



# ОГЛАВЛЕНИЕ

<b>Предисловие</b>	<b>5</b>
<b>Глава 1. Делимость</b>	<b>9</b>
Как работает умножение . . . . .	12
Десятичная система счисления . . . . .	16
Умножение в столбик . . . . .	19
Делимость чисел . . . . .	21
Признаки делимости . . . . .	24
Деление с остатком . . . . .	30
Критерии делимости . . . . .	40
Алгоритм Евклида . . . . .	45
Соотношение Безу . . . . .	50
Задачи на делимость . . . . .	53
<b>Глава 2. Простые числа</b>	<b>59</b>
Простые и составные числа . . . . .	62
Количество простых чисел . . . . .	65
Алгоритм проверки на простоту . . . . .	68
Решето Эратосфена . . . . .	70
Числа-близнецы . . . . .	77
Задачи о простых числах . . . . .	80
<b>Глава 3. Основная теорема арифметики</b>	<b>87</b>
Доказательство существования разложения . . . . .	93
Мир без основной теоремы арифметики . . . . .	94
Доказательство единственности разложения . . . . .	99

Другое доказательство единственности . . . . .	101
Мир чётных чисел . . . . .	104
Каноническое разложение на множители . . . . .	108
НОД и НОК . . . . .	110
Количество делителей у числа . . . . .	118
Задачи на основную теорему арифметики . . . . .	123
<b>Глава 4. Диофантовы уравнения</b>	<b>131</b>
Линейные диофантовы уравнения . . . . .	135
Как угадать решение . . . . .	138
Нелинейный диофант . . . . .	141
Принцип крайнего и метод спуска . . . . .	150
Другие уравнения в целых числах . . . . .	156
<b>Глава 5. Арифметика остатков</b>	<b>163</b>
Опять остатки . . . . .	166
Сравнение по модулю . . . . .	168
Свойства сравнения по модулю . . . . .	170
Задачи на нахождение остатка . . . . .	174
Опять про признаки делимости . . . . .	179
Задачи на доказательство делимости . . . . .	185
<b>Глава 6. Теоремы Ферма и Эйлера</b>	<b>197</b>
Задача про бусы . . . . .	199
Малая теорема Ферма . . . . .	202
Теорема Эйлера . . . . .	209
Теория чисел в криптографии . . . . .	214
<b>Небольшой задачник</b>	<b>223</b>
<b>Решения задач</b>	<b>227</b>
<b>Предметный указатель</b>	<b>299</b>

## ПРЕДИСЛОВИЕ

**В**сем привет! Меня зовут Борис Трушин, и я учитель математики. Я преподаю математику школьникам, студентам и учителям уже 25 лет, а последние семь лет веду довольно популярный YouTube-канал «Борис Трушин» по околошкольной математике.

Некоторые разделы и задачи из этой книги можно найти в виде видеороликов на моём канале. Специально для тех, кому проще воспринимать информацию через видео, я снабдил книгу QR-кодами со ссылками на соответствующие ролики.



Книга рассчитана на широкий круг читателей – от шестиклассников до людей, давно окончивших школу. В ней я собрал многолетний опыт преподавания теории чисел школьникам на уроках, кружках и факультативах. Книга позволяет познакомиться с теорией чисел и освоить азы этого интересного раздела математики без каких-либо предварительных знаний.

В этой книге я попытался, начав с базовых принципов работы с целыми числами, пройти путь до содержательных теорем, по дороге осваивая мно-

жество методов решения задач. А в конце вы даже узнаете одно из важных приложений теории чисел к «реальной жизни».

Плавное погружение в теорию чисел начнётся с самых азов: вы узнаете, откуда взялись свойства умножения и почему работает алгоритм деления в столбик. Затем освоите алгоритм Евклида, основную теорему арифметики, линейные диофантовы уравнения, арифметику остатков и при этом научитесь решать разнообразные «олимпиадные» задачи!

Некоторые разделы этой книги могут оказаться для вас сложными. Не расстраивайтесь, если не все доказательства будут вам понятны с первого раза. Некоторые сложные рассуждения можно пропустить при первом прочтении и вернуться к ним, когда будете готовы. Это никак не повлияет на общее понимание остального текста.

