$4^6 \equiv ? \mod 7$

$4^6 = (4^2)^3 \equiv 2^3 \equiv 1$

Now calculate

$38^{75} \equiv ? \mod 103$

$38^{75} \equiv 38^{(1+2+2^3+2^6)}$

$\equiv (38)(38^2)(38^2)^4(38^2)^{32} \mod 103$

$\equiv (38)(2)(2)^4(2)^{32} \mod 103$

$\equiv$ etc.

$\vdots$

$\equiv 46 \mod 103$

Euler's Result

If a, m are integers with $\text{hcf}(a,m) = 1$ then

$$a^{\phi(m)} \equiv 1 \mod m$$

Example $a = 4$ $m = 9$ $\phi(m) =$

$$4^{6} \equiv 1 \mod 9$$

Example

Compute $2^{1000000} \mod 77$

$$\phi(77) = \phi(7.11) = \phi(7)\phi(11)$$

$$= 6.10 = 60$$

$$1000000 = 60.16666 + 40$$

$$2^{1000000} = 2^{\phi(77).16666 + 40}$$

$$\equiv \left(2^{\phi(771)}\right)^{16666} \; 2^{40}$$

$$\equiv 2^{40} \equiv \text{etc.}$$

A special case of Euler's result is:

Fermat's Little Theorem

For a prime p and integer a not divisible by p we have

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

Proof of Fermat's Little Theorem

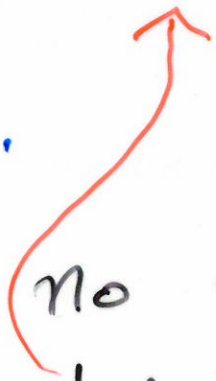
Let a, p be as in the theorem.

Consider

$1.a, 2.a, 3.a, \ldots, (p-1).a$

mod p.

Claim: no two numbers in this list are the same mod p.



Proof of claim

Suppose two numbers in the list, say $i.a$ and $j.a$, were the same.

Then

$$i.a \equiv j.a \mod p$$

or

$$i.a - j.a \equiv 0 \mod p.$$

i.e.

$$(i-j).a \equiv 0 \mod p.$$

Thus p must divide $(i-j).a$

since p does not divide a

we must have that

p divides $i-j$.

Hence $i-j \equiv 0 \mod p$,

or $i \equiv j \mod p$.

This proves the claim.

Now

$$(1.a)(2.a)(3.a)\cdots((p-1).a)$$

$$= 1.2.3.\cdots.(p-1).a^{p-1}$$

$$\equiv 1.2.3.\cdots(p-1) \mod p. \text{ by the claim}$$

So

$$1.2.\cdots(p-1).a^{p-1} \equiv 1.2.\cdots.(p-1) \pmod{p}.$$

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

QED