

П. Г. Дирихле

Лекции по теории чисел

**Москва
«Книга по Требованию»**

УДК 51
ББК 22.1
П11

П11 **П. Г. Дирихле**
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

© Издание на русском языке, оформление
«YOYO Media», 2014

© Издание на русском языке, оцифровка,
«Книга по Требованию», 2014

Эта книга является репринтом оригинала, который мы создали специально для Вас, используя запатентованные технологии производства репринтных книг и печати по требованию.

Сначала мы отсканировали каждую страницу оригинала этой редкой книги на профессиональном оборудовании. Затем с помощью специально разработанных программ мы произвели очистку изображения от пятен, клякс, перегибов и попытались отбелить и выровнять каждую страницу книги. К сожалению, некоторые страницы нельзя вернуть в изначальное состояние, и если их было трудно читать в оригинале, то даже при цифровой реставрации их невозможно улучшить.

Разумеется, автоматизированная программная обработка репринтных книг – не самое лучшее решение для восстановления текста в его первоизданном виде, однако, наша цель – вернуть читателю точную копию книги, которой может быть несколько веков.

Поэтому мы предупреждаем о возможных погрешностях восстановленного репринтного издания. В издании могут отсутствовать одна или несколько страниц текста, могут встретиться невыводимые пятна и кляксы, надписи на полях или подчеркивания в тексте, нечитаемые фрагменты текста или загибы страниц. Покупать или не покупать подобные издания – решать Вам, мы же делаем все возможное, чтобы редкие и ценные книги, еще недавно утраченные и несправедливо забытые, вновь стали доступными для всех читателей.



Серия Книжный Ренессанс

www.samizday.ru/reprint

СОДЕРЖАНИЕ.

ГЛАВА ПЕРВАЯ.

О ДЕЛИМОСТИ ЧИСЕЛ.

	стр.
1. Произведение двух или трех множителей не зависит от порядка, в котором производится умножение . . .	13
2. Произведение любого числа множителей . . .	14
3. Понятие о делимости одного числа на другое . . .	16
4. Общий наибольший делитель двух чисел . . .	16
5. Числа взаимно простые	18
6. Общий наибольший делитель нескольких чисел	19
7. Наименьшее кратное нескольких чисел	20
8. Числа простые и составные; разложение составных чисел на простые множители. Число и сумма простых чисел бесконечно велико	20
9. Нахождение всех делителей числа, если известны все его простые множители. Число и сумма этих делителей	23
10. Нахождение общего наибольшего делителя и общего наименьшего кратного нескольких чисел, если даны разложения этих чисел на простые множители	25
11. Определение числа $\varphi(m)$, которое показывает, сколько существует чисел в ряду $1, 2, 3, \dots, m$, взаимно простых с m	26
12. Доказательство теоремы $\varphi(mm') = \varphi(m) \cdot \varphi(m')$, если m и m' — числа взаимно простые	28
13. Доказательство теоремы $\sum \varphi(n) = m$, где знак суммы относится ко всем делителям n числа m	29
14. Другое доказательство той же теоремы	31
15. Определение высшей степени простого числа, входящей в произведение $1 \cdot 2 \cdot 3 \cdot \dots \cdot m$. Следствия	31
16. Общее заключение	34

ГЛАВА ВТОРАЯ.

О СРАВНЕНИЯХ.

17. Понятие о сравнимости двух чисел по отношению к третьему. Простейшие свойства сравнений	36
18. Полная система вычетов по отношению к данному модулю	39
19. Доказательство обобщенной теоремы Ферма	40
20. Другое доказательство той же теоремы	42
21. Сравнения, содержащие неизвестные величины; степень таких сравнений	44
22. Сравнения первой степени с одним неизвестным; условие их возможности; первый способ решения таких сравнений	46
23. Об алгоритме Эйлера	47
24. Второй способ решения сравнений первой степени с одним неизвестным	51
25. Решение задачи: найти все числа, которые при делении на данные числа дают данные остатки	51
26. Сравнение с одним неизвестным при простом модуле не может иметь несравнимых корней более, нежели единиц в его степени	56
27. Вывод теоремы Вильсона из теоремы Ферма	59

	стр.
§ 28. Степенные вычеты; показатель, к которому принадлежит данное число	60
§ 29. Если p — число простое и δ — делитель $p - 1$, то к показателю δ принадлежит $\varphi(\delta)$ чисел, не сравнимых по модулю p	62
§ 30. Первообразные корни простого числа. Индексы. Третий способ решения сравнений первой степени	64
§ 31. Двучленные сравнения, модуль которых простое число. Условие их возможности; число корней	68

ГЛАВА ТРЕТЬЯ.

О КВАДРАТИЧНЫХ ВЫЧЕТАХ.

