二学期 信息安全数学基础

上海交通大学试卷（A卷）

3.5元 05-09年（2008至2009学年 第2学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（II） 成绩 _____

一. (30分) 设 $f(x) = x^6 + x^5 + x^2 + x + 1$.

i) 证明： $f(x)$ 是 F_2 上的不可约多项式.

ii) 证明：由 $f(x)$ 生成的理想 $I = (f(x))$ 是 $\mathrm{F}_2[x]$ 中的极大理想.

iii) 证明：由理想 $I = (f(x))$ 生成的商环 $\mathrm{F}_{2^6} = \mathrm{F}_2[x]/(f(x))$ 是 2^6 元有限域.

iv) 求有限域 $\mathrm{F}_{2^6} = \mathrm{F}_2[x]/(f(x))$ 的生成元 g. 即 F_{2^6} 中元素 g 使得

$$\mathrm{F}_{2^6}^* = \mathrm{F}_{2^6} \setminus \{0\} = \ < g > \ = \{g,\ g^2,\ \ldots,\ g^{2^6-2},\ g^{2^6-1} = 1\}.$$

二. (40分) 设 $f(x) = x^8 + x^4 + x^3 + x^2 + 1$ 是 F_2 上的不可约多项式，有限域 $\mathrm{F}_{2^8} = \mathrm{F}_2[x]/(f(x))$.

i) 证明： Frobenius 映射 $\sigma : u \longmapsto u^2$ 是 F_{2^8} 的自同构.

ii) 设 $g = x$ 是 F_{2^8} 的生成元， $g_1 = g^{85} = x^7 + x^6 + x^4 + x^2 + x$. 计算 $g_2 = g_1^2$, $g_3 = g_1^{2^2}$.

iii) 证明 $\mathrm{K} = \{0,\ 1,\ g_1,\ g_2\}$ 是 F_{2^8} 的子域.

iv) 求 g_1 的定义多项式.

v) 求 F_{2^8} 的 Galois 群 $G = Aut_{\mathrm{F}_2}\mathrm{F}_{2^8}$ 的子群 H 使得 H 的不变域 $I(H) = \mathrm{K}$

三. (10 分) 设 $f(x)=x^6+x^5+x^2+x+1$. 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的一组正规基底.

我承诺，我将严格遵守考试纪律.

承诺人：_____

题号										
得分										
批阅人 (流水阅卷教师签名处)										

四. (10 分) 设域 $\mathbf{F}_p$ $(p>3)$ 上椭圆曲线 E: $y^2=x^3+a_4x+a_6$.
E 在 $\mathbf{F}_p$ 上的运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$,
O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,-y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$, 则

$$\begin{cases} x_3=\lambda^2-x_1-x_2, \\ y_3=\lambda(x_1-x_3)-y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1} & \text{如果 } x_1\neq x_2, \\ \dfrac{3x_1^2+a_4}{2y_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{17}$ 上椭圆曲线 E: $y^2=x^3+3x+10$ 上的点 $P=(13,11)$.
求 $2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $-P=(x_4,y_4)$.

五. (10 分) 设域 $\mathbf{F}_{2^n}$ 上椭圆曲线 E: $y^2+xy=x^3+a_2x^2+a_6$.

五. (10 分) 设域 $\mathbf{F}_{2^n}$ 上椭圆曲线 E: $y^2+xy=x^3+a_2x^2+a_6$.
E 在 $\mathbf{F}_{2^n}$ 上运算规则为: 设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$,
O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,x_1+y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$,

$$\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a_2, \\ y_3=\lambda(x_1+x_3)+x_3+y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2+y_1}{x_2+x_1} & \text{如果 } x_1\neq x_2, \\ \dfrac{x_1^2+y_1}{x_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{2^8}=\mathbf{F}_2[t]/(t^8+t^4+t^3+t^2+1)$ 上椭圆曲线 E: $y^2+xy=x^3+x^2+1$.
设 $P_1=(t^6+t^2,\ t^3+t)$. 试证明 P_1 是 E 的一个点,
并计算 $-P_1$, $2P_1$, $3P_1$.

上 海 交 通 大 学 试 卷（B卷）

（2008至2009学年 第2学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（II） 成绩 _____

一. (30分) 设 $f(x) = x^6 + x^5 + x^4 + x^2 + 1$.

i) 证明： $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

ii) 证明：由 $f(x)$ 生成的理想 $I = (f(x))$ 是 $\mathbf{F}_2$[x] 中的极大理想.

iii) 证明：由理想 $I = (f(x))$ 生成的商环 $\mathbf{F}_{2^6} = \mathbf{F}_2[x]/(f(x))$ 是 2^6 元有限域.

iv) 求有限域 $\mathbf{F}_{2^6} = \mathbf{F}_2[x]/(f(x))$ 的生成元 g. 即 $\mathbf{F}_{2^6}$ 中元素 g 使得

$$\mathbf{F}_{2^6}^* = \mathbf{F}_{2^6} \setminus \{0\} = \ < g > \ = \{g,\ g^2,\ \ldots,\ g^{2^6-2},\ g^{2^6-1} = 1\}.$$

二. (40分) 设 $f(x) = x^8 + x^4 + x^3 + x + 1$ 是 $\mathbf{F}_2$ 上的不可约多项式，有限域 $\mathbf{F}_{2^8} = \mathbf{F}_2[x]/(f(x))$.

i) 证明： Frobenius 映射 $\sigma : u \longmapsto u^2$ 是 $\mathbf{F}_{2^8}$ 的自同构.

ii) 设 $g = x$ 是 $\mathbf{F}_{2^8}$ 的生成元， $g_1 = g^{85} = x^7 + x^5 + x^4 + x^3 + x^2 + 1$. 计算 $g_2 = g_1^2,\ g_3 = g_1^{2^2}$.

iii) 证明 $\mathrm{K} = \{0,\ 1,\ g_1,\ g_2\}$ 是 $\mathbf{F}_{2^8}$ 的子域.

iv) 求 g_1 的定义多项式.

v) 求 $\mathbf{F}_{2^8}$ 的 Galois 群 $G = Aut_{\mathbf{F}_2}\mathbf{F}_{2^8}$ 的子群 H 使得 H 的不变域 $I(H) = \mathrm{K}$.

三. (10分) 设 $f(x)=x^6+x^5+x^4+x^2+1$. 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的一组正规基底.

我承诺，我将严格遵守考试纪律.

承诺人：_____

题号										
得分										
批阅人 (流水阅卷教师签名处)										

四. (10 分) 设域 $\mathbf{F}_p$ $(p>3)$ 上椭圆曲线 $E:\ y^2=x^3+a_4x+a_6$.

E 在 $\mathbf{F}_p$ 上的运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$, O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,-y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$, 则

$$\begin{cases} x_3=\lambda^2-x_1-x_2, \\ \\ y_3=\lambda(x_1-x_3)-y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1} & \text{如果 } x_1\neq x_2, \\ \\ \dfrac{3x_1^2+a_4}{2y_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{17}$ 上椭圆曲线 $E:\ y^2=x^3+5x+7$ 上的点 $P=(13,5)$.

求 $2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $-P=(x_4,y_4)$.

五. (10 分) 设域 $\mathbf{F}_{2^n}$ 上椭圆曲线 E: $y^2+xy=x^3+a_2x^2+a_6$.
E 在 $\mathbf{F}_{2^n}$ 上运算规则为: 设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$,
O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,x_1+y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$,

$$\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a_2, \\ \\ y_3=\lambda(x_1+x_3)+x_3+y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2+y_1}{x_2+x_1} & \text{如果 } x_1\neq x_2, \\ \\ \dfrac{x_1^2+y_1}{x_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{2^8}=\mathbf{F}_2[t]/(t^8+t^4+t^3+t^2+1)$ 上椭圆曲线 E: $y^2+xy=x^3+x^2+1$.
设 $P_1=(t^3+t,\ t^7+t^4+t)$. 试证明 P_1 是 E 的一个点,
并计算 $-P_1$, $2P_1$, $3P_1$.

