ZAKRES MATERIAŁU

I. Algorytm Millera-Rabina

[Algorytm] (Millera-Rabina (sprawdzanie pierwszości liczb)) [patrz wykład 9]

[Zadanie 01] Sprawdź przy pomocy algorytmu Millera-Rabina, czy liczba N jest pierwsza. Czy algorytm zwraca poprawną odpowiedź?
(a) N=165, za losową wartość przyjmij a=3
(b) N=241, za losową wartość przyjmij a=3

(a) N=165, a=3
(1) Wybieramy największe k, takie że $N-1=2^k*m$. Stąd k=2 i m=41
(2) Losowo wybieramy a, $1\le a\le N-1$. Niech a=3
(3) $b=a^m \pmod N$. Stąd b=3
(4) $b\not\equiv 1 \pmod N$, więc wykonujemy iteracje dla i=0, 1 (do k-1)
i=0: $b\not\equiv -1 \pmod N$, więc $b\leftarrow b^2=3^2 \pmod{165}=9$
i=1: $b\not\equiv -1 \pmod N$, więc $b\leftarrow b^2=9^2 \pmod{165}=81$
(5) więc liczba N=165 jest złożona

(b) N=241, a=3
(1) Wybieramy największe k, takie że $N-1=2^k*m$. Stąd k=4 i m=15
(2) Losowo wybieramy a, $1\le a\le N-1$. Niech a=3
(3) $b=a^m \pmod N$. Stąd b=233
(4) $b\not\equiv 1 \pmod N$, więc wykonujemy iteracje dla i=0, 1, 2, 3 (do k-1)
i=0: $b\not\equiv -1 \pmod N$, więc $b\leftarrow b^2=233^2 \pmod{163}=64$
i=1: $b\not\equiv -1 \pmod N$, więc $b\leftarrow b^2=64^2 \pmod{163}=240$
i=2: $b\equiv -1 \pmod N$, więc N=241 jest pierwsza, break;

Algorytm stwierdził, że liczba 241 jest pierwsza.

II. Sito kwadratowe

[Algorytm] (sito kwadratowe) [patrz wykład 10]

[Zadanie 02] Dla liczby N wyznacz największy czynnik mniejszy bądź równy $\sqrt{N}$. Skorzystaj z algorytmu sita kwadratowego.
(a) N=51129
(b) N=1346397

(a) N=51129, $\sqrt{N}$ =226.11723,
Niech m_1=5, m_2=11, m_3=17, r=3,

X	0	1	2	3	4
x^2	0	1	4	4	1
$x^2 - N$	1	2	0	0	2
S[1, x]	1	0	1	1	0

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1
$x^2 - N$	10	0	3	8	4	2	2	4	8	3	0
S[2, x]	0	1	1	0	1	0	0	1	0	1	1

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x^2	0	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
$x^2 - N$	7	8	11	16	6	15	9	5	3	3	5	9	15	6	16	11	8
S[3, x]	0	1	0	1	0	1	1	0	0	0	0	1	1	0	1	0	1

Krok	x	k_1	k_2	k_3	S[1,k_1]	S[2,k_2]	S[3,k_3]
1	227	3	4	11	1	1	1

Ponieważ 227^2-51129 = 51529-51129 = 400 = 20^2, więc szukanym czynnikiem jest 227-20 = 207.
(227-20)(227+20) = 207*247 = 51129

(b) N=1346397, $\sqrt{N}$ =1160.34348,
Niech m_1=5, m_2=11, m_3=17, r=3,

x	0	1	2	3	4
x^2	0	1	4	4	1
$x^2 - N$	3	4	2	2	4
S[1, x]	0	1	0	0	1

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1
$x^2 - N$	3	4	7	1	8	6	6	8	1	7	4
S[2, x]	1	1	0	1	0	0	0	0	1	0	1

