## Билет 8. Решение лин. сравнений и систем

Задача: $ax \equiv b \pmod m \iff ax = b + my$

$12x \equiv 6\ (18)$ НОД$(12, 18) = 6$ $\Rightarrow$ $2x \equiv 1\ (3)$

Находим $x_0 = 2$, тогда $\boxed{x_{i+1} = x_i - \frac{m}{(a,m)}}$

$x_1 = 2 - \frac{18}{6} = -1$ и $x_2 = -4$

при этом всего решений $(a, m)$ штук!

Задача: $\begin{cases} x \equiv 2\ (13) \\ x \equiv 4\ (19) \end{cases}$ Действуем по китайской теореме об остатках

1) $M = 13 \cdot 19 = 247$

2) $M_1 = \frac{247}{13} = 19$ $M_2 = 13$

3) $M_1^{-1} = 1/_{M_1} \bmod a_1 \Rightarrow M_1^{-1} = M_1^{\varphi(13)-1} \pmod{13} = 11$

$M_2^{-1} = 1/_{M_2} \bmod a_2 \Rightarrow M_2^{-1} = M_2^{\varphi(19)-1} \pmod{19} = 3$

$\Rightarrow$ 4) $x = 2 \cdot 19 \cdot 11 + 4 \cdot 13 \cdot 3\ (247) \equiv 80\ (247)$

II способ: $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 6 \pmod 7 \end{cases}$ $\leftarrow$ $\{1, 3, 5, 7, \ldots 39, 41, 43, \ldots\}$
$\{2, 5, 8, \ldots 38, 41, \ldots\}$
$\{6, 13, 20, 27, 34, 41, 48, \ldots\}$

$2 \cdot 3 \cdot 7 = 42 \Rightarrow$ реш $< 42$

$\Rightarrow x \equiv 41 \pmod{42}$