

Б.А. Венков

**Элементарная теория
чисел**

Книга 4

**Москва
«Книга по Требованию»**

УДК 93
ББК 63.3
Б11

Б.А. Венков
Б11 Элементарная теория чисел: Книга 4 / Б.А. Венков – М.: Книга по Требованию, 2023. – 219 с.

ISBN 978-5-458-24166-3

Заглавие «Элементарная теория чисел», данное настоящему реферату, не вполне отражает ту точку зрения, которая была принята при его составлении. В нем собрано все то из классической теории чисел и новых исследований, что осуществляется чисто арифметическим методом (т.е. без введения понятий анализа, геометрии, иррациональных и комплексных чисел). Этот материал удовлетворяет большей частью и требованию «элементарности» в обычном смысле этого слова. Иррациональные числа появляются лишь там, где они необходимы по самому существу дела (глава II и некоторые параграфы главы IV). Такая точка зрения принята потому, что алгебраические, геометрические и аналитические методы в теории чисел служат предметом особых рефератов этой серии

ISBN 978-5-458-24166-3

© Издание на русском языке, оформление
«YOYO Media», 2023

© Издание на русском языке, оцифровка,
«Книга по Требованию», 2023

Эта книга является репринтом оригинала, который мы создали специально для Вас, используя запатентованные технологии производства репринтных книг и печати по требованию.

Сначала мы отсканировали каждую страницу оригинала этой редкой книги на профессиональном оборудовании. Затем с помощью специально разработанных программ мы произвели очистку изображения от пятен, клякс, перегибов и попытались отбелить и выровнять каждую страницу книги. К сожалению, некоторые страницы нельзя вернуть в изначальное состояние, и если их было трудно читать в оригинале, то даже при цифровой реставрации их невозможно улучшить.

Разумеется, автоматизированная программная обработка репринтных книг – не самое лучшее решение для восстановления текста в его первоизданном виде, однако, наша цель – вернуть читателю точную копию книги, которой может быть несколько веков.

Поэтому мы предупреждаем о возможных погрешностях восстановленного репринтного издания. В издании могут отсутствовать одна или несколько страниц текста, могут встретиться невыводимые пятна и кляксы, надписи на полях или подчеркивания в тексте, нечитаемые фрагменты текста или загибы страниц. Покупать или не покупать подобные издания – решать Вам, мы же делаем все возможное, чтобы редкие и ценные книги, еще недавно утраченные и несправедливо забытые, вновь стали доступными для всех читателей.



Серия Книжный Ренессанс

www.samizday.ru/reprint

ОГЛАВЛЕНИЕ

Глава I

	Стр.
Основные понятия теории чисел	
§ 1. Разложение чисел на простые множители; алгоритм Евклида	9
§ 2. Простейшие арифметические функции	10
§ 3. Теоремы о делимости факториалов	12
§ 4. Теоремы Эйлера и Ферма; сравнения первой степени	—
§ 5. Теоремы Лагранжа и Вильсона	14
§ 6. Первообразные корни, индексы, двучленные сравнения	15
§ 7. Числа Бернулли	18
§ 8. Квадратичные вычеты; третье гауссово доказательство закона взаимности	20
§ 9. Квадратичный характер по составному модулю	23
§ 10. Обобщения сравнений	25
<i>Примечания к главе I</i>	28

Глава II

Непрерывные дроби и диофантовы приближения

§ 1. Ряды Фарея	33
§ 2. Принцип Дирихле; теоремы Кронекера и Минковского	35
§ 3. Теорема Эрмита	37
§ 4. Непрерывные дроби; перечисление свойств подходящих дробей	39
§ 5. Критерий Лежандра; теоремы Валена и Бореля	42
§ 6. Эквивалентные числа	44
§ 7. Относительные минимумы формы $x - \omega y$	47
§ 8. Арифметические приложения неравенства Дирихле	48
§ 9. Симметрические непрерывные дроби	55
§ 10. Разложение квадратных иррациональностей в непрерывную дробь	56
§ 11. Союзные числа	59
§ 12. Уравнение Пелля	61
§ 13. Вопрос Ивана Бернулли	63
<i>Примечания к главе II</i>	66

