Лекция 10
Арифметические приложения теории сравнений

Нахождение остатков при делении на данное число

- Из теории сравнений известно, что целое число a и остаток r от деления a на число m принадлежат одному и тому же классу вычетов по модулю m, т.е.

$$a \equiv r \pmod{m}$$

- Остаток r является наименьшим неотрицательным вычетом класса $\overline{a}$ по модулю m

Нахождение остатков при делении на данное число

Пусть $r_1, r_2, ..., r_n$ – остатки от деления чисел $a_1, a_2, ..., a_n$ на m. Тогда:

$$a_1 \equiv r_1 \pmod m$$

$$a_2 \equiv r_2 \pmod m$$

$$\ldots\ldots\ldots\ldots\ldots \qquad (1)$$

$$a_n \equiv r_n \pmod m$$

а) Складывая почленно сравнения (1), получим:

$$a_1 + a_2 + \ldots + a_n \equiv r_1 + r_2 + \ldots + r_n \pmod m. \qquad (2)$$

- Следовательно, нахождение остатка от деления числа $a_1 + a_2 + \ldots + a_n$ на m можно заменить более легкой задачей – нахождением остатка от деления числа $r_1 + r_2 + \ldots + r_n$ на m.

- Если $r_1 + r_2 + \ldots + r_n < m$, то $r_1 + r_2 + \ldots + r_n$ и будет искомым остатком.

Нахождение остатков при делении на данное число

Пусть $r_1, r_2, ..., r_n$ – остатки от деления чисел $a_1, a_2, ..., a_n$ на m. Тогда:

$$a_1 \equiv r_1 \pmod m$$

$$a_2 \equiv r_2 \pmod m$$

$$\ldots\ldots\ldots\ldots\ldots \qquad (1)$$

$$a_n \equiv r_n \pmod m$$

б) Умножая почленно сравнения (1), получим сравнение

$$a_1 a_2 \ldots a_n \equiv r_1 r_2 \ldots r_n \pmod m$$

в) Если $a_1 = a_2 = \ldots = a_n = a$, то получим: $a^n \equiv r^n \pmod m$

Нахождение остатков при делении на данное число

Примеры

Найдем остаток от деления числа

1. $n = (631^{57} + 250^{28}) \cdot 926$ на 12
2. 272^{1141} на 135
3. $7^{161} - 3^{80}$ на 100

Признаки делимости

- Очень часто возникает потребность, не производя самого деления, ответить на вопрос о делимости одного числа на другое

- Критерий, устанавливающий необходимое и достаточное условие делимости произвольного натурального числа a на данное натуральное число m, называется **признаком делимости на** m

Признаки делимости

Французский математик Блез Паскаль (1623-1662) открыл общий признак делимости, который в терминах сравнений может быть сформулирован следующим образом:

Т е о р е м а 1 (общий признак делимости Паскаля)

Для того чтобы число a, записанное в произвольной g-ичной системе счисления в виде:

$$a = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0$$

делилось на число m, необходимо и достаточно, чтобы число

$$b = a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0$$

делилось на m

(здесь a_i – цифры числа a, а r_i – абсолютно наименьшие вычеты соответствующих степеней g^i по модулю $m, i = 1, 2, \ldots, n$)

Частные признаки делимости для числа *a*, записанного в десятичной системе счисления в виде

$$a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$$

- *Признаки делимости на 9 и 3: для того чтобы число a делилось на 9 (на 3), необходимо и достаточно, чтобы сумма его цифр делилась на 9 (на 3)*
- *Признак делимости на 11: для того чтобы число a делилось на 11, необходимо и достаточно, чтобы знакопеременная сумма* $a_0 - a_1 + a_2 - a_3 + \ldots$ *делилась на 11*
- *Признак делимости на 7,11, 13: Для того чтобы число a делилось на 7, или на 11, или на 13, необходимо и достаточно, чтобы разность между числом, записанным последними тремя цифрами, и числом, записанным остальными цифрами данного числа (или наоборот), делилась на 7, или на 11, или на 13*