Серия
«Антология мысли»

1891—1983

И. М. Виноградов

Основы теории чисел

Книга доступна в электронной библиотечной системе
biblio-online.ru

Москва ■ Юрайт ■ **2019**

УДК 511
ББК 22.13
В49

***Автор*:**

Виноградов Иван Матвеевич (1891—1983) — советский математик, академик АН СССР.

Виноградов, И. М.

В49 Основы теории чисел / И. М. Виноградов. — М. : Издательство Юрайт, 2019. — 102 с. — (Серия : Антология мысли).

ISBN 978-5-534-09553-1

В настоящем издании публикуется труд советского математика И. М. Виноградова, в котором излагаются основы теории чисел. Репринтное издание. Текст печатается по изданию: Виноградов И. М. Основы теории чисел / И. М. Виноградов. М., Л. : Объединенное научно-техническое издательство НКТП СССР, 1936.

Для широкого круга читателей, интересующихся вопросами теории чисел.

УДК 511
ББК 22.13

ISBN 978-5-534-09553-1

Оглавление

Глава 1.

ТЕОРИЯ ДЕЛИМОСТИ.

§ 1. Основные понятия и теоремы.

a. 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,...

Сумма, разность и произведение двух целых будет также целым, но отношение двух целых может быть как целым, так и не целым.

Если отношение двух целых a и b

$$\frac{a}{b}=q$$

целое, то имеем:

$$a=bq,$$

т. е. *a равно произведению b на целое*. Мы будем говорить тогда, что *a делится* на b или, что *b делит a*. При этом a будем называть *кратным* числа b и *b — делителем* числа a.

b. В общем случае, считая b положительным, допустим, что bq наибольшее кратное b, не превосходящее a. Имеем:

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

Представление a через b в такой форме является единственным. Действительно, из

$$a=bq_1+r_1; \qquad 0\leqslant r_1<b$$

следует:

$$r_1-r=b(q-q_1),$$

т. е., что r_1-r кратно b. Но ввиду $(r_1-r)<b$ последнее возможно лишь при условии $r_1-r=0$, т. е. при $r_1=r$, откуда вытекает также $q_1=q$. Найденный результат можно формулировать так:

Всякое целое a представляется единственным образом через положительное целое b в форме:

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

Число r назовем остатком от деления a на b.

Пример. Пусть $b=14$. Имеем:

$$\begin{aligned} 177&=14\cdot 12\ +9; & 0&<9<14,\\ -64&=14(-5)+6; & 0&<6<14,\\ 154&=14\cdot 11\ +0; & 0&=0<14. \end{aligned}$$

В дальнейшем будут полезны две следующие теоремы.

c. *Если a кратно b, b кратно c, то a кратно c.*

Действительно, из $a=a_1b$; $b=b_1c$, где a_1 и b_1—целые, следует $a=a_1b_1c$, где a_1b_1 — целое, а это и доказывает теорему.

d. *Если в равенстве вида*

$$a+b+\ldots+l=r+s+\ldots+u$$

все члены кроме какого-либо одного кратны m, то и этот последний член кратен m.

Действительно, пусть таким членом будет a. Имеем:

$$b=b_1m;\ c=c_1m;\ldots;\ l=l_1m;\ r=r_1m;\ s=s_1m;\ldots;\ u=u_1m;$$

$$a=r+s+\ldots+u-b-\ldots-l=(r_1+s_1+\ldots+ \\ +u_1-b_1-\ldots-l_1)m,$$

что и доказывает теорему.

§ 2. Общий наибольший делитель двух чисел.

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 $(a, b,\ldots,l)$. 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* (В случае двух чисел понятия „взаимно простые“ и „попарно простые“ совпадают.)

Пример. $(6, 10, 15)=1$, поэтому числа 6, 10, 15 взаимно простые. Числа 10, 13, 21 не только взаимно простые, но и попарно простые: действительно $(10, 13)=(10, 21)=(13, 21)=1$.

b. Сначала займемся общим наибольшим делителем двух чисел. Здесь полезны два замечания.

Если a кратно b, то общие делители чисел a и b совпадают с делителями одного b. В частности $(a, b)=b$.

Действительно, всякий общий делитель чисел a и b в частности является делителем и одного b. Обратно, раз a кратно b, то (**c**, § 1) всякий делитель числа b является также делителем числа a, т. е. он будет общим делителем чисел b и a. Таким образом общие делители чисел a и b совпадают с делителями одного b, а так как наибольший делитель числа b есть само b, то $(a, b)=b$.

