

МАТЕМАТИКА С БОРИСОМ ТРУШИНЫМ

ТЕОРИЯ ЧИСЕЛ:

С НУЛЯ
ДО ТЕОРЕМЫ
ЭЙЛЕРА



 **БОМБОРА**
ИЗДАТЕЛЬСТВО

МАТЕМАТИКА С БОРИСОМ ТРУШИНЫМ

ТЕОРИЯ ЧИСЕЛ:
С НУЛЯ ДО ТЕОРЕМЫ ЭЙЛЕРА

УДК 511
ББК 22.13
Т80

Трушин, Борис Викторович.

Т80 Математика с Борисом Трушиным. Теория чисел: с нуля до теоремы Эйлера / Борис Трушин. — Москва : Эксмо, 2024. — 304 с. — (Математика с Борисом Трушиным).

ISBN 978-5-04-179677-8

Борис Трушин почти 25 лет учит математике школьников и студентов, является соавтором школьных учебников по алгебре и уже 7 лет ведет одноименный YouTube-канал по околошкольной математике.

Вторая книга автора плавно погружает читателя в теорию чисел и позволяет освоить азы этого интересного раздела математики без каких-либо предварительных знаний. Задачи на теорию чисел часто встречаются на математических олимпиадах и ЕГЭ. Вы пройдете увлекательный путь с самых азов, поймете, откуда взялись свойства умножения и почему работает алгоритм деления в столбик, а закончите теоремой Эйлера.

УДК 511
ББК 22.13

ISBN 978-5-04-179677-8

© Борис Трушин, текст, 2024

© Оформление. ООО «Издательство «Эксмо», 2024

ОГЛАВЛЕНИЕ

Предисловие	5
Глава 1. Делимость	9
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
Глава 2. Простые числа	59
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
Глава 3. Основная теорема арифметики	87
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
Глава 4. Диофантовы уравнения	131
Линейные диофантовы уравнения	135
Как угадать решение	138
Нелинейный диофант	141
Принцип крайнего и метод спуска	150
Другие уравнения в целых числах	156
Глава 5. Арифметика остатков	163
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
Глава 6. Теоремы Ферма и Эйлера	197
Задача про бусы	199
Малая теорема Ферма	202
Теорема Эйлера	209
Теория чисел в криптографии	214
Небольшой задачник	223
Решения задач	227
Предметный указатель	299

ПРЕДИСЛОВИЕ

Всем 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 прочитывать эту рукопись перед публикацией. Их предложения и советы помогли улучшить некоторые разделы этой книги.

29 января 2024 года
Борис Трушин

ГЛАВА 1 ДЕЛИМОСТЬ

Теория 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* называются¹ числа, которые образуются при счёте:

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

¹В 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.

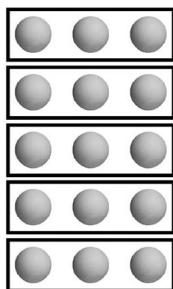
Так вот, у умножения есть ряд важных свойств, которые в школе называются *переместительным*, *сочетательным* и *распределительным* законами умножения. Давайте попробуем разобраться, откуда они взялись.

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».

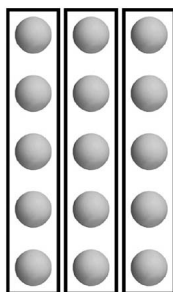
Но не все задумываются о том, почему это правило работает. Почему $3 \cdot 5$ и $5 \cdot 3$ – это одно и то же?

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:



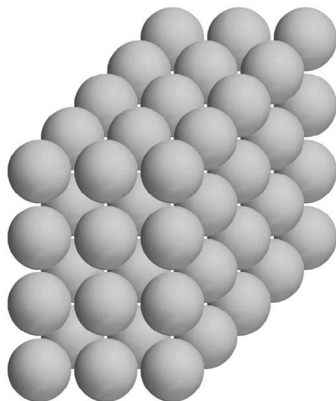
А это и означает, что пять, взятое три раза, – это то же самое, что три, взятое пять раз.

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

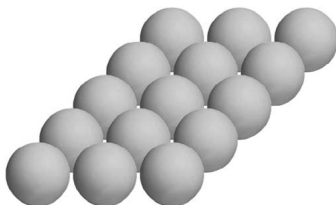
Давайте поймем, например, почему

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

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

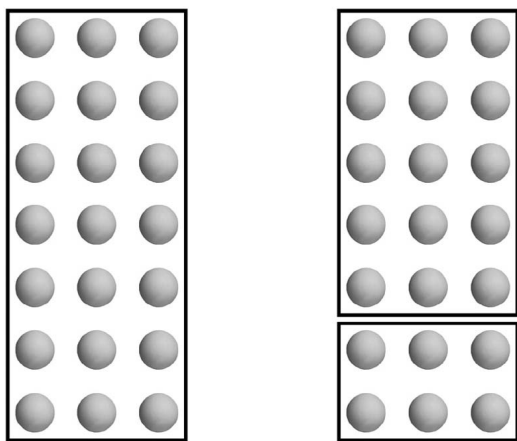
В итоге мы двумя способами посчитали одно и то же общее количество шаров. Значит,

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

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 десятичной 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	
					7	4	0	4	
				6	1	7	0	0	
			4	9	3	6	0	0	
		3	7	0	2	0	0	0	
	2	4	6	8	0	0	0	0	
2	8	9	4	4	7	0	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	
					7	4	0	4	
				6	1	7	0		
			4	9	3	6			
		3	7	0	2				
	2	4	6	8					
	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

$3 \cdot 3 = 9$ ещё меньше десяти, а $4 \cdot 3 = 12$ уже больше десяти.

Кратко факт делимости a на b записывают так: $a \div b$ (читается « a делится на b »)¹. Важно не путать записи $a : b$ и $a \div b$. Первая из них – это операция деления двух чисел, а вторая – это просто утверждение о том, что одно число делится на другое.

Важный частный случай делимости – это делимость на 2.

Числа, делящиеся на 2, называются *чётными*, а не делящиеся – *нечётными*.

Свойства делимости. У делимости есть несколько довольно очевидных свойств:

1. Ноль делится на любое натуральное число.
2. Любое натуральное число делится на 1 и само на себя.
3. Если натуральное число a делится на натуральное число b и при этом число b делится на a , то $a = b$.
4. Если $a_1 \div b$ и $a_2 \div b$, то $(a_1 + a_2) \div b$ и $(a_1 - a_2) \div b$.
5. Если $a \div b$, то для любого натурального числа c верно, что $ac \div b$ и $ac \div bc$.
6. Если $a \div b$, то и $(-a) \div b$.

¹В англоязычной литературе чаще пишут так: $b \mid a$ (читается « b делитель a »).

Доказательство. Каждое из этих свойств легко доказывается. Для доказательств большинства из них достаточно представлять себе делимость как возможность разбить набор шаров на кучки равных размеров (как мы это делали в начале главы). Но давайте учиться рассуждать более строго.

1. Для любого натурального числа b верно равенство $0 = 0 \cdot b$. Значит, ноль делится на b .
2. Для любого натурального числа a верны равенства $a = a \cdot 1$ и $a = 1 \cdot a$. Поэтому оно делится на 1 и само на себя.
3. Предположим, что $a \neq b$. Тогда, если a делится на b и $a \neq b$, то $a > b$. Но если $b < a$, то b не может делиться на a . Противоречие.
4. Если $a_1 \div b$ и $a_2 \div b$, то существуют такие целые k_1 и k_2 , что $a_1 = k_1 b$, $a_2 = k_2 b$. Тогда верны равенства:

$$a_1 + a_2 = k_1 b + k_2 b = (k_1 + k_2) \cdot b,$$

$$a_1 - a_2 = k_1 b - k_2 b = (k_1 - k_2) \cdot b.$$

Но сумма и разность целых чисел – тоже целые числа, поэтому $(k_1 + k_2)$ и $(k_1 - k_2)$ – целые, а значит, $(a_1 + a_2) \div b$ и $(a_1 - a_2) \div b$.

5. Если $a \div b$, то существует такое целое число k , что $a = kb$. Тогда для любого натурального числа c верно, что $ac = kbc$. Так как kc – целое число и $ac = (kc) \cdot b$, то $ac \div b$. Так как k – целое число и $ac = k \cdot (bc)$, то $ac \div bc$.
6. Если $a \div b$, то существует такое целое число k ,

что $a = kb$. Но тогда $(-a) = (-k) \cdot b$. Значит, $(-a) \div b$.

ПРИЗНАКИ ДЕЛИМОСТИ

При решении различных задач бывает полезно понять про конкретное число, делится ли оно на какое-то другое конкретное число. Однако часто проверить это непосредственно бывает не очень просто. К счастью, для некоторых делителей есть довольно простые *признаки делимости*. Но сначала давайте немного поговорим о том, как записывать числа в десятичной системе в общем виде.

Если, например, у четырёхзначного числа a всего a_0 единиц, a_1 десятков, a_2 сотен и a_3 тысяч, то

$$a = a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Более коротко это записывается так:

$$a = \overline{a_3 a_2 a_1 a_0}.$$

Черту сверху рисуют для того, чтобы отличить число с цифрами a_3, a_2, a_1, a_0 от произведения $a_3 a_2 a_1 a_0$. То есть, если $a_3 = 1, a_2 = 2, a_1 = 3, a_0 = 4$, то $\overline{a_3 a_2 a_1 a_0}$ – это число 1234, а $a_3 a_2 a_1 a_0$ – это произведение $1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Перейдём теперь к признакам делимости. Признаки делимости на 2, 5 и 10 основаны на том, что

если из числа вычесть его последнюю цифру¹, то останется число, кратное 10. Действительно, пусть есть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$, тогда

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 = \\ &= 10 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \dots + a_1) + a_0 = \\ &= 10 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0. \end{aligned}$$

То есть

$$\overline{a_n a_{n-1} \dots a_1 a_0} - a_0 = 10 \cdot \overline{a_n a_{n-1} \dots a_1}.$$

Признак делимости на 10. Если число оканчивается цифрой 0, то оно делится на 10.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ оканчивается на 0, тогда

$$a = 10 \cdot \overline{a_n a_{n-1} \dots a_1} : 10.$$

Признак делимости на 2. Если число оканчивается чётной цифрой (0, 2, 4, 6 или 8), то оно делится на 2.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ и $a_0 = 2k$, тогда

$$a = 10 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0 = 2 \cdot (5 \cdot \overline{a_n a_{n-1} \dots a_1} + k) : 2.$$

¹Говорить «вычесть цифру» не очень правильно. Потому что цифры – это просто символы, с помощью которых записывают числа. Их нельзя вычитать или прибавлять. Правильнее говорить «вычтем однозначное число, записанное этой цифрой». Но это очень громоздко, поэтому для краткости обычно так не делают.

Признак делимости на 5. Если число оканчивается цифрой 0 или цифрой 5, то оно делится на 5.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$. Если $a_0 = 0$, то

$$a = 10 \cdot \overline{a_n a_{n-1} \dots a_1} = 5 \cdot (2 \cdot \overline{a_n a_{n-1} \dots a_1}) : 5.$$

Если же $a_0 = 5$, то

$$a = 10 \cdot \overline{a_n a_{n-1} \dots a_1} + 5 = 5 \cdot (2 \cdot \overline{a_n a_{n-1} \dots a_1} + 1) : 5.$$

Если распространить ту же идею на две последние цифры, то получатся признаки делимости на 4, 20, 25, 50 и 100. Действительно, пусть есть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$, тогда

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 = \\ &= 100 \cdot (a_n \cdot 10^{n-2} + a_{n-1} \cdot 10^{n-3} + \dots + a_2) + \\ &\quad + a_1 \cdot 10 + a_0 = \\ &= 100 \cdot \overline{a_n a_{n-1} \dots a_2} + \overline{a_1 a_0} \end{aligned}$$

(если в последнем равенстве $a_1 = 0$, то под $\overline{a_1 a_0}$ понимается однозначное число a_0).

Сформулируем, например, признаки делимости на 100 и на 4.

Признак делимости на 100. Если число оканчивается цифрами 00, то оно делится на 100.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ оканчивается на 00, тогда

$$a = 100 \cdot \overline{a_n a_{n-1} \dots a_2} : 100.$$

Признак делимости на 4. Если две последние цифры числа образуют число¹, кратное четырём, то и само число делится на 4.

Доказательство. Пусть две последние цифры числа $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ образуют число $\overline{a_1 a_0} = 4k$, кратное четырём, тогда

$$\begin{aligned} a &= 100 \cdot \overline{a_n a_{n-1} \dots a_2} + \overline{a_1 a_0} = \\ &= 4 \cdot (25 \cdot \overline{a_n a_{n-1} \dots a_2} + k) : 4. \end{aligned}$$

Задача 1. Сформулируйте и докажите признаки делимости на 20, 25, 50.

Думаю, теперь понятно, как звучат признаки делимости на делители тысячи (8, 40, 125, 200, 250, 500, 1000). В этих признаках всё зависит от трёх последних цифр. Давайте, например, сформулируем и докажем признак делимости на 8.

Признак делимости на 8. Если три последние цифры числа образуют число, кратное восьми, то и само число делится на 8.

Доказательство. Пусть три последние цифры числа $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ образуют число $\overline{a_2 a_1 a_0} = 8k$, кратное восьми, тогда

$$\begin{aligned} a &= 1000 \cdot \overline{a_n a_{n-1} \dots a_3} + \overline{a_2 a_1 a_0} = \\ &= 8 \cdot (125 \cdot \overline{a_n a_{n-1} \dots a_3} + k) : 8. \end{aligned}$$

После этого вы легко самостоятельно справитесь со следующей задачей.

¹Если число заканчивается на 00, 04 или 08, то мы считаем, что две последние цифры числа образуют соответственно числа 0, 4 и 8.

Задача 2. Сформулируйте и докажите признак делимости на 16.

Перейдём к более сложным признакам делимости – к тем, в которых участвуют все цифры числа, а не только несколько последних.



Признак делимости на 9. Если сумма цифр числа¹ делится на 9, то и само число делится на 9.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ и

$$S = a_n + a_{n-1} + \dots + a_1 + a_0$$

– сумма его цифр, тогда

$$\begin{aligned} a - S &= (a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0) - \\ &\quad - (a_n + \dots + a_1 + a_0) = \\ &= (10^n - 1) \cdot a_n + \dots + (10^2 - 1) \cdot a_2 + (10 - 1) \cdot a_1. \end{aligned}$$

Заметим, что

$$10 - 1 = 9 \div 9,$$

$$10^2 - 1 = 100 - 1 = 99 = 11 \cdot 9 \div 9,$$

$$10^3 - 1 = 1000 - 1 = 999 = 111 \cdot 9 \div 9,$$

¹Как я уже говорил ранее, цифры – это просто символы, с помощью которых записываются числа. В этом смысле говорить про сумму цифр некорректно. Правильнее говорить как-то так: «сумма однозначных чисел, которые записываются цифрами числа». Но согласитесь, что так звучит менее понятно. Поэтому все смирились с тем, что можно говорить «сумма цифр», понимая под этим сумму соответствующих однозначных чисел.

и вообще для любого натурального m

$$10^m - 1 = \underbrace{999 \dots 99}_{m \text{ девяток}} = \underbrace{111 \dots 11}_{m \text{ единиц}} \cdot 9 \div 9.$$

Поэтому разность

$$a - S = 9 \cdot (\underbrace{111 \dots 11}_{n \text{ единиц}} \cdot a_n + \dots + 11 \cdot a_2 + a_1)$$

делится на 9. Но по условию и S делится на 9, следовательно, и $a = (a - S) + S$ тоже делится на 9.

Признак делимости на 3. Если сумма цифр числа делится на 3, то и само число делится на 3.

Доказательство. Мы только что доказали, что разность $(a - S)$ всегда делится на 9, но тогда она делится и на 3. И S делится на 3. Значит, и $a = (a - S) + S$ тоже делится на 3.

Признак делимости на 11. Если разность между суммой цифр, стоящих на чётных местах, и суммой цифр, стоящих на нечётных местах числа, делится на 11, то и само число делится на 11.



Доказательство. Пусть число

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} = a_0 + 10a_1 + 100a_2 + \dots + 10^n a_n$$

и $S' = (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots) = 11k$, тогда

$$a - S' = 11a_1 + 99a_2 + 1001a_3 + \dots$$

Справа получаются коэффициенты двух видов:

$$100 - 1 = 99, \quad 10\,000 - 1 = 9999, \quad \dots$$

$$10 + 1 = 11, \quad 1000 + 1 = 1001, \quad \dots$$

Каждый из коэффициентов первого вида можно представить так:

$$99 = 9 \cdot 11;$$

$$9999 = 909 \cdot 11;$$

$$999\,999 = 90\,909 \cdot 11;$$

...

Значит, каждый из них делится на 11.

А каждый из коэффициентов второго вида можно представить так:

$$1001 = 990 + 11 = 90 \cdot 11 + 11;$$

$$100\,001 = 99\,990 + 11 = 9090 \cdot 11 + 11;$$

$$10\,000\,001 = 9\,999\,990 + 11 = 909\,090 \cdot 11 + 11;$$

...

Значит, и из них каждый делится на 11.

Это означает, что разность $(a - S')$ всегда делится на 11. Но по условию и S' делится на 11, следовательно, и $a = (a - S') + S'$ тоже делится на 11.

Задача 3. Правда ли, что если сумма цифр числа делится на 27, то и само число делится на 27?

ДЕЛЕНИЕ С ОСТАТКОМ

Если мы хотим, например, разделить число 100 на 3, то у нас ничего не получится (вы же помните, что мы считаем, что числа бывают только целые).

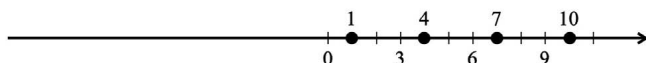
Но можно найти ближайшее число, не превосходящее 100, которое делится на 3 – число $99 = 33 \cdot 3$, и сказать, что сто – это 33 раза по 3 и ещё 1 останется.

Иными словами мы сказали, что

$$100 = 33 \cdot 3 + 1.$$

При этом 33 называется *неполным частным*, а 1 – *остатком* при делении 100 на 3.

Легко понять, что все числа с остатком 1 при делении на 3 идут с шагом 3 на числовой прямой:



Действительно,

$$1 = 0 \cdot 3 + 1;$$

$$4 = 1 \cdot 3 + 1;$$

$$7 = 2 \cdot 3 + 1;$$

$$10 = 3 \cdot 3 + 1;$$

...

Оказалось, что очень удобно продолжить это влево от нуля и сказать, что у чисел (-2) , (-5) , (-8) , (-11) , ... тоже остаток 1 при делении на 3, потому что

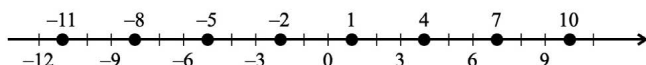
$$-2 = (-1) \cdot 3 + 1;$$

$$-5 = (-2) \cdot 3 + 1;$$

$$-8 = (-3) \cdot 3 + 1;$$

$$-11 = (-4) \cdot 3 + 1;$$

...



В итоге мы добрались с вами до строгого математического определения остатка.

Для любого целого числа a и натурального числа b существует представление числа a в виде:

$$a = kb + r,$$

где k – некоторое целое число, а r – целое число от 0 до $(b - 1)$. При этом число r называется *остатком при делении a на b* , а k – *неполным частным*.

На практике неполное частное и остаток чаще всего ищут методом деления в столбик. Давайте вспомним, в чём он заключается и почему он работает¹.

Так в чём же, по сути, заключается метод? Пусть, например, требуется разделить число 23 456 на 12 с остатком. Мы последовательно отрываем от 23 456 части, которые точно делятся на 12, пока не останется число, которое меньше 12:

$$23\,456 - 12\,000 = 11\,456;$$

$$11\,456 - 10\,800 = 656;$$

$$656 - 600 = 56;$$

$$56 - 48 = 8.$$

¹Как показывает опыт преподавания, даже для студентов профильных вузов деление в столбик является чаще всего просто заученным алгоритмом, некоторым странным набором действий, который почему-то приводит к ответу. Мало кто из них задумывается, почему этот метод работает.

В итоге мы получили следующее представление числа 23 456:

$$\begin{aligned} 23\,456 &= 12\,000 + 10\,800 + 600 + 48 + 8 = \\ &= 1000 \cdot 12 + 900 \cdot 12 + 50 \cdot 12 + 4 \cdot 12 + 8 = \\ &= 1954 \cdot 12 + 8. \end{aligned}$$

Это означает, что неполное частное при делении числа 23 456 на 12 равно 1954, а остаток равен 8.

Обычно процесс деления в столбик записывают следующим образом:

	2	3	4	5	6		1	2	
	1	2					1	9	5
	1	1	4				4		
	1	0	8						
			6	5					
			6	0					
				5	6				
				4	8				
					8				

Если вам всё ещё не понятно, как одно связано с другим, то давайте попробуем расписать подробнее.

Мы видим, что из числа 23 456 можно забрать 1000 раз по 12, то есть 12 000. Справа пишем, сколько раз по 12 мы забираем, а слева – то, что нужно забрать:

	2	3	4	5	6		1	2	
	1	2	0	0	0		1	0	0

Считаем, сколько осталось от 23 456 после того, как мы забрали 12 000:

	2	3	4	5	6		1	2	
	1	2	0	0	0		1	0	0
	1	1	4	5	6				

Видим, что из числа 11 456 можно забрать 900 раз по 12, то есть 10 800:

	2	3	4	5	6		1	2	
	1	2	0	0	0		1	0	0
	1	1	4	5	6				
	1	0	8	0	0		9	0	0

Считаем, сколько осталось от 11 456 после того, как мы забрали 10 800:

	2	3	4	5	6		1	2	
	1	2	0	0	0		1	0	0
	1	1	4	5	6				
	1	0	8	0	0		9	0	0
			6	5	6				

Видим, что из числа 656 можно забрать 50 раз по 12, то есть 600:

	2	3	4	5	6		1	2	
	1	2	0	0	0		1	0	0
	1	1	4	5	6				
	1	0	8	0	0		9	0	0
			6	5	6				
			6	0	0		5	0	

Считаем, сколько осталось от 656 после того, как мы забрали 600:

	2	3	4	5	6		1	2
	1	2	0	0	0		1	0
	1	1	4	5	6			
	1	0	8	0	0		9	0
			6	5	6			
			6	0	0		5	0
				5	6			

Видим, что из числа 56 можно забрать 4 раза по 12, то есть 48:

	2	3	4	5	6		1	2
	1	2	0	0	0		1	0
	1	1	4	5	6			
	1	0	8	0	0		9	0
			6	5	6			
			6	0	0		5	0
				5	6			
				4	8			4

Считаем, сколько осталось от 56, после того как мы забрали 48:

	2	3	4	5	6		1	2
	1	2	0	0	0		1	0
	1	1	4	5	6			
	1	0	8	0	0		9	0
			6	5	6			
			6	0	0		5	0
				5	6			
				4	8			4
					8			

В итоге мы из числа 23 456 забрали

$$1000 + 900 + 50 + 4 = 1954$$

раза по 12, и осталось 8. Значит,

$$23\,456 = 1954 \cdot 12 + 8.$$

Просто при стандартной записи деления в столбик не пишут некоторые цифры:

	2	3	4	5	6		1	2	
	1	2	0	0	0	1	0	0	0
	1	1	4	5	6				
	1	0	8	0	0		9	0	0
			6	5	6				
			6	0	0		5	0	
				5	6				
				4	8			4	
				8					

Конечно, это ускоряет процесс деления, но часто приводит к ошибкам. Поэтому, пока не привыкли, старайтесь максимально подробно делать все шаги.

Давайте теперь поймём, как деление в столбик помогает найти остаток и неполное частное при делении отрицательного числа.

Пусть, например, нужно разделить отрицательное число $(-23\,456)$ на 12 с остатком. Для этого разделим противоположное положительное число 23 456 на 12 с остатком (нам повезло, мы это уже сделали). Получаем

$$23\,456 = 1954 \cdot 12 + 8.$$

Второе решение. Попробуем найти число вида $\overline{12345678x}$, которое делится на 11. Воспользуемся признаком делимости на 11. Мы знаем, что если разность

$$(x + 7 + 5 + 3 + 1) - (8 + 6 + 4 + 2) = x - 4$$

делится на 11, то и само число $\overline{12345678x}$ делится на 11. Значит, число $\overline{123456784}$ делится на 11, а

$$123\,456\,789 = 123\,456\,784 + 5.$$

Поэтому остаток при делении $123\,456\,789$ на 11 равен 5.

Ответ. Остаток равен 5.

Задача 5. Число состоит из 1001 единицы. Какой у него остаток при делении на 11?

Решение. Заметим, что

$$\begin{aligned} \underbrace{1111 \dots 111}_{1001 \text{ единица}} &= \underbrace{1111 \dots 1110}_{1000 \text{ единиц}} + 1 = \\ &= \underbrace{1111 \dots 111}_{1000 \text{ единиц}} \cdot 10 + 1. \end{aligned}$$

У числа, состоящего из 1000 единиц, сумма цифр, стоящих на чётных местах, равна 500 и сумма цифр, стоящих на нечётных местах, равна 500. Из признака делимости на 11 следует, что такое число делится на 11. Значит, и $\underbrace{1111 \dots 1110}_{1000 \text{ единиц}}$ делится на 11, поэто-

му остаток при делении числа $\underbrace{1111 \dots 111}_{1001 \text{ единица}}$ на 11 равен 1.

Ответ. Остаток равен 1.

Задача 6. Найдите остаток¹ при делении числа

$$10^{1000} + 12^{1000}$$

на 11.

Решение. Первое слагаемое равно

$$10^{1000} = \underbrace{10000 \dots 000}_{1000 \text{ нулей}} = \underbrace{9999 \dots 999}_{1000 \text{ девяток}} + 1.$$

У числа $\underbrace{9999 \dots 999}_{1000 \text{ девяток}}$ сумма цифр, стоящих на чётных местах, равна $500 \cdot 9$ и сумма цифр, стоящих на нечётных местах, равна $500 \cdot 9$. Из признака делимости на 11 следует, что такое число делится на 11. Значит, остаток при делении числа 10^{1000} на 11 равен 1.

Далее заметим, что если два числа дают остатки 1 при делении на 11, то их произведение тоже даёт остаток 1. Действительно, пусть $x = 11n + 1$, $y = 11k + 1$, тогда

$$\begin{aligned} xy &= (11n + 1) \cdot (11k + 1) = 121nk + 11n + 11k + 1 = \\ &= 11 \cdot (11nk + n + k) + 1, \end{aligned}$$

то есть даёт остаток 1 при делении на 11.

Но $12 = 11 + 1$ даёт остаток 1 при делении на 11, поэтому $12^2 = 12 \cdot 12$ даёт остаток 1 при делении на 11, а значит и $12^3 = 12^2 \cdot 12$ даёт остаток 1, и так далее. Значит, и 12^{1000} будет давать остаток 1 при делении на 11.

¹Сейчас мы решим эту задачу «руками», используя совсем простые рассуждения, но когда вы дочитаете эту книгу до конца, вы сможете решить её в одну строчку (см. стр. 178).

В итоге получаем, что

$$10^{1000} = 11m + 1, \quad 12^{1000} = 11\ell + 1.$$

Значит, число

$$10^{1000} + 12^{1000} = 11 \cdot (m + \ell) + 2$$

даёт остаток 2 при делении на 11.

Ответ. Остаток равен 2.

А следующие пару задач попробуйте решить самостоятельно.

Задача 7. Найдите все натуральные числа, которые при делении на 5 дают остаток, равный неполному частному.

Задача 8. Найдите все четырёхзначные числа, которые при делении на 100 дают остаток 24, а при делении на 101 дают остаток 4.

КРИТЕРИИ ДЕЛИМОСТИ

Ранее мы доказали несколько признаков делимости. И в таких формулировках это именно признаки: «если сумма цифр числа делится на 9, то и само число делится на 9». Но часто бывают ситуации, когда про число нужно дать отрицательный ответ: «число **не** делится на 9».

Важно понимать, что из признака делимости напрямую не следует, что «если сумма цифр числа **не** делится на 9, то и само число **не** делится на 9».

Признак утверждает лишь то, что если сумма цифр делится, то делится и само число. Но в действительности каждый из доказанных ранее признаков делимости на самом деле является *критерием* делимости. Давайте это докажем.

Критерий делимости на 10. Число делится на 10 тогда и только тогда, когда оно оканчивается цифрой 0.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ оканчивается на цифру a_0 , тогда

$$a = 10 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0.$$

То есть при делении на 10 число a имеет остаток a_0 . Но число делится на 10 тогда и только тогда, когда его остаток при делении на 10 равен нулю. Поэтому число делится на 10 тогда и только тогда, когда $a_0 = 0$.

Критерий делимости на 2. Число делится на 2 тогда и только тогда, когда оно оканчивается чётной цифрой.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ оканчивается на цифру a_0 , тогда

$$a = 10 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0.$$

Первое слагаемое делится на 10, значит, оно делится на 2. Тогда, если a_0 делится на 2, то и число a делится на 2, как сумма двух чисел, кратных двум.

С другой стороны,

$$a_0 = a - 10 \cdot \overline{a_n a_{n-1} \dots a_1}.$$

Поэтому, если число a делится на 2, то и a_0 делится на 2, как разность двух чисел, кратных двум.

В итоге мы доказали, что число делится на 2 тогда и только тогда, когда оно оканчивается цифрой, которая делится на 2.

Аналогично формулируются и доказываются все критерии делимости, связанные с последними цифрами числа. Покажем, например, как это работает на критерии делимости на 8.

Критерий делимости на 8. Число делится на 8 тогда и только тогда, когда три последние цифры числа образуют число, кратное восьми.

Доказательство. Пусть три последние цифры числа $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ образуют число $\overline{a_2 a_1 a_0}$, тогда

$$a = 1000 \cdot \overline{a_n a_{n-1} \dots a_3} + \overline{a_2 a_1 a_0}.$$

Первое слагаемое делится на 1000, значит, оно делится на 8. Тогда, если $\overline{a_2 a_1 a_0}$ делится на 8, то и число a делится на 8, как сумма двух чисел, кратных восьми.

С другой стороны,

$$\overline{a_2 a_1 a_0} = a - 1000 \cdot \overline{a_n a_{n-1} \dots a_3}.$$

Поэтому, если число a делится на 8, то и $\overline{a_2 a_1 a_0}$ делится на 8, как разность двух чисел, кратных восьми.

В итоге мы доказали, что число делится на 8 тогда и только тогда, когда три последние цифры числа образуют число, кратное восьми.

Давайте покажем, что и признаки делимости на 3, на 9 и на 11 на самом деле являются критериями.

Критерий делимости на 9. Число делится на 9 тогда и только тогда, когда сумма его цифр делится на 9.

Доказательство. Пусть S – сумма цифр числа a . Ранее, при доказательстве признака делимости на 9 (см. стр. 28), мы доказали, что разность $(a - S)$ всегда делится на 9. Поэтому, если S делится на 9, то и $a = (a - S) + S$ тоже делится на 9. И наоборот, если a делится на 9, то и $S = a - (a - S)$ тоже делится на 9.

Таким образом, мы доказали, что число делится на 9 тогда и только тогда, когда сумма его цифр делится на 9.

Критерий делимости на 3. Число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

Доказательство. Так же, как и в предыдущем критерии, мы знаем, что разность $(a - S)$ всегда делится на 9, но это означает, что она делится и на 3. Поэтому, если S делится на 3, то и $a = (a - S) + S$ тоже делится на 3. И наоборот, если a делится на 3, то и $S = a - (a - S)$ тоже делится на 3.

Таким образом, мы доказали, что число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

Критерий делимости на 11. Число делится на 11 тогда и только тогда, когда разность между суммой цифр, стоящих на чётных местах, и суммой цифр,

стоящих на нечётных местах этого числа, делится на 11.

Доказательство. Пусть число

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} = a_0 + 10a_1 + 100a_2 \dots + 10^n a_n$$

и

$$S' = (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots).$$

Ранее, при доказательстве признака делимости на 11 (см. стр. 29), мы доказали, что разность $(a - S')$ всегда делится на 11. Поэтому, если S' делится на 11, то и $a = (a - S') + S'$ тоже делится на 11. И наоборот, если число a делится на 11, то и $S' = a - (a - S')$ тоже делится на 11.

Таким образом, мы доказали, что число делится на 11 тогда и только тогда, когда разность между суммой цифр, стоящих на чётных местах, и суммой цифр, стоящих на нечётных местах этого числа, делится на 11.

Задача 9. Натуральное число в 123 раза больше суммы своих цифр. Докажите, что оно делится на 27.

Решение. Пусть сумма цифр числа n равна S . По условию $n = 123S = 3 \cdot 41S$, следовательно, n делится на 3. Тогда из критерия делимости на 3 следует, что сумма его цифр должна делиться на 3.

Пусть $S = 3k$, где k – натуральное число. Тогда

$$n = 123S = 123 \cdot 3k = 9 \cdot 41S$$

делится на 9. Поэтому из критерия делимости на 9 следует, что сумма его цифр должна делиться на 9.

Пусть $S = 9\ell$, где ℓ – натуральное число. Тогда

$$n = 123S = 123 \cdot 9\ell = 27 \cdot 41\ell$$

делится на 27.

А со следующими задачами попробуйте справиться самостоятельно.

Задача 10. Для записи тридцатизначного числа использовано 10 нулей, 10 единиц и 10 двоек. Может ли это число быть квадратом натурального числа?

Задача 11. Докажите, что никакая степень двойки не может оканчиваться четырьмя одинаковыми цифрами.

АЛГОРИТМ ЕВКЛИДА

В этом разделе мы вспомним о том, что такое наибольший общий делитель двух чисел, и обсудим один из алгоритмов его вычисления. Но давайте начнём с определения.

Общим делителем чисел a и b называется число, на которое делятся оба этих числа. Наибольший общий делитель обозначается $\text{НОД}(a, b)$ или просто (a, b) .

Например, у чисел 105 и 126 есть несколько общих делителей:

$$1, \quad 3, \quad 7, \quad 21.$$

Наибольший из них – это 21, поэтому

$$\text{НОД}(105, 126) = 21.$$

Но бывают такие числа, у которых нет общих делителей, отличных от единицы.

Натуральные числа a и b называются *взаимно простыми*, если $\text{НОД}(a, b) = 1$.

Например, $\text{НОД}(8, 9) = 1$.

У наибольшего общего делителя есть несколько важных свойств.

Утверждение. Для любого натурального числа a верно следующее равенство:

$$\text{НОД}(a, 0) = a.$$

Доказательство. Ноль делится на любое число, а наибольший делитель числа a – это само число a . Поэтому наибольший общий делитель чисел 0 и a – это a .

Утверждение. Для любых двух натуральных чисел $a \geq b$ верно следующее равенство:

$$\text{НОД}(a - b, b) = \text{НОД}(a, b).$$

Доказательство. Пусть

$$\text{НОД}(a, b) = d_1, \quad \text{НОД}(a - b, b) = d_2.$$

Так как $\text{НОД}(a, b) = d_1$, то a и b делятся на d_1 . Тогда и $(a - b)$ делится на d_1 . То есть d_1 – общий делитель чисел $(a - b)$ и b . А d_2 – это наибольший общий делитель чисел $(a - b)$ и b . Значит, $d_2 \geq d_1$.

С другой стороны, так как $\text{НОД}(a - b, b) = d_2$, то $(a - b)$ и b делятся на d_2 . Тогда и $a = (a - b) + b$ делится на d_2 . То есть d_2 – общий делитель чисел a и b . А d_1 – это наибольший общий делитель чисел a и b . Значит, $d_1 \geq d_2$.

Но если $d_2 \geq d_1$ и $d_1 \geq d_2$, то $d_1 = d_2$. Именно это мы и должны были доказать.

Итак, мы доказали, что если $a \geq b$, то

$$\text{НОД}(a - b, b) = \text{НОД}(a, b).$$

Но если так окажется, что $a - b \geq b$, то можно применить это свойство ещё раз. То есть

$$\text{НОД}(a - 2b, b) = \text{НОД}(a - b, b) = \text{НОД}(a, b).$$

А если вновь окажется, что $a - 2b \geq b$, то можно снова использовать это свойство:

$$\text{НОД}(a - 3b, b) = \text{НОД}(a - 2b, b) = \text{НОД}(a, b).$$

А если... Ну вы поняли. Мы можем из числа a вычитать число b до тех пор, пока не останется число, меньшее b . А что это за число, которое остаётся от числа a , когда мы из него забрали столько раз число b , сколько возможно забрать? Это же просто остаток при делении числа a на число b .

Действительно, по определению неотрицательно число r называется остатком при делении a на b , если оно меньше b , и при некотором целом k справедливо равенство $a = kb + r$.

Таким образом, мы доказали следующее свойство наибольшего общего делителя.

Утверждение. Для любых двух натуральных чисел $a \geq b$ верно следующее равенство:

$$\text{НОД}(r, b) = \text{НОД}(a, b),$$

где r – остаток при делении a на b .

На этом утверждении основан важный способ вычисления наибольшего общего делителя – **алгоритм Евклида**.

Для нахождения $\text{НОД}(a, b)$ нужно заменить большее из чисел на остаток от деления его на меньшее и для полученной пары повторять эту процедуру, пока одно из чисел не станет равно нулю. Тогда второе число будет равно наибольшему общему делителю исходных чисел.

Посмотрим, как работает алгоритм Евклида на конкретных числах.

Задача 12. Найдите $\text{НОД}(300, 135)$.

Решение. Применим алгоритм Евклида¹:

$$(300, 135) = (30, 135), \quad \text{так как} \quad 300 = 2 \cdot 135 + 30;$$

$$(30, 135) = (30, 15), \quad \text{так как} \quad 135 = 4 \cdot 30 + 15;$$

$$(30, 15) = (0, 15), \quad \text{так как} \quad 30 = 2 \cdot 15 + 0;$$

$$(0, 15) = 15.$$

Ответ. $\text{НОД}(300, 135) = 15$.

¹Напомним, что при определении наибольшего общего делителя (см. стр. 45) мы договорились, что есть два равноправных обозначения: $\text{НОД}(a, b)$ и (a, b) .

При длинных преобразованиях наибольшего общего делителя мы чаще будем использовать второе обозначение.

Понятно, что если числа довольно большие, то процесс поиска наибольшего делителя при помощи алгоритма Евклида может быть очень долгим, но универсальность этого алгоритма позволяет решать довольно сложные задачи.

А иногда бывает достаточно даже не самого алгоритма Евклида, а утверждения о том, что

$$\text{НОД}(a - b, b) = \text{НОД}(a, b).$$

Посмотрим, как это работает на примере следующей задачи.

Задача 13. Докажите, что при любом натуральном n дробь $\frac{6n+1}{15n+1}$ будет несократимой.

Решение. Если перебирать конкретные маленькие значения n , то действительно получаются несократимые дроби:

$$\frac{7}{16}, \quad \frac{13}{31}, \quad \frac{19}{46}, \quad \frac{25}{61}, \quad \frac{31}{76}, \quad \frac{37}{91}, \quad \dots$$

Но как доказать, что так будет всегда? Дело в том, что дробь можно сократить, только если числитель и знаменатель имеют общий делитель, отличный от единицы. Попробуем найти наибольший общий делитель чисел $(6n+1)$ и $(15n+1)$:

$$\begin{aligned} (6n+1, 15n+1) &= (6n+1, (15n+1) - 2 \cdot (6n+1)) = \\ &= (6n+1, 3n-1) = \\ &= (6n+1 - 2 \cdot (3n-1), 3n-1) = \\ &= (3, 3n-1) = \\ &= (3, (3n-1) - (n-1) \cdot 3) = \\ &= (3, 2) = 1. \end{aligned}$$

Таким образом, мы получили, что ни при каком натуральном n у чисел $(6n + 1)$ и $(15n + 1)$ нет общего делителя, отличного от единицы. А значит, при любом натуральном n дробь $\frac{6n + 1}{15n + 1}$ является несократимой.

Повторите самостоятельно эти рассуждения для решения следующей задачи.

Задача 14. Докажите, что числа $(27n + 4)$ и $(18n + 3)$ взаимно просты при любом натуральном n .

СООТНОШЕНИЕ БЕЗУ

Давайте внимательно проследим, как в задаче 12 из чисел 300 и 135 получилось число 15.

Мы хотели найти $\text{НОД}(300, 135)$. Для этого мы дважды вычли из числа 300 число 135 и сказали, что $\text{НОД}(30, 135) = \text{НОД}(300, 135)$. Значит,

$$30 = 300 - 2 \cdot 135.$$

После этого нам нужно было найти $\text{НОД}(30, 135)$. Мы четырежды вычли из числа 135 число 30 и сказали, что $\text{НОД}(30, 15) = \text{НОД}(30, 135)$. Значит,

$$\begin{aligned} 15 &= 135 - 4 \cdot 30 = 135 - 4 \cdot (300 - 2 \cdot 135) = \\ &= 3 \cdot 135 - 4 \cdot 300. \end{aligned}$$

После этого, по сути, мы заметили, что 30 делится на 15, поэтому 15 – это и есть искомый наибольший общий делитель.

В итоге мы получили, что

$$\text{НОД}(300, 135) = 3 \cdot 135 - 4 \cdot 300.$$

То есть, $\text{НОД}(300, 135)$ можно представить в виде линейной комбинации¹ чисел 300 и 135 с целыми коэффициентами.

Это и называется **соотношением Безу**. Давайте чётко сформулируем и докажем общий факт.

Соотношение Безу². Для любых натуральных чисел a и b найдутся такие целые числа m и n , что

$$\text{НОД}(a, b) = ma + nb.$$

Доказательство. Докажем, что если некоторые числа c и d можно представить в виде линейных комбинаций чисел a и b , то и разность $(c - d)$ можно представить в таком виде. То есть, если при некоторых целых m_1, n_1, m_2, n_2 верны равенства

$$c = m_1a + n_1b, \quad d = m_2a + n_2b,$$

то найдутся такие целые числа m_3 и n_3 , что

$$c - d = m_3a + n_3b.$$

Действительно,

$$\begin{aligned} c - d &= (m_1a + n_1b) - (m_2a + n_2b) = \\ &= (m_1 - m_2) \cdot a + (n_1 - n_2) \cdot b. \end{aligned}$$

Доказали!

¹Линейной комбинацией чисел a и b называется выражение вида $(ma + nb)$.

²Для взаимно простых чисел этот факт опубликовал Клод Гаспар Баше де Мезириак в 1624 году. А в 1766 году Этьен Безу в своём «Курсе математики» обобщил теорему, распространив её на произвольные пары чисел.

А теперь давайте вспомним, как мы вычисляем $\text{НОД}(a, b)$ при помощи алгоритма Евклида. По сути, мы просто заменяем большее число на разность большего и меньшего.

Заметим, что и исходные числа можно представить в виде

$$a = 1 \cdot a + 0 \cdot b, \quad b = 0 \cdot a + 1 \cdot b.$$

Поэтому все числа, которые будут появляться при реализации алгоритма Евклида, будут являться линейными комбинациями чисел a и b . В том числе и последнее число. А последнее число – это и есть $\text{НОД}(a, b)$. Поэтому найдутся такие целые числа m и n , что

$$\text{НОД}(a, b) = ma + nb.$$

В дальнейшем чаще всего нам будет интересно не само соотношение Безу, а следующий его частный случай.

Следствие из соотношения Безу. Если натуральные числа a и b взаимно просты, то найдутся такие целые числа m и n , что

$$ma + nb = 1.$$

Доказательство. Для доказательства достаточно вспомнить, что взаимно простые числа – это числа, для которых $\text{НОД}(a, b) = 1$, и после этого воспользоваться соотношением Безу.

ЗАДАЧИ НА ДЕЛИМОСТЬ

Мы только начали знакомство с вопросами, связанными с делимостью, но этого уже достаточно, чтобы решать довольно содержательные задачи.

Задача 15. На доске выписали в порядке возрастания все натуральные числа от 1 до 10 000, а потом стёрли те, которые не делятся ни на 4, ни на 5. Какое число находится на 1001-м месте?

Решение. Рассмотрим первые двадцать чисел. Из них останется пять чисел, делящихся на 4, и четыре числа, делящихся на 5. Но при этом число 20 мы учли дважды. Значит, из первых двадцати останется восемь чисел:

4, 5, 8, 10, 12, 15, 16, 20.

Аналогично получим, что из чисел от 21 до 40 останется восемь чисел, из чисел от 41 до 60 останется восемь чисел, из чисел от 61 до 80 останется восемь чисел и так далее.

То есть в каждом блоке из двадцати последовательных натуральных чисел останется по восемь чисел. Чтобы понять, в каком блоке окажется число с номером 1001, разделим 1001 на 8 с остатком:

$$1001 = 125 \cdot 8 + 1.$$

Поэтому 1000-ое число будет последним числом в 125-м блоке:

$$125 \cdot 20 = 2500,$$

а на 1001-м месте находится следующее оставшееся число – 2504.

Ответ. На 1001-м месте находится число 2504.

Задача 16. Десять натуральных чисел выписаны в ряд. При этом каждое число, начиная с третьего, равно сумме двух предыдущих чисел. Какое наибольшее значение может быть у первого числа, если последнее равно 3000?

Решение. Пусть первые два числа равны x и y соответственно. Тогда:

- третье число равно $(x + y)$;
- четвертое равно $(x + 2y)$;
- пятое равно $(2x + 3y)$;
- шестое равно $(3x + 5y)$;
- седьмое равно $(5x + 8y)$;
- восьмое равно $(8x + 13y)$;
- девятое равно $(13x + 21y)$;
- десятое равно $(21x + 34y)$.

Значит, $21x + 34y = 3000$. Чем больше x , тем меньше y . Иными словами, нам нужно найти наименьшее натуральное y , при котором число $(3000 - 34y)$ делится на 21.

Пусть $y = 1$, тогда

$$3000 - 34y = 3000 - 34 = 2966.$$

Но $2966 = 141 \cdot 21 + 5$, поэтому оно не делится на 21.

Пусть $y = 2$, тогда

$$3000 - 34y = 3000 - 68 = 2932.$$

Но $2932 = 139 \cdot 21 + 13$, поэтому оно не делится на 21.

Пусть $y = 3$, тогда

$$3000 - 34y = 3000 - 102 = 2898.$$

При этом $2898 = 138 \cdot 21$, поэтому оно делится на 21.

Значит $y = 3$ – наименьшее значение y , при котором число $(3000 - 34y)$ делится на 21. И при этом

$$x = \frac{2898}{21} = 138.$$

Это означает, что если последнее число равно 3000, то наибольшее значение первого числа – 138.

Ответ. Наибольшее возможное значение первого числа – 138.

Задача 17. В значении числа

$$20! = 2\,432\,902\,008\,176 \, **\, 0\,000$$

две цифры заменили звёздочками. Восстановите эти цифры.

