Lecture 9 Miller – Rabin Primality Test

This lecture gives an algorithm for determining whether or not a positive integer is a prime number.

We first need a variation of Fermat's Little Theorem

Fermat's Little Theorem Version 2
If *p* is prime the for every integer *a* we have $a^p \equiv a \pmod{p}$.

Proof: If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$ (by the first version of Fermat's Little Theorem). Hence $a^p \equiv a \pmod{p}$.

If $p \mid a$ then $0 \equiv a^p \equiv a \pmod{p}$.

Note: the converse of this theorem is **not** true! For example, $2^{341} \equiv 2 \pmod{341}$. But 341 is not prime (341 = 11*31). We say that 341 is a 2 pseudoprime.

Def. In general if *n* is a composite number and $a^n \equiv a \pmod{n}$ for a specific integer *a* then we say *n* is an ***a* – pseudoprime**.

Def. If *n* is a composite number and for every integer *a* we have $a^p \equiv a \pmod{n}$ then we say that *n* is a **Carmichael number**.
(Note: it suffices to prove that *n* is a Carmichael number it suffices to show that $a^{p-1} \equiv 1 \pmod{n}$ for every *a* relatively prime to *n*)

The following version of the Chinese Remainder Theorem is often useful in proving a number is a Carmichael number.

Chinese Remainder Theorem (Version 2) Assume that $n_1, n_2, ..., n_k$ are pairwise relatively prime. Let $n = n_1 * n_2 * \cdots * n_k$. Then there is a ring isomorphism $\mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$

Pf: Define a function $f: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ by $f(x) = (x \bmod n_1, x \bmod n_2, ..., x \bmod n_k)$

(1) *f* is a one-to-one function.

Assume that $f(x) = f(y)$. Then
$x \equiv y \pmod{n_1}, x \equiv y \pmod{n_2}, \ldots, x \equiv y \pmod{n_k} \Rightarrow n_1 \mid (x-y), n_2 \mid (x-y), ..., n_k \mid (x-y)$
$\Rightarrow n \mid (x-y) \Rightarrow x \equiv y \pmod{n}$

(2) f is an onto function

Let $(a_1, a_2, ..., a_k) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. By the first version of the Chinese Remainder Theorem there is an x, which is unique mod n, such that $x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, ..., x \equiv a_k \pmod{n_k}$. So we have $f(x) = (a_1, a_2, ..., a_k)$.

(3) Addition and multiplication

$$\begin{aligned} f(x+y) &= ((x+y) \bmod n_1, (x+y) \bmod n_2, ..., (x+y) \bmod n_k) \\ &= (x \bmod n_1, x \bmod n_2, ..., x \bmod n_k) + (y \bmod n_1, y \bmod n_2, ..., y \bmod n_k) \\ &= f(x) + f(y) \end{aligned}$$

$$\begin{aligned} f(xy) &= (xy \bmod n_1, xy \bmod n_2, ..., xy \bmod n_k) \\ &= (x \bmod n_1, x \bmod n_2, ..., x \bmod n_k) * (y \bmod n_1, y \bmod n_2, ..., y \bmod n_k) \\ &= f(x) * f(y) \end{aligned}$$

Theorem: 561 is a Carmichael number.

Pf: First note that 561 is so composite: $561 = 3 * 11 * 17$ .Let a be relatively prime to 561, we need to prove that $a^{560} \equiv 1 \pmod{561}$

By Fermat's Little Theorem $a^2 \equiv 1 \pmod{3}, a^{10} \equiv 1 \pmod{11}, a^{16} \equiv 1 \pmod{17}$. Since 80 is a common multiple of 2,5,16 we then have $a^{80} \equiv 1 \pmod{3}, a^{80} \equiv 1 \pmod{11}, a^{80} \equiv 1 \pmod{17}$

By the second version of the Chinese Remainder Theorem these congruences imply that $a^{80} \equiv 1 \pmod{561} \Rightarrow a^{560} \equiv 1 \pmod{561}$. This proves that 561 is a Carmichael number.

The Miller Rabin test is based on the following theorem.

