12元

南京邮电大学 2015/2016 学年第一学期

《信息安全数学基础》期末试卷（A）

院(系)__________ 班级__________ 学号__________ 姓名__________

题号	一	二	三	四	五	六	七	八	九	总分
得分										

自觉遵守考试规则，诚信考试，绝不作弊

装订线内不要答题

得分

一、 填空题（每题2分，共20分）

1. $7^{125} \pmod{41} =$__________。

2. $m=14$，则模 m 绝对最小完全剩余系为__________。

3. $\varphi(12250)=$__________。

4. 同余方程 $5x^3-3x^2+3x+1\equiv 0 \pmod 7$ 的解为__________。

5. 以-2为二次剩余的奇素数 p 满足的形式为__________。

6. 已知 a 是模41的原根，则 a^{12} 模41的指数是__________。

7. 判定正整数集 N^+ 关于运算 $a\circ b=a+b+ab$ 是否构成群。__________群。(是或不是)

8. 整数加法子群 $(Z,+)$ 对实数加法群 $(R,+)$ 的陪集代表元集合为__________。

9. $f(x)=x^4+x+1\in F_2(x)$，$f(x)$____不可约多项式，$|F_2(x)/(f(x))|=$______。

10. n 阶可逆复方阵乘法群为 $\mathrm{GL}(n,\mathrm{C})$，$\mathrm{C}^*$ 为非零复数乘法群，定义映射 $\det:\mathrm{GL}(n,\mathrm{C})\to\mathrm{C}^*$ 为矩阵行列式运算，则 $\ker(\det)$ 为__________。

得分

二、计算题（每题 10 分，共 40 分）

1. 解同余方程组 $\begin{cases} x\equiv 1 \pmod 3 \\ 6x\equiv 2 \pmod 7 \\ 4x\equiv 6 \pmod{10} \end{cases}$

1

2. 已知整数$n=1457=31\times 47$，判断1575是否是1457的二次剩余，如果是，写出1575模1457的平方根和原平方根满足的同余方程组。

3. 求模$p=47$的所有原根

4. 已知$f(x)=2x^5+x^4+4x+3$，$g(x)=3x^2+1\in F_5(x)$，计算$(f(x),g(x))$。

得 分

三、证明题（每题 8 分，共 40 分）

1. 设 $a>2$ 是奇数. 证明：存在正整数 $d \le a-1$，使得 $(2^d-5,a)=1$。

2. 设 $m=m_1m_2$， x 和 y 分别是遍历模 m_1 和 m_2 的完全剩余系，证明：那么 $x+m_1y$ 是遍历模 m 的完全剩余系。

3. 给定正整数 a,b 和素数 p，证明：

(1). $(\{s\times a+t\times b \mid s,t\in Z\},+,\times)$ 是整数环 $(Z,+,\times)$ 的主理想。

(2). (p) 是整数环 $(Z,+,\times)$ 的极大理想和素理想

4. 叙述并证明群的同态基本定理。

5. 设群 G 是Abel群，G 的阶为 pq， 设 p 和 q 是不相同的两个素数。已知结论：$\alpha,\beta\in G$，$\mathrm{ord}(\alpha)=m,\mathrm{ord}(\beta)=n$，若 $(m,n)=1$，则 $\mathrm{ord}(\alpha\beta)=mn$ 成立，证明：G 是循环群。

自觉遵守考试规则，诚信考试，绝不作弊

南京邮电大学 2014/2015 学年第一学期

《信息安全数学基础》期末试卷（B）

院（系）__________ 班级__________ 学号__________ 姓名__________

题号	一	二	三	四	五	六	七	八	九	总分
得分										

自觉遵守考试规则，诚信考试，绝不作弊

装订线内不要答题

得分

一、 填空题（20分，每题2分）

1. 27182的16 进制表示为________________。

2. $2^{143}(\bmod 13)=$ ________________。

3. $m=13$，则模 m 的非负最小完全剩余系为________________。

4. $5x^3-3x^2+3x+1\equiv 0(\bmod 7)$ 的解为________________。

5. 设素数 $p>2$，$(p,d)=1$，则 d 是模 p 的二次非剩余的充要条件是________________。

6. 设 $m>0$，$(a,m)=1$，则 a 模 m 的指数指____________________________。

7. 模1250的原根数为________________。

8. 同态基本定理指____。

9. $f(x)=x^4+x+1\in F_2(x)$，$f(x)$ ____不可约多项式，$|F_2(x)/(f(x))|=$ ______。

10. $H=\{0,2,4,6\}$ 是8阶循环群 $(Z_8,\oplus)$ 的4阶子群，则陪集 $5+H=$ ________________。

得分

二、计算题（每题 10 分，共 40 分）

1. 求 $(42823,6409)$，并表示成42823和6409的整系数线性组合形式.

2. 解同余方程组$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 6 \\ 6x \equiv 2 \pmod 7 \end{cases}$

3. 计算$\left(\dfrac{339}{1979}\right)$

4. 求以11为二次剩余的所有奇素数

得 分

三、证明题（每题 10 分，共 40 分）

1. 证明，对任意的素数 p，有同余式 $a^p \equiv a \pmod{p}$ 成立。

2. 设 $m = m_1 m_2$，x和 y分别是遍历模 m_1 和 m_2 的完全剩余系，那么 $x + m_1 y$ 是遍历模 m 的完全剩余系。

3. 给定正整数a,b，证明$(\{s\times a+t\times b \mid s,t\in Z\},+,\times)$是整数环$(Z,+,\times)$的主理想。

4. 设G是群，其中心$C=\{a \mid a\in G,\forall g\in G,ag=ga\}$，证明：$C$是$G$的不变子群

自觉遵守考试规则，诚信考试，绝不作弊

南京邮电大学 2013/2014 学年第一 学期

《 信息安全数学基础 》期末试卷 A

本试卷共 5 页； 考试时间 110 分钟；

专业______ 班级______ 学号______ 姓名______

题号	一	二	三	四	五	六	七	八	九	十	总 分
得分											

装订线内不要答题

得分

一、计算题（40 分，每题 8 分）

1. 已知 a=1395, b=713, 计算 a 和 b 的最大公约数(a, b), 并求 s 和 t, 使得 sa+tb = (a, b).

