BabyDH 1

本题主要考查选手阅读论文能力、编程能力，要求选手对于格归约算法、Coppersmith方法有一定了解。

题目描述

题目中服务端模拟Alice与Bob两方进行了一次DH密钥交换，我们获得了他们的公钥。随后我们可以作为第三方与Alice进行一次DH交换，同时提供了一个额外的Oracle，可以泄露出我们与Alice协商出来的点x坐标和y坐标的低比特位数值。我们需要还原出该点的完整坐标值。

求解思路

根据题目中的信息，我们可以构造多项式

$$f(x,y) = (My + y')^2 - ((Mx + x')^3 + a(Mx + x') + b),$$

其中x', y'是泄露出来的数值，而$M = 2^{211}$。

使用Coppersmith方法求解该多项式的小数根，预期解法是基于Jochemsz和May提出的构造进行调整。但事实上，已经有相关场景下的研究发表，故只需要根据文中构造复现即可解出本题。

注意到本题的限时较短，考虑使用flatter工具完成快速格归约。实测发现设置参数本题中取m = 7，t = 1，在1核的Ubuntu虚拟机上耗时约25s有概率完成求解。