

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 ,
使得 $s^2 - a \pmod{p} = -1$, 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 $w = \sqrt{s^2 - a} = j + kw$

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

三次剩余

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

Permanent link:
<https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:alchemist:hardict:qrp&rev=1589615386>

Last update: 2020/05/16 15:49