$1395 = 713 \times 1 + 682$

$713 = 682 \times 1 + 31$

$682 = 31 \times 22$

$(1395, 713) = 31$

$31 = 713 - 682 \times 1$

$= 713 - (1395 - 713 \times 1) \times 1$

$= -1395 \times 1 + 713 \times 2$

$\therefore s = -1, t = 2$

2. 在 $F_2[x]$ 中，已知 $a(x)=x^5+x^3+x+1$, $b(x)=x^2+x+1$, 计算 $q(x)$ 和 $r(x)$，使得 $a(x)=b(x)q(x)+r(x)$, 并且 $r(x)$ 的次数小于 $b(x)$ 的次数；$a(x)$ 是不可约多项式嘛？

$$\begin{array}{r} x^3+x^2+x \\ x^2+x+1 \overline{\smash{)}\, x^5+x^3+x+1} \\ x^5+x^4+x^3 \\ \hline x^4+x^2+1 \\ x^4+x^3+x^2 \\ \hline x^3+x+x+1 \\ x^3+x^2+x \end{array}$$

$\therefore q(x) = x^3+x^2+x$

$r(x) = 1$

1

7

3. 求解一次同余式$9x \equiv 12 \pmod{15}$

4. 求解一次同余式组$\begin{cases} 3x \equiv 1 \pmod{7} \\ 5x \equiv 2 \pmod{6} \end{cases}$，并说明如果$5x \equiv 2 \pmod{6}$换成$4x \equiv 2 \pmod{6}$，该同余式组该如何处理？

5. 计算 Jacobi 符号$\left(\frac{51}{91}\right)$和$\left(\frac{61}{91}\right)$，并说明对于$\left(\frac{b}{a}\right)$，如果$a = pq$，其中 p 和 q 是两个奇素数，则 b 是 a 的二次剩余或二次非剩余的充要条件是什么？从而判断 51 和 61 是否是 91 的二次剩余？

得分

二、证明题（30 分，每题 10 分）

1. 证明：若 k 是素数，则对任意正整数 n，都有 $k \mid n^k - n$；结论对 k 为合数还成立吗？

2. 设 $r_1, \ldots, r_m; r_1', \ldots, r_m'$ 分别是模 m 的两组完全剩余系，证明：当 m 为偶数时，$r_1 + r_1', \ldots, r_m + r_m'$ 一定不是模 m 的完全剩余系；写出 m=18 的一组简化剩余系。

对于F中任意元素 $a+b\sqrt5$，其中 $a\neq0$ 或 $b\neq0$

存在 $c=\frac{a-b\sqrt5}{a^2-5b^2}\in F$

使 $c(a+b\sqrt5)=(a+b\sqrt5)^{-1}$ 即c是 $a+b\sqrt5$ 逆

∴ $\langle F,+,$

P17.18

P16.8

3. 设 $F=\{a+b\sqrt5 \mid a,b\in Q\}$，证明：$\langle F,+,\cdot\rangle$ 是域，~~并说明该域的素域是什么~~

证明：$\langle F,+\rangle$ 的单位元为0，显然 $\langle F,+\rangle$ 中任何元素 x 都有逆元 $-x\in F$

∴ $\langle F,+\rangle$ 是群，$\langle F,\cdot\rangle$ 是半群

∵ $\forall x,y,z\in F$ 有 $x\cdot(y+z)=x\cdot y+x\cdot z$ 成立

∴ $\langle F,+,\cdot\rangle$ 是环

∵ $\forall x,y,z\in F$，$x\neq0$ 有 $x\cdot y=x\cdot z \Rightarrow y=z$ 成立

∴ $\langle F,+,\cdot\rangle$ 中没有零因子

∵ $\forall x,y\in F$，$x\cdot y=y\cdot x$ 成立　∴ $\langle F,+,\cdot\rangle$ 是交换环

又 ∵ $\langle F,+,\cdot\rangle$ 中"+"的单位元为"0"，"·"的单位元为1

∴ $\langle F,+,\cdot\rangle$ 是含幺环

综上 $\langle F,+,\cdot\rangle$ 是域

得分

三、问答论述题（30分，每题10分）

1. 设 m>1 是整数，a 是与 m 互素的整数，请回答如下问题：

a) 什么叫 a 对模 m 的指数？什么叫原根？

b) 如果 a 对模 m 的指数是 d，那么 $a^s, s\in Z^+$ 的指数是多少？

c) 若 m=1250，模 m 存在原根吗？如果存在，模 m 有多少个不同原根？

自觉遵守考试规则，诚信考试，绝不作弊

装订线内不要答题

2. 在5级移位寄存器中，设 $c_1=1$; $c_2=0$; $c_3=0$; $c_4=1$; $c_5=1$，请回答如下问题：

a) 该线性移位寄存器的反馈逻辑函数是什么？

b) 若初始状态为(1,0,1,0,1)，写出寄存器的输出，并写出其周期，是 m 序列吗？

c) 写出该移位寄存器的链接多项式和状态转移矩阵。

3. 简要描述你进行 RSA 大数实现时的心得。

《信息安全数学基础》试卷 B

〈附答案〉

注意事项：1. 考前请将密封线内填写清楚；
2. 所有答案请直接答在试卷上；
3. 考试形式：闭卷；
4. 本试卷共 四大题，满分 100 分， 考试时间 120 分钟。

