二次剩余(QRP)

Cipolla算法(素数情况下)

wiki百科

对于 $x^{2} \equiv a \mod p$

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

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

$w\^{p} = w*(w^{2})^{\frac{p-1}{2}}=w*(s^{2}-a)^{\frac{p-1}{2}} \euqiv -w \mod p$

三次剩余