Проф. Д. Ф. ЕГОРОВ

ЭЛЕМЕНТЫ
ТЕОРИИ ЧИСЕЛ

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
МОСКВА • 1923 • ПЕТРОГРАД

Проф. Д. Ф. ЕГОРОВ

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
МОСКВА 1923 ПЕТРОГРАД

ТИПОГРАФИЯ
„КРАСНЫЙ ПЕЧАТНИК“
ПЕТРОГРАД
Международный, 75

Гиз № 3358.
5000 экз.

ПРЕДИСЛОВИЕ.

Предлагаемая книга имеет в своей основе курс лекций по теории чисел, которые я в течение ряда лет читал в Московском Университете.

Она содержит почти исключительно только самые основные результаты, вернее даже элементы теории чисел, как это можно усмотреть из самого заглавия; только последняя глава выходит несколько из области элементов и дает краткий очерк основных результатов арифметики многочленов, но и то я ограничиваюсь здесь почти всецело теми положениями теории, которые представляют полную аналогию с соответствующими теоремами элементарной арифметики и теории сравнений.

Я полагаю, что знакомство с этими результатами полезно не только само по себе, но и для лучшего освещения соответствующих положений элементарной теории чисел.

Проф. Д. Егоров.

ВВЕДЕНИЕ.

Теория чисел, как показывает самое название этой дисциплины, имеет дело с числами. Притом, в отличие от алгебры и высшего анализа, которые тоже имеют дело с числами, она есть теория *самих чисел*. Рассуждения анализа вращаются в *области чисел*. Эта область есть та область, в которой производятся операции, в которой ведутся рассуждения, но не сами числа изучаются, и притом все числа являются равноправными. Если мы проследим, как постепенно обобщается понятие о числе в математике, то увидим, что при этом последовательном обобщении все более и более стираются индивидуальные особенности чисел и, в конце концов, получается некоторая однородная область, которую можно привести во взаимно-однозначное соответствие с другой областью математических изысканий, с областью, с которой имеет дело геометрия,—с областью точек.

Теория чисел изучает самые числа, и существенной особенностью ее является именно то, что она не стирает различия между числами при дальнейшем обобщении понятия о числе. Так, дроби, которые впервые вводит элементарная арифметика, уже в элементарной алгебре при буквенном обозначении чисел, перестают отличаться от целых чисел; между тем теория чисел делает строгое различие между целым и дробным, и основным понятием в теории чисел является целое число.

Таким образом натуральный ряд 1, 2, 3, 4, 5, ..., дополненный нулем и продолженный в обратную сторону отрицательными числами, т.-е. ряд

... —5, —4, —3, —2, —1, 0, 1, 2, 3, 4, 5; ...

является той областью, в которой вращаются рассуждения теории чисел, по крайней мере ее элементарной части, ибо некоторые из высших ее отделов посвящены изучению иррациональных чисел.

Что касается самого натурального ряда, то его можно считать непосредственно данным, вводя затем отрицательные и дробные числа путем формального обобщения, или же и его возможно построить помощью ряда аксиом, хотя бы, например, аксиом, предложенных итальянским ученым Пеано.

Построив натуральный ряд, можно затем перейти к определению арифметических действий, опираясь на те же аксиомы, и таким образом построить на строгих основаниях всю арифметику. Предполагая все это выполненным, мы в дальнейшем обратимся непосредственно к вопросу о делимости чисел, который, входя в обычную систему изложения арифметики, является вместе с тем первым и основным вопросом теории чисел.

ГЛАВА ПЕРВАЯ.

О делимости чисел.

Если имеем два целых [1]) числа m и n и если $m = qn$, где q тоже целое число, то говорят, что m делится на n, и обозначают это так: $m \mid n$; n называют делителем m, а m — кратным n; очевидно q есть также делитель m; q и n называются дополнительными делителями. В вопросах делимости мы можем ограничиться рассмотрением только положительных чисел и только положительных их делителей. В самом деле на-ряду с равенством

$$m = qn$$

имеем

$$-m = q \,.\, (-n) = (-q) \,.\, n$$

и

$$m = (-q) \,.\, (-n)$$

Отсюда ясно, во-первых, что на-ряду с n делителем m является и $-n$, так что одновременно $\pm n$ служат делителями m, и можно ограничиться положительными делителями, т. к. отрицательные равны положительным делителям, взятым со знаком минус; во-вторых, ясно, что делители $-m$ совпадают с делителями m, так что можно ограничиться делителями положительных чисел.

---

[1]) В дальнейшем везде под термином „число“ будем разуметь „целое число“.

Выведем основное в теории делимости равенство.

Пусть n положительное число и m какое-нибудь число. Рассмотрим ряд кратных числа n

$$\ldots -5n, -4n, -3n, -2n, -n, 0, n, 2n, 3n, 4n, 5n, \ldots \quad (1)$$

и натуральный ряд

$$\ldots -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \ldots \quad (2)$$

Всякое число m необходимо находится в ряде (2), а т. к. ряд (1) есть часть ряда (2), то число m занимает, вообще говоря, в ряде (2) место между двумя последовательными членами ряда (1), напр., между qn и $(q+1)n$, а раз так, то m единственным образом представляется в виде

$$m = qn + r,$$

где $0 \leqslant r < n$; r указывает, на сколько мест следует в ряду (2) отойти от qn, чтобы получить число m. Для $r = 0$ имеем $m = qn$ и след. m встречается в ряде (1).

Число q есть, очевидно, целая часть частного, получаемого от деления m на n:

$$\frac{m}{n} = q + \frac{r}{n}$$

Употребляют такие обозначения:

$$q = E\frac{m}{n} \text{ — обозначение Лежандра}$$

$$q = \left[\frac{m}{n}\right] \text{ — обозначение Гаусса.}$$

Вообще если x какое-либо действительное число, то через $[x]$ обозначают целое число, удовлетворяющее неравенствам

$$[x] \leqslant x < [x] + 1.$$

Например $\quad [\sqrt{2}] = 1, \quad [-\sqrt{5}] = -3.$

§ 1. Основные теоремы о делимости.

В дальнейшем для сокращения часто будем пользоваться выше введенным обозначением вертикальной черты $(a \mid d)$ между двумя числами для обозначения того, что первое число (a) делится на второе (d). Если кроме того условиться заключение теоремы от условий ее отделять горизонтальной чертой, то 1-я теорема полно и сокращенно запишется так:

1-я теорема.

Если два числа делятся на одно и то же третье, то их сумма и разность делятся на это же число.

$$\frac{a \mid d;\ b \mid d}{(a \pm b) \mid d}$$

Доказательство. Имеем

$$a = dq_1,\ b = dq_2.$$

Складывая или вычитая, получаем

$$a \pm b = d\ (q_1 \pm q_2)$$

и следовательно

$$a \pm b \mid d$$

Очевидно теорема справедлива и для алгебраической суммы любого числа слагаемых; она может быть доказана последовательно. Так, пусть

$$a \mid d,\ b \mid d,\ c \mid d$$

Тогда по доказанному $(a+b) \mid d$ и, применяя еще раз ту же теорему, имеем и для $a+b+c=(a+b)+c$

$$(a+b+c) \mid d$$

2-я теорема.

Если первое число делится на второе, а второе на третье, то первое делится на третье.

$$\frac{a \mid b;\ b \mid c}{a \mid c}$$

Доказательство. Имеем

$$a = bq;\ b = cq'$$

Следовательно

$$a = cq'q, \text{ откуда}$$
$$a \mid c.$$

§ 2. Собственные и несобственные делители, понятие об общем наибольшем делителе и общем наименьшем кратном.

Всякое число, очевидно, делится на единицу и на самого себя. Эти делители называются несобственными делителями, в отличие от других, если таковые существуют, которые называются собственными.

Так как каждый делитель числа не может превышать этого числа, то число делителей данного числа a конечно, и всех их найдем, испытывая поочередно числа ряда $1, 2, 3, \ldots, a$. Так делителей числа 12 найдем, испытывая, на какие из чисел 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 делится 12. Таким образом найдем делителей 12-ти: 1, 2, 3, 4, 6, 12.

Пусть имеем два числа a и b. Найдем по предыдущему всех делителей

$$1, d, d', d'', \ldots, a$$

числа a и всех делителей

$$1, \delta, \delta', \delta'', \ldots, b$$

числа b. Сравнивая эти два ряда чисел, можем отобрать из них всех общих делителей чисел a и b. Пусть, в возрастающем порядке, они будут

$$1, d_1, d_2, \ldots, d_k.$$

Наибольший из них d_k называется общим наибольшим делителем чисел a и b и обозначается:

$$d_k = D\ (a, b).$$

Совершенно так же можем найти всех общих делителей и общий наибольший делитель трех и более чисел.

Например, пусть имеем три числа 12, 18, 30. Все делители 12-ти, 18-ти 30-ти, суть:

1, 2, 3, 4, 6, 12
1, 2, 3, 6, 9, 18
1, 2, 3, 5, 6, 10, 15, 30.

Общие делители 12-ти, 18-ти, 30-ти суть:

1, 2, 3, 6.

Общий наибольший делитель есть 6:

$D\ (12, 18, 30) = 6.$

Имея два числа a и b, можем искать число, которое одновременно делится на a и на b и которое можно назвать общим кратным чисел a и b. Очевидно, произведение ab есть одно из общих кратных a и b; ясно также, что всякое кратное общего кратного есть общее кратное. Наименьшее из общих кратных называется общим наименьшим кратным и обозначается $m\ (a, b)$. Ясно, что эти определения распространяются на три и более чисел.

§ 3. Понятие о модуле и его свойства.

Модулем называется всякая совокупность чисел, обладающая тем свойством, что сумма или разность двух чисел совокупности принадлежит к той же совокупности.

Докажем следующие свойства модуля:

1) Всякий модуль содержит число 0. В самом деле, пусть a есть какое-нибудь число модуля; согласно определению, к тому же модулю принадлежит и разность $a - a = 0$, и положение наше доказано.

Легко видеть, что одно число 0 образует модуль, ибо $0 + 0 = 0$, $0 - 0 = 0$. Оставляя в стороне этот тривиальный случай, можем высказать второе свойство:

2) Всякий модуль содержит как положительные, так и отрицательные числа.

В самом деле, если модуль содержит какое-нибудь число m, то так как он содержит еще и нуль, то к модулю принадлежит также число $0 - m = -m$.

3) Всякий модуль состоит из совокупности чисел кратных наименьшего положительного числа модуля.

В самом деле, выбираем из всевозможных положительных чисел модуля наименьшее число n и пусть m какое-нибудь число модуля. В силу основного равенства

$$m = qn + r, \text{ где } 0 \leqslant r < n.$$

Число $qn = n + n + n + \cdots + n$ есть число модуля, следовательно и

$$r = m - qn$$

есть также число модуля; но $r < n$, а между тем n — наименьшее положительное число модуля; поэтому предположение $r > 0$ ведет к противоречию и следовательно $r = 0$, откуда $m = qn$ — есть кратное числа n. В модуль, согласно определению, входят все числа рядов

$$n,\ n+n,\ n+n+n,\ \cdots$$
$$0,\ -n,\ -n-n,\ -n-n-n,\ \cdots$$

т.-е. все кратные числа n. Обратно ясно, что совокупность всех кратных какого-нибудь числа образует модуль. Таким образом модуль и совокупность кратных одного числа есть одно и то же.

Например, совокупность четных чисел

$$0,\ \pm 2,\ \pm 4,\ \pm 6,\ \cdots$$

есть модуль.

Совокупность всех чисел

$$\cdots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \cdots$$

есть также модуль.

§ 4. Приложение свойств модуля к выводу свойств общего наибольшего делителя.

Пусть даны два числа a и b. Рассмотрим совокупность чисел вида $ax+by$, где x и y, независимо одно от другого, принимают всевозможные целые значения: 0, ± 1, ± 2, ± 3, $\cdots$. В эту совокупность входят, например, нуль (при $x=0$, $y=0$), число a (при $x=1$, $y=0$) и число b (при $x=0$, $y=1$). Легко видеть, что совокупность эта есть модуль.

В самом деле, если ax_1+by_1 и ax_2+by_2 два числа совокупности, то и

$$ax_1+by_1 \pm (ax_2+by_2) = a(x_1 \pm x_2)+b(y_1 \pm y_2)$$

есть число той же совокупности, получаемое при $x=x_1 \pm x_2$, $y=y_1 \pm y_2$.

Раз так, то эта совокупность эквивалентна совокупности кратных числа n — наименьшего положительного числа совокупности:

$$ax+by \sim nz.$$

Пусть теперь

$$D(a, b)=\delta.$$

Так как a и b числа модуля, то $a \mid n$ и $b \mid n$; следовательно n есть общий делитель a и b, а т. к. δ — общий наибольший делитель, то

$$n \leqslant \delta.$$

Но с другой стороны n есть одно из чисел модуля и значит есть число вида $ax+by$ при некоторых значениях x и y. Пусть

$$n=a\xi+b\eta.$$

Отсюда, т. к. $a \mid \delta$ и $b \mid \delta$, следует, что и $n \mid \delta$ и следовательно

$$n \geqslant \delta.$$

Сопоставляя два результата, имеем

$$n=\delta.$$

Итак, наименьшее положительное число модуля вида $ax+by$ есть общий наибольший делитель a и b и

$$ax+by \sim D(a, b) \cdot z.$$

Отсюда можем получить такую теорему:

Если $D(a, b)=\delta$, то можно подобрать такие два целых числа ξ и η, что

$$\delta = a\xi + b\eta.$$

Это весьма важное равенство мы вывели, пользуясь понятием о модуле; но возможно, как увидим дальше, получить его и иначе, на основании алгорифма Эвклида для нахождения общего наибольшего делителя. Из этого равенства мы тотчас же выведем основное свойство общего наибольшего делителя: всякий общий делитель двух данных чисел есть делитель общего наибольшего делителя.

В самом деле, пусть $a \mid d$ и $b \mid d$; но $\delta = a\xi + b\eta$, следовательно и $\delta \mid d$.

Обратная теорема очевидна (всякий делитель общего наибольшего делителя есть общий делитель двух данных чисел); таким образом общий наибольший делитель можно бы определить как такой общий делитель, который делится на всех прочих общих делителей. Это определение и полагается в основу теории общего наибольшего делителя в высших отделах теории чисел.

Если общий наибольший делитель двух чисел a и b $D(a, b)=1$, то эти числа не имеют других общих делителей кроме 1-цы; такие числа называются взаимно-простыми.

Докажем, что частное от деления двух чисел на их общего наибольшего делителя суть числа взаимно-простые.

Пусть $D(a, b)=\delta$; $a=a'\delta$, $b=b'\delta$. Допустим, что $D(a', b') \neq 1$ и пусть $D(a', b')=d>1$; тогда $a'=a''d$, $b'=b''d$ и $a=a''d\delta$, $b=b''d\delta$; следовательно $a \mid d\delta$, $b \mid d\delta$ и число $d\delta$, которое больше δ, было бы общим делителем

чисел a и b, что противоречит предположению, что δ есть общий наибольший делитель.

Предположим, что a и b числа взаимно-простые, так что $D(a, b) = 1$. Тогда, в силу предыдущего, будет существовать равенство

$$1 = a\xi + b\eta.$$

Умножив обе части на некоторое число c, имеем

$$ac\xi + bc\eta = c.$$

Предположим, что $ac \mid d$ и $b \mid d$; тогда на основании предшествующего равенства и $c \mid d$, и мы получаем теорему:

Если произведение ac и число b имеют общего делителя d, и если a и b взаимно-просты, то второй фактор c делится на d.

Важный частный случай получим, предположив $d = b$:

Если произведение ac делится на b и если первый фактор a — взаимно-простой с b, то второй фактор c делится на b.

Следствие. Пусть $D(a, b) = 1$ и $D(c, b) = 1$; тогда и $D(ac, b) = 1$.

Докажем от противного. Предположим, что $D(ac, b) = \delta > 1$; но тогда $ac \mid \delta$ и $b \mid \delta$ и т. к. $D(a, b) = 1$, то на основании ранее данной теоремы $c \mid \delta$. Таким образом b и c имеют общего делителя $\delta > 1$, что противоречит предположению $D(c, b) = 1$.

Итак, имеем следствие: если два числа взаимно-просты с третьим, то и их произведение тоже взаимно-просто с этим числом.

Эту теорему можно обобщить:

Пусть имеем два конечных ряда чисел

$$a, b, c, \ldots \text{ и } a', b', c', \ldots$$

и пусть каждое число первого ряда взаимно-просто с каждым числом второго ряда, т.-е.

$$D(a, a') = 1, \quad D(a, b') = 1, \quad D(a, c') = 1, \ldots$$
$$D(b, a') = 1, \quad D(b, b') = 1, \quad D(b, c') = 1, \ldots$$

Тогда по предыдущему $D(ab,\ a') = 1$. Сопоставляя

$$D(ab,\ a') = 1,\ D(c,\ a') = 1,$$

имеем далее

$$D(abc,\ a') = 1.$$

Идя так далее и далее, получим

$$D(abc\ldots,\ a') = 1,$$

где $abc\ldots$ есть произведение всех чисел первого ряда. Совершенно так же получим

$$D(abc\ldots,\ b') = 1$$
$$D(abc\ldots,\ c') = 1.$$

Далее из двух равенств

$$D(abc\ldots,\ a') = 1,\quad D(abc\ldots,\ b') = 1,$$

получим на том же основании

$$D(abc\ldots,\ a'b') = 1.$$

Сопоставляя этот результат с

$$D(abc\ldots,\ c') = 1,$$

получим

$$D(abc\ldots,\ a'b'c') = 1$$

и так далее. Окончательно имеем

$$D(abc\ldots,\ a'b'c'\ldots) = 1,$$

т.-е. если имеем два ряда чисел попарно взаимно-простых, то произведение всех чисел первого ряда взаимно-просто с произведением всех чисел второго ряда.

Полагая $a = b = c = \ldots$ и $a' = b' = c' = \ldots$, получаем следствие:

$$\text{если } D(a,\ b) = 1, \text{ то и } D(a^\alpha,\ b^\beta) = 1.$$

Рассмотрим общий наибольший делитель нескольких чисел. Определение его было дано выше, и

ясно, что величина его не зависит от порядка, в котором мы рассматриваем данные числа $a, b, c, \ldots u$.

Пусть $D(a, b) = \delta$. Всякий общий делитель a и b есть делитель δ и обратно—всякий делитель δ есть общий делитель a и b.

Отсюда ясно, что всякий общий делитель чисел

$$a, b, c, \ldots u \tag{1}$$

есть общий делитель чисел

$$\delta, c, \ldots u \tag{2}$$

и обратно; а следовательно в частности общий наибольший делитель чисел ряда (1) есть общий наибольший делитель и чисел ряда (2):

$$D(a, b, c, \ldots, u) = D(\delta, c, \ldots, u) = D(D(a, b), c, \ldots, u).$$

Далее найдем $D(\delta, c) = \delta'$, и тогда

$$D(a, b, c, d, \ldots, u) = D(\delta, c, d, \ldots, u) = D(\delta', d, \ldots, u).$$

Продолжая процесс далее, дойдем до $D(\delta^{(k)}, u)$, и таким образом нахождение общего наибольшего делителя нескольких чисел сводится к нахождению общего наибольшего делителя двух чисел.

Например

$$D(27, 12, 30, 126) = D(D(27, 12), 30, 126) = D(3, 30, 126) =$$
$$= D(D(3, 30), 126) = D(3, 126) = 3.$$

Итак достаточно уметь находить общего наибольшего делителя двух чисел. Для его нахождения существует метод, данный Эвклидом.

Докажем предварительно теорему: Общий наибольший делитель делимого и делителя равен общему наибольшему делителю делителя и остатка.

Пусть от деления a на b получаем в частном q и в остатке r. Имеем соотношение $a = bq + r$, из которого ясно что если $a \mid d$ и $b \mid d$, то и $r \mid d$ и также если $b \mid d$ и $r \mid d$,

то и $a \mid d$. Таким образом общие делители a и b суть в то же время общие делители b и r и обратно, а потому совпадают и общие наибольшие делители этих пар чисел:

$$D(a,\ b) = D(b,\ r).$$

Для нахождения общего наибольшего делителя двух чисел a и b применяется метод последовательного деления: делим a на b, затем b на остаток r_1, затем r_1 на остаток r_2 последнего деления и так далее

$$\begin{array}{c|c|c|c|c|c} \overbrace{a}^{q_1} & \overbrace{b}^{q_2} & \overbrace{r_1}^{q_3} & r_2 \ldots & \overbrace{r_{n-1}}^{q_n} & r_n. \\ r_1 & r_2 & r_3 & & 0 & \end{array}$$

При этом $b > r_1 > r_2 > r_3 \ldots$, а так как ряд убывающих целых чисел (начиная с b) не может быть бесконечным, то процесс должен закончиться, и какой-нибудь остаток r_{n+1} должен равняться нулю, так что имеем равенства

$$\begin{aligned} a &= bq + r_1, \\ b &= r_1 q_1 + r_2, \\ r_1 &= r_2 q_2 + r_3, \\ &\ldots\ldots\ldots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

В силу доказанной теоремы

$$\begin{aligned} D(a,\ b) = D(b,\ r_1) = D(r_1,\ r_2) = D(r_2,\ r_3) = \ldots = \\ = D(r_{n-2},\ r_{n-1}) = D(r_{n-1},\ r_n). \end{aligned}$$

Но на основании последнего равенства $r_{n-1} \mid r_n$ и следовательно $D(r_{n-1},\ r_n) = r_n$. Таким образом $D(a,\ b) = r_n$, т.-е. общим наибольшим делителем будет последний остаток отличный от нуля [1]).

---

[1]) Определяя r_1 из 1-го равенства, вставляем во 2-е и из него находим и т. д. Наконец, из предпоследнего найдем $r_n = D(a,\ b) = a\xi + b\eta$, r_2 где ξ и η — целые числа.

§ 5. Нахождение общего наименьшего кратного двух и нескольких чисел.

Пусть даны два числа a и b и пусть $D(a, b) = \delta$ и $a = \delta\alpha$, $b = \delta\beta$, при чем, как известно, $D(\alpha, \beta) = 1$. Ищем общее кратное a и b. Как кратное a оно имеет вид $ka = k\alpha\delta$. Как кратное b оно должно делиться на $b = \beta\delta$:

$$k\alpha\delta \mid \beta\delta,$$

или, по сокращении на δ,

$$k\alpha \mid \beta.$$

Так как $D(\alpha, \beta) = 1$, то, в силу доказанного выше, необходимо $k \mid \beta$ и следовательно $k = \beta z$. Таким образом всякое кратное a и b имеет вид

$$\alpha\beta\delta z = \frac{\delta\alpha \cdot \delta\beta}{\delta} \cdot z = \frac{ab}{\delta} \cdot z,$$

где z—любое целое число. Общее наименьшее кратное получим, давая z наименьшее значение, т.-е. полагая $z = 1$. Таким образом

$$m(a,b) = \alpha\beta\delta = \frac{ab}{\delta} = \frac{a \cdot b}{D(a,b)}.$$

Эта формула дает возможность находить наименьшее кратное любых двух чисел, а предшествующая формула дает нам теорему: всякое общее кратное двух чисел есть кратное общего наименьшего кратного. Обратная теорема очевидна.

Можно распространить эту теорему и на случай общих кратных нескольких чисел, и проще всего получить этот результат, заметив, что совокупность общих кратных есть, очевидно, модуль, так как сумма и разность общих кратных есть общее кратное, а раз так, то эта совокупность сводится к совокупности кратных наименьшего положительного числа модуля, т.-е. общего наименьшего кратного.

Пусть теперь имеем ряд чисел $a, b, c, \ldots, u$. Всякое общее кратное чисел a и b есть кратное $m(a,b)$ и обратно:

всякое кратное $m(a, b)$ есть общее кратное a и b. Отсюда ясно, что всякое общее кратное чисел

$$a, b, c, \ldots, u$$

есть общее кратное чисел

$$m(a, b), c, \ldots, u$$

и обратно, а следовательно и наименьшие общие кратные этих двух рядов чисел совпадают, т.-е.

$$m(a, b, c, d, \ldots, u) = m(m(a, b), c, d, \ldots, u).$$

Повторяя это рассуждение, получаем

$$m(a, b, c, d, \ldots, u) = m(m(a, b), c, d, \ldots, u) = \\ = m(m(m(a, b), c), d, \ldots, u) \text{ и т. д.}$$

В конце концов, дело сводится к нахождению общего наименьшего кратного двух чисел.

Например

$m(9, 12, 15, 8) = m(m(9, 12), 15, 8) = m(36, 15, 8) = m(m(36, 15), 8) = \\ = m(180, 8) = 360.$

Все другие общие кратные 9, 12, 15, 8 суть кратные 360-ти.

ГЛАВА ВТОРАЯ.

Простые и составные числа. Разложение составного числа на простых множителей.

Выше мы упоминали о разделении делителей числа на собственные и несобственные. Если число a имеет собственного делителя d (отличного от 1-цы и от a), то $a = d\delta$, где и d и δ отличны от 1 и от a, и таким образом a разлагается на произведение двух множителей отличных от 1-цы и от a. Если же число a не имеет собственных делителей, то подобное разложение невозможно, т. к. обратно из $a = d\delta$ следовало бы $a \mid d$, и если d отлично от 1-цы и от a, мы бы имели собственный делитель числа a. Единственное возможное разложение для такого числа a есть $a = 1$. a, которое самоочевидно, но не есть собственное разложение. Таким образом все числа делятся на две категории: числа, имеющие собственных делителей и числа, не имеющие таковых. Первые суть числа разложимые или составные, вторые — неразложимые или простые или первоначальные.

Например, 6 есть число составное (6=2.3), а 11 — число первоначальное.

Рассмотрим первоначальное число p и какое-нибудь число a. Так как единственные делители p суть 1-ца и p, то общий наибольший делитель a и p может равняться только или p или 1. Если $D(a, p) = p$, то $a \mid p$; если $D(a, p) = 1$, то a и p — взаимно-просты и a не делится на p

Итак, всякое число, не делящееся на первоначальное число, с ним взаимно-просто: если a не делится на p, то $D(a, p) = 1$.

Докажем вторую теорему: если произведение двух чисел делится на первоначальное число, то один из факторов делится на это число.

Пусть $ab \mid p$. Если $a \mid p$, то теорема доказана; если a не делится на p, то, согласно предыдущему, $D(a, p) = 1$ и, применяя теорему, доказанную выше в теории общего наибольшего делителя, заключаем, что $b \mid p$.

Ясно, что теорема распространяется на произведения трех и более факторов. Так, если $abc \mid p$, то, рассматривая abc как произведение $a(bc)$ двух факторов, заключаем, что или $a \mid p$ или $bc \mid p$, откуда в свою очередь следует, что или $b \mid p$ или $c \mid p$.

Примечание. В высших отделах теории чисел приходится различать понятия неразложимых чисел и простых чисел. Неразложимым называют число не имеющее собственных делителей, простым — число, обладающее свойством, выраженным в последней теореме, т.-е. число, на которое произведение может делиться только тогда, когда на него делится один из факторов. В области целых рациональных чисел оба понятия совпадают. Теорема, выше доказанная, утверждает, что всякое неразложимое число есть простое. Можно так же доказать, что всякое простое число неразложимо. В самом деле, пусть простое число $p = \pi_1 \pi_2$, где π_1 и π_2 — числа отличные от 1 и от p. Но тогда $\pi_1 \pi_2 \mid p$ и по свойству простого числа необходимо или $\pi_1 \mid p$ или $\pi_2 \mid p$, что невозможно. т. к. и π_1 и π_2 меньше p.

Теорема. Всякое составное число имеет первоначального делителя.

Пусть имеем составное число m; оно, кроме 1 и m, имеет еще собственных делителей; возьмем из них наименьший d; легко видеть, что d есть необходимо первоначальное число. В самом деле, если бы d было составным числом, то имело бы собственных делителей, и мы бы имели например $d \mid a$, где $a > 1$ и $a < d$; но тогда бы и m делилось на a, и у m оказался бы собственный делитель a, меньший d противно предположению.

Основываясь на этой теореме, докажем, что **всякое составное число разлагается на произведение первоначальных множителей.**

Пусть мы имеем составное число m. По доказанному оно имеет хотя бы одного первоначального делителя p_1. Делим m на p_1, получаем частное m_1, так что

$$m = p_1 \cdot m_1,$$

при чем $m_1 < m$. Если m_1 первоначальное число, то теорема уже доказана; если нет, то по предыдущей теореме m_1 имеет первоначального делителя p_2, и

$$m_1 = p_2 \cdot m_2, \text{ и следовательно } m = p_1 \cdot p_2 \cdot m_2,$$

где $m_2 < m_1$. Если m_2 первоначальное число, то теорема уже доказана; если нет, то продолжаем процесс дальше и получаем

$$m_2 = p_3 m_3 \text{ и } m = p_1 p_2 p_3 m_3,$$

при чем $m_3 < m_2$ и т. д. Но этот процесс не может продолжаться бесконечно, потому что он приводит к ряду целых положительных чисел, убывающих по величине: $m > m_1 > m_2 > m_3 > \ldots$. Этот ряд не может быть бесконечным, т. к. чисел меньших m самое большое m—1. А закончится этот процесс тогда, когда какое-нибудь частное само будет первоначальным числом, например m_k окажется первоначальным числом: $m_k = p_{k+1}$. В таком случае $m_{k-1} = p_k$ $m_k = p_k$ p_{k+1}, и

$$m = p_1 p_2 p_3 \cdots p_{k-1} p_k p_{k+1},$$

и следовательно составное число m представлено произведением первоначальных факторов.

Докажем, что **разложение это единственное** Пусть имеем два разложения:

$$m = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s$$

и

$$m = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_t,$$

где p и q — первоначальные факторы.

Имеем равенство

$$p_1 \cdot p_2 \cdot p_3 \cdots p_s = q_1 \cdot q_2 \cdot q_3 \cdots q_t,$$

и т. к. левая часть его делится на p_1, то и правая тоже должна делиться на p_1, а т. к. правая есть произведение, то один из факторов должен делиться на первоначальное число p_1, пусть это будет q_1; но q_1, как первоначальное число, может делиться только на 1-цу и само на себя, следовательно необходимо $q_1 = p_1$. Сократив равенство на $p_1 = q_1$, получаем:

$$p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t.$$

Поступая с этим равенством по предыдущему, докажем, что например $q_2 = p_2$, и придем к равенству

$$p_3 \cdots p_s = q_3 \cdots q_t$$

и т. д. Легко усмотреть, что $s = t$; действительно, если бы s и t не были равны, то при последовательных сокращениях мы бы получили в одной части 1-цу, а в другой произведение оставшихся первоначальных факторов, что невозможно. Итак $s = t$ и все q равны различным факторам p, так что оба разложения совпадают.

Среди первоначальных множителей числа могут быть и равные; соединяя их, представим число m в виде

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

где a, b, c, ... l — различные первоначальные делители числа m, а $\alpha, \beta, \gamma, \ldots \lambda$ — целые положительные числа, указывающие, сколько раз каждый первоначальный делитель входит множителем в разложение числа m.

Числа, для которых $\alpha = \beta = \gamma = \ldots = \lambda = 1$, называются первичными; их можно определить как числа, не делящиеся ни на один квадрат. Числа непервичные, очевидно, всегда делятся на квадрат; пусть, например, хотя бы $\alpha > 1$; тогда m, очевидно, делится на a^2.

Иногда составные числа классифицируют по числу различных первоначальных факторов, входящих в разложе-

ние, т.-е. различают числа вида $m = a^{\alpha}$ или $m = a^{\alpha}b^{\beta}$ или $m = a^{\alpha}b^{\beta}c^{\gamma}$ и т. д.

Когда нам дано какое-нибудь число m, то решить вопрос, первоначальное оно или составное, можно попытками. Число первоначальное не имеет собственных делителей; значит мы должны пробовать делить m на числа, начиная от 2 и до $m-1$; если ни на одно из них m не разделится, значит оно первоначальное, в противном случае—составное. При этом нет надобности пробовать делить на числа 4, 6, ... (кратные двух), вообще на числа, кратные тем, которые уже испытаны, так как число, которое не делится на 2, не разделится и на 4, число которое не делится на 3, не разделится ни на 9 ни на 15, и т. д. Продолжать испытание можно не до $m-1$, а только до $E\sqrt{m}$; в самом дѣле, если $m \mid d$, при чем $d > E\sqrt{m}$, то $m = d\delta$ и $\delta < E\sqrt{m}$; значит, если число имеет делитель больший $E\sqrt{m}$, то непременно имеет и делитель меньший $E\sqrt{m}$, и потому достаточно испробовать все числа от 2 до $E\sqrt{m}$.

Так, чтобы узнать, первоначальное или составное число 31, достаточно испытать, делится ли оно на числа от 2 до $E\sqrt{31} = 5$, т.-е. на числа 2, 3, 4, 5; из этих чисел 4, как кратное 2-х, отбрасываем; ни на 2, ни на 3, ни на 5, 31 не делится, след. это число первоначальное.

Распределение первоначальных чисел в натуральном ряде с древних времен привлекало внимание математиков. Какой-то закон руководит этим распределением; уловить его и выразить формулой, заключающей по возможности простые функции, составляло мечту многих работников в области теории чисел.

В таком виде мечта оказалась неосуществимой: мы имеем лишь приближенные формулы того типа, о котором сказано выше; но раз дело идет об указании всех первоначальных чисел в конечном отрезке натурального ряда, т.-е. первоначальных чисел, не превышающих известного предела, то этот вопрос легко решается составлением таблицы пер-

воначальных чисел. Прием для составления такой таблицы был указан еще Эратосфеном, почему он носит название решета Эратосфена:

Пишем ряд чисел

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ... , n,

из которого мы хотим выбрать первоначальные числа.

Заметим, что 1-ца не считается первоначальным числом, так что первое первоначальное число есть 2, имеющее лишь два несобственных делителя 1 и 2. Вычеркиваем затем из нашего ряда все числа, кратные 2-х, не считая самого числа 2, для чего придется вычеркивать числа через одно (4, 6, 8, 10, ...). Первое невычеркнутое после 2-х число есть 3; оно будет необходимо первоначальное, т. к. могло бы иметь собственным делителем лишь 2, а все кратные двух уже вычеркнуты. Далее вычеркиваем все кратные 3-х, не считая самого числа 3, т.-е. начиная с 6-ти (6, 9, 12, . . .), для чего приходится вычеркивать числа через 2, отступя на 3-е место от 3-х. Первое невычеркнутое число есть 5; оно тоже первоначальное, т. к. могло бы иметь собственными делителями только предшествующие числа, но тогда бы оно было кратным 2-х или 3-х, а мы таковые кратные уже вычеркнули. Далее вычеркиваем кратные 5-ти, т.-е. вычеркиваем числа через четыре, отступя на 5-е место от 5-ти (10, 15, 20, ...). Первое невычеркнутое число 7 есть первоначальное, ибо могло бы иметь собственными делителями только предшествующие числа, а тогда бы было кратным 2-х, 3-х или 5-ти, а мы все эти кратные уже вычеркнули. Затем вычеркиваем кратные 7-ми, и т. д., и т. д., пока не исчерпаем всего ряда; оставшиеся невычеркнутыми числа суть первоначальные. Заметим, что при вычеркивании некоторые числа вычеркиваются по нескольку раз, будучи одновременно кратными нескольких первоначальных чисел.

Итак, в каждом отрезке натурального ряда можно выбрать первоначальные числа.

Возникает вопрос, сколько же всего первоначальных чисел? Другими словами, продолжая натуральный ряд все

дальше и дальше, будем ли все время получать и первоначальные числа, или же за известным числом все следующие числа будут уже только составные?

На этот вопрос дан ответ уже Эвклидом, который доказал, что первоначальных чисел бесконечное множество или иначе, что нет последнего первоначального числа. Доказательство ведется от противного. Пусть p последнее первоначальное число. Составим произведение всех первоначальных чисел от 2-х до p и прибавим к нему 1-цу. Полученное число

$$N = 2.\ 3.\ 5.\ 7.\ 11 \ldots\ldots p + 1$$

более p; следовательно, по предположению оно составное. Но раз так, оно должно бы иметь хотя одного первоначального делителя; между тем ни на одно из первоначальных чисел 2, 3, 5, 7, 11, ..., p оно не может разделиться, т. к. на каждое из этих чисел делится первое слагаемое N, но не делится второе слагаемое—1-ца. Итак, мы пришли к противоречию, и следовательно не может быть последнего первоначального числа.

Натуральный ряд чисел представляет собою арифметическую прогрессию с разностью 1. Рассмотрим теперь какую-нибудь арифметическую прогрессию с разностью m

$$n,\ n+m,\ n+2m,\ n+3m, \ldots\ldots$$

Числа этой прогрессии можно представить формулой $mx+n$, где x принимает значения $x = 0, 1, 2, 3, \ldots\ldots$

Возникает вопрос, есть ли среди чисел прогрессии первоначальные числа и сколько их?

Прежде всего ясно, что необходимо предположить $D(m, n) = 1$, потому что в противном случае вопрос сразу разрешается в отрицательном смысле: если $D(m, n) = d > 1$, то $m = m' d$, $n = n' d$ и тогда $mx + n = d(m' x + n')$, т.-е. все числа прогрессии—кратные d и значит составные.

Итак, предположим $D(m, n) = 1$; существует теорема, что в этом случае в прогрессии находится бесчисленное множество первоначальных чисел. Положение это впервые было дока-

зано Дирихле, но потребовало для своего доказательства применения целого ряда соображений из области анализа.

Некоторые простейшие случаи этой теоремы можно доказать и элементарно. Самый простой случай—натурального ряда—мы уже рассмотрели. Теперь рассмотрим прогрессию чисел вида $6x - 1$, т.-е. 5, 11, 17, 23, 29, ... , и докажем, что существует бесчисленное множество первоначальных чисел этого вида. Заметим, что первоначальное число при делении на 6 может давать в остатке только 1 или 5, ибо числа, дающие в остатке 2 или 4 суть кратные двух, а дающие в остатке 3—кратные трех. Если число дает в остатке 1, то оно имеет вид $6x + 1$, если же в остатке получается 5, то число имеет вид $6y + 5 = 6(y + 1) - 1 = 6x - 1$. Итак все первоначальные числа большие трех, имеют вид или $6x + 1$ или $6x - 1$. Допустим теперь, что первоначальных чисел вида $6x - 1$ конечное число и что последнее первоначальное число этого вида есть p. Составим произведение всех простых чисел до p и вычтем из него 1-цу; получаем число

$$N = 2.\ 3.\ 5.\ 7. \ldots\ldots p - 1,$$

которое, очевидно, вида $6z - 1$. Число N больше p, которое по предположению есть последнее первоначальное число вида $6x - 1$, следовательно N составное число. Всякое составное число есть произведение первоначальных факторов; при этом ясно, что N не делится ни на одно первоначальное число от 2-х до p, так как на каждое из этих чисел делится уменьшаемое $2.\ 3.\ 5. \ldots\ldots p$, но не делится вычитаемое—1-ца. Поэтому все первоначальные факторы N необходимо должны быть вида $6x + 1$, согласно предположению, что p есть последнее первоначальное число вида $6x - 1$. Но раз так, то N должно быть само числом вида $6k + 1$, ибо

$$N = (6x + 1)(6x' + 1)(6x'' + 1) \ldots = 6k + 1,$$

и мы таким образом приходим к противоречию, а следовательно доказываем, что не может быть последнего первоначального числа вида $6x - 1$.

Возвращаясь к натуральному ряду, можем поставить вопрос, сколько первоначальных чисел содержится в этом ряде от 1-цы до n. Назовем это число $\Pi(n)$. Для каждого значения n число $\Pi(n)$ имеет тоже определенное значение; таким образом мы имеем некоторую функцию числа n. Так как определение $\Pi(n)$ основано на понятиях из области теории чисел, то мы имеем в $\Pi(n)$ пример так называемой „числовой функции“. Аргумент n принимает лишь целые значения; но можно определение видоизменить так, чтобы аргумент принимал всевозможные действительные (положительные) значения, а именно будем считать:

$$\Pi(x) = \text{числу первоначальных чисел} \leqslant x.$$

Так, $\Pi(20,7) =$ числу первоначальных чисел не превосходящих 20, 7, т.-е. числу первоначальных чисел в ряду от 1 до 20.

При новом определении аргумент x функции $\Pi(x)$ изменяется непрерывно, но сама функция, принимая лишь целые значения, остается прерывной.

Функция $\Pi(x)$ служила предметом изучения многих математиков, но результаты их исследований еще далеки от совершенства.

Важнейший из этих результатов заключается в следующем: для функции $\Pi(x)$ можно указать приближенное выражение, которое тем ближе представляет $\Pi(x)$, чем больше величина аргумента x. Такими приближенными выражениями являются

$$\frac{x}{lgx} \text{ и } \int_2^x \frac{dx}{lgx},$$

так что

$$\Pi(x) \sim \frac{x}{lgx} \text{ и } \Pi(x) \sim \int_2^x \frac{dx}{lgx}$$

Точный смысл этого обозначения таков: отношение $\Pi(x)$ к $\frac{x}{lgx}$ или к $\int_2^x \frac{dx}{lgx}$ стремится к 1-це с возрастанием x:

$$\lim_{x \to \infty} \frac{\Pi(x)\, lgx}{x} = 1, \qquad \lim_{x \to \infty} \frac{\Pi(x)}{\int_2^x \frac{dx}{lgx}} = 1.$$

Вообще, если для функции $f(x)$ имеется другая функция $S(x)$ такая, что

$$\lim_{x \to \infty} \frac{f(x)}{S(x)} = 1,$$

то говорят, что $S(x)$ есть асимптотическое выражение $f(x)$; таким образом асимптотическими выражениями для $\Pi(x)$ служат

$$\frac{x}{lgx} \text{ и } \int_2^x \frac{dx}{lgx}.$$

Можно отметить еще такое равенство

$$\lim_{x \to \infty} \frac{(lgx)^q}{x} \left[\Pi(x) - \int_2^x \frac{dx}{lgx} \right] = 0,$$

имеющее место для любого q.

Оставляя в стороне дальнейшее развитие теории первоначальных чисел, требующей вообще применения методов высшего анализа и теории функций, возвращаемся к разложению составного числа на первоначальные факторы.

