CS681 **Computational Number Theory**

Lecture 20 and 21: Solovay Strassen Primality Testing

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

Overview

Last class we stated a similar reciprocity theorem for the Jacobi symbol. In this class we shall do the proof of it, discuss the algorithm, and also do the Solovay-Strassen primality testing.

1 Proof of the Reciprocity of $\left(\frac{m}{n}\right)$

The proof will just be induction on m. Recall the statement of the theorem

$$\begin{aligned}\left(\frac{2}{n}\right) &= (-1)^{\frac{n^2-1}{8}}\\ \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\end{aligned}$$

We shall just prove the second part here. The first part uses the same technique. Let us assume that the theorem is true for all $m' < m$. If m is a prime, we do induction on n.

Suppose $m = m_1 m_2$, then

$$\begin{aligned}\left(\frac{m_1 m_2}{n}\right)\left(\frac{n}{m_1 m_2}\right) &= \left(\frac{m_1}{n}\right)\left(\frac{n}{m_1}\right)\left(\frac{m_2}{n}\right)\left(\frac{n}{m_2}\right)\\ &= (-1)^{\frac{n-1}{2}\left(\frac{m_1-1}{2}+\frac{m_2-1}{2}\right)}\end{aligned}$$

From now on, the work shall be happening on the exponent and let us just denote $\frac{n-1}{2}E$ for the exponent of -1. We want to evaluate $E \bmod 2$ since we are looking at (-1) power the exponent and only the parity matters.

Let $m_1 = 4k_1 + b_1$ and $m_2 = 4k_2 + b_2$ where $b_1, b_2 = \pm 1$ since m is odd.

$$\begin{aligned} E &= \frac{4k_1 + 4k_2 + b_1 + b_2 - 2}{2} \\ &= \frac{b_1 + b_2 - 2}{2} \bmod 2 \\ \frac{m-1}{2} &= \frac{(4k_1 + b_1)(4k_2 + b_2) - 1}{2} \\ &= 8k_1k_2 + 2k_1b_2 + 2k_2b_1 + \frac{b_1b_2 - 1}{2} \\ &= \frac{b_1b_2 - 1}{2} \bmod 2 \end{aligned}$$

And now it is easy to check that for $b_1, b_2 = \pm 1$,

$$\frac{b_1b_2 - 1}{2} = \frac{b_1 + b_2 - 2}{2} \bmod 2$$

and therefore, $E = \frac{m-1}{2} \bmod 2$ and hence,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}E} = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \quad \square$$

2 Algorithm to compute $\left(\frac{m}{n}\right)$

The reciprocity laws give a polynomial time algorithm to compute the Jacobi symbol $\frac{m}{n}$. Note that $\left(\frac{m}{n}\right)$ depends only on $m \bmod n$ and therefore we can reduce m modulo n and compute. When $m < n$, we use the reciprocity to get $\left(\frac{n}{m}\right)$ and we reduce again.

The bases cases (cases when either of them is 1 or $gcd(m,n) > 1$ or $m = 2^k m'$ or $n = 2^k m'$ etc) are omitted[1].

The running time of this algorithm is $(\log m \log n)^{O(1)}$.

3 Solovay Strassen Primality Testing

The general philosophy of primality testing is the following:

- Find a property that is satisfied by exactly the prime numbers.

[1] the TEXsource file of this lecture note has them commented out. Uncomment them and recompile if needed

Algorithm 1 JACOBI SYMBOL $\left(\frac{m}{n}\right)$

//base cases omitted
if $m > n$ **then**
  return $\left(\frac{m \bmod n}{n}\right)$
else
  return $(-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$
end if

- Find an efficient way to check if the property is satisfied by arbitrary numbers.
- Show that for any composite number, one can "easily" find a witness that the property fails.

In the Solovay-Strassen algorithm, the property used is the following.

Proposition 1. *n is prime if and only if for all $a \in (\mathbb{Z}/n\mathbb{Z})^\star$,*

$$\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}}$$

And with the following claim, we have the algorithm immediately.

