# Урок 6. Модульная арифметика: жизнь по остаткам

**Олимпиадная математика · ~40 минут**

Часы показывают, что $10 + 5$ равно не $15$, а $3$: после 15 часов стрелка встаёт на 3. Это и есть арифметика остатков — сложение «по кругу». Оказывается, для огромного числа задач про делимость важны не сами числа, а только их остатки. И работать с остатками можно почти как с обычными числами: складывать, вычитать, умножать. Это превращает страшные вопросы про огромные степени в устный счёт.

## 🎯 Что ты узнаешь

- Что значит «сравнимы по модулю» и как считать с остатками
- Признаки делимости на 3, 9 и 11 — и почему они работают
- Как быстро находить последнюю цифру степени
- Идею малой теоремы Ферма на примерах

## 📖 Разбираемся в теме

### Сравнения по модулю

Говорят, что $a$ **сравнимо** с $b$ по модулю $m$ (пишут $a \equiv b \pmod m$), если $a$ и $b$ дают одинаковый остаток при делении на $m$ — равносильно, если $m$ делит $a-b$.

Например, $17 \equiv 2 \pmod 5$, потому что оба дают остаток 2.

> 📌 **Запомни:** Сравнения можно складывать, вычитать и умножать. Если $a\equiv b$ и $c\equiv d \pmod m$, то $a+c\equiv b+d$, $a-c\equiv b-d$ и $ac \equiv bd \pmod m$.

Это волшебство: чтобы найти остаток произведения, можно сначала заменить множители их остатками. $23 \cdot 34 \pmod 5$: заменяем на $3\cdot 4 = 12 \equiv 2 \pmod 5$. Готово, без умножения больших чисел.

> ⚠️ А вот делить в сравнениях просто так нельзя! $6\equiv 0 \pmod 6$, но нельзя «сократить на 2» и написать $3\equiv 0$. С делением нужна осторожность.

### Признаки делимости на 3 и 9

Число $\overline{a_k\dots a_1a_0}$ равно $\sum a_i \cdot 10^i$. А $10 \equiv 1 \pmod 9$, поэтому $10^i \equiv 1^i = 1 \pmod 9$. Значит всё число $\equiv \sum a_i \pmod 9$ — то есть сравнимо со своей **суммой цифр** по модулю 9!

> 📌 **Запомни:** Число и сумма его цифр дают один остаток при делении на 9 (и на 3). Отсюда признаки: делится на 9 ⇔ сумма цифр делится на 9; на 3 ⇔ сумма цифр делится на 3.

### Признак делимости на 11

Здесь $10 \equiv -1 \pmod{11}$, поэтому $10^i \equiv (-1)^i$: чётные разряды дают $+1$, нечётные $-1$. Значит число сравнимо с **знакочередующейся суммой цифр** $a_0 - a_1 + a_2 - a_3 + \dots \pmod{11}$.

> 💡 Пример: $918082$. Считаем с конца: $2-8+0-8+1-9 = -22$, делится на 11 → и само число делится на 11. Проверь делением, если не веришь!

### Последняя цифра степени

Последняя цифра числа — это его остаток по модулю 10. Остатки степеней **зациклены**. Например, степени двойки по модулю 10: $2,4,8,6,\ 2,4,8,6,\dots$ — период 4.

Чтобы найти последнюю цифру $2^{2026}$: период 4, $2026 = 4\cdot 506 + 2$, значит последняя цифра как у $2^2$, то есть **4**.

> 🤔 **А знаешь ли ты?** Циклы бывают короткие: у $5$ и $6$ последняя цифра всегда та же ($5$ и $6$), а у $7$ период тоже 4: $7,9,3,1,\dots$

### Малая теорема Ферма (на примерах)

> 📌 **Малая теорема Ферма:** Если $p$ — простое и $a$ не делится на $p$, то $a^{p-1} \equiv 1 \pmod p$.

Проверим на $p=7$, $a=2$: $2^6 = 64 = 63 + 1 = 9\cdot 7 + 1 \equiv 1 \pmod 7$. Работает! Или $p=5$, $a=3$: $3^4 = 81 = 80+1 \equiv 1 \pmod 5$. Тоже.

Зачем это нужно: чтобы схлопывать гигантские показатели. $3^{100} \pmod 7$? По Ферма $3^6\equiv 1$, а $100 = 6\cdot 16 + 4$, значит $3^{100}\equiv 3^4 = 81 \equiv 4 \pmod 7$.

> ⚠️ Теорема требует, чтобы модуль был **простым**, а основание не делилось на него. Для составного модуля она в такой форме неверна.

## ✍️ Разбор задачи

**Задача.** Найди остаток от деления $7^{2026}$ на 100 (то есть две последние цифры числа $7^{2026}$).

**Решение.** Работаем по модулю 100. Посмотрим на степени семёрки: $7^1 = 07,\quad 7^2 = 49,\quad 7^3 = 343 \equiv 43,\quad 7^4 \equiv 43\cdot 7 = 301 \equiv 01 \pmod{100}.$

Отлично, $7^4 \equiv 1 \pmod{100}$ — цикл длины 4. Теперь $2026 = 4\cdot 506 + 2$, поэтому $$7^{2026} = (7^4)^{506}\cdot 7^2 \equiv 1^{506}\cdot 49 = 49 \pmod{100}.$$ Значит, число $7^{2026}$ оканчивается на **49**. ∎

Обрати внимание, как удобно: вместо астрономического числа мы возвели в квадрат и заметили цикл.

**Задача.** Докажи, что $n^3 - n$ делится на 6 при любом целом $n$.

**Решение.** $n^3 - n = n(n-1)(n+1)$ — произведение трёх подряд идущих целых. Среди любых двух подряд есть чётное — значит произведение делится на 2. Среди любых трёх подряд есть кратное трём — значит делится на 3. Числа 2 и 3 взаимно просты, поэтому произведение делится на $2\cdot 3 = 6$. ∎

## 📝 Задачи

1. Найди остаток от деления $2^{100}$ на 3. (Подсказка: $2\equiv -1 \pmod 3$.)
2. Какова последняя цифра числа $3^{2026}$?
3. Докажи, что число $\underbrace{11\dots1}_{2026 \text{ единиц}}$ не делится на 3. А из скольких единиц составленное число (репьюнит) делится на 3?
4. Делится ли число $123456789$ на 9? На 11? Ответь с помощью признаков, не деля в столбик.
5. Докажи, что сумма $1^5 + 2^5 + 3^5 + \dots + 100^5$ делится на 5. (Подсказка: рассмотри $a^5 \bmod 5$ для остатков $a$.)
6. Найди остаток от деления $17^{17}$ на 5.
7. Докажи, что $n^5 - n$ делится на 30 при любом целом $n$. (Разложи $30 = 2\cdot3\cdot5$ и проверь делимость на каждый множитель отдельно.)
8. ⭐ Докажи, что число вида $\overline{abcabc}$ (шестизначное, где первые три цифры повторяются, например $538538$) всегда делится на 7, на 11 и на 13. (Подсказка: чему равно $\overline{abcabc}$ через $\overline{abc}$? И чему равно $7\cdot 11\cdot 13$?)