“信息安全数学基础（上）”试卷(A 卷)

一． 计算题（每题 10 分，共 60 分）。

1． 求整数 s 和 t，使得 793s+2769t=(793,2769)。

2． 31^{48413} mod 113。

3． 求解同余式 $x^3+5x^2+9\equiv 0$（mod 27）。

4． 判断同余式 $x^2\equiv 37$(mod 101)是否有解？有解时求出其所有解。

5． 求模 31 的所有原根，并且求解如下高次剩余

$x^6\equiv 2$(mod 31)。

6． （1）求相邻的四个整数，它们依次可被 4，9，25，49 整除；（2）求 13 的倍数，使得该数被 3，5，7，11 除的余数是 2。

二. 证明题（每题 10 分，共 20 分）

（1）设 a,b 为异奇偶的正整数，且(a,b)=1，证明$(a^2+b^2,a+b)=1$;

（2）设a,m是正整数，$(a,m)=1,0<a<m$，记集合$M=\{1,2,3,\cdots,m-1\}$。现对集合M中的每个数i涂上黑色或白色，要满足以下条件：（1）i和$m-i$要涂上同一种颜色;（2）当$i\neq a$时，i和$|a-i|$要涂上同一种颜色。证明：所有的数一定都涂上同一种颜色。

三. 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，$a_i\geq 1$为整数，且所有$p_i<A$，$A$为已知的小正整数。（事实上，对于一个素数而言，$a_i>1$的情况是很少出现的。）则

我们可令$\{p_1,p_2,\cdots,p_k\}$为所有小于A的素数，任意选取估计值$a\ge1$，令$r=\prod_{i=1}^{k}p_i^a$，则有$p-1\mid r$，由费马定理知$2^r\equiv1(\bmod p)$，即$p\mid(2^r-1)$。令$x=2^r \bmod n$，当$x=1$时，则选取下一个素数 3 代替 2，直到$x\ne1$为止。当$x\ne1$时，有$(x-1,n)=p$，于是可以将n因子分解得到p和q。试用这种方法分解整数$n=118829$。（提示：选取A为 14，$a=1$）（20 分）

答案

一 计算题（每题 10 分，共 60 分）。

1 解：因为 2769=793*3+390， 793=390*2+13， 390=13*30，即(793,2769)=13，
而 13=793-390*2=793-(2769-793*3)*2=793*7-2769*2
即 s=7,t=-2; (注意，此题答案不唯一)

2、解 因为$\varphi(113)=112$，48413=112*432+29，所以 31^{48413} mod 113=31^{29} mod 113，

$(29)_{10}=(11101)_2$，于是
m0=1,a0=31,b0=31, m1=0,a1=57,b1=31, m2=1,a2=85,b2=36, m3=1,a3=106,b3=87, m4=1,a4=49,b4=82
所以 31^{48413} mod 113=82

3 解 对于$f(x)=x^3+5x^2+9$，有$f'(x)=3x^2+10x$，直接验算，知同余式$f(x)\equiv0(\bmod 3)$有两个解$x\equiv0,1(\bmod 3)$。因为$f'(0)=0,f'(1)=13$，所以$3\mid f'(0),3\nmid f'(1)$，对于$x\equiv1(\bmod 3)$，依次求出对应的同余式$x^3+5x^2+9\equiv0(\bmod 27)$的解：$f'(1)\equiv1(\bmod 3)$，$f'(1)^{-1}\bmod 3=1$；其次，计算$t_1\equiv-\frac{f(1)}{3}f'(1)^{-1}\bmod 3\equiv1(\bmod 3)$，

$x_2\equiv1+3t_1\equiv4(\bmod 9)$，最后，计算$t_2\equiv-\frac{f(x_2)}{3^2}f'(1)^{-1}\bmod 3\equiv1(\bmod 3)$

$x_3\equiv x_2+3^2t_2\equiv13(\bmod 27)$。因此，对应于$x\equiv1(\bmod 3)$的同余式$f(x)\equiv0(\bmod 27)$的解为$x_3\equiv13(\bmod 27)$；对于$x\equiv0(\bmod 3)$，因为$f(0)\equiv9\equiv0(\bmod 9)$，所以$x\equiv0,3,6(\bmod 9)$都是同余式$f(x)\equiv0(\bmod 9)$的解。进一步，对于$x\equiv0(\bmod 9)$，因为$f(0)\equiv9\ne0(\bmod 27)$，所以$f(x)\equiv0(\bmod 27)$没有$x\equiv0(\bmod 9)$对应的解；对于$x\equiv3(\bmod 9)$，因为$f(3)\equiv0(\bmod 27)$，所以$x\equiv3,12,21(\bmod 27)$都是同余式

