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”(A 卷)答案

一． 计算题（每小题 10 分，共 80 分）。

1.试用两种方法计算乘法逆元素 $329^{-1}\bmod 667$ 。

解：方法一 667=329*2+9，329=9*36+5， 9=5*2-1；

所以 1=5*2-9=329*2-73*9=329*148-667*73

即 $329^{-1}\bmod 667=148$。

方法二 因为 667 的欧拉函数为 22*28=616，所以

$329^{-1}\bmod 667=329^{615}\bmod 667=148$.

2. 求解同余式组

$$\begin{cases} 5x \equiv 4(\bmod 11) \\ 87x \equiv 16(\bmod 61) \end{cases}。$$

解：原同余式等价于

$$\begin{cases} x \equiv 3(\bmod 11) \\ x \equiv 10(\bmod 61) \end{cases}。$$

利用中国剩余定理可以求出该同余式组的解为

$x\equiv 498\bmod 671$。

3. 求解同余式 $f(x) \equiv x^4 + 7x + 1 \equiv 0(\bmod 27)$ 。

解：容易验证 $f(x) \equiv x^4 + 7x + 1 \equiv 0(\bmod 3)$ 的解为 $x\equiv 1\bmod 3$，因为 $f'(x)=4x^3+7, f'(1)=11$，所以可以得到 $f(x) \equiv x^4 + 7x + 1 \equiv 0(\bmod 9)$ 的解为 $x \equiv 1\bmod 9$ ，$f(x) \equiv x^4 + 7x + 1 \equiv 0(\bmod 27)$ 的解为 $x\equiv 10\bmod 27$

4. 求解同余式 $7x^7 \equiv 8(\bmod 41)$ 。

解：原同余式等价于 $x^7 \equiv 7(\bmod 41)$ ，先求出模 41 的最小原根为 6，建立 6 的指标表，查表可以得到 $7=6^{39}\bmod 41$，令 $x=6^y\bmod 41$，则得到同余式 $7y \equiv 39(\bmod 40)$ ，于是得到该一次同余式的解为 $y \equiv 17(\bmod 40)$，再次查表得到原同余式的解为 $x\equiv 26$（mod41）。

5.求群{0，1，2，3，4，5，6，7，8，9，10，11}（关于模 12 的加法）的所有子群。

解：因为该群 G 的阶为 12，12 的所有正因数为 1，2，3，4，6，12，于是该群的所有子群为 $G_1=\{0\}$，$G_2=\{0,6\}$,$G_3=\{0,4,8\}$,$G_4=\{0,3,6,9\}$,$G_5=\{0,2,4,6,8,10\}$,$G_6=G$。

6.构造有限域 GF(9),并且给出其加法和乘法表。

解：GF(9)={0,1,2,3,4,5,6,7,8}，先找一个 GF(3)[x]的一个 2 次不可约多项式 x^2+x+2,加法表为

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

乘法表为

*	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	7	1	4	5	8	2

4	0	4	8	1	5	6	2	3	7
5	0	5	7	4	6	2	8	1	3
6	0	6	3	5	2	8	7	4	1
7	0	7	5	8	3	1	4	2	6
8	0	8	4	2	7	3	1	6	5

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^3的最小多项式。

解：因为$|\alpha^3|=5$，$2^4 \bmod 5=1$，所以最小多项式为

$M(x)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12})=x^4+x^3+x^2+x+1$

8．求解递推关系

$$\begin{cases} f(n)=5f(n-1)-8f(n-2)+4f(n-3) \\ f(0)=0, f(1)=1, f(2)=2 \end{cases}。$$

解：特征方程$x^3-5x^2+8x-4=0$的根为1，2，2，x=2对应的根为$f_1(n)=c_1 2^n+c_2 n2^n$，对应x=1的根为$f_2(n)=c_3$，因此递推关系的通解为$f(n)= c_1 2^n+c_2 n2^n+c_3$,代入初始值得到方程组$c_1+c_3=0$，$2c_1+2c_2+c_3=1$，$4c_1+8c_2+c_3=2$，于是解得$c_1=2$，$c_2=-1/2$，$c_3=-2$，所以原递推关系的解为$f(n)= 2^{n+1}-n*2^{n-1}-2$。

二．证明：形如4k+1的素数有无穷多个。（10分）

证明　反证法。如果形如$4k+1$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

$$N=(2p_1p_2\cdots p_k)^2+1$$

因为N形如$4k+1$，$N>p_i, 1\le i\le k$，所以N为合数，设p为其任意一个素因数，则p为奇数，且$(p,p_i)=1, i=1,2,\cdots k$。

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

则存在整数a使得$\frac{p-1}{2}=2a$，即p是形如$4k+1$的素数，所以存在整数$1\le j\le k$，使得$p=p_j$，这与$(p,p_i)=1,i=1,2,\cdots k$矛盾。

三. 简述对有限域概念的理解。（10 分）

答: 一个有限集合 F 上面定义了两种二元运算加法和乘法，如果对于加法而言，（F,+）是一个交换群，关于加法的单位元为 0，对于乘法，（F-{0}，*）也是一个交换群，且关于加法和乘法满足左右分配律，则称(F,+,*)是一个有限域。