(Напомним, что $20! = 1 \cdot 2 \cdot \dots \cdot 20$ – это число, равное произведению всех натуральных чисел от 1 до 20, и называется *факториал*.)

Решение. Число $20!$ точно делится на 9 и на 11. Обозначим неизвестные цифры как x и y :

$$2\,432\,902\,008\,176\,xy\,0\,000,$$

и воспользуемся критериями делимости числа на 9 и на 11.

Так как число $20!$ делится на 9, то сумма его цифр

$$\begin{aligned} S &= 2 + 4 + 3 + 2 + 9 + 0 + 2 + 0 + 0 + 8 + \\ &\quad + 1 + 7 + 6 + x + y + 0 + 0 + 0 + 0 = \\ &= 44 + x + y = 45 + (x + y - 1) \end{aligned}$$

должна делиться на 9. Значит, $(x + y - 1)$ делится на 9. Учитывая, что x и y – цифры, мы понимаем, что $(x + y - 1)$ может принимать значения от (-1) до 17. А в этом диапазоне только числа 0 и 9 делятся на 9.

С другой стороны, число $20!$ делится на 11, поэтому разность между суммой цифр, стоящих на чётных местах, и суммой цифр, стоящих на нечётных местах этого числа

$$\begin{aligned} S' &= (0 + 0 + y + 6 + 1 + 0 + 2 + 9 + 3 + 2) - \\ &\quad - (0 + 0 + x + 7 + 8 + 0 + 0 + 2 + 4) = \\ &= (23 + y) - (21 + x) = 2 + y - x \end{aligned}$$

должна делиться на 11. Учитывая, что x и y – цифры, мы понимаем, что $(2 + y - x)$ может принимать значения от (-7) до 11. А в этом диапазоне только 0 и 11 делятся на 11.

Рассмотрим четыре случая.

$$\text{Первый случай: } \begin{cases} x + y - 1 = 0; \\ 2 + y - x = 0. \end{cases}$$

Сложив оба равенства, получаем, что $2y + 1 = 0$. То есть $2y = -1$. Но y – это цифра, а значит, целое неотрицательное число. Этот случай невозможен.

Второй случай:
$$\begin{cases} x + y - 1 = 0; \\ 2 + y - x = 11. \end{cases}$$

Сложив оба равенства, получаем, что $2y + 1 = 11$. То есть $y = 5$. Но тогда $x = 1 - y = -4$. Этот случай тоже невозможен.

Третий случай:
$$\begin{cases} x + y - 1 = 9; \\ 2 + y - x = 0. \end{cases}$$

Сложив оба равенства, получаем, что $2y + 1 = 9$. То есть $y = 4$. Тогда $x = 10 - y = 6$. Тут всё хорошо, но на всякий случай проверим четвёртый случай.

Четвёртый случай:
$$\begin{cases} x + y - 1 = 9; \\ 2 + y - x = 11. \end{cases}$$

Сложив оба равенства, получаем, что $2y + 1 = 20$. То есть $2y = 19$. Но y – это цифра, а значит, целое число. И этот случай невозможен.

Таким образом, мы получили, что только при $x = 6$ и $y = 4$ число

$$2\,432\,902\,008\,176\,x\,y\,0\,000$$

делится и на 9 и на 11.

Ответ. $20! = 2\,432\,902\,008\,176\,640\,000$.

А следующие задачи попробуйте решить самостоятельно.

Задача 18. Про пять натуральных чисел известно, что сумма любых четырёх из них делится на 3. Докажите, что тогда каждое из чисел делится на 3.

Задача 19. Докажите, что число

$$999\,999\,999\,999\,999\,999\,999\,999\,999$$

делится на 243.

Задача 20. Какие значения может принимать $\text{НОД}(5a + 3b, 13a + 8b)$, если a и b – натуральные числа и $\text{НОД}(a, b) = 1001$?

Задача 21. Пусть a – произвольное тысячезначное число, кратное девяти. Пусть число b равно сумме цифр числа a ; число c равно сумме цифр числа b ; число d равно сумме цифр числа c . Найдите все возможные значения числа d .

ГЛАВА 2 ПРОСТЫЕ ЧИСЛА

В предыдущей главе мы поговорили про делимость и про делители. А сейчас давайте попробуем понять, сколько бывает делителей у разных натуральных чисел.

Выпишем для нескольких первых натуральных чисел все их делители:

число	делители
1	1
2	1, 2
3	1, 3
4	1, 2, 4
5	1, 5
6	1, 2, 3, 6
7	1, 7
8	1, 2, 4, 8
9	1, 3, 9
10	1, 2, 5, 10
11	1, 11
12	1, 2, 3, 4, 6, 12
13	1, 13
14	1, 2, 7, 14

15	1, 3, 5, 15
16	1, 2, 4, 8, 16
17	1, 17
18	1, 2, 3, 6, 9, 18
19	1, 19
20	1, 2, 4, 5, 10, 20

Посмотрев на первые двадцать чисел, мы видим, что среди них есть:

- только одно число, у которого ровно один делитель – это 1;
- много чисел, у которых ровно два делителя – это 2, 3, 5, 7, 11, 13, 17 и 19;
- есть два числа, у которых ровно три делителя – 4 и 9;
- а есть и такие, у которых четыре, пять и даже шесть различных делителей.

ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

Понятно, что единица – единственное число, у которого есть ровно один делитель не только среди первых двадцати, но и среди всех натуральных чисел, потому что любое натуральное число делится на единицу и само на себя. И для того, чтобы у числа был ровно один делитель, нужно, чтобы «само на себя» и единица совпали. А это бывает только у числа 1.

Натуральные числа, имеющие ровно два нату-

ральных делителя, отличаются от тех, у которых есть больше двух делителей, тем, что их нельзя представить в виде произведения двух меньших чисел, потому что они делятся только на единицу и само на себя! Это такие «кирпичики», из которых в каком-то смысле состоят остальные числа. Поэтому их выделяют в отдельную группу.

Натуральные числа, имеющие ровно два делителя, называются *простыми*.

Восемь первых простых чисел – 2, 3, 5, 7, 11, 13, 17 и 19 – мы нашли, рассмотрев первые двадцать натуральных чисел.

А дальше классификация натуральных чисел останавливается, и отдельно не выделяют числа, имеющие ровно три делителя, ровно четыре, ровно пять и так далее, а «сваливают» их все в общую кучу.

Все натуральные числа, кроме простых и единицы, называются *составными*.

Это означает, что составные числа делятся на что-то, кроме единицы и самого себя. Поэтому любое составное число можно представить в виде произведения двух натуральных чисел, отличных от единицы.

Задача 22. Докажите, что у любого составного числа есть простой делитель.

Первое решение. Мы знаем, что любое составное число a можно представить в виде произведения $a = b \cdot c$, где $1 < b < a$.

Если число b является простым, то мы нашли простой делитель числа a .

Если же число b составное, то его можно представить в виде произведения $b = d \cdot e$, где $1 < d < b$. Если число d является простым, то мы нашли простой делитель числа b , а значит, и числа a .

Если же число d составное, то его можно представить в виде произведения $d = f \cdot g$, где $1 < f < d$. Если число f является простым, то мы нашли простой делитель числа d , а значит, и числа b , а значит, и числа a . И так далее.

Понятно, что рано или поздно мы доберёмся до простого делителя, потому что последовательность a, b, d, \dots состоит из натуральных чисел и убывает. Она не может убывать бесконечно долго. А значит, мы дойдём до некоторого числа, которое уже нельзя представить в виде произведения двух натуральных чисел, отличных от единицы. То есть до простого числа.

Второе решение. Пусть d – наименьший делитель числа a , отличный от единицы. Докажем, что число d – простое.

Предположим, что это не так. Тогда число d можно представить в виде произведения $d = b \cdot c$, где $1 < b < d$.

Так как число a делится на d , а число d делится на b , то число b – это делитель числа a , который отличен от единицы и меньше, чем d . Но число d – это наименьший делитель числа a , отличный от единицы. Пришли к противоречию.

Значит, наше предположение о том, что наименьший делитель числа a , отличный от единицы, не является простым, было ложным.

КОЛИЧЕСТВО ПРОСТЫХ ЧИСЕЛ

Итак, мы поняли, что такое простые и составные числа. И с составными всё понятно — их много! Их очень много, их бесконечно много! Хотя бы потому, что все чётные числа, кроме двойки, являются составными. А сколько существует простых чисел? Может быть, их конечное количество и есть какое-то *самое большое простое число*?

Задача 23. В статье на научно-популярном сайте написано, что

$$2825^{89\,933} - 1$$

является самым большим простым числом. Докажите, что авторы статьи что-то перепутали.

Решение. Заметим, что 2825 – нечётное число. Поэтому и $2825^{89\,933}$ является нечётным. Но тогда число $(2825^{89\,933} - 1)$ чётное и явно больше двух. А значит, оно является составным.

На самом деле, не число $(2825^{89\,933} - 1)$, а число $(2^{82\,589\,933} - 1)$ является самым большим **известным на данный момент** простым числом. Его простоту доказали 7 декабря 2018 года.

Это очень большое число! Если его записать в десятичном виде, то в нём будет 24 862 048 цифр – это более чем в семь раз больше количества знаков во всём романе Льва Толстого «Война и мир».

Но даже оно всего лишь самое большое из *известных на данный момент* простых чисел. Возможно, когда вы будете читать эту книгу, найдут

ещё несколько простых чисел, больших этого. И вот почему.

Теорема Евклида. Простых чисел бесконечно много.

Доказательство. Предположим, что простых чисел конечное количество. Тогда можно выписать их все:

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad \dots, \quad p,$$

где p – самое большое простое число.

Рассмотрим число

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p + 1,$$

которое на единицу больше произведения всех простых чисел. Оно точно больше самого большого простого числа p , поэтому не может быть простым.

С другой стороны, оно не делится на 2, так как оно отличается на 1 от числа, делящегося на 2. По тем же причинам оно не делится на 3, на 5, ..., на p .

Значит число n не делится ни на одно простое число, то есть не может являться составным, так как в задаче 22 мы доказали, что у любого составного числа есть простой делитель.

Таким образом, предположив, что существует самое большое простое число, мы нашли число, большее единицы, которое не является ни простым, ни составным. Полученное противоречие показывает, что наше предположение неверно и простых чисел бесконечно много.

После этого доказательства может сложиться впечатление, что так можно придумывать новые

простые числа – перемножить первые несколько простых и прибавить единицу:

$$2 + 1 = 3;$$

$$2 \cdot 3 + 1 = 7;$$

$$2 \cdot 3 \cdot 5 + 1 = 31;$$

$$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211;$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311.$$

Но, например, для числа 2311 мы можем гарантировать лишь то, что среди его простых делителей нет чисел 2, 3, 5, 7 и 11. При этом оно может делиться, скажем, на 13 или на 17.

Такие числа называются **числами Евклида**. И хотя первые пять из них – 3, 7, 31, 211 и 2311 – действительно являются простыми, так будет не всегда.

Например, число

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031$$

простым не является, так как делится на 59:

$$30\,031 = 59 \cdot 509.$$

Более того, на данный момент даже не известно, конечное или бесконечное количество чисел Евклида являются простыми.

Чтобы убедиться, что вы поняли, что такое числа Евклида и как они устроены, решите самостоятельно следующую задачу.

Задача 24. Сколько существует чисел Евклида, последняя цифра которых отлична от 1?

АЛГОРИТМ ПРОВЕРКИ НА ПРОСТОТУ

Для того чтобы проверить, является ли число простым, совсем необязательно проверять, что оно не делится ни на одно число, меньшее его.

Действительно, если число a является составным, то его можно представить в виде $a = b \cdot c$, где $1 < b \leq c < n$. То есть число a делится на такое, отличное от единицы число b , что $a \leq b^2$.

Это означает, что достаточно проверить, что число a не делится ни на одно из чисел, квадрат которых не превосходит a . Но и это ещё не всё!

Как мы знаем из задачи 22, число b либо само является простым, либо делится на какое-то простое, меньшее его. Иными словами, у нас получился следующий алгоритм проверки числа на простоту.

Для того чтобы проверить, является ли натуральное число, большее единицы, простым, достаточно проверить, что оно не делится ни на одно из простых чисел, квадраты которых не превосходят данное число.

Следующая задача показывает, как применять этот алгоритм на практике.

Задача 25. Какие из данных чисел являются простыми?

101, 103, 105, 107, 109.

Решение. Применим к каждому из чисел алгоритм проверки на простоту.

Рассмотрим число 101:

- 101 не делится на 2, так как $101 = 50 \cdot 2 + 1$;
- 101 не делится на 3, так как $101 = 33 \cdot 3 + 2$;
- 101 не делится на 5, так как $101 = 20 \cdot 5 + 1$;
- 101 не делится на 7, так как $101 = 14 \cdot 7 + 3$.

А следующее простое число – это число 11, но делимость на него проверять уже не нужно, так как $11^2 = 121 > 101$. Значит, 101 не делится ни на одно из простых чисел, квадрат которых не превосходит 101. Поэтому **101 – простое число**.

Рассмотрим число 103:

- 103 не делится на 2, так как $103 = 51 \cdot 2 + 1$;
- 103 не делится на 3, так как $103 = 34 \cdot 3 + 1$;
- 103 не делится на 5, так как $103 = 20 \cdot 5 + 3$;
- 103 не делится на 7, так как $103 = 14 \cdot 7 + 5$.

Значит, 103 не делится ни на одно из простых чисел, квадрат которых не превосходит 103. Поэтому **103 – простое число**.

Рассмотрим число 105:

- 105 не делится на 2, так как $105 = 52 \cdot 2 + 1$;
- 105 делится на 3, так как $105 = 35 \cdot 3$.

Поэтому **105 – составное число**¹.

Рассмотрим число 107:

- 107 не делится на 2, так как $107 = 53 \cdot 2 + 1$;
- 107 не делится на 3, так как $107 = 35 \cdot 3 + 2$;

¹Ещё можно было сразу заметить, что $105 = 21 \cdot 5$

- 107 не делится на 5, так как $107 = 21 \cdot 5 + 2$;
- 107 не делится на 7, так как $107 = 15 \cdot 7 + 2$.

Значит, 107 не делится ни на одно из простых чисел, квадрат которых не превосходит 107. Поэтому **107 – простое число**.

Рассмотрим число 109:

- 109 не делится на 2, так как $109 = 54 \cdot 2 + 1$;
- 109 не делится на 3, так как $109 = 36 \cdot 3 + 1$;
- 109 не делится на 5, так как $109 = 21 \cdot 5 + 4$;
- 109 не делится на 7, так как $109 = 15 \cdot 7 + 4$.

Значит, 109 не делится ни на одно из простых чисел, квадрат которых не превосходит 109. Поэтому **109 – простое число**.

Отметим, что проверить делимость на 2, на 3 и на 5 можно было и с помощью соответствующих критериев делимости.

Ответ. Из чисел 101, 103, 105, 107, 109 простыми являются все числа, кроме 105.

РЕШЕТО ЭРАТОСФЕНА

Итак, мы научились для каждого конкретного (но не очень большого!) числа проверять, является ли оно простым. Но часто бывает полезно иметь список всех простых чисел, не превосходящих некоторого числа.

Даже, например, чтобы просто воспользоваться алгоритмом проверки на простоту для числа 9987,

нам нужно убедиться, что оно не делится ни на одно простое число, не превосходящее 100, а для этого нужно знать, какие числа из первой сотни являются простыми.

Давайте обсудим довольно простой способ, как это можно сделать. Этот способ называется *решетом Эратосфена*.

Пусть мы хотим получить список всех простых чисел, не превосходящих, например, 100. Выпишем все натуральные числа от 2 до 100 (число 1 мы не стали писать, потому что оно точно не является ни простым, ни составным):

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Идём по порядку. Будем для каждого числа проверять, есть ли у него делители, кроме единицы и самого себя.

Число 2 не может делиться на что-то меньше двойки, потому что меньше двойки, кроме единицы, натуральных чисел нет. Поэтому число 2 простое. Обводим двойку и вычеркиваем все остальные числа, кратные двум – 4, 6, 8, ..., то есть каждое второе число. Потому что они больше двух и делятся на 2, а значит, они составные:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Теперь смотрим на первое невычеркнутое число – это число 3. Оно не вычеркнуто, поэтому не делится на 2, а никаких других простых чисел меньше трёх нет. Поэтому число 3 простое. Обводим тройку и вычеркиваем все остальные числа, кратные трём – 6, 9, 12, ..., то есть каждое третье число, потому что они больше трёх и делятся на 3, а значит, они составные (при этом какие-то из них мы уже вычеркнули, как числа, кратные двум):

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Снова смотрим первое невычеркнутое число – это число 5. Оно не вычеркнуто, поэтому не делится ни на 2, ни на 3, а никаких других простых чисел

меньше пяти нет. Значит, число 5 простое. Обводим пятёрку и вычеркиваем все остальные числа, кратные пяти – 10, 15, 20, ..., то есть каждое пятое число, потому что они больше пяти и делятся на 5, а значит, они составные:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Понятно, что нужно делать дальше? Опять смотрим на первое невычеркнутое число – это число 7. Оно не вычеркнуто, поэтому не делится ни на одно простое меньше него. Значит, число 7 простое. Обводим семёрку и вычеркиваем все остальные числа, кратные семи:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

И так далее. Обводим первое невычеркнутое и вычеркиваем все числа, кратные ему. И повторяем процедуру вновь.

На первый взгляд кажется, что это нужно будет делать очень долго, но это необязательно делать до самого конца! Мы же знаем, что *для того, чтобы проверить, является ли натуральное число, большее единицы, простым, достаточно проверить, что оно не делится ни на одно из простых чисел, квадрат которых не превосходит данное число.* Но $11^2 = 121$ точно больше любого числа из первой сотни.

Поэтому для каждого числа, не превосходящего 100, достаточно проверить, что оно не делится ни на одно простое число, меньшее 11. А мы уже вычеркнули все числа, которые делятся на простые, меньшие 11. Значит, все оставшиеся незачеркнутые числа простые! В итоге мы получили список всех простых чисел из первой сотни натуральных:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Понятно, что руками делать это даже для первой тысячи натуральных чисел довольно долго. Но если вы немного умеете программировать, то минут за

десять напишете программу, которая выпишет все простые числа, даже из первого миллиона например.

Если посмотреть на получившийся у нас список простых чисел, то будет видно, что сначала они шли довольно кучно (2, 3, 5, 7), потом стали идти чуть реже, а в последнем десятке есть лишь одно простое число – 97.

И кажется, что чем дальше, тем ещё реже должны встречаться простые числа. Но если вспомнить задачу 25, в которой мы доказали, что числа 101, 103, 107 и 109 являются простыми, становится понятно, что всё не так просто.

Хорошо. Может быть, тогда наоборот, не бывает слишком больших «дырок» между простыми числами? Если посмотреть на простые числа из первой сотни, то там самая большая «дыра» между простыми числами 89 и 97 – там целых семь составных чисел подряд! А бывает ли больше? Может ли, например, быть десять подряд идущих составных чисел?

Оказывается, что и десять составных подряд может быть, и их не очень сложно найти. После плотной группы простых чисел – 101, 103, 107, 109, 113 – следующим простым будет только 127. Действительно,

$$\begin{array}{lll} 114 = 2 \cdot 57, & 115 = 5 \cdot 23, & 116 = 2 \cdot 58, \\ 117 = 3 \cdot 39, & 118 = 2 \cdot 59, & 119 = 7 \cdot 17, \\ 120 = 2 \cdot 60, & 121 = 11 \cdot 11, & 122 = 2 \cdot 61, \\ 123 = 3 \cdot 41, & 124 = 2 \cdot 62, & 125 = 5 \cdot 25, \\ & 126 = 2 \cdot 63. \end{array}$$

Итак, мы нашли тринадцать идущих подряд со-

ставных чисел. А может ли их быть двадцать? Или сто?.. Давайте решим следующую задачу.

Задача 26. Докажите, что существует миллион подряд идущих составных чисел.

Решение. Давайте подумаем, какими свойствами должно обладать число n , чтобы n , $(n + 1)$, $(n + 2)$, $(n + 3)$, ... были составными. Если про $(n + 1)$ не очень понятно, то для того, чтобы $(n + 2)$ было составным, достаточно сделать n чётным числом. Чтобы $(n + 3)$ было составным, достаточно сделать n числом, кратным трём. Кажется, мы решили задачу!

Рассмотрим число $n = k!$ для некоторого натурального k (напомню, что $k! = 1 \cdot 2 \cdot \dots \cdot k$ — число, равное произведению всех натуральных чисел, не превосходящих k , и называется *факториал*). Значит, число n точно делится на 2, 3, 4, ..., k . Но тогда

- $(n + 2)$ делится на 2;
- $(n + 3)$ делится на 3;
- $(n + 4)$ делится на 4;
- ...
- $(n + k)$ делится на k .

То есть мы нашли $(k - 1)$ идущих подряд составных чисел. Осталось взять $k = 1\,000\,001$, и получим миллион подряд идущих составных чисел:

$$\begin{aligned}
 &1\,000\,001! + 2, \\
 &1\,000\,001! + 3, \\
 &1\,000\,001! + 4, \\
 &\dots \\
 &1\,000\,001! + 1\,000\,001.
 \end{aligned}$$

На самом деле не обязательно было брать факториал. Достаточно было ограничиться произведением простых. Например, все следующие числа точно являются составными:

$$\begin{array}{ll}
 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 2, & 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 3 \\
 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 4, & 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 5 \\
 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 6, & 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 7 \\
 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 8, & 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 9 \\
 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 10, & 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 11 \\
 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 12.
 \end{array}$$

Итак, мы поняли, что между простыми числами могут встретиться «дыры» сколь угодно большой длины. Но означает ли это, что чем дальше, тем всё большие расстояния будут между соседними простыми? Давайте это обсудим!

ЧИСЛА-БЛИЗНЕЦЫ

Очевидно, что соседние натуральные числа могут оказаться простыми, только если это числа 2 и 3. Действительно, одно из двух соседних чисел является чётным. Но среди чётных чисел только число 2 является простым. Значит, если не считать пару (2; 3), не существует простых чисел, отличающихся на единицу.

Легко можно найти пары простых чисел, отличающихся на два:

$$(3; 5), \quad (5; 7), \quad (11; 13), \quad (17; 19),$$

(29; 31), (41; 43), (59; 61), (71; 73),
(101; 103), (107; 109), (137; 139), ...

Такие пары называются *числами-близнецами*.

При этом бывают даже «числа-тройняшки»:

(3; 5; 7).

Давайте решим следующую задачу и поймем, часто ли они встречаются.

Задача 27. Найдите все такие натуральные числа p , что числа p , $(p + 2)$, $(p + 4)$ простые.

Решение. Покажем, что из трёх чисел вида p , $(p+2)$, $(p+4)$ всегда какое-то делится на 3. Допустим, что это не так и ни одно из чисел p , $(p + 2)$, $(p + 4)$ не делится на три. Но если $(p + 4)$ не делится на 3, то и

$$p + 1 = (p + 4) - 3$$

не делится на 3. То есть p , $(p + 1)$ и $(p + 2)$ не делятся на 3. Но из трёх последовательных чисел одно всегда делится на 3. Пришли к противоречию!

Значит, какое-то из чисел p , $(p+2)$, $(p+4)$ делится на 3 и при этом является простым числом. Но простые числа делятся только на 1 и само на себя. Значит, это простое число – это 3.

Рассмотрим три случая:

- Если $p = 3$, то наши числа – это 3, 5 и 7 – все простые. Поэтому $p = 3$ подходит.
- Если $p + 2 = 3$, то наши числа – это 1, 3 и 5. Но число 1 не является простым. Поэтому этот случай не подходит.

- Если $p + 4 = 3$, то наши числа – это (-1) , 1 и 3. Но число 1 не является простым, а число (-1) даже не натуральное. Поэтому и этот случай не подходит.

Получаем, что такое возможно только при $p = 3$.

Ответ. 3.

Это значит, что $(3; 5; 7)$ – единственные «числа-тройняшки».

Хорошо, как мы видим, «тройняшек» почти совсем нет, а что можно сказать про «двойняшек»? Мы уже поняли, что чисел-близнецов довольно много. Но насколько их много? Есть ли самые большие числа-близнецы, после которых других уже нет?

Оказывается, что эта задача до сих пор не решена. Есть гипотеза, что таких пар чисел бесконечно много, но пока она не доказана.

Наибольшими известными на данный момент числами-близнецами является следующая пара огромных чисел:

$$\begin{aligned} &(2996863034895 \cdot 2^{1290000} - 1; \\ &2996863034895 \cdot 2^{1290000} + 1). \end{aligned}$$

Каждое из этих чисел содержит 388 342 цифры в десятичной записи. Они были найдены в сентябре 2016 года в рамках проекта добровольных вычислений PrimeGrid¹.

¹PrimeGrid – проект добровольных распределенных вычислений, цель которого – поиск различных простых чисел специального вида. В нем принимают участие сотни тысяч компьютеров почти из всех стран мира.

Так что вопрос о бесконечности количества чисел-близнецов до сих пор остаётся одним из многих открытых вопросов математики.

Кто знает, возможно, кто-то из читателей этой книги всерьёз заинтересуется теорией чисел и докажет эту гипотезу через пару десятков лет.

Ну а пока давайте порешаем более простые задачи о простых числах.

ЗАДАЧИ О ПРОСТЫХ ЧИСЛАХ

Задача 28. Ваня взял два листа бумаги и нарисовал на них четыре различные цифры – по одной на каждой стороне каждого листа. Ваня утверждает, что все двузначные числа, которые можно получить, разложив на столе эти листы, будут простыми. Докажите, что он не прав.

Решение. Давайте поймём, какие цифры точно нельзя использовать. Мы знаем, что числа, оканчивающиеся на 0, 2, 4, 6 или 8, чётны, поэтому не могут быть простыми. А числа, оканчивающиеся на 5, кратны пяти и тоже не могут быть простыми. Значит, если Ваня нарисовал какую-то из этих цифр, то можно разложить на столе листы так, что получившееся двузначное будет заканчиваться на одну из этих цифр и поэтому будет составным.

Если же Ваня не рисовал ни одну из цифр 0, 2, 4, 5, 6, 8, то у него остается лишь четыре возможные цифры – 1, 3, 7 и 9. Значит, все они должны быть нарисованы на листах.

Если цифры 3 и 9 нарисованы на разных листах, то из них можно сложить составные числа 39 и 93.

Если же цифры 3 и 9 нарисованы на одном листе, тогда на другом нарисованы цифры 1 и 7. Но в этом случае можно сложить составное число $91 = 7 \cdot 13$.

Таким образом, в любом случае мы можем получить составное двузначное число, разложив на столе эти листы. Значит, Ваня не прав.

Задача 29. Найдите все такие натуральные числа p , что p и $(p^2 + 2)$ простые.

Первое решение. Если $p = 3$, то число $p^2 + 2 = 11$ простое.

Если же $p \neq 3$, то p не делится на 3. Рассмотрим два случая.

- Простое число p даёт остаток 1 при делении на 3. То есть $p = 3k + 1$ при некотором натуральном k . Тогда

$$\begin{aligned} p^2 + 2 &= (3k + 1)^2 + 2 = 9k^2 + 6k + 1 + 2 = \\ &= 9k^2 + 6k + 3 = 3 \cdot (3k^2 + 2k + 1) \end{aligned}$$

делится на 3 и не равно трём. Значит, число $(p^2 + 2)$ составное.

- Простое число p даёт остаток 2 при делении на 3. То есть $p = 3k + 2$ при некотором целом неотрицательном k . Тогда

$$\begin{aligned} p^2 + 2 &= (3k + 2)^2 + 2 = 9k^2 + 12k + 4 + 2 = \\ &= 9k^2 + 12k + 6 = 3 \cdot (3k^2 + 4k + 2) \end{aligned}$$

делится на 3 и не равно трём. Значит, число $(p^2 + 2)$ составное.

Поэтому числа p и $(p^2 + 2)$ одновременно являются простыми только при $p = 3$.

Второе решение. Так же, как и в первом решении, убеждаемся, что $p = 3$ подходит и что остается рассмотреть случай, когда p не делится на 3.

Из трёх последовательных чисел $(p-1)$, p и $(p+1)$ какое-то делится на 3. Мы знаем, что это не p . Значит, какое-то из чисел $(p-1)$ и $(p+1)$ делится на 3. Но тогда и произведение $(p-1)(p+1)$ делится на 3. А значит, и число

$$p^2 + 2 = p^2 - 1 + 3 = (p-1)(p+1) + 3$$

делится на 3. И при этом оно больше, чем 3. Значит, оно составное.

Поэтому числа p и $(p^2 + 2)$ одновременно являются простыми только при $p = 3$.

Ответ. $p = 3$.

Задача 30. Найдите все простые числа, которые нельзя представить в виде суммы двух составных чисел.

Решение. Простые числа 2, 3, 5, 7 не получится представить в виде суммы двух составных чисел, потому что самое маленькое составное число – 4, поэтому сумма любых двух составных не меньше, чем 8.

Следующее простое число – 11. Его тоже нельзя представить в виде суммы двух составных чисел. Действительно, есть только пять составных чисел, которые не превосходят 11, – это 4, 6, 8, 9, 10. Сумма любых двух из них либо чётна, либо не меньше, чем 13.

Число 13 уже можно представить в таком виде: $13 = 9 + 4$. Более того, понятно, что и остальные простые числа можно будет так представить.

Действительно, пусть простое число $p \geq 13$, тогда число $(p - 9)$ чётное и оно не меньше, чем 4. Значит, $(p - 9)$ – составное число. Поэтому любое простое число $p \geq 13$ можно представить в виде суммы двух составных чисел:

$$p = 9 + (p - 9).$$

В итоге мы показали, что существует только пять простых чисел: 2, 3, 5, 7 и 11, которые нельзя представить в виде суммы двух составных чисел.

Ответ. Числа 2, 3, 5, 7 и 11 нельзя представить в виде суммы двух составных чисел.

Задача 31. Правда ли, что при всех целых n число

$$n^2 + n + 41$$

является простым?

Решение. Не верится, что это так. Хотя бы потому, что иначе у нас была бы формула, с помощью которой можно было бы найти сколь угодно большие простые числа. А люди пока не научились это делать. Поэтому хочется подобрать такое целое число n , при котором число $(n^2 + n + 41)$ окажется составным.

Попробуем подставить в $(n^2 + n + 41)$ «маленькие» значения n :

$$\begin{aligned} n = 0: & \quad n^2 + n + 41 = 0 + 0 + 41 = 41 \quad - \text{простое;} \\ n = 1: & \quad n^2 + n + 41 = 1 + 1 + 41 = 43 \quad - \text{простое;} \end{aligned}$$

$$\begin{aligned}
 n = -1: \quad n^2 + n + 41 &= 1 - 1 + 41 = 41 \quad - \text{простое;} \\
 n = 2: \quad n^2 + n + 41 &= 4 + 2 + 41 = 47 \quad - \text{простое;} \\
 n = -2: \quad n^2 + n + 41 &= 4 - 2 + 41 = 43 \quad - \text{простое;} \\
 n = 3: \quad n^2 + n + 41 &= 9 + 3 + 41 = 53 \quad - \text{простое;} \\
 n = -3: \quad n^2 + n + 41 &= 9 - 3 + 41 = 47 \quad - \text{простое;} \\
 n = 4: \quad n^2 + n + 41 &= 16 + 4 + 41 = 61 \quad - \text{простое;} \\
 n = -4: \quad n^2 + n + 41 &= 16 - 4 + 41 = 53 \quad - \text{простое.}
 \end{aligned}$$

Пока получаются только простые числа. Кажется, что просто так мы не угадаем, какое значение n нужно взять.

Давайте немного преобразуем наше выражение:

$$n^2 + n + 41 = n(n + 1) + 41.$$

А в таком виде уже очевидно, что если мы возьмем такие значения n , что либо $n = \pm 41$, либо $n + 1 = \pm 41$, то получится число, делящееся на 41:

$$\begin{aligned}
 n = 41: \quad n(n + 1) + 41 &= 41 \cdot 42 + 41 = 41 \cdot 43; \\
 n = -41: \quad n(n + 1) + 41 &= (-41) \cdot (-40) + 41 = 41^2; \\
 n = 40: \quad n(n + 1) + 41 &= 40 \cdot 41 + 41 = 41^2; \\
 n = -42: \quad n(n + 1) + 41 &= (-42) \cdot (-41) + 41 = 41 \cdot 43.
 \end{aligned}$$

Поэтому не при всех целых n число $(n^2 + n + 41)$ является простым¹.

Ответ. Нет, не при всех целых n число $(n^2 + n + 41)$ является простым.

Задача 32. Докажите, что если для некоторого натурального числа n число $(n! + 1)$ делится на $(n + 1)$, то $(n + 1)$ – простое число.

¹На самом деле, если бы мы продолжили перебирать «маленькие» значения n , то это пришлось бы делать довольно долго. Дело в том, что для всех целых n от (-40) до 39 число $(n^2 + n + 41)$ является простым!

Решение. Предположим, что существует такое натуральное число n , что $(n! + 1)$ делится на $(n + 1)$, но при этом число $(n + 1)$ составное. Тогда $(n + 1)$ делится на некоторое целое число d , такое, что

$$1 < d < n + 1.$$

Но $n!$ – это произведение всех натуральных чисел, не превосходящих n , а значит, число d есть в этом произведении. То есть $n!$ делится на d . Но тогда число $(n! + 1)$ даёт остаток 1 при делении на d и не может на него делиться.

При этом по условию задачи число $(n! + 1)$ делится на $(n + 1)$, а значит, оно должно делиться и на d , которое является делителем числа $(n + 1)$. Пришли к противоречию.

Значит, не существует такого натурального числа n , что $(n! + 1)$ делится на $(n + 1)$, но при этом число $(n + 1)$ составное.

Задача 33. Пусть $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$, то есть p_k – это k -е простое число. Докажите, что для любого $n > 1$ верно неравенство:

$$p_{n+1} < p_1 p_2 \dots p_n.$$

Решение. Найдём какое-нибудь число, которое меньше, чем произведение $p_1 p_2 \dots p_n$, и при этом не делится ни на одно из простых p_1, p_2, \dots, p_n . Легко понять, что подойдёт число

$$p_1 p_2 \dots p_n - 1.$$

Действительно, оно не делится ни на одно из простых p_k (где k от 1 до n), потому что оно на единицу меньше числа, кратного p_k .

Таким образом, число $(p_1 p_2 \dots p_n - 1)$ либо является простым, которое больше всех чисел p_k (где k от 1 до n), а значит, оно по крайней мере $(n + 1)$ -е простое число. То есть $p_{n+1} \leq p_1 p_2 \dots p_n - 1$. Либо $(p_1 p_2 \dots p_n - 1)$ – составное число, которое не делится ни на одно из простых p_k (где k от 1 до n). Но оно должно делиться на какое-нибудь простое число p (см. задачу 22 на стр. 63). Тогда p не равно ни одному из p_k (где k от 1 до n), то есть оно по крайней мере $(n + 1)$ -е простое число.

В любом случае мы получаем, что

$$p_{n+1} < p_1 p_2 \dots p_n.$$

Что и требовалось доказать.

А следующие задачи попробуйте решить самостоятельно.

Задача 34. Найдите все такие натуральные p , что числа p и $(3p + 1)$ простые.

Задача 35. Найдите наименьшее простое число, которое можно представить в виде суммы семи различных простых чисел.

Задача 36. Найдите все простые числа, которые можно представить и как сумму двух простых чисел, и как разность двух простых чисел.

Задача 37. Докажите, что остаток при делении простого числа на 30 – это либо простое число, либо 1.

Задача 38. Докажите, что если натуральное число n больше четырёх и при этом пара $(n - 1; n + 1)$ – числа-близнецы, то n делится на 6.

ГЛАВА 3

ОСНОВНАЯ
ТЕОРЕМА
АРИФМЕТИКИ

В этой главе поговорим про один важный факт, который постоянно используется в школе, но так исторически сложилось, что большинство школьников даже не знают о его существовании. То есть они его постоянно используют, но на каком-то интуитивном уровне. Они не понимают, что это не что-то само собой разумеющееся, а довольно сложное утверждение, которое нужно доказывать.

Дело в том, что соответствующий раздел математики изучается в школе в 6–7 классах, когда школьники ещё готовы безоговорочно верить учителю, а учителю проще не акцентировать внимание на том, что это действительно сложная и важная теорема.

Хотя есть и такие учителя, которые честно формулируют этот факт и честно говорят: «Мы примем его на веру, потому что доказательство слишком сложно для вашего возраста». Например, когда я преподавал математику в школе, я именно так и делал.

Мне такой подход к преподаванию в школе сложных тем видится более правильным: всякий раз, когда понимаешь, что аудитория не готова к тому, чтобы понять сложное доказательство некоторого важного утверждения, не делать вид, что оно очевидно и нечего тут доказывать, а честно признать, что доказательство сложное и мы пока его опустим.

В результате все школьники делятся на две группы. Большая часть школьников¹ вообще не задумывается о существовании этого факта, хотя они пользуются им постоянно.

Остальные же знают, что есть такой факт, что это сложная теорема, доказательство которой они никогда не видели и вряд ли увидят, потому что она выходит за рамки школьной программы. Сам я, например, когда был школьником, был из этой второй группы. Доказательство теоремы я узнал уже сильно позже.

На самом деле есть третья, очень маленькая группа школьников – те, кто учится в сильных математических классах или просто сам глубоко интересуется математикой и ему рассказали доказательство этой теоремы. Хотя, наверно, не в 6–7 классах, а когда они были уже чуть постарше. Но их настолько мало, что можно считать, что таких почти нет.

Надеюсь, что этого затянувшегося введения будет достаточно, чтобы вы поняли, что это действительно не очень простое утверждение, и совсем не страшно, если вы с первого раза не поймёте некото-

¹ На самом деле не только школьников, но и студентов профильных вузов, и даже учителей.

рые шаги доказательства. Более того, даже если вы его полностью пропустите, вы всё равно будете понимать содержание всех остальных глав этой книги.

Давайте уже перейдём к самому факту.

Основная теорема арифметики. Любое натуральное число, отличное от 1, единственным образом (с точностью до порядка сомножителей) можно разложить на произведение простых чисел¹.

Таким образом, теорема утверждает, что любое натуральное число, кроме 1, можно представить в виде произведения простых чисел и существует только один набор простых чисел, произведение которых даёт это натуральное число.

То есть, по сути, тут два утверждения – *существование* разложения на простые множители и его *единственность*.

Так вот, у школьников обычно не возникает вопросов по поводу существования разложения на простые: каждый раз, когда им нужно было

¹ При этом если само число простое, то мы считаем, что оно представляется в виде «произведения», в котором один «множитель».

Иногда в формулировке этой теоремы даже пишут «можно разложить на произведение **нескольких** простых чисел». В этом плане в математике слово «несколько» часто используется не в том смысле, как многие привыкли.

Для обычных людей «несколько» – это некоторое небольшое количество, больше двух, но меньше десяти, например. Но в задачах по математике фраза «несколько чисел» означает, что чисел может быть любое конечное количество, большее нуля. Может быть как одно число, так и миллион чисел.

разложить на множители, у них это получалось! Когда их просят разложить число на простые множители, то они просто берут и раскладывают. Они обычно не задумываются о том, любое ли число можно разложить. Для них это так же естественно, как дважды два – четыре.

А уж о единственности разложения вообще никто не задумывается. Если спросить школьников, делится ли число $5 \cdot 7 \cdot 11 \cdot 13$ на 3, все сразу ответят: «Конечно, нет! Ведь в разложении на простые множители этого числа нет множителя 3».

Но почему, если в разложении числа на простые нет множителя 3, то число не делится на 3? Если мы не знаем основной теоремы арифметики, то как понять, почему такое число не делится на 3, не вычисляя его в явном виде и не проверяя делимость непосредственно? Может быть, у него есть какое-то другое разложение и это число равно, например, ещё и $3 \cdot 19 \cdot 89$.

Вот это надо чётко понять, что если число равно произведению простых 5, 7, 11 и 13, то из этого никак напрямую не следует, что оно не делится на 3.

И вот тут, если вы достаточно уверенно уже решаете задачи по теории чисел, но впервые осознали, что основная теорема арифметики – это не какое-то очевидное утверждение, то можете поставить эксперимент. Закройте книгу и попробуйте самостоятельно доказать эту теорему.

Почти наверняка вы «докажете» её. То есть вам покажется, что вы её доказали. Но если вы внимательнее изучите своё доказательство, то, скорее всего, вы обнаружите, что внутри доказательства теоремы вы несколько раз её же и используете. Вам

очень сложно её не использовать. Для вас это что-то само собой разумеющееся. Вам будет нелегко перестать её использовать, даже когда вы её доказываете.

Вы настолько верите в это утверждение, что не задумываясь говорите, что «если делится на 2 и на 3, то оно делится на 6». Хотя это не так уж и очевидно¹, если не использовать основную теорему арифметики!

Приступим к доказательству!

ДОКАЗАТЕЛЬСТВО СУЩЕСТВОВАНИЯ РАЗЛОЖЕНИЯ НА ПРОСТЫЕ МНОЖИТЕЛИ

Про маленькие числа мы точно знаем, что их можно разложить на простые множители:

$$\begin{array}{llll} 2 = 2; & 3 = 3; & 4 = 2 \cdot 2; & 5 = 5; \\ 6 = 2 \cdot 3; & 7 = 7; & 8 = 2 \cdot 2 \cdot 2; & 9 = 3 \cdot 3; \\ 10 = 2 \cdot 5; & 11 = 11; & 12 = 2 \cdot 2 \cdot 3; & \dots \end{array}$$

Предположим, что мы не сможем так продолжать до бесконечности. И пусть n – первое число, которое невозможно разложить. То есть для всех натуральных чисел от 2 до $(n - 1)$ каждое число раскладывается в произведение простых, а число n уже не раскладывается.

¹Мы сделаем это в задаче 39 на стр. 95

Посмотрим на это число. Если оно простое, то оно уже разложилось в произведение простых. Значит, оно составное.

Тогда его можно представить в виде $n = ab$, где a и b – натуральные числа, которые больше, чем 1, но меньше, чем число n . Но мы знаем, что каждое число от 2 до $(n - 1)$ раскладывается в произведение простых. Значит, и числа a и b так раскладываются. Но тогда и число n можно представить в виде произведения всех множителей из разложения числа a и всех множителей числа b .

Таким образом, наше предположение, что найдётся число, которое не получится разложить, было ложным. Другими словами, мы доказали, что любое натуральное число, отличное от 1, можно разложить на произведение простых чисел.

Эта часть доказательства оказалась не такой уж и сложной¹.

МИР БЕЗ ОСНОВНОЙ ТЕОРЕМЫ АРИФМЕТИКИ

Сейчас бы самое время перейти к доказательству единственности разложения на простые множители, но давайте немного отвлечёмся и поговорим о том, как было бы сложно решать задачи, если бы нельзя было использовать основную теорему арифметики.

¹Можно было бы доказать существование разложения на простые множители, воспользовавшись задачей 22 на стр. 63.

Задача 39. Докажите, что если натуральное число делится на 2 и на 3, то оно делится на 6.

Решение. Давайте поймём, что мы знаем. А знаем мы лишь то, что если натуральное число n делится на 2 и на 3, то существуют такие k и m , что $n = 2k$ и $n = 3m$.

Для того чтобы доказать, что n делится на 6, можно либо доказать, что k делится на 3, либо доказать, что m делится на 2. Это не так сложно сделать, перебрав остатки (например, предположив, что m – нечётное число, и придя к противоречию), но мы обсудим более универсальный метод.

Так как $n = 2k$ и $n = 3m$, то $3n = 6k$ и $2n = 6m$. Значит,

$$n = 3n - 2n = 6k - 6m = 6(k - m)$$

делится на 6.

Видите, даже для 2 и 3 получается довольно содержательное рассуждение. Но давайте посмотрим, как это рассуждение переносится на более сложные случаи.

Задача 40. Докажите, что если натуральное число делится на 10 и на 13, то оно делится на 130.

Решение. Пусть для числа n верно, что

$$n \div 10, \quad n \div 13.$$

Тогда

$$13n \div 130, \quad 10n \div 130.$$

Следовательно, $13n - 10n = 3n$ делится на 130. Но тогда и число $3 \cdot 3n = 9n$ делится на 130.

Осталось заметить, что из делимости чисел $10n$ и $9n$ на 130, следует, что $10n - 9n = n$ делится на 130.

Попробуйте самостоятельно, повторив те же рассуждения, решить следующие задачи.

Задача 41. Докажите, что если натуральное число делится на 5 и на 7, то оно делится на 35.

Задача 42. Докажите, что если натуральное число делится на 7, на 11 и на 13, то оно делится на 1001.

По этим задачам видно, что без использования основной теоремы арифметики даже такие «очевидные» вещи не так легко доказать. Но давайте попробуем сформулировать и доказать общее утверждение.

Утверждение. Пусть натуральное число делится на взаимно простые числа a и b , тогда оно делится на произведение ab .

Доказательство. Пусть для числа n верно, что

$$n \div a, \quad n \div b.$$

Тогда

$$bn \div ab, \quad an \div ab.$$

Следствие соотношения Безу (см. стр. 52) утверждает, что если натуральные числа a и b взаимно просты, то найдутся такие целые числа m и k , что

$$ma + kb = 1.$$

Домножив это равенство на n , получим, что

$$man + kbn = n.$$

Но числа an и bn делятся на ab , а значит, и число

$$n = m \cdot an + k \cdot bn$$

делится на ab .

Таким образом, мы доказали, что если натуральное число n делится на взаимно простые числа a и b , то оно делится и на ab .

Замечание. Обратите внимание, что здесь существенную роль играет взаимная простота чисел a и b . Так, например, если число делится на 4 и на 6, то оно не обязано делиться на $24 = 4 \cdot 6$. Так, числа 12, 36 и 60 делятся на 4 и на 6, но не делятся на 24.

Вообще соотношение Безу – очень мощный факт. С помощью него, например, мгновенно доказывается следующая важная лемма.

Лемма Евклида. Пусть произведение двух натуральных чисел делится на простое число, тогда по крайней мере одно из них делится на это простое число.

Доказательство. Пусть m и n – натуральные числа, p – простое и mn делится на p . Предположим, что m не делится на p . Тогда m и p взаимно простые числа. Действительно, число p , кроме единицы, делится только само на себя, а число m не делится на p .

Как мы помним, следствие соотношения Безу утверждает, что для взаимно простых m и p найдутся такие целые числа k и ℓ , что

$$km + \ell p = 1.$$

Домножив это равенство на n , мы получим, что

$$ktn + \ell pn = n.$$

Но tn делится на p , значит, и число

$$n = k \cdot tn + \ell n \cdot p$$

делится на p .

Таким образом, мы доказали, что если произведение tn двух натуральных чисел делится на простое число p , то по крайней мере одно из них делится на p .

