

Ma 100

$$4^6 \equiv \text{mod } 7$$

$$4^6 \equiv (4^2)^3 \equiv (2)^3 \text{ mod } 7 \equiv 8 \text{ mod } 7 \equiv 1 \text{ mod } 7$$

Let's try

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

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

↳ powers of 2

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

$$38^{(64+8+2+1)} \equiv 38^6 \cdot 38^8 \cdot 38^2 \cdot 38^1 \text{ mod } 103$$

$$38^2 \equiv 2 \text{ mod } 103$$

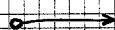
$$38^4 \equiv 2 \cdot (2)^2 \cdot 38^6$$

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

$$38^8 \cdot 2 \cdot 16 \cdot 50 \equiv 77 \text{ mod } 103$$

THEOREM

↳ EULER



Two integers which are coprime (a, m) , then $a^{\phi(m)} \equiv 1 \text{ mod } m$

Example:

$$a=4 \\ m=9$$

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

$$4^6 \equiv (4^2)^3 \equiv 7^3 \text{ mod } 9 \equiv -1^3 \text{ mod } 9 \equiv -8 \text{ mod } 9 \equiv 1 \text{ mod } 9$$

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

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

$$a = a^{k\phi(n)} \text{ mod } n$$

$$a = (a^{\phi(n)})^k \text{ mod } n$$

... assume $a \nmid n$ are coprime.

$$a \cdot (1)^k \text{ mod } n$$

$$\equiv a \text{ mod } n$$

↳ Euler's Theorem

Example

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

$$\phi(77) = \phi(7 \cdot 11) = \phi(7) \phi(11) \\ = 6 \cdot 10 = 60$$

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

$$\equiv 1 \cdot 2^{40} \text{ mod } 77$$

$$\equiv 23 \text{ mod } 77$$

Fermat's little theoremFor a prime p and integer a not divisible by p , we have

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

Proof:

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

Consider the following numbers:

$$1 \cdot a, 2 \cdot a, 3 \cdot a, \dots, (p-1) \cdot a \pmod{p}$$

↳ Claim:

No two numbers in this list are the same mod p .Proof of ClaimSuppose that two numbers in the list are the same, mod p .

$$\hookrightarrow i \cdot a, j \cdot a$$

↳ and $i \neq j$ are not equal.

Then

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

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

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

$$\therefore (i-j) \cdot a \text{ is divisible by } p$$

However,

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

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

$$i \equiv j \pmod{p} \rightarrow \text{We just supposed that } i \cdot a \text{ and } j \cdot a \text{ were the same.}$$

This proves the claim

Now:

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

$$\equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$

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

QED

(note: see blackboard for typed up proof)

Fermat's little theorem (Google)