上 海 交 通 大 学 试 卷解答（A卷）

（2008至2009学年 第2学期）

信息安全数学基础（II）

一. (30分) 设 $f(x)=x^6+x^5+x^2+x+1$.

i) 证明： $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

ii) 证明：由 $f(x)$ 生成的理想 $I=(f(x))$ 是 $\mathbf{F}_2$[x] 中的极大理想.

iii) 证明：由理想 $I=(f(x))$ 生成的商环 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 是 2^6 元有限域.

iv) 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的生成元 g. 即 $\mathbf{F}_{2^6}$ 中元素 g 使得

$$\mathbf{F}_{2^6}^*=\mathbf{F}_{2^6}\setminus\{0\}=\ <g>\ =\{g,\ g^2,\ \ldots,\ g^{2^6-2},\ g^{2^6-1}=1\}.$$

解 i) $\mathbf{F}_2$ 次数小于 $n/2=6/2$ 的不可约多项式为

$x,\ x+1, x^2+x+1,\ x^3+x+1,\ x^3+x^2+1$

因为

$$\begin{aligned} f(x) &= x(x^5+x^4+x+1)+1\\ f(x) &= (x+1)(x^5+x)+1\\ f(x) &= (x^2+x+1)(x^4+x^2+x+1)+x\\ f(x) &= (x^3+x+1)(x^3+x^2+x)+x^2+1\\ f(x) &= (x^3+x^2+1)(x^3+1)+x \end{aligned}$$

所以 $x\nmid f(x)$, $x+1\nmid f(x), x^2+x+1\nmid f(x)$, $x^3+x+1\nmid f(x)$, $x^3+x^2+1\nmid f(x)$. 因此， $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

ii) 设有理想 M 真包含理想 $I=(f(x))$, 则存在 $g(x)\in M$, 但 $g(x)\notin I$. 由此， $f(x)\nmid g(x)$, 进而 $(g(x),f(x))=1$. 根据多项式的广义欧几里得除法，存在多项式 $s(x),t(x)\in\mathbf{F}_2[x]$, 使得

$$s(x)g(x)+t(x)f(x)=1.$$

根据理想的定义，以及 $g(x),f(x)\in M$, 我们有

$$1=s(x)g(x)+t(x)f(x)\in M.$$

从而， $M=\mathbf{F}_2[x]$. 这说明 $f(x)$ 生成的理想 $I=(f(x))$ 是 $\mathbf{F}_2$[x] 中的极大理想.

iii) 因为由理想 $I=(f(x))$ 生成的商环 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 对于如下运算：

$$\begin{aligned} a(x)\oplus b(x) &:= (a(x)+b(x)) \bmod f(x)\\ a(x)\otimes b(x) &:= (a(x)b(x)) \bmod f(x) \end{aligned}$$

构成一个域，且 $1,x,x^2,x^3,x^4,x^5$ 是一组基底，所以 $\mathbf{F}_{2^6}$ 是 2^6 元有限域.

iv) $2^6-1=63=3^2\cdot 7$. 有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的元素 g 满足条件

$$\begin{cases} g(x)^{(2^6-1)/3} \neq 1 \bmod f(x)\\ g(x)^{(2^6-1)/7} \neq 1 \bmod f(x) \end{cases}$$

即为生成元.

取 $g=x$, 有

$$\begin{cases} g(x)^{(2^6-1)/3} & \equiv & x^5+x^3+x^2 \neq 1 \bmod f(x) \\ g(x)^{(2^6-1)/7} & \equiv & x^3+x^2+1 \neq 1 \bmod f(x) \end{cases}$$

因此, $g=x$ 为生成元.

二. (40 分) 设 $f(x)=x^8+x^4+x^3+x^2+1$ 是 $\mathbf{F}_2$ 上的不可约多项式, 有限域 $\mathbf{F}_{2^8}=\mathbf{F}_2[x]/(f(x))$.

i) 证明: Frobenius 映射 $\sigma: u \longmapsto u^2$ 是 $\mathbf{F}_{2^8}$ 的自同构.

ii) 设 $g=x$ 是 $\mathbf{F}_{2^8}$ 的生成元, $g_1=g^{85}=x^7+x^6+x^4+x^2+x$. 计算 $g_2=g_1^2$, $g_3=g_1^{2^2}$.

iii) 证明 $\mathbf{K}=\{0,\ 1,\ g_1,\ g_2\}$ 是 $\mathbf{F}_{2^8}$ 的子域.

iv) 求 g_1 的定义多项式.

v) 求 $\mathbf{F}_{2^8}$ 的 Galois 群 $G=Aut_{\mathbf{F}_2}\mathbf{F}_{2^8}$ 的子群 H 使得 H 的不变域 $I(H)=\mathbf{K}$.

解 i) 证明: Frobenius 映射 $\sigma: u \longmapsto u^2$ 是 $\mathbf{F}_{2^8}$ 的自同构.

首先证明: σ 是自同态. 事实上, 对任意元素 $a,b \in \mathbf{F}_{2^8}$, 有

$\sigma(a+b)=(a+b)^2=a^2+2ab+b^2=a^2+b^2=\sigma(a)+\sigma(b)$

$\sigma(a+b)=(ab)^2=(ab)^2=a^2\cdot b^2=\sigma(a)\sigma(b)$.

其次证明: σ 是单射. 事实上, $\ker\sigma=\{u|u^2=0\}=\{0\}$.

最后, $\mathbf{F}_{2^8}$ 是有限元集. σ 也是满射. 因此, Frobenius 映射 $\sigma: u \longmapsto u^2$ 是 $\mathbf{F}_{2^8}$ 的自同构.

ii) 设 $g=x$ 是 $\mathbf{F}_{2^8}$ 的生成元, $g_1=g^{85}=x^7+x^6+x^4+x^2+x$. 我们有

$$\begin{aligned} g_2=g_1^2 &\equiv x^{14}+x^{12}+x^8+x^4+x^2 \\ &\equiv x^7+x^6+x^4+x^2+x+1 \bmod f(x) \\ g_3=g_2^2 &\equiv x^{14}+x^{12}+x^8+x^4+x^2+1 \\ &\equiv x^7+x^6+x^4+x^2+x \\ &\equiv g_1 \mod f(x) \end{aligned}$$

iii) 因为 $1+g_1=g_2$, $1+g_2=g_1$, $g_1^2=g_2$, $g_2^2=g_1$, $g_1\cdot g_2=1$, 所以 $\mathbf{K}=\{0,\ 1,\ g_1,\ g_2\}$ 是 $\mathbf{F}_{2^8}$ 的子域.

iv) g_1 的定义多项式为

$h(y)=(y-g_1)(y-g_2)=y^2-(g_1+g_2)y+g_1g_2=y^2+y+1$.

v) 求 $\mathbf{F}_{2^8}$ 的 Galois 群 $G=Aut_{\mathbf{F}_2}\mathbf{F}_{2^8}$ 的子群 H 使得 H 的不变域 $I(H)=\mathbf{K}$.

$$\begin{aligned} H=A(\mathbf{K}) &= \{\sigma^d \in G \mid \sigma^d(g_1)=g_1\} \\ &= \{\sigma^d \in G \mid (g^{85})^{2^d}=g^{85}\} \\ &= \{\sigma^d \in G \mid 2^8-1 | 85(2^d-1)\} \\ &= \{\sigma^2, \sigma^4, \sigma^6, \sigma^8=e\} \end{aligned}$$

三. (10 分) 设 $f(x)=x^6+x^5+x^2+x+1$. 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的一组正规基底.

解 有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的一组正规基底为 $\beta, \beta^2, \beta^{2^2}, \beta^{2^3}, \beta^{2^4}, \beta^{2^5}$.

取 $\beta=x$, 有

$$
\begin{aligned}
\beta &\equiv x,\\
\beta^2 &\equiv x^2,\\
\beta^{2^2} &\equiv x^4,\\
\beta^{2^3} &\equiv x^5+x^4+x^2+1,\\
\beta^{2^4} &\equiv x^5+x^4+x^3+x^2+x,\\
\beta^{2^5} &\equiv x^4+x^3+x^2.
\end{aligned}
$$

系数矩阵为

$$
A=\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0\\
1 & 0 & 1 & 0 & 1 & 1\\
0 & 1 & 1 & 1 & 1 & 1\\
0 & 0 & 1 & 1 & 1 & 0
\end{pmatrix}
$$

为可逆矩阵，所以 $\beta,\beta^2,\beta^{2^2},\beta^{2^3},\beta^{2^4},\beta^{2^5}$ 是正规基底.

