П. Г. Дирихле

Лекции по теории чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
П11

П. Г. Дирихле
П11 Лекции по теории чисел / П. Г. Дирихле – М.: Книга по Требованию, 2014. – 404 с.

ISBN 978-5-458-26214-9

Настоящая книга, написанная выдающимся немецким математиком П. Г. Лежен Дирихле, принадлежит к числу лучших классических книг по теории чисел. Составленная Р. Дедекиндом по лекциям Дирихле, прочитанным в 1856-1857 годах, она до сих пор не потеряла своего актуального значения. Все желающие получить серьезную математическую подготовку и в настоящее время не могут пройти мимо этой замечательной книги. В ней содержатся основные результаты теории квадратичных форм, которые К. Гаусс изложил в своем знаменитом сочинении «Исследования по арифметике», и дано систематическое изложение исследований самого Дирихле. Эти исследования принадлежат к наиболее глубоким результатам математики XIX века и служат основанием современной теории чисел.

ISBN 978-5-458-26214-9

СОДЕРЖАНИЕ.

Глава первая.

О ДЕЛИМОСТИ ЧИСЕЛ.

Глава вторая.

О СРАВНЕНИЯХ.

ГЛАВА ТРЕТЬЯ.

О КВАДРАТИЧНЫХ ВЫЧЕТАХ.

ГЛАВА ЧЕТВЕРТАЯ.

О КВАДРАТИЧНЫХ ФОРМАХ.

Глава пятая.

ОПРЕДЕЛЕНИЕ ЧИСЛА КЛАССОВ, НА КОТОРЫЕ РАСПАДАЮТСЯ БИНАРНЫЕ КВАДРАТИЧНЫЕ ФОРМЫ С ЗАДАННЫМ ДЕТЕРМИНАНТОМ.

стр.

ДОПОЛНЕНИЯ.

Глава первая.

О ДЕЛИМОСТИ ЧИСЕЛ.

§ 1.

Мы рассмотрим в этой главе некоторые арифметические теоремы, которые хотя и встречаются в большинстве учебников, однако имеют столь важное значение в теории чисел, что строгое обоснование их является безусловно необходимым. Сюда относится прежде всего теорема, в силу которой произведение нескольких целых положительных чисел не зависит от порядка, в котором мы производим умножение. Рассмотрим сначала тот случай, когда даны *три* числа a, b, c, и составим таблицу

$$\begin{array}{llll} c, & c, & c, & c, \\ c, & c, & c, & c, \\ c, & c, & c, & c, \end{array} \qquad c$$
$$c \qquad c$$
$$c \qquad c$$

$$\begin{array}{llll} c, & c, & c, & c, \end{array} \qquad c,$$

которая состоит из b горизонтальных рядов, каждый из которых содержит a раз число c. Теперь определим сумму всех чисел, входящих в эту таблицу. При этом мы рассуждаем так: число c входит a раз в каждый горизонтальный ряд, следовательно, сумма всех чисел этого ряда равна ca, причем мы *множимое* c ставим впереди *множителя* a. Так как число таких горизонтальных рядов равно b, то сумма всех чисел таблицы равна $(ca)b$, где ca — множимое, b — множитель. Но мы можем определить ту же самую сумму другим способом, замечая, что данная таблица состоит из a вертикальных рядов, а каждый из этих рядов содержит b раз число c. Поэтому сумма чисел каждого вертикального ряда равна cb, а следовательно, сумма всех чисел таблицы равна $(cb)a$. Значит,

$$(ca)\,b = (cb)\,a.$$

Полагая здесь произвольное число c равным единице, приходим к такому следствию:

$$ab = ba,$$

т. е. *при умножении двух целых положительных чисел множимое можно заменить множителем и обратно.* По этой причине исчезает различие между названиями „множимое“ и „множитель“, и они оба называются *сомножителями.*

Мы можем, наконец, определить сумму всех чисел таблицы еще третьим способом, сосчитывая, сколько раз число c содержится в этой сумме. Число c входит a раз в каждом горизонтальном ряду, таких рядов b, следовательно, число c содержится во всей сумме ab раз. Отсюда следует, что означенная сумма равна $c(ab)$, следовательно

$$(ca)\,b = (cb)\,a = c\,(ab).$$

Соединяя этот вывод с предыдущим, относящимся к произведению двух множителей, мы приходим к следующему предложению.

Если мы имеем три целых положительных числа и произведение двух каких-нибудь из них умножим на третье, то произведение имеет одну и ту же величину, как бы ни были выбраны первые два числа из данных трех чисел.

Так как величина произведения трех целых положительных чисел не зависит от порядка перемножения, то все эти числа безразлично называются сомножителями произведения.

§ 2.

На основании предыдущего нетрудно теперь показать, что та же самая теорема имеет место для какой угодно системы S целых положительных чисел

$$a,\ b,\ c,$$

Самый общий способ для перемножения этих чисел посредством выполнения каждый раз перемножения двух чисел состоит в следующем. Берем какие-нибудь два числа, принадлежащие системе S, и составляем их произведение; система чисел S', состоящая из этого произведения и остальных чисел системы S, содержит одним числом меньше, нежели система S.

Если мы опять перемножим два числа, принадлежащие системе S', не изменяя прочих чисел этой системы, то придем к системе S'', которая содержит двумя числами меньше, нежели первоначально данная. Продолжая таким образом далее, мы приходим к одному числу, и подлежащая доказательству теорема состоит в том, что *это число, получаемое в результате указанного процесса вычислений, остается одним и тем же, в каком бы порядке ни были произведены отдельные перемножения.*

Для доказательства мы воспользуемся способом полной индукции, т. е. допустим, что теорема имеет место для n множителей, и докажем, что в таком случае она справедлива и для $n+1$ множителей.

