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 = 7 w Z13
log5 8 = 11 w Z13
log5 8 = 36 w Z13
log5 8 = 78 w Z13
log5 8 = 91 w Z13
log5 8 = 80 w Z19
log5 8 = 93 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; }

        @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 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-(1·2) -2	1-(0·2) 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	0−1·1 −1	1−0·1 1
8%5=3 8/5=(1) 3	5	1-(-1·1) 2	0-(1·1) -1	-1	1
3	5%3=2 5/3=1 2 (1)	2	-1	-1-(2·1) -3	1-(-1·1) 0
3%2=1 3/2=1 1 (1)	2	2-(-3·1) 5	-1-(0) -1	-3	0
1 1	2%1=0 0	5	-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

$x \equiv 6 \mod 7$
$x \equiv 7 \mod 13$ $\Rightarrow$ $|-6|$ $x-6 \equiv 0 \mod 7$
$x-6 \equiv 1 \mod 13$

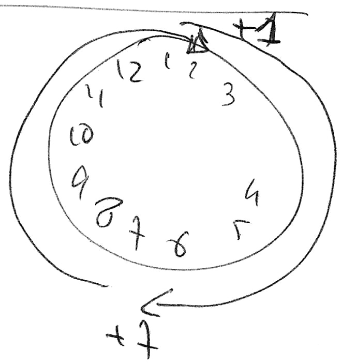
1

$\cancel{13}(0+7) \mod 13 = 7$
$(7+7) \mod 13 = 1$ $\Rightarrow$

---

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

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



$x = 7+7$ $x \equiv 0 \mod 7$
$x \equiv 1 \mod 13$

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

$x = 7+7+6$
$= 1 + 6 = 7 \mod 13$!

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

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

$x \equiv 7 \mod 11$ | | $x \equiv 3 \mod 11$

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

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

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

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

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

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

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

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

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

$x = 304$

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

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

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

$x \equiv 6 \pmod 7$ 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(mod 7*13) = 20 mod (91) = 1294
x= 29(mod 5*11) = 29 mod (55) = 1294
w
55^{-1} mod (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)

x   12 (mod 13)

x   4 (mod 5)

x   10 (mod 11)