

Elementy

Teorii

Liczeb

1. Dla $a = 184$; $b = 34$

wyznaczyć $s, t \in \mathbb{Z}$

$$sa + tb = \text{NWD}(a, b)$$

$$184 = 5 \cdot 34 + 14 \quad m = 184 - 5 \cdot 34$$

$$34 = 2 \cdot 14 + 6 \quad 6 = 34 - 2 \cdot 14$$

$$14 = 2 \cdot 6 + 2 \quad 2 = 14 - 2 \cdot 6$$

$$6 = 3 \cdot 2 + 0$$

$$2 = 14 - 2 \cdot 6 = 5 \cdot 14 - 2 \cdot 34 = 5 \cdot 184 - 27 \cdot 34$$

r _i	q _i	s _i	R:
0	184	1	0
1	34	5	1
2	14	2	-5
3	6	2	11
.	2	5	-27

Dla $n = 97$ wyzn. 23^{-1} (mod 97)

$$97 = 23 \cdot 4 + 5$$

$$23 = 5 \cdot 4 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 3 - 1 \cdot 2 = 2 \cdot 3 - 5 = 2 \cdot 23 - 3 \cdot 5 =$$

$$= 38 \cdot 23 - 9 \cdot 97$$

Odp.: 38

061. $7^{25} \bmod 23$

$$25 = 2^4 + 2^3 + 1$$

$$7^{2^4} \cdot 7^{2^3} \cdot 7^1 = 49^4 \cdot 49^3 \cdot 7 =$$

$$20 \cdot 7 \cdot 7 = 20^2 = 23$$

Ob. $5^{359} \text{ mod } 173$

$$\sqrt[173]{\cdot} = 13, \dots$$

Podzielne przez pierwastka mniejsze

od pierwastka? Nie \rightarrow jest pierwastka

$$V_p = 2, 3, 5, 7, 11, 13 (\sqrt[173]{\cdot}), p \neq 173$$

$$q = 173$$

$$\forall a \in \mathbb{Z}_q \setminus \{0\} : a^{178} = 1$$

$$5^{359} \text{ mod } 173 = 5^{2 \cdot 178 + 3} = 5^3 = 125$$

małe twierdzenie Fermata

$$\text{Ogl. } 7^{194} \pmod{720}$$

Tw. Eulera $\forall \bar{a} \in \mathbb{Z}_n^*$

$$a^{\varphi(n)} = 1$$

$$720 = 2^4 \cdot 3^2 \cdot 5$$

$$\varphi(720) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(5)$$

$$= 8 \cdot 1 \cdot 3 \cdot 2 \cdot 4 = 132$$

$$7^{132} = 1 \pmod{720}$$

$$7^{194} = 43 \pmod{720}$$

Chiny'skie twierdzenie o resztach

Niech $m_1, \dots, m_k \in \mathbb{N} > 0$

Ge dan liczbami względnie pierwszymi:

$$c \cdot n = a_1 \dots a_k$$

Dla wybranych $a_1, \dots, a_k \in \mathbb{Z}$

i stwierdzić $x \in \mathbb{Z}$ spełniających kongruencję:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Niech $m_i = \frac{n}{n_i}$ (wtedy $\text{NWD}(m_i, n_i) = 1$)

Niech $g_i = m_i^{-1} \pmod{n_i}$

Wtedy $x = \sum_{i=1}^k a_i \cdot g_i \cdot m_i$

Spełnia układ kongruencji.

