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

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

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

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

# 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$\theta \neq a$

$C=\{y=j+k\theta+l\theta^{2}\}$,$C$与$\mathbb{Z}_{p^{3}}$同构,$y^{p-1}\equiv 1 \pmod{p}$

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

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

若$z$仅含一次项$(k^{'}\theta)^{3} \equiv 1 \pmod{p}$,取$x \equiv (k^{'})^{-1} \pmod{p}$即为一个解