Kryptografia i bezpieczeństwo systemów informatycznych

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2024/2025

inf.ug.edu.pl/~amb/

Liczby pierwsze, algorytm Rabina-Millera

Szukanie liczb pierwszych

- Algorytm oczywisty
  – zakładamy, że istnieje test pierwszości liczby
  – losuje się ciąg k bitów, $k = 500, 1000$ i więcej
  – testuje się, czy liczba jest pierwsza, jeśli nie, to powtórka
- Złożoność algorytmu
  – liczba liczb pierwszych k-bitowych $\approx \log e \cdot \frac{2^k}{k}$
  – a więc średnio k iteracji starcza do znalezienia l.pierwszej
- Testowania pierwszości liczby
  – nie poprzez próbę rozkładu, ten problem jest właśnie trudny
  – algorytm decyzyjny, odpowiedź może być „tak" lub „nie"

Rodzaje algorytmów

- deterministyczne: dają zawsze odpowiedź „tak" lub „nie"
- niedeterministyczne Las Vegas: dają z pewnym prawdopodobieństwem odpowiedź prawidłową, ale mogą zwrócić błąd
- niedeterministyczne Monte Carlo: dają zawsze odpowiedź, prawidłową z pewnym prawdopodobieństwem, ale mogą dać odpowiedź fałszywą
  – mogą być skrzywione np. odpowiedź „nie" będzie zawsze prawidłowa, a odpowiedź „tak" może być błędna
- Test pierwszości: zdarzenie A – liczba nie jest pierwsza, $P(A') = \epsilon \approx \frac{\log e}{k}$, B – test jest pozytywny, $P(B|A) \leqslant \frac{1}{2}$
  – po m niezależnych testach $P(B^m|A) \leqslant 2^{-m}$, $P(A|B^m) =$

$$= \frac{P(B^m|A) \cdot P(A)}{P(B^m)} = \frac{P(B^m|A) \cdot P(A)}{P(B^m|A) \cdot P(A) + P(B^m|A') \cdot P(A')}$$

$$\leqslant \frac{2^{-m} \cdot (1-\epsilon)}{2^{-m} \cdot (1-\epsilon) + \epsilon} \approx 2^{-m} \cdot k / \log e$$

Testy pierwszości, Fermata

- Tw. Fermata: jeśli n jest pierwsza (i $NWD(a,n)=1$), to $a^{n-1}=1 \mod n$
  – a więc na pewno nie jest pierwsza w.p.p.
  – przedtem można/warto obliczyć $NWD(a,n)$
  –„świadek pierwszości": liczba a t.ż. $a^{n-1}=1 \mod n$
  – wówczas n jest „pseudopierwsza przy podstawie a"
- albo wszystkie $a<n$ są świadkami albo mniej niż połowa
  – dw: jeśli a nie jest świadkiem ale b jest, to $a\cdot b$ nie jest, czyli świadków b nie może być więcej niż połowa
  – np. $10^{32}=1 \mod 33$, ale $2^{32}=4 \mod 33$ czyli 33 jest złożona
  – liczby Carmichaela: nie są pierwsze, ale zachodzi warunek Fermata
  – jest ich bardzo niewiele, np. 561, można się nie przejmować
  – a więc: jeśli m losowych liczb a jest świadkiem pierwszości n, to szansa, że liczba n nie jest pierwsza jest niewielka ($\leqslant 2^{-m}\cdot \log n$)

Pierwiastki kwadratowe a rozkład na czynniki

- Niech $N=p\cdot q$ i znane są dwie pary pierwiastków mod N
  – czyli $(\pm a)^2=(\pm b)^2 \mod N$ ale $a+b\neq 0 \mod N$, $a-b\neq 0 \mod N$
  – czyli $N|(a+b)\cdot(a-b)$ ale $N \not| (a+b)$, $N \not| (a-b)$
  – wówczas $p|a+b$, $q|a-b$, czyli $p=NWD(N,a+b)$
- Ogólniej: znajomość nietrywialnej pary pierwiastków pozwala znaleźć rozkład
  – $NWD(N,a+b)$ jest nietrywialnym dzielnikiem N
  – np. $29^2=15^2 \mod 77$, $NWD(29-15,77)=7$, $NWD(29+15,77)=11$

Testy pierwszości, Millera—Rabina

- Zasadniczo jak w teście Fermata, obliczamy a^{n-1} dla pewnego a, $n-1=m\cdot 2^k$, $k>0$
- Zamiast szybkiego potęgowania odkładamy kwadraty na koniec definiujemy ciąg $b_0=a^m \mod n$, $b_{i+1}=b_i^2 \mod n$
  – jeśli a jest świadkiem pierwszości (Fermat), to $\exists i.\, b_i=1 \mod n$, jeśli $i=0$ albo $b_{i-1}=-1 \mod n$, to nic nie zyskujemy
  – ale jeśli $b_{i-1}\neq -1 \mod n$, to otrzymujemy nietrywialny pierwiastek z jedynki, na pewno n jest złożona a nawet znany jest rozkład
  – np. $n=561$, $n-1=35\cdot 2^4$, testujemy dla $a=2$
  $b_0=2^{35}=263 \mod 561$
  $b_1=263^2=166 \mod 561$
  $b_2=166^2=67 \mod 561$
  $b_3=67^2=1 \mod 561$
  $NWD(67-1,561)=33$, $561=33\cdot 17$
  albo $NWD(67+1,561)=17$, $561=33\cdot 17$

Szukanie liczby pierwszej

- Dana liczba n, sprawdzamy, czy 2, 3, 5, 7 i inne małe liczby są świadkami pierwszości w sensie Rabina–Millera
  – tw.: jeśli n jest złożona, to mniej niż $\frac{1}{4}$ liczb jest świadkiem pierwszości w sensie Rabina–Millera
  – np. 2 jest rzadko świadkiem pierwszości liczby złożonej
  – dla większości liczb złożonych świadków pierwszości w sensie Rabina–Millera jest dużo mniej niż $\frac{1}{4}$
  – po kilkunastu/kilkudziesięciu nieudanych próbach znalezienia nieświadka uznajemy liczbę za pierwszą
- Złożoność: dla liczby k-bitowej wynosi $O(k^3)$
  – $O(k)$ iteracji algorytmu (tw. na pewno $O(k^2)$ jest wystarczające)
  – m testów na świadka (dla liczby złożonej kontrprzykład znajdzie się po kilku testach, można postawić granicę np. $m=30$ testów)
  – k potęgowań dla testowania jednego świadka

Liczby silnie pierwsze

- Liczba p jest silnie pierwsza jeśli
  – p jest pierwsza
  – $(p-1)/2$ też jest pierwsza
- Np. $p = 2^k + 1$ może być liczbą pierwszą
  – ale $p - 1$ jest potęgą 2
  – tak daleko odbiega od silnej pierwszości, jak to możliwe
- Szukanie liczb silnie pierwszych
  – szukamy liczby pierwszej q (jedna na $\ln(q)$ liczb)
  – sprawdzamy czy $2 \cdot q + 1$ jest pierwsza (też jedna szansa na $\ln(q)$)
  – złożoność: jedna potęga wyżej
- Słabsza wersja:
  – $(p-1)/2$ ma duży dzielnik pierwszy
  – szukamy liczby pierwszej q np. 160-bitowej
  – następnie testujemy na pierwszość liczby $2 \cdot \lambda \cdot q + 1$ dla liczb λ mających $n - 160$ bitów i znajdujemy liczbę pierwszą n bitową
  – złożoność ta sama co dla zwykłych liczb pierwszych