Theorem: Let p be an odd prime and write $p - 1 = 2^k q$ (where q is odd). Let a be an integer not divisible by p. Then one of the following two conditions must be true:

(i) $a^q \equiv 1 \pmod{p}$

(ii) One of the numbers $a^q, a^{2q}, ..., a^{2^{k-1}q}$ is $\equiv -1 \pmod{p}$

Pf: By Fermat's Little Theorem $a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{2^k q} \equiv 1 \pmod{p}$. Consider the following sequence: $a^q, a^{2q}, ..., a^{2^{k-1}q}, a^{2^k q}$

Since the last number in the list is congruent to 1 mod p and each number is the square of the previous number in the sequence, there are two possibilities:
$a^q \equiv 1 \pmod{p}$ or some number in the sequence is not congruent to 1 mod p but its square is congruent to 1 mod p. The only way this can happen is that this number is $\equiv -1 \pmod{p}$.

Def. A number a is called a Miller – Rabin **witness** for n if $a^q \not\equiv 1 \pmod{p}$ and $a^{2^i q} \equiv -1 \pmod{p}$ for all $i = 0,1,\ldots,2^{k-1}q$.

Miller – Rabin Test:
Let n be a positive integer and a be a possible witness for n.
Note: the following test will determine either that a is a witness for n in which case n is composite or the test fails in which case one can check another value of a for possibly being a witness.

Step 1: If n is even or $1 < \gcd(a,n) < n$ then n is composite.
Step 2: Write $n - 1 = 2^k q$ where q is odd.
Step 3: Set $a = a^q \pmod{n}$
Step 4: For i = 0, 1, …, k – 1
Step 5: If $a \equiv -1 \pmod{n}$ then test fails
Step 6: Set a = $a^2 \bmod n$
Step 7: n is composite.

Examples:
(1) $n = 561$. $n - 1 = 2^4 * 35$. So $k = 4, q = 35$
Try $a = 2$ as a possible witness.

$2^{35} \equiv 263 \not\equiv 1 \pmod{561}$

$2^{35} \not\equiv -1 \pmod{561}$
$2^{2*35} \equiv 263^2 \equiv 166 \not\equiv -1 \pmod{561}$
$2^{2^2*35} \equiv 166^2 \equiv 67 \not\equiv -1 \pmod{561}$
$2^{2^3*35} \equiv 67^2 \equiv 1 \not\equiv -1 \pmod{561}$

So 2 is a witness for 561, hence 561 is composite.

(2) $n = 172947529$. $n - 1 = 2^3 * 21618441$. So $k = 3, q = 21618441$

$2^{21618441} \equiv 40063806 \not\equiv 1 \pmod{n}$
$2^{21618441} \not\equiv -1 \pmod{n}$
$2^{2*21618441} \equiv 40063806^2 \equiv 2257065 \not\equiv -1 \pmod{n}$
$2^{2^2*21618441} \equiv 2257065^2 \equiv 1 \not\equiv -1 \pmod{n}$

So 2 is a witness for n, hence n is composite.

(3) $n = 32789$. $n - 1 = 2^2 * 8197$. So $k = 2, q = 8197$
Try $a = 2$ as a possible witness.

$$2^{8197} \equiv 6087 \not\equiv 1 \pmod{32789}$$
$$2^{8197} \equiv 6087 \not\equiv -1 \pmod{32789}$$
$$2^{2*8197} \equiv 6087^2 \equiv 32788 \equiv -1 \pmod{32789}$$

2 is not a witness. Try $a = 3$ as a possible witness.

$$3^{8197} \equiv 26702 \not\equiv 1 \pmod{32789}$$
$$3^{8197} \equiv 26702 \not\equiv -1 \pmod{32789}$$
$$3^{2*8197} \equiv 26702^2 \equiv 32788 \equiv -1 \pmod{32789}$$

3 is not a witness. Try $a = 5$ as a possible witness.

$$5^{8197} \equiv 1 \pmod{32789}$$

5 is not a witness. Try $a = 7$ as a possible witness.

$$7^{8197} \equiv 32788 \not\equiv 1 \pmod{32789}$$
$$7^{8197} \equiv 32788 \equiv -1 \pmod{32789}$$

7 is not a witness. Try $a = 11$ as a possible witness.

$$11^{8197} \equiv 1 \pmod{32789}$$

11 is not a witness. Try $a = 13$ as a possible witness.

$$13^{8197} \equiv 1 \pmod{32789}$$

13 is not a witness. Conclude that 32789 is probably a prime (in fact it is a prime).