2023-2024 学年 期末考题（回忆版）

By 5U

给出两数 a, b 求解：

最大公因数 (a, b)

最小公倍数 [a, b]

a 关于模 m 逆元

（欧几里得除法）

写出一循环群 <g> 的真子群

/

求解同余方程组

（中国剩余定理）
（注意需要化为首一方程，模 m 需要互质）

求解某奇数的平方剩余

（勒让德符号、雅各比符号）

判断某数的原根存在性并给出所有原根

/

证明 RSA 算法最后一步

（PPT、课上证明并强调过）

证明题：

给出运算，证明构成乘法群

利用互素得出一个推论