信息安全数学基础课程试验

李晓峰 北京联合大学智慧城市学院

1、 实现一个简单的交互式命令行界面，可以输入要计算的函数，输入 exti 退出。参考工程为 gitee 上的 calculator 项目【1】。

2、 利用 GNU MP 实现以下算法（不能直接使用 GNU MP 已有函数）

序号	命令行接口	输出示例	说明
1.	prime_erat(n,m)	3,5,7	利用 Eratosthenese 筛选法，从屏幕输出从 n 到 m 的所有素数，如果此范围内不存在素数，输出 none。
2.	gcd(n,m)	5	利用欧几里得算法实现求解 n 和 m 的最大公约数的算法。
3.	lcm(n,m)	12	求解 n 和 m 的最小公倍数的算法
4.	factor(n)	2^2*3*5	求解整数 n 的标准分解式
5.	eulerfun(n)	2	计算 n 的欧拉函数
6.	inverse(n,m)	550	实现扩展欧几里得算法，求解 n 模 m 的逆元，如果不存在，输出 none。
7.	crt(a,b,c,d,e,f)	28	实现 CRT，求解 $\begin{cases} x = a(mod\ b) \\ x = c(mod\ d) \\ x = e(mod\ f) \end{cases}$
8.	order(a,m)	5	a 对模 m 的次数
9.	primroot(m)	6,7,11,12,13,15,17,19,22,24,26,28,29,30,34,35	求 m 的原根
10.	legendresym(a,p)	-1	利用二次互反律，计算 a 对 p 的 legendre 符号

3、 框架和功能测试，要编写测试用例。测试用例的基础知识可以

在网上查阅相关资料了解，如【3】【4】【5】。本课程测试用例要求如表格 1 所示。

表格 1 测试用例示例

功能测试					
用例编号：					
用例目的		（说明：描述本用例的测试目的）			
前提条件		（说明：在此说明执行此用例所需的条件，条件不满足用例则无法正常执行）			
子用例编号	输入	操作步骤	期望结果	实测结果	备注

4、 试验提交安排

提交截止时间	提交内容	备注
11.8 23:00	框架	代码和对应文档
11.15 23:00	实现 1~4	代码和对应文档
11.22 23:00	实现 5~7	代码和对应文档
11.29 23:00	实现 8~10	代码和对应文档
12.3 8:00	ppt	提交 ppt，课代表收齐上课拷贝给我
12.4	实验答辩	每人 5 分钟

5、 评分办法

评分规则为：

CR(code running)：无提交 0 分，能运行但与文档描述不符 3 分，有提交且能按文档正确运行 5 分.

DQ(document qualification)：文档文字描述，共 15 分，细则为：

- DQ-1 文档中有文字描述.无 0 分，有 5 分.
- DQ-2 文字描述质量.简练清晰 5 分，把框架或功能准确描述出来 3，描述混乱 0.
- DQ-3 有框架或功能流程图.无 0 分，不满足规范或者不准确 3 分，满足规范且准确 5 分。

TC(test cases)：测试用例，共 10 分，细则为：

- TC-1 测试用例。无 0 分，有但是描述不规范 3 分，有且描述规范 5 分.
- TC-2 测试用例设计。覆盖全面功能且考虑全面 5 分，覆盖全部功能但考虑不全面主要内容 3，未覆盖全面功能且考虑欠缺 0 分。

各个考核单元对应的评分规则如表格 2 所示。

表格 2 考核单元分值和所用评分规则

内容	评分办法	分值（占总分值）
第一次代码提交	见另外文档	3
框架	CR,DQ,TC	3
1~4	CR,DQ,TC	3
5~7	CR,DQ,TC	3
8~10	CR,DQ,TC	3
实验答辩	每人 5 分钟，准备 ppt 1、 ppt 编写规范,内容准确，逻辑性强 5 分，编写不精炼 3 分，编写混乱 0 分。 2、 演讲简练准确逻辑性强 10 分，演讲准确有逻辑但不够精炼 7 分，演讲准确 5 分，演讲不够准确 3，演讲逻辑混乱不清楚 0 分。	15

	3、 总分构成为同学互评占 30%，教师评价 70%。	
合计		30

6、 流程图绘制要求

流程图绘制规范参考百度百科“程序流程图”

7、 参考文献

【1】 https://github.com/btmills/calculator

【2】 程序流程图，https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F%E6%B5%81%E7%A8%8B%E5%9B%BE/8996271?fr=aladdin

【3】 测试用例，https://baike.baidu.com/item/%E6%B5%8B%E8%AF%95%E7%94%A8%E4%BE%8B

【4】 Test case，http://softwaretestingfundamentals.com/test-case/

【5】 Test case，http://tryqa.com/test-case/