

Упражнение 1. Решить сравнения:

- $3x \equiv 1 \pmod{7}$
- $100x \equiv 21 \pmod{23}$
- $315x \equiv -10 \pmod{275}$
- $76x \equiv 232 \pmod{220}$

Решение.

- $(3, 7) = 1 \Rightarrow$  решение единственно. Решение  $x \equiv 5 \pmod{7}$ .
- $(100, 23) = 1 \Rightarrow$  решение единственно. Решение  $x \equiv 17 \pmod{23}$ .
- $(315, 275) = 5 \Rightarrow 63x \equiv -2 \pmod{55}$ . Решение этого уравнения (алгоритмом Евклида)  $x \equiv 41 \pmod{55}$ . Решения исходного уравнения это  $x_1 \equiv 41 \pmod{275}, x_2 \equiv 96 \pmod{275}, x_3 \equiv 151 \pmod{275}, x_4 \equiv 206 \pmod{275}, x_5 \equiv 261 \pmod{275}$
- $(76, 220) = 4 \Rightarrow 19x \equiv 3 \pmod{55}$ . Решение этого уравнения  $x \equiv 32 \pmod{55}$ . Решения исходного уравнения это  $x_1 \equiv 32 \pmod{220}, x_2 \equiv 87 \pmod{220}, x_3 \equiv 142 \pmod{220}, x_4 \equiv 197 \pmod{220}$

□

Упражнение 2. Найти число целых точек на прямой  $8x - 13y + 6 = 0$ , которые лежат между прямыми  $x = 100$  и  $x = -100$ .

Решение. Решим  $8x + 6 \equiv 0 \pmod{13}$ . Т.к.  $(8, 13) = 1$ , решение единственно. Это решение  $x = 9$ . Тогда для каждого  $\tilde{x} \equiv 9 \pmod{13}$  и какого-либо  $\tilde{y}$ , являющегося решением исходного уравнения,  $(\tilde{x}, \tilde{y})$  — решение исходного уравнения. Кроме того, все решения уравнения записываются в таком виде. Всего  $\tilde{x} : \tilde{x} \equiv 9 \pmod{13}$  и  $\tilde{x} \in [-100, 100]$  существует  $\lfloor \frac{100+95}{13} \rfloor + 1 = 16$  штук, т.к. “крайние”  $\tilde{x}$  это  $-95$  и  $100$ . □

Упражнение 3. Найти все решения в целых числах:

$$34x + 26y = 6$$

Решение.

$$34x + 26y = 6$$

Решим следующее уравнение:

$$34a + 26b = (34, 26) = 2$$

Расширенный алгоритм Евклида даёт частное решение:

$i$	$r_i$	$s_i$	$t_i$	$q_i$
0	34	1	0	
1	26	0	1	
2	8	1	-1	1
3	2	-3	4	3
4	0	13	-17	4

$$a = s_3 = -3, b = t_3 = 4$$

Тогда  $x_0 = a \cdot \frac{6}{2} = -9, y_0 = b \cdot \frac{6}{2} = 12$  — частное решение исходного уравнения.

Рассмотрим решение в общем виде:

$$\begin{cases} x = x_0 + k \cdot n \\ y = y_0 + k \cdot m \end{cases}, k \in \mathbb{Z}$$

$$34(x_0 + k \cdot n) + 26(y_0 + k \cdot m) = 6$$

$$34k \cdot n + 26k \cdot m = 0$$

$$34n = -26m$$

$$17n = -13m$$

Т.к.  $(17, 13) = 1, n = \pm 13, m = \mp 17$

Ответ:  $\{\langle -9 + k \cdot 13, 12 - k \cdot 17 \rangle \mid k \in \mathbb{Z}\}$ , где  $\langle \cdot, \cdot \rangle$  обозначает пару. □

**Упражнение 4.** Решить сравнение  $(a^2 + b^2)x \equiv a - b \pmod{ab}, (a, b) = 1$

*Решение.*

$$\begin{aligned} (a^2 + b^2)x &\equiv a - b \pmod{ab} \\ (a^2 + b^2 - 2ab)x &\equiv a - b \pmod{ab} \\ (a - b)^2 x &\overset{*}{\equiv} a - b \pmod{ab} \\ (a - b)x &\equiv 1 \pmod{ab} \end{aligned}$$

Переход \* верный, т.к.  $(a - b, ab) = 1$ :

*Утверждение.*  $(a - b, ab) = 1$

*Proof.* Предположим обратное:  $(a - b, ab) = k \neq 1$ . Возьмём  $\tilde{k}$  — произвольное простое число, делящее  $k$ . Такое существует, т.к.  $k > 1$ .

Тогда  $ab : \tilde{k}$  и  $a - b : \tilde{k} \Rightarrow a = \tilde{k}p + b$ . Тогда  $(\tilde{k}p + b)b : \tilde{k} \Rightarrow \tilde{k}pb + b^2 : \tilde{k} \Rightarrow b^2 : \tilde{k}$ . По простоте  $\tilde{k} \mid b = \tilde{k}n$ , т.к. иначе  $[b]$  делитель  $\tilde{k}$ , отличный от него и единицы (случай  $b = 1$  тривиален, т.к.  $(a - 1, a) = 1$  всегда выполнено). Аналогичными выкладками  $a : \tilde{k}$  и следовательно  $(a, b) = \tilde{k} \cdot t$ , что противоречит условию.  $\square$

$x$  находится как мультипликативное обратное к  $a - b$  в кольце  $\mathbb{Z}_{ab}$ .  $\square$