На самом деле, лемму Евклида легко обобщить на произвольное количество множителей. Давайте это сделаем.

Следствие из леммы Евклида. Пусть произведение нескольких натуральных чисел делится на простое число, тогда по крайней мере одно из них делится на это простое число.

Доказательство. Пусть n_1, n_2, \dots, n_k – натуральные числа, p – простое и произведение $n_1 n_2 \dots n_k$ делится на p .

Но число $n_1 n_2 \dots n_k$ можно представить как произведение двух натуральных чисел – n_1 и $n_2 n_3 \dots n_k$. Тогда из леммы Евклида следует, что если n_1 не делится на p , то $n_2 n_3 \dots n_k$ делится на p .

Но число $n_2 n_3 \dots n_k$ опять можно представить в виде произведения двух натуральных чисел – n_2 и $n_3 n_4 \dots n_k$. И из леммы Евклида следует, что если n_2 не делится на p , то $n_3 n_4 \dots n_k$ делится на p .

И так далее. Вот так, «отрывая» по одному множителю, мы в какой-то момент найдем множитель, который делится на p .

Таким образом, мы доказали, что если произведение $n_1 n_2 \dots n_k$ нескольких натуральных чисел делится на простое число p , то по крайней мере одно из них делится на p .

Вот такой вот мир без основной теоремы арифметики. Без неё приходится доказывать даже те утверждения, которые вы привыкли считать очевидными.

Но давайте уже перейдём к доказательству единственности разложения на простые множители.

ДОКАЗАТЕЛЬСТВО ЕДИНСТВЕННОСТИ РАЗЛОЖЕНИЯ НА ПРОСТЫЕ МНОЖИТЕЛИ

Так же как при доказательстве существования разложения, заметим, что для маленьких чисел единственность разложения очевидна:

$$\begin{array}{llll} 2 = 2; & 3 = 3; & 4 = 2 \cdot 2; & 5 = 5; \\ 6 = 2 \cdot 3; & 7 = 7; & 8 = 2 \cdot 2 \cdot 2; & \dots \end{array}$$

Предположим, что не для всех чисел разложение единственно. И пусть n – первое число, которое можно разложить более чем одним способом. То есть каждое из натуральных чисел от 2 до $(n - 1)$

раскладывается в произведение простых единственным образом, а для числа n есть по крайней мере два разных разложения:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots = q_1 \cdot q_2 \cdot q_3 \cdot \dots$$

Заметим, что не может так оказаться, что простое число p_1 встречается в обоих разложениях. Иначе на него можно было бы сократить, и мы бы пришли к тому, что число $\frac{n}{p_1}$ имеет два различных разложения на простые числа. Но мы знаем, что числа, меньшие n , раскладываются на множители единственным образом.

С другой стороны, из равенства $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$ следует, что число n делится на p_1 . Значит, и произведение $q_1 \cdot q_2 \cdot q_3 \cdot \dots$ делится на p_1 . Но следствие из леммы Евклида (см. стр. 98) говорит о том, что тогда один из множителей q_k делится на p_1 . Но каждое q_k — это простое число, и оно не равно p_1 , а значит, не может делиться на p_1 . Противоречие!

Значит, наше предположение о том, что не для всех чисел разложение единственно, было ложным.

На первый взгляд может показаться, что это доказательство единственности разложения числа на простые множители получилось совсем простым. Но так кажется только потому, что к этому моменту мы уже обсудили:

- алгоритм Евклида;
- соотношение Безу и следствие из него;
- лемму Евклида и следствие из неё.

Но давайте попробуем доказать «в лоб», без каких-либо предварительных фактов.

ДРУГОЕ ДОКАЗАТЕЛЬСТВО ЕДИНСТВЕННОСТИ РАЗЛОЖЕНИЯ НА ПРОСТЫЕ МНОЖИТЕЛИ

Так же как и в предыдущем доказательстве, предположим, что не для всех чисел разложение на простые множители единственно. И пусть n – первое число, которое можно разложить более чем одним способом:



$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots = q_1 \cdot q_2 \cdot q_3 \cdot \dots$$

Чтобы было проще рассуждать, будем считать, что в каждом из разложений множители упорядочены:

$$p_1 \leq p_2 \leq p_3 \leq \dots, \quad q_1 \leq q_2 \leq q_3 \leq \dots$$

Точно так же, как и в предыдущем доказательстве, заметим, что не может так оказаться, что какое-нибудь простое число r встречается в обоих разложениях, иначе на него можно было бы сократить и мы бы пришли к тому, что число $\frac{n}{r}$ имеет два различных разложения на простые числа. Но числа, меньшие n , раскладываются на множители единственным образом.

То есть данные эти два разложения абсолютно разные – нет ни одного простого числа, которое бы-

ло бы одновременно и в том, и в другом разложении.

Заметим, что число n точно не является простым (хотя бы потому, что оно делится на два разных простых числа — p_1 и q_1). Поэтому в разложении

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$$

не меньше двух множителей.

Значит, $n \geq p_1 p_2 \geq p_1^2$. Аналогично получаем, что $n \geq q_1^2$. Итак, мы знаем, что

$$n \geq p_1^2, \quad n \geq q_1^2.$$

При этом очевидно, что хотя бы одно из этих неравенств строгое, потому что иначе $n = p_1^2 = q_1^2$, а это означает, что $p_1 = q_1$, что неверно.

Пусть для определенности мы знаем, что

$$n \geq p_1^2, \quad n > q_1^2.$$

Тогда, если перемножить эти неравенства, мы получим, что

$$n^2 > p_1^2 \cdot q_1^2 = (p_1 q_1)^2.$$

То есть $n > p_1 q_1$.

Рассмотрим число $(n - p_1 q_1)$. Оно точно натуральное, потому что целое и $n > p_1 q_1$. При этом число $n = p_1 \cdot (p_2 \cdot p_3 \cdot \dots)$ делится на p_1 и число $p_1 q_1$ делится на p_1 . Значит, и число $(n - p_1 q_1)$ делится на p_1 . Аналогично замечаем, что n и $p_1 q_1$ делится на q_1 . Значит, число $(n - p_1 q_1)$ делится на q_1 .

Но число $(n - p_1 q_1)$, очевидно, меньше, чем n , а все числа, меньшие n , раскладываются на простые множители единственным образом.

Давайте докажем, что если про некоторое натуральное число k известно, что оно раскладывается в произведение простых чисел единственным образом и при этом оно делится на простое число p , то это простое число обязано входить в это разложение.

Предположим, что данное утверждение неверно. Пусть единственное разложение $k = r_1 \cdot r_2 \cdot r_3 \cdot \dots$ не содержит простого числа p и существует такое натуральное число m , что $k = pm$. Но число m можно представить в виде произведения простых. А значит, мы получили другое разложение числа k на простые множители. Пришли к противоречию!

Всё, мы доказали, что если некоторое число раскладывается в произведение простых чисел единственным образом и при этом делится на некоторое простое число, то это простое число обязано входить в это разложение.

А мы знаем, что число $(n - p_1 q_1)$ раскладывается на простые множители единственным образом и при этом оно делится на p_1 и на q_1 . Значит, в его разложении на простые множители есть p_1 и q_1 :

$$n - p_1 q_1 = p_1 \cdot q_1 \cdot \dots$$

Тогда число $(n - p_1 q_1)$ делится на $p_1 q_1$. Но число $p_1 q_1$ тоже делится на $p_1 q_1$. Поэтому и число

$$n = (n - p_1 q_1) + p_1 q_1$$

делится на $p_1 q_1$.

Это означает, что найдется такое натуральное число ℓ , что $n = p_1 q_1 \ell$. Но тогда число

$$\frac{n}{p_1} = p_2 \cdot p_3 \cdot \dots = q_1 \ell$$

меньше n , и должно раскладываться на простые множители единственным образом.

Но, разложив число ℓ на простые множители, мы получим разложение числа $\frac{n}{p_1}$, отличное от

$$\frac{n}{p_1} = p_2 \cdot p_3 \cdot \dots,$$

потому что в нём есть простое число q_1 . Пришли к противоречию!

Всё, мы доказали единственность разложения! Мы предположили, что n – самое маленькое число, для которого разложение не единственно, и нашли меньшее число, для которого оно тоже не единственно.

Думаю, что теперь вам понятно, почему про это не говорят в 6–7 классах, когда начинают обсуждать вопросы делимости и разложения на простые множители. Даже старшекласснику будет не очень просто понять эти доказательства.

МИР ЧЁТНЫХ ЧИСЕЛ

У многих школьников, узнавших о том, что основная теорема арифметики – это не какой-то самоочевидный факт, что её нужно доказывать и это доказательство довольно сложное, часто возникает некоторое удивление. Это же что-то, к чему все привыкли, зачем это доказывать? Как это может быть неверно?

Давайте в этом разделе поговорим про что-то очень похожее на разложение на простые множители, и вы увидите, что то, что кажется очевидным, иногда может оказаться неверным.

Представьте себе «мир чётных чисел». То есть такой мир, в котором есть только чётные числа. Чётные числа можно складывать, вычитать умножать, и при этом результатом будет снова чётное число. В этом плане этот мир почти ничем не отличается от обычных целых чисел.

Там можно ввести понятие «делимости», сказав, что чётное число a делится на положительное чётное число b , если существует такое чётное число k , что $a = kb$.

Например, число 20 делится на 10, потому что $20 = 2 \cdot 10$. Но при этом 20 не делится на 4, потому что нет такого чётного числа k , что $20 = k \cdot 4$.

Может потребоваться некоторое время, чтобы к этому привыкнуть, но в этом мире действительно число 20 не делится на 4.

Более того, в этом мире даже число 2 не делится на 2. Потому что нет такого чётного числа k , что $2 = k \cdot 2$. То есть в этом мире число 2 не делится ни на что. И не только 2. Ни на что не будут делиться, например, числа 6 и 10.

Задача 43. Найдите все числа из «мира чётных чисел», которые в этом мире не делятся ни на одно число.

Теперь давайте для этого мира введем понятия «простых» чисел. Естественно назвать простыми числами все «неделимые кирпичики»:

2, 6, 10, 14, 18, 22, ...

Тогда остальные числа будут раскладываться в произведение простых:

$$\begin{array}{llll} 2 = 2; & 4 = 2 \cdot 2; & 6 = 6; & 8 = 2 \cdot 2 \cdot 2; \\ 10 = 10; & 12 = 2 \cdot 6; & 14 = 14; & 16 = 2 \cdot 2 \cdot 2 \cdot 2; \\ 18 = 18; & 20 = 2 \cdot 10; & 22 = 22; & \dots \end{array}$$

Так можно продолжать довольно долго. И на первый взгляд получается всё ровно то же, что и для натуральных чисел: есть «простые» числа и каждое число однозначно раскладывается в произведение простых. Согласны?

Думаю, что многие из вас согласятся с тем, что это выглядит довольно естественно. По крайней мере, не менее естественно, чем соответствующее утверждение для натуральных чисел. Значит, и тут должна быть верна своя «основная теорема арифметики».

И действительно, довольно долго перебирая числа из этого «мира», вы будете убеждаться, что здесь тоже работает своя «основная теорема арифметики»:

$$\begin{array}{llll} 24 = 2 \cdot 2 \cdot 6; & 26 = 26; & 28 = 2 \cdot 14; & 30 = 30; \\ 32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2; & 34 = 34; & \dots & \end{array}$$

И всё будет хорошо, пока вы не дойдёте до числа 36:

$$36 = 2 \cdot 18 = 6 \cdot 6.$$

Оказывается, что для него не выполняется «основная теорема арифметики» – его можно двумя способами представить в виде произведения «простых» чисел.

А дальше снова всё будет однозначно раскладываться:

$$38 = 38; \quad 40 = 2 \cdot 2 \cdot 10; \quad 42 = 42; \quad 44 = 2 \cdot 22;$$

$$46 = 46; \quad 48 = 2 \cdot 2 \cdot 2 \cdot 6; \quad 50 = 50; \quad 52 = 2 \cdot 26;$$

$$54 = 54; \quad 56 = 2 \cdot 2 \cdot 14; \quad 58 = 58; \quad \dots$$

Пока вы не дойдёте до числа 60:

$$60 = 2 \cdot 30 = 6 \cdot 10.$$

Думаю, что теперь вы и сами сможете придумать ещё несколько чисел из этого «мира», для которых не будет выполняться единственность разложения на «простые» числа.

Задача 44. Найдите ещё пять чисел, у которых в «мире чётных чисел» нет единственности разложения на «простые» множители.

Более того, есть числа, у которых этих разложений может быть довольно много. Например, для числа 840 есть целых пять разложений на «простые» множители:

$$840 = 2 \cdot 2 \cdot 210;$$

$$840 = 2 \cdot 6 \cdot 70;$$

$$840 = 2 \cdot 10 \cdot 42;$$

$$840 = 2 \cdot 14 \cdot 30;$$

$$840 = 6 \cdot 10 \cdot 14.$$

Задача 45. Найдите число, у которого в «мире чётных чисел» есть более десяти разложений на «простые» множители.

Ну что? Теперь вам уже не кажется, что основная теорема арифметики – это что-то само собой разумеющееся? Как мы видим, в других «мирах» она может и не соблюдаться.

КАНОНИЧЕСКОЕ РАЗЛОЖЕНИЕ ЧИСЛА НА ПРОСТЫЕ МНОЖИТЕЛИ

Благодаря основной теореме арифметики мы теперь знаем, что любое натуральное число, большее единицы, единственным образом раскладывается в произведение простых. Но как именно можно получить это разложение?

Если число очень большое, то его не так просто разложить на простые множители. В частности, на этом факте основан алгоритм шифрования RSA, который мы с вами обсудим чуть позже (см. стр. 218). Здесь же мы поговорим про более простые случаи.

Пусть, например, нам нужно разложить на простые множители число 5355. Можно заметить, что это число заканчивается на 5, а значит, оно делится на 5 (см. признак делимости на 5 на стр. 26). Разделив 5355 на 5, получим 1071. То есть $5355 = 5 \cdot 1071$.

Значит, мы свели задачу к разложению на простые множители числа 1071. Можно заметить, что его сумма цифр $1 + 0 + 7 + 1 = 9$ делится на 3, а значит, и само число делится на 3 (см. признак делимости на 3 на стр. 29). Разделив 1071 на 3, получим 357. То есть $1071 = 3 \cdot 357$.

Теперь мы свели задачу к разложению на простые множители числа 357. Заметим, что и его сум-

ма цифр $3 + 5 + 7 = 15$ делится на 3, а значит, и само число 357 делится на 3. Разделив 357 на 3, получим 119. То есть $357 = 3 \cdot 119$.

В итоге нам осталось разложить на простые множители число 119. Никакие известные нам признаки делимости с ним не справляются, поэтому просто переберём все маленькие простые числа. На 2, на 3 и на 5 оно не делится, а попробовав разделить на 7, получаем, что $119 = 7 \cdot 17$. А 17 – это уже простое число.

В итоге мы получили, что

$$\begin{aligned} 5355 &= 5 \cdot 1071 = 5355 = 5 \cdot 3 \cdot 357 = \\ &= 5 \cdot 3 \cdot 3 \cdot 119 = 5 \cdot 3 \cdot 3 \cdot 7 \cdot 17. \end{aligned}$$

Но на практике совсем необязательно так подробно всё расписывать. Обычно это записывают так:

5355	5
1071	3
357	3
119	7
17	17
1	

Слева пишут число, а справа – простое число, на которое оно делится. Результат деления пишут слева и продолжают процедуру, пока слева не получится 1. Тогда исходное число равно произведению простых из правой части.

Из основной теоремы арифметики следует, что различные представления одного и того же составного числа в виде произведения простых чисел могут отличаться лишь порядком множителей. Так,

например, разложение числа 5355 на простые множители может иметь и такой вид:

$$5355 = 5 \cdot 3 \cdot 3 \cdot 7 \cdot 17,$$

и такой:

$$5355 = 3 \cdot 3 \cdot 5 \cdot 7 \cdot 17.$$

Для того чтобы избежать такой неоднозначности, принято записывать простые множители в порядке возрастания. При этом если встречаются одинаковые простые множители, то эти простые числа пишут в соответствующей степени.

Такую упорядоченную запись назвали каноническим разложением числа на простые множители. Например, каноническое разложение 5355 имеет вид:

$$5355 = 3^2 \cdot 5 \cdot 7 \cdot 17,$$

а, например, для числа 9000 каноническим будет разложение

$$9000 = 2^3 \cdot 3^2 \cdot 5^3.$$

Давайте теперь везде, где это возможно, стараться использовать именно каноническое разложение на множители.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ И НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

В главе 1 мы уже говорили с вами про *наибольший общий делитель* (см. стр. 48) и даже показали,

как можно его найти при помощи алгоритма Евклида. Здесь же обсудим, как можно вычислить наибольший общий делитель, используя разложение чисел на простые множители. Покажем, как это делать, на примере конкретных чисел.

Задача 46. Найдите НОД(3780, 6600).

Решение. Разложим числа 3780 и 6600 на простые множители:

3780	2	6600	2
1890	2	3300	2
945	5	1650	2
189	3	825	5
63	3	165	5
21	3	33	3
7	7	11	11
1		1	

Значит,

$$3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7, \quad 6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11.$$

Из основной теоремы арифметики следует, что любой делитель числа 3780 в разложении на простые может иметь лишь множители 2, 3, 5 и 7, а любой делитель числа 6600 в разложении на простые может иметь лишь множители 2, 3, 5 и 11. Значит, любой их общий делитель в разложении на простые может иметь лишь множители 2, 3 и 5.

Итак, любой общий делитель чисел 3780 и 6600 имеет вид $2^\ell \cdot 3^m \cdot 5^n$, где ℓ, m и n – целые неотрицательные числа. При этом:

- и $3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$, и $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$ должны делиться на 2^ℓ , значит, $\ell \leq 2$ (иначе 3780 не будет делиться на 2^ℓ);

- и $3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$, и $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$ должны делиться на 3^m , значит, $m \leq 1$ (иначе 6600 не будет делиться на 3^m);
- и $3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$, и $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$ должны делиться на 5^n , значит, $n \leq 1$ (иначе 3780 не будет делиться на 5^n).

Таким образом, общий делитель будет наибольшим, если $\ell = 2$, $m = 1$ и $n = 1$. То есть

$$\begin{aligned}\text{НОД}(3780, 6600) &= \text{НОД}(2^2 \cdot 3^3 \cdot 5 \cdot 7, 2^3 \cdot 3 \cdot 5^2 \cdot 11) = \\ &= 2^2 \cdot 3 \cdot 5 = 60.\end{aligned}$$

Ответ. $\text{НОД}(3780, 6600) = 60$.

После решения этой задачи становится ясно, что нужно делать для нахождения наибольшего общего делителя двух чисел, если мы смогли разложить их на простые множители. Давайте сформулируем общий алгоритм.

Для нахождения наибольшего общего делителя двух натуральных чисел a и b нужно разложить их на простые множители и вычислить произведение общих простых множителей в наименьших степенях, с которыми эти множители входят в разложения a и b .

Теперь вы сможете самостоятельно справиться со следующими задачами.

Задача 47. Найдите $\text{НОД}(4000, 4608)$.

Задача 48. Найдите

$$\text{НОД}(2^3 \cdot 5^2 \cdot 11^2 \cdot 13^3 \cdot 23^2 \cdot 29, 2^5 \cdot 3^3 \cdot 7^2 \cdot 11 \cdot 17^2 \cdot 23).$$

Перейдём теперь к следующему важному понятию – *наименьшему общему кратному*.

Общим кратным натуральных чисел a и b называется число, которое делится на каждое из этих чисел. *Наименьшее общее кратное* обозначается $\text{НОК}(a, b)$ или просто $[a, b]$.

Например, у чисел 15 и 12 есть много общих кратных:

$$180, \quad 300, \quad 9000, \quad \dots$$

Давайте поймём, какое общее кратное будет наименьшим. Для этого перечислим все числа, которые кратны 15:

$$\begin{array}{lll} 15 \cdot 1 = 15, & 15 \cdot 2 = 30, & 15 \cdot 3 = 45, \\ 15 \cdot 4 = 60, & 15 \cdot 5 = 75, & \dots, \end{array}$$

и все числа, которые кратны 12:

$$\begin{array}{lll} 12 \cdot 1 = 12, & 12 \cdot 2 = 24, & 12 \cdot 3 = 36, \\ 12 \cdot 4 = 48, & 12 \cdot 5 = 60, & \dots, \end{array}$$

пока не найдём наименьшее кратное, которое встретится и у 15, и у 12. Это число 60. Поэтому

$$\text{НОК}(12, 15) = 60.$$

Но такой подход к нахождению наименьшего общего кратного удобен лишь для небольших чисел. Давайте обсудим, как можно его найти, используя разложение на простые множители. Рассмотрим следующий пример с теми же числами, что и в задаче 46.

Задача 49. Найдите НОК(3780, 6600).

Решение. При решении задачи 46 мы уже разложили числа 3780 и 6600 на простые множители:

$$3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7, \quad 6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11.$$

Из основной теоремы арифметики следует, что любое кратное числа 3780 в разложении на простые должно иметь $2^2 \cdot 3^3 \cdot 5 \cdot 7$, а любое кратное числа 6600 в разложении на простые должно иметь $2^3 \cdot 3 \cdot 5^2 \cdot 11$. Значит, у любого их общего кратного:

- простой множитель 2 должен быть в степени, не меньшей, чем 3;
- простой множитель 3 должен быть в степени, не меньшей, чем 3;
- простой множитель 5 должен быть в степени, не меньшей, чем 2;
- простой множитель 7 должен быть в степени, не меньшей, чем 1;
- простой множитель 11 должен быть в степени, не меньшей, чем 1.

Таким образом,

$$\begin{aligned} \text{НОК}(3780, 6600) &= \text{НОК}(2^2 \cdot 3^3 \cdot 5 \cdot 7, 2^3 \cdot 3 \cdot 5^2 \cdot 11) = \\ &= 2^3 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 = 8 \cdot 27 \cdot 25 \cdot 77 = \\ &= 27 \cdot 200 \cdot 77 = 5400 \cdot 77 = 415\,800. \end{aligned}$$

Ответ. $\text{НОК}(3780, 6600) = 415\,800$.

Давайте сформулируем общий алгоритм нахождения наименьшего общего кратного двух

чисел, если нам удалось разложить на простые множители каждое из них.

Для нахождения наименьшего общего кратного двух натуральных чисел a и b нужно разложить их на простые множители и вычислить произведение всех простых множителей, входящих хотя бы в одно из разложений, в наибольших из степеней, с которыми эти множители входят в разложение a и b .

Посмотрите, как это работает на примере следующей задачи.

Задача 50. Найдите НОК(144, 300).

Связь между НОД и НОК. Давайте на примере тех же чисел 3780 и 6600 внимательно проследим, что из их разложений на простые множители пошло в НОД, а что в НОК:

$$\text{НОД : } 3780 = \boxed{2^2} \cdot 3^3 \cdot \boxed{5} \cdot 7, \quad 6600 = 2^3 \cdot \boxed{3} \cdot 5^2 \cdot 11.$$

$$\text{НОК : } 3780 = 2^2 \cdot \boxed{3^3} \cdot 5 \cdot \boxed{7}, \quad 6600 = \boxed{2^3} \cdot 3 \cdot \boxed{5^2} \cdot \boxed{11}.$$

Таким образом, мы видим, что в НОК пошло всё то, что не пошло в НОД. Иными словами,

$$\text{НОД}(3780, 6600) \cdot \text{НОК}(3780, 6600) = 3780 \cdot 6600.$$

Давайте докажем, что так будет всегда.

Утверждение. Пусть a и b – натуральные числа, тогда

$$\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab.$$

Доказательство. Пусть p_1, p_2, p_3, \dots – все простые, которые входят в разложение на простые множители хотя бы одного из чисел a и b . Тогда числа a и b можно представить как

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \dots,$$

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \dots,$$

где $\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3, \dots$ – целые неотрицательные числа.

Например, для чисел 3780 и 6600 это выглядит так:

$$3780 = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 11^0,$$

$$6600 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0 \cdot 11^1.$$

Обозначим через γ_1 меньшее из чисел α_1 и β_1 , а через δ_1 – большее из этих чисел (если $\alpha_1 = \beta_1$, то считаем, что $\gamma_1 = \alpha_1, \delta_1 = \beta_1$). Аналогично определим числа $\gamma_2, \delta_2, \gamma_3, \delta_3, \dots$:

$$\begin{aligned} \gamma_1 &= \min\{\alpha_1, \beta_1\}, & \delta_1 &= \max\{\alpha_1, \beta_1\}, \\ \gamma_2 &= \min\{\alpha_2, \beta_2\}, & \delta_2 &= \max\{\alpha_2, \beta_2\}, \\ \gamma_3 &= \min\{\alpha_3, \beta_3\}, & \delta_3 &= \max\{\alpha_3, \beta_3\}, \\ & & \dots & \end{aligned}$$

Тогда

$$\text{НОД}(a, b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot p_3^{\gamma_3} \cdot \dots,$$

$$\text{НОК}(a, b) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot p_3^{\delta_3} \cdot \dots$$

Это означает, что

$$\text{НОД}(a, b) \cdot \text{НОК}(a, b) = p_1^{\gamma_1 + \delta_1} \cdot p_2^{\gamma_2 + \delta_2} \cdot p_3^{\gamma_3 + \delta_3} \cdot \dots$$

Осталось заметить, что $\gamma_1 + \delta_1 = \alpha_1 + \beta_1$, так как γ_1 – меньшее из чисел α_1 и β_1 , а δ_1 – большее из этих чисел. Аналогично $\gamma_2 + \delta_2 = \alpha_2 + \beta_2$, $\gamma_3 + \delta_3 = \alpha_3 + \beta_3$ и так далее. Поэтому

$$\begin{aligned} & p_1^{\gamma_1+\delta_1} \cdot p_2^{\gamma_2+\delta_2} \cdot p_3^{\gamma_3+\delta_3} \cdot \dots = \\ &= p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2} \cdot p_3^{\alpha_3+\beta_3} \cdot \dots = \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \dots) \cdot (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \dots) = ab. \end{aligned}$$

В итоге мы доказали, что

$$\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab.$$

То, что мы только что доказали, это не просто какое-то красивое равенство. Это соотношение, которое позволяет находить наименьшее общее кратное в сложных ситуациях.

Допустим, нам нужно найти наименьшее общее кратное двух больших чисел, которые у нас не получается разложить на простые множители. Для наибольшего общего делителя у нас есть алгоритм Евклида, который позволяет найти НОД, используя совсем простые действия, – по сути, нужно просто из большего числа вычитать меньшее. А что делать с наименьшим общим кратным? Есть ли какой-то способ найти его, если возникли сложности с разложением на простые множители?

До того как мы доказали формулу, связывающую НОД и НОК, такого способа у нас не было. Но теперь мы можем найти наибольший общий делитель по алгоритму Евклида, а потом, используя доказанную формулу, найти и наименьшее общее кратное!

$$\text{НОК}(a, b) = \frac{ab}{\text{НОД}(a, b)}.$$

Давайте посмотрим, как это работает, на следующем примере.

Задача 51. Найдите НОК(11 413, 11 639).

Решение. Можно попробовать, перебрав все небольшие простые числа, разложить 11 413 и 11 639 на простые множители. Но если это не получилось сделать¹, можно найти наибольший общий делитель этих чисел по алгоритму Евклида:

$$\begin{aligned}(11\,413, 11\,639) &= (11\,413, 11\,639 - 11\,413) = \\&= (11\,413, 226) = (11\,413 - 50 \cdot 226, 226) = \\&= (11\,413 - 11\,300, 226) = (113, 226) = \\&= (113, 226 - 2 \cdot 113) = (113, 0) = 113.\end{aligned}$$

Таким образом, НОД(11 413, 11 639) = 113, а значит,

$$\begin{aligned}\text{НОК}(11\,413, 11\,639) &= \frac{11\,413 \cdot 11\,639}{113} = \\&= 101 \cdot 11\,639 = 1\,175\,539.\end{aligned}$$

Ответ. НОК(11 413, 11 639) = 1 175 539.

КОЛИЧЕСТВО ДЕЛИТЕЛЕЙ У ЧИСЛА

В этом разделе мы разберёмся, от чего зависит количество делителей у натурального числа. Но сначала давайте решим пару задач.

¹А это действительно не так просто, если учесть, что эти разложения выглядят так:

$$11\,413 = 101 \cdot 113, \quad 11\,639 = 103 \cdot 113.$$

Задача 52. Если у натурального числа ровно один делитель, то это 1. Если у него ровно два делителя, то это простое число. Опишите все натуральные числа, у которых ровно три делителя.

Решение. Если число n в разложении на простые множители содержит два различных простых числа p и q , то у него уже есть как минимум четыре делителя – 1, p , q и n . Значит, $n = p^k$, где k – некоторое натуральное число.

Если $k = 1$, то у числа $n = p$ ровно два делителя – 1 и p . Если $k > 2$, то у числа $n = p^k$ не менее четырёх делителей – 1, p , p^2 и p^3 .

Остался случай, когда $k = 2$, при котором у числа $n = p^2$ действительно ровно три делителя – 1, p и p^2 .

Ответ. Если у натурального числа ровно три делителя, то это число – квадрат простого.

Задача 53. Сколько различных делителей у числа 1000?

Решение. На самом деле, не очень сложно даже выписать все делители числа 1000. Вот они в порядке возрастания:

1,	2,	4,	5,	8,	10,	20,	25,
40,	50,	100,	125,	200,	250,	500,	1000.

Но как доказать, что других нет?

До того как мы доказали основную теорему арифметики, для честного доказательства нам бы пришлось организовать довольно большой перебор. Теперь же мы можем сказать, что $1000 = 2^3 \cdot 5^3$. И это разложение единственно!

Поэтому если 1000 делится на какое-то число, то оно имеет вид $2^m \cdot 5^n$, где m и n – целые неотрицательные и не превосходят трёх. Поэтому можно даже нарисовать таблицу со всеми делителями 1000:

	5^0	5^1	5^2	5^3
2^0	1	5	25	125
2^1	2	10	50	250
2^2	4	20	100	500
2^3	8	40	200	1000

Но можно было посчитать количество делителей, не выписывая их! Мы же поняли, что они имеют вид $2^m \cdot 5^n$, где m и n – целые неотрицательные числа, не превосходящие трёх. Поэтому каждое из них принимает одно из четырёх значений – 0, 1, 2 или 3. Поэтому всего есть $4 \cdot 4 = 16$ различных пар $(m; n)$, а значит, у числа 1000 ровно 16 делителей.

Ответ. У числа 1000 есть 16 различных делителей.

А сейчас рассуждения из этой задачи помогут нам доказать общую теорему.

Теорема (о количестве делителей). Пусть разложение числа n на простые множители имеет вид

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m},$$

где p_1, p_2, \dots, p_m – различные простые числа. Тогда у числа n ровно

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$$

различных делителей.

Доказательство. Из основной теоремы арифметики следует, что любой делитель числа n имеет вид

$$p_1^{\ell_1} \cdot p_2^{\ell_2} \cdot \dots \cdot p_m^{\ell_m},$$

где число ℓ_1 принимает любое из $(k_1 + 1)$ значений – $0, 1, 2, \dots, k_1$; число ℓ_2 принимает любое из $(k_2 + 1)$ значений – $0, 1, 2, \dots, k_2$; ...; число ℓ_m принимает любое из $(k_m + 1)$ значений – $0, 1, 2, \dots, k_m$.

В итоге получаем, что различных делителей числа n столько же, сколько и всевозможных наборов $(\ell_1; \ell_2; \dots; \ell_m)$, то есть

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$$

штук.

Задача 54. Докажите, что у натурального числа нечётное количество делителей тогда и только тогда, когда это число является квадратом некоторого натурального числа.

Первое решение. Если число a является делителем числа n , то $n = ka$, где k – некоторое натуральное число. Тогда число k тоже является делителем числа n . Таким образом, каждому делителю a можно сопоставить делитель $k = \frac{n}{a}$. То есть все делители разбиваются на пары чисел, произведение которых равно n .

Поэтому количество делителей почти у любого натурального числа будет чётным, так как их можно разбить на пары. Но может так получиться, что в какой-то «паре» делителей $\left(a; \frac{n}{a}\right)$ будет два одинаковых числа. Такое возможно, только если $\frac{n}{a} = a$, то есть $n = a^2$.

А значит, у натурального числа нечётное количество делителей тогда и только тогда, когда это число является квадратом.

Второе решение. Пусть разложение нашего числа n на простые множители имеет вид

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m},$$

где p_1, p_2, \dots, p_m – различные простые числа. Тогда из только что доказанной теоремы следует, что у числа n есть ровно $(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$ различных делителей.

Произведение нескольких натуральных чисел может быть нечётным числом, только если все множители нечётны. То есть у числа n нечётное количество делителей тогда и только тогда, когда все числа k_1, k_2, \dots, k_m чётные. Пусть

$$k_1 = 2\ell_1, \quad k_2 = 2\ell_2, \quad \dots, \quad k_m = 2\ell_m,$$

тогда число

$$n = p_1^{2\ell_1} \cdot p_2^{2\ell_2} \cdot \dots \cdot p_m^{2\ell_m} = \left(p_1^{\ell_1} \cdot p_2^{\ell_2} \cdot \dots \cdot p_m^{\ell_m} \right)^2$$

является квадратом.

И мы показали, что у натурального числа нечётное количество делителей тогда и только тогда, когда это число является квадратом.

А следующие задачи попробуйте решить самостоятельно.

Задача 55. Найдите наименьшее натуральное число, которое имеет ровно:

а) три различных делителя;

- б) четыре различных делителя;
- в) пять различных делителей;
- г) шесть различных делителей;
- д) семь различных делителей;
- е) восемь различных делителей;
- ё) девять различных делителей;
- ж) десять различных делителей.

Задача 56. Некоторое натуральное число имеет ровно три *простых* делителя, а его квадрат имеет 1001 делитель. Сколько делителей имеет куб этого числа?

Задача 57. Найдите все натуральные числа, у которых ровно 15 делителей, а сумма этих делителей равна 3751.

ЗАДАЧИ НА ОСНОВНУЮ ТЕОРЕМУ АРИФМЕТИКИ

После того как мы доказали основную теорему арифметики, значительно расширился спектр задач, которые мы можем решить. Начнём с совсем простого примера.

Задача 58. Сколько различных простых делителей у числа 2772?

Решение. Мы и раньше могли, сославшись на признаки делимости на 2, 3 и 11 (см. стр. 25–29), сказать, что число 2772 делится на 2, 3 и 11. Но без знания основной теоремы арифметики для поиска остальных простых делителей нам пришлось бы

проверять делимость числа 2772 на все остальные простые, квадрат которых не превосходит 2772. Мы про это говорили, когда обсуждали алгоритм проверки числа на простоту (см. стр. 68).

Но теперь благодаря основной теореме арифметики мы понимаем, что делимость числа 2772 на 2, 3 и 11 гарантирует нам то, что в разложении на простые множители число 2772 содержит множители 2, 3 и 11. То есть 2772 делится на $2 \cdot 3 \cdot 11 = 66$ и при этом $\frac{2772}{66} = 42$.

Значит, $2772 = 2 \cdot 3 \cdot 11 \cdot 42$. И осталось только разложить число 42 на простые множители:

$$42 = 6 \cdot 7 = 2 \cdot 3 \cdot 7.$$

Поэтому

$$2772 = 2 \cdot 3 \cdot 11 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3^2 \cdot 7 \cdot 11.$$

А так как (опять же благодаря основной теореме арифметики) разложение на простые множители единственно, то мы понимаем, что у числа 2772 есть ровно четыре различных простых делителя – 2, 3, 7 и 11.

Ответ. У числа 2772 есть ровно четыре различных простых делителя.

Задача 59. Какое наименьшее натуральное число не является делителем числа 50!?

Решение. В разложении числа 50! на простые множители все простые не превосходят 50. Поэтому простое число 53 точно не входит в это разложение, а значит, число 50! точно не делится на 53.

С другой стороны, очевидно, что число $50!$ делится на $1, 2, 3, \dots, 50$. Кроме того, оно делится на $51 = 3 \cdot 17$ и на $52 = 4 \cdot 13$. Поэтому 53 – это наименьшее натуральное число, которое не является делителем числа $50!$.

Ответ. 53 – наименьшее натуральное число, которое не является делителем числа $50!$.

Задача 60. Докажите, что при всех простых $p > 3$ число $(p^2 - 1)$ делится на 24 .

Решение. Заметим, что $p^2 - 1 = (p - 1)(p + 1)$. Но число p простое и не равно двум, поэтому оно нечётное. Тогда $(p - 1)$ и $(p + 1)$ – два чётных числа, отличающихся на 2 . Поэтому одно из них делится на 4 . Значит, их произведение $(p - 1)(p + 1)$ делится на 8 .

С другой стороны, среди трёх последовательных натуральных чисел $(p - 1)$, p и $(p + 1)$ есть число, кратное трём. И это точно не p , потому что оно простое и не равно трём. Значит, произведение $(p - 1)(p + 1)$ делится на 3 .

Но если число $(p^2 - 1)$ делится и на 8 , и на 3 , то в его разложении на простые множители есть $2^3 \cdot 3$. Поэтому оно делится на 24 .

Задача 61. Вася хочет записать по кругу 11 натуральных чисел так, чтобы для каждого двух соседних чисел частное от деления большего числа на меньшее было простым числом. Таня утверждает, что это невозможно. Права ли Таня?

Первое решение. Предположим, что Васе удалось расположить таким образом числа по кругу.

Рассмотрим разложение каждого из этих чисел на простые множители. Любые два соседних разложения на множители отличаются тем, что у большего числа на один простой множитель больше, чем у меньшего.

Подсчитаем количество простых множителей у каждого числа (если среди чисел есть число 1, то считаем, что в его разложении на простые множители будет ноль множителей). Тогда у соседних чисел эти количества будут отличаться на 1 и поэтому будут разной чётности. Значит, у чисел, стоящих через одно, количество простых делителей будет одинаковой чётности.

Пронумеруем все числа, начиная с некоторого. Например, по часовой стрелке. Тогда у первого, третьего, пятого, седьмого, девятого и одиннадцатого числа количество простых множителей будет иметь одну и ту же чётность. Но первое и одиннадцатое числа стоят рядом, а значит, количества их простых множителей должны быть разной чётности. Пришли к противоречию. Значит, Васе не удастся расположить таким образом числа по кругу. Поэтому Таня права.

Второе решение. Предположим, что Васе удалось расположить таким образом числа по кругу. Соединим стрелочками соседние числа, двигаясь по часовой стрелке. И на каждой стрелочке запишем множитель, на который нужно умножить число, стоящее в начале стрелки, чтобы получилось число, стоящее в её конце. По условию этот множитель – либо простое число, либо число, обратное простому.

Если мы начнём с какого-то числа, пройдем

полный круг, то мы придём к тому же числу. Значит, произведение всех множителей, записанных на стрелочках, равно 1. Тогда в этом произведении в числителе должно быть столько же простых множителей, сколько и в знаменателе. Но всего в числителе и знаменателе множителей будет столько же, сколько и стрелочек – 11, нечётное количество. А значит, в числителе не может быть столько же простых множителей, сколько и в знаменателе. Пришли к противоречию. Значит, Васе не удастся расположить таким образом числа по кругу. Поэтому Таня права.

Ответ. Таня права.

Задача 62. Найдите $\text{НОД}(2^{1001} - 1, 2^{2024} - 1)$.

Решение. Рассмотрим произвольные натуральные числа $m < n$. Тогда

$$\begin{aligned} & \text{НОД}(2^m - 1, 2^n - 1) = \\ &= \text{НОД}(2^m - 1, 2^n - 1 - (2^m - 1)) = \\ &= \text{НОД}(2^m - 1, 2^n - 2^m) = \\ &= \text{НОД}(2^m - 1, 2^m \cdot (2^{n-m} - 1)). \end{aligned}$$

При этом очевидно, что числа $(2^m - 1)$ и 2^m взаимно простые, так как

$$\begin{aligned} \text{НОД}(2^m - 1, 2^m) &= \text{НОД}(2^m - 1, 2^m - (2^m - 1)) = \\ &= \text{НОД}(2^m - 1, 1) = 1. \end{aligned}$$

То есть у чисел $(2^m - 1)$ и 2^m в разложениях на простые множители нет общих простых. Значит,

$$\text{НОД}(2^m - 1, 2^m \cdot (2^{n-m} - 1)) = \text{НОД}(2^m - 1, 2^{n-m} - 1).$$

Таким образом, мы доказали, что

$$\text{НОД}(2^m - 1, 2^n - 1) = \text{НОД}(2^m - 1, 2^{n-m} - 1).$$

То есть больший показатель степени можно заменить на разность большего и меньшего. А это означает, что мы можем применять алгоритм Евклида не к самим числам $(2^m - 1)$ и $(2^n - 1)$, а к показателям степеней!

В итоге, если продолжить эти рассуждения, мы получим, что

$$\text{НОД}(2^m - 1, 2^n - 1) = 2^{\text{НОД}(m, n)} - 1.$$

Найдем $\text{НОД}(1001, 2024)$. Можно разложить на простые множители, а можно вновь воспользоваться алгоритмом Евклида:

$$\begin{aligned}\text{НОД}(1001, 2024) &= \text{НОД}(1001, 2024 - 2 \cdot 1001) = \\ &= \text{НОД}(1001, 22) = \\ &= \text{НОД}(1001 - 45 \cdot 22, 22) = \\ &= \text{НОД}(11, 22) = 11.\end{aligned}$$

Поэтому

$$\begin{aligned}\text{НОД}(2^{1001} - 1, 2^{2024} - 1) &= 2^{\text{НОД}(1001, 2024)} - 1 = \\ &= 2^{11} - 1 = 2048 - 1 = 2047.\end{aligned}$$

Ответ. $\text{НОД}(2^{1001} - 1, 2^{2024} - 1) = 2047$.

А следующие задачи попробуйте решить самостоятельно.

Задача 63. Найдите наименьшее натуральное число, произведение цифр которого равно 540.

Задача 64. Докажите, что если каждое из простых чисел p и q больше трёх, то разность их квадратов $(p^2 - q^2)$ делится на 24.

Задача 65. Сколько существует пар натуральных чисел, наименьшее общее кратное которых равно 250 000?

Задача 66. Найдите наибольшее натуральное n , для которого число $6500!$ делится на каждое из чисел вида k^k при $k = 1, 2, 3, \dots, n$.

Задача 67. Какое наибольшее значение может принимать наибольший общий делитель чисел $(17n + 5)$ и $(19n + 1)$, если n – натуральное число?

ГЛАВА 4 ДИОФАНТОВЫ УРАВНЕНИЯ

После всего того, что мы узнали из предыдущих глав, можно уже переходить к решению уравнений. К так называемым *диофантовым уравнениям* – уравнениям в целых числах.

Так называются уравнения, в которых все входные параметры являются целыми числами и для которых требуется найти решения также среди целых чисел. Своё название уравнения получили в честь античного математика Диофанта Александрийского, который, как считается, первым начал изучать подобные уравнения, классифицировать их и описывать методы их решения.

Наверное, самое известное диофантово уравнение выглядит так:

$$a^n + b^n = c^n,$$

где n , a , b и c – натуральные числа и $n \geq 3$. Великая теорема Ферма утверждает, что у этого уравнения нет решений. Окончательно доказана она была лишь в 1995 году, то есть прошло более 350 лет после того, как в 1637 году Пьер Ферма сформулировал

её на полях «Арифметики» Диофанта.

Но доказательство этого утверждения чрезмерно сложно, поэтому нам остаётся лишь вслед за Пьером Ферма сказать, что «это поистине чудесное доказательство, но поля книги слишком узки для него»¹.

На самом деле есть множество других важных и интересных диофантовых уравнений. Например:

- **уравнение Каталана**

$$x^n - y^m = 1,$$

где x , y , n и m – натуральные числа, большие единицы. Доказано, что единственное решение этого уравнения – это $3^2 - 2^3 = 1$;

- **уравнение Пелля**

$$x^2 - ny^2 = 1,$$

где x , y и n – натуральные числа, и число n не является точным квадратом;

- **уравнение Рамануджана – Нагеля**

$$2^n - 7 = x^2,$$

где x и n – натуральные числа.

И многие другие.

Но в этой главе мы ограничимся тем, что научимся решать лишь самые простые диофантовые уравнения.

¹Ферма делал свои пометки на полях читаемых математических текстов и часто там же формулировал пришедшие на ум задачи и теоремы. Формулировку этой теоремы он записал с припиской: «Я нашёл этому поистине чудесное доказательство, но поля книги этой слишком узки для него».

ЛИНЕЙНЫЕ ДИОФАНТОВЫ УРАВНЕНИЯ С ДВУМЯ НЕИЗВЕСТНЫМИ

Линейным диофантовым уравнением с двумя неизвестными называется уравнение вида

$$Ax + By = C,$$

где A, B, C – заданные целые ненулевые числа, а x и y – неизвестные целые числа.

Давайте научимся их решать!

Рассмотрим сначала простой случай, когда у чисел A и B есть общий делитель $d > 1$, которого нет у числа C . Тогда при любых целых x и y число $(Ax + By)$ будет делиться на d . Но тогда оно не может равняться числу C , которое на d не делится.

Таким образом, мы доказали, что если число C не делится на наибольший общий делитель чисел A и B , то уравнение не имеет решений.

Если же число C делится на наибольший общий делитель чисел A и B , то на этот общий делитель можно сократить обе части исходного уравнения и получить уравнение вида

$$ax + by = c,$$

в котором числа a и b уже не имеют общего делителя, отличного от единицы. Далее будем рассматривать именно такое уравнение.

Допустим, нам как-то удалось найти¹ какое-нибудь решение $(x_0; y_0)$ нашего уравнения. Покажем, как, зная его, получить все остальные решения.

Итак, мы знаем, что

$$ax_0 + by_0 = c.$$

Рассмотрим любую пару чисел $(x; y)$, удовлетворяющих равенству

$$ax + by = c.$$

Тогда верно равенство

$$ax + by = ax_0 + by_0.$$

Откуда получаем, что

$$a \cdot (x - x_0) = b \cdot (y_0 - y).$$

Отсюда следует, что число $a \cdot (x - x_0)$ делится на b . Но числа a и b взаимно просты. Значит, число $(x - x_0)$ делится на b . Таким образом, $x - x_0 = kb$, где k – некоторое целое число. Тогда

$$a \cdot kb = b \cdot (y_0 - y).$$

То есть $y_0 - y = ka$.

В итоге нашли все решения нашего уравнения:

$$x = x_0 + kb, \quad y = y_0 - ka,$$

где k – любое целое число.

Давайте посмотрим, как это работает, на примере следующей задачи.

¹Чуть позже (см. стр. 138) мы покажем, как всегда можно найти какое-нибудь решение такого уравнения.