题 号	一	二	三	四	总分
得 分					
评卷人					

一． 选择题：（每题 2 分，共 20 分）

1．设 a, b 都是非零整数。若 $a|b$，$b|a$，则（　　　　）。

(1)　$a=b$，(2)　$a=\pm b$，(3)　$a=-b$，(4)　$a>b$

2．大于 10 且小于 50 的素数有（　　　　）个。

(1)　9，(2)　10，(3)　11，(4)　15

3．模 7 的最小非负完全剩余系是（　　　　）。

(1)　$-3, -2, -1, 0, 1, 2, 3$，　(2)　$-6, -5, -4, -3, -2, -1, 0$，

(3)　$1, 2, 3, 4, 5, 6, 7$，　(4)　$0, 1, 2, 3, 4, 5, 6$

4．模 30 的简化剩余系是（　　　　）。

(1)　$-1, 0, 5, 7, 9, 19, 20, 29$，　(2)　$-1, -7, 10, 13, 17, 25, 23, 29$，

(3)　$1, 7, 11, 13, 17, 19, 23, 29$，　(4)　$-1, 7, 11, 13, 17, 19, 23, 29$

5．设 n 是整数，则 $(2n, 2(n+1))=$（　　　　）。

(1)　1，(2)　2，(3)　n，(4)　$2n$

6．设 a, b 是正整数，若 $[a, b]=(a, b)$，则（　　　　）。

(1)　$a=b$，(2)　$[a, b]=ab$，(3)　$(a, b)=1$，(4)　$a>b$

7．模 17 的平方剩余是（　　　　）。

(1)　3，(2)　10，(3)　12，(4)　15

8．整数 5 模 17 的指数 $\mathrm{ord}_{17}(5)=$（　　　　）。

(1)　3，(2)　8，(3)　16，(4)　32

9．欧拉(Euler)定理：设 m 是大于 1 的整数，如果 a 是满足 $(a, m)=1$ 的整数，则（　　　　）。

(1)　$a^{m}\equiv a \pmod m$，　(2)　$a^{\varphi(m)}\equiv 1 \pmod a$，

(3) $a^{\varphi(m)}=a \pmod m$, (4) $a^{\varphi(m)}=1 \pmod m$

10．Fermat 定理：设 p 是一个素数，则对任意整数 a，有（ ）。

(1) $a^{p}=a \pmod a$, (2) $a^{p}=a \pmod p$,

(3) $a^{\varphi(m)}=a \pmod m$, (4) $a^{\varphi(p)}=a \pmod p$

二． 填空题：（每题 2 分，共 20 分）

1．设 m 是正整数，a 是满足 $a \mid m$ 的整数，则一次同余式：$ax \equiv b \pmod m$ 有解的充分必要条件是____________________。当同余式 $ax \equiv b \pmod m$ 有解时，其解数为__________________。

2．设 m 是正整数，则 m 个数 $0, 1, 2, \cdots, m-1$ 中________________________ 叫做 m 的欧拉(Euler)函数，记做 $\varphi(m)$。

3．设 m 是正整数，若同余式________________________有解，则 a 叫模 m 的平方剩余。

4．设 a, b 是正整数，且有素因数分解 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}, \alpha_i \ge 0, i=1,2,\cdots,s$，$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}, \beta_i \ge 0, i=1,2,\cdots,s$，则 $(a,b)=$______________________________，$[a,b]=$____________________________________。

5．如果 a 对模 m 的指数是________________，则 a 叫做模 m 的原根。

6．3288 的素因数分解式是 ________________________________。

7．Wilson 定理：设 p 是一个素数，则_________________________________。

8．2006 年 1 月 18 日是星期三，第 $2^{20060118}$ 天是星期____________________。

9．(中国剩余定理) 设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数，则对任意的整数 $b_1, \cdots, b_k$ 同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \cdots\ \cdots\ \cdots\ \cdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

有唯一解。令 $m=m_1\cdots m_k$，$m=m_iM_i$，$i=1, \cdots, k$，则同余式组的解为：

____，

其中____________________________________。

10．正整数 n 有标准因数分解式为 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，则 n 的欧拉函数 $\varphi(n)=$____。

三．证明题 （写出详细证明过程）：（每题 7 分，共 28 分）

1．证明：如果正整数 a，b 满足$(a, b)=1$，则 $(a^n, b^n)=1$。

2．证明：设 m 是一个正整数，$a\equiv b \pmod{m}$，则$(a, m)=(b, m)$。

3．设 m 是一个正整数，a 满足$(a, m)=1$，则存在整数 a'，$1\le a'<m$ 使得 $aa'\equiv 1 \pmod{m}$。

4．设 p，q 是两个不同的奇素数，$n=pq$，a 是与 pq 互素的整数。整数 e 和 d 满足$(e, \varphi(n))=1$，$ed\equiv 1 \pmod{\varphi(n)}$，$1<e<\varphi(n)$，$1\le d<\varphi(n)$。

证明：对任意整数 c，$1\le c<n$，若 $a^e\equiv c \pmod{n}$，则有 $c^d\equiv a \pmod{n}$。

四. 计算题（写出详细计算过程）:（每题 8 分，共 32 分）

1. 计算整数 120，150，210，35 的最大公因数和最小公倍数：

[120，150，210，35]和(120，150，210，35)。

2. 设 $a=-1859$，$b=1573$，运用广义欧几里得除法

(1) 计算(a, b)； (2) 求整数 s，t 使得 $sa+tb=(a, b)$。

3. 用欧拉定理和模重复平方计算法计算 $2^{1000000} \pmod{77}$。

4. 用中国剩余定理计算 $2^{1000000} \pmod{77}$。

《信息安全数学基础》试卷 B

注意事项：1. 考前请将密封线内填写清楚；
2. 所有答案请直接答在试卷上；
3. 考试形式：闭卷；
4. 本试卷共 四大题，满分 100 分， 考试时间 120 分钟。

题 号	一	二	三	四	总分
得 分					
评卷人					

一、 选择题：（每题 2 分，共 20 分）

1. (2) 。2. (3)。3. (3) 。4. (3)。5. (2) 。6. (2) 。7. (4)。
8. (3) 。9. (4)。10. (2)

