

验证是否原根

小圆滚滚

要验证一个整数 a 是否是模 n 的原根，我们需要检查两个条件：

1. **互素条件**： a 和 n 必须互素，即 $\gcd(a, n) = 1$ 。
2. **阶数条件**： a 在模 n 下的阶数必须等于 $\varphi(n)$ ，这里 φ 是欧拉函数。

具体步骤如下：

1 步骤一：检查互素条件

首先计算 $\gcd(a, n)$ 。如果结果不为 1，那么 a 不可能是模 n 的原根。

2 步骤二：计算欧拉函数 $\varphi(n)$

计算 $\varphi(n)$ 。例如：- 如果 n 是素数 p ，那么 $\varphi(p) = p - 1$ 。

- 如果 n 是 p^k 的形式，那么 $\varphi(p^k) = p^k - p^{k-1}$ 。

- 如果 n 是多个素数的乘积，比如 $n = p \cdot q$ ，那么 $\varphi(n) = (p - 1)(q - 1)$ 。

3 步骤三：检查阶数条件

我们需要验证 a 的阶数是否为 $\varphi(n)$ 。具体来说，我们需要检查：- 对于所有能整除 $\varphi(n)$ 的素因子 p ，都有 $a^{\varphi(n)/p} \not\equiv 1 \pmod{n}$ 。

换句话说，我们需要确保 a 的阶数不是 $\varphi(n)$ 的任何真因子。

4 例子：验证 3 是否是模 7 的原根

1. **互素条件**： $\gcd(3, 7) = 1$ ，满足。

2. **欧拉函数**： $\varphi(7) = 6$ （因为 7 是素数）。

3. **阶数条件**：6 的素因子是 2 和 3。

- 检查 $3^{6/2} = 3^3 = 27 \equiv 6 \not\equiv 1 \pmod{7}$ 。

- 检查 $3^{6/3} = 3^2 = 9 \equiv 2 \not\equiv 1 \pmod{7}$ 。

由于以上两个结果都不等于 1，因此 3 是模 7 的原根。

5 总结

验证一个数 a 是否是模 n 的原根的算法可以总结为：

1. 检查 $\gcd(a, n) = 1$ 。

2. 计算 $\varphi(n)$ 并找到其所有不同的素因子。
3. 对于每个素因子 p , 检查 $a^{\varphi(n)/p} \not\equiv 1 \pmod{n}$ 。
4. 如果所有检查都通过, 则 a 是模 n 的原根; 否则, 不是。