А если вы уже немного знакомы с теорией чисел, то некоторые разделы можете смело пропускать, останавливаясь лишь на задачах, которые вызовут у вас интерес. Задач же будет много – начиная от простых упражнений, заканчивая сложными многоходовыми заданиями.

Старайтесь самостоятельно решать все предложенные здесь задачи. Но не переживайте, если не всё сразу получается. Можно отложить задачу на пару дней, а потом подумать над ней ещё. В любом случае, у вас всегда будет возможность посмотреть подробное решение, которое можно найти для каждой задачи в конце книги.

Те, кто разберётся со всеми изложенными здесь фактами и методами, решит или хотя бы поймёт ре-

шения всех предложенных задач, уже будет понимать теорию чисел на достаточно высоком уровне. Кому-то для этого будет достаточно пары недель, а у кого-то может уйти и пара лет.

Приятного вам чтения!

**Post scriptum.** Хочу выразить слова благодарности всем тем, кто учил меня математике в школе и в вузе. Всё, что я умею в математике и знаю о её преподавании, – всё благодаря этим людям.

В первую очередь это мой отец, Трушин Виктор Борисович, без которого я никогда бы не узнал и не полюбил математику, и Петрович Александр Юрьевич – мой школьный учитель алгебры, который 30 лет назад познакомил меня с теорией чисел.

А также Терёшин Дмитрий Александрович, Карасёв Роман Николаевич, Подлипский Олег Константинович, Чубаров Игорь Андреевич, Балашов Максим Викторович, Курочкин Сергей Владимирович, Бесов Олег Владимирович, Половинкин Евгений Сергеевич и ещё пара десятков потрясающих учителей и преподавателей, у которых мне посчастливилось когда-то учиться.

Спасибо вам, без вас не было бы не только этой книги, но и меня как учителя математики!

Кроме того, мне хочется отдельно поблагодарить Константина Кнопа и Тагира Валеева за то, что они взялись первыми прочитать эту рукопись перед публикацией. Их предложения и советы помогли улучшить некоторые разделы этой книги.

29 января 2024 года  
Борис Трушин



ГЛАВА **1** ДЕЛИМОСТЬ

---





**Т**еория чисел – довольно специфический раздел математики. Вначале он смущает школьников и студентов тем, что нужно забыть про существование всех чисел, кроме целых. В теории чисел нет числа *полтора*. Там на вопрос: «Можно ли три яблока разделить поровну на двоих?» ответом будет: «Нельзя, потому что три не делится на два». В этом смысле единицу лучше воспринимать не как яблоко, а как камень – что-то атомарное, что дальше уже не делится.

Так что, да, забудьте на время про все числа, кроме целых. Более того, мы даже за рамки натуральных чисел редко будем выходить.

Напомню, что *натуральными* называются<sup>1</sup> числа, которые образуются при счёте:

1, 2, 3, 4, 5, ...

---

<sup>1</sup>В ряде математических дисциплин (особенно тех, которые находятся на стыке с информатикой и компьютерными науками) число 0 тоже считается натуральным, но мы будем придерживаться классического определения.

А *целыми* называются все натуральные числа, число 0 и все числа, противоположные натуральным:

$$-1, -2, -3, -4, -5, \dots$$

Прежде чем переходить к самому важному понятию теории чисел – делимости, давайте начнем с азов и вспомним, что такое умножение и какие у него есть свойства.

## КАК РАБОТАЕТ УМНОЖЕНИЕ

Из начальной школы мы знаем, как складывают числа, и понимаем, что если нам нужно сложить несколько одинаковых чисел, то компактнее это записывается через умножение:

$$3 + 3 + 3 + 3 + 3 = 3 \cdot 5.$$

То есть  $3 \cdot 5$  – это буквально три, взятое пять раз.

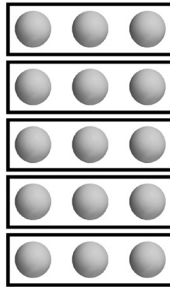
Так вот, у умножения есть ряд важных свойств, которые в школе называются *переместительным*, *сочетательным* и *распределительным* законами умножения. Давайте попробуем разобраться, откуда они взялись.

