И. М. Виноградов

Основы теории чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
И11

И. М. Виноградов
И11 Основы теории чисел / И. М. Виноградов – М.: Книга по Требованию, 2013. – 181 с.

ISBN 978-5-458-26887-5

В книге даётся систематическое изложение основ теории чисел в объёме университетского курса. Значительное количество задач вводит читателя в круг некоторых новых идей в области теории чисел.В книге излагаются основы теории чисел в объеме университетского курса. В последнее издание включена новая глава о характерах Дирихле, значительной переработке подвергнута глава о важнейших функциях, встречающихся в теории чисел, внесены изменения в решения ряда задач.

ISBN 978-5-458-26887-5

ПРЕДИСЛОВИЕ К ПЯТОМУ ИЗДАНИЮ.

Ряд русских математиков — Чебышев, Коркин, Золотарёв, Марков, Вороной и другие — занимался теорией чисел. Ознакомиться с содержанием классических работ этих замечательных учёных можно по книжке Б. Н. Делоне «Петербургская школа теории чисел».

Советские математики, работающие в области теории чисел, продолжая славные традиции своих предшественников, создали новые мощные методы, позволившие получить ряд первоклассных результатов; в разделе теории чисел книги «Математика в СССР за 30 лет» можно найти сведения о достижениях советских учёных в области теории чисел, а также соответствующие библиографические данные.

В моей книге даётся систематическое изложение основ теории чисел в объёме университетского курса. Значительное количество задач вводит читателя в круг некоторых новых идей в области теории чисел.

Настоящее пятое издание книги значительно отличается от четвёртого. Ряд изменений, способствующих большей простоте изложения, внесён во все главы книги. Особо значительными изменениями являются объединение прежних глав IV и V в одну главу IV (благодаря чему число глав сократилось до шести), а также новое, более простое доказательство существования первообразных корней.

Существенно переработаны вопросы, помещённые в конце каждой главы. Порядок следования вопросов теперь приведён в полное соответствие с порядком расположения теоретического материала. Введены некоторые новые вопросы; однако число номеров вопросов

значительно сокращено. Последнее достигнуто путём объединения под названиями **a**, **b**, **c**, ... ранее самостоятельных вопросов, близких по методу решения или по содержанию. Пересмотрены все решения вопросов; в ряде случаев эти решения упрощены или заменены лучшими. Особенно сильные изменения внесены в решения вопросов, касающихся распределения вычетов и невычетов n-й степени и первообразных корней, а также оценок соответствующих тригонометрических сумм.

И. М. Виноградов

ГЛАВА ПЕРВАЯ.

ТЕОРИЯ ДЕЛИМОСТИ.

§ 1. Основные понятия и теоремы.

а. Теория чисел занимается изучением свойств целых чисел. Целыми мы будем называть не только числа натурального ряда 1, 2, 3, ... (положительные целые), но также нуль и отрицательные целые -1, -2, -3, ...

Как правило, при изложении теоретического материала мы будем обозначать буквами только целые числа. Случаи, когда буквы могут обозначать и не целые числа, если последнее не будет ясно само по себе, мы будем особо оговаривать.

Сумма, разность и произведение двух целых a и b будут также целыми, но частное от деления a на b (если b не равно нулю) может быть как целым, так и не целым.

b. В случае, когда частное от деления a на b — целое, обозначая его буквою q, имеем $a = bq$, т. е. *a равно произведению b на целое*. Мы говорим тогда, что *a делится* на b или что *b делит a*. При этом a называем *кратным* числа b и b — *делителем* числа a. То обстоятельство, что b делит a, записывается так: $b \backslash a$.

Имеют место две следующие теоремы.

1. *Если a кратно m, m кратно b, то a кратно b;*

Действительно, из $a = a_1 m$, $m = m_1 b$ следует $a = a_1 m_1 b$, где $a_1 m_1$ — целое. А это и доказывает теорему.

2. *Если в равенстве вида $k + l + \ldots + n = p + q + \ldots + s$ относительно всех членов, кроме какого-либо одного,*

известно, что они кратны b, то и этот один член кратен b.

