# Math 261C: Randomized Algorithms

Lecture topic: Randomized Primality Testing

Lecturer: Sam Buss
Scribe notes by: Marco Carmosino
Date: May 2, 2014

## 1. Introduction & Definitions

We will present two randomized algorithms for detecting prime numbers, which have good probability of success. We use the decision problems:

**Definition 1.** $\mathsf{COMPOSITE}$ = the set of composite numbers

and

**Definition 2.** $\mathsf{PRIME}$ = the set of prime numbers.

We describe our algorithms in terms of deciding $\mathsf{COMPOSITE}$, because they have *one-sided error*: if on input $n$ the algorithm answers "yes, $n \in \mathsf{COMPOSITE}$" we will prove that this answer is always correct. If on the other hand the algorithm cannot be sure that $n \in \mathsf{COMPOSITE}$ we will prove that there is a reasonable probability that $n$ is actually prime.

## 2. The "Fermat" Test

Our first algorithm relies on Fermat's little theorem:

**Theorem 3.** *If $n \in \mathsf{PRIME}$ and $a \in (\mathbb{Z}_n - \{0\})$, then $a^{n-1} \equiv 1 \mod n$*

**Input**: $n$
**Output**: is $n \in \mathsf{COMPOSITE}$?
**begin**
  **for** $t$ *trials* **do**
    Choose $a \in (\mathbb{Z}_n - \{0\})$ uniformly at random;
    **if** $\gcd(a, n) \neq 1$ **then**
      $n \in \mathsf{COMPOSITE}$;
    **else if** $a^{n-1} \not\equiv 1 \mod n$ **then**
      $n \in \mathsf{COMPOSITE}$;
    **end**
  **end**
  Output "not sure" ; `/* We made it through all` $t$ `tests,` $n$ `may be prime */`
**end**

**Algorithm 1:** "Fermat" primality test

First note that, as promised, the output "composite" is always correct. If the algorithm is not sure, then we will show that $n$ is prime with probability $(1-2^{-t})$ or $n$ is a "Carmichael number".

**Definition 4** (Carmichael number)**.** A composite number $n$ is a *Carmichael number* if

$$\forall a \in \mathbb{Z}_n^* \; a^{(n-1)} \equiv 1 \mod n$$

Unfortunately for the Fermat test, infinitely many Carmichael numbers exist, and from the definition above it is clear that they are exactly the composite numbers that will always fool this test. So for now we will ignore them and prove:

**Theorem 5.** *For $n$ composite and not a Carmichael number, the Fermat test outputs "composite" with probability* $(1-2^{-t})$

*Proof.* Suppose $\exists a \in \mathbb{Z}_n^*$ such that $a^{(n-1)} \not\equiv 1 \mod n$. All we need to show is the $> \frac{1}{2}$ of the members of $\mathbb{Z}_n^*$ have this property. Define:

$$G_n := \{a \in \mathbb{Z}_n^* | a^{(n-1)} \equiv 1 \mod n\}$$

$G_n$ is a subgroup. If $G_n \neq \mathbb{Z}_n^*$ (as is the case for composite non-Carmichael $n$), then $|G_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$. □

## 3. The Jacobi Symbol

Recall the Legendre symbol, $\left[\frac{a}{p}\right] = a^{(p-1)/2}$ for $p$ an odd prime. The Jacobi symbol generalizes the Legendre symbol to odd composite "denominators", and has many useful properties.

**Definition 6** (Jacobi Symbol)**.** Let $n > 2$ be an odd number, with prime factorization $p_1^{k_1}, \ldots, p_\ell^{k_\ell}$. Then the Jacobi symbol of $a$ and $n$ is:

$$\left[\frac{a}{n}\right] := \prod_{p_i} \left[\frac{a}{p_i}\right]^{k_i}$$

**Theorem 7.** *The Jacobi symbol has the following properties:*

(1) *For $n$ prime, the Jacobi symbol $\left[\frac{a}{n}\right]$ is equal to the Legendre symbol $\left[\frac{a}{n}\right]$*

(2) *The Jacobi symbol always takes values in $\{0, 1, -1\}$, and takes value 0 iff* $\gcd(a, n) \neq 1$

(3) $\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right] \cdot \left[\frac{b}{n}\right]$

(4) $\left[\frac{a}{n}\right] \cdot \left[\frac{a}{m}\right] = \left[\frac{a}{nm}\right]$

(5) *if* $a \equiv b \mod n$, *then* $\left[\frac{a}{n}\right] = \left[\frac{b}{n}\right]$

(6) $\left[\frac{1}{n}\right] = 1$

(7)

$$\left[\frac{2}{n}\right] = \begin{cases} -1 & \textit{if } n \equiv 3 \textit{ or } 5 \mod 8, \\ 1 & \textit{if } n \equiv 1 \textit{ or } 7 \mod 8. \end{cases}$$

(8) *For* $a$ *odd,*

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

The proofs of parts (1)-(6) of Theorem 7 are simple, and left as an exercise. The proofs of parts (7) and (8) are postponed until the next lecture.

**Theorem 8.** *The Jacobi symbol cam be computed in polynomial time.*

*Proof.* The proof is a recursive algorithm similar to Euclid's. If $a$ is even, repeatedly use properties (7) and (3):

$$\left[\frac{a}{n}\right] = \left[\frac{2}{n}\right] \left[\frac{\frac{a}{2}}{n}\right]$$

until $a$ is odd.