二、 填空题：（每题 2 分，共 20 分）

1. 设 m 是正整数，a 是满足 $a\mid m$ 的整数，则一次同余式：$ax\equiv b \pmod m$ 有解的充分必要条件是 $(a, m)|b$ 。当同余式 $ax\equiv b \pmod m$ 有解时，其解数为 $d=(a, m)$ 。

2. 设 m 是正整数，则 m 个数 0, 1, 2, …, $m-1$ 中与 m 互素的整数的个数叫做 m 的欧拉(Euler)函数，记做 $\varphi(m)$。

3. 设 m 是正整数，若同余式 $x^2\equiv a \pmod m$，$(a, m)=1$ 有解，则 a 叫模 m 的平方剩余。

4. 设 a, b 是正整数，且有素因数分解 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s},\alpha_i\ge 0,i=1,2,\cdots,s$，$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s},\beta_i\ge 0,i=1,2,\cdots,s$，则 $(a,b)=p_1^{\min(\alpha_1,\beta_1)}\cdot p_2^{\min(\alpha_2,\beta_2)}\cdot\cdots\cdot p_s^{\min(\alpha_s,\beta_s)}$，$[a,b]=p_1^{\max(\alpha_1,\beta_1)}\cdot p_2^{\max(\alpha_2,\beta_2)}\cdot\cdots\cdot p_s^{\max(\alpha_s,\beta_s)}$。

5. 如果 a 对模 m 的指数是 $\varphi(m)$，则 a 叫做模 m 的原根。

6. 设 m 是一个正整数，若 $r_1, r_2, \cdots, r_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数，并且两两模 m 不同余，则 $r_1, r_2, \cdots, r_{\varphi(m)}$ 是模 m 的一个简化剩余系。

7. Wilson 定理：设 p 是一个素数，则 $(p-1)!\equiv -1 \pmod p$ 。

8. 2007 年 1 月 18 日是星期四，第 $2^{20070118}$ 天是星期 三 。

9. (中国剩余定理) 设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数，则对任意的整数 $b_1, \cdots, b_k$ 同余式组

$$\begin{cases} x\equiv b_1 \pmod{m_1} \\ \cdots\ \cdots\ \cdots\ \cdots \\ x\equiv b_k \pmod{m_k} \end{cases}$$

19

有唯一解。令 $m = m_1 \cdots m_k$，$m = m_i M_i$，$i = 1, \cdots, k$，则同余式组的解为：

$x \equiv M_1' M_1 b_1 + \ldots + M_k' M_k b_k \pmod m$，

其中 $M_i' M_i \equiv 1 \pmod{m_i}$，$i = 1, 2, \ldots, k$。

10．正整数 n 有标准因数分解式为 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，则 n 的欧拉函数

$$\varphi(n) = n\prod_{p|n}(1-\frac{1}{p}) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$$ 。

三．证明题（写出详细证明过程）：（每题 5 分，共 20 分）

1．证明：如果正整数 a，b 满足 $(a, b)=1$，则 $(a^n, b^n)=1$。

证明：(i)由 1.4 节定理 1：若 $(a, c)=1$，

则 $(ab, c) = (b, c)$。从而

$(a^2, b) = (aa, b) = (a, b) = 1$，以此类推

$$(a^n, b) = (aa^{n-1}, b) = (a^{n-1}, b) = (aa^{n-2}, b)$$

$$= (a^{n-2}, b) = \ldots = (a^2, b) = (aa, b) = (a, b) = 1$$

$(b, a^n) = (a^n, b) = 1$，类似的

$$(b^n, a^n) = (bb^{n-1}, a^n) = (b^{n-1}, a^n) = (bb^{n-2}, a^n)$$

$$= (b^{n-2}, a^n) = \ldots = (b^2, a^n) = (bb, a^n) = (b, a^n) = 1$$

2．证明：设 m 是一个正整数，$a \equiv b \pmod m$，则 $(a, m)=(b, m)$。

证 设 $a \equiv b \pmod m$，则存在整数 k 使得 $a = b + mk$，

根据 1.3 定理 3，有 $(a, m) = (b, m)$。

3．设 m 是一个正整数，a 满足 $(a, m)=1$，则存在整数 a'，$1 \le a' < m$ 使得 $aa' \equiv 1 \pmod m$。

证法一：(存在性证明) 因为 $(a, m)=1$，根据定理 3，

x 遍历模 m 的一个最小简化剩余系时，ax 也遍历模 m 的一个简化剩余系。因此，存在整数 $x=a'$，$1\leqslant a'<m$ 使得 aa' 属于 1 的剩余类，

即 $aa'\equiv 1 \pmod m$。

证法二：(构造性证明) 因为$(a, m)=1$，根据 1.3 定理 5，运用广义欧几里得除法，存在整数 s，t 使得

$$sa+tm=(a, m)=1$$

因此，令 $a'=s \pmod m$ 满足

$$(sa+tm)\equiv(aa'+tm)\equiv aa'\equiv 1 \pmod m$$ 。

4. 设 p，q 是两个不同的奇素数，$n=pq$，a 是与 pq 互素的整数。整数 e 和 d 满足$(e, \varphi(n))=1$，$ed\equiv 1 \pmod{\varphi(n)}$，$1<e<\varphi(n)$，$1\leq d<\varphi(n)$。