Глава III

Степенные вычеты

§ 1. Первое гауссово доказательство квадратичного закона взаимности	69
§ 2. Распределение степенных вычетов в прогрессии	72
§ 3. Биквадратичные вычеты; критерии принадлежности чисел к классам биквадратичного распределения	79
§ 4. Кубические вычеты; метод Гаусса	85
§ 5. Теорема о вычете числа a в разложении $p = a^2 + 4b^2$	89
<i>Примечания к главе III</i>	90

Глава IV

	Стр.
Гауссова теория квадратичных форм	
§ 1. О представлении целого числа бинарной квадратичной формой . . .	93
§ 2. Преобразование бинарной формы в себя	95
§ 3. Приведение форм отрицательного определителя	97
§ 4. Формы положительного определителя	98
§ 5. Периоды целочисленных форм	103
§ 6. Формы с определителем, равным квадрату	106
§ 7. Решение общего уравнения второй степени с двумя неизвестными .	108
§ 8. Порядки форм; представление чисел полной системой неэквивалентных форм данного порядка	109
§ 9. Формы и классы апсеров; некоторые специальные исследования о периодах неопределенных форм	111
§ 10. Композиция бинарных форм	116
§ 11. Сравнение чисел классов для определителей, отличающихся на квадрат	122
§ 12. Распределение бинарных форм на роды	127
§ 13. Тройничные формы, конечность числа классов, основные задачи теории	132
§ 14. Представление чисел и бинарных форм тройничными формами . . .	138
§ 15. Приложение к бинарным формам, теорема Редея	145
§ 16. Разложение чисел и бинарных форм на сумму трех квадратов . . .	147
<i>Примечания к главе IV</i>	153

Глава V

Разбиение чисел на слагаемые и методы Лиувилля

§ 1. Точечные диаграммы, теорема Эйлера-Лежандра	156
§ 2. Двойные разбиения, рекуррентные соотношения для аддитивных функций	162
§ 3. Теорема Раманужана	166
§ 4. Методы Лиувилля; вывод основных тождеств	168
§ 5. О представлении чисел формами с двумя, тремя и четырьмя переменными	176
§ 6. Количество представлений чисел суммой 2, 4, 6, 8 и 10 квадратов	183
<i>Примечания к главе V</i>	190

Глава VI

Число классов бинарных квадратичных форм

§ 1. Табличные сведения о числе классов; регулярные определители . .	192
§ 2. Соотношения Кронекера между числами классов	194
§ 3. Формулы Дирихле	203
§ 4. Доказательство формул Дирихле для чисто коренного случая отрицательного определителя	205
<i>Примечания к главе VI</i>	212
<i>Библиографический указатель</i>	215

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ЧИСЕЛ

В этой главе излагаются в конспективном виде основные понятия классической теории чисел.

§ 1. Разложение чисел на простые множители; алгоритм Евклида. Если даны два целых числа a и $b \neq 0$ и отношение $\frac{a}{b}$ число целое, то говорят, что a делится на b , или a кратно b , или что b — делитель a . Число $p > 1$ называется *простым*, если оно не имеет других делителей, кроме очевидных $\pm 1, \pm p$. Как составляются все целые числа из простых чисел, указывает следующая основная теорема:

Теорема 1. *Каждое целое число > 1 представляется и притом единственным способом в виде произведения равных или неравных простых множителей.*

Будем обозначать через $d = (a, b)$ ($d > 0$) наибольший общий делитель чисел a и $b \neq 0$. Для нахождения его служит так называемый алгоритм Евклида; именно, последовательным делением получаем конечный ряд равенств

$$\left. \begin{aligned} a &= qb + r, & b &= q_1r + r_1, \\ r &= q_2r_1 + r_2, \dots, & r_{n-2} &= q_{n-1}r_{n-1} + r_n, & r_{n-1} &= q_n r_n, \end{aligned} \right\} \quad (1)$$

в которых $q, q_1, \dots, r, r_1, \dots$ — целые числа, причем

$$0 < r < |b|, \quad 0 < r_1 < r, \quad 0 < r_2 < r_1, \dots, \quad 0 < r_n < r_{n-1}.$$

Равенства (1) представляют не что иное, как разложение $\frac{a}{b}$ в обыкновенную непрерывную дробь:

$$\frac{a}{b} = q + \frac{1}{q_1 + \frac{1}{q_2 + \dots + \frac{1}{q_{n+1}}}}. \quad (2)$$

Из них выводим: 1) что r_n делит a и b , 2) что всякий общий делитель a и b делит r_n . Следовательно, $r_n = d$; исключая из (1) r_{n-1}, \dots, r_1, r и пользуясь свойствами непрерывных дробей, получаем $d = = Qa - Pb$, где $\pm P$ и $\pm Q$ суть числитель и знаменатель предпоследней подходящей к дроби (2). Таким образом приходим к классическому решению уравнения $aX - bY = d$ в целых числах X, Y при помощи непрерывных дробей.

