二次剩余(QRP)

Cipolla算法

wiki百科

对于 $x^{2} \equiv a \mod p$

三次剩余