$$\text{Spr. } x \bmod n_j = a_j \cdot b_j u_j +$$

$$+ \sum_{i \neq j} a_i \cdot b_i u_i$$

$$\underbrace{\quad}_{\equiv 0 \pmod{u_j}}$$

Wyznaczamy największe rozpatrzenie

$x \in N$ wtedy

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases}$$

$$M = 3 \cdot 7 \cdot 11$$

$$M_1 = 77$$

$$M_2 = 33$$

$$M_3 = 21$$

$$x = 2 \cdot 77^{-1} \pmod{3} \cdot 7 \cdot 11 +$$

$$+ 5 \cdot 33^{-1} \pmod{7} \cdot 33 +$$

$$+ 1 \cdot 21^{-1} \pmod{11} - 21 =$$

$$= 2 \cdot 2 \cdot 77 + 5 \cdot 3 \cdot 33 + 10 \cdot 21 =$$

$$= 308 + 495 + 210 = 1013$$

$$1013 \pmod{231} = 89$$

Od. $\overline{35}\overline{x} \equiv \overline{45} \pmod{55}$

wyznaczyć wszystkie rozwiązania

$$\overline{x} \in \mathbb{F}_{55}$$

$$35x \equiv 45 \pmod{55}$$

$$35x + 55y = 45$$

istnieje rozwiązanie x, y tego

równania iff $\text{NWD}(35, 55)$ dzieli 45.

$$\overline{9x} \equiv \overline{9} \pmod{11}$$

wyznaczyć wszystkie rozwiązania

$$\overline{x} \in \mathbb{F}_.$$

Dla $x \in \mathbb{Z}$, \overline{x} spełnia (*) \Leftrightarrow

$$\exists y \in \mathbb{Z} : \alpha x + ny \stackrel{(**)}{\equiv} b$$

$d = \text{mod}(a, n) \Leftrightarrow \alpha x \equiv b \pmod{n}$

$d \text{ mod } (a, n) \Leftrightarrow ax \equiv b \pmod{n} \Leftrightarrow$

$b \Leftrightarrow d|b \Leftrightarrow d|b$

$$\frac{a}{d}x + \frac{n}{d} = \frac{b}{d}$$

$\exists s, t \in \mathbb{Z} : a_1 s + n_1 t = 1$

$$a_1 s b_1 + n_1 t b_1 = b_1$$

(sb_1, tb_1) rozw. szczególny (?)

rozwanie $a_1 x + n_1 y = b_1$

$$a_1 x + n_1 y = 0$$

$$a_1 x = -n_1 y \quad a_1 y \leftarrow \text{ogólne}$$

$$(x, y) = (-kn_1, ua_1) \quad u_1 | x$$

$$u \in \mathbb{Z}$$

$$(x, y) = (sb_1 - kn_1, tb_1 + uy) -$$

rozwiążane ogólnie, stąd (***)

$$35x \equiv 45 \pmod{55}$$

$$\text{NWD}(35, 55) = 5$$

$$7x \equiv 9 \pmod{11}$$

$$9 \cdot 8 \equiv 7 \pmod{11}$$

$$7^{-1} \pmod{11} = 8$$

$$x \equiv 6 \pmod{11}$$

$$x = 11k + 6 \quad k \in \mathbb{Z}$$

Niech $f: \mathbb{F}_{240}^* \ni \bar{x} \mapsto \bar{x}^{13} \in \mathbb{F}_{240}^*$

Wyukorzystując, że f jest bijekcją

wyznaczyć $d \in \mathbb{N}$, że $f^{-1}(\bar{x}) = \bar{x}^d$

$$240 = 2^4 \cdot 3 \cdot 5$$

$$\varphi(240) = 2^3 \cdot 2 \cdot 4 = 64$$

$$\varphi(2^4) = 2^{4-1} \circ (2-1).$$

$$\varphi(3) = 3-1$$

$$x \cdot 19 \equiv 1 \pmod{64}$$

$$\varphi(5) = 5-1$$

$$64 = 3 \cdot 15 + 1$$

$$15 = 2 \cdot 7 + 1$$

$$7 = 1 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$1 = 5 - 2 \cdot 2 =$$

$$= 3 \cdot 5 - 2 \cdot 7 =$$

$$= 3 \cdot (19-2 \cdot 7) - 2 \cdot 5 =$$

$$= 3 \cdot 19 - 3 \cdot 7 =$$

$$= 27 \cdot 19 - 8 \cdot 64$$

$$\begin{array}{r|l} 240 & 2 \\ 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

$$d = 27$$

Wyzkać, że równanie $\bar{x}^{23} = \bar{3}$

X

ma dokładnie jedno rozwiązanie

$\bar{x} \in \mathbb{Z}_{200}$ i wyznaczyć to rozwiązanie

Tw. Niech $n, e, d \in \mathbb{N}_0$: $\text{NWD}(e, \varphi(n)) = 1$

i $ed = 1 \pmod{\varphi(n)}$.