四. (10 分) 设域 $\mathbf{F}_p$ $(p>3)$ 上椭圆曲线 E: $y^2=x^3+a_4x+a_6$.
E 在 $\mathbf{F}_p$ 上的运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$,
O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,-y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$, 则

$$
\begin{cases} x_3=\lambda^2-x_1-x_2,\\ y_3=\lambda(x_1-x_3)-y_1. \end{cases}
\quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1} & \text{如果 } x_1\neq x_2,\\ \dfrac{3x_1^2+a_4}{2y_1} & \text{如果 } x_1=x_2. \end{cases}
$$

设 $\mathbf{F}_{17}$ 上椭圆曲线 E: $y^2=x^3+3x+10$ 上的点 $P=(13,11)$.
求 $2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $-P=(x_4,y_4)$.

解 i) 设 $x_1=13,y_1=11$, 我们有

$$x_1^3+3x_1+10\equiv 2,\quad y_1^2\equiv 2 \bmod 17$$

所以 $P=(x_1,y_1)$ 是 E 上的点.

ii)
$$
\begin{cases}
\lambda_2 = \dfrac{3x_1^2+3}{2y_1}=0\\
x_2 = \lambda_2^2-2x_1=8\\
y_2 = \lambda_2(x_1-x_2)-y_1=6
\end{cases}
$$

iii)
$$
\begin{cases}
\lambda_3 = \dfrac{y_2-y_1}{x_2-x_1}=1\\
x_3 = \lambda_3^2-x_1-x_2=14\\
y_3 = \lambda_3(x_1-x_3)-y_1=5
\end{cases}
$$

iv) $(x_4,y_4)=-P=(x_1,-y_1)=(13,-11)=(13,6)$.

五. (10 分) 设域 $\mathbf{F}_{2^n}$ 上椭圆曲线 E: $y^2+xy=x^3+a_2x^2+a_6$.
E 在 $\mathbf{F}_{2^n}$ 上运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$,
O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,x_1+y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$,

$$\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a_2, \\ y_3=\lambda(x_1+x_3)+x_3+y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2+y_1}{x_2+x_1} & \text{如果 } x_1\neq x_2, \\ \dfrac{x_1^2+y_1}{x_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathrm{F}_{2^8}=\mathrm{F}_2[t]/(t^8+t^4+t^3+t^2+1)$ 上椭圆曲线 E: $y^2+xy=x^3+x^2+1$.

设 $P_1=(t^6+t^2,\ t^3+t)$. 试证明 P_1 是 E 的一个点,

并计算 $-P_1,\ 2P_1,\ 3P_1$.

解 i) 设 $p(t)=t^8+t^4+t^3+t^2+1$, $x_1=t^6+t^2, y_1=t^3+t$, 我们有

$$x_1^3+x_1^2+1\equiv t^7+t^6+t^4+t^2+t,\ \ y_1^2+x_1\cdot y_1\equiv t^7+t^6+t^4+t^2+t \bmod p(t)$$

所以 $P=(x_1,y_1)$ 是 E 上的点.

ii) $(x_4,y_4)=-P=(x_1,x_1+y_1)=(t^6+t^2,t^6+t^2+t^3+t)=(t^6+t^2,t^6+t^3+t^2+t)$.

iii)
$$\begin{cases} \lambda_2 &= \dfrac{x_1^2+y_1}{x_1}=t^7+t^4+t^3+1 \\ x_2 &= \lambda_2^2+\lambda_2+x_1+x_1+1=t^7+t^6+t^4+t^2+t+1 \\ y_2 &= \lambda_2(x_1+x_2)+x_2+y_1=1 \end{cases}$$

iv)
$$\begin{cases} \lambda_3 &= \dfrac{y_2+y_1}{x_2+x_1}=t^7+t^4+t+1 \\ x_3 &= \lambda_3^2+\lambda_3+x_1+x_2+1=t^3+t \\ y_3 &= \lambda_3(x_1+x_3)+x_3+y_1=t^7+t^4+t \end{cases}$$

上 海 交 通 大 学 试 卷解答（B卷）

（2008至2009学年 第2学期）

信息安全数学基础（II）

一. (30分) 设 $f(x)=x^6+x^5+x^4+x^2+1$.

i) 证明： $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

ii) 证明：由 $f(x)$ 生成的理想 $I=(f(x))$ 是 $\mathbf{F}_2$[x] 中的极大理想.

iii) 证明：由理想 $I=(f(x))$ 生成的商环 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 是 2^6 元有限域.

iv) 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的生成元 g. 即 $\mathbf{F}_{2^6}$ 中元素 g 使得

$$\mathbf{F}_{2^6}^*=\mathbf{F}_{2^6}\setminus\{0\}=\ <g>\ =\{g,\ g^2,\ \ldots,\ g^{2^6-2},\ g^{2^6-1}=1\}.$$

解 i) $\mathbf{F}_2$ 次数小于 $n/2=6/2$ 的不可约多项式为

$x,\ x+1, x^2+x+1,\ x^3+x+1,\ x^3+x^2+1$

因为

$$\begin{aligned} f(x) &= x(x^5+x^4+x^3+x)+1\\ f(x) &= (x+1)(x^5+x^3+x^2)+1\\ f(x) &= (x^2+x+1)(x^4+1)+x\\ f(x) &= (x^3+x+1)(x^3+x^2)+1\\ f(x) &= (x^3+x^2+1)(x^3+x)+x^2+x+1 \end{aligned}$$

所以 $x\not| f(x),\ x+1\not| f(x), x^2+x+1\not| f(x),\ x^3+x+1\not| f(x),\ x^3+x^2+1\not| f(x)$. 因此， $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

ii) 设有理想 M 真包含理想 $I=(f(x))$, 则存在 $g(x)\in M$, 但 $g(x)\notin I$. 由此， $f(x)\not| g(x)$, 进而 $(g(x),f(x))=1$. 根据多项式的广义欧几里得除法，存在多项式 $s(x),t(x)\in\mathbf{F}_2[x]$, 使得

$$s(x)g(x)+t(x)f(x)=1.$$

根据理想的定义，以及 $g(x),f(x)\in M$, 我们有

$$1=s(x)g(x)+t(x)f(x)\in M.$$

从而， $M=\mathbf{F}_2[x]$. 这说明 $f(x)$ 生成的理想 $I=(f(x))$ 是 $\mathbf{F}_2$[x] 中的极大理想.

iii) 因为由理想 $I=(f(x))$ 生成的商环 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 对于如下运算：

$$\begin{aligned} a(x)\oplus b(x) &:= (a(x)+b(x)) \bmod f(x)\\ a(x)\otimes b(x) &:= (a(x)b(x)) \bmod f(x) \end{aligned}$$

构成一个域，且 $1,x,x^2,x^3,x^4,x^5$ 是一组基底，所以 $\mathbf{F}_{2^6}$ 是 2^6 元有限域.

iv) $2^6-1=63=3^2\cdot 7$. 有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的元素 g 满足条件

$$\begin{cases} g(x)^{(2^6-1)/3} \neq 1 \bmod f(x)\\ g(x)^{(2^6-1)/7} \neq 1 \bmod f(x) \end{cases}$$

即为生成元.

取 $g=x$, 有

$$\begin{cases} g(x)^{(2^6-1)/3} & \equiv & x^4+x^3+x^2+x+1 \neq 1 \bmod f(x) \\ g(x)^{(2^6-1)/7} & \equiv & x^5+x^4+x^2 \neq 1 \bmod f(x) \end{cases}$$

因此, $g=x$ 为生成元.

