(Fermat - Euler Theorem) Let p be a prime.

Let $a \not\equiv 0 \pmod{p}$. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

We can use this to test whether a number is prime or not.

Suppose we want to test if n is prime. If we can find some $a \not\equiv 0 \pmod{n}$ and $a^{n-1} \not\equiv 1 \mod n$, then we know n is not prime.

Defn: We say a witnesses nonprimality of n.

Example: $n = 91$

$$2^{90} = \left(2^{10}\right)^9$$

$$= (1024)^9$$

$$\equiv (23)^9 \pmod{91}$$

$$\equiv 64 \pmod{91}$$

(I used a Calculator!)

$$3^{90} \equiv ? \pmod{91}$$

Pingala's algorithm

$$3^{666} \bmod 667$$

Idea is to keep track of exponents!

666

Half

333

-1

332

166

83

82

41

40

20

10

660

$(285)3 = 188$

285

187

$13(3) = 39$

13

$(393)(3) = 512$

393

547

$(243)(243) = 353$

5	243
4	81
2	9
1	3

This test doesn't always work!

Defn: (CARMICHAEL NUMBER)

A composite number n which satisfies

$$GCD(a, n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$$

Ex: 41041 is a Carmichael number.

41041 Divisible by 11

$41041 = 11 \times 3731$

$= 11 \times 7 \times 533$

$$= 11 \times 7 \times 13 \times 41$$

$$(a, 41041) = 1 \iff (a, 7) = (a, 11) = (a, 13) = (a, 41) = 1.$$

$$a^{6} \equiv 1 \pmod{7} \Rightarrow a^{41040} \equiv 1 \pmod{7}$$

$$a^{10} \equiv 1 \pmod{11} \Rightarrow a^{41040} \equiv 1 \pmod{11}$$

$$a^{12} \equiv 1 \pmod{13} \Rightarrow a^{41040} \equiv 1 \pmod{13}$$

$$a^{40} \equiv 1 \pmod{41} \Rightarrow a^{41040} \equiv 1 \pmod{41}$$

So, $\boxed{a^{41040} \equiv 1 \pmod{41}}$

—

Every prime factor p of n satisfies $p-1 \mid n-1$.

—

So we need another test!

Let p be a prime number. Then

$$x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}$$

$(\Leftarrow:)$ If $x \equiv \pm 1 \pmod{p}$
then $x^2 \equiv 1 \pmod{p}$

$(\Rightarrow:)$ If $x^2 \equiv 1 \pmod{p} \Rightarrow (x^2-1) \equiv 0 \pmod{p}$

$\Rightarrow (x-1)(x+1) \equiv 0 \pmod{p}$

$\Rightarrow x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

$$27182^2 \equiv 1 \pmod{41041}$$

27182 $\downarrow$ not ± 1

So 41041 is not prime.

(Miller Rabin primality test)

For $N < 25326001$ and N composite either 2, 3 or 5 will work.

Primitive roots

Given n and a such that $GCD(a,n) = 1$

We say a is primitive root if multiplication by a mod n yields a single cycle of length $\phi(n)$.

Thm: If n is prime, then there exists a primitive root.

Pf: next time!