Wtedy $f: \mathbb{Z}^* \ni \bar{x} \rightarrow \bar{x}^e \in \mathbb{Z}_n^*$

jest bijekcją i $f^{-1}(\bar{x}) = \bar{x}^d$

$\forall \bar{q} \in \mathbb{Z}_n^* \exists! \bar{x} \in \mathbb{Z}_n^*: \bar{x}^e = \bar{q}$

wtedy $(\bar{x}^e)^d = \bar{q}^d$
 $\bar{x} = \bar{q}^d$

$$e = 23, n = 200$$

$$\varphi(n) = 5^2 \cdot 2^3$$

$$\varphi(2^3) = 2^2$$

$$\varphi(5^2) = 5 \cdot 4$$

$$\varphi(200) = 2^2 \cdot 5 \cdot 4 = 80$$

$$\text{NWD}(80, 23) = 1 \quad 1 = 23 - 2 \cdot 11 =$$

$$80 = 3 \cdot 23 + 11 \quad = 23 - 2(80 - 3 \cdot 23) =$$

$$23 = 2 \cdot 11 + 1 \quad = 7 \cdot 23 - 2 \cdot 80$$

$$11 = 11 \cdot 1 + 0 \quad d = 7$$

$$3^7 = 3^{2^2+2+1} = 3 \cdot 9 \cdot 81$$

$$= 3 \cdot 243 =$$

$$9 \cdot 43 = 387$$

$$= 187$$

$$(x^{23})^7 = y^7$$
$$x^{23} = y$$

$$x = 3^7 \pmod{200}$$

$$x = 187$$

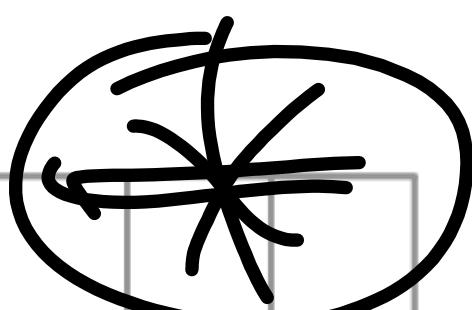
W RSA Ld. publ. $(n, e) = (187, 19)$

wyznaczyć deszyfrując wyłetadule.

$$\varphi(n) = \varphi(17) \cdot \varphi(11) = 16 \cdot 10 = 160$$

$$dl = e^{-1} \pmod{160} \quad e = 19$$

algorytm euclidesa \quad d = 53



Zad. 1) Niedu $n = 77$, podać

Liczę rozwiązań równania $x^2 = 53$

w \mathbb{Z}_{77} i wyznaczyć jedno z

rozwiązań. Zastosować chinoiskie twierdzenie o resztach.

2) Obliczyć $53^{37} \bmod 77$.

f. $\mathbb{X}_n \rightarrow \bar{X}_n \rightarrow (\bar{x}_p, \bar{x}_q) + \mathbb{F}_p + \mathbb{F}_q$

$$f(\bar{x}_n^k) = (\bar{x}_p^k, \bar{x}_q^k)$$

$$\bar{x}_q^k = f^{-1}(\bar{x}_p^k, \bar{x}_q^k)$$

$$\bar{x}_a^k = \bar{a} \text{ w } \notin \mathbb{X}_n$$

$$(\bar{x}_p, \bar{x}_q) \in (\bar{a}_p, \bar{a}_q)$$

$$\{ \bar{x} \in \mathbb{X}_n : \bar{x}^k = \bar{a} \}$$

$$\{ \bar{g}(\bar{y}, \bar{z}) \in \mathbb{F}_p \times \mathbb{F}_q : \bar{y}^k = \bar{a}_p \text{ w } \notin \mathbb{F}_p \cap$$

