
Лекция №5 (08.10.20)

---

3. Теория сравнений.

3.1. Линейные сравнения.

Уравнение вида $ax \equiv b \pmod{n}$ называется *линейныйм сравнением.* Пусть решением такого сравнения является целое x_0, тогда $ax_0 \equiv b \pmod{n}$. По определению $ax_0 \equiv b \pmod{n}$ тогда и только тогда, когда $ax_0 - b = ny_0$ для некоторого целого y_0. Таким образом, задача нахождения всех целых решений линейного сравнения $ax \equiv b \pmod{n}$ сводится к нахождению всех решений линейного диофантова уравнения $ax - ny = b$.

Теорема 1. *Линейное сравнение $ax \equiv b \pmod{n}$ имеет решение тогда и только тогда, когда $d|b$, где $d = НОД(a, n)$. Если $d|b$, то сравнение имеет d попарно несравнимых решений по модулю n.*

Доказательство. Доказательство необходимо знать. □

Следствие 1. *Если $НОД(a, n) = 1$, то линейное сравнение $ax \equiv b \pmod{n}$ имеет единственное решение по модулю n.*

Теорема 2 (Китайская теорема об остатках)**.** *Пусть $n_1, n_2, \ldots, n_r$ – положительные целые, такие, что $НОД(n_i, n_j) = 1$ для $i \neq j$. Тогда система линейных сравнений*

$$x \equiv a_1 \pmod{n_1},$$

$$x \equiv a_2 \pmod{n_2},$$

$$\ldots$$

$$x \equiv a_r \pmod{n_r}$$

имеет единственное решение по модулю $n_1 \cdot n_2 \cdot \ldots \cdot n_r$.

Доказательство. Доказательство необходимо знать. □