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x^2	0	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
$x^2 - N$	3	4	7	12	2	11	5	1	16	16	1	5	11	2	12	7	4
S[3, x]	0	1	0	0	1	0	0	1	1	1	1	0	0	1	0	0	1

Krok	x	k_1	k_2	k_3	$S[1,k_1]$	$S[2,k_2]$	$S[3,k_3]$
1	1161	4	5	12	1	0	0
2	1162	3	4	11	0	0	0
3	1163	2	3	10	0	1	1
4	1164	1	2	9	1	0	1
5	1165	0	1	8	0	1	1
6	1166	4	0	7	1	1	1
7	1167	3	10	6	0	0	0
8	1168	2	9	5	0	0	0
9	1169	1	8	4	1	1	1

Ponieważ 1161^2-1346397 = 1347921-1346397 = 1524 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1162^2-1346397 = 1350244-1346397 = 3847 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1163^2-1346397 = 1352569-1346397 = 6172 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1164^2-1346397 = 1354896-1346397 = 8499 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1165^2-1346397 = 1357225-1346397 = 10828 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1166^2-1346397 = 1359556-1346397 = 13159 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1167^2-1346397 = 1361889-1346397 = 15492 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1168^2-1346397 = 1364224-1346397 = 17827 ≠ y^2, więc idziemy do kroku (3)
Ponieważ 1169^2-1346397 = 1366561-1346397 = 20164 ≠ 142^2, więc szukanym czynnikiem jest 1169-142 = 1027.
(1169-142)(1169+142) = 1027*1311 = 1346397

III. Algorytm p-1 Pollarda

[Algorytm] (p-1 Pollarda) [patrz wykład 10]

[Zadanie 03] Rozłóż liczbę n = 1516515 na czynniki. Skorzystaj z algorytmu p-1 Pollarda. Przyjmij ograniczenie B = 80.

(1) a←2,
(2) for(int j=2; j<=80; j++) a←a^j(mod 1516515); // ostatecznie a=29404
(3) d←NWD(a-1, n) = NWD(29403, 1516515) = 33
(4) 1<d<n, więc d | 1516515 // 33 | 1516515

1516515/33 = 45955, więc 1516515 = 33*45955

IV. Algorytm Fermata

[Algorytm] (Fermata) [patrz wykład 10]

[Zadanie 04] Rozłóż na czynniki liczbę N=39767. Skorzystaj z algorytmu Fermata.

$\sqrt{N}$ = 199.4

(1) a← $2\lfloor\sqrt{N}\rfloor + 1$ = 399, b←1, r← $\lfloor\sqrt{N}\rfloor^2$ - N = 39601-39767 = 79202-39767=-166
(2) r≠0
(3) r←r+a=-166+399=233, a←a+2=399+1=401
(4) r←r-b=233-1=232, b←b+2=3
(5) r>0 (dalszy ciąg w tabelce)

```
a=399,b=1,r=-166
a=401,b=1,r=233
      b=3,r=232
      b=5,r=229
      b=7,r=224
      b=9,r=217
      b=11,r=208
      b=13,r=197
      b=15,r=184
      b=17,r=169
      b=19,r=152
      b=21,r=133
      b=23,r=112
      b=25,r=89
      b=27,r=64
      b=25,r=89
      b=27,r=64
      b=29,r=37
      b=31,r=8
      b=33,r=-23
a=403,b=33,r=378
      b=35,r=345
      b=37,r=310
      b=39,r=273
      b=41,r=234
      b=43,r=193
      b=45,r=150
      b=47,r=105
      b=49,r=58
      b=51,r=9
      b=53,r=-42
a=405,b=53,r=361
      b=55,r=308
      b=57,r=253
      b=59,r=196
      b=61,r=137
      b=63,r=76
      b=65,r=13
      b=67,r=-52
a=407,b=67,r=353
      b=69,r=286
      b=71,r=217
      b=73,r=146
      b=75,r=73
      b=77,r=-2
a=409,b=77,r=405
      b=79,r=328
      b=81,r=249
      b=83,r=168
      b=85,r=85
      b=87,r=0
p=161,q=247
```

