CSE300 - Modern Cryptography	March 7, 2000
Lecture #11	Scribe: Jie Yang

1 Primality Testing II: The Miller-Rabin Test

Today we will finish our discussion of primality testing, proving the correctness of the Miller-Rabin primality test. The Miller-Rabin test (which we denote MR) applied to a positive integer n, is the following procedure:

1. Select $x \in_R \{1, \ldots, n-1\}$
2. Compute $\gcd(x, n) = d$, if $d \neq 1$, then return ”*composite*”. (Observe that when $\gcd(x, n) = 1$, $x \in_R \mathbb{Z}_n^*$.)
3. Write $n - 1 = m \cdot 2^k$, where m is odd.
4. If $x^m \equiv 1 \pmod{n}$, then return ”*prime*”.
5. For $i = 0$ to $k - 1$ do
   if $x^{m \cdot 2^i} \equiv -1 \pmod{n}$, then return ”*prime*”,
6. Answer ”*composite*”.

Our goal is to prove two properties of this test:

- when n is prime, the test always responds with “*prime*”,
- when n is composite, the responds with “*composite*” with probability at least half.

Claim 1 *If n is prime, then*

$$\Pr[\text{MR}[n] = \text{"}prime\text{"}] = 1.$$

Proof: Let $x \in \{1, \ldots, p-1\} = \mathbb{Z}_p^*$. Observe that when p is prime, MR$[p]$ never answers ”*composite*” in Line 2. Recall Fermat's little theorem, which asserts that $\forall x \in 1, \cdots, p-1$

$$x^{p-1} = x^{m \cdot 2^k} \equiv 1 \pmod{p}$$

Now consider $x^m, x^{m \cdot 2}, \cdots, x^{m \cdot 2^k} = x^{p-1}$ and let t be the smallest element of $\{0, \cdots, k\}$ for which $x^{m2^t} \equiv 1$. (Observe that t is well-defined, since we know that $x^{m2^k} \equiv 1$.)

If $t = 0$, then $x^m \equiv 1$, and the test will respond with “*prime*” in step 4. Otherwise, observe that $x^{m2^{t-1}} \not\equiv 1$, but $\left(x^{m2^{t-1}}\right)^2 \equiv 1$. Recalling that there are only two square roots of 1 in $\mathbb{Z}/p^*$, we must have $x^{m2^{t-1}} \equiv -1$, in which case MR$[p]$ will return ”*prime*” either in line 5.

Claim 2 *If n is composite, then*

$$\Pr[\text{MR}[n] = \text{"composite"}] \geq \frac{1}{2}$$

Proof: Recall that a Carmichael number is a composite number n for which $\forall x \in \{1, \ldots, n-1\}$, $x^{n-1} \equiv 1 \bmod n$.

Case 1a: Suppose that n is neither a prime power nor a Carmichael number,

Define

$$B = \{x \mid x \in \mathbb{Z}_n^*,\ x^{n-1} \equiv 1 \bmod n\}.$$

We will see in a moment that when $x \notin B$, the Miller-Rabin test succeeds, returning "*composite*". We begin by showing that $|B|$ is small.

Check that B is a subgroup of $\mathbb{Z}_n^*$:

- $1 \in B$: $1^{n-1} = 1 \equiv 1 \pmod n$.
- $\forall x \in B, x^{-1} \in B$. Observe the following:

$$\begin{aligned}(x \cdot x^{-1})^{n-1} \equiv 1 \pmod n &\Longrightarrow x^{n-1} \cdot (x^{-1})^{n-1} \equiv 1 \pmod n \\ &\Longrightarrow (x^{-1})^{n-1} \equiv 1 \pmod n.\end{aligned}$$

- $\forall x_1,\ x_2 \in B,\ x_1 \cdot x_2 \in B$. Observe that $(x_1 x_2)^{n-1} = x_1^{n-1} \cdot x_2^{n-1} \equiv 1 \pmod n$.

Recalling that cardinality of any subgroup must divide the order of the group, and that $B \neq \mathbb{Z}_n^*$, we must have $|B| \leq \frac{|\mathbb{Z}_n^*|}{2}$

Therefore,

$$\Pr_x[x^{n-1} \not\equiv 1 \pmod n] = \Pr_x[x \notin B] \geq \frac{1}{2}.$$

Now, when $x \notin B$, that is $x^{n-1} \not\equiv 1 \pmod n$, then $\forall i \in \{0, \cdots, k-1\}$, $x^{m \cdot 2^i} \not\equiv -1 \pmod n$, and $x^m \not\equiv 1 \pmod n$. Hence $\text{MR}[n]$ will answer "composite" in the last step. This shows that

$$\Pr[\text{MR}[n] = \text{"composite"}] \geq \frac{1}{2}.$$

Case 1b: Suppose now that n is not a prime power, but it is a Carmichael number.

Let t be the largest element of $\{0, \cdots, k-1\}$ so that

$$-1 \in \{x^{m \cdot 2^t} \bmod n \mid x \in \mathbb{Z}_n^*\}.$$

Define $B_t = \{x \mid x \in \mathbb{Z}_n^*,\ x^{m \cdot 2^t} \equiv \pm 1 \pmod n)\}$

As before, we will show that when $x \notin B$, the Miller-Rabin algorithm succeeds, returning "*composite*".