При $d = 1$ числа a, b называются *взаимно простыми*. В этом случае из уравнения $Qa - Pb = 1$ видно, что при делимости ac на b целое число c должно делиться на b , что и приводит к теореме 1.

Из доказанных свойств (a, b) выводятся аналогичные свойства общего наибольшего делителя (a, b, \dots, c) нескольких чисел a, b, \dots, c , не равных одновременно нулю. Именно, (a, b, \dots, c) равен общему наибольшему делителю a и (b, \dots, c) и может быть представлен в виде линейной формы от a, b, \dots, c , с целыми коэффициентами. Аналогично общее наименьшее кратное чисел a, b, \dots, c , не равных нулю (т. е. наименьшее целое число, большее нуля, делящееся на каждое из чисел a, b, \dots, c), равно общему наименьшему кратному a и общего наименьшего кратного b, \dots, c . Для двух чисел a, b общее наименьшее кратное равно $\frac{|ab|}{(a, b)}$.

Относительно распределения простых чисел 2, 3, 5, 7, ... в ряду натуральных чисел не известно никаких точных законов. Отметим лишь важное предложение, доказанное еще в „Началах“ Евклида (кн. IX, 20) (см. А. А. Васильев ⁸⁵, стр. 27—44):

ТЕОРЕМА 2. Число простых чисел бесконечно.

Действительно, если имеется некоторое количество простых чисел p_1, p_2, \dots, p_k , то к ним всегда можно присоединить еще новое простое число; для этого нужно взять любой простой делитель числа $p_1 p_2 \dots p_k + 1$.

§ 2. Простейшие арифметические функции. Пусть $n > 0$ целое число; рассматривая все положительные делители n , обозначим через $\tau(n)$ их число и через $\zeta(n)$ — их сумму. Полагая на основании теоремы 1 $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, где p_1, p_2, \dots, p_k — различные простые числа, а a_1, a_2, \dots, a_k — положительные показатели, находим

$$\tau(n) = (a_1 + 1)(a_2 + 1) \dots (a_k + 1),$$

$$\zeta(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

Еще в древности (Евклид ⁸⁵, кн. VII) был поставлен вопрос о нахождении чисел n , равных сумме своих правильных делителей [т. е. делителей меньших n , так что $\zeta(n) = 2n$]. Такие числа называются *совершенными*. Евклидом же (кн. IX) доказана и единственная до сих пор известная теорема о совершенных числах, по которой все *четные* совершенные числа имеют вид $2^{p-1}(2^p - 1)$ при $2^p - 1$ простом. Для простоты $2^p - 1$ необходимо, чтобы показатель p был простым, но это условие недостаточно. Еще Эйлеру были известны восемь значений показателя p , при которых $2^p - 1$ простое число, именно, значения $p = 2, 3, 5, 7, 13, 17, 19, 31$ (см. Euler ¹⁷, т. I, стр. 1 и 584). Соответственно этому, Эйлер знал восемь четных совершенных чисел; нечетных совершенных чисел неизвестно ни одного, но и не доказано, что их не существует (см. примечания к этой главе).

В аналитической теории чисел важное значение имеет *функция Мёбиуса* $\mu(n)$, определяемая для $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ так: $\mu(n) = 0$, если

хоть одно из чисел $\alpha_i > 1$ и $\mu(n) = (-1)^k$ при $\alpha_1 = \alpha_2 = \dots = \alpha_k = 1$; при этом $\mu(1) = 1$. Легко доказывается основное свойство $\mu(n)$:

$$\sum \mu(d) = 0 \text{ при } n > 1,$$

где сумма берется по всем делителям d числа n . Отсюда получается важная *формула обращения*: если функция $F(n)$ для всякого целого $n > 0$ выражается через значения другой функции $f(n)$ по формуле $F(n) = \sum_{n=d\delta} f(d)$, то, обратно, для всякого n $f(n) = \sum_{n=d\delta} F(d)\mu(\delta)$, причем обе суммы распространяются на все делители d числа n или, что то же, на все представления $n = d\delta$ в виде произведения двух целых положительных множителей d, δ .