Пусть имеем для числа m такое разложение

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

и пусть d есть делитель m. Ясно, что в разложение d не может входить ни один первоначальный фактор, отличный от $a, b, c, \ldots . l$, так как на этот фактор делилось бы d, а следовательно и m, что невозможно, ибо единственные пер-

воначальные делители m суть $a, b, c, \ldots\ldots l$. Таким образом, разложение d может только иметь вид:

$$d = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots\ldots l^{\lambda'}$$

Легко далее усмотреть, что $\alpha', \beta', \gamma' \ldots\ldots \lambda'$ не могут превосходить соответственно $\alpha, \beta, \gamma, \ldots\ldots \lambda$. В самом деле пусть например $\alpha' > \alpha$ и $\alpha' = \alpha + \omega$. Так как $m \mid d$ и $d \mid a^{\alpha+\omega}$, то и $m \mid a^{\alpha+\omega}$; по сокращении на a^{α} отсюда имеем

$$b^{\beta} c^{\gamma} \ldots\ldots l^{\lambda} \mid a^{\omega},$$

что невозможно, т. к. $b^{\beta}, c^{\gamma}, \ldots\ldots l^{\lambda}$ взаимно-просты с a^{ω}. Обратно ясно, что m делится на d, если $\alpha', \beta', \gamma', \ldots\ldots \lambda'$ не превосходят $\alpha, \beta, \gamma, \ldots\ldots \lambda$, и таким образом в с е делители числа m исчерпываются формулой

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

где показатели, независимо один от другого, принимают значения

$$\alpha' = 0, 1, 2, \ldots\ldots \alpha; \quad \beta' = 0, 1, 2, \ldots\ldots \beta; \quad \gamma' = 0, 1, 2, \ldots\ldots \gamma;$$
$$\ldots\ldots \quad \lambda' = 0, 1, 2, \ldots\ldots \lambda.$$

Имея несколько чисел и зная их разложения, мы легко можем на основании изложенного найти их общий наибольший делитель и общее наименьшее кратное. Ясно, что общий делитель может содержать только общие всем числам первоначальные факторы и в степенях не превышающих степеней, в которых они входят в данные числа; поэтому общий наибольший делитель получим, взяв все общие первоначальные факторы, каждый в степени, равной наименьшей из степеней, в которых этот фактор входит в данные числа.

Так пусть даны числа

$$12 = 2^2 . 3; \; 18 = 2 . 3^2; \; 30 = 2 . 3 . 5.$$

Их общий наибольший делитель $= 2 . 3 = 6$.

Обращаясь к общему наименьшему кратному, заметим, что всякое общее кратное необходимо должно содержать

все первоначальные факторы всех данных чисел и в степени не меньшей, чем они входят в данные числа. Поэтому общее наименьшее кратное получим, взяв все первоначальные факторы всех данных чисел и каждый из них в степени равной наибольшей из степеней, в которых они входят в данные числа.

Так, для тех же чисел

$$12 = 2^2 . 3;\ 18 = 2 . 3^2;\ 30 = 2 . 3 . 5$$

общее наименьшее кратное есть

$$2^2 . 3^2 . 5 = 180.$$

ГЛАВА ТРЕТЬЯ.

Числовые функции. Интегралы по делителям.

Мы видели, что если число n представлено разложением на первоначальные факторы

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

то все делители получаются из формулы

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

где $\alpha' = 0, 1, 2, \ldots . \alpha$; $\beta' = 0, 1, 2, \ldots . \beta$; $\gamma' = 0, 1, 2, \ldots . \gamma$; . . . . . $\lambda' = 0, 1, 2, \ldots . \lambda$. Рассмотрим таблицу

$$\begin{array}{l} 1,\ a,\ a^2,\ a^3,\ \ldots .\ a^{\alpha} \\ 1,\ b,\ b^2,\ b^3,\ \ldots .\ b^{\beta} \\ 1,\ c,\ c^2,\ c^3,\ \ldots .\ c^{\gamma} \\ \ldots\ldots\ldots\ldots \\ 1,\ l,\ l^2,\ l^3,\ \ldots .\ l^{\lambda}. \end{array} \qquad (1)$$

Очевидно, все делители числа n получим, выбирая по одному члену из каждой строки таблицы и перемножая их между собою, ибо при этом получаем число вида $d = a^{\alpha'}\, b^{\beta'}\, c^{\gamma'} \ldots . l^{\lambda'}$, и при том каждый делитель получается таким образом по одному разу. Число делителей числа n поэтому равно числу различных получаемых указанным способом произведений. Сосчитаем число этих произведений. В первой строке всего $\alpha + 1$ чисел; можно взять любое из них; во второй $\beta + 1$ чисел; можно каждое из них комбинировать с каждым из чисел 1-й строки, всего получаем $(\alpha + 1)(\beta + 1)$ комбинаций. Далее каждую из этих комбинаций можем помножить на любое из $\gamma + 1$

чисел 3-й строки, отчего получим $(\alpha+1)(\beta+1)(\gamma+1)$ комбинаций, и т. д. и т. д. В конце концов, будем иметь всего

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

произведений и следовательно таково число всех делителей числа n.

Для каждого данного числа n число делителей имеет определенное численное значение; следовательно число делителей есть функция числа n, изменяющаяся с изменением n. Эту функцию обозначают $\varrho(n)$ (по Эйлеру) или $\zeta(n)$ (по Лиувиллю).

Таким образом

$$\varrho(n)=\varrho(a^{\alpha}b^{\beta}\ldots.l^{\lambda})=(\alpha+1)(\beta+1)\ldots.(\lambda+1) \qquad (2)$$

Например, $\varrho(12)=\varrho(2^2.3)=(2+1)(1+1)=6$.

Определим далее сумму всех делителей числа n. Очевидно, эту сумму получим, если сложим числа, стоящие в каждой строке таблицы (1) и все полученные суммы перемножим

$$(1+a+a^2+\ldots.+a^{\alpha})(1+b+b^2+\ldots.+b^{\beta})\ldots.(1+l+ +l^2+\ldots.+l^{\lambda}),$$

ибо при этом получим сумму всевозможных произведений типа $a^{\alpha'}b^{\beta'}\ldots.l^{\lambda'}$. Каждый фактор выше написанного произведения представляет собою сумму геометрической прогрессии, а потому, применяя известную формулу и обозначая сумму всех делителей числа n через $\int(n)$, имеем

$$\int(n)=\int(a^{\alpha}b^{\beta}\ldots.l^{\lambda})=\frac{a^{\alpha+1}-1}{a-1}\cdot\frac{b^{\beta+1}-1}{b-1}\ldots.\frac{l^{\lambda+1}-1}{l-1} \qquad (3)$$

Например, $\int(12)=\int(2^2.3)=\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}=7.4=28$.

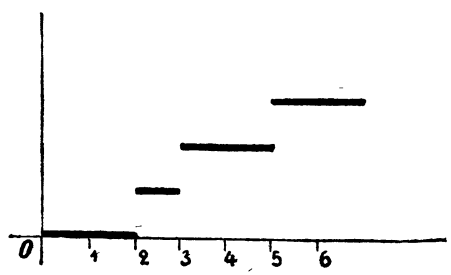
Очевидно, $\int(n)$ [1]) есть функция числа n, ибо для каждого данного числа n известна и сумма его делителей.

---

[1]) $\int(n)$ есть обозначение Эйлера. Лиувилль обозначает эту функцию через $\zeta_1(n)$.

Мы имеем, таким образом два примера числовых функций: $\varrho(n)$ и $f(n)$; в предшествующей главе имели еще третий пример — функцию $\Pi(x)$. Понятие о функции есть общее понятие, которое применимо к различным областям математики, и в теории чисел оно не имеет чего-либо специфического. Термин числовая функция указывает лишь на то, что самое определение данной функции основано на понятиях и соотношениях, взятых из области теории чисел.

Возвращаясь к трем выше упомянутым примерам, замечаем существенную разницу между функцией $\Pi(x)$ с одной стороны и функциями $\varrho(n)$ и $f(n)$—с другой. Для функции $\Pi(x)$ аргумент принимает всевозможные действительные значения (по крайней мере положительные) и может изменяться непрерывно, при чем сама функция изменяется прерывно, как указывает ее график (см. фиг. 1).



Фиг. 1.

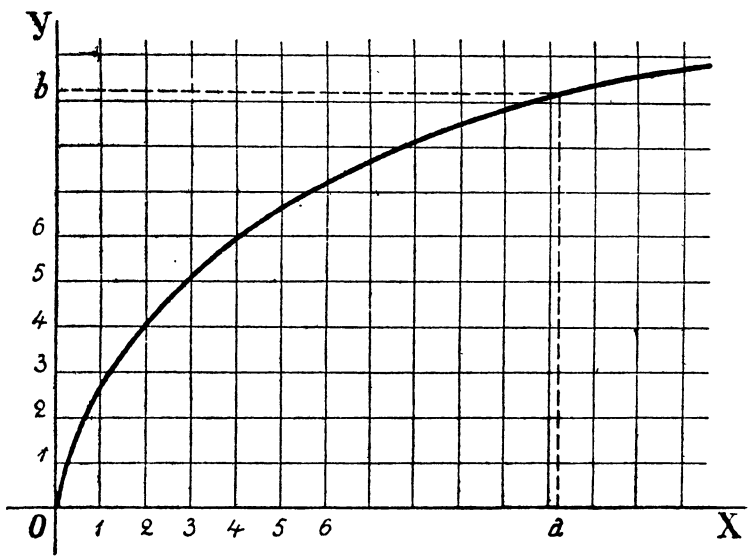
Что касается до функций $\varrho(n)$ и $f(n)$, то по самому смыслу определения аргумент принимает лишь целые (и положительные) значения.

Таким образом числовые функции бывают двух типов: 1) функции, для которых аргумент принимает всевозможные (положительные) действительные значения, 2) функции, для которых аргумент, по самому смыслу определения, принимает лишь целые значения. Функции первого типа вполне доступны обычным методам анализа и теории функций. Значения функции второго типа известны лишь для целых значений аргумента; поэтому с точки зрения анализа здесь имеем дело скорее с задачей интерполяции.

Примером функции 1-го типа может служить еще функция Ex, рассмотренная нами выше и играющая важную роль в теории функций.

Выведем одно важное соотношение, включающее эту функцию, которым нам придется пользоваться в дальнейшем.

Рассмотрим на плоскости прямоугольную систему координат и системы прямых $x = 1, 2, 3, \ldots$, $y = 1, 2, 3, \ldots$, параллельных осям координат. Эти прямые образуют сеть; точки их пересечения называем узлами сети, при чем точки на осях в счет узлов не входят; узлы сети суть точки



Фиг. 2.

с целыми положительными координатами. Предположим далее, что на плоскости имеется линия $y = \psi(x)$, проходящая через начало координат, при чем $\psi(x)$ — возрастающая функция, так что эта линия пересекает каждую ординату и каждую параллель к оси x в одной точке. Разрешая уравнение $y = \psi(x)$ относительно x, имеем $x = \Psi(y)$, где $\Psi(y)$ — функция, обладающая такими же свойствами, что и $\psi(x)$.

Дадим x какое-нибудь значение, целое или дробное, $x = a$; тогда $y = \psi(a) = b$. Прямые $x = a$, $y = b$ вместе с осями ограничивают некоторый прямоугольник. Сосчитаем число узлов сети, лежащих в этом прямоугольнике.

Счет этот произведем так: линия $y = \psi(x)$ разбивает прямоугольник на две части, и мы сосчитаем сначала число узлов, лежащих в нижней части прямоугольника — между осью x и кривой, а затем в верхней — между осью y и кривой. Число узлов в первой части определим так: сосчитаем узлы на первой ординате для $x = 1$; величина ординаты равна $\psi(1)$; это число вообще — целое с дробью (например 3 с дробью) и число узлов на ней, очевидно равно целой части числа, т.-е. $E\psi(1)$; равным образом число узлов на 2-й ординате равно $E\psi(2)$, на 3-й — $E\psi(3)$ и т. д. Последняя ордината получается для целого значения x ближайшего к a, т.-е. для Ea, и число узлов на ней $= E\psi(Ea)$. Общее число узлов в 1-й части прямоугольника равно таким образом.

$$E\psi(1) + E\psi(2) + E\psi(3) + \ldots + E\psi(Ea). \qquad (4)$$

Совершенно так же можем определить число узлов во второй части прямоугольника, которая относительно оси y занимает такое же положение, какое 1-я относительно оси x. Для этого рассматриваем уравнение кривой в виде $x = \Psi(y)$ и повторяя аналогичные рассуждения с заменой x через y и a через b, имеем число узлов во 2-й части

$$E\Psi(1) + E\Psi(2) + \ldots + E\Psi(Eb) \qquad (4').$$

Сложив суммы (4) и (4′), получаем общее число узлов в прямоугольнике:

$$E\psi(1) + E\psi(2) + \ldots + E\psi(Ea) + E\Psi(1) + E\Psi(2) + \\ + \ldots + E\Psi(Eb) \quad (5).$$

Но при этом счете совершена ошибка: узлы, лежащие на кривой, если таковые имеются, сосчитаны два раза — и в 1-й и во 2-й части; поэтому число таких узлов, которое равно числу целых значений функции $\psi(x)$ и которое обозначим $[Ц\psi(x)]$, следует вычесть из суммы (5).

С другой стороны, число узлов в прямоугольнике равно произведению целой части длины прямоугольника на целую часть высоты и следовательно имеем тождество

$$E\psi(1) + E\psi(2) + \ldots + E\psi(Ea) + E\Psi(1) + E\Psi(2) + \ldots + \\ + E\Psi(Eb) - [Ц\psi(x)] = Ea \,.\, Eb \qquad (6)$$

Из этой формулы можно получить целый ряд интересных результатов в виде соотношений, содержащих символ E. Мы ограничимся одним частным случаем, когда кривая $y = \psi(x)$ есть прямая, проходящая через начало координат и через точку (p, q), где p, q — первоначальные числа. Уравнение прямой, проходящей через начало и через точку p, q, есть

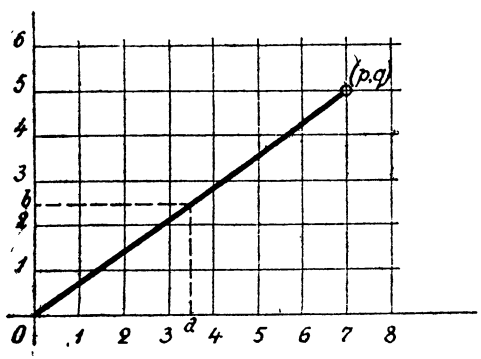
$$\frac{x}{p} = \frac{y}{q},$$

откуда

$$y = \psi(x) = \frac{q}{p} x$$

и

$$x = \Psi(y) = \frac{p}{q} y.$$



Фиг. 3.

Возьмем $a = \frac{p}{2}$; тогда $b = \frac{q}{2}$. Легко видеть, что внутри прямоугольника, определяемого числами a и b, на нашей прямой не лежит ни одного узла сети. В самом деле, уравнение прямой дает

$$\frac{p}{q} = \frac{x}{y};$$

дробь $\frac{p}{q}$ — несократимая и следовательно не может равняться другой дроби с меньшими числителем и знаменателем, так что уравнение не удовлетворяется для целых значений x и y, меньших p и q.

Таким образом в данном случае $[Ц\psi(x)] = 0$, и формула (6) дает

$$E\frac{q}{p} + E\frac{2q}{p} + E\frac{3q}{p} + \ldots + E\frac{E\frac{p}{2} \cdot q}{p} + E\frac{p}{q} + E\frac{2p}{q} + \\ + \ldots + E\frac{E\frac{q}{2} \cdot p}{q} = E\frac{p}{2} \cdot E\frac{q}{2} \cdot$$

Замечая, что p и q — нечетные числа, а $p-1$ и $q-1$ ближайшие меньшие четные, имеем

$$E\frac{p}{2}=\frac{p-1}{2},\ E\frac{q}{2}=\frac{q-1}{2},$$

и потому в окончательной форме получаем тождество:

$$E\frac{q}{p}+E\frac{2q}{p}+E\frac{3q}{p}+\ldots+E\frac{\frac{p-1}{2}\cdot q}{p}+E\frac{p}{q}+E\frac{2p}{q}+$$
$$+E\frac{3p}{q}+\ldots+E\frac{\frac{q-1}{2}\cdot p}{q}=\frac{p-1}{2}\cdot\frac{q-1}{2} \qquad (7).$$

Обращаясь к функциям 2-го типа, можем рассмотреть целый ряд функций, так или иначе связанных с делителями. Так, Лиувилль рассматривает для числа n, сумму $\mu-x$ степеней его делителей и обозначает эту сумму через $\zeta_\mu(n)$. Очевидно,

$$\text{как } \zeta_0(n)=\zeta(n)=\varrho(n);\ \zeta_1(n)=\int(n).$$

Бóльшее значение, чем все предшествующие, имеет функция, обозначаемая $\varphi(n)$ и называемая функцией Гаусса. Она равна числу чисел взаимно-простых с n и не превосходящих n. Для определения ее значения надо в ряду 1, 2, 3, . . . n выбрать числа, взаимно-простые с n и сосчитать, сколько их. Для того, чтобы получить выражение функции Гаусса, дадим предварительно общую теорию интегралов по делителям.

Пусть $\psi(n)$ какая-либо функция, определенная для целых значений аргумента n и принимающая целые значения. Пусть 1, d_1, d_2, . . . ,n суть все делители числа n. Рассмотрим сумму

$$\psi(1)+\psi(d_1)+\psi(d_2)+\psi(d_3)+\ldots+\psi(n)=\sum_n\psi(d),$$

распространенную на все делители d числа n. Такую сумму называют числовым интегралом по делителям от функции $\psi(n)$. Пусть, например, $\psi(n)=n$. Тогда имеем сумму.

$$\sum_n d=1+d_1+d_2+d_3+\ldots+n=\int(n).$$

Если $\psi(n) = n^\mu$, то имеем

$$\sum_n d^\mu = \zeta_\mu(n)$$

и в частности для $\mu = 0$

$$\sum_n d^0 = \sum_n 1 = 1 + 1 + 1 + \ldots + 1 = \zeta(n).$$

Вообще числовой интеграл по делителям функции $\psi(n)$ в свою очередь есть некоторая функция n, так что

$$\sum_n \psi(d) = \chi(n).$$

Функцию $\psi(n)$ будем называть числовой производной от функции $\chi(n)$ и обозначаем:

$$\psi(n) = D\ \chi(n).$$

Так, из предыдущего ясно, что

$$n = D\int(n)$$
$$1 = D\zeta(n)$$
$$n^\mu = D\zeta_\mu(n).$$

Операция числового дифференцирования есть, очевидно, операция обратная числовому интегрированию, так что

$$D\sum_n \psi(d) = \psi(n)$$
$$\sum_n D\psi(d) = \psi(n).$$

Рассмотрим теперь числовые интегралы более общего вида. Обозначаем через δ делитель дополнительный к делителю d и для двух функций $\psi(n), \chi(n)$ строим сумму

$$\psi(1)\ \chi(n) + \psi(d_1)\chi(\delta_1) + \psi(d_2)\chi(\delta_2) + \psi(d_3)\chi(\delta_3) + \ldots +$$
$$+ \psi(n)\chi(1) = \sum_n \psi(d)\chi(\delta) = \sum_n \psi(d)\chi\left(\frac{n}{d}\right).$$

Легко видеть, что эта сумма может быть иначе определена, как сумма

$$\sum_{uv=n} \psi(u)\ \chi(v),$$

распространенная на все целые положительные решения уравнения $uv = n$; действительно из равенства $uv = n$ непосредственно следует, что и u и v—делители n и притом взаимно-дополнительные.

Рассмотрим далее двукратный числовой интеграл

$$\sum_{n} \psi(d) \sum_{\delta} \chi(d') \omega(\delta'), \tag{8}$$

где d' и δ' два взаимно-дополнительных делителя числа δ, так что $\delta = d'\delta'$, $n = d\delta$ и следовательно $n = d\,d'\,\delta'$. Легко видеть, что наша сумма есть не что иное, как сумма

$$\sum_{uvw=n} SSS\, \psi(u)\, \chi(v)\, \omega(w), \tag{9}$$

распространенная на все целые положительные решения уравнения

$$uvw = n,$$

ибо и u, и v и w, как явствует из равенства $uvw = n$, суть делители числа n, при том произведение vw есть делитель δ дополнительный для делителя $d = u$ и, наконец, v и w—два дополнительных делителя d' и δ' числа $\delta = vw$. Но сумма (9) совершенно равноправна относительно трех аргументов и трех функций $\psi(n)$, $\chi(n)$, $\omega(n)$; а потому в числовом интеграле (8) можно произвольно переставлять эти функции, не меняя величины интеграла, и следовательно имеем тождество

$$\sum_{n} \psi(d) \sum_{\delta} \chi(d') \omega(\delta') = \sum_{n} \chi(d) \sum_{\delta} \omega(d') \psi(\delta') =$$
$$= \sum_{n} \omega(d) \sum_{\delta} \psi(d') \chi(\delta'), \tag{10}$$

выражающее переместительность кратных числовых интегрирований. Это тождество легко обобщить на числовые интегралы бо́льшей кратности и, с другой стороны, на суммы более общего вида, предполагая, что суммирование распространяется на все целые положительные решения не уравнения $uvw = n$, а более общего уравнения, например $u^{\mu} vw = n$ (в этом случае u есть делитель n, которого μ-я степень тоже делит n).

Из тождества (10) и вышеупомянутых его обобщений можно получить целый ряд результатов, между прочим большое число тождеств, данных Лиувиллем. Мы ограничимся применением тождества (10) к выражению числовой производной через числовой интеграл. Для этой цели рассмотрим числовую функцию $\mu(n)$, называемую функцией

Mertens'a. Она определяется такими условиями: для непервичного n (т.-е. для n, делящегося на квадрат) $\mu(n) = 0$ $\mu(1) = 1$, и для первичного n $\mu(n) = \pm 1$ в зависимости от того, четное или нечетное число простых множителей входит в n, так что, если $a, b, c, \ldots$ простые факторы числа, то

$$\mu(1) = 1,\ \mu(a) = -1,\ \mu(ab) = +1,\ \mu(abc) = -1,\ \ldots\ .$$
$$\text{и } \mu(a^\alpha b^\beta c^\gamma \ldots) = 0,$$

если хотя один из показателей $\alpha, \beta, \gamma, \ldots$ больше единицы.

Рассмотрим числовой интеграл по делителям от функции $\mu(n)$; это есть некоторая функция $\pi(n)$:

$$\sum_n \mu(d) = \pi(n)$$

Для $n = 1$

$$\pi(1) = \sum_1 \mu(d) = \mu(1) = 1$$

Для $n > 1$

$$\pi(n) = \sum_n \mu(d) = \sum_{a^\alpha b^\beta c^\gamma \ldots l^\nu} \mu(d) = \mu(1) + \mu(a) + \mu(b) + \mu(c) +$$

$$+ \ldots + \mu(ab) + \mu(bc) + \ldots + \mu(abc) + \ldots + \mu(abc \ldots l),$$

т. к. все члены суммы, соответствующие непервичным делителям числа n, исчезают. Пусть число различных первоначальных факторов $a, b, c, \ldots l$ числа n равно ν. Тогда число комбинаций $ab, bc, \ldots$ равно $\frac{\nu(\nu-1)}{1.2}$, число делителей вида $abc, \ldots$ равно $\frac{\nu(\nu-1)(\nu-2)}{1.2.3}$ и т. д., и т. к. $\mu(a) = \mu(b) =$ $= \ldots = -1$, $\mu(ab) = \mu(bc) = \ldots = +1$ и т. д., то

$$\pi(n) = 1 - \nu + \frac{\nu(\nu-1)}{1.2} - \frac{(\nu-1)(\nu-2)}{1.2.3} + \ldots \pm 1 =$$
$$= (1-1)^\nu = 0$$

Итак, функция $\pi(n)$ равна единице для $n = 1$ и нулю для всех прочих значений n.

Теперь рассмотрим числовой интеграл

$$\sum_n \mu(d)\, \psi(\delta),$$

который есть некоторая функция $f(n)$ от n, так что

$$f(n) = \Sigma \mu(d) \psi(\delta) \tag{11}$$

Возьмем числовой интеграл по делителям от функции $f(n)$

$$\sum_n f(d) = \sum_n \sum_d \mu(d') \psi(\delta').$$

В правой части равенства мы имеем кратный числовой интеграл того типа, как в тождестве (10), при чем только одна из трех функций, входящих в тождество, заменена единицей [например, в средней части тождества (10) можно положить $\chi(d) = 1$, $\omega(d') = \mu(d')$]; воспользовавшись тождеством (10), имеем

$$\sum_n f(d) = \sum_n \sum_d \mu(d') \psi(\delta') = \sum_n \psi(d) \sum_\delta \mu(d') = \sum_n \psi(d) \pi(\delta)$$

Но функция $\pi(n)$ отлична от нуля только для $n = 1$, и тогда $= 1$; поэтому в последней сумме не исчезает только один член для $\delta = 1$ и следовательно $d = n$, и таким образом окончательно имеем

$$\sum_n f(d) = \psi(n),$$

откуда обратно

$$f(n) = D\psi(n)$$

Сопоставляя с равенством (11) имеем

$$D\psi(n) = \sum_n \mu(d) \psi(\delta). \tag{12}$$

Таким образом числовая производная произвольной функции $\psi(n)$ выражена через числовой интеграл. Пользуясь формулой (12) и замечая, что $\mu(d)$ отлично от нуля только для первичных делителей числа n, получаем выражение для числовой производной функции $\psi(n)$, полагая $n = a^\alpha b^\beta c^\gamma \ldots l^\lambda$;

$$D\psi(n) = \psi(n) - \psi\left(\frac{n}{a}\right) - \psi\left(\frac{n}{b}\right) - \psi\left(\frac{n}{c}\right) - \ldots - \psi\left(\frac{n}{l}\right) + \\ + \psi\left(\frac{n}{ab}\right) + \psi\left(\frac{n}{bc}\right) + \psi\left(\frac{n}{ca}\right) + \ldots - \psi\left(\frac{n}{abc}\right) - \ldots \\ \pm \psi\left(\frac{n}{abc\ldots l}\right) \tag{13}$$

Обращаясь к функции $\varphi(n)$, докажем для нее прежде всего теорему Гаусса. Для этой цели рассмотрим ряд чисел

$$1, 2, 3, \ldots, n-1, n.$$

Любое число m этого ряда имеет с числом n некоторого общего наибольшего делителя d; $D(m, n) = d$, при чем d может быть только одним из делителей числа n. Все числа данного ряда разобьем на группы, относя в одну группу те из них, для которых вышеупомянутый общий наибольший делитель есть одно и то же число d. Все числа этой группы имеют вид $m = xd$; при этом число x, как частное от деления m на d должно быть взаимно-просто с частным $\frac{n}{d} = \delta$, т. к. $d = D(m, n)$; вместе с тем x не может превышать $\frac{n}{d} = \delta$, т. к. в противном случае $m = xd$ было бы больше $d \cdot \delta = n$. Итак, все числа m одной группы получим; давая x значения взаимно-простые с δ и не превышающие δ; таковых по определению функции Гаусса, ровно $\varphi(\delta)$ и следовательно столько будет чисел группы, соответствующей общему наибольшему делителю d. Определив число чисел в каждой группе, найдем число всех чисел ряда, просуммировав $\varphi(\delta)$ для всех возможных значений $\delta = \frac{n}{d}$, т.-е. для всех делителей числа n; но общее число чисел данного ряда есть n, и следовательно имеем тождество

$$n = \sum_{n} \varphi(d), \tag{14}$$

составляющее теорему Гаусса. Из этой теоремы, пользуясь формулой (13), непосредственно получаем

$$\varphi(n) = Dn = n - \frac{n}{a} - \frac{n}{b} - \frac{n}{c} - \ldots + \frac{n}{ab} + \frac{n}{bc} + \ldots - \frac{n}{abc} - \ldots \pm \frac{n}{abc \ldots l} = n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots\left(1-\frac{1}{l}\right) \tag{15}$$

или полагая $n = a^{\alpha} b^{\beta} \ldots l^{\lambda}$, в другом виде

$$\varphi(n) = a^{\alpha-1} b^{\beta-1} \ldots l^{\lambda-1} (a-1)(b-1)\ldots(l-1) \tag{15'}$$

Дополнительно надо еще положить

$$\varphi\ (1) = 1;$$

это следует из общего замечания;

$$D\psi\,(1) = \Sigma\psi\,(d)\,\mu\,(\delta) = \psi\,(1)\,\mu\,(1) = \psi\,(1),$$

откуда для $\varphi(n) = Dn$ и имеем $\varphi\ (1) = 1$.

Для примера возьмем $n = 12 = 2^2 . 3^1$

$$\varphi\ (12) = 2.(2-1)\ (3-1) = 4;$$

действительно, числа взаимно-простые с 12-ю и не превосходящие 12-ти суть 1, 5, 7, 11, и их число равно 4. Для того же числа 12 имеем

$$\sum_{12}\varphi\,(d) = \varphi\,(1) + \varphi\,(2) + \varphi\,(3) + \psi\,(4) + \varphi\,(6) + \varphi\,(12) =$$

$$= 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

Функции $\varrho(n), \int(n), \varphi(n)$ имеют много общего между собою; все они получают простое элементарное выражение, раз дано разложение числа n на первоначальные множители. Из выражений этих функций следует для всех них равенство

$$\psi\,(a^\alpha b^\beta \ldots l^\lambda) = \psi\,(a^\alpha), \psi\,(b^\beta) \ldots \psi\,(l^\lambda),$$

а из него более общее соотношение

$$\psi\,(mn) = \psi\,(m).\,\psi\,(n) \qquad (16)$$

для любых двух взаимно-простых чисел m и n. Обратно, раз имеет место свойство (16) то

$$\psi(a^\alpha b^\beta \ldots l^\lambda) = \psi\,(a^\alpha).\,\psi\,(b^\beta c^\gamma \ldots l^\lambda) = \psi\,(a^\alpha)\psi\,(b^\beta)\,\psi\,(c^\gamma \ldots l^\lambda) =$$

$$= \ldots = \psi\,(a^\alpha)\,\psi\,(b^\beta)\,\psi\,(c^\gamma) \ldots \psi\,(l^\gamma)$$

Свойство, выражаемое равенством (16), можно независимо доказать для функции $\varphi(n)$, и тогда обратно из него вывести выражение $\varphi(n)$ и затем доказать теорему Гаусса. Это будет нами сделано впоследствии (Гл. IV, § 1).

ГЛАВА ЧЕТВЕРТАЯ.

§ 1. Распределение чисел по классам относительно данного модуля; представители классов; сравнения по модулю.

Пусть имеем модуль, определяемый своим наименьшим положительным числом m, т. - е. совокупность кратных числа m. Два числа a и b принадлежат к одному классу относительно модуля, если разность чисел $a—b$ есть число данного модуля; говорят также, что эти два числа a и b сравнимы по модулю m и обозначают так:

$$a \equiv b \ (Mod.\ m).$$

При этом термин модуль употребляют уже в измененном смысле, обозначая им не всю совокупность чисел, а наименьшее положительное число m этой совокупности. В дальнейшем всегда будет ясно, в каком именно смысле употребляется термин „модуль“.

Если разность $a — b$ есть число модуля, то это значит, что $a — b$ есть кратное числа m

$$a - b = mx$$

или иначе, что разность $a — b$ делится на m:

$$a - b \mid m$$

Легко видеть, что все приведенные свойства совершенно равноправны и из одного следуют все другие. Можно, на-

конец, дать еще одно определение сравнимости чисел по модулю m. В силу основного свойства числа a и b по отношению к числу m единственным образом представимы в виде:

$$a = mq + r$$
$$b = mq' + s$$

где $0 \leqslant r < m$, $0 \leqslant s < m$ и числа r и s могут быт получены как остатки от делеиия a и b на m. Разность $a - b$ имеет вид:

$$a - b = m(q - q') + r - s$$

и $a - b$ делится на m тогда и только тогда, когда $r - s$ делится на m. Для определенности будем считать $r \geqq s$, в таком случае

$$0 \leqslant r - s < m$$

и $r - s$ может делиться на m только если $r - s = 0$. Итак, два числа принадлежат к одному классу по модулю m тогда и только тогда, когда они равноостаточны при делении на m.

Определим, какие и сколько будет классов по данному модулю m,

Возьмем ряд чисел

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

Все числа этого ряда принадлежат к различным классам по модулю m. В самом деле для двух чисел этого ряда r и s (при чем, напр. $r > s$) разность $r - s < m$ и следовательно не может делиться на m; а поэтому r и s необходимо принадлежат к различным классам. С другой стороны, легко видить, что всякое число необходимо принадлежит к одному классу с одним из чисел ряда (1). В самом деле, по основному свойству теории делимости, всякое число a единственным образом представимо в виде

$$a = mq + r,$$

где $0 \leqslant r < m$ и след. r есть число ряда (1). Разность

$$a - r = mq$$

делится на m и след. числа a и r одного класса по модулю m.

Так как в ряду (1) m чисел, то значит число классов по модулю m равно как раз m, и, конечно, каждый класс заключает бесконечное множество различных чисел, т. к. все числа распределяются по этим классам.

Какое-нибудь число класса иногда называется представителем класса. Значит, числа ряда (1)—это представители различных классов. Если мы знаем какого-нибудь представителя a класса m, то все числа этого класса получаются по формуле

$$a + mx,$$

где $x = 0, \pm 1, \pm 2, \pm 3, \ldots$ Действительно, если число b того же класса, что и a, то разность $b - a$ должна делиться на m и обратно, если $b - a \mid m$, то b и a одного класса; таким образом $b - a = mx$ и

$$b = a + mx.$$

Мы видим следовательно, что весь класс вполне определяется одним из своих представителей.

Поясним еще термин вычет. Если имеем какое-нибудь число a, то всякое другое число того же класса называется вычетом числа a по модулю m. Наименьший положительный вычет числа есть, очевидно, одно из чисел ряда (1); действительно, для числа a имеем

$$a = mq + r,$$

где $0 \leqslant r < m$ и r есть вычет a и при том наименьший положительный вычет по модулю m. Рассматривая на ряду с числами r числа $r - m$, получаем отрицательные вычеты; из двух вычетов r и $r - m$ меньший по абсолютной величине называется наименьшим абсолютным вычетом.

Так, по модулю, 10, наименьший положительный вычет 23 есть 3, наименьший положительный вычет 37 есть 7; отрицательные вычеты этих чисел суть $3 - 10 = -7$ и $7 - 10 = -3$; абсолютно наименьший вычет 23-х есть $+3$, а 37-ми—3.

Систему представителей всех классов иногда называют полной системой вычетов.

Так, полной системой вычетов по модулю 10 может служить ряд

0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Любое число принадлежит к одному из классов, характеризуемых числами этого ряда; так, 17 принадлежит к одному классу с 7-ю, —23—к тому же классу, +23 к классу, имеющему представителем число 3 и т. д.

Относительно чисел, принадлежащих к одному классу, докажем следующую теорему: все эти числа имеют одних и тех же общих делителей с модулем, а следовательно одного и того же общего наибольшего делителя с модулем. В самом деле, если a одно из чисел, то другое число того же класса равно $a+mx$ и если $a \mid d$ и $m \mid d$, то одновременно и $a+mx \mid d$, откуда следует справедливость теоремы и, между прочим, следует

$$D(a, m) = D(a+mx, m).$$

Если в частности один из представителей класса—число взаимно-простое с модулем, то и все числа класса взаимно-просты с модулем. Числа взаимно-простые с модулем m иногда называются единицами по модулю m; таким образом можно сказать, что весь класс состоит из единиц по модулю, если один представитель класса есть единица по модулю.

Обращаясь к выше приведенному примеру $m = 10$, для которого представители классов суть

0, 1, 2, 3, 4, 5, 6, 7, 8, 9,

видим, что классы, имеющие представителями 1, 3, 7, 9, состоят из единиц по модулю 10.

Систему представителей классов, состоящих из единиц по модулю, называют приведенной системой вычетов.

В приведенном примере 1, 3, 7, 9 есть приведенная система вычетов по модулю 10.

Докажем теорему, которой нам придется пользоваться в дальнейшем.

Рассмотрим линейный многочлен или, как обычно говорят, линейную форму $ax+b$, при чем коэффициент a и модуль m суть числа взаимно-простые, так что $D(a,m)=1$. Дадим переменному x ряд значений $r_1, r_2, r_3, \ldots$ образующих систему различных вычетов по модулю m. Получаем ряд чисел

$$ar_1+b,\ ar_2+b,\ ar_3+b,\ldots; \qquad (2)$$

покажем, что все они различных классов по модулю m. Действительно, если бы два различных числа ar_i+b и ar_j+b ряда (2) были одного класса, то их разность

$$ar_i+b-(ar_j+b)=a(r_i-r_j)$$

должна была бы делиться на m; а так как $D(a,m)=1$, то необходимо, чтобы r_i-r_j делилось на m, что невозможно так как r_i и r_j—представители различных классов по модулю m. В частности если x принимает значения, образующие полную систему вычетов $r_1, r_2, r_3, \ldots r_m$, то в ряду (2) имеем m членов, которые все различных классов и следовательно этот ряд

$$ar_1+b,\ ar_2+b,\ ar_3+b,\ldots ar_m+b$$

образует точно так же полную систему вычетов.

Число вычетов полной системы равняется, как мы видели, модулю m. Определим число вычетов приведенной системы. Приведенную систему можем получить, выбрав из полной системы, например, из ряда $1, 2, 3, \ldots m$, числа взаимно-простые с m; но чисел взаимно-простых с m в ряду $1, 2, 3, \ldots m$, по определению функции Гаусса, ровно $\varphi(m)$; следовательно приведенная система вычетов состоит из $\varphi(m)$ чисел.

Так, по модулю 10 приведенная система 1, 3, 7, 9 состоит из $\varphi(10)=4$ чисел.

Мы имеем теперь возможность для функции $\varphi(n)$ доказать основное свойство $\varphi(mn)=\varphi(m).\varphi(n)$ при m и n взаимно-простых.

Для этой цели ряд чисел

$$1,\ 2,\ 3,\ \ldots,\ mn \qquad (3)$$

расположим в виде таблицы

$$\left.\begin{array}{rrrr} 1, & 2, & 3, \ldots\ldots & m \\ m+1, & m+2, & m+3, \ldots\ldots & 2m \\ 2m+1, & 2m+2, & 2m+3, \ldots\ldots & 3m \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ (n-1)\,m+1, & (n-1)\,m+2, & (n-1)\,m+3, \ldots & nm \end{array}\right\} \qquad (A)$$

Числа каждого столбца принадлежат к одному классу по модулю m; представителями этих классов могут служить числа 1-й строки, образующие полную систему вычетов по модулю m (ряд чисел 1, 2, 3, ..., $m-1$, m как и ряд 0, 1, 2, 3, ..., $m-1$, образует полную систему вычетов; в первом ряду только число 0 заменено числом m, которые оба принадлежат к одному классу).

Наша задача состоит в отобрании из таблицы (A) чисел взаимно-простых с mn; но если для числа a $D(a, mn) = 1$, то и $D(a, m) = 1$, $D(a, n) = 1$ и обратно, при m и n взаимно-простых, из $D(a, m) = 1$, $D(a, n) = 1$ следует $D(a, mn) = 1$. Поэтому прежде всего из таблицы (A) отбираем числа взаимно-простые с m; но таковые располагаются по классам, т.-е. следует отобрать классы взаимно-простые с модулем m, а для этого достаточно выбрать представителей классов из первой строки таблицы взаимно-простых с модулем m. В ряду чисел 1, 2, 3, ... m взаимно-простых с m ровно $\varphi(m)$; таким образом в таблице (A) $\varphi(m)$ столбцов состоят из чисел взаимно-простых с m, а остальные столбцы таких чисел не содержат. Теперь остается из $\varphi(m)$ упомянутых столбцов выбрать числа, взаимно-простые с n; это будут числа взаимно-простые с m и с n, а следовательно с mn. Итак, рассмотрим числа одного из столбцов; все они имеют вид $mx+k$ и получаются для $x = 0, 1, 2, \ldots, n-1$, т.-е. для значений x, образующих полную систему вычетов по модулю n; раз так, то по вышедоказанной теореме числа каждого столбца

образуют точно так же полную систему вычетов и следовательно в числе их взаимно-простых с n ровно $\varphi(n)$. Таким образом чисел взаимно-простых с mn во всей таблице (A) мы насчитали $\varphi(m).\ \varphi(n)$. С другой стороны, числа таблицы (A) образуют ряд (3) и по определению функции Гаусса в этому ряду чисел взаимно-простых с mn ровно $\varphi(mn)$. Таким образом имеем

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

для двух взаимно-простых чисел m и n.

Доказав основное свойство функции $\varphi(n)$, можем вывести ее выражение. Применяя последовательно это свойство имеем

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

Остается вывести выражение $\varphi(a^\alpha)$. Берем ряд чисел 1, 2, 3, ... a^α и для того, чтобы сосчитать, сколько в нем чисел взаимно-простых с a^α, определим наоборот, сколько в ряду чисел не взаимно-простых с a^α. Если $D\ (a^\alpha, b) \neq 1$, то необходимо $b \mid a$, т. к. делители a^α исключительно степени a. Итак $b = a.\ x$, и числа этого типа в ряду 1, 2, 3, ... a^α получим, давая x значения $x = 1,\ 2,\ 3,\ \ldots,\ a^{\alpha-1}$; поэтому чисел этого типа в нашем ряду $a^{\alpha-1}$, а следовательно остальных чисел, т.-е. чисел взаимно-простых с a^α, всего

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

таким образом

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

и следовательно

$$\varphi(n) = \varphi\ (a^\alpha\ b^\beta_{\ldots}\ l^\lambda) = a^{\alpha-1}\ b^{\beta-1}_{\ldots}\ l^{\lambda-1}\ (a-1)\ (b-1)\ \ldots(l-1) =$$
$$= n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\ \ldots\ \left(1 - \frac{1}{l}\right).$$

Имея это выражение для функции $\varphi(n)$, можем, наконец, доказать теорему Гаусса. Для этой цели рассмотрим вообще функцию $\psi(n)$, обладающую свойством

$$\psi(mn) = \psi(m).\ \psi(n) \quad \text{при } D(m, n) = 1.$$

Рассмотрим числовой интеграл

$$\sum_n \psi(d) = \overset{\alpha'=\alpha}{\underset{\alpha'=0}{S}} \overset{\beta'=\beta}{\underset{\beta'=0}{S}} \dots \overset{\lambda'=\lambda}{\underset{\lambda'=0}{S}} \psi(a^{\alpha'} b^{\beta'} \dots l^{\lambda'})$$

Но

$$\psi(a^{\alpha'} b^{\beta'} \dots l^{\lambda'}) = \psi(a^{\alpha'})\,\psi(b^{\beta'}) \dots \psi(l^{\lambda'}),$$

а потому

$$\sum_\mu \psi(d) = \overset{\alpha'=\alpha}{\underset{\alpha'=0}{S}} \psi(a^{\alpha'}).\ \overset{\beta'=\beta}{\underset{\beta'=0}{S}} \psi(b^{\beta'}) \dots \overset{\lambda'=\lambda}{\underset{\lambda'=0}{S}} \psi(l^{\lambda'}) =$$
$$= \sum_{a^\alpha} \psi(d).\ \sum_{b^\beta} \psi(d) \dots \sum_{l^\lambda} \psi(d).$$

Итак, достаточно определить числовой интеграл типа $\sum\limits_{a^\alpha} \psi(d)$ для того, чтобы уметь вычислять общий числовой интеграл.