**Переместительный закон умножения**, или, как говорят математики, *коммутативность*, – это то самое правило, которое вы заучили в начальной школе как «от перемены мест множителей произведение не меняется».

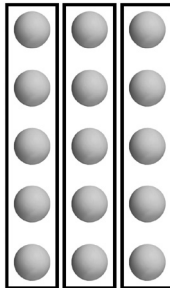
Но не все задумываются о том, почему это правило работает. Почему  $3 \cdot 5$  и  $5 \cdot 3$  – это одно и то же?

Почему  $3 + 3 + 3 + 3 + 3$  равно  $5 + 5 + 5$ ? Понятно, что можно вычислить каждую из сумм, и оба раза получить 15. Но как заранее понять, что получается одно и то же, не выполняя сложение?

Давайте рассуждать. Что такое  $3 \cdot 5$ ? Это три, взятое пять раз. Изобразим это в виде пяти наборов из трёх шаров:



Но количество получившихся шаров можно было посчитать и по-другому – сгруппировав их по пять:



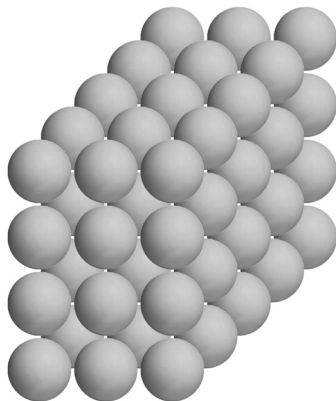
А это и означает, что пять, взятое три раза, – это то же самое, что три, взятое пять раз.

**Сочетательный закон умножения**, или *ассоциативность*, – это правило о том, что при умножении трёх множителей порядок умножения не влияет на результат.

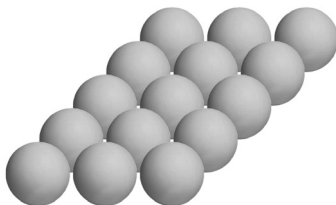
Давайте поймем, например, почему

$$(3 \cdot 5) \cdot 4 = 3 \cdot (5 \cdot 4).$$

Представим себе несколько шаров, сложенных в виде прямоугольного параллелепипеда размером  $3 \times 5 \times 4$ :



Сколько здесь шаров? С одной стороны, здесь четыре слоя,



в каждом из которых  $3 \cdot 5$  шаров. То есть здесь всего  $(3 \cdot 5) \cdot 4$  шаров.

Но, с другой стороны, все шары можно разбить на горизонтальные ряды.



А рядов таких всего  $5 \cdot 4$  штук. Поэтому общее число шаров – это  $5 \cdot 4$  раз по три шара, то есть  $3 \cdot (5 \cdot 4)$ .

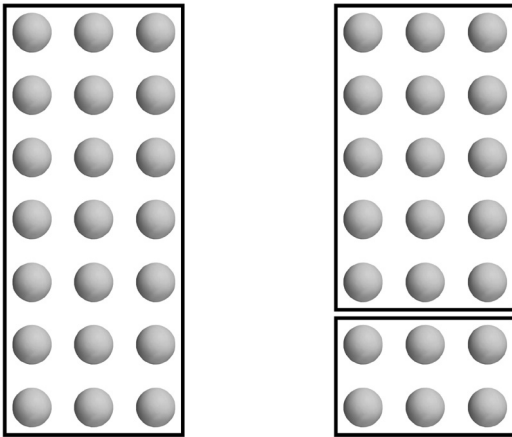
В итоге мы двумя способами посчитали одно и то же общее количество шаров. Значит,

$$(3 \cdot 5) \cdot 4 = 3 \cdot (5 \cdot 4).$$

**Распределительный закон умножения**, или *дистрибутивность*, – это то, что школьники называют правилом раскрытия скобок:

$$3 \cdot (5 + 2) = 3 \cdot 5 + 3 \cdot 2.$$

Давайте опять с помощью шаров поймем, почему, например,  $3 \cdot 7 = 3 \cdot 5 + 3 \cdot 2$ :



Вместо того чтобы сразу взять семь раз по три шара, можно взять пять раз по три, а потом ещё два раза по три. Вот и всё!

