Лекция 4
Теория сравнений – теория остатков

Числовые сравнения. Понятие сравнения

Определение 1

Целые числа *a* и *b* называются сравнимыми по модулю *m*, если разность *a* - *b* делится на *m*

Обозначение: $a \equiv b \pmod{m}$

Примеры

$$5 \equiv -1 \pmod{6}$$

$$18 \equiv 0 \pmod{6}$$

$$1717 \equiv 37 \pmod{10}$$

Теорема 1

Следующие утверждения равносильные:

- ***(1)*** $a \equiv b \pmod{m}$
- ***(2) существует t ϵ Z ,что*** $a = b + mt$
- ***(3) a и b при делении на m дают одинаковые остатки (т.е. a и b равноостаточны)***

Доказательство

1. Докажем, что из (1) следует (2).

По определению имеем:

$$a \equiv b \pmod{m} \Rightarrow (a-b) \vdots m \Rightarrow a-b = mt, t \in Z \Rightarrow a = b + mt$$

2. Докажем, что из (2) следует (3). Существует t ϵ Z , что

$$a = b + mt$$

Разделим b на m с остатком, тогда

$$b = mq + r,\ 0 \le r < m\ , a = mt + mq + r = m(t+q) + r$$

Следовательно, a и b имеют одинаковые остатки

3. Докажем, что из (3) следует (1)

a и b при делении на m имеют одинаковые остатки:

$$a = mq_1 + r \text{ и } b = mq_2 + r$$

Тогда

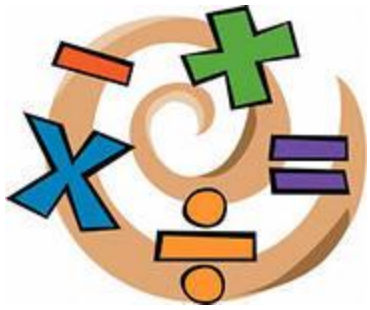
$$a - b = m(q_1 - q_2) \vdots m, \text{ т.е. } a \equiv b \pmod{m}$$

Определение 2

Числа a и b называются сравнимыми по модулю m, если они имеют одинаковые остатки при делении на m

Определение 3

Числа a и b называются сравнимыми по модулю m, если a от b отличается на число, кратное m



Основные свойства сравнений

1. (рефлексивность)

$a \equiv a \pmod{m}$ *для любого* $a \in Z$

2. (симметричность)

Если $a \equiv b \pmod{m}$ *то* $b \equiv a \pmod{m}$

3. (транзитивность)

Если $b \equiv a \pmod{m}$ $b \equiv c \pmod{m}$ *то* $a \equiv c \pmod{m}$

- *Свойства 1, 2, 3 следуют из того, что сравнимые числа имеют одинаковые остатки при делении на* m
- *Из свойств 1–3 вытекает, что отношение сравнимости на множестве целых чисел является отношением эквивалентности*

Основные свойства сравнений

4. Если $a \equiv b (\mathrm{mod}\, m)$, $d \in Z$, *то* $a + d \equiv b + d (\mathrm{mod}\, m)$

Доказательство

Если $a \equiv b (\mathrm{mod}\, m)$ то $(a - b) \vdots m$ и $(a + d - (b + d)) \vdots m$

Следовательно, $a + d \equiv b + d (\mathrm{mod}\, m)$

5. Любое слагаемое сравнения можно переносить в другую часть с противоположным знаком

Доказательство

Пусть $a + b \equiv c (\mathrm{mod}\, m)$

Прибавим к обеим частям сравнения $-b$

получим $a \equiv c - b (\mathrm{mod}\, m)$

Основные свойства сравнений

6. Обе части сравнения можно умножать на одно и то же целое число, т.е.если $a \equiv b(\mathrm{mod}\, m), то\ ac \equiv bc(\mathrm{mod}\, m)$

Доказательство

Если $a \equiv b(\mathrm{mod}\, m)$, то $(a-b) \vdots m$

для любого $c \in Z$ $c(a-b) \vdots m$, или $(ac-bc) \vdots m$

Следовательно $ac \equiv bc(\mathrm{mod}\, m)$

7. Сравнения по одному и тому же модулю можно почленно складывать

Доказательство

$a \equiv b(\mathrm{mod}\, m) \Rightarrow a + c \equiv b + c(\mathrm{mod}\, m)$ (свойство 4)