Обращаясь к функции $\varphi(n)$, имеем

$$\sum_{a^\alpha} \varphi(d) = \overset{\alpha'=\alpha}{\underset{\alpha'=0}{S}} \varphi(a^{\alpha'}) = \overset{\alpha'=\alpha}{\underset{\alpha'=0}{S}} [a^{\alpha'} - a^{\alpha'-1}] =$$
$$= 1 + a^2 - a + a^3 - a^2 + a^4 - a^3 + \dots +$$
$$+ a^{\alpha-1} - a^{\alpha-2} + a^\alpha - a^{\alpha-1} = a^\alpha$$

и следовательно

$$\sum_n \varphi(d) = a^\alpha b^\beta \dots l^\lambda = n.$$

§ 2. Общие свойства сравнений; теорема Фермата (малая).

Сравнением называем соединение двух чисел одного класса знаком $\equiv$ сравнения.

Теорема 1. Каждое число сравнимо само с собой по любому модулю.

$$a \equiv a,$$

ибо $a-a = 0$ принадлежит к любому модулю, (как совокупности чисел, кратных данному числу).

Теорема 2. Два числа, сравнимые с третьим, сравнимы между собою.

$$\frac{a \equiv c,\ b \equiv c}{a \equiv b} \qquad (Mod.\ m).$$

Первое доказательство. $a - c$ принадлежит к модулю, определяемому числом m, $b - c$ тоже, а следовательно и разность

$$(a - c) - (b - c) = a - b$$

принадлежит к тому же модулю, т.-е.

$$a \equiv b\ (Mod.\ m).$$

Второе доказательство. Из данных сравнений следует

$$a - c = mx,\quad b - c = my.$$

Вычитая, имеем

$$(a - c) - (b - c) = a - b = m\,(x - y),$$

откуда следует

$$a \equiv b\ (Mod.\ m).$$

Третье доказательство.

$$a - c \mid m,\ b - c \mid m$$

следовательно

$$(a - c) - (b - c) = a - b \mid m$$

и

$$a \equiv b\ (Mod.\ m).$$

Все эти доказательства весьма близки одно к другому, и дальнейшие теоремы не будем доказывать всегда всеми перечисленными способами.

Теорема 3. Сравнения можно почленно складывать и вычитать

$$\frac{a \equiv b\ (Mod.\ m)}{c \equiv d\ (Mod.\ m)}$$
$$a \pm c \equiv b \pm d\ (Mod\ m)$$

Доказательство.

$$\begin{matrix} a - b = mx \\ \pm \\ c - d = my \end{matrix}$$

Складывая или вычитая, имеем $(a \pm c) - (b \pm d) = m(x \pm y)$ а следовательно,

$$a \pm c \equiv b \pm d \ (Mod.\ m).$$

Теорема 4. Сравнения можно почленно перемножать.

$$\begin{matrix} a \equiv b \ (Mod.\ m) \\ c \equiv d \ (Mod.\ m) \\ \hline ac \equiv bd \ (Mod.\ m). \end{matrix}$$

Первое доказательство.

$$\begin{matrix} a = b + mx \\ c = d + my \end{matrix}$$

Перемножая, имеем $ac = bd + mxd + mby + m^2xy$,

откуда $ac - bd$ есть кратное m и следовательно

$$ac \equiv bd \ (Mod.\ m).$$

Второе доказательство. $a - b$ есть число модуля; следовательно и произведение $(a - b).\ c$ есть число модуля; точно также $c - d$, а след. и $(c - d).\ b$ есть число модуля. А в таком случае и $(a - b)\,c + (c - d)\,b = ac - bd$ есть тоже число модуля и следовательно,

$$ac \equiv bd \ (Mod.\ m).$$

Следствие 1. Если $a \equiv b \ (Mod.\ m)$,
то $a^p \equiv b^p \ (Mod.\ m)$.

Следствие 2. Если $a \equiv b \ (Mod.\ m)$,
то и $ak \equiv bk \ (Mod.\ m)$;

т.-е. две части сравнения можно умножать на одно и то же число.

Все перечисленные свойства сравнений вполне аналогичны свойствам равенств. Возникает вопрос о сокращении двух частей сравнения на одно и то же число. Ответ на этот вопрос дает.

Теорема 5. Две части сравнения можно сократить на общего множителя, разделив одновременно модуль на общего наибольшего делителя этого общего множителя и модуля.

$$\frac{ak \equiv bk \ (Mod.\ m)}{a \equiv b \ \left(Mod.\ \frac{m}{D(k,m).}\right)}$$

Доказательство.

Из данного сравнения следует

$$ak - bk = k(a-b) \mid m.$$

Пусть $D(k, m) = s$; $k = k's$, $m = m's$, так что $D(k',m') = 1$. Итак, имеем

$$k's.(a-b) \mid m's$$

или, по сокращении на s

$$k'(a-b) \mid m'.$$

Но так как $D(k',m') = 1$, то

$$a - b \mid m'$$

и следовательно $a \equiv b \ (Mod.\ m')$.

Следствие 1. Пусть $D(k, m) = s = 1$; тогда $m' = m$, и имеем $a \equiv b \ (Mod.\ m)$, т.-е. две части сравнения можно сокращать на общего множителя, взаимно-простого с модулем.

Следствие 2. Пусть $m \mid k$ и след. $D(k, m) = k$, тогда $m' = \frac{m}{k}$, и имеем $a \equiv b \ \left(Mod.\ \frac{m}{k}\right)$, т.-е. две части срав-

нения и модуль одновременно можно сокращать на общего множителя.

Теперь обращаемся к рассмотрению случая, когда два числа одновременно сравнимы по нескольким модулям.

Пусть

$$a \equiv b \ (Mod.\ m)$$
$$a \equiv b \ (Mod.\ m')$$
$$a \equiv b \ (Mod.\ m'')$$
$$\ldots\ldots\ldots$$

Это означает, что разность $a - b$ принадлежит к модулю, определяемому числом m и в то же время к модулю, определяемому числом m', и т. д. Но числа общие нескольким модулям, очевидно, образуют тоже некоторый модуль, ибо сумма и разность двух таких чисел тоже принадлежит одновременно модулям, определяемым числами $m, m', m'', \ldots$. Этот новый модуль характеризуется числом M, наименьшим положительным числом этого модуля. M есть, следовательно, наименьшее положительное число, принадлежащее одновременно к данным модулям, т.-е. кратное $m, m', m'', \ldots$; таким образом M есть общее наименьшее кратное $m, m', m'', \ldots$, и по модулю M оказываются сравнимыми a и b.

Итак, из сравнимости a и b по ряду модулей следует сравнимость этих же чисел по общему наименьшему кратному этих модулей.

Обратное положение, совершенно очевидное, можно выразить так: из сравнимости двух чисел по модулю следует их сравнимость по всем делителям этого модуля.

$$\frac{a \equiv b \ (Mod.\ m)}{a \equiv b \ (Mod.\ d), \text{ где } m \mid d.}$$

Пусть теперь имеем числа $m, m', m'', \ldots$ попарно взаимно-простые, т.-е.

$$D\ (m, m') = D\ (m, m'') = \ldots = D\ (m', m'') = \ldots = 1.$$

Тогда общее наименьшее кратное этих чисел равно их произведению, и из ряда сравнений

$$\begin{aligned} a &\equiv b \ (Mod.\ m) \\ a &\equiv b \ (Mod.\ m') \\ a &\equiv b \ (Mod.\ m'') \\ &\cdots\cdots\cdots \end{aligned} \qquad (1)$$

следует сравнение

$$a \equiv b \ (Mod.\ m\,m'm'' \ldots) \qquad (2)$$

Обратно из последнего сравнения следуют первоначально данные; таким образом группа сравнений (1) эквивалентна одному сравнению (2).

В частности пусть $n = a^{\alpha}\, b^{\beta} \ldots l^{\lambda}$ и пусть

$$A \equiv B \ (Mod.\ n)$$

тогда, согласно предыдущему, это сравнение эквивалентно системе сравнений

$$\begin{aligned} A &\equiv B \ (Mod.\ a^{\alpha}) \\ A &\equiv B \ (Mod.\ b^{\beta}) \\ &\cdots\cdots\cdots \\ A &\equiv B \ (Mod.\ l^{\lambda}) \end{aligned}$$

Выше были доказаны теоремы 1-я, 2-я, 3-я и 4-я относительно сравнений.

Из них можно вывести следующую общую теорему:

Пусть

$$a \equiv b \ (Mod.\ m)$$

и пусть $f(x) = a_0 x^h + a_1 x^{h-1} + a_2 x^{h-2} + \ldots + a_{h-1} x + a_h$ многочлен с целыми коэффициентами

В таком случае

$$f(a) \equiv f(b) \ (Mod.\ m).$$

Действительно, из сравнения

$$a \equiv b \ (Mod.\ m)$$

следует

$$a^{h-s} \equiv b^{h-s} \ (Mod.\ m)$$

и далее

$$a_s a^{h-s} \equiv a_s b^{h-s} \ (Mod.\ m);$$

складывая все такие сравнения для $s=0,1,2,\ldots.h$, получаем

$$f(a)\equiv f(b)\ (Mod.\ m)$$

Применим эту теорему к одному элементарному вопросу — к выводу признаков делимости.

Пусть число m написано по системе счисления с основанием N;

$$m=a_0N^h+a_1N^{h-1}+a_2N^{h-2}+\ldots+a_{h-1}N+a_h;$$

все a_s меньше N и суть цифры числа m.

Пусть k некоторое другое число и пусть

$$N\equiv r\ (Mod.\ k),$$

тогда по предыдущему

$$m\equiv a_0r^h+a_1r^{h-1}+a_2r^{h-2}+\ldots+a_{h-1}r+a_h\ (Mod.\ k).$$

Все числа одного класса имеют одних и тех же общих делителей с модулем; следовательно, если $m\mid k$, то и $a_0r^h+a_1r^{h-1}+\ldots+a_{h-1}r+a_h\mid k$ и обратно. Это и дает признак делимости числа m на k.

Пусть, например, $N=10$ и $k=9$; тогда r можно взять $=1$ и $a_0r^h+a_1r^{h-1}+\ldots+a_h=a_0+a_1+\ldots+a_h$ есть сумма цифр числа m; таким образом получаем известный элементарный признак делимости числа, написанного по десятеричной системе, на 9. Если $N=10$, $k=11$, то $r=-1$ и $m\equiv a_h-a_{h-1}+a_{h-2}-\ldots\pm a_0$ (Мод. 11); признак делимости числа на 11 получается такой: из суммы цифр, стоящих на нечетных местах, следует вычесть сумму цифр, стоящих на четных местах; полученная разность должна делиться на 11.

Теорема Фермата—Эйлера.

Рассмотрим линейную форму ax относительно модуля m, предполагая $D(a, m)=1$. Если x пробегает полную систему вычетов по модулю m, то и ax по доказанному (см. § 1) пробегает полную систему вычетов. Выберем из

полной системы вычеты, взаимно-простые с m, т.-е. заставим x пробегать приведенную систему вычетов

$$r_1,\ r_2,\ r_3,\ \ldots,\ r_{\varphi(m)}.$$

Для ax получаем значения

$$ar_1,\ ar_2,\ ar_3,\ \ldots,\ ar_{\varphi(m)};$$

все они различных классов, как было доказано, и все взаимно-просты с модулем m, ибо из $D(a,\ m)=1$ и $D(r_i,m)=1$ следует $D(ar_i,\ m)=1$.

Таким образом ax пробегает приведенную систему вычетов и поэтому каждое ar_i принадлежит к одному и тому же классу с некоторым r_j, так что имеем

$$ar_i \equiv r_j \ (Mod.\ m).$$

Перемножаем все подобные сравнения для всех значений $i=1,\ 2,\ \ldots\ \varphi(m)$. Слева получаем произведение $ar_1 \cdot ar_2 \ldots ar_{\varphi(m)} = a^{\varphi(m)}\ r_1 \cdot r_2 \ldots r_{\varphi(m)}$; справа произведение всех $r_1,\ r_2,\ \ldots\ r_{\varphi(m)}$, хотя и в другом порядке; таким образом имеем

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \ (Mod.\ m).$$

Но $D\ (r_1 r_2 \ldots r_{\varphi(m)},\ m)=1$, ибо каждое из r_i — взаимно-просто с m; поэтому, сокращая обе части сравнения на $r_1 r_2 \ldots r_{\varphi(m)}$, имеем

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

Это сравнение, в котором a — любое число взаимно-простое с m, и выражает теорему Фермата.

Рассмотрим пример: $m=9,\ a=14;\ \varphi\ (9)=6$

$$14^6 \equiv (Mod.\ 9).$$

Для поверки замечаем $14 \equiv 5\ (Mod.\ 9)$; $14^6 \equiv 5^6\ (Mod.\ 9)$; $5^6 \equiv 25 \cdot 5^4 \equiv 7 \cdot 5^4 = 35 \cdot 5^3 \equiv -1 \cdot 5^3 = -25 \cdot 5 \equiv 2 \cdot 5 = 10 \equiv 1\ (Mod.\ 9)$.

Важный частный случай теоремы имеем для $m=p$ — абсолютно-простого числа.

В этом случае $\varphi(m) = \varphi(p) = p - 1$, и мы имеем

$$a^{p-1} \equiv 1 \ (Mod.\ p),$$

если $D(a, p) = 1$, т.-е. если a не делится на p. Но можно теорему формулировать так, чтобы она имела место для любого числа. Помножим для этого две части предшествующего сравнения на a и получаем

$$a^p \equiv a \ (Mod.\ p).$$

Это сравнение справедливо по предыдущему, если a не делится на p, но оно имеет место и тогда, когда a делится на p, ибо тогда обе части делятся на p и следовательно сравнимы с нулем по модулю p.

Итак,

$$a^p \equiv a \ (Mod.\ p)$$

для любого числа a.

Ввиду важности доказанной теоремы дадим другой ее вывод методом математической индукции.

Так как

$$1^p \equiv 1 \ (Mod.\ p),$$

то теорема верна для $a = 1$. Допустим, что она верна для n; докажем, что она имеет место и для $n + 1$.

Итак, пусть

$$n^p \equiv n \ (Mod.\ p)$$

$$(n+1)^p = n^p + \frac{p}{1} \cdot n^{p-1} + \frac{p(p-1)}{1 \cdot 2} \cdot n^{p-2} + \ldots +$$

$$+ \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \ldots k} n^{p-k} + \ldots + 1.$$

Легко усмотреть, что все биномиальные коэффициенты за исключением крайних (1-ца и 1-ца) делятся на p. В самом деле

$$\frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \cdot 3 \ldots k}$$

есть целое число; следовательно произведение

$$p \cdot [(p-1)\ (p-2)\ldots(p-k+1)]$$

делится на $1 . 2 . 3 \ldots k$; так как $k < p$, то $D(p, 1 . 2 . 3 \ldots k) = 1$, а следовательно

$$(p-1)\ (p-2) \ldots (p-k+1) \mid 1 . 2 . 3 \ldots k$$

и потому биномиальный коэффициент есть число кратное p. Раз так, то все члены разложения $(n+1)^p$, кроме первого и последнего, делятся на p, и значит

$$(n+1)^p \equiv n^p + 1 \ (Mod.\ p).$$

Вычитая из двух частей по $n+1$, получаем

$$(n+1)^p - (n+1) \equiv n^p - n \ (Mod.\ p)$$

и так как по предположению

$$n^p - n \equiv 0 \ (Mod.\ p),$$

то

$$(n+1)^p - (n+1) \equiv 0 \ (Mod.\ p).$$

Итак, если теорема верна для n, то и для $n+1$, а т. к. она верна для $n = 1$, то в силу принципа математической индукции, она верна вообще.

Дадим еще третье доказательство этой теореме:

$$a = 1 + 1 + 1 + \ldots + 1$$

$$a^p = (1 + 1 + 1 + \ldots + 1)^p = 1^p + 1^p + 1^p + \ldots + 1^p + \\ + SS \ldots S \frac{p!}{\alpha_1!\, \alpha_2! \ldots \alpha_a!} \cdot 1^{\alpha_1} \cdot 1^{\alpha_2} \ldots 1^{\alpha_a}$$

где

$$\alpha_1 + \alpha_2 + \ldots + \alpha_a = p.$$

Полиномиальный коэффициент $\frac{p!}{\alpha_1!\, \alpha_2! \ldots \alpha_a!}$ есть число целое; следовательно

$$[1 . 2 . 3 \ldots (p-1)] . p \mid \alpha_1!\, \alpha_2! \ldots \alpha_a!$$

Но

$$D(p,\ \alpha_1!\ \alpha_2!\ldots\alpha_a!) = 1,$$

значит

$$1\cdot 2\cdot 3\ldots(p-1)\ |\ \alpha_1!\ \alpha_2!\ldots\alpha_a!$$

и следовательно все полиномиальные коэффициенты — кратные p, а отсюда непосредственно заключаем

$$a^p = (1+1+\ldots+1)^p \equiv 1^p+1^p+\ldots+1^p \equiv 1+1+\ldots+1 \equiv$$
$$\equiv a\ (Mod.\ p).$$

ГЛАВА ПЯТАЯ.

§ 1. Сравнения с одной неизвестной; понятие об их решении.

Общие свойства сравнений, рассмотренные нами, вполне аналогичны свойствам равенств; можно сказать, что сравнение есть равенство с точностью до кратных модуля. Руководствуясь упомянутой аналогией, естественно обратиться далее к рассмотрению для сравнений вопроса, аналогичного вопросу о решении уравнений. Подобно тому, как алгебра рассматривает равенства, содержащие неизвестные, так называемые уравнения, и изыскивает те значения неизвестных, для которых эти равенства удовлетворяются, точно так же будем рассматривать сравнения, содержащие неизвестные x, y, z,...., и будем изыскивать те (целые) значения неизвестных, для которых сравнения удовлетворяются; найти эти значения значит „решить“ сравнения.

Мы ограничимся сравнениями с одной неизвестной x и, главным образом, алгебраическими.

В силу общего свойства сравнений, согласно которому к двум частям сравнения можно прибавлять и отнимать поровну, легко заключаем, что в сравнении, как и в равенстве можно члены переносить из одной части в другую с обратным знаком. Для полноты приведем доказательства этого следствия:

Пусть

$$a + b - c \equiv d - e + f (Mod.\ m).$$

Имеем, очевидно

$$c \equiv c \ (Mod.\ m)$$
$$-d \equiv -d \ (Mod.\ m).$$

Складывая почленно, получаем

$$a + b - d \equiv c - e + f \ (Mod.\ m)$$

и видим, что члены $-c$ и $+d$ перенесены из одной части в другую с обратными знаками.

Опираясь на это свойство, мы всякое алгебраическое сравнение с одной неизвестной можем привести к виду

$$f(x) \equiv 0 \ (Mod.\ m),$$

где

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

многочлен с целыми коэффициентами.

Возникает вопрос, можно ли две части сравнения сокращать на общий численный фактор, подобно тому как это делается для уравнений, или множить две части на общий фактор. Если принять во внимание ранее изложенные общие свойства сравнений, то ясно, что это возможно в том случае, когда упомянутый фактор — число взаимно-простое с модулем. Если же сокращаем две части на фактор, не взаимно-простой с модулем, то и модуль приходится разделить на общий наибольший делитель модуля и упомянутого фактора.

Допустим теперь, что число a удовлетворяет сравнению

$$f(x) \equiv 0 \ (Mod.\ m)$$

так что

$$f(a) \equiv 0 \ (Mod.\ m),$$

и пусть β есть число того же класса, что a, так что

$$\beta \equiv a \ (Mod.\ m).$$

Тогда в силу свойства, доказанного в гл. IV

$$f(\beta) \equiv f(a) \equiv 0 \ (Mod.\ m),$$

и следовательно одновременно с числом a все числа класса, представителем которого служит a, удовлетворяют тому же сравнению. Таким образом сравнению

$$f(x) \equiv 0 \ (Mod.\ m)$$

всегда удовлетворяют не отдельные числа, а целые классы чисел по модулю m. Мы будем называть решением сравнения не одно число a, а весь соответствующий класс чисел, так что решение определяется сравнением

$$x \equiv a \ (Mod.\ m),$$

и в этом—полная аналогия с решениями уравнений, которые определяются равенством вида $x = a$.

Из изложенного следует, что для нахождения всех решений сравнения

$$f(x) \equiv 0 \ (Mod.\ m)$$

достаточно испытать какую-либо полную систему вычетов по модулю m, например, числа ряда 0, 1, 2, 3, ..., m—1.

Сколько чисел этого ряда окажется удовлетворяющих данному сравнению, столько это последнее имеет решений. Решения эти состоят из классов чисел, имеющих представителями те числа ряда 0, 1, 2, ..., m—1, которые удовлетворяют данному сравнению.

Пусть, например, дано сравнение

$$x^2 \equiv 4 \ (Mod.\ 5).$$

Испытываем ряд чисел 0, 1, 2, 3, 4. При подстановке оказывается, что сравнению удовлетворяют числа 2 и 3, ибо

$$2^2 = 4 \equiv 4 \ (Mod.\ 5) \text{ и } 3^2 = 9 \equiv 4 \ (Mod.\ 5).$$

Таким образом данное сравнение имеет два решения

$$x \equiv 2 \ (Mod.\ 5) \text{ и } x \equiv 3 \ (Mod.\ 5).$$

Первое решение состоит из класса чисел

$$\ldots, -8, -3, 2, 7, 12, \ldots$$

второе—из класса

$$\ldots, -7, -2, 3, 8, 13, \ldots$$

Покажем теперь, как решение сравнения

$$f(x) \equiv 0 \ (Mod.\ m)$$

может быть сведено к решению совсем иной задачи теории чисел.

Сравнение

$$f(x) \equiv 0 \ (Mod.\ m)$$

выражает требование, чтобы левая часть была числом кратным модулю m. Таким образом мы должны иметь

$$f(x) = my,$$

и, следовательно, задача решения данного сравнения вполне эквивалентна задаче решения в целых числах неопределенного уравнения с двумя неизвестными x, y:

$$f(x) = my.$$

Мы видим, следовательно, что решение сравнений есть частный случай общей задачи решения в целых числах неопределенных уравнений. Эта последняя задача составляет предмет главы теории чисел, известной под названием неопределенного анализа. Теория сравнений есть теория неопределенных уравнений первой степени относительно одного из неизвестных.

Из других задач неопределенного анализа упомянем задачу решения в целых числах неопределенного уравнения 2-й степени

$$ax^2 + bxy + cy^2 = m.$$

Решение этого уравнения тесно связано с исследованием левой части уравнения для целых значений x, y, что составляет предмет так называемой теории бинарных квадратичных форм — одной из глав классической теории чисел.

§ 2. Решение сравнений первой степени.

Сравнение первой степени перенесением членов из одной части в другую и приведением подобных членов всегда может быть приведено к виду

$$ax \equiv b \ (Mod.\ m) \tag{1}$$

Согласно замечанию, сделанному в конце предшествующего параграфа, решение этого сравнения эквивалентно решению в целых числах неопределенного уравнения

$$ax - my = b, \tag{2}$$

и таким образом методы, которые существуют для решения этого неопределенного уравнения (между прочим, метод непрерывных дробей), приводят и к решению сравнения (1). Но мы в дальнейшем пойдем иным путем и рассмотрим задачу о решении сравнения (1) независимо от решения неопределенного уравнения (2). При этом приходится рассматривать два случая:

1) Пусть, во-первых, коэффициент a взаимно-прост с модулем m: $D(a, m)=1$. Докажем, что сравнение в этом случае всегда возможно и имеет одно и только одно решение. Для доказательства рассмотрим линейную форму

$$ax - b$$

и будем подставлять в нее вместо x какую-либо полную систему вычетов, например, значения $x = 0, 1, 2, \ldots, m-1$. Так как $D(a, m) = 1$, то согласно теореме, доказанной в главе IV, получим при этом полную систему вычетов и, следовательно, один и только один раз получим число, принадлежащее к одному классу с числом 0. Таким образом для одного и только для одного из чисел ряда

$$0, 1, 2, \ldots, m-1 \tag{3}$$

будем иметь $ax - b \equiv 0 \ (Mod.\ m)$ или

$$ax \equiv b \ (Mod.\ m),$$

а это, согласно изложенному в § 1, и означает, что данное сравнение (1) имеет одно решение, определяемое сравнением

$$x \equiv \alpha \ (Mod.\ m),$$

где α—число ряда (3), удовлетворяющее сравнению (1). Число α находится попытками — путем последовательных подстановок в сравнение (1) чисел ряда (3).

Вместо этого способа попыток можно предложить другой, основанный на применении теоремы Фермата.

Так как $D(a, m) = 1$, то на основании упомянутой теоремы

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

и легко видеть, что решение сравнения (1) есть

$$x \equiv b a^{\varphi(m)-1} \ (Mod.\ m). \qquad (4)$$

В самом деле, вставляя $ba^{\varphi(m)-1}$ вместо x в данное сравнение, имеем

$$a.ba^{\varphi(m)-1} = a^{\varphi(m)}.\ b \equiv 1.\ b \equiv b \ (Mod.\ m).$$

Возьмем числовой пример

$$12x \equiv 5 \ (Mod.\ 25).$$

Так как $D(12, 25) = 1$, то имеем рассмотренный 1-й случай. Испытываем числа 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ..., 24. При $x = 15$ получаем

$$12.15 = 180 \equiv 5 \ (Mod.\ 25).$$

Итак, решение сравнения есть

$$x \equiv 15 \ (Mod.\ 25).$$

Применяем второй метод

$$x \equiv 5.12^{\varphi(25)-1} \equiv 5.12^{5^2-5-1} \equiv 5.12^{19} \ (Mod.\ 25).$$

Дальнейшие выкладки можем вести так:

$$x \equiv 5.12^{19} \equiv 5.12.12^{18} \equiv 5.12.144^9 \equiv 5.12(-6)^9 \equiv 5.12.(-6).$$
$$(-6)^8 \equiv 5.12.(-6).36^4 \equiv 5.12.(-6).11^4 \equiv -360.11^4 \equiv$$
$$\equiv -10.121^2 \equiv -10.(-4)^2 \equiv -160 \equiv 15 \ (Mod.\ 25).$$

2) Пусть, во-вторых, $D(a,m) = \delta > 1$. Для возможности сравнения необходимо, чтобы известный член b делился на δ. В самом деле для любого значения x число $ax \mid \delta$,

и следовательно ax и модуль m имеют общего делителя δ; но число b одного класса с ax и следовательно должно иметь тех же общих делителей с модулем, как и ax, а потому необходимо $b|\delta$. Итак, пусть это требование выполнено; тогда можем сократить две части сравнения и модуль сравнения (1) на δ и получим сравнение

$$a'x \equiv b' \ (Mod.\ m') \tag{5}$$

если положим

$$a = a'\delta,\ b = b'\delta,\ m = m'\delta.$$

Из сравнения (1) следует сравнение (5), но и обратно, из сравнения (5) следует сравнение (1). В самом деле, из сравнения (5) имеем

$$a'x - b' = m'k;$$

умножая две части равенства на δ, получаем

$$ax - b = mk,$$

или

$$ax \equiv b \ (Mod.\ m).$$

Таким образом, решение сравнений (1) и (5) — две эквивалентные задачи. Так как a' и m' — частные от деления a и m на их общего наибольшего делителя, то $D(a',m')=1$ и следовательно мы имеем при решении сравнения (5) выше разобранный первый случай. Сравнение (5) таким образом имеет одно решение

$$x \equiv \alpha \ (Mod.\ m') \tag{6}$$

и эти же числа, образующие один класс по модулю m', удовлетворяют и сравнению (1). Но один класс по модулю m', как легко убедимся, распадается на несколько классов по модулю m, и таким образом первоначальное сравнение приходится считать имеющим несколько решений, ибо за одно решение для него считаем класс чисел по модулю m. Чтобы разбить решения (6) на классы по модулю m, замечаем, что из сравнения (6) следует

$$x = \alpha + m'y \tag{7}$$

Давая y значение $0, 1, 2, 3, \ldots\ldots\ldots, \delta - 1$, получаем значения

$$x = \alpha,\ \alpha + m',\ \alpha + 2m',\ \ldots,\ \alpha + (\delta - 1)\, m', \qquad (8)$$

которые все принадлежат к различным классам по модулю m; действительно разность двух каких-либо чисел ряда (8) есть

$$\alpha + y_1 m' - (\alpha + y_2 m') = (y_1 - y_2)m',$$

где $y_1 - y_2 < \delta$ и следовательно эта разность меньше $\delta m' = m$ и не может быть кратным m. С другой стороны, всякое число вида (7) сравнимо с одним из чисел ряда (8) по модулю m. Действительно, относительно числа δ число y представимо в виде

$$y = k\delta + r,$$

где

$$0 \leqslant r < \delta.$$

Таким образом

$$x = \alpha + m'y = \alpha + k\delta m' + rm' = \alpha + rm' + km,$$

где $\alpha + rm'$ есть одно из чисел ряда (8). В конце концов оказывается, что сравнение (1) имеет δ различных решений

$$\begin{gathered} x \equiv \alpha \ (Mod.\ m) \\ x \equiv \alpha + m' \ (Mod.\ m) \\ x \equiv \alpha + 2m' \ (Mod.\ m) \\ \ldots\ldots\ldots\ldots \\ x \equiv \alpha + (\delta - 1)\ m' \ (Mod.\ m). \end{gathered} \qquad (9)$$

Рассмотрим численный пример

$$42x \equiv 132 \ (Mod.\ 30).$$

$D(42,30) = 6$; условие возможности $132 \mid 6$ выполнено. По сокращении на 6 имеем

$$7x \equiv 22 \ (Mod.\ 5)$$

Испытывая числа $0, 1, 2, 3, 4$, находим решение

$$x \equiv 1 \ (Mod.\ 5),$$

которое дает 6 решений

$$x \equiv 1, 6, 11, 16, 21, 26 \ (Mod.\ 30)$$

первоначального сравнения.

Рассмотрим один важный частный случай сравнения первой степени, а именно сравнение

$$ax \equiv 1 \ (Mod.\ m), \tag{10}$$

при чем $D(a,m) = 1$. Согласно предыдущему сравнение это имеет единственное решение; назовем его a', так что

$$aa' \equiv 1 \ (Mod.\ m). \tag{11}$$

Легко видеть, что и $D(a', m) = 1$, т. к. если бы a' и m имели общего делителя, отличного от 1, то левая часть и модуль сравнения (11) делились бы на это число, а следовательно, и правая часть, т.-е. 1, должна была бы делиться на это число, что невозможно. Два числа a и a', как видно из сравнения (11), равноправны, и если рассмотрим сравнение

$$a'x \equiv 1 \ (Mod.\ m), \tag{12}$$

то ему удовлетворяет число a.

Такие два числа, как a и a', называются союзными числами (numeri socii). В сущности приходится говорить о союзных классах чисел, и все классы чисел, взаимно-простых с модулем, распределяются на пары союзных классов.

Числа, взаимно-простые с модулем, называют единицами по модулю; таким образом классы единиц по модулю распределяются в пары союзных классов. Две единицы a и a' союзных классов связаны соотношением вида (11).

§ 3. Совокупные сравнения 1-й степени.

Пусть требуется определить неизвестное x так, чтобы для него одновременно удовлетворялся ряд сравнений:

$$\left.\begin{aligned} ax &\equiv b \ (Mod.\ m) \\ a'x &\equiv b' \ (Mod.\ m') \\ a''x &\equiv b'' \ (Mod.\ m'') \\ &\cdots\cdots\cdots \end{aligned}\right\} \tag{1}$$

Первый метод определения x есть метод последовательного решения. Пусть одно из решений первого сравнения

$$ax \equiv b \ (Mod.\ m)$$

есть

$$x \equiv \alpha \ (Mod.\ m);$$

отсюда

$$x = \alpha + my,$$

где y любое целое число. Вставляем это выражение во 2-е сравнение; получаем сравнение первой степени

$$a'my \equiv b' - a'\alpha \ (Mod.\ m')$$

с неизвестным y. Пусть его решение есть

$$y \equiv \beta \ (Mod.\ m')$$

Отсюда

$$y = \beta + m'z.$$

Подставляя в 3-е сравнение

$$x = \alpha + my = mm'z + \alpha + m\beta,$$

получаем сравнение 1-й степени

$$a''mm'z \equiv b'' - a''\alpha - a''m\beta$$

для определения z, и т. д. В конце концов, если только система (1) совместна, найдем выражение для x, удовлетворяющее одновременно всем сравнениям системы.

Пример.

$5x \equiv 7$ (*Mod.* 9); $2x \equiv 10$ (*Mod.* 6); $3x \equiv 5$ (*Mod.* 4). Подставляя в 1-е сравнение числа 0, 1, 2, 3, 4, 5, 6, 7, 8, находим его решение

$$x \equiv 5 \ (Mod.\ 9).$$

Подставляя

$$x = 5 + 9y$$

во 2-е, находим

$$10 + 18y \equiv 10 \ (Mod.\ 6)$$

или

$$18y \equiv 0 \ (Mod.\ 6)$$

или, по сокращении

$$3y \equiv 0 \ (Mod.\ 1).$$

Очевидно, для любого y это сравнение удовлетворяется, т. к. на 1-цу делится всякое число. Таким образом остается

$$x = 5 + 9y$$

вставить в третье сравнение; получаем

$$15 + 27y \equiv 5 \ (Mod.\ 4)$$

или

$$27y \equiv -10 \ (Mod.\ 4).$$

Решение этого сравнения есть

$$y \equiv 2 \ (Mod.\ 4)$$

Таким образом $y = 2 + 4z$

и, подставляя в выражение x, имеем

$$x = 5 + 18 + 36z = 23 + 36z,$$

где z — произвольное число. Отсюда следует

$$x \equiv 23 \ (Mod.\ 36)$$

и таким образом один класс чисел по модулю 36 образует решение данной совокупной системы.

Дадим второй метод решения системы сравнений, более совершенный в теоретическом отношении.

Имея систему

$$\begin{aligned} ax &\equiv b \quad (Mod.\ m) \\ a'x &\equiv b' \quad (Mod.\ m') \\ a''x &= b'' \quad (Mod.\ m'') \\ &\cdots\cdots\cdots \end{aligned} \tag{1}$$

решаем в отдельности каждое сравнение и пусть решения их будут

$$\begin{aligned} x &\equiv \alpha \ (Mod.\ m) \\ x &\equiv \beta \ (Mod.\ m') \\ x &\equiv \gamma \ (Mod.\ m'') \\ &\cdots\cdots\cdots \end{aligned} \tag{2}$$

Очевидно, число x, удовлетворяющее системе (1), должно одновременно удовлетворять всем сравнениям (2), и таким образом решение системы (1) приводится к решению более простой системы (2). Заметим, что 2-я система может быть не единственная для данной системы (1). В самом деле каждое из сравнений (1) может допускать не одно, а несколько

решений, а тогда всевозможные системы (2) получим, комбинируя всеми возможными способами все решения α 1-го сравнения со всеми решениями β 2-го, со всеми решениями γ 3-го и т. д.

Обращаемся к дальнейшему упрощению системы (2). Пусть разложение на простые множители первого модуля m есть

$$m = p^{\pi} \cdot q^{\varkappa} \ldots.$$

Тогда сравнение $x \equiv a (Mod.\ m)$ эквивалентно, как было показано, ряду сравнений

$$x \equiv a\ (Mod.\ p^{\pi}),\quad x \equiv a\ (Mod.\ q^{\varkappa}) \ldots.$$

Так же поступаем со вторым, третьим и т. д. сравнением системы (2). В результете получим систему сравнений по модулям, которые суть степени простых чисел. При этом может оказаться, что два или более из этих сравнений имеют место по модулям, которые суть степени одного и того же простого числа. Например, p может входить в разложения m и m', и тогда имеем одновременно

$$x \equiv a\ (Mod.\ p^{\pi}) \text{ и } x \equiv a'\ (Mod.\ p^{\pi'}) \qquad (3)$$

Пусть $\pi > \pi'$; в таком случае $p^{\pi'}$ есть делитель p^{π} и следовательно на-ряду с первым сравнением имеет место сравнение

$$x \equiv a\ (Mod.\ p^{\pi'}).$$

Сравнивая его со вторым, приходим к условию

$$a \equiv a'\ (Mod.\ p^{\pi'})$$

непротиворечивости двух сравнений (3). Пусть оно выполнено; тогда, оставляя 1-е сравнение без изменения, 2-е можем написать в виде

$$x \equiv a\ (Mod.\ p^{\pi'}).$$

Так как $\pi > \pi'$, то последнее сравнение есть следствие 1-го из сравнений (3), и таким образом 2-е из этих сравнений поглощается первым. Таким образом каждые два сравнения по модулям, которые суть степени одного и того же про-

стого числа, сводятся к одному; поступая так последовательно, мы и несколько сравнений этого типа сведем к одному и, в конце концов, приведем данную систему к системе вида

$$\begin{aligned} x &\equiv \alpha \ (Mod.\ p^{\pi}) \\ x &\equiv \beta \ (Mod.\ q^{\varkappa}) \\ x &\equiv \gamma \ (Mod.\ r^{\varrho}) \\ &\ldots\ldots\ldots \end{aligned} \tag{4}$$

Эту систему и предстоит нам разрешить. Мы рассмотрим более общую задачу, а именно решение системы

$$\begin{aligned} x &\equiv \alpha \ (Mod.\ a) \\ x &\equiv \beta \ (Mod.\ b) \\ x &\equiv \gamma \ (Mod.\ c) \\ &\ldots\ldots\ldots \end{aligned} \tag{5}$$

где все модули попарно взаимно-простые:

$$D(a,b) = D(b,c) = D(a,c) = \ldots\ldots = 1.$$

Очевидно, система (4) есть частный случай системы (5).

Для решения системы (5) определим ряд чисел $r, s, t, \ldots$, которые бы удовлетворяли условиям:

$$\begin{array}{lll} r \equiv 1 \ (Mod.\ a) & s \equiv 0 \ (Mod.\ a) & t \equiv 0 \ (Mod.\ a) \\ r \equiv 0 \ (Mod.\ b) & s \equiv 1 \ (Mod.\ b) & t \equiv 0 \ (Mod.\ b) \\ r \equiv 0 \ (Mod.\ c) & s \equiv 0 \ (Mod.\ c) & t \equiv 1 \ (Mod.\ c) \\ \ldots\ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots \end{array} \tag{6}$$

Каждое из этих чисел сравнимо с 1 по одному из модулей и с 0 по всем остальным. Это означает для r, например, что r делится на b, на c, ... и следовательно, т. к. все модули попарно взаимно-простые, есть кратное произведения $bc\ldots$. Полагая $r = r'bc\ldots$, имеем

$$bc\ldots r' \equiv 1 \ (Mod.\ a),$$

откуда и найдем r'; r' есть numerus socius для произведения $bc\ldots$ всех модулей, кроме a. Точно также найдем

$$s = s'.\ ac\ldots,$$

где s' — союзное число для произведения $ac\ldots\ldots$ по модулю b, и т. д. Найдя r, s, $t\ldots\ldots$, имеем формулу

$$x \equiv r\alpha + s\beta + t\gamma + \ldots\ldots \ (Mod.\ abc\ldots\ldots) \qquad (7)$$

решения системы (5).

В самом деле, т. к. по определению r, s, t, $\ldots\ldots$ первое из этих чисел сравнимо с 1 по модулю a, а все остальные делятся на a, то имеем

$$r\alpha + s\beta + t\gamma + \ldots\ldots \equiv \alpha \ (Mod.\ a)$$

и аналогично

$$r\alpha + s\beta + t\gamma + \ldots\ldots \equiv \beta \ (Mod.\ b)$$
$$r\alpha + s\beta + t\gamma + \ldots\ldots \equiv \gamma \ (Mod.\ c)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

и следовательно сравнения системы (5) можно представить в виде:

$$\begin{aligned} x &\equiv r\alpha + s\beta + t\gamma + \ldots\ldots \ (Mod.\ a) \\ x &\equiv r\alpha + s\beta + t\gamma + \ldots\ldots \ (Mod.\ b) \\ x &\equiv r\alpha + s\beta + t\gamma + \ldots\ldots \ (Mod.\ c) \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \qquad (8)$$

А в такой форме очевидно, что эта система эквивалентна одному сравнению (7), ибо модули a, b, c, $\ldots\ldots$ суть делители модуля $abc\ldots\ldots$, а с другой стороны, модуль $abc\ldots\ldots$ есть наименьшее кратное модулей a, b, $c\ldots\ldots$

ГЛАВА ШЕСТАЯ.

Алгебраические сравнения высших степеней.

§ 1. Общая теория.

Общий вид алгебраического сравнения есть

$$f(x) \equiv 0 \ (Mod.\ m), \tag{1}$$

где

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots\ldots + a_{n-1} x + a_n \tag{2}$$

многочлен с целыми коэффициентами.

Пусть имеем ряд чисел a_0', a_1', $\ldots\ldots a_n'$ таких, что

$$\begin{aligned} a_0' &\equiv a_0 \ (Mod.\ m) \\ a_1' &\equiv a_1 \ (Mod.\ m) \\ &\cdots\cdots\cdots \\ a_n' &\equiv a_n \ (Mod.\ m). \end{aligned} \tag{3}$$

Умножая две части каждого из этих сравнений на x^n, x^{n-1}, $\ldots$, x, 1 и складывая, получаем

$$a_0' x_n + a'_1 x^{n-1} + \ldots + a'_{n-1} x + a_n' \equiv f(x) \ (Mod.\ m)$$

для любого значения x, и таким образом усматриваем, что данное сравнение (1) эквивалентно сравнению

$$a_0' x^n + a_1' x^{n-1} + a'_2 x^{n-2} + \ldots + a'_n \equiv 0 \ (Mod.\ m). \tag{4}$$

т.-е. другими словами—коэффициенты членов сравнения можно заменять любыми числами, с ними

сравнимыми по модулю сравнения. В частности, члены, коэффициенты которых делятся на модуль, можно вовсе отбрасывать, т. к. коэффициенты их сравнимы с нулем.