Обозначим через $\varphi(n)$ количество чисел, меньших n и с ним взаимно простых [$\varphi(1) = 1$]; эта функция введена Эйлером (см. ¹⁷, т. II, стр. 127). Выражение $\varphi(n)$ в простых множителях числа n следующее:

$$\begin{aligned} \varphi(n) &= p_1^{\alpha_1-1} (p_1 - 1) p_2^{\alpha_2-1} (p_2 - 1) \dots p_k^{\alpha_k-1} (p_k - 1) = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right). \end{aligned} \quad (3)$$

Классический способ доказательства этой формулы (L.-Dirichlet ¹⁴, § 11) И. М. Виноградов предложил заменить следующим, более простым: пусть $\varepsilon_k^p = 1$, если целое число k делится на простое число p , и $\varepsilon_k^p = 0$ в противном случае. Тогда

$$\begin{aligned} \varphi(n) &= \sum_{m=1}^n (1 - \varepsilon_m^{p_1}) (1 - \varepsilon_m^{p_2}) \dots (1 - \varepsilon_m^{p_k}) = \\ &= n - \sum_{m=1}^n \varepsilon_m^{p_1} - \sum_{m=1}^n \varepsilon_m^{p_2} - \dots + \sum_{m=1}^n \varepsilon_m^{p_1} \varepsilon_m^{p_2} + \dots \pm \sum_{m=1}^n \varepsilon_m^{p_1} \varepsilon_m^{p_2} \dots \varepsilon_m^{p_k} = \\ &= n - \frac{n}{p_1} - \frac{n}{p_2} - \dots + \frac{n}{p_1 p_2} + \dots \pm \frac{n}{p_1 p_2 \dots p_k} = n \prod_{r=1}^k \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

При помощи (3) (или непосредственно) выводится важное свойство функции $\varphi(n)$ (Gauss ²⁰, D. A., art. 39)¹:

$$\sum_{n=d\delta} \varphi(d) = n. \quad (4)$$

Все четыре введенные нами функции $\tau(n)$, $\zeta(n)$, $\mu(n)$ и $\varphi(n)$ удовлетворяют функциональному уравнению $f(mn) = f(m)f(n)$ при взаимно простых m и n . Рассмотренные в этом параграфе выражения $\tau(n)$, $\zeta(n)$, $\mu(n)$ и $\varphi(n)$ представляют простейшие *арифметические* функции, т. е.

¹ Буквами D. A. обозначаются во всем дальнейшем „Disquisitiones Arithmeticae“ Гаусса. Для удобства читателей ссылки делаются на немецкий перевод этого и других сочинений Гаусса по теории чисел.

величины, определяемые для целочисленного аргумента n . Изменения их с возрастанием аргумента отличаются чрезвычайной прихотливостью. Одна из этих функций, именно $\zeta(n)$, более изучена благодаря связи ее с представлением чисел суммой четырех квадратов в замечательной формуле Эйлера (гл. V, теоремы 20 и 23); природо же остальных функций: $\tau(n)$, $\mu(n)$ и $\varphi(n)$ остается для нас неизвестной. В дальнейших главах этой статьи читатель встретит много примеров других арифметических функций.

§ 3. Теоремы о делимости факториалов. В дальнейшем будем обозначать через $[x]$ целую часть вещественного числа x (т. е. целое число k , определяемое условием $k \leq x < k + 1$) и через $\{x\}$ — дробную часть x , т. е. разность $x - [x]$. Для некоторых вопросов нужно знать показатель, с которым входит данное простое число p в разложение на простые множители произведения $1 \cdot 2 \cdot 3 \cdots n = n!$ Этот показатель (L.-Dirichlet¹⁴, § 15) находится равным $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$. Отсюда получаем независимое от комбинаторики доказательство целостности биномиального коэффициента $\frac{(a+b+c+\dots)!}{a!b!c!\dots}$, если подсчитаем, сколько раз входит какое-нибудь простое число p в числитель и знаменатель этого выражения, и воспользуемся очевидным свойством знака $[]$: $[x+y] \geq [x] + [y]$.

