19 April 2024

Fermat's Little Theorem

If integer n is prime, then for any integer a,

$$a^n \equiv a \pmod{n}.$$

a^n and a have the same remainder mod n.

Equivalently, $a^{n-1} \equiv 1 \pmod{n}$.

EXAMPLE: $n = 7$:

$a = 1$: $a^{7-1} = 1^6 = 1$ ✓

$a = 2$: $2^{7-1} = 2^6 = 64 \equiv 1 \pmod{7}$ ✓

$a = 3$: $3^{7-1} = 3^6 = 729 \equiv 1 \pmod{7}$ ✓

Fermat's Little Theorem Primality Test (FLTPT)

Suppose we want to determine whether a big integer n is prime.

Choose some integer a between 1 and n.

Compute $b = a^{n-1} \pmod{n}$.

If $b \neq 1$, then n is definitely composite.

If $b = 1$, then n might be prime.

Repeat several times using different values of a.

$$\log_{10}(a^b) = b \cdot \log_{10} a$$

EXAMPLE: $3^{32} \pmod 7$ (n=7)

$3^2 = 9$

$3^4 = (3^2)^2 = 81$

$3^8 = (3^4)^2 = 6561$

$3^{16} = (3^8)^2 = 43,046,721$

$3^{32} = (3^{16})^2 = 1,853,020,188,851,841$

$\equiv 2 \pmod 7$

$3^2 = 9 \equiv 2 \pmod 7$

$3^4 = 2^2 = 4 \pmod 7$

$3^8 = 4^2 = 16 \equiv 2 \pmod 7$

$3^{16} = 2^2 = 4 \pmod 7$

$3^{32} = 4^2 = 16 \equiv 2 \pmod 7$