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 $b : \underset{\vdots m}{Aab} + \underset{\vdots m}{Mmb} = b \Rightarrow b \vdots m \downarrow$

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 $c: Aca+Bcb=c$.
Видим, что пара целых чисел $(x_0,y_0)=(Ac,bc)$ является решением уравнения.
Мы нашли частное (одно из) решение нашего уравнения. Найдем все решения (x,y).

$$\begin{cases} ax_0+by_0=c, \\ ax+by=c. \end{cases} \Rightarrow a(x-x_0)+b(y-y_0)=0,\ a(x-x_0)=-b(y-y_0)$$

. НОД$(a,b)=1$, значит $(x-x_0)\vdots b$, т.е. $x-x_0=bt$ или $x=x_0+bt$, где t — целое.
Тогда $y-y_0=\frac{-a(x-x_0)}{b}=-at$ или $y=y_0-at$.
Таким образом, все пары вида (x_0+bt,y_0-at), где t — целое, являются решениями (*).

Замечание. Общее решение диофантова уравнения представляет собой сумму частного решения уравнения и решения соответствующего однородного уравнения (уравнения $ax+by=0$).

Легко понять, что решениями однородного уравнения являются все пары вида $(bt,-at)$, где t — целое.

Пример. 7x - 23y = 131 Проверка решения: $c \vdots$ НОД$(a,b) \Rightarrow$ имеет решения.
Можно угадать частное решение (22,1), так как 154 - 23 = 131.
Тогда все решения — $(22-33t,1-7t)$, $t\in\mathbb{Z}$.

1.4 Сравнения

Основная идея теории сравнений заключается в том, что два числа a и $b(\in\mathbb{Z})$, имеющие при делении на $m\in\mathbb{N}$ один и тот же остаток, обнаруживают целый ряд одинаковых свойств по отношению к m.

Так по отношению к 2 мы выделяем четные и нечетные числа. Знаем, например, что сумма/разность четных - четное число, произведение четных - четное и т.д.

Определение. Целые числа a и b называются сравнимыми по модулю $m(a\equiv b(mod\ m))$, если при делении на m они дают одинаковые остатки. **(1)**

Пример. $8\equiv 3(mod\ 5)\equiv 103(mod\ 5)\equiv -2(mod\ 5)\equiv -17(mod\ 5)$ и т.д.

Определение. $a\equiv b(mod\ m)\Leftrightarrow (a-b)\vdots m$. **(2)**

Докажем эквивалентность определений 1 и 2.
$\uparrow$
1) **(1)** $\Rightarrow$ **(2)**. Пусть остатки одинаковы, т.е. $a=q_1m+r,\ b=q_2m+r\Rightarrow a-b=m(q_1-q_2),\ (q_1-q_2)\in\mathbb{Z}$, т.е. $(a-b)\vdots m$;
2) **(2)** $\Rightarrow$ **(1)**. От противного.
Пусть остатки разные, т.е. $a=q_1m+r_1,\ b=q_2m+r_2$, где $0\le r_1<|m|,\ 0\le r_2<|m|\,(-|m|<-r_2\le 0)$.

Тогда $a-b=m(q_1-q_2)+r_1-r_2$ и $-|m|<r_1-r_2<|m|\,(|r_1-r_2|<|m|\,(\mathbf{3}))\Rightarrow(r_1-r_2)\vdots m$
Но тогда по свойству делимости 4, если $r_1-r_2\neq 0$, то $|r_1-r_2|\ge|m|$, противоречие с **(3)**. Таким образом, $r_1=r_2$. $\downarrow$

1.5 Свойства сравнений