Rok akademicki 2022 -2023, półsemestr letni

TEST 2

Zadanie1
Znaleźć logarytm dyskretny log58 w Z*13 i w Z*19 .

log5 8 = 3 w Z13
log5 8 = 4 w Z19

```
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; }

        if (true){
        for (int i=0;i<100;i++){
                if ( Z_19( log5( i ))==8) { System.out.println( "log5 8 = " + Z_19(i) + " w Z19" ); break; }
        }
        for (int i=0;i<100;i++){
                if ( Z_13( log5( i ))==8) { System.out.println( "log5 8 = " + Z_13(i) + " w Z13" ); break; }
        }}

        // log5 8 = 4 w Z19
        // log5 8 = 3 w Z13
```

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 pierscieniu Z12 ponieważ: 4*2=8 i 4*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 Zm.
x musi być względnie pierwsze z m

Jak zastosować twierdzenie Eulera do obliczania elementu odwrotnego do .

Jak zastosować rozszerzony algorytm Euklidesa do obliczania elementu odwrotnego do x nal Zm.

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

a	b	xa	ya	xb	yb
8	17	1	0	0	1
8	17%8 = 4; 17/8=2	1	0	$0-(1\cdot2)$ -2	$1-(0\cdot2)$ 1

przykład: znaleźć odwrotny do 8 w Z13

a	b	xa	ya	xb	yb
8	13	1	0	0	1
8	13%8=5; 13/8=1; 5 (1)	1	0	$0-1\cdot1$ -1	$1-0\cdot1$ 1
8%5=3; 8/5=(1); 3	5	$1-(-1\cdot1)$ 2	$0-(1\cdot1)$ -1	-1	1
3	5%3=2; 5/3=1; 2 (1)	2	-1	$-1-(2\cdot1)$ -3	$1-(-1\cdot1)$ 0
3%2=1; 3/2=1; 1 (1)	2	$2-(-3\cdot1)$ 5	$-1-(0)$ -1	-3	0
1 1	2%1=0; 0	$\boxed{5}$	$\boxed{-1}$		

$5\cdot8-1\cdot13=1$
$5\cdot8=1$
$40\%13=1$

$8^{-1}=5$

Zadanie 4
Ile jest elementów odwracalnych w pierścieniu Zm. Wykazać, że stanowią one grupę.
w pierścieniu Zm jest tyle odwracalnych elementów ile jest liczb pierwszych w tym pierścieniu czyli φ(m)
Stanowią one grupę ponieważ
jeśli $p^{-1}=q$ to $p=q^{-1}$
ponieważ: pΘq =1 to qΘp =1

Zadanie 5
Oblicz wartość funkcji Eulera

a) φ(3458) = φ (2) * φ (1729) = φ (2) * φ (7) *φ (13) * φ (19) = 1*1*1*1 = 1
b) φ(2^1000) = 1/2*(2^1000) = 2^999
c) φ(2^n), gdzie n należy do N =2^(n-1)
d) φ(3^n), gdzie n należy do N = (3^n)/1,5
e) φ(φ(2^1000)) = φ (2^999) = 2^998

x=2^n = x=2*2*2*2 czyli ma tylko dzielnik 2, a więc φ(2^n) - n/2
φ (a*b) = φ (a) * φ (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) φ(3458) = φ (2) * φ (7) *φ (13) * φ (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 ≡ 6 (mod 7)   x1 = 20
x ≡ 7 (mod 13) x1 = 20
x ≡ 4 (mod 5)   x2 = 29
x ≡ 7 (mod 11) x2 = 29

1

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

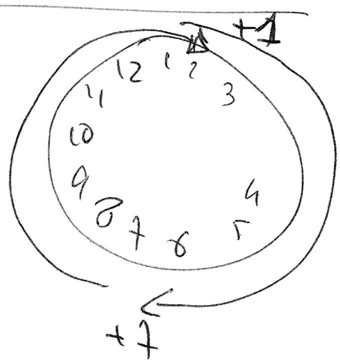
$$\cancel{13}(0+7) \bmod 13 = 7$$

$$(7+7) \bmod 13 = 1 \Rightarrow$$

---

a) $x+7 = 0 \bmod 7$; $x+7+7 = x \bmod 7$

b) $x+7+7 = (+1) \bmod 13$



$x = 7+7$ $x \equiv 0 \bmod 7$

$x \equiv 1 \bmod 13$

$+6$ $x = 7+7+6 \equiv 6 \bmod 7$

$x = 7+7+6$

$= 1 + 6 = 7 \bmod 13$!

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

$x \equiv 4 \mod 5$ $\quad$ | -4 | $\quad x \equiv 0 \mod 5$ $\quad$ 7

$x \equiv 7 \mod 11$ $\quad\quad\quad\quad\quad\;\; x \equiv 3 \mod 11$

$\frac{11}{5} = 2\frac{1}{5}$ $\quad\quad$ $11 \% 5 = \underline{1}$

$2 \cdot 5 \% 11 = \underline{-1}$

$(-1+11) \mod 11 = 10$

$2 \cdot 5 \cdot 10 = 100 = 1 \mod (11)$

$3 \cdot 2 \cdot 5 \cdot 10 = 300 \mod (11) = 3$

$x = 300 \quad x \equiv 0 \mod 5$

$x \equiv 300 \quad x \equiv 3 \mod 11$

$x = 300+4 \quad x \equiv 4 \mod 5$

$x = 300+4 \quad x \equiv 4+3 \mod 11$

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

$X = 304$ $\quad$ $x = 139 - 55 = 84 - 55 = \underline{29}$

$\underline{\underline{X = 29}}$!

