- aisling.mccluskey@nuigalway.ie
- 1st homework: 29 Sept.
- 30 Sept.: deadline for Maths studies

$4^6 \equiv ?$ mod 7

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

Now

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

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

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

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

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

$\equiv 38.2.16.63$ mod 103

$\equiv 79$ mod 103

Euler's Result

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

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

Example $a = 4$, $m = 9$, $\gcd(4, 9) = 1$

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

$\phi(9) = 6$

Example Assuming Euler's result, let's calculate

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

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

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

$$= 6 \cdot 10$$

$$= 60.$$

$$2^{1000000} = \left(2^{60}\right)^{16666} 2^{40} \pmod{77}$$

because $1000000 = 60 \cdot 16666 + 40$

$$\equiv 1^{16666} \cdot 2^{40}$$

$$\equiv 2^{40}$$

$$\vdots$$

$$\equiv 23 \pmod{77}$$

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 two numbers 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 claim

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

Then

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

thus

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

and

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

so $(i-j).a$ is divisible by p. Since p does not divide a, we must have that p divides $i-j$. i.e.

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

this proves the claim.

Now

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

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

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

by our claim.

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

QED