If $a$ is odd and $a < n$, use properties (5) and (8), with $n' = n \mod a$:

$$\left[\frac{a}{n}\right] = (-1)^{\cdots} \left[\frac{n'}{a}\right]$$

If $a$ is odd and $a > n$, use (5):

$$\left[\frac{a}{n}\right] = \left[\frac{a \mod n}{n}\right]$$

We are always reducing the value of $|a| + |n|$, and finally when $a = 1$ or 2, we use (6) or (7). □

## 4. Solovay-Strassen Primality Test

Due to Solovay-Strassen, SIAM J. on Computing, 6 (1977) pp 84-85, erratum in SICOMP 7 (1978) 118. This algorithm uses properties of the Jacobi symbol to avoid failure on Carmicheal numbers.

**Theorem 9.** *There exists a randomized polynomial time algorithm which on input $n > 2$ and composite will output "composite" with probability $> \frac{1}{2}$, and on input $n > 2$ and prime will output "not sure".*

This algorithm also has the "one-sided error" property discussed earlier, and can be iterated $t$ times to reduce the probability that it makes an error, giving a success probability of $\left(1 - \frac{1}{2^t}\right)$.

**Input**: odd $n > 2$
**Output**: is $n \in \mathsf{COMPOSITE}$?
**begin**
  Choose $a \in (\mathbb{Z}_n - \{0\})$ uniformly at random;
  **if** $\gcd(a, n) \neq 1$ **then**
    $n \in \mathsf{COMPOSITE}$;
  Compute $a^{(n-1)/2} \mod n$, and $\left[\frac{a}{n}\right]$;
  **else if** $a^{(n-1)/2} \mod n \neq \left[\frac{a}{n}\right]$ **then**
    $n \in \mathsf{COMPOSITE}$;
  **end**
  Output "not sure" ; `/* n may be prime! */`
**end**

**Algorithm 2:** Solovay-Strassen primality test

The key idea here is that the two methods of computing $\left[\frac{a}{n}\right]$ must agree if $n$ is prime. Clearly, if the algorithm outputs "composite", $n \in \mathsf{COMPOSITE}$. What remains is to show that, enough of the time, these two methods of computing the Jacobi symbol with *disagree* for composite $n$.

**Claim 10.** *If $n \in$ COMPOSITE, then the algorithm outputs "composite" with probability $\geq \frac{1}{2}$*

*Proof.* Define:

$$J_n := \{a \in (\mathbb{Z}_n - \{0\}) : a^{(n-1)/2} = \left[\frac{a}{n}\right] \mod n\}$$

This is exactly the set of numbers that will confuse Solovay-Strassen. Observe that $J_n$ is a subgroup of $\mathbb{Z}_n^*$, and so to bound our proability of error it will suffice to show that $J_n \neq \mathbb{Z}_n^*$, since then $|J_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$.

If we suppose towards a contradiction that $J_n = \mathbb{Z}_n^*$, we can split into two cases based on the prime factorization of $n$. Write $n = p_1^{k_1} \dots p_\ell^{k_\ell}$.

The first case is when $k_1 = 1, \ell \geq 2$ Let $g \in \mathsf{GEN}[Z_{p_1}^*]$, that is, $g$ is a generator of $Z_p^*$. Then by the Chinese Remainder Theorem, there is a a (unique) $a \in \mathbb{Z}_n^*$ such that $a \equiv g \mod p_1$ and $a \equiv 1 \mod p_2^{k_2} \dots p_\ell^{k_\ell}$. Then by (4) we have:

$$\begin{aligned}\left[\frac{a}{n}\right] &= \left[\frac{a}{p_1}\right]\left[\frac{a}{p_2^{k_2}\dots p_\ell^{k_\ell}}\right] \\ &= g^{(p_1-1)/2}\cdot 1 \\ &= (-1)\cdot(1) \\ &= -1\end{aligned}$$

So by $J_n = \mathbb{Z}_n^*$ $\left[\frac{a}{n}\right] = -1$, contradicting our choice of $a$, since $a = 1 \mod p_2^{k_2}\dots p_\ell^{k_\ell}$ implies that $a^{(p-1)/2} \not\equiv -1 \mod p_2^{k_2}\dots p_\ell^{k_\ell}$ and hence that $a^{(p-1)/2} \not\equiv -1 \mod n$.

The second case is when $k_1 \geq 2, \ell \geq 1$. We take $a$ as in case 1. Then by $J_n = \mathbb{Z}_n^*$,

$$a^{(n-1)/2} \equiv \left[\frac{a}{n}\right] = \pm 1$$

We know that $a^{(n-1)} \equiv 1 \mod n$, therefore $a^{(n-1)} \equiv 1 \mod p_1^{k_1}$.

Thus $\phi(p_1^{k_1})|(n-1)$, because $\phi(p_1^{k_1})$ is equal to the order of $a$. So $p_1^{(k-1)}(p-1)|(n-1)$, thus $p_1|(n-1)$ (since $k_1 > 1$). This contradicts that $p_1|n$, as $p_1$ was one of our factors of $n$, concluding the proof.

$\square$