Если

$$a=bq+r$$

(r *здесь никакими неравенствами не ограничено*), *то общие делители чисел* a *и* b *совпадают с таковыми чисел* b *и* r. *В частности* $(a, b)=(b, r)$.

Действительно, вышенаписанное равенство показывает, что всякий общий делитель чисел a и b делит также и r (**d**, § **1**) и, следовательно, является общим делителем чисел b и r.

Обратно, то же равенство показывает, что всякий общий делитель чисел b и r делит и a и, следовательно, является общим делителем чисел a и b.

Таким образом общие делители чисел a и b совпадают с общими делителями чисел b и r.

В частности должны совпадать и наибольшие из этих делителей, т. е. $(a, b)=(b, r)$.

c. Общий наибольший делитель двух чисел можно находить применяя *алгоритм Эвклида*. Последний состоит в нижеследующем. Пусть a и b — положительные целые. Согласно **b**, § **1** имеем ряд равенств:

$$\begin{array}{rlr} a = bq + r_1; & 0<r_1<b; & \\ b = r_1q_1+r_2; & 0<r_2<r_1; & \text{(A)} \\ r_1 = r_2q_2+r_3; & 0<r_3<r_2; & \\ \ldots\ldots\ldots & & \\ r_{n-2} = r_{n-1}q_{n-1}+r_n; & 0<r_n<r_{n-1}; & \\ r_{n-1} = r_nq_n. & & \end{array}$$

Что этот ряд равенств действительно конечен, следует из того, что ряд $b, r_1, r_2, \ldots$ есть ряд убывающих неотрицательных целых. Закончиться последний ряд может только некоторым $r_{n+1}=0$, так как, получая $r_{n+1}>0$, мы наш алгоритм могли бы продолжать далее.

d. Рассматривая равенства (А) идя сверху вниз, убедимся (**b**), что общие делители чисел a и b одинаковы с таковыми чисел b и r_1, далее одинаковы с общими делителями чисел r_1 и r_2, чисел r_2 и $r_3, \ldots$, чисел r_{n-1} и r_n, наконец, с делителями одного числа r_n.

Одновременно с этим имеем:

$$(a, b)=(b, r_1)=(r_1, r_2)=\cdots=(r_{n-1}, r_n)=r_n.$$

Из вышеизложенных рассуждений заключаем, что:

1. *Общий наибольший делитель чисел* a *и* b *равен* r_n, *т. е. последнему неравному нулю остатку алгоритма Эвклида.*

2. *Общие делители чисел* a *и* b *совпадают с делителями их общего наибольшего делителя.*

3. *Общие делители чисел* a и b *делят все* $r_1, r_2, \ldots, r_{n-1}$.

Пример. Применим алгоритм Эвклида к отысканию (546, 231). Имеем:

$$
\begin{array}{r|l}
546 & 231 \\
462 & 2 \\
\hline
231 & 84 \\
168 & 2 \\
\hline
84 & 63 \\
63 & 1 \\
\hline
63 & 21 \\
63 & 3 \\
\hline
\text{„} \;\; \text{„} &
\end{array}
$$

что можно также записать в форме:

$$
\begin{aligned}
546 &= 231 \cdot 2 + 84, \\
231 &= 84 \cdot 2 + 63, \\
84 &= 63 \cdot 1 + 21, \\
63 &= 21 \cdot 3.
\end{aligned}
$$

Мы видим, что последний неравный нулю остаток есть $r_3 = 21$, значит $(546, 231) = 21$.

e. *Если a и b разделим на какой-либо их общий делитель δ, то на δ разделится и их общий наибольший делитель.*

Если a и b умножим на какое-либо целое m, то на m умножится и их общий наибольший делитель.

Действительно, разделим равенства (A) почленно на δ. Получим равенства, где вместо $a, b, r_1, \ldots, r_n$ будут стоять новые целые (**d**, **3**):

$$\frac{a}{\delta}, \ \frac{b}{\delta}, \ \frac{r_1}{\delta}, \ldots, \frac{r_n}{\delta}$$

и таким образом

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

Аналогично путем почленного умножения на m всех равенств (A) докажем и вторую часть теоремы.

Из доказанного предложения вытекают очевидные следствия. Частные $\frac{a}{d}$ и $\frac{b}{d}$ от деления чисел a и b на их общий наибольший делитель взаимно просты.

Обратно, если частные $\frac{a}{d}$ и $\frac{b}{d}$ от деления чисел a и b на их общий делитель d взаимно просты, то d есть общий наибольший делитель этих чисел.

