5 умножаем на b_1 и к полученному произведению $5b_1$ прибавляем a_{n-2}. Полученную сумму $5b_1 + a_{n-2}$ обозначаем через b_2; 5 умножаем на b_2 и к полученному произведению $5b_2$ прибавляем a_{n-3} и т. д. Последняя сумма b_n и будет выражать число, написанное по десятичной системе счисления. Пусть, например, требуется число 42113, написанное по пятеричной системе, написать по десятичной системе.

Вычисления располагаем так:

	4	2	1	1	3
5	4	22	111	556	2783

Обозначая основание системы счисления знаком внизу, будем иметь:

$$42113_5 = 2783_{10}.$$

106. Теперь решим обратную задачу: число 7863, написанное по десятичной системе счисления, написать по пятеричной системе счисления.

Рассуждаем: так как при основании 5 каждая единица 2-го разряда содержит пять единиц 1-го разряда, то, чтобы узнать, сколько в данном числе 7863 единиц 2-го разряда, то-есть пятерок, делим 6863 на 5; получаем в частном 1572, а в остатке 3. Мы узнали, что наше число 7863 содержит в себе 1572 единицы 2-го разряда и 3 единицы 1-го разряда. Далее, так как при основании 5 каждая единица 3-го разряда содержит 5 единиц 2-го разряда, то, чтобы узнать, сколько в 1572 единицах 2-го разряда содержится единиц 3-го разряда, делим 1572 на 5; получаем в частном 314 единиц 3-го разряда и 2 единицы 2-го разряда. Рассуждая и далее так, мы придем к заключению, что наше число состоит из 2 единиц 6-го разряда, 2 единиц 5-го разряда, 2 единиц 4-го разряда, 4 единиц 3-го разряда, 2 единиц 2-го разряда и 3 единиц 1-го разряда.

Для сохранения места и времени последовательные деления располагают письменно так:

$$\begin{array}{r|l}
7863 & 5 \\
\hline
3 & 1572 \\
\hline
 & 2 \\
\end{array}
\qquad
\begin{array}{r|l}
1572 & 5 \\
\hline
314 & 5 \\
\hline
4 & 62 \\
\hline
 & 2 \\
\end{array}
\qquad
\begin{array}{r|l}
62 & 5 \\
\hline
12 & 5 \\
\hline
 & 2 \\
\end{array}$$

Обозначая основание системы значком внизу, будем иметь:

$$7863_{10} = 222423_5.$$

107. Покажем теперь, как число $5\alpha\,2\beta\,8$, написанное по двенадцатиричной системе счисления, написать по десятичной системе (α означает 10, β означает 11).

Рассуждаем так: всякое число, написанное по двенадцатиричной системе, может быть представлено суммой следующего вида:

$$a_0 + a_1 12 + a_2 12^2 + a_3 12^3 + \ldots + a_n 12^n.$$

В данном случае имеем:

$$5 \cdot 12^4 + 10 \cdot 12^3 + 2 \cdot 12^2 + 11 \cdot 12 + 8 = 121318.$$

Результат можно было получить по схеме:

	5	10	2	11	8
12	5	70	842	10115	121388

Таким образом, $5\alpha\,2\beta\,8_{12} = 121388_{10}$.

Поверка.

121388	12			
8	10115	12		
$11=\beta$	842	12		
2	70	12		
$10=\alpha$	5			

Обозначая 10 через α, а 11—через β, получим:

$$121388_{10}=5\alpha\ 2\beta\ 8_{12}.$$

108. Мы сказали, что можно построить систему счислен при каком угодно основании, не равном единице. Значит, на меньшее число, которое может служить основанием, равно Следовательно, цифры двоичной системы будут 0 и 1. Поэто в двоичной системе число N представляется в виде суммы ст пеней числа 2:

$$N=a_0+a_1 2+a_2 2^2+a_3 2^3+a_4 2^4+\ldots+a_n 2^n.$$

Вычислив правую часть этого равенства, мы получим числ написанное по десятичной системе счисления. Так, наприме

$$111_2=(2^2+2+1)_{10}=7_{10}$$
$$1110100_2=(2^6+2^5+2^4+0+2^2+0+0)_{10}=116_{10}.$$

На изображении чисел посредством степеней числа 2 осн вано множество фокусов. (Проф. Г. Шуберт. Математическ развлечения и игры. Изд. 2-е, Одесса, стр. 49).

109. Примем число g за основание системы счисления. Тогд любое число N может быть представлено суммой следующег вида:

$$N=a_n g^n+a_{n-1} g^{n-1}+a_{n-2}g^{n-2}+\ldots+a_4 g^4+a_3 g^3+a_2 g^2+a_1 g+a$$

Имеем:

$$N-a_0=(a_n g^{n-1}+a_{n-1} g^{n-2}+a_{n-2} g^{n-3}+\ldots+a_3 g^2+a_2 g+a_1)g,$$
$$N-(a_1 g+a_0)=(a_n g^{n-2}+a_{n-1} g^{n-3}+\ldots+a_4 g^2+a_3 g+a_2)g^2,$$
$$N-(a_2 g^2+a_1 g+a_0)=(a_n g^{n-3}+a_{n-1} g^{n-4}+\ldots+a_4 g+a_3)g^3.$$

Переходя от равенств к сравнениям, получим:

$$N\equiv a_0 \pmod g \qquad (1)$$
$$N\equiv a_1 g+a_0 \pmod{g^2} \qquad (2)$$
$$N\equiv a^2 g^2+a_1 g+a_0 \pmod{g^3}. \qquad (3)$$

Из сравнения (1) следует, что делимость числа N на g з висит от делимости a_0 на g. Если a_0 делится на g, то N разд лится на g и на делителей g (п. 14).

Если a_0 не делится на g, но делится на какого-нибудь дел теля g, то и N разделится на этого делителя g. Пусть $g=1$ Тогда мы получаем такие правила:

1) На 10 делится то число, которое оканчивается нулем.

2) На 2 делится то число, которое оканчивается четной цифрой или нулем.

3) На 5 делится то число, которое оканчивается нулем или пятью.

Полагаем $g = 12$. N будет делиться на 12 и на делителей 12 (6, 4, 3, 2), если a_0 есть нуль.

Если a_0 не нуль, то N не разделится на 12. Если a_0 не нуль, то делимость N на какое-нибудь из чисел 2, 3, 4, 6, скажем, на 6, зависит от делимости a_0 на 6.

Рассмотрим сравнение (2). Из этого сравнения следует, что делимость N на g^2 зависит от делимости $a_1 g + a_0$ на g^2. Если $a_0 g + a_0$ делится на g^2, то N разделится на g^2 и на делителей g^2. Если $a_1 g + a_0$ не делится на g^2, но делится на какого-нибудь делителя g^2, то и N разделится на этого делителя g. При $g = 10$ сравнение (2) примет вид:

$$N \equiv 10\ a_1 + a_0 \pmod{10^2}.$$

Получаем такие правила:

4) На 100 делится то число, которое оканчивается двумя нулями.

5) На 4 (25) делится то число, которое оканчивается двумя нулями или у которого последние две цифры составляют число, кратное 4 (25).

При $g = 12$ N будет делиться как на 144, так и на делителей 144 (72, 48, 36, 24, 18, . . .), написанных по десятичной системе, если a_1 и a_0 суть нули. Если $a_1 g + a_0$ не делится на 144, а делится на какого-нибудь делителя 144, напр., на 48, то и N разделится на этого делителя. Таким образом, делимость N на какого-нибудь делителя 144, скажем, на 36, зависит от делимости $a_1 g + a_0$ на 36. В частности, делимость N на какое-нибудь из чисел 2, 3, 4, 6, напр., на 6, зависит исключительно от делимости a_0 на 6.

Рассмотрим теперь сравнение (3). Из этого сравнения следует, что делимость N на g^3 зависит от делимости $a_2 g^2 + a_1 g + a_0$ на g^3. Если $a_2 g^2 + a_1 g + a_0$ делится на g^3, то и N разделится на g^3 и на его делителей. Если $a_2 g^2 + a_1 g + a_0$ не делится на g^3, но делится на какого-нибудь его делителя, то и N разделится на этого делителя. При $g = 10$ сравнение (3) примет вид:

$$N \equiv 100\, a_2 + 10 a_1 + a_0 \pmod{10^3}.$$

Получаем такое правило:

6) На 8 (125) делится то число, которое оканчивается тремя нулями или у которого последние три цифры составляют число, кратное 8 (125).

110. Делимость на число $g - 1$. Если принять g за основание системы счисления, то число N можем представить так:

$$N = a_0 + a_1 g + a_2 g^2 + a_3 g^3 + \ldots + a_n g^n.$$

Имеем ряд очевидных сравнений:

$$\left.\begin{array}{l} 1 \equiv 1 \\ g \equiv 1 \\ g^2 \equiv 1 \\ g^3 \equiv 1 \\ \cdot\ \cdot\ \cdot\ \cdot \\ g^n \equiv 1 \end{array}\right\} \pmod{g-1}$$

Умножив первое сравнение на a_0, второе — на a_1, и т. д., получим такие сравнения:

$$\left.\begin{array}{l} a_0 \equiv a_0 \\ a_1 g \equiv a_1 \\ a_2 g^2 \equiv a_2 \\ a_3 g^3 \equiv a_3 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_n g^n \equiv a_n \end{array}\right\} \pmod{g-1}$$

Сложив эти сравнения почленно и зная, что

$$a_0 + a_1 g + a_2 g^2 + + a_3 g^3 + \ldots + a_n g^n = N,$$

получим:

$$N \equiv a_0 + a_1 + a_2 + \ldots + a_n \pmod{g-1}.$$

Из этого сравнения вытекает такое правило:

Правило. *На $g-1$ делится то число, у которого сумма цифр делится на $g-1$.*

При $g = 10$ получаем признак делимости на 9 и на 3 (пп. 23 и 24), а при $g = 12$ получаем признак делимости на 11.

111. Делимость на $g+1$. Если принять g за основание системы счисления, то число N можем представить так:

$$N = a_0 + a_1 g + a_2 g^2 + a_3 g^3 + \ldots + a_n g^n. \qquad (1)$$

Имеем ряд очевидных сравнений

$$\left.\begin{array}{l} 1 \equiv 1 \\ g \equiv -1 \\ g^2 \equiv 1 \\ g^3 \equiv -1 \\ \cdot\ \cdot\ \cdot\ \cdot \\ g^n \equiv (-1)^n \end{array}\right\} \pmod{g+1}$$

Первое сравнение умножаем на a_0, второе — на a_1, третье — на a_2 и т. д., получаем такие сравнения:

$$\left.\begin{array}{l} a_0 \equiv a_0 \\ a_1 g \equiv -a_1 \\ a_2 g^2 \equiv a^2 \\ a_3 g^3 \equiv -a_3 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_n g^n \equiv (-1)^n a_n \end{array}\right\} \pmod{g+1}$$

Сложив эти сравнения почленно и приняв во внимание равенство (1), находим:

$$N \equiv (a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots) \pmod{g+1}.$$

Из этого сравнения следует, что делимость числа N на $g+1$ зависит от делимости разности $(a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots)$ на $g+1$. Можно поэтому высказать следующее правило:

Правило. *Число N делится на $g+1$ тогда и только тогда, когда разность между суммою его цифр, стоящих на четных местах, и суммой его цифр, стоящих на нечетных местах, делится на $g+1$.*

При $g = 10$ получаем признак делимости на 11 (п. 27), а при $g = 12$ — признак делимости на 13.

112. Признак делимости на 7. Приняв 10 за основание системы счисления, число N представим так:

$$N = a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \ldots + a_n 10^n. \qquad (1)$$

Имеем очевидные сравнения по модулю 7:

$10^0 \equiv 1$	$10^6 \equiv 1$	$10^{12} \equiv 1$	$10^{18} \equiv 1$
$10^1 \equiv 3$	$10^7 \equiv 3$	$10^{13} \equiv 3$	$10^{19} \equiv 3$
$10^2 \equiv 2$	$10^8 \equiv 2$	$10^{14} \equiv 2$	$10^{20} \equiv 2$
$10^3 \equiv 6$	$10^9 \equiv 6$	$10^{15} \equiv 6$	$10^{21} \equiv 6$
$10^4 \equiv 4$	$10^{10} \equiv 4$	$10^{16} \equiv 4$	$10^{22} \equiv 4$
$10^5 \equiv 5$	$10^{11} \equiv 5$	$10^{17} \equiv 5$	$10^{23} \equiv 5$

. . . . . .

и т. д.

Первое сравнение умножаем на a_0, второе — на a_1, третье — на a_2 и т. д.; получаем такие сравнения по модулю 7:

$a_0 \equiv a_0$	$a_6 10^6 \equiv a_6$	$a_{12} 10^{12} \equiv a_{12}$	$a_{18} 10^{18} \equiv a_{18}$
$a_1 10 \equiv 3a_1$	$a_7 10^7 \equiv 3a_7$	$a_{13} 10^{13} \equiv 3a_{13}$	$a_{19} 10^{19} \equiv 3a_{19}$
$a_2 10^2 \equiv 2a_2$	$a_8 10^8 \equiv 2a_8$	$a_{14} 10^{14} \equiv 2a_{14}$	$a_{20} 10^{20} \equiv 2a_{20}$
$a_3 10^3 \equiv 6a_3$	$a_9 10^9 \equiv 6a_9$	$a_{15} 10^{15} \equiv 6a_{15}$	$a_{21} 10^{21} \equiv 6a_{21}$
$a_4 10^4 \equiv 4a_4$	$a_{10} 10^{10} \equiv 4a_{10}$	$a_{16} 10^{16} \equiv 4a_{16}$	$a_{22} 10^{22} \equiv 4a_{22}$
$a_5 10^5 \equiv 5a_5$	$a_{11} 10^{11} \equiv 5a_{11}$	$a_{17} 10^{17} \equiv 5a_{17}$	$a_{23} 10^{23} \equiv 5a_{23}$

. . . . . .

и т. д.

