EE 720: An Introduction to Number Theory and Cryptography (Spring 2020)

Lecture 19 — April 1, 2020

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Miller-Rabin Primality Test

2 Recap

- **Fermat's little theorem:** If p is a prime and a is any integer not divisible by p, then $a^{p-1} = 1 \bmod p$.
- One strategy for checking whether an odd integer $N > 1$ is prime or not is to choose a random integer a from $\{1, 2, 3, \ldots, N-1\}$ and computing $a^{N-1} \bmod N$. If $a^{N-1} \neq 1 \bmod N$ then we have deduced that N is not a prime because it violates Fermat's little theorem. If $a^{N-1} = 1 \bmod N$, then we get no information about the primality of N, i.e. N may or may not be prime.
- 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.
- But integers in the range $1, 2, \ldots, N-1$ **not** belonging to $\mathbb{Z}_N^*$ are rare.
- For an integer N, we say that the integer $a \in \mathbb{Z}_N^*$ is a *witness for compositeness of* N if $a^{N-1} \neq 1 \bmod N$.
- **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.
- By the above theorem, if there exists a witness that N is composite, then a randomly chosen $a \in \{1, 2, \ldots, N-1\}$ will be a witness for the compositeness of N probability is at least half. So if we choose t distinct integers $a_1, a_2, \ldots, a_t$ independently and uniformly from $\{1, 2, \ldots, N-1\}$ then the probability that $a_i^{N-1} = 1 \bmod N$ for all $i = 1, 2, \ldots, t$ is $\frac{1}{2^t}$.
  - To say it in another way, if a witness exists that N is composite, then with probability $1 - \frac{1}{2^t}$ we will get $a_i^{N-1} \neq 1 \bmod N$ for at least one of the t values of a_i.
  - If we choose a t like 100 or 200 and get $a_i^{N-1} = 1 \bmod N$ for all i, then we can be fairly confident that N is prime. But this works only if somehow we know that there exists a witness for the compositeness of N.
- 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.

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' ← {0,1}^{n-2}
    p := 1||p'||1
    Run the Miller-Rabin test on p
    if the output is "prime," then
        return p
return fail
```

3 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.
- 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. For prime N, one of two things can happen:

  - Either $a^u = \pm 1 \bmod N$. In this case, the remaining sequence has only ones.
  - Or one of $a^{2u} \bmod N,\ a^{2^2 u} \bmod N,\ a^{2^3 u} \bmod N,\ \ldots,\ a^{2^{r-1} u} \bmod N$ 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. Stated explicitly, $a \in \mathbb{Z}_N^*$ is a strong witness that N is composite if

  - $a^u \neq \pm 1 \bmod N$ **and**
  - $a^{2^i u} \neq -1 \bmod N$ for all $i \in \{1, 2, \ldots, r-1\}$.

  If we can find even one strong witness, we can conclude that N is composite.

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

Algorithm 2 The Miller-Rabin primality test

Input: Odd integer $N > 1$ 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 ≥ 1 and odd u such that N − 1 = 2^r u
for j = 1 to t do
    a ← {1, ..., N − 1}
    if a^u ≠ ±1 mod N and a^(2^i u) ≠ −1 mod N for i ∈ {1, ..., r − 1} then
        return composite
return fail
```

- We say that a integer N is a **prime power** if $N = p^r$ where $r \geq 1$ and p is a prime.
- **Theorem 8.40:** 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.
  - Proof in Katz/Lindell on pages 309, 310. Left for self-study exercise.
- 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.

4 References and Additional Reading

- Sections 8.2.1, 8.2.2 from Katz/Lindell