Элементы теории чисел. Теория сравнений.

Ученик 10-4 класса Оконешников Д.Д. по лекции к.ф.-м.н. Протопоповой Т.В.

от 20 января 2021 г.

1 Лекция №13

1.1 Каноническое разложение числа. НОД. НОК

Весь алгоритм:	**Пример.** НОД(5083,3553)-?
1) $a = q_1 b + r_1$	$\Rightarrow r_1 = a - q_1 b = A_1 a + B_1 b$
2) $b = q_2 r_1 + r_2$	$\Rightarrow r_2 = b - q_2 r_1 = b - q_2(A_1 a + B_1 b) = -q_2 A_1 a + (1 - B_1 q_2) b = A_2 a + B_2 b$
3) $r_1 = q_3 r_2 + r_3$	$\Rightarrow r_3 = r_1 - q_3 r_2 = A_1 a + B_1 b - q_3(A_2 a + B_2 b) =$
...	$= (A_1 - q_3 A_2) a + (B_1 - q_3 B_2) b = A_3 a + B_3 b$
k) $r_{k-2} = q_k r_{k-1} + r_k$	$r_k = A_k a + B_k b$ или НОД$(a, b) = Aa + Bb$, где $A,\ B$ — целые
k+1) $r_{k-1} = q_{k+1} r_k + 0$	
НОД$(a, b) = r_k$	

Утверждение. Если $d =$ НОД(a, b), то существуют целые A и $B : d = Aa + Bb$.

Замечание. Если НОД$(a, b) = 1$ (т.е. a и b взаимно просты), то существуют целые A и $B : 1 = Aa + Bb$.

1.2 Доказательство свойств делимости 8 и 9

Свойство 8. Если $ab \vdots m$ и НОД$(a, m) = 1$, то $b \vdots m$

$\uparrow$ Имеем НОД$(a, m) = 1 \Rightarrow \exists A,\ M : Aa + Mm = 1$.

Домножим последнее равенство на $b : Aab + Mmb = b \Rightarrow b \vdots m \downarrow$

$\vdots_m \qquad \vdots_m$

Свойство 9. Если $a \vdots m,\ a \vdots k$ и НОД$(m, k) = 1$, то $a \vdots mk$

$\uparrow$

1) $a \vdots m \Rightarrow a = mq_1$

2) $a \vdots k \Rightarrow mq_1 \vdots k$

3) из 2) и НОД$(m, k) = 1 \Rightarrow$ по свойству 8 $q_1 \vdots k \Rightarrow q_1 = kq_2$

4) $a = mq_1 = mkq_2$, т.е. $a \vdots mk \downarrow$

1.3 Решение уравнений ax + by = c

Определение. Диофантово уравнение первой степени - уравнение вида $ax + by = c$, где a, b, c, x, y — целые числа.

Пусть НОД$(a, b) = d$.

1) Если $c \vdots d$, то делим на d правую и левую части уравнения и получаем $a_1 x + b_1 y = c_1$, где НОД$(a_1, b_1) = 1$.
2) Если c не делится на d, то уравнение решений не имеет.

Таким образом, будем рассматривать уравнения (*) $ax + by = c,\ $ НОД$(a, b) = 1$.

Так как НОД$(a, b) = 1$, то по следствию из алгоритма Евклида $\exists$ целые $A,\ B : Aa + Bb = 1$. Домножим равенство на $c : Aca + Bcb = c$.