Fermat Little Theorem

Monday, April 13, 2026 11:24 AM

Recall: Divisibility

Missing
700# 4, 9, 14, 17, 28,
800# 11
Ex #825 on 4/8

1) Divisibility by 7

$1234568 = 1\times10^6 + 2\times10^5 + 3\times10^4 + 4\times10^3 + 5\times10^2 + 6\times10^1 + 8$

$\equiv -1 + 2 - 3 + 1 - 2 - 3 - 1 + 2 + 3 + 1 \pmod 7$

$\equiv 6 \pmod 7$

1234234

e.g. $1234234 \pmod 7$

$\equiv 1$

e.g. $65713 \pmod 7$

$\equiv 6 \pmod 7$

exer: $1234235 \equiv 15 \equiv 1 \pmod 7$

exer $1000000 \equiv 1$

$100000000 \equiv 2$

2) Fermat Little Theorem

if p is prime, $\forall a \in \mathbb{Z}$ co-prime to p $(p \nmid a)$

then

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

In general $a^{p} \equiv a \pmod{p}$

3] e.g. ① $2^{10} \pmod{11}$

$\equiv 1024$ (- + - +)

$\equiv 1 \pmod{11}$

e.g. ② $18^{6} \pmod{7}$

$\equiv 1$ by FLT

e.g ③ $3700^{26} \pmod{11}$

$\equiv 4^{26} \equiv (4^{10})^{2} \cdot 4^{6}$ $= (2^{2})^{6} = 2^{12} = 2^{11} \cdot 2^{2} = 4$

$\equiv 1^{2} \cdot 4^{6}$ by FLT

$\equiv (2^{2})^{6}$

$\equiv 2^{12} \equiv 2^{10} \cdot 2^{2}$

$\equiv 1 \cdot 4$ by FLT

e.g $35^{124} \pmod{11}$

mod 11 (mod 10)

$\equiv 2^{4}$

$\equiv 16 \equiv 5 \pmod{11}$

4] Note

$$a^{e} \pmod p \quad \text{// for prime } p$$

mod p / mod (p-1)

$$\equiv x^{y} \pmod p$$

5] exer: ①

$$1234^{172} \pmod{11}$$

$$2^{2} \equiv 4$$

exer. ②

$$16^{50} \pmod 7$$

$$\equiv 2^{2} \equiv 4 \pmod 7$$

6] Pseudoprimes

Def^{n}. Let b be a positive integer, and n is a composite, then if $b^{n-1} \equiv 1 \pmod n$, then n is calle a psendoprime to the base b.

e.g. $n = 341 = 11 \times 31$

but $2^{340} \equiv 1 \pmod{341}$

it is pseudoprime to base 2.

7] Primality Test

To check if n is prime

① choose a base b ; s.t. $\gcd(b,n) = 1$

if $\gcd \neq 1 \Rightarrow n$ is not prime

② if $b^{n-1} \not\equiv 1 \pmod n$

return "Not prime"

else // Pseudoprime base b

goto ① // find another base

e.g. Is 1003 prime?

$2^{1002} \equiv 990 \pmod{1003}$

$\not\equiv 1 \Rightarrow$ not prime

e.g Is 341 prime?

base 2: $2^{340} \equiv 1 \pmod{341} \Rightarrow$ pseudoprime

base 7: $7^{340} \equiv 56 \not\equiv 1 \Rightarrow$ Not prime

8] Carmichael Numbers

if n is composite and pseudoprime to all possible bases then n is called a Carmichael number.

e.g. $561 = 3 \cdot 11 \cdot 17$ is a Carmicael number

$5^{560} \equiv 1 \pmod{561}$

$7^{560} \equiv 1 \pmod{561}$

e.g. $1105 = 5 \cdot 13 \cdot 17$ is a Carmichael number

$$2^{1104} \equiv 1 \pmod{1105}$$

Exer.

$$3^{2210} \pmod{1105}$$

$$\equiv (3^{1104})^2 \cdot 3^2$$

$$\equiv 1^2 \cdot 9 \pmod{1105}$$

Midterm Review

7 — 30 (out of 28)

Avg : 20 $\approx$ 66% → 71%

Avg. F13 = 72 → 77%

Avg F14 = 72 → 77%

9, 5, 6, 10, 24, 28, 29, 30