---

**Лекция №4 (28.09.20)**

---

## 3. Теория сравнений.

## 3.1. Основные свойства сравнений.

**Определение 1.** *Пусть $n$ – фиксированное положительное целое число. Два целых числа $a$ и $b$ называются сравнимыми по модулю $n$ и обозначаются как*

$$a \equiv b \pmod{n},$$

*если $n|(a-b)$. В таком случае $a - b = kn$ для некоторого целого числа $k$.*

Для заданного целого $a$ пусть $q$ и $r$ – его частное и остаток при делении на $n$:

$$a = qn + r, 0 \leq r < n.$$

Тогда из определения сравнения следует, что $a \equiv r \pmod{n}$. Поскольку существует $n$ вариантов для выбора $r$, очевидно, что каждое целое число сравнимо по модулю $n$ ровно с одним из значений $0, 1, 2..., n-1$. В частности, $a \equiv 0 \pmod{n}$ тогда и только тогда, когда $n|a$. Множество $n$ целых чисел $0, 1, 2, ..., n-1$ называется *множеством наименьших положительных вычетов по модулю $n$.*

В общем, $n$ целых чисел $a_1, a_2, ..., a_n$ образуют *полную систему вычетов по модулю $n$*, если каждое целое число сравнимо по модулю $n$ с одним и только одним из $a_k$; иными словами, $a_1, a_2, ..., a_n$ сравнимы по модулю $n$ с $0, 1, 2, ..., n-1$, взятыми в некотором порядке.

Следующая теорема дает полезную характеристику сравнению по модулю $n$ в терминах остатков от деления на $n$.

**Теорема 1.** *Для произвольных целых чисел $a$ и $b$: $a = b \pmod{n}$ тогда и только тогда, когда $a$ и $b$ имеют один и тот же неотрицательный остаток при делении на $n$.*

*Доказательство.* Доказательство необходимо знать. □

Некоторые из простейших свойств сравнений представлены в следующей теореме.

**Теорема 2.** *Пусть $n > 0$ фиксировано, $a, b, c, d$ – произвольные целые числа. Тогда выполняются следующие свойства:*

1. $a \equiv a \pmod{n}$.
2. *Если* $a \equiv b \pmod{n}$, *то* $b \equiv a \pmod{n}$.
3. *Если* $a \equiv b \pmod{n}$ *и* $b \equiv c \pmod{n}$, *то* $a \equiv c \pmod{n}$.
4. *Если* $a \equiv b \pmod{n}$ *и* $c \equiv d \pmod{n}$, *то* $a + c \equiv b + d \pmod{n}$ *и* $ac \equiv bd \pmod{n}$.
5. *Если* $a \equiv b \pmod{n}$, *то* $a + c \equiv b + c \pmod{n}$ *и* $ac \equiv bc \pmod{n}$.
6. *Если* $a \equiv b \pmod{n}$, *то* $a^k \equiv b^k \pmod{n}$ *для любого натурального числа* $k$.

*Доказательство.* Доказательство необходимо знать. □

В предыдущей теореме для $a \equiv b \pmod{n}$ выполняется $ca = cb \pmod{n}$ для любого $c$. Обратное, однако, будет неверно.

**Теорема 3.** *Если* $ca \equiv cb \pmod{n}$, *то* $a \equiv b \pmod{\frac{n}{d}}$, *где* $d =$ *НОД*$(c, n)$.

*Доказательство.* Доказательство необходимо знать. □

**Следствие 1.** *Если* $ca \equiv cb \pmod{n}$ *и НОД*$(c, n) = 1$, *то* $a \equiv b \pmod{n}$

**Следствие 2.** *Если* $ca \equiv cb \pmod{p}$ *и $p$ не делит $c$ ($p$ – простое число), то* $a \equiv b \pmod{p}$.

## 3.2. Некоторые признаки делимости.

При заданном целом $b > 1$ любое положительное целое число $N$ может быть однозначно представлено в виде:

$$N = a_m b^m + a_{m-1} b^{m-1} + ... + a_2 b^2 + a_1 b^1 + a_0,$$

где $a_k$ могут принимать значения от 0 до $b - 1$. Алгоритм деления даёт целые числа $q_1$ и $a_0$, удовлетворяющие равенству:

$$N = q_1 b + a_0, \qquad 0 \leq a_0 \leq b.$$

Если $q_1 \geq b$, мы можем ещё раз применить алгоритм деления и получим

$$N = q_2 b + a_1, \qquad 0 \leq a_1 \leq b.$$

Теперь подставим $q_1$ в исходное равенство, получим

$$N = (q_2 b + a_1)b + a_0 = q_2 b^2 + a_1 b^1 + a_0.$$

До тех пор, пока $q_2 > b$, мы можем продолжать деление. Следующим шагом получим $q_2 = q_3 b + a_2$, где $0 \leq a_2 \leq b$ и

$$N = q_3 b^3 + a_2 b^2 + a_1 b^1 + a_0.$$

Так как $N > q_1 > q_2 > ... \geq 0$ строго убывающая числовая последовательность, этот процесс конечен. В итоге мы получаем

$$N = a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b^1 + a_0.$$

Для определения того, делится ли целое число на 9 или 11, не выполняя при этом деления, понадобится следующая теорема.

**Теорема 4.** *Пусть $P(x) = \sum_{k=0}^{m} c_k x^k$ – многочлен от $x$ с целыми коэффициентами $c_k$. Если $a \equiv b \pmod{n}$, то $P(a) \equiv P(b) \pmod{n}$.*

Если $P(x)$ – многочлен с целыми коэффициентами, то $a$ является решением сравнения $P(x) \equiv 0 \pmod{n}$, если $P(a) \equiv 0 \pmod{n}$.

**Следствие 3.** *Если $a$ является решением $P(x) \equiv 0 \pmod{n}$ и $a \equiv b \pmod{n}$, то $b$ тоже является решением этого сравнения.*

**Теорема 5.** *Пусть $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ – десятичное представление натурального числа $N$, $0 \leq a_k \leq 10$ и пусть $S = a_0 + a_1 + \ldots + a_m$. Тогда $9 \mid N$ тогда и только тогда, когда $9 \mid S$.*

*Доказательство.* Доказательство необходимо знать. □

**Теорема 6.** *Пусть $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ – десятичное представление натурального числа $N$, $0 \leq a_k \leq 10$ и пусть $T = a_0 - a_1 + a_2 - \ldots + (-1)^m a_m$. Тогда $11 \mid N$ тогда и только тогда, когда $11 \mid T$.*

*Доказательство.* Доказательство необходимо знать. □