Отношение сравнимости

Многие свойства чисел, а также вопросы разрешимости уравнений в целых числах удобно описывать в терминах сравнений.

Определение 2.1. Пусть $m \in \mathbb{N}$, $m > 1$. Целые числа a и b называются *сравнимыми по модулю* m (обозначается $a \equiv b \pmod{m}$), если разность $a - b$ делится на m.

Отношение сравнимости обладает следующими свойствами.

1. *Рефлексивность*: $a \equiv a \pmod{m}$.

2. *Симметричность*: если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.

3. *Транзитивность*: если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

4. Сравнения можно почленно складывать (вычитать): если $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, то $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$.

Доказательство. Из определения отношения сравнимости имеем: $a_1 - b_1$ делится на m, $a_2 - b_2$ делится на m. Тогда, по свойству 2 делимости, сумма и разность $(a_1 - b_1) \pm (a_2 - b_2)$ делятся на m, откуда $(a_1 \pm a_2) - (b_1 \pm b_2)$ делится на m. □

5. Сравнения можно почленно перемножать: если $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, то $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

6. Обе части сравнения и модуль можно разделить на их общий делитель: если $ac \equiv bc \pmod{mc}$, где $c \neq 0$, то $a \equiv b \pmod{m}$.

7. Обе части сравнения можно разделить на их общий делитель d, если d взаимно прост с модулем.

8. Если m_1 — делитель числа m и $a \equiv b \pmod{m}$, то $a \equiv b \pmod{m_1}$.

9. Если $f(x)$ — полином с целыми коэффициентами и $a \equiv b \pmod{m}$, то $f(a) \equiv f(b) \pmod{m}$.

Отношение, обладающее свойствами рефлексивности, симметричности и транзитивности, называется *отношением эквивалентности.* Таким образом, отношение сравнимости является отношением эквивалентности на множестве $\mathbb{Z}$ целых чисел.

Отношение эквивалентности разбивает множество, на котором оно определено, на *классы эквивалентности.* Любые два класса эквивалентности либо не пересекаются, либо совпадают.

Классы эквивалентности, определяемые отношением сравнимости, называются *классами вычетов по модулю m.* Класс вычетов, содержащий число a, обозначается $a \pmod{m}$ или $\bar{a}$ и представляет собой множество чисел вида $a + km$, где $k \in \mathbb{Z}$; число a называется *представителем* этого класса вычетов.

Множество классов вычетов по модулю m обозначается $\mathbb{Z}/m\mathbb{Z}$, состоит ровно из m элементов и относительно операций сложения и умножения является *кольцом классов вычетов* по модулю m.

Пример 2.1. Если $m=2$, то $\mathbb{Z}/2\mathbb{Z} = \{0 \pmod 2,\ 1 \pmod 2\}$, где $0 \pmod 2 = 2\mathbb{Z}$ — множество всех четных чисел, $1 \pmod 2 = 2\mathbb{Z}+1$ — множество всех нечетных чисел. □

Пример 2.2. При $m=15$ отношение сравнимости разбивает множество $\mathbb{Z}$ на 15 классов вычетов: $\mathbb{Z}/15\mathbb{Z} = \{0 \pmod{15},\ 1 \pmod{15},\ \ldots,\ 14 \pmod{15}\}$, где $0 \pmod{15} = \{\ldots, -30, -15, 0, 15, 30, \ldots\}$, $1 \pmod{15} = \{\ldots, -29, -14, 1, 16, 31, \ldots\}$, …, $14 \pmod{15} = \{\ldots, -16, -1, 14, 29, 44, \ldots\}$. □

Определение 2.2. *Полной системой вычетов* по модулю m называется совокупность m целых чисел, содержащая точно по одному представителю из каждого класса вычетов по модулю m. Совокупность чисел $0, 1, 2, \ldots, m-1$ называется *системой наименьших неотрицательных вычетов*. Совокупность чисел

$$0, \pm 1, \ldots, \pm\frac{m-1}{2} \text{ при нечетном } m;$$

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2} \text{ при четном } m$$

называется *системой абсолютно наименьших вычетов* по модулю m. Каждый из абсолютно наименьших вычетов по абсолютной величине не превосходит половины модуля. Часть полной системы вычетов, состоящая из чисел, взаимно простых с модулем, называется *приведенной системой вычетов*.

Пример 2.3. Найдем различные системы вычетов по модулю $m=6$.

Полная система вычетов: {0, 1, 2, 3, 4, 5}, или {6, –5, 14, 9, –14, –19}, или {0, 1, 2, –3, –2, –1}.

Система наименьших неотрицательных вычетов: {0, 1, 2, 3, 4, 5}.

Система абсолютно наименьших вычетов: {–2, –1, 0, 1, 2, 3}.

Приведенная система вычетов: {1, 5}. □