Homework deadline: Fri 4th October

$4^6 \equiv ? \mod 7$

$4^6 \equiv (4^2)^3 \equiv (2)^3 \equiv 1 \mod 7$

Let's try:

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

Let's try

$38^{75} \equiv 38^{(64+8+2+1)}$

$\equiv 38\,(38^2)(38^8)(38^{64}) \mod 103$

$\equiv 38\,(2)(2^4)(38^{64})$

$\equiv 38.2.16.16^8$

$\equiv \ldots$

$\equiv 38.2.16.63 \mod 103$

$\equiv 79$

Euler's result

If a, m are integers with $\gcd(a, m) = 1$, then

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

Example $a = 4$, $m = 9$.

$$\phi(9) = 6$$

$$4^6 \equiv (4^2)^3 \equiv 7^3 \equiv (-2)^3 \equiv 1 \mod 9$$

Remark Suppose $d \equiv e^{-1} \mod \phi(n)$ with $n = pq$, p, q distinct primes.

$$(a^e)^d = a^{ed} = a^{1 + k\phi(n)}$$

assume $\gcd(a, n) = 1$

$$= a\left(a^{\phi(n)}\right)^k$$

$$\equiv a\, 1^k \mod n$$

$$\equiv a \mod n.$$

Example Calculate

$$2^{1000000} \mod 77$$

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

$$= 6 \cdot 10 = 60$$

$$2^{1000000} \equiv (2^{60})^{16666} \, 2^{40} \mod 77$$

$$\equiv 1^{16666} \, 2^{40} \mod 77$$

$$\equiv 2^{40} \mod 77$$

$$\vdots$$

$$\equiv 23 \mod 77$$

Special case of Euler's result:

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 two numbers as in the theorem.

Consider

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

CLAIM: no two numbers in the green list are the same mod p.

Proof of claim

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

Then

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

Then

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

and

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

So $(i-j)a$ is divisible by p.

Since a is not divisible by p we must have

$(i-j)$ is divisible by p.

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

or $i \equiv j \mod p$.

This proves the claim. $=$

Now

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

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

$$\equiv 1.2.3.\cdots(p-1) \mod p$$

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

QED $=$