Théorie algorithmique des nombres

Cours no. 10

Jean-Sébastien Coron

Université du Luxembourg

November 22, 2009

Summary

- Algorithmic number theory.
  - Probabilistic primality testing
  - Application to prime-number generation.

Trial division

- Goal
  - Given an integer n, determine whether n is prime or composite.
- Simplest algorithm: trial division.
  - Test if n is divisible by 2, 3, 4, 5,... We can stop at $\sqrt{n}$.
  - Algorithm determines if n is prime or composite, and outputs the factors of n if n is composite.
- Very inefficient algorithm
  - Requires around $\sqrt{n}$ arithmetic operations.
  - If n has 256 bits, then 2^{128} arithmetic operations. If 2^{30} operations/s, this takes 10^{22} years !

Probabilistic primality testing

- Goal: describe an efficient probabilistic primality test.
  - Can test primality for a 512-bit integer n in less than a second.
- Probabilistic primality testing.
  - The algorithm does not find the factors of n.
  - The algorithm may make a mistake (pretend that an integer n is prime whereas it is composite).
  - But the mistake can be made arbitrarily small (*e.g.* $< 2^{-100}$, so this makes no difference in practice.

Distribution of prime numbers

- Let $\pi(x)$ be the number of primes in the interval $[2, x]$.
- Theorem (Prime number theorem)
  - We have $\pi(x) \simeq x/\log x$.
- Fact (approximation of the n-th prime number)
  - Let p_n denote the n-th prime number. Then $p_n \simeq n \cdot \log n$. More explicitely,

$$n \log n < p_n < n(\log n + \log \log n) \quad \text{for } n \geq 6$$

The Fermat test

- Fermat's little theorem
  - If n is prime and a is an integer between 1 and $n-1$, then $a^{n-1} \equiv 1 \mod n$.
  - Therefore, if the primality of n is unknown, finding $a \in [1, n-1]$ such that $a^{n-1} \not\equiv 1 \mod n$ proves that n is composite.
- Fermat primality test with security parameter t.

```
For i = 1 to t do
    Choose a random a ∈ [2, n − 2]
    Compute r = a^(n−1) mod n
    If r ≠ 1 then return "composite"
Return "prime'
```

Analysis of Fermat's test

- Let $L_n = \{a \in [1, n-1] : a^{n-1} \equiv 1 \mod n\}$
- Theorem:
  - If n is prime, then $L_n = \mathbb{Z}_n^*$. If n is composite and $L_n \subsetneq \mathbb{Z}_n^*$, then $|L_n| \leq (n-1)/2$.
- Proof:
  - If n is prime, $L_n = \mathbb{Z}_n^*$ from Fermat.
  - If n is composite, since L_n is a sub-group of $\mathbb{Z}_n^*$ and the order of a subgroup divides the order of the group, $|\mathbb{Z}_n^*| = m \cdot |L_n|$ for some integer m.

$$|L_n| = \frac{1}{m}|\mathbb{Z}_n^*| \leq \frac{1}{2}|\mathbb{Z}_n^*| \leq \frac{n-1}{2}$$

Analysis of Fermat's test

- If n is composite and $L_n \subsetneq \mathbb{Z}_n^*$
  - then $a^{n-1} = 1 \mod n$ with probability at most $1/2$ for a random $a \in [2, n-2]$.
  - The algorithm outputs "prime" wih probability at most 2^{-t}.
- Unfortunately, there are odd composite numbers n such that $L_n = \mathbb{Z}_n^*$.
  - Such numbers are called Carmichael numbers. The smallest Carmichael number is 561.
  - Carmichael numbers are rare, but there are an infinite number of them, so we cannot ignore them.

The Miller-Rabin test

- The Miller-Rabin test is based on the following fact:
  - Let n be a prime > 2, let $n - 1 = 2^s \cdot r$ where r is odd. Let a be any integer such that $\gcd(a, n) = 1$. Then either $a^r \equiv 1 \mod n$ or $a^{2^j \cdot r} \equiv -1 \mod n$ for some j, $0 \leq j \leq s - 1$.
- Proof:
  - Since n is prime, $a^{n-1} \equiv 1 \mod n$.
  - Consider the minimum $0 \leq j \leq s - 1$ such that $a^{r \cdot 2^{j+1}} \equiv 1 \mod n$. Let $\beta := a^{r \cdot 2^j} \mod n$
  - Then $\beta^2 \equiv 1 \mod n$. We must have $\beta = \pm 1$ because a polynomial of degree 2 has at most two roots over $\mathbb{Z}_n$ for n prime.

The Miller-Rabin test

Write $n-1 = 2^s \cdot r$ for odd r.
For $i = 1$ to t do
  Generate a random $a \in [2, n-2]$. Let $\beta \leftarrow a^r \mod n$.
  If $\beta \neq 1$ and $\beta \neq -1$ do
    $j \leftarrow 1$.
    While $j \leq s-1$ and $\beta \neq -1$ do
      Let $\beta \leftarrow \beta^2 \mod n$
      If $\beta = +1$ return "composite"
      $j \leftarrow j+1$
    If $\beta \neq -1$ return "composite"
Return "prime"

The Miller-Rabin test

- Property
  - If n is prime, then the Miller-Rabin test always declares n as prime.
  - If $n \geq 3$ is composite, then the probability that the Miller-Rabin test outputs "prime" is less than $\left(\frac{1}{4}\right)^t$
- Most widely used test in practice.
  - With $t = 40$, error probabitility less than 2^{-80}. Much less than the probability of a hardware failure.
  - Can test the primality of a 512-bit integer in less than a second.
  - Complexity: $\mathcal{O}(\log^3 n)$

Prime number generation

- To generate a prime integer of size ℓ bits
  - Generate a random integer n of size ℓ bits
  - Test its primality with Miller-Rabin.
  - If n is declared prime, output n, otherwise generate another n again.