Классы вычетов

Сравнимость чисел по модулю

Натуральные числа a и b *сравнимы по модулю* m, если

$$(a-b)\vdots m.$$

Запись сравнимости чисел по модулю:

$$a \equiv b \mod m.$$

В этом случае говорят также, что числа a и b находятся в отношении сравнения и записывают

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

Сравнению

$$a = 0 \bmod m$$

удовлетворяют все числа a, которые делятся на m нацело (т.е. кратные m).

Классы вычетов

Определение. Класс эквивалентности отношения сравнения по данному модулю m называется *классом вычетов по модулю* m:

$$a/_{\equiv(\mathrm{mod}\, m)} = \{x \in Z \mid x \equiv a \pmod m\} = \overline{a} \pmod m.$$

Определение. Вычетом класса вычетов по модулю m называется любое из чисел, принадлежащих этому классу вычетов.

Теорема (о структуре класса вычетов). Для класса вычетов $\overline{a} \pmod m$ справедлива формула

$$\overline{a} \pmod m = \{a + k \cdot m \mid k \in N\}.$$

Теорема. Любые два класса вычетов по модулю m либо совпадают, либо не пересекаются.

Наименьший положительный остаток от деления числа a на число m называют наименьшим неотрицательным *вычетом* a по модулю m.

Обозначим множество классов вычетов по модулю m символом

$$Z/_{mZ} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Введём на множестве $Z/_{mZ}$ операции сложения и умножения классов вычетов.

Определение. Суммой двух классов вычетов $\overline{a}$ и $\overline{b}$ называется класс вычетов, порождённый элементом $a+b$, т.е.

$$\overline{a} \oplus \overline{b} = \overline{a+b}.$$

Определение. Произведением двух классов вычетов $\overline{a}$ и $\overline{b}$ называется класс вычетов, порождённый элементом $a \cdot b$, т.е.

$$\overline{a} \otimes \overline{b} = \overline{a \cdot b}.$$

Теорема. Справедливы следующие утверждения:

1. Алгебра $\langle Z/_{mZ}, \oplus \rangle$ является абелевой группой.
2. Алгебра $\langle Z/_{mZ}, \oplus, \otimes \rangle$ является коммутативным кольцом.

Определение. Полной системой вычетов по данному модулю m называется множество чисел, взятых по одному и только по одному из каждого класса вычетов по данному модулю m.

Множество всех чисел, сравнимых с a по модулю m, называется классом вычетов a по модулю m, и обычно обозначается как $[a]_m$ или $\overline{a}_m$. Таким образом, сравнение $a \equiv b \pmod m$ равносильно равенству классов вычетов $[a]_m = [b]_m$.

Поскольку сравнимость по модулю m является отношением эквивалентности на множестве целых чисел Z, то классы вычетов по модулю m представляют собой классы эквивалентности; их количество равно m. Множество всех классов вычетов по модулю m обозначается Z_m или $Z/_{mZ}$.

Операции сложения и умножения на Z индуцируют соответствующие операции на множестве Z_m:

$$[a]_m + [b]_m = [a+b]_m;$$

$$[a]_m \cdot [b]_m = [a \cdot b]_m.$$

Относительно этих операций множество Z_m является конечным кольцом, а для простого m - конечным полем.