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（A）

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。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	2022 年 12 月 21 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×（10 分，10 小题，每小题 2 分）

1）设 p 是一个素数，a 为整数。如果 $p\nmid a$，则 p 与 a 互素。（ ）

2）设 a，b，c 是三个整数，且 $bc\neq 0$。如果 $b|a$，$c|a$ 则 $bc|a$。（ ）

3）每个正整数都可以唯一地表示成不同的 2 的幂的和。（ ）

4）设 m 是一个正整数，$a\equiv b\ (mod\, m)$，则 $\frac{a}{d}\equiv\frac{b}{d}(\mathrm{mod}\,\frac{m}{d})$。（ ）

5）若a_1,a_2是模 p 的非平方剩余，则a_1a_2是模 p 的平方非剩余。（ ）

6）对于模 m，有$ord_m(ab)=[ord_m(a)，ord_m(b)]$ 。( )

7）存在无穷多个伪素数、Euler 伪素数、强伪素数。（ ）

8）每个循环群都是交换群。（ ）

9）域中的每个元素都可逆。（ ）

10） 设 G,G' 是两个群，f 是 G 到 G' 的一个映射，如果对任意的 a, $b\in G$, 有 $f(ab)=f(a)f(b)$, 则 f 叫做 G 到 G' 的一个同构。（ ）

二. 填空题（20 分，10 个小题，每小题 2 分）

1） 计算最小公倍数 [120, 150, 210, 35] = ____________________。

2） 模 10 的最小非负完全剩余系={______________________}。

3） 同余方程 $4x \equiv 10 \pmod{15}$ 的解是__________________________。

4） $\left(\frac{137}{227}\right)$=________。

5） 模 m 的原根存在的充分必要条件是：__________________________

__________________。

6） 设 H 是有限群 G 的子群，则子群 H 的阶是 $|G|$ 的______________。

7） 设 H={(12), (13)}为 S_3 的一个子群，陪集 $H(23)$ =_______________

_____________。

8） 群 G 中元素 a 的阶等于 10，则 a^4 的阶为__________。

9） 环 R 的平凡理想包括____________________。

10） 设：$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$，$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$，则 $\sigma_1\sigma_2$ =________。

三. 简答题（15 分，5 个小题，每小题 3 分）

1）什么是 a 对模 m 的指数？

2）什么是对于基 b 的伪素数？

3）什么是群？

4）什么是整环？

5）什么是域？

四． 计算题（25 分，5 个小题，每小题 5 分）

1）设 a=198，b=252，求整数 s，t，使得 $sa+tb=(a,b)$。

2）韩信点兵：有兵一队，若列成五行纵队，则末行一人；成六行纵队，则末行五人；成七行纵队，则末行四人，成十一行纵队，则末行十人，求兵数。

3）求模 43 的原根。

4）设 $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix}$，$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix}$，计算 $\sigma_1\sigma_2$，$\sigma_2\sigma_1$,σ_1^{-1}.

5）求有限域 $F_{16} = F_2[x]/(x^4+x+1)$ 的所有本原元。

五、证明题（20 分，4 个小题, 每题 5 分）

1）证明 $N = 137$ 为素数。

2）证明：设 m 是一个正整数，a 是满足 $a \mid m$ 的整数，则一次同余式 $ax \equiv b(\bmod m)$ 有解的充分必要条件是 $(a,m) \mid b$。而且，当同余式有解时，其解为 $x \equiv \frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} (\bmod \frac{m}{(a,m)}) \right) + t \frac{m}{(a,m)} (\bmod m)$

$t = 0,1,\cdots,(a,m)-1$。

3）设 p 是一个素数，$F_p = Z/pZ$. 设 $F_p^* = F_p \setminus \{0\}$. 证明：集合 F_p^* 对于乘法 $a \otimes b = (ab(\bmod p))$ 构成一个交换乘群。

4）设 f 是群 G 到群 G' 的一个同态，证明：

(i) $f(e) = e'$，即同态将单位元映到单位元。

(ii) $\ker f = \{a \mid a \in G, f(a) = e'\}$ 是 G 的子群，则 f 是单同态的充要条件是 $\ker f = \{e\}$ 。