二. (40 分) 设 $f(x)=x^8+x^4+x^3+x+1$ 是 $\mathbf{F}_2$ 上的不可约多项式, 有限域 $\mathbf{F}_{2^8}=\mathbf{F}_2[x]/(f(x))$.

i) 证明: Frobenius 映射 $\sigma: u \longmapsto u^2$ 是 $\mathbf{F}_{2^8}$ 的自同构.

ii) 设 $g=x+1$ 是 $\mathbf{F}_{2^8}$ 的生成元, $g_1=g^{85}=x^7+x^5+x^4+x^3+x^2+1$.
计算 $g_2=g_1^2$, $g_3=g_1^{2^2}$.

iii) 证明 $\mathrm{K}=\{0,\ 1,\ g_1,\ g_2\}$ 是 $\mathbf{F}_{2^8}$ 的子域.

iv) 求 g_1 的定义多项式.

v) 求 $\mathbf{F}_{2^8}$ 的 Galois 群 $G=Aut_{\mathbf{F}_2}\mathbf{F}_{2^8}$ 的子群 H 使得 H 的不变域 $I(H)=\mathrm{K}$.

解 i) 证明: Frobenius 映射 $\sigma: u \longmapsto u^2$ 是 $\mathbf{F}_{2^8}$ 的自同构.

首先证明: σ 是自同态. 事实上, 对任意元素 $a,b \in \mathbf{F}_{2^8}$, 有

$\sigma(a+b)=(a+b)^2=a^2+2ab+b^2=a^2+b^2=\sigma(a)+\sigma(b)$

$\sigma(a+b)=(ab)^2=(ab)^2=a^2\cdot b^2=\sigma(a)\sigma(b)$.

其次证明: σ 是单射. 事实上, $\ker\sigma=\{u|u^2=0\}=\{0\}$.

最后, $\mathbf{F}_{2^8}$ 是有限元集. σ 也是满射. 因此, Frobenius 映射 $\sigma: u \longmapsto u^2$ 是 $\mathbf{F}_{2^8}$ 的自同构.

ii) 设 $g=x$ 是 $\mathbf{F}_{2^8}$ 的生成元, $g_1=g^{85}=x^7+x^5+x^4+x^3+x^2+1$. 我们有

$$\begin{aligned} g_2=g_1^2 &\equiv x^{14}+x^{10}+x^8+x^6+x^4+1 \\ &\equiv x^7+x^5+x^4+x^3+x^2 \bmod f(x) \\ g_3=g_2^2 &\equiv x^{14}+x^{10}+x^8+x^6+x^4 \\ &\equiv x^7+x^5+x^4+x^3+x^2+1 \\ &\equiv g_1 \mod f(x) \end{aligned}$$

iii) 因为 $1+g_1=g_2$, $1+g_2=g_1$, $g_1^2=g_2$, $g_2^2=g_1$, $g_1\cdot g_2=1$, 所以 $\mathrm{K}=\{0,\ 1,\ g_1,\ g_2\}$ 是 $\mathbf{F}_{2^8}$ 的子域.

iv) g_1 的定义多项式为

$h(y)=(y-g_1)(y-g_2)=y^2-(g_1+g_2)y+g_1g_2=y^2+y+1$.

v) 求 $\mathbf{F}_{2^8}$ 的 Galois 群 $G=Aut_{\mathbf{F}_2}\mathbf{F}_{2^8}$ 的子群 H 使得 H 的不变域 $I(H)=\mathrm{K}$.

$$\begin{aligned} H=A(\mathrm{K}) &= \{\sigma^d \in G \mid \sigma^d(g_1)=g_1\} \\ &= \{\sigma^d \in G \mid (g^{85})^{2^d}=g^{85}\} \\ &= \{\sigma^d \in G \mid 2^8-1 | 85(2^d-1)\} \\ &= \{\sigma^2, \sigma^4, \sigma^6, \sigma^8=e\} \end{aligned}$$

三. (10 分) 设 $f(x)=x^6+x^5+x^4+x^2+1$. 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的一组正规基底.

解 有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的一组正规基底为 $\beta, \beta^2, \beta^{2^2}, \beta^{2^3}, \beta^{2^4}, \beta^{2^5}$.

取 $\beta=x$, 有

$$
\begin{aligned}
\beta &\equiv x,\\
\beta^2 &\equiv x^2,\\
\beta^{2^2} &\equiv x^4,\\
\beta^{2^3} &\equiv x^5+x^4+x^3+x^2+x,\\
\beta^{2^4} &\equiv x^3+x^2+1,\\
\beta^{2^5} &\equiv x^5+x^2.
\end{aligned}
$$

系数矩阵为

$$
A=\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0\\
0 & 1 & 1 & 1 & 1 & 1\\
1 & 0 & 1 & 1 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 1
\end{pmatrix}.
$$

为可逆矩阵，所以 $\beta,\beta^2,\beta^{2^2},\beta^{2^3},\beta^{2^4},\beta^{2^5}$ 是正规基底.

四. (10 分) 设域 $\mathbf{F}_p$ $(p>3)$ 上椭圆曲线 E: $y^2=x^3+a_4x+a_6$.

E 在 $\mathbf{F}_p$ 上的运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$,

O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,-y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$, 则

$$
\begin{cases}
x_3=\lambda^2-x_1-x_2,\\
\\
y_3=\lambda(x_1-x_3)-y_1.
\end{cases}
\qquad \text{其中 } \lambda=\begin{cases}
\dfrac{y_2-y_1}{x_2-x_1} & \text{如果 } x_1\neq x_2,\\
\\
\dfrac{3x_1^2+a_4}{2y_1} & \text{如果 } x_1=x_2.
\end{cases}
$$

设 $\mathbf{F}_{17}$ 上椭圆曲线 E: $y^2=x^3+5x+7$ 上的点 $P=(13,5)$.

求 $2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $-P=(x_4,y_4)$.

解 i) 设 $x_1=13, y_1=5$, 我们有

$$
x_1^3+5x_1+7\equiv 8,\quad y_1^2\equiv 8 \bmod 17
$$

所以 $P=(x_1,y_1)$ 是 E 上的点.

ii)
$$
\begin{cases}
\lambda_2 &= \dfrac{3x_1^2+3}{2y_1}=7\\
x_2 &= \lambda_2^2-2x_1=6\\
y_2 &= \lambda_2(x_1-x_2)-y_1=10
\end{cases}
$$

iii)
$$
\begin{cases}
\lambda_3 &= \dfrac{y_2-y_1}{x_2-x_1}=9\\
x_3 &= \lambda_3^2-x_1-x_2=11\\
y_3 &= \lambda_3(x_1-x_3)-y_1=13
\end{cases}
$$

iv) $(x_4,y_4)=-P=(x_1,-y_1)=(13,-11)=(13,6)$.

五. (10 分) 设域 $\mathbf{F}_{2^n}$ 上椭圆曲线 E: $y^2+xy=x^3+a_2x^2+a_6$.

E 在 $\mathbf{F}_{2^n}$ 上运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$,

O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,x_1+y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$,

$$\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a_2, \\ y_3=\lambda(x_1+x_3)+x_3+y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2+y_1}{x_2+x_1} & \text{如果 } x_1\neq x_2, \\ \dfrac{x_1^2+y_1}{x_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathrm{F}_{2^8}=\mathrm{F}_2[t]/(t^8+t^4+t^3+t^2+1)$ 上椭圆曲线 $E:\ y^2+xy=x^3+x^2+1$.

设 $P_1=(t^3+t,\ t^7+t^4+t)$. 试证明 P_1 是 E 的一个点,

并计算 $-P_1,\ 2P_1,\ 3P_1$.

解 i) 设 $p(t)=t^8+t^4+t^3+t^2+1$, $x_1=t^3+t, y_1=t^7+t^4+t$, 我们有

$$x_1^3+x_1^2+1\equiv t^7+t^6+t^4+t^2+t+1,\ \ y_1^2+x_1\cdot y_1\equiv t^7+t^6+t^4+t^2+t+1 \bmod p(t)$$

所以 $P=(x_1,y_1)$ 是 E 上的点.

ii) $(x_4,y_4)=-P=(x_1,x_1+y_1)=(t^3+t,t^3+t+t^7+t^4+t)=(t^3+t,t^7+t^4+t^3)$.

iii)
$$\begin{cases} \lambda_2 &= \dfrac{x_1^2+y_1}{x_1}=t^6+t^3+t^2+t \\ x_2 &= \lambda_2^2+\lambda_2+x_1+x_1+1=t^7+t^6+t^4+t^2+t \\ y_2 &= \lambda_2(x_1+x_2)+x_2+y_1=1 \end{cases}$$

iv)
$$\begin{cases} \lambda_3 &= \dfrac{y_2+y_1}{x_2+x_1}=t^7+t^6+t^4+t^3+t^2 \\ x_3 &= \lambda_3^2+\lambda_3+x_1+x_2+1=t^7+t^4+t \\ y_3 &= \lambda_3(x_1+x_3)+x_3+y_1=t^7+t^6+t^4+t^3+t^2+1 \end{cases}$$

上 海 交 通 大 学 试 卷（A卷）

（2007至2008学年 第2学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（II） 成绩 _____

一. (20分) 设 $f(x)=x^6+x+1$.

i) 证明： $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

ii) 证明：由 $f(x)$ 生成的理想 $(f(x))=\{g(x)f(x)\mid g(x)\in \mathbf{F}_2[x]\}$ 是 $\mathbf{F}_2$ 中的素理想.

