REU 2006 · Discrete Math · Lecture 12

Instructor: László Babai
Scribe: Duru Türkoğlu, Eliana Zoque

July 28, 2006. Last updated July 30, 2006 at 1:00 p.m.
NOT PROOF-READ

12 Primality Test (Continued)

12.1 Solovay-Strassen Test (Analysis)

Recall that the Solovay-Strassen Primality test is given as follows:
For given n, odd, ≥ 3, pick random a, $1 \leq a \leq n-1$.

1. if $\gcd(a, n) \neq 1$, halt COMPOSITE.
2. else if $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$ (Jacobi symbol), halt "maybe PRIME".
3. else halt COMPOSITE.

If n is prime the output is always "maybe PRIME" because for every prime p, we have $a^{\frac{p-1}{2} \equiv \left(\frac{a}{p}\right)} \pmod p$. Therefore there is no error if the input number is prime.

If n is composite we claim that $Pr(error) \leq 1/2$. Clearly, the only step we can make an error is in line 2, outputting "maybe PRIME" instead of COMPOSITE.

Consider the following subgroups of $\mathbb{Z}_n^\times$:

$$R = \left\{a \in \mathbb{Z}_n^\times \mid a^{n-1} \equiv 1 \pmod n\right\}$$

$$H^* = \left\{a \in \mathbb{Z}_n^\times \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod n\right\}$$

$$K^* = \left\{ a \in \mathbb{Z}_n^\times \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{p}\right) = 1 \pmod n \right\}$$
$$L = \left\{ a \in \mathbb{Z}_n^\times \mid \left(\frac{a}{p}\right) = 1 \pmod n \right\}$$

Now, we want to find the index of L in $\mathbb{Z}_n^\times$, $[\mathbb{Z}_n^\times : L]$. Consider the following map

$$\begin{aligned} f : \mathbb{Z}_n^\times &\to \{\pm 1\} \\ a &\mapsto \left(\frac{a}{p}\right) \end{aligned}$$

f is a group homomorphism since the multiplication is preserved under Jacobi symbol, i.e. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. Note that $L = \ker f = f^{-1}(1)$. Therefore $[\mathbb{Z}_n^\times : L]$ can be equal to 1 or 2. $[\mathbb{Z}_n^\times : L] = 1$ implies $L = \mathbb{Z}_n^\times$; we are going to prove that this is possible. Recall the definition of the Jacobi symbol:

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right)^{k_i}$$

where $n = \prod p_i^{k_i}$. If n is a perfect square, say $n = l^2$ then $(\forall a \in \mathbb{Z}_n^\times) \left(\left(\frac{a}{n}\right) = 1\right)$ i.e. $L = \mathbb{Z}_n^\times$. Is the converse true?

Claim 12.1.1. *If n is not a square $(\exists a \in \mathbb{Z}_n^\times) \left(\left(\frac{a}{n}\right) = -1\right)$.*

Proof. There is a odd k_i. Find a so that $\left(\frac{a}{p_i}\right) = -1$ and $a \equiv 1 \mod p_j$ for all $j \neq i$ (such a exists by the Chinese Reminder Theorem). Clearly, this particular a satisfies $\left(\frac{a}{n}\right) = -1$. □

We conclude the following observation

Observation 12.1.2.

$$[\mathbb{Z}_n^\times : L] = \begin{cases} 1 & \text{if } n \text{ is a square;} \\ 2 & \text{otherwise.} \end{cases}$$

It was an exercise from last class to prove that $K^* \leq H^* \leq R \leq \mathbb{Z}_n^\times$. Note that $H^* \leq R$ since $\left(\frac{a}{n}\right)$ for all $a \in \mathbb{Z}_n^\times$; and $K^* \leq H^*$ is evident, in fact we have more: $K^* = H^* \cap L$.

Theorem 12.1.3. *$H^* \neq \mathbb{Z}_n^\times$.*

Proof. Suppose $H^* = \mathbb{Z}_n^\times$. Then $R = \mathbb{Z}_n^\times$, so n is a Carmichel number by definition (definition is the condition $R = \mathbb{Z}_n^\times$.) In particular, n is square-free. Let $n = rs$ with $\gcd(r, s) = 1$; $r, s \geq 3$. We are to prove that there exists an element in $\mathbb{Z}_n^\times$ which is not an element of H^*. We will prove further that there exists $a \in \mathbb{Z}_n^\times$ so that $a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$. By the contrary assumption we have $K^* = H^* \cap L = \mathbb{Z}_n^\times \cap L = L$ and $L \neq \mathbb{Z}_n^\times = H^*$ since n is square-free, in particular it is not a square. Thus $(\exists b)\left(b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) = -1 \pmod{n}\right)$ which implies $b^{\frac{n-1}{2}} \equiv -1 \pmod{r}$. Using CRT, choose a such that

$$\left.\begin{array}{ll} a \equiv b & \pmod{r} \\ a \equiv 1 & \pmod{s} \end{array}\right\} \Rightarrow \left.\begin{array}{ll} a^{\frac{n-1}{2}} \equiv -1 & \pmod{r} \\ a^{\frac{n-1}{2}} \equiv 1 & \pmod{s} \end{array}\right\} \Rightarrow a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{rs}.$$

We found an element $a \in \mathbb{Z}_n^\times$ not in H^*. This contradicts $H^* = \mathbb{Z}_n^\times$. □

Since the subgroup H^* is proper in $\mathbb{Z}_n^\times$, we conclude that the error occurs at most half of the times (index is at least 2.)

