实验一 多线程程序设计与性能分析

一、实验内容

利用**多线程设计**实现NTT的加速

二、内容说明

1. 用多线程设计方法，对NTT的C++简易实现代码进行优化(见附件ntt.cpp)，降低”ntt”函数的运行时间，时间测试方式详见代码。在实验设计中尽量考虑输入线程数、硬件配置（例如处理器核数、cache大小）等各种你认为对运行时间会产生影响的参数。  
 2. 数论变换（Number Theoretic Transform，NTT）是离散傅里叶变换（Discrete Fourier Transform, DFT）在有限域下的等价物，在计算机科学和密码学中有广泛应用。附件代码中实现了用NTT加速大数乘法的过程。关于NTT的介绍与代码逻辑可以参考：  
<https://zhuanlan.zhihu.com/p/80297169>

三、考察重点

1. 多线程编程基本方法

**2. 实验设计、数据统计方法与分析结论**

四、注意事项

1. 程序实际执行时间还取决于编译器种类、优化选项、操作系统、CPU型号等因素，本实验需要控制这些无关因素，仅对比多线程下优化效果。

2. **实验报告交代清楚实验的硬件软件环境**。

3. 数论变换的直接用途为多项式的系数表示向点值表示的转换，转换后的点值表示可用于快速进行多项式乘法。如果将十进制大数按位视为多项式系数的等价表示，则可以用相同的思想加速大数乘法。感兴趣的同学可以自行查找相关资料。

4. 无法完全理解数学原理也不会影响实验，实验只需理解ntt函数中嵌套循环之间的数据计算关系，从而思考多线程计算方法并完成实验目标。

五、实验报告要求

**1. 4人一组完成，提交一份实验报告（尽量凑齐4个人一组）；**

**2. 提交形式为.zip压缩文件，命名方式为“张三-李四-王五-赵六-实验一报告.pdf”（命名方式不正确会扣分）。压缩包中需中包括修改后的代码文件和实验报告文件，实验报告格式为word或pdf，并在报告开头写上全组成员名字学号。发送到山大网盘：**

https://icloud.qd.sdu.edu.cn:7777/link/1B7289A9E41097E57B19D2CEAC48BF10**，**

**3. 提交报告的截止时间为4月4日（周四晚上11点59分59秒）。晚交的报告将会被扣分。**

**4. 所有雷同的实验报告（包括和之前高年级提交的实验报告雷同），本次实验不得分。同一学生本学期出现2次及以上雷同的实验报告，本学期实验为0分。**

**5. 借用板子需严格遵守实验室的规章流程，同时请爱护实验器材，板子先关闭开关再拔线断电，如有器材损坏第一时间报告助教**