Задача 68. Найдите все пары целых чисел, для которых справедливо равенство

$$15x + 25y = 35.$$

Решение. Разделив обе части равенства на 5, получим, что исходное уравнение равносильно следующему равенству

$$3x + 5y = 7.$$

Несложно заметить, что

$$7 = 10 - 3 = (-1) \cdot 3 + 2 \cdot 5.$$

Поэтому уравнение $3x + 5y = 7$ можно переписать в виде

$$3x + 5y = (-1) \cdot 3 + 2 \cdot 5.$$

То есть

$$3 \cdot (x + 1) = 5 \cdot (2 - y).$$

Правая часть делится на 5. Значит, и левая часть делится на 5. Но числа 3 и 5 взаимно просты. Поэтому число $(x + 1)$ делится на 5. То есть $x + 1 = 5k$, где k – некоторое целое число. Значит,

$$3 \cdot 5k = 5 \cdot (2 - y).$$

Поэтому $2 - y = 3k$.

Таким образом получаем, что

$$x = 5k - 1, \quad y = 2 - 3k,$$

где k – любое целое число.

Это означает, что существует бесконечно много решений:

k	...	-3	-2	-1	0	1	2	3	...
x	...	-16	-11	-6	-1	4	9	14	...
y	...	11	8	5	2	-1	-4	-7	...

Ответ. $x = 5k - 1$, $y = 2 - 3k$, где k – любое целое число.

КАК УГАДАТЬ РЕШЕНИЕ

В предложенном алгоритме решения линейного диофантова уравнения есть один изъян. А именно этот момент: *допустим, нам как-то удалось найти какое-нибудь решение уравнения*. И, хотя во многих случаях действительно легко подобрать какое-нибудь решение, остаётся вопрос: что же делать, если не получилось этого сделать? Например, попробуйте найти какое-нибудь решение уравнения

$$201x + 302y = 123.$$

Как мы поняли из предыдущего раздела, нам достаточно научиться находить какое-нибудь решение уравнения вида

$$ax + by = c,$$

в котором числа a и b не имеют общего делителя, отличного от единицы. Но давайте мы ещё сильнее упростим себе задачу. Ограничимся лишь случаем, когда $c = 1$. То есть найдём какое-нибудь решение $(x_0; y_0)$ уравнения

$$ax + by = 1.$$

Тогда

$$ax_0 + by_0 = 1,$$

а значит,

$$a \cdot cx_0 + b \cdot cy_0 = c.$$

То есть, если мы нашли какое-нибудь решение $(x_0; y_0)$ уравнения

$$ax + by = 1,$$

то пара чисел $(cx_0; cy_0)$ будет решением уравнения

$$ax + by = c.$$

Итак, мы свели задачу к нахождению какого-нибудь решения уравнения вида

$$ax + by = 1,$$

в котором числа a и b не имеют общего делителя, отличного от единицы. Но для этого достаточно вспомнить следствие из соотношения Безу (см. стр. 52). Там мы доказали, что если натуральные числа a и b взаимно просты, то найдутся такие целые числа m и n , что

$$ma + nb = 1.$$

Более того, мы научились искать коэффициенты m и n , используя алгоритм Евклида!

Давайте вспомним, как это делается, на конкретном примере.

Задача 69. Найдите все пары целых чисел, для которых справедливо равенство

$$201x + 302y = 123.$$

Решение. Давайте воспользуемся алгоритмом Евклида для чисел 201 и 302, отслеживая для каждого получающегося числа, как оно выражается через 201 и 302:

$$\begin{array}{l|l}
 (201, 302) & \\
 (201, 101) & 101 = 302 - 201; \\
 (100, 101) & 100 = 201 - 101 = 201 - (302 - 201) = \\
 & \quad = 2 \cdot 201 - 302; \\
 (100, 1) & 1 = 101 - 100 = \\
 & \quad = (302 - 201) - (2 \cdot 201 - 302) = \\
 & \quad = 2 \cdot 302 - 3 \cdot 201.
 \end{array}$$

Таким образом, $2 \cdot 302 - 3 \cdot 201 = 1$. Поэтому

$$(2 \cdot 123) \cdot 302 - (3 \cdot 123) \cdot 201 = 123.$$

Значит, уравнение $201x + 302y = 123$ можно переписать в виде

$$201x + 302y = 246 \cdot 302 - 369 \cdot 201.$$

Отсюда получаем, что

$$201 \cdot (x + 369) = 302 \cdot (246 - y).$$

Правая часть делится на 302. Значит, и левая часть делится на 302. Но 201 и 302 взаимно просты (мы даже это только что доказали при помощи алгоритма Евклида). Поэтому $(x + 369)$ делится на 302. То есть $x + 369 = 302k$, где k – некоторое целое число. Значит,

$$201 \cdot 302k = 302 \cdot (246 - y).$$

Поэтому $246 - y = 201k$.

Таким образом, получаем, что

$$x = 302k - 369, \quad y = 246 - 201k,$$

где k – любое целое число.

Ответ. $x = 302k - 369$, $y = 246 - 201k$, где k – любое целое число.

Заметим, что найденное таким образом решение уравнения $(-369; 246)$ не является «самым маленьким». Есть решения, которые гораздо «ближе к нулю».

Легко заметить, что ближе всего к нулю будет решение при $k = 1$: $x = -67$, $y = 45$. А теперь представьте, сколько бы мы потратили времени, чтобы перебором подобрать это решение!

НЕЛИНЕЙНЫЙ ДИОФАНТ

В этом разделе мы научимся решать ещё один тип диофантовых уравнений, на этот раз нелинейных. А именно, давайте поймём, как решить уравнение вида



$$Ax + By + C = Dxy,$$

где A , B , C и D – заданные целые числа, при этом $D \neq 0$, а x и y – неизвестные целые числа.

А начнём мы с самого простого уравнения такого вида.

Задача 70. Найдите все пары целых чисел, для которых справедливо равенство

$$x + y = xy.$$

Решение. Запишем уравнение в виде

$$xy - x - y = 0.$$

Заметим, что если прибавить единицу к обеим частям равенства, то левую часть можно разложить на множители:

$$\begin{aligned}xy - x - y + 1 &= 1; \\x(y - 1) - (y - 1) &= 1; \\(x - 1)(y - 1) &= 1.\end{aligned}$$

Но произведение двух целых чисел может быть равно единице, только если это 1 и 1 или (-1) и (-1) .

В первом случае получаем пару чисел $x = y = 2$, а во втором – пару $x = y = 0$.

Ответ. $x = y = 2$ или $x = y = 0$.

Попробуем подобным образом решить уравнение посложнее.

Задача 71. Найдите все пары целых чисел, для которых справедливо равенство

$$2x + 3y + 4 = 5xy.$$

Решение. Запишем уравнение в виде

$$5xy - 2x - 3y = 4.$$

Хочется опять что-то добавить к левой части, чтобы она разложилась на множители. Если из первых двух слагаемых вынести множитель x , то получится

$$x(5y - 2).$$

Поэтому хочется и из $3y$ как-то получить $(5y - 2)$. Но 3 не делится на 5.

И тут помогает следующая идея – давайте обе части уравнения умножим на 5:

$$\begin{aligned} 25xy - 10x - 15y &= 20; \\ 5x(5y - 2) - 3 \cdot 5y &= 20. \end{aligned}$$

А теперь прибавим к обеим частям равенства $3 \cdot 2$:

$$\begin{aligned} 5x(5y - 2) - 3 \cdot 5y + 3 \cdot 2 &= 26; \\ 5x(5y - 2) - 3(5y - 2) &= 26; \\ (5x - 3)(5y - 2) &= 26. \end{aligned}$$

Получилось равенство, похожее на то, что было в предыдущей задаче. Но в отличие от того, что было там, существует больше случаев, когда произведение двух целых чисел равно 26.

После разложения числа 26 на простые множители $26 = 2 \cdot 13$ видно, что произведение двух целых чисел может дать 26, если это 1 и 26 или 2 и 13. Но при этом в каждой паре может быть как один, так и другой порядок.

А кроме этого, есть ещё столько же пар с отрицательными значениями! Итого, нужно перебрать восемь случаев:

$5x - 3$	$5y - 2$	Решение
1	26	$5x = 4$ и $5y = 28$. Нет решений
2	13	$5x = 5$ и $5y = 15 \Rightarrow x = 1$ и $y = 3$
13	2	$5x = 16$ и $5y = 4$. Нет решений
26	1	$5x = 29$ и $5y = 3$. Нет решений
-1	-26	$5x = 2$ и $5y = -24$. Нет решений
-2	-13	$5x = 1$ и $5y = -11$. Нет решений

$$\begin{array}{c|c|c} -13 & -2 & 5x = -10 \text{ и } 5y = 0 \Rightarrow x = -2 \text{ и } y = 0 \\ -26 & -1 & 5x = -23 \text{ и } 5y = 1. \text{ Нет решений} \end{array}$$

В итоге получаем, что равенству удовлетворяют только две пары целых чисел – (1; 3) и (–2; 0).

Ответ. $x = 1$ и $y = 3$ или $x = -2$ и $y = 0$.

Теперь мы готовы к тому, чтобы сформулировать общий алгоритм решения уравнения вида

$$Ax + By + C = Dxy,$$

где A, B, C и D – заданные целые числа, при этом $D \neq 0$, а x и y – неизвестные целые числа.

Шаг первый. Перепишем его в виде

$$Dxy - Ax - By = C.$$

Шаг второй. Домножим обе части равенства на число D :

$$D^2xy - ADx - BDy = CD.$$

Шаг третий. Добавим к обеим частям равенства число AB :

$$D^2xy - ADx - BDy + AB = CD + AB.$$

Шаг четвёртый. Группируем слагаемые и раскладываем левую часть равенства на множители:

$$Dx(Dy - A) - B(Dy - A) = CD + AB;$$

$$(Dx - B)(Dy - A) = CD + AB.$$

Шаг пятый. Говорим, что произведение целых чисел $(Dx - B)$ и $(Dy - A)$ должно быть равно целому

числу $(CD + AB)$, и перебираем все возможные пары чисел, которые в произведении дают это число.

Вот такой вот алгоритм решения. Выглядит не очень сложно, но реальная сложность реализации будет зависеть от того, как много пар целых чисел дают в произведении число $(CD + AB)$.

Однако иногда можно оптимизировать этот алгоритм! Рассмотрим следующую задачу, которая, на первый взгляд, не сильно отличается от предыдущей.

Задача 72. Найдите все пары целых чисел, для которых справедливо равенство

$$2x + 3y + 4 = 6xy.$$

Решение. Попробуем применить к нему вышеизложенный алгоритм. Перепишем равенство в виде

$$6xy - 2x - 3y = 4.$$

Домножим обе части равенства на число 6:

$$36xy - 12x - 18y = 24.$$

Добавим к обеим частям равенства число 6:

$$36xy - 12x - 18y + 6 = 30.$$

Группируем слагаемые и раскладываем левую часть равенства на множители:

$$6x(6y - 2) - 3(6y - 2) = 30;$$

$$(6x - 3)(6y - 2) = 30.$$

Теперь нам нужно перебрать все пары целых чисел, произведение которых равно 30. Но их очень много:

(1; 30), (2; 15), (3; 10), (5; 6),
 (6; 5), (10; 3), (15; 2), (30; 1),
 (-1; -30), (-2; -15), (-3; -10), (-5; -6),
 (-6; -5), (-10; -3), (-15; -2), (-30; -1).

Но можно этот перебор сильно сократить!

Заметим, что $6x - 3 = 3(2x - 1)$, а $6y - 2 = 2(3y - 1)$.
 Поэтому равенство

$$(6x - 3)(6y - 2) = 30$$

равносильно следующему

$$(2x - 1)(3y - 1) = 5.$$

Поэтому случаев будет всего четыре:

$2x - 1$	$3y - 1$	Решение
1	5	$2x = 2$ и $3y = 6 \Rightarrow x = 1$ и $y = 2$
5	1	$2x = 6$ и $3y = 2$. Нет решений
-1	-5	$2x = 0$ и $3y = -4$. Нет решений
-5	-1	$2x = -4$ и $3y = 0 \Rightarrow x = -2$ и $y = 0$

В итоге получаем, что равенству удовлетворяют только две пары целых чисел - (1; 2) и (-2; 0).

Ответ. $x = 1$ и $y = 2$ или $x = -2$ и $y = 0$.

Этот пример показывает, что если в уравнении

$$Dxy - Ax - By = C$$

у чисел D и A (или у чисел D и B) есть общий делитель, отличный от единицы, то для возможности в дальнейшем разложить левую часть на множители равенство можно умножить не на D , а на более маленькое число. Но давайте лучше будем это замечать в каждой конкретной задаче, а не будем пересложнять общий алгоритм, добавляя в него соответствующие уточнения.

К уравнениям такого типа сводится много разных задач. Например, лет пять назад в качестве самого сложного задания единого государственного экзамена была такая задача.

Задача 73. Найдите все возможные пары натуральных чисел m и n , для которых $m \leq n$ и

$$\frac{1}{m} + \frac{1}{n} = \frac{1}{14}.$$

Решение. Если домножим обе части равенства на $14mn$, то получим, что исходное уравнение равносильно следующему:

$$14n + 14m = mn.$$

Теперь перепишем это равенство в виде

$$mn - 14n - 14m = 0.$$

И добавим 14^2 к обоим его частям:

$$\begin{aligned} mn - 14n - 14m + 14^2 &= 196, \\ n(m - 14) - 14(m - 14) &= 196, \\ (m - 14)(n - 14) &= 196. \end{aligned}$$

Теперь нам нужно перебрать все пары целых чисел, произведение которых равно 196. Заметим, что

$$196 = 14^2 = 2^2 \cdot 7^2.$$

Поэтому у 196 есть девять натуральных делителей:

$$\begin{array}{lll} 1, & 7, & 7^2 = 49, \\ 2, & 2 \cdot 7 = 14, & 2 \cdot 7^2 = 98, \\ 2^2 = 4, & 2^2 \cdot 7 = 28, & 2^2 \cdot 7^2 = 196. \end{array}$$

И ещё столько же соответствующих отрицательных «делителей».

Таким образом, есть девять положительных пар чисел $(m - 14; n - 14)$, дающих в произведении 196:

$$\begin{array}{lll} (1; 196), & (7; 28), & (49; 4), \\ (2; 98), & (14; 14), & (98; 2), \\ (4; 49), & (28; 7), & (196; 1), \end{array}$$

и столько же отрицательных:

$$\begin{array}{lll} (-1; -196), & (-7; -28), & (-49; -4), \\ (-2; -98), & (-14; -14), & (-98; -2), \\ (-4; -49), & (-28; -7), & (-196; -1). \end{array}$$

Прежде чем броситься перебирать все 18 случаев, давайте заметим, что m и n – натуральные числа, поэтому

$$m - 14 > -14, \quad n - 14 > -14.$$

А в последних девяти парах хотя бы одно из чисел не превосходит (-14) . Значит, ни одна из этих пар не подходит.

Кроме того, по условию $m \leq n$. Поэтому

$$m - 14 \leq n - 14.$$

То есть из первых девяти пар возможны только первые пять:

$m - 14$	$n - 14$	m	n
1	196	15	210
2	98	16	112
4	49	18	63
7	28	21	42
14	14	28	28

В итоге, мы получили, что у уравнения

$$\frac{1}{m} + \frac{1}{n} = \frac{1}{14}$$

есть пять решений в натуральных числах, для которых $m \leq n$.

Ответ. (15; 210), (16; 112), (18; 63), (21; 42), (28; 28).

А следующие задачи попробуйте решить самостоятельно.

Задача 74. Найдите все пары целых чисел, для которых справедливо равенство

$$4m + 5n = 2mn - 9.$$

Задача 75. Найдите все прямоугольники, стороны которых выражаются натуральными числами, а площадь численно равна периметру.

ПРИНЦИП КРАЙНЕГО И МЕТОД БЕСКОНЕЧНОГО СПУСКА

Часто встречаются задачи, в которых нужно доказать отсутствие решений в целых числах у некоторого уравнения. В подобных случаях часто помогают принцип крайнего и метод бесконечного спуска. В каком-то смысле для подобных задач это почти одно и то же.

Чтобы разобраться с тем, что это такое и как оно работает, рассмотрим следующую задачу.

Задача 76. Докажите, что уравнение

$$a^2 + b^2 = 2^n$$

не имеет решений, в которых a , b и n – натуральные числа и $a \neq b$.

Решение. Предположим, что такое равенство возможно. Давайте рассуждать. В правой части равенства стоит число 2^n , а когда фигурирует двойка, то хочется разобраться с чётностью.



Заметим, что чётность квадрата числа зависит от чётности самого числа. Действительно, квадрат чётного числа чётен, квадрат нечётного – нечётен. Поэтому если числа a и b разной чётности, то число

$$a^2 + b^2$$

будет нечётным и не может быть равно степени двойки. Значит, числа a и b одинаковой чётности.

Предположим, что числа a и b нечётные. Любое нечётное число можно представить в виде $(2k + 1)$, где k – целое число. Но тогда квадрат этого числа

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

будет иметь остаток 1 при делении на 4. Из этого следует, что число $(a^2 + b^2)$ будет давать остаток 2 при делении на 4.

Но среди степеней двойки только одна даёт остаток 2 при делении на 4 – это $2^1 = 2$. Остальные степени двойки делятся на $2^2 = 4$ и поэтому дают остаток 0 при делении на 4.

Осталось заметить, что при условии $a \neq b$ равенство

$$a^2 + b^2 = 2$$

не имеет решения в натуральных числах. Такое равенство возможно лишь при $a = b = 1$.

Итак, мы поняли, что числа a и b не могут быть разной чётности, показали, что они не могут быть оба нечётными, осталось рассмотреть случай, когда они оба чётны. Тогда их можно представить как $a = 2m$ и $b = 2\ell$, где $m \neq \ell$ – натуральные числа. Подставив это в исходное уравнение, получим, что

$$\begin{aligned}(2m)^2 + (2\ell)^2 &= 2^n, \\ 4m^2 + 4\ell^2 &= 2^n, \\ m^2 + \ell^2 &= 2^{n-2}.\end{aligned}$$

Что же получилось? Мы хотели найти два различных числа, сумма квадратов которых равна степени двойки, поняли, что они должны быть чётными, и пришли к двум меньшим числам, сумма квадратов которых равна степени двойки!

А дальше можно рассуждать по-разному. Например, так. Мы предположили, что существуют пары различных чисел, сумма квадратов которых равна степени двойки. Давайте из всех этих пар выберем ту, которая самая маленькая в каком-то смысле. Например, ту, в которой меньшее из чисел самое маленькое из всех меньших чисел во всех подходящих парах. Если есть несколько пар с таким меньшим числом, то выберем любую из них.

Как мы поняли, в нашей паре оба числа будут чётными: $a = 2m$ и $b = 2\ell$, где $m \neq \ell$ – натуральные числа. Но тогда, если $(a^2 + b^2)$ – некоторая степень двойки, то и $(m^2 + \ell^2)$ будет степенью двойки.

Но в паре $(m; \ell)$ числа в два раза меньше, чем в паре $(a; b)$, а мы предположили, что $(a; b)$ – это пара, в которой меньшее из чисел самое маленькое из всех меньших чисел во всех подходящих парах. И при этом нашли подходящую пару, в которых числа ещё меньше! Пришли к противоречию. Значит, уравнение

$$a^2 + b^2 = 2^n$$

не имеет решений, в которых a, b и n – натуральные числа и $a \neq b$.

Подобные рассуждения, когда мы предполагаем, что существуют решения, выбираем из них самое *какое-то* и потом находим *ещё более какое-то*, тем самым придя к противоречию, называются *принципом крайнего*¹.

¹Принципом крайнего мы уже пользовались ранее. Например, при доказательстве основной теоремы арифметики. Там, предполагая, что теорема верна не для всех чисел, рассматривали *самое маленькое число*, для которого она не верна.

Но для многих такие рассуждения слишком сложны, поэтому обсудим и другие подходы к решению.

Смотрите, что мы уже сделали? Мы предположили, что существуют натуральные числа $a \neq b$, сумма квадратов которых равна степени двойки. Поняли, что тогда эти числа должны быть чётными, и пришли к тому, что для чисел $m = \frac{a}{2}$ и $\ell = \frac{b}{2}$ также верно утверждение, что $m \neq \ell$ – натуральные числа, сумма квадратов которых равна степени двойки. Но тогда и для чисел m и ℓ мы сможем повторить всё то же самое.

Если числа m и ℓ разной чётности, то число $(m^2 + \ell^2)$ будет нечётным и не может быть равно степени двойки. Если числа m и ℓ оба нечётные, то число $(m^2 + \ell^2)$ будет давать остаток 2 при делении на 4 и при этом

$$2^n = m^2 + \ell^2 \geq 1^2 + 3^2 = 10.$$

Значит $n > 1$, и 2^n делится на 4.

Поэтому числа m и ℓ оба чётны. Но тогда для чисел $s = \frac{m}{2}$ и $t = \frac{\ell}{2}$ также верно утверждение, что $s \neq t$ – натуральные числа, сумма квадратов которых равна степени двойки. Но тогда и для чисел s и t мы снова сможем повторить всё то же самое. И так далее.

То есть мы поняли, что если сумма квадратов двух чисел равна степени двойки, то они чётные, и после деления на 2 вновь получается пара чисел, сумма квадратов которых равна степени двойки. И мы можем так «спускаться» бесконечно долго. По-

этому такой способ рассуждения называется *методом бесконечного спуска*¹.

Но понятно, что никакие числа не могут делиться на 2 бесконечно много раз. Пришли к противоречию! Значит, уравнение $a^2 + b^2 = 2^n$ не имеет решений, в которых a , b и n – натуральные числа и $a \neq b$.

На самом деле, после того как мы уже поняли основную идею задачи, рассуждать можно было и иначе – без принципа крайнего и метода бесконечного спуска. Можно посмотреть, в какой степени двойка входит в разложения чисел a и b на простые множители. Если она входит в одинаковой степени, то

$$a = 2^k \cdot c, \quad b = 2^k \cdot d,$$

где c и d – произведение остальных простых множителей, а значит, нечётные числа². Тогда, разделив

¹ Стоит отметить, что спуск можно делать очень по-разному. Например, в этой задаче, после того как мы поняли, что числа a и b должны быть одной чётности, можно было представить их как $a = x + y$, $b = x - y$ (или наоборот, если $a < b$), где $x = \frac{a+b}{2}$, $y = \frac{a-b}{2}$. Тогда из равенства $a^2 + b^2 = 2^n$ следует равенство $(x+y)^2 + (x-y)^2 = 2^n$, откуда после раскрытия скобок и сокращения на 2 получаем равенство $x^2 + y^2 = 2^{n-1}$. То есть предположив, что сумма квадратов каких-то двух различных натуральных чисел равна 2^n , мы нашли другие два различных натуральных числа, сумма квадратов которых равна 2^{n-1} .

² Легко заметить, что в этом месте можно было обойтись без основной теоремы арифметики и разложения на простые множители. Достаточно было сказать, что 2^k – максимальная степень двойки, на которую делится число a . Тогда $a = 2^k \cdot c$, и число c точно будет нечётным. Так как иначе число a будет делиться и на 2^{k+1} .

Но когда мы уже доказали основную теорему арифметики, странно ею не пользоваться.

равенство $a^2 + b^2 = 2^n$ на 2^{2k} , мы получим, что

$$c^2 + d^2 = 2^{n-2k}.$$

Но мы знаем, что сумма квадратов двух различных натуральных нечётных чисел не может быть равна степени двойки.

Если же двойка входит в разложения на простые множители чисел a и b в разной степени (для определённости пусть в число a она входит в меньшей степени, чем в число b), то

$$a = 2^k \cdot c, \quad b = 2^k \cdot d,$$

где c – нечётное число, а d – чётное. Тогда, разделив равенство $a^2 + b^2 = 2^n$ на 2^{2k} , мы снова получим, что

$$c^2 + d^2 = 2^{n-2k}.$$

Но сумма квадратов двух чисел разной чётности не может быть равна степени двойки.

Таким образом, уравнение $a^2 + b^2 = 2^n$ не имеет решений, в которых a , b и n – натуральные числа и $a \neq b$.

Попробуйте, используя подобные рассуждения, решить самостоятельно следующие задачи.

Задача 77. Докажите, что уравнение

$$2n^2 = m^2$$

не имеет решений в натуральных числах¹.

¹Решив эту задачу, вы докажете иррациональность числа $\sqrt{2}$, потому что вы покажете, что не существует рационального числа $\frac{m}{n}$, квадрат которого равен 2.

Задача 78. Докажите, что уравнение

$$27k^4 + 9\ell^4 + 3m^4 = n^4$$

не имеет решений в натуральных числах.

Задача 79. Докажите, что уравнение

$$\ell^2 + m^2 + n^2 = 2\ell mn$$

не имеет решений в натуральных числах.

ДРУГИЕ УРАВНЕНИЯ В ЦЕЛЫХ ЧИСЛАХ

В этом разделе без какой-либо систематизации обсудим различные уравнения в целых числах и разберёмся, какие подходы используются при их решении.

Задача 80. Найдите все пары натуральных чисел, для которых справедливо равенство

$$x^2 - y^2 = 111.$$

Решение. Разложив левую часть равенства на множители, получим

$$(x - y)(x + y) = 111.$$

Разложим 111 на простые множители: $111 = 3 \cdot 37$. Есть восемь пар целых чисел, произведение которых равно 111:

$$\begin{aligned} 111 &= 1 \cdot 111 = 3 \cdot 37 = 37 \cdot 3 = 111 \cdot 1 = (-1) \cdot (-111) = \\ &= (-3) \cdot (-37) = (-37) \cdot (-3) = (-111) \cdot (-1). \end{aligned}$$

Но, во-первых, множитель $(x + y)$ равен сумме двух натуральных чисел, а значит, он положителен. Поэтому последние четыре варианта невозможны. А, во-вторых, разность двух натуральных чисел всегда меньше, чем их сумма. Поэтому остаётся лишь два случая:

$x - y$	$x + y$	x	y
1	111	$\frac{1 + 111}{2} = 56$	$\frac{111 - 1}{2} = 55$
3	37	$\frac{3 + 37}{2} = 20$	$\frac{37 - 3}{2} = 17$

Здесь мы воспользовались тем, что

$$x = \frac{(x - y) + (x + y)}{2}, \quad y = \frac{(x + y) - (x - y)}{2}.$$

Поэтому у уравнения есть только два решения: (56; 55) и (20; 17).

Ответ. (20; 17) и (56; 55).

Задача 81. Найдите все пары целых чисел, для которых справедливо равенство

$$x^2 - 2xy - 3y^2 + 2x - y + 3 = 0.$$

Решение. Попробуем представить это уравнение в виде

$$(ax + by + c)(dx + ey + f) = g,$$

где коэффициенты a, b, c, d, e, f и g – какие-то целые числа.

Для этого воспользуемся *методом неопределённых коэффициентов*. То есть предположим, что в

таким виде представить можно, раскроем скобки и попробуем подобрать значения коэффициентов так, чтобы после раскрытия скобок получилось исходное равенство.

Итак, после раскрытия скобок и приведения подобных слагаемых мы получим

$$adx^2 + (ae + bd)xy + bey^2 + (af + cd)x + (bf + ec)y + (cf - g) = 0.$$

И мы хотим, чтобы это равенство превратилось в

$$x^2 - 2xy - 3y^2 + 2x - y + 3 = 0.$$

Значит, нам нужно, чтобы

$$\begin{cases} ad = 1, \\ ae + bd = -2, \\ be = -3, \\ af + cd = 2, \\ bf + ec = -1, \\ cf - g = 3. \end{cases}$$

У нас нет цели найти все решения этой системы. Нам достаточно подобрать какое-нибудь одно. Поэтому в первом уравнении можно, например, взять $a = d = 1$, тогда следующие два равенства переписутся в виде

$$\begin{cases} be = -3, \\ e + b = -2. \end{cases}$$

Напоминает теорему Виета, не правда ли? Сумма чисел равна (-2) , а произведение равно (-3) . Очевидно, что это числа 1 и (-3) . Пусть, например, $b = 1$, $e = -3$.

В итоге остались следующие три равенства:

$$\begin{cases} f + c = 2, \\ f - 3c = -1, \\ cf - g = 3. \end{cases}$$

Вычитая из первого равенства второе, получим $4c = 3$. И выходит, что целых значений c нет. Но тут главное – не опустить руки и попробовать продолжить! Мы получаем, что $c = \frac{3}{4}$. Тогда

$$\begin{aligned} f &= 2 - c = \frac{5}{4}, \\ g &= cf - 3 = \frac{15}{16} - 3 = -\frac{33}{16}. \end{aligned}$$

Это означает, что уравнение

$$\left(x + y + \frac{3}{4}\right)\left(x - 3y + \frac{5}{4}\right) = -\frac{33}{16}$$

равносильно исходному. Но домножив обе части этого равенства на 16, мы получим равенство

$$(4x + 4y + 3)(4x - 12y + 5) = -33,$$

в котором все коэффициенты целые!

А дальше мы уже умеем рассуждать. Нужно просто перебрать все пары чисел, произведение которых равно (-33) . Учитывая то, что $33 = 3 \cdot 11$, получаем восемь возможных пар:

$$\begin{aligned} 33 &= 1 \cdot (-33) = 3 \cdot (-11) = 11 \cdot (-3) = 33 \cdot (-1) = \\ &= (-1) \cdot 33 = (-3) \cdot 11 = (-11) \cdot 3 = (-33) \cdot 1. \end{aligned}$$

Рассмотрим эти восемь случаев.

Случай I.

$$\begin{cases} 4x + 4y + 3 = 1, \\ 4x - 12y + 5 = -33. \end{cases}$$

Тогда $4x + 4y = -2$. Но это невозможно, так как левая часть делится на 4, а правая – нет.

Случай II.

$$\begin{cases} 4x + 4y + 3 = 3, \\ 4x - 12y + 5 = -11. \end{cases}$$

Тогда

$$\begin{cases} x + y = 0, \\ x - 3y = -4. \end{cases}$$

Если вычесть из первого равенства второе, то получится $4y = 4$. Значит, $y = 1$. Поэтому $x = -1$.

Случай III.

$$\begin{cases} 4x + 4y + 3 = 11, \\ 4x - 12y + 5 = -3. \end{cases}$$

Тогда

$$\begin{cases} x + y = 2, \\ x - 3y = -2. \end{cases}$$

Если вычесть из первого равенства второе, то получится $4y = 4$. Значит, $y = 1$. Поэтому $x = 2 - 1 = 1$.

Случай IV.

$$\begin{cases} 4x + 4y + 3 = 33, \\ 4x - 12y + 5 = -1. \end{cases}$$

Тогда $4x + 4y = 30$. Но это невозможно, так как левая часть делится на 4, а правая – нет.

Случай V.

$$\begin{cases} 4x + 4y + 3 = -1, \\ 4x - 12y + 5 = 33. \end{cases}$$

Тогда

$$\begin{cases} x + y = -1, \\ x - 3y = 7. \end{cases}$$

Если вычесть из первого равенства второе, то получится $4y = -8$. Значит, $y = -2$. Поэтому $x = -1 + 2 = 1$.

Случай VI.

$$\begin{cases} 4x + 4y + 3 = -3, \\ 4x - 12y + 5 = 11. \end{cases}$$

Тогда $4x + 4y = -6$. Но это невозможно, так как левая часть делится на 4, а правая – нет.

Случай VII.

$$\begin{cases} 4x + 4y + 3 = -11, \\ 4x - 12y + 5 = 3. \end{cases}$$

Тогда $4x + 4y = -14$. Но это невозможно, так как левая часть делится на 4, а правая – нет.

Случай VIII.

$$\begin{cases} 4x + 4y + 3 = -33, \\ 4x - 12y + 5 = 1. \end{cases}$$

Тогда

$$\begin{cases} x + y = -9, \\ x - 3y = -1. \end{cases}$$

Если вычесть из первого равенства второе, то получится $4y = -8$. Значит, $y = -2$. Поэтому

$$x = -9 + 2 = -7.$$

В итоге мы получили четыре решения уравнения: $(-1; 1)$, $(1; 1)$, $(1; -2)$ и $(-7; -2)$.

Ответ. $(-1; 1)$, $(1; 1)$, $(1; -2)$ и $(-7; -2)$.

Теперь попробуйте самостоятельно решить следующие задачи.

Задача 82. Сколько пар натуральных чисел удовлетворяет равенству $2x + 5y = 1000$?

Задача 83. Помощники Деда Мороза разложили 1001 новогодний подарок в 40 мешков. Оказалось, что в некоторых мешках лежит по 22 подарка, а в остальных – по n . Какие значения может принимать число n ?

Задача 84. Найдите все пары натуральных чисел, для которых справедливо равенство

$$\text{НОД}(x, y) + \text{НОК}(x, y) = 101.$$

Задача 85. Найдите все тройки натуральных чисел, для которых справедливо равенство

$$4 \cdot (y^2 - z^2 - xz) = x^2 + x + 6.$$

Задача 86. Найдите все пары натуральных чисел, для которых справедливо равенство

$$3^m + 360 = n^2.$$

ГЛАВА 5 АРИФМЕТИКА ОСТАТКОВ

В этой главе мы с вами научимся работать с остатками, что поможет нам решать довольно содержательные задачи. Например, вы легко сможете найти остаток при делении числа 521^{637} на 17. Здесь я просто написал два случайных трёхзначных числа и какое-нибудь не очень большое двузначное. Вы же можете написать любые другие числа и совсем скоро убедитесь, что сможете решить любую такую задачу.

Понятно, что вы и сейчас можете решить эту задачу «руками». Сначала посмотреть, какой остаток при делении на 17 у числа 521. Потом вычислить 521^2 и найти, какой остаток у него. И так продолжать искать остатки у чисел 521^3 , 521^4 , 521^5 , ..., пока они не начнут повторяться. Затем доказать, что остатки заиклятся, и после этого понять, какой остаток будет у числа 521^{637} .

Но такое решение будет довольно долгим и скучным. Мы же научимся решать подобные задачи проще, быстрее и для любых чисел.

ОПЯТЬ ОСТАТКИ

В первой главе мы с вами уже говорили про остатки (см. стр. 30). Тогда мы поняли, что для любого целого числа a и натурального числа b существует представление числа a в виде

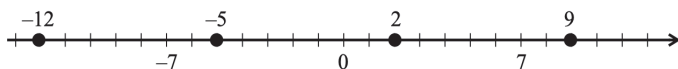


$$a = kb + r,$$

где k – некоторое целое число, а r – целое число от 0 до $(b - 1)$. При этом число r называется *остатком* при делении a на b .

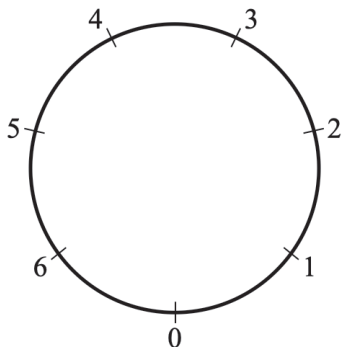
Давайте чуть подробнее обсудим, как на числовой прямой располагаются числа с одинаковым остатком при делении на какое-нибудь натуральное число m . Посмотрим, например, на числа, имеющие остаток 2 при делении на 7:

$$\begin{array}{ll} 9 = 1 \cdot 7 + 2, & 2 = 0 \cdot 7 + 2, \\ 16 = 2 \cdot 7 + 2, & -5 = (-1) \cdot 7 + 2, \\ 23 = 3 \cdot 7 + 2, & -12 = (-2) \cdot 7 + 2, \\ 30 = 4 \cdot 7 + 2, & -19 = (-3) \cdot 7 + 2, \\ \dots & \dots \end{array}$$



Все эти числа идут с шагом 7. Каждое из них на 2 больше какого-то числа, кратного семи. Поэтому, когда нас интересует только остаток при делении на какое-то число, можно воспринимать числовую прямую не как прямую, а как окружность, на

которую эта числовая прямая «намотана» так, что числа с одинаковыми остатками попадают в одни и те же точки:



При этом число 7 попадёт в точку 0, число 8 – в точку 1, число 9 – в точку 2 и так далее. В частности, все числа с остатком 2 при делении на 7

..., -19, -12, -5, 2, 9, 16, 23, 30, ...

попадут в точку 2.

Поэтому, если вас интересуют только остатки, то очень удобно считать, что целые числа расположены не на числовой прямой, а «бегают» по окружности.

На самом деле к подобному отношению к числовой прямой вы привыкли с детства. Когда вы смотрите на стрелочные часы, вы видите время, «намотанное» на окружность. По стрелочным часам вы не можете определить ни год, ни месяц, ни день недели. Вы даже не можете по ним понять, утро сейчас или вечер. По сути, часы показывают вам, какой сейчас «остаток от времени» при делении на 12 часов.

СРАВНЕНИЕ ПО МОДУЛЮ

Если нас интересует лишь остаток при делении числа на 7, например, то для нас числа 9 и 30 – это одно и то же. Им соответствует одна и та же точка на нашей окружности, у них обоих остаток равен 2.



В математике, когда что-то с чем-то в каком-то смысле одно и то же (или, как говорят математики, *эквивалентно*), обычно используется знак « \equiv ». Так и этом случае принято писать

$$9 \equiv 30 \pmod{7}.$$

Давайте дадим общее определение.

Говорят, что числа a и b *сравнимы по модулю m* , если они имеют одинаковые остатки при делении на m . И обозначается это следующим образом:

$$a \equiv b \pmod{m} \quad \text{или} \quad a \overset{m}{\equiv} b.$$

Это просто короткая форма записи утверждения, что *числа одинаковые с точки зрения делимости на m* .

Например,

$$13 \equiv 5 \pmod{4};$$

$$15 \equiv 39 \pmod{6};$$

$$-12 \equiv 3 \pmod{5};$$

$$14 \not\equiv 21 \pmod{3};$$

$$11 \not\equiv -7 \pmod{4}.$$

По этим примерам видно, что требуется некоторое усилие, чтобы, используя определение, понять, сравнимы ли два числа друг с другом по некоторому модулю m . Для этого нужно найти для каждого числа его остаток при делении на m и проверить, одинаковый он или нет. Но можно поступить проще!

Когда мы «наматывали» числовую ось на окружность, мы поняли не только то, что числа с одинаковыми остатками при делении на 7 попадают в одну и ту же точку, но и то, что попасть в ту же точку можно, только совершив несколько полных оборотов, то есть нужно изменить число на величину, кратную семи. Поэтому, для того чтобы понять, что у двух чисел остатки при делении на 7 равны, достаточно проверить, что их разность делится на 7. А это сделать гораздо проще.

Давайте сформулируем общее утверждение.

Утверждение. $a \equiv b \pmod{m}$ тогда и только тогда, когда разность $(a - b)$ делится на m .

Доказательство. Если $a \equiv b \pmod{m}$, то у чисел a и b одинаковые остатки при делении на m , значит,

$$a = km + r, \quad b = \ell m + r.$$

Тогда разность

$$\begin{aligned} a - b &= (km + r) - (\ell m + r) = km + r - \ell m - r = \\ &= km - \ell m = (k - \ell)m \end{aligned}$$

делится на m .

Докажем теперь в другую сторону. Пусть известно, что разность $(a - b)$ делится на m . И пусть числа

a и b дают, соответственно, остатки r_1 и r_2 при делении на m :

$$a = km + r_1, \quad b = \ell m + r_2.$$

Тогда

$$\begin{aligned} a - b &= (km + r_1) - (\ell m + r_2) = km + r_1 - \ell m - r_2 = \\ &= (km - \ell m) + (r_1 - r_2) = (k - \ell)m + (r_1 - r_2). \end{aligned}$$

Но если $(a - b)$ делится на m и $(k - \ell)m$ делится на m , то и $(r_1 - r_2)$ должно делиться на m .

Но числа r_1 и r_2 – это остатки при делении на m . Значит, каждое из них может принимать значения только от 0 до $(m - 1)$. Поэтому разность $(r_1 - r_2)$ может принимать значения от $(0 - (m - 1))$ до $((m - 1) - 0)$. Но среди чисел от $-(m - 1)$ до $(m - 1)$ есть только одно число, кратное m , – это число 0, потому что ближайшие к нулю числа, кратные m , – это $(-m)$ и m , которые не попадают в нужный промежуток.

И мы доказали, что если разность $(a - b)$ делится на m , то числа a и b дают одинаковые остатки при делении на m .

СВОЙСТВА СРАВНЕНИЯ ПО МОДУЛЮ

А теперь давайте докажем важные свойства сравнения по модулю, которые как раз и позволяют решать множество задач на делимость.



Утверждение. Пусть

$$a \equiv b \pmod{m},$$

$$c \equiv d \pmod{m}.$$

Тогда

$$a + c \equiv b + d \pmod{m},$$

$$a - c \equiv b - d \pmod{m},$$

$$ac \equiv bd \pmod{m}.$$

Иными словами, сравнения по одинаковому модулю можно почленно складывать, вычитать и умножать.

Доказательство. Мы только что доказали, что два числа имеют одинаковый остаток при делении на m тогда и только тогда, когда их разность делится на m . Таким образом, мы знаем, что разности $(a - b)$ и $(c - d)$ делятся на m , и хотим доказать, что тогда каждая из разностей

$$(a + c) - (b + d), \quad (a - c) - (b - d), \quad ac - bd$$

делится на m .

Заметим, что разность

$$(a + c) - (b + d) = a + c - b - d = (a - b) + (c - d)$$

делится на m , потому что равна сумме двух чисел, кратных m .

Аналогично разность

$$(a - c) - (b - d) = a - c - b + d = (a - b) - (c - d)$$

делится на m , потому что равна разности двух чисел, кратных m .

С произведением чуть сложнее. Вообще говоря, в математике есть два основных приёма, которые помогают сворачивать выражения – «умножить на единичку» и «прибавить нолик». Вот здесь помогает добавление нолика. Смотрите, у нас есть ac , а нам как-то нужно получить, например, $(a - b)$, потому что мы знаем, что эта разность делится на m . Для этого можно из ac вычесть bc . Но чтобы выражение не изменилось, нужно обратно добавить bc :

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

По сути, для того чтобы сделать это преобразование, мы «прибавили нолик»¹, а конкретно – выражение $(-bc + bc)$.

Но $c(a - b)$ делится на $(a - b)$, значит, делится и на m , а $b(c - d)$ делится на $(c - d)$, значит, делится и на m . Поэтому разность $(ac - bd)$ делится на m .

Из последнего доказанного свойства есть важное следствие. Пусть

$$a \equiv b \pmod{m},$$

¹Заметим, что доказать делимость на m разности $(ac - bd)$ можно было и «в лоб». Действительно, пусть числа a и b дают остаток r_1 , а числа c и d – остаток r_2 при делении на m . То есть

$$a = km + r_1, \quad b = \ell m + r_1, \quad c = pm + r_2, \quad d = qm + r_2.$$

Тогда разность

$$\begin{aligned} ac - bd &= (km + r_1)(pm + r_2) - (\ell m + r_1)(qm + r_2) = \\ &= (kpm^2 + r_1pm + r_2km + r_1r_2) - \\ &\quad - (\ell qm^2 + r_1qm + r_2\ell m + r_1r_2) = \\ &= m \cdot (kpm + r_1p + r_2k - \ell qm - r_1q - r_2\ell) \end{aligned}$$

кратна m .

тогда, применив последнее свойство к парам чисел $(a; b)$ и $(a; b)$, мы получим, что

$$a^2 \equiv b^2 \pmod{m}.$$

Теперь, применив последнее свойство к парам $(a; b)$ и $(a^2; b^2)$, получим, что

$$a^3 \equiv b^3 \pmod{m}.$$

Применив его к парам $(a; b)$ и $(a^3; b^3)$, получим

$$a^4 \equiv b^4 \pmod{m}.$$

И так далее.

Тем самым мы доказали следующее утверждение.

Утверждение. Пусть

$$a \equiv b \pmod{m}.$$

Тогда для любого натурального n

$$a^n \equiv b^n \pmod{m}.$$

Иначе говоря, обе части сравнения можно возводить в любую натуральную степень¹.

¹Если знать формулу разности n -ых степеней

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1}),$$

то последнее утверждение можно доказать иначе. Действительно, из этой формулы следует, что $(a^n - b^n)$ делится на $(a - b)$. Поэтому, если $(a - b)$ делится на m , то и $(a^n - b^n)$ делится на m .

Например,

$$16 \equiv 9 \pmod{7} \quad \Rightarrow \quad 256 \equiv 81 \pmod{7};$$

$$5 \equiv 2 \pmod{3} \quad \Rightarrow \quad 125 \equiv 8 \pmod{3};$$

$$10 \equiv 3 \pmod{7} \quad \Rightarrow \quad 10\,000 \equiv 81 \pmod{7}.$$

Благодаря этим свойствам мы уже можем решать довольно сложные задачи на делимость. Давайте посмотрим некоторые из них.

ЗАДАЧИ НА НАХОЖДЕНИЕ ОСТАТКА

Задача 87. Найдите остаток при делении числа 2^{1111} на 15.

Решение. Основная идея решения таких задач заключается в том, что нужно найти такую степень (в данном случае) двойки, которая недалеко от числа, кратного 15. Например, $2^4 = 16$ на 1 больше, чем 15. Поэтому



$$2^4 = 16 \equiv 1 \pmod{15}.$$

Используя то, что $1111 = 277 \cdot 4 + 3$, получаем

$$\begin{aligned} 2^{1111} &= 2^3 \cdot 2^{1108} = 8 \cdot (2^4)^{277} = \\ &= 8 \cdot 16^{277} \equiv 8 \cdot 1^{277} = 8 \pmod{15}. \end{aligned}$$

Мы показали, что у числа 2^{1111} такой же остаток при делении на 15, как и у числа 8. То есть остаток равен 8.

Ответ. Остаток равен 8.

Задача 88. Найдите остаток при делении числа 2^{1111} на 17.

Решение. Если мы попробуем найти степень двойки, у которой маленький остаток при делении на 17, то окажется, что это не очень просто. Пока степень двойки меньше 17, остаток будет совпадать с самим числом, а это нам ничего не даёт. У числа $2^5 = 32$ остаток равен 15, у $2^6 = 64$ остаток равен 13, а дальше уже не очень хочется считать.

Но! Тут важно вспомнить, что есть ещё и отрицательные числа. Нам необязательно заменять именно на остаток. Можно же сказать, что

$$2^4 = 16 \equiv -1 \pmod{17}.$$

Тогда

$$\begin{aligned} 2^{1111} &= 2^3 \cdot 2^{1108} = 8 \cdot (2^4)^{277} = 8 \cdot 16^{277} \equiv \\ &\equiv 8 \cdot (-1)^{277} = 8 \cdot (-1) = -8 \pmod{17}. \end{aligned}$$

Таким образом, мы показали, что у числа 2^{1111} такой же остаток при делении на 17, как и у числа

$$-8 = (-1) \cdot 17 + 9.$$

То есть остаток равен 9.

