Б.А. Венков

Математика в монографиях

Книга 4. Элементарная теория чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Б11

Б.А. Венков
Б11 Математика в монографиях: Книга 4. Элементарная теория чисел / Б.А. Венков – М.: Книга по Требованию, 2013. – 222 с.

ISBN 978-5-458-27162-2

Заглавие "Элементарная теория чисел", данное настоящему реферату, не вполне отражает ту точку зрения, которая была принята при его составлении. В нём 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 это серии.

ISBN 978-5-458-27162-2

ПРЕДИСЛОВИЕ

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.

ОГЛАВЛЕНИЕ

Глава I

Основные понятия теории чисел

Глава II

Непрерывные дроби и диофантовы приближения

Глава III

Степенные вычеты

Глава IV

Гауссова теория квадратичных форм

Глава V

Разбиение чисел на слагаемые и методы Лиувилля

Глава VI

Число классов бинарных квадратичных форм

ГЛАВА I

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ЧИСЕЛ

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

§ 1. Разложение чисел на простые множители; алгорифм 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 ± 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 алгорифм Евклида; именно, последовательным делением получаем конечный ряд равенств

$$\left.\begin{aligned} a = qb + r, \quad b = q_1 r + r_1, \\ r = q_2 r_1 + r_2, \ \ldots, \quad r_{n-2} = q_n r_{n-1} + r_n, \quad r_{n-1} = q_{n+1} r_n, \end{aligned}\right\} \tag{1}$$

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

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

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

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{n+1}}}}. \tag{2}$$

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) $r_{n-1}, \ldots, r_1, r$ 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 $(a, b, \ldots, c)$ нескольких чисел $a, b, \ldots, c$, не равных одновременно нулю. Именно, $(a, b, \ldots, c)$ равен общему наибольшему делителю a и $(b, \ldots, c)$ и может быть представлен в виде линейной формы от $a, b, \ldots, c$, с целыми коэфициентами. Аналогично общее наименьшее кратное чисел $a, b, \ldots, c$, не равных нулю (т. е. наименьшее целое число, большее нуля, делящееся на каждое из чисел $a, b, \ldots, c$), равно общему наименьшему кратному a и общего наименьшего кратного $b, \ldots, c$. 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 $p_1, p_2, \ldots, p_k$, то к ним всегда можно присоединить еще новое простое число; для этого нужно взять любой простой делитель числа $p_1 p_2 \ldots p_k + 1$.

§ 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 $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, где $p_1, p_2, \ldots, p_k$ — различные простые числа, а $\alpha_1, \alpha_2, \ldots, \alpha_k$ — положительные показатели, находим

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1),$$

$$\zeta(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

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 $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ так: $\mu(n) = 0$, если

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

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

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:

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1) =$$
$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right). \tag{3}$$

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

$$\varphi(n) = \sum_{m=1}^{n} (1 - \varepsilon_m^{p_1})(1 - \varepsilon_m^{p_2}) \ldots (1 - \varepsilon_m^{p_k}) =$$

$$= n - \sum_{m=1}^{n} \varepsilon_m^{p_1} - \sum_{m=1}^{n} \varepsilon_m^{p_2} - \ldots + \sum_{m=1}^{n} \varepsilon_m^{p_1}\varepsilon_m^{p_2} + \ldots \pm \sum_{m=1}^{n} \varepsilon_m^{p_1}\varepsilon_m^{p_2} \ldots \varepsilon_m^{p_k} =$$

$$= n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots + \frac{n}{p_1 p_2} + \ldots \pm \frac{n}{p_1 p_2 \ldots p_k} = n \prod_{r=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

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

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

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); природа 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 $k \leqslant x < k+1$) 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.-Dirichlet [14], § 15) находится равным $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$ Отсюда получаем независимое от комбинаторики доказательство целости биномиального коэфициента $\frac{(a+b+c+\ldots)!}{a!\,b!\,c!\ldots}$, если подсчитаем, сколько раз входит какое-нибудь простое число p в числитель и знаменатель этого выражения, и воспользуемся очевидным свойством знака [ ]: $[x+y] \geqslant [x]+[y]$.

Многочисленные подобные теоремы, утверждающие целость различных выражений, составленных из факториалов, читатель найдет в книге P. Bachmann, Niedere Zahlentheorie [4] (часть I, стр. 57). Из них наиболее интересна теорема Ландау. Пусть имеются две системы линейных форм $f_i(x_1, \ldots, x_n) = a_{i_1}x_1 + \ldots + a_{i_n}x_n$ $(i = 1, 2, \ldots, m)$ и $g_i(x_1, \ldots, x_n) = b_{i_1}x_1 + \ldots + b_{i_n}x_n$ $(i = 1, 2, \ldots, p)$ с неотрицательными целыми коэфициентами a_{i_j}, b_{i_j}. Для того чтобы выражение

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

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

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

§ 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 $a \equiv b\ (c)$. 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 Гауссом [20] (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, ..., $k-1$, 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, ..., $k-1$. 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 простом числа 1, 2, ..., $k-1$.

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.-Dirichlet[14], § 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 $x \equiv \alpha \pmod{a}$, $x \equiv \beta \pmod{b}$, ..., $x \equiv \gamma \pmod{c}$, где $a, b, \ldots, c$ — положительные, а $\alpha, \beta, \ldots, \gamma$ — произвольные целые числа. Особенно важен частный случай, когда модули $a, b, \ldots, c$ попарно взаимно простые; в этом случае указанная система сравнений всегда имеет решения,

и числа x, ей удовлетворяющие, образуют один класс по модулю $ab\ldots c$ (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 $ax^m + bx^{m-1} + \ldots + c$ называются *сравнимыми* по простому модулю p, если коэфициенты 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 $x^m + ax^{m-1} + \ldots$ представляется по модулю p в виде произведения простых функций:

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

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

Пусть $A(x) = a_0x^m + \ldots$, $a_0 \not\equiv 0\ (p)$ — 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* $a_0x^m + a_1x^m + \ldots + a_m \equiv 0 \pmod p$ $(a_0 \not\equiv 0)$ *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

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