Сложив эти сравнения почленно и приняв во внимание равенство (1), получим:

$$N \equiv (a_0 + a_6 + a_{12} + \ldots) + 2(a_2 + a_8 + a_{14} + \ldots) + 3(a_1 + a_7 + a_{13} + \ldots) + 4(a_4 + a_{10} + a_{16} + \ldots) + 5(a_5 + a_{11} + a_{17} + \ldots) + 6(a_3 + a_9 + a_{15} + \ldots) \pmod 7.$$

Из этого сравнения следует:

Делимость данного числа N на 7 зависит от делимости суммы

$$(a_0+a_6+a_{12}+\ldots)+2(a_2+a_8+a_{14}+\ldots)+$$
$$+3(a_1+a_7+a_{13}+\ldots)+4(a_4+a_{10}+a_{16}+\ldots)+$$
$$+5(a_5+a_{11}+a_{17}+\ldots)+6(a_3+a_9+a_{15}+\ldots)$$

на 7.

ГЛАВА ВОСЬМАЯ

Распределение чисел на классы по данному модулю. Теоремы Ферма и Эйлера

113. Возьмем натуральное число k, большее единицы. Существует бесчисленное множество целых чисел, дающих при делении на k один и тот же остаток r, где r есть одно и только одно из чисел ряда 0, 1, 2, 3, . . ., $k-1$.

Назовем совокупность всех чисел, дающих при делении на k один и тот же остаток r, классом чисел по модулю k. Термин „класс" введен Гауссом. Известно, что все числа, дающие при делении на k один и тот же остаток r, называются равноостаточными относительно k, а равноостаточные числа относительно k сравнимы между собою по модулю k (п. 89). Поэтому можно дать и такое определение класса: *совокупность всех чисел, сравнимых между собою по данному модулю k, называется классом.*

114. Различных классов чисел по модулю k может быть только k. И, в самом деле, от деления целых чисел на k могут получиться только такие остатки:

$$0,\ 1,\ 2,\ 3,\ 4,\ \ldots,\ k-1. \qquad (1)$$

Среди чисел этого ряда нет двух чисел, сравнимых между собою по модулю k. Действительно, возьмем из ряда (1) два каких угодно числа α и β (α больше β). Разность этих чисел $\alpha-\beta$ никогда не разделится на k и вот почему: каждое из чисел α и β меньше k, а разность их $\alpha-\beta$ подавно меньше k. Отсюда следует, что все k чисел ряда (1) принадлежат к различным классам чисел по модулю k.

115. Общий вид всех чисел, дающих при делении на k один и тот же остаток r, будет $kq+r$ (1), где r есть одно и только одно из чисел ряда 0, 1, 2, 3, 4, . . ., $k-1$, а q принимает значения 0, ±1, ±2, ±3, ±4, . . . При $r=0$ выражение (1) принимает вид kq.

Таким образом, kq есть общее выражение всех чисел, кратных k. Числа, кратные k, находятся в ряду

$$\ldots,\ -5k,\ -4k,\ -3k,\ -2k,\ -k,\ 0,\ k,\ 2k,\ 3k,\ 4k,\ 5k,\ \ldots$$

Мы видим, что любые два числа этого ряда сравнимы между собою по модулю k. Полагая, например, $k=7$, мы получим ряд чисел, кратных 7:

$$\ldots, -35, -28, -21, -14, -7, 0, 7, 14, 21, 28, 35, \ldots$$

При $r=1$ выражение (1) принимает вид $kq+1$.

Мы получили формулу класса чисел, дающих при делении на k один и тот же остаток 1. Все числа этого класса находятся в ряду

$$\ldots, -3k+1, -2k+1, -k+1, 1, k+1, 2k+1, 3k+1, \ldots$$

Мы видим, что любые два числа этого ряда сравнимы между собою по модулю k. Полагая $k=7$, мы получим:

$$\ldots, -34, -27, -20, -13, -6, 1, 8, 15, 22, 29, \ldots$$

Любые два числа этого ряда сравнимы между собою по модулю 7. При $r=2$ формула (1) принимает вид $kq+2$.

Мы получили формулу класса чисел, дающих при делении на k один и тот же остаток 2. Все числа этого же класса находятся в ряду

$$\ldots, -3k+2, -2k+2, -k+2, 2, k+2, 2k+2, 3k+2, \ldots$$

Мы видим, что любые два числа этого ряда сравнимы между собою по модулю k. Полагая $k=7$, мы получим:

$$\ldots, -26, -10, -12, -5, 2, 9, 16, 23, 30, \ldots$$

Любые два числа этого ряда сравнимы между собою по модулю 7. Полагая в формуле (1) последовательно $r=3, 4, 5, \ldots, k-1$, мы получим формулы классов чисел, дающих при делении на k соответственно одни и те же остатки $3, 4, 5, \ldots, k-1$:

$$kq+3,\ kq+4,\ kq+5,\ \ldots,\ kq+k-1.$$

116. Назовем 0 представителем класса чисел, кратных k; 1 назовем представителем класса чисел, дающих при делении на k один и тот же остаток 1; 2—представителем класса чисел, дающих при делении на k один и тот же остаток 2, и т. д.; $k-1$ назовем представителем класса чисел, дающих при делении на k один и тот же остаток $k-1$. Возьмем представителей из этих классов и расположим их в возрастающий ряд:

$$0, 1, 2, 3, 4, 5, \ldots, k-1. \qquad (1)$$

Эти представители классов называются остатками или вычетами по модулю k. Систему целых чисел мы назовем полной системой вычетов по модулю k, если она содержит точно по одному представителю от каждого класса по модулю k.

Числа

$$1, 2, 3, 4, 5, \ldots, k \qquad (15)$$

также образуют полную систему вычетов по модулю k. В этом случае k является представителем класса чисел, кратных k. Вообще, всякие k последовательных чисел образуют полную

систему вычетов по модулю k. Так, например, полной системой вычетов по модулю 12 может служить любой из рядов

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11;
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12;
12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23.

Полезно знать и такое определение полной системы вычетов: полной системой вычетов по модулю k называется любая система k чисел, любые два числа которой не сравнимы между собою по модулю k.

Все числа, принадлежащие к одному классу, имеют много общих свойств, так что по отношению к модулю их можно рассматривать как одно число.

117. Теорема. *Если представитель класса r и модуль сравнения k имеют общего наибольшего делителя d, то d будет также общим наибольшим делителем модуля k и любого числа s этого класса.*

Доказательство. Имеем

$$s \equiv r \pmod{k}.$$

Так как член сравнения r и модуль сравнения k делятся на d, то на d разделится и другой член сравнения s (п. 100). Значит, d есть общий делитель k и s. В то же время d есть и общий наибольший делитель чисел k и s. В самом деле, если бы k и s делились на какое-нибудь число d_1, большее d, то на d_1 должен был бы делиться и член сравнения r, а это невозможно. Итак, d есть общий наибольший делитель k и s: $d = (k, s)$. Таким образом, теорема доказана полностью.

Следствие. *Если представитель класса взаимно прост с модулем сравнения k, то и любое число s этого класса есть число взаимно простое с модулем k.*

Доказательство. Имеем:

$$s \equiv r \pmod{k}.$$

Если бы член сравнения s и модуль сравнения k делились на какое-нибудь число d, отличное от единицы, то на d должен был бы делиться и член сравнения r, а это невозможно: k и r взаимно простые числа. Итак, теорема доказана.

118. Если из полной системы вычетов по модулю k выпишем все числа, взаимно простые с модулем k, и из полученных чисел составим новый ряд, то полученный ряд будет состоять исключительно из одних чисел, взаимно простых с модулем k. *Такая система целых чисел, состоящая исключительно из представителей всех классов, взаимно простых с модулем k, называется приведенной системой вычетов по модулю k.* Так как среди чисел полной системы вычетов по модулю k есть $\varphi(k)$ чисел, меньших k и взаимно простых с ним, то приведенная система вычетов по модулю k содержит $\varphi(k)$ чисел. *Итак, приведенная система вычетов по модулю k состоит из $\varphi(k)$ чисел.*

Так, например, приведенной системой вычетов по модулю 12 служит ряд 1, 5, 7, 11, а в этом ряду 4 числа и $\varphi(12)=4$.

119. Теорема. *Если подставим в линейное выражение* $ax-b$ *вместо* x *последовательно все* k *чисел полной системы вычетов*

$$0,\ 1,\ 2,\ 3,\ \ldots,\ k-1, \qquad (1)$$

то при a *и* k *взаимно простых мы опять получим полную систему вычетов по модулю* k.

Доказательство. Предположим обратное: пусть два каких-нибудь числа α и β ряда (1) обладают таким свойством, что, будучи подставлены в выражение $ax-b$, дают числа одного и того же класса $a\alpha-b$ и $a\beta-b$, а числа одного и того же класса, как известно, всегда сравнимы между собою по данному модулю k; в таком случае разность $a\alpha-b-(a\beta-b)=(\alpha-\beta)a$ должна делиться на k. Но произведение $(\alpha-\beta)a$ никогда не разделится на k и вот почему: a и k взаимно простые числа, а $\alpha-\beta$ меньше k. Таким образом, теорема доказана.

Между числами ряда (1) находится одно и только одно число, при котором выражение $ax-b$ разделится на k.

Когда в выражение $ax-b$ *вместо неопределенного символа* x *подставляют одно за другим числа полной системы вычетов, то говорят, что* x *пробегает полную систему вычетов.*

Пример. Возьмем выражение $5x+3$. Полной системой вычетов по модулю 12 служит ряд

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11.$$

Коэффициент 5 и модуль 12—числа взаимно простые. Пусть x пробегает полную систему вычетов по модулю 12. Получим такой ряд чисел:

$$3,\ 8,\ 13,\ 18,\ 23,\ 28,\ 33,\ 38,\ 43,\ 48,\ 53,\ 58.$$

Легко заметить, что среди чисел этого ряда нет двух чисел, сравнимых между собою по модулю 12. Мы видим, что в этом ряду есть одно только число 48, делящееся на 12 (сравнимое с 0 по модулю 12).

120. *Когда при делении целого положительного числа* a *на целое положительное число* k *получают частное* q *и неотрицательный остаток* r, *то говорят, что остаток* r *есть наименьший положительный вычет числа* a *по модулю* k.

По свойству деления должно быть:

$$a=kq+r. \qquad (1)$$

Наименьшими положительными вычетами чисел по модулю k могут быть только следующие числа: $0,\ 1,\ 2,\ \ldots,\ k-1$, ибо остаток (вычет) всегда меньше делителя (модуля).

Теперь покажем, как найти наименьший положительный вычет отрицательного числа $-a$ по модулю k. Равенство (1) влечет за собою следующие равенства:

$$-a=-kq-r=-kq-r+k-k=-(q+1)k+(k-r).$$

Разность $k-r$ называется наименьшим положительным вычетом отрицательного числа $-a$ по модулю k.

Итак, под наименьшим положительным вычетом отрицательного числа $-a$ будем понимать разность $k-r$.

Так, например, наименьший положительный вычет числа 27 по модулю 5 есть 2, наименьший положительный вычет числа 13 по модулю 5 есть 3, наименьший положительный вычет числа -1 по модулю 5 есть 4.

Равенство (1) можно представить в таком виде:

$$a = kq + r = kq + r + k - k = (q+1)k + r - k.$$

Отрицательное число $r-k$ называется наименьшим отрицательным вычетом положительного числа a по модулю k.

Все числа, наименьший положительный вычет которых по модулю 7 есть 2, определяются по формуле

$$7q + 2,$$

где $q = 0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots$ Эти числа представятся таким рядом

$$\ldots, -33, -26, -19, -12, -5, 2, 9, 16, 23, 30, 37, \ldots$$

121. Мы сказали, что целое положительное число a сравнимо со своим наименьшим положительным вычетом r по модулю k. В то же время a сравнимо и со своим отрицательным вычетом $r-k$ по модулю k. В самом деле, разность $a-(r-k) = a-r+k$ разделится на k. Это вытекает из того, что как $a-r$ делится на k, так и k делится на k, а делимость разности $a-(r-k)$ на k выражается сравнением.

$$a \equiv r-k \pmod{k}.$$

Наименьший отрицательный вычет числа a по модулю k может равняться нулю, если число a делится на модуль k. Наименьший отрицательный числа 7 по модулю 5 есть -3, наименьший отрицательный вычет числа 14 по модулю 5 есть -1, наименьший отрицательный вычет числа -23 по модулю 5 есть -3.

Все числа, наименьший отрицательный вычет которых по модулю 7 есть -4, определяются по формуле

$$7q-4,$$

где $q = 0, \pm 1, \pm 2, \pm 3, \pm 4 \ldots$ Эти числа можно расположить в ряд: $\ldots, -39, -32, -25, -18, -11, -4, 3, 10, 17, 24, 31, \ldots$

Мы видим, что любые два числа этого ряда сравнимы между собою по модулю 7.

Тот из двух вычетов a по модулю k, наименьшего положительного и наименьшего отрицательного, которого абсолютная величина меньше, называется абсолютным малым вычетом числа a по модулю k. Если абсолютные величины обоих вычетов равны, то мы будем говорить, что существует два абсолютно малых вычета: положительный и отрицательный.

Если a не делится на k, то равенство абсолютных величин вычетов может быть тогда, когда модуль k есть четное число.

Примеры. 1. Наименьший положительный вычет числа 23 по модулю 7 есть 2, а наименьший отрицательный вычет его есть $2-7=-5$. Следовательно, абсолютно малый вычет 23 по модулю 7 есть 2.

2. Наименьший положительный вычет 45 по модулю 8 есть 5, а наименьший отрицательный вычет его есть $5-8=-3$. Следовательно, абсолютный малый вычет 45 по модулю 8 есть -3.

3. Наименьший отрицательный вычет -38 по модулю 7 есть -3; наименьший положительный вычет этого числа будет $7-3=4$. Следовательно, абсолютно малый вычет -38 по модулю 7 есть -3.

4. Наименьший положительный вычет числа 44 по модулю 8 есть 4, а наименьший отрицательный вычет его есть -4. Так как оба вычета по абсолютной величине равны, то получатся два абсолютно малых вычета: $+4$ и -4.

