10.03.25

Алг. Евклида, ч. 2

$gcd(a, b) = gcd(b, a \bmod b) = d$

$a \geq b$

ост. от дел. a на b

$(28, 12) \to (12, 4) \to (4, 0)$

gcd

$28 \cdot x + 12 \cdot y = 4$

$\begin{cases} x_0 = 1 \\ y_0 = -2 \end{cases}$ $\quad 28 \cdot 1 - 12 \cdot 2 = 4$

~~$\begin{cases} x = 2 \\ y = -4 \end{cases}$~~ 8

$\begin{cases} x_1 = x_0 + \Delta x \\ y_1 = y_0 + \Delta y \end{cases}$ | $\begin{cases} x_1 = x_0 + \Delta x = 1 - 3 = -2 \\ y_1 = y_0 + \Delta y = -2 + 7 = 5 \end{cases}$

Проверим: $-28 \cdot 2 + 12 \cdot 5 = 4$

$-56 + 60$

$28(x_0 + \Delta x) + 12(y_0 + \Delta y) = 4$

$28 \Delta x = -12 \Delta y$

$7 \Delta x = -3 \Delta y$

$\Delta x, \Delta y \rightsquigarrow k\Delta x, k\Delta y$

$k \in \mathbb{Z}$

$\Delta x = -3$

$\Delta y = 7$

$\begin{cases} x_1 = x_0 + k\Delta x \\ y_1 = y_0 + k\Delta y \end{cases}$ $\quad k \in \mathbb{Z}$

$ax + by = c$

$gcd(a, b) = d$

$d \cdot \left(\frac{a}{d}x + \frac{b}{d}y\right) = c$

Пример

$6x + 10y = 3$

$c \nmid d \Rightarrow$ решений нет (в целых числах)

РАСШИРЕННЫЙ АЛГ. ЕВКЛИДА

a	b	$\lfloor \frac{a}{b} \rfloor$	x	y	d
	a mod b				
12	28	0	x	y	4
28	12	2			4
12	4	3			4
4	0	-	1	0	4

$gcd(a,b) = d$

a', b'

$a' \equiv 0 \mod b'$

$a' = m \cdot b'$

$a' = m\, b'$

$b' = b'$

$gcd(a', b') = gcd(a, b)$

алг.:

$a \cdot 1 + b \cdot 0 = gcd(a,b)$

(4) (0) (4)

$a_{next} = b$

$b_{next} = a \mod b$

ПРИМЕР: 5, 23

	a	b	$\lfloor \frac{a}{b} \rfloor$
1)	5	23	0
2)	23	5	4
3)	5	3	1
4)	3	2	1
5)	2	1	2
6)	1	0	

СБОРКА x, y СНИЗУ ВВЕРХ

$a_k \quad b_k \quad \lfloor \frac{a_k}{b_k} \rfloor \quad x_k \quad y_k$

$a_{k+1} \quad b_{k+1} \quad x_{k+1} \quad y_{k+1}$

$a_{k+1} = b_k$

$b_{k+1} = a_k \mod b_k = a_k - \lfloor \frac{a_k}{b_k} \rfloor b_k$

$\frac{a}{b} = \frac{b+b+\ldots+b+b+r}{b} = \frac{\xi b}{b} + \frac{r}{b}$

$a = \xi b + r$

$\xi = \lfloor \frac{a}{b} \rfloor$

$a_k \quad b_k \quad \lfloor \frac{a_k}{b_k} \rfloor \quad x_k \quad y_k$

$a_{k+1} \quad b_{k+1} \quad x_{k+1} \quad y_{k+1}$

$a_{k+1} = b_k$

$b_{k+1} = a_k \mod b_k = a_k - \lfloor \frac{a_k}{b_k} \rfloor b_k$

$$\gcd(a,b) = d = \gcd(a_k, b_k) = \gcd(a_{k+1}, b_{k+1})$$

$$a_k x_k + b_k y_k = a_{k+1} x_{k+1} + b_{k+1} y_{k+1}$$

$$a_k x_k + b_k y_k = b_k x_{k+1} + \left(a_k - \left\lfloor \frac{a_k}{b_k} \right\rfloor b_k\right) y_{k+1}$$