Corollary 12.1.4. *$Pr(error) \leq 1/2$ because $Pr(error) = 1/[\mathbb{Z}_n^\times : H^*]$*

The idea in this proof is to prove a subgroup is proper in the larger group, then we can conclude that for a random element x chosen from the larger group, the probability of x being in the subgroup drops instantly to $\leq 1/2$. For this we just need to prove that we can find one element outside of the subgroup yet in the larger group.

12.2 Miller-Rabin Primality Test

Like the Solovay-Strassen test, this test is also a 1-sided Monte Carlo test, meaning that we may only make a 1-sided error. We are still going to be sure when the algorithm outputs COMPSITE, that it is a composite number, i.e. if the input is prime then the output will be "maybe PRIME". The algorithm is as follows:

Given n odd, ≥ 3, pick random a, $1 \leq a \leq n - 1$. Define ℓ and m to satisfy, $n - 1 = 2^\ell \cdot m$ with m odd.

1. $\underline{\text{if}}$ $\gcd(a, n) \neq 1$, $\underline{\text{halt}}$ COMPOSITE.

```
2. else if $a^{n-1} \not\equiv 1 \pmod{n}$ halt COMPOSITE.
3. else $j := \ell - 1$
4. while $(j \geq 0)$
5. if $a^{2^j \cdot m} \not\equiv \pm 1 \pmod{n}$ halt COMPOSITE.
6. else if $a^{2^j \cdot m} \equiv -1 \pmod{n}$ halt "maybe PRIME".
7. else $j \leftarrow j - 1$
8. end while
9. halt "maybe PRIME".
```

The idea in the algorithm is that whenever we have a square congruent to 1 modulo $n, (b^2 \equiv 1 \pmod{n})$, we investigate whether $b \equiv \pm 1 \pmod{n}$ or not. If $b \equiv -1 \pmod{n}$, we output "maybe PRIME" and continue our search further in the case that the congruence is 1. Clearly, in the last case that the congruence is neither of them, we certify that n is COMPOSITE with the "witness" b. We continue this search until we cannot go further.

12.2.1 Analysis

Claim 12.2.1. *1. If n is prime we always get "maybe PRIME".*

2. If n is composite, $Pr(error) \leq 1/2$.

Proof. 1. We cannot output "COMPOSITE" if n is prime, because whenever we output COMPOSITE we certify that n is composite.

2. If n is not a Carmichel number ($R \neq \mathbb{Z}_n^\times$) then with probability $\geq 1/2$ we stop at lines 1 or 2 ($[\mathbb{Z}_n^\times : R] \geq 2$.) Now we may assume that n is a Carmichel number thus square-free.

   Clearly we may make an error only if we halt in lines 6 or 9. Also as long as $a^{2^j \cdot m} \equiv 1 \pmod{n}$ we do not make an error, provided that we do not diminish j to 0. So we look at the first level where $(\forall a)\left(a^{2^j \cdot m} \equiv 1 \mod n\right)$. Let

$$j_0 = \min\left\{j \mid (\forall a)\left(a^{2^j \cdot m} \equiv 1 \mod n\right)\right\}$$

The idea is to look at $a^{2^{j_0-1}\cdot m}$, and then apply CRT trick (factoring $n = rs$) to find b so that $b^{2^{j_0-1}\cdot m} \equiv -1 \pmod{r}$ and $b \equiv 1 \pmod{s}$ which in turn yields a witness for the compositeness of n. Again by the subgroup argument the number of the witnesses are going to be at least half of the possible values, then we are done. But to be able to use this trick we need $j_0 \geq 1$, in other words we need to prove

$$\text{NOT} \quad \left(\forall a \in \mathbb{Z}_n^\times\right)(a^m \equiv 1 \mod n)$$

This is easy to achieve: take $a = -1$.

□

The Miller-Rabin algorithm was originally designed to be a deterministic algorithm. The input a was not random, instead we run the algorithm repeatedly for values of $a = 1, 2, \ldots$ upto a certain bound. Every composite number has a witness of compositeness, but can we find a bound for the smallest witness? If we do, we can use this bound for the deterministic primality test. Apply the Miller-Rabin algorithm for every number up to the bound, and check the primality of n. If ever we prove compositeness, for sure the number is composite. Otherwise we have a proof of primality, by failing to prove compositeness for all values of a which would have included the witness of compositeness.

Gary Miller proved in 1978 that the smallest witness is smaller than $c\,(\log n)^2$, for a constant c, assuming the extended Riemann hypothesis. But showing that the deterministic primality test has a polynomial time algorithm, required less than proving the extended Riemann hypothesis. Nevertheless, if the extended Riemann hypothesis is proven, the above algorithm is far more faster than the algorithm of Manindra Agrawal, Neeraj Kayal and Nitin Saxena which proves PRIMES is in P.