武汉大学计算机学院

2012-2013 学年度第一学期 2011 级

《信息安全数学基础》期末考试试卷(A 卷)答案

一.计算题（每小题 10 分，共 60 分）。

1. 计算勒让得符号$\left(\frac{2}{3}\right),\left(\frac{2}{17}\right),\left(\frac{3}{17}\right)$

解 $\left(\frac{2}{3}\right)=(-1)^{\frac{9-1}{8}}=-1$；

$\left(\frac{2}{17}\right)=(-1)^{\frac{289-1}{8}}=(-1)^{36}=1$；

$\left(\frac{3}{17}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1$。

2. 求解同余式组

$$\begin{cases} x\equiv 2(\bmod 9)\\ 3x\equiv 4(\bmod 5)\\ 4x\equiv 3(\bmod 7)\end{cases}$$

解 因为$3^{-1}\bmod 5=2$，$4^{-1}\bmod 7=2$，所以同余式

$$3x\equiv 4(\bmod 5) \text{ 和 } 4x\equiv 3(\bmod 7)$$

的解分别为

$$x\equiv 3(\bmod 5) \text{ 和 } x\equiv 6(\bmod 7),$$

因此求解原同余式组等价于求解同余式组

$$\begin{cases} x\equiv 2(\bmod 9)\\ x\equiv 3(\bmod 5)\\ x\equiv 6(\bmod 7)\end{cases}$$

$$m_1=9, m_2=5, m_3=7,$$

$$M_1=35, M_2=63, M_3=45,$$

利用乘法逆元素的性质可以分别计算M_1',M_2',M_3'为

$$M_1'=M_1^{-1}\bmod 9=35^{-1}\bmod 9=8;$$

$$M_2'=M_2^{-1}\bmod 5=63^{-1}\bmod 5=2;$$

$$M_3' = M_3^{-1} \bmod 7 = 45^{-1} \bmod 7 = 3^{-1} \bmod 7 = 5,$$

从而由中国剩余定理可得同余式组的解为

$$x \equiv 35 \cdot 8 \cdot 2 + 63 \cdot 2 \cdot 3 + 45 \cdot 5 \cdot 6 \pmod{315},$$

即

$x \equiv 560 + 378 + 1350 \equiv 83 \pmod{315}$。

3 求解同余式

$$f(x) \equiv x^4 + 7x + 4 \equiv 0 \pmod{27}。$$

解 对于 $f(x) = x^4 + 7x + 4$，有 $f'(x) = 4x^3 + 7$，直接验算，知同余式 $f(x) \equiv 0 \pmod 3$ 有一解

$$x_1 \equiv 1 \pmod 3。$$

首先计算

$$f'(x_1) \equiv 2 \pmod 3, \quad f'(x_1)^{-1} \bmod 3 = 2,$$

其次，计算

$$t_1 \equiv -\frac{f(x_1)}{3} f'(x_1)^{-1} \bmod 3 \equiv 1 \pmod 3,$$

$$x_2 \equiv x_1 + 3t_1 \equiv 4 \pmod 9,$$

最后，计算

$$t_2 \equiv -\frac{f(x_2)}{3^2} f'(x_1)^{-1} \bmod 3 \equiv 2 \pmod 3,$$

$$x_3 \equiv x_2 + 3^2 t_2 \equiv 22 \pmod{27},$$

因此，同余式 $f(x) \equiv 0 \pmod{27}$ 的解为

$$x_3 \equiv 22 \pmod{27}。$$

4. 假设椭圆曲线 $y^2 = x^3 + x + 6 \pmod{11}$ 上的两点 $P = (x_1, y_1), Q = (x_2, y_2)$ 之和为 $P_3 = (x_3, y_3) = P + Q \neq O$ 的计算公式为

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = (x_1 - x_3)\lambda - y_1$$

其中(a) $x_1 \neq x_2$ 时，$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$，(b) $x_1 = x_2$，且 $Q \neq -P$ 时，$\lambda = \dfrac{3x_1^2 + 1}{2y_1}$

若 $P = (8,3)$，试求 3P。

解：由公式可知：

(1) $2P = (8,3) + (8,3)$

这里 $\lambda = (3 \times 8^2 + 1)(2 \times 3)^{-1} \equiv 1 \pmod{11}$

于是 $x_3 \equiv 1^2 - 8 - 8 \equiv 7 \pmod{11}, y_3 \equiv 1 \times (8 - 7) - 3 \equiv 9 \pmod{11}$

