Scribe: Cryptography and Network Security (Week 10 Class 3)

Aditya Anand

12-Oct-2020

1 Introduction

In this lecture we shall study a simple yet powerful primality test, and also look at the Chinese Remainder Theorem - a fundamental result in elementary number theory. We will look at the Solovay-Strassen primality testing algorithm, which is, like typical primality tests, a randomized one.

2 The Solovay-Strassen Primality Test

The goal of the primality testing problem is to check, given a positive integer n, if it is prime. We are primarily interested in polynomial time algorithms - here it is important to note that the input size is logarithmic in n, and hence we are looking for an algorithm running in time $\mathbf{O}(\log^c n)$ for some positive integer c.

The algorithm itself is very simple, while the analysis is a little involved. Let us take a look at the algorithm:

- On input n, choose an integer a uniformly at random from $\{1, 2...n-1\}$.
- Let $x \leftarrow (\frac{a}{n})$ (the notation is for the Jacobi symbol).
- If $x = 0$ return composite
- Let $y \leftarrow a^{\frac{n-1}{2}} \mod n$
- If $x \equiv y \mod n$ return prime
- Else, return composite

Let us first try to understand the correctness of the algorithm.

Lemma 1. *On input prime p, the Solovay-Strassen algorithm outputs prime.*

Proof. Since the Jacobi and Legendre symbols $(\frac{a}{n})$ coincide with n is prime, and $(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} \mod n$, the result follows. □

The main task will be to analyze the error probability on composites.

3 Probability of error

We use the following Lemma whose proof will be discussed in the next lecture.

Lemma 2. *Given an odd composite number n as input, the equality $(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} \bmod n$ holds with probability atmost $\frac{1}{2}$. Consequently, the Solovay-Strassen returns prime with probability atmost $\frac{1}{2}$.*

Let A denote the event that the input integer is an odd composite number, and B be the event that the algorithm returns prime on m independent iterations on a given input. We are interested in $Pr[A|B]$. By Bayes' theorem

$$Pr[A|B] = \frac{Pr[A]Pr[B|A]}{Pr[A]Pr[B|A] + Pr[A']Pr[B|A']}$$

Clearly, from the previous lemma $Pr[B|A] \leq 2^{-m}$. Thus it remains to compute $P[A]$. Since we know the distribution of prime numbers, the prime number theorem helps us to compute this probability. Choose a N, so that $N \leq n \leq 2N$.

The prime number theorem then tells us that there are approximately $\frac{2N}{\log(2N)} - \frac{N}{\log N} \sim \frac{N}{\log N} \sim \frac{n}{\log n}$ many primes between N and $2N$. Since there are roughly $\frac{n}{2}$ odd integers in this range, we get $Pr[A] \sim 1 - \frac{2}{\log n}$.

Plugging it in the above expression and evaluating, we obtain

$$Pr[A|B] = \frac{Pr[A]Pr[B|A]}{Pr[A]Pr[B|A] + Pr[A']Pr[B|A']}$$

$$Pr[A|B] = \frac{(1 - \frac{2}{\log n})2^{-m}}{(1 - \frac{2}{\log n})2^{-m} + \frac{2}{\log n}}$$

Note that Lemma 1 gives $Pr[B|A'] = 1$ Thus,

$$Pr[A|B] = (\log n - 2)/(\log n - 2 + 2^{m+1})$$

Thus the error probability falls exponentially with m. For $m = 100$, this value is about 10^{-28}.

4 Chinese Remainder Theorem

The Chinese Remainder Theorem gives a nice characterization of solutions to systems of linear congruences with coprime modulii. The proof is constructive, crisp and straightforward.

Theorem 1. *Given a system of congruences $x \equiv a_i \bmod m_i$ for $i \in \{1, 2..r\}$, where the m_i's are pairwise co-prime modulii, there is a unique solution modulo $M = \Pi_{i=1}^{r} a_i$. Further, let $M_i = \frac{M}{m_i}$ and let y_i denote the inverse of M_i modulo m_i. Then this unique solution is given by $T = \sum_{i=1}^{r} a_i M_i y_i \bmod M$.*

Proof. We first prove that T is indeed a solution. Note that the inverses y_i exist since M_i is co-prime with respect to m_i (this is because m_i's themselves are co-prime). Clearly, modulo m_i, only the term $a_i M_i y_i$ survives, simply because every other term is a multiple of m_i. By construction, $M_i y_i$ is 1 mod m_i. Thus $T \equiv a_i \bmod M_i$ and T is a valid solution.

Suppose there is another solution T' modulo M. Then $T - T'$ must be 0 mod m_i for each i in order to satisfy each congruence, and it follows that $T \equiv T' \bmod M$, a contradiction, proving the uniqueness. □

Let us take a simple example. Consider the congruences $x \equiv 1 \bmod 3$ and $x \equiv 7 \bmod 11$. We get $M = 33$, $M_1 = 11$, $M_2 = 3$. The inverses $y_1 = 2 \bmod 3$ and $y_2 = 4 \bmod 11$. The unique solution is $1 * 2 * 11 + 7 * 3 * 4 \bmod 33$ which is 7 mod 33.

A small comment on the RSA algorithm and how CRT can be potentially used to speed up decryption: once you have the two primes p and q whose product is N, it may make more sense to compute the decryption $y^d \bmod p$ and q separately by fast exponentiation, and then use CRT to combine the result. This is relevant since N may be very large, and operations will be faster with half the order of magnitude.

5 Conclusion

In this lecture we studied the Solovay-Strassen algorithm for primality testing. We also stated and proved the Chinese Remainder Theorem, an important fundamental result. In the next lecture we will state Lagrange's theorem for groups and complete the probability analysis of the Solovay-Strassen algorithm.