实验八 素数的原根

14061075 修闽珂

1. 算法原理：
2. 原根的求法求出x-1所有不同的质因子p1,p2...pm，对于任何2<=a<=x-1,判定a是否为x的原根，只需要检验a^((x-1)/p1),a^((x-1)/p2),...a^((x-1)/pm)这m个数中，是否存在一个数mod x为1，若存在，a不是x的原根，否则就是x的原根。
3. 原根数量的求法：x欧拉函数值得欧拉函数值
4. 算法流程

算法流程如下：

1. 准备好求最大公因式、模重复平方、素性检验、欧拉函数的算法，准备好求质因数的函数，准备判断原根的函数（算法的实现同算法原理所示）
2. 生成随机数，判断是不是素数，如果是就继续，不是就重新生成素数。
3. 循环，从2开始，判断当前数是不是原根，如果是就输出，同时计已输出的原根数。循环到达x-1或者输出10个原根就结束循环。
4. 记最小原根，用模重复平方算法计算离散对数。
5. 测试样例结果

详见附件(太长)