Ответ. Остаток равен 9.

Задача 89. Найдите остаток при делении числа

$$(75 \cdot 56)^{28} + (58 \cdot 34)^{31}$$

на 19.

Решение. Заметим, что

$$75 \equiv -1 \pmod{19};$$

$$56 \equiv -1 \pmod{19};$$

$$58 \equiv 1 \pmod{19};$$

$$34 \equiv -4 \pmod{19}.$$

Тогда

$$75 \cdot 56 \equiv (-1) \cdot (-1) = 1 \pmod{19};$$

$$58 \cdot 34 \equiv 1 \cdot (-4) = -4 \pmod{19}.$$

Значит,

$$(75 \cdot 56)^{28} \equiv 1^{28} = 1 \pmod{19},$$

$$\begin{aligned} (58 \cdot 34)^{31} &\stackrel{19}{\equiv} (-4)^{31} = -4^{31} = -4 \cdot (4^2)^{15} = -4 \cdot 16^{15} \stackrel{19}{\equiv} \\ &\stackrel{19}{\equiv} -4 \cdot (-3)^{15} = 4 \cdot 3^{15} = 4 \cdot (3^3)^5 = 4 \cdot 27^5 \stackrel{19}{\equiv} \\ &\stackrel{19}{\equiv} 4 \cdot 8^5 = 4 \cdot 8 \cdot (8^2)^2 = 32 \cdot 64^2 \stackrel{19}{\equiv} 32 \cdot 7^2 = \\ &= 32 \cdot 49 \stackrel{19}{\equiv} (-6) \cdot 11 = -66 \equiv 10 \pmod{19}. \end{aligned}$$

В этой длинной цепочке¹ мы воспользовались тем, что

$$16 \equiv -3 \pmod{19}; \quad 27 \equiv 8 \pmod{19};$$

$$64 \equiv 7 \pmod{19}; \quad 32 \equiv -6 \pmod{19};$$

$$49 \equiv 11 \pmod{19}; \quad -66 \equiv 10 \pmod{19}.$$

¹Напомню, что при определении сравнения по модулю (см. стр. 168) мы договорились, что есть два равноправных обозначения:

$$a \equiv b \pmod{m} \quad \text{и} \quad a \stackrel{m}{\equiv} b.$$

При длинных преобразованиях мы чаще будем использовать второе обозначение.

В итоге получаем, что

$$(75 \cdot 56)^{28} + (58 \cdot 34)^{31} \equiv 1 + 10 = 11 \pmod{19}.$$

Ответ. Остаток равен 11.

На примере этой задачи видно, как работает основная идея. Мы сначала перешли от исследования числа $(58 \cdot 34)^{31}$ к числу 4^{31} , потом к 3^{15} и так далее, постепенно понижая показатель степени, пока не дошли до числа 10.

Теперь мы, наконец, готовы обсудить задачу, которая была анонсирована в начале главы.

Задача 90. Найдите остаток при делении числа 521^{637} на 17.

Решение. Заметим, что $510 = 30 \cdot 17$, поэтому

$$521 = 510 + 11 \equiv 11 \equiv -6 \pmod{17}.$$

Значит,

$$\begin{aligned} 521^{637} &\stackrel{17}{\equiv} (-6)^{637} = -6^{637} = -6 \cdot (6^2)^{318} = \\ &= -6 \cdot 36^{318} \stackrel{17}{\equiv} -6 \cdot 2^{318} = -6 \cdot 2^2 \cdot (2^4)^{79} = \\ &= -24 \cdot 16^{79} \stackrel{17}{\equiv} -24 \cdot (-1)^{79} = -24 \cdot (-1) = \\ &= 24 \equiv 7 \pmod{17}. \end{aligned}$$

Здесь мы воспользовались тем, что

$$\begin{array}{ll} 521 \equiv -6 \pmod{17}; & 36 \equiv 2 \pmod{17}; \\ 16 \equiv -1 \pmod{17}; & 24 \equiv 7 \pmod{17}. \end{array}$$

И в итоге получили, что

$$521^{637} \equiv 7 \pmod{17}.$$

Поэтому остаток при делении числа 521^{637} на 17 равен 7.

Ответ. Остаток равен 7.

Помните, в самом начале книги мы довольно долго искали остаток при делении числа

$$10^{1000} + 12^{1000}$$

на 11 (см. задачу 6 на стр. 39). Сейчас мы можем сделать это в одну строчку:

$$10^{1000} + 12^{1000} \stackrel{11}{\equiv} (-1)^{1000} + 1^{1000} = 1 + 1 = 2.$$

Чтобы убедиться, что вы поняли, как работает сравнение по модулю, решите самостоятельно следующие задачи.

Задача 91. Найдите остаток при делении числа 10^{70} на 27.

Задача 92. Найдите последнюю цифру числа 2^{1111} .

Задача 93. Найдите остаток при делении числа

$$2^{1234} + 7^{1234}$$

на 11.

Задача 94. Найдите две последние цифры числа 7^{777} .

ОПЯТЬ ПРО ПРИЗНАКИ ДЕЛИМОСТИ

В первой главе мы с вами уже доказывали некоторые признаки делимости (см. стр. 24), сейчас же покажем, как сравнение по модулю позволяет не просто доказать все эти (и некоторые другие) признаки, но и ответить на вопрос, чему равен остаток.



Пусть $a = \overline{a_n a_{n-1} \dots a_1 a_0}$, тогда

$$a = 10 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0 \stackrel{2, 5, 10}{\equiv} 0 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0 = a_0.$$

Таким образом, мы доказали, что у числа a такой же остаток при делении на 2, на 5 и на 10, как у его последней цифры a_0 .

Аналогично получаем, что

$$a = 100 \cdot \overline{a_n a_{n-1} \dots a_2} + \overline{a_1 a_0} \stackrel{4, 20, 25, 50, 100}{\equiv} 0 \cdot \overline{a_n a_{n-1} \dots a_2} + \overline{a_1 a_0} = \overline{a_1 a_0}.$$

Это означает, что у числа a такой же остаток при делении на 4, на 20, на 25, на 50 и на 100, как у числа $\overline{a_1 a_0}$, образованного двумя его последними цифрами.

Точно как же доказываются соответствующие «признаки делимости» на любой делитель степени десятки. Чтобы убедиться в этом, решите самостоятельно следующие задачи.

Задача 95. Как по десятичной записи числа найти его остаток при делении на 8?

Задача 96. Как по десятичной записи числа найти его остаток при делении на 16?

Идём дальше. Пусть

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} = a_0 + 10a_1 + 10^2 a_2 + \dots + 10^n a_n.$$

При делении на что число 10 имеет маленький остаток? При делении на 3 и на 9 число 10 даёт остаток 1. Поэтому

$$10 \overset{3,9}{\equiv} 1 \quad \Rightarrow \quad 10^k \overset{3,9}{\equiv} 1^k = 1.$$

Из этого следует, что

$$\begin{aligned} a &= a_0 + 10a_1 + 10^2 a_2 + \dots + 10^n a_n \overset{3,9}{\equiv} \\ &\overset{3,9}{\equiv} a_0 + a_1 + a_2 + \dots + a_n. \end{aligned}$$

Таким образом, мы доказали, что у числа a такой же остаток при делении на 3 и на 9, как у его суммы цифр.

Тут важно отметить, что мы поняли, что есть такие простые признаки делимости на 3 и на 9, не потому, что 3 – это какое-то приятное простое число, а 9 – его квадрат, а потому, что 3 и 9 – это делители числа $(10 - 1)$.

Если бы у нас была, например, шестнадцатеричная система счисления, то такие красивые признаки делимости были бы для делителей числа $15 = 16 - 1$, то есть для 3, 5 и 15. А если бы мы пользовались двенадцатеричной системой счисления, то такой признак был бы только для $11 = 12 - 1$.

Но есть число, по модулю которого 10 сравнимо с (-1) . Это число 11. Поэтому

$$10 \equiv -1 \pmod{11} \quad \Rightarrow \quad 10^k \equiv (-1)^k \pmod{11},$$

то есть 10 в нечётной степени сравнимо с (-1) , а в чётной – с 1 по модулю 11.

Это значит, что

$$\begin{aligned} a &= a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \dots + 10^n a_n \equiv \\ &\equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n \cdot a_n \pmod{11}. \end{aligned}$$

В итоге мы доказали, что у числа a такой же остаток при делении на 11, как у его *знакопеременной суммы цифр*:

$$a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n \cdot a_n.$$

Помните, в самом начале книги мы обсуждали два способа, как можно найти остаток при делении числа 123 456 789 на 11 (см. задачу 4 на стр. 37). Сейчас мы можем ответить на этот вопрос мгновенно:

$$123\,456\,789 \equiv 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5 \pmod{11}.$$

Можно было бы обобщить признаки делимости на 9 и на 11, разбив число не на отдельные разряды, а на группы по две цифры

$$a = \overline{a_n a_{n-1} \dots a_1 a_0} = \overline{a_1 a_0} + 100 \cdot \overline{a_3 a_2} + 100^2 \cdot \overline{a_5 a_4} + \dots,$$

и посмотреть, по какому модулю число 100 сравнимо с ± 1 .

Но, к сожалению, ничего интересного здесь не получится, потому что, если

$$100 \equiv 1 \pmod{m},$$

то число m является делителем числа 99. На 3, на 9 и на 11 у нас есть более простые признаки делимости, и вряд ли нам пригодятся признаки делимости на 33 и на 99. Но, если интересно, то и их можно сформулировать:

$$\begin{aligned} a = \overline{a_1 a_0} + 100 \cdot \overline{a_3 a_2} + 100^2 \cdot \overline{a_5 a_4} + \dots &\stackrel{33, 99}{=} \\ &\stackrel{33, 99}{=} \overline{a_1 a_0} + \overline{a_3 a_2} + \overline{a_5 a_4} + \dots \end{aligned}$$

С (-1) всё ещё более грустно, потому что, если

$$100 \equiv -1 \pmod{m},$$

то число m является делителем числа 101, которое простое. Поэтому мы сможем сформулировать лишь признак делимости на 101:

$$\begin{aligned} a = \overline{a_1 a_0} + 100 \cdot \overline{a_3 a_2} + 100^2 \cdot \overline{a_5 a_4} + 100^3 \cdot \overline{a_7 a_6} + \dots &\stackrel{101}{=} \\ &\stackrel{101}{=} \overline{a_1 a_0} - \overline{a_3 a_2} + \overline{a_5 a_4} - \overline{a_7 a_6} + \dots \end{aligned}$$

Но давайте попробуем продолжить, разбив число группы по три цифры

$$\begin{aligned} a &= \overline{a_n a_{n-1} \dots a_1 a_0} = \\ &= \overline{a_2 a_1 a_0} + 1000 \cdot \overline{a_5 a_4 a_3} + 1000^2 \cdot \overline{a_8 a_7 a_6} + \dots \end{aligned}$$

и посмотрев, по какому модулю число 1000 сравнимо с ± 1 .

Если

$$1000 \equiv 1 \pmod{m},$$

то число m является делителем числа 999. Давайте разложим его на простые множители:

$$999 = 9 \cdot 111 = 3^2 \cdot 3 \cdot 37 = 3^3 \cdot 37.$$

Но на 3, на 9 у нас есть более простые признаки делимости, остаются не самые интересные делители 27, 37, 111, 333, 999. Мы получаем, что по каждому из этих модулей

$$\begin{aligned} a &= \overline{a_2 a_1 a_0} + 1000 \cdot \overline{a_5 a_4 a_3} + 1000^2 \cdot \overline{a_8 a_7 a_6} + \dots \equiv \\ &\equiv \overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} + \dots \end{aligned}$$

Но вряд ли мы будем использовать такие признаки делимости.

А вот с (-1) всё интереснее! Если

$$1000 \equiv -1 \pmod{m},$$

то число m является делителем числа

$$1001 = 7 \cdot 11 \cdot 13.$$

И если на 11 у нас есть более простой признак делимости, то для 7 и 13 (а заодно и для не очень интересных 77, 91, 143 и 1001) мы получили, что по каждому из этих модулей

$$\begin{aligned} a &= \overline{a_2 a_1 a_0} + 1000 \cdot \overline{a_5 a_4 a_3} + 1000^2 \cdot \overline{a_8 a_7 a_6} + \dots \equiv \\ &\equiv \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \dots \end{aligned}$$

Давайте посмотрим, как это работает, на примере следующих задач.

Задача 97. Найдите остаток при делении числа 12 345 678 на 7.

Решение. Мы только что доказали, что

$$12\,345\,678 \equiv 678 - 345 + 12 = 333 + 12 = 345 \pmod{7}.$$

Учитывая то, что 350 делится на 7, получаем, что

$$345 \equiv -5 \equiv 2 \pmod{7}.$$

Поэтому

$$12\,345\,678 \equiv 2 \pmod{7}.$$

Таким образом, остаток при делении числа 12 345 678 на 7 равен 2.

Ответ. Остаток равен 2.

Задача 98. Найдите остаток при делении числа 123 456 789 на 13.

Решение. Мы доказали, что

$$\begin{aligned} 123\,456\,789 &\equiv 789 - 456 + 123 = \\ &= 333 + 123 = 456 \pmod{13}. \end{aligned}$$

Учитывая то, что 390 делится на 13, получаем, что

$$456 \equiv 66 \equiv 1 \pmod{13}.$$

Поэтому

$$123\,456\,789 \equiv 1 \pmod{13}.$$

Таким образом, остаток при делении числа 123 456 789 на 13 равен 1.

Ответ. Остаток равен 1.

А для решения следующих задач достаточно знаний, полученных в этом разделе.

Задача 99. Докажите, что если у чисел n и $2n$ одинаковая сумма цифр, то число n делится на 9.

Задача 100. Существует ли натуральное число, которое при делении на сумму своих цифр и в остатке, и в неполном частном даёт 100?

Задача 101. Найдите значения цифр a и b , если известно, что число

$$\overbrace{1234 \dots 1234}^{1234 \text{ раза}} a1234b \overbrace{1234 \dots 1234}^{1234 \text{ раза}}$$

делится на 99.

ЗАДАЧИ НА ДОКАЗАТЕЛЬСТВО ДЕЛИМОСТИ

До этого мы применяли сравнение по модулю для поиска остатков у конкретных чисел. А в этом разделе поговорим о том, как оно помогает доказывать делимость в общем виде.



И начнём с совсем простых задач.

Задача 102. Докажите, что при всех натуральных n число $(7^n - 1)$ делится на 6.

Решение. Так как $7 \equiv 1 \pmod{6}$, то

$$7^n \equiv 1^n = 1 \pmod{6}.$$

Значит, разность $(7^n - 1)$ делится на 6.

Задача 103. Докажите, что при всех натуральных n число $(7^{n+2} + 8^{2n+1})$ делится на 57.

Решение. Заметим, что

$$\begin{aligned}7^{n+2} &= 7^2 \cdot 7^n = 49 \cdot 7^n; \\8^{2n+1} &= 8 \cdot 8^{2n} = 8 \cdot (8^2)^n = 8 \cdot 64^n \equiv 8 \cdot 7^n \pmod{57}.\end{aligned}$$

Поэтому

$$7^{n+2} + 8^{2n+1} \overset{57}{\equiv} 49 \cdot 7^n + 8 \cdot 7^n = 57 \cdot 7^n \equiv 0 \cdot 7^n = 0 \pmod{57}.$$

То есть при всех натуральных n число

$$7^{n+2} + 8^{2n+1}$$

делится на 57.

Задача 104. Докажите, что при всех чётных натуральных n число $(5^n + 23)$ делится на 24.

Решение. Так как n – чётное число, то оно равно $2k$, где k – натуральное. Тогда

$$5^n = 5^{2k} = (5^2)^k = 25^k \equiv 1^k = 1 \pmod{24}.$$

Поэтому

$$5^n + 23 \overset{24}{\equiv} 1 + 23 = 24 \equiv 0 \pmod{24}.$$

То есть при всех чётных натуральных n число $(5^n + 23)$ делится на 24.

Задача 105. Докажите, что при всех нечётных натуральных n число $(5^n + 11^n + 2)$ делится на 6.

Решение. Так как n – нечётное число, то оно равно $(2k + 1)$, где k – целое неотрицательное. Тогда

$$\begin{aligned} 5^n &= 5^{2k+1} = 5 \cdot 5^{2k} = 5 \cdot (5^2)^k = \\ &= 5 \cdot 25^k \equiv 5 \cdot 1^k = 5 \pmod{6}; \\ 11^n &\equiv 5^n \equiv 5 \pmod{6}. \end{aligned}$$

Значит,

$$5^n + 11^n + 2 \overset{6}{\equiv} 5 + 5 + 2 = 12 \equiv 0 \pmod{6}.$$

То есть при всех нечётных натуральных n число $(5^n + 11^n + 2)$ делится на 6.

Пока во всех задачах нужно было доказать делимость на некоторое фиксированное число. Но те же рассуждения работают и в более сложных конструкциях, когда и само число, и его делитель зависят от произвольного натурального n .

Задача 106. Докажите, что при всех натуральных $n > 1$ число

$$(2^n - 1)^n - 3$$

делится на $(2^n - 3)$.

Решение. Пусть $m = 2^n - 3$, тогда

$$2^n - 1 = (2^m - 3) + 2 = m + 2 \equiv 2 \pmod{m}.$$

Значит,

$$(2^n - 1)^n - 3 \overset{m}{\equiv} 2^n - 3 = m \equiv 0 \pmod{m}.$$

То есть при всех натуральных $n > 1$ число

$$(2^n - 1)^n - 3$$

делится на $(2^n - 3)$.

А следующие задачи попробуйте решить самостоятельно.

Задача 107. Докажите, что при всех натуральных n число $(2^{4n} - 1)$ делится на 15.

Задача 108. Докажите, что при всех натуральных n число $(13^n + 3^{n+2})$ делится на 10.

Задача 109. Докажите, что при всех чётных натуральных n число $(7^n - 1)$ делится на 12.

Задача 110. Докажите, что при всех нечётных натуральных n число $(5^n + 2^n)$ делится на 7.

Задача 111. Докажите, что при всех нечётных натуральных n число $(n^{n+2} + (n+2)^n)$ делится на $(2n+2)$.

Давайте теперь обсудим другой тип задач. Посмотрим, как можно рассуждать, когда переменная n находится не в показателе степени, а в её основании.



Задача 112. Докажите¹, что при всех натуральных n число $(n^3 - n)$ делится на 3.

Решение. Число n может иметь один из трёх остатков при делении на три – 0, 1 или 2. Посмотрим, как связаны остатки при делении на 3 у чисел n и n^3 :

¹Стоит отметить, что эту задачу легко решить и без сравнения по модулю. Действительно,

$$n^3 - n = n(n^2 - 1) = n(n-1)(n+1),$$

поэтому оно равно произведению трёх последовательных чисел $(n-1)$, n и $(n+1)$. А среди трёх последовательных чисел есть то, которое делится на 3.

n	n^3
0	$0^3 = 0$
1	$1^3 = 1$
2	$2^3 = 8 \equiv 2$

Это означает, что при всех натуральных n

$$n^3 \equiv n \pmod{3}.$$

Поэтому разность $(n^3 - n)$ делится на 3.

Таким образом, идея заключается в том, что по модулю 3 число n может быть только 0, 1 или 2. И для доказательства делимости достаточно перебрать эти три случая. Давайте отработаем этот приём на следующей задаче.

Задача 113. Докажите, что при всех натуральных n число $(n^5 - n)$ делится на 5.

Решение. Число n может иметь один из пяти остатков при делении на пять – 0, 1, 2, 3 или 4. Посмотрим, как связаны остатки при делении на 5 у чисел n и n^5 :

n	n^5
0	$0^5 = 0$
1	$1^5 = 1$
2	$2^5 = 32 \equiv 2$
3	$3^5 = 243 \equiv 3$
4	$4^5 = 1024 \equiv 4$

В итоге мы получили, что при всех натуральных n

$$n^5 \equiv n \pmod{5}.$$

Поэтому разность $(n^5 - n)$ делится на 5.

Заметим, что если не хочется считать, чему равны значения 3^5 и 4^5 , то можно поступить, например, так:

$$3^5 = 3 \cdot 9^2 \stackrel{5}{\equiv} 3 \cdot 4^2 = 3 \cdot 16 \stackrel{5}{\equiv} 3 \cdot 1 = 3;$$

$$4^5 = (2^5)^2 \stackrel{5}{\equiv} 2^2 = 4.$$

Но можно и ещё сильнее сократить вычисления. Давайте убедимся в этом на следующей задаче.

Задача 114. Докажите, что при всех натуральных n число $(n^7 - n)$ делится на 7.

Решение. Число n может иметь один из семи остатков при делении на семь – 0, 1, 2, 3, 4, 5 или 6. Посмотрим, как связаны остатки при делении на 7 у чисел n и n^7 . Начнём заполнять табличку:

n	n^7
0	$0^7 = 0$
1	$1^7 = 1$
2	$2^7 = 2 \cdot 8^2 \stackrel{7}{\equiv} 2 \cdot 1^2 = 2$
3	$3^7 = 3 \cdot 9^3 \stackrel{7}{\equiv} 3 \cdot 2^3 = 24 \stackrel{7}{\equiv} 3$

И вот тут, в середине, можно остановиться и больше ничего не делать. Знаете почему? Потому что

$$4^7 \stackrel{7}{\equiv} (-3)^7 = -3^7 \stackrel{7}{\equiv} -3 \stackrel{7}{\equiv} 4;$$

$$5^7 \stackrel{7}{\equiv} (-2)^7 = -2^7 \stackrel{7}{\equiv} -2 \stackrel{7}{\equiv} 5;$$

$$6^7 \stackrel{7}{\equiv} (-1)^7 = -1 \stackrel{7}{\equiv} 6.$$

То есть, как только мы доказали, что $3^7 \equiv 3$, мы мгновенно получили, что и $4^7 \equiv 4$.

В итоге мы получили, что при всех натуральных n

$$n^7 \equiv n \pmod{7}.$$

Поэтому разность $(n^7 - n)$ делится на 7.

После этой серии задач может показаться, что для любого нечётного k будет верно утверждение:

$$n^k \equiv n \pmod{k}.$$

Но давайте посмотрим, что будет при $k = 9$.

Задача 115. Верно ли, что при всех натуральных n число $(n^9 - n)$ делится на 9.

Решение. Посмотрим, как связаны остатки при делении на 9 у чисел n и n^9 . Начнём заполнять таблицу:

n	n^9
0	$0^9 = 0$
1	$1^9 = 1$
2	$2^9 = 8^3 \equiv (-1)^3 = -1 \equiv 8$

То есть, если $n \equiv 2$, то $n^9 \equiv 8$. А значит, не при всех натуральных n число $(n^9 - n)$ делится на 9.

Ответ. Неверно, не при всех натуральных n число $(n^9 - n)$ делится на 9.

Значит, это правило не работает для любого нечётного числа k . Неправда, что для всех таких k

будет верно утверждение:

$$n^k \equiv n \pmod{k}.$$

А для каких будет? Что общего между числами 3, 5 и 7? Что это за свойство, которым обладают эти числа и не обладает число 9? Они простые! На самом деле, верно следующее утверждение.

Пусть p – простое число, тогда при всех натуральных n число $(n^p - n)$ делится на p .

Это утверждение называется *малой теоремой Ферма*, и в следующей главе мы с вами докажем эту теорему!

Но для каждого конкретного (не очень большого) простого числа можно доказывать теорему «руками», как мы это делали для 3, 5 и 7. Чтобы в этом убедиться, давайте возьмём, например, число 37 и покажем, как можно даже для него легко доказать малую теорему Ферма.

Задача 116. Докажите, что при всех натуральных n число $(n^{37} - n)$ делится на 37.

Решение. Точно так же, как и раньше, нам нужно перебрать все возможные остатки. С нулём и единицей всё совсем очевидно:



$$0^{37} = 0, \quad 1^{37} = 1.$$

Проверим двойку:

$$2^{37} = 2^2 \cdot (2^5)^7 = 4 \cdot 32^7 \equiv 4 \cdot (-5)^7 = -4 \cdot 5^7 =$$

$$\begin{aligned}
 &= -4 \cdot 5 \cdot (5^3)^2 = -20 \cdot 125^2 \equiv -20 \cdot 14^2 = \\
 &= -20 \cdot 196 \equiv -20 \cdot 11 = -220 \equiv 2.
 \end{aligned}$$

Тоже получилось, но не очень быстро. И кажется, что дальше будет только сложнее.

Давайте выпишем все 37 остатков при делении на 37 и будем вычёркивать те, для которых мы уже доказали наше утверждение:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36			

Но это ещё не всё! Мы же помним, что $36 \equiv -1$, а $35 \equiv -2$. Поэтому

$$\begin{aligned}
 36^{37} &\equiv (-1)^{37} = -1 \equiv 36 \pmod{37}; \\
 35^{37} &\equiv (-2)^{37} = -2^{37} \equiv -2 \equiv 35 \pmod{37}.
 \end{aligned}$$

Но и это ещё не всё! Если мы доказали для остатка 2, то мы доказали для $4 = 2^2$, $8 = 2^3$ и так далее, потому что

$$\begin{aligned}
 4^{37} &= (2^{37})^2 \equiv 2^2 = 4; \\
 8^{37} &= (2^{37})^3 \equiv 2^3 = 8.
 \end{aligned}$$

То есть мы уже доказали для 4, 8, 16 и 32:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36			

Но если мы доказали для остатка 4, то доказали и для $33 \equiv -4$; если доказали для остатка 8, то доказали и для $29 \equiv -8$; если доказали для остатка 16, то доказали и для 21; если доказали для остатка 32, то доказали и для 5:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36			

И при этом мы пока честно считали только для 2^{37} . Но давайте продолжим! Мы же знаем, что если $a^{37} \equiv a$ и $b^{37} \equiv b$, то и

$$(ab)^{37} = a^{37} \cdot b^{37} \equiv ab \pmod{37}.$$

Это значит, что мы уже доказали для остатков $10 = 2 \cdot 5$, $20 = 4 \cdot 5$, $25 = 5^2$, а значит, и для $27 \equiv -10$, $17 \equiv -20$, $12 \equiv -25$:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36			

Идем дальше: $34 = 2 \cdot 17$, а $3 \equiv -34$. То есть мы доказали для остатка 3. А значит, уже есть

$$\begin{array}{lll} 6 = 2 \cdot 3, & 9 = 3^2, & 15 = 3 \cdot 5, \\ 18 = 2 \cdot 9, & 24 = 3 \cdot 8, & 30 = 3 \cdot 10. \end{array}$$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36			

Но тогда есть

$$\begin{array}{lll} 31 \equiv^{37} -6, & 28 \equiv^{37} -9, & 22 \equiv^{37} -15, \\ 19 \equiv^{37} -18, & 13 \equiv^{37} -24, & 7 \equiv^{37} -30. \end{array}$$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36			

Осталось заметить, что $14 = 2 \cdot 7$ и $26 = 2 \cdot 13$, а $11 \equiv^{37} -26$ и $23 \equiv^{37} -14$. И в итоге мы проверили все остатки! И мы получили, что при всех натуральных n

$$n^{37} \equiv n \pmod{37}.$$

Поэтому разность $(n^{37} - n)$ делится на 37.

То есть оказалось, что проверить нужно было только двойку, а всё остальное получилось автоматически. Так что важно иногда быть немного ленивым и не бросаться сразу что-то делать, а немного подумать, чтобы в итоге всё получилось само собой.

ГЛАВА 6

ТЕОРЕМЫ ФЕРМА И ЭЙЛЕРА

Вот мы и добрались до главы, в которой наконец докажем две важные теоремы теории чисел – малую теорему Ферма и теорему Эйлера. Но пока давайте отдохнём от теории чисел и обсудим один красивый комбинаторный сюжет¹.

ЗАДАЧА ПРО БУСЫ

Задача 117. Сколько существует различных бус, состоящих из p бусинок одинакового размера (где p – простое), каждая из которых одного из n цветов?

Если одни бусы переходят в другие при повороте, то это одни и те же бусы, но при этом считаем,

¹Те из вас, кто уже прочитал мою книжку по комбинаторике, наверняка помнят эту задачу. На мой взгляд, это очень важная задача, связывающая воедино комбинаторику и теорию чисел, поэтому я решил, что стоит о ней рассказать и в этой книге тоже.

что бусы лежат на столе, то есть переворачивать их нельзя.

Решение. Сразу количество различных бус тяжело посчитать, потому что нужно как-то учесть, что бусы, переходящие друг в друга при повороте, – это одни и те же бусы. Поэтому давайте сначала посчитаем количество *цепочек*. Цепочка – это бусы, которые разрезали в каком-то месте, то есть это просто бусинки, выстроенные в ряд. У цепочки есть начало и конец:



Сколько различных цепочек можно сделать, если должно быть p бусинок, каждая из которых одного из n цветов? Это совсем просто. Первая – любого цвета – n вариантов, вторая – любого цвета – n вариантов и так далее. Всего получается $n \cdot n \cdot n \cdot \dots \cdot n = n^p$ различных цепочек.

Теперь давайте поймём, как связано количество цепочек и количество бус. Каждые бусы можно разрезать в любом из n мест – между любыми двумя бусинками. Поэтому кажется, что количество цепочек должно быть в n раз больше, чем количество бус. Но это не совсем так, потому что есть бусы, которые при разрезании в разных местах образуют одну и ту же цепочку! Например, если у бус все бусинки одного цвета, то, где бы вы их ни разрезали, вы получите одну и ту же одноцветную цепочку.

Если бы число p не было простым, например если бы оно было чётным числом, то бусинки бы

могли чередоваться, и, разрезав их в разных местах, можно было бы получить одну и ту же цепочку. Но когда p – простое число, то такая проблема есть лишь у одноцветных бус.

Дело в том, что, если при разрезании некоторых бус в разных местах получаются одинаковые цепочки, значит, эти бусы переходят сами в себя при некотором повороте. Но тогда в этих бусах есть некоторая повторяющаяся последовательность бусинок. Значит, число p делится на количество бусинок в этой повторяющейся последовательности. Но число p – простое, поэтому делится только на единицу и на p .

В первом случае получаем, что все бусинки одного цвета. А во втором – что эта «повторяющаяся последовательность бусинок» состоит из всех бусинок, то есть для того, чтобы совместить бусы сами с собой, нам пришлось сделать полный круг, а значит, нет двух разных мест, разрезав бусы в которых мы получаем одинаковые цепочки.

Давайте пока забудем про одноцветные бусы и одноцветные цепочки, тогда бус будет ровно в p раз меньше, чем цепочек. Неодноцветных цепочек всего $(n^p - n)$, так как из всех n^p цепочек только n цепочек одного цвета. Значит, неодноцветных бус будет $\frac{n^p - n}{p}$. Но одноцветных бус тоже n штук. В итоге получаем, что существует

$$\frac{n^p - n}{p} + n$$

различных бус из p бусинок, каждая из которых одного из n цветов.

Ответ. $\left(\frac{n^p - n}{p} + n \right)$ бус.

На первый взгляд непонятно, зачем мы обсудили тут эту задачу. Но давайте присмотримся к ответу! Мы доказали, что всего существует $\left(\frac{n^p - n}{p} + n\right)$ различных бус. Но количество бус – это целое число. Следовательно, и $\frac{n^p - n}{p}$ – это целое число. А это означает, что число $(n^p - n)$ делится на p . И мы с вами только что доказали малую теорему Ферма!

Неожиданно, не правда ли? Мы просто решили не самую сложную комбинаторную задачу и случайно доказали важную теорему теории чисел.

Но не зря же мы с вами пять глав обсуждали теорию чисел! Поэтому в следующем разделе мы получим другое, более теоретико-числовое доказательство.

МАЛАЯ ТЕОРЕМА ФЕРМА

Начнём издалека. Давайте обсудим такой вопрос. Мы с вами доказали, что сравнения по модулю можно складывать, вычитать и умножать. А можно ли делить? На этот вопрос часто неверно отвечают те, кто только начал заниматься теорией чисел. Давайте решим такую задачу.



Задача 118. Пусть для некоторых целых чисел a , b , c и натурального числа m известно, что

$$ac \equiv bc \pmod{m}.$$

Верно ли тогда, что $a \equiv b \pmod{m}$.

Решение. Итак, мы знаем, что разность $(ac - bc)$ делится на m , то есть что $c(a - b)$ делится на m , и хотим понять, правда ли тогда, что и разность $(a - b)$ делится на m .

Но если бы это было так, то это бы означало, что множитель c никак не помогает делиться на m . Однако понятно, что так будет не всегда, потому что для этого нужно, чтобы у чисел c и m не было общего делителя, отличного от единицы.

Теперь уже не сложно привести пример, когда утверждение задачи неверно. Например, мы знаем, что

$$6 \equiv 2 \pmod{4}.$$

Но при этом

$$3 \not\equiv 1 \pmod{4}.$$

Значит, просто так сокращать нельзя!

Ответ. Утверждение неверно.

Так что в общем случае нельзя сравнение по модулю сокращать на какое-то число. Но, пока мы решали эту задачу, мы поняли, когда сокращать можно!

Если числа c и m взаимно просты, то разность $(a - b)$ делится на m тогда и только тогда, когда и $c(a - b)$ делится на m . Дело в том, что если в разложении на простые множители числа c нет таких же множителей, как в разложении m , то делимость числа $c(a - b)$ на m зависит только от делимости $(a - b)$ на m . Таким образом, мы только что доказали следующее важное утверждение.

Утверждение. Пусть для некоторых целых чисел a, b, c и натурального числа m известно, что

$$ac \equiv bc \pmod{m}, \quad \text{НОД}(c, m) = 1.$$

Тогда $a \equiv b \pmod{m}$.

Благодаря этому утверждению мы сейчас докажем малую теорему Ферма.

Малая теорема Ферма. Пусть p – простое число, тогда для любого натурального n

$$n^p \equiv n \pmod{p}.$$

Доказательство. Если n делится на p , то утверждение очевидно. Действительно, в этом случае

$$n \equiv 0 \pmod{p}, \quad n^p \equiv 0^p = 0 \pmod{p}.$$

Пусть теперь число n не делится на p . Рассмотрим числа $n, 2n, 3n, \dots, (p-1)n$ и для каждого из них найдём его остаток при делении на p : $r_1, r_2, r_3, \dots, r_{p-1}$. Тогда

$$n \equiv r_1 \pmod{p};$$

$$2n \equiv r_2 \pmod{p};$$

$$3n \equiv r_3 \pmod{p};$$

...

$$(p-1)n \equiv r_{p-1} \pmod{p}.$$

Что мы знаем про числа $r_1, r_2, r_3, \dots, r_{p-1}$? Во-первых, ни одно из них не равно нулю, потому что число n не делится на p , и ни один из множителей $2, 3, \dots, (p-1)$ не делится на p , так как все они меньше, чем p .

Во-вторых, давайте покажем, что среди этих остатков нет одинаковых. Действительно, если предположить, что в каких-то двух строчках одинаковый остаток:

$$\ell n \equiv r \pmod{p},$$

$$kn \equiv r \pmod{p},$$

то мы получим, что

$$\ell n \equiv kn \pmod{p}.$$

Но число n не делится на простое p , а значит, они взаимно просты. Тогда, воспользовавшись предыдущим утверждением, мы получаем, что на n можно сократить:

$$\ell \equiv k \pmod{p}.$$

И при этом ℓ и k — это числа от 1 до $(p - 1)$. Их разность не может делиться на p , потому что она меньше, чем p .

Итак, мы знаем, что все остатки $r_1, r_2, r_3, \dots, r_{p-1}$ принимают значения от 1 до $(p - 1)$ и среди них нет одинаковых. А так как их ровно $(p - 1)$, то среди них присутствуют все числа от 1 до $(p - 1)$ в некотором порядке! Из этого следует, что

$$r_1 \cdot r_2 \cdot r_3 \cdot \dots \cdot r_{p-1} = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p - 1) = (p - 1)!.$$

Тогда перемножив все $(p - 1)$ сравнений, мы получим, что

$$n \cdot 2n \cdot 3n \cdot \dots \cdot (p - 1)n \equiv r_1 \cdot r_2 \cdot r_3 \cdot \dots \cdot r_{p-1} \pmod{p},$$

а значит,

$$(p - 1)! \cdot n^{p-1} \equiv (p - 1)! \pmod{p}.$$

Осталось заметить, что числа $(p-1)!$ и p взаимно просты, потому что число p – простое, а $(p-1)!$ равно произведению нескольких чисел, меньших, чем p . Поэтому можно сократить на $(p-1)!$:

$$n^{p-1} \equiv 1 \pmod{p}.$$

Домножив это сравнение на n , получаем утверждение теоремы.

Отметим здесь, что часто именно так и формулируют малую теорему Ферма.

Малая теорема Ферма (альтернативная формулировка). Пусть p – простое число, тогда для любого натурального n , не кратного p ,

$$n^{p-1} \equiv 1 \pmod{p}.$$

Задача 119. Докажите, что если p – простое число, то

$$(a+b)^p - a^p - b^p$$

делится на p при любых натуральных a и b .

Решение. Воспользуемся малой теоремой Ферма. Мы знаем, что

$$a^p \equiv a \pmod{p};$$

$$b^p \equiv b \pmod{p};$$

$$(a+b)^p \equiv a+b \pmod{p}.$$

Но тогда

$$(a+b)^p - a^p - b^p \equiv (a+b) - a - b = 0 \pmod{p}.$$

То есть число

$$(a + b)^p - a^p - b^p$$

делится на p .

Задача 120. Пусть p – простое число и натуральное число n не кратно p . И пусть k – наименьшее натуральное число, при котором

$$n^k \equiv 1 \pmod{p}.$$

Докажите, что $(p - 1)$ делится на k .

Решение. Благодаря малой теореме Ферма мы знаем, что

$$n^{p-1} \equiv 1 \pmod{p}.$$

Поэтому $p - 1 \geq k$.

Предположим, что $(p - 1)$ не делится на k и остаток при делении $(p - 1)$ на k равен r :

$$p - 1 = \ell k + r, \quad 0 < r < k.$$

Тогда из сравнения

$$n^k \equiv 1 \pmod{p}$$

следует, что

$$n^{p-1} = n^{\ell k + r} = (n^k)^\ell \cdot n^r \equiv 1^\ell \cdot n^r = n^r \pmod{p}.$$

Но

$$n^{p-1} \equiv 1 \pmod{p}.$$

Значит,

$$n^r \equiv n^{p-1} \equiv 1 \pmod{p}.$$

И при этом $r < k$.

Но по условию k – наименьшее натуральное число, при котором

$$n^k \equiv 1 \pmod{p}.$$

Пришли к противоречию! Значит, наше предположение о том, что $(p-1)$ не делится на k , было неверно.

Благодаря малой теореме Ферма мы можем ещё быстрее искать остатки и доказывать делимость. Убедимся в этом на примере следующих задач.

Задача 121. Докажите, что число

$$1^{50} + 2^{50} + 3^{50} + 4^{50} + 5^{50} + 6^{50}$$

делится на 13.

Решение. Можно было бы, конечно, решить так же, как мы делали это в предыдущей главе, исследуя отдельно каждое слагаемое. Но малая теорема Ферма позволяет сразу сказать, что для любого натурального n , не кратного 13,

$$n^{12} \equiv 1 \pmod{13}.$$

Поэтому

$$n^{50} = (n^{12})^4 \cdot n^2 \equiv n^2 \pmod{13}.$$

Таким образом,

$$\begin{aligned} 1^{50} + 2^{50} + 3^{50} + 4^{50} + 5^{50} + 6^{50} &\overset{13}{\equiv} 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 = \\ &= 1 + 4 + 9 + 16 + 25 + 36 = 91 \equiv 0 \pmod{13}. \end{aligned}$$

Это означает, что $(1^{50} + 2^{50} + 3^{50} + 4^{50} + 5^{50} + 6^{50})$ делится на 13.

Задача 122. Докажите, что число $(1001^{144} - 1)$ делится на 323.

Решение. Заметим, что $323 = 17 \cdot 19$. Поэтому, если мы докажем, что наше число делится и на 17, и на 19, то мы докажем, что оно делится на 323.

Так как число $1001 = 7 \cdot 11 \cdot 13$, то оно не делится ни на 17, ни на 19. Поэтому из малой теоремы Ферма следует, что

$$1001^{16} \equiv 1 \pmod{17};$$

$$1001^{18} \equiv 1 \pmod{19}.$$

Но тогда

$$1001^{144} = (1001^{16})^9 \equiv 1^9 = 1 \pmod{17};$$

$$1001^{144} = (1001^{18})^8 \equiv 1^8 = 1 \pmod{19}.$$

Откуда следует, что разность $(1001^{144} - 1)$ делится и на 17, и на 19, а значит, она делится на 323.

ТЕОРЕМА ЭЙЛЕРА

Малая теорема Ферма очень облегчает решение задач, но только, когда нас интересуют остатки при делении на простые числа. Тогда мы можем сказать, что для любого натурального n , не кратного простому p , остаток при делении n^{p-1} на p равен единице.



А что делать в общем случае? На этот вопрос отвечает *теорема Эйлера*. Но прежде чем её сформулировать, дадим следующее важное определение.

Функцией Эйлера $\varphi(m)$ натурального числа m называется количество натуральных чисел, меньших m и взаимно простых с m .

Например, $\varphi(6) = 2$, потому что среди натуральных чисел, меньших шести – 1, 2, 3, 4 и 5, только числа 1 и 5 взаимно просты с 6. А для любого простого p функция Эйлера $\varphi(p) = p - 1$, потому что все натуральные числа, меньшие p , взаимно просты с p .

Задача 123. Пусть p и q – различные простые числа. Докажите, что $\varphi(pq) = (p - 1)(q - 1)$.

Теперь мы готовы сформулировать и доказать теорему Эйлера.

Теорема Эйлера. Пусть n и m – взаимно простые натуральные числа, тогда

$$n^{\varphi(m)} \equiv 1 \pmod{m}.$$

Доказательство. Пусть $\alpha_1, \alpha_2, \dots, \alpha_{\varphi(m)}$ – все натуральные числа, меньшие m и взаимно простые с m . Рассмотрим числа $\alpha_1 n, \alpha_2 n, \dots, \alpha_{\varphi(m)} n$ и для каждого из них найдём его остаток при делении на m : $r_1, r_2, \dots, r_{\varphi(m)}$. Тогда

$$\alpha_1 n \equiv r_1 \pmod{m};$$

$$\alpha_2 n \equiv r_2 \pmod{m};$$

...

$$\alpha_{\varphi(m)} n \equiv r_{\varphi(m)} \pmod{m}.$$

Давайте покажем, что среди этих остатков нет одинаковых. Действительно, если предположить,

что в каких-то двух строчках одинаковый остаток:

$$\alpha_\ell n \equiv r \pmod{m},$$

$$\alpha_k n \equiv r \pmod{m},$$

то мы получим, что

$$\alpha_\ell n \equiv \alpha_k n \pmod{m}.$$

Но числа n и m взаимно просты. Тогда мы можем это сравнение сократить на n :

$$\alpha_\ell \equiv \alpha_k \pmod{m}.$$

И при этом α_ℓ и α_k – это числа от 1 до $(m - 1)$. Их разность не может делиться на m , потому что она меньше, чем m .

Покажем теперь, что все остатки взаимно просты с m . Предположим, что это не так и в какой-то строчке

$$\alpha n \equiv r \pmod{m}$$

стоит такой остаток r , что m и r имеют общий делитель $d > 1$.

Но если разность $(\alpha n - r)$ делится на m , то она делится и на его делитель d . И при этом r делится на d . Значит, и число αn делится на d . Иными словами, мы получили, что у чисел m и αn есть общий делитель $d > 1$. Но и число α , и число n взаимно просты с m . Пришли к противоречию!

Итак, мы знаем, что все остатки $r_1, r_2, \dots, r_{\varphi(m)}$ взаимно просты с m и среди них нет одинаковых. Но мы знаем, что существует лишь $\varphi(m)$ натуральных чисел, меньших m и взаимно простых с m , – это $\alpha_1, \alpha_2, \dots, \alpha_{\varphi(m)}$. А это означает, что среди чисел $r_1, r_2,$

$\dots, r_{\varphi(m)}$ встречается каждое из $\alpha_1, \alpha_2, \dots, \alpha_{\varphi(m)}$ и при этом ровно один раз. Поэтому

$$r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} = \alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_{\varphi(m)}.$$

Тогда, перемножив все $\varphi(m)$ сравнений, мы получим, что

$$\alpha_1 n \cdot \alpha_2 n \cdot \dots \cdot \alpha_{\varphi(m)} n \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \pmod{m},$$

а значит,

$$\alpha_1 \alpha_2 \dots \alpha_{\varphi(m)} \cdot n^{\varphi(m)} \equiv \alpha_1 \alpha_2 \dots \alpha_{\varphi(m)} \pmod{m}.$$

Осталось заметить, что числа $\alpha_1 \alpha_2 \dots \alpha_{\varphi(m)}$ и m взаимно просты, потому что каждый множитель взаимно прост с m . Поэтому последнее сравнение можно сократить на $\alpha_1 \alpha_2 \dots \alpha_{\varphi(m)}$:

$$n^{\varphi(m)} \equiv 1 \pmod{m}.$$

И мы доказали теорему Эйлера!

Задача 124. Пусть число $m = pq$, где p и q – различные простые числа. Тогда для любых натуральных n и k справедливо, что

$$n^{k\varphi(m)+1} \equiv n \pmod{m}.$$

Решение. Заметим, что если числа n и m взаимно простые, то утверждение задачи напрямую следует из теоремы Эйлера:

$$n^{k\varphi(m)+1} = n \cdot \left(n^{\varphi(m)}\right)^k \equiv n \cdot 1^k = n \pmod{m}.$$

Поэтому интересен лишь случай, когда числа n и m имеют общий делитель. То есть $n = \ell p^\alpha q^\beta$, где натуральное число ℓ не делится ни на p , ни на q (то есть взаимно просто с m), а показатели α и β – целые неотрицательные, и хотя бы один из них не равен нулю.