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

Действительно, тогда в равенствах (A) имеем $r_n = 1$. Умножая эти равенства кроме последнего на c, имеем:

$$
\begin{aligned}
ac &= bcq + r_1c, \\
bc &= rcq_1 + r_2c, \\
r_1c &= r_2cq_2 + r_3c, \\
&\cdots\cdots\cdots\cdots \\
r_{n-2}c &= r_{n-1}cq_{n-1} + c.
\end{aligned}
$$

Отсюда, идя сверху вниз, убеждаемся, что (ac, b) делит $r_1c, r_2c, \ldots$ и, наконец, c. Так как, кроме того, оно делит и b, то оно делит (c, b).

Обратно, очевидно, что (c, b) делит ac и b и, следовательно, (ac, b).

Таким образом (ac, b) и (c, b) взаимно делят друг друга и, следовательно, равны между собою.

Отсюда следствие:

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 (**b**, § **2**) имеем $(ac, b) = b$; значит, и $(c, b) = b$, т. е. c кратно b.

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

Действительно (f), имеем:

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

а тогда, полагая для краткости $a_1a_2\ldots a_m = A$, точно таким же путем найдем:

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

§ 3. Общий наибольший делитель любого количества чисел.

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

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

Число d_n и будет общим наибольшим делителем всех данных чисел.

Действительно (**d**, 2, § **2**), 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 таковыми 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 приведенное доказательство, видим, что и для общего наибольшего делителя более чем двух чисел верна теорема **d**, 2, § **2**. Верны также и теоремы **e**, § **2**, потому что от разделения на δ или умножения на m всех чисел $a_1, a_2, \ldots, a_n$ точно так же и все $d_2, d_3, \ldots, d_n$ разделятся на δ или умножатся на m.

§ 4. Общее наименьшее кратное.

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

b. Мы займемся сначала выяснением общего вида всех общих кратных двух целых. 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 переписать в виде:

$$\frac{a_1 k}{b_1},$$

где $(a_1, b_1) = 1$. Поэтому (следствие f, § 2) k должно делиться на b_1,

$$k = b_1 t = \frac{b}{d} t,$$

где t — целое, откуда

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

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

Наименьшее положительное из этих кратных получим при $t = 1$

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

оно, следовательно, и будет общим наименьшим кратным. Введя m, полученную для M, формулу можно переписать так:

$$M = mt.$$

Последнее и предпоследнее равенства приводят к теоремам:

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

Общее наименьшее кратное двух чисел равно их произведению, деленному 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 $m(a, b)$ общее наименьшее кратное чисел a и b, составим ряд чисел:

$$m(a_1, a_2) = m_2; \quad m(m_2, a_3) = m_3; \quad \ldots; \quad m(m_{n-1}, a_n) = m_n.$$

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

Действительно (предпоследняя теорема b), общие кратные чисел a_1 и a_2 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 приведенное доказательство, видим, что и для общего наименьшего кратного верна предпоследняя теорема b. Кроме того, убеждаемся в справедливости следующей теоремы:

Общее наименьшее кратное чисел попарно простых равно их произведению.

§ 5. Связь алгоритма Эвклида с непрерывными дробями.

a. Пусть $\alpha > 0$. Обозначая буквою q наибольшее целое, меньшее или равное α, имеем:

$$\alpha = q + x = q + \frac{1}{\alpha_1}; \qquad \alpha_1 > 1.$$

Точно так же находим:

$$\alpha_1 = q_1 + x_1 = q_1 + \frac{1}{\alpha_2}; \qquad \alpha_2 > 1,$$

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

$$\alpha_{n-1} = q_{n-1} + x_{n-1} = q_{n-1} + \frac{1}{\alpha_n}; \qquad \alpha_n > 1,$$

$$\alpha_n = q_n + x_n,$$

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

$$\alpha = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n + x_n}}}.$$

Это разложение естественно закончится, если придем к некоторому $x_n = 0$, что, как увидим дальше, всегда будет при рациональном α и, очевидно, никогда не закончится при иррациональном α. В этом последнем случае число чисел $q, q_1, q_2, \ldots,$ будет беспредельно велико.

Числа $q, q_1, q_2, \ldots,$ называются неполными частными: дроби же

$$\delta_1 = q; \quad \delta_2 = q + \frac{1}{q_1}; \quad \delta_3 = q + \cfrac{1}{q_1 + \cfrac{1}{q_2}}; \ldots$$

называются *подходящими дробями*.

b. Нетрудно показать, что подходящие дроби с нечетными номерами меньше или равны α, а дроби с четными номерами $\geqslant \alpha$ (знак $=$ возможен только при рациональном α).

