1. 证明以下费马定理及推论:

定理 1 (费马定理) 若 p 是素数,a 是正整数且不能被 p 整除,则有

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

推论 1 若 p 是素数且 a 是任意正整数,则 $a^p \equiv a \pmod p$。

2. 证明以下欧拉定理及推论:

定理 2 (欧拉定理) 对于任意互素的正整数 a 和 n,有 $a^{\phi(n)} \equiv 1 \pmod n$。

推论 2 若 n 是素数,则对任意正整数 a,有 $a^{\phi(n)+1} \equiv a \pmod n$。

3. 证明欧拉函数满足以下性质:

性质 1 若正整数 n 的素因子分解为 $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$,则

$$\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1)$$

4. 利用 Miller-Rabin 素性测试验证 13 为素数。

2025 年 3 月 19 日