

## TEST 2

### Zadanie1

Znaleźć logarytm dyskretny  $\log_5 8$  w  $Z^{*13}$  i w  $Z^{*19}$ .

$\log_5 8 = 3$  w  $Z^{13}$

$\log_5 8 = 4$  w  $Z^{19}$

```
public Integer log4( Integer x ){
    Integer ret=4;
    for (int i=1; i<x; i++ ){
        ret=ret*4;
    }
    return ret;
}

public Integer log5( Integer x ){
    Integer ret=5;
    for (int i=1; i<x; i++ ){
        ret=ret*5;
    }
    return ret;
}

public Integer Z_11( Integer x ){ return x%11; }
public Integer Z_12( Integer x ){ return x%12; }
public Integer Z_13( Integer x ){ return x%13; }
public Integer Z_17( Integer x ){ return x%17; }
public Integer Z_19( Integer x ){ return x%19; }

@Test
public void test2(){

    // Znaleźć logarytm dyskretny log58 w Z*13 i w Z*19 .
    // log5 8 =

    //      8      x
    // log5 -> 8=5
    for (int i=0;i<100;i++){
        if ( Z_13( log5( i ) )==8) System.out.println( "log5 8 = " + i + " w Z13" );
    }

    for (int i=0;i<100;i++){
        if ( Z_19( log5( i ) )==8) System.out.println( "log5 8 = " + i + " w Z19" );
    }
}
```

## Zadanie 2

Znaleźć element odwrotny do 8 w  $Z^{*17}$ . = 15

Znaleźć element odwrotny do 8 w  $Z^{*13}$ . = 5

Czy istnieje element odwrotny do 8 w  $Z^{*12}$ ?

- nie, 8 nie jest względnie pierwsze w pierścieniu  $Z_{12}$  ponieważ:  $4 \cdot 2 = 8$  i  $4 \cdot 3 = 12$

```
// https://www.youtube.com/watch?v=x12La1oBKHM
int a=8;
for ( int i=0;i<1000;i++){
    if ( Z_17(a*i)==1 ) { System.out.println( "8^-1 Z17 = " + i ); break; }
}
```

## Zadanie 3

Podać warunek konieczny i wystarczający odwracalności elementu  $x$  należącego do  $Z_m$ .

$x$  musi być względnie pierwsze z  $m$

Jak zastosować twierdzenie Eulera do obliczania elementu odwrotnego do  $x$  w  $Z_m$ .

Jak zastosować rozszerzony algorytm Euklidesa do obliczania elementu odwrotnego do  $x$  w  $Z_m$ .

$Z_{17} \quad a=8$   
 $8^{-1}=?$

a	b	$x_a$	$y_a$	$x_b$	$y_b$
8	17	1	0	0	1
8	$17 \% 8 = 1$ $17/8 = 2$	1	0	$0 - (1 \cdot 2) = -2$	$1 - (0 \cdot 2) = 1$

przykład: znaleźć odwrotny do 8 w  $Z_{13}$

a	b	$x_a$	$y_a$	$x_b$	$y_b$
8	13	1	0	0	1
8	$13 \% 8 = 5$ $13/8 = 1$	1	0	$0 - 1 \cdot 1 = -1$	$1 - 0 \cdot 1 = 1$
$8 \% 5 = 3$ $8/5 = 1$	5	$1 - (-1 \cdot 1) = 2$	$0 - (-1 \cdot 1) = 1$	-1	1
$5 \% 3 = 2$ $5/3 = 1$	2	2	-1	$-1 - (2 \cdot 1) = -3$	$1 - (-1 \cdot 1) = 0$
$3 \% 2 = 1$ $3/2 = 1$	2	5	-1	-3	0
$2 \% 1 = 0$	1	5	-1		

$$\begin{aligned}
 5 \cdot 8 - 1 \cdot 13 &= 1 \\
 5 \cdot 8 &= 1 \\
 40 \% 13 &= 1 \\
 8^{-1} &= 5
 \end{aligned}$$

