第三届（2018）全国高校密码数学挑战赛

赛题二

一、 赛题名称：整数分解

二、 赛题描述

2.1 问题描述

已知一个无平方因子的正整数N, 求N的素因子, 即求整除N的素数. 整数N的十进制表示请参见附件“数据文件.txt”.

2.2 成绩评判

参赛者在论文摘要中应明确列出所求每一个素因子, 在论文正文中应详细描述每个素因子求出的方法. 参赛者能够正确求解N的素因子越多, 得分越高.

三、 密码学背景及相关问题的研究进展

RSA 是著名的公钥密码算法, 1977 年由 Rivest, Shamir 和 Adleman 一起提出, 在实际中有着广泛的应用. RSA 算法的安全性依赖于大整数分解的困难性, 这使得整数分解问题成为现代密码学非常关注的数学问题之一. 关于整数分解方法的综述可以参见文[1]. 以下简要介绍一下整数分解方法的发展.

设N是一个正整数. 试除法是最初等的整数分解算法, 该方法思想简单, 但能够快速分解出N中的小素因子. Pollard 于 1975 年提出著名的ρ方法. 该方法的基本思想是通过多项式迭代产生数列, 从中寻找整数x_1, x_2满足 $\gcd(x_1 - x_2, N)$是N的一个非平凡因子. 此外, 1974 年, Pollard 基于费马定理, 提出了$p-1$方法. 虽然该方法不是一个具有一般性的分解算法, 但是其思想却被应用到一些现代的分解算法中. 比如，基于 Pollard $p-1$方法的思想， Lenstra 提出了椭圆曲线分解方法。此外，费马曾提出一个基于二次同余的想法, 即如果可以找正整数s, t满足$s^2 \equiv t^2 (\mathrm{mod}\ N)$, 则$\gcd(s \pm t, N)$可能是$N$的一个非平凡因子。为了提高搜索满足条件的整数$s, t$的效率，人们引入了分解基的概念。一个分解基是不超过某个上界B的素数集合; 若一个正整数的素因子均在该分解基中, 则称为B-平滑的.

分解基方法的基本思想是生成一批满足$x^2 (\mathrm{mod}\ N)$是B-平滑数的整数x，然后根据它们在分解基上的分解构造出整数s, t满足$s^2 \equiv t^2 (\mathrm{mod}\ N)$. 现代分解算法大都采用基于分解基的方法，比如连分数分解法、二次筛法和数域筛法等。数域筛法是目前分解大整数最有效的算法。

四、参考文献

[1] Henri Cohen. A course in computational algebraic number theory, volume 138 of Graduate texts in mathematics. Springer, 1993. （第 8 章、第 9 章、第 10 章）