

# C1 大作业说明

陈宇梁

PB25000330

## 1 项目介绍

这是计算机程序设计的期末大作业 C1，题目是：编写一个程序，使用 Miller Rabin 算法，测试并产生一个随机的 1024 位大素数。本代码实现了这个功能，并且达到了较好效率。

## 2 代码说明/算法介绍

整体架构：这份代码利用自定义数据结构 BigInt 存储数据，实现了基本的加减乘除以及随机数生成，并采用 Miller-rabin 算法检验素数。

一些优化：

1. 在 Miller-rabin 算法中，由于需要用到许多次乘法运算，因此为了加速代码，我们采用了快速幂算法，并且使用快速的蒙哥马利模乘(Montgomery) 算法实现模运算的快速完成。
2. 在利用 Miller-Rabin 算法检验素数之前，我们使用了 3~19 的所有小素数对生成的随机数进行筛选，这样可以排除一些非素数的情形，加快检验速度。

附代码流程：

