Обозначение. $d =: gcd(a,b)$

$a, b \in \mathbb{Z}_{>0}$
d - наибольший общий делитель a, b, если $d|a,\ d|b$
$\forall d' \in \mathbb{Z}\ d'|a,\ d'|b \quad d'|d$
$M = \{ax + by : x, y \in \mathbb{Z}\}$

Утверждение. $gcd(a,b) = min(M \cap \mathbb{Z}_{>0})$

$z = ax_0 + by_0 = min(M \cap \mathbb{Z}_{>0}) \quad z \vdots gcd(a,b)$

ЧТО-ТО ЛАЖА КАКАЯ-ТО СВЕРХУ

Алгоритм Евклида.
$a, b \in \mathbb{Z},\ t \in \mathbb{Z}$
$gcd(a,b) = gcd(a, b + ta)$

$a, b \in \mathbb{Z}_{>0} \quad a > b$
$a = bq_1 + r_1,\ r_1 < b$
$b = r_1 q_2 + r_2,\ r_2 < r_1$
$r_1 = r_2 q_3 + r_3,\ r_3 < r_2$
$\vdots$
$r_{k-2} = r_{k-1} q_k + r_k$
$r_{k-1} = r_k q_{k+1} + 0$
$\Rightarrow r_k = gcd(a,b)$

$r_{k-1} = r_{k-3} - r_{k-2} q_{k-1}$
$r_k = r_{k-2} - r_{k-1} q_k = \alpha r_{k-3} + \beta r_{k-2}$

Пример. $gcd(22, 14)$
$22 = 14 * 1 + 8$
$14 = 8 * 1 + 6$
$8 = 6 * 1 + 2$
$6 = 2 * 3 + 0$
$2 = 8 - 6 = 8 - (14 - 8) = -14 + 2 * 8 = -14 + 2(22 - 14) = 2 * 22 - 3 * 14$

$\mathbf{ax + by = c}$ $(*)$

Уравнение разрешимо в $\mathbb{Z} \Leftrightarrow c \vdots gcd(a,b) = d$
$c = d * c'$
$\exists x_0, y_0 \in \mathbb{Z} : ax_0 + by_0 = d \quad \Rightarrow \quad a(x_0 c') + b(y_0 c') = dc' = c$
Рассмотрим однородное уравнение $ax + by = 0$ $(\square)$
Если $(x_1, y_1), (x_2, y_2)$ - решения $(*)$, то
$(x_1 - x_2, y_1 - y_2)$ - решение $(\square)$
$x = b,\ y = -a$ - решение $(\square)$
$x = bk,\ y = -ak, k \in \mathbb{Z}$ - решение $(\square)$

$x = \frac{b}{d}k,\ y = \frac{-a}{d}k$ - решение ($\square$)

Все решения ($*$): $x = x_0c' + \frac{b}{d}k,\ y = y_0c' - \frac{a}{d}k,\ k \in \mathbb{Z}$

Пример.

$4439x + 1679y = 161$
$gcd(4439, 1679) = 23$
$161 \vdots 23$
$4439 * 14 - 1679 * 37 = 23$
$14 * 7 = 98$
$-37 * 7 = -259$
$x = 98 + 73k$
$y = -259 - 193k$

$\mathbf{a \equiv b(mod\ m)}$

"a сравнимо с b по модулю m если
$\exists k \in \mathbb{Z} : a = b + mk$
Обозначение. $a \equiv b(m),\ a \underset{m}{\equiv} b$
Свойства.

1. $\equiv$ - эквивалентность, т.е.
   а) $a \equiv a\ (m)$
   б) $a \equiv b\ (m) \to b \equiv a\ (m)$
   в) $a \equiv b\ (m), b \equiv c\ (m) \Rightarrow a \equiv c\ (m)$

2. $a \equiv b\ (m),\ c \equiv d\ (m) \Rightarrow a + c \equiv b + d\ (m)$

3. Если $ad \equiv bd\ (mod\ md)$, то $a \equiv b\ (mod\ m)$

a, b, m
$ax \equiv b(mod\ m)$
$\exists k \in \mathbb{Z} : ax = b + mk$
$ax - mk = b$ - разрешимо относительно x, k
$\Leftrightarrow b \vdots gcd(a, m)$

Пример.

$105x \equiv 42\ (mod\ 213)$
$105x = 42 + 213k$

$3 = 213 - 2 * 105$
$x_0 = -2,\ k_0 = -1$
$105x = 42 - 213k$
$x = -28 + 71n$

$k = -14 - 35n$
$x \underset{213}{\equiv} 43, 114, 185$

$A = \{0, 1, ..., m-1\}$
$a, b \in A \quad a \bigoplus b = a + b \ (mod\ m)$
$a \bigodot b \ = ab \ (mod\ m)$
$(a \bigoplus b) \bigoplus x = a \bigoplus (b \bigoplus c)$
$a \bigoplus b = b \bigoplus a$
$1 \bigodot a = a$
$0 \bigoplus a = a$
$\ominus a = (m - a) \ mod\ m$

$ax \equiv b \ (m) \Leftrightarrow a \bigodot x = b$ - как элементы A

$\overline{a} = \{b \in \mathbb{Z} : b \equiv a \ (mod\ m)\} =$
$\{a + mk : k \in \mathbb{Z}\} = a + m\mathbb{Z}$ - класс вычетов по модулю m.

$\overline{a} + \overline{b} = \{a + mk + b + mn : k, n \in \mathbb{Z}\} =$
$\{(a + b) + ml : k \in \mathbb{Z}\} = \overline{a + b}$

$\overline{a + b} \subseteq \overline{ab}$

Для каких $a \quad \exists b : \overline{a} * \overline{b} = \overline{1}$
$ax \equiv 1 \ (mod\ m)$ разрешимо
$\Leftrightarrow 1 \vdots gcd(a, m)$, т.е. $a \perp m$

Пример.
$4x \equiv 5 \ (mod\ 7)$
$\overline{4}x = \overline{5} | * \overline{2} \Rightarrow \overline{1}x = \overline{5} * \overline{2} = \overline{10} = \overline{3}$
$\overline{2} * \overline{4} = \overline{1}$

Домашнее задание:

1. $7^n x + 9y = 1$
   $\forall m \ 7^m x + 9y \equiv 1 \ (m)$
   Вопрос: каковы возможные значения $7^n mod\ 9$?

2. $2166x + 3534y + 1302z = 126$