Отсюда между прочим явствует, что определение степени сравнения требует известной предосторожности: если многочлен $f(x)$ — n-й степени, то мы можем сказать, что сравнение (1) есть сравнение n-й степени только при условии, что старший коэффициент a_0 не делится на модуль; в противном случае член a_0x^n можно отбросить, и вообще степень сравнения есть степень наивысшего из членов, коэффициенты которых не делятся на модуль.

Так, сравнение

$$16x^5 - 4x^4 + 5x^3 - 2x^2 + 4x - 1 \equiv 0 \ (Mod.\ 4)$$

не 5-й степени, а только 3-й, и оно эквивалентно сравнению

$$x^3 - 2x^2 - 1 \equiv 0 \ (Mod.\ 4).$$

Пусть разложение модуля m на простые факторы есть

$$m = p^\pi q^\varkappa r^\varrho \ldots\ldots$$

В таком случае сравнение (1), как было выяснено в свое время, эквивалентно системе сравнений

$$\begin{aligned} f(x) &\equiv 0 \ (Mod.\ p^\pi) \\ f(x) &\equiv 0 \ (Mod.\ q^\varkappa) \\ f(x) &\equiv 0 \ (Mod.\ r^\varrho) \\ &\cdots\cdots\cdots \end{aligned} \qquad (5)$$

и решение сравнения (1) приводится к решению системы (5). Докажем теперь, что решение системы (5) приводится к решению в отдельности каждого из сравнений, входящих в состав этой системы. Пусть, в самом деле, мы решили в отдельности каждое из упомянутых сравнений и решения эти суть:

$$\begin{aligned} x &\equiv \alpha \ (Mod.\ p^\pi) \\ x &\equiv \beta \ (Mod.\ q^\varkappa) \\ x &\equiv \gamma \ (Mod.\ r^\varrho) \\ &\cdots\cdots\cdots \end{aligned} \qquad (6)$$

Но тогда всякое число x, удовлетворяющее системе (5), должно одновременно удовлетворять всем сравнениям (6) и обратно, и таким образом решение системы (5) приводится к решению в отдельности каждого из сравнений этой системы и затем к решению системы (6) совокупных сравнений 1-й степени — задаче, рассмотренной в главе V (§ 3). Если при решении отдельных сравнений (5) получается по нескольку решений, то их приходится комбинировать всеми возможными способами, и таким образом получается не одна, а несколько систем вида (6).

В результате предшествующих рассуждений выясняется, что решение общего алгебраического сравнения приводится к решению сравнения вида

$$f(x) \equiv 0 \ (Mod.\ p^{\pi}) \tag{7},$$

т.-е. сравнения по модулю, который есть степень простого числа. Рассмотрим эту последнюю задачу. Заметим прежде всего, что всякое решение сравнения (7) удовлетворяет и сравнению типа

$$f(x) \equiv 0 \ (Mod.\ p^{\pi'}) \tag{8},$$

где $\pi' < \pi$; это непосредственно ясно из того, что модуль $p^{\pi'}$ есть делитель модуля p^{π}. Между прочим, все решения сравнения (7) удовлетворяют и сравнению

$$f(x) \equiv 0 \ (Mod.\ p) \tag{9}$$

и найдутся среди решений этого последнего. Покажем теперь, как можно итти последовательно: найдя решения сравнения (9) по модулю p, найти решения сравнения по модулю p^2, затем по модулю p^3 и т. д. и, наконец, дойти до данного сравнения.

Пусть мы решили сравнение

$$f(x) \equiv 0 \ (Mod.\ p^{\pi'}); \tag{10}$$

покажем, как тогда решить сравнение

$$f(x) \equiv 0 \ (Mod.\ p^{\pi'+1}). \tag{11}$$

Все решения сравнения (11) удовлетворяют сравнению (10), значит найдутся среди его решений. Обратного утверждения высказать нельзя: среди решений сравнения (10) могут быть такие, которые не удовлетворяют сравнению (11), и надо из решений сравнения (10) выбрать те, которые одновременно удовлетворяют и сравнению (11).

Пусть решение сравнения (10) есть

$$x \equiv a \ (Mod.\ p^{\pi'})$$

или

$$x = a + p^{\pi'} \cdot y. \tag{12}$$

При любом целом значении y выражение (12) удовлетворяет сравнению (10); подберем y так, чтобы удовлетворялось сравнение (11). Подставляя вместо x его выражение (12) в сравнение (11), получаем

$$f(a + p^{\pi'} . y) \equiv 0 \ (Mod.\ p^{\pi'+1})$$

или, развертывая по степеням $p^{\pi'} \cdot y$,

$$f(a) + p^{\pi'} \cdot y \cdot \frac{f'(a)}{1} + p^{2\pi'} \cdot y^2 \cdot \frac{f''(a)}{1 \cdot 2} +$$
$$+ p^{3\pi'} \cdot y^3 \cdot \frac{f'''(a)}{1 \cdot 2 \cdot 3} + \cdots \equiv 0 \ (Mod.\ p^{\pi'+1}). \tag{13}$$

В левой части мы имеем конечное число членов, и коэффициенты

$$\frac{f'(a)}{1}, \quad \frac{f''(a)}{1 \cdot 2}, \quad \frac{f'''(a)}{1 \cdot 2 \cdot 3}, \quad \ldots$$

— целые числа, что следует из того, что $f(x)$ есть многочлен и разложение (13) можно бы получить хотя бы элементарным путем, заменяя в каждом члене $f(x)$ x его выражением (12) и развертывая по биному Ньютона. Начиная с третьего члена, все члены содержат степени p бо́льшие $\pi' + 1$ и потому делятся на модуль. Отбрасывая их, получаем сравнение

$$f(a) + p^{\pi'} y f'(a) \equiv 0 \ (Mod.\ p^{\pi'+1}) \tag{14}$$

Так как a есть корень сравнения (10), то $f(a)$ делится на $p^{\pi'}$, и мы имеем

$$f(a) = k \cdot p^{\pi'}.$$

Вставляя в сравнение и сокращая оба члена и модуль на $p^{\pi'}$, окончательно получаем для определения y сравнение 1-й степени

$$k + f'(a) \cdot y \equiv 0 \ (Mod.\ p). \tag{15}$$

Решив его и вставив найденное выражение y в формулу (12), найдем решение сравнения (11). Умея таким образом переходить от сравнения (10) к сравнению (11), мы решение сравнения (7) сведем к решению сравнения (9) $f(x) \equiv 0$ $(Mod.\ p)$, от которого будем последовательно восходить к сравнениям по модулю p^2, p^3, ... и, наконец, p^π путем решения ряда сравнений 1-й степени типа (15).

Примечание. Выше было указано, что решение сравнения (7) приводится к решению сравнения (9) по модулю простому и ряда сравнений первой степени типа (15). Следует разобрать, возможно ли это последнее сравнение и имеет ли оно определенное решение. Коэффициент $f'(a)$, вообще говоря, не делится на модуль p и следовательно взаимно-прост с ним, а в таком случае сравнение (15) возможно и имеет единственное решение, так что y определяется равенством вида

$$y = y_0 + zp,$$

где z — произвольное целое число. Подставляя в формулу (12), имеем

$$x = a + y_0 p^{\pi'} + z \cdot p^{\pi'+1},$$

или

$$x \equiv a + y_0 p^{\pi'} \ (Mod.\ p^{\pi'+1})$$

— решение сравнения (11); таким образом из одного решения сравнения (10) получаем одно решение сравнения (11). Исключение имеет место тогда, когда $f'(a)$ делится на p. В этом случае в сравнении (15) член, содержащий y отпадает, и мы имеем

$$k \equiv 0 \ (Mod.\ p). \tag{16}$$

Приходится различать два случая:

1) Пусть число k делится на p; тогда сравнение (16) удовлетворяется; число y остается произвольным, и все решения сравнения (10) удовлетворяют сравнению (11). Так как один

класс чисел по модулю $p^{\pi'}$ распадается, как легко усмотреть на p классов по модулю $p^{\pi'+1}$, то из одного решения сравнения (10) получается p решений сравнения (11).

2) Пусть число k не делится на p. Тогда сравнение (16) заключает в себе противоречие, и из решения сравнения (10) не получается ни одного решения сравнения (11). Если так дело обстоит с каждым решением сравнения (10) (в случае, если оно имеет несколько решений), то сравнение (11) невозможно, а следовательно невозможны и все сравнения по модулям p^{π}, где $\pi > \pi'$ т. к. всякое решение сравнения по модулю p^{π} должно бы удовлетворять сравнению (11).

§ 2. Сравнения по простому модулю. Теорема Вильсона.

Как было показано в предшествующем параграфе, решение алгебраического сравнения приводится к решению сравнений по модулям простым. Рассмотрим теперь свойства алгебраических сравнений по простому модулю вида

$$f(x) \equiv 0 \ (Mod.\ p). \tag{1}$$

Степенью такого сравнения, согласно с определением, данным выше, называем степень наивысшего из членов, коэффициенты которых не делятся на модуль p.

Теорема 1. Старший коэффициент в сравнении можно сделать равным единице.

Пусть коэффициент старшего члена есть a_0. По предположению a_0 не делится на p и следовательно $D(a_0, p) = 1$. Но в таком случае можно найти для a_0 союзное число a_0', так что $a_0 a_0' \equiv 1 \ (Mod.\ p)$, и тогда сравнение можно переписать в эквивалентной форме

$$a_0 x^n + a_1 a_0 a_0' x^{n-1} + a_2 a_0 a_0' x^{n-2} + \cdots \equiv 0 \ (Mod.\ p)$$

или

$$a_0 (x^n + a_1 a_0' x^{n-1} + a_2 a_0' x^{n-2} + \cdots + a_n a_0') \equiv 0 \ (Mod.\ p).$$

Так как $D(a_0, p) = 1$, то на a_0 мы имеем право сократить и таким образом получаем сравнение

$$x^n + a_1 a_0' x^{n-1} + a_2 a_0' x^{n-2} + \ldots + a_n a_0' \equiv 0 \ (Mod.\ p), \quad (2)$$

эквивалентное данному, и теорема доказана.

Примечание. Доказательство наше дает, собственно говоря, больше, а именно из предшествующих рассуждений следует, что для любого значения x имеет место тождественное сравнение

$$f(x) \equiv a_0 \ (x^n + a_1 a_0' \ x^{n-1} + \ldots + a_n a_0') \ (Mod.\ p). \quad (3)$$

Таким образом по модулю p всякий многочлен можно представить в виде произведения старшего коэффициента на многочлен, старший коэффициент которого равен единице. Этот последний многочлен называется первообразной формой данного многочлена.

Теорему 1-ую можно было бы доказать несколько проще, умножая непосредственно данное сравнение на a_0'. При этом получили бы эквивалентное данному сравнение со старшим коэффициентом сравнимым с единицей, и цель была бы достигнута; но при этом мы бы не получили того добавления, которое изложено в настоящем примечании.

В дальнейшем предполагаем старший член сравнения (1) $f(x) \equiv 0 \ (Mod.\ p)$ с коэффициентом равным единице, так что

$$f(x) = x^n + b_1 x^{n-1} + b_2 x^{n-2} + \ldots + b_n$$

и пусть $x \equiv a \ (Mod.\ p)$ есть решение сравнения (1). Производя деление многочлена $f(x)$ на разность $x - a$

$$\frac{f(x)}{R} \Big| \frac{x-a}{f_1(x)}$$

получаем в частном многочлен $f_1(x)$ степени $n-1$ с целыми коэффициентами и со старшим коэффициентом равным единице, а в остатке R — число, не зависящее от x. В тождество

$$f(x) = (x-a) \ f_1(x) + R \quad (4)$$

вносим вместо x a и получаем

$$f(a) = R.$$

Так как по условию a есть решение сравнения (1), то

$$R \equiv 0 \ (Mod.\ p) \tag{5}$$

и равенство (4) дает тождественное сравнение

$$f(x) \equiv (x - a)\ f_1(x) \ (Mod.\ p), \tag{6}$$

справедливое для всякого значения x (действительно, для любого x разность левой и правой части $= R$, т.-е. числу, делящемуся на модуль p).

Пусть теперь β какое-либо другое решение сравнения (1), отличное от a.

Заменяя x через β в тождественном сравнении (6) и замечая, что $f(\beta) \equiv 0 \ (Mod.\ p)$, имеем

$$(\beta - a).\ f_1(\beta) \equiv 0 \ (Mod.\ p)$$

или иначе

$$(\beta - a).\ f_1(\beta) \mid p$$

Но так как β и a два различных решения сравнения (1), то разность $\beta - a$ не делится на p и следовательно $D(\beta - a, p) = 1$, а потому необходимо $f_1(\beta)$ делится на p или иначе

$$f_1(\beta) \equiv 0 \ (Mod.\ p),$$

т.-е. всякое решение сравнения (1), отличное от решения $x \equiv a \ (Mod.\ p)$, удовлетворяет сравнению

$$f_1(x) \equiv 0 \ (Mod.\ p). \tag{7}$$

Применяя к этому последнему сравнению те же рассуждения и предполагая, что

$$x \equiv \beta \ (Mod.\ p)$$

есть решение сравнения (1), имеем тождественное сравнение

$$f_1(x) \equiv (x - \beta).\ f_2(x) \ (Mod.\ p), \tag{8}$$

где $f_2(x)$ есть многочлен n—2-й степени со старшим коэффициентом = 1. Сопоставляя сравнения (6) и (8), имеем тождественное сравнение

$$f(x) \equiv (x-\alpha)\ (x-\beta).\ f_2(x)\ (Mod.\ p).$$

Если имеем еще решения сравнения (1), отличные от α и β, то процесс можно вести дальше. Пусть имеется n различных решений сравнения (1) $\alpha, \beta, \gamma, \ldots \omega$. В таком случае, в конце концов, дойдем до частного $f_n(x)$ нулевой степени, и очевидно $f_n(x) = 1$, так что окончательно получаем тождественное сравнение

$$f(x) \equiv (x-\alpha)\ (x-\beta)\ (x-\gamma) \ldots (x-\omega)\ \ (Mod.\ p) \qquad (9)$$

Легко усмотреть, что более n различных решений сравнение (1) иметь не может. В самом деле пусть

$$x \equiv \Omega\ (Mod.\ p)$$

есть решение отличное от $\alpha, \beta, \gamma, \ldots \omega$. Заменив x через Ω в тождественном сравнении (9), мы бы получили

$$(\Omega-\alpha)\ (\Omega-\beta)\ (\Omega-\gamma) \ldots (\Omega-\omega) \equiv 0\ (Mod.\ p). \qquad (10)$$

Но разности $\Omega-\alpha, \Omega-\beta, \ldots \Omega-\omega$ по условию не делятся на p и следовательно взаимно-просты с p, а в таком случае и их произведение есть число взаимно-простое с p, и таким образом сравнение (10) не может иметь места.

В результате мы доказали теорему:

Теорема 2. Сравнение со старшим коэффициентом равным единице не может иметь решений больше своей степени.

Из хода доказательства следует еще

Теорема 3. Если сравнение со старшим коэффициентом равным единице имеет ровно столько решений, какова его степень, то левая часть его $f(x)$ представима в виде

$$f(x) \equiv (x-\alpha)\ (x-\beta)\ (x-\gamma) \ldots (x-\omega)\ (Mod.\ p) \qquad (11)$$

где $\alpha, \beta, \gamma, \ldots \omega$ — решения данного сравнения.

Теоремы 2-я и 3-я аналогичны теоремам высшей алгебры, с тем существенным различием, что уравнение n-й степени имеет ровно n корней, а сравнение n-й степени может иметь менее n решений и даже вовсе не иметь их.

Так, сравнение,

$$x^2 \equiv 2 \ (Mod.\ 5)$$

не имеет решений, в чем можно убедиться, испытывая числа 0, 1, 2, 3, 4 — представителей классов по модулю 5.

Теоремы 2-я и 3-я предполагают, что старший коэффициент сравнения равен единице. Сохраняя определение степени сравнения, данное в начале и пользуясь теоремой 1-й, легко убеждаемся, что теорема 2-я имеет место и в том случае, если старший коэффициент не равен единице. Что касается до теоремы 3-й, то в силу тождественного сравнения (3) в общем случае формулируем ее следующим образом:

Теорема 4. Если сравнение имеет решений столько, какова его степень, определяемая по модулю p, то имеем тождественное сравнение

$$f(x) \equiv a_0 \ (x-\alpha) \ (x-\beta) \ . \ . \ . \ (x-\omega) \ (Mod.\ p), \qquad (12)$$

где $f(x)$ — левая часть данного сравнения, a_0 старший коэффициент (не делящийся на p), $\alpha, \beta, \gamma \ . \ . \ . \ \omega$ — решения сравнения.

Возвратимся теперь к определению степени в первоначальном алгебраическом смысле и поставим вопрос, каково может быть число решений сравнения n-й степени

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ . \ . \ . + a_n \equiv 0 \ (Mod.\ p) \qquad (13)$$

Если a_0 не делится на p, то это сравнение есть сравнение степени n в прежнем смысле (по модулю p) и следовательно имеет не более n решений; если a_0 делится на p, но a_1 не делится на p, то степень этого сравнения по модулю p есть $n-1$ и следовательно оно может иметь не более $n-1$, а значит и не более n решений. Так можно

продолжать далее, и если только не все коэффициенты делятся на p, то число решений, очевидно, не может превышать n. Остается предположить, что все коэффициенты делятся на p; в таком случае сравнение (13) удовлетворяется для любого значения x и число его решений (равное p) может быть более n. Таким образом получается:

Теорема 5. Если сравнение

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \ (Mod.\ p)$$

имеет более n решений, то все коэффициенты его делятся на модуль p.

Теоремы 3-я и 4-я дают, по модулю p, выражение многочлена $f(x)$ в виде произведения. Мы имеем дело в этих теоремах с сравнениями тождественными, имеющими место при любом значении x; легко видеть, что разность левой и правой части такого сравнения, напр., сравнения (11) или (12), есть многочлен, все коэффициенты которого делятся на p. Вообще если разность двух многочленов $f(x)$ и $f_1(x)$ есть многочлен с коэффициентами, делящимися на p, т.-е.

$$f(x) - f_1(x) = p \cdot \chi(x), \tag{14}$$

то это означает, что имеем тождественное сравнение

$$f(x) \equiv f_1(x) \ (Mod.\ p), \tag{15}$$

и обратно из тождественного сравнения (15) следует равенство (14).

Пусть теперь

$$f(x) - \varphi(x) \cdot \psi(x) = p \cdot \chi(x), \tag{16}$$

где $\varphi(x)$ и $\psi(x)$ — тоже два многочлена; тогда имеем тождественное сравнение

$$f(x) \equiv \varphi(x) \cdot \psi(x) \ (Mod.\ p) \tag{17}$$

и говорим, что $f(x)$ по модулю p разложено на два множителя $\varphi(x)$ и $\psi(x)$.

Пусть степени $\varphi(x)$ и $\psi(x)$ по модулю p равны соответственно μ и ν; тогда старшие из членов не делящихся на

p в многочленах $\varphi(x)$ и $\psi(x)$ равны соответственно b_0x^μ и c_0x^ν, при чем $D(b_0, p) = D(c_0, p) = 1$. От перемножения их получается старший из неделящихся на p членов $f(x)$

$$b_0c_0x^{\mu+\nu},$$

и таким образом видим, что степень, по модулю p, произведения равна сумме степеней производителей.

Пусть сравнение

$$f(x) \equiv 0 \ (Mod.\ p),$$

имеет решение

$$x \equiv a \ (Mod.\ p).$$

Заменяя x через a в тождественном сравнении (17), получаем

$$\varphi(a) \,.\, \psi(a) \equiv f(a) \equiv 0 \ (Mod.\ p),$$

или

$$\varphi(a) \,.\, \psi(a) \mid p,$$

откуда необходимо следует, что или $\varphi(a) \mid p$, или $\psi(a) \mid p$ другими словами

или $$\varphi(a) \equiv 0 \ (Mod.\ p),$$

или $$\psi(a) \equiv 0 \ (Mod.\ p).$$

Таким образом, если тождественно

$$f(x) \equiv \varphi(x) \,.\, \psi(x) \ (Mod.\ p),$$

то всякое решение сравнения

$$f(x) \equiv 0 \ (Mod.\ p), \tag{18}$$

удовлетворяет одному из сравнений

$$\varphi(x) \equiv 0 \ (Mod.\ p), \tag{19}$$

или

$$\psi(x) \equiv 0 \ (Mod.\ p). \tag{20}$$

Обратно, очевидно, всякое решение одного из этих сравнений удовлетворяет сравнению $f(x) \equiv 0 \ (Mod.\ p)$.

Пусть степени $\varphi(x)$ и $\psi(x)$ по модулю p суть μ и ν; тогда степень $f(x)$ равна $n = \mu + \nu$. Допустим, что сравнение

$$f(x) \equiv 0 \ (Mod.\ p)$$

имеет максимальное число решений равное $n = \mu + \nu$ (в силу теоремы 2-й и 5-й).

В таком случае каждое из сравнений

$$\varphi(x) \equiv 0 \ (Mod.\ p)$$
$$\psi(x) \equiv 0 \ (Mod.\ p)$$

тоже имеет максимальное число решений, т.-е. первое — μ решений, второе ν решений. Действительно, все $\mu + \nu$ решений сравнения (18) распределяются, по предыдущему, между сравнениями (19) и (20). Пусть одно из них не имеет максимального числа решений, напр., пусть сравнение (19) имеет менее μ решений; тогда сравнение (20) должно иметь более ν решений; но это невозможно, так как число решений сравнения не может превышать его степени по модулю p.

Применим установленные нами общие результаты к выводу теоремы, известной под названием теоремы Вильсона.

Рассмотрим сравнение

$$x^{p-1} - 1 \equiv 0 \ (Mod.\ p).$$

По теореме Фермата этому сравнению удовлетворяют все числа, не делящиеся на p, иначе говоря все классы, кроме одного, состоящего из чисел кратных p. Таким образом решениями этого сравнения являются нижеследующие:

$$x \equiv 1,\ 2,\ 3,\ \ldots,\ p-1 \ (Mod.\ p).$$

Число их равно степени $p-1$ сравнения, и по теореме 3-й имеем тождественное сравнение

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\ldots(x-p+1) \ (Mod.\ p).$$

Полагая в нем $x = 0$, получаем:

$$-1 \equiv (-1)^{p-1} \cdot 1 \cdot 2 \cdot 3 \ldots (p-1) = (-1)^{p-1}(p-1)! \ (Mod.\ p).$$

p есть первоначальное число, а потому нечетное, коль скоро $p > 2$.

Таким образом для $p > 2$ имеем (т. к. $p - 1$ четное число и $(-1)^{p-1} = 1$):

$$(p-1)! \equiv -1 \ (Mod.\ p),$$

или

$$(p-1)! + 1 \equiv 0 \ (Mod.\ p). \qquad (21)$$

Но, если $p = 2$, то сравнение (21) все равно имеет место ибо оно тогда дает

$$1 + 1 \equiv 0 \ (Mod.\ 2),$$

и таким образом мы получаем теорему Вильсона: Для всякого первоначального числа p имеет место равнение

$$(p-1)! + 1 = 1 \cdot 2 \cdot 3 \ldots (p-1) + 1 \equiv 0 \ (Mod.\ p) \qquad (21)$$

Например, для $p = 5$ имеем
$1 \cdot 2 \cdot 3 \cdot 4 + 1 = 24 + 1 = 25 \equiv 0 \ (Mod.\ 5)$.

Интересно отметить, что теорема Вильсона обратима, т.-е. имеет место обратное положение:

Если $(p-1)! + 1 \equiv 0 \ (Mod.\ p)$, то p — абсолютно-простое число.

В самом деле пусть p составное число и имеет собственного делителя a, бо́льшего 1-цы и меньшего p. В числе факторов $(p-1)!$ необходимо входит a; таким образом в сравнении

$$(p-1)! \equiv -1 \ (Mod.\ p),$$

левая часть и модуль делятся на a, а правая часть на a не делится, и мы приходим к противоречию.

В виду справедливости обратной теоремы, теорема Вильсона, очевидно, дает критерий для первоначального числа.

Рассмотрим, во-вторых, сравнение

$$x^{\delta} - 1 \equiv 0 \ (Mod.\ p), \qquad (22)$$

где δ есть делитель числа $p-1$ (число $p-1$ во всяком случае четное, а следовательно необходимо составное), так что

$$p-1=\delta\,.\,\omega. \tag{23}$$

При этих обозначениях имеем

$$x^{p-1}-1=x^{\delta\omega}-1=(x^{\delta})^{\omega}-1^{\omega},$$

и следовательно x^p—1, как разность ω — x степеней делится нацело на разность первых степеней $x^{\delta}-1$, так что

$$x^{p-1}-1=(x^{\delta}-1)\,.\,\psi(x), \tag{24}$$

где $\psi(x)$ многочлен с целыми коэффициентами, так как старший коэффициент делителя x — 1 равен единице. Легко убедиться, что старший коэффициент $\psi(x)$ равен тоже единице и степень $\psi(x)$ по модулю p равна

$$p-1-\delta=\delta(\omega-1).$$

Равенство (24) дает нам право написать тождественное сравнение

$$x^{p-1}-1\equiv(x^{\delta}-1)\,.\,\psi(x)\ (Mod.\ p). \tag{25}$$

Замечая, что по теореме Фермата сравнение

$$x^{p-1}-1\equiv 0\ (Mod.\ p)$$

удовлетворяется для чисел 1, 2, 3, . . . , $p-1$ и следовательно имеет максимальное число решений, и применяя предшествующие результаты, касающиеся тождественного сравнения (25), непосредственно заключаем, что и сравнение (22) имеет максимальное число, т.-е. δ решений.

Так, взяв $p=19$, имеем $p-1=18$, и так как 18 делится на числа 2, 3, 6 и 9, то сравнения

$$x^2-1\equiv 0\ (Mod.\ 19),\quad x^3-1\equiv 0\ (Mod.\ 19),$$
$$x^6-1\equiv 0\ (Mod.\ 19),\quad x^9-1\equiv 0\ (Mod.\ 19),$$

все имеют максимальное число решений: первое—2, второе—3, третье—6, четвертое—9.

Возвращаемся к общей теории сравнений по первоначальному модулю.

$$f(x) \equiv 0 \ (Mod\ .\ p).$$

Докажем, что степень сравнения можно понизить до p—1, т.-е. другими словами можно заменить данное сравнение другим, эквивалентным ему, имеющим те же корни, но степень которого не выше $p-1$.

Пусть степень $f(x)$ равна или более p.

Разделим многочлен $f(x)$ на $x^p - x$. В частном получим некоторый многочлен $\psi(x)$ и в остатке многочлен $f_1(x)$ степени $p-1$ или ниже (степень остатка ниже степени делителя). Коэффициенты обоих многочленов—целые числа, т. к. старший коэффициент делителя равен единице. Соотношение между делимым, делителем, частным и остатком дает нам тождество

$$f(x) = (x^p - x) \cdot \psi(x) + f_1(x) . \tag{26}$$

из которого легко заключаем, что сравнение

$$f(x) \equiv 0 \ \ (Mod\ .\ p) \tag{1}$$

эквивалентно сравнению

$$f_1(x) \equiv 0 \ \ (Mod\ .\ p) \tag{27}$$

В самом деле по теореме Фермата, для любого числа a имеем

$$a^p - a \equiv 0 \ \ (Mod\ .\ p),$$

а следовательно, из тождества (26) для всякого числа a получаем:

$$f(a) \equiv f_1(a) \ \ (Mod\ .\ p).$$

Таким образом, если имеет место одно из двух сравнений

$$f(a) \equiv 0 \text{ или } f_1(a) \equiv 0 \ \ (Mod.\ p),$$

то необходимо имеет место и другое, а потому сравнения (1) и (27) эквивалентны, и таким образом доказана

Теорема 6. Степень алгебраического сравнения по первоначальному модулю p может быть понижена до $p-1$.

Пусть, например, имеем сравнение

$$x^{13}-1\equiv 0 \ (Mod.\ 11).$$

Производим деление

$$\begin{array}{l|l} x^{13}-1 & x^{11}-x \\ \underline{x^{13}-x^{3}} & \overline{x^{2}} \\ x^{3}-1 & \end{array}$$

В остатке получаем x^3-1 и следовательно, данное сравнение эквивалентно сравнению

$$x^3-1\equiv 0 \ (Mod.\ 11).$$

Предполагая, согласно доказанной теореме, степень сравнения

$$f(x)\equiv 0 \ (Mod.\ p) \tag{28}$$

не выше $p-1$, выведем критерий того, что оно имеет максимальное число решений.

Старший коэффициент многочлена $f(x)$ будем предполагать равным единице (на каковое предположение имеем право) и разделим разность x^p-x на $f(x)$. Пусть частное есть $\psi(x)$, а остаток $R(x)$. Имеем тождественное равенство

$$x^p-x=f(x)\cdot\psi(x)+R(x). \tag{29}$$

Докажем, что необходимое и достаточное условие для того, чтобы сравнение (28) имело максимальное число решений, состоит в том, что коэффициенты остатка $R(x)$ все должны делиться на модуль p.

В самом деле, пусть, во-первых, все эти коэффициенты делятся на p; тогда тождественно

$$R(x)\equiv 0 \ (Mod.\ p).$$

и из равенства (29) вытекает тождественное сравнение

$$x^p-x\equiv f(x)\cdot\psi(x) \quad (Mod.\ p). \tag{30}$$

Так как по теореме Фермата сравнение

$$x^p-x\equiv 0 \ (Mod.\ p)$$

удовлетворяется для всякого числа, а следовательно имеет максимальное (p) число решений (p — классов чисел по модулю p), то по одной из выше доказанных теорем из тождественного сравнения (30) заключаем, что сравнение

$$f(x) \equiv 0 \ (Mod\ .\ p) \tag{28}$$

тоже имеет максимальное число решений.

Пусть, во-вторых, сравнение (28) имеет максимальное число решений, равное степени многочлена $f(x)$. Пусть a одно из этих решений; вставляя a вместо x в равенство (29) и замечая, что по теореме Фермата

$$a^p - a \equiv 0 \ (Mod\ .\ p),$$

получаем:

$$R(a) \equiv 0 \ (Mod\ .\ p).$$

Таким образом все решения сравнения (28) удовлетворяют сравнению:

$$R(x) \equiv 0 \ (Mod\ .\ p); \tag{31}$$

а так как степень многочлена $R(x)$ ниже степени $f(x)$ (степень остатка ниже степени делителя), то сравнение (31) имеет число решений, превосходящее его степень, а это возможно, по одной из доказанных теорем, только тогда, когда все его коэффициенты делятся на модуль.

Таким образом получается

Теорема 7. Необходимое и достаточное условие того, чтобы сравнение

$$f(x) \equiv 0 \ (Mod\ .\ p),$$

где $f(x)$ многочлен степени ниже p со старшим коэффициентом равным единице, имело максимальное число решений, состоит в том, что остаток от деления $x^p - x$ на $f(x)$ должен иметь все коэффициенты, делящиеся на модуль p.

ГЛАВА СЕДЬМАЯ.

Сравнения второй степени.

§ 1. Приведение сравнения 2-й степени к простейшему виду; квадратичные вычеты.

Общий вид сравнения 2-й степени.

$$ax^2 + bx + c \equiv 0 \ (Mod . m), \tag{1}$$

где a, b, c — целые числа

Отметим те случаи, когда сравнение 2-й степени приводится к сравнению 1-й степени.

Это будет

1) если $a \mid m$, ибо тогда первый член может быть отброшен,

2) если $m = 2$, ибо тогда модуль — простое число $m = p = 2$, и согласно теории, изложенной в предшествующей главе, степень сравнения может быть понижена до $p - 1 = 1$.

В дальнейшем поэтому будем считать $m > 2$ и a не делящимся на m.

Помножим сравнение (1) и модуль его на число $4a$; получаем сравнение

$$4a^2x^2 + 4abx + 4ac \equiv 0 \ (Mod . 4am), \tag{2}$$

из которого обратно сравнение (1) получается делением двух частей и модуля на $4a$. Ввиду этого сравнения (1) и (2) эквивалентны. Сравнение (2) далее представляем в виде

$$(2ax + b)^2 \equiv b^2 - 4ac \ (Mod . 4am),$$

и таким образом, вводя новое неизвестное z, приводим задачу к решению сравнения

$$z^2 \equiv q \ (Mod.\ 4am), \tag{3}$$

где $q = b^2 - 4ac$. Имея решение z сравнения (3), определим x из сравнения 1-й степени

$$2ax + b \equiv z \ (Mod.\ 4am). \tag{4}$$

Приведение общего сравнения 2-й степени к двучленному виду иногда может быть выполнено более простым способом. Так, пусть модуль m есть простое число $p > 2$. По условию a не делится на p и следовательно $D(a, p) = 1$, но т. к. p нечетное число, то и $D(4a, p) = 1$, а потому можно на $4a$ помножить только 2 части сравнения (1), не изменяя модуля, и сравнение (1) заменить эквивалентным ему сравнением.

$$4a^2x^2 + 4abx + 4ac \equiv 0 \ (Mod.\ p). \tag{2'}$$

Вводя новое переменное z, приходим к двучленному сравнению

$$z^2 \equiv q \ (Mod.\ p), \tag{3'}$$

решив которое, определяем x из сравнения 1-й степени

$$2ax + b \equiv z \ (Mod.\ p). \tag{4'}$$

В силу всего предшествующего остается рассмотреть двучленное сравнение 2-й степени вида

$$z^2 \equiv q \ (Mod.\ m). \tag{5}$$

Если это сравнение возможно, то число q сравнимо с точным квадратом, есть вычет квадрата (z^2), и потому называется **квадратичным вычетом** (по модулю m); если же сравнение (5) невозможно, то q называется **квадратичным невычетом**. Ясно, что все числа одного класса — одновременно квадратичные вычеты или невычеты.

Предположим сначала, что q и m числа взаимно-простые ($D(q, m) = 1$); мы увидим далее, что к этому случаю при-

водится и тот, когда общий наибольший делитель q и m отличен от единицы. Легко видеть, что всякое решение ξ сравнения (5), в предположении $D(q, m) = 1$, необходимо есть число взаимно-простое с m. В самом деле, допустив, что ξ и m имеют общего делителя d, замечаем, что и ξ^2 делится на d, и из сравнения

$$\xi^2 \equiv q \ (Mod.\ m)$$

заключаем, что и q делится на d и следовательно q и m, противно предположению, имеют общего делителя d.

Докажем несколько теорем относительно двучленного сравнения

$$x^2 \equiv q \ (Mod.\ m). \tag{6}$$

Теорема 1. Если ξ есть решение сравнения (6), то число $m - \xi$ тоже удовлетворяет ему.

Действительно

$$(m - \xi)^2 = m^2 - 2m\xi + \xi^2 \equiv \xi^2 \equiv q \ (Mod.\ m).$$

Теорема 2. Если ξ есть решение сравнения (6) и z — решение сравнения

$$z^2 \equiv 1 \ (Mod.\ m), \tag{7}$$

то

$$x \equiv \xi z \ (Mod.\ m) \tag{8}$$

есть также решение сравнения (6) и обратно, всякое решение сравнения (6) получается из формулы (8), где z какое-либо решение сравнения (7).

Первая часть теоремы доказывается непосредственно, ибо

$$(\xi z)^2 = \xi^2 z^2 \equiv q.\ 1 = q \ (Mod.\ m).$$

Для доказательства 2-й части предположим, что ξ' есть какое-либо решение сравнения (6), так что на-ряду с

$$\xi^2 \equiv q \ (Mod.\ m)$$

имеем

$$\xi'^2 \equiv q \ (Mod.\ m)$$

и следовательно $\xi'^2 \equiv \xi^2 \ (Mod.\ m)$ (9),

и при этом, в силу сделанных выше замечаний

$$D(\xi', m) = D(\xi, m) = 1.$$

Пусть η — союзное число для числа ξ, так что

$$\xi\eta \equiv 1 \ (Mod.\ m). \qquad (10)$$

Возведя произведение $\xi'\eta$ в квадрат, имеем в силу сравнений (9) и (10):

$$(\xi'\eta)^2 = \xi'^2\eta^2 \equiv \xi^2\eta^2 = (\xi\eta)^2 \equiv 1 \ (Mod.\ m)$$

и следовательно произведение $\xi'\eta$ есть некоторое решение сравнения (7).

Таким образом

$$\xi'\eta \equiv z \ (Mod.\ m).$$

Умножая обе части на ξ, имеем

$$\xi'\xi\eta \equiv \xi z \ (Mod.\ m)$$

или, в силу (10):

$$\xi' \equiv \xi z \ (Mod.\ m),$$

что и доказывает вторую часть теоремы.

Пусть z_1 и z_2 — различные решения сравнения (7). Легко усмотреть, что формула (8) дает соответственно два различных решения сравнения (6). Действительно, если бы мы предположили

$$\xi z_1 \equiv \xi z_2 \ (Mod.\ m),$$

то сократив обе части на число ξ, взаимно-простое с модулем, получили бы противно предположению

$$z_1 \equiv z_2 \ (Mod.\ m).$$

Таким образом, если сравнение (6) возможно, то оно имеет ровно столько решений, сколько сравнение (7), и следова-

тельно, если только число q есть квадратичный вычет, то число решений не зависит от q и является функцией модуля m.

Применим теперь к сравнению (6) результаты общей теории алгебраических сравнений (см. гл. VI). Разложим модуль m на первоначальные факторы, из числа которых особо выделим 2; разложение m пусть будет

$$m = 2^{\omega} p_1^{\pi_1} p_2^{\pi_2} \ldots \ldots \qquad (11)$$

В таком случае решение данного сравнения (6) равносильно решению совокупной системы

$$\begin{aligned} x^2 &\equiv q \quad (Mod.\ 2^{\omega}) \\ x^2 &\equiv q \quad (Mod.\ p_1^{\pi_1}) \\ x^2 &\equiv q \quad (Mod.\ p_2^{\pi_2}) \\ &\ldots\ldots\ldots \end{aligned} \qquad (12),$$

а это в свою очередь приводится к нахождению в отдельности решений каждого из сравнений системы (12) и затем к решению совокупной системы сравнений 1-й степени

$$\begin{aligned} x &\equiv \alpha \quad (Mod.\ 2^{\omega}) \\ x &\equiv \beta \quad (Mod.\ p_1^{\pi_1}) \\ x &\equiv \gamma \quad (Mod.\ p_2^{\pi_2}) \\ &\ldots\ldots\ldots \end{aligned} \qquad (13),$$

где α, β, γ, ... — решения 1-го, 2-го, 3-го,.... сравнений системы (12). Последняя задача в свое время была разрешена, и таким образом все дело сводится к решению в отдельности каждого из сравнений (12); отсюда между прочим следует, что число q есть квадратичный вычет по модулю m тогда и только тогда, когда оно есть в отдельности квадратичный вычет по модулям 2^{ω}, $p_1^{\pi_1}$, $p_2^{\pi_2}$....

Сравнения (12) — двух типов: или модуль есть степень двух (2^{ω}), или он есть степень нечетного первоначального числа, бо́льшего двух (p^{π}).

Обращаемся к рассмотрению сравнения 1-го типа

$$x^2 \equiv q \pmod{2^\omega}. \tag{14}$$

1) Пусть, во-первых $\omega = 1$. Сравнение

$$x^2 \equiv q \pmod{2},$$

где q, как взаимно-простое с модулем, есть необходимо нечетное число, удовлетворяется, как легко видеть, любым нечетным числом (x должно необходимо быть нечетным числом, т. к. оно должно быть взаимно-простым с модулем).

В самом деле, взяв $x = 2k + 1$, имеем

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 1 \equiv q \pmod{2}.$$

Так как все нечетные числа по модулю 2 образуют один класс, то сравнение (14) при $\omega = 1$ имеет одно решение.

2) Пусть, во-вторых, $\omega = 2$. Сравнение

$$x^2 \equiv q \pmod{4},$$

если имеет решение, то удовлетворяется нечетными числами, т. к. решение должно быть взаимно-простое с модулем.

Взяв $x = 2k + 1$, имеем

$$x^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4}.$$

Итак, необходимое и достаточное условие возможности сравнения есть

$$q \equiv 1 \pmod{4}, \tag{15}$$

и при выполнении его сравнению удовлетворяют все нечетные числа. Так как по модулю 4 нечетные числа образуют два класса (числа вида $4k+1$ и $4k-1$), то сравнение (14) при $\omega = 2$ имеет два решения.

3) Пусть, наконец, $\omega \geqslant 3$. Прежде всего, если имеет место сравнение

$$x^2 \equiv q \pmod{2^\omega}, \tag{16}$$

то те же значения x удовлетворяют и сравнению

$$x^2 \equiv q \pmod{8}, \tag{17}$$

модуль которого есть делитель модуля данного сравнения. Так как q нечетное число, то сравнению (17) могут удовлетворять только нечетные числа. Любое нечетное число можно представить в виде

$$x = 4k \pm 1.$$

Подставляя в сравнение (17), имеем

$$x^2 = 16k^2 \pm 8k + 1 \equiv 1 \equiv q \ (Mod.\ 8).$$

Итак, необходимое и достаточное условие возможности сравнения (17) есть

$$q \equiv 1 \ (Mod.\ 8). \tag{18}$$

При выполнении его сравнению (17) удовлетворяют все нечетные числа, которые по модулю 8 распределяются в 4 класса (представители классов 1, 3, 5, 7), и таким образом сравнение (17) при выполнении условия (18) имеет 4 решения.