Давайте докажем, например, что

$$p^{k\varphi(m)+1} \equiv p \pmod{m}.$$

Действительно, мы уже знаем (см. задачу 123 на стр. 210), что в данном случае $\varphi(m) = (p-1)(q-1)$. Поэтому

$$p^{k\varphi(m)+1} = p \cdot \left(p^{q-1}\right)^{k(p-1)}.$$

Но из теоремы Ферма следует, что

$$p^{q-1} \equiv 1 \pmod{q}.$$

А значит,

$$p^{k\varphi(m)+1} = p \cdot \left(p^{q-1}\right)^{k(p-1)} \equiv p \cdot 1^{k(p-1)} = p \pmod{q}.$$

Поэтому разность

$$p^{k\varphi(m)+1} - p$$

делится на q . Но она, очевидно, делится и на p . Поэтому она делится на $m = pq$. А это и означает, что

$$p^{k\varphi(m)+1} \equiv p \pmod{m}.$$

Отсюда сразу получаем, что для любого α верно, что

$$(p^\alpha)^{k\varphi(m)+1} = \left(p^{k\varphi(m)+1}\right)^\alpha \equiv p^\alpha \pmod{m}.$$

Аналогично получаем, что

$$\left(q^{\beta}\right)^{k\varphi(m)+1} = \left(q^{k\varphi(m)+1}\right)^{\beta} \equiv q^{\beta} \pmod{m}.$$

А учитывая то, что числа ℓ и m взаимно простые,

$$\ell^{k\varphi(m)+1} \equiv \ell \pmod{m}.$$

Объединяя всё это, получаем требуемое утверждение:

$$\begin{aligned} n^{k\varphi(m)+1} &= \left(\ell p^{\alpha} q^{\beta}\right)^{k\varphi(m)+1} = \\ &= \ell^{k\varphi(m)+1} \cdot (p^{\alpha})^{k\varphi(m)+1} \cdot (q^{\beta})^{k\varphi(m)+1} \equiv \\ &\equiv \ell \cdot p^{\alpha} \cdot q^{\beta} = n \pmod{m}. \end{aligned}$$

ТЕОРИЯ ЧИСЕЛ В КРИПТОГРАФИИ

Часто школьники, и не только, спрашивают: «А зачем всё это нужно? Есть ли всему этому хоть какое-то применение, или это та самая чистая математика, у которой нет никакого приложения?» Так вот, в этом разделе мы поговорим об одном важном применении теории чисел.



На самом деле, вы используете теорию чисел каждый день! Ну, не совсем вы. Ваши гаджеты её используют и делают это постоянно. И без теории чисел не было бы того мира, в котором мы сейчас живём.

Но начнём издалека. Люди, с того момента как появилась письменность, хотели научиться шифровать информацию, которую они передают друг другу. Хотели научиться делать так, чтобы только получатель мог понять, что ему написали, потому что по дороге гонца могли убить, а голубя перехватить. И людям хотелось, чтобы информация, которую гонец или голубь должны были передать, не была понятна противнику. Так появились первые шифры.

Самый простой и наиболее известный из них – *шифр Цезаря*. И хотя он назван в честь Юлия Цезаря, который использовал его, чтобы защитить свои военные сообщения, этот способ шифрования очень прост и был придуман задолго до рождения Цезаря.

Шифр Цезаря заключается в следующем. Рассмотрим какой-нибудь алфавит (например русский) и запишем все буквы по кругу: А, Б, В, Г, Д и так далее. И повернём этот круг, например, на одну букву. Так что А перейдёт в Б, Б перейдёт в В и так далее, а Я перейдёт в А. И вместо каждой из букв, пишем те, в которые они перешли:

ЦЕЗАРЬ → ЧЁИБСЭ

А для того чтобы расшифровать, нужно просто повернуть круг с буквами в другую сторону.

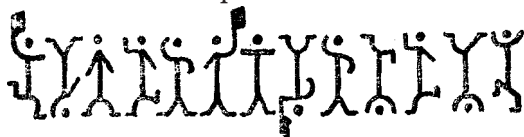
Конечно, можно поворачивать не на одну букву, а на 2, на 3, на 5, на 10, на сколько хотите¹. Главное, чтобы получатель тоже знал, на сколько вы поворачиваете. Вот так получается довольно много разных шифров.

¹Если верить биографам Юлия Цезаря, то сам он использовал сдвиг на три буквы.

Но у шифра Цезаря кроме его очевидного преимущества – простоты (им очень просто и зашифровать, и расшифровать текст), есть большой недостаток. Если тот, кто перехватил вашу информацию, знает, что текст был зашифрован с помощью шифра Цезаря, то ему достаточно (даже если он не знает то, на сколько вы сдвигали алфавит) просто перебирать все варианты сдвига, пока шифровка не превратится в осмысленный текст.

Следующим этапом был *шифр подстановки*, в котором замена происходит не по кругу, а мы просто заменяем каждую букву на какую-то другую. И даже не обязательно на букву, а какой-то символ. То есть каждой букве сопоставляем какой-то символ.

Такой шифр обсуждался, например, в романе Конан Дойля «Пляшущие человечки». Там каждая буква заменялась на изображение человечка:



Тут уже кажется, что разгадать шифр гораздо сложнее. Потому что в отличие от шифров Цезаря, которые не так сложно перебрать – их всего около 30 штук (в зависимости от того, сколько букв в используемом алфавите), тут вариантов гораздо больше.

Если считать, что в алфавите 30 букв, и попытаться перебрать все возможные способы сопоставить символу букву, то получится, что нужно перебрать 30! вариантов. А это очень много!

С такими шифрами простым перебором уже не справиться. И довольно долго это был один из са-

мых эффективных способов шифровки, потому что даже современный компьютер не сможет быстро перебрать все $30!$ вариантов.

Но оказалось, что и эти шифры расшифровать тоже не очень сложно. На помощь пришёл статистический анализ текста. Оказывается, что если взять несколько довольно больших отрывков текста, то частота вхождения каждой конкретной буквы будет более-менее одинаковой для всех этих отрывков. То есть, проанализировав несколько больших текстов, мы для каждой буквы, например, русского алфавита сможем узнать её среднюю частоту вхождения в любой текст.

Это означает, что если кто-то зашифровал некоторый текст, то, рассчитав частоту вхождения каждого символа в этот текст и сравнив эти частоты с известными средними частотами вхождения букв в тексты, мы сможем довольно быстро понять, какому символу соответствует какая буква.

Поэтому вот такая простая замена хотя и гораздо более сложна для расшифровки, но не подходит для передачи действительно важных посланий.

Что же делать дальше? Можно, например, шифровать следующим образом – брать не по одной букве, а скажем, по две. Брать два соседних символа и зашифровывать эту пару каким-то значком. В этом случае зашифровывать и расшифровывать вручную уже невозможно, потому что пар букв примерно $30^2 = 900$ – около тысячи разных сочетаний. Нужно иметь большую таблицу соответствий пар букв значкам.

И при этом всё равно, если зашифрованный текст довольно большой, то тот же статистический

анализ, пусть и хуже, но всё ещё работает.

И вот тут на помощь пришла теория чисел. Это случилось не так давно – лет пятьдесят назад. И при этом 50 лет назад для разработки того способа шифрования, который используется и сейчас, были применены методы математики, разработанные за 200 лет до этого!

Метод, про который я хочу вам рассказать, называется *алгоритмом RSA*. Он назван по первым буквам фамилий авторов этого метода – Rivest, Shamir и Adleman. И если знать всё то, что вы изучили, пока читали эту книгу, то он не покажется вам очень сложным.

Так в чём же он заключается? Пусть $n = pq$, где p и q – различные простые числа. Тогда мы знаем (см. задачу 123 на стр. 210), что количество натуральных чисел, меньших n и взаимно простых с n , равно

$$\varphi(n) = (p - 1)(q - 1).$$

Обозначим эту величину через N .

Давайте выберем какие-нибудь не очень маленькие натуральные числа α и β , такие, что их произведение $\alpha\beta$ даёт остаток 1 при делении на N . Существование такой пары вытекает из следствия из соотношения Безу (см. стр. 52).

Действительно, в качестве α можно взять любое число, взаимно простое с N (например, любое простое, не являющееся делителем числа N). Тогда следствие из соотношения Безу утверждает, что найдутся такие целые числа ℓ и m , что

$$\ell\alpha + mN = 1.$$

Тогда, если взять в качестве β остаток при делении ℓ на N , мы получим, что

$$\alpha\beta \stackrel{N}{\equiv} \ell\alpha = 1 - mN \equiv 1 \pmod{N}.$$

То есть $\alpha\beta = kN + 1$, где k – натуральное число.

И вот сейчас начинается процесс шифрования. Пусть есть некоторый текст. Но что такое текст для компьютера? Это всего лишь последовательность из нулей и единиц. То есть это просто некоторое очень большое число. Обозначим его через I и наложим единственное условие, что это натуральное число, меньшее n . И мы хотим это число передать от одного человека к другому.

Что же мы делаем? Мы этому человеку, который хочет передать информацию, сообщаем два числа – число n и число α . И он должен свою информацию I возвести в степени α и найти остаток при делении получившегося числа на n :

$$I^\alpha \equiv J \pmod{n}.$$

Получилось число J . Это и есть наша зашифрованная информация.

И он сообщает, кому нужно, это число J . При этом и число n , и число α не секретны, их можно передавать открытым способом. Можно просто по телефону, например, сообщить. И получившееся число J не секретно. Если его кто-то перехватит, он не сможет, зная числа n , α и J , восстановить число I , при условии, что число n довольно большое (чуть позже мы поймём, почему это так).

А дальше происходит следующее. Получатель берет число J , возводит его в степень β и находит остаток при делении получившегося числа на n .

При этом число β знает только он (чуть позже мы обсудим, почему его сложно подобрать). И смотрите, что получается:

$$J^\beta \stackrel{n}{\equiv} I^{\alpha\beta} = I^{kN+1} = I^{k\varphi(n)+1}.$$

А мы с вами знаем (см. задачу 124 на стр. 212), что если $n = pq$, то

$$I^{k\varphi(n)+1} \equiv I \pmod{n}.$$

Таким образом,

$$J^\beta \equiv I \pmod{n}.$$

То есть он получил исходное число I .

В итоге мы доказали следующее. Пусть $I < n$, и пусть J – это остаток при делении числа I^α на n . Тогда остаток при делении числа J^β на n равен I .

А что делать, если необходимо передать число, которое больше n ? Его просто «режут на куски», каждый из которых меньше n , и шифруют каждый «кусочек» по отдельности. В каком-то смысле это и есть тот самый обобщенный шифр подстановки, в котором мы шифруем не по одной букве и даже не по две, а сразу блоком из сотен букв.

Дело в том, что сейчас при использовании алгоритма RSA берут простые числа p и q настолько большими, чтобы их произведение n было порядка 10^{600} , а в особо важных случаях – даже 10^{1000} . То есть это чрезвычайно громадное число! Говоря компьютерным языком, мы режем всю нашу информацию на кусочки по 2048 или даже по 4096 бит и по этому алгоритму заменяем каждый кусочек на другой кусочек такой же длины. Если считать, что нам достаточно 8 бит, чтобы записать любой символ, то каждый такой кусочек содержит от 250 до 500 букв!

Давайте поймём, почему такой шифр очень надёжен. Как мы помним, числа n и α не секретны, а число β знает только получатель. Пусть удалось перехватить число J , тогда для восстановления исходного числа I нам нужно по числам n и α восстановить число β . Но β – это такое число, что произведение $\alpha\beta$ даёт остаток 1 при делении на $N = \varphi(n)$. А чтобы узнать $\varphi(n)$, нам нужно разложить на произведение двух простых известное число n .

И вот в этом месте и есть основная сложность. Оказывается, что сейчас нет алгоритмов, которые за короткое время способны разложить 600-значное число на простые множители. Причём, когда я говорю про «короткое время», я имею в виду годы вычислений на суперкомпьютере.

В итоге получается, что если вы не умеете раскладывать большие числа на простые множители, то, даже имея информацию о том, чему равны n и α , вы никак не узнаете, чему равно β , и не сможете расшифровать информацию!

На этом этом принципе работают, например, секретные чаты в мессенджерах. Ваше устройство берёт любые два больших простых числа (у него есть специальный громадный массив таких чисел, из которых можно выбирать), перемножает их и получает n , затем вычисляет N и по нему подбирает α и β . Затем пересылает числа n и α в мессенджер вашего друга, который с их помощью шифрует каждое отправляемое другом сообщение. И то же самое делает мессенджер вашего друга – берёт какие-то свои два больших простых числа, вычисляет свои n' , α' и β' и отправляет числа n' и α' в ваш мессенджер. В итоге каждое сообщение шифруется, но прочитать его может только тот

мессенджер, который знает своё β .

Более того, если это суперсекретный чат, то ваши мессенджеры могут для каждого следующего сообщения подбирать новую пару больших простых чисел. Поэтому, даже если вы перехватите какое-то сообщение и будете знать, с помощью каких n и α оно зашифровано, у вас могут уйти годы на то, чтобы расшифровать одно это сообщение, в котором может быть написано лишь: «Привет, Вася! Как дела?»

Основное преимущество этого шифра в том, что, даже имея ключ, который шифрует информацию, всё равно невозможно понять, как расшифровать обратно. Этим современная криптография отличается от всего того, что было раньше.

Фактически у вас имеется специальная шкатулка, ключ от которой есть только у вас. Вы пересылаете её в открытом виде обычной почтой своему другу. Он кладёт в неё секретное письмо, захлопывает и отправляет обратно вам. И всё! Открыть сможете только вы.

И всё это основано на теории чисел! Здорово, правда? А этот способ шифрования используется много где: от защиты программного обеспечения и цифровых подписей до банков. Поэтому пока одни ищут всё новые и новые большие простые числа, другие мечтают найти быстрый алгоритм разложения любого числа на простые множители, который позволил бы им взломать любой шифр¹.

¹Стоит отметить, что знакомые IT-шники, прочитав этот раздел, сказали, что в реальных задачах использовать RSA довольно сложно. Обычно его используют лишь для передачи ключей какого-нибудь алгоритма симметричного шифрования, а потом все данные шифруют уже этим алгоритмом.

НЕБОЛЬШОЙ ЗАДАЧНИК

Вот мы и подошли к концу! К этому моменту мы обсудили большое количество фактов и методов из теории чисел и отрешали более сотни задач. Теперь у вас есть возможность проверить, насколько хорошо у вас получается самостоятельно решать такие задачи.

В этом разделе собраны дополнительные задачи для самостоятельного решения. Я постарался отсортировать их для вас от простых к сложным, но не всегда то, что кажется простым мне, окажется просто и для вас. Поэтому не расстраивайтесь, если какие-то задачи у вас не получится быстро решить.

Задача 125. Можно ли все клетки:

- а) таблицы 2×3 ,
- б) таблицы 3×4 ,

заполнить натуральными числами так, чтобы в каждом столбце и в каждой строке суммы чисел оказались различными простыми числами?

Задача 126. Какое наибольшее количество двузначных составных чисел можно выбрать так, что любые два из них взаимно просты?

Задача 127. Найдите наибольшее натуральное n , для которого верно следующее утверждение: для любого простого числа p , такого, что $2 < p < n$, разность $(n - p)$ также является простым числом.

Задача 128. Сколько существует натуральных чисел, делящихся на 1001 и имеющих ровно 1001 различный делитель?

Задача 129. Найдите наименьшее натуральное число, которое при делении на 2 даёт остаток 1, при делении на 3 даёт остаток 2, при делении на 4 даёт остаток 3, ..., при делении на 10 даёт остаток 9.

Задача 130. Можно ли число 2024 представить в виде суммы четырёх квадратов нечётных чисел?

Задача 131. Является ли число $(3^{200} + 4^{99} + 6^{100})$ простым?

Задача 132. Простые числа p, q, r таковы, что

$$p + q + r = 50, \quad pq + qr + rp = 647.$$

Найдите произведение pqr .

Задача 133. Найдите все пары таких натуральных чисел m и n , что $mn = 1\,000\,000$ и при этом $(m^2 + n^2)$ делится на $1\,000\,000$.

Задача 134. Отметим все натуральные числа, у которых суммы цифр являются простыми числами. Какое наибольшее количество отмеченных может быть среди пяти подряд идущих натуральных чисел?

Задача 135. Докажите, что для любого простого p , большего пяти, найдётся число $111\dots 11$, состоящее из одних единиц, которое делится на p .

Задача 136. Найдите все такие натуральные числа n , что числа $(4n + 9)$ и $(9n + 4)$ являются квадратами натуральных чисел.

Задача 137. Пусть натуральное число n не делится на простое p . Докажите, что тогда существует такое натуральное число m , что mn даёт остаток 1 при делении на p .

Задача 138. Пусть $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$, то есть p_k — это k -е простое число. Может ли при каком-нибудь $n > 1$ среднее арифметическое

$$\frac{p_1 + p_2 + \dots + p_n}{n}$$

оказаться простым числом?

Задача 139. Докажите, что при любых натуральных n и k число

$$n^{2k+1} + (n-1)^{k+2}$$

делится на $n^2 - n + 1$.

Задача 140. Какое наибольшее количество чисел можно выбрать из набора $\{1; 2; 3; \dots; 1001\}$, чтобы разность любых двух выбранных чисел не являлась простым числом?

Задача 141. Докажите, что для любого натурального $n > 1$ между числами n и $n!$ есть по крайней мере одно простое число.

Задача 142. Мы знаем¹, что существует миллион последовательных натуральных чисел, среди которых нет ни одного простого числа. А существует ли миллион последовательных натуральных чисел, среди которых ровно десять простых чисел?

¹См. задачу 26 на стр. 76.

Задача 143. Найдите все пары простых чисел p и q , для которых верно следующее свойство: число $(5p + 1)$ делится на q , а число $(5q + 1)$ делится на p .

Задача 144. Найдите все пары натуральных чисел, для которых справедливо равенство:

$$m^2 = n! + 5n + 13.$$

Задача 145. Для натурального числа n выписали все его делители в порядке возрастания:

$$1 = k_1 < k_2 < \dots < k_m = n.$$

Найдите все возможные значения количества делителей числа n^3 , если известно, что $k_2 \cdot k_3 \cdot k_8 \cdot k_9 > n^2$.

Задача 146. Найдите наименьшее натуральное n , для которого выполнено следующее условие: если p – простое число и число n делится на $(p - 1)$, то оно делится и на p .

Задача 147. Простые числа a_1, a_2, \dots, a_{11} образуют арифметическую прогрессию, все члены которой больше 11. Докажите, что разность прогрессии делится на 2310.

Задача 148. Докажите, что существует бесконечно много простых чисел, дающих остаток 3 при делении на 4.

Задача 149. Найдите все тройки натуральных чисел, для которых справедливо равенство:

$$4 \cdot k! = m! - 2 \cdot n!.$$

Задача 150. Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ – многочлен степени $n \geq 1$ с целыми коэффициентами. Могут ли все значения $P(0), P(1), P(2), \dots$ оказаться простыми числами?

РЕШЕНИЯ ЗАДАЧ

1. Признак делимости на 20. Если две последние цифры числа образуют число, кратное 20 (00, 20, 40, 60 или 80), то и само число делится на 20.

Доказательство. Пусть две последние цифры числа $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ образуют число $\overline{a_1 a_0} = 20k$, кратное 20, тогда

$$\begin{aligned} a &= 100 \cdot \overline{a_n a_{n-1} \dots a_2} + \overline{a_1 a_0} = \\ &= 20 \cdot (5 \cdot \overline{a_n a_{n-1} \dots a_2} + k) : 20. \end{aligned}$$

Признак делимости на 25. Если две последние цифры числа образуют число, кратное 25 (00, 25, 50 или 75), то и само число делится на 25.

Доказательство. Пусть две последние цифры числа $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ образуют число $\overline{a_1 a_0} = 25k$, кратное 25, тогда

$$\begin{aligned} a &= 100 \cdot \overline{a_n a_{n-1} \dots a_2} + \overline{a_1 a_0} = \\ &= 25 \cdot (4 \cdot \overline{a_n a_{n-1} \dots a_2} + k) : 25. \end{aligned}$$

Признак делимости на 50. Если число оканчивается на 00 или 50, то оно делится на 50.

Доказательство. Пусть число $a = \overline{a_n a_{n-1} \dots a_1 a_0}$.
Если $\overline{a_1 a_0} = 00$, то

$$\begin{aligned} a &= 100 \cdot \overline{a_n a_{n-1} \dots a_2} = \\ &= 50 \cdot (2 \cdot \overline{a_n a_{n-1} \dots a_2}) \div 50. \end{aligned}$$

Если же $\overline{a_1 a_0} = 50$, то

$$\begin{aligned} a &= 100 \cdot \overline{a_n a_{n-1} \dots a_2} + 50 = \\ &= 50 \cdot (2 \cdot \overline{a_n a_{n-1} \dots a_2} + 1) \div 50. \end{aligned}$$

2. Признак делимости на 16. Если четыре последние цифры числа образуют число, кратное 16, то и само число делится на 16.

Доказательство. Пусть четыре последние цифры числа

$$a = \overline{a_n a_{n-1} \dots a_1 a_0}$$

образуют число $\overline{a_3 a_2 a_1 a_0} = 16k$, кратное 16, тогда

$$\begin{aligned} a &= 10\,000 \cdot \overline{a_n a_{n-1} \dots a_4} + \overline{a_3 a_2 a_1 a_0} = \\ &= 16 \cdot (625 \cdot \overline{a_n a_{n-1} \dots a_4} + k) \div 16. \end{aligned}$$

3. Ответ. Нет.

Можно подобрать конкретное число, не делящееся на 27, сумма цифр которого делится на 27, но мы поступим иначе.

Заметим, что у каждого из чисел 9990 и 9981 сумма цифр равна 27, но их разность равна 9, поэтому оба числа не могут делиться на 27. А значит, существует число, не делящееся на 27, сумма цифр которого делится на 27.

7. **Ответ.** 6, 12, 18 и 24.

Числа при делении на 5 могут давать один из пяти остатков – 0, 1, 2, 3 или 4. Если у числа остаток равен r и неполное частное равно остатку, то это число

$$5 \cdot r + r = 6r.$$

Значит, нам подходящие числа имеют вид $6r$, где r принимает значения от 0 до 4 – это числа 0, 6, 12, 18 и 24. Но число 0 не является натуральным. Поэтому остаются только 6, 12, 18 и 24.

8. **Ответ.** 2024.

Пусть число n удовлетворяет условию. Тогда

$$n = 100k + 24, \quad n = 101\ell + 4,$$

где k и ℓ – некоторые натуральные числа.

Отсюда следует, что

$$100k + 24 = 101\ell + 4,$$

то есть

$$100 \cdot (k - \ell) + 20 = \ell.$$

Пусть $m = k - \ell$, тогда $\ell = 100m + 20$. А значит,

$$\begin{aligned} n &= 101\ell + 4 = 101 \cdot (100m + 20) + 4 = \\ &= 10\,100 \cdot m + 2024. \end{aligned}$$

Если $m \geq 1$, то число $n > 10\,000$ и не может быть четырёхзначным. Остаётся единственный возможный случай: $m = 0$.

При этом число 2024 действительно подходит:

$$2024 = 100 \cdot 20 + 24, \quad 2024 = 101 \cdot 20 + 4.$$

10. **Ответ.** Нет.

Сумма цифр этого числа равна

$$10 \cdot 0 + 10 \cdot 1 + 10 \cdot 2 = 30.$$

Так как сумма цифр делится на 3, то и само число делится на 3. Но сумма цифр не делится на 9, значит, и само число не делится на 9. Докажем, что так не бывает¹.

Предположим, что наше число равно n^2 . Тогда число n при делении на 3 может иметь один из трёх остатков – 0, 1 или 2.

Пусть $n = 3k$, где k – некоторое натуральное число. Тогда $n^2 = 9k^2$ делится на 9. Но мы знаем, что n^2 не делится на 9.

Пусть $n = 3k + 1$, где k – некоторое натуральное число. Тогда

$$n^2 = 9k^2 + 6k + 1 = 3 \cdot (3k^2 + 2k) + 1$$

не делится на 3. Но мы знаем, что n^2 делится на 3.

Пусть $n = 3k + 2$, где k – некоторое натуральное число. Тогда

$$n^2 = 9k^2 + 12k + 4 = 3 \cdot (3k^2 + 4k + 1) + 1$$

не делится на 3. Но мы знаем, что n^2 делится на 3.

В каждом из трёх случаев мы пришли к противоречию. Значит, наше предположение о том, что данное число является квадратом натурального числа, было ложным.

¹Если бы мы уже знали основную теорему арифметики, которую докажем лишь в третьей главе, то в этом месте можно было бы остановиться, сказав, что если квадрат числа делится на 3, то он обязан делиться и на 9.

11. Заметим, что рассматриваемое число как минимум четырёхзначное, поэтому, если оно и является степенью двойки, то эта степень довольно большая.

Так как любая степень двойки – это чётное число, то она должна оканчиваться на чётную цифру. Кроме того, никакая степень двойки не делится на 10, поэтому не может оканчиваться на 0. Осталось рассмотреть четыре случая – 2222, 4444, 6666 и 8888.

Степень двойки делится на 4, поэтому число, составленное из двух последних цифр, должно делиться на 4. Но 22 и 66 не делятся на 4.

Степень двойки делится на 8, поэтому число, составленное из трёх последних цифр, должно делиться на 8. Но 444 не делится на 8.

Степень двойки делится на 16, поэтому число, составленное из четырёх последних цифр, должно делиться на 16. Но $8888 = 8 \cdot 1111$ не делится на 16.

Значит, никакая степень двойки не может оканчиваться четырьмя одинаковыми цифрами¹.

14. Найдём наибольший общий делитель чисел $(27n + 4)$ и $(18n + 3)$:

$$\begin{aligned}(27n + 4, 18n + 3) &= ((27n + 4) - (18n + 3), 18n + 3) = \\ &= (9n + 1, 18n + 3) = \\ &= (9n + 1, (18n + 3) - 2 \cdot (9n + 1)) = \\ &= (9n + 1, 1) = 1.\end{aligned}$$

¹Отметим здесь, что существуют степени двойки, которые оканчиваются тремя одинаковыми цифрами. Как следует из нашего решения, они могут оканчиваться лишь на 888. Например, $2^{39} = 549\,755\,813\,888$.

Это означает, что при любом натуральном n числа $(27n + 4)$ и $(18n + 3)$ взаимно просты.

18. Обозначим данные числа a, b, c, d и e . Из условия следует, что числа

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

делятся на 3. Но тогда и их разность

$$(a + c + d + e) - (b + c + d + e) = a - b$$

делится на 3. Из этого следует, что у чисел a и b одинаковый остаток при делении на 3.

Рассуждая аналогично, получаем, что у всех пяти чисел должен быть одинаковый остаток при делении на 3.

Но если у всех чисел при делении на 3 будет остаток 1, то и у суммы любых четырёх из них будет остаток 1. А если у всех чисел при делении на 3 будет остаток 2, то и у суммы любых четырёх из них будет остаток 2.

Поэтому единственный случай, когда у всех чисел одинаковый остаток при делении на 3 и сумма любых четырёх из них делится на 3, – это когда у всех чисел остаток при делении на 3 равен нулю.

19. Заметим, что

$$\begin{aligned} 999\,999\,999\,999\,999\,999\,999\,999 &= \\ &= 9 \cdot 111\,111\,111\,111\,111\,111\,111\,111 = \\ &= 9 \cdot 111 \cdot 1\,001\,001\,001\,001\,001\,001\,001. \end{aligned}$$

При этом из признаков делимости на 3 и на 9 следует, что число 111 делится на 3, а число

$$1\,001\,001\,001\,001\,001\,001\,001$$

делится на 9.

Поэтому число

$$999\,999\,999\,999\,999\,999\,999\,999$$

делится на $9 \cdot 3 \cdot 9$.

20. Ответ. 1001.

Вычислим

$$\text{НОД}(5a + 3b, 13a + 8b),$$

используя алгоритм Евклида:

$$\begin{aligned} (5a + 3b, 13a + 8b) &= (5a + 3b, 13a + 8b - 2(5a + 3b)) = \\ &= (5a + 3b, 3a + 2b) = \\ &= ((5a + 3b) - (3a + 2b), 3a + 2b) = \\ &= (2a + b, 3a + 2b) = \\ &= (2a + b, (3a + 2b) - (2a + b)) = \\ &= (2a + b, a + b) = \\ &= ((2a + b) - (a + b), a + b) = \\ &= (a, a + b) = (a, (a + b) - a) = \\ &= (a, b) = 1001. \end{aligned}$$

21. Ответ. 9.

Из критерия делимости на 9 следует, что если число делится на 9, то и сумма его цифр делится на 9.

Сумма цифр тысячезначного числа a не превосходит $1000 \cdot 9 = 9000$. Поэтому в числе b не более четырёх цифр и оно делится на 9.

Сумма цифр числа b не превосходит $4 \cdot 9 = 36$. Поэтому в числе c не более двух цифр, количество десятков не превосходит 3 и оно делится на 9.

Сумма цифр числа c не превосходит $3 + 9 = 12$. Поэтому число d не превосходит 12 и оно делится на 9. Значит, $d = 9$.

24. Ответ. 2.

Посмотрим на первые несколько чисел Евклида:

$$2 + 1 = 3;$$

$$2 \cdot 3 + 1 = 7;$$

$$2 \cdot 3 \cdot 5 + 1 = 31;$$

$$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211;$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311.$$

Видно, что первые два числа заканчиваются не на 1, а все остальные – на 1.

Действительно, если из числа Евклида (начиная с третьего) вычесть единицу, то получится произведение, содержащее 2 и 5, то есть кратное десяти:

$$2 \cdot 3 \cdot 5 = 3 \cdot 10;$$

$$2 \cdot 3 \cdot 5 \cdot 7 = (3 \cdot 7) \cdot 10;$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = (3 \cdot 7 \cdot 11) \cdot 10;$$

...

А значит, само число Евклида заканчивается на 1.

34. Ответ. 2.

Заметим, что если простое число p нечётно, то число $(3p + 1)$ чётно и больше двух, поэтому

не может быть простым. Значит, число p чётно. Но единственное чётное простое число – это 2. Осталось проверить, что при $p = 2$ число

$$3p + 1 = 3 \cdot 2 + 1 = 7$$

тоже простое.

Таким образом, числа p и $(3p + 1)$ могут быть одновременно простыми, только если $p = 2$.

35. Ответ. 79.

Пусть p – наименьшее простое число, которое можно представить в виде суммы семи различных простых чисел. Среди простых чисел есть только одно чётное – это число 2.

Поэтому все семь слагаемых должны быть нечётными числами, потому что иначе число p равно сумме двойки и шести нечётных простых, то есть равно чётному числу, большему двух, то есть составному.

Сумма семи самых маленьких простых нечётных чисел равна

$$3 + 5 + 7 + 11 + 13 + 17 + 19 = 75.$$

Значит $p \geq 75$. Наименьшее простое число, которое не меньше 75, – это 79.

Попробуем подобрать семь простых слагаемых так, чтобы получилось число 79. Для этого достаточно в предыдущей сумме увеличить одно из слагаемых на 4. Осталось лишь заметить, что $19 + 4 = 23$ – простое число. Поэтому

$$3 + 5 + 7 + 11 + 13 + 17 + 23 = 79.$$

Таким образом, мы показали, что если простое число меньше 79 (а значит, меньше и 75, потому что между 75 и 79 нет простых чисел), то его нельзя представить в виде семи различных простых, и привели пример, как можно представить таким образом число 79.

Значит, 79 – наименьшее простое число, которое можно представить в виде суммы семи различных простых чисел.

36. Ответ. 5.

Так как искомое число p равно сумме двух простых чисел, то оно точно больше, чем 2. Значит, p – нечётное число.

Но число p должно быть равно сумме и разности двух простых чисел, значит, и в сумме, и в разности участвуют числа разной чётности, потому что и сумма, и разность чисел одинаковой чётности – чётное число, а искомое число p нечётно.

Но единственное чётное простое число – это 2. Поэтому

$$p = q + 2, \quad p = r - 2,$$

где q и r – простые числа. То есть тройка чисел

$$q = p - 2, \quad p, \quad r = p + 2$$

должна содержать только простые числа.

Из задачи 27 мы знаем, что есть только одна тройка чисел с таким свойством – (3; 5; 7). Значит, существует только одно простое число, которое можно представить и как сумму двух простых чисел, и как разность двух простых чисел – это число 5:

$$5 = 3 + 2, \quad 5 = 7 - 2.$$

37. Остатком при делении натурального числа на 30 могут быть только числа от 0 до 29. Выпишем их все и отметим те, которые не являются ни простым числом, ни единицей:

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29

Если натуральное число при делении на 30 даёт остаток 0, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26 или 28, то оно делится на 2 и больше, чем 2. Значит, оно составное.

Если натуральное число при делении на 30 даёт остаток 9, 15, 21 или 27, то оно делится на 3 и больше, чем 3. Значит, оно составное.

Если натуральное число при делении на 30 даёт остаток 25, то оно делится на 5 и больше, чем 5. Значит, оно составное.

Таким образом, ни один из отмеченных остатков не может получиться при делении на 30 у простых чисел. А это означает, что остаток при делении простого числа на 30 – это либо простое число, либо 1.

38. Так как $n > 4$, то среди простых чисел $(n - 1)$ и $(n + 1)$ нет 2 и 3. Значит, они оба нечётны и не делятся на 3. Но если они нечётны, то n делится на 2. Кроме того, из трёх последовательных чисел $(n - 1)$, n , $(n + 1)$ одно должно делиться на 3, и это ни $(n - 1)$, ни $(n + 1)$. Поэтому число n делится на 2 и на 3, а

значит¹, делится на 6.

41. Пусть для числа n верно, что $n : 5$ и $n : 7$. Тогда $7n : 35$ и $5n : 35$. Следовательно,

$$7n - 5n = 2n$$

делится на 35. Но тогда и число $2 \cdot 2n = 4n$ делится на 35.

Осталось заметить, что из делимости чисел $5n$ и $4n$ на 35 следует, что

$$5n - 4n = n$$

делится на 35.

42. Пусть известно, что $n : 7$ и $n : 11$. Тогда $11n : 77$ и $7n : 77$. Следовательно,

$$11n - 7n = 4n$$

делится на 77. Но тогда и число $2 \cdot 4n = 8n$ делится на 77. Осталось заметить, что из делимости чисел $8n$ и $7n$ на 77 следует, что

$$8n - 7n = n$$

¹На самом деле, до того как мы доказали основную теорему арифметики (см. главу 3), нужно обосновывать, как из делимости на 2 и 3 следует делимость на 6. Это можно сделать, например, так: если число делится на 2, то у него могут быть остатки 0, 2 или 4 при делении на 6; если число делится на 3, то у него могут быть остатки 0 или 3 при делении на 6. Значит, если число делится и на 2, и на 3, то у него может быть только остаток 0 при делении на 6, а значит, оно делится на 6.

Про другой способ обоснования мы говорим в задаче 39 на стр. 95.

делится на 77.

Итак, мы уже доказали, что $n : 77$. Если же дополнительно известно, что $n : 13$, тогда $13n : 1001$ и $77n : 1001$. Но тогда и $6 \cdot 13n = 78n$ делится на 1001. Осталось заметить, что из делимости чисел $78n$ и $77n$ на 1001 следует, что

$$78n - 77n = n$$

делится на 1001.

43. Ответ. 2, 6, 10, 14, 18, 22, ... – все чётные числа, которые не делятся на 4 в обычном смысле.

Если число из «мира чётных чисел» ни на что не делится, значит, его нельзя представить в виде произведения двух чётных чисел. Значит, оно не делится на 4 в обычном смысле.

С другой стороны, если число делится на 4 в обычном смысле, то его можно представить как произведение числа 2 и некоторого чётного числа. Значит, в «мире чётных чисел» у него есть хотя бы один делитель – 2.

Таким образом, числа из «мира чётных чисел», которые в этом мире не делятся ни на одно число, – это 2, 6, 10, 14, 18, 22, ... – все чётные числа, которые не делятся на 4 в обычном смысле.

44. Ответ. Например, 84, 100, 132, 140 и 196.

Давайте поймём, что есть особенного в числах 36 и 60. Если их разложить на обычные простые множители

$$36 = 2 \cdot 2 \cdot 3 \cdot 3, \quad 60 = 2 \cdot 2 \cdot 3 \cdot 5,$$

то можно увидеть, что кроме двух двоек (без которых число было бы «простым») в разложении есть два нечётных множителя.

Именно поэтому 36 можно представить и как $2 \cdot (2 \cdot 3 \cdot 3)$, и как $(2 \cdot 3) \cdot (2 \cdot 3)$. А число 60 можно представить и как $2 \cdot (2 \cdot 3 \cdot 5)$, и как $(2 \cdot 3) \cdot (2 \cdot 5)$.

Теперь несложно придумать ещё пять чисел с таким свойством¹. Например,

$$\begin{aligned}84 &= 2 \cdot 2 \cdot 3 \cdot 7; \\100 &= 2 \cdot 2 \cdot 5 \cdot 5; \\132 &= 2 \cdot 2 \cdot 3 \cdot 11; \\140 &= 2 \cdot 2 \cdot 5 \cdot 7; \\196 &= 2 \cdot 2 \cdot 7 \cdot 7.\end{aligned}$$

Действительно, у каждого из них два разложения на «простые» множители:

$$\begin{aligned}84 &= 2 \cdot 42 = 6 \cdot 14; \\100 &= 2 \cdot 50 = 10 \cdot 10; \\132 &= 2 \cdot 66 = 6 \cdot 22; \\140 &= 2 \cdot 70 = 10 \cdot 14; \\196 &= 2 \cdot 98 = 14 \cdot 14.\end{aligned}$$

¹На самом деле необязательно ограничиваться числами с таким свойством. Сделав это, мы пропустили, например, числа $72 = 2^3 \cdot 3^2$ и $108 = 2^2 \cdot 3^3$, для каждого из которых есть два разложения на «простые» множители:

$$72 = 2 \cdot 2 \cdot 18 = 2 \cdot 6 \cdot 6, \quad 108 = 2 \cdot 54 = 6 \cdot 18.$$

А пропущенное число $180 = 2^2 \cdot 3^2 \cdot 5$ можно разложить даже тремя способами:

$$180 = 2 \cdot 90 = 6 \cdot 30 = 10 \cdot 18.$$

45. **Ответ.** Например, 9240 или $2^2 \cdot 3^{20}$.

Первое решение. Рассмотрим, например, число

$$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11.$$

Его можно разложить на «простые» множители более чем десятью различными способами:

$$9240 = 2 \cdot 2 \cdot (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = 2 \cdot 2 \cdot 2310;$$

$$9240 = 2 \cdot (2 \cdot 3) \cdot (2 \cdot 5 \cdot 7 \cdot 11) = 2 \cdot 6 \cdot 770;$$

$$9240 = 2 \cdot (2 \cdot 5) \cdot (2 \cdot 3 \cdot 7 \cdot 11) = 2 \cdot 10 \cdot 462;$$

$$9240 = 2 \cdot (2 \cdot 7) \cdot (2 \cdot 3 \cdot 5 \cdot 11) = 2 \cdot 14 \cdot 330;$$

$$9240 = 2 \cdot (2 \cdot 11) \cdot (2 \cdot 3 \cdot 5 \cdot 7) = 2 \cdot 22 \cdot 210;$$

$$9240 = (2 \cdot 3) \cdot (2 \cdot 5) \cdot (2 \cdot 7 \cdot 11) = 6 \cdot 10 \cdot 154;$$

$$9240 = (2 \cdot 3) \cdot (2 \cdot 7) \cdot (2 \cdot 5 \cdot 11) = 6 \cdot 14 \cdot 110;$$

$$9240 = (2 \cdot 3) \cdot (2 \cdot 11) \cdot (2 \cdot 5 \cdot 7) = 6 \cdot 22 \cdot 70;$$

$$9240 = (2 \cdot 5) \cdot (2 \cdot 7) \cdot (2 \cdot 3 \cdot 11) = 10 \cdot 14 \cdot 66;$$

$$9240 = (2 \cdot 5) \cdot (2 \cdot 11) \cdot (2 \cdot 3 \cdot 7) = 10 \cdot 22 \cdot 42;$$

$$9240 = (2 \cdot 7) \cdot (2 \cdot 11) \cdot (2 \cdot 3 \cdot 5) = 14 \cdot 22 \cdot 30.$$

И это ещё далеко не все способы¹.

Второе решение. Если не пытаться придумать «не очень большое число» с таким свойством², то можно взять, например, число $2^2 \cdot 3^{20}$. Его тоже можно разложить на «простые» множители более чем десятью различными способами:

$$2^2 \cdot 3^{20} = 2 \cdot (2 \cdot 3^{20}) = (2 \cdot 3) \cdot (2 \cdot 3^{19}) =$$

¹Мы, например, совсем не использовали разложения такого типа:

$$9240 = 2 \cdot (2 \cdot 3 \cdot 5) \cdot (2 \cdot 7 \cdot 11) = 2 \cdot 30 \cdot 154.$$

²Можно попробовать рассмотреть вопрос о нахождении наименьшего числа с таким свойством, но подобный вопрос больше подойдёт для конкурса по программированию.

$$\begin{aligned} &= (2 \cdot 3^2) \cdot (2 \cdot 3^{18}) = (2 \cdot 3^3) \cdot (2 \cdot 3^{17}) = \\ &= (2 \cdot 3^4) \cdot (2 \cdot 3^{16}) = (2 \cdot 3^5) \cdot (2 \cdot 3^{15}) = \\ &= (2 \cdot 3^6) \cdot (2 \cdot 3^{14}) = (2 \cdot 3^7) \cdot (2 \cdot 3^{13}) = \\ &= (2 \cdot 3^8) \cdot (2 \cdot 3^{12}) = (2 \cdot 3^9) \cdot (2 \cdot 3^{11}) = \\ &= (2 \cdot 3^{10}) \cdot (2 \cdot 3^{10}). \end{aligned}$$

47. Ответ. 32.

Разложим оба числа на простые множители:

$$4000 = 2^5 \cdot 5^3, \quad 4608 = 2^9 \cdot 3^9.$$

Поэтому $\text{НОД}(4000, 4608) = 2^5 = 32$.

48. Ответ. 2024.

Решение. Для каждого простого числа, которое входит в разложение обоих чисел

$$2^3 \cdot 5^2 \cdot 11^2 \cdot 13^3 \cdot 23^2 \cdot 29, \quad 2^5 \cdot 3^3 \cdot 7^2 \cdot 11 \cdot 17^2 \cdot 23$$

(а это только 2, 11 и 23), выбираем наименьшую степень, в которой это простое число входит в них.

Получаем, что

$$\begin{aligned} \text{НОД}(2^3 \cdot 5^2 \cdot 11^2 \cdot 13^3 \cdot 23^2 \cdot 29, 2^5 \cdot 3^3 \cdot 7^2 \cdot 11 \cdot 17^2 \cdot 23) &= \\ &= 2^3 \cdot 11 \cdot 23 = 8 \cdot 11 \cdot 23 = 88 \cdot 23 = 2024. \end{aligned}$$

50. Ответ. 3600.

Решение. Разложим оба числа на простые множители:

$$144 = 2^4 \cdot 3^2, \quad 300 = 2^2 \cdot 3 \cdot 5^2.$$

Поэтому $\text{НОК}(144, 300) = 2^4 \cdot 3^2 \cdot 5^2 = 3600$.

55. **Ответ.** а) 4; б) 6; в) 16; г) 12; д) 64; е) 24; ё) 36; ж) 48.

Из теоремы о количестве делителей мы знаем, что количество делителей числа

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m}$$

равно $(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$.

а) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 3.$$

Тогда, учитывая то, что 3 – простое число, получаем, что это возможно, только если $m = 1$ и $k_1 = 2$. То есть $n = p^2$, где p – простое число¹. Наименьшее число такого вида – $2^2 = 4$.

б) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 4.$$

Тогда, учитывая то, что $4 = 2^2$, получаем, что это возможно, если $m = 1$, $k_1 = 3$ или $m = 2$, $k_1 = k_2 = 1$. То есть либо $n = p^3$, либо $n = pq$, где p и q – различные простые числа.

Наименьшее число вида $n = p^3$ – это $2^3 = 8$; а наименьшее число вида $n = pq$ – это $2 \cdot 3 = 6$. Поэтому наименьшее натуральное число, которое имеет ровно четыре различных делителя, – это 6.

в) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 5.$$

¹Можно было сразу это сказать, сославшись на задачу 52.

Тогда, учитывая то, что 5 – простое число, получаем, что это возможно, только если $m = 1$ и $k_1 = 4$. То есть $n = p^4$, где p – простое число. Наименьшее число такого вида – $2^4 = 16$.

г) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 6.$$

Тогда, учитывая то, что $6 = 2 \cdot 3$, получаем, что это возможно, если $m = 1$, $k_1 = 5$ или $m = 2$, $k_1 = 1$, $k_2 = 2$. То есть либо $n = p^5$, либо $n = pq^2$, где p и q – различные простые числа.

Наименьшее число вида $n = p^5$ – это $2^5 = 32$; а наименьшее число вида $n = pq^2$ – это $3 \cdot 2^2 = 12$. Поэтому наименьшее натуральное число, которое имеет ровно шесть различных делителей, – это 12.

д) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 7.$$

Тогда, учитывая то, что 7 – простое число, получаем, что это возможно, только если $m = 1$ и $k_1 = 6$. То есть $n = p^6$, где p – простое число. Наименьшее число такого вида – $2^6 = 64$.

е) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 8.$$

Тогда, учитывая то, что $8 = 2^3$, получаем, что это возможно, если $m = 1$, $k_1 = 7$, или $m = 2$, $k_1 = 1$, $k_2 = 3$, или $m = 3$, $k_1 = k_2 = k_3 = 1$. То есть либо $n = p^7$, либо $n = pq^3$, либо $n = pqr$, где p , q и r – различные простые числа.

Наименьшее число вида $n = p^7$ – это $2^7 = 128$; наименьшее число вида $n = pq^3$ – это $3 \cdot 2^3 = 24$; а

наименьшее число вида $n = pqr$ – это $2 \cdot 3 \cdot 5 = 30$. Поэтому наименьшее натуральное число, которое имеет ровно восемь различных делителей, – это 24.

ё) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 9.$$

Тогда, учитывая то, что $9 = 3^2$, получаем, что это возможно, если $m = 1$, $k_1 = 8$ или $m = 2$, $k_1 = k_2 = 2$. То есть либо $n = p^8$, либо $n = p^2q^2$, где p и q – различные простые числа.

Наименьшее число вида $n = p^8$ – это $2^8 = 256$; а наименьшее число вида $n = p^2q^2$ – это $2^2 \cdot 3^2 = 36$. Поэтому наименьшее натуральное число, которое имеет ровно девять различных делителей, – это 36.

ж) Пусть количество делителей

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 10.$$

Тогда, учитывая то, что $10 = 2 \cdot 5$, получаем, что это возможно, если $m = 1$, $k_1 = 9$ или $m = 2$, $k_1 = 1$, $k_2 = 4$. То есть либо $n = p^9$, либо $n = pq^4$, где p и q – различные простые числа.

Наименьшее число вида $n = p^9$ – это $2^9 = 512$; а наименьшее число вида $n = pq^4$ – это $3 \cdot 2^4 = 48$. Поэтому наименьшее натуральное число, которое имеет ровно десять различных делителей, – это 48.

56. Ответ. 3040.

