武汉大学计算机学院

2014-2015 学年度第一学期 2013 级弘毅班

《信息安全数学基础》期末考试试卷（A）答案

一．计算题（每小题 10 分，共 50 分）。

1.求整数 s 和 t，使得 sa+tb=(a,b)：

(1) a=127, b=833; (2) a=987,b=2668。

解：因为 833=127*6+71， 127=71*1+56， 71=56+15，
56=15*3+11， 15=11+4，11=4*3-1；
所以 1=4*3-11=15*3-11*4=15*15-56*4=15*71-56*19=
71*34-127*19=833*34-127*223，
即 s=34,t=-223,(a,b)=1;
（2）因为 2668=987*2+694，987=694+293， 694=293*2+108， 293=108*2+77，
108=77+31， 77=31*2+15， 31=15*2+1；
所以 1=31-15*2=31*5-77*2=108*5-77*7=108*19-293*7=
694*19-293*45=694*64-987*45=2668*64-987*173
即 s=-173,t=64,(a,b)=1.(注意，此题答案不唯一)

2.运用模重复平方法计算 $473^{17} \bmod 713$。

解：令 $x = 473^{17}$，因为 $713 = 23 \times 31$，所以计算 $x \bmod 713$ 等价于求解同余式组

$$\begin{cases} x \equiv 473^{17} \equiv a (\bmod 23) \\ x \equiv 473^{17} \equiv b (\bmod 31) \end{cases}$$

利用同余的性质，上面同余式组可以简化为

$$\begin{cases} x \equiv 13^{17} \equiv a (\bmod 23) \\ x \equiv 8^{17} \equiv b (\bmod 31) \end{cases}$$

因为 $(17)_{10} = (10001)_2$

由模重复平方算法 2.1.1 可以依次计算得到

$m_0 = 1, \quad a_0 = 13, \quad b_0 = 13$，

$m_1 = 0, \quad a_1 = 8, \quad b_1 = 13$，

$m_2 = 0, \quad a_2 = 18, \quad b_2 = 13$，

$m_3 = 0, \quad a_3 = 2, \quad b_3 = 13$，

$m_4 = 1, \quad a_4 = 4, \quad b_4 = 6$

所以第一个同余式为 $x \equiv 6 (\bmod 23)$

同理计算第二个同余式为 $x \equiv 2(\mathrm{mod}\,31)$

由中国剩余定理可得同余式组

$$\begin{cases} x \equiv 6(\mathrm{mod}\,23) \\ x \equiv 2(\mathrm{mod}\,31) \end{cases}$$

的解为 $x \equiv 31\cdot 3\cdot 6 + 23\cdot 27\cdot 2 \equiv 374(\mathrm{mod}\,713)$

所以 $473^{17} \bmod 713 = 374$。

3.求解同余式 $x^2+x+7\equiv 0$（mod 27）。

解 因为（4，27）=1，所以由同余式的性质可以得到

$4x^2+4x+28\equiv 0$（mod 27），即 $4x^2+4x+1\equiv 0$（mod 27），于是

$(2x+1)^2\equiv 0$（mod 27），因此 $2x+1\equiv 0$（mod 9）,利用一次同余式的求解方法得

$x\equiv 4$（mod 9）,所以原同余式的解为

$x\equiv 4$，13，22（mod 27）。

4.判断同余式 $x^2\equiv 102(\mathrm{mod}\ 259)$是否有解？有解时求出其所有解。

解 因为 $259 = 7\times 37$ 不是素数, 原同余式等价于同余式组 $\begin{cases} x^2 \equiv 102 \equiv 4(\mathrm{mod}\,7) \\ x^2 \equiv 102 \equiv 28(\mathrm{mod}\,37) \end{cases}$

因为 $\left(\frac{4}{7}\right) = \left(\frac{28}{37}\right) = 1$，故同余式有解，解数为 4。因为 $7 \bmod 4 = 3$，所以容易计算

第一个同余式的解为 $x \equiv \pm 4^{\frac{7+1}{4}} \equiv \pm 2(\mathrm{mod}\,7)$，而 $37 \bmod 4 = 1$，所以可以计算出

第二个同余式的解为 $x \equiv \pm 18(\mathrm{mod}\,37)$，应用中国剩余定理求得同余式的解为

$x \equiv \pm 19, \pm 93(\mathrm{mod}\,259)$。

5. 设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$，$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 3 & 6 & 1 \end{pmatrix}$，