Возьмем систему S, состоящую из $n+1$ чисел

$$a,\ b,\ c,\ d,\ e,$$

Выберем два какие-нибудь числа, например a и b, и составим их произведение ab. Тогда образуется числовая система, содержащая n чисел:

$$ab,\ c,\ d,\ e,$$

и, следовательно, конечный результат, согласно нашему предположению, не зависит от порядка выполнения отдельных перемножений. При другом

порядке перемножения можно было бы ожидать другого результата только тогда, когда первая пара чисел отличалась бы от a, b, причем надо различать два случая.

Во-первых, может случиться, что при новом расположении системы *одно* из двух чисел a, b, например a, сочетается с одним из остальных чисел c, d, e, ..., например с c, так что новая система содержит n чисел

$$ac,\ b,\ d,\ e,$$

Так как расположение чисел прежней и новой систем не оказывает никакого влияния на окончательный результат, то мы первую систему чисел располагаем так, что числа ab и c стоят рядом, а вторую — так, что числа ac и b стоят рядом. Таким образом в первом случае имеем систему

$$(ab)\,c,\ d,\ e,$$

а во втором

$$(ac)\,b,\ d,\ e,$$

Так как, в силу доказанного в предыдущем параграфе, произведения $(ab)\,c$ и $(ac)\,b$ равны, то обе системы чисел тождественны, и окончательный результат перемножения будет один и тот же для обеих систем, из которых каждая содержит $n-1$ чисел.

Во-вторых, может случиться, что при новом расположении системы не будет взято *ни одно* из чисел a, b, а два из остальных чисел, например c, d, так что имеем систему чисел

$$a,\ b,\ cd,\ e,$$

Теперь мы можем как в новой системе, так и в данной производить перемножение в каком угодно порядке. Поэтому мы соединяем в данной системе числа c, d, а в новой — числа a, b и получаем следующую систему $n-1$ чисел:

$$ab,\ cd,\ e,\ \ldots$$

Для обеих систем, следовательно, окончательный результат один и тот же, а потому теорема доказана вообще.

В самом деле, на основании предыдущего параграфа теорема справедлива для трех чисел; значит, она имеет место и для четырех, пяти, шести и т. д. чисел. Результат перемножения называется произведением данных чисел, а эти последние — сомножителями произведения и ставятся одно возле другого в произвольном порядке.

Только что доказанную теорему можно применять и тогда, когда при перемножении какого угодно числа сомножителей мы соединяем эти сомножители в группы и находим произведения чисел, входящих в каждую из этих групп. Эти последние произведения, будучи перемножены, дают результат, тождественный с произведением всех данных чисел. Это следует из того, что подобный порядок перемножения соответствует одному из возможных способов расположения данных сомножителей, например

$$abcde = (ab)\,c\,(de) = (abcd)\,e = (abe)\,(cd).$$

Нетрудно распространить эту теорему и на тот случай, когда между сомножителями встречается какое угодно число *отрицательных* чисел; знак произведения будет положительный или отрицательный, смотря по тому, будет ли число отрицательных сомножителей четное или нечетное. Наконец, нужно иметь в виду, что и целое число *нуль* может быть сомножителем. В этом случае произведение всегда равно нулю.

§ 3.

Когда число a [1]) есть произведение двух чисел b и m, так что $a = mb$, то a называется *кратным* b. Вместо этого говорят также, что a *делится* на b, или b есть *делитель* a, или, наконец, b *входит множителем* в a. Все эти термины одинаково употребительны, и так как в теории чисел очень часто приходится обозначать подобную зависимость между двумя числами, то весьма удобно иметь для этой цели несколько различных терминов. Из определения кратных чисел вытекают следующие положения, которыми впоследствии придется часто пользоваться.

1. Если a — кратное b, b — кратное c, то и a — кратное c.

В самом деле, по предположению $a = mb$, $b = nc$, где m и n — какие-то целые числа; следовательно, $a = m(nc) = (mn)c$ и a делится на c.

И вообще, если в ряду чисел каждое делится на следующее за ним, то каждое число есть кратное всех последующих чисел.

2. Если числа a и b — кратные числа c, то их сумма и разность также кратные числа c. Действительно, из того, что $a = mc$, $b = nc$, следует, что $a \pm b = (m \pm n)c$.

§ 4.

В учении о делимости чисел весьма важное значение имеет следующий вопрос [2]).

Даны два целых положительных числа a и b; требуется найти общие делители этих чисел, т. е. такие числа δ, которые делят одновременно a и b.

Мы можем допустить, что a больше или, по крайней мере, не меньше b. Пусть a от деления на b дает в частном m и в остатке c, причем c меньше b, следовательно

$$a = mb + c.$$

Положим, что δ делит a и b, тогда это же число δ делит и c. В самом деле, a и b являются кратными δ, следовательно (§ 3), и mb и $a - mb = c$ — также кратные δ. Отсюда мы заключаем, что всякий общий делитель чисел a и b есть также общий делитель b и c. Обратно, если δ есть общий делитель чисел b, c, то тогда mb и $a = mb + c$ также делятся на δ, следовательно, всякий общий делитель чисел b и c есть в то же время общий делитель чисел a и b. Значит, общие делители чисел a и b вполне совпадают с общими делителями чисел b и c, и нахождение общих делителей первой пары чисел сводится к нахождению

[1]) Под словом *число* мы всегда будем подразумевать *целое* число.

[2]) „*Начала*“ Евклида, книга VII, теорема 2.