122. Теорема Ферма. Если a не делится на простое число p, то имеет место сравнение

$$a^{p-1}\equiv 1 \pmod p.$$

Доказательство. Возьмем возрастающий ряд натуральных чисел от 1 до $p-1$ включительно:

$$1,\ 2,\ 3,\ 4,\ \ldots,\ m,\ \ldots,\ n,\ \ldots,\ p-1. \qquad (1)$$

В этом ряду находятся числа, меньшие p и взаимно простые с ним. Умножив каждые из чисел ряда (1) на a, получим ряд:

$$1a,\ 2a,\ 3a,\ 4a,\ \ldots,\ ma,\ \ldots,\ na,\ \ldots,\ (p-1)a. \qquad (2)$$

Ни одно из чисел этого ряда не делится на p (п. 48, сл. 2). Пусть остатки от деления чисел ряда (2) на p будут соответственно:

$$r_1,\ r_2,\ r_3,\ r_4,\ \ldots,\ r_m,\ \ldots,\ r_n,\ \ldots,\ r_{p-1}. \qquad (3)$$

Всех остатков будет $p-1$.

Докажем, что все эти остатки различны между собою. В самом деле, если бы мы допустили, что между этими остатками существуют два равных остатка, например, $r_m=r_n$, то разность $na-ma=(n-m)a$ должна была бы делиться на p, а это невозможно, так как a и $n-m$ суть числа простые относительно p. Так как остатки (3) все различны и каждый из них меньше p, то они представляют собою числа натурального ряда 1, 2, 3, 4, 5, $\ldots$, $p-1$, взятые, быть может, только в другом порядке. В таком случае должно существовать равенство

$$r_1r_2r_3\ldots r_{p-1}=1\cdot 2\cdot 3\cdot 4\ldots(p-1). \qquad (1)$$

Зная, что всякое число сравнимо со своим остатком, если за модуль принять делителя (п. 88), мы получаем следующий ряд сравнений по модулю p:

$$\left.\begin{aligned} 1a&\equiv r_1\\ 2a&\equiv r_2\\ 3a&\equiv r_3\\ &\ldots\\ (p-1)a&\equiv r_{p-1}\end{aligned}\right\}\pmod p$$

Перемножая почленно эти сравнения между собою, мы найдем:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \ldots (p-1)a^{p-1} \equiv r_1 r_2 r_3 \ldots r_{p-1} \pmod{p}.$$

Зная, что $r_1 r_2 r_3 \ldots r_{p-1} = 1 \cdot 2 \cdot 3 \ldots (p-1)$, мы предыдущее сравнение заменяем таким сравнением:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \ldots (p-1)a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1) \pmod{p}.$$

Члены этого сравнения могут быть сокращены на произведение $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \ldots (p-1)$ (п. 97). Выполнив это сокращение, найдем:

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

что и требовалось доказать.

Следствие. *Каково бы ни было a, но если p число простое, то имеет место сравнение*

$$a^p \equiv a \pmod{p}. \qquad (1)$$

Доказательство. Возьмем выражение $a^p - a = a(a^{p-1} - 1)$. Докажем, что это выражение при любом значении a разделится на простое число p. Рассмотрим два случая. Первый случай: a делится на p. Тогда и произведение $a(a^{p-1} - 1)$ разделится на p, а делимость этого произведения на p выражается сравнением

$$a(a^{p-1} - 1) \equiv 0 \pmod{p},$$

или, что одно и то же, сравнением

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

Таким образом, теорема для этого случая доказана.

Рассмотрим второй случай: a не делится на p. В таком случае разность $a^{p-1} - 1$ разделится на p; тогда на p разделится и произведение $a(a^{p-1} - 1)$, а делимость этого произведения на выражается сравнением (1). Таким образом, и для этого случая теорема доказана.

Проверить справедливость сравнений:

1) $2^{12} \equiv 1 \pmod{13}$
2) $2^4 \equiv 1 \pmod{5}$
3) $10^{16} \equiv 1 \pmod{17}$

Решение. Прежде всего вспомним, что произведение нескольких чисел и произведение их остатков равноостаточны относительно одного и того же делителя, а равноостаточные числа сравнимы между собою по данному модулю 17.

Находим:

$$10^{16} \equiv 100^8 \equiv 15^8 \equiv 225^4 \equiv 4^4 \equiv 4 \cdot 64 \equiv 4 \cdot 13 \equiv 1 \pmod{17}$$

4) $40^{30} \equiv 1 \pmod{31}$.

Решение. $40^{30} \equiv 9^{30} \equiv 81^{15} \equiv 19^{15} \equiv 19 \cdot 19^{14} \equiv 19 \cdot 361^7 \equiv$
$\equiv 19 \cdot 20^7 \equiv 19 \cdot 20 \cdot 400^3 \equiv 8 \cdot 28^3 \equiv 8 \cdot 28 \cdot 28^2 \equiv 224 \cdot 784 \equiv$
$\equiv 7 \cdot 9 \equiv 1 \pmod{31}$.

123. Теорема Эйлера. *Если a и b два каких угодно взаимно простых числа, то имеет место сравнение*

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

Доказательство. a и b — два каких угодно взаимно простых числа. Пусть будет $k = \varphi(b)$; пусть эти k чисел будут

$$c_1,\ c_2,\ c_3,\ \ldots,\ c_m,\ \ldots,\ c_n,\ \ldots,\ c_k. \qquad (1)$$

Умножив каждое из чисел ряда (1) на a, получим:

$$c_1a,\ c_2a,\ c_3a,\ \ldots,\ c_ma,\ \ldots,\ c_na,\ \ldots,\ c_ka. \qquad (2)$$

Обозначим остатки от деления чисел этого ряда на b соответственно через

$$r_1,\ r_2,\ r_3,\ \ldots,\ r_m,\ \ldots,\ r_n,\ \ldots,\ r_k. \qquad (3)$$

Докажем, что все эти остатки различны между собою. В самом деле, если бы мы допустили, что между этими остатками существует два равных остатка, например, $r_m = r_n$, то разность $ac_n - ac_m = (c_n - c_m)a$ должна была бы делиться на b, а это невозможно, так как a и b числа взаимно простые, а $c_n - c_m$ меньше b.

Так как остатки (3) все различны, меньше b и взаимно просты с b, то они представляют собою числа ряда (1), взятые, быть может, только в другом порядке. В таком случае должно существовать такое равенство:

$$c_1c_2c_3 \ldots c_m \ldots c_n \ldots c_k = r_1r_2r_3 \ldots r_m \ldots r_n \ldots r_k \qquad (4)$$

Так как всякое число сравнимо со своим остатком, если за модуль принять делителя (п. 88), то получим следующий ряд сравнений по модулю b:

$$\left.\begin{aligned} c_1a &\equiv r_1 \\ c_2a &\equiv r_2 \\ c_3a &\equiv r_3 \\ &\ldots\ldots \\ c_ka &\equiv r_k \end{aligned}\right\} \pmod{b}$$

Перемножая почленно эти сравнения между собою, мы найдем:

$$c_1c_2c_3 \ldots c_k a^k \equiv r_1r_2r_3 \ldots r_k \pmod{b}.$$

Зная, что $c_1c_2c_3 \ldots c_k = r_1r_2r_3 \ldots r_k$, мы предыдущее сравнение заменяем таким сравнением:

$$c_1c_2c_3 \ldots c_k a^k \equiv c_1c_2c_3 \ldots c_k \pmod{b}.$$

Члены этого сравнения могут быть сокращены на произведение $c_1c_2c_3 \ldots c_k$ (п. 97). Выполнив это сокращение, найдем

$$a^k \equiv 1 \pmod{b}. \qquad (5)$$

Но так как $k = \varphi(b)$, то предыдущее сравнение может быть представлено в таком виде:

$$a^{\varphi(b)} \equiv 1 \pmod{b}. \qquad (6)$$

Таким образом, теорема доказана полностью.

Это важное сравнение принято называть обобщенной теоремой Ферма, так как при b, равном простому числу p, получим из теоремы Эйлера, как следствие, теорему Ферма:

$$a^{p-1} \equiv 1 \pmod{p}. \qquad (7)$$

Примеры. 1) $10^{\varphi(9)} \equiv 1 \pmod 9$

Решение. $\varphi(9) = \varphi(3^2) = 3(3-1) = 6$, а $10^6 \equiv 1 \pmod 9$.

2) $15^{\varphi(8)} \equiv 1 \pmod 8$.

Решение. $\varphi(8) = 8\left(1 - \frac{1}{2}\right) = 4$; $15^4 \equiv 7^4 \equiv 49^2 \equiv 1 \pmod 8$.

3) $14^{\varphi(15)} \equiv 1 \pmod{15}$.

Решение. $\varphi(15) = \varphi(5)\,\varphi(3) = 8$.

$14^8 \equiv 196^4 \equiv 1 \pmod{15}$.

ГЛАВА ДЕВЯТАЯ

Сравнение первой степени

124. Сравнение с одним неизвестным x по выполнении надлежащих преобразований (раскрытие скобок, перенесение неизвестных членов в левую часть сравнения, а известных членов — в правую часть и приведение подобных членов в каждой части) может быть приведено к виду

$$ax \equiv b \pmod{k}. \qquad (1)$$

Заметим, что коэффициент a мы всегда можем сделать положительным, переменив в случае надобности перед членами сравнения знаки на противоположные. *Числа, которые, будучи подставлены в сравнение (1) вместо неизвестного x, удовлетворяют этому сравнению, называются корнями сравнения. Решить сравнение (1) значит найти его корни. Два сравнения, которым удовлетворяют одни и те же числа, называются равносильными, эквивалентными. Если α есть корень сравнения (1), то и все числа, сравнимые с α по подулю k, будут корнями этого сравнения* (п. 103). Эти корни считаются, как один корень сравнения (1). Напротив, два или несколько чисел, удовлетворяющих сравнению (1), но не сравнимых между собою по модулю k, считаются за различные корни сравнения (1). При решении сравнений вида (1) могут представиться два случая:

1) *Коэффициент a и модуль k числа взаимно простые:*

$$(a, k) = 1.$$

2) *Коэффициент a и модуль k имеют общего наибольшего делителя d:* $(a, k) = d$.

Рассмотрим оба случая.

125. *Первый случай: коэффициент a и модуль k числа взаимно простые:* $(a, k) = 1$.

Докажем, что *сравнение* $ax \equiv b \pmod{k}$ (1) *в этом случае всегда возможно и имеет одно и только одно решение.*

В самом деле, подставляя в линейное выражение $ax - b$ вместо x последовательно числа полной системы вычетов по модулю k

$$0, 1, 2, 3, 4, \ldots, k-1, \qquad (2)$$

мы получим систему чисел, не сравнимых между собою по модулю k (п. 119). Отсюда следует, что между числами (2) находится одно и только одно число, при котором выражение $ax-b$ разделится на k, выражение $ax - b$ окажется сравнимым с 0 по модулю k. Значит, найденное число удовлетворяет сравнению (1). Это-то число и называется корнем сравнения (1). Обозначим этот корень сравнения через α. Число α находится попытками — путем подстановок в сравнение (1) чисел ряда (2). Такой метод решения сравнений называется *методом проб*. Формула

$$x \equiv \alpha \pmod{k}$$

означает, что α есть корень сравнения (1). Таким обозначением мы как бы подчеркиваем, что нами рассматривается весь класс чисел, как одно целое, а не его отдельные числа, соответствующие тому или другому значению x.

Все числа, удовлетворяющие сравнению (1), получим по формуле

$$kq + \alpha,$$

давая q значения $0, \pm 1, \pm 2, \pm 3, \ldots$. Эти числа находятся в ряду

$$\ldots, -3k + \alpha, -2k + \alpha, -k + \alpha, \alpha, \alpha + k, \alpha + 2k, \alpha + 3k, \ldots$$

Но это бесконечное множество чисел, удовлетворяющих сравнению (1), принадлежит к одному классу с числом α по модулю k, а потому оно считается за одно решение сравнения (1).

Пример. $5x \equiv 3 \pmod{9}$. (1)

Решение. Коэффициент 5 и модуль 9 — числа взаимно простые. Приведенная система вычетов по модулю 9 представится рядом

$$0, 1, 2, 3, 4, 5, 6, 7, 8.$$

Подставляем в наше сравнение вместо x числа приведенной системы вычетов. При $x = 6$ сравнение удовлетворяется:

$$5 \cdot 6 \equiv 3 \pmod{9}.$$

Следовательно, решение сравнения (1) представляется так:

$$x \equiv 6 \pmod{9}.$$

Все числа, удовлетворяющие сравнению (1), получим по формуле

$$9q + 6,$$

давая q значение $0 \pm 1, \pm 2, \pm 3, \ldots$

Числа

$$\ldots, -21, -12, -3, 6, 15, 24, 33, \ldots$$

хотя и удовлетворяют нашему сравнению (1), но так как они принадлежат к одному классу чисел с числом 6 по модулю 9, то считаются за одно решение нашего сравнения.

126. Укажем второй способ решения сравнения

$$ax \equiv b \pmod{k}. \qquad (1)$$

Коэффициент a и модуль k числа взаимно простые.

Второй способ решения (1) основан на применении теоремы Эйлера.

Имеем

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

Умножая обе части этого сравнения на b, получаем:

$$ba^{\varphi(k)} \equiv b \pmod{k}.$$

Числа ax и $ba^{\varphi(k)}$, сравнимые с третьим числом b по модулю k, сравнимы между собою по тому же модулю k (п. 90); имеем:

$$ax \equiv ba^{\varphi(k)} \pmod{p}.$$

Сокращая обе части этого сравнения на a, окончательно получаем:

$$x \equiv ba^{\varphi(k)-1} \pmod{k}. \qquad (2)$$

Если k есть простое число p, то формула (2) примет вид:

$$x \equiv ba^{p-2} \pmod{p}.$$

Примеры. 1) $5x \equiv 3 \pmod{9}$.

Решение.

$$\varphi(9) = \varphi(3^2) = 3(2-1) = 6; \quad \varphi(9) - 1 = 5.$$

Получаем:

$$x \equiv 3 \cdot 5^5 \equiv 3 \cdot 5 \cdot 25^2 \equiv 6 \cdot 7^2 \equiv 6 \cdot 4 \equiv 6 \pmod{9}.$$

Действительно, при $x = 6$ наше сравнение удовлетворяется

2) $7x \equiv -2 \pmod{10}$.

Решение. Имеем:

$$\varphi(10) = \varphi(2)\varphi(5) = 4.$$

$$x \equiv (-2) \cdot 7^3 \equiv (-14) \cdot 7^2 \equiv (-4) \cdot 9 \equiv -6 \pmod{10}.$$

Заменяя здесь -6 его наименьшим положительным вычетом по модулю 10, находим:

$$x \equiv 4 \pmod{10}.$$

3) $8x \equiv 5 \pmod{11}$.