Многочисленные подобные теоремы, утверждающие целостность различных выражений, составленных из факториалов, читатель найдет в книге Р. В а с h m a n n, *Niedere Zahlentheorie*⁴ (часть I, стр. 57). Из них наиболее интересна теорема Ландау. Пусть имеются две системы линейных форм $f_i(x_1, \dots, x_n) = a_{i1}x_1 + \dots + a_{in}x_n$ ($i = 1, 2, \dots, m$) и $g_i(x_1, \dots, x_n) = b_{i1}x_1 + \dots + b_{in}x_n$ ($i = 1, 2, \dots, p$) с неотрицательными целыми коэффициентами a_{ij} , b_{ij} . Для того чтобы выражение

$$\frac{f_1(x_1, \dots, x_n)! f_2(x_1, \dots, x_n)! \dots f_m(x_1, \dots, x_n)!}{g_1(x_1, \dots, x_n)! g_2(x_1, \dots, x_n)! \dots g_p(x_1, \dots, x_n)!}$$

было числом целым для любой системы целых неотрицательных значений x_1, x_2, \dots, x_n , необходимо и достаточно, чтобы во всей области $0 \leq y_1 \leq 1$, $0 \leq y_2 \leq 1$, \dots , $0 \leq y_n \leq 1$ значений переменных y_1, y_2, \dots, y_n удовлетворялось неравенство

$$\sum_{i=1}^m [f_i(y_1, \dots, y_n)] \geq \sum_{i=1}^p [g_i(y_1, \dots, y_n)].$$

§ 4. Теоремы Эйлера и Ферма; сравнения первой степени. Если разность двух чисел a, b делится на число $c \neq 0$, то говорят, что a сравнимо с b по модулю c , и пишут: $a \equiv b \pmod{c}$ или просто $a \equiv b \pmod{c}$. Сравнения с одним и тем же модулем можно складывать, вычитать, перемножать и сокращать (на множитель, взаимно простой с модулем), благодаря чему операции над сравнениями имеют большую аналогию с действиями над уравнениями. Знак сравнения был введен Гауссом²⁰ (D. A., art. 2) и оказался чрезвычайно удобным символом для передачи

арифметических рассуждений. Пусть k — целое число, большее нуля; объединим в один *класс* все числа, сравнимые с одним и тем же числом по модулю k (термин „класс“ принадлежит Гауссу, *Theoria residuorum biquadraticorum*, II, art. 42, см.²⁰, стр. 551). Так как для каждого числа a имеем $a = qk + r$, где r — одно из чисел $0, 1, 2, \dots, k-1$, и эти числа несравнимы по модулю k , то видим, что существует k различных классов для модуля k . Выбрав по одному представителю из каждого класса, получим систему k чисел, называемую *полной системой вычетов* по модулю k ; такую систему составляют, например, числа $0, 1, 2, \dots, k-1$. Если одно число класса взаимно просто с k , то и все числа этого класса обладают тем же свойством; таких классов будет, очевидно, $\varphi(k)$. Взяв по одному представителю от каждого из этих классов, получим *приведенную систему вычетов* по модулю k ; таковы, например, при k простым числа $1, 2, \dots, k-1$.

Пусть $(a, k) = 1$ и x пробегает приведенную систему вычетов по модулю k ; тогда произведения ax будут несравнимы по модулю k , так как из $ax \equiv ax'$ вытекает $x \equiv x'$. Кроме того, числа ax — взаимно простые с k ; следовательно, эти числа сравнимы по модулю k с числами x , взятыми только в другом порядке. Сравнивая произведения тех и других чисел по модулю k , приходим к важной теореме Эйлера (см.¹⁷, т. I, стр. 274):

ТЕОРЕМА 3. *Для всякого числа a , взаимно простого с данным числом $k > 0$, имеет место сравнение $a^{\varphi(k)} \equiv 1 \pmod{k}$.*

В частности, для простого $k = p$ и для a , не делящегося на p , имеем

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

Эта теорема, одна из самых важных в теории чисел, была найдена Ферма. Эйлер доказал ее несколькими способами и обобщил на случай составного модуля k .