Действительно, пусть таким членом будет k. Имеем

$$l = l_1 b, \ \ldots, \ n = n_1 b, \ p = p_1 b, \ q = q_1 b, \ \ldots, \ s = s_1 b,$$

$$k = p + q + \ldots + s - l - \ldots - n =$$

$$= (p_1 + q_1 + \ldots + s_1 - l_1 - \ldots - n_1)\, b.$$

А это и доказывает теорему.

c. В общем случае, включающем, как частный, и случай, когда a делится на b, имеем теорему:

Всякое целое a представляется единственным способом через положительное целое b в форме

$$a = bq + r; \quad 0 \leqslant r < b.$$

Действительно, одно представление a в такой форме получим, взяв bq равным наибольшему кратному числа b, не превосходящему a. Допустив, что также $a = bq_1 + r_1$, $0 \leqslant r_1 < b$, получим $0 = b(q - q_1) + r - r_1$, откуда следует (2, b), что $r - r_1$ кратно b. Но ввиду $|r - r_1| < b$ последнее возможно лишь при $r - r_1 = 0$, т. е. при $r = r_1$, откуда вытекает также $q = q_1$.

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

Пример. Пусть $b = 14$. Имеем

$$177 = 14 \cdot 12 + 9; \qquad 0 < 9 < 14,$$

$$-64 = 14 \cdot (-5) + 6; \qquad 0 < 6 < 14,$$

$$154 = 14 \cdot 11 + 0; \qquad 0 = 0 < 14.$$

§ 2. Общий наибольший делитель.

a. В дальнейшем мы будем рассматривать лишь положительные делители чисел. Всякое целое, делящее одновременно целые $a, b, \ldots, l$, называется их *общим делителем*. Наибольший из общих делителей называется *общим наибольшим делителем* и обозначается символом $(a, b, \ldots, l)$. Ввиду конечности числа общих делителей существование общего наибольшего делителя очевидно. Если $(a, b, \ldots, l) = 1$, то $a, b, \ldots, l$ называются *взаимно*

простыми. Если каждое из чисел $a, b, \ldots, l$ взаимно просто с каждым другим из них, то $a, b, \ldots, l$ называются *попарно простыми*. Очевидно, числа попарно простые всегда и взаимно простые; в случае же двух чисел понятия «попарно простые» и «взаимно простые» совпадают.

Примеры. Числа 6, 10, 15 ввиду $(6, 10, 15) = 1$ — взаимно простые. Числа 8, 13, 21 ввиду $(8, 13) = (8, 21) = (13, 21) = 1$ — попарно простые.

b. Сначала займёмся общими делителями двух чисел.

1. *Если a кратно b, то совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b; в частности, $(a, b) = b$.*

Действительно, всякий общий делитель чисел a и b является делителем и одного b. Обратно, раз a кратно b, то (**1**, **b**, § **1**) всякий делитель числа b является также делителем числа a, т. е. он будет общим делителем чисел b и a. Таким образом совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b. А так как наибольший делитель числа b есть само b, то $(a, b) = b$.

2. *Если*

$$a = bq + c,$$

то совокупность общих делителей чисел a и b совпадает с совокупностью общих делителей чисел b и c; в частности, $(a, b) = (b, c)$.

Действительно, написанное выше равенство показывает, что всякий общий делитель чисел a и b делит также и c (**2**, **b**, § **1**) и, следовательно, является общим делителем чисел b и c. Обратно, то же равенство показывает, что всякий общий делитель чисел b и c делит a и, следовательно, является общим делителем чисел a и b. Таким образом общие делители чисел a и b суть те же, что и общие делители чисел b и c; в частности, должны совпадать и наибольшие из этих делителей, т. е. $(a, b) = (b, c)$.

c. Для разыскания общего наибольшего делителя, а также для вывода его важнейших свойств применяется *алгоритм Эвклида*. Последний состоит в нижеследующем.

Пусть a и b — положительные целые. Согласно с, § 1 находим ряд равенств:

$$\left.\begin{aligned} a &= bq_1 + r_2, && 0 < r_2 < b, \\ b &= r_2q_2 + r_3, && 0 < r_3 < r_2, \\ r_2 &= r_3q_3 + r_4, && 0 < r_4 < r_3, \\ &\dots\dots\dots\dots\dots\dots\dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, && 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_n, \end{aligned}\right\} \qquad (1)$$

заканчивающийся, когда получаем некоторое $r_{n+1} = 0$. Последнее неизбежно, так как ряд b, r_2, r_3, ... как ряд убывающих целых не может содержать более чем b положительных.

d. Рассматривая равенства (1), идя сверху вниз, убеждаемся (b), что общие делители чисел a и b одинаковы с общими делителями чисел b и r_2, далее одинаковы с общими делителями чисел r_2 и r_3, чисел r_3 и r_4, ..., чисел r_{n-1} и r_n, наконец, с делителями одного числа r_n. Одновременно с этим имеем

$$(a,\ b) = (b,\ r_2) = (r_2,\ r_3) = \dots = (r_{n-1},\ r_n) = r_n.$$

Мы приходим к следующим результатам.