Решение. Имеем:

$$x \equiv 5 \cdot 8^9 \equiv 40 \cdot 64^4 \equiv 7 \cdot 9^4 \equiv 7 \cdot 81^2 \equiv 7 \cdot 4^2 \equiv 7 \cdot 5 \equiv 2 \pmod{11}.$$

Действительно, при $x = 2$ наше сравнение выполняется.

4) Возьмем сравнение

$$ax \equiv b \pmod{k}. \qquad (1)$$

Пусть наименьшие положительные вычеты a и b по модулю k соответственно будут a_1 и b_1. Тогда

$$a = kq_1 + a_1,\ b = kq_2 + b_1.$$

Тогда наше сравнение примет вид:

$$kq_1x + a_1x \equiv kq_2 + b_1 \pmod{k}. \qquad (4)$$

Возьмем очевидное сравнение (оно возможно при всех значениях x)

$$kq_1x \equiv kq_2 \pmod{k}.$$

Вычитая это сравнение почленно из сравнения (4), получаем сравнение, эквивалентное данному сравнению (1):

$$a_1x \equiv b_1 \pmod{k}.$$

Таким образом, мы доказали, что числа a и b могут быть заменены их наименьшими положительными вычетами a_1 и b_1 по модулю k.

Применим сказанное к решению сравнений:

5) $15x \equiv 8 \pmod{13}$.

Решение. Получаем

$$2x \equiv 8 \pmod{13}.$$

Сократив обе части полученного сравнения на 2, имеем:

$$x \equiv 4 \pmod{13}.$$

Действительно, при $x = 4$ наше сравнение удовлетворяется.

6) $14x \equiv 53 \pmod{11}$.

Решение. Имеем:

$$3x \equiv 9 \pmod{11}.$$

Сокращая обе части сравнения на 3, получаем окончательно

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

Действительно, наше сравнение выполняется при $x = 3$.

7) $41x \equiv 68 \pmod{13}$.

Решение. Наименьшие положительные вычеты 41 и 68 по модулю 13 соответственно равны 2 и 3. Тогда данное сравнение заменится эквивалентным ему сравнением

$$2x \equiv 3 \pmod{13},$$

которое удовлетворяется при $x = 8$. Следовательно, решение данного сравнения представится так:

$$x \equiv 8 \pmod{13}.$$

Решим еще один пример:

8) $37x \equiv -61 \pmod{17}$.

Решение. Заменим 37 и -61 их наименьшими положительными вычетами 3 и 7 по модулю 17. Получаем:

$$3x \equiv 7 \pmod{17}.$$

Решив это сравнение, найдем:

$$x \equiv 8 \pmod{17}.$$

Действительно, данное сравнение удовлетворяется при $x = 8$.

127. *Решение сравнений с помощью непрерывных дробей.* Пусть дано сравнение

$$ax \equiv b \pmod{k}. \qquad (1)$$

Заметим, что a и k — числа взаимно простые.

Сущность этого способа заключается в том, что решение сравнения (1) сводится к нахождению какого-нибудь целого значения x из неопределенного уравнения

$$ax - ky = b. \qquad (2)$$

Действительно, сравнение (1) означает, что разность $ax - b$ делится на k. Обозначая частное от деления $ax - b$ на k через y, находим:

$$\frac{ax-b}{k} = y,$$

откуда для определения x и y получаем неопределенное уравнение первой степени с двумя неизвестными (2).

Теория непрерывных дробей дает нам возможность найти одну пару целых решений неопределенного уравнения (2). Зная одно значение x, мы тем самым найдем и решение сравнения (1). Покажем, как это делается. Возьмем дробь $\frac{k}{a}$, обратим ее в непрерывную дробь и найдем предпоследнюю подходящую дробь $\frac{P_{n-1}}{Q_{n-1}}$ (последняя подходящая дробь есть $\frac{k}{a}$); берем затем разность подходящих дробей:

$$\frac{P_{n-1}}{Q_{n-1}} - \frac{k}{a} = \frac{(-1)^{n-1}}{aQ_{n-1}}.$$

Освободив это равенство от знаменателей, получим:

$$P_{n-1}\, a - Q_{n-1}\, k = (-1)^{n-1},$$

$$P_{n-1}\, a - (-1)^{n-1} = Q_{n-1}\, k.$$

Переходя от равенства к сравнению, получим:

$$P_{n-1}\, a \equiv (-1)^{n-1} \pmod{k}. \qquad (3)$$

Здесь могут встретиться два случая; первый случай: $n-1$ число четное; второй случай: $n-1$ число нечетное. Рассмотрим оба случая. Первый случай: $n-1$ четное число.

Тогда получаем:

$$P_{n-1}\, a \equiv 1 \pmod{k}.$$

Умножив обе части этого сравнения на b, находим:

$$abP_{n-1} \equiv b \pmod{k}.$$

Сравнивая это сравнение с сравнением (1), получаем:

$$ax \equiv abP_{n-1} \pmod{k},$$

откуда

$$x \equiv bP_{n-1} \pmod{k}.$$

Рассмотрим второй случай: $n-1$ число нечетное. Тогда сравнение (3) примет вид:

$$P_{n-1}a \equiv -1 \pmod{k}.$$

Умножив обе части этого сравнения на $-b$, получаем:

$$-abP_{n-1} \equiv b \pmod{k}.$$

Сравнив это сравнение с сравнением (1), находим:

$$ax \equiv -abP_{n-1} \pmod{k},$$

откуда

$$x \equiv -bP_{n-1} \pmod{k}. \qquad (5)$$

Соединяя обе формулы решений в одну, получим:

$$x \equiv (-1)^{n-1} bP_{n-1} \pmod{k}.$$

Таким образом, чтобы найти решение сравнения

$$ax \equiv b \pmod{k}$$

с помощью непрерывных дробей, нужно определить числителя предпоследней подходящей непрерывной дроби от обращения дроби $\frac{k}{a}$ в непрерывную дробь, и указателя порядка этой предпоследней подходящей дроби. Тогда решение сравнения (1) выразится формулой:

$$x \equiv (-1)^{n-1} bP_{n-1} \pmod{k}. \qquad (6)$$

Пример. Решим сравнение $7x \equiv 5 \pmod{19}$.

Решение. Дробь $\frac{19}{7}$ обратим в непрерывную; находим $\frac{19}{7} = (2, 1, 2, 2)$. Предпоследняя подходящая дробь $\frac{8}{3}$ третьего порядка, $P_3 = 8$. Применив формулу (6), получим:

$$x \equiv -40 \pmod{19} \text{ или } x \equiv -2 \pmod{19}.$$

Но это решение мы можем представить в другом виде, заменив -2 его наименьшим положительным вычетом по модулю 19, который есть 17. Получаем:

$$x \equiv 17 \pmod{19}.$$

128. *Рассмотрим второй случай: коэффициент a и модуль сравнения*

$$ax \equiv b \pmod{k} \qquad (1)$$

имеют общего наибольшего делителя d : $(a, k) = d$.

Этот же общий наибольший делитель коэффициента a и модуля k должен делить и b; если это условие не соблюдено, то сравнение (1) не имеет решения. И, действительно, мы показали, что решение сравнения (1) сводится к нахождению одного из кого-нибудь целого значения x из уравнения

$$ax - ky = b. \qquad (2)$$

Но из алгебры известно, что когда коэффициенты a и k имеют общего множителя, который не делит нацело b, то неопределенное уравнение (2) не имеет целых решений. А раз уравнение (2) не имеет целых решений, то и сравнение (1) не имеет решений. *Отсюда следует, что существуют сравнения первой степени, не имеющие решений, как, например, сравнения*

$$15x \equiv 7 \pmod{25},\ 12x \equiv 5 \pmod{14},\ 4x \equiv 3 \pmod{10}.$$

Мы исключим из рассмотрения такие сравнения. Докажем теорему:

Теорема. *Если общий наибольший делитель d чисел a и k делит b, то сравнение*

$$ax \equiv b \pmod{k} \qquad (1)$$

имеет d корней.

Доказательство. Обозначим частные от деления a и k на d соответственно через a_1 и k_1; ясно, что a_1 и k_1 числа взаимно простые (п. 34). Имеем: $a = a_1 d$, $k = k_1 d$. Пусть будет b_1 частное от деления b на d: $b = db_1$. Подставив найденные для a, b, k выражения в сравнение (1) и разделив обе части полученного сравнения и модуль на d, получим сравнение:

$$a_1 x \equiv b_1 \pmod{k_1}. \qquad (2)$$

Полученное сравнение (2) имеет одно решение, которое по одному из указанных способов мы можем найти. Пусть каким-нибудь способом мы нашли, что

$$x \equiv \alpha \pmod{k_1}. \qquad (3)$$

У нас α есть одно и только одно из чисел ряда

$$0,\ 1,\ 2,\ 3,\ \ldots,\ k_1 - 1.$$

Покажем, что α удовлетворяет и сравнению (1). Это доказать не трудно. Имеем:

$$a_1\alpha \equiv b_1 \pmod{k_1}.$$

Из определения сравнения следует, что $\frac{a_1\alpha - b_1}{k_1}$ = целому числу.

Умножив числителя и знаменателя выражения $\frac{a_1\alpha - b_1}{k_1}$ на d и помня, что $a_1 d = a$, $b_1 d = b$, $k_1 d = k$, получаем:

$$\frac{a_1 d\alpha - b_1 d}{k_1 d} = \frac{a\alpha - b}{k} = \text{целому числу},$$

Откуда

$$a\alpha \equiv b \pmod{k},$$

что и требовалось доказать.

Теперь докажем, что всякое решение сравнения (1) удовлетворяет и сравнению (2). Пусть будет

$$x \equiv \beta \pmod{k}$$

решением сравнения (1). Тогда из определения сравнения следует, что

$$\frac{a\beta - b}{k} = \text{целому числу}.$$

Разделив числителя и знаменателя выражения $\frac{a\beta - b}{k}$ на d и помня, что $\frac{a}{d} = a_1$, $\frac{b}{d} = b_1$, $\frac{k}{d} = k_1$, находим:

$$\frac{\frac{a\beta}{d} - \frac{b}{d}}{\frac{k}{d}} = \frac{a_1\beta - b_1}{k_1} = \text{целому числу}.$$

Переходя от равенства к сравнению, получаем:

$$a_1\beta \equiv b_1 \pmod{k},$$

что и нужно было доказать.

Мы знаем, что сравнение (2) имеет одно и только одно решение

$$x \equiv \alpha \pmod{k}.$$

Тогда все числа, удовлетворяющие сравнению (2), а, стало быть, и сравнению (1), будут заключаться в формуле

$$x = \alpha + k_1 q,$$

где q есть любое целое число.

Но один класс чисел по модулю k может распасться на несколько классов по модулю k_1. В самом деле, давая q значения

$$0, 1, 2, 3, \ldots, d-1,$$

получим d чисел:

$$\alpha,\ \alpha + k_1,\ \alpha + 2k_1,\ \alpha + 3k_1,\ \ldots,\ \alpha + (d-1)\,k_1. \qquad (4)$$

Любое из чисел этого ряда меньше k, а разность каждых двух чисел этого ряда по абсолютной величине подавно будет меньше k. Следовательно, числа нашего ряда принадлежат к d различным классам по модулю k. Но так как эти числа принадлежат к d различным классам по модулю k, то эти числа и будут составлять d различных решений сравнения (1); эти решения определяются посредством решения сравнения (2) формулами:

$$\left.\begin{aligned} x &\equiv \alpha \\ x &\equiv \alpha + k_1 \\ x &\equiv \alpha + 2k_1 \\ &\cdots\cdots \\ x &\equiv \alpha + (d-1)\,k_1 \end{aligned}\right\} \pmod{k}. \qquad (5)$$

Таким образом, теорема доказана.

Пример. $15x \equiv 18 \pmod{21}$. (1)

Решение. Общий наибольший делитель коэффициента 15 и модуля 21 равен 3; так как 3 делит 18, то сравнение возможно и имеет три решения. Деля обе части сравнения (1) и модуль на 3, получим сравнение

$$5x \equiv 6 \pmod{7}. \quad (2)$$

Решив сравнение (2), получим:

$$x \equiv 4 \pmod{7}.$$

Составляем три числа: 4, $4 + 7 = 11$, $4 + 2 \cdot 7 = 18$. Тогда решения сравнения (1) выразятся формулами:

$$\left.\begin{array}{l} x \equiv 4 \\ x \equiv 11 \\ x \equiv 18 \end{array}\right\} \pmod{21}.$$

129. *Теперь покажем, как найти все значения x, одновременно удовлетворяющие системе сравнений такого вида:*

$$\begin{array}{l} a_1 x \equiv b_1 \pmod{k_1} \\ a_2 x \equiv b_2 \pmod{k_2} \\ a_3 x \equiv b_3 \pmod{k_3} \\ \cdots\cdots\cdots \\ a_n x \equiv b_n \pmod{k_n}. \end{array} \quad (I)$$

Заметим, что a_i и k_i — числа взаимно простые ($i = 1, 2, 3, \ldots, n$).

