

E T L

ZADANIA

1) Wyznaczyć $x, y \in \mathbb{Z}$ takie, że

$$33x + 21y = \text{nwd}(33, 21)$$

$$33 = 1 \cdot 21 + 12$$

Euclides

$$21 = 1 \cdot 12 + 9$$

$$12 = 1 \cdot 9 + 3$$

$$9 = 3 \cdot 3 + 0$$

$$3 = 12 - 9 = 12 - (21 - 12) = 2 \cdot 12 - 21 =$$

$$= 2 \cdot (33 - 21) - 21 = 2 \cdot 33 - 3 \cdot 21$$

jednym z rozwiązań jest $x = 2, y = 3$.

2) Wyznaczyć $g^{-1} \pmod{23}$.

Szukamy $gx \equiv 1 \pmod{23}$

$$23 = 2 \cdot 9 + 5$$

Euclides

$$9 = 1 \cdot 5 + 4$$

$$5 = 1 \cdot 4 + 1$$

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

$$\begin{aligned} 1 &= 5 - 4 \cdot 1 = 5 - (9 - 5) = 2 \cdot 5 - 9 = \\ &= 2 \cdot (23 - 2 \cdot 9) - 9 = 2 \cdot 23 - 5 \cdot 9 \end{aligned}$$

$$g^{-1} \equiv -5 \pmod{23} \equiv 18 \pmod{23}$$

3) Wyznaczyć wszystkie rozwiązania dla:

a)

$$\begin{cases} x \equiv 6 \pmod{8} \\ y \equiv 7 \pmod{11} \end{cases}$$

Chińskie zasiedzenie o resztach:

$$x = 8k + 6$$

$$8k + 6 \equiv 7 \pmod{11}$$

$$8k \equiv 1 \pmod{11}$$

Euclides:

$$11 = 1 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

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

$$1 = 3 - 1 \cdot 2 = 3 - (8 - 2 \cdot 3) =$$

$$= 3 \cdot 3 - 8 = 3 \cdot (11 - 8) - 8 =$$

$$= 3 \cdot 11 - 4 \cdot 8$$

$$8k \equiv 1 \pmod{11} \Rightarrow k = 7 + 11m$$

$$x = 8k + 6 = 8(11m + 7) + 6 = 88m + 62$$

$$x \equiv 62 \pmod{88}$$

$$6) \begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x \equiv 7 \pmod{9} \end{cases}$$

$$x = 4a + 1$$

$$4a + 1 \equiv 2 \pmod{5} \Rightarrow 4a \equiv 1 \pmod{5}$$

$$4 \cdot 4 \equiv 1 \pmod{5} \Rightarrow a = 5b + 4$$

$$x = 4(5b + 4) + 1 = 20b + 17$$

a więc rozwiążemy:

$$\begin{cases} x \equiv 17 \pmod{20} \\ x \equiv 7 \pmod{9} \end{cases}$$

$$20c + 17 \equiv 7 \pmod{9}$$

$$20c \equiv -10 \pmod{9}$$

$$20c \equiv 8 \pmod{9}$$

$$2c \equiv 8 \pmod{9}$$

$$c = 4 \Rightarrow c = 9d + 4$$

$$x = 20(9d + 4) + 17 = 180d + 17$$

$$x = 97 \pmod{180}$$

4) Podać liczbę rozwiązań równania $x^2 \equiv 58$
w \mathbb{Z}^{27} i wyznaczyć jedno z rozwiązań.

$$e=2, n=58$$

$$2^3 = 8 \quad 25 \cdot 8 = 200 \quad \text{wg 12.6}$$

$$\varphi(n) = 2^4 \cdot 3$$

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$$

$$\varphi(2^4) = 1$$

$$\varphi(3) = 1$$

$$\varphi(58) = 2^3 = 8$$

$$\begin{matrix} 1 \\ 2 \\ 3 \end{matrix}$$

$$\text{NWD}(8, 1) = 1$$

$$d = 23 - 2 \cdot 11 =$$

$$80 = 3 \cdot 23 + 11$$

$$= 23 - 2(80 - 3 \cdot 23) =$$

$$23 = 2 \cdot 11 + 1$$

$$= 7 \cdot 23 - 2 \cdot 80$$

$$11 = 11 \cdot 1 + 0$$

$$d = 7$$

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

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

$$x^{23} = y$$

$$= 3 \cdot 243 =$$

$$3 \cdot 43 = 387$$

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

$$= 187$$

$$x = 187$$

5)

6) Uzasadnić, że $7^k \equiv 1 \pmod{990}$ dla pewnego k ; podać przykład takiego k .

$$990 = 495 \times 2 = 99 \times 5 \times 2 = 33 \times 5 \times 3 \times 2 = 11 \times 5 \times 3^2 \times 2$$

$$\begin{aligned}\phi(990) &= \phi(2) \times \phi(3^2) \times \phi(5) \times \phi(11) = \\ &= 1 \times 3 \cdot 2 \times 4 \times 10 = 240\end{aligned}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}, a = 7, n = 990$$

$$7^{240} \equiv 1 \pmod{990}$$

7) Obliczyć:

a) $5^{122} \pmod{77}$ używając euklidesa

$$77 = 11 \times 7$$

$$\phi(77) = \phi(11) \times \phi(7) = 10 \times 6 = 60$$

$$5^{60} \equiv 1 \pmod{77} \Rightarrow 5^2 \equiv 1 \pmod{77}$$

$$5^{122} \pmod{77} \equiv 25 \pmod{77}$$

b) $5^{43} \pmod{77}$ używając chinijskiego twierdzenia

$$77 = 11 \times 7$$

$$5^{43} \pmod{7} \equiv 5 \pmod{7}$$

$$\phi(7) = 6 \quad 43 \pmod{6} \equiv 1$$

$$5^{43} \pmod{11} \equiv 5^3 \pmod{11} \equiv 4 \pmod{11}$$

$$\phi(11) = 10 \quad 43 \pmod{10} \equiv 3$$

$$\begin{cases} x \equiv 5 \pmod{7} & x = 5 + 7k \equiv 4 \pmod{11} \\ x \equiv 4 \pmod{11} & 7k \equiv -1 \pmod{11} \equiv 10 \pmod{11} \end{cases}$$

$$x = 5 + 3 \times 7 = 26$$

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

$$k = 7 \times 8 \pmod{11} \equiv 3 \pmod{11}$$

8) Stosując metode potęgowania

obliczyć $3^{12} \bmod 25$.

$$3^2 \bmod 25 \equiv 9 \bmod 25$$

$$3^4 \bmod 25 \equiv 81 \bmod 25 \equiv 6$$

$$3^8 \bmod 25 = (3^4)^2 \bmod 25 = 6^2 \bmod 25 \equiv 11$$

$$3^{12} \bmod 25 = 3^8 \cdot 3^4 \bmod 25 \equiv 11 \cdot 6 \bmod 25 \equiv 16$$

9) Wyznaczyć wykładnik deszyfrujący w RSA

2 krokiem publicznym $(n, e) = (55, 7)$

$$n = 55 = 5 \times 11 \quad \phi(55) = \phi(11) \times \phi(5) = 10 \times 4 = 40$$

$$e \cdot d \equiv 1 \pmod{40}$$

$$e = 7$$

$$40 = 5 \times 7 + 5$$

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

$$5 = 2 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$1 = 5 - 2 \times 2 = 5 - (7-5) \times 2 =$$

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

$$= 3 \times (40 - 5 \times 7) - 2 \times 7 = 3 \times 40 - 17 \times 7$$

$$- 17 \times 7 \equiv 1 \pmod{40}$$

$$23 \times 7 \equiv 1 \pmod{40}$$

$$d = 23$$

10) Wyznaczyć $k \in \mathbb{N}$ takie, że $x^{6k} \equiv x^2 \pmod{19}$

$$\forall x \in \mathbb{Z}_{19}^*$$

$$19 = 7 \times 19$$

11)

$$12) \quad 12x \equiv 15 \pmod{33}$$

$$4x \equiv 5 \pmod{11}$$

$$\begin{aligned} 11 &= 4 \cdot 2 - 3 & 1 &= 4 - 3 = 4 - (11 - 4 \cdot 2) = \\ 4 &= 1 \cdot 3 + 1 & &= 3 \cdot 4 - 11 \\ 3 &= 3 \cdot 1 + 0 & x &\equiv 4 \pmod{11} \end{aligned}$$

$$x = 4, 15, 26$$

13)

15)

21) W ciele $F_2[x]/(x^3+x+1)$ wyznaczyć
wielomian minimalny elementu $\alpha = \bar{x}^2 + \bar{x}$

$$x^3+x+1=0 \Rightarrow x^3=x+1$$

$$\alpha = \bar{x}^2 + \bar{x}$$

$$\begin{aligned}\alpha^2 &= (\bar{x}^2 + \bar{x})^2 = \bar{x}^4 + \bar{x}^2 = \bar{x}(\bar{x}+1) + \bar{x}^2 = \\ &= 2 \cdot \bar{x}^2 + \bar{x} = \bar{x} \quad (2\bar{x}=0)\end{aligned}$$

$$\begin{aligned}\alpha^3 &= \alpha \cdot \alpha^2 = (\bar{x}^2 + \bar{x}) \cdot \bar{x} = \bar{x}^3 + \bar{x}^2 = \\ &= (\bar{x}+1) + \bar{x}^2 = \bar{x}^2 + \bar{x} + 1\end{aligned}$$

$$\alpha^3 = \alpha + 1 \Rightarrow \alpha^3 + \alpha + 1$$

minimalny wielomian: $\bar{x}^3 + \bar{x} + 1$

23) Sprawdź czy na wykresie

$E: y^2 = x^3 + 2x + 3$ nad ciałem \mathbb{F}_p dla $p=127$
istnieje punkt $(x,y) \in E$, taki, że $x=5, y \in \mathbb{F}_p$

$$y^2 = 125 + 10 + 3 = 138 \equiv 11 \pmod{127}$$

25) f) 8 jest świadkiem złożoności 24 w testie pierwszości millera-rabina.