$$\bar{z}^k = \bar{a}_q \text{ w } \notin \mathbb{F}_q$$

$$B \rightarrow (\bar{q}, \bar{z}) \rightarrow q^{-1}(\bar{q}, \bar{z}) \leftarrow A$$

$$1) x^2 = \overline{53} \text{ } \mathbb{Z}_{77} \rightarrow \mathbb{Z}_{77} \rightarrow \mathbb{Z}_7 \times \mathbb{Z}_{11} \text{ bijektiv}$$

$$53 \bmod 7 = 4$$

$$53 \bmod 11 = 9$$

$$\begin{cases} \bar{q}^2 = \bar{4} \text{ } \cup \mathbb{Z}_7 \\ \bar{z}^2 = \bar{9} \text{ } \cup \mathbb{Z}_{11} \end{cases} \quad \begin{cases} \bar{q} = \bar{2}, -\bar{2} = \bar{2}, \bar{5} \\ \bar{z} = \bar{3}, -\bar{3} = \bar{3}, \bar{8} \end{cases}$$

$$\{(2,3)(2,8)(5,3)(5,8)\} = B$$

$$x = 2 \bmod 7$$

$$x = 8 \bmod 11$$

$$x = 2 \cdot (11^{-1} \bmod 7)^{-11} + 8 \cdot (7^{-1} \bmod 11) \cdot 7$$

$$= 2 \cdot 2 \cdot 11 + 8 \cdot 8 \cdot 7 = 492 \bmod 77 =$$

$$= 30$$

$$2) \quad 53 \bmod 7 = 4$$

$$53 \bmod 11 = 9$$

$$53^{37} = \begin{cases} \bar{4}^{37} & \text{w.r.t. } p=7 \\ \bar{9}^{37} & \text{w.r.t. } p-1=6 \end{cases}$$

$$\bar{4}^{37} = \bar{4}^{6 \cdot 6 + 1} = \bar{4}^1 = \bar{4}$$

$$\bar{9}^{37} = \bar{9}^{3 \cdot 10 + 7} = \bar{9}^7 \text{ w.r.t. } q=11$$

$$\bar{9}^7 = \bar{9} \cdot \bar{9}^2 \cdot \bar{9}^4 = \bar{9} \cdot \bar{4} \cdot \bar{4}^2$$

$$81 \bmod 11 = \bar{18} \cdot \bar{2} \cdot \bar{16} = \bar{7} \cdot \bar{2} \cdot \bar{5}$$

$$= \bar{3} \cdot \bar{5} = \bar{4}$$

Niech $n = pq$, dla parzystych $p \neq q$.

Ponaz, że:

- 1) Jeli znamy n i $\varphi(n)$, to możemy efektywnie rozwiązać p i q .
- 2) Jesli p i q są głisiami, to $-(-$.
($|p-q|$ jest male)
- 3) Jaki dla $d = \text{nwd}((p-1, q-1))$,
liczby $\frac{p-1}{d}$ i $\frac{q-1}{d}$ są małe,
to możemy efektywnie wyzn. p i q

$$1. \quad n = pqr$$

$$\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$$

$$\left\{ \begin{array}{l} n = pqr \Rightarrow q = \frac{n}{p} \end{array} \right.$$

$$\left\{ \begin{array}{l} \varphi(n) = (p-1)(q-1) \Rightarrow (p-1)\left(\frac{n}{p}-1\right) = \end{array} \right.$$