证明：对任意整数 c，$1\leq c<n$，若 $a^e\equiv c \pmod n$，则有 $c^d\equiv a \pmod n$。

证明　因为$(e, \varphi(n))=1$，根据 2.3 定理 4，存在整数 d，$1\leqslant d<\varphi(n)$，使得

$$ed\equiv 1 \pmod{\varphi(n)}$$

因此，存在一个正整数 k 使得 $ed=1+k\varphi(n)$ 。

现在，根据定理 1，得到

$$a^{\varphi(p)}\equiv 1 \pmod p$$

两端作 $k(\varphi(n)/\varphi(p))$ 次幂，并乘以 a 得到

$$a^{1+k\varphi(n)}\equiv a \pmod p$$

即　$a^{ed}\equiv a \pmod p$

同理，　$a^{ed}\equiv a \pmod q$

因为 p 和 q 是不同的素数，根据 2.1 定理 12，

$$a^{ed}\equiv a \pmod n$$

因此，

$$c^d\equiv(a^e)^d\equiv a \pmod n$$

四．计算题（写出详细计算过程）：（每题 5 分，共 20 分）

1．计算整数 120，150，210，35 的最大公因数和最小公倍数：

[120，150，210，35]和(120，150，210，35)。

解

[120，150，210，35]=4200

(120，150，210，35)=5

2．设 $a=-1859$，$b=1573$，运用广义欧几里得除法

(1) 计算(a, b)； (2) 求整数 s，t 使得 $sa+tb=(a, b)$。

$737=1\cdot635+102$， $102=737-1\cdot635$

$635=6\cdot102+23$， $23=635-6\cdot102$

$102=4\cdot23+10$， $10=102-4\cdot23$

$23=2\cdot10+3$， $3=23-2\cdot10$

$10=3\cdot3+1$， $1=10-3\cdot3$

$1=10-3\cdot3$

$=(102-4\cdot23)-3(23-2\cdot10)$

$=102-7\cdot23+6\cdot10$

$=102-7\cdot23+6(102-4\cdot23)$

$=7\cdot102-31\cdot23$

$=7\cdot102-31\cdot(635-6\cdot103)$

$=193\cdot102-31\cdot635$

$=193\cdot(737-1\cdot635)-31\cdot635$

$=193\cdot\underline{737}-224\cdot\underline{635}$

所以 $s=193$， $t=-224$，使得

$$193\cdot 737+(-224)\cdot 635=1。$$

3．用欧拉定理和模重复平方计算法计算 $2^{1000000}\pmod{77}$。

解法一：　利用 2.4 定理 1 (Euler 定理)及模重复平方计算法直接计算。
因为 $77=7\cdot 11$， $\varphi(77)=\varphi(7)\varphi(11)=60$，所以由 2.4 定理 1 (Euler 定理)，

$$2^{60}\equiv 1\pmod{77}$$

又 $1000000=16666\cdot 60+40$，所以

$$2^{1000000}=(2^{60})^{16666}\cdot 2^{40}\equiv 2^{40}\pmod{77}$$

设 $m=77$， $b=2$，令 $a=1$，将 40 写成二进制，

$$40=2^3+2^5$$

运用模重复平方法，依次计算如下：

(1)　$n_0=0$，计算

$$a_0=a\equiv 1,\ b_1\equiv b^2\equiv 4\pmod{77}$$

(2) $n_1=0$，计算

$$a_1=a_0\equiv 1,\ b_2\equiv b_1^2\equiv 16\pmod{77}$$

(3) $n_2=0$，计算

$$a_2=a_1\equiv 1,\ b_3\equiv b_2^2\equiv 25\pmod{77}$$

(4)　$n_3=1$，计算

$$a_3=a_2\cdot b_3\equiv 25,\quad b_4\equiv b_3^2\equiv 9\pmod{77}$$

(5) $n_4=0$,计算

$$a_4=a_3\equiv 25,\ b_5\equiv b_4^2\equiv 4\pmod{77}$$

(6) $n_5=1$，计算

$$a_5=a_4\cdot b_5\equiv 23\pmod{77}$$

25

最后，计算出

$$2^{1000000} \equiv 23 \pmod{77}$$

解法二： 令 $x = 2^{1000000}$，因为 $77 = 7 \cdot 11$，所以，

计算 $x = 2^{1000000} \pmod{77}$ 等价于求解同余式组

$$x \equiv b_1 \pmod 7$$

$$x \equiv b_2 \pmod{11}$$

因为 Euler 定理给出 $2^{\varphi(7)} \equiv 2^6 \equiv 1 \pmod 7$，

以及 $1000000 = 166666 \cdot 6 + 4$，所以

$b_1 \equiv 2^{1000000} \equiv (2^6)^{166666} \cdot 2^4 \equiv 2 \pmod 7$。

类似地，因为 $2^{\varphi(11)} \equiv 2^{10} \equiv 1 \pmod{11}$，

$1000000 = 100000 \cdot 10$，所以

$b_2 \equiv 2^{1000000} \equiv (2^{10})^{1000000} \equiv 1 \pmod{11}$。

$$x \equiv 2 \pmod 7$$
$$x \equiv 1 \pmod{11}$$

令 $m_1 = 7, m_2 = 11, m = m_1 \cdot m_2 = 77$

$$M_1 = m_2 = 11, M_2 = m_1 = 7$$

分别求解同余式

$M_1' \cdot 11 \equiv 1 \pmod 7$，$M_2' \cdot 7 \equiv 1 \pmod{11}$

得到 $M_1' = 2, M_2' = 8$。

故 $x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23 \pmod{77}$

因此，$2^{100000000} \equiv 23 \pmod{77}$。

信息安全数学基础

注意事项：

1. 请考生按要求在试卷装订线内填写姓名、学号和年级专业。
2. 请仔细阅读各种题目的回答要求，在规定的位置填写答案。
3. 不要在试卷上乱写乱画，不要在装订线内填写无关的内容。
4. 满分 100 分，考试时间为 120 分钟。

题　号	一	二	三	四	五	六	七	八	总 分	统分人
得　分										

得　分	
评分人	

一、设 a, b 是任意两个不全为零的整数，证明：若 m 是任一整数，则 [am, bm]=[a, b]m.（共 10 分）

解：

$$[am,bm]=\frac{abm^2}{(am,bm)} \quad (3分)$$

$$=\frac{abm^2}{(a,b)m} \quad (3分)$$

$$=\frac{abm}{(a,b)} \quad (2分)$$

$$=[a,b]m \quad (2分)$$

得　分	
评分人	

二、设 n=pq，其中 p, q 是素数．证明：如果 $a^2 \equiv b^2 \pmod n, n \nmid a-b, n \nmid a+b$，则 $(n,a-b)>1, (n,a+b)>1$（共 10 分）

