Laboratorium z kryptografii

Zajęcia 9-10: Liczby pierwsze - test Lucasa

1 Algorytm Fermata - rozkład na czynniki pierwsze

Faktoryzacja liczby złożonej a przy wykorzystaniu Algorytmu Fermata w głównej części opiera się przedstawieniu naturalnej liczby nieparzystej d jako różnicy kwadratów dwóch innych liczb nieparzystych x oraz y:

$$\begin{aligned} d &= x^2 - y^2 && (1) \\ &= (x+y)(x-y) && (2) \end{aligned}$$

Jeżeli żaden z nawiasów nie jest równy jeden, otrzymuje się rozkład liczby d na iloczyn $x+y$ i $x-y$. Ponieważ dowolna złożona liczba nieparzysta może zostać przedstawiona w taki sposób[1], to rozkład na czynniki pierwsze można przeprowadzić za pomocą następującego algorytmu:

1. Przedstawienie liczby a w postaci iloczynu k-tej potęgi dwójki oraz liczby nieparzystej d:
$$a = 2^k d \qquad (3)$$
2. Wyliczenie $x = \left\lfloor \sqrt{d} \right\rfloor$. Jeżeli $x = \sqrt{d}$ to $x^2 = d$ więc jest dzielnikiem d z krotnością dwa. Jeżeli nie to x=x+1.
3. Przeprowadzenie pętli:
Dopóki $x < \frac{d+1}{2}$
   i) obliczyć $y^2 = x^2 - d$
   ii) Jeżeli $y^2 > 0$ i $\left\lfloor \sqrt{y^2} \right\rfloor = \sqrt{y^2}$ to $x+y$ i $x-y$ są dzielnikami d - przerwanie pętli
   Jeżeli nie to $x = x + 1$
4. Powtórzenie kroków 2 oraz 3 dla liczb $d' = x + y$ i $d'' = x - y$ dopóki będą niepodzielne

Przykłady:
Niech $a = 78$, wtedy:

1. $a = 2^1 \cdot 39$
2. $x = \lfloor \sqrt{39} \rfloor = 6 \neq \sqrt{39} \Rightarrow x = 6 + 1$
3. dopóki $x < \frac{39+1}{2} = 20$
   i) $y^2 = 7^2 - 39 = 10$
   ii) $y^2 = 10 > 0$ i $\lfloor \sqrt{10} \rfloor \neq \sqrt{10}$
   iii) $x = 7 + 1$
   iv) $y^2 = 8^2 - 39 = 25$
   v) $y^2 = \lfloor \sqrt{25} \rfloor = \sqrt{25}$
   vi) $x + y = 8 + 5 = 13$ oraz $x - y = 8 - 5 = 3$
   vii) przerwanie pętli

[1] wystarczy zauważyć, że $d = x_1 x_2 = \left(\frac{x_1+x_2}{2}\right)^2 - \left(\frac{x_1-x_2}{2}\right)^2$

4. $d = 3$ i powrót do kroku 2. (po przejściu całej pętli nie znaleziono rozkładu $\Rightarrow$ liczba pierwsza)

5. $d = 13$ i powrót do kroku 2. (po przejściu całej pętli nie znaleziono rozkładu $\Rightarrow$ liczba pierwsza)

6. Dzielniki liczby 78 to $(2, 3, 13)$ a ich odpowiednie krotności to $(1, 1, 1)$

Niech $a = 5148$

1. $a = 2^2 \cdot 1287$

2. $x = \lfloor \sqrt{1287} \rfloor = 35 \neq 35.8748 = \sqrt{1287} \Rightarrow x = 35 + 1$

3. dopóki $x < \frac{1287+1}{2} = 644$
   i) $y^2 = 36^2 - 1287 = 9$
   ii) $y^2 = 9 > 0$ i $\lfloor \sqrt{9} \rfloor = \sqrt{9}$
   iii) $x + y = 36 + 3 = 39$ oraz $x - y = 36 - 3 = 33$
   iv) przerwanie pętli

4. $d = 39$ i powrót do kroku 2

5. $x = \lfloor \sqrt{39} \rfloor = 6 \neq \sqrt{39} \Rightarrow x = 6 + 1$

6. dopóki $x < \frac{39+1}{2} = 20$
   i) $y^2 = 7^2 - 39 = 10$
   ii) $y^2 = 10 > 0$ i $\lfloor \sqrt{10} \rfloor \neq \sqrt{10}$
   iii) $x = 7 + 1$
   iv) $y^2 = 8^2 - 39 = 25$
   v) $y^2 = \lfloor \sqrt{25} \rfloor = \sqrt{25}$
   vi) $x + y = 8 + 5 = 13$ oraz $x - y = 8 - 5 = 3$
   vii) przerwanie pętli