Claim 2. *If n was composite, then for a randomly chosen from $(Z/n\mathbb{Z})^\star$,*

$$\Pr_{a \in (\mathbb{Z}/n\mathbb{Z})^\star}\left[\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}}\right] \geq \frac{1}{2}$$

Thus, the algorithm is the following.

All that's left to do is prove the claim. For that, let us look at a more general theorem which would be very useful.

Theorem 3. *Let ψ_1 and ψ_2 be two homomorphisms from a finite group G to a group H. If $\psi_1 \neq \psi_2$, that is there is atleast one $g \in G$ such that $\psi_1(g) \neq \psi_2(g)$, then ψ_1 and ψ_2 differ at atleast $|G|/2$ points.*

This intuitively means that two different homomorphisms can either be the same or have to be very different.

Proof. Consider the set

$$H = \{g \in G \;:\; \psi_1(g) = \psi_2(g)\}$$

Algorithm 2 SOLOVAY-STRASSEN: check if n is prime

Pick a random element $a < n$.
if $gcd(a, n) > 1$ **then**
    return COMPOSITE
end if
Compute $a^{\frac{n-1}{2}}$ using repeated squaring and $\left(\frac{a}{n}\right)$ using the earlier algorithm.
if $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}}$ **then**
    return COMPOSITE
else
    return PRIME
end if

Note that clearly 1 belongs to H and if $a, b \in H$, then so is ab as $\psi_1(ab) = \psi_1(a)\psi_1(b) = \psi_2(a)\psi_2(b) = \psi_2(ab)$. Inverses are inside as well and therefore, H is a subgroup of G. Also since $\psi_1 \neq \psi_2$, they differ at atleast one point say g_0. Then $g_0 \notin H$ and hence H is a proper subgroup of G.

By Lagrange's theorem, $|H|$ divides $|G|$ and since $|H| < |G|$, $|H|$ can atmost be $|G|/2$. Since every element in $G \setminus H$ is a point where ψ_1 and ψ_2 differ, it follows that ψ_1 and ψ_2 differ at atleast $|G|/2$ points. $\square$

The claim directly follows from the theorem since both the Jacobi symbol and the map $a \mapsto a^{\frac{n-1}{2}}$ are homomorphisms and hence will differ in atleast half of the elements of $(\mathbb{Z}/n\mathbb{Z})^\star$.

Thus, the Solovay-Strassen algorithm has the following error bounds:

- If n is a prime, the program outputs PRIME with probability 1.
- If n is not a prime, the program outputs COMPOSITE with probability atleast $\frac{1}{2}$.

Of course, the confidence can be boosted by making checks on more such a's.

All that's left to do is to prove the proposition.

4 Proof of the Proposition 1

We want to show that if n is not a prime, there the two homomorphisms $a \mapsto a^{\frac{n-1}{2}}$ and $a \mapsto \left(\frac{a}{n}\right)$ are not the same. Thus, it suffices to find a single $a \in (\mathbb{Z}/n\mathbb{Z})^\star$ such that $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}}$.

Case 1: n is not square free

Suppose n had a prime factor p such that p^2 divides n. Recall that for all $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, the Euler ϕ function evaluates to:

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$$

And hence, if $p^2 \mid n \implies p \mid \phi(n)$. Now look at the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\star$, this has $\phi(n)$ elements. A theorem of Cayley tells us that if $p \mid |G|$ then G has an element of order p.[2] Let g be an element of order p in $(\mathbb{Z}/n\mathbb{Z})^\star$.

What is the value of $g^{\frac{n-1}{2}}$? Can this be ± 1? If it were ± 1, then $g^{n-1} = 1$. This means that the order of g divides $n-1$, or $p \mid n-1$ which is impossible since $p \mid n$. And therefore, $g^{\frac{n-1}{2}} \neq \pm 1$ and therefore, certainly cannot be $\left(\frac{g}{n}\right)$ which takes values only ± 1 for all g coprime to n.