Пусть $n = p^k q^\ell r^m$, где p , q и r – различные простые числа, а k , ℓ и m – натуральные числа. Тогда $n^2 = p^{2k} q^{2\ell} r^{2m}$, и из теоремы о количестве делителей мы знаем, что количество его делителей равно

$$(2k + 1)(2\ell + 1)(2m + 1).$$

Но по условию задачи это количество должно быть равно $1001 = 7 \cdot 11 \cdot 13$.

Учитывая, что каждый из множителей $(2k + 1)$, $(2\ell + 1)$ и $(2m + 1)$ больше единицы, а числа 7, 11 и 13 – простые, получаем, что равенство

$$(2k + 1)(2\ell + 1)(2m + 1) = 1001$$

возможно, только если числа k , ℓ и m в некотором порядке равны 3, 5 и 6.

Таким образом, $n = p^3 q^5 r^6$, где p , q и r – различные простые числа. Тогда $n^3 = p^9 q^{15} r^{18}$ и количество его делителей равно

$$(9 + 1) \cdot (15 + 1) \cdot (18 + 1) = 10 \cdot 16 \cdot 19 = 3040.$$

57. Ответ. 2025.

Из теоремы о количестве делителей мы знаем, что количество делителей числа

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m}$$

равно $(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$.

По условию $(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 15 = 3 \cdot 5$. Поэтому либо $n = p^{14}$, либо $n = p^4 q^2$, где p и q – различные простые числа.

Пусть $n = p^{14}$, тогда сумма делителей равна

$$1 + p + p^2 + \dots + p^{14}.$$

Но $p^{14} \geq 2^{14} = 16\,384$. Поэтому сумма всех делителей не может быть равна 3751.

Пусть $n = p^4 q^2$, тогда сумма делителей равна

$$\begin{aligned}
 1 + p + p^2 + p^3 + p^4 + q + pq + p^2q + p^3q + p^4q + \\
 + q^2 + pq^2 + p^2q^2 + p^3q^2 + p^4q^2 = \\
 = (1 + p + p^2 + p^3 + p^4)(1 + q + q^2).
 \end{aligned}$$

Поэтому

$$(1 + p + p^2 + p^3 + p^4)(1 + q + q^2) = 3751.$$

Разложим число 3751 на простые множители:

$$3751 = 11 \cdot 341 = 11 \cdot 11 \cdot 31.$$

Заметим, что

$$\begin{aligned}
 1 + p + p^2 + p^3 + p^4 &\geq 1 + 2 + 2^2 + 2^3 + 2^4 = 31; \\
 1 + q + q^2 &\geq 1 + 2 + 2^2 = 7.
 \end{aligned}$$

Поэтому есть лишь три случая. Либо

$$1 + p + p^2 + p^3 + p^4 = 31, \quad 1 + q + q^2 = 121,$$

либо

$$1 + p + p^2 + p^3 + p^4 = 121, \quad 1 + q + q^2 = 31,$$

либо

$$1 + p + p^2 + p^3 + p^4 = 341, \quad 1 + q + q^2 = 11.$$

Пусть $1 + p + p^2 + p^3 + p^4 = 31$ и $1 + q + q^2 = 121$. Но при $q \leq 7$

$$1 + q + q^2 \leq 1 + 7 + 49 = 57 < 121,$$

а при $q \geq 11$ уже

$$1 + q + q^2 \geq 1 + 11 + 121 = 143 > 121.$$

А между 7 и 11 нет простых чисел. Значит, этот случай невозможен.

Пусть $1 + p + p^2 + p^3 + p^4 = 121$ и $1 + q + q^2 = 31$. При $p = 3$

$$1 + p + p^2 + p^3 + p^4 = 1 + 3 + 9 + 27 + 81 = 121,$$

но значение $(1 + p + p^2 + p^3 + p^4)$ растёт с ростом p . Поэтому при $p < 3$ оно меньше 121, а при $p > 3$ оно больше 121. Значит, равенство возможно только при $p = 3$.

Аналогично замечаем, что при $q = 5$

$$1 + q + q^2 \leq 1 + 5 + 25 = 31,$$

и равенство возможно только при $q = 5$.

Значит, в этом случае

$$n = p^4 q^2 = p^4 \cdot 5^2 = 81 \cdot 25 = 2025.$$

Пусть $1 + p + p^2 + p^3 + p^4 = 341$ и $1 + q + q^2 = 11$. Но при $q = 2$

$$1 + q + q^2 \leq 1 + 2 + 4 = 7 < 11,$$

а при $q \geq 3$ уже

$$1 + q + q^2 \geq 1 + 3 + 9 = 13 > 11.$$

А между 2 и 3 нет простых чисел. Значит, этот случай невозможен.

В итоге получаем, что 2025 – это единственное натуральное число, у которого ровно 15 делителей, а сумма этих делителей равна 3751.

63. Ответ. 2569.

Заметим, что произведение цифр искомого числа должно быть $540 = 5 \cdot 3^3 \cdot 2^2$. Поэтому, если разложить каждую его цифру на простые множители и перемножить, должно получиться $5 \cdot 3^3 \cdot 2^2$.

Простое число 5 в разложении могло появиться только из-за цифры 5. Произведение оставшихся цифр должно быть равно 108. Значит, их не менее трёх, так как произведение двух цифр не превосходит $9 \cdot 9 = 81$. Поэтому искомое число имеет не менее четырёх цифр.

Попытаемся найти наименьшее четырёхзначное число с произведением цифр 540. Очевидно, что в наименьшем числе нет цифры 1, так как она лишь увеличивает количество цифр, но никак не влияет на произведение. Кроме того, в нём все цифры идут в порядке возрастания, чтобы самая маленькая отвечала за количество тысяч, а самая большая – за количество единиц.

Учитывая, что цифры 1 в числе нет, самое маленькое значение для первой цифры – 2. А в числе ещё есть цифра 5, поэтому произведение двух оставшихся цифр равно $54 = 3^3 \cdot 2$. То есть две другие цифры – это 6 и 9 (потому что одна из них в разложении на простые должна содержать двойку, и в каждом из них одна или две тройки). Наименьшее число с такими цифрами – это 2569. Если же первая цифра будет больше двойки, то число будет больше, чем 2569.

Таким образом, мы доказали, что 2569 – это наименьшее натуральное число, произведение цифр которого равно 540.

64. Первое решение. В задаче 60 (см. стр. 125) мы доказали, что при всех простых $p > 3$ число $(p^2 - 1)$ делится на 24. Значит, и $(p^2 - 1)$, и $(q^2 - 1)$ делятся на 24. Поэтому их разность

$$(p^2 - 1) - (q^2 - 1) = p^2 - q^2$$

делится на 24.

Второе решение. Заметим, что

$$p^2 - q^2 = (p - q)(p + q).$$

При этом числа p и q простые и не равны двум, поэтому они оба нечётны. Тогда $(p - q)$ и $(p + q)$ – два чётных числа, которые отличаются на $2q$. Но $2q$ не делится на 4. Поэтому из чётных чисел $(p - q)$ и $(p + q)$ одно делится на 4, а другое – нет. Значит, их произведение $(p - q)(p + q)$ делится на 8.

С другой стороны, $2q$ не делится на 3, так как q – простое и не равно трём. Значит, у чисел $(p - q)$ и $(p + q)$ разные остатки при делении на 3. Предположим, что ни один из остатков не равен нулю, тогда у одного из них остаток равен 1, а у другого – равен 2. Но тогда их сумма

$$(p - q) + (p + q) = 2p$$

должна делиться на 3. Что невозможно, так как p – простое и не равно трём.

Значит, одно из чисел $(p - q)$ и $(p + q)$ имеет остаток 0 при делении на 3. То есть произведение $(p - q)(p + q)$ делится на 3. Но если число $(p^2 - q^2)$ делится и на 8, и на 3, то в его разложении на простые множители есть $2^3 \cdot 3$. Поэтому оно делится на 24.

65. Ответ. 59.

Поскольку $250\,000 = 2^4 \cdot 5^6$ и оно должно делиться на каждое из чисел пары, то разложение на простые множители каждого из наших чисел имеет вид $2^x \cdot 5^y$, где $0 \leq x \leq 4$ и $0 \leq y \leq 6$.

Для того чтобы наименьшее общее кратное таких чисел оказалось равно 250 000, нужно, чтобы реализовалась одна из двух возможностей:

- одно из чисел равно 250 000, а другое число – любой делитель числа 250 000;
- ни одно из чисел не равно 250 000, но в разложении одного из чисел должен присутствовать множитель 2^4 , а в разложении другого – множитель 5^6 .

В первом случае второе число – это любой делитель числа 250 000. А у него всего $(4 + 1) \cdot (6 + 1) = 35$ различных делителей.

Во втором случае получаем, что наши числа равны $2^4 \cdot 5^m$ и $2^n \cdot 5^6$, где $0 \leq m \leq 5$, $0 \leq n \leq 3$, так как ни одно из них не равно 250 000. Таким образом, есть шесть возможных значений первого числа и независимо от этого четыре возможных значения второго числа. То есть в этом случае имеется $6 \cdot 4 = 24$ возможных пары.

В итоге получаем, что существует $35 + 24 = 59$ пар натуральных чисел, у которых наименьшее общее кратное равно 250 000.

66. Ответ. 82.

Решение. Заметим, что $80^2 = 6400$, $81^2 = 6561$, поэтому $80^2 < 6500 < 81^2$. Значит, число 6500! точно делится на k^k при $k \leq 80$, так как среди чисел

от 1 до 6500 есть не менее k чисел, делящихся на k . И точно не делится на 83^{83} , так как 83 – простое число и среди чисел от 1 до 6500 меньше 83 чисел, делящихся на 83, и нет ни одного, которое бы делилось на 83^2 , поэтому в разложении числа $6500!$ на простые множители 83 входит в степени меньшей, чем 83.

Осталось лишь проверить, делится ли число $6500!$ на 81^{81} и на 82^{82} .

Среди чисел от 1 до 6500 более 2000 делятся на 3. Значит, число $6500!$ делится на 3^{2000} , а 3^{2000} делится на $81^{81} = 3^{324}$. Поэтому число $6500!$ делится на 81^{81} .

Среди чисел от 1 до 6500 есть более 100, которые делятся на 41, и более 3000 чисел, которые делятся на 2. Значит, число $6500!$ делится на $2^{3000} \cdot 41^{100}$, а $2^{3000} \cdot 41^{100}$ делится на $82^{82} = 2^{82} \cdot 41^{82}$. Поэтому число $6500!$ делится на 82^{82} .

В итоге мы получили, что $n = 82$ – наибольшее натуральное число, для которого $6500!$ делится на каждое из чисел вида k^k при $k = 1, 2, 3, \dots, n$.

67. Ответ. 78.

Решение. Заметим, что если оба числа $(17n + 5)$ и $(19n + 1)$ делятся на некоторое число d , то и число

$$19 \cdot (17n + 5) - 17 \cdot (19n + 1) = 78$$

делится на d . Значит, любой общий делитель этих двух чисел не превосходит 78. Попробуем найти такое n , что оба числа $(17n+5)$ и $(19n+1)$ делятся на 78.

Если числа $(17n + 5)$ и $(19n + 1)$ делятся на 78, то и число

$$(19n + 1) - (17n + 5) = 2n - 4$$

делится на 78.

Такое возможно при $n = 2$. Но тогда

$$17n + 5 = 34 + 5 = 39, \quad 19n + 1 = 38 + 1 = 39.$$

И их наибольший общий делитель равен лишь 39.

Следующее n , при котором такое возможно, – это $n = 41$, так как $2 \cdot 41 - 4 = 78$. Тогда

$$17n + 5 = 697 + 5 = 702, \quad 19n + 1 = 779 + 1 = 780.$$

При этом $702 = 9 \cdot 78$, а $780 = 10 \cdot 78$. Поэтому их наибольший общий делитель равен 78.

Таким образом, мы доказали, что ни при каком натуральном n наибольший общий делитель чисел $(17n+5)$ и $(19n+1)$ не превосходит 78, и нашли $n = 41$, при котором он равен 78.

Значит, 78 – это наибольшее значение, которое может принимать НОД($17n + 5$, $19n + 1$).

74. Ответ. $(-7; 1)$, $(2; -17)$, $(3; 21)$, $(12; 3)$.

Решение. Исходное равенство равносильно каждому из следующих:

$$2mn - 4m - 5n = 9,$$

$$2mn - 4m - 5n + 10 = 19,$$

$$2m(n - 2) - 5(n - 2) = 19,$$

$$(2m - 5)(n - 2) = 19.$$

Так как 19 – простое число, то его можно представить в виде произведения двух целых чисел лишь четырьмя способами:

$$19 = 1 \cdot 19 = 19 \cdot 1 = (-1) \cdot (-19) = (-19) \cdot (-1).$$

Рассмотрим эти четыре случая:

$2m - 5$	$n - 2$	m	n
1	19	3	21
19	1	12	3
-1	-19	2	-17
-19	-1	-7	1

Получаем, что всего существует четыре решения: $(3; 21)$, $(12; 3)$, $(2; -17)$, $(-7; 1)$.

75. **Ответ.** 3×6 и 4×4 .

Пусть стороны прямоугольника равны a и b . Тогда его площадь равна ab , а периметр равен $2(a+b)$. Мы хотим, чтобы выполнялось равенство:

$$ab = 2(a + b).$$

Оно равносильно следующим равенствам:

$$ab - 2(a + b) = 0,$$

$$ab - 2a - 2b = 0,$$

$$ab - 2a - 2b + 4 = 4,$$

$$a(b - 2) - 2(b - 2) = 4,$$

$$(a - 2)(b - 2) = 4.$$

Теперь нам нужно перебрать все пары целых чисел, произведение которых равно 4:

$$4 = 1 \cdot 4 = 2 \cdot 2 = 4 \cdot 1 =$$

$$= (-1) \cdot (-4) = (-2) \cdot (-2) = (-4) \cdot (-1).$$

Но a и b – натуральные числа, поэтому

$$a - 2 > -2, \quad b - 2 > -2.$$

А в последних трёх парах хотя бы одно из чисел не превосходит (-2) . Значит, ни одна из этих пар не подходит.

Рассмотрим три оставшиеся пары:

$a - 2$	$b - 2$	a	b
1	4	3	6
2	2	4	4
4	1	6	3

Но прямоугольники 3×6 и 6×3 – это один и тот же прямоугольник.

В итоге мы получили, что существует два прямоугольника, стороны которых выражаются натуральными числами, а площадь численно равна периметру, – это прямоугольники 3×6 и 4×4 .

77. Первое решение. Предположим, что нашли натуральные числа m и n , для которых верно равенство $2n^2 = m^2$. Тогда $m^2 = 2 \cdot n^2$ – чётное число. Поэтому m – чётное число. Пусть $m = 2m_1$. Но тогда

$$2n^2 = (2m_1)^2,$$

$$2n^2 = 4m_1^2,$$

$$n^2 = 2m_1^2.$$

Значит, n^2 – чётное число. Поэтому n – чётное число. Пусть $n = 2n_1$. Но тогда

$$(2n_1)^2 = 2m_1^2,$$

$$4n_1^2 = 2m_1^2,$$

$$2n_1^2 = m_1^2.$$

Значит, m_1^2 – чётное число. Поэтому m_1 – чётное число. Пусть $m_1 = 2m_2$. Но тогда... Ну вы поняли. У нас получился бесконечный спуск.

Предположив, что равенство $2n^2 = m^2$ верно для некоторой пары $(n; m)$ натуральных чисел, мы показали, что оно будет верно и для меньшей пары $\left(\frac{m}{2}; n\right)$. А значит, мы всегда сможем получать новую пару решений, деля одно из чисел пополам. Но число не может бесконечно делиться на 2. И мы пришли к противоречию! Значит, уравнение $2n^2 = m^2$ не имеет решений в натуральных числах.

Второе решение. Если воспользоваться принципом крайнего, то можно не заниматься бесконечным спуском. Давайте снова предположим, что уравнение $2n^2 = m^2$ имеет решения в натуральных числах, и из всех решений выберем то решение $(n; m)$, в котором число n – самое маленькое из всех возможных решений.

А дальше опять замечаем, что $m^2 = 2 \cdot n^2$ – чётное число. Поэтому m – чётное число. И если $m = 2m_1$, то

$$2n^2 = (2m_1)^2,$$

$$2n^2 = 4m_1^2,$$

$$n^2 = 2m_1^2.$$

Но это означает, что пара чисел $(m_1; n)$ – тоже решение исходного уравнения. И при этом $m_1^2 = \frac{n^2}{2}$, значит, $m_1 < n$. Но мы же выбрали решение $(n; m)$ так, что в нём число n – самое маленькое из всех возможных решений, и при этом нашли решение $(m_1; n)$, в котором $m_1 < n$. Пришли к противоречию! Значит, уравнение $2n^2 = m^2$ не имеет решений в натуральных числах.

Третье решение. А можно было обойтись основной теоремой арифметики. Предположим, что нашли натуральные числа m и n , для которых верно равенство $2n^2 = m^2$. Разложим их на простые множители:

$$n = 2^k \cdot \dots, \quad m = 2^\ell \cdot \dots,$$

где k и ℓ – целые неотрицательные числа.

Тогда

$$\begin{aligned} 2n^2 &= 2 \cdot (2^k \cdot \dots)^2 = 2^{2k+1} \cdot \dots, \\ m^2 &= (2^\ell \cdot \dots)^2 = 2^{2\ell} \cdot \dots \end{aligned}$$

Но $2n^2 = m^2$, поэтому $2n^2$ и m^2 – это одно и то же число, а разложение на простые множители единственно. И при этом в разложение числа $2n^2$ двойка входит в нечётной степени, а в разложение числа m^2 – в чётной степени. Противоречие! Значит, уравнение $2n^2 = m^2$ не имеет решений в натуральных числах.

78. Предположим, что нашли такие натуральные числа, для которых верно равенство

$$27k^4 + 9\ell^4 + 3m^4 = n^4.$$

Тогда число $n^4 = 3 \cdot (9k^4 + 3\ell^4 + m^4)$ кратно трём. Значит, и n – кратно трём (так как, если число не содержит тройки в разложении на простые множители, то и его четвёртая степень не содержит тройки в разложении). Пусть $n = 3n_1$, тогда

$$\begin{aligned} 27k^4 + 9\ell^4 + 3m^4 &= (3n_1)^4, \\ 27k^4 + 9\ell^4 + 3m^4 &= 81n_1^4, \\ 9k^4 + 3\ell^4 + m^4 &= 27n_1^4. \end{aligned}$$

Тогда число $m^4 = 3 \cdot (9n_1^4 - 3k^4 - \ell^4)$ кратно трём. Значит, и m кратно трём. Пусть $m = 3m_1$, тогда

$$9k^4 + 3\ell^4 + (3m_1)^4 = 27n_1^4,$$

$$9k^4 + 3\ell^4 + 81m_1^4 = 27n_1^4,$$

$$3k^4 + \ell^4 + 27m_1^4 = 9n_1^4.$$

Тогда число $\ell^4 = 3 \cdot (3n_1^4 - k^4 - 9m_1^4)$ кратно трём. Значит, и ℓ кратно трём. Пусть $\ell = 3\ell_1$, тогда

$$3k^4 + (3\ell_1)^4 + 27m_1^4 = 9n_1^4,$$

$$3k^4 + 81\ell_1^4 + 27m_1^4 = 9n_1^4,$$

$$k^4 + 27\ell_1^4 + 9m_1^4 = 3n_1^4.$$

Тогда число $k^4 = 3 \cdot (n_1^4 - 9\ell_1^4 - 3m_1^4)$ кратно трём. Значит, и k кратно трём. Пусть $k = 3k_1$, тогда

$$(3k_1)^4 + 27\ell_1^4 + 9m_1^4 = 3n_1^4,$$

$$81k_1^4 + 27\ell_1^4 + 9m_1^4 = 3n_1^4,$$

$$27k_1^4 + 9\ell_1^4 + 3m_1^4 = n_1^4.$$

И мы получили, что если набор $(k; \ell; m; n)$ натуральных чисел является решением нашего уравнения, тогда они все кратны трём и числа $\left(\frac{k}{3}; \frac{\ell}{3}; \frac{m}{3}; \frac{n}{3}\right)$ тоже являются решениями нашего уравнения. Но тогда они тоже все кратны трём, и числа $\left(\frac{k}{9}; \frac{\ell}{9}; \frac{m}{9}; \frac{n}{9}\right)$ тоже являются решениями нашего уравнения. Но тогда...

В итоге мы получили бесконечный спуск! Мы получили, что если натуральные числа $(k; \ell; m; n)$ являются решением нашего уравнения, то они

делятся на любую степень тройки, чего не бывает. Пришли к противоречию! Значит, уравнение

$$27k^4 + 9\ell^4 + 3m^4 = n^4$$

не имеет решений в натуральных числах.

79. Предположим, что решение есть. Заметим, что правая часть равенства

$$\ell^2 + m^2 + n^2 = 2\ell mn$$

делится на 2, значит, и левая должна делиться на 2. Следовательно все три слагаемых в левой части не могут быть нечётными (так как сумма трёх нечётных чисел нечётна). Поэтому хотя бы одно слагаемое должно быть чётным.

Пусть, например, число ℓ^2 чётное. Тогда и само число ℓ чётно. Пусть $\ell = 2\ell_1$, тогда

$$(2\ell_1)^2 + m^2 + n^2 = 2 \cdot (2\ell_1) \cdot mn,$$

$$4\ell_1^2 + m^2 + n^2 = 4\ell_1 mn.$$

Отсюда следует, что число

$$m^2 + n^2 = 4 \cdot (\ell_1 mn - \ell_1^2)$$

делится на 4.

А мы знаем (см. решение задачи 76 на стр. 150), что сумма двух квадратов может быть кратна четырём, только если это квадраты чётных чисел. Поэтому числа m и n тоже чётны. Пусть $m = 2m_1$ и $n = 2n_1$, тогда

$$4\ell_1^2 + (2m_1)^2 + (2n_1)^2 = 4\ell_1 \cdot (2m_1) \cdot (2n_1),$$

$$4\ell_1^2 + 4m_1^2 + 4n_1^2 = 16\ell_1 m_1 n_1,$$

$$\ell_1^2 + m_1^2 + n_1^2 = 4\ell_1 m_1 n_1.$$

Рассуждая аналогично, мы понимаем, что хотя бы один из квадратов должен быть чётным, значит, он делится на 4, поэтому сумма двух других квадратов должна делиться на 4, что возможно, только если это квадраты чётных чисел. То есть $\ell_1 = 2\ell_2$, $m_1 = 2m_2$ и $n_1 = 2n_2$:

$$\begin{aligned}(2\ell_2)^2 + (2m_2)^2 + (2n_2)^2 &= 4 \cdot (2\ell_2) \cdot (2m_2) \cdot (2n_2), \\ 4\ell_2^2 + 4m_2^2 + 4n_2^2 &= 32\ell_2 m_2 n_2, \\ \ell_2^2 + m_2^2 + n_2^2 &= 8\ell_2 m_2 n_2.\end{aligned}$$

Затем точно так же заметим, что числа ℓ_2 , m_2 и n_2 обязаны быть чётными, то есть $\ell_2 = 2\ell_3$, $m_2 = 2m_3$ и $n_2 = 2n_3$, из чего получим, что

$$\ell_3^2 + m_3^2 + n_3^2 = 16\ell_3 m_3 n_3.$$

И так далее.

Таким образом, мы поняли, что если натуральные числа ℓ , m и n удовлетворяют равенству $\ell^2 + m^2 + n^2 = 2\ell mn$, то они делятся на любую степень двойки, что невозможно. Пришли к противоречию! Значит, уравнение

$$\ell^2 + m^2 + n^2 = 2\ell mn$$

не имеет решений в натуральных числах.

82. Ответ. 99.

Первое решение. Преобразуем уравнение:

$$\begin{aligned}5y &= 1000 - 2x, \\ 5y &= 2 \cdot (500 - x).\end{aligned}$$

Правая часть делится на 2, значит, и левая часть $5y$ должна делиться на 2. Но число 2 – простое, и 5 на 2

не делится. Значит, y делится на 2. Таким образом, $y = 2k$, где k – целое число. Тогда

$$5 \cdot 2k = 2 \cdot (500 - x),$$

$$5k = 500 - x,$$

$$x = 500 - 5k.$$

При этом нас интересуют только натуральные решения. Значит,

$$\begin{cases} x = 500 - 5k > 0, \\ y = 2k > 0. \end{cases}$$

То есть $0 < k < 100$. Значит, число k может принимать любые целые значения от 1 до 99. Итого получаем 99 решений.

Второе решение. Так как $2x + 5y = 1000$ делится на 5, то число $2x$ делится на 5, значит, x делится на 5. Аналогично получаем, что y делится на 2. Тогда $x = 5x_1$, $y = 2y_1$, где x_1 и y_1 – натуральные числа, и исходное уравнение переписывается в виде

$$2 \cdot (5x_1) + 5 \cdot (2y_1) = 1000,$$

$$10x_1 + 10y_1 = 1000,$$

$$x_1 + y_1 = 100.$$

Очевидно, что это уравнение имеет в натуральных числах ровно 99 решений: x_1 меняется от 1 до 99, а y_1 дополняет его до 100. Поэтому и исходное уравнение имеет ровно 99 решений.

83. Ответ. 33 или 143.

Первое решение. Пусть в каких-то k мешках лежало по 22 подарка, а в остальных $(40 - k)$ – по n .

Тогда

$$k \cdot 22 + (40 - k) \cdot n = 1001.$$

Вычтем из обеих частей равенства 880:

$$k \cdot 22 - 880 + (40 - k) \cdot n = 1001 - 880;$$

$$-22 \cdot (40 - k) + (40 - k) \cdot n = 121;$$

$$(40 - k) \cdot (n - 22) = 11^2.$$

Учитывая то, что $0 < 40 - k < 40$, получаем, что есть только два случая:

$40 - k$	$n - 22$	k	n
1	121	39	143
11	11	29	33

Поэтому либо $n = 33$, либо $n = 143$.

Второе решение. Если бы в каждом мешке было по 22 подарка, то всего было бы 880 подарков. Но подарков на $1001 - 880 = 121$ больше. Значит, «лишний» 121 подарок нужно разложить поровну по некоторым мешкам.

Так как $121 = 11^2$, а всего мешков 40, то либо в 11 мешках будет по 11 «лишних» подарков, либо в одном мешке будет 121 «лишний» подарок. В первом случае $n = 22 + 11 = 33$, а во втором случае $n = 22 + 121 = 143$.

84. Ответ. (1; 100), (4; 25), (25; 4) или (100; 1).

Пусть $d = \text{НОД}(x; y)$. Тогда $x = ad$, $y = bd$, где a и b – взаимно простые числа. При этом

$$\text{НОК}(x; y) = \frac{xy}{\text{НОД}(x; y)} = \frac{abd^2}{d} = abd.$$

И уравнение принимает вид

$$d + abd = 101.$$

Левая часть делится на d , а правая – простое число 101. Поэтому либо $d = 1$, либо $d = 101$. Но если $d = 101$, то $abd = 0$, что невозможно. Остаётся случай $d = 1$, при котором $ab = 100$.

То есть нам нужно найти количество пар взаимно простых чисел x и y , произведение которых равно 100. Значит, x – это делитель числа 100, $y = \frac{100}{x}$ и при этом они взаимно просты.

Так как у числа $100 = 2^2 \cdot 5^2$ есть ровно

$$(2 + 1) \cdot (2 + 1) = 9$$

различных делителей, то нужно из девяти пар чисел

$$\begin{array}{lll} (1; 100), & (2; 50), & (4; 25), \\ (5; 20), & (10; 10), & (20; 5), \\ (25; 4), & (50; 2), & (100; 1), \end{array}$$

произведение которых равно 100, выбрать те, где числа взаимно просты. Это, очевидно, только пары (1; 100), (4; 25), (25; 4) и (100; 1).

85. Ответ. $x = 1$, $y = 2$ и $z = 1$.

Преобразуем немного наше уравнение:

$$\begin{aligned} 4 \cdot (y^2 - z^2 - xz) &= x^2 + x + 6; \\ 4y^2 - 4z^2 - 4xz &= x^2 + x + 6; \\ 4y^2 - 4z^2 - 4xz - x^2 &= x + 6; \\ 4y^2 - (4z^2 + 4xz + x^2) &= x + 6; \end{aligned}$$

$$\begin{aligned}(2y)^2 - (2z + x)^2 &= x + 6; \\ (2y + 2z + x)(2y - 2z - x) &= x + 6.\end{aligned}$$

Правая часть равенства положительна, значит, и левая положительна. При этом первый множитель больше нуля при любых натуральных значениях x , y и z . Значит, и $2y - 2z - x > 0$.

Заметим, что

$$2y + 2z + x \geq 2 + 2 + x = x + 4.$$

Поэтому, если $2y - 2z - x \geq 2$, то

$$(2y + 2z + x)(2y - 2z - x) \geq (x + 4) \cdot 2 = 2x + 8 > x + 6.$$

Получается, что

$$0 < 2y - 2z - x < 2.$$

То есть $2y - 2z - x = 1$ и исходное уравнение равносильно системе:

$$\begin{cases} 2y - 2z - x = 1, \\ 2y + 2z + x = x + 6. \end{cases}$$

Из второго равенства следует, что $y + z = 3$. И учитывая то, что y и z – натуральные числа, получаем, что либо $y = 1$ и $z = 2$, либо $y = 2$ и $z = 1$.

В первом случае из равенства $2y - 2z - x = 1$ следует, что $2 - 4 - x = 1$. То есть $x = -3$ – не натуральное число.

А во втором случае из равенства $2y - 2z - x = 1$ следует, что $4 - 2 - x = 1$. То есть $x = 1$.

В итоге получаем, что y исходного уравнения есть единственное решение: $x = 1$, $y = 2$ и $z = 1$.

86. **Ответ.** $m = 4, n = 21$ или $m = 6, n = 33$.

Заметим, что левая часть равенства

$$3^m + 360 = n^2$$

всегда делится на 3. Значит, и правая часть равенства делится на 3. Это означает, что число n кратно трём.

Пусть $n = 3n_1$, где n_1 – натуральное число. Тогда

$$3^m + 360 = 9n_1^2.$$

Откуда следует, что верно равенство

$$3^m = 9n_1^2 - 360.$$

В нём правая часть делится на 9, значит, и левая часть делится на 9. То есть $m \geq 2$.

Пусть $m = m_1 + 2$, где m_1 – целое неотрицательное число. Тогда

$$9 \cdot 3^{m_1} + 360 = 9n_1^2.$$

Откуда следует, что

$$3^{m_1} + 40 = n_1^2.$$

Здесь левая часть нечётна при любом m_1 . Поэтому число n_1^2 должно быть нечётным. Значит, и число n_1 нечётно.

Заметим, что квадрат нечётного числа

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4 \cdot (k^2 + k) + 1$$

даёт остаток 1 при делении на 4. Значит, и число $(3^{m_1} + 40)$ даёт остаток 1 при делении на 4. То есть число 3^{m_1} даёт остаток 1 при делении на 4.

Заметим, что

$$\begin{aligned} 3^0 &= 1 = 0 \cdot 4 + 1; & 3^1 &= 3 = 0 \cdot 4 + 3; \\ 3^2 &= 9 = 2 \cdot 4 + 1; & 3^3 &= 27 = 6 \cdot 4 + 3; \\ 3^4 &= 81 = 20 \cdot 4 + 1; & & \dots \end{aligned}$$

То есть остатки при делении на 4 у степеней тройки чередуются.

Действительно, если $3^k = \ell \cdot 4 + 1$, то

$$3^{k+1} = 3 \cdot (\ell \cdot 4 + 1) = 3\ell \cdot 4 + 3.$$

И наоборот, если $3^k = \ell \cdot 4 + 3$, то

$$3^{k+1} = 3 \cdot (\ell \cdot 4 + 3) = 3\ell \cdot 4 + 9 = (3\ell + 2) \cdot 4 + 1.$$

Поэтому, если 3^{m_1} даёт остаток 1 при делении на 4, то m_1 – это чётное число. Пусть $m_1 = 2m_2$, тогда наше уравнение приобретает вид

$$3^{2m_2} + 40 = n_1^2.$$

То есть

$$n_1^2 - 3^{2m_2} = 40.$$

И, раскладывая левую часть на множители¹, получаем

$$(n_1 - 3^{m_2}) \cdot (n_1 + 3^{m_2}) = 40.$$

¹Заметим, что здесь можно было обойтись без разложения на множители. Обозначив $x = 3^{m_2}$, мы получаем, что квадрат числа n_1 на 40 больше, чем квадрат нечётного числа x . Поэтому число n_1 тоже нечётное, а значит, оно больше, чем x , хотя бы на 2. Отсюда получаем, что

$$x^2 + 40 = n_1^2 \geq (x + 2)^2 = x^2 + 4x + 4.$$

Из этого следует, что $x \leq 9$. А учитывая, что $x = 3^{m_2}$, понимаем, что достаточно перебрать три случая: $x = 1$, $x = 3$ и $x = 9$.

Такой подход лучше работает, чем предложенный в решении, когда в правой части стоит число, у которого в разы больше делителей, чем у числа 40.

Каждый из множителей – это делитель числа $40 = 2^3 \cdot 5$, то есть принимает одно из следующих значений: 1, 2, 4, 5, 8, 10, 20 или 40. Причём первый множитель меньше второго. Поэтому нужно перебрать только четыре случая:

$$1 \cdot 40 = 40; \quad 2 \cdot 20 = 40; \quad 4 \cdot 10 = 40; \quad 5 \cdot 8 = 40.$$

Но сумма $(n_1 - 3^{m_2}) + (n_1 + 3^{m_2}) = 2n_1$ должна быть чётной. Поэтому остаётся лишь два случая:

$n_1 - 3^{m_2}$	$n_1 + 3^{m_2}$	n_1	3^{m_2}
2	20	$\frac{2+20}{2} = 11$	$\frac{20-2}{2} = 9$
4	10	$\frac{4+10}{2} = 7$	$\frac{10-4}{2} = 3$

В первом случае $n_1 = 11$, $m_2 = 2$. Поэтому

$$n = 3n_1 = 33, \quad m = m_1 + 2 = 2m_2 + 2 = 6.$$

Во втором случае $n_1 = 7$, $m_2 = 1$. Поэтому

$$n = 3n_1 = 21, \quad m = m_1 + 2 = 2m_2 + 2 = 4.$$

91. Ответ. 10.

$$\begin{aligned}
 10^{70} &= (10^2)^{35} = 100^{35} \stackrel{27}{\equiv} (-8)^{35} = -8^{35} = \\
 &= -8 \cdot (8^2)^{17} = -8 \cdot 64^{17} \stackrel{27}{\equiv} -8 \cdot 10^{17} = \\
 &= -8 \cdot 10 \cdot (10^2)^8 = -80 \cdot (100)^8 \stackrel{27}{\equiv} 1 \cdot (-8)^8 = \\
 &= 8^8 = (8^2)^4 = 64^4 \stackrel{27}{\equiv} 10^4 = (10^2)^2 = 100^2 \stackrel{27}{\equiv} \\
 &\stackrel{27}{\equiv} (-8)^2 = 64 \equiv 10 \pmod{27}.
 \end{aligned}$$

92. Ответ. 8.

Заметим, что последняя цифра числа – это просто остаток при делении этого числа на 10.

Первое решение.

$$\begin{aligned} 2^{1111} &= 2 \cdot (2^5)^{222} = 2 \cdot 32^{222} \stackrel{10}{\equiv} 2 \cdot 2^{222} = 2^{223} = \\ &= 2^3 \cdot (2^5)^{44} = 2^3 \cdot 32^{44} \stackrel{10}{\equiv} 2^3 \cdot 2^{44} = 2^{47} = \\ &= 2^2 \cdot (2^5)^9 = 2^2 \cdot 32^9 \stackrel{10}{\equiv} 2^2 \cdot 2^9 = 2^{11} = \\ &= 2 \cdot (2^5)^2 = 2 \cdot 32^2 \stackrel{10}{\equiv} 2 \cdot 2^2 = 8. \end{aligned}$$

Второе решение. Заметим, что

$$2^4 = 16 \equiv 6 \pmod{10}.$$

И при этом

$$6^2 = 36 \equiv 6 \pmod{10}.$$

Это означает, что

$$\begin{aligned} 6^3 &= 6 \cdot 6^2 \equiv 6 \cdot 6 = 36 \equiv 6 \pmod{10}; \\ 6^4 &= 6 \cdot 6^3 \equiv 6 \cdot 6 = 36 \equiv 6 \pmod{10}; \\ &\dots \\ 6^n &= 6 \cdot 6^{n-1} \equiv 6 \cdot 6 = 36 \equiv 6 \pmod{10}. \end{aligned}$$

Поэтому

$$\begin{aligned} 2^{1111} &= 2^3 \cdot (2^4)^{277} \stackrel{10}{\equiv} 2^3 \cdot 6^{277} \stackrel{10}{\equiv} 2^3 \cdot 6 = \\ &= 8 \cdot 6 = 48 \equiv 8 \pmod{10}. \end{aligned}$$

93. Ответ. 8.

$$2^{1234} = 2^4 \cdot (2^5)^{246} = 16 \cdot 32^{246} \stackrel{11}{\equiv} 5 \cdot (-1)^{246} = 5;$$

$$\begin{aligned}
7^{1234} &= (7^2)^{617} = 49^{617} \stackrel{11}{\equiv} 5^{617} = 5 \cdot (5^2)^{308} = 5 \cdot 25^{308} \stackrel{11}{\equiv} \\
&\stackrel{11}{\equiv} 5 \cdot 3^{308} = 5 \cdot (3^2)^{154} = 5 \cdot 9^{154} \stackrel{11}{\equiv} 5 \cdot (-2)^{154} = \\
&= 5 \cdot 2^{154} = 5 \cdot 2^4 \cdot (2^5)^{30} = 5 \cdot 16 \cdot 32^{30} \stackrel{11}{\equiv} \\
&\stackrel{11}{\equiv} 5 \cdot 5 \cdot (-1)^{30} = 25 \equiv 3 \pmod{11}.
\end{aligned}$$

Поэтому

$$2^{1234} + 7^{1234} \equiv 5 + 3 = 8 \pmod{11}.$$

94. Ответ. 07.

Заметим, что две последние цифры числа – это просто остаток при делении этого числа на 100.

Посмотрим первые несколько степеней семёрки:

$$\begin{aligned}
7^1 &= 7; \\
7^2 &= 49; \\
7^3 &= 343 \equiv 43 \pmod{100}; \\
7^4 &= 7 \cdot 7^3 \stackrel{100}{\equiv} 7 \cdot 43 = 301 \equiv 1 \pmod{100}.
\end{aligned}$$

Поэтому

$$7^{777} = 7 \cdot (7^4)^{194} \equiv 7 \cdot 1^{194} = 7 \pmod{100}.$$

Значит, две последние цифры числа 7^{777} – это 07.

95. Ответ. У числа такой же остаток при делении на 8, как у числа, образованного тремя его последними цифрами.

Пусть $a = \overline{a_n a_{n-1} \dots a_3 a_2 a_1 a_0}$, тогда

$$\begin{aligned}
a &= 1000 \cdot \overline{a_n a_{n-1} \dots a_3} + \overline{a_2 a_1 a_0} \equiv \\
&\equiv 0 \cdot \overline{a_n a_{n-1} \dots a_3} + \overline{a_2 a_1 a_0} = \overline{a_2 a_1 a_0} \pmod{8}.
\end{aligned}$$

Это означает, что у числа a такой же остаток при делении на 8, как у числа $\overline{a_3 a_1 a_0}$, образованного тремя его последними цифрами.

96. Ответ. У числа такой же остаток при делении на 16, как у числа, образованного четырьмя его последними цифрами.

Пусть $a = \overline{a_n a_{n-1} \dots a_4 a_3 a_2 a_1 a_0}$, тогда

$$\begin{aligned} a &= 10\,000 \cdot \overline{a_n a_{n-1} \dots a_4} + \overline{a_3 a_2 a_1 a_0} \equiv \\ &\equiv 0 \cdot \overline{a_n a_{n-1} \dots a_4} + \overline{a_3 a_2 a_1 a_0} = \overline{a_3 a_2 a_1 a_0} \pmod{16}. \end{aligned}$$

Это означает, что у числа a такой же остаток при делении на 16, как у числа $\overline{a_4 a_3 a_1 a_0}$, образованного четырьмя его последними цифрами.

99. Мы знаем, что у любого числа такой же остаток при делении на 9, как у его суммы цифр. Но тогда из условия следует, что

$$2n \equiv n \pmod{9}.$$

Вычтя из обеих частей сравнения n , получим, что

$$n \equiv 0 \pmod{9}.$$

То есть число n делится на 9.

100. Ответ. Нет.

Предположим, что такое число n существует. Пусть сумма его цифр равна S . Тогда из условия следует, что верно равенство

$$n = 100S + 100.$$

Но мы знаем, что для любого числа

$$S \equiv n \pmod{3}.$$

Поэтому

$$n = 100S + 100 \equiv S + 1 \equiv n + 1 \pmod{3}.$$

Но $n \not\equiv n + 1 \pmod{3}$, так как $(n + 1) - n = 1$ не делится на 3.

Пришли к противоречию. Значит, не существует натурального числа, которое при делении на сумму своих цифр и в остатке, и в неполном частном даёт 100.

101. **Ответ.** $a = 6$ и $b = 0$.

Так как данное число n делится на $99 = 9 \cdot 11$, то оно делится на 9 и на 11. Из признаков делимости на 9 и на 11 следует, что

$$\begin{aligned} n &\stackrel{9}{\equiv} (1 + 2 + 3 + 4) \cdot (2 \cdot 1234 + 1) + a + b = \\ &= 10 \cdot 2469 + a + b \stackrel{9}{\equiv} (1 + 0) \cdot (2 + 4 + 6 + 9) + a + b = \\ &= 21 + a + b \equiv 3 + a + b \pmod{9}. \end{aligned}$$

$$\begin{aligned} n &\stackrel{11}{\equiv} 4 - 3 + 2 - 1 + 4 - 3 + 2 - 1 + 4 - 3 + 2 - 1 + \dots \\ &\quad \dots + b - 4 + 3 - 2 + 1 - a + 4 - 3 + 2 - 1 + \dots \\ &\quad \dots + 4 - 3 + 2 - 1 + 4 - 3 + 2 - 1 + 4 - 3 + 2 - 1 = \\ &= (4 - 3 + 2 - 1) \cdot (2 \cdot 1234 - 1) + b - a = \\ &= 2 \cdot 2467 + b - a \stackrel{11}{\equiv} 2 \cdot (7 - 6 + 4 - 2) + b - a = \\ &= 2 \cdot 3 + b - a = 6 + b - a. \end{aligned}$$

Так как число n делится на 9 и на 11, то

$$3 + a + b \equiv 0 \pmod{9}; \quad 6 + b - a \equiv 0 \pmod{11}.$$

Но a и b – цифры, поэтому

$$3 \leq 3 + a + b \leq 21; \quad -3 \leq 6 + b - a \leq 15.$$

Значит, либо $a + b = 6$, либо $a + b = 15$, и при этом либо $b - a = -6$, либо $b - a = 5$. Получается четыре случая.

Но если заметить, что сумма и разность двух целых чисел всегда имеют одинаковую чётность (так как в сумме дают $2b$ – чётное число), то возможны лишь два варианта:

$a + b$	$b - a$	a	b
6	-6	$\frac{6 - (-6)}{2} = 6$	$\frac{6 + (-6)}{2} = 0$
15	5	$\frac{15 - 5}{2} = 5$	$\frac{15 + 5}{2} = 10$

Здесь мы воспользовались тем, что

$$a = \frac{(a + b) - (b - a)}{2}, \quad b = \frac{(a + b) + (b - a)}{2}.$$

Осталось заметить, что второй случай невозможен, так как цифра a не может быть равна 10. В итоге получаем¹, что $a = 6$ и $b = 0$.

107. Заметим, что $2^{4n} = (2^4)^n = 16^n$ и

$$16 \equiv 1 \pmod{15}.$$

¹Можно было бы сразу воспользоваться признаком делимости на 99 (см. стр. 182). Тогда, после несложных преобразований, мы получили бы, что число $(\overline{a1} + \overline{4b} - 2)$ делится на 99. При этом оно явно положительное и меньше, чем 198. Значит, $\overline{a1} + \overline{4b} - 2 = 99$. То есть $\overline{a1} + \overline{4b} = 101$. Откуда получаем, что $b = 0$ и $a = 6$.

Значит,

$$16^n \equiv 1^n = 1 \pmod{15}.$$

Поэтому разность $(16^n - 1)$ делится на 15.

108. Так как $13 \equiv 3 \pmod{10}$, то

$$13^n \equiv 3^n \pmod{10}.$$

Значит,

$$\begin{aligned} 13^n + 3^{n+2} &\stackrel{10}{\equiv} 3^n + 3^2 \cdot 3^n = 3^n + 9 \cdot 3^n = \\ &= 10 \cdot 3^n \equiv 0 \cdot 3^n = 0 \pmod{10}. \end{aligned}$$

То есть у числа $(13^n + 3^{n+2})$ такой же остаток при делении на 10, как и у нуля. А значит, оно делится на 10.

109. Так как n чётное число, то оно равно $2k$, где k – натуральное. Тогда

$$7^n = 7^{2k} = (7^2)^k = 49^k \equiv 1^k = 1 \pmod{12}.$$

Поэтому при всех чётных натуральных n разность $(7^n - 1)$ делится на 12.

110. **Первое решение.** Так как n – нечётное число, то оно равно $(2k + 1)$, где k – целое неотрицательное. Тогда

$$\begin{aligned} 5^n &= 5^{2k+1} = 5 \cdot 5^{2k} = 5 \cdot (5^2)^k = \\ &= 5 \cdot 25^k \equiv 5 \cdot 4^k \pmod{7}; \\ 2^n &= 2^{2k+1} = 2 \cdot 2^{2k} = 2 \cdot 4^k. \end{aligned}$$

Значит,

$$5^n + 2^n \stackrel{7}{\equiv} 5 \cdot 4^k + 2 \cdot 4^k = 7 \cdot 4^k \equiv 0 \cdot 4^k = 0 \pmod{7}.$$

То есть при всех нечётных натуральных n число $(5^n + 2^n)$ делится на 7.

Второе решение. Заметим, что

$$5^n \equiv (-2)^n \pmod{7}.$$

А учитывая нечётность числа n , получаем, что

$$(-2)^n \equiv -2^n \pmod{7}.$$

Поэтому

$$5^n + 2^n \equiv -2^n + 2^n = 0 \pmod{7}.$$

То есть при всех нечётных натуральных n число $(5^n + 2^n)$ делится на 7.

