
Лекция №1 (03.09.20)

---

1. Теория делимости.

1.1. Алгоритм деления.

Теорема 1 (Алгоритм Деления). *Для любых целых a и b, при $b > 0$, существуют и определяются однозначно целые q и r, удовлетворяющие условию*

$$a = qb + r, \qquad 0 \leq r < b.$$

Целые числа q и r называются, соответсвенно, частным и остатком при делении a на b.

Следствие 1. *Если a и b – целые и $b \neq 0$, тогда существуют единственные целые q и r, такие, что*

$$a = qb + r, \qquad 0 \leq r < |b|.$$

1.2. Наибольший общий делитель.

Определение 1. *Говорят, что целое b делится на целое число $a \neq 0$ и обозначается $a \mid b$, если существует некоторое целое число c, такое, что $b = ac$. В случае, если b не делится на a, то пишут $a \nmid b$.*

Теорема 2. *Для целых a, b, c и d выполняется:*

1. $a|0$, $1|a$, $a|a$.
2. $a|1 \Leftrightarrow a = \pm 1$.
3. *Если* $a|b$ *и* $c|d$, *то* $ac|bd$.
4. *Если* $a|b$ *и* $b|c$, *то* $a|c$.
5. $a|b$ *и* $b|a \Leftrightarrow a = \pm b$.
6. *Если* $a|b$ *и* $b \neq 0$, *то* $|a| \leq |b|$.

7. *Если* $a|b$ *и* $a|c$, *то* $a|(bx+cy)$ *для произвольных целых* x *и* y.

Определение 2. *Если* a *и* b *– произвольные целые, то будем называть целое* d *общим делителем чисел* a *и* b, *если* $d|a$ *и* $d|b$.

Определение 3. *Пусть* a *и* b *– целые числа, и, по крайней мере, одно из них отлично от нуля. Наибольшим общим делителем чисел* a *и* b *называется положительное целое* $d = НОД(a,b)$, *такое, что*

- $d|a$ *и* $d|b$;
- *если* $c|a$ *и* $c|b$, *то* $c \leq d$.

Теорема 3. *Для целых* a *и* b, *отличных от нуля, существуют целые* x *и* y, *такие, что*

$$НОД(a,b) = ax + by.$$

Определение 4. *Целые* a *и* b, *отличные от нуля, называются взаимно простыми, если* $НОД(a,b) = 1$.

Теорема 4. *Пусть* a *и* b *– целые, отличные от нуля. Тогда* a *и* b *– взаимно просты тогда и только тогда, когда существуют целые* x *и* y, *такие, что* $1 = ax + by$.

Следствие 2. *Если* $НОД(a,b) = d$, *то* $НОД\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Следствие 3. *Если* $a|c$, $b|c$ *и* $НОД(a,b) = 1$, *то* $ab|c$.

Теорема 5 (Лемма Евклида)**.** *Если* $a|bc$ *и* $НОД(a,b) = 1$, *то* $a|c$.

Теорема 6. *Пусть* a,b *– целые числа, отличные от нуля. Для положительного целого* $d : d = НОД(a,b)$ *тогда и только тогда, когда*

1. $d|a$ *и* $d|b$
2. *если* $c|a$ *и* $c|b$, *то* $c|d$.