$$= n - \frac{n}{p} - p + 1 = \varphi(n) \quad | \cdot p$$

$$np - n - p^2 + p = \varphi(n) \cdot p$$

$$- p^2 + p(n - \varphi(n) + 1) - n = 0$$

$$\Delta = b^2 - 4ac =$$

$$\overbrace{n}^1 \quad \overbrace{n}^1 \quad \overbrace{k}^1 - \text{aprox } 2^n \text{ cardow}$$

$$2. \quad n = pqr, \quad p < q, \quad p < \sqrt{n} < q$$

$$3. \quad \frac{p-1}{d} = k_1, \quad \frac{q-1}{d} = k_2, \quad (k_1, k_2) \in \mathbb{Z}, \quad k_1, k_2 \in \mathbb{B}$$

$$p = dk_1 + 1, \quad q = dk_2 + 1$$

$$k_1, k_2 \in \mathbb{B}$$

$$(dk_1 + 1)(dk_2 + 1) = n$$

$$k_1 k_2 d^2 + (k_1 + k_2) d + 1 = 0$$

Reszty kwadratowe modulo p .

p - liczba pierwsza $\neq 2$

\mathbb{F}_p , $\bar{a} \in \mathbb{F} \setminus \{0\}$, $\bar{a} = \bar{G}^2$ dla pewnego $\bar{G} \in \mathbb{F}$ to \bar{a} nazywamy resztą kwadratową w \mathbb{F}_p . ($\text{mod } p$)

Niech $QR_p = \{\bar{G}^2 : \bar{G} \in \mathbb{F}_p \setminus \{0\}\}$

$NR_p = \mathbb{Z}_p \setminus (QR_p \cup \{0\})$

Dowolny element w $\bar{a} \in NR_p$

nazywamy resztą kwadratową mod p .

Reszta reszt: $|QR_p| = |NR_p| = \frac{p-1}{2}$

$f: \mathbb{F} \setminus \{0\} \rightarrow \bar{G} \rightarrow \bar{G}^2 \in QR_p$, suriekcja '2-to-1',

bo $x^2 = G^2 \Leftrightarrow \bar{x} = \pm \bar{G}$, stąd

$$|QR_p| = \frac{p-1}{2}$$

$$(NR_p) = |(\mathbb{F}_p \setminus \{0\}) \setminus QR_p| = p-1 - \frac{p-1}{2}.$$

Nicreszt mamy tyle co reszt.

Tw. Zat.że pierwiastek

takeq, że $p \equiv 3 \pmod{4}$.

Jesli $\bar{a} \in \mathbb{F}_p$, i colli jest kongruencja,

to $\bar{a}^{\frac{p+1}{4}}$ jest pierwiastkiem

kwadratowym $\exists \alpha \in \mathbb{F}_p$.

Dowód $(\bar{a}^{\frac{p+1}{4}})^2 = \bar{a}^{\frac{p+1}{2}} = (\bar{b})^{\frac{p+1}{2}} = \bar{b}^{p+1} =$

$\exists \bar{b} \in \mathbb{F}: \bar{b}^2 = \bar{a}$ $= \bar{b}^{p-1} \bar{b}^2 = \bar{b}^2 = \bar{a}$

mtf

Zad. Wyznaczyć rozw. równania $\bar{x}^2 = \bar{6}$
w \mathbb{Z}_{23} .

$$p=23 \equiv 3 \pmod{4}$$

$$\begin{aligned}\bar{6}^{\frac{p+1}{4}} &= \bar{6}^6 = \bar{36}^3 = \bar{13}^3 = \bar{169} \cdot \bar{13} = \\ &= \bar{30} \cdot \bar{13} = \bar{104} = \bar{12}\end{aligned}$$

$$\text{Spr. } \bar{12}^2 = \bar{144} = \bar{6}$$

$$x = \pm \bar{12} = \bar{11}, \bar{12}$$

p - k. pierwsza

\mathbb{F}_p - ciało p -elementowe. (\mathbb{F}_p)

Niech le fo gdzie ciało. k -ciało,

$$n \in \mathbb{N} > 0, n \cdot 1 = \underbrace{1 + \dots + 1}_n$$

Jesli istnieje $n \in \mathbb{N}$:

$$n \cdot 1 = 0, \text{ to } \text{char}(k) \stackrel{\text{def}}{=}$$

$$\min \{ n \in \mathbb{N} > 0 : n \cdot 1 = 0 \}$$

Jesli $\forall n \in \mathbb{N} > 0 : n \cdot 1 \neq 0$, to

$\text{char}(k) = \infty$.

