

算法实现题 7-1 模平方根问题（习题 7-10）

★问题描述：

设 p 是一个奇素数， $1 \leq x \leq p-1$ ，如果存在一个整数 y ， $1 \leq y \leq p-1$ ，使得 $x \equiv y^2 \pmod{p}$ ，则称 y 是 x 的模 p 平方根。例如 63 是 55 的模 103 平方根。试设计一个求整数 x 的模 p 平方根的拉斯维加斯算法。算法的计算时间应为 $\log p$ 的多项式。

★编程任务：

设计一个拉斯维加斯算法，对于给定的奇素数 p 和整数 x ，计算 x 的模 p 平方根。

★数据输入：

由文件 input.txt 给出输入数据。第一行有 2 个正整数 p 和 x 。

★结果输出：

将计算出的 x 的模 p 平方根输出到文件 output.txt。当不存在 x 的模 p 平方根时，输出 0。

输入文件示例

input.txt
103 55

输出文件示例

output.txt
63