N = 39767 = p*q = 161*247

```
class faktoryzacja{
...

private void w(String s){System.out.println(s);}

public int aFermata(int n){
int a=2*(int)Math.sqrt(n)+1;
int b=1;
int r=(int)Math.pow((int)Math.sqrt(n),2)-n;
w("a="+a+",b="+b+",r="+r);
do{
  if(r==0){    w("p="+(a-b)/2+",q="+(a+b-2)/2);return (a-b)/2;}
  r+=a;a+=2;   w("a="+a+",b="+b+",r="+r);
  do{r-=b;b+=2;w("b="+b+",r="+r);
  }while(r>0);
}while(r<=0);
return -1;}

...
}
```

Jak wykorzystać metodę `aFermata()`.

[Przykład] (realizacja `f.aFermata(377);` [patrz przykład z wykładu 10]).

```
a=39,b=1,r=-16
a=41,b=1,r=23
      b=3,r=22
      b=5,r=19
```


KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

```
      b=7,r=14
      b=9,r=7
      b=11,r=-2
a=43,b=11,r=39
      b=13,r=28
      b=15,r=15
      b=17,r=0
p=13,q=29
```

V. Wielomiany i krzywe eliptyczne

[Zadanie 04] Czy poniższe wielomiany są rozkładalne w pierścieniu $Z_2[x]$? Sprawdź, czy zostały dobrze rozłożone i wybierz poprawne odpowiedzi.

(a) $f(x)=(x^5+x^4+x^3+1)=(x^2+1)(x^3+x^2+1)$ (nie)rozkładalny w $Z_2[x]$
(b) $g(x)=(x^5+x^2+x+1)=(x^2+1)(x^3+x+1)$ (nie)rozkładalny w $Z_2[x]$
(c)- $h(x)=(x^5+x^2+1)=(x^2+x+1)(x^3+x^2+1)$ (nie)rozkładalny w $Z_2[x]$
(d)- $i(x)=(x^5+x^4+x^3+x)$ (nie)rozkładalny w $Z_2[x]$

Rozwiązanie

(a) $f(x)=(x^5+x^4+x^3+1)=(x^2+1)(x^3+x^2+1)$
wielomian f(x) jest poprawnie rozłożony, jest rozkładalny w $Z_2[x]$
(b) $g(x)=(x^5+x^2+x+1)=(x^2+1)(x^3+x+1)$
wielomian g(x) jest poprawnie rozłożony, jest rozkładalny w $Z_2[x]$
(c)- $h(x)=(x^5+x^2+1)=(x^2+x+1)(x^3+x^2+1)$
wielomian h(x) nie jest poprawnie rozłożony, wielomian ten nie jest rozkładalny w $Z_2[x]$ (patrz wykład 11)
(d)- $i(x)=(x^5+x^4+x^3+x)= (x^4+x^3+x^2+1)x$
wielomian i(x) jest rozkładalny w $Z_2[x]$

[Zadanie 05] Zaznacz każdy zbiór punktów, który stanowi podzbiór jakiejś krzywej eliptycznej E nad Z_5.

(a) {(2,0),(3,2),(3,3),(4,1),(4,4)}
(b) {(1,2),(1,3),(4,0)} // a=1, b=2
(c) {(0,2),(0,3),(0,4),(1,3),(2,2),(2,3)} // -
(d) {(0,1),(0,2)(0,3),(1,1),(1,2)} // -

Rozwiązanie

Krzywą eliptyczną $y^2 = x^3 + ax + b$ nad Z_p jest zbiór rozwiązań $(x, y) \in Z_p x Z_p$ kongruencji

$y^2 \equiv x^3 + ax + b \pmod p$, gdzie a, b są stałymi spełniającymi własność $4a^3 + 27b^2 \not\equiv 0 \pmod p$.