#### Zadanie 4

Ile jest elementów odwracalnych w pierścieniu  $Z_m$ . Wykazać, że stanowią one grupę.

w pierścieniu  $Z_m$  jest tyle odwracalnych elementów ile jest liczb pierwszych w tym pierścieniu czyli  $\varphi(m)$

Stanowią one grupę ponieważ

jeśli  $p^{-1}=q$  to  $p=q^{-1}$

ponieważ:  $p \odot q = 1$  to  $q \odot p = 1$

#### Zadanie 5

Oblicz wartość funkcji Eulera

a)  $\varphi(3458) = \varphi(2) * \varphi(1729) = \varphi(2) * \varphi(7) * \varphi(13) * \varphi(19) = 1*1*1*1 = 1$

b)  $\varphi(2^{1000}) = 1/2 * (2^{1000}) = 2^{999}$

c)  $\varphi(2^n)$ , gdzie  $n$  należy do  $N = 2^{(n-1)}$

d)  $\varphi(3^n)$ , gdzie  $n$  należy do  $N = (3^n)/1,5$

e)  $\varphi(\varphi(2^{1000})) = \varphi(2^{999}) = 2^{998}$

$x=2^n = x=2*2*2*2$  czyli ma tylko dzielnik 2, a więc  $\varphi(2^n) = n/2$

$\varphi(a*b) = \varphi(a) * \varphi(b)$

```
for ( int i=1;i<900;i++){  
    if ( 1729%i==0 ){ System.out.println( i ); }  
}
```

rozkład : 7, 13, 19, 91, 133, 247

liczby pierwsze : 7, 13,

a)  $\varphi(3458) = \varphi(2) * \varphi(7) * \varphi(13) * \varphi(19) = 1$

#### Zadanie 6

Podaj definicję funkcji jednokierunkowej i przykład takiej funkcji.

Funkcja jednokierunkowa to zestaw działań matematycznych które działając na wartość wejściową dają pewien wynik, jednak uzyskanie wartości wejściowej z wyniku jest niemożliwe.

Najprostrzą taką funkcją jest funkcja modulo, zwraca ona resztę z dzielenia argumentu przez podstawę. mając podstawę i wynik nie określimy wartości argumentu - jedynie zbiór w którym argument się znajduje.

### Zadanie 7

Rozwiązać układ kongruencji

$$x \equiv 6 \pmod{7} \quad x_1 = 20$$

$$x \equiv 7 \pmod{13} \quad x_1 = 20$$

$$x \equiv 4 \pmod{5} \quad x_2 = 29$$

$$x \equiv 7 \pmod{11} \quad x_2 = 29$$

$$\begin{aligned} x &\equiv 6 \pmod{7} \\ x &\equiv 7 \pmod{13} \end{aligned} \Rightarrow \left| \begin{array}{l} -6 \\ -1 \end{array} \right| \begin{array}{l} x-6 \equiv 0 \pmod{7} \\ x-6 \equiv 1 \pmod{13} \end{array}$$

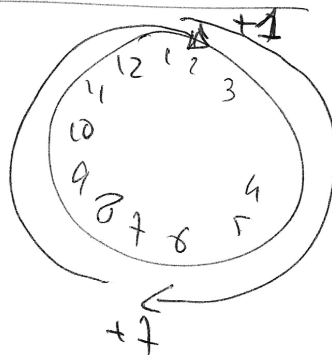
①

$$13(0+7) \pmod{13} = 7$$

$$(7+7) \pmod{13} = 1 \Rightarrow$$

$$a) \quad x+7 = \textcircled{0} \pmod{7} ; \quad x+7+7 = x \pmod{7}$$

$$b) \quad x+7+7 = \textcircled{+1} \pmod{13}$$



$$x = 7+7 \quad x \equiv 0 \pmod{7}$$

$$x \equiv 1 \pmod{13}$$

$$+6 \quad x = 7+7+6 \equiv 6 \pmod{7}$$

$$x = 7+7+6$$

$$= 1 + 6 = 7 \pmod{13} !$$

$$x = 6+7+7 = 20 !$$

$$\begin{array}{l|l} x \equiv 4 \pmod{5} & x \equiv 0 \pmod{5} \\ x \equiv 7 \pmod{11} & x \equiv 3 \pmod{11} \end{array} \quad \begin{array}{c} -4 \\ -4 \end{array}$$