Check that B_t is a subgroup of $\mathbb{Z}_n^*$:

- $1 \in B_t$ because $1^{m\cdot 2^t} = 1 \equiv 1 \pmod{n}$.
- $\forall x \in B_t,\ x^{-1} \in B_t$, where $x \cdot x^{-1} \equiv 1 \pmod{n}$. Observe that

$$(x \cdot x^{-1})^{n-1} \equiv \pm 1 \pmod{n} \Longrightarrow x^{n-1} \cdot (x^{-1})^{n-1} \equiv \pm 1 \pmod{n}$$
$$\Longrightarrow (x^{-1})^{n-1} \equiv \pm 1 \pmod{n}.$$

- $\forall x_1,\ x_2 \in B_t,\ x_1 \cdot x_2 \in B_t$. Observe that $(x_1 x_2)^{n-1} = x_1^{n-1} \cdot x_2^{n-1} \equiv \pm 1 \pmod{n}$.

Claim 3 *$B_t \neq \mathbb{Z}_n^*$, and hence $|B_t| \leq \frac{|\mathbb{Z}_n^*|}{2}$.*

Proof: By the definition of t, $\exists v \in \mathbb{Z}_n^*$ for which $v^{m\cdot 2^t} \equiv -1 \pmod{n}$. Recall n is not a prime power, so that n can be written $n = a \cdot b$ where $\gcd(a, b) = 1$, and $a, b > 1$.

By the Chinese remainder theorem, $\exists w,\ 0 \leq w < n$, so that

$$w \equiv v \pmod{a}$$
$$w \equiv 1 \pmod{b}$$

Considering that both v and 1 are elements of $\mathbb{Z}_n^*$, you can check that w must be. We will now show, however, that $w \notin B_t$, as desired.

Consider $w^{m\cdot 2^t}$: we must have

$$w^{m\cdot 2^t} \equiv v^{m\cdot 2^t} \equiv -1 \pmod{a}$$
$$w^{m\cdot 2^t} \equiv 1^{m\cdot 2^t} \equiv 1 \pmod{b}$$

But in this case, $w^{m\cdot 2^t} \not\equiv \pm 1 \pmod{n}$, since, of course, if $w = 1$ then $w \equiv 1 \pmod{a}$ and $w \equiv 1 \pmod{b}$; similarly for $w \equiv n - 1$: since $p \mid n$ and $q \mid n$, $n - 1 \equiv -1 \pmod{p}$ and $n - 1 \equiv -1 \pmod{q}$.

As before, we must have

$$|B_t| \leq \frac{1}{2}|\mathbb{Z}n|$$

Claim 4 *If $x \notin B_t$ is selected in step 1, then* $\mathrm{MR}[n] =$ *"composite".*

Proof: Observe that if $x \notin B_t$, then $x^{m\cdot 2^t} \not\equiv \pm 1$. Furthermore, by the definition of t, for each $s > t$, $x^{m2^s} \not\equiv -1$. Hence $x^{m2^s} \not\equiv -1 \pmod{n}$ for all $s = 0, \ldots, k-1$, so that $\mathrm{MR}[n]$ must answer "*composite*". (Observe that if $x^{m2^\ell} \equiv \pm 1 \pmod{n}$ then $x^{m2^{\ell'}} \equiv 1 \pmod{n}$ for all $\ell' > \ell$.

<u>Conclusion:</u> From Claim 3, we have that

$$\Pr_x[x \in B_t] \leq \frac{1}{2}.$$

From Claim 4, we have that

$$\Pr[\text{MR}[n] = \text{"}\textit{composite}\text{"}] \geq \Pr_x[x \notin B_t] \geq \frac{1}{2}.$$

Case 2: Suppose n is a prime power

Recall that if $n = p^k$, then $\mathbb{Z}_n^*$ is a cyclic group: $\exists\gamma$, such that $\langle\gamma\rangle = \{\gamma, \gamma^2, \ldots, \gamma^{o(\gamma)}\} = \mathbb{Z}_n^*$. Then

$$o(\gamma) = |\mathbb{Z}_n^*| = \phi(n) = \phi(p^k) = p^{k-1}(p-1).$$

In particular, recall that for each $i \neq j$ with $1 \leq i, j \leq \phi(n)$, $\gamma^i \neq \gamma^j$.

As in the first case we considered, define $B = \{x \mid x^{n-1} \equiv 1 \pmod{n}\}$. As before, you may check that B is a subgroup of $\mathbb{Z}_n^*$.

Because $p \nmid p^k - 1$ we must have $p^{k-1}(p-1) \nmid p^k - 1$. Then

$$\gamma^{n-1} = \gamma^{p^k - 1} \equiv \gamma^{(n-1) \bmod \phi(n)} \not\equiv 1 \pmod{n}$$

because $\phi(n) = p^{k-1}(p-1) \nmid n - 1 = p^k - 1$. Hence

$$B \neq \mathbb{Z}_n^*$$

and we may proceed as in the first case to show that $\text{MR}[n]$ will answer "*composite*" in Line 6 with probability at least $\frac{1}{2}$.

Hence

$$\Pr[\text{MR}[n] = \text{"}\textit{composite}\text{"}] = \Pr_x[x \notin B] \geq \frac{1}{2}.$$

Observe that by the previous proof, the naive algorithm we discussed previously works for all non-Carmichael numbers. In particular, when n is prime, it answers "*prime*" with probability 1, and when n is a composite non-Carmichael number, it answers "*composite*" with probability at least $\frac{1}{2}$.

Naive(n)

1. Select $x \in_R \{1, \cdots, n-1\}$.
2. If $x^{n-1} \equiv 1 \pmod{n}$, answer "*prime*".
3. Answer "*composite*".