Так как сравнение (16) при $\omega > 3$ влечет за собой сравнение (17), то следовательно условие (18) есть вместе с тем необходимое условие возможности сравнения (16). Покажем, что оно и достаточное. Для этой цели пойдем методом перехода от n к $n+1$. Предполагая $\omega > 3$, и следовательно $\omega - 1 \geqq 3$, допустим, что сравнение

$$x^2 \equiv q \ (Mod.\ 2^{\omega-1}) \tag{19}$$

при выполнении условия (18) возможно и пусть ξ есть одно из его решений, так что

$$\xi^2 - q = 2^{\omega-1} \cdot \eta. \tag{20}$$

Так как все решения сравнения (16) удовлетворяют и сравнению (19), то мы в праве искать решение (16) из формулы

$$x = \xi + k \cdot 2^{\omega-1} \tag{21}$$

или из более общей

$$x = \xi + z \cdot 2^{\omega-2} \tag{22}$$

[формула (21) получается из (22) при частном предположении $z = 2k$].

Вставляя (22) в сравнение (16) имеем

$$\xi^2 + 2 . \xi z . 2^{\omega-2} + z^2 . 2^{2\omega-4} \equiv q \ (Mod.\ 2^\omega)$$

или, в силу равенства (20)

$$2^{\omega-1} . \eta + 2^{\omega-1} . \xi z + z^2 . 2^{2\omega-4} \equiv 0 \ (Mod.\ 2^\omega).$$

Так как $\omega - 1 \geqq 3$, то $2\omega - 4 \geqslant \omega$, и последний член левой части, как делящийся на модуль, можно отбросить. Сокращая оставшиеся члены и модуль на $2^{\omega-1}$, получаем

$$\eta + \xi z \equiv 0 \ (Mod.\ 2)$$

или, так как ξ нечетное число,

$$z \equiv -\eta \ (Mod.\ 2)$$

или

$$z = -\eta + 2k.$$

Вставляя в формулу (22), получаем

$$x = \xi - \eta . 2^{\omega-2} + k . 2^{\omega-1}$$

или

$$x \equiv \xi - \eta . 2^{\omega-2} \ (Mod.\ 2^{\omega-1}). \qquad (23)$$

Найденный класс чисел распадается на два класса по модулю 2^ω и дает два решения сравнения (16).

Принимая во внимание, что для $\omega = 3$ условие (18) оказалось не только необходимым, но и достаточным, мы в силу принципа математической индукции заключаем, что оно является таковым же и для любого $\omega > 3$.

Резюмируя все предшествующее, скажем:

q — квадратичный вычет по модулю 2, если q любое нечетное число,

q — квадратичный вычет по модулю 4, если $q \equiv 1 \ (Mod.\ 4)$,

q — квадратичный вычет по модулю 2^ω ($\omega \geqq 3$), если $q \equiv 1 \ (Mod.\ 8)$.

Обращаемся теперь к рассмотрению сравнения 2-го типа

$$x^2 \equiv q \ (Mod.\ p^n), \qquad (24)$$

где p — первоначальное число > 2 и следовательно нечетное. Применяем общую теорию, данную для алгебраического сравнения

$$f(x) \equiv 0 \ (Mod.\ p^{\pi})$$

(см. гл. VI).

Допустим, что мы умеем решать сравнение

$$x^2 \equiv q \ (Mod.\ p^{\pi'}) \tag{25}$$

и пусть ξ — число, ему удовлетворяющее, так что

$$\xi^2 - q = p^{\pi'} . \eta. \tag{26}$$

Обращаемся к сравнению

$$x^2 \equiv q \ (Mod.\ p^{\pi'+1}). \tag{27}$$

Его решения удовлетворяют сравнению (25), а потому мы в праве искать x, удовлетворяющее (27), из формулы

$$x = \xi + p^{\pi'} . z. \tag{28}$$

Вставляя в (27), имеем

$$\xi^2 + 2\xi p^{\pi'} . z + p^{2\pi'} . z^2 \equiv q \ (Mod.\ p^{\pi'+1})$$

или, пользуясь равенством (26):

$$p^{\pi'} . \eta + 2\xi z . p^{\pi'} + p^{2\pi'} . z^2 \equiv 0 \ (Mod.\ p^{\pi'+1}). \tag{29}$$

Последний член, очевидно, делится на модуль; отбросив его и сократив остальные члены и модуль на $p^{\pi'}$, получаем

$$\eta + 2\xi . z \equiv 0 \ (Mod.\ p). \tag{30}$$

Для определения z мы получили сравнение 1-й степени. Коэффициент при z есть число взаимно-простое с модулем p, так как решение ξ сравнения (25), как было ранее замечено,—число взаимно-простое с модулем $p^{\pi'}$, а следовательно и с p и т. к. $D(2,p) = 1$; поэтому сравнение (30) возможно и имеет одно решение, которое выразим формулой

$$z = z_0 + kp. \tag{31}$$

Вставляя в равенство (28), получаем

$$x = \xi + p^{\pi'} . z_0 + k . p^{\pi'+1}$$

или

$$x \equiv \xi + p^{\pi'} . z_0 \ (Mod.\ p^{\pi'+1}). \qquad (32)$$

Таким образом из одного решения сравнения (25) получили одно решение сравнения (27). Отсюда непосредственно следует, что решение сравнения (24) приводится к решению сравнения

$$x^2 \equiv q \ (Mod.\ p). \qquad (33)$$

Если последнее возможно, то возможно и сравнение (24), которое имеет столько же решений, сколько и (33), и решения эти получаются из решений сравнения (33), согласно предыдущему, последовательным переходом сначала к сравнению

$$x^2 \equiv q \ (Mod.\ p^2),$$

затем к сравнению

$$x^2 \equiv q \ (Mod.\ p^3)$$

и т. д.

Из изложенного следует, что число q есть квадратичный вычет по модулю p^π, если оно есть квадратичный вычет по модулю p.

Принимая во внимание все предшествующее, можем высказать такое положение:

Для того, чтобы число q взаимно-простое с модулем

$$m = 2^\omega \ p_1^{\pi_1} \ p_2^{\pi_2} \ldots ,$$

было квадратичным вычетом по этому модулю, необходимо и достаточно, чтобы: 1) оно было квадратичным вычетом для всех нечетных первоначальных факторов $p_1, p_2, \ldots$ модуля m и 2) если $\omega > 1$, то кроме того при $\omega = 2$, чтобы $q \equiv 1$ (*Mod.* 4), а при $\omega \geqslant 3$, чтобы $q \equiv 1$ (*Mod.* 8).

Примечание. В то время как метод, данный для решения сравнения (24), есть не что иное как общий метод, данный в главе VI для сравнения

$$f(x) \equiv 0 \ (Mod.\ p^\pi),$$

метод, помощью которого исследовалось сравнение (14), отличается от общего метода. Является вопрос, почему случай модуля = = степени двух представляется исключительным. Ответом на этот вопрос служит то обстоятельство, что при $p=2$ мы имеем дело как раз с тем случаем, который был упомянут и в общей теории, как исключительный. Действительно, мы имеем здесь

$$f(x)=x^2-q$$
$$f'(x)=2x$$

и след. $f'(a)=2a$ при любом a делится на модуль 2 (ср. гл. VI).

Согласно последним результатам нам остается рассмотреть сравнения типа

$$x^2\equiv q \ (Mod.\ p)$$

и теорию квадратичных вычетов по простому модулю >2, т. к. общий вопрос приводится к рассмотрению этого более простого. Но прежде чем перейти к упомянутой теории, рассмотрим еще случай общего сравнения

$$x^2\equiv q \ (Mod.\ m) \tag{34}$$

в предположении, что q и m не взаимно-простые числа, так что $D(q, m)=d>1$.

Пусть

$$m=m'd, \qquad q=q'd,$$

при чем $D(q', m')=1$, и пусть

$$d=p_1^{2k_1+\delta_1}\cdot p_2^{2k_2+\delta_2}\cdot p_3^{2k_3+\delta_3}\cdot\ldots=Пр^{2k+\delta} \tag{35}$$

есть разложение d на первоначальные факторы, при чем δ_1, δ_2, δ_3, ... суть числа равные каждое или нулю, или единице ($\delta=0$, если p входит в четной степени в разложение d, и $\delta=1$, если p входит в нечетной степени.

Обращаясь к сравнению (34) видим, что так как $q \mid d$ и $m \mid d$, то и $x^2 \mid d$. Отсюда следует, что x^2 делится на любой фактор $p^{2k+\delta}$, а значит x необходимо делится на любое $p^{k+\delta}$ и следовательно

$$x \mid Пр^{k+\delta},$$

так что

$$x=Пр^{k+\delta}\cdot y, \tag{36}$$

Вставив это выражение в сравнение (34), представим его в виде

$$Пр^{2k+\delta}.\ Пр^{\delta}.\ y^2 \equiv q'\ .\ Пр^{2k+\delta}\ (Mod.\ m'.\ Пр^{2k+\delta}).$$

Сокращая оба члена и модуль на общий множитель $Пр^{2k+\delta}$, получаем

$$Пр^{\delta}.\ y^2 \equiv q'\ (Mod.\ m'). \tag{37}$$

Так как q' и m' числа взаимно-простые, то и левая часть должна быть числом взаимно-простым с m', а потому необходимо

$$D\ (Пр^{\delta},\ m') = 1. \tag{38}$$

Это есть первое условие возможности сравнения (34).

Далее делаемъ подстановку

$$z = Пр^{\delta}.\ y. \tag{39}$$

Тогда в силу (37)

$$z^2 = Пр^{2\delta}.\ y^2 \equiv Пр^{\delta}.\ q'\ (Mod.\ m'). \tag{40}$$

Так как, в силу (38) первый фактор правой части взаимно-прост с m' и то же имеет место и для второго фактора, то

$$D\ (Пр^{\delta}.\ q',\ m') = 1,$$

и мы имеем рассмотренный ранее случай, а в силу этого приходим ко второму условию возможности сравнения (34): число $Пр^{\delta}q'$ должно быть квадратичным вычетом по модулю m'.

Покажем, что эти условия не только необходимы, но и достаточны.

Допустим, что оба условия выполнены; тогда прежде всего существует z — решение сравнения (40). Кроме того в силу (38) существует число P союзное для $Пр^{\delta}$ по модулю m', так что

$$P\ .\ Пр^{\delta} \equiv 1\ (Mod.\ m'). \tag{41}$$

Помножив обе части сравнения (40) на P^2 и положив

$$Pz \equiv y\ (Mod.\ m')$$

(y определяется сравнением 1-й степени), имеем

$$y^2 \equiv P \,.\, P \,.\, Пр^{\delta} \,.\, q' \equiv Pq' \pmod{m'}.$$

Умножая обе части этого сравнения на $Пр^{\delta}$, получаем

$$Пр^{\delta} \,.\, y^2 \equiv Пр^{\delta} \cdot Pq' \equiv q' \pmod{m'}.$$

Теперь обе части и модуль умножаем на $d = Пр^{2k+\delta}$; получаем

$$Пр^{2k+\delta} \,.\, y^2 \equiv q \pmod{m}.$$

Взяв

$$x = Пр^{k+\delta} \,.\, y,$$

имеем окончательно

$$x^2 \equiv q \pmod{m},$$

т.-е. получаем решение сравнения (34).

Мы видим таким образом, что решение сравнения (34) в случае $D(q, m) = d > 1$ приводится к решению сравнения (40), в котором правая часть и модуль — числа взаимно-простые, т.-е. к случаю уже рассмотренному. Этот случай, как мы видели, приводит нас к необходимости исследования случая первоначального (> 2) модуля, т.-е. к теории квадратичных вычетов по модулю абсолютно-простому.

§ 2. Теория квадратичных вычетов по модулю абсолютно-простому. Символ Лежандра; закон взаимности двух простых чисел. Символ Якоби.

Сравнение 2-й степени

$$x^2 \equiv q \pmod{p}, \tag{1}$$

где p — абсолютно-простое число > 2, не может иметь более двух решений. Покажем, что если оно имеет одно решение α, то имеет и второе, отличное от α. В самом деле, в силу общего замечания (§ 1) на-ряду с числом α сравнению (1) удовлетворяет и число $p - \alpha$. Остается показать, что α и $p - \alpha$ принадлежат к различным классам. Допустим, что

$$p - \alpha \equiv \alpha \pmod{p};$$

но тогда имели бы

$$2\alpha \equiv p \equiv 0 \pmod{p},$$

что невозможно, т. к. и 2 и a — числа взаимно-простые с p. Итак, сравнение (1) может или вовсе не допускать решений или же имеет их два, т. е. максимальное число; поэтому критерием возможности сравнения (1), т.-е. критерием того, что q есть квадратичный вычет по модулю p, является критерий максимального числа решений сравнения (1). Для получения его, согласно результатам гл. VI, следует разделить $x^p - x$ на $x^2 - q$, и определить остаток деления. Разность $x^p - x$ представляем в следующем виде:

$$x^p - x = x(x^{p-1} - 1) =$$
$$= x\left[(x^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}} + q^{\frac{p-1}{2}} - 1\right] =$$
$$= x\left[(x^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}}\right] + x\left(q^{\frac{p-1}{2}} - 1\right).$$

Выражение в квадратных скобках в 1-м члене делится без остатка на $x^2 - q$ (разность одинаковых, $\frac{p-1}{2}$ — х, степеней x^2 и q делится на разность их первых степеней); поэтому остаток деления равен

$$x\left(q^{\frac{p-1}{2}} - 1\right)$$

и, в силу результатов гл. VI, искомый критерий состоит в том, чтобы $q^{\frac{p-1}{2}} - 1$ делилось на p. Итак, q есть квадратичный вычет по модулю p, если

$$q^{\frac{p-1}{2}} \equiv 1 \ (Mod.\ p). \qquad (2)$$

Заметим, что в силу теоремы Фермата

$$q^{p-1} - 1 \equiv 0 \ (Mod.\ p)$$

или

$$\left(q^{\frac{p-1}{2}} - 1\right)\left(q^{\frac{p-1}{2}} + 1\right) \equiv 0 \ (Mod.\ p).$$

Произведение может делиться на первоначальное число p только, если один из факторов делится на p; поэтому необходимо имеет место одно из двух сравнений

$$q^{\frac{p-1}{2}} \equiv 1 \ (Mod.\ p) \text{ или } q^{\frac{p-1}{2}} \equiv -1 \ (Mod.\ p)$$

и, конечно, одновременно оба не могут иметь место. Отсюда заключаем, что критерий можно формулировать так:

$$q^{\frac{p-1}{2}} \equiv +1 \ (Mod.\ p), \tag{2}$$

если q — квадратичный вычет, и

$$q^{\frac{p-1}{2}} \equiv -1 \ (Mod.\ p), \tag{2'}$$

если q — квадратичный невычет.

Например, пусть $p = 7$, $q = 5$; $5^{\frac{7-1}{2}} = 5^3 = 125 \equiv -1$ (*Mod.* 7); следовательно 5 — квадратичный невычет по модулю 7 и сравнение $x^2 \equiv 5$ (*Mod.* 7) не имеет ни одного решения.

В свое время уже было упомянуто, что два числа одного класса — одновременно квадратичные вычеты или невычеты или, как говорят, обладают одним и тем же квадратичным характером, и это явствует из таких соображений:

если

$$q' \equiv q \ (Mod.\ p)$$

и если имеет место одно из двух сравнений

$$x^2 \equiv q \ (Mod.\ p)$$

и

$$x^2 \equiv q' \ (Mod\ p),$$

то имеет место и другое.

Таким образом все классы чисел взаимно-простых с модулем p, т.-е. все классы за исключением класса чисел, делящихся на p, разделяются на классы, состоящие из

квадратичных вычетов и классы, состоящие из квадратичных невычетов.

Для определения тех и других существует такой простой прием: квадратичные вычеты суть вычеты квадратов. Поэтому будем различные числа возводить в квадрат и находить вычеты этих квадратов или, что то же,—классы, характеризуемые этими квадратами. При этом ясно, что если $x' \equiv x \ (Mod.\ p)$, то и $x^2 \equiv x'^2 \ (Mod.\ p)$; поэтому достаточно возводить в квадрат представителей различных классов, притом, конечно, за исключением класса чисел, кратных p, т. к. мы предполагаем все время в сравнении

$$x^2 \equiv q \ (Mod.\ p)$$

q, а следовательно и x — взаимно-простыми с p. Посмотрим теперь, не будут ли получаться от возведения в квадрат представителей различных классов результаты, принадлежащие к одному классу. Предположив

$$x'^2 \equiv x^2 \ (Mod.\ p),$$

имеем

$$x'^2 - x^2 = (x' - x)(x' + x) \equiv 0 \ (Mod.\ p),$$

откуда

$$\text{или } x' - x \equiv 0 \ (Mod.\ p)$$
$$\text{или } x' + x \equiv 0 \ (Mod.\ p).$$

Первое предположение отпадает, в силу допущения, что x' и x числа различных классов; второе дает

$$x' \equiv -x \equiv p - x \ (Mod.\ p).$$

После этих замечаний ясно, какие числа следует возводить в квадраты из ряда 1, 2, 3, ... , $p-1$ (приведенная система вычетов): возьмем числа меньшие $\frac{p}{2}$, т.-е. числа $1, 2, 3, \ldots \ldots \frac{p-1}{2}$ и их возводим в квадрат:

$$1^2, 2^2, 3^2, \ldots \ldots, \left(\frac{p-1}{2}\right)^2. \qquad (3)$$

Остальные числа, бо́льшие $\frac{p}{2}$, оставляем, т. к. каждое такое число x' вместе с одним из чисел x, меньших $\frac{p}{2}$, в сумме дает p, и тогда

$$x' = p - x$$

и следовательно, по предыдущему,

$$x'^2 \equiv x^2 \ (Mod.\ p).$$

Числа же ряда (3) все разных классов, т. к. для двух чисел r и s меньших $\frac{p}{2}$, $r - s < p$ и $r + s < p$, и следовательно $r - s$ и $r + s$ не делятся на p а потому

$$r^2 - s^2 = (r - s)(r + s) \not\equiv 0 \ (Mod.\ p).$$

Таким образом, ряд (3) дает представителей классов квадратичных вычетов; число их равно $\frac{p-1}{2}$, а так как общее число классов чисел, не делящихся на p, есть $p - 1$, то и квадратичных невычетов тоже $\frac{p-1}{2}$.

Пример $p = 7$. Возводим в квадрат числа 1, 2, 3, получаем 1, 4, 9 или, беря вычеты, 1, 4, 2. Остальные вычеты 3, 5, 6 приведенной системы — квадратичные невычеты.

Переходим теперь к рассмотрению так называемого символа Лежандра, введение которого позволяет заменить критерий квадратичного вычета, данный выше, более простым. Первоначальный критерий требовал возведения q в степень $\frac{p-1}{2}$, что при сколько-нибудь значительном p, требует больших выкладок.

Для получения нового критерия вводим символ

$$\left(\frac{q}{p}\right) \tag{4}$$

равный $+1$ или -1, смотря по тому, квадратичный вычет или невычет есть число q по модулю p или иначе, смотря по тому, какое из двух сравнений

$$\begin{aligned} q^{\frac{p-1}{2}} &\equiv 1 \ (Mod.\ p) \\ q^{\frac{p-1}{2}} &\equiv -1 \ (Mod.\ p) \end{aligned} \tag{5}$$

имеет место. Конечно, одно из этих сравнений исключает другое, т. к. в противном случае имели бы

$$1 \equiv -1 \ (Mod.\ p)$$

или

$$2 \equiv 0 \ (Mod.\ p),$$

что невозможно, т. к. 2 не делится на число $p > 2$.

На основании изложенного легко усмотреть, что символ Лежандра вполне определяется условиями:

$$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \ (Mod.\ p). \qquad \left|\left(\frac{q}{p}\right)\right| = 1 \qquad (6).$$

В самом деле, в силу 2-го

$$\left(\frac{q}{p}\right) = \pm 1,$$

а в силу 1-го тот или другой из двух знаков будет получаться в соответствии с тем, какое из двух сравнений (5) имеет место. Заметим еще, что числитель q символа Лежандра, в силу наших условий, всегда предполагается числом взаимно-простым со знаменателем p или, что то же, не делящимся на p (p—абсолютно простое число > 2).

Для вывода свойств символа Лежандра докажем предварительно лемму: Если $\varepsilon = \pm 1$ и $\varepsilon' = \pm 1$ и если $\varepsilon' \equiv \varepsilon$ $(Mod.\ p)$, то $\varepsilon' = \varepsilon$.

Действительно, если бы ε' не равнялось ε, то имели бы

$$+1 \equiv -1 \ (Mod.\ p),$$

откуда $2 \equiv 0$ $(Mod.\ p)$ или $2 \mid p$, что невозможно.

Теперь пользуясь этой леммой и определением символа Лежандра, докажем ряд его свойств:

Теорема 1. Если

$$q' \equiv q \ (Mod.\ p),$$

то

$$\left(\frac{q'}{p}\right) = \left(\frac{q}{p}\right).$$

Действительно, если

$$q' \equiv q \ (Mod.\ p),$$

то и

$$q'^{\frac{p-1}{2}} \equiv q^{\frac{p-1}{2}} \ (Mod.\ p),$$

откуда, по определению символа Лежандра,

$$\left(\frac{q'}{p}\right) \equiv \left(\frac{q}{p}\right) \ (Mod.\ p),$$

а, следовательно, в силу леммы

$$\left(\frac{q'}{p}\right) = \left(\frac{q}{p}\right).$$

Теорема 2.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

По определению символа Лежандра имеем

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \ (Mod.\ p)$$

и в то же время

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (Mod.\ p)$$

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \ (Mod.\ p).$$

Сопоставляя эти результаты, получаем

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \ (Mod.\ p),$$

а так как и правая и левая часть этого сравнения могут иметь лишь значения ± 1, то, в силу леммы, имеем

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Легко усмотреть, что теорема 2-я распространяется на любое число множителей:

$$\left(\frac{abc\ldots k}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\cdot\cdot\cdot\left(\frac{k}{p}\right).$$

Доказать этот результат можно последовательно, применяя теорему 2-ю для двух множителей. Так например

$$\left(\frac{abc}{p}\right)=\left(\frac{ab\,.\,c}{p}\right)=\left(\frac{ab}{p}\right)\cdot\left(\frac{c}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)$$

и так далее.

Возвращаясь к теореме 1-й, легко усматриваем, что она выражает такое свойство квадратичных вычетов: два числа одного и того же класса — одновременно квадратичные вычеты или невычеты, иначе говоря — имеют один и тот же квадратичный характер. Свойство это уже было упомянуто выше.

Аналогично, теорема 2-я выражает нижеследующее свойство: произведение двух квадратичных вычетов или невычетов есть квадратичный вычет; произведение квадратичного вычета на невычет есть невычет.

Теорема 3.

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

Действительно

$$\left(\frac{1}{p}\right)\equiv 1^{\frac{p-1}{2}}=1\ (Mod.\ p)$$

по определению символа Лежандра, а отсюда, в силу леммы

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

Теорема эта выражает такое свойство: единица есть квадратичный вычет для любого первоначального числа >2, что, конечно, очевидно, т. к. $1=1^2$ и следовательно

$$1\equiv 1^2\ (Mod.\ p).$$

Теорема 4.

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

Действительно,

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}} \quad (Mod.\ p)$$

по определению, а в силу леммы отсюда

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

Правая часть равна $+1$, когда

$$\frac{p-1}{2}=2k,$$

т.-е. для

$$p=4k+1,$$

и равна -1, когда

$$\frac{p-1}{2}=2k+1,$$

т.-е. для

$$p=4k+3.$$

Таким образом -1 есть квадратичный вычет для простых чисел вида $4k+1$ и квадратичный невычет для простых чисел вида $4k+3$.

Теоремы 3-я и 4-я носят название „дополнительных предложений“ (по отношению к теореме, которую мы докажем далее и которая выражает так называемый „закон взаимности двух простых чисел“); кроме этих двух, существует еще третье дополнительное предложение, которое будет доказано ниже, но которое формулируем здесь же:

Теорема 5.

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Заметим, что простое число p, как нечетное, необходимо имеет вид $4k\pm1$ (при делении на 4 нечетного числа

остатки могут быть только нечетные, т.-е. 1 и 3, или что то же, — 1). Отсюда

$$p^2 = (4k \pm 1)^2 = 16k^2 \pm 8k + 1$$
$$\frac{p^2 - 1}{8} = 2k^2 \pm k = k(2k \pm 1).$$

Второй фактор есть число нечетное, следовательно произведение будет числом четным или нечетным в зависимости от того, будет ли k числом четным или нечетным. В первом случае $k = 2h$ и следовательно

$$p = 8h \pm 1,$$

во втором $k = 2h + 1$ и следовательно

$$p = 8h + 5 \text{ или } p = 8h + 3.$$

Таким образом, 2 есть квадратичный вычет для простых чисел вида $8h \pm 1$ (или иначе—для чисел вида $8h + 1$ и $8h + 7$) и квадратичный невычет для простых чисел вида $8h + 3$ и $8h + 5$.

Теоремы 1—5 позволяют внести значительные упрощения в вычисление данного символа $\left(\frac{q}{p}\right)$.

Действительно, прежде всего, на основании теоремы 1-й, числитель q символа можно заменить его наименьшим вычетом по модулю p; затем, если бы мы при этом взяли отрицательный вычет, то мы могли бы привести дело к символу с положительным числителем на основании теорем 2-й и 4-й, ибо для любого отрицательного числа $-a$ (взаимно-простого с p) имеем

$$\left(\frac{-a}{p}\right) = \left(\frac{-1 \cdot a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{a}{p}\right).$$

Таким образом вычисление данного символа приводится к вычислению символа, числитель которого есть положительное число, меньшее знаменателя. Разлагая числителя

на первоначальные множители и применяя снова теорему 2-ую, мы приведем дело к вычислению символов вида

$$\left(\frac{2}{p}\right) \text{ и } \left(\frac{q}{p}\right),$$

где q — первоначальное число меньшее p.

Символ $\left(\frac{2}{p}\right)$ определяется по теореме 5-й, и таким образом дело сводится к вычислению символов вида

$$\left(\frac{q}{p}\right),$$

где q — абсолютно-простое нечетное число меньшее p.

Дальнейшее упрощение на основании только предшествующих теорем невозможно, и для вычисления символов последнего типа приходится перейти к доказательству формулы, выражающей так называемый закон взаимности двух простых чисел.

Начнем с вывода так называемой леммы Гаусса.

Предполагая число q как всегда взаимно-простым с абсолютно — простым числом p, рассмотрим числа ряда

$$1.q,\ 2.q,\ 3.q,\ \ldots\ldots\ldots\ \frac{p-1}{2}.q \tag{7}$$

и их наименьшее положительные вычеты

$$r_1,\ r_2,\ r_3,\ \ldots\ldots\ r_{\frac{p-1}{2}} \tag{8}$$

Имеем, очевидно, ряд сравнений

$$\left.\begin{aligned} 1\ .\ q &\equiv r_1 \quad (Mod.\ p)\\ 2\ .\ q &\equiv r_2 \quad (Mod.\ p)\\ 3\ .\ q &\equiv r_3 \quad (Mod.\ p)\\ &\ldots\ldots\ldots\\ \frac{p-1}{2}\ .\ q &\equiv r_{\frac{p-1}{2}} \quad (Mod.\ p) \end{aligned}\right\} \tag{9}$$

Все вычеты (8) меньше p, но некоторые из них могут быть меньше $\frac{p}{2}$, а другие больше $\frac{p}{2}$. Назовем вычеты

большие $\frac{p}{2}$ буквами α с индексами, а вычеты меньшие $\frac{p}{2}$ — буквами β с индексами. Пусть число первых есть μ, а вторых ν, так что $\mu+\nu=\frac{p-1}{2}$, и вычеты (8) разбиваются на две группы

$$\alpha_1, \alpha_2, \ldots, \alpha_\mu \tag{10}$$

и

$$\beta_1, \beta_2, \ldots, \beta_\nu \tag{11}$$

Легко видеть, что все вычеты r ряда (8) различны между собою. В самом деле, если бы мы имели

$$r_i = r_j,$$

то из сравнений (9) получили бы

$$iq \equiv jq \ (Mod.\ p),$$

или, предполагая $i > i$,

$$(j-i)q \equiv 0 \ (Mod.\ p).$$

Произведение $(j-i)q$ должно таким образом делиться на p; но т. к. $D(q, p)=1$, то приходим к требованию

$$(j-i) \mid p,$$

а это невозможно, т. к. оба числа j и i меньше p, а след. и их разность тоже.

Раз все r различны между собою, то значит различны между собою и все числа α и все числа β групп (10) и (11), а также каждое α отлично от каждого β. Возьмем теперь вместо чисел α разности $p-\alpha$; так как $\alpha > \frac{p}{2}$, то $p-\alpha < \frac{p}{2}$. Все числа $p-\alpha$ между собою различны; покажем, что они отличны и от чисел β.

В самом деле, пусть

$$p-\alpha=\beta.$$

Но тогда

$$\alpha+\beta=p$$

и значит

$$\alpha+\beta \mid p.$$

Но α и β суть некоторые из чисел r, например r_i и r_j. и следовательно мы имели бы

$$r_i + r_j \mid p$$

или

$$r_i + r_j \equiv 0 \ (Mod.\ p)$$

Но это, на основании сравнений (9), дало бы

$$(i+j)\,q \equiv 0 \ (Mod.\ p)$$

или

$$(i+j)\,q \mid p.$$

Так как $D\,(q,\ p) = 1$, то отсюда имели бы

$$(i+j) \mid p,$$

что невозможно, т. к. каждое из чисел i, j меньше $\frac{p}{2}$ (ибо i и j индексы из ряда 1, 2, 3, . . . , $\frac{p-1}{2}$) и следовательно их сумма меньше p.

Теперь рассмотрим числа

$$\begin{matrix} p-\alpha_1,\ p-\alpha_2,\ p-\alpha_3,\ \ldots\ p-\alpha_\mu \\ \beta_1,\ \beta_2,\ \beta_3,\ \ldots\ \beta_\nu \end{matrix} \qquad (12)$$

Все они различны между собою, общее число их $= \frac{p-1}{2}$ и каждое из них меньше $\frac{p}{2}$. Отсюда явствует, что совокупность чисел (12) есть не что иное, как в ином, вообще говоря, порядке ряд чисел

$$1,\ 2,\ 3,\ \ldots,\ \frac{p-1}{2}. \qquad (13)$$

Перемножим почленно все сравнения (9) получим

$$1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \cdot q^{\frac{p-1}{2}} \equiv r_1 \cdot r_2 \cdot r_3 \ldots r_{\frac{p-1}{2}} \ (Mod.\ p). \qquad (14)$$

Каждое r есть некоторое α или β и следовательно

$$r_1 . r_2 . r_3 . \ldots . r_{\frac{p-1}{2}} \equiv \alpha_1 . \alpha_2 \ldots . \alpha_\mu . \beta_1 . \beta_2 . \ldots . \beta_\nu$$

или так как

$$\alpha \equiv \alpha - p \ (Mod.\ p),$$

$$r_1 r_2 \ldots r_{\frac{p-1}{2}} \equiv (\alpha_1 - p)\ (\alpha_2 - p) \ldots . (\alpha_\mu - p)\ \beta_1\ \beta_2 \ldots \beta_\nu =$$

$$= (-1)^\mu (p - \alpha_1)\ (p - \alpha_2) \ldots (p - \alpha_\mu)\ \beta_1\ \beta_2 \ldots \beta_\nu \ (Mod.\ p). \quad (15).$$

Но числа (12) совпадают с числами ряда (13), а потому $(p - \alpha_1)\ (p - \alpha_2) \ldots (p - \alpha_\mu)\ \beta_1\ \beta_2 \ldots \beta_\nu = 1 . 2 . 3 \ . \ . \ . \ \frac{p-1}{2}$ и следовательно сравнение (15) принимает вид

$$r_1 . r_2 . \ . \ . \ r_{\frac{p-1}{2}} \equiv (-1)^\mu . 1 . 2 . 3 \ldots . \frac{p-1}{2},$$

а сравнение (14) дает нам

$$1 . 2 . 3 \ldots . \frac{p-1}{2} . q^{\frac{p-1}{2}} \equiv (-1)^\mu . 1 . 2 . 3 \ldots . \frac{p-1}{2} (Mod.\ p) \quad (16).$$

Сокращая две части на $1 . 2 . 3 \ldots . \frac{p-1}{2}$, как на число взаимно-простое с модулем, имеем

$$q^{\frac{p-1}{2}} \equiv (-1)^\mu \ (Mod.\ p),$$

а отсюда, в силу определения символа Лежандра

$$\left(\frac{q}{p}\right) \equiv (-1)^\mu \ (Mod.\ p)$$

и, наконец, в силу начальной леммы:

$$\left(\frac{q}{p}\right) = (-1)^\mu. \quad (17)$$

Равенство (17) и выражает лемму Гаусса; здесь μ есть число наименьших положительных вычетов ряда

$$1.q,\quad 2.q,\quad 3.q\ \ldots\ .\ \frac{p-1}{2}.q,$$

превышающих $\frac{p}{2}$.

Формула (17) позволяет находить величину символа Лежандра. Возьмем, напр., $p=7$, $q=5$.

Составим произведения 1.5, 2.5, 3.5.

Их наименьшие положительные вычеты суть 5, 3 и 1; из них больше $\frac{7}{2}=3\frac{1}{2}$ только один вычет 5; следовательно $\mu=1$, а значит

$$\left(\frac{5}{7}\right)=-1,$$

т.-е. 5 есть квадратичный невычет по модулю 7.

Преобразуем теперь формулу (17); при этом мы: 1) вычислим символ $\left(\frac{2}{p}\right)$ и 2) выведем формулу для символа $\left(\frac{q}{p}\right)$ в случае q нечетного.

Для этой цели вместо сравнений (9) напишем равенства, заметив, что r_i есть остаток от деления iq на p. Таким образом получаем:

$$\begin{aligned}
1\,.\,q &= p\,.\,E\frac{q}{p}+r_1\\
2\,.\,q &= p\,.\,E\frac{2q}{p}+r_2\\
3\,.\,q &= p\,.\,E\frac{3q}{p}+r_3\\
&\ldots\ldots\ldots\ldots\\
\frac{p-1}{2}\,.\,q &= p\,.\,E\frac{\frac{p-1}{2}\cdot q}{p}+r_{\frac{p-1}{2}}
\end{aligned}\qquad(18)$$

Складывая равенства (18) и замечая, что

$$1+2+3+\ldots.+\frac{p-1}{2}=\frac{1}{2}\cdot\left(\frac{p-1}{2}+1\right)\cdot\frac{p-1}{2}=$$

$$=\frac{1}{2}\cdot\frac{p+1}{2}\cdot\frac{p-1}{2}=\frac{p^2-1}{8}$$

и что сумма всех r_i равняется

$$S\alpha + S\beta,$$

где, при сохранении прежних обозначений, через $S\alpha$ и $S\beta$ обозначены сумма всех вычетов больших $\frac{p}{2}$ (обозначенных $\alpha_1, \alpha_2, \ldots \alpha_\mu$) и сумма всех вычетов меньших $\frac{p}{2}$ (обозначенных $\beta_1, \beta_2, \ldots \beta_\nu$), имеем

$$q \cdot \frac{(p^2-1)}{8} = p \cdot \left[E\frac{q}{p} + E\frac{2q}{p} + E\frac{3q}{p} + \ldots + E\frac{\frac{p-1}{2} \cdot q}{p}\right] + S\alpha + S\beta. \quad (19)$$

Выше мы рассматривали совокупность чисел

$$p - \alpha_1,\ p - \alpha_2,\ \ldots\ p - \alpha_\mu,\ \beta_1,\ \beta_2,\ \ldots\ \beta_\nu$$

и доказали, что она совпадает с совокупностью чисел ряда

$$1,\ 2,\ 3,\ \ldots,\ \frac{p-1}{2}.$$

Отсюда, складывая все числа совокупности, имеем

$$S(p-\alpha) + S\beta = 1 + 2 + 3 + \ldots + \frac{p-1}{2} = \frac{p^2-1}{8}$$

или

$$\mu p - S\alpha + S\beta = \frac{p^2-1}{8}. \quad (20)$$

Вычитая из равенства (19) равенство (20) на-крест, получаем:

$$\frac{p^2-1}{8} \cdot (q-1) = p\left[E\frac{q}{p} + E\frac{2q}{p} + \ldots + E\frac{\frac{p-1}{2} \cdot q}{p}\right] - \mu p + 2S\alpha. \quad (21)$$

Рассмотрим отдельно два случая — когда $q = 2$ и когда q — нечетное число.

1) Пусть $q = 2$; тогда $q - 1 = 1$. Так как $p > 2$, то все дроби $\frac{q}{p}$, $\frac{2q}{p}$, $\ldots \frac{\left(\frac{p-1}{2}\right) \cdot q}{p}$ правильные и следовательно все члены в квадратных скобках формулы (21) равны нулю.

Таким образом получаем

$$\frac{p^2-1}{8} = -\mu p + 2Sa.$$

Так как для нас важно лишь, четное или нечетное число μ, входящее в формулу (17), ибо в первом случае символ $\left(\frac{q}{p}\right) = +1$, а во втором — 1, то вместо последнего равенства рассмотрим сравнение по модулю 2

$$\frac{p^2-1}{8} \equiv -\mu p \quad (Mod.\ 2)$$

или, т. к. нечетное число p удовлетворяет сравнению

$$p \equiv -1 \ (Mod.\ 2),$$

то иначе

$$\frac{p^2-1}{8} \equiv \mu \ (Mod.\ 2).$$

Обращаясь к формуле (17) отсюда заключаем, что для $q = 2$ ее можно заменить такой формулой

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Другими словами мы доказали ранее формулированную теорему 5.

2) Пусть q число нечетное; тогда $q-1$ число четное и левая часть равенства (21) сравнима с нулем по модулю 2. Замечая еще, что

$$p \equiv 1 \ (Mod.\ 2) \text{ и } 2Sa \equiv 0 \ (Mod.\ 2),$$

получаем из равенства (21) сравнение

$$\mu \equiv E\frac{q}{p} + E\frac{2q}{p} + \ldots + E\frac{\frac{p-1}{2}\cdot q}{p} \quad (Mod.\ 2),$$

а следовательно из формулы (18) для q нечетного получаем

$$\left(\frac{q}{p}\right) = (-1)^{E\frac{q}{p} + E\frac{2q}{p} + \ldots + E\frac{\frac{p-1}{2}\cdot q}{p}}. \qquad (22)$$

Формула (22) позволяет довольно просто вычислять символ Лежандра с нечетным числителем; например

$$\left(\frac{5}{7}\right) = (-1)^{E\frac{5}{7}+E\frac{10}{7}+E\frac{15}{7}} = (-1)^{0+1+2} = -1.$$

Выше мы видели, что вычисление символа Лежандра приводится в конечном счете к вычислению символов типа $\left(\frac{q}{p}\right)$, где q — абсолютное простое число большее 2, но меньшее p. Теперь предстоит дать метод для сведения символов этого типа к более простым и для окончательного их вычисления.

Этого достигнем, доказав на основании предшествующего результата закон взаимности двух простых чисел, который формулируем в виде следующей теоремы:

Теорема 6. Если p и q два различных нечетных абсолютно-простых числа, то

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \qquad (23)$$

Правая часть равенства (23) равна — 1 только в том случае, если и $\frac{p-1}{2}$ и $\frac{q-1}{2}$ нечетные числа, т.-е. если и p и q числа вида $4k+3$; если хотя одно из них вида $4k+1$, правая часть равна $+1$ и значит оба символа $\left(\frac{q}{p}\right)$ и $\left(\frac{p}{q}\right)$ одновременно равны $+1$ или -1. Таким образом теорему 6-ую можно еще формулировать следующим образом:

Пусть p и q два различных абсолютно-простых числа больших 2. Если хотя одно из них — вида $4k+1$, то квадратичные характеры q относительно p и p относительно q совпадают; если оба числа вида $4k+3$, то вышеупомянутые квадратичные характеры противоположны.

В этом виде теорема действительно является „законом взаимности двух простых чисел“.

Приступаем к доказательству формулы (23). Так как и q и p нечетные числа, то в силу формулы (22) имеем

$$\left(\frac{q}{p}\right) = (-1)^{E\frac{q}{p} + E\frac{2q}{p} + \cdots + E\frac{\frac{p-1}{2}\cdot q}{p}}$$

$$\left(\frac{p}{q}\right) = (-1)^{E\frac{p}{q} + E\frac{2p}{q} + \cdots + E\frac{\frac{q-1}{2}\cdot p}{q}}.$$

Перемножая эти два равенства, получаем

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{E\frac{q}{p} + E\frac{2q}{p} + \cdots + E\frac{\frac{p-1}{2}\cdot q}{p} + E\frac{p}{q} + E\frac{2p}{q} + \cdots + E\frac{\frac{q-1}{2}\cdot p}{q}}.$$

Но в силу формулы (4) главы III показатель при (-1) в правой части равен $\frac{p-1}{2}\cdot\frac{q-1}{2}$, и таким образом окончательно имеем

$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

т.-е. формулу (23).

Умножая две части равенства на $\left(\frac{p}{q}\right)$ и замечая, что

$$\left(\frac{p}{q}\right)^2 = (\pm 1)^2 = +1,$$

можем представить формулу (23) еще в следующем виде:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{p}{q}\right). \qquad (24)$$

Формула (24) позволяет разрешить вопрос, к которому мы выше привели вычисление любого символа Лежандра. Мы видели, что это вычисление приводится к нахождению символов, в которых числитель q есть первоначальное нечетное число, меньшее знаменателя p. Пусть

$$\left(\frac{q}{p}\right)$$

такой символ. Тогда можем применить к нему формулу (2.4 и он сведется к символу $\left(\frac{p}{q}\right)$, в котором числитель уже больше знаменателя и следовательно по отношению к нему опять применимы упрощения на основании теорем 1—5. Таким образом процесс может продолжаться все дальше. При этом числители символов все уменьшаются, и, в конце концов, придем к символам $\left(\frac{2}{p}\right)$ или $\left(\frac{1}{p}\right)$, величины которых известны.

Для примера вычислим символ

$$\left(\frac{2212}{1847}\right)^{1)}$$

Делим числитель на знаменатель:

$$\begin{array}{l|l} 2212 & 1847 \\ \hline 1847 & 1 \\ \hline 365 & \end{array}$$

По 1-й теореме

$$\left(\frac{2212}{1847}\right)=\left(\frac{365}{1847}\right)$$

Разлагая числитель на множители, имеем

$$365 = 5.73$$

По 2-й теореме

$$\left(\frac{365}{1847}\right)=\left(\frac{5.73}{1847}\right)=\left(\frac{5}{1847}\right)\cdot\left(\frac{73}{1847}\right)$$

Применяя к символу

$$\left(\frac{5}{1847}\right),$$

числитель которого первоначальное число, формулу (24) имеем

$$\left(\frac{5}{1847}\right)=\left(-1\right)^{2.92^{1}}\cdot\left(\frac{1847}{5}\right)=\left(\frac{1847}{5}\right)$$

Так как

$$1847 \equiv 2 \ (\textit{Mod.}\ 5),$$

то по 1-й теореме

$$\left(\frac{1847}{5}\right)=\left(\frac{2}{5}\right)$$

---

1) Знаменатель 1847—первоначальное число.

