Теория сравнений и ее приложения

Сравнение по модулю

Числа, дающие при делении на m одинаковые остатки, называются сравнимыми по модулю m. Обозначение: $a \equiv b(\text{mod } m)$

- Отношение сравнимости удовлетворяет условиям:
  - рефлексивности: $a \equiv a \text{ mod } m$,
  - симметричности: если $a \equiv \text{ mod } m$, то и $b \equiv a \text{ mod } m$,
  - транзитивности: если $a \equiv b \text{ mod } m$, а $b \equiv c \text{ mod } m$, то $a \equiv c \text{ mod } m$.
-
- Сравнения по одному и тому же модулю можно почленно складывать.
- Два сравнения по одному и тому же модулю можно почленно вычитать одно из другого.
- К обеим частям сравнения можно прибавлять одно и то же целое число.
- Сравнения по одному и тому же модулю можно почленно перемножать.
- Обе части сравнения можно умножать на одно и то же целое число.

Свойства сравнений, зависящие от модуля

- Если $a \equiv b \ (\text{mod } m)$ и $m \ \vdots \ n$, то $a \equiv b \ (\text{mod } n)$.
- Обе части сравнения и модуль можно умножить на одно и то же целое положительное число.
- Если $ak \equiv bk \text{ mod } m$ и $(k, m)=d$, то $a \equiv b \text{ mod } \frac{m}{d}$.
- Если сравнение $a \equiv b$ имеет место по нескольким разным модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.
- Пусть P(x) - многочлен с целыми коэффициентами, a и b - переменные, принимающие целые значения. Тогда если $a \equiv b \ (\text{mod } m)$, то $P(a) \equiv P(b) \ (\text{mod } m)$. Если $a \equiv b \ (\text{mod } m)$ и $c_i \equiv d_i \ (\text{mod } m)$, то $c_n a^n + c_{n-1} a^{n-1} + \ldots + c_1 a + c_0 = d_n b^n + d_{n-1} b^{n-1} + \ldots + d_1 b + d_0 \ (\text{mod } m)$.

Таким образом, в сравнении по модулю m отдельные слагаемые и множители можно заменять числами, сравнимыми по тому же модулю m. В частности, все числа, кратные модулю, можно заменять нулями (так как если $a \vdots m$, то $a \equiv 0 (\mathrm{mod}\ m)$).