湖南科技大学考试试题纸（ A 卷）

（ 2022－2023 学年度第 二 学期）

课程名称: 信息安全数学基础 开课单位: 计算机学院 命题教师: 李志刚

授课对象: 计算机 学院 21 年级 信息安全专业 1,2,3 班

考试时量: 100 分钟 考核方式: 考试 考试方式: 闭卷

审核人: 审核时间: 年 月 日

一、 证明题（本题共 16 分，每小题 8 分）

1. 证明：存在整数 m，使得 5 可以整除 $3m+1$。
2. 证明：$2^{70} \equiv 4 \pmod{15}$

二、综合题（本题共 84 分，其中第 1,2,3,4,6,7 小题,每小题 10 分；第 5 小题 8 分；第 8 小题 16 分，要求**写出必要的过程**）

1. 用中国剩余定理解同余方程组$x \equiv 3(\mathrm{mod}\ 4)$，$x \equiv 2\ (\mathrm{mod}\ 5)$，$x \equiv 0\ (\mathrm{mod}\ 7)$。

2. 计算$(a)123$ 和 49 最大公约数 (5 分) (b)求$49^{-1}(mod\ 123)$ 。(5 分)

3. 判断同余方程$x^2 \equiv 26(\mathrm{mod}\ 119)$是否有解。

4. 已知 2 是模 19 的一个原根，则计算2^8 模 19 的阶；(5 分)求解$16^x \equiv 4(mod\ 19)$。 (5 分)

5. 设 G 是一个定义了二元运算的非空子集，如果该二元运算满足如下：…… 那么称 G 为一个群。

请把上述群的定义补充完整。

6. (a)在多项式环$\mathbb{Z}[x]$上用带余除法计算$g(x)$除$f(x)$的商式$q(x)$和余式$r(x)$。这里$f(x)=x^4+x-2$，$g(x)=x^2+1$，而$f(x)=q(x)g(x)+r(x)$。(5 分)

(b)在多项式环$\mathbb{Z}_3[x]$上用带余除法计算$g(x)$除$f(x)$的商式$q(x)$和余式$r(x)$。这里$f(x)=x^5+x+2$，$g(\mathrm{x})=2x^2+x$，而$f(x)=q(x)g(x)+r(x)$。(5 分)

7. 设$\mathbb{Z}$是整数集合，则$\mathbb{Z}$上定义两个新的运算：$a \oplus b = a+b-1$ $a \odot b = a+b-ab$ 运算$\oplus$ ， $\odot$ 均为$\mathbb{Z}$上的二元运算。(a)问：已知$\mathbb{Z}$对于$\oplus$ 构成加法交换群，请给出其零元，指出 5 的负元。(5 分) (b)验证运算$\odot$满足结合律。 (5 分)

8. 设$p(x)=x^3+2x+2$ 是$\mathbb{Z}_3[x]$中的不可约多项式，则$\mathbb{Z}_3[x]/(p(x))$是一个有 27 个元素的有限域，(a)计算域中的元素$(x+1)$和(x^2+2)的乘积。(5 分) (b)计算元素$(x+2)$的加法负元。(5 分) (c)计算元素x的乘法逆元。(6 分)