$c \equiv d(\mathrm{mod}\, m) \Rightarrow b + c \equiv b + d(\mathrm{mod}\, m)$

По 3 свойству: $a + c \equiv b + d(\mathrm{mod}\, m)$

Основные свойства сравнений

8. Сравнения по одному и тому же модулю можно почленно перемножать

Доказательство

$a \equiv b(\mathrm{mod}\, m) \Rightarrow ac \equiv bc(\mathrm{mod}\, m)$ (свойство 6)

$c \equiv d(\mathrm{mod}\, m) \Rightarrow bc \equiv bd(\mathrm{mod}\, m)$

Тогда по 3 свойству: $ac \equiv bd(\mathrm{mod}\, m)$

9. Обе части сравнения можно возводить в одну и ту же степень с натуральным показателем (следует из свойства 8)

10. Если $a \equiv b(\mathrm{mod}\, m)$ *и* $f(x) \equiv c_0 + c_1 x + \ldots + c_n x^n$ – *произвольный многочлен с целыми коэффициентами, то* (это свойство является следствием свойств 9, 6, 7)

$f(a) \equiv f(b)(\mathrm{mod}\, m)$

Основные свойства сравнений

11. Обе части сравнения и модуль можно умножить на одно и то же натуральное число

$$a \equiv b(\mathrm{mod}\, m),\ c \in N \Rightarrow ac \equiv bc(\mathrm{mod}\, mc)$$

Доказательство

Если $a \equiv b(\mathrm{mod}\, m)$, то $(a-b) \vdots m;\ a-b=mt;\ ac-bc=mct$

Следовательно, $(ac-bc) \vdots mc$ и $ac \equiv bc(\mathrm{mod}\, mc)$

12. Обе части сравнения и модуль можно разделить на их общий натуральный делитель

$$ak \equiv bk(\mathrm{mod}\, mk) \Rightarrow a \equiv b(\mathrm{mod}\, m)$$

Доказательство

Если $ak \equiv bk(\mathrm{mod}\, mk)$, то $ak-bk=mkt,\ t \in Z$, или $k(a-b)=mkt$

$$a-b=mt \Rightarrow (a-b) \vdots m \Rightarrow a \equiv b(\mathrm{mod}\, m)$$

Основные свойства сравнений

13. Обе части сравнения можно разделить на их общий множитель, если он взаимно прост с модулем

Доказательство

$ak \equiv bk (\mathrm{mod}\ m)$, следовательно $k(a-b) \vdots m$

Если $(k, m) = 1$, то $(a-b) \vdots m$ (по свойству взаимно простых чисел), т.е $a \equiv b (\mathrm{mod}\ m)$

14. Сравнимые по модулю m числа имеют один и тот же наибольший общий делитель с числом m, т.е.

если $a \equiv b (\mathrm{mod}\ m)$, *то* $(a, m) = (b, m)$

Доказательство

Т. к. $a \equiv b (\mathrm{mod}\ m)$ то для некоторого $t \in Z$ $a = mt + b$

По лемме к алгоритму Евклида $(a, m) = (b, m)$

Основные свойства сравнений

15. Можно добавлять (или отбрасывать) к любой части сравнения слагаемые, кратные модулю

Пусть $a \equiv b(\mathrm{mod}\, m)$

Т.к. $mt \equiv 0(\mathrm{mod}\, m)$, где $t \in Z$, то $a + mt \equiv b(\mathrm{mod}\, m)$ (свойство 7)

16. $a \equiv b(\mathrm{mod}\, mk) \Rightarrow a \equiv b(\mathrm{mod}\, m)$

Если $a \equiv b(\mathrm{mod}\, mk)$, то $a - b$ делится на mk,

а значит и на m, следовательно, $a \equiv b(\mathrm{mod}\, m)$

17. Если $a \equiv b(\mathrm{mod}\, m_1), a \equiv b(\mathrm{mod}\, m_2), \ldots, a \equiv b(\mathrm{mod}\, m_n)$, то

$a \equiv b(\mathrm{mod}\, m)$, где $m = [m_1, m_2, \ldots, m_n]$

Доказательство

Так как $(a-b) \vdots m_1, (a-b) \vdots m_2, \ldots, (a-b) \vdots m_n$, то $(a-b)$ – общее кратное чисел $m_1, m_2, \ldots, m_n$ и оно делится на НОК этих чисел