⑦

$$\frac{11}{5} = 2\frac{1}{5}$$

$$11 \% 5 = 1$$

$$2 \cdot 5 \% 11 = -1$$

$$(-1 + 11) \pmod{11} = 10$$

$$2 \cdot 5 \cdot 10 = 100 = 1 \pmod{11}$$

$$3 \cdot 2 \cdot 5 \cdot 10 = 300 \pmod{11} = 3$$

$$x = 300 \quad x \equiv 0 \pmod{5}$$

$$x \equiv 300 \quad x \equiv 3 \pmod{11}$$

$$x = 300 + 4 \quad x \equiv 4 \pmod{5}$$

$$x = 300 + 4 \quad x \equiv 4 + 3 \pmod{11}$$

$$x = 304$$

$$x - 55 = 249 - 55 = 194 - 55 = 139$$

$$x = 139 - 55 = 84 - 55 = \underline{29}$$

$$\underline{\underline{x = 29}} \quad \text{!}$$

$$x \equiv 6 \pmod{7} \quad x_1 = 20$$

$$x \equiv 7 \pmod{13} \quad x_1 = 20$$

$$x \equiv 4 \pmod{5} \quad x_2 = 29$$

$$x \equiv 7 \pmod{11} \quad x_2 = 29$$

$$x = 20 \pmod{7 \cdot 13} = 20 \pmod{91} = 1294$$

$$x = 29 \pmod{5 \cdot 11} = 29 \pmod{55} = 1294$$

w

$$55^{-1} \pmod{91} = 48$$

$$\begin{array}{l|l} x \equiv 20 \pmod{91} & x \equiv -9 \pmod{91} = 82 \pmod{91} \\ x \equiv 29 \pmod{55} & x \equiv 0 \pmod{55} \end{array} \quad \begin{array}{l} -29 \\ \end{array}$$

(3)

$$55 \equiv 0 \pmod{55}$$

$$48 \cdot 55 \equiv 1 \pmod{91} \leftarrow$$

$$82 \cdot 48 \cdot 55 \equiv 82 \pmod{91}$$

$$82 \cdot 48 \cdot 55 \% (91 \cdot 55) = 1265$$

$$x = 1265 + 29 = 1294$$

$$55^{-1} = 48 \pmod{91}$$

# Zadanie 8

Rozwiązać układ kongruencji

- $x \equiv 6 \pmod{7} = 494$
- $x \equiv 12 \pmod{13} = 494$
- $x \equiv 4 \pmod{5} = 494$
- $x \equiv 10 \pmod{11} = 494$

$$\begin{array}{l|l} x \equiv 6 \pmod{7} & x \equiv 0 \pmod{7} \\ x \equiv 12 \pmod{13} & x \equiv 6 \pmod{13} \\ x \equiv 4 \pmod{5} & x \equiv 0 \pmod{5} \\ x \equiv 10 \pmod{11} & x \equiv 6 \pmod{11} \end{array} \begin{array}{l} \\ +6 \\ +4 \\ \end{array}$$