证明：由 $a^2 \equiv b^2 \pmod n$，得 $n \mid a^2-b^2$，即 $n \mid (a+b)(a-b)$　　(2分)

又 $n=pq$，则 $pq \mid (a+b)(a-b)$，因为 p 是素数，于是 $p \mid (a+b)$ 或 $p \mid (a-b)$，　(2分)

同理，$q \mid (a+b)$ 或 $q \mid (a-b)$　　(2分)

由于 $n \nmid a-b, n \quad a+b$，所以如果 $p \mid (a+b)$，则 $q \mid (a-b)$，反之亦然.　(2分)

由 $p \mid (a+b)$ 得 $(n,a+b)=p>1$　　(1分)

由 $q \mid (a-b)$ 得 $(n,a-b)=q>1$　　(1分)

得　分	
评分人	

三、求出下列一次同余数的所有解.(共 10 分)

$$3x \equiv 2 \pmod 7$$

解：(1) 求同余式 $3x \equiv 1 \pmod 7$ 的解，运用广义欧几里得除法得：

$x \equiv 5 \pmod 7$　　（5 分）

（2）求同余式 $3x \equiv 2 \pmod 7$ 的一个特解：

$x \equiv 10 \pmod 7$　　（4 分）

（3）写出同余式 $3x \equiv 2 \pmod 7$ 的全部解：

$x \equiv 10 + 2t \pmod 7, t = 0$　　（1 分）

得　分	
评分人	

四、求解同余式组：(共 15 分)

$$\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 6 \\ x \equiv b_3 \pmod 7 \\ x \equiv b_4 \pmod{11} \end{cases}$$

解：令 m=5. 6. 7. 11=2310

$M_1 = 6.7.11 = 462$ (1分)

$M_2 = 5.7.11 = 385$ (1分)

$M_3 = 5.6.11 = 330$ (1分)

$M_4 = 5.6.7 = 210$ (1分)

分别求解同余式 $M_i' M_i \equiv 1 \pmod{m_i}, i = 1,2,3,4$

得到：$M_1' = 3, M_2' = 1, M_3' = 1, M_4' = 1$ (4分)

故同余式的解为：

$x \equiv 3 \cdot 462 \cdot b_1 + 385 \cdot b_2 + 330 \cdot b_3 + 210 \cdot b_4 \pmod{2310}$ (2分)

得　分	
评分人	

五、求满足方程 $E: y^2 = x^3 + 5x + 1 \pmod 7$ 的所有点.(共 10 分)

解:对 x=0, 1, 2, 3, 4, 5, 6, 分别求出 y.

$x=0, y^2\equiv 1(\bmod 7), y\equiv 1,6(\bmod 7)$ （2分）
$x=1, y^2\equiv 0(\bmod 7), y\equiv 0(\bmod 7)$ (2分)
$x=2, y^2\equiv 5(\bmod 7)$, 无解 (1分)
$x=3, y^2\equiv 3(\bmod 7)$, 无解 (1分)
$x=4, y^2\equiv 1(\bmod 7), y\equiv 1,6(\bmod 7)$ (2分)
$x=5, y^2\equiv 4(\bmod 7), y\equiv 2,5(\bmod 7)$ (1分)
$x=6, y^2\equiv 2(\bmod 7), y\equiv 3,4(\bmod 7)$ (1分)

得　分	
评分人	

六、判断同余式 $x^2\equiv 137(\bmod 227)$ 是否有解.（共 15 分）

解:因为 227 是素数，$\left(\frac{137}{227}\right)=\left(\frac{-90}{227}\right)=\left(\frac{-1}{227}\right)\left(\frac{2\cdot 3^2\cdot 5}{227}\right)=-\left(\frac{2}{227}\right)\left(\frac{5}{227}\right)$ （3分）

又 $\left(\frac{2}{227}\right)=(-1)^{\frac{227^2-1}{8}}=(-1)^{\frac{226\cdot 228}{8}}=-1$ （3分）

又 $\left(\frac{5}{227}\right)=(-1)^{\frac{5-1}{2}\frac{227-1}{2}}\left(\frac{227}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1$ （3分）

因此，$\left(\frac{137}{227}\right)=-1$ （3分）

同余式 $x^2\equiv 137(\bmod 227)$ 无解.　(3 分)

得　分	
评分人	

七、设 $m>1$ 是整数，a 是与 m 互素的整数，假如 $ord_m(a)=st$，那么 $ord_m(a^s)=t$.（共 10 分）

解：　由 $ord_m(a)=st$ 得：$a^{st}=(a^s)^t\equiv 1(\bmod m)$（5分）

由 $ord_m(a)=st$ 知，t 是同余式 $(a^s)^t\equiv 1(\bmod m)$ 成立的最小正整数，

故，$ord_m(a^s)=t$.（5 分）

得　分	
评分人	

八、证明整数环 Z 是主理想环．（共 10 分）

证：设 I 是 Z 中的一个非零理想. 当 $a \in I$ 时，有 $0 = 0a \in I$ 及 $-a = (-1)a \in I$．(2 分)

因此，I 中有正整数存在．　(1 分)

设 d 是 I 中的最小正整数，则 $I = (d)$　(1 分)

事实上，对任意 $a \in I$，存在整数 q, r 使得　(1 分)

$$a = dq + r, 0 \le r < d \qquad (1 分)$$

这样，由 $a \in I$ 及 $dq \in I$，得到 $r = a - dq \in I$．　(1 分)

但 $r < d$ 以及 d 是 I 中的最小正整数. 因此，r=0，$a = dq \in (d)$．(1 分)

从而 $I \subset (d)$，(1 分)

又显然 $(d) \subset I$．故 $I = (d)$，故 Z 是主理想．(1 分)

得　分	
评分人	

九、设 p 是素数，则 $P = (p)$ 是整数环 Z 的素理想．（共 10 分）

证：对任意整数 a, b，若 $ab \in P = (p)$, 则 $p \mid ab$．(3 分)

