二次剩余

一个数 a 如果不是 p 的倍数且模 p 同余于某个数的平方，则称 a 为模 p 的 **二次剩余**。而一个不是 p 的倍数的数 b 不同余于任何数的平方，则称 b 为模 p 的 **二次非剩余**

对二次剩余求解，也就是对常数 a 解下面的这个方程 $$ x^2\equiv a\pmod p $$ 通俗一些，可以认为是求模意义下的开方。这里只讨论 **p 为奇素数** 的求解方法，将会使用 Cipolla 算法。