

# 二次剩余(QRP)

## Cipolla算法(素数情况下)

[wiki百科](#)

对于  $x^2 \equiv a \pmod{p}$

可以随机找一个数  $s$ ,  $\text{s.t.} (\frac{s^2 - a}{p}) = -1$ , 即  $s$  不是  $p$  的二次剩余, 可以知道找到  $s$  的期望次数为 2

考虑  $\mathbb{Z}(w = \sqrt{s^2 - a}) = \{j + kw\}$  以及如下定理

- 普通列表项目  $w^p = w(w^2)^{\frac{p-1}{2}} = w(s^2 - a)^{\frac{p-1}{2}} \equiv -w \pmod{p}$
- 普通列表项目  $(a+b)^p \equiv a^p + b^p \pmod{p}$

解为  $x \equiv (s+w)^{\frac{p+1}{2}}$ :

$$(s+w)^{p+1} = (s+w)^p (s+w) \equiv (s^p + w^p)(s+w) \equiv (s-w)(s+w) = (s^2 - w^2) \equiv a \pmod{p}$$

## 三次剩余

$x^3 \equiv a \pmod{p}$

如果  $a=0, p \leq 3$  考虑特判

$p=3k+2, x \equiv a^{\frac{2p-1}{3}}$  且为唯一解

若不为唯一解, 则说明其有 3 次单位根  $1, \alpha, \alpha^2$ , 故每种解三个一组, 而  $3 \nmid p-1$  矛盾

$p=3k+1$ , 其有 3 次单位根, 且可能无解

先利用  $a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$  判断有无解

找到  $b^3 \equiv a \pmod{p}$ , 则解为  $b, b\alpha, b\alpha^2$

类比二次剩余 Cipolla 算法, 设  $a$  的根为  $\theta \neq a$

$C = \{j + k\theta + l\theta^2\}$ , 随机生成  $j, k, l$  得到  $y = j + k\theta + l\theta^2$

$z \equiv y^{\frac{p-1}{3}} \pmod{p}, z^3 \equiv 1 \pmod{p}$

Last update: 2020-2021:teams:alchemist:hardict:grp <https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:alchemist:hardict:grp&rev=1589616566>  
2020/05/16 16:09

---

From:  
<https://wiki.cvbbacm.com/> - **CVBB ACM Team**

Permanent link:  
<https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:alchemist:hardict:grp&rev=1589616566> 

Last update: **2020/05/16 16:09**