1. *Совокупность общих делителей чисел a и b совпадает с совокупностью делителей их общего наибольшего делителя.*

2. *Этот общий наибольший делитель равен r_n, т. е. последнему не равному нулю остатку алгоритма Эвклида.*

Пример. Применим алгоритм Эвклида к отысканию (525, 231). Находим (вспомогательные вычисления приведены слева)

525 | 231	$525 = 231 \cdot 2 + 63,$
462 | 2	$231 = 63 \cdot 3 + 42,$
231 | 63	$63 = 42 \cdot 1 + 21,$
189 | 3	$42 = 21 \cdot 2.$
63 | 42	
42 | 1	
42 | 21	
42 | 2	
0	

Здесь последний положительный остаток есть $r_4 = 21$. Значит, $(525, 231) = 21$.

e. 1. *Обозначая буквою m любое положительное целое, имеем* $(am, bm) = (a, b)\,m$.

2. *Обозначая буквою δ любой общий делитель чисел a и b, имеем* $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}$; *в частности, имеем* $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$, *т. е. частные от деления двух чисел на их общий наибольший делитель суть числа взаимно простые.*

Действительно, умножим равенства (1) почленно на m. Получим новые равенства, где вместо a, b, r_2, ..., r_n будут стоять am, bm, r_2m, ..., r_nm. Поэтому $(am, bm) = r_nm$, и таким образом верно утверждение **1**.

Применяя утверждение **1**, находим

$$(a, b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta;$$

отсюда следует утверждение **2**.

f. 1. *Если* $(a, b) = 1$, *то* $(ac, b) = (c, b)$.

Действительно, (ac, b) делит ac и bc, значит (**1**, **d**), оно делит и (ac, bc), ввиду **1**, **e** равное c; но (ac, b) делит и b, поэтому оно делит и (c, b). Обратно, (c, b) делит ac и b, поэтому оно делит и (ac, b). Таким образом (ac, b) и (c, b) взаимно делят друг друга и, следовательно, равны между собою.

2. *Если* $(a, b) = 1$ *и ac делится на b, то c делится на b.*

Действительно, ввиду $(a, b) = 1$ имеем $(ac, b) = (c, b)$. Но раз ac кратно b, то (**1**, **b**) имеем $(ac, b) = b$, значит, и $(c, b) = b$, т. е. c кратно b.

3. *Если каждое a_1, a_2, ..., a_m взаимно просто с каждым b_1, b_2, ..., b_n, то и произведение $a_1a_2 \ldots a_m$ взаимно просто с произведением $b_1b_2 \ldots b_n$.*

Действительно (теорема **1**), имеем

$$(a_1a_2a_3 \ldots a_m, b_k) = (a_2a_3 \ldots a_m, b_k) =$$
$$= (a_3 \ldots a_m, b_k) = \ldots = (a_m, b_k) = 1,$$

и далее, полагая для краткости $a_1a_2 \ldots a_m = A$, точно таким же путём найдём,

$$(b_1b_2b_3 \ldots b_n, A) = (b_2b_3 \ldots b_n, A) = \\ = (b_3 \ldots b_n, A) = \ldots = (b_n, A) = 1.$$

g. Задача отыскания общего наибольшего делителя более чем двух чисел сводится к таковой для двух чисел. Именно, чтобы найти общий наибольший делитель чисел $a_1, a_2, \ldots, a_n$, составляем ряд чисел:

$$(a_1, a_2) = d_2, \ (d_2, a_3) = d_3, \ (d_3, a_4) = d_4, \ \ldots, \ (d_{n-1}, a_n) = d_n.$$

Число d_n и будет общим наибольшим делителем всех данных чисел.