二. (20分) 设 $f(x)=x^6+x+1$.

i) 证明商集 $\mathbf{F}_2[x]/(f(x))$ 对于如下加法和乘法两种运算构成一个 2^6 元域：

$$a(x)+b(x) := (a(x)+b(x) \mod f(x))$$
$$a(x)\cdot b(x) := (a(x)\cdot b(x) \mod f(x))$$

这里 $(a(x) \mod f(x))$ 表示 $a(x)$ 被 $f(x)$ 除的次数最小的余式.

ii) 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的生成元 g. 即 $\mathbf{F}_{2^6}$ 中元素 g 使得

$$\mathbf{F}_{2^6}^*=\mathbf{F}_{2^6}\setminus\{0\}= <g> =\{g,\ g^2,\ \ldots,\ g^{2^6-2},\ g^{2^6-1}=1\}.$$

三. (20分) 设 $f(x)=x^6+x+1$.

i) 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的 $2^3=8$ 元子域 E (写出所有元素).

ii) 求 3 次多项式 $h(y)\in \mathbf{F}_2[y]$ 使得 E 同构于有限域 $\mathbf{F}_{2^3}=\mathbf{F}_2[y]/(h(y))$.

四. (10分) 设域 $\mathbf{F}_p$ $(p>3)$ 上椭圆曲线 E: $y^2=x^3+a_4x+a_6$.

E 在 $\mathbf{F}_p$ 上的运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$, O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,-y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$, 则

$$\begin{cases} x_3=\lambda^2-x_1-x_2, \\ \\ y_3=\lambda(x_1-x_3)-y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1} & \text{如果 } x_1\neq x_2, \\ \\ \dfrac{3x_1^2+a_4}{2y_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{17}$ 上椭圆曲线 E: $y^2=x^3+3x+7$ 上的点 $P=(4,7)$.

求 $2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $-P=(x_4,y_4)$.

我承诺，我将严格遵守考试纪律.

承诺人：_____

题号										
得分										
批阅人 (流水阅卷教师签名处)										

五. (10 分) 设域 $\mathbf{F}_{2^n}$ 上椭圆曲线 E: $y^2+xy=x^3+a_2x^2+a_6$.

E 在 $\mathbf{F}_{2^n}$ 上运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$, O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,x_1+y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$,

$$\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a_2, \\ \\ y_3=\lambda(x_1+x_3)+x_3+y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2+y_1}{x_2+x_1} & \text{如果 } x_1\neq x_2, \\ \\ \dfrac{x_1^2+y_1}{x_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{2^8}=\mathbf{F}_2[t]/(t^8+t^4+t^3+t^2+1)$ 上椭圆曲线 E: $y^2+xy=x^3+x^2+1$.

设 $P_1=(t^6+t^2,\ t^3+t)$. 试证明 P_1 是 E 的一个点，

并计算 $-P_1$, $2P_1$, $3P_1$.

六. (20 分) 设 $\mathbf{F}_q$ 是特征为 p 的有限域, $q=p^n$.

i) 证明：对任意 a, $b\in\mathbf{F}_q$, 有

$(a+b)^p=a^p+b^p$.

ii) 证明： Frobenius 映射 $\sigma: x\longmapsto x^p$ 是 $\mathbf{F}_q$ 的线性变换.

iii) 证明：映射 $Tr:=\sigma+\sigma^2+\cdots+\sigma^n$:

$Tr(x)=\sigma(x)+\sigma^2(x)+\cdots+\sigma^n(x)=x^p+x^{p^2}+\cdots+x^{p^n}$

是 $\mathbf{F}_q$ 的线性变换.

上 海 交 通 大 学 试 卷（B卷）

（2007至2008学年 第2学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（II） 成绩 _____

一. (20分) 设 $f(x)=x^6+x^5+1$.

i) 证明： $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

ii) 证明：由 $f(x)$ 生成的理想 $(f(x))=\{g(x)f(x)\mid g(x)\in \mathbf{F}_2[x]\}$ 是 $\mathbf{F}_2$ 中的素理想.

二. (20分) 设 $f(x)=x^6+x^5+1$.

i) 证明商集 $\mathbf{F}_2[x]/(f(x))$ 对于如下加法和乘法两种运算构成一个 2^6 元域：

$$a(x)+b(x) \;:=\; (a(x)+b(x) \mod f(x))$$

$$a(x)\cdot b(x) \;:=\; (a(x)\cdot b(x) \mod f(x))$$

这里 $(a(x) \mod f(x))$ 表示 $a(x)$ 被 $f(x)$ 除的次数最小的余式.

ii) 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的生成元 g. 即 $\mathbf{F}_{2^6}$ 中元素 g 使得

$$\mathbf{F}_{2^6}^*=\mathbf{F}_{2^6}\setminus\{0\}= \;<g>\; =\{g,\, g^2,\, \ldots,\, g^{2^6-2},\, g^{2^6-1}=1\}.$$

三. (20分) 设 $f(x)=x^6+x^5+1$.

i) 求有限域 $\mathbf{F}_{2^6}=\mathbf{F}_2[x]/(f(x))$ 的 $2^3=8$ 元子域 E (写出所有元素).

ii) 求 3 次多项式 $h(y)\in \mathbf{F}_2[y]$ 使得 E 同构于有限域 $\mathbf{F}_{2^3}=\mathbf{F}_2[y]/(h(y))$.

四. (10分) 设域 $\mathbf{F}_p$ $(p>3)$ 上椭圆曲线 $E:\; y^2=x^3+a_4x+a_6$.

E 在 $\mathbf{F}_p$ 上的运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$, O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,-y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$, 则

$$\begin{cases} x_3=\lambda^2-x_1-x_2, \\ \\ y_3=\lambda(x_1-x_3)-y_1. \end{cases} \qquad \text{其中 } \lambda=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1} & \text{如果 } x_1\neq x_2, \\ \\ \dfrac{3x_1^2+a_4}{2y_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{17}$ 上椭圆曲线 $E:\; y^2=x^3+7x+1$ 上的点 $P=(4,5)$.

求 $2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $-P=(x_4,y_4)$.

我承诺，我将严格遵守考试纪律.

承诺人：_____

题 号										
得 分										
批阅人 (流水阅卷教师签名处)										

五. (10 分) 设域 $\mathbf{F}_{2^n}$ 上椭圆曲线 $E:\ y^2+xy=x^3+a_2x^2+a_6$.

E 在 $\mathbf{F}_{2^n}$ 上运算规则为：设 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$, O 为无穷远点. 则

(1) $O+P_1=P_1+O$; (2) $-P_1=(x_1,x_1+y_1)$;

(3) 如果 $P_3=(x_3,y_3)=P_1+P_2\neq O$,

$$\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a_2, \\ \\ y_3=\lambda(x_1+x_3)+x_3+y_1. \end{cases} \quad \text{其中 } \lambda=\begin{cases} \dfrac{y_2+y_1}{x_2+x_1} & \text{如果 } x_1\neq x_2, \\ \\ \dfrac{x_1^2+y_1}{x_1} & \text{如果 } x_1=x_2. \end{cases}$$

设 $\mathbf{F}_{2^8}=\mathbf{F}_2[t]/(t^8+t^4+t^3+t^2+1)$ 上椭圆曲线 $E:\ y^2+xy=x^3+x^2+1$.

设 $P_1=(t^3+t,\ t^7+t^4+t)$. 试证明 P_1 是 E 的一个点，

并计算 $-P_1$, $2P_1$, $3P_1$.