Действительно, δ_n получается отбрасыванием x_{n-1} в равенстве

$$\alpha = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{n-3} + \cfrac{1}{q_{n-2} + \cfrac{1}{q_{n-1} + x_{n-1}}}}}};$$

но от такого отбрасывания

$$\begin{aligned} &q_{n-1} + x_{n-1} \text{ уменьшится,} \\ &q_{n-2} + x_{n-2} \text{ увеличится,} \\ &q_{n-3} + x_{n-3} \text{ уменьшится,} \\ &\dots\dots\dots\dots\dots \end{aligned}$$

$$q + x = \alpha \begin{cases} \text{при } n \text{ нечетном уменьшится,} \\ \text{,, } n \text{ четном увеличится.} \end{cases}$$

Последнее и доказывает наше утверждение.

c. В частности убеждаемся, *что α ограничено любыми двумя соседними подходящими дробями*:

$$\delta_s, \ \delta_{s+1}$$

(одно из чисел s, $s+1$ четное, другое нечетное).

d. Закон образования подходящих дробей легко найдем, замечая, что δ_{s+1} $(s>0)$ получается из δ_s заменой в буквенном выражении для δ_s числа q_{s-1} на

$$q_{s-1} + \frac{1}{q_s}.$$

Действительно, вводя в рассмотрение несуществующую подходящую дробь

$$\delta_0 = \frac{1}{0},$$

мы можем подходящие дроби последовательно представить в следующем виде $\left(\text{здесь равенство } \frac{A}{B} = \frac{P_s}{Q_s} \text{ обозначает } A = P_s;\ B = Q_s\right)$:

$$\delta_0 = \frac{1}{0} = \frac{P_0}{Q_0}; \qquad \delta_1 = \frac{q}{1} = \frac{P_1}{Q_1},$$

$$\delta_2 = q + \frac{1}{q_1} = \frac{qq_1 + 1}{1 \cdot q_1 + 0} = \frac{P_1 q_1 + P_0}{Q_1 q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{P_1\left(q_1 + \frac{1}{q_2}\right) + P_0}{Q_1\left(q_1 + \frac{1}{q_2}\right) + Q_0} = \frac{(P_1 q_1 + P_0)\, q_2 + P_1}{(Q_1 q_1 + Q_0)\, q_2 + Q_1} =$$

$$= \frac{P_2 q_2 + P_1}{Q_2 q_2 + Q_1} = \frac{P_3}{Q_3}$$

и т. д. и вообще

$$\delta_{s+1} = \frac{P_s q_s + P_{s-1}}{Q_s q_s + Q_{s-1}} = \frac{P_{s+1}}{Q_{s+1}}. \qquad (1)$$

e. Основываясь на последнем равенстве, легко установим простое *выражение разности* $\delta_s - \delta_{s-1}$ *соседних подходящих дробей.* Действительно,

$$\delta_s - \delta_{s+1} = \frac{P_s}{Q_s} - \frac{P_{s+1}}{Q_{s+1}} = \frac{\varepsilon_s}{Q_s Q_{s+1}}; \quad \varepsilon_s = P_s Q_{s+1} - Q_s P_{s+1}. \qquad (2)$$

Ввиду (1) имеем далее:

$$\varepsilon_s = P_s(Q_s q_s + Q_{s-1}) - Q_s(P_s q_s + P_{s-1}) =$$
$$= -(P_{s-1}Q_s - Q_{s-1}P_s) = -\varepsilon_{s-1},$$

т. е. $\varepsilon_s = -\varepsilon_{s-1}$; но

$$\varepsilon_0 = 1 \cdot 1 - 0 \cdot q = 1,$$

следовательно, ряд $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots$ *совпадает с рядом* $1, -1, +1, \ldots$

f. Принимая во внимание равенство, определяющее ε_s, и полученный результат, убеждаемся, что $(P_s, Q_s) = 1$.

g. Из **c** и (2) выводим:

$$|\alpha - \delta_s| \leqslant \frac{1}{Q_s Q_{s+1}}.$$

h. Если α — рациональная несократимая дробь

$$\alpha = \frac{a}{b},$$

то разложение этой дроби в непрерывную тесно связано с алгоритмом Эвклида. Действительно, имеем:

$$a = bq + r_1, \quad \frac{a}{b} = q + \frac{r_1}{b},$$
$$b = r_1 q_1 + r_2, \quad \frac{b}{r_1} = q_1 + \frac{r_2}{r_1},$$
$$r_1 = r_2 q_2 + r_3, \quad \frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}},$$
$$r_{n-1} = r_n q_n, \quad \frac{r_{n-1}}{r_n} = q_n,$$

откуда

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n}}};$$

в этом случае

$$\delta_{n+1} = \frac{P_{n+1}}{Q_{n+1}} = \frac{a}{b},$$