$$a_k x_k + b_k y_k = b_k x_{k+1} + a_k y_{k+1} - \left\lfloor \frac{a_k}{b_k} \right\rfloor b_k y_{k+1}$$

$$a_k(x_k - y_{k+1}) + b_k\left(y_k - x_{k+1} + \left\lfloor \frac{a_k}{b_k} \right\rfloor y_{k+1}\right) = 0$$

если $\begin{cases} x_k = y_{k+1} \\ y_k = x_{k+1} - \left\lfloor \frac{a_k}{b_k} \right\rfloor y_{k+1} \end{cases}$

	a	b	$\left\lfloor \frac{a}{b} \right\rfloor$	d	x	y
1)	12	28	0	4	−2	1
2)	28	12	2	4	1	−2
3)	12	4	3	4	0	1
4)	4	0	–	4	1	0

$x_3 = y_4 = 0$

$y_3 = 1 - 3 \cdot 0 = 1$

$a_3 x_3 + b_3 y_3 = \gcd = 4?$

$12 \cdot 0 + 4 \cdot 1 = 4$

$x_2 = y_3 = 1$

$y_2 = 0 - 2 \cdot 1 = -2$

$28 \cdot 1 + 12 \cdot (-2) = 4$

$x_1 = y_2 = -2$

$y_1 = 1 - 0 \cdot (-2) = 1$

$12 \cdot (-2) + 28 \cdot 1 = 4$

МОДУЛЬНАЯ АРИФМЕТИКА

$$a \cdot a^{-1} = 1$$

$4^{-1} \mod 7$

$x = 4^{-1}$

$4 \cdot 4^{-1} = 4x \equiv 1 \mod 7$

$\mathbb{Z} \to \mathbb{Z}_5$

$\{0, 1, 2, 3, 4\}$

$+, *$

$1 + 2 \equiv 3 \mod 5$

$8 \equiv 3 \mod 5$

$13 \equiv 3 \mod 5$

$3 + 4 \equiv 2 \mod 5$

$x \cdot 4 \equiv 1 \mod 5$

$3 \cdot 4 \equiv 2 \mod 5$

$(4^{-1} + m \cdot 5) \cdot 4 \equiv 1 \mod 5$

$4^{-1} \cdot 4 + m \cdot 5 \cdot 4 \equiv 1$

$0 \equiv 5 \mod 5$

$9 \equiv 4 \mod 5$

$4 \cdot 4 \equiv 1 \mod 5$

$\mathbb{Z}_6$

$\{0, 1, 2, 3, 4, 5\}$

$2 \cdot 5 \equiv 4$

$2 \cdot 3 \equiv 0$

$a \cdot a^{-1} = 1$

$11^{-1} \mod 17$

x т. ч. $x \cdot 11 \equiv 1 \mod 17$

ИЩЕМ ТАКОЕ ЧИСЛО x, ЧТО $x \cdot 11 \equiv 1 \mod 17$

x - "ОБРАТНЫЙ ОСТАТОК"

1 — ОСТАТОК ОТ ДЕЛЕНИЯ НА 17

$14 \cdot 11 \equiv 1$

$(14 - 17) \cdot 11 \equiv 1 \mod 17$

$0 \equiv 0 \mod 17$

$17 \equiv 0 \mod 17$

$K \cdot 17 \equiv 0 \mod 17$

$14 \cdot 11 - 17 \cdot 11$

$14 \cdot 11 - 11 \cdot 17 \equiv 1$

$-3 \cdot 11 \equiv 1$

$-33 \equiv 1$

$+2 \cdot 17$

$-33 + 34 \equiv 1 \mod 17$

ПЕРЕФОРМУЛИРУЕМ ЗАДАЧУ

$x \cdot n \equiv 1 \mod p$

$x \cdot n \ \% \ p = 1$

ЦЕЛАЯ ЧАСТЬ $\left\lfloor \frac{x \cdot n}{p} \right\rfloor = y$

$x \cdot n = y \cdot p + 1$

$n \cdot x + p \cdot (-y) = 1$

РАСШ. АЛГ. ЕВКЛ.