§ 32. Квадратичные вычеты и невычеты	71
§ 33. Если модуль p — число простое и нечетное, то совокупность чисел, не делящихся на p , распадается на одинаковое число вычетов и невычетов. Характер произведения нескольких множителей. Символ Лежандра	71
§ 34. Элементарное доказательство предыдущей теоремы, а также теорем Ферма и Вильсона	74
§ 35. Случай, когда модуль есть степень простого нечетного числа	75
§ 36. Случай, когда модуль есть степень двух	77
§ 37. Случай, когда модуль есть какое угодно число	80
§ 38. Обобщенная теорема Вильсона	82
§ 39. Приведение задачи нахождения всех модулей, для которых данное число есть квадратичный вычет, к трем случаям	83
§ 40. Число -1 есть квадратичный вычет всех простых чисел вида $4n + 1$ и невычет всех простых чисел вида $4n + 3$	84
§ 41. Число 2 есть квадратичный вычет всех простых чисел вида $8n + 1$ и $8n + 7$ и невычет всех простых чисел вида $8n + 3$ и $8n + 5$	85
§ 42. Закон взаимности	87
§ 43. Первая часть доказательства этого закона; видоизменение предыдущего критерия для определения характера данного числа. Новое доказательство теоремы для числа 2	89
§ 44. Вторая часть доказательства	92
§ 45. Применение закона взаимности к решению задачи определения характера заданного числа по отношению к данному простому числу	95
§ 46. Символ Якоби как обобщение символа Лежандра. Обобщенный закон взаимности	96
§ 47. Применение этого закона к определению значения символа Якоби	101
§ 48. Второе доказательство закона взаимности; предварительные замечания	103
§ 49. Первая часть доказательства	104
§ 50. Лемма: если q есть простое число вида $8n + 1$, то существует по крайней мере одно простое нечетное число, меньшее $2\sqrt{q} + 1$, по отношению к которому q есть квадратичный невычет	106
§ 51. Вторая часть доказательства закона взаимности	107
§ 52. Определение линейных форм, в которых содержатся все простые числа, по отношению к которым данное число есть квадратичный вычет или невычет	111

ГЛАВА ЧЕТВЕРТАЯ.

О КВАДРАТИЧНЫХ ФОРМАХ.

§ 53. Бинарные квадратичные формы; их коэффициенты и переменные; их детерминант. Исключение форм, детерминант которых является точным квадратом	117
§ 54. Преобразование форм. Собственные и несобственные подстановки	118

	стр.
§ 55. Соединенные подстановки	120
§ 56. Собственная и несобственная эквивалентность форм	122
§ 57. Формы, не собственно эквивалентные самим себе	124
§ 58. Двусторонние формы. Каждая форма, несобственно эквивалентная самой себе, эквивалентна некоторой двусторонней форме	126
§ 59. Распределение всех форм с определенным детерминантом по классам; полная система неэквивалентных форм. Две основные проблемы учения об эквивалентности	128
§ 60. Собственное представление чисел посредством квадратичных форм; корни сравнений, к которым принадлежат представления. Сведение к двум основным проблемам	129
§ 61. Приведение второй проблемы: из одной заданной подстановки, посредством которой форма переходит в эквивалентную ей форму, найти все подобные подстановки,—к случаю, в котором обе формы тождественны. Делители форм и классов	132
§ 62. Приведение проблемы: найти все подстановки, посредством которых форма переходит сама в себя,—к задаче полного разрешения уравнения Пелля. Решение этого уравнения для случая отрицательного детерминанта	135
§ 63. Постановка первой проблемы в учении об эквивалентности: решить, эквивалентны ли две формы одинакового детерминанта или нет, и в первом случае найти подстановку, посредством которой одна из обеих форм переходит в другую. Соседние формы	137
§ 64. Отрицательные детерминанты. Положительные формы. Приведенные формы. Каждая форма эквивалентна некоторой приведенной форме	138
§ 65. Исключительные случаи, когда две нетождественные приведенные формы эквивалентны	141
§ 66. Эквивалентность или неэквивалентность двух форм одинакового отрицательного детерминанта узнается путем сравнения их с приведенными формами	143
§ 67. Число классов форм для отрицательного детерминанта конечно	144
§ 68. Разложение чисел на сумму двух точных квадратов	147
§ 69. Разложение чисел на сумму точного квадрата и удвоенного точного квадрата	149
§ 70. Представление чисел посредством форм $x^2 + 3y^2$ и $2x^2 + 2xy + 2y^2$	150
§ 71. Представление чисел посредством форм $x^2 + 5y^2$ и $2x^2 + 2xy + 3y^2$	153
§ 72. Положительные детерминанты. Первый и второй корни формы	154
§ 73. Соотношения между одноименными или разноименными корнями двух собственно или несобственно эквивалентных форм. Соседние формы	155
§ 74. Приведенные формы с положительным детерминантом; свойства их корней	157
§ 75. Существует лишь конечное число приведенных форм с данным положительным детерминантом	159
§ 76. Каждая форма с положительным детерминантом эквивалентна некоторой приведенной форме	161
§ 77. Каждая приведенная форма с положительным детерминантом имеет одну и только одну соседнюю справа приведенную форму и точно так же одну и только одну соседнюю слева приведенную форму	163
§ 78. Распределение приведенных форм с положительным детерминантом на периоды с одинаковым числом членов	165
§ 79. Разложение корней приведенных форм с положительным детерминантом в периодические непрерывные дроби	168
§ 80. Отступление, касающееся преобразования неправильных непрерывных дробей в правильные	171
§ 81. Лемма из теории непрерывных дробей	173
§ 82. Две любые эквивалентные приведенные формы с положительным детерминантом принадлежат к одному и тому же периоду. Окончание решения проблемы об эквивалентности двух форм с одинаковым положительным детерминантом	175

