Laboratorium z kryptografii
Zajęcia 7-8: Liczby pierwsze - test Lucasa

1 Algorytm szybkiego potęgowania modulo

Obliczanie reszty z dzielenia pewnej liczby naturalnej a podniesionej do potęgi b przez c (tj. $a^b \mod c$), gdzie $a, b, c \in \mathbb{N}$ wymaga przeprowadzenia $b-1$ mnożeń oraz jednego dzielenia. Dodatkowo dla dużych liczb a oraz b liczba a^b przed wyciągnięciem reszty z dzielenia może osiągać ogromne wartości. Wykorzystując jedną z podstawowych własności arytmetyki modularnej:

$$((a \mod c) \cdot (b \mod c)) \mod c = (a \cdot b) \mod c$$

oraz rozkład wykładnika b na reprezentację binarną $(b_n, b_{n-1}, \ldots, b_1, b_0)$:

$$b = b_0 2^0 + b_1 2^1 + \ldots + b_n 2^n$$

liczbę $a^b \mod c$ można zapisać jako:

$$\begin{aligned} a^b &= a^{b_0 2^0 + b_1 2^1 + \ldots + b_n 2^n} \pmod c \\ &= a^{b_0 2^0} a^{b_1 2^1} \cdot \ldots \cdot a^{b_n 2^n} \pmod c \end{aligned}$$

Przykładowo niech dane będzie wyrażenie $4^{21} \mod 7$, wtedy:

$$\begin{aligned} 4^1 \mod 7 &= 4 \\ 4^2 \mod 7 &= (4^1)^2 = 16 \mod 7 = 2 \\ 4^4 \mod 7 &= (4^2)^2 = 4 \mod 7 = 4 \\ 4^8 \mod 7 &= (4^4)^2 = 16 \mod 7 = 2 \\ 4^{16} \mod 7 &= (4^8)^2 = 4 \mod 7 = 4 \end{aligned}$$

ponieważ wykładnik $b = 21$ w postaci binarnej wynosi $b = (10101)$, to:

$$\begin{aligned} 4^{21} &= 4^1 \cdot 4^4 \cdot 4^{16} \pmod 7 \\ &= 4 \cdot 4 \cdot 4 \pmod 7 \\ &= 1 \pmod 7 \end{aligned}$$

Przykład $1897^{50498} \mod 16112$

$$\begin{aligned}
1897^{1} \mod 16112 &= 1897 \\
1897^{2} \mod 16112 &= (1897^{1})^2 \mod 16112 = 5633 \\
1897^{4} \mod 16112 &= (1897^{2})^2 \mod 16112 = 6161 \\
1897^{8} \mod 16112 &= (1897^{4})^2 \mod 16112 = 14161 \\
1897^{16} \mod 16112 &= (1897^{8})^2 \mod 16112 = 3969 \\
1897^{32} \mod 16112 &= (1897^{16})^2 \mod 16112 = 11537 \\
1897^{64} \mod 16112 &= (1897^{32})^2 \mod 16112 = 1137 \\
1897^{128} \mod 16112 &= (1897^{64})^2 \mod 16112 = 3809 \\
1897^{256} \mod 16112 &= (1897^{128})^2 \mod 16112 = 7681 \\
1897^{512} \mod 16112 &= (1897^{256})^2 \mod 16112 = 11729 \\
1897^{1024} \mod 16112 &= (1897^{512})^2 \mod 16112 = 5185 \\
1897^{2048} \mod 16112 &= (1897^{1024})^2 \mod 16112 = 9409 \\
1897^{4096} \mod 16112 &= (1897^{2048})^2 \mod 16112 = 9953 \\
1897^{8192} \mod 16112 &= (1897^{4096})^2 \mod 16112 = 5633 \\
1897^{16384} \mod 16112 &= (1897^{8192})^2 \mod 16112 = 6161 \\
1897^{32768} \mod 16112 &= (1897^{16384})^2 \mod 16112 = 14161
\end{aligned}$$

Ponieważ $50498 = (1100010101000010)_2$, to:

$$\begin{aligned}
1897^{50498} &= 1897^{32768+16384+1024+256+64+2} \pmod{16112} \\
&= 14161 \cdot 6161 \cdot 5185 \cdot 7681 \cdot 1137 \cdot 5633 \pmod{16112} \\
&= 8993 \pmod{16112}
\end{aligned}$$

Inne przykłady

i) $5^{41} \mod 137 = 62$

ii) $15^{12347} \mod 707 = 113$

iii) $73^{987654} \mod 613 = 195$

iv) $2234^{1234567} \mod 9876 = 2900$

2 Algorytm Fermata - rozkład na czynniki pierwsze

Twierdzenie 1 *Małe twierdzenie Fermata*
Jeżeli n jest liczbą pierwszą, to dla dowolnej liczby całkowitej q, liczba $q^n - q$ jest wielokrotnością liczby n, tzn.:

$$q^n - q = 0 \pmod{n}.$$

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 $\lfloor \sqrt{10} \rfloor \neq \sqrt{10}$

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

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

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 $(2, 2, 1, 1)$

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

gdzie x_i jest dzielnikiem (będący liczbą pierwszą) liczby $n-1$

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 23321 jest pierwsza!

4 ZADANIA

1. Zaimplementować algorytm szybkiego potęgowania modulo ($a^b \mod c$) działający w zakresie a, c <32 000 oraz b <2 000 000 000. Liczby a, b i c mają być wczytywane z konsoli. Program ma wyświetlać wynik.

2. Napisać program dokonujący rozkładu zadanej z konsoli liczby naturalnej na czynniki pierwsze. Program na zwracać wszystkie pierwsze dzielniki liczby (bez powtórzeń) oraz ich krotności.

3. Napisać program przeprowadzający test Lucasa dla zadanych z konsoli liczb n oraz q. Program ma zwracać komunikat „Jest liczbą pierwszą/test nie rozstrzyga", wartości $q^{\frac{n-1}{x_i}} \pmod n$ dla każdego dzielnika x_i oraz wartości $q^{n-1} \pmod n$.

Punktacja - łącznie 10 punktów

- 3 punkty - poprawnie działający algorytm szybkiego potęgowania modulo
- 3 punkty - poprawnie działający algorytm Fermata
- 1 punkty - poprawnie działający test Lucasa dla $n < 10000$
- 3 punkty - poprawnie działający test Lucasa dla $n < 32000$