信息安全数学基础期末考试试卷及答案（A 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，$R^* = R \setminus \{0\}$ 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 $sa + tb = (a,b)$。

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

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

装

订

线

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$17x \equiv 14 (\mathrm{mod}\, 21)$。

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。

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$p^{q-1} + q^{p-1} \equiv 1 (\mathrm{mod}\, pq)$。

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：$ed \equiv 1 (\mathrm{mod}\, \varphi(n))$。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	

答案

一、填空题（每空 2 分，共 24 分）

1. 两个整数 a，b，其最大公因数和最小公倍数的关系为$ab = [a,b](a,b)$。

2. 给定一个正整数 m，两个整数 a,b 叫做模 m 同余，如果$m \mid a-b$，记作 $a \equiv b (\mathrm{mod}\, m)$；否则，叫做模 m 不同余，记作$a \not\equiv b (\mathrm{mod}\, m)$。

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

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$ord_m(a)$。如果 a 对模 m 的指数是$\varphi(m)$，则 a 叫做模 m 的 原根 。

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$b^{n-1} \equiv 1 (\mathrm{mod}\, n)$，则

装

订

线

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 $f(ab)=f(a)f(b)$，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 循环 群，并且有 $H=<0>$ 或 $H=<m>(\text{或}=mZ)$。

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

二、计算题(每题 8 分，共 24 分)

1. 解：
3589=2*1613+363
1613=4*363+161
363=2*161+41
161=3*41+38
41=1*38+3
38=12*3+2
3=1*2+1
2=2*1
(a,b)=1,从而
1=3-1*2
=3-1*(38-12*3)
=-38+13*(41-1*38)
=13*41-14*(161-3*41)
=-14*161+55*(363-2*161)
=55*363+(-124)*(1613-4*363)
=(-124)*1613+551*(3589-2*1613)
=551*3589+(-1226)*1613
所以 s=-1226 t=551

2. 解：因为（-2/67）=(65/67)
=(13/67)(5/67)
$=(-1)^{12*66/4}(-1)^{4*66/4}(2/13)(2/5)$
$=1*1*(-1)^{(13*13-1)/8}(-1)^{(5*5-1)/8}$
=-1*(-1)=1
所以-2 是 67 的平方剩余
所以 $x^2\equiv -2(\text{mod}67)$有 2 个解。

3. 解：因为$\varphi(19)=18$,所以只需对 18 的因数 d=1,2,3,6,9,18 计算 $a^d(\text{mod}19)$
因为 $3^1\equiv 3$，$3^2\equiv 9$，$3^3\equiv 8$，$3^6\equiv 7$，$3^9\equiv -1$，$2^{18}\equiv 1(\text{mod}19)$
所以 3 模 19 的指数为 18；

三、解同余方程（每题 10 分，共 20 分）

1. 解：因为（17，21）=1 | 14 故原同余式有解。

又 17x≡1（mod21，所以 特解 x_0'≡5（mod21）。

同余式 17x≡14（mod21）的一个特解为 x_0≡14*x_0'=14*5≡7（mod21）

所有解为：x≡7（mod21）

2. 解：令 $m_1=3, m_2=5, m_3=7$， $m=3*5*7=105$，

$$M_1=5*7=35, M_2=3*7=21, M_3=3*5=15。$$

分别求解同余式 $M_i'M_i\equiv 1(\mathrm{mod}\, m_i)$（$i$=1,2,3）

得到 $M_1'=2$， $M_2'=1$， $M_3'=1$。故同余式的解为

$$\begin{aligned} x &\equiv M_1'M_1*2+M_2'M_2*3+M_3'M_3*2(\mathrm{mod}105)\\ &\equiv 2*35*2+1*21*3+1*15*2(\mathrm{mod}105)\\ &\equiv 23(\mathrm{mod}105)\end{aligned}$$

四、证明题（每题 7 分，共 21 分）

1. 证明：因为 $a^3-a=(a-1)a(a+1)$

当 a=3k，k∈Z　3|a　则 3|a^3−a

当 a=3k−1，k∈Z　3|a+1　则 3|a^3−a

当 a=3k+1，k∈Z　3|a−1　则 3|a^3−a

所以 a^3−a 能被 3 整除。

又因为(a−1)，a，(a+1)是 3 个连续的整数，所以至少有一个是偶数，从而 2|a^3−a。因此，a^3−a 能够被 6 整除。

2. 证明：因为(p, q)=1　p, q 都为素数　所以 φ (p)=p−1，φ (q)=q−1

由 Euler 定理知：$p^{\varphi(q)}$≡1(modq)　$q^{\varphi(p)}$≡1(modp)

即 p^{q-1}≡1(modq)　q^{p-1}≡1(modp)

又 q^{p-1}≡0(modq)　p^{q-1}≡0(modp)

所以 $p^{q-1}+q^{p-1}$≡1(modq)　$q^{p-1}+p^{q-1}$≡1(modp)

又[p, q]=pq　所以 $p^{q-1}+q^{p-1}$≡1(modpq)

3. 证明：对任意 $a,b\in\ker f$，有 $f(a)=e', f(b)=e'$，从而，

$$f(ab^{-1})=f(a)f(b^{-1})=f(a)f(b)^{-1}=f(a)f(a)^{-1}=e'。$$

因此，$b\in\ker f$，$\ker f$ 是群 G 的子群。

对任意 $a\in G$, $b\in\ker f$, 我们有

$$f(aba^{-1})=f(a)f(b)f(a^{-1})=f(a)ef(a)^{-1}=f(a)f(a)^{-1}=e'。$$

这说明 $aba^{-1}\in\ker f$。从而，$\ker f$ 是群 G 的正规子群。