Урок 3. Простые числа

Криптография · ~35 минут

Пора отвлечься от букв и заняться числами — потому что настоящая, современная криптография держится не на алфавитах, а на свойствах чисел. И главные герои здесь — простые числа, «атомы» арифметики, из которых собрано всё остальное.

🎯 Что ты узнаешь

- Что такое простое и составное число.
- Как быстро найти все простые до сотни (решето Эратосфена).
- Почему любое число раскладывается на простые единственным способом.
- Почему простых чисел бесконечно много (доказательство Евклида).
- Как вообще проверяют, простое ли число.

📖 Разбираемся в теме

Определение

Простое число — это натуральное число больше 1, которое делится только на 1 и на само себя. Первые простые: 2, 3, 5, 7, 11, 13, 17, 19, 23…

Число, у которого есть делители помимо 1 и себя, называется **составным**: 4 = 2·2, 6 = 2·3, 12 = 2·2·3.

> ⚠️ Число **1 не считается ни простым, ни составным**. Это не каприз — так удобно, чтобы разложение на множители было единственным (об этом ниже). А число **2** — единственное чётное простое.

Решето Эратосфена

Как найти все простые, скажем, до 30? Древнегреческий учёный Эратосфен придумал изящный способ — «просеивание».

1. Выпиши все числа от 2 до 30.
2. Первое невычеркнутое — 2. Оно простое. Вычеркни все числа, кратные 2 (4, 6, 8, …).
3. Следующее невычеркнутое — 3. Оно простое. Вычеркни кратные 3 (6, 9, 12, …).
4. Следующее — 5. Вычеркни кратные 5. Потом 7. И так далее.

```
2 3 · 5 · 7 · · · 11
13 · · · 17 · 19 · · · 23
· · · · 29

зелёным — уцелевшие простые
```

Простые до 30: **2, 3, 5, 7, 11, 13, 17, 19, 23, 29**.

> 💡 Полезная хитрость: вычёркивать кратные числа p можно начиная сразу с p·p. Все меньшие кратные (например, для 5 — это 10, 15, 20) уже вычеркнуты меньшими простыми. Поэтому просеивать до N достаточно простыми до $\sqrt{N}$.

Основная теорема арифметики

> 📌 **Запомни:** любое натуральное число больше 1 можно разложить в произведение простых, и притом **единственным способом** (с точностью до порядка сомножителей).

Например: $84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3 \cdot 7$. Другого набора простых, дающих 84, не существует. Именно поэтому простые называют

«атомами» чисел: как из атомов собраны все вещества, так из простых — все числа.

Простых бесконечно много (Евклид, ~300 г. до н.э.)

Это одно из самых красивых доказательств в математике. Оно идёт **от противного**.

Предположим, что простых **конечное** число, и мы выписали их все: $p_1, p_2, \dots, p_n$. Построим число

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1.$$

Теперь заметим: N при делении на любое из наших простых p_i даёт **остаток 1** (ведь произведение делилось нацело, а мы добавили единицу). Значит, ни одно из перечисленных простых не делит N.

Но у N обязан быть какой-то простой делитель (по основной теореме арифметики). Получается, существует простое, которого нет в нашем «полном» списке — противоречие! Значит, предположение неверно, и простых **бесконечно много**. ∎

> 🤔 **А знаешь ли ты?** Самое большое известное на сегодня простое число имеет более 41 миллиона цифр. Если его напечатать обычным шрифтом, лента растянется на тысячи километров. И всё равно — впереди бесконечность ещё бóльших простых.

Как проверяют простоту

Самый простой способ проверить, простое ли число n, — делить его на 2, 3, 5, 7, … Причём проверять делители нужно только **до $\sqrt{n}$**: если бы у n был делитель больше корня, то в паре к нему шёл бы делитель меньше корня, и мы бы его уже нашли.

Пример: простое ли 97? $\sqrt{97} \approx 9{,}8$. Проверяем делимость на 2, 3, 5, 7 — ни на одно не делится. Значит, **97 простое**.

> 💡 Для огромных чисел (сотни цифр), которые используются в реальной криптографии, перебор делителей не годится — их слишком много. Там применяют хитрые быстрые тесты на простоту, которые с огромной вероятностью дают верный ответ, не находя делителей вовсе.

✍️ Разбор примера

Задача: разложи 360 на простые множители.

Делим на самое маленькое простое, пока делится, потом переходим к следующему:

- 360 : 2 = 180
- 180 : 2 = 90
- 90 : 2 = 45
- 45 не делится на 2, делим на 3: 45 : 3 = 15
- 15 : 3 = 5
- 5 — простое.

Собираем: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$.

Проверка: $8 \cdot 9 \cdot 5 = 360$. ✅

📝 Задачи

1. Выпиши все простые числа до 50 с помощью решета Эратосфена.
2. Разложи на простые множители: **84**.
3. Разложи на простые множители: **561**. (Подсказка: попробуй маленькие простые.)
4. Простое ли число **91**? Обоснуй. А **101**?
5. До какого числа-делителя достаточно проверять, чтобы убедиться, что **199** простое?

6. Сколько всего простых чисел от 1 до 20? Перечисли их.
7. В доказательстве Евклида взяли «все простые» 2, 3, 5 и построили $N = 2\cdot3\cdot5 + 1 = 31$. Проверь: делится ли 31 на 2, 3 или 5? Какой вывод это иллюстрирует?
8. *Со звёздочкой.* Объясни, почему если бы число 1 считали простым, разложение на множители перестало бы быть единственным.