Действительно (**1, d**), общие делители чисел a_1 и a_2 совпадают с делителями d_2; поэтому общие делители чисел a_1, a_2 и a_3 совпадают с общими делителями чисел d_2 и a_3, т. е. совпадают с делителями d_3. Далее убедимся, что общие делители чисел a_1, a_2, a_3, a_4 совпадают с делителями d_4 и т. д. и, наконец, что общие делители чисел $a_1, a_2, \ldots, a_n$ совпадают с делителями d_n. А так как наибольший делитель d_n есть само d_n, то оно будет общим наибольшим делителем чисел $a_1, a_2, \ldots, a_n$.

Просматривая приведённое доказательство, убеждаемся, что теорема **1, d** верна и для более чем двух чисел. Верны также и теоремы **1, e** и **2, e**, потому что от умножения на m или разделения на δ всех чисел $a_1, a_2, \ldots, a_n$ точно так же и все $d_2, d_3, \ldots, d_n$ умножатся на m или разделятся на δ.

§ 3. Общее наименьшее кратное.

a. Всякое целое, кратное всех данных чисел, называется их *общим кратным*. Наименьшее положительное общее кратное называется *общим наименьшим кратным*.

b. Сначала займёмся общим наименьшим кратным двух чисел. Пусть M — какое-либо общее кратное целых

a и b. Так как оно кратно a, то $M = ak$, где k — целое. Но M кратно и b, поэтому целым должно быть и

$$\frac{ak}{b},$$

что, полагая $(a, b) = d$, $a = a_1 d$, $b = b_1 d$, можно представить в виде $\frac{a_1 k}{b_1}$, где $(a_1, b_1) = 1$ (2, e, § 2). Поэтому (2, f, § 2) k должно делиться на b_1, $k = b_1 t = \frac{b}{d} t$, где t — целое. Отсюда

$$M = \frac{ab}{d} t.$$

Обратно, очевидно, что всякое M такой формы кратно как a, так и b, и, таким образом, эта форма даёт общий вид всех общих кратных чисел a и b.

Наименьшее положительное из этих кратных, т. е. общее наименьшее кратное, получим при $t = 1$. Оно будет

$$m = \frac{ab}{d}.$$

Введя m, можно полученную для M формулу переписать так:

$$M = mt.$$

Последнее и предпоследнее равенства приводят к теоремам:

1. *Общие кратные двух чисел совпадают с кратными их общего наименьшего кратного.*

2. *Общее наименьшее кратное двух чисел равно их произведению, делённому на их общий наибольший делитель.*

c. Пусть требуется найти общее наименьшее кратное более чем двух чисел $a_1, a_2, \ldots, a_n$. Обозначая вообще символом $[a, b]$ общее наименьшее кратное чисел a и b, составим ряд чисел:

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

Полученное таким путём m_n и будет общим наименьшим кратным всех данных чисел.

Действительно (1, b), общие кратные чисел a_1 и a совпадают с кратными m_2, поэтому общие кратные чисел a_1, a_2 и a_3 совпадают с общими кратными m_2 и a_3, т. е. совпадают с кратными m_3. Далее убедимся, что общие кратные чисел a_1, a_2, a_3, a_4 совпадают с кратными m_4 и т. д. и, наконец, что общие кратные чисел $a_1, a_2, \ldots, a_n$ совпадают с кратными m_n, а так как наименьшее положительное кратное m_n есть само m_n, то оно и будет общим наименьшим кратным чисел $a_1, a_2, \ldots, a_n$.

Просматривая приведённое доказательство, видим, что теорема 1, b верна и для более чем двух чисел. Кроме того, убеждаемся в справедливости следующей теоремы:

Общее наименьшее кратное попарно простых чисел равно их произведению.

§ 4. Связь алгоритма Эвклида с непрерывными дробями.

а. Пусть α — любое вещественное число. Обозначим буквою q_1 наибольшее целое, не превосходящее α. При нецелом α имеем

$$\alpha = q_1 + \frac{1}{\alpha_2}; \quad \alpha_2 > 1.$$

Точно так же при нецелых $\alpha_2, \ldots, \alpha_{s-1}$ имеем

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}; \quad \alpha_3 > 1;$$

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

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}; \quad \alpha_s > 1,$$

ввиду чего получаем следующее *разложение* α *в непрерывную дробь*:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}}. \qquad (1)$$