# Сравнения по модулю. Теория

Сегодня мы поговорим о важной новой теме в теории чисел: сравнениях по модулю. По сути, это более удобная форма для записи остатков. Собственно, начнем с определения и простейших свойств.

**Определение 2.** Целые числа, разность которых делится на $m$, называются *сравнимыми по модулю* $m$. Другими словами, если $a-b$ делится на $m$, то $a$ и $b$ сравнимы по модулю $m$. Запись: $a \equiv b \pmod{m}$.

Из этого определения следует, что если $a \equiv b \pmod{m}$, то $a$ и $b$ дают одинаковые остатки при делении на $m$. И ради этого уже стоит вводить сравнения: до этого удобного способа написать, что у чисел равные остатки, не было!

Конечно, сравнения были бы бесполезны, если у записи выше не было каких-то свойств. И они есть, более того, эти свойства напоминают нам свойства обычных равенств. Поэтому их легко запомнить и применять.

Очень важно, что эти свойства нам не даны свыше, а мы можем их доказать из определения сравнений, чем и займемся сразу после формулировки всех свойств.

**Свойства сравнений.**

- Сравнения можно умножать на число:
  если $a \equiv b \pmod{m}$, то $ka \equiv kb \pmod{m}$.
- Сравнения можно складывать и вычитать:
  если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$.
- Сравнения можно перемножать:
  если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $ac \equiv bd \pmod{m}$.
- Сравнения можно возводить в степень:
  если $a \equiv b \pmod{m}$, то $a^k \equiv b^k \pmod{m}$.

Первые два свойства сразу следуют из определения, достаточно написать вместо сравнения разность. Докажем в качестве примера первое свойство.

---

**Пример 1**

Докажите, что если $a \equiv b \pmod{m}$, то $ka \equiv kb \pmod{m}$.

---

◀ Из того, что $a \equiv b \pmod{m}$ следует, что разность $a-b \vdots m$. Умножим разность на число $k$, тогда делимость не пропадет: $k(a-b) \vdots m$. Раскроем скобки: $ka-kb \vdots m$. Теперь от делимости вернемся к сравнениям: из последней делимости по определению сравнений следует, что $ka \equiv kb \pmod{m}$, что и требовалось доказать. ▶

**Упр. 3.** Докажите второе свойство сами.

Не так легко доказывается третье свойство, поэтому приведем его доказательство в качестве второго примера. Доказательство этих свойств заодно помогает нам лучше разобраться, как работают сравнения, что безусловно большой плюс для дальнейшего решения задач.

---

**Пример 2**

Докажите, что если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$.

---

◀ По первому свойству, которое мы уже доказали, первое данное в условии сравнение можно умножить на число $c$, тогда мы получим $ac \equiv bc \pmod m$. Аналогично второе сравнение можно умножить на $b$: $bc \equiv bd \pmod m$. Объединяя выведенные условия, имеем $ac \equiv bc \equiv bd \pmod m$, или, отбрасывая промежуточное сравнение, $ac \equiv bd \pmod m$, что и требовалось доказать. ▶

**Упр. 4.** Посмотрите на доказательство выше. В нем есть небольшой пробел: мы пользуемся тем, что формально еще не доказывали. Чем? Закройте этот пробел в доказательстве сами.

Последнее свойство следует из третьего, когда мы перемножаем сравнение само с собой $k$ раз, чтобы получить $k$-е степени.

Итак, теперь, когда мы доказали все свойства, пора сформулировать главный

**Вывод.** В сравнениях мы можем заменять число (не степень!!) на любое число, дающее тот же остаток по рассматриваемому модулю.

---

**Пример 3**

Докажите, что при любом натуральном $n$ выполнено $2^{4n} - 1 \vdots 15$.

---

◀ Перепишем условие в виде сравнения. Нам нужно доказать, что $2^{4n} \equiv 1 \pmod{15}$. Распишем левую часть по-другому, возведя двойку в 4-ю степень:

$$2^{4n} \equiv (2^4)^n \equiv 16^n \equiv 1^n \equiv 1 \pmod{15}.$$

В последних двух сравнениях мы заменили 16 на 1 по модулю 15, потому что они сравнимы, а дальше заметили, что 1 в любой степени — по прежнему 1. В итоге сравнение доказано. ▶

Как видите, сравнения по модулю — удобный инструмент. Пожалуй, решение любой задачи можно сформулировать и без сравнений, но это будет крайне громоздко. Пора и самим порешать задачи с использованием новой техники. Желаем успехов!

# Сравнения по модулю. Задачи

**1.** Докажите, что число $1000 \cdot 1001 \cdot 1002 \cdot 1003 - 24$ делится на 999.

**2.** Докажите, что число $1000 \cdot 1001 \cdot 1002 \cdot 1003 - 24$ делится на 1004.

*Подсказка.* На какое маленькое число можно заменить 1000, когда заходит речь про сравнения по модулю 1004?

**3.** Докажите, что при любом четном натуральном $n$ число $5^n + 23 \vdots 24$.

**4.** Известно, что $a + 2c$ и $b + 3d$ делятся на 7. Докажите, что $ab - 6cd$ делится на 7.

**5.** На какую цифру оканчивается число $9^{2015} + 7^{2016}$?

**6.** Докажите, что при любом натуральном $n$ выполнено $13^n + 3^{n+2} \vdots 10$.

**7.** Числа от 1 до $2n$ выписали в ряд в некотором порядке. Затем к каждому из чисел прибавили номер того места, на котором оно стоит (т. е. к первому добавили 1, ко второму прибавили 2 и т. д.). Докажите, что среди полученных сумм найдутся две, дающие одинаковые остатки по модулю $2n$.

**8.** Докажите, что число $5^{70} + 6^{70}$ делится на 61.