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》期末考试试卷答案(B 卷)

一 计算题（每小题 10 分，共 60 分）。

1 求模 6 剩余类加法群 $\langle Z_6,+\rangle$ 到模 7 剩余类乘法群 $\langle Z_7-\{0\},\times\rangle$ 的所有同构映射。

解 因为 $\langle Z_6,+\rangle=\langle 1\rangle=\langle 5\rangle$，$\langle Z_7-\{0\},\times\rangle=\langle 3\rangle=\langle 5\rangle$，所以模 6 剩余类加法群 $\langle Z_6,+\rangle$ 到模 7 剩余类乘法群 $\langle Z_7-\{0\},\times\rangle$ 的所有同构映射为

$f_1:1^k\to 3^k$
$1\to 3, 2\to 2, 3\to 6, 4\to 4, 5\to 5, 0\to 1$，
$f_2:1^k\to 5^k$
$1\to 5, 2\to 4, 3\to 6, 4\to 2, 5\to 3, 0\to 1$

$f_3:5^k\to 3^k$
$5\to 3, 4\to 2, 3\to 6, 2\to 4, 1\to 5, 0\to 1$，
$f_4:5^k\to 5^k$
$5\to 5, 4\to 4, 3\to 6, 2\to 2, 1\to 3, 0\to 1$

2．分别用模 4 和模 5 的完全剩余系和简化剩余系来表示模 20 的完全剩余系和简化剩余系。

解 取模 4 的一组完全剩余系为 0,1,2,3，取模 5 的一组完全剩余系为 0,1,2,3,4，则有模 20 的一组完全剩余系为 0,4,8,12,16,5,9,13,17,21,10,14,18,22,26,15,19,23,27,31。

取模 4 的一组简化剩余系为 1,3，取模 5 的一组简化剩余系为 1,2,3,4，则得模 20 的一组简化剩余系为 9,13,17,21,19,23,27,31。

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．求 4 阶对称群 S4 的所有四阶子群。

解：

四阶子群{（1），（1234），（13）（24），（1432）}，
{（1），（1243），（14）（23），（1342）}，
{（1），（1324），（12）（34），（1423）}，
{（1），（12），（34），（12）（34）}，
{（1），（13），（24），（13）（24）}，
{（1），（14），（23），（14）（23）}

5． 求模 31 的所有原根，并且求解如下高次剩余

$x^6\equiv 2(\bmod\ 31)$。

解 由原根的判断方法计算 $\varphi(31)=30=2*3*5$，2^6mod31=2, 2^{10}mod31=1，3^6mod31=16, 3^{10}mod31=25，3^{15}mod31=30, 所以模 31 的最小原根为 3，其他的所有原根分别为 3，17，13，24，22，12，11，21。因为 3^{24}mod 31=2，令 $x\equiv 3^y(\bmod 31)$，则有 $6y\equiv 24(\bmod 30)$，所以 $y\equiv 4,9,14,19,24,29(\bmod 30)$，于是所以 $x\equiv 19,29,10,12,2,21(\bmod 31)$。

6．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

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

由中国剩余定理知

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

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

利用乘法逆元素的性质可以分别计算 M_1', M_2', M_3' 为

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

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

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

从而同余式组的解为

$$x \equiv 35 \cdot 8 \cdot 2 + 63 \cdot 2 \cdot 3 + 45 \cdot 5 \cdot 6 (\bmod 315)$$

即

$$x \equiv 560 + 378 + 1350 \equiv 83(\bmod 315)$$

二．证明题（共一题，20 分）

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 $8k+3$， $N > p_i, 1 \le i \le k$ ，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 $1 \le j \le k$，使得 $q = p_j$，这与 $(q, p_i) = 1, i = 1,2,\cdots k$ 矛盾。

三 解答题（共一题，20 分）

在 RSA 系统中，存在一种 $p-1$ 因子分解法，使得我们可以轻易地分解因子 n 。若 $n = pq$，且 $p-1$ 的所有素因数均很小，即 $p-1 = \prod_{i=1}^{t} p_i^{a_i}$ ，其中， p_i 为第 i 个素数， $a_i \ge 1$ 为整数，且所有 $p_i < A$，A 为已知的小正整数。试用这种方法分解整数 $n = 118829$。（提示：选取 A 为 14， $a = 1$）（20 分）

解 首先令 A 为 14， $a = 1$，则

$$r = \prod_{i=1}^{k} p_i^a = 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030,$$

$$x = 2^r \bmod n = 103935,$$

$$(x-1, n) = (103934, 118829) = 331,$$

所以 $n = 331 \times 359$。