六. (20 分) 设 $\mathbf{F}_q$ 是特征为 p 的有限域, $q=p^n$.

i) 证明：对任意 $a,\ b\in\mathbf{F}_q$, 有

$$(a+b)^p=a^p+b^p.$$

ii) 证明： Frobenius 映射 $\sigma: x\longmapsto x^p$ 是 $\mathbf{F}_q$ 的线性变换.

iii) 证明：映射 $Tr:=\sigma+\sigma^2+\cdots+\sigma^n$:

$$Tr(x)=\sigma(x)+\sigma^2(x)+\cdots+\sigma^n(x)=x^p+x^{p^2}+\cdots+x^{p^n}$$

是 $\mathbf{F}_q$ 的线性变换.

2005-2006 年第一学期 2005～2006 二学期

信息安全数学基础 (II) 考试题 (A 卷)

姓名 _____ 学号 _____

一. (10 分) 将置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 5 & 7 & 8 & 4 & 2 & 1 \end{pmatrix}$ 表示成循环的乘积.

二. (15 分)

i) 判断 $f(x) = x^4 + x + 1$ 是否为 $\mathbf{F}_2$ 不可约多项式?

ii) 设 $g(x) = x^3 + x + 1$, 求多项式 $s(x), t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = 1 \pmod 2.$$

三. (15 分) 设 $f(x) = x^4 + x + 1$.

i) 求出有限域 $\mathbf{F}_{2^4} = \mathbf{F}_2/(f(x))$ 的生成元 g,

ii) 计算 g^k, $0 \le k \le 2^4 - 2$.

四. (15 分) 设 $f(x) = x^4 + x + 1$.

i) 求 $\beta \in \mathbf{F}_2/(f(x))$ 使得 β, β^2, β^{2^2}, β^{2^3} 构成 $\mathbf{F}_2/(f(x))$ 在 $\mathbf{F}_2$ 的基底.

ii) 设 $\alpha = \beta + \beta^2 + \beta^{2^2} + \beta^{2^3}$, 计算 α^{16}.

五. (15 分) 设 $\mathbf{F}_{17}$ 上椭圆曲线 $E: y^2 = x^3 + 3x + 1$, 设 $P = (2, 7)$.

i) 证明: P 是 E 上的点,

ii) 求 $-P$, $2P$ 和 $3P$.

六. (15 分) 设 $f(x) = x^8 + x^4 + x^3 + x + 1$. 在 $\mathbf{F}_2$ 上证明: $f(x) \mid x^{256} - x$.

七. (15 分)

i) 证明: $\mathbf{F}_7[x]$ 是主理想环,

ii) 证明: $I = (f(x))$ 是 $\mathbf{F}_7[x]$ 的素理想当且仅当 $f(x)$ 是不可约多项式.

2005-2006 年第一学期
信息安全数学基础 (II) 考试题 (A 卷) 解答

姓名 _____ 学号 _____

一. (10 分) 将置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 5 & 7 & 8 & 4 & 2 & 1 \end{pmatrix}$ 表示成循环的乘积.

解

$$\sigma = \begin{pmatrix} 1 & 3 & 9 \\ 3 & 9 & 1 \end{pmatrix}\begin{pmatrix} 2 & 6 & 8 \\ 6 & 8 & 2 \end{pmatrix}\begin{pmatrix} 4 & 5 & 7 \\ 5 & 7 & 4 \end{pmatrix} = (1,3,9)(2,6,8)(4,5,7)$$

二. (15 分)

i) 判断 $f(x) = x^4 + x + 1$ 是否为 $\mathbf{F}_2$ 不可约多项式?

ii) 设 $g(x) = x^3 + x + 1$, 求多项式 $s(x), t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = 1 \pmod 2.$$

解

i) 次数 ≤ 2 的不可约多项式为 x, $x+1$, x^2+x+1, 因为

$$\begin{aligned} x^4 + x + 1 &= (x^3 + 1)x + 1 \\ x^4 + x + 1 &= (x^3 + x^2 + x)(x + 1) + 1 \\ x^4 + x + 1 &= (x^2 + x)(x^2 + x + 1) + x + 1 \end{aligned}$$

所以 x, $x+1$, x^2+x+1 都不能整除 x^4+x+1, 从而 x^4+x+1 是不可约多项式.

ii) 因为

$$x^4 + x + 1 = x(x^3 + x + 1) + x^2 + 1, \quad x^3 + x + 1 = x(x^2 + 1) + 1,$$

所以

$$1 = x^3 + x + 1 + x(x^4 + x + 1 + x(x^3 + x + 1)) = x(x^4 + x + 1) + (x^2 + 1)(x^3 + x + 1)$$

即 $s(x) = x, t(x) = x^2 + 1$.

三. (15 分) 设 $f(x) = x^4 + x + 1$.

i) 求出有限域 $\mathbf{F}_{2^4} = \mathbf{F}_2/(f(x))$ 的生成元 g,

ii) 计算 g^k, $0 \leq k \leq 2^4 - 2$.

解 i) 因为 $|\mathbf{F}_{2^4}^*| = 15 = 3 \cdot 5$, 所以满足

$$g(x)^3 \neq 1 \pmod{x^4 + x + 1}, \quad g(x)^5 \neq 1 \pmod{x^4 + x + 1}$$

的元素 $g(x)$ 都是生成元.

对于 $g(x)=x$, 有

$$x^3 \equiv x^3 \not\equiv 1 \pmod{x^4+x+1}, \quad x^5 \equiv x^2+x \not\equiv 1 \pmod{x^4+x+1},$$

所以 $g(x)=x$ 是 $\mathrm{F}_2[x]/(x^4+x+1)$ 的生成元.

对于 $t=0,1,2,\ldots,14$, 计算 $g(x)^t \pmod{x^4+x+1}$:

$$\begin{array}{lll} g(x)^0 \equiv 1, & g(x)^1 \equiv x, & g(x)^2 \equiv x^2, \\ g(x)^3 \equiv x^3, & g(x)^4 \equiv x+1, & g(x)^5 \equiv x^2+x, \\ g(x)^6 \equiv x^3+x^2, & g(x)^7 \equiv x^3+x+1, & g(x)^8 \equiv x^2+1, \\ g(x)^9 \equiv x^3+x, & g(x)^{10} \equiv x^2+x+1, & g(x)^{11} \equiv x^3+x^2+x, \\ g(x)^{12} \equiv x^3+x^2+x+1, & g(x)^{13} \equiv x^3+x^2+1, & g(x)^{14} \equiv x^3+1. \end{array}$$

四. (15 分) 设 $f(x)=x^4+x+1$.

i) 求 $\beta \in \mathrm{F}_2/(f(x))$ 使得 β, β^2, β^{2^2}, β^{2^3} 构成 $\mathrm{F}_2/(f(x))$ 在 F_2 的基底.

ii) 设 $\alpha=\beta+\beta^2+\beta^{2^2}+\beta^{2^3}$, 计算 α^{16}.

解 i) 对于 $\beta=x$, 我们有

$$\begin{aligned} \beta &= x \\ \beta^2 &= x^2 \\ \beta^4 &= x+1 \\ \beta^8 &= x^2+1 \end{aligned}$$

所以 β, β^2, β^{2^2}, β^{2^3} 不构成一个基底.

对于 $\beta=x^3$, 我们有

$$\begin{aligned} \beta &= x^3 &&= x^3 \\ \beta^2 &= x^6 &&= x^3+x^2 \\ \beta^4 &= x^{12} &&= x^3+x^2+x+1 \\ \beta^8 &= x^9 &&= x^3+x \end{aligned}$$

所以 β, β^2, β^{2^2}, β^{2^3} 构成一个基底, 是正规基.

ii) 因为 $\alpha=\beta+\beta^2+\beta^{2^2}+\beta^{2^3}=1$, 所以 $\alpha^{16}=1$.

五. (15 分) 设 F_{17} 上椭圆曲线 E: $y^2=x^3+3x+1$, 设 $P=(2,7)$.

i) 证明: P 是 E 上的点,

ii) 求 $-P$, $2P$ 和 $3P$.

