破解D-H协议(crack)

题目描述

Diffie-Hellman密钥交换协议是一种简单有效的密钥交换方法。它可以让通讯双方在没有事先约定密钥（密码）的情况下，通过不安全的信道（可能被窃听）建立一个安全的密钥 K，用于加密之后的通讯内容。

假定通讯双方名为Alice和Bob，协议的工作过程描述如下（其中 mod 表示取模运算）：

1. 协议规定一个固定的质数 P，以及模 P 的一个原根 g。P 和 g 的数值都是公开的，无需保密。
2. Alice 生成一个随机数 a，并计算 $A=g^a \bmod P$，将 A 通过不安全信道发送给 Bob。
3. Bob 生成一个随机数 b，并计算 $B=g^b \bmod P$，将 B 通过不安全信道发送给 Alice。
4. Bob 根据收到的 A 计算出 $K=A^b \bmod P$，而 Alice 根据收到的 B 计算出 $K=B^a \bmod P$。
5. 双方得到了相同的 K，即 $g^{ab} \bmod P$。K 可以用于之后通讯的加密密钥。

可见，这个过程中可能被窃听的只有 A、B，而 a、b、K 是保密的。并且根据 A、B、P、g 这4个数，不能轻易计算出 K，因此 K 可以作为一个安全的密钥。

当然安全是相对的，该协议的安全性取决于数值的大小，通常 a、b、P 都选取数百位以上的大整数以避免被破解。然而如果 Alice 和 Bob 编程时偷懒，为了避免实现大数运算，选择的数值都小于 2^{31}，那么破解他们的密钥就比较容易了。

输入格式

输入文件第一行包含两个空格分开的正整数 g 和 P。
第二行为一个正整数 n，表示 Alice 和 Bob 共进行了 n 次连接（即运行了 n 次协议）。
接下来 n 行，每行包含两个空格分开的正整数 A 和 B，表示某次连接中，被窃听的 A、B 数值。

输出格式

输出包含 n 行，每行1个正整数 K，为每次连接你破解得到的密钥。

输入样例

```
3 31
3
27 16
21 3
9 26
```

输出样例

```
4
21
25
```

数据范围

- 对于30%的数据，$2 \le A,B,P \le 1000$
- 对于100%的数据，$2 \le A,B < P < 2^{31}$，$2 \le g < 20$，$1 \le n \le 20$