Lecture 7

$$4^6 \equiv 1 \mod 7$$

Now calculate

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

$$38^{(1+2+2^3+2^6)} = (38)(38^2)(38^2)^4(38^2)^3$$

$$\equiv (38)(2)(2^4)(2^3) \mod 103$$

$$\equiv (38)(50)$$

$$\equiv (19)(2 \cdot 50) \equiv (19)(100)$$

$$\equiv (19)(-3) \equiv -57$$

$$\equiv 46 \mod 103$$

Euler's Result

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

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

Example $a = 4,\ m = 9$

$$4^{\phi(9)} \equiv ? \mod 9$$

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

Example

Compute $2^{1000000} \mod 77$

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

$$= 6 \cdot 10 = 60$$

$$1000000 = (60)(16666) + 40$$

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

$$= \left(2^{\phi(77)}\right)^{16666} \left(2^{40}\right) \equiv 2^{40}$$

$$\equiv \text{etc.}$$

these two lists of numbers are not the same. Then for some i and j we would have

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

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

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

Thus p must divide $(i-j)a$. Since p does not divide a we have p divides $i-j$. Then $i \equiv j \mod p$. This yields the claim.)

Using the claim we get

$$1.a.2.a.3.a.\cdots(p-1).a \equiv 1.2.3.\cdots.(p-1) \mod p$$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Therefore

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

QED.