111. Так как $n + 2 = (2n + 2) - n$, то

$$n + 2 \equiv -n \pmod{2n + 2}.$$

И учитывая то, что n – нечётное число, получаем, что

$$(n + 2)^n \equiv (-n)^n = -n^n \pmod{2n + 2}.$$

Таким образом,

$$n^{n+2} + (n + 2)^n \equiv n^{n+2} - n^n = n^n(n^2 - 1) \pmod{2n + 2}.$$

Значит, если мы покажем, что $n^n(n^2 - 1)$ делится на $(2n + 2)$, то и $(n^{n+2} + (n + 2)^n)$ делится на $(2n + 2)$. Но

$$n^2 - 1 = (n - 1)(n + 1).$$

А так как число n – нечётное, то число $(n - 1)$ – чётное. Поэтому произведение $(n - 1)(n + 1)$ делится на

$2(n+1) = 2n+2$. Откуда следует, что при всех нечётных натуральных n число $(n^{n+2} + (n+2)^n)$ делится на $(2n+2)$.

123. Если натуральное число меньше pq и не взаимно просто с ним, то оно либо делится на p , либо делится на q . При этом чисел, кратных p , всего $(q-1)$:

$$p, \quad 2p, \quad 3p, \quad \dots, \quad (q-1)p.$$

А чисел, кратных q , всего $(p-1)$:

$$q, \quad 2q, \quad 3q, \quad \dots, \quad (p-1)q.$$

Поэтому количество натуральных чисел, меньших pq и взаимно простых с pq , всего

$$\begin{aligned} (pq-1) - (q-1) - (p-1) &= \\ &= pq - q - p + 1 = (p-1)(q-1). \end{aligned}$$

125. **Ответ.** а) можно; б) нельзя.

а) Попробуем сделать так, чтобы суммы были маленькими простыми числами. Сделаем в первом и втором столбце суммы 2 и 3:

1	1	
1	2	

Попробуем сделать сумму в первой строке, равную 5:

1	1	3
1	2	

Но тогда для любого числа в последней ячейке сумма в последней строке будет равна сумме в последнем столбце. А они должны быть различными.

Тогда попробуем сделать сумму в первой строке, равную 7:

1	1	5
1	2	

Осталось подобрать такое число x , что и $(1 + 2 + x)$, и $(5 + x)$ оказались простыми числами. Например, их можно сделать 11 и 13:

1	1	5
1	2	8

И итоге суммы по строкам и по столбцам равны пяти различным простым числам – 2, 3, 7, 11 и 13. А значит, таблицу 2×3 можно заполнить требуемым образом.

б) Если попробовать повторить рассуждения из предыдущего пункта, то почему-то ничего не получается. Давайте поймём почему.

Предположим, что нам удалось расставить числа в таблице требуемым образом. Тогда каждая из получившихся сумм окажется больше, чем 2 (потому что мы складываем три или четыре натуральных числа). Поэтому все соответствующие суммы должны быть нечётными, так как они простые и больше, чем 2.

Давайте поймём, что мы уже знаем про нашу таблицу. С одной стороны, суммы чисел в каждой из трёх строк – нечётны. Тогда сумма чисел во всей таблице – это сумма трёх нечётных чисел, нечётное

число. С другой стороны, суммы чисел в каждом из четырёх столбцов нечётны. Но тогда сумма чисел во всей таблице – это сумма четырёх нечётных чисел, чётное число.

То есть, предположив, что нам удалось заполнить таблицу, мы пришли к выводу, что сумма всех чисел в таблице должна быть одновременно чётной и нечётной. А это невозможно. Значит, таблицу 3×4 нельзя заполнить требуемым образом.

126. Ответ. 4.

Пусть мы выбрали n двузначных составных чисел, удовлетворяющих условию. Посмотрим на наименьший простой делитель каждого из них. Это n различных простых чисел (иначе не любые два из выбранных чисел будут взаимно просты), и все они меньше 11 (иначе составное число будет не меньше, чем $11^2 = 121$, и не будет двузначным).

Различных простых чисел, которые меньше, чем 11, всего четыре – 2, 3, 5 и 7. Поэтому $n \leq 4$. Приведём пример для $n = 4$:

$$2 \cdot 19 = 38, \quad 3 \cdot 17 = 51, \quad 5 \cdot 13 = 65, \quad 7 \cdot 11 = 77.$$

Поэтому четыре – это наибольшее количество двузначных составных чисел, любые два из которых взаимно просты.

127. Ответ. 10.

Для начала давайте поймём, почему n не может быть очень большим. Действительно, если $n > 7$, то в качестве числа p можно будет взять числа 3, 5 и 7. И тогда числа $(n - 7)$, $(n - 5)$ и $(n - 3)$ должны быть простыми. Но эти три числа идут с «шагом» 2, а мы

знаем (см. задачу 27 на стр. 78), что есть только одна тройка простых чисел с таким свойством – (3; 5; 7). Поэтому, если $n - 7 > 3$, то числа $(n - 7)$, $(n - 5)$ и $(n - 3)$ не могут быть простыми одновременно. Значит, $n \leq 10$.

Пусть $n = 10$. Тогда в качестве такого простого числа p , что $2 < p < n$, можно взять только числа 3, 5 и 7. Но тогда $(n - p)$ будет 7, 5 и 3 соответственно. А значит, при $n = 10$ условие задачи выполнено.

В итоге мы доказали, что при $n > 10$ условие выполнено быть не может, и показали, что при $n = 10$ оно выполнено. Значит, 10 – наибольшее натуральное n , для которого верно наше утверждение.

128. Ответ. 6.

Из теоремы о количестве делителей мы знаем, что количество делителей числа

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m}$$

равно $(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$. При этом число n делится на $1001 = 7 \cdot 11 \cdot 13$, а значит, среди простых делителей числа n точно есть 7, 11 и 13. Поэтому $m \geq 3$.

Но из условия задачи следует, что произведение $(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 1001$, а 1001 нельзя разложить в произведение больше чем трёх множителей, отличных от единицы. А на три множителя можно разложить лишь единственным способом – $1001 = 7 \cdot 11 \cdot 13$. Следовательно, $m = 3$, а числа k_1 , k_2 и k_3 , – это 6, 10 и 12 в некотором порядке.

Итак, мы поняли, что число $n = p_1^6 \cdot p_2^{10} \cdot p_3^{12}$, где $(p_1; p_2; p_3)$ – некоторая перестановка тройки чисел

(7; 11; 13). То есть n – это одно из следующих чисел:

$$7^6 \cdot 11^{10} \cdot 13^{12}; \quad 11^6 \cdot 7^{10} \cdot 13^{12}; \quad 13^6 \cdot 7^{10} \cdot 11^{12}; \\ 7^6 \cdot 13^{10} \cdot 11^{12}; \quad 11^6 \cdot 13^{10} \cdot 7^{12}; \quad 13^6 \cdot 11^{10} \cdot 7^{12}.$$

Поэтому существует шесть натуральных чисел, делящихся на 1001 и имеющих ровно 1001 различных делитель.

129. **Ответ.** 2519.

Пусть число n удовлетворяет условию. Тогда число $(n + 1)$ делится на 2, на 3, на 4, на 5, на 6, на 7, на 8, на 9 и на 10. Учитывая то, какие разложения на простые множители у этих чисел:

$$\begin{array}{lll} 2 = 2, & 3 = 3, & 4 = 2^2, \\ 5 = 5, & 6 = 2 \cdot 3, & 7 = 7, \\ 8 = 2^3, & 9 = 3^2, & 10 = 2 \cdot 5, \end{array}$$

мы понимаем, что число $(n + 1)$ должно делиться на

$$2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520.$$

Наименьшее число, кратное 2520, – это само число 2520. Поэтому наименьшее значение $n + 1 = 2520$, то есть наименьшее $n = 2519$.

130. **Ответ.** Нельзя.

Пусть $a = 2k + 1$ – некоторое нечётное число. Тогда

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Заметим, что $k(k + 1)$ – произведение двух соседних целых чисел, одно из которых должно быть чётным. Значит, число $k(k + 1)$ делится на 2. Поэтому число $4k(k + 1)$ делится на 8.

В итоге мы доказали, что квадрат нечётного числа всегда при делении на 8 даёт остаток 1. Поэтому сумма четырёх квадратов нечётных чисел при делении на 8 будет давать остаток 4.

Но число $2024 = 8 \cdot 253$ делится на 8, а значит, не может быть представлено в виде суммы четырёх квадратов нечётных чисел.

131. Ответ. Не является.

Заметим, что

$$\begin{aligned} 4^{99} + 6^{100} + 3^{200} &= \left(2^{99}\right)^2 + 2 \cdot 2^{99} \cdot 3^{100} + \left(3^{100}\right)^2 = \\ &= \left(2^{99} + 3^{100}\right)^2. \end{aligned}$$

Поэтому число $(4^{99} + 6^{100} + 3^{200})$ является квадратом числа, большего единицы, а значит, составным числом.

132. Ответ. 1102.

Так как сумма трёх натуральных чисел чётна, то они не могут быть все нечётными. Но единственное чётное простое число – это 2. Значит, одно из наших чисел равно 2. Пусть, например, $r = 2$.

Тогда условие принимает вид:

$$\begin{cases} p + q + 2 = 50; \\ pq + 2p + 2q = 647. \end{cases}$$

То есть

$$\begin{cases} p + q = 48; \\ pq + 2(p + q) = 647. \end{cases}$$

Откуда получаем, что

$$pq = 647 - 2(p + q) = 647 - 2 \cdot 48 = 647 - 96 = 551.$$

Но тогда¹ $pqr = 551 \cdot 2 = 1102$.

133. **Ответ.** $m = n = 1000$.

Пусть $d = \text{НОД}(m; n)$. Тогда $m = ad$, $n = bd$, где a и b – взаимно простые числа.

Мы знаем, что $(m^2 + n^2)$ делится на mn , поэтому $(a^2 + b^2) \cdot d^2$ делится на abd^2 . Значит, $(a^2 + b^2)$ делится на ab .

Но числа $(a^2 + b^2)$ и ab взаимно простые. Действительно, если ab делится на простое число p , то в силу взаимной простоты чисел a и b лишь одно из них делится на p . Поэтому сумма $(a^2 + b^2)$ на p не делится.

Поэтому $(a^2 + b^2)$ может делиться на ab , только если $ab = 1$. Значит, $a = b = 1$. Следовательно, $m = n$. А учитывая то, что $mn = 1\,000\,000$, получаем единственную возможную пару – $m = n = 1000$.

134. **Ответ.** 4.

Если несколько последовательных чисел лежат в одном десятке, то они отличаются лишь последней цифрой и суммы их цифр будут тоже последовательными числами.

Из пяти последовательных чисел не меньше трёх попадёт в один десяток, и суммы их цифр будут последовательными числами, а трёх последовательных простых чисел не существует. Значит, все пять чисел не могут оказаться отмеченными.

Попробуем придумать пять подряд идущих на-

¹Если разложить на простые множители число $551 = 19 \cdot 29$, то можно в явном виде указать единственную тройку простых чисел, удовлетворяющую условию, – $\{2; 19; 29\}$.

натуральных чисел, среди которых будет четыре отмеченных. Легко понять, что среди сумм цифр будет как минимум две чётные, хотя бы одна из них должна оказаться простой, а значит, равной 2. Перебрав небольшие числа с суммой цифр 2 – это 2, 11, 20, 101, 110, 200, замечаем, что у пяти чисел 199, 200, 201, 202 и 203 суммы цифр равны 19, 2, 3, 4 и 5. Поэтому числа 199, 200, 201 и 203 отмечены.

В итоге мы доказали, что все пять подряд идущих натуральных чисел отмеченными быть не могут, и привели пример, когда из пяти чисел четыре будут отмечены. Значит, четыре – наибольшее возможное количество отмеченных чисел среди пяти подряд идущих натуральных.

135. Рассмотрим p чисел:

$$1, \quad 11, \quad 111, \quad \dots, \quad \underbrace{111 \dots 11}_p.$$

p единиц

Предположим, что ни одно из них не делится на p . Тогда у каждого из них есть какой-то ненулевой остаток при делении на p . Но таких остатков всего $(p - 1)$, а чисел p . Значит, есть два числа с одинаковыми остатками и их разность делится на p .

Если вычесть из большего числа меньшее, то получится число вида

$$111 \dots 11000 \dots 00.$$

И оно делится на p .

Представим эту разность в виде

$$111 \dots 11 \cdot 10^k.$$

Так как простое число $p > 5$, то 10^k не делится на p . Значит, число $111 \dots 11$ делится на p . И мы получили¹, что в любом случае среди чисел

$$1, \quad 11, \quad 111, \quad \dots, \quad \underbrace{111 \dots 11}_{p \text{ единиц}}$$

есть число, которое делится на p .

136. **Ответ.** 28.

Пусть a и b – натуральные числа, такие, что

$$a^2 = 4n + 9, \quad b^2 = 9n + 4.$$

Тогда

$$9a^2 = 36n + 81, \quad 4b^2 = 36n + 16.$$

Поэтому $9a^2 - 4b^2 = 65$.

Таким образом, $(3a - 2b)(3a + 2b) = 5 \cdot 13$. А так как второй множитель положительный и произведение положительно, то и первый множитель положителен. При этом он меньше, чем второй. Поэтому есть лишь два случая:

$3a - 2b$	$3a + 2b$	Решение
1	65	$6a = 66 \Rightarrow a = 11 \Rightarrow b = 16$
5	13	$6a = 18 \Rightarrow a = 3 \Rightarrow b = 2$

Если $4n + 9 = a^2 = 121$ и $9n + 4 = b^2 = 256$, то

$$n = \frac{121 - 9}{4} = \frac{256 - 4}{9} = 28.$$

¹Заметим, что в этом доказательстве нам не важна простота числа p . Достаточно потребовать, чтобы натуральное число p было взаимно просто с 10, то есть не содержало ни 2, ни 5 в разложении на простые множители.

Если же $4n + 9 = a^2 = 9$ и $9n + 4 = b^2 = 4$, то $n = 0$. Но по условию число n должно быть натуральным. Значит, этот случай нам не подходит.

В итоге получаем, что есть единственное решение при $n = 28$.

137. Малая теорема Ферма утверждает, что

$$n^{p-1} \equiv 1 \pmod{p}.$$

Поэтому в качестве числа m можно взять n^{p-2} . Тогда

$$mn = n^{p-1} \equiv 1 \pmod{p}.$$

138. **Ответ.** Не может.

Предположим, что $q = \frac{p_1 + p_2 + \dots + p_n}{n}$ – простое число. Так как в числителе n слагаемых, каждое из которых, начиная со второго, больше, чем 2, то $q > 2$. Значит, q – нечётное число. При этом

$$nq = p_1 + p_2 + \dots + p_n.$$

Если n – чётное число, то nq – чётное. Но в сумме $(p_1 + p_2 + \dots + p_n)$ лишь одно чётное слагаемое $p_1 = 2$, а остальные $(n-1)$ слагаемых – нечётные числа. Это означает, что в сумме $(p_1 + p_2 + \dots + p_n)$ присутствует нечётное количество нечётных слагаемых. То есть эта сумма нечётна. Это невозможно, потому что она равна чётному числу nq .

Если же n – нечётное число, то nq – произведение двух нечётных и поэтому является нечётным числом. Тогда в сумме $(p_1 + p_2 + \dots + p_n)$ одно чётное слагаемое и $(n-1)$ нечётных слагаемых, то есть

в ней чётное количество нечётных слагаемых. Значит, эта сумма чётна. Но это невозможно, потому что она равна нечётному числу nq .

Таким образом, при каком-нибудь $n > 1$ среднее арифметическое $\frac{p_1 + p_2 + \dots + p_n}{n}$ не может оказаться простым числом.

139. Пусть $m = n^2 - n + 1$. Тогда

$$n - 1 = n^2 - m \equiv n^2 \pmod{m}.$$

Поэтому

$$\begin{aligned} (n - 1)^{k+2} &= (n - 1)^2 \cdot (n - 1)^k \equiv \\ &\equiv (n - 1)^2 \cdot (n^2)^k = (n - 1)^2 \cdot n^{2k} \pmod{m}. \end{aligned}$$

Значит,

$$\begin{aligned} n^{2k+1} + (n - 1)^{k+2} &\stackrel{m}{\equiv} n^{2k+1} + (n - 1)^2 \cdot n^{2k} = \\ &= n^{2k} \cdot (n + (n - 1)^2) = \\ &= n^{2k} \cdot (n + n^2 - 2n + 1) = \\ &= n^{2k} \cdot (n^2 - n + 1) = \\ &= n^{2k} \cdot m \equiv 0 \pmod{m}. \end{aligned}$$

Поэтому при любых натуральных n и k число $(n^{2k+1} + (n - 1)^{k+2})$ делится на $n^2 - n + 1$.

140. **Ответ.** 251.

Пусть выбрано некоторое натуральное число n . Тогда числа $(n + 2)$, $(n + 3)$, $(n + 5)$, $(n + 7)$ взять уже нельзя, потому что они отличаются от n на простые числа.

То есть, если мы взяли число n , то из следующих семи чисел мы можем выбрать только среди чисел $(n+1)$, $(n+4)$, $(n+6)$. Но любые два из них отличаются на 2, 3 или 5. Поэтому из этих трёх чисел мы сможем взять не больше одного.

В итоге мы поняли, что если выбрано некоторое число, то из следующих семи чисел мы сможем выбрать не более одного. Это означает, что из любых восьми подряд идущих чисел мы можем выбрать не более двух. То есть из чисел от 1 до 8 выбрали не больше двух, из чисел от 9 до 16 выбрали не больше двух, ..., из чисел от 985 до 992 выбрали не больше двух, из чисел от 993 до 1000 выбрали не больше двух.

Числа от 1 до 1000 разбиваются на $\frac{1000}{8} = 125$ восьмёрок подряд идущих чисел, в каждой из которых мы можем взять не более двух чисел. И остаётся ещё число 1001. Итого, можно выбрать не более чем $2 \cdot 125 + 1 = 251$ число.

Если же выбрать числа 1, 5, 9, ..., 993, 997, 1001 (то есть все числа вида $(4k + 1)$, где k меняется от 0 до 250), то разность между любыми двумя будет кратна 4, а значит, не является простым числом.

В итоге мы доказали, что больше 251 числа выбрать нельзя, и привели пример 251 числа, которые выбрать можно. Значит, 251 – это наибольшее количество чисел, которое можно выбрать из набора $\{1; 2; 3; \dots; 1001\}$ так, что разность любых двух выбранных чисел не является простым числом.

141. Рассмотрим число $(n! - 1)$. Если оно простое, то мы нашли число, которое удовлетворяет условию. Если же оно составное, то оно делится на

какое-то простое число p .

Но $n!$ делится на 2, поэтому число $(n! - 1)$ на 1 отличается от числа, кратного двум, а значит, не делится на 2. Аналогично рассуждаем дальше: $n!$ делится на 3, поэтому число $(n! - 1)$ на 1 отличается от числа, кратного трём, а значит, не делится на 3 и так далее.

Значит, число $(n! - 1)$ не делится на 2, 3, ..., n , и при этом оно делится на простое число p . Значит, $n < p < n!$. Таким образом, между числами n и $n!$ есть по крайней мере одно простое число.

142. Ответ. Существует.

Посмотрим на миллион чисел от 1 до 1 000 000. Там довольно много простых чисел. Сложно посчитать, сколько именно, но явно больше десяти – там есть 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, а это уже больше десяти.

Потом посмотрим на миллион чисел от 2 до 1 000 001. Потом на миллион чисел от 3 до 1 000 002. И так далее. Обозначим через n_k количество простых чисел среди миллиона последовательных чисел от k до $(999\,999\,999 + k)$:

миллион чисел	количество простых
от 1 до 1 000 000	n_1
от 2 до 1 000 001	n_2
от 3 до 1 000 002	n_3
от 4 до 1 000 003	n_4
...	
от k до $(999\,999\,999 + k)$	n_k
...	

Давайте поймем, на сколько могут отличаться

значения соседних n_k и n_{k+1} . При переходе от набора чисел $\{ \text{от } k \text{ до } (999\,999\,999+k) \}$ к набору $\{ \text{от } (k+1) \text{ до } (1\,000\,000\,000+k) \}$ мы убираем число k и добавляем число $(1\,000\,000\,000+k)$. Количество простых чисел в наборе при этом не может измениться больше чем на один – мы убрали ноль или одно простое число и добавили ноль или одно простое число.

Таким образом, значение n_{k+1} может быть равно $(n_k - 1)$, n_k или $(n_k + 1)$. При этом $n_1 > 10$, а для некоторого m , как мы знаем¹, $n_m = 0$.

Но мы показали, что при переходе от n_1 к n_2 , от n_2 к n_3 , от n_3 к n_4 , ..., от n_{m-1} к n_m значение меняется не больше чем на 1. Поэтому, если это значение изменилось с $n_1 > 10$ до $n_m = 0$, то где-то между ними было $n_\ell = 10$.

Таким образом, существуют миллион последовательных натуральных чисел, среди которых ровно десять простых чисел.

143. **Ответ.** $p = 2$, $q = 11$ или $q = 2$, $p = 11$.

Так как $5p + 1$ делится на q , а $5q + 1$ делится на p , то произведение

$$(5p + 1)(5q + 1) = 25pq + 5p + 5q + 1$$

делится на pq . Тогда и число $(5p + 5q + 1)$ делится на pq , а значит, $5p + 5q + 1 \geq pq$.

Условия задачи симметричны, поэтому можно считать, что, например, $q \leq p$. Тогда

$$pq \leq 5p + 5q + 1 \leq 10p + 1 < 11p.$$

Отсюда следует, что $q < 11$. Поэтому q может быть равно только 2, 3, 5 или 7.

¹ Например, при $m = 1\,000\,000\,001! + 2$ (см. задачу 26 на стр. 76).

Пусть $q = 2$, тогда p – простой делитель числа

$$5q + 1 = 5 \cdot 2 + 1 = 11.$$

То есть $p = 11$. И при этом действительно

$$5p + 1 = 5 \cdot 11 + 1 = 56$$

делится на $q = 2$.

Пусть $q = 3$, тогда p – простой делитель числа

$$5q + 1 = 5 \cdot 3 + 1 = 16.$$

То есть $p = 2 < q$, а мы рассматриваем случай, когда $p \geq q$.

Пусть $q = 5$, тогда p – простой делитель числа

$$5q + 1 = 5 \cdot 5 + 1 = 26.$$

Учитывая то, что $p \geq q$, получаем, что $p = 13$. Но

$$5p + 1 = 5 \cdot 13 + 1 = 66$$

не делится на $q = 5$.

Пусть $q = 7$, тогда p – простой делитель числа

$$5q + 1 = 5 \cdot 7 + 1 = 36.$$

Но все простые делители числа 36 – это числа 2 и 3, меньше 7, а мы рассматриваем случай, когда $p \geq q$.

В итоге, предположив, что $q \leq p$, мы получили единственное решение: $q = 2$ и $p = 11$. Если же $q \geq p$, то есть ещё решение: $p = 2$ и $q = 11$.

144. **Ответ.** $m = 5, n = 2$.

Пусть $n \geq 5$, тогда $n!$ делится на 5. Поэтому

$$m^2 = n! + 5n + 13 \equiv 3 \pmod{5}.$$

Посмотрим, какие остатки бывают у квадратов при делении на 5:

m	m^2
0	$0^2 = 0$
1	$1^2 = 1$
2	$2^2 = 4$
3	$3^2 = 9 \equiv 4$
4	$4^2 = 16 \equiv 1$

То есть остаток при делении на 5 у квадрата не может быть равен 3.

Значит, $n < 5$. Переберём все возможные значения n .

Пусть $n = 1$, тогда

$$m^2 = 1! + 5 \cdot 1 + 13 = 1 + 5 + 13 = 18$$

– не квадрат.

Пусть $n = 2$, тогда

$$m^2 = 2! + 5 \cdot 2 + 13 = 2 + 10 + 13 = 25 = 5^2.$$

Пусть $n = 3$, тогда

$$m^2 = 3! + 5 \cdot 3 + 13 = 6 + 15 + 13 = 34$$

– не квадрат.

Пусть $n = 4$, тогда

$$m^2 = 4! + 5 \cdot 4 + 13 = 24 + 20 + 13 = 57$$

– не квадрат.

Получили единственное решение $m = 5, n = 2$.

145. **Ответ.** 25 или 49.

Так как в условии

$$k_2 \cdot k_3 \cdot k_8 \cdot k_9 > n^2$$

фигурирует k_9 , то делителей у числа n не меньше девяти. То есть $m \geq 9$.

С другой стороны, мы знаем, что делители разбиваются на пары, произведения в которых равны n , поэтому

$$k_1 k_m = k_2 k_{m-1} = k_3 k_{m-2} = \dots = n.$$

То есть

$$k_2 \cdot k_3 \cdot k_{m-2} \cdot k_{m-1} = n^2,$$

но

$$k_2 \cdot k_3 \cdot k_8 \cdot k_9 > n^2.$$

Поэтому $m - 2 < 8$, так как иначе

$$n^2 = k_2 \cdot k_3 \cdot k_{m-2} \cdot k_{m-1} \geq k_2 \cdot k_3 \cdot k_8 \cdot k_9 > n^2,$$

что невозможно. В итоге получаем, что $9 \leq m < 10$. Поэтому $m = 9$.

Из теоремы о количестве делителей мы понимаем, что у числа может быть ровно девять делителей, когда оно имеет вид $n = p^8$ или $n = p^2 q^2$, где p и q – различные простые числа. Тогда $n^3 = p^{24}$ или $n^3 = p^6 q^6$, а значит, количество делителей числа n^3 равно $24 + 1 = 25$ или $(6 + 1) \cdot (6 + 1) = 49$.

146. **Ответ.** 1806.

Пусть число n удовлетворяет этому условию. Так как натуральное число n точно делится на 1, то оно должно делиться и на простое число 2. Так как n

делится на 2, то оно должно делиться и на простое число 3.

Итак, мы уже знаем, что число n делится на $2 \cdot 3 = 6$. Но тогда оно делится и на простое число 7. То есть число n точно делится на $2 \cdot 3 \cdot 7 = 42$. Но тогда оно делится и на простое число 43. Поэтому число n делится на $2 \cdot 3 \cdot 7 \cdot 43 = 1806$.

Таким образом, наименьшее n , удовлетворяющее условию (если, конечно, такое число вообще существует), не меньше, чем 1806. Проверим, подходит ли само число 1806.

Выпишем все делители числа $1806 = 2 \cdot 3 \cdot 7 \cdot 43$:

1, 2, 3, 6, 7, 14, 21, 42, 43, 86,

129, 258, 301, 602, 903, 1806.

Увеличим каждый из них на единицу:

2, 3, 4, 7, 8, 15, 22, 43, 44, 87,

130, 259, 302, 603, 904, 1807.

И выкинем те, которые не являются простыми:

$$4 = 2^2,$$

$$8 = 2^3,$$

$$15 = 3 \cdot 5,$$

$$22 = 2 \cdot 11,$$

$$44 = 2^2 \cdot 11,$$

$$87 = 3 \cdot 29,$$

$$130 = 2 \cdot 5 \cdot 13,$$

$$259 = 7 \cdot 37,$$

$$302 = 2 \cdot 151,$$

$$603 = 3^2 \cdot 67,$$

$$904 = 2^3 \cdot 113,$$

$$1807 = 13 \cdot 139.$$

И остались только простые числа 2, 3, 7 и 43, на которые число 1806 делится. То есть действительно, если p – простое число и число 1806 делится на $(p - 1)$, то оно делится и на p .

147. Рассмотрим остатки при делении чисел a_1, a_2, \dots, a_{11} на 11. Все эти числа простые, и все они больше 11, поэтому ни одно из них не делится на 11. А значит, у каждого из них может быть один из десяти возможных остатков – 1, 2, ..., 10. Но у нас 11 членов прогрессии.

Значит, при некоторых $m > n$ два члена a_m и a_n прогрессии дают одинаковые остатки при делении на 11. Поэтому их разность делится на 11.

Но разность этих членов имеет вид

$$a_m - a_n = (m - n)d,$$

где d – разность прогрессии. При этом $(m - n)$ меньше 11 и не может делиться на 11. Поэтому d делится на 11.

Рассмотрим теперь остатки при делении чисел a_1, a_2, \dots, a_7 на 7. Все эти числа простые, и все они больше 11, поэтому ни одно из них не делится на 7. А значит, у каждого из них может быть один из шести возможных остатков – 1, 2, ..., 6. Но у нас здесь 7 членов прогрессии.

Значит, при некоторых $k > \ell$ два a_k и a_ℓ из первых семи членов прогрессии дают одинаковые остатки при делении на 7. Поэтому их разность делится на 7.

Но разность этих членов имеет вид

$$a_k - a_\ell = (k - \ell)d.$$

При этом $(k - \ell)$ меньше 7 и не может делиться на 7. Поэтому d делится на 7.

Аналогично рассуждая, получим, что разность прогрессии делится на 5, на 3 и на 2. Поэтому она

делится на

$$11 \cdot 7 \cdot 5 \cdot 3 \cdot 2 = 2310.$$

Таким образом, мы доказали¹, что если 11 простых чисел образуют арифметическую прогрессию, все члены которой больше 11, то разность прогрессии делится на 2310.

148. Предположим, что их конечное количество. Пусть

$$p_1 = 3, \quad p_2 = 7, \quad p_3 = 11, \quad p_4 = 19, \quad \dots, \quad p_n$$

– все простые, дающие остаток 3 при делении на 4.

Рассмотрим число

$$N = 4p_2p_3p_4 \dots p_n + 3.$$

Оно даёт остаток 3 при делении на 4 и больше любого из простых чисел, дающих остаток 3 при делении на 4. Значит, оно составное.

Кроме того, оно нечётное и не делится ни на одно из простых $p_2, p_3, p_4, \dots, p_n$. На $p_1 = 3$ оно тоже не делится, потому что $4p_2p_3p_4 \dots p_n$ не делится на 3. Поэтому все его простые делители – нечётные числа, дающие остаток 1 при делении на 4.

¹Важно отметить, что мы лишь доказали то, что если такая последовательность есть, то разность прогрессии должна делиться на 2310. Из нашего доказательства никак не следует, что такая последовательность существует.

Но такая прогрессия действительно есть. Например,

$$110\,437, \quad 124\,297, \quad 138\,157, \quad 152\,017, \quad 165\,877, \quad 179\,737, \\ 193\,597, \quad 207\,457, \quad 221\,317, \quad 235\,177, \quad 249\,037.$$

Более того, даже следующий член прогрессии – 262 897 – тоже будет простым числом.

Видно, что разность этой прогрессии равна $13860 = 2310 \cdot 6$.

Но произведение любого количества чисел, дающих остаток 1 при делении на 4, будет числом, дающим остаток 1 при делении на 4. А число N при делении на 4 даёт остаток 3. Пришли к противоречию!

Значит, существует бесконечно много простых чисел, дающих остаток 3 при делении на 4.

149. **Ответ.** (1; 3; 1) и (5; 6; 5).

Запишем данное равенство в виде

$$m! = 4 \cdot k! + 2 \cdot n!.$$

Пусть ℓ – большее из чисел k и n . Тогда $k \leq \ell$ и $n \leq \ell$, поэтому

$$m! \leq 6 \cdot \ell!,$$

и при этом $m > \ell$, так как из условия следует, что $m! > k!$ и $m! > n!$.

Таким образом, мы получаем, что

$$6 \cdot \ell! \geq m! \geq (\ell + 1)!.$$

Тогда

$$6 \cdot \ell! \geq (\ell + 1) \cdot \ell!.$$

То есть $\ell + 1 \leq 6$. Поэтому $\ell \leq 5$. Это означает, что

$$m! \leq 6 \cdot \ell! \leq 6 \cdot 5! = 6!.$$

Поэтому $m \leq 6$.

С другой стороны,

$$m! = 4 \cdot k! + 2 \cdot n! \geq 4 + 2 = 6 = 3!.$$

Поэтому $m \geq 3$.

Осталось перебрать все значения m от 3 до 6.

Пусть $m = 3$, тогда получаем, что

$$4 \cdot k! + 2 \cdot n! = 6.$$

То есть $k = n = 1$.

Пусть $m = 4$, тогда получаем, что

$$4 \cdot k! + 2 \cdot n! = 24.$$

Но тогда $k < 3$ и $n < 4$. Поэтому

$$4 \cdot k! + 2 \cdot n! \leq 4 \cdot 2! + 2 \cdot 3! = 20 < 24.$$

Значит, этот случай невозможен.

Пусть $m = 5$, тогда получаем, что

$$4 \cdot k! + 2 \cdot n! = 120.$$

Но тогда $k < 5$ и $n < 5$. Если $k = n = 4$, то

$$4 \cdot k! + 2 \cdot n! = 6 \cdot 4! = 144 \neq 120.$$

Поэтому хотя бы одно из чисел k и n не превосходит трёх и

$$4 \cdot k! + 2 \cdot n! \leq 4 \cdot 4! + 2 \cdot 3! = 108 < 120.$$

Пусть $m = 6$, тогда получаем, что

$$4 \cdot k! + 2 \cdot n! = 720.$$

Но тогда $k < 6$ и $n < 6$. Поэтому

$$4 \cdot k! + 2 \cdot n! \leq 4 \cdot 5! + 2 \cdot 5! = 6 \cdot 5! = 720.$$

Значит, равенство возможно, только если $k = n = 5$.

В итоге получаем, что есть только две тройки решений – $(1; 3; 1)$ и $(5; 6; 5)$.

150. **Ответ.** Не могут.

Пусть нашёлся многочлен

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

удовлетворяющий условию.

Тогда значение $P(0) = a_0$ должно быть некоторым простым числом p . Поэтому $a_0 = p$. Посмотрим значения многочлена $P(x)$ при x равном $p, 2p, 3p, 4p, \dots$:

$$P(kp) = a_n (kp)^n + a_{n-1} (kp)^{n-1} + \dots + a_1 (kp) + p.$$

Получаем, что при любом натуральном k значение $P(kp)$ кратно p .

Но по условию все эти значения должны быть простыми. Значит, при любом натуральном k значение $P(kp) = p$. Это означает, что у уравнения n -й степени

$$P(x) - p = 0$$

бесконечно много корней.

Пришли к противоречию, а значит, не могут все значения $P(0), P(1), P(2), \dots$ оказаться простыми числами.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

алгоритм RSA	218
алгоритм Евклида	48
алгоритм нахождения НОД	48, 112
алгоритм нахождения НОК	115
алгоритм проверки числа на простоту	68
арабские цифры	17
арифметика остатков	171
ассоциативность	13
великая теорема Ферма	133
взаимно простые числа	46
двенадцатеричная система счисления	17, 180
деление в столбик	32
деление с остатком	30
делимость чисел	21
делитель	21
десятичная система счисления	17
диофантовы уравнения	133
дистрибутивность	15
знакопеременная сумма цифр	181
каноническое разложение на множители	110
количество делителей	120
коммутативность	12
кратное	21
критерий делимости на 2	41, 179
критерий делимости на 3	43, 180
критерий делимости на 4	179

критерий делимости на 5	179
критерий делимости на 7	183
критерий делимости на 8	42, 270
критерий делимости на 9	43, 180
критерий делимости на 10	41, 179
критерий делимости на 11	43, 181
критерий делимости на 13	183
критерий делимости на 16	270
критерий делимости на 20	179
критерий делимости на 25	179
критерий делимости на 27	183
критерий делимости на 33	182
критерий делимости на 37	183
критерий делимости на 50	179
критерий делимости на 77	183
критерий делимости на 91	183
критерий делимости на 99	182
критерий делимости на 100	179
критерий делимости на 101	182
критерий делимости на 111	183
лемма Евклида	97
линейная комбинация	51
линейные диофантовы уравнения	135
малая теорема Ферма	192, 202, 204, 206
метод бесконечного спуска	154
метод неопределённых коэффициентов	157
наибольший общий делитель	45, 112
наименьшее общее кратное	113, 117
натуральные числа	11
неполное частное	32
нечётные числа	22
основная теорема арифметики	91
единственность разложения	99, 101
существование разложения	93

остаток	32, 166
переместительный закон умножения	12
признак делимости на 2	25, 41, 179
признак делимости на 3	29, 43, 180
признак делимости на 4	27, 179
признак делимости на 5	26, 179
признак делимости на 7	183
признак делимости на 8	27, 42, 270
признак делимости на 9	28, 43, 180
признак делимости на 10	25, 41, 179
признак делимости на 11	29, 43, 181
признак делимости на 13	183
признак делимости на 16	228, 270
признак делимости на 20	179, 227
признак делимости на 25	179, 227
признак делимости на 27	183
признак делимости на 33	182
признак делимости на 37	183
признак делимости на 50	179, 227
признак делимости на 77	183
признак делимости на 91	183
признак делимости на 99	182
признак делимости на 100	26, 179
признак делимости на 101	182
признак делимости на 111	183
принцип крайнего	152
простые числа	63
распределительный закон умножения	15
решето Эратосфена	71
самое большое известное простое число	65
самые большие известные числа-близнецы	79
свойства делимости	22
свойства наибольшего общего делителя	46
свойства сравнения по модулю	171

связь между НОД и НОК	115
соотношение Безу	51
составные числа	63
сочетательный закон умножения	13
сравнение по модулю	168
теорема Евклида	66
теорема Эйлера	210
теорема о количестве делителей	120
умножение	12
умножение в столбик	19
уравнение $Ax + By + C = Dxу$	141
уравнение $Ax + By = C$	135
уравнение Каталана	134
уравнение Пелля	134
уравнение Рамануджана – Нагеля	134
уравнения в целых числах	133
факториал	55, 76
функция Эйлера	210
целые числа	12
числа Евклида	67
числа-близнецы	78
чётные числа	22
шестидесятеричная система счисления	18
шестнадцатеричная система счисления	180
шифр RSA	218
шифр Цезаря	215
шифр подстановки	216

МАТЕМАТИКА С БОРИСОМ ТРУШИНЫМ

Трушин Борис Викторович

МАТЕМАТИКА С БОРИСОМ ТРУШИНЫМ
ТЕОРИЯ ЧИСЕЛ: С НУЛЯ ДО ТЕОРЕМЫ ЭЙЛЕРА

Главный редактор *Р. Фасхутдинов*
Руководитель направления *В. Обручев*
Ответственный редактор *Ю. Лаврова*
Художественный редактор *Е. Каменева*
Младший редактор *А. Клементьева*

Страна происхождения: Российская Федерация
Шығарылған елі: Ресей Федерациясы

ООО «Издательство «Эксмо»

123308, Россия, г. Москва, ул. Зорге, д. 1, стр. 1, эт. 20, каб. 2013. Тел.: 8 (495) 411-68-86.
Home page: www.eksmo.ru E-mail: info@eksmo.ru

Өндіруші: «Издательство «Эксмо» ЖШС

123308, Ресей, Мәскеу қаласы, Зорге көшесі, 1-үй, 1-құрылыс, 20 қабат, 2013-қаб.
Тел.: 8 (495) 411-68-86. Home page: www.eksmo.ru E-mail: info@eksmo.ru

Tayyar belgici: «Эксмо»

Интернет-магазин : www.book24.ru

Интернет-магазин : www.book24.kz

Интернет-дүкен : www.book24.kz

Импортёр в Республику Казахстан ТОО «РДЦ-Алматы».
Қазақстан Республикасында импорттаушы «РДЦ-Алматы» ЖШС.

Дистрибутор и представитель по приему претензий на продукцию
в Республике Казахстан: ТОО «РДЦ-Алматы»

Дистрибутор және Қазақстан Республикасында өнімге шағымдар
қабылдау жөніндегі өкіл: «РДЦ-Алматы» ЖШС.

Алматы қ., Домбровский көш., 3 «а», литер Б, офис 1.
Тел.: 8 (727) 251-59-90/91/92. E-mail: RDC-Almaty@eksmo.kz

Сведения о подтверждении соответствия издания согласно законодательству РФ
о техническом регулировании можно получить на сайте Издательства «Эксмо»:
www.eksmo.ru/certification

Техникалық реттеу туралы РФ заңнамасына сай басылымның сайкестігін растау
туралы мәліметтерді мына адрес бойынша алуға болады: <http://eksmo.ru/certification/>

Произведено в Российской Федерации

Ресей Федерациясында өндірілген

Сертификаттауға жатпайды

Дата изготовления / Подписано в печать 06.02.2024.
Формат 84x108¹/₃₂. Печать офсетная. Усл. печ. л. 15,96.
Тираж экз. Заказ

ISBN 978-5-04-179677-8



9 785041 796778 >

12+



ТЕРИТОРИЯ
КНИЖНЫЙ МАГАЗИН
Официальная франшиза
издательства «Эксмо»

Литрес

Я ТАК ЧИТАЮ

■ ЧИТАЙ · ГОРОД

Москва. ООО «Торговый Дом «Эксмо»

Адрес: 123308, г. Москва, ул. Зорге, д. 1, строение 1.

Телефон: +7 (495) 411-50-74. **E-mail:** reception@eksмо-sale.ru

По вопросам приобретения книг «Эксмо» зарубежными оптовыми покупателями обращаться в отдел зарубежных продаж ТД «Эксмо»
E-mail: international@eksмо-sale.ru

International Sales: International wholesale customers should contact Foreign Sales Department of Trading House «Eksmo» for their orders.
international@eksмо-sale.ru

По вопросам заказа книг корпоративным клиентам, в том числе в специальном оформлении, обращаться по тел.: +7 (495) 411-68-59, доб. 2151.

E-mail: borodkin.da@eksмо.ru

Оптовая торговля бумажно-беловыми

и канцелярскими товарами для школы и офиса «Канц-Эксмо»:

Компания «Канц-Эксмо»: 142702, Московская обл., Ленинский р-н, г. Видное-2, Белокаменное ш., д. 1, а/я 5. Тел./факс: +7 (495) 745-28-87 (многоканальный).
e-mail: kanc@eksмо-sale.ru, сайт: **www.kanc-eksмо.ru**

Филиал «Торгового Дома «Эксмо» в Нижнем Новгороде

Адрес: 603094, г. Нижний Новгород, улица Карпинского, д. 29, бизнес-парк «Грин Плаза»
Телефон: +7 (831) 216-15-91 (92, 93, 94). **E-mail: reception@eksmonn.ru**

Филиал ООО «Издательство «Эксмо» в г. Санкт-Петербурге

Адрес: 192029, г. Санкт-Петербург, пр. Обуховской обороны, д. 84, лит. «Е»
Телефон: +7 (812) 365-46-03 / 04. **E-mail: server@szko.ru**

Филиал ООО «Издательство «Эксмо» в г. Екатеринбург

Адрес: 620024, г. Екатеринбург, ул. Новинская, д. 2и
Телефон: +7 (343) 272-72-01 (02/03/04/05/06/08)

Филиал ООО «Издательство «Эксмо» в г. Самаре

Адрес: 443052, г. Самара, пр-т Кирова, д. 75/1, лит. «Е»
Телефон: +7 (846) 207-55-50. **E-mail: RDC-samara@mail.ru**

Филиал ООО «Издательство «Эксмо» в г. Ростове-на-Дону

Адрес: 344023, г. Ростов-на-Дону, ул. Страны Советов, 44А
Телефон: +7(863) 303-62-10. **E-mail: info@rnd.eksмо.ru**

Филиал ООО «Издательство «Эксмо» в г. Новосибирске

Адрес: 630015, г. Новосибирск, Комбинатский пер., д. 3
Телефон: +7(383) 289-91-42. **E-mail: eksмо-nsk@yandex.ru**

Обособленное подразделение в г. Хабаровске

Фактический адрес: 680000, г. Хабаровск, ул. Фрунзе, 22, оф. 703
Почтовый адрес: 680020, г. Хабаровск, А/Я 1006
Телефон: (4212) 910-120, 910-211. **E-mail: eksмо-khv@mail.ru**

Республика Беларусь: ООО «ЭКМО АСТ Си энд Си»

Центр оптово-розничных продаж Cash&Carry в г. Минск
Адрес: 220014, Республика Беларусь, г. Минск, проспект Жукова, 44, пом. 1-17, ТЦ «Outleto»
Телефон: +375 17 251-40-23; +375 44 581-81-92
Режим работы: с 10.00 до 22.00. **E-mail: exmoast@yandex.by**

Казахстан: «РДЦ Алматы»

Адрес: 050039, г. Алматы, ул. Домбровского, 3А
Телефон: +7 (727) 251-58-12, 251-59-90 (91, 92, 99). **E-mail: RDC-Almaty@eksмо.kz**

Полный ассортимент продукции ООО «Издательство «Эксмо» можно приобрести в книжных магазинах «Читай-город» и заказать в интернет-магазине: www.chitalai-gorod.ru.

Телефон единой справочной службы: 8 (800) 444-8-444. Звонок по России бесплатный.

Интернет-магазин ООО «Издательство «Эксмо»

www.eksмо.ru

Розничная продажа книг с доставкой по всему миру.

Тел.: +7 (495) 745-89-14. **E-mail: imarket@eksмо-sale.ru**



Хочешь стать
автором «Эксмо»?



eksмо.ru

Официальный
интернет-магазин
издательства «Эксмо»



ЭКМО

eksмо.ru

eksмо

Издательство «Эксмо» — универсальное
издательство №1 в России, является
одним из лидеров книжного рынка Европы.

БОРИС ТРУШИН ПОЧТИ 25 ЛЕТ ПРЕПОДАЕТ МАТЕМАТИКУ ШКОЛЬНИКАМ И СТУДЕНТАМ, ЯВЛЯЕТСЯ СОАВТОРОМ УЧЕБНИКОВ ПО АЛГЕБРЕ И УЖЕ 7 ЛЕТ ВЕДЕТ ОДНОИМЕННЫЙ YOUTUBE-КАНАЛ ПО ОКОЛОШКОЛЬНОЙ МАТЕМАТИКЕ.

В своих видеороликах Борис показывает красоту математики и учит не бояться сложных задач. И хотя большинство роликов рассчитаны на школьников и студентов, они привлекают и взрослых, которые осознали, что хотят начать разбираться в математике.

Самые интересные идеи и подходы из видеороликов Бориса доступны и в книгах, одну из которых вы держите в руках!

Вторая книга автора плавно погружает читателя в ТЕОРИЮ ЧИСЕЛ и позволяет освоить азы этого интересного раздела математики без каких-либо предварительных знаний. Задачи на теорию чисел часто встречаются на математических олимпиадах и даже в ЕГЭ. Вы пройдете увлекательный путь с самых азов: поймете откуда взялись свойства умножения и почему работает алгоритм деления в столбик, а завершите теоремой Эйлера. По дороге освоите алгоритм Евклида, основную теорему арифметики, линейные диофантовы уравнения и арифметику остатков.

ПРИЯТНОГО МАТЕМАТИЧЕСКОГО ПУТЕШЕСТВИЯ!

ISBN 978-5-04-179677-8



9 785041 796778 >

БОМБОРА
ИЗДАТЕЛЬСТВО

БОМБОРА – лидер на рынке полезных и вдохновляющих книг.
Мы любим книги и создаем их, чтобы вы могли творить, открывать мир, пробовать новое, расти. Быть счастливыми. Быть на волне.