Из рассуждения, которым мы пользовались при доказательстве теоремы Эйлера, вытекает и другой результат: сравнение первой степени $ax \equiv b \pmod{k}$ при a и b взаимно простых с k имеет только одно решение относительно x (считая все числа одного и того же класса за одно решение). При обобщении на случай любых a и b (L.-Dirichlet¹⁴, § 22) получается теорема: для возможности сравнения $ax \equiv b \pmod{k}$ необходимо, чтобы b делилось на $(a, k) = \delta$, и в этом случае оно имеет δ несравнимых по модулю k решений относительно x . Что касается отыскания самих решений x сравнения $ax \equiv b \pmod{k}$, то эти решения могут быть получены по правилу § 1 при помощи непрерывных дробей, ввиду того, что рассматриваемое сравнение эквивалентно неопределенному уравнению $ax - ky = b$.

При перенесении различных теорем теории чисел, доказанных для простых модулей, на составные модули, нужно решение следующей задачи: найти все числа x , удовлетворяющие системе сравнений $x \equiv \alpha \pmod{a}$, $x \equiv \beta \pmod{b}$, \dots , $x \equiv \gamma \pmod{c}$, где a, b, \dots, c — положительные, а $\alpha, \beta, \dots, \gamma$ — произвольные целые числа. Особенно важен частный случай, когда модули a, b, \dots, c попарно взаимно простые; в этом случае указанная система сравнений всегда имеет решения,

и числа x , ей удовлетворяющие, образуют один класс по модулю $ab \dots$ (L.-Dirichlet ¹⁴, § 25).

Если a и a' пробегают все числа классов K и K' по модулю k , то произведение aa' остается всегда в одном классе, который обозначим через KK' . Обозначая через 1 класс, к которому принадлежит число 1, и пользуясь доказанной выше теоремой о сравнениях первой степени, видим, что для каждого класса K , состоящего из чисел, взаимно простых с k , можно найти один вполне определенный („обратный“) класс K' , такой, что $KK' = 1$. Таким образом система $\varphi(k)$ классов, на которые распределяются числа, взаимно простые с k , удовлетворяет всем определениям *конечной группы*. Эта группа, очевидно, абелева.

§ 5. Теоремы Лагранжа и Вильсона. Два целочисленных полинома $P(x)$ и $P_1(x)$ вида $ax^m + bx^{m-1} + \dots + c$ называются *сравнимыми* по простому модулю p , если коэффициенты при одинаковых степенях x в них сравнимы по модулю p ; записывается так: $P(x) \equiv P_1(x) \pmod{p}$. Если $P(x) \equiv P_1(x) Q(x) \pmod{p}$, где $Q(x)$ — целочисленный полином, то говорят, что функция $P(x)$ *делится* на $P_1(x)$ по модулю p . Если $P(x)$ не имеет других делителей по модулю p , кроме $aP(x)$ и a [a — целое число, $\not\equiv 0 \pmod{p}$], то полином $P(x)$ называется *неприводимым* или *простым* по модулю p . Таким будет, например, всякий полином первой степени $x + a$. Простые по модулю p полиномы находятся в полной аналогии с обыкновенными простыми числами; именно, существует теорема: всякая целочисленная функция $A(x)$ вида $x^m + ax^{m-1} + \dots$ представляется по модулю p в виде произведения простых функций:

$$A(x) \equiv P_1(x)^{\alpha_1} P_2(x)^{\alpha_2} \dots P_k(x)^{\alpha_k} \pmod{p}, \quad (5)$$

и притом единственным образом (сравнимые по модулю p полиномы не считаются различными). В сравнении (5) $P_1(x), P_2(x), \dots$ суть простые и различные (т. е. несравнимые) по модулю p функции со старшим коэффициентом 1, а $\alpha_1, \alpha_2, \dots$ — положительные показатели. Теорема эта доказывается так же, как и аналогичная теорема для чисел (§ 1), причем устанавливаются сначала алгоритм Евклида и свойства общего наибольшего делителя двух целых функций по модулю p (см., например, Вачшп ⁴, часть I, гл. VII, § 19).