Dla pierścienia Z_5 mamy następujące możliwe pary (a, b): (0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (1, 0), (1, 1), (1, 2), (1, 3), (1, 4), (2, 0), (2, 1), (2, 2), (2, 3), (2, 4), (3, 0), (3, 1), (3, 2), (3, 3), (3, 4), (4, 0), (4, 1), (4, 2), (4, 3), (4, 4).

Pary nie spełniają warunku $4a^3 + 27b^2 \not\equiv 0 \pmod p$.

(a) {(2,0),(3,2),(3,3),(4,1),(4,4)}⊂E (?), gdzie E: $y^2 = x^3 + ax + b$ (jak znaleźć a i b?)

* sprawdźmy przypadek, gdy a=0

dla (a=0, b=0) mamy $y^2 = x^3 + 0$

sprawdźmy kolejne punkty

(2, 0): $0^2 \not\equiv 2^3 \pmod 5$

dla (a=0, b=1) mamy $y^2 = x^3 + 1$

sprawdźmy kolejne punkty

(2, 0): $0^2 \not\equiv 2^3 + 1 \pmod 5$

dla (a=0, b=2) mamy $y^2 = x^3 + 2$

(2, 0): $0^2 \equiv 2^3 + 2 \pmod 5$ (ok)

(3, 2): $2^2 \equiv 3^3 + 2 \pmod 5$ (ok)

(3, 3): $3^2 \equiv 3^3 + 2 \pmod 5$ (ok)

(4, 1): $1^2 \equiv 4^3 + 2 \pmod 5$ (ok)

(4, 4): $4^2 \equiv 4^3 + 2 \pmod 5$ (ok)

więc {(2,0),(3,2),(3,3),(4,1),(4,4)}⊂E, gdzie E: $y^2 = x^3 + 0x + 2$ nad Z_5.

(b) {(1,2),(1,3),(4,0)}⊂E (?), gdzie E: $y^2 = x^3 + ax + b$ (jak znaleźć a i b?)

* a nie może być równe 0, ponieważ wówczas $y^2 \equiv x^3 + b \pmod 5$ i

dla punktu (0, 1) mamy $1^2 = 1 \equiv b \pmod 5$, a

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$.

* sprawdźmy przypadek, gdy a=1

dla (a=1, b=0) mamy $y^2 = x^3 + x$

sprawdźmy kolejne punkty

(1, 2): $2^2 \not\equiv 1^3 + 1 \pmod 5$

dla (a=1, b=1) mamy $y^2 = x^3 + x + 1$

sprawdźmy kolejne punkty

(1, 2): $2^2 \not\equiv 1^3 + 1 + 1 \pmod 5$

dla (a=1, b=2) mamy $y^2 = x^3 + x + 2$

sprawdźmy kolejne punkty

(1, 2): $2^2 \equiv 1^3 + 1 + 2 \pmod 5$ (ok)

(1, 3): $3^2 \equiv 1^3 + 1 + 2 \pmod 5$ (ok)

(4, 0): $0^2 \equiv 4^3 + 4 + 2 \pmod 5$ (ok)

więc {(1,2),(1,3),(4,0)}⊂E, gdzie E: $y^2 = x^3 + x + 2$ nad Z_5.

(c) {(0,2),(0,3),(0,4),(1,3),(2,2),(2,3)}⊂E (?), gdzie E: $y^2 = x^3 + ax + b$ (jak znaleźć a i b?)

* a nie może być równe 0, ponieważ wówczas $y^2 \equiv x^3 + b \pmod 5$ i

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$, a

dla punktu (0, 4) mamy $4^2 = 16 \equiv 1 \equiv b \pmod 5$.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

* a nie może być równe 1, ponieważ wówczas $y^2 \equiv x^3 + x + b \pmod 5$ i

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$, a

dla punktu (0, 4) mamy $4^2 = 16 \equiv 1 \equiv b \pmod 5$.