Thus g is a witness that $\left(\frac{g}{n}\right) \neq g^{\frac{n-1}{2}}$.

Case 2: n is a product of distinct primes

Now n will be square-free if and only if it is a product of distinct primes. Suppose $n = p_1 p_2 \cdots p_k$

Suppose there is some some a such that $a^{\frac{n-1}{2}} \neq \left(\frac{a}{p_1}\right)$, are we done? Yes we are. We can use such a a to find a g such that $g^{\frac{n-1}{2}} \neq \left(\frac{g}{n}\right)$.

By the Chinese Remainder Theorem, we know that $(\mathbb{Z}/n\mathbb{Z})^\star \cong (\mathbb{Z}/p_1\mathbb{Z})^\star \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\star$. Let g be the element in $(\mathbb{Z}/n\mathbb{Z})^\star$ such that $g \mapsto (a, 1, 1, \cdots, 1)$ by the CRT map. By the definition of the Jacobi Symbol,

$$\left(\frac{g}{n}\right) = \prod_{i \in 1}^{k} \left(\frac{g}{p_i}\right) = \prod_{i=1}^{k} \left(\frac{g \mod p_i}{p_i}\right) = \left(\frac{a}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_k}\right) = \left(\frac{a}{p_1}\right)$$

[2] actually it is more. It says that for every prime power $p^\alpha \mid |G|$, there is a subgroup of order p^α in G.

And $g^{\frac{n-1}{2}} = (a^{\frac{n-1}{2}}, 1, \cdots, 1)$. What we know is that $a^{\frac{n-1}{2}} \neq \left(\frac{a}{p_1}\right)$. Suppose $\left(\frac{a}{p_1}\right) = 1$, then $\left(\frac{a}{p_1}\right) = \left(\frac{g}{n}\right) = 1$. But $g^{\frac{n-1}{2}}$ on the other hand looks like $(a^{\frac{n-1}{2}}, 1, \cdots, 1)$ and we know that $\left(\frac{a}{p_1}\right) = 1 \neq a^{\frac{n-1}{2}}$. Therefore, $g^{\frac{n-1}{2}}$ looks like $(*, 1, \cdots, 1)$ where the first coordinate is *not* 1. And therefore, this is not 1. Therefore $\left(\frac{g}{n}\right) \neq g^{\frac{n-1}{2}}$.

Suppose $\left(\frac{a}{p_1}\right) = -1$, then things are even simpler. $\left(\frac{g}{n}\right) = -1$ but $g^{\frac{n-1}{2}}$ looks like $(*, 1, \cdots, 1) \neq -1$. Therefore $\left(\frac{g}{n}\right) \neq g^{\frac{n-1}{2}}$.

And of course, it works for any prime factor p of n. Thus, the bad case is when for all a and for all prime factors p_i, $\left(\frac{a}{p_i}\right) = a^{\frac{n-1}{2}}$. Since n is composite, there are at least 2 distinct prime factors p_1 and p_2. Pick $a \in (\mathbb{Z}/p_1\mathbb{Z})^\star$ which is a quadratic residue ($\left(\frac{a}{p_1}\right) = 1$) and a $b \in (\mathbb{Z}/p_2\mathbb{Z})^\star$ that is a non-residue ($\left(\frac{b}{p_2}\right) = -1$). Now look at the element $g \in (\mathbb{Z}/n\mathbb{Z})^\star$ that maps to $(a, b, 1, 1, \cdots, 1)$ by the chinese remainder theorem.

Now $g^{\frac{n-1}{2}} = (a^{\frac{n-1}{2}}, b^{\frac{n-1}{2}}, 1, \cdots, 1) = (1, -1, 1, \cdots 1)$ which is not ± 1. And hence clearly, $\left(\frac{g}{n}\right) \neq g^{\frac{n-1}{2}}$.

That completes the proof of correctness of the Solovay-Strassen primality test.