LESSON 14

PRIMALITY TESTS

Discrete Log Problem

Diffie Hellman Key Exchange

PRIMALITY TESTS

Recall Fermat's Theorem.

Theorem: If p is a prime and $\gcd(a,p)=1$, then $a^{p-1} \equiv 1 \bmod p$

The Tests are based on this result. Specifically, if $a^{p-1} \equiv 1 \bmod p$ does not hold, then p is not a prime. The Test does not conclusively prove that p is a prime, but it can show that p is not a prime

Ex. Let $p=6$, $a=2$. $2^5 \equiv 32 \bmod 6$
$= 2 \neq 1$. So 6 is not a prime.

Ex. Let $p = 341$ and $a = 2$.

$2^{340} \equiv 1 \mod 341$. This does not tell us that 341 is a prime. In fact $341 = 11 \cdot 31$

341 is called a psuedoprime to the base 2.

Ex Let $p = 341$ and $a = 3$. Then

$3^{340} \equiv 56 \mod 341$. Hence p is not a prime.

Some non primes are psuedoprimes for every base a with $\gcd(a, p-1) = 1$

Ex $p = 561$. p is such a number:

$a^{p-1} \equiv 1 \mod p$ for all a with $\gcd(a, p-1) = 1$. Since $561 = 3 \cdot 11 \cdot 17$, p is not a prime.

Def A non-prime p such that $a^{p-1} \equiv 1 \mod$ for all a with

$\gcd(a, p) = 1$ is called a Carmichael number after a number theorist from 100 years ago

The integers tested are often quite large Hence the first prime divisor might also be large. If we were testing $a = 2, 3, \ldots$ we would need to get to the first prime divisor for $a^{p-1} \equiv 1 \bmod p$ to fail when p is a Carmichael number

The first 3 psuedo primes base 2 are 341, 561, 645 so primes are much more abondant than psuedoprimes

Another fact is that Carmichael numbers are always

The product of at least 3 primes.

Stronger Test

The Strong Psuedoprime Test

Suppose $\gcd(b, n) = 1$. We assume that n is odd. Then

$$n - 1 = 2^s t \quad \text{where } t \text{ is odd}$$

Then
$$\begin{aligned} b^{n-1} - 1 &= (b^{2^{(s-1)}t} - 1)(b^{2^{(s-1)}t} + 1) \\ &= \\ &= (b^t - 1)(b^t + 1)(b^{2t} + 1)(b^{4s} + 1) \\ &\quad \cdots (b^{2^{(s-1)}t} + 1) \end{aligned}$$

If n is a prime, then $b^{(n-1)} \equiv 1 \bmod n$, hence n divides the right hand side of the expansion. Thus n, being a prime, divides one of the

terms in the expansion. If not, then n is not a prime

This is the test

We use $b^r - 1$ is divisible by $n \Leftrightarrow b^r \equiv 1 \mod n$

Hence n divides one of the terms in the expansion $\Leftrightarrow$ One of the congruences hold

$$b^t \equiv 1 \mod n$$
$$b^t \equiv -1 \mod n$$
$$b^{2t} \equiv -1 \mod n$$
$$b^{4t} \equiv -1 \mod n$$
$$\vdots$$
$$b^{2^{(p-1)}t} \equiv -1 \mod n$$

It makes it easier computationally to go through this list by squaring the preceeding term.

If none of them hold, n is not a prime

Ex Let $n = 341$

$341 - 1 = 4 \cdot 85$

$t = 85, \quad s = 2$

$$b^{n-1} - 1 = (b^{85} - 1)(b^{85} + 1)(b^{170} + 1)$$

Let $b = 2$. If n is a prime, it must divide one of the three terms in the expansion or one must hold

$$2^{85} \equiv 1 \mod 341$$
$$2^{85} \equiv -1 \mod 341$$
$$2^{170} \equiv -1 \mod 341.$$