Решим первое сравнение. Пусть будет

$$x \equiv \alpha_1 \pmod{k_1}$$

его решение. Тогда все числа, удовлетворяющие первому сравнению, заключаются в формуле $x = \alpha_1 + k_1 y_1$ (1), где y_1 есть какое угодно целое число. Чисел, удовлетворяющих первому сравнению, бесчисленное множество. Но из этих чисел нам надо выбрать те, которые удовлетворяют одновременно и второму сравнению. Подставляя во второе сравнение вместо x найденное для него выражение $\alpha_1 + k_1 y_1$, получаем условие для определения y_1:

$$a_2 \alpha_1 + a_2 k_1 y_1 \equiv b_2 \pmod{k_2}, \text{ или } a_2 k_1 y_1 \equiv b_2 - a_2 \alpha_1 \pmod{k_2}. \quad (2)$$

Обозначим через d_1 общего наибольшего делителя коэффициента $a_2 k_1$ и модуля k_2. Если d_1 делит разность $b_2 - a_2 \alpha_1$, то сравнение (2) имеет решение; тогда всякому значению y_1 будет соответствовать определенное значение x, определяемое по формуле (1). Всякое такое значение x будет удовлетворять обоим первым сравнениям нашей системы (I). Если же d_1 не делит разности $b_2 - a_2 \alpha_1$, то сравнение (2) не имеет решения, стало быть, система (I) невозможна. Положим, что d_1 делит разность $b_2 - a_2 \alpha_1$,

Разделив обе части сравнения (2) и модуль k_2 на d_1 и решив полученное сравнение, которое имеет только один корень, находим:

$$y_1 \equiv \alpha_2 \pmod{\frac{k_2}{d_1}}, \text{ откуда } y_1 = \alpha_2 + \frac{k_2}{d_1} \cdot y_2,$$

где y_2 есть какое угодно целое число. Подставив найденное для y, выражение в равенство (1), находим:

$$x = \alpha_1 + k_1 y_1 = \alpha_1 + k_1\alpha_2 + \frac{k_1 k_2}{d_1} \cdot y_2. \qquad (3)$$

Число $\frac{k_1 k_2}{d_1}$ (п. 60) есть общее наименьшее кратное модулей k_1 и k_2, которое обозначим через k_{12}. Получаем:

$$x = \alpha_1 + k_1\alpha_2 + k_{12}\, y_2. \qquad (4)$$

Переходя от равенства к сравнению, находим:

$$x \equiv \alpha_1 + k_1\alpha_2 \pmod{k_{12}}. \qquad (5)$$

Если модули k_1 и k_2—числа взаимно простые, то формула (5) примет вид:

$$x \equiv \alpha_1 + k_1\alpha_2 \pmod{k_1 k_2}. \qquad (6)$$

Мы нашли, что совокупность значений x, удовлетворяющих одновременно первым двум сравнениям системы, выражается формулой (5) или же формулой (6).

Теперь из всех значений x, одновременно удовлетворяющих обоим первым сравнениям системы (I), нам надо выбрать те, которые удовлетворяют и третьему сравнению системы. Эти значения x мы найдем из условия

$$\begin{aligned} a_3\alpha_1 + a_3 k_1\alpha_2 + a_3\, k_{12}\, y_2 &\equiv b_3 \pmod{k_3}, \\ a_3 k_{12}\, y_2 &\equiv b_3 - (a_3\alpha_1 + a_3 k_1\alpha_2) \pmod{k_3}. \end{aligned} \qquad (7)$$

Обозначим через d_2 общего наибольшего делителя коэффициента $a_3 k_{12}$ и модуля k_3. Если d_2 делит и разность $b_3 - (a_3\alpha_1 + a_3 k_1\alpha_2)$, то сравнение (7) имеет решения. Тогда всякому значению y_2 будет соответствовать определенное значение x, определяемое по формуле (4). Всякое такое значение x будет удовлетворять одновременно первым трем сравнениям системы (I). Если же d_2 не делит разности $b_3 - (a_3\alpha_1 + a_3 k_1\alpha_2)$, то сравнение (7), а следовательно, и вся система (I) невозможны. Предположим, что сравнение (7) возможно. Разделив обе части сравнения (7) и модуль k_3 на d_2 и решив полученное сравнение, найдем:

$$y_2 \equiv \alpha_3 \left(\text{mod } \frac{k_3}{d_2}\right),$$

откуда

$$y_2 = \alpha_3 + \frac{k_3}{d_2}\, y_3,$$

где y_3 есть какое угодно целое число. Подставив значение y_2 в равенство (4), получим:

$$x = \alpha_1 + k_1\alpha_2 + k_{12}\alpha_3 + \frac{k_{12}k_3}{d_2}\, y_3.$$

Заметим, что общее наименьшее кратное двух чисел равно частному от деления их произведения на их общего наибольшего делителя (п. 60). Значит, число $\frac{k_{12}k_3}{d_2}$ есть общее наименьшее кратное k_{12} и k_3, где k_{12} есть общее наименьшее кратное модулей k_1 и k_2. Из теоремы „Чтобы найти общее наименьшее кратное трех чисел, нужно найти сперва общее наименьшее кратное первых двух чисел, а затем общее наименьшее кратное этого общего наименьшего кратного и третьего числа. Это последнее общее наименьшее кратное и будет искомым общим наименьшим кратным трех данных чисел", следует, что число $\frac{k_3 k_{12}}{d_2}$ есть общее наименьшее кратное модулей k_1, k_2, k_3, которое обозначим через k_{123}.

Тогда предыдущее равенство примет вид:

$$x = \alpha_1 + k_1\alpha_2 + k_{12}\alpha_3 + k_{123}\, y_3.$$

Переходя от равенства к сравнению, найдем:

$$x \equiv \alpha_1 + k_1\alpha_2 + k_{12}\alpha_3 \pmod{k_{123}}. \qquad (8)$$

Мы нашли, что совокупность всех чисел, удовлетворяющих одновременно первым трем сравнениям системы (I), выражается формулой (8). Если модуль k_1, k_2, k_3 — числа попарно простые, то формула (8) примет вид:

$$x \equiv \alpha_1 + k_1\alpha_2 + k_1k_2\alpha_3 \pmod{k_1k_2k_3}. \qquad (9)$$

Рассуждая таким же путем и далее, мы в конце концов придем к такому заключению:

Несколько сравнений вида (I) *или вовсе не имеют решения, или же имеют одно решение, состоящее из чисел одного класса по модулю, равному общему наименьшему кратному модулей* k_1, k_2, k_3, . . ., k_n.

Тогда решение системы сравнений (I) выразится формулой

$$x \equiv \alpha_1 + k_1\alpha_2 + k_{12}\alpha_3 + k_{123}\alpha_4 + \ldots + \\ + k_{123\ldots(n-1)}\alpha_n \pmod{k_{123\ldots n}} \qquad (10)$$

Если же модули $k_1, k_2, k_3, \ldots, k_n$ — числа попарно простые, то формула (10) примет вид:

$$x \equiv \alpha_1 + k_1\alpha_2 + k_1k_2\alpha_3 + k_1k_2k_3\alpha_4 + \ldots + \\ + k_1k_2k_3\ldots k_{n-1}\alpha_n \pmod{k_1k_2k_3\ldots k_n}. \qquad (11)$$

В последнем случае система всегда возможна.

130. Пример 1. Решить систему сравнений:

$$7x \equiv 2 \pmod 9,\ 11x \equiv 1 \pmod{21},\ 4x \equiv 5 \pmod{15}.$$

Решение. Решив первое сравнение, найдем $x \equiv 8 \pmod 9$; $\alpha_1 = 8$. Все числа, удовлетворяющие первому сравнению, заключаются в формуле $x = 8 + 9y_1$. Подставив значение x во второе сравнение, получим: $88 + 99y_1 \equiv 1 \pmod{21}$, или $99y_1 \equiv -87 \pmod{21}$. Общий наибольший делитель коэффициента 99

и модуля 21 равен 3; 3 делит —87; разделив обе части предыдущего сравнения и модуль на 3, получим $33y_1 \equiv -29 \pmod 7$, а это сравнение может быть приведено к виду $5y_1 \equiv -1 \pmod 7$. Это сравнение имеет решение $y_1 \equiv 4 \pmod 7$; $\alpha_2 = 4$. Все числа, удовлетворяющие сравнению $5y_1 \equiv -1 \pmod 7$, заключаются в формуле $y_1 = 4 + 7y_2$. Подставив выражение y_1 в равенство $x = 8 + 9y_1$, найдем: $x = 44 + 63y_2$. Подставляя выражение x в третье сравнение, получим:

$$176 + 252y_2 \equiv 5 \pmod{15}, \text{ или } 252y_2 \equiv -171 \pmod{15}.$$

Общий наибольший делитель коэффициента 252 и модуля 15 равен 3; 3 делит —171. Разделив обе части сравнения и модуль на 3, получаем: $84y_2 \equiv -57 \pmod 5$, или $4y_2 \equiv 3 \pmod 5$.

Решив это сравнение, получим: $y_2 \equiv 2 \pmod 5$; $\alpha_3 = 2$.

Применим формулу:

$$x \equiv \alpha_1 + k_1\alpha_2 + k_{12}\alpha_3 \pmod{k_{123}}.$$

$$k_{12} = m(9, 21) = 63; \quad k_{123} = m(9, 21, 15) = m(63, 15) = 315.$$

Получаем

$$x \equiv 8 + 9 \cdot 4 + 63 \cdot 2 \pmod{315},$$

или

$$x \equiv 170 \pmod{315}.$$

Таким образом, один класс чисел по модулю 315 образует решение нашей системы сравнений.

Пример 2. Решить систему сравнений:

$$2x \equiv 1 \pmod 3, \quad 3x \equiv 2 \pmod 5, \quad 4x \equiv 5 \pmod 7,$$
$$3x \equiv 8 \pmod{11}.$$

Решение. Решим первое сравнение; находим: $x \equiv 2 \pmod 3$; $\alpha_1 = 2$. Все числа, удовлетворяющие первому сравнению, заключаются в формуле $x = 2 + 3y_1$. Подставим выражение x во второе сравнение, получим $6 + 9y_1 \equiv 2 \pmod 5$, или $9y_1 \equiv -4 \pmod 5$. Это сравнение может быть приведено к виду $4y_1 \equiv -4 \pmod 5$, или $y_1 \equiv -1 \pmod 5$, откуда $y_1 \equiv 4 \pmod 5$; $\alpha_2 = 4$. Все числа, удовлетворяющие этому сравнению, заключаются в формуле $y_1 = 4 + 5y_2$. Подставив выражение y_1 в равенство $x = 2 + 3y_1$, получим: $x = 14 + 15y_2$. Подставив выражение x в третье сравнение, получим: $56 + 60y_2 \equiv 5 \pmod 7$, или $60y_2 \equiv -51 \pmod 7$. Это сравнение может быть заменено сравнением $4y_2 \equiv 5 \pmod 7$.

Решив это сравнение, найдем: $y_2 \equiv 3 \pmod 7$; $\alpha_3 = 3$. Все числа, удовлетворяющие сравнению $4y_2 \equiv 5 \pmod 7$, заключаются в формуле $y_2 = 3 + 7y_3$; подставив выражение y_2 в равенство $x = 14 + 15y_2$, находим: $x = 59 + 105y_3$; подставив полученное выражение x в последнее сравнение нашей системы, находим:

$$177 + 315y_3 \equiv 8 \pmod{11} \text{ или } 315y_3 \equiv -169 \pmod{11}.$$

Заменим это сравнение эквивалентным ему сравнением $7y_3 \equiv -4 \pmod{11}$. Заменив -4 его наименьшим положительным вычетом 7 по модулю 11, получим: $7y_3 \equiv 7 \pmod{11}$ или $y_3 \equiv 1 \pmod{11}$; $\alpha_4 = 1$.

Применив формулу

$$x \equiv \alpha_1 + k_1\alpha_2 + k_1k_2\alpha_3 + k_1k_2k_3\alpha_4 \pmod{k_1k_2k_3k_4},$$

получим:

$$x \equiv 2 + 4 \cdot 3 + 3 \cdot 5 \cdot 3 + 3 \cdot 5 \cdot 7 \cdot 1 \pmod{3 \cdot 5 \cdot 7 \cdot 11},$$

или

$$x \equiv 174 \pmod{1155}.$$

ГЛАВА ДЕСЯТАЯ

Сравнения высших степеней по простому модулю. Теорема Вильсона

131. Определения. *Пусть*

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \qquad (1)$$

будет целая функция n-й степени с целыми коэффициентами a_0, a_1, a_2, a_3, . . ., a_n.

Если коэффициент a_0 *старшего члена функции (1) не делится на p, то сравнение*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod{p} \qquad (2)$$

называется сравнением n-й степени.

Если при $x = \alpha$ *значение функции* $f(x)$ *делится на число p, то говорят, что* α *есть корень сравнения (2), и пишут:*

$$f(\alpha) \equiv 0 \pmod{p}. \qquad (3)$$

Тому же сравнению (2) будут удовлетворять и все числа сравнимые с α по модулю p (п. 103). Весь этот класс чисел считается за один корень сравнения (2). Разные корни сравнения (2) не должны быть сравнимы между собою по модулю p. Значит, когда в теории чисел идет вопрос о нахождении всех решений сравнения (2), то дело идет о нахождении различных классов чисел по модулю p.

Чтобы найти корни сравнения (2), надо подставлять в это сравнение вместо x последовательно числа полной системы вычетов по модулю p:

$$0, 1, 2, 3, \ldots, p-1. \qquad (4)$$

Те из чисел ряда (4), которые будут удовлетворять сравнению (2), и будут его корнями.

В то время как всякое уравнение n-й степени имеет n решений, есть, однако, сравнения высших степеней, которые не имеют ни одного решения. Так, например, сравнение

$$x^4 - 2x^3 - 3x^2 + 4x + 2 \equiv 0 \pmod{5}$$

не имеет ни одного решения, в чем можно убедиться, испытывая числа 0, 1, 2, 3, 4,— представителей всех классов по

модулю 5. Мы видим, что аналогия между сравнениями высших степеней и алгебраическими уравнениями не сохраняется во всей полноте.

Важнейшие и самые любопытные результаты, добытые в теории сравнений высших степеней, относятся к случаю, когда модуль p есть простое число. Вот почему мы будем рассматривать исключительно сравнения высших степеней по простому модулю p.

132. Теорема. *Из сравнения*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod{p} \quad (1)$$

может быть исключен всякий член, коэффициент которого делится на p.

Доказательство. Пусть коэффициент a_2 при x^{n-2} делится на p. Из делимости a_2 на p следует сравнение

$$a_2 \equiv 0 \pmod{p}.$$

Умножив обе части этого сравнения на x^{n-2}, получим:

$$a_2x^{n-2} \equiv 0 \pmod{p}.$$

Вычитая почленно это сравнение из сравнения (1), находим:

$$a_0x^n + a_1x^{n-1} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod{p}. \quad (2).$$

Сравнение (1) мы заменили сравнением (2), в котором отсутствует член a_2x^{n-2} сравнения (1). Коэффициент a_2 этого члена делится на p. То же самое может быть сделано со всяким другим членом сравнения (1), если коэффициент его делится на p.

В виду этого сравнение (1) может быть названо сравнением степени n-й, если коэффициент a_0 старшего члена a_0x^n не делится на p; если a_0 делится на p, но a_1 не делится на p, то сравнение (1) будет уже сравнением не n-й степени, а степени $n-1$.

