Lecture 12 Primality testing § 3.4.

For RSA need a good way to generate primes.

Some RSA keys have been attacked by accumulating a long list of public keys $N_1, N_2, \ldots$ & computing gcd of each pair. If two people used same prime, this breaks both people's keys.

So need a good way to produce large primes. To insure our number isn't divisible by small primes pick it as $1 + (p_1 \cdots p_r) \cdot k$ where $p_1, \ldots, p_r$ are the first r primes.

We need a way to efficiently check if such

a candidate is prime.

We use the Miller-Rabin test which is a probabilistic test.

Rmk Miller Rabin only works deterministically if we assume generalized Remann hypothesis.

There is a test from 2004 called AKC which works independent of GRH, but it is much slower so everyone uses Miller-Rabin.

Recall p prime $\Rightarrow \forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a^{p-1} \equiv 1$

$\Rightarrow \forall a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

If N is composite, then for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$,

$a^{\phi(N)} \equiv 1 \pmod{N}$.

Usually, $a^N \not\equiv a \pmod N$ when N composite.

Ex $N = 15 = 3 \cdot 5$

$\phi(N) = (3-1)(5-1) = 8 \Rightarrow a^8 \equiv 1 \pmod N$

For $a = 2$, $a^{15} = 2^{15} = 128 \equiv 8 \not\equiv a$.

So N is prime $\Rightarrow a^N \equiv a$ for all $a \in \mathbb{Z}$.

If $\exists\ a \in \mathbb{Z}$ s.t. $a^N \not\equiv a \pmod N$ then N is composite.

Def A witness of composition of N is an integer a s.t $a^N \equiv a \pmod N$.

Unfortunately not every composite number has a witness of composition.

Def A Carmichael number is a composite number w/o any witnesses of compositon.

Ex $561 = 3 \cdot 11 \cdot 17$.

$\operatorname{lcm}(3-1, 11-1, 17-1) = \operatorname{lcm}(2, 10, 16) = 80$.

$\Rightarrow$ for all $a \in (\mathbb{Z}/561\mathbb{Z})^\times$, $a^{80} \equiv 1 \pmod{561}$.

b/c $80 \mid 561 - 1$, $a^{560} \equiv 1 \bmod 561$

for all $a \in (\mathbb{Z}/561)^\times$.

Miller-Robin Test

Idea: In $(\mathbb{Z}/p)^\times$, 1 has only two square roots ± 1. In $(\mathbb{Z}/N)^\times$ when N is composite, 1 has at least 4 square roots.

Prop Suppose that p is an odd prime and $p-1 = 2^k q$ w/ q odd. Suppose $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Then either

(1) $a^q \equiv 1 \pmod p$, or

(2) one of $a^q, a^{2q}, \dots, a^{2^{k-1}q}$ is congruent to $-1 \bmod p$.

Ex $p = 13$, $p-1 = 12 = 2^2 \cdot 3 \Rightarrow k=2$ & $q=3$.

$a = 4 \in (\mathbb{Z}/13\mathbb{Z})^\times$

✗ (1) $a^q = 4^3 = 64 \equiv -1 \neq 1 \pmod{13}$

(2) $a^q \equiv -1$ ✓

Pf Know $a^{p-1} \equiv a^{2^k q} \equiv 1 \mod p$.

$\Rightarrow a^{2^{k-1} q} =$ square root of $a^{2^k q} = \pm 1$.

If it's -1, then ✓

otherwise it's 1 & we can repeat.

At some point we have to hit a -1 or all

$a^{2^i q} \equiv 1$ in particular $a^q \equiv 1$. □

Summary Given N, write $N-1 = 2^k q$.

N is prime $\Rightarrow$ either $a^q \equiv 1$ or $\exists i$ s.t. $a^{2^i q} \equiv -1$ for all $a \in \mathbb{Z}$.

N is composite $\Leftarrow$ $\exists a \in \mathbb{Z}$ s.t. $a^q \not\equiv 1$ & $a^{2^i q} \not\equiv -1$ for all i.

B/c if N is composite, there are more than two solutions to $x^2 \equiv 1 \mod N$.

Ex $N = 561$, $N-1 = 2^4 \cdot 35$

$a = 2$

(1) $a^{35} \equiv 1$? $\quad 2^{35} \equiv 263 \not\equiv 1$ ×

(2) $a^{2^k \cdot 35} \equiv -1$?

$a^{2 \cdot 35} \equiv -1$? $\quad 2^{70} \equiv 166 \not\equiv -1$ ×

$a^{4 \cdot 35} \equiv -1$? $\quad 2^{140} \equiv 67 \not\equiv -1$ ×

$a^{8 \cdot 35} \equiv -1$? $\quad 2^{280} \equiv 1 \not\equiv -1$ ×

So a is a Miller-Rabin witness.

& $a^{49} = 67$ is an extra square root of 1 which wouldn't exist if 561 were prime.

There are 8 square roots of 1 in $\mathbb{Z}/561\mathbb{Z}$:

1, 67, 188, 254, 307, 373, 494, 560

To check if N is composite, randomly choose a's to see whether they are Miller-Rabin witnesses. If N is odd composite, at least 75% of $a = 1, \ldots, N-1$ are MR-witnesses.

Examples

(1) If $N = m_1 m_2$ m_1 & m_2 relatively prime $N-1 = 2^k q$

Chinese Remainder thm says

$$(\mathbb{Z}/N)^\times \cong (\mathbb{Z}/m_1)^\times \times (\mathbb{Z}/m_2)^\times$$

$$\downarrow$$

Pick $a \hookrightarrow (1, -1)$

Then a is a Miller Rabin witness:

$a^q \hookrightarrow (1^q, (-1)^q) = (1, -1)$ b/c q odd.

So $a^q \equiv -1 \mod m_2 \Rightarrow a^q \not\equiv 1$.

$a^q \equiv 1 \mod m_1 \Rightarrow a^q \not\equiv -1$.

$a^{2q} \hookrightarrow (1^2, (-1)^2) = (1,1) \Rightarrow a^{2q} = 1$.

$\Rightarrow$ a Miller-Rabin Witness.

So we can see explicitly that if N is divisible by distinct primes, there is a MR-witness.

(Though algorithm depends on there being lots of MR witnesses). Other case is that N is a prime power. Here too we can check $\exists$ at least one MR witness:

(2) $N = p^n$, $N-1 = 2^k q$.

Pick $a = -(p^{n-1}+1)$

$$a^n = (-1)^n \left(1 + n p^{n-1} + \binom{n}{2}\left(p^{n-1}\right)^2 + \cdots\right)$$

$$\equiv (-1)^n \left(1 + n p^{n-1}\right) \mod p^n$$

If we set $n = 2p$, we see

$$a^{2p} = (-1)^{2p}\left(1 + (2p) p^{n-1}\right) \equiv 1 \mod p^n.$$

So a has order $2p$.

(1) $a^q \not\equiv 1$ since q is odd.

(2) $a^{2^j q} \not\equiv -1$ b/c that would imply

$$q^{2^{j+1}q} \equiv 1 \quad \Rightarrow 2p \mid 2^{j+1}q$$

$$\Rightarrow p \mid 2^j q$$

$$\Rightarrow p \mid p^2 - 1 \quad \text{a contradiction.}$$