В ПОИСКАХ ОБЩЕГО РЕШ. ДИОФ. УРАВН.

$a x + b y = c$

$\gcd(a, b) = d$

$c \nmid d \Rightarrow$ РЕШЕНИЙ НЕТ

$c : d \Rightarrow$ РЕШЕНИЙ БЕСК. МНОГО

ПУСТЬ x_0, y_0 УДОВЛ. $a x_0 + b y_0 = d$

$\cdot \frac{c}{d}$

$a \frac{x_0 c}{d} + b \frac{y_0 c}{d} = \frac{d \cdot c}{d}$

$x_1 = x_0 \cdot \frac{c}{d}$

$y_1 = y_0 \cdot \frac{c}{d}$

ТЕПЕРЬ НАЙДЁМ ВСЕ РЕШЕНИЯ

$ax + by = 0$

$// \gcd(a,b) = d$

$a = d m_a \;;\; m_a = \frac{a}{\gcd(a,b)}$

$b = d m_b \;;\; m_b = \frac{b}{\gcd(a,b)}$

$d(m_a x + m_b y) = 0$

$m_a x + m_b y = 0$

$x = -\frac{m_b}{m_a} y$

$a(x_0 + \Delta x) + b(y_0 + \Delta y) = c$

$\underline{a x_0} + a\Delta x + \underline{b y_0} + b\Delta y = \underline{c}$

$a\Delta x = -b\Delta y$

$d\left(\frac{a}{\gcd(a,b)}\Delta x + \frac{b}{\gcd(a,b)}\Delta y\right) = 0$

$x_2 = x_1 + \frac{b}{\gcd} k$ — ШАГ ПО X

$k \in \mathbb{Z}$

$y_2 = y_1 - \frac{a}{\gcd} k$ — ШАГ ПО Y

$a x_1 + a\frac{b}{\gcd} + b y_1 - b\frac{a}{\gcd}$

КАК ПОЛУЧ. ОБЩ. РЕШ. ИЗ ЧАСТНОГО:

$$\begin{cases} x_{общ} = x_1 + \frac{b}{\gcd(a,b)} \cdot k \\ y_{общ} = y_1 - \frac{a}{\gcd(a,b)} \cdot k \end{cases} \qquad k \in \mathbb{Z}$$

РАССМОТРИМ ПРИМЕР

$4x + 10y = 12$

$\gcd(4, 10) = 2$

$12 : 2$ РЕШ $\exists$

$$\begin{cases} x_0 = -2 \\ y_0 = 1 \end{cases} \qquad 4 \cdot (-2) + 10 \cdot 1 = 2$$

$$\begin{cases} x_1 = -2 \cdot \frac{12}{2} = -12 \\ y_1 = 1 \cdot \frac{12}{2} = 6 \end{cases} \qquad 4 \cdot (-12) + 10 \cdot 6 = 12$$

← ЧАСТН. РЕШ. ИСК. УР.

$$\begin{cases} x = -12 + \frac{10}{2} \cdot k = -12 + 5k \\ y = 6 - \frac{4}{2} \cdot k = 6 - 2k \end{cases} \qquad k \in \mathbb{Z}$$

x:	-12	-7	-2	-17	-22	...
y:	6	4	2	8	10	
	0	1	2	-1	-2	...

$$4 \cdot (-2) + 10 \cdot 2 = -8 + 20 = 12$$

$$4 \cdot (-12 + 5k) + 10(6 - 2k) = 12$$

$$-48 + 4 \cdot 5k + 60 - 10 \cdot 2k = 12$$