Fermat Little Theorem

Wednesday, February 4, 2026 6:52 PM

Recall : Modular Arithmetic

1] Exer : $5678 \pmod{13}$

$$5678 = 5\times10^3 + 6\times10^2 + 7\times10^1 + 8 \pmod{13}$$

$$1 \quad 4 \quad 3 \quad -1 \quad -4 \quad -3 \quad 1$$

$$\equiv -5 + 2 + 5 + 8$$

$$\equiv 10$$

2] Thrm: Fermat Little Theorem

if p is prime, then for all a coprime to p

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

e.g.

① $2^{10} \equiv 1024$

$\equiv 1 \pmod{11}$

② $3^{13} \pmod{11}$

$\equiv 3^{10}\cdot 3^3$

$\equiv 1 \cdot 27$ by FLT

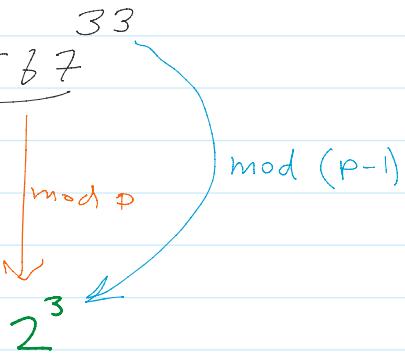
$\equiv 5 \pmod{11}$

③ $2468^{27} \pmod{11}$

$\equiv (4^{10})^2 \cdot 4^7$ 4 Mariam

$\equiv 2^{14} \equiv 2^4 \equiv 16 \equiv 5$

④ 4567^{33} 8



⑤ $9876^{1234} \pmod{11}$

$\equiv (-2)^4 \equiv 16 \equiv 5 \pmod{11}$

⑥ $2378^{2572} \pmod{11}$

$\equiv 2^2 \equiv 4$

⑦ $16^{4251} \pmod{7}$

$\equiv 2^3 \equiv 8 \equiv 1$

⑧ $2^{41} \pmod{7}$

$\equiv 2^{-1} \pmod{7}$

$\equiv 4 \pmod{7}$

Zeros

6
12
18
24
30
36
41 42 43
48

3] Enigma

Key space size $|K|$

① 3 rotors (no plugs): 26^3 keys

② 3 different rotors (no plugs): $3! \cdot 26^3$

③ 3 rotors with one cable (plug pair) $\binom{26}{2} \cdot 26^3$

$= \frac{26 \cdot 25}{2} \cdot 26^3$

④ with 3 out of 5 different rotors, 2 cables

$\binom{5}{3} \cdot \frac{\binom{26}{2}\binom{24}{2}}{2} \cdot 3! \cdot 26^3$

4] Playfair

Key length $= 25$

Key space size $|K| = 25!$

5] Hill cipher of $n \times n$ key matrix

Key length n^2

$|K| \leq 26^{n \times n}$