故 $2P = (7,9)$

(2) $3P = (8,3) + (7,9)$

这里 $\lambda = (9 - 3)(7 - 8)^{-1} \equiv 5 \pmod{11}$

于是 $x_3 \equiv 25 - 8 - 7 \equiv 10 \pmod{11}, y_3 \equiv 5 \times (8 - 10) - 3 \equiv 9 \pmod{11}$

故 $3P = (10,9)$。

5.构造有限域 GF(8)={0，1，2，3，4，5，6，7}的加法和乘法表。

解：GF(8)={0,1,2,3,4,5,6,7}，先找一个 GF(2)[x]的一个 3 次不可约多项式 x^3+x+1,加法表为

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

乘法表为

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

6 求模 11 的一组最小正完全剩余系 $r_1, r_2, \cdots, r_{11}$，满足

$$r_i \equiv -1 \pmod 2, r_i \equiv 1 \pmod 3,$$

$$r_i \equiv 1 \pmod 5, r_i \equiv 0 \pmod 7, 1 \le i \le 11。$$

解 取 $m_1 = 2, m_2 = 3, m_3 = 5, m_4 = 7, m_5 = 11$，以及

$$m = m_1 m_2 m_3 m_4 m_5，\quad m_i M_i = m, M_i' = M_i^{-1} \bmod m_i, 1 \le i \le 5$$

当 x_i 遍历模 11 的完全剩余系时，

$$r_i = -M_1 M_1' + M_2 M_2' + M_3 M_3' + M_5 M_5' x_i，\quad i = 1, 2, \cdots, 11,$$

满足题目要求。分别计算 M_i, M_i' 得

$$M_1 = 1155，\quad M_1' = 1；$$

$$M_2 = 770，\quad M_2' = 2；$$

$$M_3 = 462，\quad M_3' = 3；$$

$$M_5 = 210，\quad M_5' = 1，$$

即

$$x=-1155+770\cdot 2+462\cdot 3+210x_i=1771+210x_i=210(8+x_i)+91，$$

所以具有这样性质的模 11 的最小正完全剩余系是：

$91,210+91,210\cdot 2+91,\cdots,210\cdot 10+91$。

二．证明题（每小题 10 分，共 20 分）

（1）证明：如果 p 是素数，并且 $p\equiv 3(\bmod 4)$，那么

$$\frac{p-1}{2}!\equiv \pm 1(\bmod p)。$$

证 因为 p 是素数，所以有如下一些等价式：

$$a^2\equiv 1(\bmod p)\Leftrightarrow p\mid(a-1)(a+1)\Leftrightarrow p\mid a-1 \text{或} p\mid a+1$$

$$\Leftrightarrow a\equiv 1(\bmod p) \text{或} a\equiv -1(\bmod p)$$

于是我们只需证明 $(\frac{p-1}{2}!)^2\equiv 1(\bmod p)$ 即可。

由假设条件 $p\equiv 3(\bmod 4)$，令 $p=4k+3,k\geq 0$，则有

$$\begin{aligned}&(\frac{p-1}{2}!)^2\equiv((2k+1)!)^2\\&\equiv(2k+1)\cdot\{-(p-(2k+1))\}\cdot(2k)\cdot\{-(p-2k)\}\cdots 1\cdot\{-(p-1)\}\\&\equiv(-1)^{2k+1}(2k+1)\cdot(2k+2)\cdot 2k\cdot(2k+3)\cdots 1\cdot(4k+2)\\&\equiv(-1)^{2k+1}(p-1)!\\&\equiv(-1)^{2k+1}\cdot(-1)\equiv 1(\bmod p)\end{aligned}$$

所以结论成立。

（2）若群 G 的每一个元都适合方程 $x^2=e$, 那么 G 是交换群。

证明：任意 x,y 属于群 G，$(xy)^2=x^2*y^2=e*e=e$， 所以 $x*y=y*x$，即群 G 是交换群。

三. 简述题（20 分）

如果四个不同的元素{e, a, b, c}构成的集合和该集合上的二元运算能够成为一个群，试给出该群不同构的两种运算表。

解：因为该集合的元素个数为 4，而该代数系统能够成为一个群，所以元素 a,b,c 的阶为 2 或者 4，如果存在元素的阶为 4，不妨设|a|=4，则该运算表为

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

如果不存在元素的阶为 4，则 a,b,c 的阶都为 2，于是，ab=ba=c,bc=cb=a,ac=b=ca，则该运算表为

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e