$$7+7 = 0 \pmod{7}$$

$$7+7 = 1 \pmod{13}$$

$$6 \cdot 7 \cdot 7 = 0 \pmod{7}$$

$$6 \cdot 7 \cdot 7 = 6 \pmod{13}$$

$$7 \cdot 13 = 91$$

$$-\boxed{27+6} = 33$$

$$x = 33 + 6$$

$$x \equiv 294 + 6 = 300$$

$$x = 39$$

$$0 \pmod{5}$$

$$6 \pmod{11}$$

$$5 \cdot 9 = 0 \pmod{5}$$

$$5 \cdot 9 = 1 \pmod{11}$$

$$5 \cdot 9 \cdot 6 = 6 \pmod{11} = 270$$

$$270 - 55 \cdot x = 30 \quad | +4 | = 54$$

$$x \equiv 39 \pmod{91}$$

$$x \equiv 54 \pmod{55}$$

$$-15 \pmod{91}$$

$$-15 \pmod{91} = 76$$

$$0 \pmod{55}$$

$$0 \pmod{55}$$

$$48 \cdot 55 = 1 \pmod{91}$$

$$-15 \pmod{91} = 76$$

$$15 \cdot 48 \cdot 55 =$$

$$76 \cdot 48 \cdot 55 = 0 \pmod{55}$$

$$440 + 54 = 494$$

$$76 \cdot 48 \cdot 55 = -15 \pmod{91} = 440$$

# Zadanie 9

Znaleźć 2 ostatnie cyfry zapisu siódmkowego liczby  $2^{1000}$

Zad 9 Znaleźć 2 ostatnie cyfry  
zapisu siódmkowego liczby  $2^{1000}$

①

$$2 = 2 \bmod (49)$$

$$2^2 = 4 \bmod (49)$$

$$2^3 = 8 \bmod (49)$$

$$2^4 = 16 \bmod (49)$$

$$2^5 = 32 \bmod (49)$$

$$2^6 = 64 \bmod (49)$$

$$2^7 = 128 \equiv \bmod (49)$$

$$2^7 = 128 \equiv 30 \bmod (49)$$

$$2^8 = 256 \equiv 11 \bmod (49)$$

$$2^9 = 512 \equiv 22 \bmod (49)$$

$$2^{10} = 1024 \equiv 44 \bmod (49)$$

$$2^{11} = 2048 \equiv 39 \bmod (49)$$

$$2^{12} = 4096 \equiv 29 \bmod (49)$$

$$2^{13} = 8192 \equiv 9 \bmod (49)$$

$$2^{14} = 16384 \equiv 18 \bmod (49)$$

$$2^{15} = 32768 \equiv 36 \bmod (49)$$

$$2^{16} = 65536 \equiv 23 \bmod (49)$$

$$2^{17} =$$

$$2^{21} = \dots \equiv 1 \bmod (49)$$

$$2^{1000} \bmod (49) =$$

$$2^{21} \cdot 2^{21} \dots \cdot 2^{13} \bmod (49) =$$

$$2^{21} \bmod (49) \cdot 2^{21} \bmod (49) \cdot 2^{13} \bmod (49) =$$

$$1 \cdot 1 \dots \cdot 2^{13} \bmod (49) =$$

$$2^{13} = 1024 = 8$$

$$= 8192 \equiv 9 \bmod (49)$$

a zatem 2 ostatnie  
cyfry to

09

$$2^{1000} \bmod (49) = \underline{\underline{09}}$$



# Zadanie 10

Dodać następujące wielomiany (bajty) w pierścieniu  $Z[x] = (x^8 + x^4 + x^3 + x + 1) \text{ GF}(2^8)$

- a) '57'+'02'
- b) '03'+'03'
- c) 'FF'+'0F'

$$\begin{array}{r} A = 0x57 = 0101 | 0111 \\ B = 0x02 = 0000 | 0010 \\ \hline 0101 | 0101 \\ \hline 5 \quad 5 \end{array}$$

$$+ \begin{array}{r} 011 \\ \dots 011 \\ \hline \dots 000 \end{array}$$

$$0x57 + 0x02 = \underline{0x55}$$

$$0x03 + 0x03 = \underline{0}$$

$$0xFF + 0x0F = \text{XOR} + \begin{array}{r} 1111 | 1111 \\ 0000 | 1111 \\ \hline 1111 | 0000 \\ \hline F \quad 0 \end{array}$$

$$0xFF + 0x0F = \underline{0xF0}$$