

费马小定理，欧拉定理

Fermat's Little Theorem, Euler's Theorem

费马小定理 Fermat's Little Theorem

Theorem: 若 p 是质数，则：

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

特别地，若 a 不是 p 的倍数，则：

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

Proof: 设 p 为质数， a 不是 p 的倍数（即 $\gcd(a, p) = 1$ ）。取一模 p 的完全剩余系 $A = \{1, 2, \dots, p-1\}$ ，容易证明 $\{aA_i\}$ 也是模 p 的完全剩余系。于是有：

$$\begin{aligned} aA_1 aA_2 \cdots aA_{p-1} &\equiv A_1 A_2 \cdots A_{p-1} \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

证毕。

Application:

- 求解逆元:** 因为当 p 是质数且 a 不是 p 的倍数时， $a^{p-1} \equiv 1 \pmod{p}$ ，所以 $a \cdot a^{p-2} \equiv 1 \pmod{p}$ ，故 a^{p-2} 是 a 在模 p 意义下的逆元。
- 指数取模:** 设 p 为质数，则 $a^b \equiv a^{b \bmod (p-1)} \pmod{p}$ 。

Proof: 设 $b = k(p-1) + r$ ，即 $k = \left\lfloor \frac{b}{p-1} \right\rfloor$ ， $r = b \bmod (p-1)$ ，则

$$a^b \equiv a^{k(p-1)+r} \equiv (a^{p-1})^k \cdot a^r \equiv a^r \equiv a^{b \bmod (p-1)} \pmod{p}.$$

证毕。

欧拉定理 Euler's Theorem

Theorem: 若 $(a, m) = 1$ ，则：

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Proof: 取一模 m 的缩剩余系 $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ ，容易证明 $\{ar_i\}$ 也是模 m 的一个缩剩余系。于是有：

$$\begin{aligned} ar_1 ar_2 \cdots ar_{\varphi(m)} &\equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m} \\ a^{\varphi(m)} &\equiv 1 \pmod{m} \end{aligned}$$

证毕。

Application:

- 求解逆元:** 若 $(a, m) = 1$ ，则 $a^{\varphi(m)-1}$ 是 a 在模 m 意义下的逆元。
- 指数取模:** 设 $(a, m) = 1$ ，则 $a^b \equiv a^{b \bmod \varphi(m)} \pmod{m}$ 。

Proof: 设 $b = k \cdot \varphi(m) + r$ ，即 $k = \left\lfloor \frac{b}{\varphi(m)} \right\rfloor$ ， $r = b \bmod \varphi(m)$ ，则

$$a^b \equiv a^{k \cdot \varphi(m) + r} \equiv (a^{\varphi(m)})^k \cdot a^r \equiv a^r \equiv a^{b \bmod \varphi(m)} \pmod{m}.$$

证毕。

扩展欧拉定理

Theorem: $a^b \equiv \begin{cases} a^{b \bmod \varphi(m)} & \gcd(a, m) = 1 \\ a^b & \gcd(a, m) \neq 1, b < \varphi(m) \\ a^{(b \bmod \varphi(m)) + \varphi(m)} & \gcd(a, m) \neq 1, b \geq \varphi(m) \end{cases} \pmod{m}.$

Proof: 暂略。

Application:

- 指数取模。