# Задание 6. Модульная арифметика и алгоритм Евклида.

**1**

(1) Ищем решение уравнения $ax + by = d$, получаем $a_1, b_1$. Искомым решением будет пара $ka_1, kb_1$.

(2) Пусть дано уравнение в целых числах на $a, b$:

$$ax + by = h.$$

Это уравнение разрешимо тогда и только тогда, когда $h \vdots \gcd(x, y)$.

*Доказательство.* Обозначим $d = \gcd(x, y)$. Тогда для любых целых $a, b$ выполняется $ax \vdots d, by \vdots d \Rightarrow ax + by \vdots d$. То есть не существует целых $a, b$, таких, что $ax + by \not\vdots d$. Отсюда следует необходимость условия $h \vdots \gcd(x, y)$. Достаточность — пункт 1. □

(3) Пусть $(a_1, b_1), (a_2, b_2)$ — частные решения. Тогда $a_1x + b_1y = a_2x + b_2y = d$. Отсюда

$$(a_1 - a_2)x + (b_1 - b_2)y = 0.$$

Пусть теперь $a_0x + b_0y = 0$. Тогда $(a_1 + a_0)x + (b_1 + b_0)y = d$. Итак, все решения уравнения отличаются от произвольного частного на решение однородного. Общее решение уравнения $ax + by = 0$ несложно найти. Обозначим $e = \text{НОК}(x, y)$ и перепишем уравнение в виде $ax = -by$. Видно, что и левая и правая части должны делиться на $x$ и $y$, т.е. должны быть кратны $e$. Поэтому общее решение имеет вид $\left(\frac{e}{x}t, -\frac{e}{y}t\right), t \in \mathbb{Z}$.

Итак, $a_1, b_1$ — частное решение, $a_0 = \frac{e}{x}, b_0 = -\frac{e}{y}$. Тогда общее решение исходного уравнения имеет вид $(a_1 + ta_0, b_1 + tb_0), t \in \mathbb{Z}$.

**2** Решите уравнения в целых числах. Нужно найти все решения, а не только частное.

(1) $238x + 385y = 133$,

(2) $143x + 121y = 52$.

(1) Найдем частное решение расширенным алгоритмом Евклида:

$$s_0 = 1, t_0 = 0$$
$$s_1 = 0, t_1 = 1$$
$$385 = 238 + 147, s_2 = 1, t_2 = -1$$
$$238 = 147 + 91, s_3 = 0 - 1 = -1, t_3 = 2$$
$$147 = 91 + 56, s_4 = 1 + 1 = 2, t_4 = -3$$
$$91 = 56 + 35, s_5 = -1 - 2 = -3, t_5 = 5$$
$$56 = 35 + 21, s_6 = 5, t_6 = -8$$
$$35 = 21 + 14, s_7 = -8, t_7 = 13$$
$$21 = 14 + 7, s_8 = 13, t_8 = -21$$
$$14 = 2 * 7$$

Получаем, что $283 * (-21) + 385 * 13 = 7$, откуда $283 * (-399) + 385 * (247) = 133$. Общее решение однородного уравнения:$x = 55t, y = -34t, t \in \mathbb{Z}$.

Общее решение имеет вид:

$$x = 55t - 283, y = -34t + 247.$$

(2) Найдем частное решение расширенным алгоритмом Евклида:

$$s_0 = 1, t_0 = 0$$
$$s_1 = 0, t_1 = 1$$
$$143 = 121 + 22, s_2 = 1, t_2 = -1$$
$$121 = 22 * 5 + 11, s_3 = 0 - 5 = -5, t_3 = 6$$
$$22 = 11 * 2$$

Получаем, что $143 * (-5) + 121 * 5 = 11$, а 52 не делится на 11. **Решений нет**.

**3** Решите сравнение $68x + 85 \equiv 0 (\mod 561)$ с помощью расширенного алгоритма Евклида. Требуется найти все решения в вычетах.
Решения уравнения экивалентно решению Диовантового уравнения $68x + 561y = -85$.

$$s_0 = 1, t_0 = 0$$
$$s_1 = 0, t_1 = 1$$
$$561 = 8 * 68 + 17, s_2 = 1, t_2 = -8$$
$$68 = 17 * 4$$

Получаем $68 * (-8) + 561 * 1 = 17$, откуда $68 * (40) + 561 * (-5) = -85$.
Общее решение однородного имеет вид $x = 33t, y = -4t, t \in \mathbb{Z}$.
**Ответ:** $x \equiv 40 + 33t (\mod 561), t = 0, \ldots, 16$.

**4** Найдите обратный остаток $7^{-1} (\mod 102)$.
Обозначим искомый остаток за $x$. Тогда $x$ является решением уравнения $7x + 102y = 1$.

$$s_0 = 1, t_0 = 0$$
$$s_1 = 0, t_1 = 1$$
$$102 = 14 * 7 + 4, s_2 = 1, t_2 = -14$$
$$7 = 1 * 4 + 3, s_3 = -1, t_3 = 15$$
$$4 = 3 + 1, s_4 = 2, t_4 = -29$$

Получаем $102 * 2 + 7 * (-29) = 1$. **Ответ:** $7^{-1} \equiv -29 \equiv 73 (\mod 102)$.