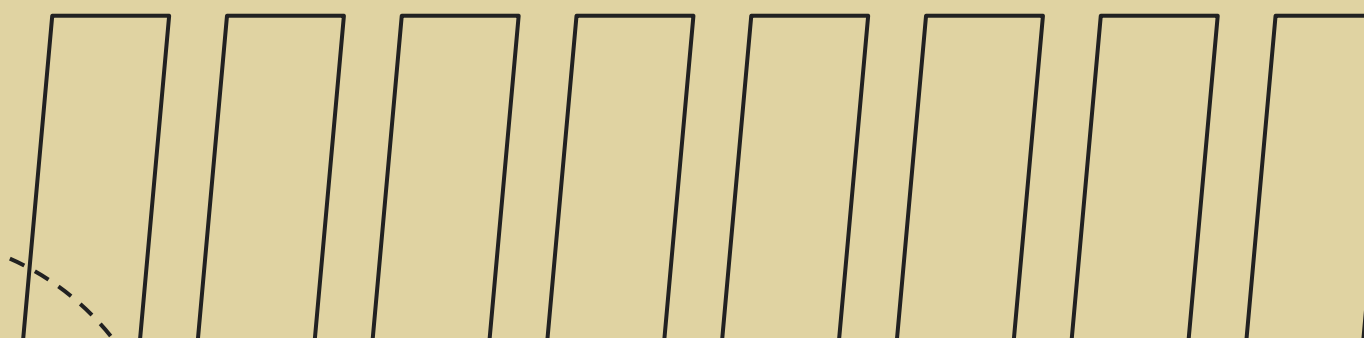
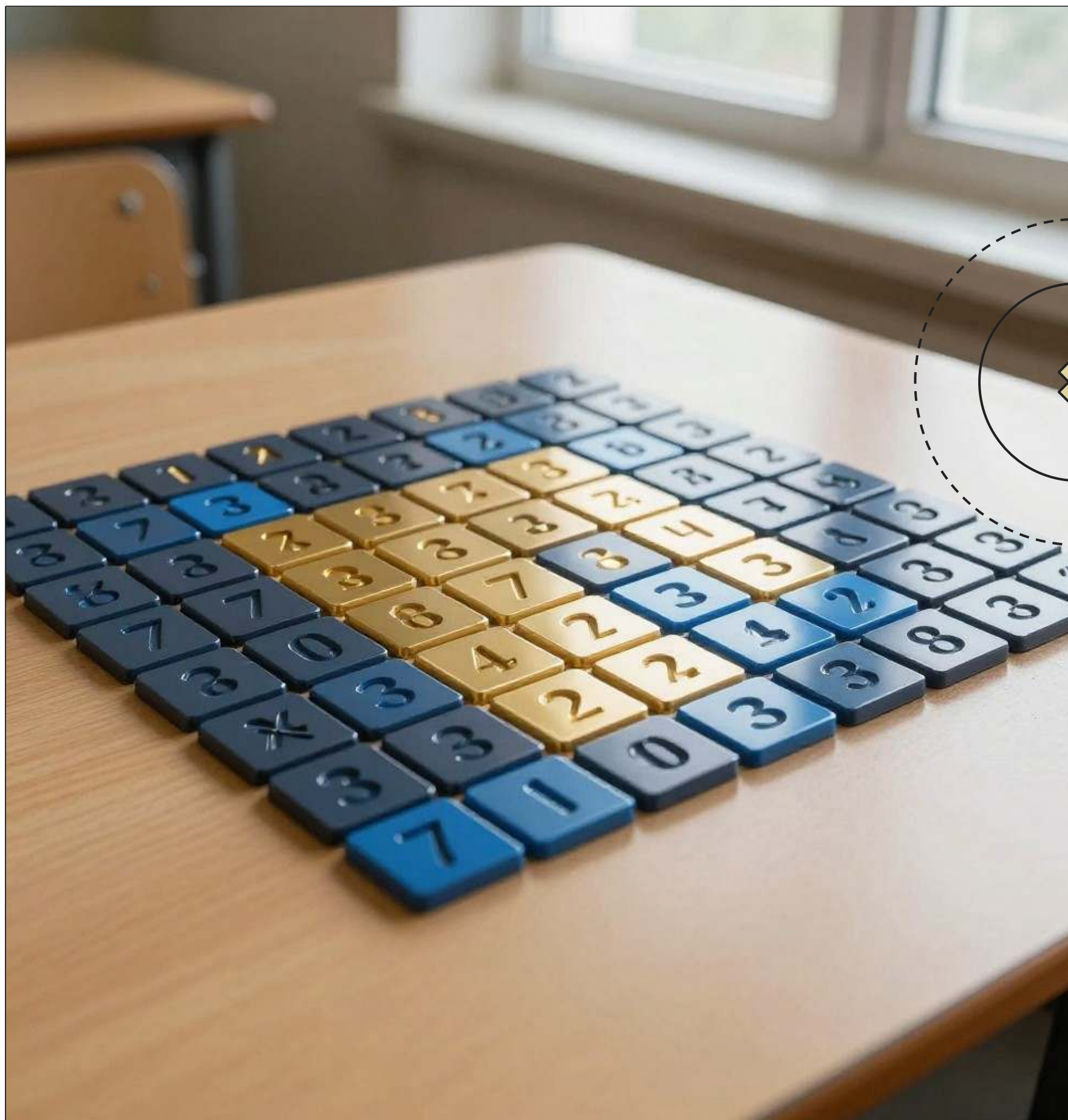


