## 模重复平方算法

140613 14061075 修闽珂

1. 算法原理

(0)令a = 1 , 并将n写成二进制：

其中ni ∈{0 , 1} , i = 0,1,…,k-1 .

(1)如果n0 = 1,则计算 a0 ≡ a·b( mod m) ,

否则取a0 = a ,即计算 (2) 如果n1 = 1,则计算

a1 ≡ a0·b1 ( mod m) ,

否则取a1 = a0 ,即计算 

… …

(k-1)如果nk-2 = 1,则计算ak-2≡ak-3·bk-2 ( mod m) ,

否则取ak-2 = ak-3 ,即计算 

(k)如果nk-1 = 1,则计算

ak-1≡ak-2·bk-1 ( mod m) ,

否则取ak-1 = ak-2 , 即计算



1. 测试样例

见附件中的txt。

1. 算法流程
   1. 定义模重复平方算法的函数，完全仿照算法原理
   2. 打开文件
   3. 按行读入数字并转换成三个独立的整数
   4. 分别用模重复平方算法和普通算法求模并输出各自所用时间
   5. 关闭文件
2. 心得体会

这个算法是一种快速计算平房模的算法。较之于普通模幂运算快了不少。