定理１．(ラグランジュの定理)
有限群 G とその部分群 H に対し，$|G| = [G : H]|H|$ が成り立つ．特に，$|H|$ は $|G|$ の約数である．
(証明)
ラグランジュの定理の定理７を参照．

系２．
x が有限群 G の元ならば，x の位数 $|x|$ は $|G|$ の約数である．
(証明)
$|x|$ は，x が生成する G の部分群 $\langle x\rangle = \{x^m | m \in \mathbb{Z}\}$ の位数に等しい．G が有限だから，定理１より $|x|$ は $|G|$ の約数である．　∎

系３．(系２の言い換え)
x が有限群 G の元ならば，$x^{|G|} = e$ である．
(証明)
系２より，ある非負整数 n が存在して $|G| = n|x|$ となるから，$x^{|G|} = e^n = e$ である．∎

補題４．
任意の素数 p に対し，$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times := \{1, 2, \cdots, p-1\}$ は p を法とする乗法 $\cdot_p$ に関して群をなす．
(証明)
まず，任意の $a, b \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ に対し，演算の定義から $a \cdot_p b$ は $0 \leq a \cdot_p b < p$ を満たす整数である．今，a, b はともに p の倍数でないから，素因数分解の一意性より，積 ab は p の倍数でない．したがって $0 < a \cdot_p b < p$ となるから，$a \cdot_p b \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$，つまり $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ は p を法とする乗法に関して閉じている．

単位元の存在：$1 \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ は任意の $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ に対し，$1 \cdot_p a = a \cdot_p 1 = a$ を満たすので，$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ の単位元である．

結合法則：任意の $a, b, c \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ に対し，$a \cdot_p b \equiv ab,\ b \cdot_p c \equiv bc \pmod p$ なので

$$(a \cdot_p b) \cdot_p c \equiv (ab) \cdot_p c \equiv (ab)c \equiv abc \pmod p$$

$$a \cdot_p (b \cdot_p c) \equiv a \cdot_p (bc) \equiv a(bc) \equiv abc \pmod p$$

より，$(a \cdot_p b) \cdot_p c = a \cdot_p (b \cdot_p c)$ である．

逆元の存在：$a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ を任意の元とする．このとき，次の $p-1$ 個の整数

$$1 \cdot_p a, \quad 2 \cdot_p a, \quad \cdots, \quad (p-1) \cdot_p a \quad (\bigstar)$$

を考える．これらは全て相異なる．実際，整数 i, j が $i \neq j,\ 0 < i < j < p$ であるとし，$i \cdot_p a = j \cdot_p a$ と仮定すると，$ia \equiv ja \pmod{p}$ より $(j-i)a \equiv 0 \pmod{p}$ である．$j-i$ は素数 p の倍数でないから，素因数分解の一意性より，a が p の倍数となるが，これは $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ であることに反する．よって $i \cdot_p a \neq j \cdot_p a$ である．

したがって，$(\bigstar)$ は $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ の $p-1$ 個の整数を全て尽くす．よって，$(\bigstar)$ の中に 1 も含まれるので，それを $i \cdot_p a$ とすれば，$i \cdot_p a = a \cdot_p i = 1$ より，i が a の逆元である． ∎

定理５．(フェルマーの小定理)
p を素数とするとき，整数 a が p と互いに素ならば

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

が成り立つ．
(証明)
a と p が互いに素より，$a \equiv i \pmod{p}$ となる $i \in \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ が存在する．ここで $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ の位数は $p-1$ であり，補題４から $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ は p を法とする乗法に関して群をなすから，系３より

$$\underbrace{i \cdot_p i \cdot_p \cdots \cdot_p i}_{p-1 \text{ 個}} = 1$$

が成り立つ．よって $\cdot_p$ の定義から

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

となる．したがって $a^{p-1} \equiv i^{p-1} \equiv 1 \pmod{p}$ が成り立つ． ∎

(参考文献)
[1] 木村達雄・竹内光弘・宮本雅彦・森田純「代数の魅力」数学書房(2009)
[2] “ラグランジュの定理(群論)”. Wikipedia. 2023-02-02. https://ja.wikipedia.org/wiki/ラグランジュの定理_(群論)