解 i) 因为 $(x^3+3x+1)(2)=2^3+3\cdot 2+1=15\equiv 7^2 \pmod{17}$, 所以 $P=(2,7)$ 是 E 上的点.

ii) 令 $P=(2,7)=(x_1,y_1)$, 则 $-P=(x_1,-y_1)=(2,10)$. 又设 $2P=(x_2,y_2)$, $3P=(x_3,y_3)=P+2P$, 则

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=12, \qquad x_2=\lambda_2^2-2x_1=4, \qquad y_3=\lambda_2(x_1-x_2)-y_1=3$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=15, \qquad x_3=\lambda_3^2-x_1-x_2=15, \qquad y_3=\lambda_3(x_1-x_3)-y_1=2$$

六. (15 分) 设 $f(x)=x^8+x^4+x^3+x+1$. 在 F_2 上证明: $f(x) \mid x^{256}-x$.

证 首先证明 $f(x)=x^8+x^4+x^3+x+1$ 是不可约多项式. 次数 $\le 8/2=4$ 的不可约多项式为 $x,\ x+1,\ x^2+x+1,\ x^3+x+1,\ x^3+x^2+1,\ x^4+x+1,\ x^4+x^3+1$, 因为

$$\begin{aligned}
x^8+x^4+x^3+x+1 &= (x^7+x^3+x^2+1)x+1\\
x^8+x^4+x^3+x+1 &= (x^7+x^6+x^5+x^4+x^2+x)(x+1)+1\\
x^8+x^4+x^3+x+1 &= (x^6+x^5+x^3)(x^2+x+1)+x+1\\
x^8+x^4+x^3+x+1 &= (x^5+x^3+x^2+1)(x^3+x+1)+x^2\\
x^8+x^4+x^3+x+1 &= (x^5+x^4+x^3)(x^3+x^2+1)+x+1\\
x^8+x^4+x^3+x+1 &= (x^4+x)(x^4+x+1)+x^3+x^2+1\\
x^8+x^4+x^3+x+1 &= (x^4-x^3+x^2-x+1)(x^4+x^3+1)+x^3+x^2
\end{aligned}$$

所以 $x,\ x+1,\ x^2+x+1,\ x^3+x+1,\ x^3+x^2+1,\ x^4+x+1,\ x^4+x^3+1$ 都不能整除 $f(x)$, 从而 $f(x)$ 是不可约多项式.

在有限域 $\mathbf{F}_{2^8}=\mathbf{F}_2[x]/(f(x))$ 中, 有

$$x^{2^8-1}-1\equiv 0 \pmod{f(x)},$$

故在 $\mathbf{F}_2$ 上, $f(x)\mid x^{256}-x$.

七. (15 分)

i) 证明: $\mathbf{F}_7[x]$ 是主理想环,

ii) 证明: $I=(f(x))$ 是 $\mathbf{F}_7[x]$ 的素理想当且仅当 $f(x)$ 是不可约多项式.

证 i) 易证: $\mathbf{F}_7[x]$ 是环. 现证明: $\mathbf{F}_7[x]$ 的每个理想 I 是主理想.

在 I 中取一个次数 $n\ge 1$ 为最小的多项式 $f(x)$, 则

$$I=(f(x))=\{q(x)f(x)\mid q(x)\in \mathbf{F}_7[x]\}$$

事实上, 对于 $g(x)\in I$, 如果 $g(x)\not\vdots f(x)$, 则存在 $q(x),r(x)\in \mathbf{F}_7[x]$ 使得

$$g(x)=q(x)f(x)+r(x),\qquad \deg r(x)<\deg f(x).$$

因为 I 是理想, 所以由 $f(x),g(x)\in I$, 可推出

$$r(x)=g(x)-q(x)f(x)\in I$$

这与 $f(x)$ 是 I 中次数最小的多项式矛盾. 故结论成立.

ii) 充分性. 如果 n 次 $f(x)$ 不是不可约多项式, 则存在多项式 $f_1(x),\ f_2(x)\in \mathbf{F}_7[x],\ 1<\deg f_i(x)<n$ 使得 $f(x)=f_1(x)f_2(x)$, 这时 $I_i=(f_i(x))$ 都是 $I=(f(x))$ 的真理想, 且使得 $I=I_1\cdot I_2$, 这与 I 是素理想矛盾.

必要性. 如果 I 不是素理想, 则存在真理想 I_1,I_2 使得 $I=I_1\cdot I_2$. 因为 $\mathbf{F}_7[x]$ 是主理想环, 所以存在非常数多项式 $f_i(x)$ 使得 $I_i=(f_i(x))$. 进而 $f(x)=cf_1(x)f_2(x)$, 其中 c 是常数. 这与 $f(x)$ 是不可约多项式矛盾.

2005-2006 年第一学期
信息安全数学基础 (II) 考试题 (B 卷)

姓名 _____ 学号 _____

一. (10 分) 将置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 8 & 9 & 7 & 3 & 1 & 2 \end{pmatrix}$ 表示成循环的乘积.

二. (15 分)

i) 判断 $f(x) = x^4 + x^3 + 1$ 是否为 $\mathbf{F}_2$ 不可约多项式?

ii) 设 $g(x) = x^3 + x + 1$, 求多项式 $s(x), t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = 1 \pmod 2.$$

三. (15 分) 设 $f(x) = x^4 + x^3 + 1$.

i) 求出有限域 $\mathbf{F}_{2^4} = \mathbf{F}_2/(f(x))$ 的生成元 g,

ii) 计算 g^k, $0 \le k \le 2^4 - 2$.

四. (15 分) 设 $f(x) = x^4 + x^3 + 1$.

i) 求 $\beta \in \mathbf{F}_2/(f(x))$ 使得 β, β^2, β^{2^2}, β^{2^3} 构成 $\mathbf{F}_2/(f(x))$ 在 $\mathbf{F}_2$ 的基底.

ii) 设 $\alpha = \beta + \beta^2 + \beta^{2^2} + \beta^{2^3}$, 计算 α^{16}.

五. (15 分) 设 $\mathbf{F}_{17}$ 上椭圆曲线 E: $y^2 = x^3 + 3x + 1$, 设 $P = (7, 5)$.

i) 证明: P 是 E 上的点,

ii) 求 $-P$, $2P$ 和 $3P$.

六. (15 分) 设 $f(x) = x^8 + x^4 + x^3 + x^2 + 1$. 在 $\mathbf{F}_2$ 上证明: $f(x) \mid x^{256} - x$.

七. (15 分)

i) 证明: $\mathbf{F}_{11}[x]$ 是主理想环,

ii) 证明: $I = (f(x))$ 是 $\mathbf{F}_{11}[x]$ 的素理想当且仅当 $f(x)$ 是不可约多项式.

2005-2006 年第一学期
信息安全数学基础 (II) 考试题 (B 卷) 解答

姓名 _____ 学号 _____

一. (10 分) 将置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 8 & 9 & 7 & 3 & 1 & 2 \end{pmatrix}$ 表示成循环的乘积.

解

$$\sigma = \begin{pmatrix} 1 & 4 & 8 \\ 4 & 8 & 1 \end{pmatrix}\begin{pmatrix} 2 & 5 & 9 \\ 5 & 9 & 2 \end{pmatrix}\begin{pmatrix} 3 & 6 & 7 \\ 6 & 7 & 3 \end{pmatrix} = (1,4,8)(2,5,9)(3,6,7)$$

二. (15 分)

i) 判断 $f(x) = x^4 + x^3 + 1$ 是否为 $\mathbf{F}_2$ 不可约多项式?

ii) 设 $g(x) = x^3 + x + 1$, 求多项式 $s(x), t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = 1 \pmod 2.$$

解

i) 次数 ≤ 2 的不可约多项式为 x, $x+1$, x^2+x+1, 因为

$$\begin{aligned} x^4 + x^3 + 1 &= (x^3 + x^2)x + 1 \\ x^4 + x^3 + 1 &= x^3(x+1) + 1 \\ x^4 + x^3 + 1 &= (x^2+1)(x^2+x+1) + x \end{aligned}$$

所以 x, $x+1$, x^2+x+1 都不能整除 $x^4 + x^3 + 1$, 从而 $x^4 + x^3 + 1$ 是不可约多项式.

ii) 因为

$$x^4 + x^3 + 1 = (x+1)(x^3 + x + 1) + x^2, \quad x^3 + x + 1 = x \cdot x^2 + x + 1, \quad x^2 = (x+1)(x+1) + 1,$$

所以

$$\begin{aligned} 1 &= x^2 + (x+1)(x^3 + x + 1 + x \cdot x^2) \\ &= (x+1)(x^3 + x + 1) + (x^2 + x + 1)(x^4 + x^3 + 1 + (x+1)(x^3 + x + 1)) \\ &= (x^2 + x + 1)(x^4 + x^3 + 1) + (x^3 + x)(x^3 + x + 1) \end{aligned}$$

即 $s(x) = x^2 + x + 1, t(x) = x^3 + x$.

