# Fermat's Little Theorem (1)

- Fermat discovered many beautiful results on prime numbers.
- **Fermat's Little Thm** is one of them.
- It is simple, but very useful.
  It has applications to Number Theory and Cryptography.

Pierre de Fermat (1607?-1665)

# Fermat's Little Theorem (2)

**Fermat's Little Theorem**

For any **prime number** P and any $1 \le A \le P-1$,

$$A^{P-1} \equiv 1 \pmod{P}.$$

**Examples:**

- $(P = 5, A = 2)$

  $2^4 \equiv 16 \equiv 1 \pmod{5}.$

- $(P = 11, A = 3)$

  $3^{10} \equiv 59049 \equiv 1 \pmod{11}.$

Pierre de Fermat (1607?-1665)

# Fermat's Little Theorem (3)

**Proof of Fermat's Little Thm:**

$$A \times B \pmod{P} \quad \text{for} \quad B = 1, 2, \cdots, P-1$$

are **not congruent** (mod P) to each other. Hence

$$A \times (A \times 2) \times \cdots \times (A \times (P-1))$$

$$\equiv 1 \times 2 \times \cdots \times (P-1)$$

$$\Rightarrow \quad A^{P-1} \times (P-1)! \equiv (P-1)!$$

$$((P-1)! = 1 \times 2 \times \cdots \times (P-1))$$

$$\Rightarrow \quad (A^{P-1} - 1) \times (P-1)! \equiv 0$$

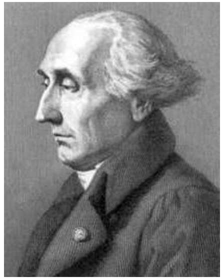
$$\Rightarrow \quad A^{P-1} \equiv 1.$$

# Fermat's Little Theorem (4)

- In the proof of Fermat's Little Thm,

  $$\mathbf{(P-1)!} = 1 \times 2 \times \cdots \times (P-1)$$

  plays an important role.
- We can calculate it (mod P) by **Wilson's Thm.**
- We shall prove Wilson's Thm using **Lagrange's Thm** on roots of polynomials (mod P).



Joseph-Louis Lagrange (1736-1813)

https://en.wikipedia.org/wiki/Joseph-Louis_Lagrange

# Fermat's Little Theorem (5)

**Wilson's Theorem**: for a **prime number** P,

$$(P-1)! \equiv -1 \pmod{P}$$

**Examples**:

- (P=2) $1! \equiv 1 \equiv -1 \pmod{2}$
- (P=3) $2! \equiv 1 \times 2 \equiv 2 \equiv -1 \pmod{3}$
- (P=7) $6! \equiv 1 \times 2 \times 3 \times 4 \times 5 \times 6$
  $\equiv 720 \equiv -1 \pmod{7}$

# Fermat's Little Theorem (6)

## Lagrange's Theorem

$F(X) = X^D + C_1X^{D-1} + \cdots + C_{D-1}X + C_D$

- If $F(A) \equiv 0 \pmod{P}$,

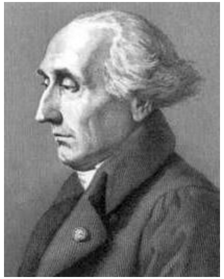
  $$\mathbf{F(X) \equiv (X-A)G(X)}$$

  for some $G(X)$.

- If $0 \le A_1 < \cdots < A_K \le P-1$ and $F(A_J) \equiv 0 \pmod{P}$,

  $$\mathbf{F(X) \equiv (X-A_1)\cdots(X-A_K)H(X)}$$

  for some $H(X)$. ($\Rightarrow$ **$K \le D$**)



Joseph-Louis Lagrange (1736-1813)

# Fermat's Little Theorem (7)

**Proof of Lagrange's Thm:**

$$F(X) = X^D + C_1X^{D-1} + \cdots + C_{D-1}X + C_D$$

$$F(A) = A^D + C_1A^{D-1} + \cdots + C_{D-1}A + C_D$$

$$F(X)-F(A) = (X^D-A^D) + C_1(X^{D-1}-A^{D-1}) + \cdots + C_{D-1}(X - A)$$

$$= (X-A)G(X) \quad \text{for some } G(X).$$

Since $F(A) \equiv 0$,

$$\mathbf{F(X) \equiv (X-A)G(X)}.$$

The second assertion is proved by **induction on K**.

# Fermat's Little Theorem (8)

**Proof of Wilson's Theorem**:

By **Fermat's Little Thm**,

$$A^{P-1} \equiv 1 \quad \text{for } A = 1, 2, \cdots, P-1.$$

By **Lagrange's Thm**,

$$X^{P-1} - 1 \equiv (X-1)(X-2) \cdots (X-(P-1)).$$

Comparing constant terms,

$$-1 \equiv (-1)^{P-1} \times (P-1)! \equiv (P-1)!$$

# Fermat's Little Theorem (9)

- **An application of Lagrange's Thm**

**Theorem**

There are **at most D** elements $1 \le A \le P-1$ satisfying $\mathbf{A^D - 1 \equiv 0 \pmod{P}}$.

$F(X) = X^D - 1$

If $1 \le A \le P-1$ satisfies $A^D - 1 \equiv 0$,

$$F(A) \equiv 0 \pmod{P}.$$

By **Lagrange's Thm**, # of such A is $\le D$.