69

Euler's Theorem: If $n > 1$, $\gcd(a, n) = 1$, then

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

Corollary: If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

Primality Test: A primality test is a test to determine whether or not a given number is prime.

1. **Direct Method:** check each integer from 2 to $\sqrt{n}$ to see whether any is a factor of n.

e.g check whether 100 is prime or not

$\sqrt{100} = 10$

From 2 to 10, check that 2, 5, 10 are divisors or factors of $n = 100$.

71

Fermat's Primality Test:

If $a^n \not\equiv a \pmod{n}$ holds for some choice of a then n is necessarily Composite.

Is $n = 117$ prime?

Take $a = 2$

$$2^7 = 128 \equiv 11 \pmod{117}$$

$$2^{117} = 2^{7\cdot 16+5} \equiv 11^{16}\cdot 2^5 \pmod{117}$$

$$11^2 \equiv 4 \pmod{117}$$

$$11^{16} \equiv 4^8 \equiv 2^{16} \pmod{117}$$

$$2^{117} \equiv 2^{21} \pmod{117} = (2^7)^3 \pmod{117}.$$

$$\equiv 11^3 \equiv 44 \pmod{117}$$

$$\not\equiv 2 \pmod{117}$$

$\Rightarrow$ 117 is not a prime.

Note: If n is a prime, then for any a, we have

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

If n is not prime, $n = 561$

$$561 = 3 \times 11 \times 17$$

By the chinese remainder Theorem

$$a^{560} \equiv 1 \pmod{561} \qquad (a,n) = 1$$

$$a^{561} \equiv a \pmod{561}$$

But if $a^{n-1} \not\equiv 1 \pmod{n}$

then n is certainly not prime.

13

Rabin – Miller Primality Test

Let p be an odd prime and $p-1 = 2^h m$ with m odd and $h \geq 1$. Then any integer a $(1 < a < p-1)$ satisfies $a^m \equiv 1 \pmod{p}$ or $a^{2^j \cdot m} \equiv -1 \pmod{p}$; $j = 1, 2, \ldots, h-1$.

<u>Proof</u>: Assume that a has order k modulo p.

$\Rightarrow \quad k \mid p-1 = 2^h m$

(if $o(a) = k$ & $a^t \equiv 1 \pmod{p}$ then $k \mid t$)

If k is odd, then By Euclid's Lemma

$k \mid m \Rightarrow m = kr$ for some $r \in \mathbb{Z}$.

(14)

$$\therefore \quad a^m = (a^k)^r \equiv 1^r \equiv 1 \pmod{p}$$

If k is even:

$$k = 2^{j+1} \cdot d \quad ; \quad j \geq 0, \ d \text{ is odd integer.}$$

Now $2^{j+1} \cdot d \mid 2^h \cdot m$

$$\Rightarrow \quad j+1 \leq h \quad \text{and} \quad d \mid m$$

Also, $a^k \equiv 1 \pmod{p}$

$$\Rightarrow \quad a^{2^{j+1} \cdot d} \equiv 1 \pmod{p}$$

$$\Rightarrow \quad a^{2^j \cdot d} \equiv \pm 1 \pmod{p}$$

$a^{2^j \cdot d} \equiv 1 \pmod{p}$ is not possible

as $o(a) = k$

$$\therefore \quad a^{2^j \cdot d} \equiv -1 \pmod{p}$$

75

Now $m = dt$, t is odd integer.

$$\Rightarrow a^{2^j \cdot m} = a^{2^j \cdot d \cdot t} = \left(a^{2^j d}\right)^t$$

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

Hence the result.

<u>Exc:</u> Test $n = 2201$ for Compositeness.

$n - 1 = 2^3 \cdot 275$

$m = 275$

$a = 2$

$2^1 \equiv 2 \pmod{2201}$

$2^2 \equiv 4 \pmod{2201}$

$2^4 \equiv 16 \pmod{2201}$

$2^8 \equiv 256 \pmod{2201}$

76

$$2^{16} \equiv 1707 \pmod{2201}$$

$$2^{32} \equiv 1926 \pmod{2201}$$

$$2^{64} \equiv 791 \pmod{2201}$$

$$2^{128} \equiv 597 \pmod{2201}$$

$$2^{256} \equiv 2048 \pmod{2201}$$

$$2^{275} = 2^{256+16+2+1}$$

$$= 2^{256} \cdot 2^{16} \cdot 2^{2} \cdot 2^{1}$$

$$\equiv 2048 \cdot 1707 \cdot 8 \pmod{2201}$$

$$\equiv 1582 \pmod{2201}$$

Hence 2201 fails the Rabin–Miller Primality Test for $a=2$. Thus 2201 is Composite.