$f(x)\equiv 0(\bmod 27)$对应于 $x\equiv 3(\bmod 9)$的解；对于 $x\equiv 6(\bmod 9)$，因为 $f(6)\equiv 0(\bmod 27)$，所以 $x\equiv 6,15,24(\bmod 27)$都是同余式 $f(x)\equiv 0(\bmod 27)$对应于 $x\equiv 6(\bmod 9)$的解。即同余式$f(x)\equiv 0(\bmod 27)$的解为$x\equiv 3,6,12,13,15,21,24(\bmod 27)$。

4 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 $x\equiv 21,80(\bmod 101)$。

5 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 解 （1）设最小的一个数为 x，则

$x\equiv 0(\bmod 4), x+1\equiv 0(\bmod 9), x+2\equiv 0(\bmod 25), x+3\equiv 0(\bmod 49)$，

由中国剩余定理易解得$x\equiv 29348(\bmod 44100)$；

（2）设这个数为 13x，则 $13x\equiv 2(\bmod 3)$，$13x\equiv 2(\bmod 5)$，$13x\equiv 2(\bmod 7)$，

$13x\equiv 2(\bmod 11)$，

由中国剩余定理易解得$x\equiv 89(\bmod 1155)$。

二. 证明题（每题 10 分，共 20 分）

（1）证明：因为$a^2+b^2=(a+b)a+b(b-a)$，所以$(a^2+b^2, a+b)=(a+b, b(b-a))$，又因为 a+b=b+a，所以(a+b, b)=(b, a)=(a, b)=1,

从而$(a^2+b^2, a+b)=(a+b, b(b-a))=(a+b, a-b)=(a+b, 2b)=(a+b, 2)=1$.（最后一步用到了 a, b 异奇偶的条件）

（2）证 我们的想法是把要涂色的集合M扩充到全体整数，除已知两条外另外满足：（3）属于模m的同一个剩余类中的数涂上相同的颜色；（4）0和a要涂上同一种颜色。这样就可以对全体整数涂色，这样的涂色应该满足如下性质：

① 对任意的整数j，j和$-j$一定涂相同的颜色。因为对于任意的整数j，必存在整数i，使得$0\le i<m, j\equiv i(\bmod m)$，由（3）知$j$和$i$同色；而$-j\equiv -i\equiv m-i(\bmod m)$，所以由（3）知$-j$和$m-i$同色，从而由（1）和（4）知$-j$和$j$同色。

② 对任意的整数 j， $j和j-a$ 同色，从而属于模 a 的同一个剩余类中的数涂上相同的颜色。

因为对于任意的整数 j，必存在整数 i，使得 $0\le i<m, j\equiv i(\bmod m)$，由（3）知 $j和i$ 同色，而由（2）知 $i和|a-i|$ 同色，进而由①知，$i-a和|a-i|$ 同色，进而推出 $j和i-a$ 同色；由条件（3）知，属于模 m 的同一个剩余类中的数同色，因为 $j\equiv i(\bmod m)$，所以 $(i-a)\equiv(j-a)(\bmod m)$，因此 $j-a和i-a$ 同色，从而 $j和j-a$ 同色。

由①和②知，对于任意的整数 j， $j和j+sm+ta$ 同色，其中 $s和t$ 为任意的整数。由条件 $(a,m)=1$ 知，存在整数 s_1,t_1，使得 $s_1m+t_1a=1$，所以 $j和j+1$ 同色，即所有整数同色。

三. 解　　首先令 A 为 14，$a=1$，则

$$r=\prod_{i=1}^{k}p_i^a=2\times3\times5\times7\times11\times13=30030,$$

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

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

所以 $n=331\times359$。

“信息安全数学基础下册”试卷(A 卷)

一． 名词解释（20 分）

1.循环群；2.群同构；3.正规子群；4.有限域。

二．设 $\sigma=\begin{pmatrix}a&b&c&d&e&f\\b&c&d&e&a&f\end{pmatrix}$，$\tau=\begin{pmatrix}a&b&c&d&e&f\\d&e&b&c&f&a\end{pmatrix}$，