Пусть $A(x) = a_0x^m + \dots, a_0 \not\equiv 0 \pmod{p}$ — целочисленная функция и число $x = \alpha$ удовлетворяет сравнению $A(x) \equiv 0 \pmod{p}$. Деля $A(x)$ на $x - \alpha$, получим $A(x) = (x - \alpha)A_1(x) + A(\alpha) \equiv (x - \alpha)A_1(x) \pmod{p}$, т. е. $A(x)$ делится по модулю p на простую функцию $x - \alpha$. Итак, решение сравнения $A(x) \equiv 0 \pmod{p}$ равносильно выделению линейных простых делителей функции $A(x)$ по модулю p . Так как количество различных простых делителей $A(x)$ по модулю p не может превышать степени m этой функции, то получаем *теорему Лагранжа*:

ТЕОРЕМА 4. Сравнение m -й степени $a_0x^m + a_1x^{m-1} + \dots + a_m \equiv 0 \pmod{p}$ ($a_0 \not\equiv 0$) не может иметь более m несравнимых решений.

По теореме Ферма (§ 4) сравнение $x^{p-1} - 1 \equiv 0 \pmod{p}$ имеет $p - 1$ несравнимых решений 1, 2, ..., $p - 1$, откуда выводим, что разложение $x^{p-1} - 1$ на простые множители по модулю p имеет вид

$$x^{p-1} - 1 \equiv (x - 1)(x - 2) \dots (x - p + 1) \pmod{p}.$$

Сравнивая свободные члены в обеих частях, получаем *теорему Вильсона*: $1 \cdot 2 \cdot 3 \dots (p-1) \equiv -1 \pmod{p}$. Теорема эта, справедливая для всякого простого числа, особенно интересна тем, что она выражает *характеристическое* свойство простых чисел; в самом деле, очевидно, что если для какого-нибудь числа p выражение $1 \cdot 2 \cdot 3 \dots (p-1) + 1$ делится на p , то число p должно быть простым. Соединяя в произведении $1 \cdot 2 \cdot 3 \dots (p-1)$ множители, равноотстоящие от концов, получаем из теоремы Вильсона сравнение $\left[1 \cdot 2 \cdot 3 \dots \frac{p-1}{2}\right]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ (при $p > 2$), откуда для простого числа p формы $4n+3$ вытекает сравнение $1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \equiv \pm 1 \pmod{p}$. Знак \pm , стоящий в этом сравнении, не находится в простой зависимости с числом p ; вопрос об этом знаке был поставлен Дирихле (см. ¹³, т. I, стр. 107). Так как -1 есть квадратичный невычет для простого числа p формы $4n+3$ (см. § 8 этой главы), то в сравнении

$$1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \equiv \pm 1 \pmod{p} \quad (6)$$

будет стоять знак $+$ или $-$, смотря по тому, будет ли количество β квадратичных невычетов по модулю p среди чисел $1, 2, 3, \dots, \frac{p-1}{2}$ четным или нечетным. Обозначая через α количество квадратичных вычетов среди чисел $1, 2, 3, \dots, \frac{p-1}{2}$, имеем по формуле Дирихле (см. главу VI) $\alpha - \beta = h(-p)$, где $h(-p)$ есть число классов чисто коренных положительных бинарных форм определителя $-p$. Присоединяя сюда очевидное равенство $\alpha + \beta = \frac{p-1}{2}$, получаем $\beta = \frac{p+1}{4} - \frac{1+h(-p)}{2}$. Таким образом знак в сравнении (6) находится в зависимости от вычета по модулю 4 величины $h(-p)$, меняющейся чрезвычайно неправильно с изменением p . Кронекер, пользуясь открытыми им рекуррентными соотношениями для числа классов, видоизменил этот критерий (см. далее главу VI).

§ 6. Первообразные корни, индексы, двучленные сравнения. Пусть p — простой модуль и a — не делящееся на p число. Уже из теоремы Ферма (§ 4) видно, что существуют положительные показатели δ (например $\delta = p-1$), для которых $a^\delta \equiv 1 \pmod{p}$. Если δ — наименьший показатель такого рода, то говорят, что a *принадлежит к показателю* δ по модулю p ; этот показатель δ должен быть делителем числа $p-1$, так как в противном случае из $a^\delta \equiv 1$ и $a^{p-1} \equiv 1$ вытекало бы $a^{(\delta, p-1)} \equiv 1 \pmod{p}$, причем $(\delta, p-1) < \delta$. Число g , принадлежащее к показателю $\delta = p-1$, называется *первообразным корнем*. Для такого числа степени $1, g, g^2, \dots, g^{p-2}$, очевидно, несравнимы по модулю p и образуют поэтому приведенную систему вычетов по модулю p , так что для каждого $a \not\equiv 0 \pmod{p}$ найдется показатель α , для которого $a \equiv g^\alpha \pmod{p}$. Понятие о первообразном корне введено Эйлером (см. ¹⁷, т. I, стр. 516); однако Эйлеру не удалось строго доказать существо-