Jesli $p = \text{char}(k) > 0$, to p jest
l. pierwszy.

$$\text{char}(\mathbb{F}_p) = p$$

Def. F_q - ciało skończone q -elementowe.

$$\exists 0 < n_1 < n_2 : n_1 \cdot 1 = n_2 \cdot 1$$

$$(n_2 - n_1) \cdot 1 = 0$$

$F_p = \{0, 1, \dots, p-1\}$ - podcięcie ($\text{mod } p$)

$F_p \subset F_q$ - rozszerzenie ciał

F_q przedłużeniem wektorowym nad ciałem F_p .

Niech $d = \dim_{F_p} F_q$. Niech $b_1, \dots, b_d \in F_q$

Baza F_q nad F_p .

$$F_p^d \ni (x_1 \dots x_d) \rightarrow x_1 b_1 + \dots + x_d b_d \in F_q$$

Gijecja $\overleftarrow{\quad}$

$$\text{Stąd } |F_q| = |F_p^d| = p^d$$

Skonstruować ciało F_p^d

$f \in F_p[x]$ wielomiany stopnia d.

$$\begin{aligned} & \cancel{F_p[x]/(f)} = \\ & = r(x) : r \in F_p[x], \\ & \deg r < d. \end{aligned}$$

$\cancel{\mathbb{K}[x]/f \rightarrow \mathbb{K}[x] / H} =$
 $\bar{g} : g \in \mathbb{K}(x)$

Rzeczywisty reszt modulo f jest przednią
linią modulo f .

Tw. $F_p[x]/(f)$ - ciało $\Leftrightarrow f$ - niewielomian

$$\omega \ F_p[x]$$

Tw. Niech K będzie ciałem i $f \in K[x]$

$$\deg(f) = 2 \vee 3.$$

Wtedy f jest rozkładalny w $K[x]$

f. ma pierwiastek w K .

Dowodząc łatwo 25 elem.

$$F_5 = \{0, 1, 2, 3, 4\}$$

$$f_5 \subset [x] \quad f(x) = x^2 + 1, \text{ rozkł. w } F_5[x]$$

$$f(x) = x^2 + 2 \quad \left. \begin{array}{l} f(0) = 2 \\ f(1) = 3 \\ f(2) = 6 \\ f(3) = 11 \\ f(4) = 18 \end{array} \right\} \neq 0$$

$$\text{Ob. } (3\bar{x}+2)^2 = 9\bar{x}^2 + 12\bar{x} + \bar{4} = -\bar{3} + \bar{2}\bar{x} + \bar{4} = -\bar{4} + \bar{2}\bar{x}$$

$$f_{\mathbb{F}_3} = \cancel{F_3[x]}(f(x)) = \left\{ \alpha_0 + \alpha_1 \bar{x} + \alpha_2 \bar{x}^2 : \right.$$

$$\left. : \alpha_0, \alpha_1, \alpha_2 \in F_3 \right\}$$

Wyznaczyć wielomiany minimalny

$$w(x) = \overline{F}[x] \text{ elementu } \alpha = \bar{x}^2 + 3$$

Wielomiany minimalny to wielomiany minimalnego stopnia, uformowane tak, że α jest jego pierwiastkiem.

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$$

iloczyn nieweskt jest resztą.

$$\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right)$$

$$\left(\frac{a}{n}\right) = \left(\frac{a \text{ mod } n}{n}\right)$$

1) Prawo wzajemności dla symbolu Jacobego.

$$\left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}} \left(\frac{m}{n}\right)$$

$$2) \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