于是 $p \mid a$ 或 $p \mid b$．　(3 分)

因此得到，$a \in P$ 或 $b \in P$．　(3 分)

因此，$P = (p)$ 是整数环 Z 的素理想．(1 分)

信息安全数学基础

注意事项：

1. 请考生按要求在试卷装订线内填写姓名、学号和年级专业。
2. 请仔细阅读各种题目的回答要求，在规定的位置填写答案。
3. 不要在试卷上乱写乱画，不要在装订线内填写无关的内容。
4. 满分 100 分，考试时间为 120 分钟。

题　号	一	二	三	四	五	六	七	八	总 分	统分人
得　分										

得　分	
评分人	

一、设 a, b 是任意两个不全为零的整数，证明：若 m 是任一正整数，则（am, bm）=（a, b）m.（共 10 分）

解：设 $d=(a,b)$, $d_1=(am,bm)$, 由定理 5，存在整数 s, t 使得

$Sa+tb=d$　两端同时乘 m, 得到 $s(am)+t(bm)=dm$ 因此 $d_1|dm$.（5 分）

又显然有 $dm|am$, $dm|bm$, 所以 $dm|d_1$. 故 $d_1=(am,dm)$（5 分）

得　分	
评分人	

二、设 p 是素数. 证明：如果 $a^2\equiv b^2(\mathrm{mod}\ p)$ 则 $p|\ a-b$ 或 $p|\ a+b$（共 10 分）

证明：因为 $a^2\equiv b^2(\mathrm{mod}\ p)$，所以 $p|(a-b)(a+b)$，如果 P 不整除（a+b),因为 P 为素数，所以(P,a+b)=1,有定理可知 $p|\ a-b$（5 分）;

同理，如果 P 不整除（a-b),因为 P 为素数，所以(P,a-b)=1,有定理可知 $p|\ a+b$（5 分）

得　分	
评分人	

三、求出下列一次同余数的所有解.（共 10 分）

$$6x\equiv 3(\mathrm{mod}\,9)$$

解：(1) 求同余式 $6x\equiv 3(\mathrm{mod}\,9)$ 的解，运用广义欧几里得除法得：

$x\equiv 5(\mathrm{mod}\ 3)$　　（5 分）

（2）求同余式 $6x \equiv 3 \pmod 9$ 的一个特解：

$x \equiv 5 \pmod 3$　（4 分）

（3）写出同余式 $6x \equiv 3 \pmod 9$ 的全部解：

$X \equiv 5 + 3t \pmod 9$　$(t=0,1,2)$　（1 分）

得　分	
评分人	

四、求解同余式组：(共 15 分)

$$f(x) \equiv x^4 + 2x^3 + 8x + 9 = 0$$

$$\begin{cases} x = b_1 \pmod 5 \\ x = b_2 \pmod 6 \\ x = b_3 \pmod 7 \\ x = b_4 \pmod{11} \end{cases}$$

解：原同余式等价同余式组 $\begin{cases} f(x) \equiv 0 \pmod 5 \\ f(x) \equiv 0 \pmod 7 \end{cases}$ 直接验算，

$f(x) \equiv 0 \pmod 5$ 的解为 $x \equiv 1, 4 \pmod 5$

$f(x) \equiv 0 \pmod 7$ 的解为 $x \equiv 3, 5, 6 \pmod 7$

由中国剩余定理，可求得同余式组 $\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 7 \end{cases}$ 的解为

$x \equiv 3\square 7\square b_1 + 3\square 5\square b_2 \pmod{35}$，故原同余式的解为 $x \equiv 31, 26, 6, 24, 19, 34 \pmod{35}$，共 6 个。

得　分	
评分人	

五、求满足方程 $E: y^2 = x^3 + 2x + 1 \pmod 7$ 的所有点. (共 10 分)

解：对 x=0, 1, 2, 3, 4, 5, 6, 分别求出 y.

$x = 0, y^2 \equiv 1 \pmod 7, y \equiv 1, 6 \pmod 7$（2分）

$x = 1, y^2 \equiv 4 \pmod 7, y \equiv 2, 5 \pmod 7$（2分）

$x = 2, y^2 \equiv 6 \pmod 7$, 无解 (1分)

$x=3, y^2 \equiv 6 \pmod 7$, 无解 (1分)

$x=4, y^2 \equiv 3 \pmod 7$, 无解 (2分)

$x = 5, y^2 \equiv 3 \pmod 7$, 无解 (1分)

$x = 6, y^2 \equiv 5 \pmod 7$, 无解 (1分)

得　分	
评分人	

六、判断同余式 $x^2 \equiv 286 (\bmod 563)$ 是否有解.（共 15 分）

解:不用考虑 563 是否是素数，直接计算雅可比符号，因为

$$\left(\frac{286}{563}\right)=\left(\frac{2}{563}\right)\left(\frac{143}{563}\right)=(-1)^{\left(\frac{563^2-1}{8}\right)}(-1)^{\frac{143-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{143}\right)=\left(\frac{-9}{143}\right)=\left(\frac{-1}{143}\right)=-1$$

所以原同余式无解

得　分	
评分人	

七、求所有素数 p 使得 5 为模 p 二次剩余。(共 10 分)

解： 即求所有素数 P, st $(\frac{5}{p})$=1, 易知，P 是大于 5 的素数，根据二次互反律 $(\frac{5}{p}) = (-1)^{\frac{p-1}{2}\frac{5-1}{2}}(\frac{p}{5}) = (\frac{5}{p})$ (1 分)

$(\frac{p}{5}) = \{ (\frac{1}{5})=1$ p=1 (mod 5) (2 分)

$\{(\frac{2}{5})=1$ p=2 (mod 5)　(2 分)

$\{(\frac{3}{5})=-1$ p=3 (mod 5)　(2 分)

$\{(\frac{-1}{5})=1$　p= -1(mod 5)　(2 分)

