北京邮电大学《信息安全数学基础》
2021-2022学年第一学期期末试卷

装

订

线

一、 填空题（本大题共8小题，每空2分，共24分）

得分	

1. 两个整数 a，b，其最大公因数和最小公倍数的关系为_____。

2. 给定一个正整数 m，两个整数 a,b 叫做模 m 同余，如果_____，记作 $a \equiv b(\mathrm{mod}\, m)$；否则，叫做模 m 不同余，记作_____。

3. 设 m，n 是互素的两个正整数，则 $\varphi(mn) =$ _____。

4. 设 $m>1$ 是整数，a 是与 m 互素的正整数。则使得 $a^e \equiv 1(\mathrm{mod}\, m)$ 成立的最小正整数 e 叫做 a 对模 m 的指数，记做_____。如果 a 对模 m 的指数是 $\varphi(m)$，则 a 叫做模 m 的_____。

5. 设 n 是一个奇合数，设整数 b 与 n 互素，如果整数 n 和 b 满足条件_____，则 n 叫做对于基 b 的拟素数。

6. 设 G,G' 是两个群，f 是 G 到 G' 的一个映射。如果对任意的 $a,b \in G$，都有_____，那么 f 叫做 G 到 G' 的一个同态。

7. 加群 Z 的每个子群 H 都是_____群，并且有 $H = <0>$ 或 $H =$ _____。

8. 我们称交换环 R 为一个域，如果 R 对于加法构成一个_____群，$R^* = R\backslash\{0\}$ 对于乘法构成一个_____群。

二、计算题（本大题共 3小题，每小题8分，共24分）

得分	

1. 令 $a = 1613$，$b = 3589$。用广义欧几里德算法求整数 s,t，使得 $sa + tb = (a,b)$

装

2. 求同余方程 $x^2 \equiv -2(\mathrm{mod}\,67)$ 的解数。

订

线

3. 计算 3 模 19 的指数 $\mathrm{ord}_{19}(3)$。

三、解同余方程（本大题共2小题，每小题10分，共20分）

得分	

1. 求解一次同余方程 $17x \equiv 14(\mathrm{mod}\,21)$。

装

订

线

2. 解同余方程组 $\begin{cases} x \equiv 2(\mathrm{mod}\ 3) \\ x \equiv 3(\mathrm{mod}\ 5) \\ x \equiv 2(\mathrm{mod}\ 7) \end{cases}$

四、证明题（本大题共3小题，每小题7分，共21分）

得分	

1. 证明：如果 a 是整数，则 $a^3 - a$ 能够被 6 整除。

装

订

线

2. f 是群 G 到 G' 的一个同态， $\ker f=\{a \mid a \in G, f(a)=e'\}$ ，其中 e' 是 G' 的单位元。证明： $\ker f$ 是 G 的正规子群。

3. 证明：如果 p 和 q 是不同的素数，则 $p^{q-1}+q^{p-1}=1(\mathrm{mod}\, pq)$ 。

装

订

线

五、应用题（共11分）RSA公钥加密算法的密钥生成步骤如下：选择两个大的素数p和q，计算$n=pq$。选择两个正整数e和d，满足：$ed=1(\mathrm{mod}\ \varphi(n))$。Bob的公钥是（$n$，$e$），对外公布。Bob的私钥是$d$，自己私藏。如果攻击者分解$n$得到$p=47$，$q=23$，并且已知$e=257$，试求出Bob的私钥$d$。

得分	