Этих трёх свойств достаточно, чтобы уметь делать все те преобразования выражений, которые вы учились делать в начальной школе.

Например, правило для раскрытия скобок в выражениях вида  $(a + b) \cdot (c + d)$  – «нужно каждое слага-

емое из первой скобки умножить на каждое слагаемое из второй и сложить результаты этих произведений» – следует из распределительного и переместительного законов:

$$(a + b) \cdot (c + d) = (a + b) \cdot c + (a + b) \cdot d;$$

(распределительный закон)

$$(a + b) \cdot c + (a + b) \cdot d = c \cdot (a + b) + d \cdot (a + b);$$

(переместительный закон)

$$c \cdot (a + b) + d \cdot (a + b) = (c \cdot a + c \cdot b) + (d \cdot a + d \cdot b);$$

(распределительный закон)

$$(c \cdot a + c \cdot b) + (d \cdot a + d \cdot b) = a \cdot c + b \cdot c + a \cdot d + b \cdot d.$$

(переместительный закон)

Но когда мы уже понимаем, как работает умножение и какие у него есть свойства, то можно сразу писать

$$(a + b) \cdot (c + d) = a \cdot c + b \cdot c + a \cdot d + b \cdot d.$$

Более того, обычно, для краткости записи, в буквенных выражениях знак умножения вообще не пишут:

$$(a + b)(c + d) = ac + bc + ad + bd.$$

Давайте потихоньку и к этому привыкать.

## ДЕСЯТИЧНАЯ СИСТЕМА СЧИСЛЕНИЯ

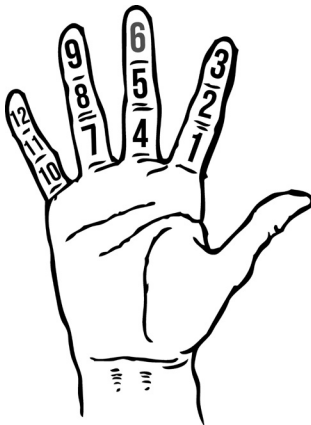
Тот способ записи чисел, к которому мы все привыкли с детства, называется *десятичной системой*

счисления. В ней для записи числа используется десять знаков: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, которые называются *арабскими цифрами*.

Считается, что количество цифр связано с количеством пальцев на руках у человека. Людям было удобно считать на пальцах десятками: досчитал до десяти – отложил камешек, ещё раз досчитал – отложил ещё один, и так далее. И если в результате подсчёта у тебя, например, пять отложенных камешков и семь загнутых пальцев, значит, ты досчитал до 57.

Когда камешков становится много, то заменяем десять камешков на большой камень. Теперь каждый большой камень символизирует десять десятков, то есть сотню. И так далее.

Но десятичная система не единственная, которую использовало человечество. У многих народов имела хождение *двенадцатеричная система*. Она возникла, когда люди считали предметы не загибая пальцы, а указывая большим пальцем руки на фаланги остальных четырёх пальцев той же руки.





Именно поэтому во многих языках сохранилось и используется до сих пор специальное слово «дюжина» – аналогичное слову «десяток» из десятичной системы.

Даже ещё в двадцатом веке в Англии применялась двенадцатеричная денежная система: один шиллинг был равен дюжине пенни. Более того, двенадцатеричная система до сих пор используется в английской системе мер. Так, например, один фут равен дюжине дюймов.

Не говоря уже о том, что циферблат часов разделён на 12 часов, а год – на 12 месяцев.

Свои отголоски в современном мире имеет и придуманная более четырёх тысяч лет назад шу-мерами *шестидесятеричная система счисления*, которая, по-видимому, являлась результатом наложения двух более древних систем счисления – двенадцатеричной и пятеричной.

Так, например, в одном часе шестьдесят минут, а в одной минуте – шестьдесят секунд. Более того, деление на минуты и секунды принято и при измерении углов – там тоже в одном градусе шестьдесят минут, а в одной минуте шестьдесят секунд. Например, угол в один радиан равен примерно  $57^{\circ}17'45''$  – 57 градусам 17 минутам и 45 секундам.

Но давайте вернёмся к привычной нам десятичной системе счисления. Вот есть, например, число

23 456.

