华东师范大学期末试卷

2019-2020 第一学期

课程名称：<u>网络安全数学基础</u>
学生姓名：______________ 学　　号：______________
专　　业：______________ 年级/班级：______________
课程性质：公共必修、公共选修、**<u>专业必修</u>**、专业选修

一	二	三	四	五	六	七	八	总分	**阅卷人姓名**

…………………………………………………………………………………

一、计算题

1、求解同余方程组$\begin{cases} x \equiv -2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{7} \end{cases}$

2、设素数 p=2000000000000000000000000029967≈2^{100}≈10^{30}，q=41。判断同余式 $x^2 \equiv q \pmod{p}$是否有解。

3、设 $\mathbf{F}_2[x]$中有$f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$,$g(x) = x^8 + x^4 + x^3 + x + 1$，求 $s(x)$,$t(x)$使得 $s(x)\cdot f(x)+t(x)\cdot g(x) = (f(x),g(x))$

4、设 $\mathbf{F}_{23}$ 上椭圆曲线 E:$y^2 = x^3 + 11x + 18$上的点 P(6,1)，Q(9,15)，求 P+Q，2P。

二、证明题

1、证明高斯环 $\mathbf{Z}[\sqrt{-1}]=\{a+b\sqrt{-1} | a, b \in \mathbf{Z}\}$为整环。

2、证明 $\mathbf{F}_2[x]$上多项式$f(x) = x^4 + x^3 + x^2 + x + 1$是不可约多项式。

3、证明对任意 a∈G，$a \mapsto a^{-1}$是群 G 的自同构当且仅当 G 是 Abel 群。

4、设A是交换环，如果A中存在正整数 m 使得$a^m = 0$，元素a称为幂零。根据习题 10.7.5，我们已知幂零元的加法是封闭的（无需再证明），即幂零元a和b的和$a + b$也是幂零元。

（1）令$\mathcal{R}$代表A中所有幂零元所构成的集合，证明$\mathcal{R}$是环A的一个理想。

（2）证明商环$A/\mathcal{R}$中没有$\bar{0}$（$\bar{0} = 0/\mathcal{R}$）以外的幂零元。

5、 (1) 设D是整环，并且包含在整环E之中，而$f \in D[x]$的次数是n，则f在E中至多有n个不同的根。

(2) 设p是素数，$n \geq 1$是整数，$\mathcal{F}$是由p^n个元素组成的有限域。证明：$\mathcal{F}$中所有元素恰好构成多项式$f(x) = x^{p^n} - x \in Z_p[x]$的所有根。

答案：
计算题：
1. m1 = 3, M1=28, $M1^{-1} \equiv 1(mod\ \ 3)$
m2 = 4, M2=21, $M2^{-1} \equiv 1(mod\ \ 4)$
m3 = 7, M1=12, $M1^{-1} \equiv 3(mod\ \ 7)$
解为$x \equiv 1\times 1\times 28+3\times 1\times 21+2\times 3\times 12 \equiv 79\ \ (\mathrm{mod}\ \ 84)$

2.

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)=\left(\frac{-2}{41}\right)=1,$$

而$\left(\frac{-2}{41}\right)=\left(\frac{-1}{41}\right)\left(\frac{2}{41}\right)=(-1)^{\frac{41-1}{2}}(-1)^{\frac{41^2-1}{8}}=1,$

所以$\left(\frac{q}{p}\right)=1$，同余式有解。

3. 运用多项式欧几里得除法，有

$$f(x)=q_0(x)g(x)+r_0(x),\quad q_0(x)=x^5+x^3,\quad r_0=x^7+x^6+1,$$
$$g(x)=q_1(x)r_0(x)+r_1(x),\quad q_1(x)=x+1,\quad r_1=x^6+x^4+x^3,$$
$$r_0(x)=q_2(x)r_1(x)+r_2(x),\quad q_2(x)=x+1,\quad r_2=x^5+x^3+1,$$
$$r_1(x)=q_3(x)r_2(x)+r_3(x),\quad q_3(x)=x,\quad r_3=x^3+x,$$
$$r_2(x)=q_4(x)r_3(x)+r_4(x),\quad q_4(x)=x^2,\quad r_4=1.$$

从而

$$\begin{aligned}r_4(x)&=q_4(x)\big(q_3(x)r_2(x)+r_1(x)\big)+r_2(x)\\&=(x^3+1)\big(q_2(x)r_1(x)+r_0(x)\big)+q_4(x)r_1(x)\\&=(x^4+x^3+x^2+x+1)\big(q_1(x)r_0(x)+g(x)\big)+(x^3+1)r_0(x)\\&=(x^5+x^3)\big(q_0(x)g(x)+f(x)\big)+(x^4+x^3+x^2+x+1)g(x)\\&=(x^5+x^3)f(x)+(x^{10}+x^6+x^4+x^3+x^2+x+1)g(x)\end{aligned}$$