по 5-й теореме

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

Итак

$$\left(\frac{5}{1847}\right)=-1$$

Применяя формулу (24) к символу $\left(\frac{73}{1847}\right)$, имеем

$$\left(\frac{73}{1847}\right)=\left(-1\right)^{36.923}\cdot\left(\frac{1847}{73}\right)=\left(\frac{1847}{73}\right)$$

Так как

$$1847\equiv 22\ (\textit{Mod.}\ 73),$$

то по 1-й теореме

$$\left(\frac{1847}{73}\right)=\left(\frac{22}{73}\right)$$

По 2-й теореме

$$\left(\frac{22}{73}\right)=\left(\frac{2.11}{73}\right)=\left(\frac{2}{73}\right)\cdot\left(\frac{11}{73}\right)$$

Первый из символов находим по теореме 5-й:

$$\left(\frac{2}{73}\right)=\left(-1\right)^{\frac{73^2-1}{8}}=+1,$$

так как 73 есть число вида $8k+1$. Ко второму применяем формулу (24):

$$\left(\frac{11}{73}\right)=\left(-1\right)^{\frac{11-1}{2}\cdot\frac{73-1}{2}}\cdot\left(\frac{73}{11}\right)=\left(-1\right)^{5.36}\cdot\left(\frac{73}{11}\right)=\left(\frac{73}{11}\right)$$

По 1-й теореме

$$\left(\frac{73}{11}\right)=\left(\frac{-4}{11}\right),$$

т. к. $73\equiv -4\ (\textit{Mod.}\ 11)$.

По теоремам 2-й и 4-й

$$\left(\frac{-4}{11}\right)=\left(\frac{-1}{11}\right)\cdot\left(\frac{4}{11}\right)=\left(-1\right)^{\frac{11-1}{2}}\cdot\left(\frac{2}{11}\right)^2=-1.+1=-1$$

Итак

$$\left(\frac{73}{1847}\right)=-1,$$

и окончательно

$$\left(\frac{2212}{1847}\right)=\left(-1\right).\left(-1\right)=+1,$$

т.-е. 2212 есть квадратичный вычет по модулю 1847.

Из рассмотрения хотя бы разобранного примера легко усмотреть, что вычисление символа Лежандра ведется применением, с одной стороны, теоремы 1-й и закона взаимности и, с другой—теоремы 2-й. Если бы приходилось применять лишь первые две теоремы, то мы бы имели весьма простой метод, требующий только последовательных делений (числитель символа заменяется остатком от деления его на знаменатель: затем, когда числитель меньше знаменателя, символ обращаем, пользуясь законом взаимности, и т. д.). Единство плана нарушается необходимостью применения теоремы 2-й, когда числитель меньше знаменателя, но составное число.

Возможно значительно упростить вычисление и приблизиться к единству плана, если ввести в рассмотрение так называемый символ Якоби, представляющий собою обобщение символа Лежандра. К исследованию его мы теперь и обратимся.

Пусть P положительное нечетное число и m любое число взаимно-простое с P. Введем в рассмотрение символ

$$\left(\frac{m}{P}\right),$$

определив его следующим образом:

1) если P — первоначальное число, то символ $\left(\frac{m}{P}\right)$ равен символу Лежандра, т.-е. равен ± 1, смотря по тому есть ли m квадратичный вычет или невычет по модулю P; 2) если P есть составное число и если

$$P=p'p''p'''\ .\ .\ .=\Pi p,$$

где $p', p'', p''', \ldots$ — первоначальные факторы P, то

$$\left(\frac{m}{P}\right)=\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\left(\frac{m}{p'''}\right)\ldots=\Pi\left(\frac{m}{p}\right). \qquad (25)$$

где

$\left(\frac{m}{p'}\right)$, $\left(\frac{m}{p''}\right)$, $\left(\frac{m}{p'''}\right)$, . . . , очевидно — символы Лежандра и, значит, вновь введенный символ Якоби всегда равен $+1$ или -1. Символ Лежандра, очевидно, есть частный случай символа Якоби, в предположении, что знаменатель есть первоначальное число.

Покажем, что свойства символа Лежандра, выражаемые теоремами 1—6, обобщаются и на символ Якоби.

Свойство 1. Если

$$m_1 \equiv m_2 \ (Mod.\ P)$$

то

$$\left(\frac{m_1}{P}\right)=\left(\frac{m_2}{P}\right)$$

Действительно, если $P = p' p'' p''' \ldots$, то из данного сравнения следует

$$\begin{aligned} m_1 &\equiv m_2 \ (Mod.\ p') \\ m_1 &\equiv m_2 \ (Mod.\ p'') \\ m_1 &\equiv m_2 \ (Mod.\ p''') \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

при том m_1 и m_2 — числа взаимно-простые с p', p'', p'''—, т. к. по условию

$$D\ (m_1,\ P) = D\ (m_2,\ P) = 1$$

а потому по теореме 1-й

$$\begin{aligned} \left(\frac{m_1}{p'}\right) &= \left(\frac{m_2}{p'}\right) \\ \left(\frac{m_1}{p''}\right) &= \left(\frac{m_2}{p''}\right) \\ \left(\frac{m_1}{p'''}\right) &= \left(\frac{m_2}{p'''}\right). \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

Перемножая почленно эти равенства, получаем, в силу определения символа Якоби:

$$\left(\frac{m_1}{P}\right) = \left(\frac{m_2}{P}\right).$$

Свойство II.

$$\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right).$$

По теореме 2-й мы имеем

$$\left(\frac{ab}{p'}\right) = \left(\frac{a}{p'}\right)\left(\frac{b}{p'}\right)$$
$$\left(\frac{ab}{p''}\right) = \left(\frac{a}{p''}\right)\left(\frac{b}{p''}\right)$$
$$\cdots\cdots\cdots$$

Перемножая почленно, имеем

$$\Pi\left(\frac{ab}{p}\right) = \Pi\left(\frac{a}{p}\right) . \Pi\left(\frac{b}{p}\right)$$

или, в силу определения символа Якоби

$$\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$$

Свойство III.

$$\left(\frac{1}{P}\right) = 1.$$

Действительно, по теореме 3-й

$$\left(\frac{1}{p'}\right) = 1$$
$$\left(\frac{1}{p''}\right) = 1$$
$$\cdots\cdots$$

Перемножая почленно и пользуясь определением символа Якоби, имеем

$$\left(\frac{1}{P}\right) = 1.$$

Свойство IV.

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

По определению символа Якоби и в силу теоремы 4-й, имеем

$$\left(\frac{-1}{P}\right) = \Pi\left(\frac{-1}{p}\right) = \Pi\,(-1)^{\frac{p-1}{2}} = (-1)^{\Sigma\frac{p-1}{2}}. \quad (26)$$

Рассмотрим тождество

$$P = \Pi\,p = \Pi\,[1 + (p-1)] = 1 + \Sigma\,(p-1) + 4k,$$

которое получим выполняя умножение в произведении $\Pi\,[1+(p-1)]$, выписывая члены, получаемые от перемножения первых членов множителей $[1+(p-1)]$, т. е. 1-ц, и от перемножения одного из 2-х членов на первые, и замечая, что остальные члены содержат, по крайней мере, два фактора типа $p-1$, которые суть четные числа, а потому делятся на 4. Перенося 1 из правой части в левую и деля на 2, имеем

$$\frac{P-1}{2} = \Sigma\frac{p-1}{2} + 2k.$$

Таким образом $\Sigma\,\frac{p-1}{2}$ отличается от $\frac{P-1}{2}$ на четное число, а потому в равенстве (26) в показателе можно произвести замену $\Sigma\,\frac{p-1}{2}$ через $\frac{P-1}{2}$, и окончательно получаем

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$$

Свойство V.

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$$

По определению символа Якоби и в силу теоремы 5-й, имеем

$$\left(\frac{2}{P}\right) = \Pi\left(\frac{2}{p}\right) = \Pi\,(-1)^{\frac{p^2-1}{8}} = (-1)^{\Sigma\frac{p^2-1}{8}}. \quad (27)$$

С другой стороны, имеем

$$P^2 = \Pi\,p^2 = \Pi\,[1 + (p^2-1)].$$

Выполняя справа умножение, отбираем, во-первых, член, получаемый от перемножения всех первых членов множителей $[1+(p^2-1)]$, т.-е. 1-цу, и, во-вторых, члены, получаемые от перемножения одного из вторых членов p^2-1 на первые, т.-е. $\Sigma(p^2-1)$; остальные члены содержат, по крайней мере, два фактора типа p^2-1; но $p=4k\pm1$, следов. $p^2-1=16k^2\pm8k=8k'$ и значит все остальные члены делятся на 64, а потому имеем

$$P^2=1+\Sigma(p^2-1)+64k;$$

перенося 1 влево и деля на 8, получаем

$$\frac{P^2-1}{8}=\Sigma\frac{p^2-1}{8}+8k.$$

Таким образом $\Sigma\frac{p^2-1}{8}$ от $\frac{P^2-1}{8}$ отличается на четное число, почему в равенстве (27) можно $\Sigma\frac{p^2-1}{8}$ в показателе заменить через $\frac{P^2-1}{8}$, и тогда получаем потребную формулу

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

Свойство VI. Если P и Q два нечетных положительных взаимно-простых числа, то

$$\left(\frac{Q}{P}\right)\cdot\left(\frac{P}{Q}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Предполагая разложения на первоначальные факторы

$$P=p'\,p''\,p'''\ldots=\Pi p$$
$$Q=q'\,q''\,q'''\ldots=\Pi q,$$

при чем все q отличны от p в силу условия $D(P,Q)=1$, имеем по определению символа Якоби и в силу теоремы 2-ой

$$\left(\frac{Q}{P}\right)=\Pi\left(\frac{Q}{p}\right)=\Pi\Pi\frac{q}{p}$$
$$\left(\frac{P}{Q}\right)=\Pi\left(\frac{P}{q}\right)=\Pi\Pi\frac{p}{q}$$

Здесь $\Pi\,\Pi$ означает двойное произведение распространенное на все p', p'', p''', . . . и на все q', q'', q''', ...

Перемножая, имеем

$$\left(\frac{\partial}{P}\right) \cdot \left(\frac{P}{Q}\right) = \Pi\Pi\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right)$$

или в силу теоремы 6-й:

$$\left(\frac{Q}{P}\right) \cdot \left(\frac{P}{Q}\right) = \Pi\Pi\,(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = (-1)^{\Sigma\Sigma\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{28}$$

Но ранее было доказано (см. свойство IV), что

$$\Sigma\,\frac{p-1}{2} \equiv \frac{P-1}{2} \;(Mod.\ 2)$$

$$\Sigma\,\frac{q-1}{2} \equiv \frac{Q-1}{2} \;(Mod.\ 2)$$

Отсюда

$$\Sigma\Sigma\,\frac{p-1}{2}\cdot\frac{q-1}{2} = \left(\Sigma\,\frac{p-1}{2}\right)\cdot\left(\Sigma\,\frac{q-1}{2}\right) \equiv \frac{P-1}{2}\cdot\frac{Q-1}{2}\;(Mod.\ 2),$$

а потому в равенстве (28) $\Sigma\Sigma\,\frac{p-1}{2}\cdot\frac{q-1}{2}$ в показателе можно заменить через $\frac{P-1}{2}\cdot\frac{Q-1}{2}$, и таким образом получаем формулу

$$\left(\frac{Q}{P}\right) \cdot \left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}} \tag{29}$$

обобщающую закон взаимности.

На основании доказанных шести свойств символа Якоби мы легко можем вычислить каждый данный символ Якоби

$$\left(\frac{Q}{P}\right).$$

Во-первых, на основании I свойства числитель Q можем заменить наименьшим вычетом R по модулю P. Затем, если R число четное и, может быть, отрицательно, представляем его в виде

$$R = (-1)^k \cdot 2^m \cdot S,$$

где k или 0 или 1-ца, а S—нечетное положительное число (если R—само нечетное число, то $m = 0$; если R положительно, то $k = 0$). Применяя свойства II, IV, V, имеем

$$\left(\frac{Q}{P}\right) = \left(\frac{R}{P}\right) = \left(\frac{(-1)^k \cdot 2^m \cdot S}{P}\right) = \left(\frac{-1}{P}\right)^k \cdot \left(\frac{2}{P}\right)^m \cdot \left(\frac{S}{P}\right) =$$

$$= (-1)^{\frac{P-1}{2} \cdot k} \cdot (-1)^{\frac{P^2-1}{8} \cdot m} \cdot \left(\frac{S}{P}\right)$$

Дело сводится к вычислению символа

$$\left(\frac{S}{P}\right),$$

в котором числитель нечетное положительное число меньшее знаменателя. Здесь применяем формулу (29) или ей равносильную

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \cdot \left(\frac{P}{Q}\right), \qquad (30)$$

получаемую умножением двух частей (29) на $\left(\frac{P}{Q}\right)$. Получаем

$$\left(\frac{S}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{S-1}{2}} \cdot \left(\frac{P}{S}\right).$$

В новом символе $\left(\frac{P}{S}\right)$ числитель больше знаменателя; заменяем его наименьшим вычетом и поступаем опять по прежнему и т. д. При этом процессе получаются символы со все меньшими числителями; поэтому, в конце концов, дойдем до символов типа

$$\left(\frac{2}{P}\right) \text{ или } \left(\frac{1}{P}\right),$$

величины которых известны.

Указанный путь вычисления мы можем применить и к символу Лежандра, т. к. он есть частный случай символа Якоби, и таким образом приходим к более простому методу вычисления символа Лежандра, не требующему разложения числителя на первоначальные множители.

Для примера вычислим этим методом символ $\left(\frac{2212}{1847}\right)$, который мы вычисляли выше.

$$\left(\frac{2212}{1847}\right)=\left(\frac{365}{1847}\right)=(-1)^{\frac{1847-1}{2}\cdot\frac{365-1}{2}}\cdot\left(\frac{1847}{365}\right)=\left(\frac{1847}{365}\right)=\left(\frac{22}{365}\right)=$$

$$=\left(\frac{2}{365}\right)\cdot\left(\frac{11}{365}\right)=(-1)^{\frac{365^2-1}{8}}\cdot\left(\frac{11}{365}\right)=-\left(\frac{11}{365}\right)=$$

$$=-(-1)^{\frac{365-1}{2}\cdot\frac{11-1}{2}}\cdot\left(\frac{365}{11}\right)=-\left(\frac{365}{11}\right)=-\left(\frac{2}{11}\right)=$$

$$=-(-1)^{\frac{11^2-1}{8}}=+1.$$

Теория символа Лежандра позволяет формулировать окончательно условия того, что данное число q является квадратичным вычетом по модулю

$$m=2^{\omega}p_1^{\pi_1}p_2^{\pi_2}p_3^{\pi_3}\ldots\ldots$$

Принимая во внимание изложенное в § 1, мы эти условия формулируем так:

1) Если $\omega=2$, то должно быть $q\equiv 1\ (Mod.\ 4)$;
   если $\omega\geqslant 3$, то должно быть $q\equiv 1\ (Mod.\ 8)$.
2) Должны удовлетворяться условия

$$\left(\frac{q}{p_1}\right)=1,\ \left(\frac{q}{p_2}\right)=1,\ \left(\frac{q}{p_3}\right)=1,\ \ldots\ldots$$

Примечание. Данное выше определение символа Якоби можно еще несколько расширить, а именно можно отказаться от ограничения, состоящего в том, что знаменатель символа должен быть числом положительным, и определить символ с отрицательным знаменателем условием

$$\left(\frac{Q}{-P}\right)=\left(\frac{Q}{P}\right).$$

Для нового определения символа сохраняются все свойства за исключением VI-го, которое впрочем сохраняется, если по крайней мере одно из двух чисел P и Q — положительное.

Нами разрешен вопрос о критерии возможности сравнения

$$x^2 \equiv q \ (Mod.\ p).$$

Интересно указать, как же, в случае возможности, решить это сравнение, к решению которого, как мы видели приводится решение общего сравнения 2-й степени.

Можно найти решение общим приемом — путем испытаний, вставляя в сравнение числа 1, 2, 3, ... p—1, и следует заметить, что этот прием на практике часто и приходится применять.

Укажем на другой прием, который применим в некоторых случаях.

Условие возможности сравнения дает

$$q^{\frac{p-1}{2}} \equiv 1 \ (Mod.\ p).$$

Допустим, что показатель есть нечетное число

$$\frac{p-1}{2} = 2k+1,$$

т. е. другими словами

$$p = 4k+3$$

Условие возможности принимает вид

$$q^{2k+1} \equiv 1 \ (Mod.\ p)$$

Умножая обе части на q, имеем

$$q^{2k+2} \equiv q \ (Mod.\ p).$$

Сравнивая с данным сравнением, непосредственно усматриваем, что оно допускает решение

$$x \equiv q^{k+1} \ (Mod.\ p)$$

Второе решение, как всегда, найдем вычитая первое (или его наименьший вычет) из p.

Так решается сравнение для модуля вида $4k+3$;

Пример. $x^2 \equiv 30 \ (Mod.\ 7)$

Сравнение возможно, ибо

$$\left(\frac{30}{7}\right) = \left(\frac{2}{7}\right) = \left(-1\right)^{\frac{7^2-1}{8}} = +1;$$

так как

$$p = 7 = 4.1 + 3,$$

то решение сравнения есть

$$x \equiv 30^2 \equiv 2^2 = 4 \ (Mod.\ 7).$$

Второе решение

$$x \equiv 7 - 4 = 3 \ (Mod.\ 7).$$

Пусть теперь модуль p есть число вида $4k+1$. Условие возможности сравнения дает

$$q^{2k} \equiv 1 \ (Mod.\ p)$$

или

$$(q^k - 1)\ (q^k + 1) \equiv 0 \ (Mod.\ p).$$

Из двух факторов левой части или первый, или второй делятся на p. Пусть это будет первый; тогда

$$q^k \equiv 1 \ (Mod.\ p).$$

Если k есть нечетное число

$$k = 2h + 1,$$

то умножая две части на q, имеем

$$q^{2h+2} \equiv q \ (Mod.\ p)$$

и отсюда находим решение сравнения

$$x \equiv q^{h+1} \ (Mod.\ p).$$

Если k есть четное число

$$k = 2h,$$

то имеем

$$q^{2h} \equiv 1 \ (Mod.\ p)$$

или

$$(q^h - 1)\ (q^h + 1) \equiv 0 \ (Mod.\ p).$$

Если из двух множителей левой части первый делится на p, то имеем

$$q^h \equiv 1 \ (Mod.\ p)$$

и можно продолжать прежние рассуждения.

Выше мы решали вопрос: найти все квадратичные вычеты данного модуля. Естественно поставить теперь такой вопрос: дано число n, найти все модули m, для которых n есть квадратичный вычет. Так как, согласно результатам § 1-го, n есть квадратичный вычет для составного модуля только в том случае, если оно есть квадратичный вычет в отдельности для всех его простых факторов, то задача сводится к нахождению простых модулей p, для которых n есть квадратичный вычет. Можно сказать, что задача эта есть задача решения уравнения

$$\left(\frac{n}{p}\right) = +1,$$

где p есть неизвестное; вопрос, решенный нами ранее, сводился к решению уравнения

$$\left(\frac{q}{p}\right) = +1,$$

где p — дано, а q — неизвестное число.

Покажем, как наша задача может быть сведена к другой, ей эквивалентной. Если n есть квадратичный вычет по модулю p, то возможно сравнение

$$x^2 - n \equiv 0 \ (Mod.\ p),$$

другими словами, для некоторого численного значения x многочлен $x^2 - n$ или, как говорят, форма $x^2 - n$ делится на число p. В таком случае принято говорить, что p есть делитель формы $x^2 - n$, и следовательно задача наша эквивалентна задаче изыскания (простых) делителей формы $x^2 - n$.

Преобразуем ее еще, заменив форму $x^2 - n$ однородной формой

$$t^2 - nu^2.$$

Покажем, что делители формы $x^2 - n$ суть делители формы $t^2 - nu^2$ и обратно делители формы $t^2 - nu^2$, при взаимно-простых t и u, суть делители формы $x^2 - n$.

Первое положение очевидно, ибо при $t = x$, $u = 1$ вторая форма переходит в первую. Пусть теперь p есть делитель $t^2 - nu^2$ при взаимно-простых t и u, так что при этих значениях t и u

$$t^2 - nu^2 \mid p$$

Необходимо имеем

$$D(u, p) = 1,$$

так как если бы u и p имели общего простого делителя, то из делимости

$$t^2 - nu^2 \mid p$$

следовало бы, что и t имеет этого общего делителя с p, а значит t и u—не взаимно-простые что противно предположению. Раз $D(u, p) = 1$, можно найти x, удовлетворяющее сравнению

$$ux \equiv t \ (Mod.\ p).$$

Но тогда из

$$t^2 - nu^2 \equiv 0 \ (Mod.\ p)$$

следует

$$u^2x^2 - nu^2 \equiv 0 \ (Mod.\ p)$$

или

$$u^2(x^2 - n) \mid p$$

и т. к.

$$D(u, p)=1,$$

то

$$x^2-n \mid p,$$

т.-е. p есть делитель формы x^2-n.

Таким образом, задача наша эквивалентна задаче изыскания делителей формы

$$t^2-nu^2.$$

Мы ограничимся рассмотрением нескольких частных случаев

1) Пусть $n=1$

Так как

$$\left(\frac{n}{p}\right)=\left(\frac{1}{p}\right)=+1,$$

то любое простое число есть делитель формы

$$t^2-u^2;$$

иначе: 1 есть квадратичный вычет по любому модулю, что и очевидно, т. к. $1=1^2$.

2) Пусть $n=-1$

$$\left(\frac{n}{p}\right)=\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

Для того чтобы $(-1)^{\frac{p-1}{2}}=+1$ необходимо $\frac{p-1}{2}=2k$ или $p=4k+1$. Итак делители формы

$$t^2+u^2$$

суть простые числа вида $4k+1$.

3) Пусть $n=2$

$$\left(\frac{n}{p}\right)=\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}},$$

что равно $+1$ для $p = 8k \pm 1$. Итак делители формы

$$t^2 - 2u^2$$

суть простые числа вида $8k \pm 1$.

В каждом из трех случаев решения задачи группируются в одной или нескольких арифметических прогрессиях (все простые числа, числа вида $4k+1$, числа вида $8k \pm 1$); можно было бы показать, что так дело обстоит и в самом общем случае.

ГЛАВА ВОСЬМАЯ.

Двучленные сравнения высших степеней.

Общий вид двучленного сравнения есть

$$ax^n \equiv b \ (Mod.\ k), \tag{1}$$

при чем a и b предполагаем взаимно-простыми с модулем k. В таком случае, очевидно, и решение x должно быть числом взаимно-простым с модулем, так как в противном случае левая, а следовательно и правая часть сравнения должна бы иметь общих делителей с модулем.

Называя через a' число союзное с a по модулю k, так что

$$a'a \equiv 1 \ (Mod.\ k)$$

и умножая две части сравнения (1) на a', приведем его к виду

$$aa'x^n \equiv x^n \equiv a'b \ (Mod.\ k),$$

или

$$x^n \equiv q \ (Mod.\ k), \tag{2}$$

при чем

$$D(q, k) = 1,$$

а следовательно и решение x должно быть взаимно-простым с модулем k.

Если сравнение (2) имеет решения, то число q называется n-ичным (квадратичным, кубичным, биквадратичным, ...) вычетом по модулю k.

Пусть ξ есть решение сравнения (2) и пусть z какое-нибудь решение сравнения

$$z^n \equiv 1 \ (Mod.\ k). \tag{3}$$

Легко видеть, что

$$x \equiv \xi z \ (Mod.\ k) \tag{4}$$

есть решение сравнения (2).
Действительно

$$x^n = \xi^n z^n \equiv q.1 = q \ (Mod.\ k).$$

Обратно пусть ξ' какое-нибудь, отличное от ξ решение сравнения (2).

Тогда

$$\xi'^n \equiv \xi^n \equiv q \ (Mod.\ k).$$

Пусть ξ_1 число союзное ξ по модулю k, так что

$$\xi_1 \xi \equiv 1 \ (Mod.\ k).$$

Рассмотрим произведение $\xi_1 \xi'$; возводя его в n-ую степень имеем

$$(\xi_1 \xi')^n = \xi_1^n . \xi'^n \equiv \xi_1^n . \xi^n \equiv (\xi_1 \xi)^n \equiv 1 \ (Mod.\ k).$$

Таким образом $\xi_1 \xi'$ есть некоторое решение z сравнения (3):

$$\xi_1 \xi' \equiv z \ (Mod.\ k).$$

Умножая обе части на ξ и замечая, что

$$\xi_1 \xi \equiv 1 \ (Mod.\ k),$$

получаем

$$\xi' \equiv \xi z \ (Mod.\ k).$$

Таким образом формула (4) дает все решения сравнения (2), и если это последнее возможно, то оно имеет ровно столько решений, сколько сравнение (3), так как формула (4), как легко убедиться, для различных z дает различные x.

Выведем критерий возможности сравнения (2), ограничиваясь случаем модуля абсолютно-простого.

По предположению существует такое число x, что

$$x^n \equiv q \ (Mod.\ p). \tag{5}$$

Пусть

$$D(n, p-1) = d; \ n = n'd.$$

Возведем q в степень $\frac{p-1}{d}$. Имеем

$$q^{\frac{p-1}{d}} \equiv x^{n\frac{p-1}{d}} \equiv x^{(p-1)n'} \equiv 1 \ (Mod.\ p)$$

по теореме Фермата.

Итак, если сравнение (5) возможно, т.-е. q есть n-ичный вычет по модулю p, то

$$q^{\frac{p-1}{d}} \equiv 1 \ (Mod.\ p). \tag{6}$$

Можно было бы доказать, что условие (6) не только необходимое, но и достаточное.

В случае $n=2$

$$d = D(2, p-1) = 2,$$

и условие (6) дает знакомое нам условие

$$q^{\frac{p-1}{2}} \equiv 1 \ (Mod.\ p)$$

квадратичного вычета.

Обращаемся к исследованию сравнения вида (3), которое всегда возможно, т. к. очевидно допускает решение

$$z \equiv 1 \ (Mod.\ k)$$

Рассмотрим одновременно два таких сравнения

$$z^r \equiv 1 \ (Mod.\ k) \tag{7}$$

$$z^s \equiv 1 \ (Mod.\ k) \tag{8}$$

Пусть z_1 — число союзное z, так что

$$z_1 z \equiv 1 \ (Mod.\ k) \tag{9}$$

Возводя обе части в степень s, имеем

$$z^s \cdot z_1^{\,s} \equiv 1 \ (Mod.\ k)$$

или, в силу (8):

$$z^s \cdot z_1^{\,s} \equiv z^s \ (Mod.\ k).$$

Сокращая обе части на число z^s взаимно-простое с модулем (ибо $D(z, k) = 1$), получаем

$$z_1^{\,s} \equiv 1 \ (Mod.\ k). \qquad (10)$$

Таким образом сравнению (8) на-ряду с числом z удовлетворяет и союзное число. Это, конечно, общее свойство сравнений вида (3). Возведем обе части сравнения (7) в некоторую степень x, а обе части сравнения (10) в степень y и перемножим их; получим

$$z^{rx} \cdot z_1^{\,sy} \equiv 1 \ (Mod.\ k).$$

Это сравнение можно переписать так:

$$z^{rx-sy} \cdot z^{sy} \cdot z_1^{\,sy} \equiv z^{rx-sy} \cdot (zz_1)^{sy} \equiv 1 \ (Mod.\ k)$$

или, в силу (9):

$$z^{rx-sy} \equiv 1 \ (Mod.\ k),$$

где x и y любые положительные числа (предполагается лишь $rx > sy$).

Пусть теперь общий наибольший делитель чисел r и s

$$D(r, s) = \delta.$$

тогда можно подыскать такие два положительных числа x и y, чтобы имело место равенство

$$\delta = rx - sy,$$

и мы получаем

$$z^{\delta} \equiv 1 \ (Mod.\ k). \qquad (11)$$

Итак, если z удовлетворяет двум сравнениям (8) и (9), то удовлетворяет и сравнению того же вида (11), где δ— общий наибольший делитель степеней данных сравнений.

Теперь заметим, что z, как число взаимно-простое с модулем, необходимо удовлетворяет, в силу теоремы Ферма, сравнению

$$z^{\varphi(k)} \equiv 1 \ (Mod.\ k). \tag{12}$$

Поэтому, если z удовлетворяет какому-нибудь сравнению

$$z^n \equiv 1 \ (Mod.\ k), \tag{3}$$

то, в силу предшествующего, оно удовлетворяет и сравнению

$$z^d \equiv 1 \ (Mod.\ k), \tag{13}$$

где

$$d = D(n,\ \varphi(k))$$

и следовательно есть делитель $\varphi(k)$.

Таким образом достаточно рассмотреть только сравнения вида

$$z^d \equiv 1 \ (Mod.\ k), \tag{13}$$

где d — делитель $\varphi(k)$, т. к. решения всякого сравнения типа (3), как мы видели, удовлетворяют необходимо некоторому сравнению типа (13). Обратно, очевидно, всякое решение сравнения (13) удовлетворяет сравнению (3), если

$$d = D(n,\ \varphi(k)),$$

ибо для решения сравнения (13) имеем

$$z^n = \left(z^d\right)^{\frac{n}{d}} \equiv 1^{\frac{n}{d}} \equiv 1 \ (Mod.\ k).$$

Пусть в частности k есть простое число p; тогда $\varphi(k) = p-1$, и d есть делитель числа $p-1$. Сравнение

$$z^d \equiv 1 \ (Mod.\ p) \tag{14}$$

в этом случае, как мы видели в свое время, имеет максимальное число решений, т.-е. ровно d.

Все решения сравнения (14) можно классифицировать на такие, которые не удовлетворяют ни одному сравнению того же типа низшей степени, и на такие, которые удовлетворяют сравнениям низших степеней. Решения 1-го типа называются первообразными. Ясно, что число 1, которое удовлетворяет всякому сравнению типа (3), не есть первообразное решение.

Пусть a есть первообразное решение сравнения (14). Рассмотрим ряд степеней a:

$$a^0 = 1,\ a,\ a^2,\ a^3,\ \ldots,\ a^{d-1}. \tag{15}$$

Легко видеть, что каждое из чисел (15) есть решение сравнения (14). В самом деле

$$(a^s)^d = (a^d)^s \equiv 1^s \equiv 1\ (Mod.\ p).$$

С другой стороны, каждые два числа ряда (15) различны по модулю p: в самом деле, если бы имели

$$a^r \equiv a^s\ (Mod.\ p),$$

то, сокращая две части на a^s (считаем $r > s$), имели бы

$$a^{r-s} \equiv 1\ (Mod.\ p),$$

где $r - s < d$, и a, противно предположению, удовлетворяло бы сравнению типа

$$z^m \equiv 1\ (Mod.\ p),$$

где $m < d$.

Итак ряд (15) исчерпывает все d решений сравнения (14).

ГЛАВА ДЕВЯТАЯ.

Степенные вычеты и указатели.

§ 1. Степенные вычеты. Показатель, к которому принадлежит число по данному модулю.

Рассмотрим модуль k и число a взаимно-простое с модулем. Рассмотрим ряд степеней числа a:

$$a^0 = 1,\ a,\ a^2,\ a^3,\ a^4, \ldots\ldots \qquad (1)$$

Ряд (1)—бесконечный, а число классов по модулю k конечно, поэтому необходимо различные члены ряды (1) принадлежат к одному и тому же классу. Пусть в частности

$$a^{s+n} \equiv a^s \ (Mod.\ k),$$

где $n > 0$. В силу того, что a—число взаимно-простое с модулем

$$D(a^s,\ k) = 1$$

и сокращая две части сравнения на a^s, имеем

$$a^n \equiv 1 \ (Mod.\ k).$$

Итак, для всякого числа a, взаимно-простого с модулем, найдется такая положительная степень n, в которой это число сравнимо с 1-цей. Таких показателей n само собою разумеется бесконечное множество, ибо на-ряду с n всякое кратное n обладает тем же свойством. Пусть δ есть наименьший из всех этих показателей, т.-е. пусть δ есть наи-

меньшее положительное число, в степени которого a сравнимо с 1-цей. Другими словами

$$a^{\delta} \equiv 1 \ (Mod.\ k) \tag{2}$$

и

a^h не сравнимо с единицей $(Mod.\ k)$

для

$$0 < h < \delta.$$

Такое число δ называется показателем, к которому принадлежит a по модулю k.

Рассмотрим начальную часть ряда (1)

$$a^0 = 1,\ a,\ a^2,\ a^3, \ldots\ldots, a^{\delta-1}. \tag{3}$$

В нем всего δ членов. Легко видеть, что все они различных классов по модулю k.

В самом деле, пусть

$$a^r \equiv a^s \ (Mod.\ k),$$

где r и s — числа ряда

$$0,1,2,3, \ldots\ldots, \delta - 1 \tag{4}$$

и $r > s$. Сокращая на a^s, имеем

$$a^{r-s} \equiv 1 \ (Mod.\ k).$$

Здесь r и s числа ряда (4) и следовательно

$$0 < r - s < \delta$$

и таким образом приходим к противоречию с определением показателя δ.

Итак, числа ряда (3) все принадлежат к различным классам. Покажем, что остальные члены ряда (1) принадлежат к тем же классам, что и числа ряда (3). Так,

$$a^{\delta} \equiv 1 \equiv a^0 \ (Mod.\ k)$$
$$a^{\delta+1} \equiv a^{\delta} a \equiv a \ (Mod.\ k)$$
$$a^{\delta+2} \equiv a^{\delta} a^2 \equiv a^2 \ (Mod.\ k)$$
$$\ldots\ldots\ldots\ldots$$

Вообще рассмотрим a^m и разделим m на δ и пусть частное есть s и остаток r, так что

$$m = s\delta + r.$$

Имеем, очевидно:

$$a^m = a^{s\delta + r} = (a^\delta)^s a^r \equiv 1 . a^r \equiv a^r \ (Mod.\ k).$$

Но r, как остаток, меньше δ и следовательно есть число ряда (4), а значит a^r — число ряда (3).

Мы видим таким образом, что ряд (1) есть ряд периодический: первые δ его членов принадлежат к различным классам по модулю k; дальше периодически повторяются представители тех же классов.

Рассмотрим какие-нибудь два члена a^m и $a^{m'}$ ряда (1). Когда они будут одного класса? Называя через r и r' остатки от деления m и m' на δ, имеем

$$a^m \equiv a^r \ (Mod.\ k)$$
$$a^{m'} \equiv a^{r'} \ (Mod.\ k),$$

где a^r и $a^{r'}$ члены ряда (3) и значит принадлежат к одному классу только в случае совпадения. Таким образом a^m и $a^{m'}$ принадлежат к одному классу тогда и только тогда, когда $r = r'$, т.-е. когда

$$m \equiv m' \ (Mod.\ \delta).$$

В частности решим вопрос, какие члены ряда (1) будут одного класса с первым числом $a^0 = 1$, т.-е. другими словами для каких значений s

$$a^s \equiv 1 \ (Mod.\ k).$$

Согласно предыдущему, это будет тогда и только тогда, когда

$$s \equiv 0 \ (Mod.\ \delta),$$

т.-е. для значений s кратных δ. Мы знаем (в силу теоремы Фермата), что

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

Отсюда, согласно предыдущему

$$\varphi(k) \mid \delta,$$

т.-е. показатель, к которому принадлежит число по данному модулю k, есть необходимо делитель $\varphi(k)$.

Если в частности модуль k есть простое число p, то $\varphi(k) = p - 1$, и δ должно быть делителем $p - 1$.

Сделаем теперь такое замечание:
если

$$a \equiv b \ (Mod.\ k),$$

то и

$$a^n \equiv b^n \ (Mod.\ k),$$

и значит одновременно, если $a^n \equiv 1$, то и $b^n \equiv 1$ и обратно. Отсюда ясно, что все числа одного класса принадлежат к одному и тому же показателю по данному модулю. Можно поэтому говорить не об отдельных числах, а о классах чисел, принадлежащих к данному показателю δ; при изыскании же чисел, принадлежащих к данному показателю, можно ограничиться рассмотрением системы вычетов, а так как числа мы предполагали выше взаимно-простыми с модулем, то следует рассматривать приведенную систему вычетов и, значит, в случае простого модуля p ряд чисел

$$1, 2, 3, \ldots\ldots, p - 1.$$

Пример. Возьмем $p = 7$; тогда будем рассматривать систему вычетов

$$a = 1, 2, 3, 4, 5, 6.$$

Для каждого a определяем соответствующее δ, возводя a последовательно в степени 1, 2, ... и определяя первый показатель, при котором получается степень a, сравнимая с единицей.

Так, имеем:

$$a = 1 ; 1^1 = 1 \equiv 1 \ (Mod.\ 7)$$
$$a = 2 ; 2^1 = 2 ; 2^2 = 4 ; 2^3 = 8 \equiv 1 \ (Mod.\ 7)$$
. . . . . .

Получаем таблицу:

a	1	2	3	4	5	6
δ	1	3	6	3	6	2

(5)

Из этой таблицы усматриваем, что к показателю $\delta = 3$ принадлежат два класса чисел, имеющих представителями 2 и 4; к показателю 2 принадлежит один класс чисел, имеющий представителем 6, и т. д.

Возможные значения $\delta = 1, 3, 6, 2$ все суть делители $p - 1 = 6$ как и должно быть в силу общих результатов.

Пусть теперь обратно дано число δ—один из делителей числа $p - 1$. Возникает вопрос, всегда ли найдется класс чисел, принадлежащих к показателю δ по модулю p и сколько будет таких классов. Предположим сначала, что по крайней мере один класс принадлежит к показателю δ. Пусть представитель этого класса есть число a. Ищем другие числа (других классов), тоже принадлежащие к показателю δ. Все они суть решения сравнения

$$x^{\delta} \equiv 1 \ (Mod.\ p) \qquad (6).$$

Но не все решения этого сравнения принадлежат к показателю δ, а только такие, которые не удовлетворяют ни одному сравнению того же вида низшей степени (так называемые первообразные решения, см. гл. VIII). Во всяком случае числа, принадлежащие к показателю δ, следует искать среди решений сравнения (6).

Возвратимся к ряду (3). Легко видеть, что каждое число этого ряда удовлетворяет сравнению (6); действительно

$$(a^r)^{\delta} = (a^{\delta})^r \equiv 1^r = 1 \ (Mod.\ p).$$

С другой стороны, все члены ряда (3), как мы видели, различных классов, и число их равно δ; следовательно числа ряда (3) исчерпывают решения сравнения (6), а потому только среди них следует искать числа, принадлежащие к показателю δ. Определим, к какому показателю принадле-

жит какое-либо число a^r ряда (3). Пусть этот показатель есть h. Тогда

$$(a^r)^h = a^{rh} \equiv 1 \ (Mod.\ p),$$

и h есть наименьшее положительное число, для которого подобное сравнение имеет место. Но ранее было доказано, что если a принадлежит к показателю δ по модулю p, и если

$$a^s \equiv 1 \ (Mod.\ p),$$

то число s есть кратное δ. Таким образом имеем требование

$$rh|\delta.$$

Пусть

$$D(r,\delta) = \varepsilon,$$
$$r = \varepsilon.r', \qquad \delta = \varepsilon.\delta',$$

при чем

$$D(r',\delta') = 1.$$

Мы имеем требование

$$\varepsilon r' h | \varepsilon \delta'$$

или, по сокращении на ε,

$$\varepsilon' h | \delta'.$$

Но т. к. $D(\varepsilon', \delta') = 1$, то приходим к требованию

$$h|\delta',$$

и т. к. h должно быть наименьшим положительным числом, удовлетворяющим этому требованию, то очевидно

$$h = \delta' = \frac{\delta}{D(r, \delta)},$$

и к такому показателю по модулю p принадлежит a^r.

Мы желаем найти такие значения r, для которых $h = \delta$. Это будет, очевидно, в случае

$$D(r, \delta) = 1,$$

т.-е. для значений r взаимно-простых с δ, а т. к. r есть одно из чисел ряда

$$0,\ 1,\ 2,\ \cdots,\ \delta - 1,$$

то таких значений r (меньших δ и взаимно-простых с δ) будет $\varphi(\delta)$, где $\varphi(\delta)$ — функция Гаусса.

Итак, число классов чисел, принадлежащих к показателю δ, равно $\varphi(\delta)$, но в предположении, что существует хотя одно число, принадлежащее к показателю δ. Вот от этого предположения и постараемся теперь освободиться.

Называя, вообще, через $\psi(\delta)$ число классов, принадлежащих к показателю δ, мы, согласно предыдущему, имеем только две возможности: или $\psi(\delta) = 0$, или $\psi(\delta) = \varphi(\delta)$.

Рассмотрим для данного модуля p все возможные делители δ числа $p-1$; это суть всевозможные значения показателя δ при модуле p. Каждый класс, кроме класса чисел кратных p, принадлежит к одному из этих показателей. К определенному значению δ принадлежит $\psi(\delta)$ классов, а значит всего классов по модулю p имеется

$$\sum_{-1} \psi(\delta),$$

где Σ есть знак числового интеграла по делителям числа $p-1$. С другой стороны, общее число классов по модулю p, за исключением класса чисел кратных p, равно $p-1$; следовательно

$$\sum_{p-1} \psi(\delta) = p - 1. \tag{7}$$

На-ряду с равенством (7) рассмотрим равенство

$$\sum_{p-1} \varphi(\delta) = p - 1, \tag{8}$$

выражающее известную теорему Гаусса для функции $\varphi(\delta)$, и вычтем из равенства (8) равенство (7); получим

$$\sum_{p-1} \{\varphi(\delta) - \psi(\delta)\} = 0. \tag{9}$$

Так как $\psi(\delta)$ или равно нулю или совпадает с $\varphi(\delta)$, то все члены суммы в левой части равенства (9) — или положи-

тельные числа или равны нулю. Но в таком случае сумма может равняться нулю только тогда, когда каждое слагаемое в отдельности равно нулю, и, следовательно, для любого δ

$$\psi(\delta) = \varphi(\delta),$$

т.-е. число классов, принадлежащих к показателю δ, независимо от какого бы то ни было предположения, всегда равно $\varphi(\delta)$.

