武汉大学计算机学院 2010-2011 学年第一学期

“信息安全数学基础”答案(B 卷)

一. 计算题（每小题 10 分，共 80 分）。

1. 计算勒让德符号$\left(\frac{23}{31}\right)$，$\left(\frac{21}{29}\right)$，$\left(\frac{37}{101}\right)$。

解 $\left(\frac{23}{31}\right)=\left(\frac{-8}{31}\right)=\left(\frac{-1}{31}\right)\left(\frac{2}{31}\right)=-(-1)^{30*32/8}=-1$；

$\left(\frac{21}{29}\right)=\left(\frac{-8}{29}\right)=-1$；

$\left(\frac{37}{101}\right)=\left(\frac{101}{37}\right)=\left(\frac{27}{37}\right)=\left(\frac{3}{37}\right)=\left(\frac{1}{3}\right)=1$；

2. 判断同余式 $x^2\equiv37(\mathrm{mod}\ 101)$是否有解？有解时求出其所有解。

解因为 101 为奇素数，且$\left(\frac{37}{101}\right)=\left(\frac{101}{37}\right)=\left(\frac{27}{37}\right)=\left(\frac{3}{37}\right)=\left(\frac{1}{3}\right)=1$，故同余式有解，解数为 2。因为$101 \bmod 4=1$，且 101-1=100=2*2*25 所以容易由公式计算出该同余式的解为$x\equiv 21,80(\mathrm{mod}101)$。

3. 求解同余式 $x^2+x+7\equiv0$（mod 27）。

解 因为（4，27）=1，所以由同余式的性质可以得到
$4x^2+4x+28\equiv0$（mod 27），即 $4x^2+4x+1\equiv0$（mod 27），于是
$(2x+1)^2\equiv0$（mod 27），因此 $2x+1\equiv0$（mod 9）,利用一次同余式的求解方法得 $x\equiv4$（mod 9）,所以原同余式的解为
$x\equiv4$，13，22（mod 27）。

4. 求模 47 的所有原根，并且建立它的关于最小正原根的指标表，由此求解如下高次剩余
$x^5\equiv29(\mathrm{mod}\ 47)$。

解 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。当$(d,\varphi(47))=(d,46)=1$时，5^d是模 47 的原根，所以模 47 的所有

原根为 5，31，23，11，40，13，43，41，38，10，15，22，33，26，39，35，29，20，30，45，44，19。

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 $x \equiv 5^y (\bmod 47)$ 因为 $29 \equiv 5^{35} \equiv 5^{5y} (\bmod 47)$，于是 $5y \equiv 35 (\bmod 46)$，$y \equiv 7 (\bmod 46)$，所以 $x \equiv 11 (\bmod 47)$。

5. 求 $F_{2^4} = F_2[x]/(x^4 + x^3 + 1)$ 中的生成元 $g(x)$，并且计算出所有的生成元。

解：首先证明 $g(x) = x$ 是一个生成元，（k, 15）=1，则 $g(x)^k$ 为所有的生成元。

K=1, 2, 4, 7, 8, 11, 13, 14, $g(x)^k$ 分别为：

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

6. 求 $F_{2^4} = F_2[x]/(x^4 + x^3 + 1)$ 的所有不可约多项式。

解：$F_{2^4} = F_2[x]/(x^4 + x^3 + 1)$ 中的所有 16 个元素为 0，1，x,x+1, x^2,x^2+1, x^2+x, x^2+x+1, x^3, x^3+1， x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+ x^2+x+1,其中所有的不可约多项式

x,x+1, x^2+x+1, x^3+x+1, x^3+x^2+1。

7.对于由 GF（2）上的不可约多项式 x^4+x+1 扩成的有限域 GF（2^4），设α是一个本原元，求α的最小多项式

解：因为|α|=15，2^4mod15=1，所以最小多项式为

M(x)=(x-α)(x-α^2)(x-α^4)(x-α^{18})=x^4+x+1

8．求解递推关系

$$\begin{cases} f(n) = f(n-1) + 9f(n-2) - 9f(n-3) \\ f(0) = 0, f(1) = 1, f(2) = 2 \end{cases}。$$

解：特征方程为 $x^3 - x^2 - 9x + 9 = 0$ 的根为 1，3，-3，故通解为

$$f(n) = c_1 1^n + c_2 3^n + c_3 (-3)^n$$

由初始值得

$$\begin{cases} c_1+c_2+c_3=0 \\ c_1+3c_2-3c_3=1 \\ c_1+9c_2+9c_3=2 \end{cases}$$

解得$c_1=-\dfrac{1}{4}, c_2=\dfrac{1}{3}, c3=-\dfrac{1}{12}$，因此$f(n)=-\dfrac{1}{4}+3^{n-1}-\dfrac{1}{12}(-3)^n$。

二．证明：形如 8k-1 的素数有无穷多个。（10 分）

证明　反证法。如果形如$8k-1$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

$N=(p_1p_2\cdots p_k)^2-2$

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

$$\left(\frac{2}{p}\right)=\left(\frac{2+N}{p}\right)=\left(\frac{(p_1p_2\cdots p_k)^2}{p}\right)=1=(-1)^{\frac{p\cdot p-1}{8}},$$

即p是形如$8k-1$或$8k+1$的素数，则N一定存在形如$8k-1$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. 简述有限域的构造方式。（10 分）

答：在有限集合 F 上面定义了两种二元运算加法和乘法，首先确定集合 F 的元素个数 n，n 必须为 q 或 q^k 的形式，如果 n=q 则，加法和乘法定义为模 n 的剩余类加法和乘法。如果 $n=q^k$,则需要先寻找 GF(q)[x]上的一个不可约多项式 m(x)，加法和乘法定义为关于模 m(x)多项式的加法和乘法。