8ВМ, спецкурс, занятие 16

23 декабря 2022

Отношения. Сравнения по модулю.

Определение. Пусть есть множество M. Говорится, что на множестве M *задано* некоторое *отношение* R, если про каждую пару элементов M известно, находятся ли они в этом отношении.

Если a и b находятся в отношении R, то мы пишем aRb. Если не находятся — то $a\not Rb$.

Примеры отношений:

- Отношения $=$, $>$, $\leq$ на множестве всех чисел.
- Отношение «быть другом» на множестве учеников гимназии №1543.
- Отношение «иметь хотя бы один равный угол» на множестве треугольников.

Определение.

- Если для всех элементов a верно, что aRa, то отношение R называется *рефлексивным*. Например, отношение $\leq$ является рефлексивным (так как $a \leq a$ для всех чисел a). А отношение «быть другом» рефлексивным не является. (поскольку люди не являются друзьями сами себе.)
- Если из aRb всегда следует bRa, то отношение R называется *симметричным*. Например, отношение «быть другом» является симметричным (поскольку дружба взаимна: если a друг b, то и b друг a). А отношение $\leq$ симметричным не является ($3 \leq 5$, но при этом $5 \not\leq 3$).
- Если из aRb и bRc всегда следует, что aRc, то отношение R называется *транзитивным*. Например, отношение $\leq$ является транзитивным (если $a \leq b$ и $b \leq c$, то $a \leq c$). А отношение «быть другом» транзитивным не является (если Вася друг Пети, а Петя друг Миши, то Вася совсем не обязательно друг Миши).
- Если отношение R является рефлексивным, симметричным и транзитивным, то оно называется *отношением эквивалентности*.

Если задано отношение эквивалентности, то все элементы множества можно разбить на *классы эквивалентности*. Внутри одного класса все элементы эквивалентны, а элементы из разных классов не эквивалентны.

Определение. Целые числа a и b *сравнимы по модулю* m, если $(a-b) \vdots m$. 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 они дают одинаковые остатки при делении на 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 $0 \leq r_1, r_2 \leq m-1$. Тогда $(r_1 - r_2) \vdots m$. Но при этом $-(m-1) \leq r_1 - r_2 \leq m-1$. В этом промежутке есть единственное число, кратное m — это 0. Поэтому $r_1 - r_2 = 0$ и $r_1 = r_2$. □

Отношение сравнимости по модулю m является

- рефлексивным: $a \equiv a \pmod{m}$;
- симметричным: если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$;
- транзитивным: если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$,

и следовательно является отношением эквивалентности. Можно разбить все целые числа на m классов эквивалентности (в каждом классе будут числа, дающие один и тот же остаток при делении на 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 $a - c \equiv b - d \pmod{m}$;
- $ka \equiv kb \pmod{m}$;
- $ac \equiv bd \pmod{m}$.

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 $ac \equiv bd \pmod{m}$. □

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

Поскольку $6 \equiv -1 \pmod{7}$, то $6^{1543} \equiv (-1)^{1543} = -1 \equiv 6 \pmod{7}$. (В номере 2 вы докажете, что сравнения можно возводить в степень.) Значит, 6^{1543} дает остаток 6 при делении на 7.

Пример. При каких n число $n^2 - 6n - 4$ делится на 13?

$$n^2 - 6n - 4 \equiv 0 \pmod{13}$$
$$n^2 - 6n - 4 + 13 \equiv 0 \pmod{13}$$
$$(n-3)^2 \equiv 0 \pmod{13}$$

Поскольку 13 — простое число, то если $(n-3)^2$ делится на 13, то и $n-3$ делится на 13.

$$n - 3 \equiv 0 \pmod{13}$$
$$n \equiv 3 \pmod{13}$$

То есть n дает остаток 3 при делении на 13.

1 Какие из следующих отношений являются рефлексивными, симметричными, транзитивными, отношениями эквивалентности? Для отношений эквивалентности укажите разбиение на классы эквивалентности.

a «a любит b» на множестве людей на Земле;

b «a и b учатся в одном классе» на множестве учеников гимназии 1543;

c «a является братом b» на множестве людей на Земле;

d «a моложе b» на множестве людей на Земле;

e $a \vdots b$ на множестве целых чисел;

f «a и b имеют одну и ту же последнюю цифру» на множестве натуральных чисел;

g «площадь фигуры a равна площади фигуры b» на множестве фигур на плоскости;

h «две стороны треугольника a равны двум сторонам треугольника b» на множестве треугольников на плоскости;

i «два угла треугольника a равны двум углам треугольника b» на множестве треугольников на плоскости.

2 Пусть $a \equiv b \pmod m$.

a По индукции докажите, что $a^n \equiv b^n \pmod m$ для любого натурального числа n.

b Пусть $P(x)$ — какой-то многочлен с целыми коэффициентами. Докажите, что $P(a) \equiv P(b) \pmod m$.

c Пусть $a, b > 0$. Правда ли, что $c^a \equiv c^b \pmod m$ для любого натурального c?

3 Найдите остатки от деления:

a $13^{16} - 2^{55} \cdot 5^{15}$ на 3;

b $(116 + 17^{17})^{21} \cdot 7^{49}$ на 7;

c $776^{776} + 777^{777} + 778^{778}$ на 3;

d $(n^2-1)^{1000} \cdot (n^2+1)^{1001}$ на n;

e $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + 999 \cdot 1000$ на 10;

f $43^{23} + 23^{43}$ на 66;

g $1 \cdot 3 \cdot 5 \cdot \ldots \cdot 2019 \cdot 2021 + 2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2020 \cdot 2022$ на 2023.

4 Докажите признаки делимости:

a $\overline{a_n \ldots a_1 a_0} \equiv a_0 \pmod 2$;
$\overline{a_n \ldots a_1 a_0} \equiv a_0 \pmod 5$;
$\overline{a_n \ldots a_1 a_0} \equiv a_0 \pmod{10}$;

b $\overline{a_n \ldots a_1 a_0} \equiv \overline{a_1 a_0} \pmod 4$;

c $\overline{a_n \ldots a_1 a_0} \equiv a_n + \cdots + a_1 + a_0 \pmod 3$;
$\overline{a_n \ldots a_1 a_0} \equiv a_n + \cdots + a_1 + a_0 \pmod 9$;

d $\overline{a_n \ldots a_1 a_0} \equiv (-1)^n a_n + \cdots + a_2 - a_1 + a_0 \pmod{11}$

5 Найдите a три последние цифры; b шесть последних цифр числа $1^{999} + 2^{999} + \cdots + 999999^{999}$.

6 Докажите, что $(2^n - 1)^n - 3$ делится на $2^n - 3$ при любом n.

7 Докажите, что $2^{2^{2023}} - 1$ делится на 17.

8 Докажите, что для любого натурального n число $2^{5n+3} + 5^n \cdot 3^{n+2}$ делится на 17.