Вернемся теперь к вопросу, рассмотренному в главе VIII, т.-е. к решению сравнения

$$x^n \equiv 1 \ (Mod.\ p).$$

Мы видели, что его решение приводится к решению сравнения

$$x^\delta \equiv 1 \ (Mod.\ p), \tag{10}$$

где

$$\delta = D(p-1, n).$$

В главе VIII мы упоминали о первообразных решениях этого сравнения, т.-е. о таких, которые не удовлетворяют ни одному сравнению того же вида низшей степени. Теперь ясно, что каждое такое первообразное решение есть число, принадлежащее к показателю δ, и сравнение (10) имеет $\varphi(\delta)$ первообразных решений. Если a есть одно из чисел, принадлежащих к показателю δ, то все решения сравнения (10) даются рядом

$$a^0 = 1,\ a,\ a^2,\ \cdots,\ a^{\delta-1}.$$

§ 2. Первообразные корни данного модуля; теория указателей (индексов).

Мы видели, что для простого модуля p существуют числа, принадлежащие к любому показателю δ, делителю числа $p-1$. Между прочим существуют числа, принадлежащие к показателю $p-1$, и число их, согласно § 1, равно $\varphi(p-1)$.

Такие числа называют **первообразными корнями** модуля p.

Пусть g—первообразный корень. Тогда

$$g^{p-1} \equiv 1 \ (Mod.\ p).$$

и

$$g^s \text{ не сравнимо с единицей } (Mod.\ p) \tag{1}$$

для

$$0 < s < p-1.$$

Ряд степеней первообразного корня g

$$g^0 = 1,\ g,\ g^2,\ g^3,\ \cdots\cdots g^{p-2}, \tag{2}$$

согласно результатам § 1, состоит из представителей различных классов, а т. к. общее число членов ряда (2) есть $p-1$, то в ряде (2) мы имеем приведенную систему вычетов по модулю p, или систему представителей всех классов, кроме класса чисел, делящихся на p.

Таким образом, устранив в дальнейшем раз навсегда числа, делящиеся на p, мы для всякого числа c (не делящегося на p) найдем один и только один член ряда (2), с которым c сравнимо по данному модулю:

$$c \equiv g^\gamma \ (Mod.\ p). \tag{3}$$

Другими словами в ряду чисел

$$0,\ 1,\ 2,\ 3,\ \cdots,\ p-2 \tag{4}$$

находится одно и только одно число γ, для которого имеет место сравнение (3). Это число γ называется **указателем или индексом** числа c при основании g и обозначается

$$\gamma = \mathrm{Ind}_g\, c. \tag{5}$$

Каждое число (не делящееся на p) имеет единственный, вполне определенный индекс; точнее, индекс принадлежит одновременно целому классу чисел, ибо, если

$$c' \equiv c \ (Mod.\ p),$$

то, очевидно,

$$\mathrm{Ind}_g c' = \mathrm{Ind}_g c,$$

и каждому индексу (каждому числу ряда (4)) соответствует один класс чисел.

Если бы вместо сравнения (3) мы имели равенство

$$c = g^{\gamma},$$

то число γ было бы логарифмом числа c при основании g. Таким образом индексы в теории чисел аналогичны логарифмам в алгебре. Интересно отметить, что аналогия простирается и дальше: свойства индексов аналогичны свойствам логарифмов, как это будет показано далее.

Для примера рассмотрим число $p = 7$. В § 1 была составлена табличка (5), из которой можно было усмотреть, к какому показателю по модулю 7 принадлежат все классы чисел. Из этой таблички видно, что к показателю $p - 1 = 6$ принадлежат два числа 3 и 5. Таким образом эти два числа и суть первообразные корни по модулю 7. Возьмем одно из них, например 3, за основание системы индексов. Возводя 3 в степени 0, 1, 2, 3, 4, 5, имеем

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 9 \equiv 2, \quad 3^3 = 27 \equiv 6, \quad 3^4 = 81 \equiv 4,$$
$$3^5 = 243 \equiv 5 \quad (\textit{Mod.}\ 7)$$

и таким образом можем составить две таблицы:

N	1	2	3	4	5	6
Ind. N	0	2	1	4	5	3

Ind. N	0	1	2	3	4	5
N	1	3	2	6	4	5

Помощью первой находим индекс данного числа, помощью 2-й по данному индексу находим число. Таблицы, составленные нами, вполне аналогичны таблицам логарифмов и антилогарифмов.

Такие таблицы можно составить для любого простого модуля, выбирая за основание один из первообразных корней модуля.

Докажем теперь ряд теорем для индексов, вполне аналогичных основным теоремам теории логарифмов.

Теорема 1.

$$\text{Ind. } 1 = 0.$$

Действительно, если

$$g^{\gamma} \equiv 1 \ (Mod.\ p)$$

и γ может иметь только одно из значений 0, 1, 2, 3, ····, $p-2$,

то очевидно $\gamma = 0$, и тогда

$$g^0 = 1 \equiv 1 \quad (Mod.\ p).$$

Теорема 2.

$$\text{Ind } (ab) \equiv \text{Ind } a + \text{Ind } b \quad (Mod.\ p - 1)$$

В самом деле пусть

$$\text{Ind}_g\, a = \gamma_1,\ \text{Ind}_g\, b = \gamma_2,\ \text{Ind}_g\, (ab) = \gamma$$

В таком случае

$$a \equiv g^{\gamma_1} \ (Mod.\ p)$$
$$b \equiv g^{\gamma_2} \ (Mod.\ p)$$
$$ab \equiv g^{\gamma} \ (Mod.\ p)$$

Перемножая почленно первые два сравнения и сравнивая с третьим, имеем

$$g^{\gamma_1+\gamma_2} \equiv g^{\gamma} \ (Mod.\ p).$$

В свое время нами была доказана теорема, что две различных степени числа a, принадлежащего к показателю δ, сравнимы по данному модулю в том случае, если показатели степеней сравнимы по модулю δ. Применяя к данному случаю, где $a = g$ и $\delta = p - 1$, имеем

$$\gamma \equiv \gamma_1 + \gamma_2 \ (Mod.\ p - 1)$$

или

$$\text{Ind } (ab) \equiv \text{Ind } a + \text{Ind } b \ (Mod.\ p - 1)$$

Очевидно, теорема распространяется на произведение любого числа множителей. Так

$$\text{Ind } (abc) \equiv \text{Ind } (ab) + \text{Ind } c \equiv \text{Ind } a + \text{Ind } b + \text{Ind } c \ (Mod.\ p-1).$$

Вообще

$$\text{Ind } (abc \dots k) \equiv \text{Ind } a + \text{Ind } b + \text{Ind } c + \dots + \text{Ind } k \ (Mod.\ p-1).$$

Теорема 3.

$$\text{Ind } (a^n) \equiv n \text{ Ind } a \quad (Mod.\ p-1)$$

Действительно,

$$\text{Ind } (a^n) = \text{Ind } (aa \dots a) \equiv \text{Ind } a + \text{Ind } a + \dots + \text{Ind } a = n \text{ Ind } a \ (Mod.\ p-1).$$

Теорема 4. Индекс основания равен единице.

Действительно,

$$g = g^1 \equiv g^1 \ (Mod.\ p-1)$$

Следовательно,

$$\text{Ind } g = 1$$

Теорема 5.

$$\text{Ind } (-1) = \frac{p-1}{2}$$

В силу теоремы Фермата

$$g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv 0 \ (Mod.\ p).$$

Из двух факторов 2-й части первый заведомо не делится на p, т. к. в противном случае мы бы имели

$$g^{\frac{p-1}{2}} \equiv 1 \ (Mod.\ p),$$

что противоречило бы основному свойству g, как первообразного корня (ср. выше формулы (1)). Поэтому на p

делится необходимо второй фактор и, следовательно, имеем

$$g^{\frac{p-1}{2}} \equiv -1 \ (Mod.\ p),$$

откуда непосредственно следует

$$\mathrm{Ind}\ (-1) = \frac{p-1}{2}.$$

Все приведенные теоремы (за исключением, пожалуй, последней) вполне аналогичны основным теоремам теории логарифмов (логарифм единицы равен нулю, логарифм основания равен единице, логарифм произведения равен сумме логарифмов производителей). Покажем, что переход от одного основания индексов к другому совершается тоже аналогично переходу от одного основания логарифмов к другому. Пусть для модуля p имеются первообразные корни g и g', и пусть индекс числа c при основании g есть γ. Тогда имеем

$$g^{\gamma} \equiv c \ (Mod.\ p)$$

Два числа одного класса имеют равные индексы; поэтому, взяв индексы по основанию g', имеем

$$\mathrm{Ind}_{g'}\ (g^{\gamma}) = \mathrm{Ind}_{g'}\ c$$

Левая часть равенства, в силу теоремы 3-й сравнима по модулю $p-1$ с

$$\gamma\ \mathrm{Ind}_{g'}\ g,$$

и потому окончательно имеем

$$\mathrm{Ind}_{g'}\ c \equiv \gamma.\ \mathrm{Ind}_{g'}\ g \equiv \mathrm{Ind}_{g}\ c.\ \mathrm{Ind}_{g'}\ g \ (Mod.\ p-1).$$

Таким образом от индексов при основании g переходим к индексам при новом основании g', умножая все прежние индексы на постоянный фактор

$$\mathrm{Ind}_{g'}\ g,$$

который играет роль „модуля“ для перехода от одних логарифмических таблиц к другим.

Вообще, если имеем сравнение

$$A \equiv B \ (Mod.\ p),$$

то из него следует

$$\text{Ind. } A = \text{Ind. } B,$$

т. к. числа одного класса имеют равные индексы. Если одна или обе части сравнения представляют собою произведения или степени, то, применяя вышедоказанные теоремы, получим вместо равенства сравнение по модулю p —1. Весь этот процесс можно охарактеризовать так, что от двух частей данного сравнения берем индексы, и в результате получаем сравнение по модулю $p-1$.

Так например, пусть дано сравнение 1-й степени

$$ax \equiv b \ (Mod.\ p)$$

Взяв индексы от двух частей, получаем

$$\text{Ind } a + \text{Ind } x \equiv \text{Ind } b \ (Mod\ p—1).$$

откуда

$$\text{Ind } x \equiv \text{Ind } b - \text{Ind } a \ (Mod.\ p—1)$$

По таблицам, зная Ind x, непосредственно находим x, и таким образом получаем новый метод решения сравнений 1-й степени

§ 3. Приложение теории индексов к решению двучленных сравнений.

Рассмотрим двучленное сравнение

$$x^n \equiv q \ (Mod.\ p). \qquad (1)$$

Взяв индексы двух частей, имеем

$$n \text{ Ind } x \equiv \text{Ind } q \ (Mod.\ p—1) \qquad (2)$$

Для неизвестного Ind x получилось сравнение 1-й степени. Пусть

$$D\ (n,\ p—1) = \delta. \qquad (3)$$

Условие возможности сравнения (2), а следовательно, и сравнения (1) есть

$$\mathrm{Ind}\ q \mid \delta; \tag{4}$$

при выполнении его сравнение (2) имеет δ решений—значений индекса x, по которым, помощью таблиц индексов, найдем δ решений данного сравнения (1).

Условие (4) можно заменить другим, ему эквивалентным. Положим

$$\mathrm{Ind}_g\ q = \gamma.$$

Тогда

$$q \equiv g^{\gamma}\ (Mod.\ p). \tag{5}$$

По условию $\gamma \mid \delta$ и значит

$$\gamma = \delta h.$$

Возводя две части сравнения (5) в степень $\frac{p-1}{\delta}$, имеем

$$q^{\frac{p-1}{\delta}} \equiv g^{\gamma \frac{p-1}{\delta}} = g^{h\delta \cdot \frac{p-1}{\delta}} = g^{h(p-1)} =$$
$$= (g^{p-1})^{h} \equiv 1^{h} = 1\ (Mod.\ p).$$

Итак, из условия (4) следует

$$q^{\frac{p-1}{\delta}} \equiv 1 \quad (Mod.\ p). \tag{6}$$

Покажем обратно, что из сравнения (6) следует условие (4). В самом деле из (6) следует

$$1 \equiv q^{\frac{p-1}{\delta}} \equiv (g^{\gamma})^{\frac{p-1}{\delta}} = g^{(p-1)\frac{\gamma}{\delta}}\ (Mod.\ p).$$

Но так как g—первообразный корень, то только степени его, кратные $p-1$ могут быть сравнимы с единицей, а потому необходимо $\frac{\gamma}{\delta}$ — целое число, т.-е. имеем условие (4).

Таким образом выполнение сравнения (6) есть необходимое и достаточное условие возможности сравнения (1)

или, что то же, условие того, что q есть n—ичный вычет по модулю p.

Необходимость этого условия была установлена выше (гл. VIII); теперь установлена и достаточность его.

Помощью индексов можно непосредственно решать и сравнения более общего вида

$$ax^n \equiv b \ (Mod.\ p).$$

Взяв индексы двух частей, имеем

$$\text{Ind } a + n \text{ Ind } x \equiv \text{Ind } b \ (Mod.\ p—1)$$

или

$$n \text{ Ind } x \equiv \text{Ind } b - \text{Ind } a \ (Mod.\ p—1).$$

Для Ind x опять получилось сравнение 1-й степени.

§ 4. Показательные сравнения.

Результаты §§ 1 и 2 позволяют рассмотреть один тип трансцендентных сравнений, а именно показательные сравнения, т.-е. сравнения вида

$$a^x \equiv A \ (Mod.\ p). \qquad (1)$$

Здесь предполагаем a и A не делящимися на p, а следовательно и взаимно-простыми с p. Случай a, делящегося на p, не представляет интереса; тогда необходимо и $A \mid p$, и сравнение (1) удовлетворяется для любого значения x).

Пусть a принадлежит к показателю δ по модулю p. Тогда ряд степеней

$$a^0,\ a^1,\ a^2,\ a^3,\ \ldots,\ a^{\delta-1} \qquad (2)$$

дает представителей различных классов, а другие степени a дают представителей тех же классов, что члены ряда (2). Таким образом мы получаем только δ классов, между тем как всех классов, не делящихся на p, всего p — 1. Таким образом, если только δ не равно p — 1, т.-е. если a не есть первообразный корень модуля p, сравнение (1) не всегда

возможно (δ, как делитель числа $p-1$, вообще, меньше $p-1$). Оно возможно, если A принадлежит к одному из δ классов имеющих представителями члены ряда (2). В таком случае для некоторого значения x_0, где x_0—одно из чисел ряда

$$0,\ 1,\ 2,\ \ldots,\ \delta-1, \tag{3}$$

имеем

$$a^{x_0} \equiv A \ (Mod.\ p). \tag{4}$$

Сопоставляя сравнения (1) и (4) мы на основании результатов § 1, заключаем

$$x \equiv x_0 \ (Mod.\ \delta) \tag{5}$$

или

$$x = x_0 + k\delta. \tag{6}$$

Заметим, что в формуле (6) содержится $\frac{p-1}{\delta}$ различных классов по модулю $p-1$; в самом деле давая k значения

$$k = 0,\ 1,\ 2,\ \ldots,\ \frac{p-1}{\delta} - 1, \tag{7}$$

мы получаем числа разных классов по модулю $p-1$; всякое другое значение k можно представить в виде

$$k = s \cdot \frac{p-1}{\delta} + r,$$

где r одно из чисел ряда (7), и следовательно

$$x = x_0 + s\ (p-1) + r\delta$$

или

$$x \equiv x_0 + r\delta \ \ (Mod.\ p-1),$$

т.-е. x по модулю $p-1$ сравнимо с одним из значений, получаемых подстановкой в формулу (6) значений k из ряда (7). Таким образом можно сказать, что сравнение (1), если оно возможно, имеет $\frac{p-1}{\delta}$ различных решений, считая за одно решение класс чисел по модулю $v-1$:

$$x \equiv x_0 + k\delta \ (Mod.\ p-1)$$
$$k = 0,\ 1,\ 2,\ \ldots,\ \frac{p-1}{\delta} - 1. \tag{8}$$

Заметим, что роль классов по модулю $p-1$ по отношению к показательному сравнению (1) очевидна: если x_0 есть число удовлетворяющее сравнению (1) и если

$$x \equiv x_0 \ (Mod.\ p-1),$$

то, очевидно, и x удовлетворяет сравнению, ибо

$$x = x_0 + k\ (p-1)$$

и

$$a^x = a^{x_0} \cdot a^{k(p-1)} = a^{x_0} \cdot (a^{p-1})^k \equiv a^{x_0} \cdot 1^k = a^{x_0}\ (Mod.\ p)$$

по теореме Фермата.

Те же результаты можно получить, применяя теорию индексов.

Взяв индексы двух частей сравнения (1), имеем:

$$x \cdot Ind\ a \equiv Ind\ A\ (Mod.\ p-1). \qquad (9)$$

Для определения x получили сравнение 1-й степени по модулю $p-1$.

Пусть

$$D\ (Ind\ a,\ p-1) = \omega. \qquad (10)$$

Тогда условие возможности сравнения (9), а следовательно и (1) есть

$$Ind\ A \mid \omega. \qquad (11)$$

При выполнении его сравнение (9), а следовательно, и данное, имеет ω решений.

Легко усмотреть согласие этого результата с прежним. Действительно, если a принадлежит к показателю δ, то

$$a^{\delta} \equiv 1\ (Mod.\ p).$$

Взяв индексы двух частей, имеем

$$\delta \cdot Ind\ a \equiv 0\ (Mod.\ p)$$

Сокращая на общего наибольшего делителя ω две части и модуль сравнения, имеем

$$\delta \cdot \frac{\operatorname{Ind} a}{\omega} \equiv 0 \left(Mod \cdot \frac{p-1}{\omega}\right)$$

или

$$\delta \cdot \frac{\operatorname{Ind} a}{\omega} \mid \frac{p-1}{\omega},$$

а так как частные $\frac{\operatorname{Ind} a}{\omega}$ и $\frac{p-1}{\omega}$ числа взаимно-простые, то

$$\delta \mid \frac{p-1}{\omega};$$

но т. к. δ должно быть наименьшим числом удовлетворяющим сравнению

$$a^{\delta} \equiv 1 \ (Mod \cdot p),$$

то, очевидно,

$$\delta = \frac{p-1}{\omega},$$

откуда

$$\omega = \frac{p-1}{\delta}.$$

В частном случае, когда $\delta = p-1$ и следовательно $\omega = 1$ сравнение (9), а значит и данное, всегда возможно; a в этом случае есть первообразный корень модуля p; сравнение имеет только одно решение, которое, очевидно, есть индекс A при основании a.

ГЛАВА ДЕСЯТАЯ.

Основы арифметики многочленов.

До сих пор все наши рассуждения имели место в области целых (положительных и отрицательных) чисел.

Рассмотрим теперь другую, более обширную область, элементами которой являются уже не числа, а всевозможные многочлены вида

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0, \qquad (1)$$

где $a_0, a_1, \ldots, a_m$ — целые числа. Легко видеть, что область целых чисел входит как составная часть в эту новую область, ибо многочлен нулевой степени нашей области—

$$f(x) = a_0$$

есть не что иное, как целое число.

Заметим, что в многочленах (1) нашей области x рассматриваем не как переменное, принимающее те или иные численные значения, а просто как некоторый символ, так что в сущности многочлен (1) является не чем иным, как совокупностью

$$a_0, a_1, \ldots a_m \qquad (2)$$

нескольких целых чисел—своих коэффициентов, и наша область есть область, элементы которой суть группы целых чисел, взятых в определенном порядке; порядок этот указывается степенями x^0, x, $x^2 \ldots$, при которых $a_0, a_1, a_2, \ldots$ находятся коэффициентами.

Два элемента области, т.-е. два многочлена будем считать равными только тогда, когда их коэффициенты соответственно равны и следовательно, между прочим, когда оба многочлена одной степени:

$$a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0 = b_m x^m + b_{m-1} x^{m-1} + \\ + \ldots + b_0,$$

если

$$a_0 = b_0,\ a_1 = b_1,\ \ldots,\ a_{m-1} = b_{m-1},\ a_m = b_m.$$

Правила действий в области многочленов устанавливаем по общим правилам алгебры. Так,

$$(a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m) + (b_0 + b_1 x + b_2 x^2 + \ldots + \\ + b_m x^m) = (a_0 + b_0) + (a_1 + b_1) x + (a_2 + b_2) x^2 + \ldots + \\ + (a_m + b_m) x^m$$

$$(a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m) \cdot (b_0 + b_1 x + b_2 x^2 + \ldots + \\ + b_n x^n) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \\ + \ldots + a_m b_n x^{m+n}$$

и т. д.

Легко видеть, что в области многочленов имеет место обычная арифметика. Можно в этой области исследовать вопросы о делимости и о разложении на простые факторы.

Многочлен $f(x)$ нашей области делится на многочлен $\varphi(x)$ той же области, если

$$f(x) = \varphi(x) \cdot \psi(x),$$

при чем и $\psi(x)$ — тоже элемент нашей области, т.-е. многочлен с целыми коэффициентами. Ясно, что степень делителя не выше степени данного многочлена. Старший коэффициент делителя должен нацело делить старший коэффициеент данного многочлена; то же самое имеет место и для младших коэффициентов; можно установить ограничения и для других коэффициентов делителя, и в результате оказывается, что конечным числом попыток можно найти всех делителей данного многочлена.

Очевидно, всякий многочлен $f(x)$ делится на ± 1 и на $\pm f(x)$. Если он не допускает других делителей, то его называем **неразложимым** или **простым**. Ясно, между прочим, что общий наибольший делитель всех коэффициентов неразложимого многочлена равен единице, т. к. если бы этот общий наибольший делитель был отличен от единицы, то он был бы делителем многочлена, который таким образом не был бы неразложимым.

Многочлен, общий наибольший делитель коэффициентов которого равен единице, называется вообще **первообразным многочленом**. Таким образом **неразложимый многочлен необходимо есть первообразный многочлен**.

Ясно, что делители первообразного многочлена сами суть первообразные многочлены.

Всякий многочлен $f(x)$ может быть представлен в виде

$$f(x) = D \cdot f_1(x),$$

где D — общий наибольший делитель коэффициентов, а $f_1(x)$ — первообразный многочлен.

Очевидно, что при разложении многочлена на простые множители можно ограничиться, в силу последнего замечания, случаем первообразного многочлена (разложение фактора D — вопрос исследованный).

Из всех делителей многочлена $f_1(x)$ можно выбрать делителя наинизшей степени; очевидно, он будет неразложимым многочленом, т. к., будучи первообразным, не может иметь делителей той же степени, а делители низшей степени невозможны, т. к. они были бы делителями $f_1(x)$ низшей степени, чем избранный нами делитель.

Таким образом доказано, что **всякий многочлен имеет неразложимого делителя**, а отсюда совершенно так же, как в арифметике целых чисел, следует разложимость всякого многочлена на простые (неразложимые) факторы.

Возможно доказать и единственность этого разложения, доказав теорему: **произведение двух многочленов**

делится на неразложимый многочлен только в том случае, если один из факторов на него делится.

В области чисел мы в свое время рассматривали совокупность чисел кратных одному данному числу. Такая совокупность обладала тем свойством, что сумма или разность двух чисел совокупности принадлежит той же совокупности, и мы называли ее модулем. В новой области можно сохранить то же определение модуля, как совокупности элементов области, т.-е. многочленов, и легко видеть, что совокупность многочленов, делящихся на данное число m, т.-е. многочленов вида $m\varphi(x)$, где $\varphi(x)$ — многочлен с целыми коэффициентами, есть модуль. Мы особенно часто будем рассматривать модуль вида

$$p \cdot \psi(x), \tag{3}$$

где p — первоначальное число.

Если разность двух элементов области, т.-е. двух многочленов $f_1(x)$ и $f_2(x)$ принадлежит к модулю (3), то мы скажем, что $f_1(x)$ и $f_2(x)$ сравнимы по модулю p:

$$f_1(x) \equiv f_2(x) \ (Mod.\ p), \tag{4}$$

если

$$f_1(x) - f_2(x) = p \cdot \psi(x). \tag{5}$$

Следует заметить, что сравнения типа (4) мы в свое время уже рассматривали в теории алгебраических сравнений высших степеней под названием „тождественных сравнений“ (гл. VI).

Там же было введено важное понятие о степени сравнения по модулю p, иначе говоря о степени многочлена по модулю p. Многочлен $f(x)$ имеет по модулю p степень равную n, если первый член, не делящийся на p, т.-е. с коэффициентом не делящимся на p, имеет степень n. Была также доказана теорема, что степень, по модулю p, произведения равна сумме степеней производителей. Возможно доказать еще следующую важную теорему:

Если

$$\varphi(x) \cdot \psi(x) \equiv 0 \ (Mod.\ p),$$

то-есть если

$$\varphi(x) \cdot \psi(x) = p \cdot \chi(x),$$

то необходимо
или

$$\varphi(x) \equiv 0 \ (Mod.\ p)$$

или

$$\psi(x) \equiv 0 \ (Mod.\ p),$$

т.-е. все коэффициенты или 1-го или 2-го многочлена делятся на p. Эта теорема вполне аналогична теореме элементарной арифметики: если произведение двух чисел делится на первоначальное число p, то необходимо или первый или второй фактор делится на p.

В области чисел мы рассматривали классы по модулю p; их оказалось конечное число, а именно p. Определим число классов по модулю p в области многочленов. Легко видеть что этих классов — бесконечное множество. В самом деле, два многочлена одного класса сравнимы по модулю p, а значит — одной и той же степени по модулю p (все коэффициенты двух многочленов, сравнимых по модулю p, в свою очередь сравнимы по модулю p). Значит многочлены различных степеней по модулю p необходимо принадлежат к различным классам. А так как степени можно брать сколь угодно высокие, то ясно, что и классов бесконечное множество.

Посмотрим, сколько классов многочленов данной степени m по модулю p. Многочлены эти рассматриваем в виде

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m,$$

при чем коэффициенты a_0, a_1, a_2, $\ldots$ a_m следует рассматривать по модулю p: при этом a_m может иметь одно из следующих значений $a_m = 1, 2, \ldots, p-1$ (при $a_m | p$ степень была бы меньше m), а все остальные a_i могут принимать значения 0, 1, 2, $\ldots$, $p-1$. Различных комбинаций значений

$a_0, a_1, a_2, \ldots a_{m-1}$, очевидно будет p^m; умножая на $(p-1)$— число значений a_m, получаем число классов многочленов степени m:

$$p^m(p-1).$$

В связи со сравнениями по модулю p можно рассмотреть интересную и важную классическую теорию делимости по модулю p.

Если

$$f(x) \equiv \varphi(x) \cdot \psi(x) \ (Mod.\ ), p \tag{6}$$

т.-е. если

$$f(x) = \varphi(x) \cdot \psi(x) + p \cdot \chi(x), \tag{7}$$

то говорим, что $\varphi(x)$ и $\psi(x)$ суть делители $f(x)$ по модулю p и обозначаем так:

$$\begin{aligned} f(x) &\mid \varphi(x) \ (Mod.\ p) \\ f(x) &\mid \psi(x) \ (Mod.\ p). \end{aligned} \tag{8}$$

Ясно, что степень делителя по модулю p не может превосходить степени данного многочлена $f(x)$.

Заметим, что любой многочлен $f(x)$ по модулю p делится на любое число α, не делящееся на p.

В самом деле пусть α' — союзное число для α, так что

$$\alpha\alpha' \equiv 1 \ (Mod.\ p)$$

В таком случае

$$f(x) \equiv \alpha\alpha' f(x) = \alpha \cdot [\alpha' f(x)] \ (Mod.\ p)$$

и значит

$$f(x) \mid \alpha \ (Mod.\ p).$$

Итак все числа, не делящиеся на p, представителями которых можно взять

$$1, 2, 3, \ldots, p-1, \tag{9}$$

делят любой элемент нашей области; с этой точки зрения числа ряда (9) являются действительно „единицами“ по модулю p.

Многочлен $f(x)$, в силу предыдущего, имеет делителей α и $\alpha' f(x)$; первый есть „единица“ по модулю p, второй — многочлен, не отличающийся существенно от $f(x)$ (отличается от $f(x)$ множителем α', который тоже есть единица по модулю p); эти делители назовем несобственными; степени их по модулю p равны нулю и степени данного многочлена.

Многочлен, который по модулю p имеет только несобственных делителей, называется неприводимым по модулю p или прим-многочленом или прим-функцией по модулю p.

Если имеем одновременно

$$f_1(x) \equiv \varphi(x) \cdot \psi_1(x) \ (Mod.\ p)$$
$$f_2(x) \equiv \varphi(x) \cdot \psi_2(x) \ (Mod.\ p),$$

то $\varphi(x)$ называем общим делителем $f_1(x)$ и $f_2(x)$ по модулю p.

Общий наибольший делитель по модулю p находится процессом, который представляет собою обобщение процесса Эвклида.

Пусть степени многочленов $f_1(x)$ и $f_2(x)$ по модулю p равны m_1 и m_2 и пусть $m_1 \geqq m_2$.

Возможно написать сравнение

$$f_1(x) \equiv f_2(x) \cdot q_1(x) + f_3(x) \ (Mod.\ p), \qquad (10)$$

при чем степень $f_3(x)$ $m_3 < m_2$.

В самом деле, пусть старший член $f_1(x)$ есть $a_1 x^{m_1}$, а старший член (по модулю p) $f_2(x)$ $a_2 x^{m_2}$, при чем a_1 и a_2 не делятся на p и значит

$$D(a_1, p) = D(a_2, p) = 1.$$

Можно подыскать такое число α_2, чтобы

$$a_2 \alpha_2 \equiv a_1 \ (Mod.\ p).$$

(Для определения α_2 имеем сравнение 1-й степени с коэффициентом взаимно-простым с модулем).

В таком случае

$$f_1(x) - f_2(x)a_2x^{m_1-m_2} \equiv \varphi(x) \ (Mod.\ p),$$

при чем степень $\varphi(x)$ по модулю p уже меньше m_1 и вообще равна m_1—1. Точно так же можем продолжать далее: если старший коэффициент $\varphi(x)$ есть b_1, то находим β_2 из сравнения

$$a_2\beta_2 \equiv b_1 \ (Mod.\ p)$$

и, в силу определения β_2, имеем

$$\varphi(x) - f_2(x)\beta_2x^{m_1-1-m_2} \equiv \psi(x) \ (Mod.\ p),$$

при чем $\psi(x)$ по модулю p уже низшей степени, чем $\varphi(x)$, а именно, вообще говоря, степени m_1—2. Этот процесс будем продолжать далее и далее, пока будут получаться многочлены $\varphi(x)$, $\psi(x)$, ... степеней не ниже степени m_2 многочлена $f_2(x)$; закончится он, когда получится, наконец, многочлен $f_3(x)$ степени $m_3 < m_2$. Таким образом получаем ряд сравнений

$$\begin{aligned}
f_1(x) &\equiv f_2(x) \cdot a_2 x^{m_1-m_2} + \varphi(x) \ (Mod.\ p)\\
\varphi(x) &\equiv f_2(x) \cdot \beta_2 x^{m_1-m_2-1} + \psi(x) \ (Mod.\ p)\\
\psi(x) &\equiv f_2(x) \cdot \gamma_2 x^{m_1-m_2-2} + \chi(x) \ (Mod.\ p)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\omega(x) &\equiv f_2(x) \cdot \pi_2 x^{m_1-m_2-i} + f_3(x) \ (Mod.\ p)
\end{aligned}$$

Складывая почленно все эти сравнения, получаем

$$f_1(x) \equiv f_2(x) \cdot q_1(x) + f_3(x) \ (Mod.\ p).$$

т.-е. сравнение (10), при чем

$$q_1(x) = \alpha_2 x^{m_1-m_2} + \beta_2 x^{m_1-m_2-1} + \ldots + \pi_2 x^{m_1-m_2-i}.$$

Аналогично поступая с $f_2(x)$ и $f_3(x)$, получим

$$f_2(x) \equiv f_3(x) \cdot q_2(x) + f_4(x) \ (Mod.\ p), \qquad (11)$$

при чем степень $f_4(x)$ ниже степени $f_3(x)$ (по модулю p).

Процесс можем продолжать все далее и далее, при чем степени (по модулю p) вновь получаемых многочленов $f_4(x)$, $f_5(x)$, ... все понижаются. Отсюда ясно, что процесс этот должен закончиться; но это будет только тогда, когда, в конце-концов, придем к многочлену $f_{k-1}(x)$, сравнимому с нулем по модулю p, и таким образом получим ряд сравнений:

$$\begin{aligned} f_1(x) &\equiv f_2(x) \cdot q_1(x) + f_3(x) \ (Mod.\ p) \\ f_2(x) &\equiv f_3(x) \cdot q_2(x) + f_4(x) \ (Mod.\ p) \\ f_3(x) &\equiv f_4(x) \cdot q_3(x) + f_5(x) \ (Mod.\ p) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (12) \\ f_{k-2}(x) &\equiv f_{k-1}(x) \cdot q_{k-2}(x) + f_k(x) \ (Mod.\ p) \\ f_{k-1}(x) &\equiv f_k(x) \cdot q_{k-1}(x) \ (Mod.\ p). \end{aligned}$$

Легко доказать, что последний из полученных многочленов („последний остаток“) $f_k(x)$ есть общий наибольший делитель по модулю p многочленов $f_1(x)$ и $f_2(x)$, при чем под общим наибольшим делителем двух или нескольких элементов области мы разумеем такой общий делитель, который делится на всех общих делителей этих элементов.

В самом деле, во-первых, последнее из сравнений (12) указывает, что

$$f_{k-1}(x) \mid f_k(x) \ (Mod.\ p).$$

Но в таком случае из предпоследнего легко следует

$$f_{k-2}(x) \mid f_k(x) \ (Mod.\ p)$$

и т. д. Наконец, из второго и 1-го получим, что $f_k(x)$ есть общий делитель по модулю p данных многочленов $f_1(x)$ и $f_2(x)$. Во-вторых, пусть $d(x)$ какой-нибудь общий делитель по модулю p многочленов $f_1(x)$ и $f_2(x)$. Тогда из 1-го из сравнений (12) легко заключаем, что

$$f_3(x) \mid d(x) \ (Mod.\ p)$$

Из 2-го сравнения затем легко следует

$$f_4(x) \mid d(x) \qquad (Mod.\ p)$$

и т. д. Наконец, из предпоследнего, имея уже

$$f_{k-2}(x) \mid d(x) \qquad (Mod.\ p)$$
$$f_{k-1}(x) \mid d(x) \qquad (Mod.\ p),$$

получаем

$$f_k(x) \mid d(x) \qquad (Mod.\ p).$$

Сопоставляя два полученных результата заключаем, что $f_k(x)$ есть общий наибольший делитель по модулю p многочленов $f_1(x)$ и $f_2(x)$. Заметим еще, что всякий делитель многочлена $f_k(x)$ есть общий делитель $f_1(x)$ и $f_2(x)$. Это следует из общей теоремы:

Если

$$f(x) \mid \varphi(x) \qquad (Mod.\ p)$$
$$\text{и } \varphi(x) \mid \psi(x) \qquad (Mod.\ p),$$
$$\text{то } f(x) \mid \psi(x) \qquad (Mod.\ p).$$

Доказывается эта теорема непосредственно: из условий ее имеем

$$f(x) = \varphi(x) \cdot \varphi_1(x) + p \cdot q(x)$$
$$\varphi(x) = \psi(x) \cdot \psi_1(x) + p \cdot s(x),$$

а отсюда

$$f(x) = \psi(x) \cdot \psi_1(x) \cdot \varphi_1(x) + p\,[s(x) \cdot \varphi_1(x) + q(x)],$$

т.-е.

$$f(x) \mid \psi(x) \qquad (Mod.\ p).$$

Из определения общего наибольшего делителя легко следует, что он (для данных элементов), единственный, в смысле сравнения по модулю p и до множителя, который есть единица по модулю p.

В самом деле пусть $d(x)$ и $\delta(x)$—два общих наибольших делителя по модулю p одних и тех же элементов. Тогда из определения следует одновременно

$$d(x) \mid \delta(x) \qquad (Mod.\ p)$$
$$\delta(x) \mid d(x) \qquad (Mod.\ p)$$

или иначе;

$$d(x) \equiv a \cdot \delta(x) \qquad (Mod.\ p)$$
$$\delta(x) \equiv b \cdot d(x) \qquad (Mod.\ p), \tag{13}$$

где a и b—два элемента области.

Из двух сравнений (13) следует

$$d(x) \equiv ab \cdot d(x) \qquad (Mod.\ p). \tag{14}$$

Т. к. две части должны быть одной степени по модулю p, то необходимо ab, а значит в отдельности a и b нулевой степени по модулю p, т.-е. числа, и далее очевидно

$$ab \equiv 1 \qquad (Mod.\ p),$$

откуда ясно, что a и b , по модулю p,—два союзных числа, не делящихся на p, т.-е. две единицы по модулю p.

Таким образом $d(x)$ и $\delta(x)$ по модулю p отличаются друг от друга только множителем, который есть единица по модулю p.

Обратно, конечно, очевидно, что если $d(x)$ есть общий наибольший делитель по модулю p нескольких элементов области, то этим же свойством обладает и

$$e \cdot d(x),$$

где e — любая единица по модулю p, т.-е. одно из чисел сравнимых с 1, 2, 3, ... , p—1.

Возвращаясь к сравнениям (12), мы из предпоследнего получаем

$$f_k(x) \equiv f_{k-2}(x) - q_{k-2}(x) \cdot f_{k-1}(x)\ (Mod.\ p).$$

Из предыдущего сравнения имеем

$$f_{k-1}(x) \equiv f_{k-3}(x) - q_{k-3}(x) \cdot f_{k-2}(x).\ (Mod.\ p)$$

Вставляя в только что полученное, приходим к результату

$$f_k(x) \equiv -q_{k-2}(x) \cdot f_{k-3}(x) + [1 + q_{k-2}(x)\ q_{k-3}(x)] \cdot f_{k-2}(x) \cdot$$
$$(Mod.\ p).$$

Таким образом $f_k(x)$ по модулю p линейно выражается через $f_{k-2}(x)$ и $f_{k-3}(x)$. Продолжая так же далее, т.-е. переходя в ряде сравнений (12) последовательно от каждого сравнения к предыдущему, в конце-концов выразим $f_k(x)$ линейно через данные многочлены $f_1(x)$ и $f_2(x)$. Изменяя обозначение для общего наибольшего делителя по модулю p и обозначая его через $d(x)$, имеем сравнение

$$d(x) \equiv f_1(x) \cdot s_1(x) + f_2(x) \cdot s_2(x) \ (Mod.\ p), \qquad (15)$$

которое вполне аналогично известному основному равенству в теории общего наибольшего делителя двух чисел.

Обратимся к частному случаю: пусть $d(x)$ есть единица по модулю p, т.-е.

$$d(x) \equiv e \ (Mod.\ p),$$

где $e = 1, 2, 3, \ldots, p-1$.

В таком случае говорят, что $f_1(x)$ и $f_2(x)$ взаимно-просты по модулю p. Сравнение (15) принимает здесь вид

$$f_1(x)\, s_1(x) + f_2(x).\, s_2(x) \equiv e \ (Mod.\ p). \qquad (16)$$

Умножая две части на число e' союзное e по модулю p и полагая

$$e' s_1(x) = X_1, \ e' s_2(x) = X_2,$$

имеем в другой форме

$$f_1(x).\, X_1 + f_2(x).\, X_2 \equiv 1 \ (Mod.\ p). \qquad (17)$$

Здесь $f_1(x)$ и $f_2(x)$ — два взаимно-простых по модулю p многочлена, X_1 и X_2—два многочлена области.

Умножим две части сравнения (17) на какой-либо многочлен $\varphi(x)$; получаем

$$f_1(x).\, \varphi(x).\, X_1 + f_2(x).\, \varphi(x).\, X_2 \equiv \varphi(x) \ (Mod.\ p) \ . \qquad (18)$$

Рассмотрим с одной стороны произведение $f_1(x) . \varphi(x)$ и с другой — многочлен $f_2(x)$. Из сравнения (18) непосредственно ясно, что всякий общий делитель по модулю p произведения $f_1(x)\ \varphi(x)$ и многочлена $f_2(x)$, взаимно-простого

по модулю p с $f_1(x)$, есть вместе с тем делитель $\varphi(x)$. Это следует из элементарных теорем о делимости произведения (кратное кратного) и суммы, которые, очевидно, имеют место и для делимости по модулю p.

В частности результат, конечно, верен и для общего наибольшего делителя по модулю p произведения $f_1(x)\varphi(x)$ и $f_2(x)$.

Пусть в частности

$$f_1(x)\varphi(x) \mid f_2(x) \ (Mod.\ p).$$

Тогда $f_2(x)$ есть общий (легко усмотреть, что и наибольший) делитель по модулю p $f_1(x)\varphi(x)$ и $f_2(x)$ и следовательно, по предыдущему:

$$\varphi(x) \mid f_2(x) \ (Mod.\ p).$$

Получилась теорема, аналогичная теореме элементарной арифметики: если произведение делится на элемент, взаимно-простой по модулю p, с одним из факторов, то на него делится по модулю p другой фактор.

Пусть теперь $f_1(x)$ и $f_2(x)$ попрежнему взаимно-просты по модулю p, но пусть кроме того и $\varphi(x)$ есть многочлен взаимно-простой с $f_2(x)$ по модулю p. Докажем, что в таком случае и произведение $f_1(x).\varphi(x)$ взаимно-просто по модулю p с $f_2(x)$. В самом деле, пусть общий наибольший делитель по модулю p произведения $f_1(x).\varphi(x)$ и многочлена $f_2(x)$ не есть единица по модулю p, а есть некоторый многочлен $d(x)$. Тогда по нашей основной теореме

$$\varphi(x) \mid d(x) \ (Mod.\ p)$$

и так как одновременно

$$f_2(x) \mid d(x) \ (Mod.\ p),$$

то приходим к противоречию с предположением о том, что $\varphi(x)$ и $f_2(x)$ взаимно-просты по модулю p, и следовательно доказано от противного, что произведение

$$f_1(x)\varphi(x)$$

взаимно-просто с $f_2(x)$.

Теорема эта вполне аналогична соответствующей теореме элементарной арифметики и, как и она, непосредственно распространяется на любое число факторов.