所以，s(x)= x^5+x^3，t(x)= $x^{10}+x^6+x^4+x^3+x^2+x+1$

4. 令$\lambda_1=\frac{15-1}{9-6}=\frac{14}{3}\equiv 20\ \ (mod\ \ 23),$

则$x_3=20^2-6-9\equiv 17(mod\ \ 23), y_3=20\times(6-17)-1\equiv 9(mod\ \ 23),$
所以P+Q=(17,9)

令$\lambda_2=\frac{3\times 6^2+11}{2}=\frac{119}{2}\equiv 2\ \ (mod\ \ 23),$

则$x_3=2^2-6-6\equiv 15(mod\ \ 23), y_3=2\times(6-15)-1\equiv 4(mod\ \ 23),$

证明题：

1. 证：

(1)Z[$\sqrt{-1}$]对于加法

$$(a+b\sqrt{-1})\oplus(c+d\sqrt{-1})=(a+c)+(b+d)\sqrt{-1}$$

构成一个交换加群。零元为 0，$(\mathrm{a}+\mathrm{b}\sqrt{-1})$的负元为$-\left(\mathrm{a}+\mathrm{b}\sqrt{-1}\right)=-a+(-b)\sqrt{-1}$

(2)Z[$\sqrt{-1}$]对于乘法，

$$(a+b\sqrt{-1})\otimes(c+d\sqrt{-1})=(ac-bd)+(ad+bc)\sqrt{-1}$$

满足集合律和分配律，还满足交换律，有单位元 1。

(3)Z[$\sqrt{-1}$]无零因子。若$\mathrm{a}+\mathrm{b}\sqrt{-1}\neq 0$为零因子，则存在非零元$\mathrm{c}+\mathrm{d}\sqrt{-1}$使得，

$$(a+b\sqrt{-1})\otimes(c+d\sqrt{-1})=(ac-bd)+(ad+bc)\sqrt{-1}=0,$$

从而 ac-bd=0, ad+bc = 0, 则$\mathrm{ac}^2=c(bd)=d(-ad), a(c^2+d^2)=0$. 那么 a = b = 0,矛盾。

因此，**Z**[$\sqrt{-1}$]是整环。

2. 证明：

次数≤2 的不可约多项式 *p(x)*：$x, x+1, x^2+x+1$作 *p(x)|f(x)*是否成立的判断。

$$f(x)=x(x^3+x^2+x)+1,$$
$$f(x)=(x+1)(x^3+x)+1,$$
$$f(x)=(x^2+x+1)x^2+x+1,$$

综上，$\mathbf{F}_2$[x]上多项式$f(x)=x^4+x^3+x^2+x+1$是不可约多项式。

3. 证明：

将每一元变为其逆元是自同构

$\Leftrightarrow (ab)^{-1}=a^{-1}b^{-1}, \forall a,b\in G$

$\Leftrightarrow ab=(a^{-1}b^{-1})^{-1}=ba, \forall a,b\in G$

$\Leftrightarrow G$是Abel群。

4. 证明：

1) 只需证对于任何$a\in A$，和$r\in\mathcal{R}$，有$ar\in\mathcal{R}$和$ra\in\mathcal{R}$成立即可。这个结论是显然的，因为$r\in\mathcal{R}\to r^m=0\to(ar)^m=(ra)^m=a^m r^m=0$。

2) $a/_{\mathcal{R}}$（$a\in A$）是幂零元$\to a^m/_{\mathcal{R}}=\bar{0}\to a^m\in\mathcal{R}\to(a^m)^n=0\to a\in\mathcal{R}\to$

$^{a}/_{\mathcal{R}} = \bar{0}$。

5. 证明:

(1) 设$c_1, c_2, \cdots$是f在E中全体相异的根，我们有$f(x) = q_1(x)(x - c_1)$，从而$f(c_2)=\ q_1(c_2)(c_2 - c_1)$。由于$c_1 \neq c_2$并且$E$是整环，可知$q_1(c_2) = 0$。于是，$x - c_2$整除$q_1(x)$，即$f(x) = q_2(x)(x - c_1)(x - c_2)$。现在采用数学归纳法证明：如果$c_1, c_2, \cdots, c_m$是$f$在$E$中相异的根，则$g_m(x) = (x - c_1)(x - c_2)\cdots(x - c_m)$整除$f$。又$g_m(x)$的次数是$m$，所以$m \leq n$。

(2) $\mathcal{F}$中非零元素乘法群的阶是$p^n - 1$，从而对每个非零元素$u \in \mathcal{F}$都有$u^{p^n - 1} = 1_{\mathcal{F}}$，即每个非零元素$u$都是多项式$x^{p^n - 1} - 1_{\mathcal{F}}$的根，从而也是$f$的根。又$0 \in \mathcal{F}$也是$f$的根，而根据（1）的结论，知$f$在$\mathcal{F}$中恰好有$p^n$个不同的根，而这些根又恰好是$\mathcal{F}$中全部元素。