NOI 2018 全国青少年信息学奥林匹克竞赛

重庆代表队选拔赛·第一试

试题一览

题目	破解D-H协议	社交网络	交错序列
代号	crack	sns	seq
输入文件	crack.in	sns.in	seq.in
输出文件	crack.out	sns.out	seq.out
测试点数目	10	20	20
单测试点分值	10	5	5
满分分值	100	100	100
时间限制	1秒	1秒	1秒
内存限制	512MB	512MB	512MB

2018年4月7日

注意：可以使用64位整数和C++ STL，但这不一定是解题必须的。

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，$2 \le A,B < P < 2^{31}$，$2 \le g < 20$，$1 \le n \le 20$

社交网络(sns)

题目描述

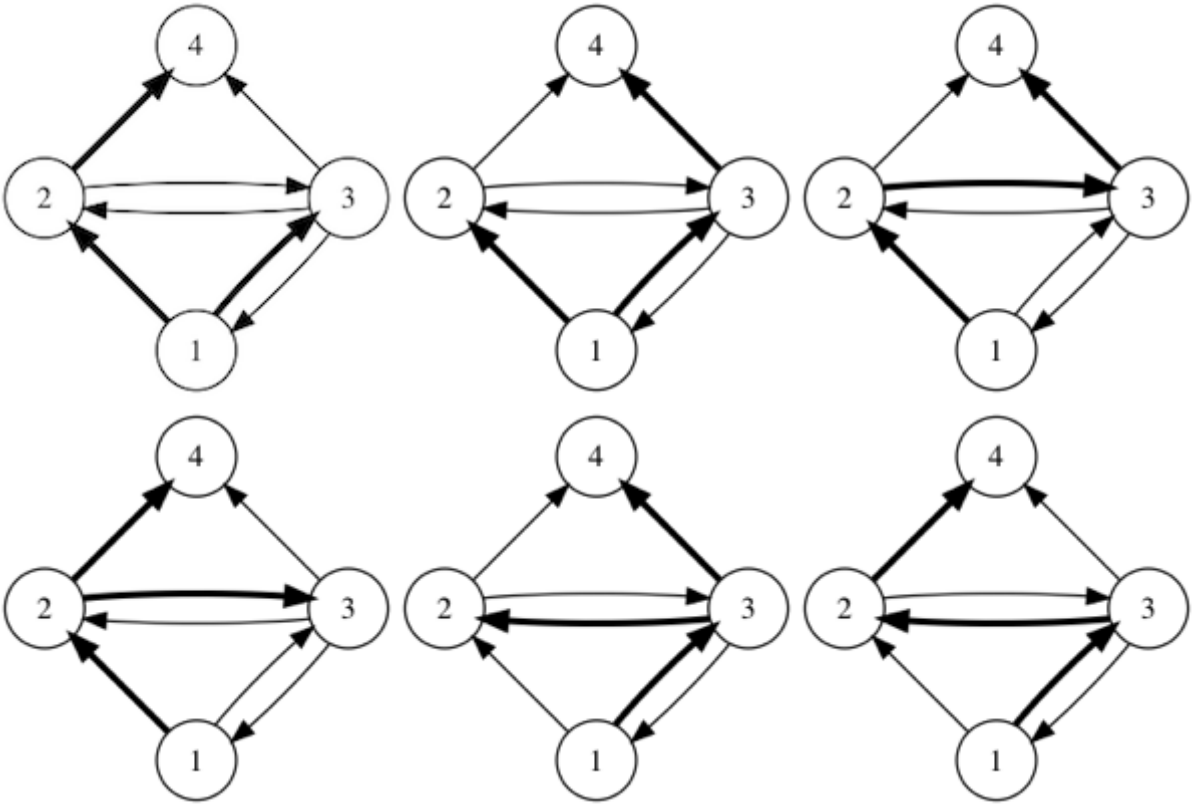
当今社会，在社交网络上看朋友的消息已经成为许多人生活的一部分。通常，一个用户在社交网络上发布一条消息（例如微博、状态、Tweet等）后，他的好友们也可以看见这条消息，并可能转发。转发的消息还可以继续被人转发，进而扩散到整个社交网络中。

在一个实验性的小规模社交网络中我们发现，有时一条热门消息最终会被所有人转发。为了研究这一现象发生的过程，我们希望计算一条消息所有可能的转发途径有多少种。为了编程方便，我们将初始消息发送者编号为 1 ，其他用户编号依次递增。

该社交网络上的所有好友关系是已知的，也就是说对于 A、B 两个用户，我们知道 A 用户可以看到 B 用户发送的消息。注意可能存在单向的好友关系，即 A 能看到 B 的消息，但 B 不能看到 A 的消息。

还有一个假设是，如果某用户看到他的多个好友转发了同一条消息，他只会选择从其中一个转发，最多转发一次消息。从不同好友的转发，被视为不同的情况。

如果用箭头表示好友关系，下图展示了某个社交网络中消息转发的所有可能情况。（初始消息是用户 1 发送的，加粗箭头表示一次消息转发）



输入格式

输入文件第一行，为一个正整数 n ，表示社交网络中的用户数；第二行为一个正整数 m ，表示社交网络中的好友关系数目。

接下来 m 行，每行为两个空格分隔的整数 a_i 和 b_i ，表示一组好友关系，即用户 a_i 可以看到用户 b_i 发送的消息。

输出格式

输出文件共一行，为一条消息所有可能的转发途径的数量，除以 10007 所得的余数。

输入样例

```
4
7
2 1
3 1
1 3
2 3
3 2
4 3
4 2
```

输出样例

```
6
```

数据范围

- 对于30%的数据，$1 \le n \le 10$
- 对于100%的数据，$1 \le n \le 250$，$1 \le a_i, b_i \le n$，$1 \le m \le n(n-1)$

交错序列(seq)

题目描述

我们称一个仅由 0、1 构成的序列为”交错序列“，当且仅当序列中没有相邻的 1（可以有相邻的0）。例如，000，001，101，都是交错序列，而 110 则不是。

对于一个长度为 n 的交错序列，统计其中 0 和 1 出现的次数，分别记为 x 和 y。给定参数 a、b，定义一个交错序列的特征值为 $x^a y^b$。注意这里规定任何整数的 0 次幂都等于 1（包括 $0^0=1$）。

显然长度为 n 的交错序列可能有多个。我们想要知道，所有长度为 n 的交错序列的特征值的和，除以 m 的余数。（m 是一个给定的质数）

例如，全部长度为 3 的交错串为：000、001、010、100、101。当 a=1，b=2 时，可计算：
$3^1\times0^2+2^1\times1^2+2^1\times1^2+2^1\times1^2+1^1\times2^2=10$

输入格式

输入文件共一行，包含三个空格分开的整数 n，a，b 和 m。

输出格式

输出文件共一行，为计算结果。

输入样例1

```
3 1 2 1009
```

输出样例1

```
10
```

输入样例2

```
4 3 2 1009
```

输出样例2

```
204
```

数据范围

- 对于30%的数据，1≤n≤15
- 对于100%的数据，1≤n≤10000000，0≤a,b≤45，m<100000000