EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)

Lecture 19 — March 25, 2019

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Primality Testing Algorithms

2 Primality Testing

- `GenRSA` is a PPT algorithm that on input 1^n, outputs a modulus N that is the product of two n-bit primes, along with integers $e, d > 1$ satisfying $ed = 1 \bmod \phi(N)$.
- But how to randomly generate n-bit primes? Generate a random n-bit odd integer and check whether it is prime.
- **Bertrand's postulate:** For any $n > 1$, the fraction of n-bit integers that are primes is at least $\frac{1}{3n}$.
- So if we choose $3n^2$ random n-bit integers, the probability that a prime is not chosen is

$$\left(1 - \frac{1}{3n}\right)^{3n^2} = \left(\left(1 - \frac{1}{3n}\right)^{3n}\right)^n \leq \left(e^{-1}\right)^n = e^{-n}.$$

  We have use the result that for all $x \geq 1$ it holds that $\left(1 - \frac{1}{x}\right)^x \leq e^{-1}$.
- **Fermat's little theorem:** If p is a prime and a is any integer not divisible by p, then $a^{p-1} = 1 \bmod p$.
- For $a \in \{1, 2, \ldots, N-1\}$, if $a \notin \mathbb{Z}_N^*$ then $a^{N-1} \neq 1 \bmod N$, i.e. such an a is a witness for the compositeness of N. This is because $\gcd(a, N) \neq 1$ implies $\gcd(a^{N-1}, N) \neq 1$. Then $a^{N-1} \neq 1 \bmod N$. To see why, recall that the gcd of two integers is the smallest positive integer which can be written as a linear combination of those integers.
- But integers in the range $1, 2, \ldots, N-1$ **not** belonging to $\mathbb{Z}_N^*$ are rare. If N is prime, then there are no such integers as $\mathbb{Z}_N^* = \{1, 2, \ldots, N-1\}$. For composite $N = p_1^{e_1} \cdots p_k^{e_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are positive integers, the cardinality of $\mathbb{Z}_N^*$ is $\phi(N) = p_1^{e_1-1}(p_1 - 1) \cdots p_k^{e_k-1}(p_k - 1)$. Then the probability that a random element in $\{1, 2, \ldots, N-1\}$ is in $\mathbb{Z}_N^*$ is given by

$$\frac{\phi(N)}{N-1} \approx \frac{\phi(N)}{N} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

  If $p_1, p_2, \ldots, p_k$ are large primes, then this fraction is close to 1. If they are small primes, then it is easy to check that N is composite and fancy primality testing algorithms are not required.

- With this context, let us focus on the integers in $\mathbb{Z}_N^*$. For an integer N, we say that the integer $a \in \mathbb{Z}_N^*$ is a *witness for compositeness of* N if $a^{N-1} \neq 1 \bmod N$.

- For $a \in \{1, 2, \ldots, N-1\}$, if $a \in \mathbb{Z}_N^*$ then $\gcd(a, N) = 1$ and $\gcd(a^{N-1}, N) = 1$. This implies that $Xa^{N-1} + Yn = 1$ for some integers X, Y. So $Xa^{N-1} = 1 \bmod N$ but $a^{N-1} \bmod N$ may or may not be equal to 1. So the a's in $\mathbb{Z}_N^*$ may or may not be witnesses.

- **Theorem:** If there exists a witness (in $\mathbb{Z}_N^*$) that N is composite, then at least half the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite.

  Proof. Consider the subset H of $\mathbb{Z}_N^*$ which consists of elements $a \in \mathbb{Z}_N^*$ satisfying $a^{N-1} = 1 \bmod N$. In other words, H is the set of elements in $\mathbb{Z}_N^*$ which are **not witnesses**. H is a subgroup of $\mathbb{Z}_N^*$ by the below Proposition. By the hypothesis, $H \neq \mathbb{Z}_N^*$. By Lagrange's theorem, the order of H is a proper divisor of $|\mathbb{Z}_N^*|$. Since the largest proper divisor of an integer m is possibly $m/2$, the size of H is at most $|\mathbb{Z}_N^*/2|$. So at least half the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite. $\square$

- **Proposition 8.36:** Let G be a finite group and $H \subseteq G$. If H is nonempty and for all $a, b \in H$ we have $ab \in H$, then H is a subgroup of G.

- Suppose there is a composite integer N for which a witness for compositeness exists. Consider the following procedure which fails to detect the compositeness of N with probability at most 2^{-t}.