* a nie może być równe 2, ponieważ wówczas $y^2 \equiv x^3 + 2x + b \pmod 5$ i

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$, a

dla punktu (0, 4) mamy $4^2 = 16 \equiv 1 \equiv b \pmod 5$.

* a nie może być równe 3, ponieważ wówczas $y^2 \equiv x^3 + 3x + b \pmod 5$ i

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$, a

dla punktu (0, 4) mamy $4^2 = 16 \equiv 1 \equiv b \pmod 5$.

* a nie może być równe 4, ponieważ wówczas $y^2 \equiv x^3 + 4x + b \pmod 5$ i

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$, a

dla punktu (0, 4) mamy $4^2 = 16 \equiv 1 \equiv b \pmod 5$.

Podany zbiór nie jest podzbiorem żadnej krzywej eliptycznej nad Z_5.

(d) $\{(0,1),(0,2)(0,3),(1,1),(1,2)\} \subset E$ (?), gdzie E: $y^2 = x^3 + ax + b$ (jak znaleźć a i b?)

* a nie może być równe 0, ponieważ wówczas $y^2 \equiv x^3 + b \pmod 5$ i

dla punktu (0, 1) mamy $1^2 = 1 \equiv b \pmod 5$, a

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$.

* a nie może być równe 1, ponieważ wówczas $y^2 \equiv x^3 + x + b \pmod 5$ i

dla punktu (0, 1) mamy $1^2 = 1 \equiv b \pmod 5$, a

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$.

* a nie może być równe 2, ponieważ wówczas $y^2 \equiv x^3 + 2x + b \pmod 5$ i

dla punktu (0, 1) mamy $1^2 = 1 \equiv b \pmod 5$, a

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$.

* a nie może być równe 3, ponieważ wówczas $y^2 \equiv x^3 + 3x + b \pmod 5$ i

dla punktu (0, 1) mamy $1^2 = 1 \equiv b \pmod 5$, a

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$.

* a nie może być równe 4, ponieważ wówczas $y^2 \equiv x^3 + 4x + b \pmod 5$ i

dla punktu (0, 1) mamy $1^2 = 1 \equiv b \pmod 5$, a

dla punktu (0, 2) mamy $2^2 = 4 \equiv b \pmod 5$.

Podany zbiór nie jest podzbiorem żadnej krzywej eliptycznej nad Z_5.

[Zadanie 06] Dla jakich parametrów a, $b \in Z_5$ poniższe punkty są wybranymi elementami pewnej krzywej eliptycznej E nad Z_5.

{(1,2),(1,3),(2,1),(2,4),(3,0)} // a=0,b=3

Rozwiązanie

* sprawdźmy przypadek, gdy a=0

dla (a=0, b=0) mamy $y^2 = x^3 + 0$

sprawdźmy kolejne punkty

(1, 2): $2^2 \not\equiv 1^3 \pmod 5$

dla (a=0, b=1) mamy $y^2 = x^3 + 1$

sprawdźmy kolejne punkty

(1, 2): $2^2 \not\equiv 1^3 + 1 \pmod 5$

dla (a=0, b=2) mamy $y^2 = x^3 + 2$

(1, 2): $2^2 \not\equiv 1^3 + 2 \pmod 5$

dla (a=0, b=3) mamy $y^2 = x^3 + 3$

(1, 2): $2^2 \equiv 1^3 + 3 \pmod 5$ (ok)

(1, 3): $3^2 \equiv 1^3 + 3 \pmod 5$ (ok)

(2, 1): $1^2 \equiv 2^3 + 3 \pmod 5$ (ok)

(2, 4): $4^2 \equiv 2^3 + 3 \pmod 5$ (ok)

(3, 0): $0^2 \equiv 3^3 + 3 \pmod 5$ (ok)

więc $\{(1,2),(1,3),(2,1),(2,4),(3,0)\} \subset E$, gdzie E: $y^2 = x^3 + 0x + 3$ nad Z_5.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego