

# Notatki ETZ

1) Wyznaczyć  $x, y$  takie, że

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

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

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

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

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

Euclides

$$3 = 12 - 9 = 12 - (21 - 12) =$$

$$= 2 \cdot 12 - 21 = 2 \cdot (33 - 21) - 21 =$$

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

$$x = 2, y = 3$$

2) Wyznaczyć  $g^{-1} \pmod{23}$ .

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

Euclides

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

$$1 = 2 \cdot 23 - 5 \cdot 9$$

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

+ 3) Wyznaczyć  $x$

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

$$x = 3 + 5a$$

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

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

$$a \equiv 2$$

$$a = 2 + 9b$$

$$x = 13 + 45b$$

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

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

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

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

$$c \equiv 1$$

$$c = 1 + 7d$$

$$x = 13 + 45b = 13 + 45(1 + 7d) = 58 + 315d$$

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

$$+ 4) x^{23} \equiv 3 \pmod{200}$$

$$e = 23, n = 200$$

$$200 = 5^2 \cdot 2^3$$

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

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

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

$$\text{NWD}(80, 23) = 1$$

Euclides

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

...

$$1 = 7 \cdot 23 - 2 \cdot 80$$

$$d = 7$$

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

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

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

$$= 9 \cdot 243 = 9 \cdot 43 = 387 =$$

$$= 187$$

$$x \equiv 187$$

6) Uzasadnić, że  $7^k \equiv 1 \pmod{990}$  dla pewnego  $k > 0$  i

$$990 = 495 \cdot 2 = 99 \cdot 5 \cdot 2 =$$

$$= 33 \cdot 5 \cdot 3 \cdot 2 = 11 \cdot 5 \cdot 3^2 \cdot 2$$

$$\varphi(2) = 1, \varphi(3^2) = 3 \cdot 2, \varphi(5) = 4$$

$$\varphi(11) = 10, \varphi(990) = 240$$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$a = 7, n = 990$$

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

7) Obliczyć  $5^{122} \pmod{77}$  używając Eulera

$$77 = 11 \cdot 7, \varphi(77) = 60$$

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

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

8)  $5^{43} \pmod{77}$  twierdzenie chin'skie

$$\varphi(7) = 6, 43 \pmod{6} \equiv 1$$

$$\varphi(11) = 10, 43 \pmod{10} \equiv 3$$

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

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

$$\begin{cases} x \equiv 5 \pmod{7} & k = 7 \cdot 8 \pmod{11} \\ x \equiv 4 \pmod{11} & k = 3 \pmod{11} \end{cases}$$

$$5 + 7k \equiv 4 \pmod{11} \quad x = 5 + 3 \cdot 7$$

$$7k \equiv 10 \pmod{11} \quad = 26$$

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

$$8) 3^{12} \pmod{25}$$

$$3^2 \pmod{25} = 9 \pmod{25}$$

$$3^4 \pmod{25} = \dots$$

$$3^8 \pmod{25} = \dots$$

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

9) Wyznaczyć współczynniki deszyfrujący RSA dla  $p, q = (55, 7)$ .

$$55 = 11 \cdot 5, \varphi(55) = 40$$

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

$$e = 7$$

$$40 = 5 \cdot 7 + 5$$

$$7 = 1 \cdot 5 + 2 \quad \text{Euclides}$$

...

$$1 = 3 \cdot 40 - 17 \cdot 7$$

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

$$23 \cdot 7 \equiv 1$$

$$d = 23$$

12)  $12x \equiv 15 \pmod{33}$   $z_3$

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

$$11 = 4 \cdot 2 + 3$$

$$\text{Euclides } 1 = 3 \cdot 4 - 11$$

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

$$x = \{4, 15, 26\}$$

22) Oblicz  $\left(\frac{92}{175}\right)$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$\left(\frac{92}{175}\right) = \left(\frac{46}{175}\right) \cdot \left(\frac{2}{175}\right) = \left(\frac{23}{175}\right) \cdot \left(\frac{2}{175}\right)^2$$

$$\left(\frac{175}{23}\right) \cdot (-1)^{\frac{175-1}{2} \cdot \frac{23-1}{2}} = \left(\frac{14}{23}\right) \cdot (-1)$$

$$= \left(\frac{7}{23}\right) \cdot \left(\frac{2}{23}\right)^{(-1)} = \left(\frac{23}{7}\right) \cdot (-1)^{\frac{23-1}{2} \cdot \frac{7-1}{2}} =$$

$$= \left(\frac{2}{7}\right) = 1$$



Z5 6) Wykazać, że

8 jest świadkiem

złożoności 21 u teście  
pierwszości Millera-Rabina

Maks. potęga 2 dzieląca  $n-1$   
 $20 = 2^2 \cdot 5$ ,  $S=2$ ,  $d=5$

$$2^S \cdot d = n-1$$

Sprawdzamy  $a^d \not\equiv 1 \pmod n$

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

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

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

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

Ponieważ jeden z warunków  
został spełniony, 8 nie jest  
świadkiem złożoności 21.

a) Wykazać, że 2 jest świadkiem  
złożoności 21 w teście  
pierwszości Fermata.

