CS 681: Computational Number Theory and Algebra **Lecture 15**

Two Randomized Algorithms for Primality Testing

Lecturer: Manindra Agrawal **Scribe: Sudeepa Roy**

August 19, 2005

1 Introduction

In the last lecture we studied the deterministic algorithm for primality testing. In this lecture we will study two randomized polynomial time algorithms that work more efficiently for many practical purposes.

2 Miller-Rabin Algorithm

This algorithm was proposed in 70's. Miller and Rabin gave two versions of the same algorithm to test whether a number n is prime or not. Whereas Rabin's algorithm works with a randomly chosen $a \in Z_n$, and is therefore a randomized one, Miller's version tests deterministically for all a's, where $1 \leq a \leq 4\log^2 n$. But correctness of Miller's algorithm depends on correctness of *Extended Riemann Hypothesis*. We will discuss Rabin's version of the algorithm here.

Algorithm

Let ψ be an automorphism in Z_n.
Let $n - 1 \ = \ s \times 2^t$ for odd s.

1. Test if $n \ = \ m^j$ for $j > 1$. If yes, output COMPOSITE.
2. Randomly choose $a \in Z_n$.
3. Test if $a^{n-1} \ = \ 1(\mod n \ )$. If no, output COMPOSITE.
4. Compute $u_i \ = \ a^{s \times 2^i}(\mod n \ )$ for $0 \leq i < t$.
5. If there is an i such that $u_i \ = \ 1$ and $u_{i-1} \ \neq \pm 1$, output COMPOSITE.
6. output PRIME.

Correctness

Observation 2.1 $\Pr_{a \in Z_n}[\textit{test is correct} \mid n \textit{ is prime}\,] \;=\; 1.$

Now let us consider the case when n is composite.
Let primes p and q divides n.

Either (1) $u_0 \;=\; 1 \;=\; u_1 \;=\; \cdots \;=\; u_{i-1}$
or (2) $\exists i > 0, u_i \;=\; 1$ and $u_{i-1} \;=\; -1$

case (1):

$u_0 \; = a^s \;=\; 1(\mod n\,) \Rightarrow a^s \;=\; 1(\mod p\,)$ and $a^s \;=\; 1(\mod q\,)$
Hence,

$$\begin{aligned}
&\Pr_{a \in Z_n}[a^s \;=\; 1(\mod n\,)] \\
&\leq \Pr_{a \in Z_n}[a^s \;=\; 1(\mod p\,) \wedge a^s \;=\; 1(\mod q\,)] \\
&= \Pr_{a \in Z_n}[a^s \;=\; 1(\mod p\,)] \times \Pr_{a \in Z_n}[a^s \;=\; 1(\mod p\,) | a^s \;=\; 1(\mod q\,)] \\
&= \Pr_{a \in Z_p}[a^s \;=\; 1(\mod p\,)] \times \Pr_{a \in Z_q}[a^s \;=\; 1(\mod q\,)]
\end{aligned}$$

Where the last step can be argued as follows.

Let $|\{a_0 \in Z_p : a_0^s = 1(\mod p\,)\}| = k$. Then $\Pr_{a \in Z_p}[a^s \;=\; 1(\mod p\,)] = \frac{k}{p}$. Copies of a_0 in Z_n are $a_0, a_0 + p, \cdots, a_0 + (\frac{n}{p} - 1)p$, i.e., $\frac{n}{p}$ copies.
Hence, $\Pr_{a \in Z_n}[a^s \;=\; 1(\mod p\,)] = \frac{n}{p} \times k \times \frac{1}{n} = \frac{k}{p} = \Pr_{a \in Z_p}[a^s \;=\; 1(\mod p\,)] = \frac{k}{p}$.
Now among these copies, $a_0, a_0 + qp, \cdots$ fall in class $[a_0]$, $a_0 + p, a_0 + (q+1)p, \cdots$ fall in class $[a_0 + p]$, and so on. Hence arguing as before it can be shown that
$\Pr_{a \in Z_n}[a^s = 1(\mod p\,) | a^s = 1(\mod q\,)] = \Pr_{a \in Z_q}[a^s = 1(\mod q\,)]$

Now $a^s = 1(\mod p\,)$ and $a^{p-1} = 1(\mod p\,)$
$\Rightarrow a^{\gcd(s,p-1)} = 1(\mod p\,)$
$\Rightarrow a^{\frac{p-1}{2}} = 1(\mod p\,)$ [as s odd and $p-1$ even, hence the gcd is odd and divides $\frac{p-1}{2}$]
So,
$$\Pr_{a \in Z_p}[a^s \;=\; 1(\mod p\,)] = \Pr_{a \in Z_p}[a^s \;=\; 1(\mod p\,)] \leq \tfrac{1}{2}.$$

Therefore,
$$\Pr_{a \in Z_n}[a^s \;=\; 1(\mod n\,)] \leq \tfrac{1}{4}$$

case (2):