Рассмотрим теперь в качестве делителя неприводимый по модулю p многочлен или „прим-функцию“ $P(x)$. Одновременно рассмотрим какой-либо другой многочлен $f(x)$ и поставим вопрос, каков может быть общий наибольший делитель по модулю p многочленов $f(x)$ и $P(x)$.

Так как $P(x)$ имеет по определению только несобственных делителей, то мыслимы лишь два случая: или вышеупомянутый общий наибольший делитель есть единица по модулю p, или он существенно не отличается от $P(x)$, т.-е. сравним по модулю p с

$$e \,.\, P\,(x),$$

где e — единица по модулю p, и тогда, в силу общего замечания, сделанного выше, может быть заменен и непосредственно $P(x)$. В первом случае, $f\,(x)$ и $P\,(x)$ взаимно-просты по модулю p, во втором, очевидно, $f\,(x)$ по модулю p делится на $P(x)$.

Итак, произвольный многочлен по модулю p или делится на прим-функцию по этому модулю, или же взаимно-прост с ней. Теорема эта опять аналогична известной теореме элементарной арифметики.

Пусть теперь произведение

$$f_1(x) \,.\, f_2(x)$$

по модулю p делится на прим-функцию $P\,(x)$.

При этом $f_1\,(x)$, по предыдущему, или делится по модулю p на $P\,(x)$ или взаимно-прост с $P\,(x)$ по модулю p.

Во втором случае применяем теорему ранее доказанную относительно произведения и заключаем, что необходимо $f_2\,(x)$ по модулю p делится на $P\,(x)$.

Итак, если произведение двух факторов по модулю p делится на прим-функцию, то необходимо на нее делится один из факторов. Теорема эта вполне аналогична теореме элементарной арифметики о делимости произведения на

первоначальное число и совершенно так же, как и она, непосредственно распространяется на любое число факторов.

Имея все эти теоремы, можем приступить к разложению любого многочлена области на произведение прим-функций совершенно по тому же плану, как это делается в элементарной арифметике при разрешении вопроса о разложении числа на первоначальные множители.

Предварительно заметим, что конечным числом операций можно найти всех делителей по модулю p любого данного многочлена $f(x)$.

Действительно, во-первых, степень по модулю p делителя не выше таковой же степени делимого. Будем искать последовательно делителей 0-й, 1-й, 2-й, ... степеней до степени данного многочлена.

Между прочим очевидно, что делители 0-й степени всегда существуют и суть единицы по модулю p, а делители степени равной степени данного многочлена несущественно отличны от него, т.-е. сравнимы по модулю p с

$$e\, f(x),$$

где e — единица по модулю p.

Предположим теперь степень вообще равную μ. Так как мы рассматриваем многочлены по модулю p, то дело сводится к рассмотрению многочленов

$$a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_\mu x^\mu ,$$

где каждый из коэффициентов принимает лишь значения

$$0,\ 1,\ 2,\ \ldots,\ p-1,$$

а для a_μ исключено и значение 0.

Таковых многочленов конечное число и из них путем попыток отберем, если они есть, делителей по модулю p данного многочлена $f(x)$.

Найдя всех делителей по модулю p данного многочлена, выбираем из числа их делитель $P_1(x)$ наинизшей (не считая нулевой) степени.

Легко усмотреть, что $P_1(x)$ есть прим-функция по модулю p. В самом деле, если бы многочлен $P_1(x)$ таковой не был, то он имел бы по модулю p собственного делителя $d(x)$, степени ниже степени $P_1(x)$; но тогда бы многочлен $d(x)$ был делителем по модулю p данного многочлена $f(x)$ степени, противно предположению, ниже чем $P_1(x)$.

Итак, мы доказали, что всякий многочлен имеет по модулю p неприводимый делитель.

В силу этого

$$f(x) \equiv P_1(x) \cdot f_1(x) \ (Mod.\ p),$$

где $P_1(x)$ — прим-функция по модулю p.

Применяя этот же результат к $f_1(x)$, имеем

$$f_1(x) \equiv P_2(x) \cdot f_2(x) \ (Mod.\ p).$$

Продолжая также далее, имеем

$$f_2(x) \equiv P_3(x) \cdot f_3(x) \ (Mod.\ p)$$
$$f_3(x) \equiv P_4(x) \cdot f_4(x) \ (Mod.\ p)$$

и так далее, где $P_1(x)$, $P_2(x)$, $P_3(x)$, ... суть прим-функции по модулю p, и где степени по модулю p многочленов $f_1(x)$, $f_2(x)$, $f_3(x)$, ... очевидно уменьшаются.

Ввиду последнего обстоятельства процесс не может быть бесконечным и, значит, наконец, мы придем к многочлену $f_{k-1}(x)$, который сам есть прим-функция по модулю p. Обозначая его через $P_k(x)$, имеем

$$f_{k-2}(x) \equiv P_{k-1}(x) \cdot f_{k-1}(x) \equiv P_{k-1}(x) P_k(x) \ (Mod.\ p).$$

Вставляя $f_{k-2}(x)$ в предшествующее сравнение и восходя так далее и далее к началу, получим окончательно

$$f(x) \equiv P_1(x) P_2(x) \ \ldots . P_k(x) \ (Mod.\ p), \qquad (19)$$

т.-е. разложение $f(x)$ на произведение прим-функций по модулю p.

Этому разложению можно придать другой, более определенный вид. Для этой цели достаточно воспользоваться одним из результатов, данных в общей теории алгебраических сравнений высших степеней (гл. VI), в силу которого любой многочлен $\varphi(x)$ по модулю p представим в виде

$$\varphi(x) \equiv a_0 \cdot \Phi(x) \ (Mod.\ p),$$

где a_0—старший коэффициент, а $\Phi(x)$—многочлен со старшим коэффициентом $= 1$, так называемая „первообразная форма“ многочлена $\varphi(x)$. Доказывается это положение очень просто: если

$$\varphi(x) \equiv a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_m \ (Mod.\ p)$$

и если a_0' есть число союзное a_0 по модулю p, то очевидно

$$\varphi(x) \equiv a_0 \left[x^m + a_0' a_1 x^{m-1} + a_0' a_2 x^{m-2} + \ldots + a_0' a_m\right] \equiv$$

$$\equiv a_0 \Phi(x) \ (Mod.\ p).$$

Применяя это положение к каждой из прим-функций $P_1(x)$, $P_2(x) \ldots . P_k(x)$, получаем

$$f(x) \equiv a . P^{(1)}(x) . P^{(2)}(x) . P^{(3)}(x) \ldots . P^{(k)}(x) \ (Mod.\ p), \qquad (20)$$

где $P^{(1)}(x)$, $P^{(2)}(x), \ldots .$ — первообразные формы прим-функций (со старшим коэффициентом $= 1$), а a, как произведение старших коэффициентов $P_1(x)$, $P_2(x), \ldots .$, — единица по модулю p.

Докажем, что разложение (20) — единственное. Пусть одновременно

$$f(x) \equiv \beta . Q^{(1)}(x) . Q^{(2)}(x) \ldots . Q^{(l)}(x) \ (Mod.\ p). \qquad (21)$$

Сопоставляя (20) и (21), имеем

$$a P^{(1)}(x) P^{(2)}(x) \ldots P^{(k)}(x) \equiv \beta Q^{(1)}(x) Q^{(2)}(x) \ldots Q^{(l)}(x) \ (Mod.\ p). \qquad (22)$$

Левая, а следовательно и правая часть по модулю p делится на $P^{(1)}(x)$; но $P^{(1)}(x)$ — прим-функция, следовательно один из факторов правой части по модулю p делится на $P^{(1)}(x)$.

Пусть, например,

$$Q^{(1)}(x) \mid P^{(1)}(x) \ (Mod.\ p).$$

Но $Q^{(1)}(x)$ тоже прим-функция и собственных делителей иметь не может; значит $P^{(1)}(x)$ несущественно отлично от $Q^{(1)}(x)$, т.-е.

$$Q^{(1)}(x) \equiv \mu\, P^{(1)}(x) \ (Mod.\ p), \tag{23}$$

где μ — единица по модулю p. Так как старшие коэффициенты $Q^{(1)}(x)$ и $P^{(1)}(x)$ равны единице, то из сравнения (23) следует, очевидно, $\mu = 1$, и мы имеем

$$Q^{(1)}(x) \equiv P^{(1)}(x) \ (Mod.\ p). \tag{24}$$

Заменяя в сравнении (22) $Q^{(1)}(x)$ через $P^{(1)}(x)$ и перенося члены, имеем

$$P^{(1)}(x)\,[\alpha\, P^{(2)}(x) \ldots P^{(k)}(x) - \beta\, Q^{(2)}(x) \ldots Q^{(l)}(x)] \equiv 0 \ (Mod.\ p).$$

Левая часть должна делиться на p и т. к. первый фактор есть первообразная прим-функция по модулю p и, как таковая, не есть кратное p, то необходимо делится на p 2-й фактор, откуда

$$\alpha P^{(2)}(x) \cdot P^{(3)}(x) \ldots P^{(k)}(x) \equiv \beta\, Q^{(2)}(x)\, Q^{(3)}(x) \ldots Q^{(l)}(x) (Mod.\ p). \tag{25}$$

Поступая со сравнением (25) так же, как поступали с (22), получим

$$Q^{(2)}(x) \equiv P^{(2)}(x) \ (Mod.\ p)$$

Продолжая рассуждения, будем иметь

$$Q^{(3)}(x) \equiv P^{(3)}(x) \ (Mod.\ p)$$
$$Q^{(4)}(x) \equiv P^{(4)}(x) \ (Mod.\ p)$$
$$\ldots\ldots\ldots\ldots$$

При этом выясняется, что $k = l$, так как в противном случае в одной из частей сравнения (22) после ряда сокращений на $P^{(1)}(x)$, $P^{(2)}(x)$ и т. д. получили бы число, а в другой—произведение прим-функций и, следовательно, многочлен степени большей 0 по модулю p.

Итак ясно, что все $Q^{(j)}(x)$ совпадают по модулю p с $P^{(j)}(x)$ и, наконец, по сокращении, окончательно дополнительно следует

$$\alpha \equiv \beta \ (Mod.\ p).$$

Таким образом разложение (20) по модулю p — единственное, и мы видим, что в построенной нами теории делимости и разложения по модулю p имеют силу все законы элементарной арифметики.

Возвратимся к самому определению делимости по модулю p. Мы говорим, что $f(x)$ по модулю p делится на $\varphi(x)$, если имеет место равенство.

$$f(x) = \varphi(x).\ \psi(x) + p.\ \chi(x). \tag{26}$$

Рассмотрим при данных p и $\varphi(x)$ всевозможные многочлены $f(x)$, делящиеся на $\varphi(x)$ по модулю p. Совокупность их получим, понимая под $\psi(x)$ и $\chi(x)$ любые многочлены области. Легко видеть из формулы (26), что эта совокупность есть „модуль“, т.-е. что сумма и разность двух элементов совокупности принадлежат той же совокупности. Модуль этот определяется двумя элементами области — числом p и многочленом $\varphi(x)$; эти два элемента вместе называем модульной системой и говорим, что многочлен $f(x)$ сравним с нулем по модульной системе p, $\varphi(x)$, обозначая это следующим образом

$$f(x) \equiv 0 \ [Modd.\ p,\ \varphi(x)]. \tag{27}$$

Сравнение это, таким образом, вполне эквивалентно утверждению того факта, что $f(x)$ по модулю p делится на $\varphi(x)$; то и другое, в свою очередь, эквивалентно равенству (26).

Если имеем два многочлена $f_1(x)$ и $f_2(x)$, и их разность принадлежит к модулю $\varphi(x).\ \psi(x) + p.\ \chi(x)$ или иначе, если их разность по модулю p делится на $\varphi(x)$, то говорим, что $f_1(x)$ и $f_2(x)$ сравнимы по модульной системе p, $\varphi(x)$, и обозначаем это так:

$$f_1(x) \equiv f_2(x) \ [Modd.\ p,\ \varphi(x)]. \tag{28}$$

Мы видим таким образом, что теория делимости по модулю p приводит к теории сравнений по модульной системе $p, \varphi(x)$. Эта последняя есть лишь часть общей теории сравнений по модульным системам, о которой скажем несколько слов.

Возьмем несколько элементов $f_1(x), f_2(x), f_3(x), \ldots f_k(x)$ области.

Совокупность элементов вида

$$f(x) = \lambda_1(x) f_1(x) + \lambda_2(x) f_2(x) + \ldots + \lambda_k(x) f_k(x), \qquad (29)$$

где $\lambda_1(x), \lambda_2(x), \ldots \lambda_k(x)$ — произвольные элементы области, есть, очевидно, модуль, определяемый „модульной системой“ $f_1(x), f_2(x), \ldots f_k(x)$. Вместо равенства (29) пишем сравнение

$$f(x) \equiv 0 \ [Modd.\ f_1(x), f_2(x), \ldots, f_k(x)]. \qquad (30)$$

Вообще, если разность двух многочленов $f(x)$ и $g(x)$ принадлежит к модулю (29), то говорим, что $f(x)$ и $g(x)$ сравнимы по модульной системе $f_1(x), f_2(x), \ldots f_k(x)$, и обозначаем это так:

$$f(x) \equiv g(x) \ [Modd.\ f_1(x), f_2(x), \ldots f_k(x)]. \qquad (31)$$

Легко усмотреть, что для сравнений по модульной системе имеют место большинство основных свойств численных сравнений по численному модулю, установленных выше. Так, из определения ясно, что два равных многочлена сравнимы по любой модульной системе, что два многочлена, сравнимые с одним и тем же третьим, сравнимы между собою. Легко также доказать, что два сравнения по одной и той же модульной системе можно почленно складывать или вычитать и перемножать.

В самом деле, если одновременно

$$f(x) \equiv g(x) \ [Modd.\ f_1(x), f_2(x), \ldots f_k(x)]$$
$$\overline{f}(x) \equiv \overline{g}(x) \ [Modd.\ f_1(x), f_2(x), \ldots f_k(x)],$$

то это равносильно равенствам

$$f(x) = g(x) + \lambda_1(x) f_1(x) + \lambda_2(x) f_2(x) + \ldots + \lambda_k(x) f_k(x)$$
$$\overline{f}(x) = \overline{g}(x) + \mu_1(x) f_1(x) + \mu_2(x) f_2(x) + \ldots + \mu_k(x) f_k(x)$$

Складывая или вычитая и перемножая эти равенства почленно и перенося затем члены, мы получаем

$$f(x) \pm \overline{f}(x) - [g(x) \pm \overline{g}(x)] = \sum_{i=1}^{k} [\lambda_i(x) \pm \mu_i(x)] \cdot f_i(x)$$

$$f(x) \cdot \overline{f}(x) - g(x) \cdot \overline{g}(x) = \sum_{i=1}^{k} [g(x)\mu_i(x) + \overline{g}(x)\lambda_i(x)] \cdot f_i(x) +$$

$$+ \sum_{=1}^{k} \sum_{j=1}^{k} \lambda_i(x)\mu_j(x) \cdot f_i(x) \cdot f_i(x).$$

Правые части равенств линейно выражаются через $f_1(x)$, $f_2(x)$, ... $f_k(x)$, и это относится также к последней двойной сумме, которую можно расположить хотя бы по индексу j, при чем коэффициентами при $f_1(x), f_2(x), \ldots . f_k(x)$ в свою очередь будут суммы линейные относительно тех же функций. Принимая во внимание определение сравнений по модульной системе, отсюда непосредственно заключаем

$$f(x) \pm \overline{f}(x) \equiv g(x) \pm \overline{g}(x) \quad [Modd.\ f_1(x),\ f_2(x), \ldots . f_k(x)]$$

$$f(x) \cdot \overline{f}(x) \equiv g(x) \cdot \overline{g}(x) \quad [Modd.\ f_1(x),\ f_2(x), \ldots ,\ f_k(x)].$$

Оставляя дальнейшее развитие общей теории сравнений по модульным системам, разрешим вопрос, который возникает естественным образом: отчего мы не рассматривали модульные системы в области чисел? Вопрос этот легко разрешается простым замечанием, что всякая модульная система в области чисел эквивалентна обыкновенному модулю. В самом деле, пусть нам даны числа $m_1, m_2, \ldots . m_k$; совокупность чисел вида

$$\lambda_1 m_1 + \lambda_2 m_2 + \ldots . + \lambda_k m_k, \tag{32}$$

где λ_1, $\lambda_2, \ldots \lambda_k$ — любые целые числа, есть, очевидно, „модуль“ в смысле ранее установленном. Но в свое время было доказано, что всякий модуль в области целых чисел есть не что иное, как совокупность кратных наименьшего положительного числа модуля, так что совокупность чисел вида (32) эквивалентна совокупности

$$\lambda m, \tag{33}$$

где λ — произвольное целое число, а m — наименьшее положительное число совокупности (32). Отсюда, в свою очередь, вполне очевидно, что сравнение по модульной системе $m_1, m_2, \ldots m_k$ эквивалентно сравнению по модулю m.

Итак рассматривать модульные системы в области чисел совершенно излишне; совершенно иначе дело обстоит в области многочленов: там модульная система вообще говоря не эквивалентна одному модулю или, как иначе говорят, модульной системе 1-й ступени. Конечно, и в этой области следует поставить вопрос о возможном упрощении данной модульной системы, о сведении ее к наименьшему числу элементов или, иначе, к модульной системе наинизшей ступени. Ограничимся замечанием, что две модульные системы $[f_1(x), f_2(x), \ldots f_k(x)]$ и $[g_1(x), g_2(x), \ldots g_l(x)]$ называются эквивалентными, если каждый элемент первой принадлежит к модулю, определяемому второй, и обратно, т.-е. если все $f(x)$ линейно выражаются через $g(x)$ и обратно:

$$\begin{aligned} f_i(x) &= \lambda_{i1}(x) \cdot g_1(x) + \lambda_{i2}(x) \cdot g_2(x) + \ldots + \lambda_{il}(x) \cdot g_l(x) \\ g_j(x) &= \mu_{j1}(x) \cdot f_1(x) + \mu_{j2}(x) \cdot f_2(x) + \ldots + \mu_{jk}(x) \cdot f_k(x) \\ &(i = 1, 2, \ldots k;\ j = 1, 2, \ldots l) \end{aligned} \tag{34}$$

или иначе, если имеют место сравнения

$$\begin{aligned} f_i(x) &\equiv 0 \ [Modd.\ g_1(x), g_2(x), \ldots g_l(x)] \\ g_j(x) &\equiv 0 \ [Modd.\ f_1(x), f_2(x), \ldots f_k(x)] \end{aligned} \tag{35}$$

Из определения сравнений по модульной системе и из сравнений (35) непосредственно очевидно, что если какие-нибудь два элемента области сравнимы по 1-й модульной системе, то они сравнимы и по 2-й и обратно.

Возвращаемся к тому частному случаю модульной системы, с которого мы начали. Мы имели дело с модульной системой 2-й ступени, при чем один из элементов был многочлен нулевой степени, т.-е. целое число и в частности первоначальное число p; второй элемент, многочлен $\varphi(x)$, предполагаем, конечно, неделящимся на p. В этих пред-

положениях легко усмотреть, что система $[p, \varphi(x)]$ не может быть эквивалентна модульной системе первой ступени, т.-е. состоящей из одного элемента. В самом деле, т. к. на этот элемент m, между прочим должно делится p, ибо

$$p \equiv 0 \ (Mod.\ m),$$

то необходимо $m = p$, и тогда требование

$$\varphi(x) \equiv 0 \ (Mod.\ p)$$

приводит к противоречию с условиями.

Заметим, что многочлен $\varphi(x)$ можно заменить любым, сравнимым с ним по модулю p. Действительно, если $\Phi(x)$ такой многочлен, то модульные системы $[p, \varphi(x)]$ и $[p, \Phi(x)]$ эквивалентны, ибо имеем

$$\begin{aligned} p &= p \\ \Phi(x) &= \varphi(x) + p \,.\, \psi(x) \\ \varphi(x) &= \Phi(x) - p \,.\, \psi(x), \end{aligned}$$

а это частные случаи равенств (34).

В силу сделанного замечания мы вправе считать многочлен $\varphi(x)$ редуцированным по модулю p, т.-е. старший коэффициент его равным одному из чисел $1,2,3,\ldots, p-1$, а остальные — одному из чисел $0,1,2,3,\ldots, p-1$; степень $\varphi(x)$ по модулю p будем предполагать равной μ.

Рассмотрим число классов в нашей области по модульной системе $[p, \varphi(x)]$. Пусть $f(x)$ какой-либо элемент области. Выше, когда мы говорили об определении для двух многочленов общего наибольшего делителя по модулю p, мы применяли к ним обобщенный алгорифм Эвклида. Применяя первый шаг этого процесса к многочленам $f(x)$ и $\varphi(x)$, мы (см. выше), имеем

$$f(x) \equiv \varphi(x) \,.\, q(x) + r(x) \ (Mod.\ p), \qquad (36)$$

где степень по модулю p многочлена $r(x)$ ниже таковой же степени $\varphi(x)$, т.-е. меньше μ; в случае если бы степень (по

модулю p) $f(x)$ уже была бы меньше μ, следует лишь положить $q(x) = 0$, $r(x) = f(x)$. Из равенства (36) следует

$$f(x) \equiv r(x) \ [Modd.\ p, \varphi(x)], \tag{37}$$

при чем $r(x)$ имеет вид

$$r(x) \equiv a_0 + a_1 x + a_2 x^2 + \ldots + a_{\mu-1} x^{\mu-1} \ (Mod.\ p). \tag{38}$$

Ясно, что $r(x)$ определяется лишь по модулю p: если

$$\overline{r}(x) \equiv r(x) \ (Mod.\ p),$$

то очевидно и

$$\overline{r}(x) \equiv r(x) \ [Modd.\ p, \varphi(x)].$$

Все многочлены $f(x)$, сравнимые по модульной системе $(p, \varphi(x))$ с одним и тем же многочленом $r(x)$ вида (38), определенном по модулю p, принадлежат к одному классу. Остается в формуле (38) коэффициентам $a_0, a_1, \ldots, a_{\mu-1}$ давать всевозможные различные по модулю p значения, т.-е. 0, 1, 2, 3, . . . , $p-1$; так как для каждого из коэффициентов возможно p различных значений, то всех различных $r(x)$ получаем, очевидно, p^μ. Все эти $r(x)$ принадлежат уже к различным классам по модульной системе $[p, \varphi(x)]$.

Действительно, если бы мы имели для двух различных

$$r_1(x) \text{ и } r_2(x)$$
$$r_1(x) \equiv r_2(x) \ [Modd.\ p, \varphi(x)],$$

то это значило бы, что разность $r_1(x) - r_2(x)$ по модулю p делится на $\varphi(x)$, что невозможно, т. к. степень по модулю p этой разности, согласно предыдущему, ниже таковой же степени $\varphi(x)$. Итак, число классов по модульной системе $[p, \varphi(x)]$ конечно и равно p^μ, где μ — степень $\varphi(x)$ по модулю p.

Обращаемся к рассмотрению специального случая модульной системы, когда второй элемент ее есть прим-функция по модулю p. Будем обозначать такую модульную систему.

$$[p, P(x)];$$

степень по модулю p прим-функции $P(x)$ будем предполагать равной m. Согласно предыдущему число классов по этой системе равно p^m. Из этих классов есть только один класс многочленов, делящихся по модулю p на $P(x)$, — это класс, характеризуемый выбором

$$r(x) \equiv 0 \ (Mod.\ p),$$

ибо для этого класса

$$f(x) \equiv 0 \ [Modd.\ p, P(x)],$$

и это сравнение, как было своевременно замечено, эквивалентно требованию

$$f(x) \mid P(x) \ (Mod.\ p).$$

Так как всякий элемент области, не делящийся на прим-функцию по модулю p, как мы видели, взаимно-прост с этой прим-функцией, то, значит, остальные $p^m - 1$ классов состоят из многочленов, взаимно-простых с $P(x)$ по модулю p.

Вообще можно заметить, что все элементы одного класса по модульной системе $(p, \varphi(x))$ имеют одних и тех же общих делителей с $\varphi(x)$ по модулю p.

В самом деле, если

$$f(x) \equiv g(x) \ [Modd.\ p, \varphi(x)],$$

т.-е.

$$f(x) - g(x) = p \cdot \psi(x) + \varphi(x) \cdot s(x)$$

и если одновременно

$$g(x) \mid d(x) \ (Mod.\ p)$$

и

$$\varphi(x) \mid d(x) \ (Mod.\ p),$$

т.-е.

$$g(x) = d(x) \cdot a(x) + p \cdot q(x)$$
$$\varphi(x) = d(x) \cdot b(x) + p \cdot t(x),$$

то

$$f(x) = d(x)\,[a(x) + b(x)\,s(x)] + p\,.\,[\psi(x) + q(x) + s(x)\,t(x)],$$

т.-е.

$$f(x) \mid d(x)\ (Mod.\ p),$$

и точно так же ясно, что если $d(x)$ есть по модулю p общий делитель $\varphi(x)$ и $f(x)$, то и

$$g(x) \mid d(x)\ (Mod.\ p).$$

Возвращаясь к модульной системе $(p, P(x))$, докажем по отношению к ней теорему Ферма та.

Пусть $p^m - 1 = \nu$ и пусть

$$f_1(x), f_2(x), \ldots f_\nu(x) \qquad (39)$$

представители классов взаимно-простых с $P(x)$ по модулю p. Пусть $f(x)$ также многочлен взаимно-простой с $P(x)$ по модулю p.

Произведения

$$f(x)\,.\,f_1(x), f(x)\,.\,f_2(x), \ldots f(x)\,.\,f_\nu(x), \qquad (40)$$

по одной из вышедоказанных теорем, все—взаимно-простые с $P(x)$ по модулю p.

При этом все они различных классов по модульной системе $[p, P(x)]$. В самом деле, если бы имели

$$f(x)\,.\,f_i(x) \equiv f(x)\,.\,f_j(x)\ [Modd.\ p, P(x)],$$

или иначе

$$f(x)\,.\,[f_i(x) - f_j(x)] \equiv 0\ [Modd.\ p, P(x)],$$

то это означало бы, что левая часть по модулю p делится на прим-функцию $P(x)$, а так как $f(x)$ многочлен взаимно-простой с $P(x)$ по модулю p, то мы бы имели

$$[f_i(x) - f_j(x)] \mid P(x)\ (M\ d.\ p)$$

или

$$f_i(x) \equiv f_j(x)\ [Modd.\ p, P(x)],$$

что невозможно, так как $f_i(x)$ и $f_j(x)$—представители различных классов.

Таким образом ряд (40) элементов области, как и ряд (39), представляет собою „приведенную систему вычетов“, т. - е. систему представителей классов, взаимно-простых с $P(x)$ по модулю p, и следовательно каждый из элементов ряда (40) сравним с одним и только одним из элементов ряда (39), а произведение всех элементов ряда (40) сравнимо с произведением элементов ряда (39). Выполняя эти перемножения, получаем

$$f^{\nu}(x) \cdot f_1(x) f_2(x) \dots f_{\nu}(x) \equiv f_1(x) f_2(x) \dots f_{\nu}(x) \quad [Modd.\ p, P(x)]$$

или

$$[f^{\nu}(x) - 1] \cdot f_1(x) f_2(x) \dots f_{\nu}(x) \equiv 0 \quad [Modd.\ p, P(x)]$$

В силу последнего сравнения произведение, стоящее в левой части, делится на прим-функцию $P(x)$ по модулю p. Второй фактор, т. - е. $f_1(x) f_2(x) \dots f_{\nu}(x)$, взаимно-прост с $P(x)$ по молулю p; следовательно первый делится на $P(x)$ по модулю p или иначе

$$f^{\nu}(x) - 1 \equiv 0 \quad [Modd.\ p, P(x)]$$

или окончательно

$$f^{p^m - 1}(x) \equiv 1 \quad [Modd.\ p, P(x)] \tag{41}$$

для любого многочлена $f(x)$, не делящегося на $P(x)$ по модулю p.

Умножив обе части на $f(x)$, получаем теорему Ферма в виде

$$f^{p^m}(x) \equiv f(x) \quad [Modd.\ p, P(x)], \tag{42}$$

при чем это сравнение справедливо и для $f(x)$, делящегося на $P(x)$ по модулю p.

Обращаемся теперь к рассмотрению решения в нашей области алгебраических сравнениий с одним неизвестным.

Неизвестное будем обозначать через X, так как x у нас уже имеет другое значение. Общий вид алгебраического сравнения с одним неизвестным

$$F(X) = A_0 X^\mu + A_1 X^{\mu-1} + A_2 X^{\mu-2} + \ldots + A_\mu \equiv \equiv 0\,[Modd.\, p, P(x)], \qquad (43)$$

при чем $A_0, A_1, \ldots A_\mu$—элементы области, т.-е. многочлены относительно x.

Если сравнению (43) удовлетворяет какое-нибудь значение X в нашей области, т.-е. какой-нибудь многочлен относительно x, то, в силу основных свойств сравнений, удовлетворяет и любое другое значение, сравнимое с первым по данной модульной системе. Таким образом решением является весь класс элементов области по данной модульной системе, и мы так и будем считать число решений сравнений, принимая за одно решение целый класс элементов, одновременно удовлетворяющих сравнению.

Рассмотрим в частности сравнение

$$X^{p^m} \equiv X\ [Modd.\ p, P(x)]. \qquad (44)$$

Согласно теореме Фермата ему удовлетворяют всевозможные элементы области; различными решениями являются p^m классов, на которые распределяются элементы области по данной модульной системе, в том числе и класс элементов делящихся на $P(x)$ по модулю p или, что то же, сравнимых с нулем по данной модульной системе. Число решений сравнения (44) таким образом равно его степени.

Докажем вообще, что число решений сравнения (43) не может превышать его степени μ, если только не все коэффициенты $A_0, A_1, \ldots A_\mu$ сравнимы с нулем по данной модульной системе (в этом случае сравнение обращается в тождественное), или иначе, если не все коэффициенты делятся на $P(x)$ по модулю p.

Предположим, что теорема верна для сравнений (μ—1-й) степени и докажем, что она имеет место и для μ-й степени.

Допустим, что число решений сравнения (43) больше μ и пусть

$$X_1, X_2, \ldots, X_\mu, X_{\mu+1}$$

$\mu+1$ из его решений.

Составим произведение

$$G(X) = A_0 (X - X_1)(X - X_2) \ldots (X - X_\mu)$$

и рассмотрим сравнение

$$F(X) - G(X) \equiv 0 \ [Modd.\ p, P(x)]. \qquad (45)$$

Ему, очевидно, удовлетворяют

$$X_1, X_2, \ldots X_\mu,$$

а степень его равна $\mu - 1$ и следовательно меньше числа решений. Согласно предположению, к нему можем применить доказываемую теорему и вывести из нее, что все коэффициенты левой части (45) сравнимы с нулем по данной модульной системе и, значит, сравнение имеет место для любого значения X. Положим в частности

$$X = X_{\mu+1}$$

Получаем

$$F(X_{\mu+1}) - G(X_{\mu+1}) \equiv 0 \ [Modd.\ p, P(x)]$$

или, так как $X_{\mu+1}$ есть решение сравнения (43),

$$G(X_{\mu+1}) \equiv 0 \ [Modd.\ p, P(x)].$$

Последний результат можно представить в таком виде: $G(X_{\mu+1}) = A_0 (X_{\mu+1} - X_1)(X_{\mu+1} - X_2) \ldots (X_{\mu+1} - X_\mu) \mid P(x) \ (Mod.\ p)$. Сравнение (43) мы предполагали степени равной μ; поэтому A_0 не сравнимо с нулем по данной модульной системе, т.-е. не делится на $P(x)$ по модулю p и значит взаимно-просто с $P(x)$ по модулю p. Поэтому необходимо делится на $P(x)$ по модулю p произведение остальных факторов, а следовательно, в силу одной из доказанных ранее теорем, один

из этих факторов, т.-е. мы должны для одного из значений $i = 1, 2, \ldots . \mu$ иметь

$$X_{\mu+1} - X_i \mid P(x) \ (Mod.\ p)$$

или

$$X_{\mu+1} \equiv X_i \quad [Modd.\ p,\ P(x)],$$

что противно предположению, в силу которого $X_{\mu+1}$ и X_i — различные решения сравнения (43).

Итак, если теорема верна для $\mu - 1$, то верна и для μ. Покажем, что она верна для сравнений 1-й степени, и тогда в силу принципа математической индукции непосредственно станет ясным, что теорема справедлива вообще.

Пусть сравнение 1-й степени

$$A_0 X + A_1 \equiv 0 \ [Modd.\ p,\ P(x)]$$

имеет два различных решения X_1 и X_2.

Вставляя их, имеем,

$$A_0 X_1 + A_1 \equiv 0 \ [Modd.\ p,\ P(x)]$$
$$A_0 X_2 + A_1 \equiv 0 \ [Modd.\ p,\ P(x)]$$

Вычитая, получаем

$$A_0 (X_1 - X_2) \equiv 0 \ [Modd.\ p,\ P(x)]$$

или иначе

$$A_0 (X_1 - X_2) \mid P(x) \ (Mod.\ p).$$

Разность $X_1 - X_2$ различных решений не сравнима с нулем по модульной системе, иначе говоря не делится на $P(x)$ по модулю p, следовательно необходимо

$$A_0 \mid P(x) \ (Mod.\ p)$$

или

$$A_0 \equiv 0 \ [Mod.\ p,\ P(x)]$$

противно допущению, что мы имеем сравнение 1-й степени.

Итак теорема вполне доказана. Применим ее к выводу в нашей области теоремы Вильсона.

Рассмотрим сравнение

$$X^{m-1} - 1 \equiv 0 \ [Modd.\ p,\ P(x)].$$

По теореме Фермата оно имеет $p^m - 1$ решений

$$f_1(x),\ f_2(x),\ \ldots\ f_{p^m-1}(x) \qquad (46)$$

представителей всех классов, не сравнимых с нулем по данной модульной системе. Сравнению

$$X^{p^m-1} - 1 - [X - f_1(x)]\,[X - f_2(x)]\ \ldots\ [X - f_{p^m-1}(x \equiv 0, \qquad (47)$$

очевидно, удовлетворяют все $p^m - 1$ решения (46); между тем степень его, очевидно, меньше $p^m - 1$, а потому все коэффициенты левой части должны быть сравнимы с нулем по данной модульной системе; сравнение должно иметь место тождественно. Мы в праве поэтому положить в нем $X = 0$, и в результате получаем

$$f_1(x)\,f_2(x)\ldots f_{p^m-1}(x).(-1)^{p^m-1} \equiv 1\ [Modd.\ p, P(x)]$$

или, так как p, а значит и p^m нечетное число, то в окончательном виде:

$$f_1(x)\,f_2(x)\ldots\ f_{p^m-1}(x) \equiv -1\ [Modd.\ p,\ P(x)]. \qquad (48)$$

Здесь $f_1(x), f_2(x), \ldots f_{p^m-1}(x)$ — представители всех классов, не сравнимых с нулем по модульной системе, подобно тому, как в классической теореме Вильсона

$$1.2.3\ldots(p-1) \equiv -1\ (Mod.\ p)$$

1, 2, 3, ..., $p - 1$ — представители всех классов, не делящихся на модуль p.

Теорию сравнений по модульной системе $[p, P(x)]$ можно бы развивать и далее.

Равным образом можно бы извлечь целый ряд следствий из полученных до сих пор результатов. Оставляя все это в стороне, ограничимся одним замечанием.

В силу доказанной нами теоремы Фермата сравнению

$$X^{p^m} - X \equiv 0\ [Modd.\ p,\ P(x)]$$

удовлетворяет любой элемент области. Поэтому, между прочим, мы в праве положить

$$X = x.$$

В результате получаем

$$x^{p^m} - x \equiv 0 \ [Modd.\ p, P(x)]$$

или

$$^{p^m}- x \mid P(x) \ (Mod.\ p)$$

Таким образом прим-функция степени m по модулю p есть необходимо делитель по модулю p разности

$$x^{p^m} - x.$$

Это замечание может служить исходным пунктом для построения прим-функций данной степени и для пополнения, таким образом, ранее развитой теории делимости по модулю p.

Оглавление.

ГЛАВА ПЯТАЯ.

ГЛАВА ШЕСТАЯ.

Алгебраические сравнения высших степеней:

ГЛАВА СЕДЬМАЯ.

Сравнения второй степени:

ГЛАВА ВОСЬМАЯ.

ГЛАВА ДЕВЯТАЯ.

Степенные вычеты и указатели:

ГЛАВА ДЕСЯТАЯ.

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО.
ГЛАВНОЕ УПРАВЛЕНИЕ ✿ МОСКВА.

Руководства и учебники для высшей школы.

МАТЕМАТИКА и АСТРОНОМИЯ.

АДАМОВ, А. А.—Задачник по высшей алгебре. Изд. 1922 г. Стр. 234.

ГРЭНВИЛЬ, В. — Элементы дифференций и интегрального исчисления. Вып. I. — Дифференциальное исчисление. Изд. 2-е 1922 г., проредактир. и дополн. Н. Н. Лузиным. Стр. 288.

ИВАНОВ, А. А. — Введение в астрономию. С 91 рис. и 7 табл. Изд. 1922 г. Стр. 191.

ЛАХТИН, К. Л. — Кривые распределения и построение для них интерполяционных формул по способам Пирсона и Брукса. Изд. 1922 г. Стр. 151.

МЛОДЗЕЕВСКИЙ, В. К. — Основы высшей алгебры. Изд. 1922 г. Стр. 112. — Основы аналитической геометрии в пространстве. Изд. 4-е 1922 г. Стр. 151.

ПОПРУЖЕНКО, М.—Начала анализа. С 45 черт. Изд. 1922 г. Стр. 125.

ФИЗИКА и ХИМИЯ.

БЕРКЕНГЕЙМ, А. М.—Основы теоретической химии. (Современные воззрения на строение материи). Изд. 3-е, вновь переработ. и дополн. 1922 г. Стр. 358. С 43 рис. и табл.

ГЕЛЬМГОЛЬЦ, Г.—О сохранении силы (физическое исследование). Перевод и примечания Н. Лазарева. Изд. 1922 г. Стр. 71. (Серия „Классики Естествознания", № 5).

ГЕОРГИЕВИЧ, Г. и ГРАНМУЛЕН, Е. — Химия красящих веществ. Под ред. и с доп. В. В Тарвина. Изд. 3-е 1922 г. Стр. 612.

КАБЛУКОВ. — Основные начала физической химии. Вып. II. Электрохимия, с 44 рис. Изд. 2-е испр. и доп. 1922 г. Стр. 307.

ЛЕБЕДЕВ, П. Н. — Давление света. Под ред. Н. Лазарева и П. Кравца. С 25 фигур. Изд. 1922 г. Стр. 91. (Серия „Классики Естествознания", № 4).

РЕЙХЕ, Ф. и ЭПШТЕЙН, П.— Теория квантов. Изд. 1922 г. Стр. 89.

РЕФОРМАТСКИЙ, А. — Неорганическая химия. С 7 портр. и 263 рис. Изд. 11-е. Стр. 370.

СМИТ, А. — Введение в химию. Руководство к практическим занятиям. Изд. 1922 г. Берлин. Стр. 185.

УОКЕР, Д.— Введение в физическую химию. С предисловием академика П. И. Вальдена. Изд. 2-е, исправл. и просмотренное Н. А. Шиловым. 1923 г. Петроград. Стр. 350.

ФАЯНС, Н.— Радиоактивность и современное учение о химических элементах. Перевод и дополн. Э. В. Шпольского. С 12 рис. и 10 табл. Изд. 1922 г. Стр. 121. (Серия „Современные проблемы Естествознания", № 1).

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ГЛАВНОЕ УПРАВЛЕНИЕ ❁ МОСКВА.

ШАРВИН, В. В. — Введение в химию. Краткий курс неорганической химии. С 73 рис. Изд. 3-е 1922 г. Стр. 416.

ЕСТЕСТВОЗНАНИЕ.

БЕРГ.—Климат и жизнь. Изд. 1922 г. Стр. 196.

ЗАВОДОВСКИЙ, Н. — Пол и развитие его признаков. К анализу формообразования. С 20 табл. в красках и 126 фигурами в тексте. Изд. 1922 г. Стр. 255.

ЛУЧИЦКИЙ, В. И.—Курс петрографии. Изд. 2-е доп. и испр. Стр. 341.

НИКИТИНСКИЙ, Я. Я. — Практические занятия по микробиологии. Изд. 1922 г. Стр. 92.

НЕЧАЕВ, А. В. — Минералогия. Под ред. А. Д. Архангельского. С таблицей. Изд. 3-е просмотр. 1922 г. Стр. 338.

ОГ, Э. — Геология, т. I. Геологические явления. Под ред. А. П. Павлова. С фигурами и рисунками. Изд. 2-е. Стр. 496.

РЁЗЕРФОРД. — Строение атома и искусственное разложение элементов. Подготовил к печати Э. В. Шпольский. Стр. 177. (Серия „Современные проблемы естествознания", № 3).

РЕФОРМАТСКИЙ, С. Н. — Начальный курс органической химии. Изд. 14-е. 1922 г. Берлин. Стр. 285.

СЕВЕРНОВ, А. Н. — Этюды из теории эволюции. Индивидуальное развитие и эволюция. Изд. 1922 г. Берлин. Стр. 310.

СМОРОДИНЦЕВ, И. А.—Ферменты растительн. и животн. царства. Ч. I.—Общая ферментология. С 26 рис. Изд. 1922 г. Стр. 340.

Его же. Ч. II.—Частная ферментология. С включением методики исследования. С 6-ю рис. в тексте. Изд. 1922 г. Стр. 261.

ФУНК, К. Ф. — Витамины. Их значения для физиологии и патологии. С 38 рис. в тексте и 2-мя табл. Под ред. и с пред. Н. Д. Зелинского. Стр. 190.

ЯКОВЛЕВ, Н. Н.—Учебник палеонтологии. С 823 фигур. в тексте. Изд. 2-е, изменен. и дополнен. 1922 г. Петроград. Стр. 447.

ТОРГОВЫЙ СЕКТОР ГОСУДАРСТВЕННОГО ИЗДАТЕЛЬСТВА:

Москва, Ильинка, Биржевая площадь, уг. Богоявленского пер., № 4.
Телефоны: 1-57-57, 47-35.

РОЗНИЧНАЯ ПРОДАЖА:

1) Советская площадь (под гостиницей „Дрезден").
2) Моховая, 17.
3) Б. Никитская, 13 (рядом с консерваторией).
4) Никольская, 3.