	стр.
§ 83. Решение уравнения Пелля в положительных числах для положительных детерминантов путем рассмотрения периодов приведенных форм	178
§ 84. Наименьшее положительное и решение уравнения Пелля	184
§ 85. Представление всех решений уравнения Пелля посредством его наименьшего положительного решения	185

Г л а в а п я т а я .

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

§ 86. Установление области чисел, которые могут быть собственно представлены посредством полной системы начальных форм первого или второго вида	189
§ 87. Число этих представлений в случае отрицательного детерминанта; в случае положительного детерминанта число представлений приводится к конечному посредством новых ограничений, налагаемых на представляющие числа	190
§ 88. Краткое обозрение. Два способа получения одной и той же области чисел. Фундаментальное уравнение	193
§ 89. Преобразование его правой части.	195
§ 90. Фундаментальное уравнение преобразуется так, что допускаются и несобственные представления	198
§ 91. Отступление, касающееся числа всех представлений некоторого числа посредством системы форм. Применение к разложению чисел на сумму двух точных квадратов	200
§ 92. Отступление, касающееся некоторых бесконечных рядов, встречающихся в теории эллиптических функций	203
§ 93. Ограничения, налагаемые на формы, являющиеся представителями классов форм	204
§ 94. Распределение пар представляющих чисел на определенное число двойных арифметических прогрессий	206
§ 95. Предельное значение левой части фундаментального уравнения в случае отрицательного детерминанта	209
§ 96. Выражение числа классов для отрицательного детерминанта в виде предельного значения некоторого бесконечного ряда	212
§ 97. Соотношение между числом классов форм первого вида и числом классов форм второго вида для отрицательного детерминанта	213
§ 98. Предельное значение левой части фундаментального уравнения в случае положительного детерминанта; выражение числа классов в виде предельного значения некоторого бесконечного ряда	214
§ 99. Соотношение между числом классов форм первого вида и числом классов форм второго вида для положительного детерминанта	218
§ 100. Приведение определения числа классов к случаю, когда детерминант не делится ни на какой квадрат	220
§ 101. Исследование сходимости и непрерывности подлежащих рассмотрению бесконечных рядов	223
§ 102. Особое рассмотрение первого главного случая, в котором детерминант имеет вид $4l + 1$	226
§ 103. Суммирование бесконечного ряда в этом случае	227
§ 104. Окончательный результат в этом случае	230
§ 105. Суммирование бесконечного ряда в остальных случаях	234
§ 106. Сводка формул, посредством которых определяется число классов.	240
§ 107. Рассмотрение формул, соответствующих положительным детерминантам; преобразование окончательного результата в случае $D \equiv 1 \pmod{4}$	242
§ 108. Преобразование в случае $D \equiv 3 \pmod{4}$	244
§ 109. Преобразование в случае $D \equiv 2 \pmod{8}$	246
§ 110. Преобразование в случае $D \equiv 6 \pmod{8}$	247

стр.

ДОПОЛНЕНИЯ.