$\exists i : \; a^{s.2^i} \;=\; 1(\mod n\,)$ and $a^{s.2^{i-1}} \;=\; -1(\mod n\,)$

Let $\hat{s} \;=\; s.2^{i-1}$
So, $a^{\hat{s}} \;=\; -1(\mod n\ )$ and $a^{2\hat{s}} \;=\; 1(\mod n\ )$
Hence as in case (1),

$\Pr\limits_{a \in Z_n}[a^{\hat{s}} \;=\; -1(\mod n\ )]$
$\leq \Pr\limits_{a \in Z_n}[a^{\hat{s}} \;=\; -1(\mod p\ ) \wedge a^{\hat{s}} \;=\; -1(\mod q\ )]$
$= \Pr\limits_{a \in Z_n}[a^{\hat{s}} \;=\; -1(\mod p\ )] \times \Pr\limits_{a \in Z_n}[a^{\hat{s}} \;=\; -1(\mod p\ )|a^{\hat{s}} \;=\; -1(\mod q\ )]$
$= \Pr\limits_{a \in Z_p}[a^{\hat{s}} \;=\; -1(\mod p\ )] \times \Pr\limits_{a \in Z_q}[a^{\hat{s}} \;=\; -1(\mod q\ )]$

Now $a^{2\hat{s}} \;=\; 1(\mod p\ )$ and $a^{p-1} \;=\; 1(\mod p\ )$
$\Rightarrow a^{\gcd(2\hat{s},\ p-1)} \;=\; 1(\mod p\ )$
$\Rightarrow a^{\frac{1}{2}\gcd(2\hat{s},\ p-1)} \;=\; \pm 1(\mod p\ )$

As $a^{\hat{s}} \;=\; -1(\mod p\ )$, so $a^{\frac{1}{2}\gcd(2\hat{s},\ p-1)} \;=\; -1(\mod p\ )$

Now, $\gcd(2\hat{s},\ p-1) \leq \frac{1}{2}(p-1)$
Hence, $\Pr\limits_{a \in Z_p}[a^{\hat{s}} \;=\; 1(\mod p\ )] \leq \frac{1}{2}$.
Similarly, $\Pr\limits_{a \in Z_q}[a^{\hat{s}} \;=\; 1(\mod q\ )] \leq \frac{1}{2}$.

Therefore,
$\Pr\limits_{a \in Z_n}[a^{\hat{s}} \;=\; -1(\mod n\ )] \leq \frac{1}{4}$

Combining case (1) and case (2),

$\Pr\limits_{a \in Z_n}[\text{test outputs PRIME} \mid n \text{ is composite }]$
$= \Pr[\text{ case (1) happens or case (2) happens }]$
$\leq \Pr[\text{ case (1) happens }] \;+\; \Pr[\text{ case (2) happens }]$
$\leq \frac{1}{4} + \frac{1}{4}$
$= \frac{1}{2}$

Hence the test is correct with probability $\geq \frac{1}{2}$.
The probability of success can be boosted further by repeating the test a few times, where output will be COMPOSITE if any of the single test output is COMPOSITE, else PRIME.

Time Complexity

- Computing u_0 : $\tilde{O}(\log n) \times O(\log s) = \tilde{O}(\log^2 n)$ [by repeated squaring $O(\log s)$ times, $s \leq n$, then multiplying and taking modulo n each time all with $\log n$

bits numbers using FFT takes $\tilde{O}(\log n)$ time]

- Computing $u_1, u_2, \cdots, u_t$: $\tilde{O}(\log^2 n)$ [$t \leq \log n$, squaring and taking modulo n takes $\tilde{O}(\log n)$ time].
- Testing if $n = m^j$ holds for some $j > 1$ can be done in $\tilde{O}(\log^2 n)$ time.

Hence the time complexity of the algorithm is $\tilde{O}(\log n)$.

2.1 Another Randomized Algorithm for Primality Testing

Algorithm

The outline of the algorithm is as follows.

1. Choose a random monic polynomial $Q(x)$ of degree $\log n$ over Z_n.
2. Test if $(x+1)^n = x^n + 1(\mod n,\ Q(x))$.
3. If yes, output PRIME, else output COMPOSITE.

Correctness

Lemma 2.1 $(x+1)^n = x^n + 1$ *if and only if* n *is prime.*

Proof. 'If' part is trivial.
For the 'only if' part, consider n is composite.
$(1+x)^n = \sum_{j=0}^{n} \binom{n}{j} x^j$
If $p|n$ and n is prime, then $\binom{n}{p} \neq 0(\mod n\ )$
Hence $(x+1)^n - x^n - 1 \neq 0(\mod n)$

So we need to consider the case when n is composite, and $(x+1)^n = x^n+1(\mod q(x)\ )$ It can be shown that with high probability, $q(x)$ does not divide $(x+1)^n - x^n - 1$ (mod n). For details of the proof, refer to [1].

References

[1] Manindra Agrawal and Somenath Biswas, *Primality and Identity Testing via Chinese Remaindering.*,FOCS 1999: 202-209