所以 $P\equiv 1$ (mod 5) or $P\equiv -1$ (mod 5) (1 分)

得　分	
评分人	

八、设 p 是一个奇素数，并且 $\frac{p-1}{2}$ 也是一个奇素数，设 a 是与 p 互素的正整数，如果 $a\neq 1$，$a^2\neq 1$，$a^{\frac{p-1}{2}}\neq 1 (\bmod p)$ 则 a 是模 p 的原根。(共 10 分)

证明：即证 a 的指数等于 p-1, 也就是满足 $a^{p-1}\equiv 1$ (mod p)的 p-1 是最小的。(2 分)

假设存在整数 X < p-1, st $a^x\equiv 1$ (mod p) (2 分)

因为 $\frac{p-1}{2}$ 为奇素数，p-1= $\frac{p-1}{2}$ *2(该分解是唯一的)(3 分)

3

因为 $a \neq 1$, $a^{\frac{p-1}{2}} \neq 1 \pmod p$ 所以 x 不存在，即 p-1 为最小。(3 分)

得 分	
评分人	

九、设 p 是素数，则 $P=(p)$ 是整数环 Z 的素理想.（共 10 分）

证：对任意整数 a, b，若 $ab \in P=(p)$,则$p \mid ab$.（3 分）

于是 $p \mid a$或$p \mid b$.（3 分）

因此得到，$a \in P$或$b \in P$.（3 分）

因此，$P=(p)$ 是整数环 Z 的素理想.（1 分）

2014年信息安全数学基础期末考试试题

1 证明：如果a是整数，则a^3-a能被3整除。

2 用广义欧几里德算法求最大公因子$(4655,12075)$

3 设m是一个正整数，$a\equiv b(\bmod m)$，如果$d\mid m$，证明：$a\equiv b(\bmod d)$。

4 解方程$987x\equiv 610(\bmod 2668)$

5 解方程组$\begin{cases} x\equiv 2(\bmod 3) \\ x\equiv 1(\bmod 5) \\ x\equiv 1(\bmod 7) \end{cases}$

6 计算3模19的指数。

7、计算$\left(\frac{6}{53}\right)$的 Legendre 符号

8 证明：91 是对基 3 的拟素数。

9 设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$G$的子群。

10 设a是群G的一个元素。证明：映射$\sigma: x\to axa^{-1}$是G到自身的自同构。

2014年信息安全数学基础期末考试试题

答案

1 证明：因为 $a^3-a=(a-1)a(a+1)$

当 $a=3k$，$k\in Z$　$3|a$　则 $3|a^3-a$

当 $a=3k-1$，$k\in Z$　$3|a+1$　则 $3|a^3-a$

当 $a=3k+1$，$k\in Z$　$3|a-1$　则 $3|a^3-a$

所以 a^3-a 能被 3 整除。

2. $12075=2*4655+2765$

$4655=1*2765+1890$

$2765=1*1890+875$

$1890=2*875+140$

$875=6*140+35$

$140=4*35$

所以 $(4655,12075)=35$

3. 因为 d|m，所以存在整数 m' 使得 $m=dm'$。又因为 $a\equiv b(\bmod m)$，所以存在整数 k 使得 $a=b+mk$。该式又可以写成 $a=b+d(m'k)$。故 $a\equiv b(\bmod d)$。

4. $987x\equiv 610(\bmod 2668)$

计算最大公因式(987,2668)=1，所以原同余式有解且只有一个解。利用广义欧几里德除法，求同余式 $987x\equiv 1(\bmod 2668)$ 的解为 $x_0'=2495(\bmod 2668)$。再写出同余式 $987x\equiv 610(\bmod 2668)$ 的解为 $x_0=610*x_0'=610*2495\equiv 1190(\bmod 2668)$。

5 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 $M_i'M_i\equiv 1(\bmod m_i)$　（i=1,2,3）

得到 $M_1'=2$，$M_2'=1$，$M_3'=1$。故同余式的解为

$$\begin{aligned} x &\equiv M_1'M_1*2+M_2'M_2*1+M_3'M_3*1(\bmod 105) \\ &\equiv 2*35*2+1*21*1+1*15*1(\bmod 105) \\ &\equiv 71(\bmod 105) \end{aligned}$$

6 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(mod12)

因为$3^1\equiv3$，$3^2\equiv9$，$3^3\equiv8$，$3^6\equiv7$，$3^9\equiv-1$，$2^{18}\equiv1$(mod13)

所以3模19的指数为18；

7

$$\left(\frac{6}{53}\right)=\left(\frac{2}{53}\right)\left(\frac{3}{53}\right)$$

$$=(-1)^{(53^2-1)/8}\cdot(-1)^{(3-1)(53-1)/4}\left(\frac{53}{3}\right)$$

$$=-1\cdot1\cdot\left(\frac{2}{3}\right)=-1\cdot(-1)^{(3^2-1)/8}=1$$

8 证明：因为91=13*7是奇合数，　　(3, 91)=1

又$3^6=729\equiv1$(mod91)　　则$3^{91-1}=3^{90}\equiv(3^6)^{15}\equiv1$(mod91)

则91是对于基3的拟素数。

9 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，$ab^{-1}\in\ker f$，$\ker f$是群G的子群。

10 证明：（1）任取$x,y\in G$。计算

$$\sigma(xy)=a(xy)a^{-1}=axeya^{-1}=axa^{-1}aya^{-1}=\sigma(x)\sigma(y)$$

因此σ是同态映射。

（2）若$x,y\in G$，且$\sigma(x)=\sigma(y)$。那么$axa^{-1}=aya^{-1}$，从而

$$x=a^{-1}axa^{-1}a=a^{-1}aya^{-1}a=y，$$

因此σ是单射。

（3）任取$c\in G$。由于$\sigma(a^{-1}ca)=a(a^{-1}ca)a^{-1}=ece=c$，故$\sigma$是满射。

综上所述，映射$\sigma:x\to axa^{-1}$是G到自身的自同构。