

# 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。

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

Permanent link:  
[https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:legal\\_string:lgwza:%E4%BA%8C%E6%AC%A1%E5%89%A9%E4%BD%99&rev=1610887367](https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:legal_string:lgwza:%E4%BA%8C%E6%AC%A1%E5%89%A9%E4%BD%99&rev=1610887367)

Last update: 2021/01/17 20:42