За что отвечает каждая его цифра? В этом числе цифра 6 – это количество единиц, цифра 5 – количество десятков, цифра 4 – количество сотен, цифра 3 –

количество тысяч, а цифра 2 – десятков тысяч.

Иными словами,

$$\begin{aligned} 23\,456 &= 20\,000 + 3000 + 400 + 50 + 6 = \\ &= 2 \cdot 10\,000 + 3 \cdot 1000 + 4 \cdot 100 + 5 \cdot 10 + 6 = \\ &= 2 \cdot 10^4 + 3 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10 + 6. \end{aligned}$$

Именно поэтому числа, записанные в десятиричной системе, легко умножать на десять:

$$\begin{aligned} 23\,456 \cdot 10 &= (2 \cdot 10^4 + 3 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10 + 6) \cdot 10 = \\ &= 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 = \\ &= 234\,560. \end{aligned}$$

Благодаря этому важному свойству и распределительному закону умножения работает хорошо вам знакомый метод умножения в столбик.

## УМНОЖЕНИЕ В СТОЛБИК

Давайте вспомним метод умножения в столбик и наконец поймем, почему он работает. Пусть нам нужно, например, умножить 1234 на 23 456:

$$\begin{aligned} 1234 \cdot 23\,456 &= \\ &= 1234 \cdot (2 \cdot 10^4 + 3 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10 + 6) = \\ &= 1234 \cdot 6 + 1234 \cdot 5 \cdot 10 + 1234 \cdot 4 \cdot 10^2 + \\ &\quad + 1234 \cdot 3 \cdot 10^3 + 1234 \cdot 2 \cdot 10^4. \end{aligned}$$

А как посчитать, чему равно, например, произведение  $1234 \cdot 6$ ? Это же

$$\begin{aligned} (1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4) \cdot 6 &= \\ &= 4 \cdot 6 + 3 \cdot 6 \cdot 10 + 2 \cdot 6 \cdot 10^2 + 1 \cdot 6 \cdot 10^3 = \\ &= 24 + 180 + 1200 + 6000 = 7404. \end{aligned}$$

Аналогично получаем, что

$$\begin{aligned} 1234 \cdot 5 \cdot 10 &= 6170 \cdot 10; \\ 1234 \cdot 4 \cdot 10^2 &= 4936 \cdot 10^2; \\ 1234 \cdot 3 \cdot 10^3 &= 3702 \cdot 10^3; \\ 1234 \cdot 2 \cdot 10^4 &= 2468 \cdot 10^4. \end{aligned}$$

Поэтому

$$\begin{aligned} 1234 \cdot 23\,456 &= \\ &= 7404 + 61\,700 + 493\,600 + 3\,702\,000 + 24\,680\,000. \end{aligned}$$

Чтобы было проще складывать эти числа, их записывают так, чтобы соответствующие разряды оказались друг под другом:

					1	2	3	4	
					2	3	4	5	6
					<hr/>				
					7	4	0	4	
					6	1	7	0	0
					4	9	3	6	0
					3	7	0	2	0
					2	4	6	8	0
					<hr/>				
					2	8	9	4	4

Однако нули в конце промежуточных чисел, получившиеся из-за степеней десятки, обычно не

пишут, а записывают результаты умножения цифр второго числа на первое число «лесенкой»:

						1	2	3	4				
						2	3	4	5	6			
						<hr/>							
						7	4	0	4				
						6	1	7	0				
						4	9	3	6				
						3	7	0	2				
						2	4	6	8				
						<hr/>							
						2	8	9	4	4	7	0	4

Хотя это довольно часто приводит к ошибкам у школьников.

Вот так работает хорошо вам известный способ умножения в столбик. По сути, это многократно применённый распределительный закон умножения.

## ДЕЛИМОСТЬ ЧИСЕЛ

Вот мы, наконец, и добрались до понятия делимости.

Говорят, что целое число  $a$  *делится* на натуральное число  $b$ , если найдется такое целое число  $k$ , что  $a = kb$ . При этом говорят, что число  $b$  является *делителем* числа  $a$ , а число  $a$  *кратно* числу  $b$ .

Например, десять делится на пять, потому что  $10 = 2 \cdot 5$ . Но десять не делится на три, потому что