1. Элементы теории чисел

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

$$a = 0 \mod m$$

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:

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

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

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

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

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

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

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

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

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

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

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

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.

Пример. Полной системой вычетов по модулю 6 является следующее множество чисел

$$\{0, -5, 8, 15, 4, 11\}.$$

Множество всех чисел, сравнимых с a по модулю m, называется классом вычетов a по модулю m, и обычно обозначается как $[a]_m$ или $\bar{a}_m$. 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.

Простые числа

Число, которое не имеет никаких делителей, кроме 1 и самого себя, называется простым числом. Примеры простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, …

Любое число N может быть представлено в виде произведения степеней простых чисел (*каноническое* представление числа). Такое представление единственно (с точностью до перестановки сомножителей). Так, число

$$600 = 2^3 3^1 5^2.$$

НОД и НОК

НОК(a, b) обозначают через [a, b].

НОД(a, b) обозначают через (a, b).

Определение НОК И НОД чисел. Алгоритм Евклида

Для произвольного целого числа a и произвольного целого положительного числа b существуют такие числа t и r, что $a = bt + r$, где $0 \le r < b$. Причем такое представление единственное.

Можно показать, что если $b|a$ (b делит a нацело), то $(a, b) = b$, и если $a = bt + r$, то $(a, b) = (b, r)$.

Для нахождения наибольшего общего делителя двух чисел a и b известен алгоритм Евклида: пусть $a \ge b$. Рассмотрим следующую последовательность равенств:

$$a = bt_1 + r_2,\ 0 < r_2 < b;$$

$$b = r_2 t_2 + r_3,\ 0 < r_3 < r_2;$$

$$r_2 = r_3 t_3 + r_4,\ 0 < r_4 < r_3 \ldots$$

$$r_{n-1} = r_n t_n + r_{n+1},\ 0 = r_{n+1}.$$

Поскольку $a \ge b > r_2 > r_3 > \ldots \ge 0$, то алгоритм имеет конечное число шагов. Согласно вышеприведенным свойствам, $(a, b) = (b, r_2) = (r_2, r_3) = \ldots = r_n$. Таким образом, наибольший общий делитель чисел a и b равен последнему ненулевому остатку в последовательности равенств, т. е. r_n. А наименьшее общее кратное a и b равно $[a, b] = ab/(a, b)$.

Функция Эйлера

Функция Эйлера $\varphi(m)$ определяется для всех целых чисел m как количество чисел ряда 1, 2, 3, ..., m взаимно простых с m. Так, $\varphi(1) = 1$ (по определению), $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ и т. д. Легко показать, что для $m = p$ (простых чисел) $\varphi(p) = p-1$. Для $m = p^n$ функция

Эйлера $\varphi(p^n) = p^{n-1}(p-1)$. Для произвольного числа m, представленного в канонической форме $m = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, функция Эйлера определяется следующим образом: $\varphi(m) = m(1-1/p_1)(1-1/p_2)\dots(1-1/p_s)$.

Например: $\varphi(11) = 10$; $\varphi(9) = 6$; $\varphi(18) = 6$.

Упражнения.

Вычислить функцию Эйлера $\varphi(m)$ для чисел m = 7, 12, 15, 17, 23, 24, 25, 28, 37, 54, 64.

Классы вычетов, получаемые в соответствии с функцией Эйлера, всегда образуют абелеву группу по умножению. А это, в частности, означает, что для любого представителя из этих классов можно найти обратный элемент из представителей этих же классов.

Теорема Ферма. Если p - простое число и НОД$(a, p)=1$, то

$$a^{p-1} \equiv 1 \mod p.$$

Теорема Эйлера. Если $m>1$ и НОД$(a,m)=1$, то

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Эта теорема обобщает теорему Ферма, т.к. при $m=p$, $\varphi(m)=p-1$.

Упражнения.

На основании теорем Ферма и Эйлера доказать справедливость сравнений:

a) $2^{36} \equiv 3^{36} \equiv \dots \equiv 36^{36} \equiv 1 \mod 37$;

b) $2^{100} \equiv 3^{100} \equiv \dots \equiv 100^{100} \equiv 1 \mod 101$;

c) $2^8 \equiv 4^8 \equiv 7^8 \equiv 8^8 \equiv 11^8 \equiv 13^8 \equiv 14^8 \equiv 1 \mod 15$.

Показатели чисел по модулю и примитивные корни

Пусть $(a, m) = 1$. Рассмотрим бесконечную последовательность степеней числа a: $a^0 = 1$, a^1, a^2, a^3, ... В соответствии с теоремой Эйлера существует целое положительное число s, такое, что

$$a^s \equiv 1 \mod m.$$

Наименьшее из них обозначается через *e* и называется *показателем числа a* по модулю *m*. Иногда е называют *порядком числа a* по модулю *m*.

Если показатель e числа a по модулю m равен $\varphi(m)$, то a называют примитивным элементом по модулю m.

Пример. По каким модулям число $a = 2$ является примитивным элементом? m = **3, 5, 7, 9, 11, 15, 17, 19.**