Простые числа: от 2 до бесконечности

Числа, которые задают порядок в мире чисел.

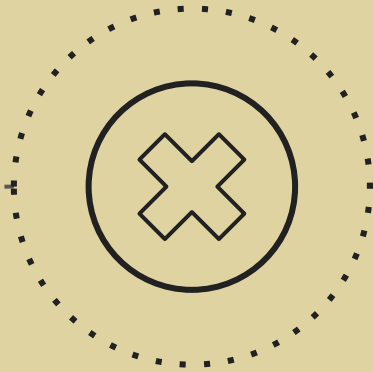




Почему простые числа важны

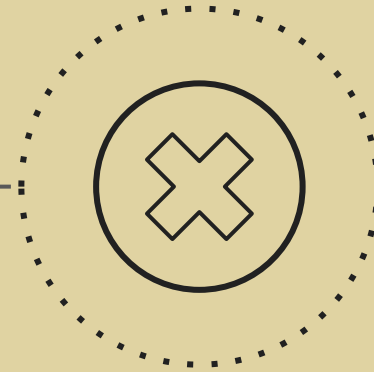
Простые числа помогают понимать делимость, строить алгоритмы и защищать данные. Сначала разберём, как их распознавать, потом научимся быстро находить и увидим, почему их никогда не бывает мало.

Простое и составное



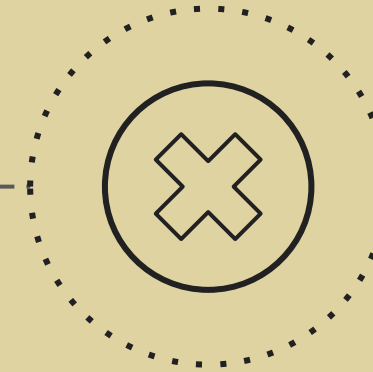
Два делителя

Простое число делится только на 1 и само себя. У него ровно два делителя, поэтому оно служит базовой «единицей» для многих свойств натуральных чисел.



Больше делителей

Составное число имеет больше двух делителей. Его можно разложить на несколько множителей, поэтому оно строится из более простых числовых «кирпичиков».



Сравнение на примерах

Примеры помогают увидеть правило сразу: 2, 3, 5, 7 и 11 – простые; 4, 6, 8, 9 и 10 – составные.

Особые случаи: 1 и 2

01

Единица — исключение

Число 1 не относят ни к простым, ни к составным: у него только один делитель. Это особый случай, который удобно запомнить отдельно.

02

Двойка особенная

Число 2 — самое маленькое простое число. Оно единственное чётное простое, потому что каждое другое чётное число делится ещё и на 2.

03

Чётные числа после 2

Все остальные чётные числа, кроме 2, составные. Если число больше 2 и чётное, оно обязательно имеет делитель 2 и потому не может быть простым.

Проверка до корня

01

Правило проверки

Чтобы проверить число на простоту, достаточно искать делители, не превышающие корень из него. Если таких делителей нет, число считается простым.

02

Проверяем только нужные делители

Для числа 29 нужно попробовать деление на 2, 3 и 5. Следующее число 6 уже не нужно проверять, потому что 6×6 больше 29.

03

Быстрее обычного перебора

Такой способ экономит время: вместо длинного перебора мы останавливаемся раньше и быстро получаем ответ для каждого числа.

Почему проверяют до $\sqrt{n}$

Логика произведения

Если число раскладывается как $n = a \times b$, то оба множителя не могут быть больше корня из n одновременно. Иначе их произведение стало бы слишком большим.

Граница проверки

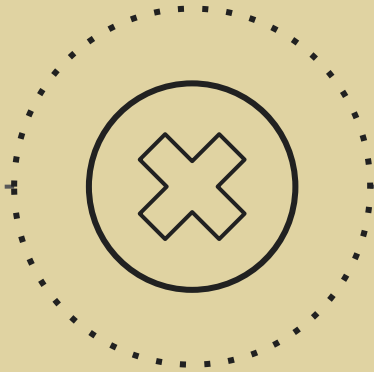
Значит, у любого составного числа есть хотя бы один делитель, не превышающий $\sqrt{n}$. Именно поэтому дальше этой границы проверять не нужно.



Меньше лишних действий

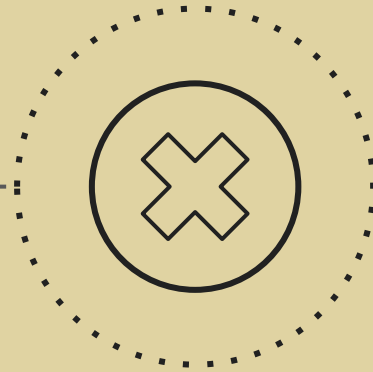
Это правило заметно сокращает количество делений и делает проверку простоты гораздо удобнее для больших чисел.

Два коротких примера



Проверка 37

Число 37 не делится на 2, 3 и 5. Поскольку его корень меньше 7, дальнейшая проверка почти не нужна, и вывод получается быстро: 37 — простое.

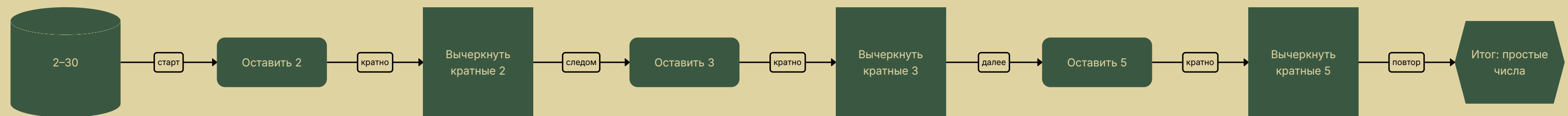


Проверка 39

Число 39 делится на 3 без остатка: $39 = 3 \times 13$. Значит, оно составное, и этого одного делителя достаточно для ответа.

Идея решета Эратосфена

✕ Последовательное вычёркивание кратных от 2 до 30.



Решето на числах до 30

Таблица показывает, какие числа остаются после работы решета на промежутке от 2 до 30.

После удаления кратных 2, 3 и 5 остаются только простые числа до 30.

Шаг	Остаются
Старт	2–30
Итог	2, 3, 5, 7, 11, 13, 17, 19, 23, 29
Пример	Кратные вычёркнуты

**первым новым кандидатом
становится следующий
простой множитель.**

На этом шаге решета остаются только
числа, не кратные ни 2, ни 3.

5

**удобно представить
как произведение
простых чисел.**

Пример 60 помогает увидеть
разложение на простые множители
наглядно и без лишних шагов.

60

**такой набор
для каждого составного
числа единственный.**

Единственность разложения означает,
что у числа есть только один набор
простых множителей и их степеней.

1

Примеры разложения



84: путь через дерево разложения

Число 84 можно разложить поэтапно: сначала выделить 2, затем ещё 2, потом 3 и 7. Дерево разложения помогает увидеть, как одно составное число постепенно превращается в произведение простых множителей.



90: повторяем шаги до конца

У числа 90 тоже есть свой маршрут к простым множителям: 2, 3, 3 и 5. Если на пути встречается составной множитель, его снова раскладывают, пока не останутся только простые числа.

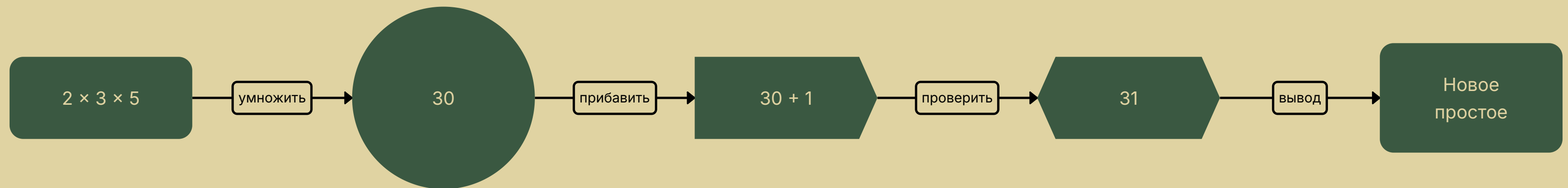
**после такого шага
всегда можно искать
следующий простой.**

Добавление 1 к произведению всех
известных простых создаёт новое
число, которое не делится на них.

1

Мини-пример Евклида

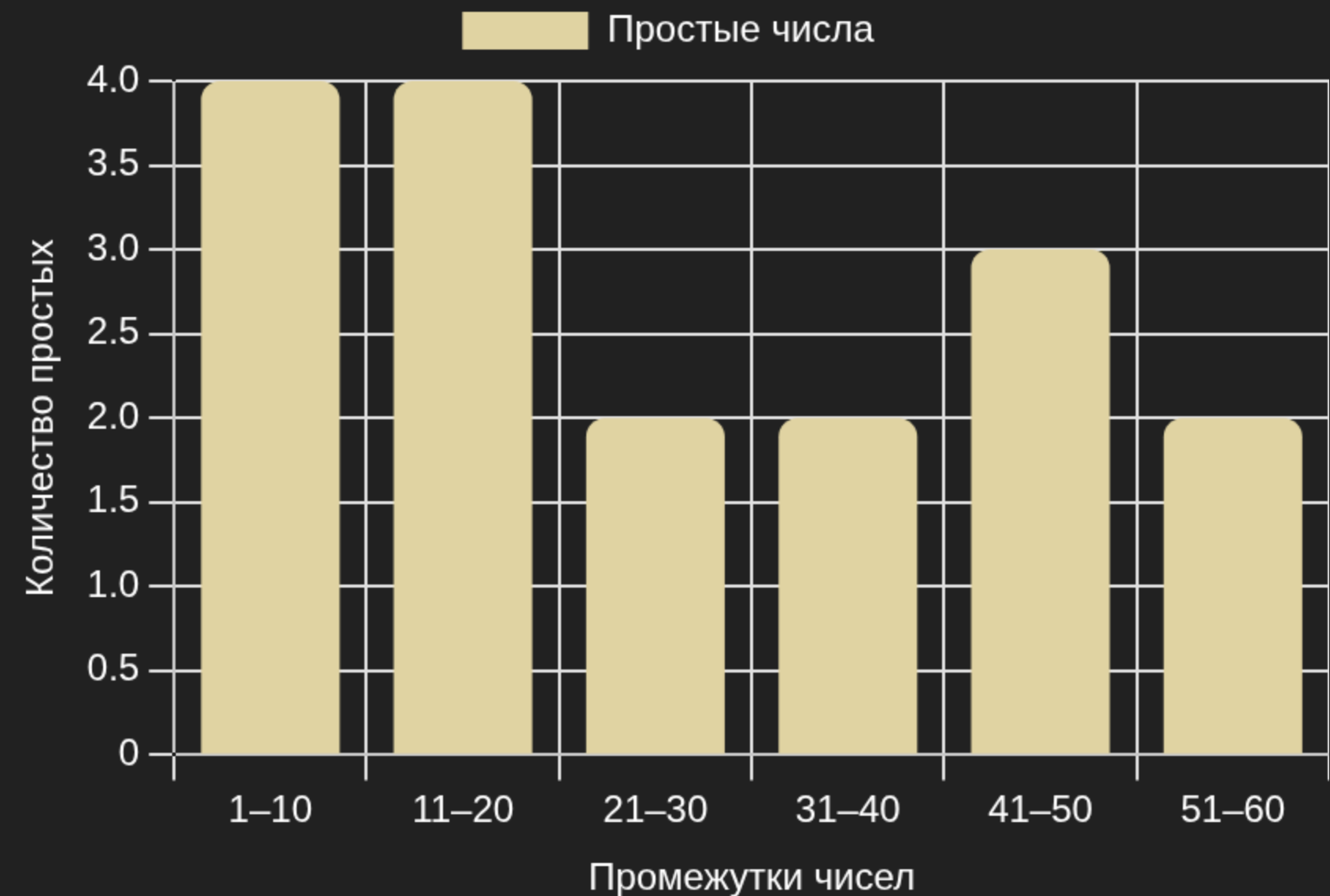
✘ По идее Евклида: произведение известных простых берут целиком, затем добавляют 1 и проверяют делимость.



Как распределены простые

На коротком отрезке видно, что простые встречаются неравномерно: рядом могут быть плотные группы и заметные пропуски.

После 20 простые становятся реже, а промежутки без них заметнее, хотя совсем не исчезают.



Подсчёт простых чисел в интервалах по 10 чисел

Простые окна и близнецы



Близкая пара

Пара 3 и 5 — это простые-близнецы: между ними нет ни одного другого простого числа. Такие пары помогают увидеть, что простые могут появляться очень близко друг к другу.



Почти рядом

5 и 7 — ещё один пример соседства простых. Между ними всего одно чётное число, поэтому такой промежуток особенно легко заметить на числовой прямой.



Повторяющийся МОТИВ

11 и 13 показывают, что простые-близнецы встречаются снова и снова. Они не идут регулярно, но на небольших числах такие пары попадают довольно часто.



Поиск на практике

17 и 19 завершают цепочку знакомых примеров. Такие пары удобно искать, когда уже понимаешь, какие числа не могут быть простыми.

**это длина промежутка
между соседними
простыми в этом примере.**

Разрыв между 89 и 97 показывает,
что рядом с большими числами
простые могут долго не появляться.

8

Зачем простые нужны в криптографии



Почему работает RSA

В RSA берут два больших простых числа и перемножают их. Получается число, которое легко получить, но очень трудно разложить обратно на множители без специальных методов.

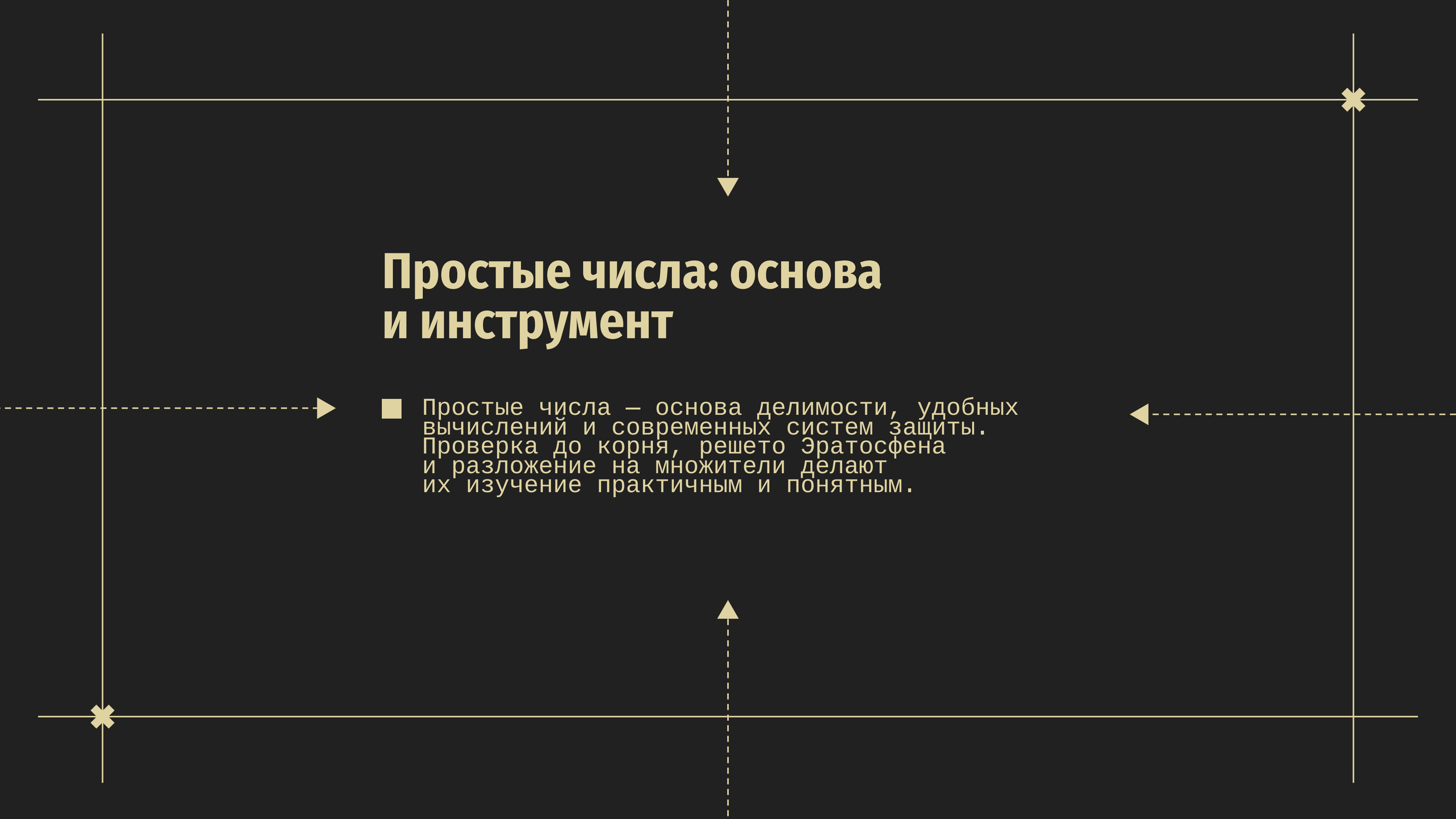


**hard to factor back,
easy to move forward:**

Сложно обратно, просто вперёд

Именно трудность разложения защищает сообщения. Даже если кто-то знает произведение, найти исходные простые числа намного сложнее, чем выполнить обычное умножение.





Простые числа: основа и инструмент

- Простые числа — основа делимости, удобных вычислений и современных систем защиты. Проверка до корня, решето Эратосфена и разложение на множители делают их изучение практичным и понятным.