北京邮电大学 2022 —— 2023 学年第一学期

《信息安全数学基础》期末考试试题（B）

专业：＿＿＿＿ 班级：＿＿＿＿ 学号：＿＿＿＿ 班内序号：＿＿＿＿ 姓名：＿＿＿＿

装……订……线　密……封……线

考试注意事项	一、学生参加考试须带学生证或学院证明，未带者不准进入考场。学生必须按照监考教师指定座位就坐。 二、书本、参考资料、书包等物品一律放到考场指定位置。 三、学生不得另行携带、使用稿纸，要遵守《北京邮电大学考场规则》，有考场违纪或作弊行为者，按相应规定严肃处理。 四、学生必须将答题内容做在试题答题处，做在草稿纸上无效。 五、学生的姓名、班级、学号、班内序号等信息由教材中心统一印制。

考试课程	信息安全数学基础	考试时间	2023 年 2 月 16 日

题号	一	二	三	四	五	六	七	八	总分
满分	20	20	15	25	20				
得分									
阅卷教师									

一．判断题，对打√，错打×（20 分，10 小题，每小题 2 分）

1） 两个整数的最大公因数一定存在。 （ ）

2） 设 p 是一个素数, 若 $p|ab$, 则 $p|a$ 且 $p|b$。 （ ）

3） 任意给出的五个整数中必有三个数能被整数 3 整除。（ ）

4） 模 29 有 28 个原根。 （ ）

5） 设 n 是正整数, 若 2^n-1 是素数, 则 n 不一定是素数。 （ ）

6） 群 G_1 和 G_2 是群 G 的正规子群，则 G_1G_2 也是 G 的正规子群。（ ）

7） 循环群的子群不一定是循环群。（ ）

8） 多项式集 $R[X]$是有单位元的交换环。（ ）

9） $x^4+x^3+x^2+1$是$F_2[x]$中的不可约多项式。（ ）

10） 任意一个置换都可以表示为一些不相交轮换的乘积。在不考虑乘积次序的情况下, 该表达式是唯一的。（ ）

二． 填空题（20 分，10 个小题，每小题 2 分）

1） 转换十六进制 $(ABC8)_{16}$ 为二进制________________。

2） 8^{1234} 被 13 除的余数是________。

3） 计算 $[2n+1,2n-1]=$________________________。

4） $\varphi(30) =$____________。

5） 设 p 是奇素数，则模 p 的所有二次剩余的乘积对模 p 的剩余是______________。

6） 设 G 和 G' 都是群，f 是 G 到 G' 的一个映射。如果对任意的 $a, b \in G$，都有____________________，那么 f 叫做 G 到 G' 的一个同态。

7） 在特征为 p 的无零因子的交换环 R 中，设 p 为素数，则对任意 $a, b \in R$，有 $(a+b)^p =$ ______________________。

8） 设 p 是素数，$f(x)$ 是 $\mathrm{F}_p[X]$ 中的 n 次多项式。若 $\mathrm{ord}_p(f(x))=$________，则 $f(x)$ 为 F_p 上的本原多项式。

9） 设 $f(x) = x^3 + x + 1, g(x) = x^2 + x$ 为 F_2 上的多项式，那么 $f(x)$ 被 $g(x)$ 除的余式为_______。

10） n 元置换全体组成的集合 S_n 对置换的乘法构成一个群，该群的阶是________。

三． 简答题（15 分，5 个小题，每小题 3 分）

1）什么是模 m 的完全剩余系？

2）什么是对于基 b 的强伪素数？

3）什么是交换群？

4）什么是左（右）陪集、陪集？

5）什么是理想？

四． 计算题（25 分，5 个小题，每小题 5 分）

1）判断同余式 $2x^3+5x^2+6x+1\equiv 0\ (\mathrm{mod}\, 7)$ 是否有三个解。

2）解一次同余方程组

$$\begin{cases} x \equiv 3\ (mod\ 7) \\ x \equiv 2\ (\mathrm{mod}\ 5) \\ x \equiv 5 (mod\ 11) \end{cases}$$ 。

3）求模 $m = 25$的全部原根。

4）求解同余方程$6 * 9^x \equiv 11 (mod\ 17)$。

5）设$a(x)=x^8+x^4+x^3+x^2+1$，$b(x)=x^5+x+1$是数域F_2上的多项式，计算$s(x),t(x)$使得$s(x)\cdot a(x)+t(x)\cdot b(x)=(a(x),b(x))$ 。

五、证明题（20 分，4 个小题，每题 5 分）

1）设 a,b 是两个正整数，证明 $(2^a-1,2^b-1)=2^{(a,b)}-1$。

2）证明 $1105 = 13 \cdot 17 \cdot 5$　是 Carmichael 数

3）证明群 G 中的元素a与其逆元a^{-1}有相同的阶。

4）证明 $SL_2(\mathbb{Z})=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{Z}, ad-bc=1\right\}$是一个乘法群，其生成元为 $T=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$。