

二次剩余(QRP)

Cipolla算法

[wiki百科](#)

对于 $x^2 \equiv a \pmod p$

三次剩余

From:

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

Permanent link:

<https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:alchemist:hardict:grp&rev=1589614885> 

Last update: 2020/05/16 15:41