8В, спецкурс, занятие 16
12 января 2024
Сравнения по модулю

Определение. Целые числа a и b *сравнимы по модулю* m, если они дают одинаковый остаток от деления на m. Обозначение

$$a \equiv b \pmod{m}.$$

Обычно считается, что $m > 0$.

Лемма. Числа a и b сравнимы по модулю m тогда и только тогда, когда $(a-b) \vdots m$.

Доказательство. Пусть a и b дают одинаковый остаток r при делении на m. Тогда $a = k_1 m + r$, $b = k_2 m + r$ и $a - b = m(k_1 - k_2) \vdots m$.

Теперь пусть $(a-b) \vdots m$ и они дают остатки r_1 и r_2 при делении на m. То есть $a = k_1 m + r_1$, $b = k_2 m + r_2$, где $0 \le r_1, r_2 \le m-1$. Тогда $(r_1 - r_2) \vdots m$. Но при этом $-(m-1) \le r_1 - r_2 \le m-1$. В этом промежутке есть единственное число, кратное m — это 0. Поэтому $r_1 - r_2 = 0$ и $r_1 = r_2$. □

Предложение. Простейшие свойства сравнимости по модулю:

- *рефлексивность*: $a \equiv a \pmod{m}$;
- *симметричность*: если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$;
- *транзитивность*: если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$,

Предложение. Сравнения можно складывать, вычитать и умножать на числа и друг на друга. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то

- $a + c \equiv b + d \pmod{m}$ и $a - c \equiv b - d \pmod{m}$;
- $ka \equiv kb \pmod{m}$;
- $ac \equiv bd \pmod{m}$.
- $a^n \equiv b^n \pmod{m}$ для произвольного натурального n.

Доказательство. Если $(a-b) \vdots m$ и $(c-d) \vdots m$, то $((a \pm c) - (b \pm d)) \vdots m$.

Если $(a-b) \vdots m$, то $(ka - kb) \vdots m$.

Если $a \equiv b \pmod{m}$, то $ac \equiv bc \pmod{m}$. Если $c \equiv d \pmod{m}$, то $bc \equiv bd \pmod{m}$. Тогда по транзитивности $ac \equiv bd \pmod{m}$.

Возможность возводить сравнения в степень напрямую следует из возможности их умножать (по индукции). □

Пример. Найдите остаток от деления 6^{1543} на 7.

Поскольку $6 \equiv -1 \pmod{7}$, то $6^{1543} \equiv (-1)^{1543} = -1 \equiv 6 \pmod{7}$. Значит, 6^{1543} дает остаток 6 при делении на 7.

Пример. Докажите, что число 1543 нельзя представить в виде суммы двух или трех квадратов.

По модулю 4 квадраты дают только остатки 0 и 1, поэтому $a^2 + b^2 \equiv 0, 1$ или $2 \pmod{4}$. А $1543 \equiv 3 \pmod{4}$.

По модулю 8 квадраты дают только остатки 0, 1 и 4, поэтому $a^2 + b^2 + c^2 \not\equiv 7 \pmod{8}$. Но $1543 \equiv 7 \pmod{8}$.

Все числа в этом листочке целые

1$^{\vee}$ Найдите, с чем сравнимо выражение:
a) $2025 \cdot 2026 \cdot 2027 \cdot 2028 \cdot 2029 \pmod{11}$;
b) $2023 \cdot 2022 \cdot 2021 \cdot 2020 \cdot 2019 \pmod{23}$;
c) $497 \cdot 20304 \cdot 999 + 7891 \cdot 9002 - 678 \pmod{100}$;
d) $5^{222} \pmod{24}$ и $5^{222} \pmod{26}$;
e) $(17 + 30 \cdot 12^{111})^{66} - (32 + 10^{43})^{33} \pmod{11}$;
f) $2^{101} + 47^{101} \pmod{31}$.

Кто уверен в своем знании сравнений, может сдать только пункты d, e, f. Если они будут решены правильно, то a, b, c поставятся автоматически.

2 Докажите, что
a) $15^{2023} + 43^{2023}$ делится на 58;
b) $5^{70} + 6^{70}$ делится на 61;
c) $(2^n - 1)^n - 3$ делится на $2^n - 3$ при любом n.
d) $2^{2^{2023}} - 1$ делится на 17.

3 Известно, что $abc + 1$ делится на $ab - b + 1$. Докажите, что $bc - c + 1$ и $ab - a + 1$ – тоже.

4 Можно ли среди чисел $\frac{100}{1}, \frac{99}{2}, \ldots, \frac{1}{100}$ выбрать пять, произведение которых равнялось бы единице?

При решении задач в целых числах бывает полезно рассмотреть происходящее по какому-то модулю. Чаще всего это модули 3, 4 или 5, реже 7 и 8.

Рекомендуется составить в тетради таблички, какие остатки могут давать квадраты целых чисел по этим модулям.

5 Может ли число $n^4 + 2n^2 + 3$ быть простым (при $n \geq 1$)?

6 $p_1, \ldots, p_n$ — первые $n \geq 2$ простых чисел. Докажите, что число
a) $p_1 p_2 \ldots p_n - 1$; b) $p_1 p_2 \ldots p_n + 1$ не является квадратом.

7 Докажите, что уравнения не имеют целых решений.
a) $3x^2 - 4y^2 = 13$; b) $2x^2 - 5y^2 = 7$.

8 Найдите все натуральные решения уравнений
a) $n! - 4n^2 + 18 = m^2 + 4nm - 20m$; b) $2^x + 7 = y^2$.

9* В клетках таблицы $n \times n$ расставляют числа от 1 до n^2 так, чтобы последовательные числа находились в соседних по стороне клетках, а числа, сравнимые по модулю n, располагались в разных строках и разных столбцах.
a) Докажите, что при нечетных $n > 1$ такая расстановка невозможна.
b) Докажите, что при четных n такие расстановки существуют.