  1. For $i = 1, 2, \ldots, t$, repeat steps 2 and 3.
  2. Pick a uniformly from $\{1, 2, \ldots, N-1\}$.
  3. If $a^{N-1} \neq 1 \bmod N$, return "composite".
  4. If all the t iterations had $a^{N-1} = 1 \bmod N$, return "prime".

- But there exist composite numbers for which $a^{N-1} = 1 \bmod N$ for all integers $a \in \mathbb{Z}_N^*$. These are called *Carmichael numbers*. The number $561 = 3 \cdot 11 \cdot 17$ is one such number.

2.1 Miller-Rabin Primality Test

- The Miller-Rabin algorithm takes two inputs: an integer p and a parameter t (in unary format) that determines the error probability. It runs in time polynomial in $\|p\|$ and t.

- **Theorem:** If p is prime, then the Miller-Rabin test always outputs "prime". If p is composite, then the algorithm outputs "composite" except with probability at most 2^{-t}.

- The algorithm for generating a random n-bit prime using the Miller-Rabin test is shown in Algorithm 1.

- **Lemma:** We say that $x \in \mathbb{Z}_N^*$ is a **square root of 1 modulo** N if $x^2 = 1 \bmod N$. If N is an odd prime, then the only square roots of 1 modulo N are $\pm 1 \bmod N$.[1]

- The Miller-Rabin primality test is based on the above lemma.

[1] Note that $-1 \bmod N = N - 1 \in \mathbb{Z}_N^*$

Algorithm 1 Generating a random n-bit prime

Input: Length n

Output: A uniform n-bit prime

for $i = 1$ to $3n^2$ **do**
  $p' \leftarrow \{0,1\}^{n-2}$
  $p \coloneqq 1\|p'\|1$
  Run the Miller-Rabin test on p
  if the output is "prime," **then**
    return p
return fail

- By Fermat's little theorem, if N is an odd prime $a^{N-1} = 1 \bmod N$ for all $a \in \{1, 2, \ldots, N-1\}$. Suppose $N - 1 = 2^r u$ where $r \geq 1$ is an integer and u is an odd integer. Then

$$a^u \bmod N,\ a^{2u} \bmod N,\ a^{2^2 u} \bmod N,\ a^{2^3 u} \bmod N,\ \ldots,\ a^{2^r u} \bmod N$$

  is a sequence where each element is the square of the previous element. In other words, each element is the square root modulo N of the next element. Since the last element in the sequence is a 1, by the above lemma the previous elements can only be ± 1. So one of two things can happen:

  - Either $a^u = 1 \bmod N$. In this case, the whole sequence has only ones.
  - Or one of $a^u \bmod N,\ a^{2u} \bmod N,\ a^{2^2 u} \bmod N,\ a^{2^3 u} \bmod N,\ \ldots,\ a^{2^{r-1} u} \bmod N$ is equal to -1.

- We say that $a \in \mathbb{Z}_N^*$ is a **strong witness that** N **is composite** if both the above conditions do not hold. If we can find even one strong witness, we can conclude that N is composite.

- We say that a integer N is a **prime power** if $N = p^r$ where $r \geq 1$.

- **Theorem:** Let N be an odd number that is not a prime power. Then at least half the elements of $\mathbb{Z}_N^*$ are strong witnesses that N is composite.

- An integer N is a **perfect power** if $N = \hat{N}^e$ for integers $\hat{N}$ and $e \geq 2$. There exists a polynomial time algorithm to check that a given integer is a perfect power. If N is a perfect power, it is composite. If N is not a perfect power and it is not a prime, it cannot be a prime power. So the hypothesis of the above theorem will be satisfied.

- The Miller-Rabin test is given in Algorithm 2.

3 References and Additional Reading

- Sections 8.2.1, 8.2.2 from Katz/Lindell

Algorithm 2 The Miller-Rabin primality test

Input: Odd integer $N > 2$ and parameter 1^t

Output: A decision as to whether N is prime or composite

if N is a perfect power **then**
    return composite
Compute $r \geq 1$ and odd u such that $N - 1 = 2^r u$
for $j = 1$ to t **do**
    $a \leftarrow \{0, \ldots, N-1\}$
    if $a^u \neq \pm 1 \bmod N$ and $a^{2^i u} \neq -1 \bmod N$ for $i \in \{1, \ldots, r-1\}$ **then**
        return composite
return fail