Пример. Сравнение

$$14x^7 - 35x^6 - 7x^5 + 28x^4 + 3x^3 - 2x^2 - 7x + 6 \equiv 0 \pmod{7}$$

есть сравнение не 7-й степени, а сравнение 3-й степени, и оно эквивалентно сравнению

$$3x^3 - 2x^2 + 6 \equiv 0 \pmod{7}.$$

133. Теорема. *Любой коэффициент сравнения*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod{p} \quad (1)$$

может быть заменен его наименьшим положительным вычетом по модулю p.

Доказательство. Пусть r_2 будет наименьший положительный вычет коэффициента a_2 по модулю p. Получаем:

$$a_2 \equiv r_2 \pmod{p}, \text{ или } a_2 - r_2 \equiv 0 \pmod{p}.$$

Умножив обе части этого сравнения на x^{n-2}, находим:

$$a_2x^{n-2} - r_2x^{n-2} \equiv 0 \pmod{p}.$$

Вычитая почленно это сравнение из сравнения (1), получаем

$$a_0x^n + a_1x^{n-1} + r_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod{p}.$$

Таким образом, член a_2x^{n-2} мы заменили членом r_2x^{n-2}.

То же самое может быть сделано со всяким членом сравнения (1), если его коэффициент отрицателен или больше модуля p.

Пример. Сравнение

$$17x^4 - 13x^3 + 5x^2 - x + 2 \equiv 0 \pmod{7}$$

может быть заменено эквивалентным ему сравнением

$$3x^4 + x^3 + 5x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

134. Теорема. *Сравнение n-й степени*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod{p} \quad (1)$$

можно преобразовать в эквивалентное ему сравнение, в котором коэффициент при x^n равен единице.

Доказательство. Возьмем сравнение

$$a_0x \equiv 1 \pmod{p} \quad (2)$$

и решим его. Пусть α будет его корень. Имеем:

$$a_0\alpha \equiv 1 \pmod{p}, \text{ или } a_0\alpha - 1 \equiv 0 \pmod{p}. \quad (3)$$

Умножая сравнение (3) последовательно на

$$a_1x^{n-1},\ a_2x^{n-2}, a_3x^{n-3}, \ldots, a_n,$$

получаем сравнения:

$$\left.\begin{aligned} a_0a_1\alpha x^{n-1} - a_1x^{n-1} &\equiv 0 \\ a_0a_2\alpha x^{n-2} - a_2x^{n-2} &\equiv 0 \\ a_0a_3\alpha x^{n-3} - a_3x^{n-3} &\equiv 0 \\ \cdots\cdots\cdots\cdots & \\ a_0a_n\alpha - a_n &\equiv 0 \end{aligned}\right\} \pmod{p}$$

Складывая почленно эти сравнения с сравнением (1), получаем сравнение

$$a_0x^n + a_0a_1\alpha x^{n-1} + a_0a_2\alpha x^{n-2} + a_0a_3\alpha x^{n-3} + \ldots + a_0a_n\alpha \equiv 0 \pmod{p}.$$

Так как a_0 есть число простое относительно модуля p, то полученное сравнение может быть сокращено на a_0. Получаем сравнение:

$$x^n + a_1\alpha x^{n-1} + a_2\alpha x^{n-2} + a_3\alpha x^{n-3} + \ldots + a_n\alpha \equiv 0 \pmod{p}, \quad (4)$$

эквивалентное сравнению (1). Таким образом, теорема доказана.

Отсюда мы приходим к такому правилу:

Правило. *Чтобы преобразовать сравнение (1) в эквивалентное ему сравнение (4), в котором коэффициент старшего члена равен единице, нужно предварительно решить сравнение*:

$$a_0x \equiv 1 \pmod{p},$$

старший член a_0x^n данного сравнения заменить членом x^n, а все остальные члены его умножить на корень сравнения $a_0x \equiv 1 \pmod p$. Полученное таким путем сравнение (4) будет искомым.

Пример. $3x^3 - 5x^2 + 2x - 7 \equiv 0 \pmod{11}$.

Решение. Предварительно решаем сравнение

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

Находим:

$$x \equiv 4 \pmod{11}; \alpha \equiv 4.$$

Применив наше правило, получим сравнение

$$x^3 - 20x^2 + 8x - 28 \equiv 0 \pmod{11},$$

которое, в свою очередь, может быть заменено сравнением

$$x^3 + 2x^2 + 8x + 5 \equiv 0 \pmod{11}.$$

135. Теорема. *Если сравнение n-й степени*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod p$$

имеет n различных корней $x_1, x_2, x_3, x_4, \ldots, x_n$, то это сравнение может быть заменено эквивалентным ему сравнением, левая часть которого есть произведение n разностей между переменным x и каждым из корней $x_1, x_2, x_3, \ldots, x_n$ сравнения, умноженное на коэффициент a_0 при x^n.

Доказательство. Дано сравнение

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod p, \quad (1)$$

$x_1, x_2, x_3, \ldots, x_n$ — его различные корни. Имеем:

$$\left.\begin{array}{l} f(x_1) \equiv 0 \\ f(x_2) \equiv 0 \\ f(x_3) \equiv 0 \\ \ldots\ldots \\ f(x_n) \equiv 0 \end{array}\right\} \pmod p.$$

Требуется доказать, что сравнение (1) может быть заменено эквивалентным ему сравнением:

$$a_0(x-x_1)(x-x_2)(x-x_3)\ldots(x-x_n) \equiv 0 \pmod p.$$

Левую часть сравнения (1) обозначим через $f(x)$:

$$f(x) \equiv a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$$

Имеем:

$$f(x) \equiv 0 \pmod p. \quad (2)$$

Делим функцию (x) на разность $x - x_1$; обозначим частное через $f_1(x)$, а остаток — через r_1. Частное $f_1(x)$ будет многочлен степени $n-1$ с целыми коэффициентами, и первый его член будет a_0x^{n-1}, а остаток r_1 будет постоянное число.

По свойству деления должно быть:

$$f(x) = (x-x_1)f_1(x) + r_1. \quad (3)$$

По теореме Безу имеем:

$$f(x_1) = r_1;$$

$f(x_1) \equiv 0 \pmod{p}$; следовательно, и $r_1 \equiv 0 \pmod{p}$.

Принимая во внимание равенство (3), сравнение (2) можем представить в таком виде:

$$(x-x_1)\, f_1(x) + r_1 \equiv 0 \pmod{p}.$$

Член этого сравнения r_1, как делящийся на p, исключим из сравнения. Получаем эквивалентное сравнению (2) сравнение:

$$(x-x_1)\, f_1(x) \equiv 0 \pmod{p}. \qquad (4)$$

Мы знаем, что x_2 есть другой корень сравнения (2). Сравнение (4), как равносильное сравнению (2), должно выполняться при $x \equiv x_2$. Получаем:

$$(x_2-x_1)\, f_1(x_2) \equiv 0 \pmod{p}.$$

Из этого сравнения следует, что произведение $(x_2-x_1)\, f_1(x_2)$ делится на p. Так как сомножитель x_2-x_1 не равен нулю и не делится на модуль p, то сомножитель $f_1(x_2)$ должен делиться на p (п. 40). Из делимости $f_1(x_2)$ на p следует, что x_2 есть корень сравнения

$$f_1(x) \equiv 0 \pmod{p}. \qquad (5)$$

Делим $f_1(x)$ на разность $x-x_2$; обозначим частное через $f_2(x)$, а остаток — через r_2. Частное $f_2(x)$ будет многочлен степени $n-2$ с целыми коэффициентами, и первый его член будет a_0x^{n-2}, а остаток r_2 будет постоянное число. По свойству деления должно быть:

$$f_1(x) = (x-x_2)\, f_2(x) + r_2. \qquad (6)$$

Полагая в этом тождестве $x = x_2$, получаем:

$f_1(x_2) = r_2$, а $f_1(x_2) \equiv 0 \pmod{p}$; следовательно, и $r_2 \equiv 0 \pmod{p}$.

Подставив в сравнение (4) вместо $f_1(x)$ его выражение, имеем:

$$(x-x_1)(x-x_2) f_2(x) + r_2(x-x_1) \equiv 0 \pmod{p}.$$

Член этого сравнения $r_2(x-x_1)$, как делящийся на p, исключим из сравнения. Получаем эквивалентное сравнению (2) сравнение

$$(x-x_1)(x-x_2) f_2(x) \equiv 0 \pmod{p}. \qquad (7)$$

Мы знаем, что x_3 есть корень этого сравнения. Получаем:

$$(x_3-x_1)(x_3-x_2 f(x_3) \equiv 0 \pmod{p}.$$

Из этого сравнения следует, что произведение

$$(x_3 - x_1)(x_3 - x_2)\, f_2(x_3)$$

делится на p. Так как ни одно из чисел $x_3 - x_1$ и $x_3 - x_2$ не равно нулю и не делится на простое число p, то и их произведение не разделится на p (п. 44).

В таком случае число $f_2(x_3)$ должно делиться на p. Из делимости $f_2(x_3)$ на p следует, что x_3 есть корень сравнения

$$f_2(x) \equiv 0 \pmod{p}.$$

Делим $f_2(x)$ на разность $x - x_3$, частное обозначаем через $f_3(x)$, а остаток — через r_3. Частное $f_3(x)$ будет многочлен степени $n-3$ с целыми коэффициентами, а остаток r_3 будет постоянное число.

По свойству деления должно быть:

$$f_2(x) = (x - x_3) f_3(x) + r_3.$$

Полагая в этом тождестве $x = x_3$, получаем: $f_2(x_3) = r_3$, а $f(x_3) \equiv 0 \pmod{p}$; следовательно и $r_3 \equiv 0 \pmod{p}$.

Мы нашли, что сравнение (2) эквивалентно сравнению (7). Подставив в сравнение (7) вместо многочлена $f_2(x)$ его выражение

$$(x - x_3) f_3(x) + r_3,$$

получим сравнение

$$(x - x_1)(x - x_2)[(x - x_3) f_3(x) + r_3] \equiv 0 \pmod{p},$$

или сравнение

$$(x - x_1)\, x - x_2)(x - x_3) f_3(x) + r_3 (x - x_1)(x - x_2) \equiv 0 \pmod{d}.$$

Исключив из этого сравнения делящийся на p член

$$r_3(x - x_1)(x - x_2),$$

получим эквивалентное сравнению (2) сравнение:

$$(x - x_1)(x - x_2)(x - x_3) f_3(x) \equiv 0 \pmod{p}.$$

Продолжая и далее так рассуждать, мы получим в конце концов эквивалентное сравнению (2) сравнение:

$$(x - x_1)(x - x_2)(x - x_3) \ldots (x - x_{n-1}) f_{n-1}(x) \equiv 0 \pmod{p}, \quad (9)$$

где $f_{n-1}(x)$ есть целая функция первой степени с целыми коэффициентами, и первый ее член есть $a_0 x$.

Сравнение (9) выполняется при $x = x_n$. Получаем:

$$(x_n - x_1)(x_n - x_2)(x_n - x_3) \ldots (x_n - x_{n-1}) f_{n-1}(x_n) \equiv 0 \pmod{p}.$$

Так как ни один из сомножителей $x_n - x_1$, $x_n - x_2, \ldots$, $x_n - x_{n-1}$ не равен нулю и не делится на простое число p, то на p не разделится и их произведение (п. 45). В таком случае сомножитель $f_{n-1}(x_n)$ должен делиться на p (п. 42).

Из делимости числа $f_{n-1}(x_n)$ на p следует, что x_n есть корень сравнения

$$f_{n-1}(x) \equiv 0 \pmod{p}.$$

Делим $f_{n-1}(x)$ на разность $x - x_n$, частное будет a_0, а остаток r_n — постоянное число. По свойству деления должно быть

$$f_{n-1}(x) = a_0(x - x_n) + r_n.$$

Полагая в этом тождестве $x = x_n$, получаем

$$f_{n-1}(x_n) = r_n,\ f_{n-1}(x_n) \equiv 0 \pmod{p};$$

следовательно, и $r_n \equiv 0 \pmod{p}$. Подставив выражение $f_{n-1}(x)$ в сравнение (9), находим:

$$(x - x_1)(x - x_2)(x - x_3) \ldots (x - x_{n-1})[a_0(x - x_n) + r_n] \equiv$$
$$\equiv 0 \pmod{p}.$$

Исключив из этого сравнения делящийся на p его член $r_n(x - x_1)(x - x_2)(x - x_3) \ldots (x - x_{n-1})$, получим эквивалентное сравнению (2) сравнение

$$a_0(x - x_1)(x - x_2)(x - x_3) \ldots (x - x_n) \equiv 0 \pmod{p}. \quad (10)$$

Таким образом, теорема доказана.

136. Теорема. *Сравнение n-й степени*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n \equiv 0 \pmod{p} \quad (1)$$

не может иметь более n корней.

Доказательство. Если сравнение (1) имеет n корней

$$x_1,\ x_2,\ x_3,\ x_4, \ldots, x_n, \quad (2)$$

то можем написать эквивалентное ему сравнение

$$a_0(x - x_1)(x - x_2)(x - x_3) \ldots (x - x_n) \equiv 0 \pmod{p} \quad (3)$$

Требуется доказать, что сравнение (3) не имеет никаких других корней, кроме n корней (2). Предположим обратное: допустим, что сравнение (3) имеет еще $n+1$ корень x_{n+1}, не сравнимый ни с одним из корней (2) по модулю p. При нашем предположении сравнение (3) при $x = x_{n+1}$ должно выполняться; имеем:

$$a_0(x_{n+1} - x_1)(x_{n+1} - x_2)(x_{n+1} - x_3) \ldots (x_{n+1} - x_n) \equiv 0 \pmod{p}.$$

Легко заметить, что это сравнение невозможно, так как a_0 не делится на p и ни одна из разностей $x_{n+1} - x_i$ не равна нулю ($i = 1, 2, 3, \ldots, n$) и не делится на p, ибо все корни $x_1, x_2, x_3, \ldots, x_n, x_{n+1}$ предполагаются различными и не сравнимыми между собою по модулю p. Следовательно, наше допущение что сравнение (3), кроме n корней (2), имеет еще $n+1$ корень x_{n+1}, является неверным. Таким образом, теорема доказана.