Maksymalna potęga 2 dającego $n-1$

$$20 = 2^2 \cdot 5 \quad s=2, d=5 \quad 2^s \cdot d = n-1$$

Sprawdzamy czy $a^d \not\equiv 1 \pmod{n}$

$$8^5 \pmod{21}, \quad 8^2 \pmod{21} = 1$$

$$8^4 \pmod{21} = (8^2)^2 \pmod{21} = 1$$

$$8^5 \pmod{21} = 8$$

Sprawdzamy $a^{2^r d} \not\equiv n-1 \pmod{n}$ dla $\{0, \dots, s-1\}$

$$8^{2^0 \cdot 5} = 8^5 \equiv 8 \pmod{21}$$

$$8^{2^1 \cdot 5} = 8^{10} \equiv 8^5 \pmod{21} \equiv 64 \pmod{21} \equiv 1 \pmod{21}$$

Ponieważ jeden z warunków zostanie spełniony,

8 nie jest świadkiem złożoności 21

a) 2 jest świadkiem złożoności 21 w testie
pierwoszkości Fermata.

jesli n jest pierwsze, a a jest niewydaelne
przez n , to:

$$a^{n-1} \equiv 1 \pmod{n}$$

$$2^{20} \equiv 2^4 \cdot 2^{16} \equiv 16 \cdot 16 \equiv 4 \pmod{21}$$

$2^{20} \not\equiv 1 \pmod{21}$, a więc 2 jest świadkiem
złożoności 21.

TEST

Zadanie 1.

RSA $n = 143$, $e = ?$, $d = ?$

$$d \cdot e = 1 \pmod{\varphi(n)}$$

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

$$\varphi(143) = (11-1)(13-1) = 10 \cdot 12 = 120$$

$$120 = 17 \cdot 7 + 1$$

$$1 = 120 - 17 \cdot 7$$

$$-17 \cdot 7 = 1 \pmod{120}$$

$$-17 \pmod{120} = 103$$

Zadanie 2.

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{9} \\ x \equiv 2 \pmod{7} \end{cases}$$

$$x = 3 + 5a$$

$$3 + 5a \equiv 4 \pmod{9}$$

$$5a \equiv 1 \pmod{9}$$

$$a = 2$$

$$a = 2 + 9b$$

$$x = 13 + 45b$$

$$\begin{cases} x \equiv 13 \pmod{45} \\ x \equiv 2 \pmod{9} \end{cases}$$

$$13 + 45c \equiv 2 \pmod{7}$$

$$45c \equiv -11 \pmod{7}$$

$$45c \equiv -4 \pmod{7}$$

$$45c \equiv 3 \pmod{7}$$

$$15c \equiv 1 \pmod{7}$$

$$c = 1$$

$$c = 1 + 7d$$

$$\begin{aligned} x &= 13 + 45b = 45(1+7d) + 13 = \\ &= 45 + 315d + 13 = 58 + 315d \end{aligned}$$

$$x \equiv 58 \pmod{315}$$

Zadanie 3.

$$e=2, n=312$$

$$\varphi(312) = 2^3 \cdot 3 \cdot 13$$

312	2
156	2
78	2
39	3
13	

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

$$\varphi(3) = 2 \quad \varphi(312) = 2^3 \cdot 12 = 96$$

$$\varphi(13) = 12$$

$$\text{NWD}(2, 96) = 2 \quad \text{NIE 1 STNIĘJE}$$

Zadanie 4

W ciele $\mathbb{F}[x]_5 / (x^2 + 3x + 4)$ wyznaczyć:

a) $(3x+4) \cdot (2x+3) = 6x^2 + 9x + 8x + 12 =$

$$= 6x^2 + 17x + 12 = x^2 + 2x + 2$$

$$x^2 = -3x - 4$$

$$(-3x - 4) + 2x + 2 = -x - 2 = 4x + 3$$

b) element odwrotny $\beta = 4x + 1$

$$(4x+1)y \equiv 1 \pmod{x^2 + 3x + 4}$$

$$(4x+1)(ax+b) \equiv 1 \pmod{x^2 + 3x + 4}$$

$$4ax^2 + 4bx + ax + b \equiv 1 \pmod{x^2 + 3x + 4}$$

$$4ax^2 + (4b+a)x + b \equiv 1 \pmod{x^2 + 3x + 4}$$

$$-12ax - 16a \equiv -2ax - a \pmod{5}$$

$$-2ax - a + (4b+a)x - b \equiv 1$$

$$\begin{cases} -a + 4b \equiv 0 \pmod{5} & a \equiv 2 \pmod{5} \\ b - a \equiv 1 \pmod{5} & b \equiv 3 \pmod{5} \end{cases}$$

$$b \equiv a + 1$$

$$\beta^{-1} \equiv 2x + 3$$

Zadanie 5

Lecgandre, Twierdzenie
reszt

