FERMAT'S LITTLE THEOREM

If n is prime, then for any integer a,

$$\underbrace{a^n \equiv a \pmod{n}}_{}$$

a^n and a have same remainder mod n

EXAMLE: $n = 7$:

$$1^7 \equiv 1 \pmod{7}$$
$$2^7 = 128 \equiv 2 \pmod{7}$$
$$3^7 = 2187 \equiv 3 \pmod{7}$$

Equivalently, $a^{n-1} \equiv 1 \pmod{n}$ if n is prime and a is not a multiple of n.

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

IDEA:

Choose some integer a between 1 and n.

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

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

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

Repeat several times using different values of a.

MODULAR EXPONENTIATION BY REPEATED SQUARING

EXAMPLE:

$3^{32} = ?$

$3^2 = 9$

$3^4 = (3^2)^2 = \boxed{81}$

$3^8 = (3^4)^2 = 81^2 = 6561$

$3^{16} = (3^8)^2 = 6561^2 = 43,046,721$

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

$\equiv 2 \pmod 7$

$3^{32} \pmod 7$

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

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

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

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

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