137. Теорема. *Если сравнение*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n \equiv \pmod{p}, \quad (1)$$

левая часть которого есть многочлен n-й степени с целыми коэффициентами, имеет более n корней, то все коэффициенты этого многочлена (этого сравнения) делятся на модуль p.

Доказательство. Пусть сравнение (1), кроме n различных корней

$$x_1,\ x_2,\ x_3,\ \ldots,\ x_n, \qquad (2)$$

имеет еще $n+1$ корень x_{n+1}, не сравнимый ни с одним из предыдущих корней (2) по модулю p. Требуется доказать, что $a_i \equiv 0 \pmod p$, где $i = 0, 1, 2, 3, \ldots, n$.

По условию теоремы должно быть: $f(x_j) \equiv 0 \pmod p$, где $j = 1, 2, 3, 4, \ldots, n, n+1$. Зная n корней (2) сравнения (1), можно написать эквивалентное ему сравнение

$$a_0 (x - x_1)(x - x_2)(x - x_3) \ldots (x - x_n) \equiv 0 \pmod p.$$

Это сравнение выполняется при $x = x_{n+1}$; имеем:

$$a_0 (x_{n+1} - x_1)(x_{n+1} - x_2)(x_{n+1} - x_3) \ldots (x_{n+1} - x_n) \equiv 0 \pmod p.$$

Так как ни одна из разностей $x_{n+1} - x_k$ $(k = 1, 2, 3, \ldots, n)$ не равна нулю и не делится на p, ибо все корни $x_1, x_2, \ldots, x_n, x_{n+1}$ предполагаются различными и не сравнимыми по модулю p, то a_0 должно делиться на p; имеем: $a_0 \equiv 0 \pmod p$. Исключив из сравнения (1) член $a_0 x^n$, получаем сравнение

$$a_1 x^{n-1} + a_2 x^{n-2} + a_3 x^{n-3} + \ldots + a_n \equiv 0 \pmod p. \qquad (3)$$

Это сравнение имеет $n-1$ корней $x_1, x_2, x_3, \ldots, x_{n-1}$; можно написать эквивалентное ему сравнение

$$a_1 (x - x_1)(x - x_2)(x - x_3) \ldots (x - x_{n-1}) \equiv 0 \pmod p.$$

Это сравнение выполняется при $x = x_n$; имеем:

$$a_1 (x_n - x_1)(x_n - x_2)(x_n - x_3) \ldots (x_n - x_{n-1}) \equiv 0 \pmod p.$$

Так как ни одна из разностей $x_n - x_\lambda$ $(\lambda = 1, 2, 3, \ldots, n-1)$ не равна нулю и не делится на p, ибо все корни $x_1, x_2, x_3, \ldots, x_n$ предполагаются различными и не сравнимыми по модулю p, то a_1 должно делиться на p; имеем:

$$a_1 \equiv 0 \pmod p.$$

Исключив из сравнения (3) член $a_1 x^{n-1}$, получим сравнение

$$a_2 x^{n-2} + a_3 x^{n-3} + a_4 x^{n-4} + \ldots + a_n \equiv 0 \pmod p. \qquad (4)$$

Применяя к сравнению (4) те же рассуждения, какие мы применили к сравнению (3), придем к заключению, что a_2 делится на p:

$$a_2 \equiv 0 \pmod p.$$

Продолжая рассуждать и далее подобным же образом, мы в конце концов придем к сравнению

$$a_{n-1}x + a_n \equiv 0 \pmod{p}, \qquad (5)$$

имеющему два корня x_1 и x_2.

Получаем сравнения:

$$\left.\begin{aligned} a_{n-1}x_1 + a_n &\equiv 0 \\ a_{n-1}x_2 + a_n &\equiv 0 \end{aligned}\right\} \pmod{p}.$$

Вычитая из первого сравнения почленно второе, получим

$$a_{n-1}(x_1 - x_2) \equiv 0 \pmod{p}.$$

Произведение $a_{n-1}(x_1 - x_2)$ делится на p. Но так как $x_1 - x_2$ не равно нулю и не делится на p, то a_{n-1} должно делиться на p. Получаем:

$$a_{n-1} \equiv 0 \pmod{p}.$$

Исключая из сравнения (5) член $a_{n-1}x$, получим сравнение

$$a_n \equiv 0 \pmod{p},$$

из которого видно, что a_n делится на p.

Таким образом, теорема доказана.

Следствие. *Если все коэффициенты сравнения делятся на модуль сравнения, то исключением их из сравнения сравнение приведется к тождеству*

$$0 \equiv 0 \pmod{p}.$$

Пример. Сравнение

$$10x^2 - 15x + 20 \equiv 0 \pmod{5}$$

удовлетворяется при любом значении $x = 0, 1, 2, 3, 4$.

Примечание. В алгебре имеется такая теорема: „Если функция n-й степени $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$ имеет более n корней, то все ее коэффициенты равны 0“.

Этой теореме алгебры соответствует в теории чисел только что доказанная нами теорема: „Если сравнение...“

138. Теорема Вильсона. *Произведение всех натуральных чисел, меньших данного простого числа p, сложенное с единицей, делится на p.*

Доказательство. Возьмем простое число p. Требуется доказать, что имеет место сравнение:

$$1 \cdot 2 \cdot 3 \ldots (p-1) + 1 \equiv 0 \pmod{p}.$$

По теореме Ферма имеем сравнение:

$$x^{p-1} - 1 \equiv 0 \pmod{p}. \qquad (1)$$

Ряд чисел, меньших данного простого числа p и взаимно простых с ним, имеет следующий вид:

$$1, 2, 3, 4, \ldots, p-1. \qquad (2)$$

Любое из чисел этого ряда удовлетворяет сравнению (1). Так как числа ряда (2) не сравнимы между собою по модулю p, то они и являются корнями сравнения (1). Следовательно, сравнение (1) может быть заменено эквивалентным ему сравнением

$$(x-1)(x-2)(x-3)(x-4)\ldots[x-(p-1)] \equiv 0 \pmod{p}, \qquad (3)$$

или сравнением

$$x^{p-1} + s_1 x^{p-2} + s_2 x^{p-3} + s_3 x^{p-4} + s_4 x^{p-5} + \ldots + \\ + 1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1 \equiv 0 \pmod{p}, \qquad (4)$$

где s_1 означает сумму всех вторых членов биномов, s_2—сумму всевозможных произведений вторых членов биномов, взятых по два, s_3—сумму всевозможных произведений вторых членов биномов, взятых по три, и т. д.; произведение всех вторых членов биномов есть

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1).$$

Вычитая из сравнения (3) почленно сравнение (1), получим сравнение

$$(x-1)(x-2)(x-3)\ldots[x-(p-1)] - x^{p-1} + 1 \equiv (\mathrm{mod}\ p), \qquad (5)$$

которое имеет $p-1$ корней:

$$1, 2, 3, 4, \ldots, p-1.$$

Легко заметить, что левая часть сравнения (5) есть функция степени $p-2$

$$s_1 x^{p-2} + s_2 x^{p-3} + s_3 x^{p-4} + \ldots + 1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1) + 1$$

с свободным членом

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1) + 1.$$

Из наличия у сравнения (5) $p-1$ корней следует, что все его коэффициенты должны быть кратны p. Последний коэффициент есть

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1) + 1 = (p-1)! + 1,$$

и он делится на p, а делимость этого коэффициента на p выражается сравнением

$$(p-1)! + 1 \equiv 0 \pmod{p},$$

что и требовалось доказать.

Примечание. Теорема Вильсона справедлива и при $p = 2$; в этом случае получается очевидное сравнение

$$1 + 1 \equiv 0 \pmod{2}.$$

Примеры.

1) $(3-1)!+1=1.\ 2+1=3$, а $3\equiv 0 \pmod 3$.

2) $(5-1)!+1=1.\ 2\cdot 3\cdot 4+1=25$, а $25\equiv 0 \pmod 5$.

3) $(7-1)!+1=1\cdot 2\cdot 3\cdot 45\cdot 6+1=721$, а $721\equiv 0 \pmod 7$.

139. *Теорема Вильсона допускает обратную теорему, которую мы сейчас докажем.*

Обратная теорема. *Если произведение всех натуральных чисел, меньших p, сложенное с единицей, делится на p, то p есть простое число.*

Доказательство. Имеем сравнение

$$(p-1)!+1\equiv 0 \pmod p. \qquad (1)$$

Требуется доказать, что p есть простое число. Допустим противное: пусть p будет составное число:

$$p=p_1p_2p_3\ldots p_n,$$

где $p_1, p_2, p_3, \ldots, p_n$ расположены в порядке их возрастания.

Множители $p_1, p_2, p_3, \ldots, p_n$ находятся среди чисел

$$2, 3, 4, 5, \ldots, p-1.$$

Член сравнения $(p-1)!=1\ldots p_1\ldots p_2\ldots p_3\ldots p_n\ldots(p-1)$ и модуль p делятся на любое из простых чисел $p_1, p_2, p_3, \ldots, p_n$, а другой член сравнения 1 не делится ни на одно из этих чисел, а следовательно и на их произведение. Отсюда следует и невозможность деления суммы $(p-1)!+1$ на p, а из невозможности деления суммы $(p-1)!+1$ на p следует и невозможность сравнения (1) при составном модуле p. Таким образом, наше допущение, что p есть составное число, приводит нас к невозможному сравнению; значит, наше допущение неверно, и нам остается согласиться с заключением теоремы, что p есть простое число.

Мы видим, что теорема Вильсона дает нам признак для распознавания простых чисел: если число $(p-1)!+1$ делится на p, то p обязательно должно быть простым числом. Однако теорема Вильсона практического значения не имеет, так как даже при не очень большом значении p выкладки для проверки правильности сравнения (1) становятся необычайно громоздкими.

Пример. $(4-1)!+1=1\cdot 2\cdot 3+1=7$, а 7 не делится на 4.

140. Теорема. *Если сравнение n-й степени*

$$a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n\equiv 6 \pmod p \qquad (1)$$

имеет n корней, и его левая часть разлагается на произведение двух многочленов $\psi_1(x)$ и $\psi_2(x)$ с целыми коэффициентами, то каждое из двух сравнений

$$\psi_1(x)\equiv 0 \pmod p \text{ и } \psi_2(x)\equiv 0 \pmod p \qquad (2)$$

имеет ровно столько корней, сколько единиц в показателе его степени.

Доказательство. Возьмем три многочлена с целыми коэффициентами соответственно степеням n, m и k так, чтобы $n = m + k$; получаем:

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n, \quad (3)$$

$$\psi_1(x) = b_0x^m + b_1x^{m-1} + b_2x^{m-2} + b_3x^{m-3} + \ldots + b_m, \quad (4)$$

$$\psi_2(x) = c_0x^k + c_1x^{k-1} + c_2x^{k-2} + c_3x^{k-3} + \ldots + c_k. \quad (5)$$

Согласно условию теоремы, между функциями (3), (4), (5) существует соотношение

$$f(x) = \psi_1(x)\ \psi_2(x). \quad (6)$$

Требуется доказать, что каждое из сравнений (2) имеет столько корней, сколько единиц в показателе его степени, а именно: сравнение $\psi_1(x) \equiv 0 \pmod p$ имеет m корней, а сравнение $\psi_2(x) \equiv 0 \pmod p$ k корней.

Заметим, что $a_0 \equiv b_0c_0$; называя сравнение (1) сравнением n-й степени, мы этим утверждали, что коэффициент a_0 не делится на p. Из неделимости a_0 на p следует, что коэффициенты b_0 и c_0 взаимно просты с p. Отсюда следует, что ни одно из сравнений (2) не может иметь более корней, чем единиц в показателе его степени. Из соотношения (6) следует, что каждый корень сравнения (1) является корнем одного из сравнений (2), и, обратно, корни сравнений (2), в свою очередь, являются корнями сравнения (1).

Таким образом, сумма корней сравнений (2) должна быть равна n. С другой стороны, ни одно из сравнений (2), например, сравнение $\psi_1(x) \equiv 0 \pmod p$, не может иметь корней меньше, нежели единиц в показателе его степени, скажем, $m-1$, ибо тогда число корней другого сравнения $\psi_2(x) \equiv 0 \pmod p$ непременно превысило бы его степень, став $k+1$, что, конечно, невозможно. Отсюда следует, что каждое из сравнений (2) имеет ровно столько разных корней, сколько есть единиц в степени этого сравнения, а это нам и нужно было доказать.

141. Теорема. *Решение сравнения*

$$f(x) \equiv 0 \pmod p, \quad (1)$$

степень которого больше или равна p, может быть всегда сведено к решению сравнения

$$\varphi(x) \equiv 0 \pmod p,$$

где $\varphi(x)$ *есть остаток от деления функции* $f(x)$ *на* $x^p - x$.

Доказательство. Обозначим через $\psi(x)$ и $\varphi(x)$ соответственно частное и остаток от деления функции $f(x)$ на $x^p - x$. По свойству деления должно быть:

$$f(x) = (x^p - x)\ \psi(x) + \varphi(x).$$

Тогда сравнение (1) примет вид:

$$(x^p - x)\ \psi(x) + \varphi(x) \equiv 0 \pmod p. \quad (2)$$

Выражение $x^p - x$ делится на p при всех значениях x. В силу этого произведение $(x^p - x)\psi(x)$ будет делиться на p при любом значении x. В виду этого из сравнения (2) может быть исключен член $(x^p - x)\psi(x)$; тогда сравнение (2) заменится сравнением $\varphi(x) \equiv 0 \pmod p$, что и требовалось доказать.

Примечание. *На основании этой теоремы степень сравнения с модулем 2 может быть понижена до 1, степень сравнения с модулем 3 может быть понижена до 2, и т. д.*

Пример. Возьмем сравнение

$$x^4 - 2x^3 + x^2 + x + 1 \equiv 0 \pmod 3.$$

Находим остаток от деления $x^4 - 2x^3 + x^2 + x + 1$ на $x^3 - x$. Искомый остаток равен $2x^2 - 2x + 1$. Следовательно, данное сравнение заменится сравнением

$$2x^2 - x + 1 \equiv 0 \pmod 3.$$

142. Определение. *Если сравнение имеет столько корней, сколько единиц в показателе его степени, то говорят: „Сравнение имеет максимальное число корней".*

143. Теорема. *Если сравнение*

$$f(x) \equiv 0 \pmod p \qquad (1)$$

степени не выше $p-1$ имеет максимальное число корней, то все коэффициенты остатка от деления двучлена $x^p - x$ на функцию $f(x)$ должны делиться на p.