$x \equiv 6 \pmod 7$ $x1 = 20$
$x \equiv 7 \pmod{13}$ $x1 = 20$
$x \equiv 4 \pmod 5$ $x2 = 29$
$x \equiv 7 \pmod{11}$ $x2 = 29$

$x = 20(\bmod 7*13) = 20 \bmod (91) = 1294$
$x = 29(\bmod 5*11) = 29 \bmod (55) = 1294$
w
$55^{-1} \bmod (91)=48$

$$\left.\begin{array}{l} X \equiv 20 \bmod (91) \\ X \equiv 29 \bmod (55) \end{array}\right| -29 \left| \begin{array}{l} X \equiv -9 \bmod (91) = 82 \bmod (91) \\ X \equiv 0 \bmod (55) \end{array}\right.$$

3

$55 = 0 \bmod (55)$

$48 \cdot 55 = 1 \bmod (91)$

$82 \cdot 48 \cdot 55 = 82 \bmod (91)$

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

$X = 1265 + 29 = 1294$

$55^{-1} = 48 \bmod (91)$

Zadanie 8

Rozwiązać układ kongruencji
x 6 (mod 7) = 494
x 12 (mod 13) = 494
x 4 (mod 5) = 494
x 10 (mod 11) = 494

1

$x \equiv 6 \mod (7)$ | $x \equiv 0 \mod (7)$
$x \equiv 12 \mod (13)$ | $x \equiv 6 \mod (13)$ | $+6$
$x \equiv 4 \mod (5)$ | $x \equiv 0 \mod (5)$
$x \equiv 10 \mod (11)$ | $x \equiv 6 \mod (11)$ | $+4$

$7 \cdot 13 = 91$

$7 \cdot 7 = 0 \mod (7)$
$7 \cdot 7 = 1 \mod (13)$
$6 \cdot 7 \cdot 7 = 0 \mod (7)$
$6 \cdot 7 \cdot 7 = 6 \mod (13)$

$-\boxed{27+6} = 33$
$x \equiv 294 + 6 = 300$

$x = 33 + 6$
$x = 39$

$0 \mod (5)$
$6 \mod (11)$
$5 \cdot 9 = 0 \mod (5)$
$5 \cdot 9 = 1 \mod (11)$
$5 \cdot 9 \cdot 6 = 6 \mod (11) = 270$
$270 - 55 \cdot x = 50 \;|+4| = 54$

$x \equiv 39 \mod (91)$ | $-15 \mod (91)$ | $-15 \mod (91) = 76$
$x \equiv 54 \mod (55)$ | $+54$ | $0 \mod (55)$ | $0 \mod (55)$

$48 \cdot 55 = 1 \mod (91)$ $\quad -15 \mod 91 = 76$

$15 \cdot 48 \cdot 55 =$

$76 \cdot 48 \cdot 55 = 0 \mod (55)$
$76 \cdot 48 \cdot 55 = -15 \mod (91)) = 440$

$440 + 54 = 494$

Zadanie 9

Znaleźć 2 ostatnie cyfry zapisu siódemkowego liczby 2^1000

Zad 9 Znaleźć 2 ostatnie cyfry zapisu siódemkowego liczby 2^1000

①

$2 = 2 \bmod (49)$
$2^2 = 4 \bmod (49)$
$2^3 = 8 \bmod (49)$
$2^4 = 16 \bmod (49)$
$2^5 = 32 \bmod (49)$
$2^6 = \cancel{64}\ 15 \bmod (49)$
$2^7 = 128 \equiv \bmod (49)$
$2^7 = 128 \equiv 30 \bmod (49)$
$2^8 = 256 \equiv 11 \bmod (49)$
$2^9 = 512 \equiv 22 \bmod (49)$
$2^{10} = 1024 = 44 \bmod (49)$
$2^{11} = 2048 \equiv 39 \bmod (49)$
$2^{12} = 4096 \equiv 29 \bmod (49)$
$2^{13} = 8192 \equiv 9 \bmod (49)$
$2^{14} = 16384 \equiv 18 \bmod (49)$
$2^{15} = 32767 \equiv 36 \bmod (49)$
$2^{16} = 65535 \equiv 23 \bmod (49)$
$2^{17} =$
$2^{21} = \ldots \equiv 1 \bmod (49)$

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

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

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

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

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

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

a zatem 2 ostatnie cyfry to

09

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

Zadanie 10

Dodać następujące wielomiany (bajty) w pierścieniu Z[x]=(x^8+x^4+x^3+x+1) GF(2^8)
a) ‘57’+’02’
b) ‘03’+’03’
c) ‘FF’+’0F’

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

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

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

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

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

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