Д. Ф. Егоров

Элементы теории чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Д11

Д. Ф. Егоров
Д11 Элементы теории чисел / Д. Ф. Егоров – М.: Книга по Требованию, 2012. – 202 с.

ISBN 978-5-458-26215-6

Предлагаемая книга имеет в своей основе курс лекций по теории чисел, которые автор 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.

ISBN 978-5-458-26215-6

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

$$-m = q \cdot (-n) = (-q) \cdot n$$

и

$$m = (-q) \cdot (-n)$$

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

$$n,\ n+n,\ n+n+n,\ \ldots.$$
$$0,\ -n,\ -n-n,\ -n-n-n,\ \ldots.$$

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

$$0,\ \pm 2,\ \pm 4,\ \pm 6,\ \ldots.$$

есть модуль.

Совокупность всех чисел

$$\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots.$$

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: $0, \pm 1, \pm 2, \pm 3, \cdots$. 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