Доказательство. Пусть n будет степень сравнения $f(x)$, а $\psi(x)$ и $\varphi(x)$ — соответственно частное и остаток от деления двучлена $x^p - x$ на функцию $f(x)$. По свойству деления должно быть:

$$x^p - x = f(x)\psi(x) + \varphi(x),$$

или

$$\varphi(x) = x^p - x - f(x)\psi(x). \qquad (2)$$

Пусть

$$x_1, x_2, x_3, \ldots, x_n \qquad (3)$$

будут корни сравнения (1).

Возьмем сравнение:

$$f(x)\psi(x) \equiv 0 \pmod p. \qquad (4)$$

Как известно, сравнение (1), будучи n-й степени, имеет n корней (3). Следовательно, сравнению (4) удовлетворяют все n корней сравнения (1), а что касается сравнения

$$x - x^p \equiv 0 \pmod p,$$

то оно имеет p корней, где p больше n.

Из этого следует, что сравнение

$$x^p - x - f(x)\varphi(x) \equiv 0 \pmod p \qquad (5)$$

имеет по крайней мере n корней.

Принимая во внимание тождество (2), сравнение (5) заменим сравнением

$$\varphi(x) \equiv 0 \pmod{p}, \tag{6}$$

которое также должно иметь по крайней мере n корней, хотя степень его меньше n. Отсюда следует, что все коэффициенты остатка $\varphi(x)$ должны делиться на p, что и требовалось доказать.

Пример. Возьмем сравнение

$$x^3 - 2x^2 - 5x + 6 \equiv 0 \pmod{7}.$$

Это сравнение имеет три корня: 1, 3, 5. Значит, наше сравнение имеет максимальное число корней.

Остаток от деления двучлена $x^7 - x$ на $x^3 - 2x^2 - 5x + 6$ есть $210x^2 + 252x - 462$; все коэффициенты этого остатка, как видно, делятся на 7.

Эта теорема допускает обратную теорему, которую сейчас докажем.

144. Обратная теорема. *Если все коэффициенты остатка от деления двучлена $x^p - x$ на функцию $f(x)$ степени n $(n \leqq p-1)$ делятся на p, то сравнение n-й степени*

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

имеет максимальное число корней.

Доказательство. Делим двучлен $x^p - x$ на функцию $f(x)$; частное от деления пусть будет $\psi(x)$, а остаток $\varphi(x)$. По свойству деления должно быть:

$$x^p - x = f(x)\psi(x) + \varphi(x),$$

откуда

$$f(x)\ \psi(x) = x^p - x - \varphi(x). \tag{2}$$

Требуется доказать, что сравнение (1) имеет максимальное число корней. Рассуждаем так: сравнение

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

имеет p корней.

Так как все коэффициенты остатка $\varphi(x)$ кратны p, то сравнение

$$\varphi(x) \equiv 0 \pmod{p}$$

также имеет p корней.

В виду этого и сравнение

$$x^p - x - \psi(x) \equiv 0 \pmod{p} \tag{3}$$

имеет p корней.

Принимая во внимание тождество (2), сравнение (3) заменяем сравнением

$$f(x)\psi(x) \equiv 0 \pmod{p}, \tag{4}$$

которое также должно иметь p корней.

Так как p-й степени сравнение (4) имеет p корней, а его левая часть распадается на два многочлена $f(x)$ и $\psi(x)$ соответственно степеням n и $p-n$, то каждое из сравнений

$$f(x)\equiv 0 \pmod p \text{ и } \psi(x)\equiv 0 \pmod p$$

должно иметь максимальное число корней.

Отсюда следует, что сравнение (1) имеет n корней, а это нам и нужно было доказать.

Пример. Показать, что сравнение

$$x^3+2x^2-x-2\equiv 0 \pmod 5 \qquad (1)$$

имеет три корня.

Решение. Делим x^5-x на x^3+2x^2-x-2; в остатке получаем $-10x^2+10$. Коэффициенты остатка делятся на 5. Следовательно, наше сравнение имеет три корня, в чем можно убедиться, испытывая числа 0, 1, 2, 3, 4, — представителей классов чисел по модулю 5. Видим, что сравнению (1) удовлетворяют числа 1, 3, 4. Итак,

$$\left.\begin{aligned} x&\equiv 1\\ x&\equiv 3\\ x&\equiv 4 \end{aligned}\right\} \pmod 5.$$

Таблица простых чисел,

не превосходящих 6000

2	**179**	**419**	**661**	**947**	**1229**	**1523**	**1823**	**2131**
3	181	421	673	953	1231	1531	1831	2137
5	191	431	677	967	1237	1543	1847	2141
7	193	433	683	971	1249	1549	1861	2143
11	197	439	691	977	1259	1553	1867	2153
13	199	443	701	983	1277	1559	1871	2161
17	211	449	709	991	1279	1567	1873	2179
19	223	457	719	997	1283	1571	1877	2203
23	227	461	727	1009	1289	1579	1879	2207
29	229	463	733	1013	1291	1583	1889	2213
31	**233**	**467**	**739**	**1019**	**1297**	**1597**	**1901**	**2221**
37	239	479	743	1021	1301	1601	1907	2237
41	241	487	751	1031	1303	1607	1913	2239
43	251	491	757	1033	1307	1609	1931	2243
47	257	499	761	1039	1319	1613	1933	2251
53	263	503	769	1049	1321	1619	1949	2267
59	269	509	773	1051	1327	1621	1951	2269
61	271	521	787	1061	1361	1627	1973	2273
67	277	523	797	1063	1367	1637	1979	2281
71	281	541	809	1069	1373	1657	1987	2287
73	**283**	**547**	**811**	**1087**	**1381**	**1663**	**1993**	**2293**
79	293	557	821	1091	1399	1667	1997	2297
83	307	563	823	1093	1409	1669	1999	2309
89	311	569	827	1097	1423	1693	2003	2311
97	313	571	829	1103	1427	1697	2011	2333
101	317	577	839	1109	1429	1699	2017	2339
103	331	587	853	1117	1433	1709	2027	2341
107	337	593	857	1123	1439	1721	2029	2347
109	347	599	859	1129	1447	1723	2039	2351
113	349	601	863	1151	1451	1733	2053	2357
127	**353**	**607**	**877**	**1153**	**1453**	**1741**	**2063**	**2371**
131	359	613	881	1163	1459	1747	2069	2377
137	367	617	883	1171	1471	1753	2081	2381
139	373	619	887	1181	1481	1759	2083	2383
149	379	631	907	1187	1483	1777	2087	2389
151	383	641	911	1193	1487	1783	2089	2393
157	389	643	919	1201	1489	1787	2099	2399
163	397	647	929	1213	1493	1789	2111	2411
167	401	653	937	1217	1499	1801	2113	2417
173	409	659	941	1223	1511	1811	2129	2423

2437	**2833**	**3259**	**3659**	**4073**	**4507**	**4943**	**5393**	**5801**
2441	2837	3271	3671	4079	4513	4951	5399	5807
2447	2843	3299	3673	4091	4517	4957	5407	5813
2459	2851	3301	3677	4093	4519	4967	5413	5821
2467	2857	3307	3691	4099	4523	4969	5417	**5827**
2473	2861	3313	3697	4111	4547	4973	5419	5839
2477	2879	3319	3701	4127	4549	4987	5431	5843
2503	2887	3323	3709	4129	4561	4993	5437	5849
2521	2897	3329	3719	4133	4567	4999	5441	5851
2531	2903	3331	3727	4139	4583	5003	5443	5857
2539	**2909**	**3343**	**3733**	**4153**	**4591**	**5009**	**5449**	**5861**
2543	2917	3347	3739	4157	4597	5011	5471	5867
2549	2927	3359	3761	4159	4603	5021	5477	5869
2551	2939	3361	3767	4177	4621	5023	5479	5879
2557	2953	3371	3769	4201	4637	5039	5483	5881
2579	2957	3373	3779	4211	4639	5051	5501	5897
2591	2963	3389	3793	4217	4643	5059	5503	5903
2593	2969	3391	3797	4219	4649	5077	5507	5923
2609	2971	3407	3803	4229	4651	5081	5519	5927
2617	2999	3413	3821	4231	4657	5087	5521	5939
2621	**3001**	**3433**	**3823**	**4241**	**4663**	**5099**	**5527**	**5953**
2633	3011	3449	3833	4243	4673	5101	5531	5981
2647	3019	3457	3847	4253	4679	5107	5557	5987
2657	3023	3461	3851	4259	4691	5113	5563	
2659	3037	3463	3853	4261	4703	5119	5569	
2663	3041	3467	3863	4271	4721	5147	5573	
2671	3049	3469	3877	4273	4723	5153	5581	
2677	3061	3491	3881	4283	4729	5167	5591	
2683	3067	3499	3889	4289	4733	5171	5623	
2687	3079	3511	3907	4297	4751	5179	5639	
2689	**3083**	**3517**	**3911**	**4327**	**4759**	**5189**	**5641**	
2693	3089	3527	3917	4337	4783	5197	5647	
2699	3109	3529	3919	4339	4787	5209	5651	
2707	3119	3533	3923	4349	4789	5227	5653	
2711	3121	3539	3929	4357	4793	5231	5657	
2713	3137	3541	3931	4363	4799	5233	5659	
2719	3163	3547	3943	4373	4801	5237	5669	
2729	3167	3557	3947	4391	4813	5261	5683	
2731	3169	3559	3967	4397	4817	5273	5689	
2741	3181	3571	3989	4409	4831	5279	5693	
2749	**3187**	**3581**	**4001**	**4421**	**4861**	**5281**	**5701**	
2753	3191	3583	4003	4423	4871	5297	5711	
2767	3203	3593	4007	4441	4877	5303	5717	
2777	3209	3607	4013	4447	4889	5309	5737	
2789	3217	3613	4019	4451	4903	5323	5741	
2791	3221	3617	4021	4457	4909	5333	5743	
2797	3229	3623	4027	4463	4919	5347	5749	
2801	3251	3631	4049	4481	4931	5351	5779	
2803	3253	3637	4051	4483	4933	5381	5783	
2819	3257	3643	4057	4493	4937	5387	5791	

ОГЛАВЛЕНИЕ

Предисловие 1

Глава четвертая

Простые числа

65— 69. Классификация натуральных чисел. Число простых чисел бесконечно велико. Решето Эратосфена. Функция $\pi(n)$ 3

70— 77. Как узнать, есть ли данное число простое или составное. Разложение составного числа на простых сомножителей. Однозначность разложения. Нахождение общего наибольшего делителя и общего наименьшего кратного нескольких чисел, разложенных на простых сомножителей 6

Глава пятая

Числовые функции

78— 85. Определение числовой функции. Собственные и несобственные делители числа. Число делителей данного числа. Сумма делителей данного числа. Совершенные и дружественные числа. Функция Эйлера. Доказательство теоремы $\varphi(mn) = \varphi(m)\,\varphi(n)$, если m и n числа взаимно простые 14

Глава шестая

Сравнения и их свойства

86—103. Определения. Сравнимость всякого числа с самим собою. Равноостаточные числа. Сравнения с одним и тем же модулем можно почленно складывать, вычитать и умножать. Члены сравнения можно умножать на одно и то же число; — возвышать в одну и ту же целую положительную степень. Члены сравнения и модуль можно умножать на одно и то же натуральное число. Члены сравнения можно сокращать на их общего наибольшего делителя, взаимно простого с модулем. Члены сравнения и модуль можно сокращать на их общего наибольшего делителя. Свойство чисел, сравнимых между собою по нескольким попарно простым модулям. Если числа a и b сравнимы между собою по модулю k, то значения функции $f(x)$ при $x=a$ и $x=b$ также сравнимы между собою по модулю k 24

Глава седьмая

Признаки делимости чисел

104—112. Понятие о системе счисления. Различные системы счисления. Переход от одной системы счисления к системе с другим основанием. Признаки делимости на 2, 5, 4, 8, 3, 9, 10, 125, 7, 11 . 3

Глава восьмая

Распределение чисел на классы по данному модулю. Теоремы Ферма и Эйлера

113—123. Распределение чисел на классы по данному модулю. Полная система вычетов по данному модулю. Приведенная система вычетов по данному модулю. Свойства чисел одного и того же класса. Теорема Ферма и ее следствие. Теорема Эйлера 3

Глава девятая

Сравнения первой степени

124—130. Определения. Виды сравнений первой степени и способы их решения. Система сравнений. Упражнения 46

Глава десятая

Сравнение высших степеней. Теорема Вильсона

131—134. Определения. Исключение из сравнения членов с коэффициентами, кратными модуля сравнения. Замена коэффициентов сравнения их наименьшими положительными вычетами по модулю сравнения p. Преобразование данного сравнения в равносильное ему сравнение, коэффициент высшего члена которого равен единице .

135—139. Представление левой части сравнения n-й степени, имеющего n корней, в виде произведения n линейных множителей. Сравнение n-й степени не может иметь более n корней. Случай, когда сравнение, левая часть которого есть функция n-й степени, имеет более n корней. Теорема Вильсона . . . . . .

140—144. Если сравнение n-й степени $f(x) \equiv 0 \pmod{p}$ имеет n корней и $f(x) = \psi_1(x)\,\psi_2(x)$, то каждое из двух сравнений $\psi_1(x) \equiv 0 \pmod{p}$ и $\psi_2(x) \equiv 0 \pmod{p}$ имеет столько корней, сколько единиц в показателе его степени. Приведение сравнения к виду, в котором степень его меньше модуля. Что значит „сравнение имеет максимальное число корней". Признак, по которому узнают, имеет ли сравнение максимальное число корней или нет 58

Приложение

Таблица простых чисел, не превосходящих 6000 73

Отв. редактор *А. А. Назаров.* Техредактор *А. А. Веселовская.*

ГЕ4200. Сдано в набор 29/XII 1940 г. Подписано к печати 17/III 1941 г. Формат 60×84/16. Объем 4¾ п. л. 2⅜ б. л. 5 уч.-изд. л. 48000 зн. в п. л. Тираж 1500 экз.

Вологда, тип. изд-ва „Красный Север", ул. К. Маркса, 70. Заказ 4285.