7. 13 i 3 liczby pierwsze

8. $d = 33$ i powrót do kroku 2 (wynik daje 11 i 3 -drugi raz)

9. Dzielniki liczby 5148 to $(2, 3, 11, 13)$ o krotnościach $(2, 2, 1, 1)$

2 Test Lucasa

Test Lucasa jest deterministycznym testem pierwszości danej naturalnej liczby nieparzystej n. Wykorzystuje się w nim rozkład liczby $n - 1$ na czynniki pierwsze:

$$n - 1 \quad = \quad x_1^{k-1} \cdot \ldots \cdot x_m^{k-m}. \tag{4}$$

Liczba n jest liczbą pierwszą jeżeli istnieje liczba $q \in \{2, \ldots, n-1\}$ dla której spełnione są następujące warunki:

1. $q^{n-1} = 1 \pmod{n}$

2. $\forall_{i \in \{1,\ldots,m\}}\ q^{\frac{n-1}{p_i}} \neq 1 \pmod{n}$

Przykłady:

a) $n = 2297$ i $q = 456$, wtedy $n - 1 = 2^3 \cdot 41^1 \cdot 7^1$ oraz:

$$\begin{aligned} 456^{2296} &= 1 \pmod{2297} \\ 456^{\frac{2296}{2}} &= 2296 \neq 1 \pmod{2297} \\ 456^{\frac{2296}{41}} &= 1967 \neq 1 \pmod{2297} \\ 456^{\frac{2296}{7}} &= 1 \pmod{2297} \end{aligned}$$

test nie rozstrzyga czy liczba 2297 jest pierwsza.

b) $n = 2297$ i $q = 12$, wtedy $n - 1 = 2^3 \cdot 41^1 \cdot 7^1$ oraz:

$$\begin{aligned} 12^{2296} &= 1 \pmod{2297} \\ 12^{\frac{2296}{2}} &= 2296 \neq 1 \pmod{2297} \\ 12^{\frac{2296}{41}} &= 1463 \neq 1 \pmod{2297} \\ 12^{\frac{2296}{7}} &= 1231 \neq 1 \pmod{2297} \end{aligned}$$

liczba 2297 jest pierwsza!

c) $n = 23321$ i $q = 223$, wtedy $n - 1 = 2^3 \cdot 5^1 \cdot 11^1 \cdot 53^1$ oraz:

$$\begin{aligned} 223^{23320} &= 1 \pmod{23321} \\ 223^{\frac{23320}{2}} &= 23320 \neq 1 \pmod{23321} \\ 223^{\frac{23320}{11}} &= 5341 \neq 1 \pmod{23321} \\ 223^{\frac{23320}{53}} &= 19802 \neq 1 \pmod{2297} \\ 223^{\frac{23320}{5}} &= 1 \pmod{23321} \end{aligned}$$

test nie rozstrzyga czy liczba 23321 jest pierwsza.

d) $n = 23321$ i $q = 2223$, wtedy $n - 1 = 2^3 \cdot 5^1 \cdot 11^1 \cdot 53^1$ oraz:

$$\begin{aligned} 2223^{23320} &= 1 \pmod{23321} \\ 2223^{\frac{23320}{2}} &= 23320 \neq 1 \pmod{23321} \\ 2223^{\frac{23320}{11}} &= 9538 \neq 1 \pmod{23321} \\ 2223^{\frac{23320}{53}} &= 19948 \neq 1 \pmod{2297} \\ 2223^{\frac{23320}{5}} &= 4033 \neq 1 \pmod{23321} \end{aligned}$$

liczba 2297 jest pierwsza!

3 ZADANIA

1. Napisać program dokonujący rozkładu zadanej z konsoli liczby naturalnej na czynniki pierwsze. Program na zwracać wszystkie pierwsze dzielniki liczby (bez powtórzeń) oraz ich krotności.
2. Napisać program przeprowadzający test Lucasa dla zadanych z konsoli liczb n oraz q. Program ma zwracać komunikat „Jest liczbą pierwszą/test nie rozstrzyga”, wartości $q^{\frac{n-1}{p_i}} \pmod{n}$ dla każdego dzielnika p_i oraz wartości $q^{n-1} \pmod{n}$.

Punktacja - łącznie 10 punktów

- 3 punkty - poprawnie działający algorytm Fermata
- 2 punkty - wyświetlenie dzielników (bez powtórzeń) oraz ich krotności
- 1 punkty - poprawnie działający test Lucasa dla $n < 1000$
- 2 punkty - poprawnie działający test Lucasa dla $n < 10000$
- 2 punkty - poprawnie działający test Lucasa dla $n < 32000$