# Урок 4. Модульная арифметика

**Криптография · ~35 минут**

Ты уже сталкивался с ней в уроке 1, когда буквы «заворачивались» через конец алфавита. Это и есть арифметика остатков — способ считать «по кругу». Именно на ней стоит вся современная криптография, так что этот урок — фундамент для RSA и Диффи–Хеллмана.

## 🎯 Что ты узнаешь

- Что такое «арифметика часов» и запись по модулю.
- Как складывать и умножать по модулю.
- Что такое обратный элемент по модулю.
- Как быстро возводить в степень по модулю (даже огромную).

## 📖 Разбираемся в теме

### Арифметика часов

Посмотри на циферблат часов. Если сейчас 10 часов и пройдёт 5 часов — будет не 15, а **3** часа. Мы посчитали $10 + 5 = 15$, а потом «завернулись»: $15 - 12 = 3$. Часы работают **по модулю 12**.

> 📌 **Запомни:** $a \bmod m$ — это остаток от деления $a$ на $m$. Например, $17 \bmod 5 = 2$, потому что $17 = 3\cdot 5 + 2$. Число $m$ называют **модулем**.

Говорят, что два числа **сравнимы по модулю m**, если у них одинаковый остаток. Пишут: $17 \equiv 2 \pmod 5$ (читается «17 сравнимо с 2 по модулю 5»).

### Сложение и умножение по модулю

Главное удобство: **остаток можно брать в любой момент** — хоть в конце, хоть по ходу дела, результат один и тот же.

Пример по модулю 7:

- $(5 + 6) \bmod 7 = 11 \bmod 7 = 4$.
- $(4 \cdot 5) \bmod 7 = 20 \bmod 7 = 6$.

> 💡 Чтобы не иметь дела с большими числами, бери остаток пораньше. Например, $(6 \cdot 6 \cdot 6) \bmod 7$: считаем $6\cdot 6 = 36 \equiv 1$, тогда $6\cdot 6\cdot 6 \equiv 1 \cdot 6 = 6 \pmod 7$. Не пришлось вычислять 216!

### Обратный элемент

В обычной арифметике «обратное к 3» — это $\tfrac13$, потому что $3 \cdot \tfrac13 = 1$. По модулю дробей нет, но идея та же: **обратный к a по модулю m** — это такое число $x$, что

$$a \cdot x \equiv 1 \pmod m.$$

Найдём обратный к 3 по модулю 7. Перебираем $x = 1, 2, 3, \dots$:

- $3\cdot 1 = 3$
- $3\cdot 2 = 6$
- $3\cdot 3 = 9 \equiv 2$
- $3\cdot 4 = 12 \equiv 5$
- $3\cdot 5 = 15 \equiv 1$ ✅

Значит, обратный к 3 по модулю 7 — это **5**. Записывают $3^{-1} \equiv 5 \pmod 7$.

> ⚠️ Обратный существует **не всегда**! Он есть тогда и только тогда, когда $a$ и $m$ **взаимно просты** (их наибольший общий делитель равен 1). Например, у 2 нет обратного по модулю 4, потому что $\gcd(2,4)=2$: сколько ни умножай 2 на что-нибудь, по модулю 4 единицу не получишь.

Обратный элемент — ключевая деталь RSA: именно так закрытый ключ «отменяет» действие открытого.

### Быстрое возведение в степень

В криптографии постоянно приходится считать что-то вроде $7^{13} \bmod 33$. Умножать 7 само на себя 13 раз долго, а числа получаются гигантские. Есть трюк — **возведение в степень через квадраты**.

Идея: чтобы получить $a^{13}$, разложим показатель по степеням двойки: $13 = 8 + 4 + 1$. Значит

$$a^{13} = a^{8} \cdot a^{4} \cdot a^{1}.$$

А степени $a^2, a^4, a^8$ получаются последовательным возведением в квадрат — каждый раз **беря остаток**, чтобы числа не разрастались.

Посчитаем $7^{13} \bmod 33$:

- $7^1 \equiv 7$
- $7^2 = 49 \equiv 16 \pmod{33}$
- $7^4 = (7^2)^2 \equiv 16^2 = 256 \equiv 25 \pmod{33}$ (256 = 7·33 + 25)
- $7^8 = (7^4)^2 \equiv 25^2 = 625 \equiv 31 \pmod{33}$ (625 = 18·33 + 31)

Теперь $7^{13} = 7^8 \cdot 7^4 \cdot 7^1 \equiv 31 \cdot 25 \cdot 7$. Считаем по шагам:

- $31 \cdot 25 = 775 \equiv 16 \pmod{33}$ (775 = 23·33 + 16)
- $16 \cdot 7 = 112 \equiv 13 \pmod{33}$ (112 = 3·33 + 13)

Итог: $7^{13} \equiv 13 \pmod{33}$. ✅

> 🤔 **А знаешь ли ты?** Чтобы возвести число в степень с 1000-значным показателем (как в реальном RSA), наивный способ потребовал бы больше умножений, чем атомов во Вселенной. А метод квадратов справляется примерно за пару тысяч умножений — компьютер делает это мгновенно.

## ✍️ Разбор примера

**Задача: найди обратный к 5 по модулю 11.**

Ищем $x$, при котором $5x \equiv 1 \pmod{11}$:

- $5\cdot 1 = 5$
- $5\cdot 2 = 10$
- $5\cdot 3 = 15 \equiv 4$
- $5\cdot 4 = 20 \equiv 9$
- $5\cdot 5 = 25 \equiv 3$
- $5\cdot 6 = 30 \equiv 8$
- $5\cdot 7 = 35 \equiv 2$
- $5\cdot 8 = 40 \equiv 7$
- $5\cdot 9 = 45 \equiv 1$ ✅

Ответ: $5^{-1} \equiv 9 \pmod{11}$. Проверка: $5\cdot 9 = 45 = 4\cdot 11 + 1$. ✅

## 📝 Задачи

1. Вычисли: $(23 + 19) \bmod 7$.
2. Вычисли: $(8 \cdot 9) \bmod 5$.
3. Который час покажут часы (модуль 12), если сейчас 9, и пройдёт 20 часов?
4. Найди обратный к 4 по модулю 9.
5. Объясни, почему у числа 6 нет обратного по модулю 9.
6. Вычисли $2^{10} \bmod 1000$ методом квадратов (или как удобнее).
7. Вычисли $3^{100} \bmod 7$. (Подсказка: посмотри, чему равно $3^6 \bmod 7$, — это сильно упростит дело.)
8. *Со звёздочкой.* Докажи, что если $a \equiv b \pmod m$, то и $a^2 \equiv b^2 \pmod m$.