

Attendance

MA180 - 4064

MA185 - 9353

MA190 - 7549

$$4^6 \equiv ? \pmod{7}$$

$$4^6 = (4^2)^3 \equiv 1^3 \equiv 1 \pmod{7}$$

Now calculate

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

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

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

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

$$\equiv (38)(2)(16)(63) \pmod{103}$$

$$\equiv 79 \pmod{103}$$

Euler's Result

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

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

Example $a = 4, m = 9, \phi(9) = 6$

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

Example

Compute $2^{1000000} \pmod{77}$

$$\begin{aligned}\phi(77) &= \phi(7 \cdot 11) = \phi(7) \phi(11) \\ &= 6 \cdot 10 = 60\end{aligned}$$

$$1000000 = 60 \cdot 16666 + 40$$

$$2^{1000000} = (2^{60})^{16666} \cdot 2^{40}$$

$$\begin{aligned}
 2^{10000000} &\equiv (2^{\phi(77)})^{16666} \cdot 2^{40} \\
 &\equiv 2^{40} \\
 &\equiv 23 \pmod{77}
 \end{aligned}$$

A special case of Euler's result

Fermat's Little Theorem

For a prime p and integer a not divisible by p

we have

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

Proof of Fermat's Little Theorem

Let a, p be as in the theorem.

Consider

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

$\text{mod } p$

CLAIM: no two numbers in this list are the same $\text{mod } p$.

Proof of claim

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

Then

$$i.a \equiv j.a \pmod{p}$$

$$i.a - j.a \equiv 0 \pmod{p}$$

and

$$(i-j).a \equiv 0 \pmod{p}.$$

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

Since p does not divide a

then p must divide $i-j$.

Hence

$$i-j \equiv 0 \pmod{p}$$

$$\text{or } i \equiv j \pmod{p}.$$

This proves the claim.

Now

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

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

$$\equiv 1.2.3. \dots (p-1) \pmod{p}, \text{ by our claim.}$$

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

$$Q \subseteq D$$