三. (15 分) 设 $f(x) = x^4 + x^3 + 1$.

i) 求出有限域 $\mathbf{F}_{2^4} = \mathbf{F}_2/(f(x))$ 的生成元 g,

ii) 计算 g^k, $0 \leq k \leq 2^4 - 2$.

解 i) 因为 $|\mathbf{F}_{2^4}^*| = 15 = 3 \cdot 5$, 所以满足

$$g(x)^3 \neq 1 \pmod{x^4 + x^3 + 1}, \quad g(x)^5 \neq 1 \pmod{x^4 + x^3 + 1}$$

的元素 $g(x)$ 都是生成元.

对于 $g(x)=x$, 有

$$x^3 \equiv x^3 \not\equiv 1 \pmod{x^4+x^3+1}, \quad x^5 \equiv x^3+x+1 \not\equiv 1 \pmod{x^4+x3+1},$$

所以 $g(x)=x$ 是 $\mathbf{F}_2[x]/(x^4+x^3+1)$ 的生成元.

对于 $t=0,1,2,\ldots,14$, 计算 $g(x)^t \pmod{x^4+x^3+1}$:

$$\begin{array}{lll}
g(x)^0 \equiv 1, & g(x)^1 \equiv x, & g(x)^2 \equiv x^2, \\
g(x)^3 \equiv x^3, & g(x)^4 \equiv x^3+1, & g(x)^5 \equiv x^3+x+1, \\
g(x)^6 \equiv x^3+x^2+x+1, & g(x)^7 \equiv x^2+x+1, & g(x)^8 \equiv x^3+x^2+x, \\
g(x)^9 \equiv x^2+1, & g(x)^{10} \equiv x^3+x, & g(x)^{11} \equiv x^3+x^2+1, \\
g(x)^{12} \equiv x+1, & g(x)^{13} \equiv x^2+x, & g(x)^{14} \equiv x^3+x^2.
\end{array}$$

四. (15 分) 设 $f(x)=x^4+x^3+1$.

i) 求 $\beta \in \mathbf{F}_2/(f(x))$ 使得 β, β^2, β^{2^2}, β^{2^3} 构成 $\mathbf{F}_2/(f(x))$ 在 $\mathbf{F}_2$ 的基底.

ii) 设 $\alpha=\beta+\beta^2+\beta^{2^2}+\beta^{2^3}$, 计算 α^{16}.

解 i) 对于 $\beta=x$, 我们有

$$\begin{aligned}
\beta &= x \\
\beta^2 &= x^2 \\
\beta^4 &= x^3+1 \\
\beta^8 &= x^3+x^2+x
\end{aligned}$$

所以 β, β^2, β^{2^2}, β^{2^3} 构成一个基底, 是正规基.

ii) 因为 $\alpha=\beta+\beta^2+\beta^{2^2}+\beta^{2^3}=1$, 所以 $\alpha^{16}=1$.

五. (15 分) 设 $\mathbf{F}_{17}$ 上椭圆曲线 E: $y^2=x^3+3x+1$, 设 $P=(7,5)$.

i) 证明: P 是 E 上的点,

ii) 求 $-P$, $2P$ 和 $3P$.

解 i) 因为 $(x^3+3x+1)(7)=7^3+3\cdot 7+1=8\equiv 5^2 \pmod{17}$, 所以 $P=(7,5)$ 是 E 上的点.

ii) 令 $P=(7,5)=(x_1,y_1)$, 则 $-P=(x_1,-y_1)=(7,12)$. 又设 $2P=(x_2,y_2)$, $3P=(x_3,y_3)=P+2P$, 则

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=12, \qquad x_2=\lambda_2^2-2x_1=7, \qquad y_3=\lambda_2(x_1-x_2)-y_1=12$$

因为 $2P=-P$, 所以 $3P=O$ (无穷远点).

六. (15 分) 设 $f(x)=x^8+x^4+x^3+x^2+1$. 在 $\mathbf{F}_2$ 上证明: $f(x) \mid x^{256}-x$.

证 首先证明 $f(x)=x^8+x^4+x^3+x^2+1$ 是不可约多项式. 次数 $\le 8/2=4$ 的不可约多项式为

x, $x+1$, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1, 因为

$$\begin{aligned}
x^8+x^4+x^3+x^2+1 &= (x^7+x^3+x^2+x)x+1\\
x^8+x^4+x^3+x^2+1 &= (x^7+x^6+x^5+x^4+x^2)(x+1)+1\\
x^8+x^4+x^3+x^2+1 &= (x^6+x^5+x^3+1)(x^2+x+1)+x\\
x^8+x^4+x^3+x^2+1 &= (x^5+x^3+x^2+1)(x^3+x+1)+x\\
x^8+x^4+x^3+x^2+1 &= (x^5+x^4+x^3)(x^3+x^2+1)+x^2+1\\
x^8+x^4+x^3+x^2+1 &= (x^4+x)(x^4+x)+x^3+x+1\\
x^8+x^4+x^3+x^2+1 &= (x^4+x^3+x^2+x+1)(x^4+x^3+1)+x^3+x
\end{aligned}$$

所以 x, $x+1$, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1 都不能整除 $f(x)$, 从而 $f(x)$ 是不可约多项式.

在有限域 $\mathbf{F}_{2^8}=\mathbf{F}_2[x]/(f(x))$ 中，有

$$x^{2^8-1}-1\equiv 0 \pmod{f(x)},$$

故在 $\mathbf{F}_2$ 上， $f(x)\mid x^{256}-x$.

七. (15 分)

i) 证明： $\mathbf{F}_{11}[x]$ 是主理想环.

ii) 证明： $I=(f(x))$ 是 $\mathbf{F}_{11}[x]$ 的素理想当且仅当 $f(x)$ 是不可约多项式.

证 i) 易证： $\mathbf{F}_{11}[x]$ 是环. 现证明： $\mathbf{F}_{11}[x]$ 的每个理想 I 是主理想.

在 I 中取一个次数 $n\geq 1$ 为最小的多项式 $f(x)$, 则

$$I=(f(x))=\{q(x)f(x)\mid q(x)\in \mathbf{F}_{11}[x]\}$$

事实上，对于 $g(x)\in I$, 如果 $g(x)\not\mid f(x)$, 则存在 $q(x),r(x)\in \mathbf{F}_{11}[x]$ 使得

$$g(x)=q(x)f(x)+r(x),\qquad \deg r(x)<\deg f(x).$$

因为 I 是理想，所以由 $f(x),g(x)\in I$, 可推出

$$r(x)=g(x)-q(x)f(x)\in I$$

这与 $f(x)$ 是 I 中次数最小的多项式矛盾. 故结论成立.

ii) 充分性. 如果 n 次 $f(x)$ 不是不可约多项式, 则存在多项式 $f_1(x)$, $f_2(x)\in \mathbf{F}_{11}[x]$, $1<\deg f_i(x)<n$ 使得 $f(x)=f_(x)f_2(x)$, 这时 $I_i=(f_i(x))$ 都是 $I=(f(x))$ 的真理想，且使得 $I=I_1\cdot I_2$, 这与 I 是素理想矛盾.

必要性. 如果 I 不是素理想，则存在真理想 I_1,I_2 使得 $I=I_1\cdot I_2$. 因为 $\mathbf{F}_{11}[x]$ 是主理想环，所以存在非常数多项式 $f_i(x)$ 使得 $I_i=(f_i(x))$. 进而 $f(x)=cf_1(x)f_2(x)$, 其中 c 是常数. 这与 $f(x)$ 是不可约多项式矛盾.

3.5