I. О некоторых теоремах из гауссовой теории деления окружности.	
§ 111.	Лемма из теории рядов Фурье 251
§ 112.	Определение значения суммы $\varphi(h, n)$ в случае, когда $n \equiv 0 \pmod{4}$ и $h = 1$ 252
§ 113.	Общие теоремы относительно сумм $\varphi(h, n)$ 256
§ 114.	Определение $\varphi(1, n)$ 257
§ 115.	Определение $\varphi(h, n)$, когда n есть нечетное простое число; третье доказательство закона взаимности и теорем относительно характера чисел -1 и 2 259
§ 116.	Доказательство одной теоремы, использованной в § 103, 105 262
II. О предельном значении одного бесконечного ряда.	
§ 117.	Доказательство одной теоремы из теории гармонических рядов 266
§ 118.	Формулировка и истолкование более общего предложения 267
§ 119.	Его доказательство 268
III. Об одном геометрическом предложении.	
§ 120.	Соотношение между величиной площади плоской фигуры и числом точек числовой решетки, лежащих внутри этой фигуры 271
IV. О родах, на которые распадаются классы квадратичных форм с определенным детерминантом.	
§ 121.	Предложения относительно характера всех чисел, представимых посредством одной и той же квадратичной формы 272
§ 122.	Распределение квадратичных форм по родам 274
§ 123.	Доказательство того, что половине возможных полных характеров не соответствует действительно существующих форм 277
§ 124.	Вывод некоторого равенства между двумя произведениями из двух бесконечных рядов каждое 278
§ 125.	Доказательство того, что половине возможных полных характеров соответствуют действительно существующие роды и что каждый из этих родов содержит одинаковое число классов форм 280
§ 126.	Завершение этого доказательства 284
V. Теория степенных вычетов для составных модулей.	
§ 127.	Третье доказательство обобщенной теоремы Ферма (§ 19) 287
§ 128.	Доказательство существования первообразных корней для модуля, являющегося произвольной степенью нечетного простого числа 288
§ 129.	Теория индексов для таких модулей 291
§ 130.	Случай, когда модуль равен степени числа 2; индексы 292
§ 131.	Случай, когда модуль есть произвольное составное число; индексы 294
VI. Доказательство теоремы, что всякая бесконечная арифметическая прогрессия, первый член и разность которой суть целые числа, не имеющие общего множителя, содержит бесконечно много простых чисел.	
§ 132.	Доказательство одного общего равенства между некоторым бесконечным произведением и некоторым бесконечным рядом 296
§ 133.	Уточнение этого предложения; распределение рядов L по трем классам L_1, L_2, L_3 298
§ 134.	Предельные значения этих рядов 300
§ 135.	Доказательство того, что предельные значения рядов L_2 отличны от нуля; связь с теорией квадратичных форм 303

	стр.
§ 136. Доказательство того, что предельные значения рядов L_3 отличны от нуля	305
§ 137. Доказательство теоремы об арифметической прогрессии	308
VII. О некоторых предложениях из теории деления окружности.	
§ 138. Доказательство одного свойства выражения $\varphi(m)$	310
§ 139. Построение уравнения, корни которого являются первообразными корнями m -й степени из единицы; разложение левой части его на два множителя в случае, когда m есть нечетное число P , не делящееся ни на какой квадрат	313
§ 140. Вычисление коэффициентов этих множителей	316
VIII. Об уравнении Пелля.	
§ 141. Предложение о рациональных приближенных значениях для квадратного корня из положительного числа D , не являющегося квадратом	319
§ 142. Доказательство предложения, что уравнение $t^2 - Du^2 = 1$ всегда разрешимо в целых числах t, u , из которых последнее, u , отлично от нуля	321
IX. О сходимости и непрерывности некоторых бесконечных рядов.	
§ 143. Метод частного суммирования	323
§ 144. Свойства рядов Дирихле	327
X. О композиции бинарных квадратичных форм.	
§ 145. Лемма относительно сравнений второй степени	332
§ 146. Композиция двух согласных форм. Фундаментальная теорема	333
§ 147. Композиция двух или большего числа согласных классов	335
§ 148. Важнейшие частные случаи композиции	337
§ 149. Периоды и группы начальных классов первого вида	338
§ 150. Сравнение числа классов произвольного делителя с числом начальных классов первого вида	340
§ 151. Результат этого сравнения	342
§ 152. Композиция родов	347
§ 153. Число двусторонних начальных классов первого вида	349
§ 154. Четвертое доказательство закона взаимности	352
§ 155. О числе действительно существующих родов	355
§ 156. Получение всех решений уравнения $ax^2 + by^2 + cz^2 = 0$ из одного заданного	356
§ 157. Основная теорема о разрешимости этого уравнения	365
§ 158. Каждый класс главного рода получается посредством сдвигания	368

ПРИЛОЖЕНИЕ.

Геометрия бинарных квадратичных форм.

Б. Н. Делоне.

§ 1. Определения и некоторые общие теоремы о параллелепипедальных системах точек	370
§ 2. Давнейшие теоремы о параллелограмматической системе точек на плоскости	375
§ 3. Теория расположения точек параллелограмматической системы относительно некоторых заданных асимптот	380
§ 4. Теория положительных бинарных квадратичных форм	390
§ 5. Теория неопределенных бинарных квадратичных форм	395

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

$$\begin{array}{cccc} c, & c, & c, & c, & c \\ c, & c, & c, & c, & c \\ c, & c, & c, & c, & c \\ & & & & c, \end{array}$$

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, \dots , 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:

$$ab, cd, e, \dots$$

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.