Now $2^{85} \equiv 32 \mod 341$

and $(2^{85})^2 \equiv 32^2 \mod 341 \equiv 1 \mod 341$

So none of the congruences hold and n is not a prime

This method could fail, for some a, that n is not a prime. Then one of the congruences would hold. The first n is $n = 2047$ when a is 2. n is called a strong psuedoprime to the base 2 Unlike psuedoprimes, the strong psuedoprime test can not always fail so there are no analogues to Carmichael numbers In fact

Theorem A composite n ~~can~~ is shown to be composite for at least 1/2 of the a's with $\gcd(a, n) = 1$

Thus if this test has ~~at~~ a congruence satisfied for a for t different bases (a's) the chance it is composite is $\leq \left(\frac{1}{2}\right)^t$. So the chance it is prime is $1-\left(\frac{1}{2}\right)^t$.

So after t different bases either

1. It is shown to be composite (No congruence satisfied)
2. The probability it is prime is $\geq 1-\left(\frac{1}{2}\right)^t$ (this is when in each of the t a's some congruence is satisfied

The Discrete Log Problem
(D. L. P.)

Let a, b, x and n be integers such that $b \equiv a^x \bmod n$. Suppose a, b and n are known. Can x be found? If n is reasonably small, trial and error could be used. (Let $x = 1, 2, \ldots$) However, if n is big, this is a very difficult problem, one which can be used in cryptography

Ex. Let $a = 2$, $b = 15$, $n = 17$.
Start with $x = 1, 2, \ldots$
until we find $2^5 \equiv 15 \bmod 17$.
Hence $x = 5$

Bob picks an integer b, computes $z = c^b \bmod p$ and sends z and $K = x^b = c^{ab} \bmod p$ which he keeps. Alice computes $z^a \equiv c^{ab} \bmod p = K$.

Now Bob has $K = x^b \equiv c^{ab} \bmod p$

and Alice has

$$z^a = c^{ab} \bmod p = K$$

The common value they have K also gives them a public key to use.

Eve knows c, p, x and z.

where $x = c^a \bmod p$ and

$z = c^b \bmod p$.

She wants $K = c^{ab} \bmod p$

She can find K if she can find a and b. BUT finding a or b is the hard D.L.P Alice and Bob are depending that Eve can not find them.

Ex. Alice picks $p = 23$ and $c = 5$. and sends (p, c) to Bob

Alice picks $a = 6$ and finds

$$x = c^a \bmod p = 5^6 \bmod 23 = 8$$

which she send to Bob

Bob picks $b = 15$ and finds both

$$y = c^b = 5^{15} \bmod 23 = 19$$

and

$$K = x^b = 8^{15} \bmod 23 = 2$$

Bob sends y to Alice who computes

$$y^a = c^{ab} \bmod 23$$

Both y^a and x^b equal

$$K = c^{ab} \bmod p$$

K is the key they will use

Notice Eve knows

$p = 23$, $c = 5$, $x = 8$, $y = 19$

How can Eve find K?

The Diffie Hellman Key Exchange

A Key exchange is Alice and Bob constructing a key to use in cryptography. In a classic 1976 paper, Diffie and Hellman were showing a key exchange and the ideas led to public key cryptography although that was not their intention

D-FFIE-Hellman

Alice picks a prime p and an integer c with $\gcd(c,p)=1$ and sends (c,p) to Bob

Alice also picks an integer a, computes $x = c^a \bmod p$ and sends x to Bob

Summarizing, Eve knows p, c, x, y. where

$x = c^a \bmod p \quad y = c^b \bmod p$

She can find $K = c^{cb} \bmod p$ if she can solve the DLP for a and b.

She can also find K if she can compute c^{ab} from her information. This is called the Diffie-Hellmen problem (or DHP). If she can solve the DLP then she can solve the DHP. So the DLP is at least as hard as the DHP. It is not known if solving the DHP will allow a solution to the DLP. Again the DHP is Given $x \equiv c^a \bmod p$, $y = c^b \bmod p$, find

$K = c^{ab} \bmod p$

Problem. Let $c = 5$, $p = 23$

If $c^a \bmod p = 4$

$c^b \bmod p = 17$

Find $c^{cb} \bmod p$