MA 190

$4^6 \equiv$ mod 7

$4^6 = (4^2)^3 \equiv (2)^3 \bmod 7 = 8 \bmod 7 = 1 \bmod 7$

Let's try

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

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

↳ powers of 2

$a^{x+y} = a^x \cdot a^y$

$38^{(64+8+2+1)} \equiv 38 \cdot 38^2 \cdot 38^8 \cdot 38^{64} \bmod 103$

$38^2 = 2 \bmod 102$

$38 \cdot 2 \cdot (2)^4 \cdot 38^{64}$

$38 \cdot 2 \cdot 16 \cdot 2^8$

$38 \cdot 2 \cdot 16 \cdot 50 \equiv 79 \bmod 103$

**THEOREM**

by EULER

Two integers which are coprime $(a, m)$, then $a^{\varphi(m)} \equiv 1 \bmod m$

Example:

$a = 4$

$m = 9$

$\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 6$

$4^6 \equiv (4^2)^3 \equiv 7^3 \bmod 9 \equiv -2^3 \bmod 9 \equiv -8 \bmod 9 \equiv [1 \bmod 9]$

Remark: Suppose you had integers $e, d$. Suppose $d \equiv e^{-1} \bmod n$. Will $n = pq$, $p, q$ distinct primes

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

$a \cdot a^{k\varphi(n)} \bmod n$

$a \cdot (a^{\varphi(n)})^k \bmod n$ ... assume $a$ & $n$ are coprime.

$a \cdot (1)^k \bmod n$ → Euler's theorem

$\equiv a \bmod n$

Example

$2^{1,000,000} \equiv ? \bmod 77$

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

$= 6 \cdot 10 = 60$

$2^{1,000,000} \equiv (2^{60})^{16666} \cdot 2^{40} \bmod 77$

$\equiv 1 \cdot 2^{40} \bmod 77$

$\equiv 23 \bmod 77.$

MA 190 PROVING A SPECIAL CASE OF THIS THEOREM

(note: see blackboard for typed up proof)

## Fermat's little theorem

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

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

Fermat's last theorem (vaguely)

Proof:

Let $a$ and $p$ be two integers, as in the theorem.

Consider the following numbers:

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

↳ Claim:

No two numbers in this list are the same mod $p$.

Proof Of Claim

Suppose that two numbers in the list are the same, mod $p$.

↳ and $i \neq j$ are not equal.

↳ $i \cdot a$, $j \cdot a$

Then

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

$$\therefore i \cdot a - j \cdot a \equiv 0 \mod p$$

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

$\therefore (i-j)a$ is divisible by $p$

HOWEVER,

since $a$ is not divisible by $p$, $(i-j)$ must be

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

$i \equiv j \mod p$ → we just supposed that $ia$ and $ja$ were the same.

This proves the claim

Now:

$$(1a)(2a)(3a)\ldots(p-1)(a) = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p-1 \cdot a^{(p-1)}$$

$$\equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \mod p$$

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

QED