Jeśli  $n$  jest pierwsze,  
a  $a$  jest niepodzielne  
przez  $n$ , to:

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

$$2^{20} \equiv 1 \pmod{21}$$

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

SYMBOL JACOBIEGO

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

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

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

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \pm 1 \pmod 8 \\ -1 & \pm 3 \pmod 8 \end{cases}$$

$$\left(\frac{1}{n}\right) = 1, \left(\frac{-1}{n}\right) = -1 \text{ dla } n \equiv 3 \pmod 4$$

$$\left(\frac{-1}{n}\right) = 1 \text{ dla } n \equiv 1 \pmod 4$$

Zad. 3. Czy istnieje

$$k^2 \equiv 312 \pmod{317}$$

$$e=2, n=312 \leftarrow 317$$

$$\varphi(312) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(13) = 96$$

NWD(2, 96) = 2, nie istnieje

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

a) wyznaczyć  
 $(3x+4) \cdot (2x+3)$

$$(3x+4) \cdot (2x+3) =$$

$$= 6x^2 + 9x + 8x + 12 \equiv$$

$$= x^2 + 2x + 2$$

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

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

$$= 4x + 3$$

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

$$(4x+1)(ax+b) \equiv 1 \pmod X$$

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

$$-12ax - 16a \equiv -2ax - a$$

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

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

$$a \equiv 2 \pmod 5$$

$$b \equiv 3 \pmod 5$$

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

16) Należy podać przykłady  
wielomianów nierozkładalnych  
stopni  $d=2, 3$  dla

$$F_2: d=2: x^2 + x + 1$$

$$d=3: x^3 + x + 1$$

$$F_3: d=2: x^2 + 1$$

$$d=3: x^3 + x + 1$$

$$F_5: d=2: x^2 + 2$$

$$d=3: x^3 + 2x + 1$$

Zad 5 Sprawdzić, czy

pierścień ilorazowy jest ciałem.

$$R = \mathbb{F}_{29}[x] / (x^2 + 5x - 3) \quad (X)$$

$$\Delta = 5^2 + 4 \cdot 3 = 37$$

$$\left(\frac{37}{29}\right) = \left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3$$

$$\left(\frac{2}{29}\right) = (-1)^{\frac{29^2-1}{8}} = (-1)^{105} = -1$$

$$\left(\frac{2}{29}\right) = (-1)^{\frac{29^2-1}{8}} = (-1)^{105} = -1$$

$$\left(\frac{8}{29}\right) = (-1)^3 = -1$$

A więc 8 nie jest resztą kwadratu,  
dlatego 37 nie jest.  
Pierścień jest ciałem.

b) Wyznaczyć wielomian  
unormowany minimalnego  
stopnia  $f \in \mathbb{F}_{29}[x]$ , taki że  
 $f(3\bar{x}+5) = 0$   
 $f = x^2 + ax + b$   
 $\bar{x}^2 = 3 - 5\bar{x}$

$$(3+5\bar{x})^2 + a(3\bar{x}+5) + b = 0$$

$$9\bar{x}^2 + 30\bar{x} + 25 + 3a\bar{x} + 5a + b = 0$$

$$9(3-5\bar{x}) + 30\bar{x} + 25 + 3a\bar{x} + 5a + b = 0$$

$$5) \text{ Czy } 11 \mid 3^{1005} + 5^{1003}$$

$$3^{1005} + 5^{1003} \equiv 0 \pmod{11}$$

$$a^{p-1} \equiv 1 \pmod p, \quad p=11$$

$$3^{10} \equiv 1 \pmod{11}$$

$$5^{10} \equiv 1 \pmod{11}$$

$$3^{1005} = 3^5 \pmod{11} \equiv 1 \pmod{11}$$

$$5^{1003} = 5^3 \pmod{11} \equiv 4 \pmod{11}$$

$$1 + 4 = 5 \not\equiv 0 \pmod{11}$$