вание первообразного корня для всякого простого числа p . Это было сделано впервые Гауссом (см. ²⁰, D. A., art. 54). Доказательство Гаусса, воспроизводимое ниже, является одним из самых блестящих примеров арифметического рассуждения. Пусть $\psi(\delta)$ есть количество несравнимых по модулю p чисел, принадлежащих к заданному делителю δ числа $p-1$ как к показателю. Предположим, что существует хоть одно из таких чисел, например a ; тогда δ чисел $1, a, a^2, \dots, a^{\delta-1}$ несравнимы по модулю p . Все эти числа удовлетворяют сравнению $x^\delta \equiv 1 \pmod{p}$, так что других решений это сравнение иметь не может (теорема 4). Поэтому остальные числа (кроме a), принадлежащие к показателю δ , нужно искать среди степеней $1, a, a^2, \dots, a^{\delta-1}$. Рассматривая же степень a^s , находим, что показатель d , к которому она принадлежит, есть наименьшее число, для которого sd делится на δ . Таким образом $d = \delta$ тогда и только тогда, когда $(s, \delta) = 1$. Итак, при $\psi(\delta) > 0$ непременно $\psi(\delta) = \varphi(\delta)$. Разобьем числа $1, 2, \dots, p-1$ на группы, отнеся в одну группу все числа, принадлежащие к одному и тому же показателю δ ; в группе, соответствующей δ , будет $\psi(\delta)$ чисел, так что получаем соотношение $\sum \psi(\delta) = p-1$, где сумма берется по всем делителям δ числа $p-1$. Сравнивая его с аналогичным соотношением для функции φ : $\sum \varphi(\delta) = p-1$ [формула (4)], находим для всякого δ $\psi(\delta) = \varphi(\delta)$, что для $\delta = p-1$ и дает теорему Гаусса:

ТЕОРЕМА 5. *Для всякого простого числа p существует $\varphi(p-1)$ несравнимых по модулю p первообразных корней.*

Разыскание первообразных корней при большом p требует значительных вычислений и совершается путем проб. Гаусс дал метод, позволяющий уменьшить количество этих проб (см. ²⁰, D. A., art. 73). Лишь для некоторых специальных форм модуля p П. Л. Чебышеву (см. ⁸², стр. 198) удалось а priori указать первообразный корень. Простейшие из теорем Чебышева следующие: 1) для простого числа p формы $2^n + 1$ ($n > 1$) первообразным корнем является число 3, 2) если в простом числе $p = 4N + 1$ число $N > 2$ и также простое, то первообразным корнем p будет 2.

Пусть $a \not\equiv 0 \pmod{p}$; показатель a в сравнении $a \equiv g^a \pmod{p}$, определяемый с точностью до слагаемого, кратного $p-1$, называется *индексом* числа a . Система этих индексов (при фиксированном g) обладает полной аналогией с системой логарифмов, так как, очевидно,

$$\text{Ind}(ab) \equiv \text{Ind } a + \text{Ind } b, \quad \text{Ind } \frac{a}{b} \equiv \text{Ind } a - \text{Ind } b \pmod{p-1}$$

(через $\frac{a}{b}$ обозначаем корень сравнения $bx \equiv a \pmod{p}$). Если построены таблицы, дающие для каждого числа $1, 2, \dots, p-1$ его индекс, и обратно, то эти таблицы приносят такую же пользу при решении сравнений, как и таблица логарифмов при обычных действиях; например, решение сравнений $ax \equiv b$, $x^n \equiv A \pmod{p}$ приводится к вычитанию и делению по модулю $p-1$. Таблицы индексов были вычислены Якоби ³⁰ для всех простых чисел p до 1000.