计算 $\sigma\tau$，$\tau\sigma$，σ^{-1}。

解：$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 4 & 6 & 2 \end{pmatrix}$；

$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 6 & 4 & 1 \end{pmatrix}$；

$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 3 & 4 & 6 \end{pmatrix}$。

二．证明题（每小题 10 分，共 20 分）

1. 设$m \geq 3$，证明：模m的最小正简化剩余系的各数之和等于$m\varphi(m)/2$。

证明：设$a_1, a_2, \cdots a_s$是所有小于$m/2$且和m互素的正整数，则有

$m/2 < m - a_i < m,$且（$m - a_i, m$）$= 1, i = 1,2,\cdots, s$，

并且对于任意一个正整数a，如果它满足

$m/2 < a < m,$且（a, m）$= 1$，

则有$0 < m - a < m/2,$且（$m - a, m$）$= 1$，因此一定存在一个正整数$a_i, 1 \leq i \leq s$，使得

$m - a = a_i$，即$a = m - a_i$，所以

$a_1, a_2, \cdots a_s, m - a_s, m - a_{s-1}, \cdots, m - a_1$

构成模m的最小正简化剩余系，所以得$\varphi(m) = 2s$，且

$a_1 + a_2 + \cdots + a_s + m - a_s + \cdots + m - a_1 = ms = m\varphi(m)/2$。

2. 应用勒让德符号证明形如 8k+3 的素数有无穷多个。

证明：反证法。如果形如$8k+3$的素数只有有限多个。设这些素数为$p_1, p_2, \cdots p_k$，考虑整数

$$N = (p_1 p_2 \cdots p_k)^2 + 2$$

因为N形如$8k+3$，$N > p_i, 1 \leq i \leq k$，所以N为合数，设p为其任意一个素因数，则p为奇数，且$(p, p_i) = 1, i = 1,2,\cdots k$。

$$\left(\frac{-2}{p}\right) = \left(\frac{-2+N}{p}\right) = \left(\frac{(p_1 p_2 \cdots p_k)^2}{p}\right) = 1 = (-1)^{\frac{p\cdot p-1}{8} + \frac{p-1}{2}},$$

即p是形如$8k+1$或$8k+3$的素数，则N一定存在形如$8k+3$的素因数q（否则N是形如$8k+1$的素因数，矛盾），所以存在整数$1 \leq j \leq k$，使得$q = p_j$，这与$(q, p_i) = 1, i = 1,2,\cdots k$矛盾。

三．简述题（每小题 10 分，共 30 分）

1. 简述求模 47 的最小原根的方法以及由此求解如下高次剩余 $x^5 \equiv 29 \pmod{47}$的步骤。

答：因为$\varphi(47)=46=2\times23$，所以只需验证g^2,g^{23} 模 47 是否为 1 即可，逐个计算可得：

$2^2 \bmod 47=4,2^{23} \bmod 47=1$，

$3^2 \bmod 47=9,3^{23} \bmod 47=1$，

$5^2 \bmod 47=25,5^{23} \bmod 47=46$

故 5 是模 47 的原根。

分别计算$5^n \bmod 47$为 5，25，31，15，23，21，11，8，40，12，13，18，43，27， 41，17，38，2，10，3，15，28，46，42，22，16，33，24，26，36，39，7，35，34，29，4，20，6，30，9，45，37，44，32，19，1。

令 $x\equiv5^y(\bmod 47)$ 因为 $29\equiv5^{35}\equiv5^{5y}(\bmod 47)$，于是 $5y\equiv35(\bmod 46)$，$y\equiv7(\bmod 46)$，所以$x\equiv11(\bmod 47)$。

2. 给出集合{0,1,2,3,4,5,6,7}上的加法和乘法运算表，使得该系统构成有限域。

答：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

3. 简述群的定义。

答：设$<G, *>$是代数系统，$*$为G上的二元运算，如果$*$运算是可结合的，则称$<G, *>$为半群。如果$<G, *>$为半群，并且二元运算$*$存在单位元$e \in G$，则称$<G, *>$为幺半群。如果$<G, *>$为半群，并且二元运算$*$存在单位元$e \in G$，G中的任何元素x都有逆元$x^{-1} \in G$，则称$<G, *>$为群，可简记为G。