计算 $\sigma\tau$，$\tau\sigma$，σ^{-1}。（10 分）

三．求 4 阶对称群 S_4 的所有子群。（10 分）

四．求 $F_{2^4}=F_2[x]/(x^4+x+1)$ 中的生成元 $g(x)$，并且计算出所有的生成元。（15 分）

五．求模 6 剩余类加法群<Z_6,+>到模 7 剩余类乘法群<Z_7-{0}, ×>的所有同构映射。（15 分）

六．求$\{3\cdot a,4\cdot b,5\cdot c\}$的 10 组合数。（15 分）

七．求解递推关系

$$\begin{cases} f(n)=-f(n-1)+3f(n-2)+5f(n-3)+2f(n-4) \\ f(0)=1,f(1)=0,f(2)=1,f(3)=2. \end{cases}$$ 。（15 分）

答案(A 卷)

一 名词解释（每小题 5 分，共 20 分）。

1 循环群: 设$<G,\ *>$为群，如果存在一个元素$a\in G$，使$G=\{a^k\mid k\in Z\}$，则称G为循环群，记作$G=<a>$，称a是G的生成元；

2 群同构: 设$(R_1,+)$和$(R_2,\oplus)$是两个群，函数$f:R_1\to R_2$是一一映射，若任意$a,b\in R_1$，有$f(a+b)=f(a)\oplus f(b)$，则称f是$(R_1,+)$到$(R_2,\oplus)$的群同构；

3 正规子群：设 H 是 G 的子群,如果对 H 中的任意元素 a,都有 aH=Ha，则称 H 是 G 的正规子群。

4 有限域：设$(R,+,\bullet)$是交换环，如果对于 R 的每一个非零元素，关于运算$\bullet$都有可逆元，且集合 R 中元素个数有限，则称$(R,+,\bullet)$为有限域。

二、解

$$\sigma\tau=\begin{pmatrix} a & b & c & d & e & f \\ e & b & c & f & d & a \end{pmatrix};$$

$$\tau\sigma=\begin{pmatrix} a & b & c & d & e & f \\ e & a & c & d & f & b \end{pmatrix};$$

$$\sigma^{-1}=\begin{pmatrix} a & b & c & d & e & f \\ e & a & b & c & d & f \end{pmatrix};$$

三 求 4 阶对称群 S4 的所有子群。（10 分）

解：一阶子群{（1）}

二阶子群{（1），（12）}，{（1），（13）}，{（1），（14）}，{（1），（23）}，{（1），（24）}，{（1），（34）}，{（1），（12）(34)}，{（1），（13）(24)}，{（1），（14）(23)}

三阶子群{（1），（123），（132）}，{（1），（124），（142）}，{（1），（134），（143）}，{（1），（234），（243）}

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）}

六阶子群{（1），（12），（13），（23），（123），（132）}，{（1），（12），（14），（24），（124），

（142）}，{（1），（13），（14），（34），（134），（143）}，{（1），（23），（24），（34）（234），（243）}

八阶子群{（1），（1234），（13）（24），（1432），(13),(24),(12)(34),(14)(23)},{（1），（1243），（13）（24），（1342），(14),(23),(12)(34),(14)(23)}, {（1），（1324），（13）（24），（1423），(12),(34),(12)(34),(14)(23)}

二十四阶子群 S4

四、解: 首先判断 x 为 $F_{2^4}=F_2[x]/(x^4+x+1)$ 的生成元，（k, 15）=1，则 x^k 为所有的生成元。

k=1, 2, 4, 7, 8, 11, 13, 14， x^k 分别为：

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

五、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

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

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

六、解 令$S_\infty=\{\infty\cdot a,\infty\cdot b,\infty\cdot c\}$，则$S_\infty$的 10 组合数为

$$\binom{10+3-1}{10}=\binom{12}{2}=66$$

设集合 A 是 S_∞ 的 10 组合数全体，则 $|A|=66$，现在要求在 10 组合数中 a 的个数小于等于 3，b 的个数小于等于 4，c 的个数小于等于 5。定义性质集合 $P=\{P_1,P_2,P_3\}$，其中：

P_1：10 组合数中 a 的个数大于等于 4；

P_2：10 组合数中 a 的个数大于等于 5；

P_3：10 组合数中 a 的个数大于等于 6；

将满足性质 P_i 的 10 组合全体记为 $A_i\,(1\le i\le 3)$，那么 A_1 中的元素可以看作是由 S_∞ 的 10-4=6 组和再拼上 4 个 a 构成的，所以

$$|A_1| = \binom{10-4+3-1}{10-4} = \binom{8}{6} = 28$$

类似地，有

$|A_2| = \binom{10-5+3-1}{10-5} = \binom{7}{5} = 21$， $|A_3| = \binom{10-6+3-1}{10-6} = \binom{6}{4} = 15$，

$|A_1 \cap A_2| = \binom{10-4-5+3-1}{10-4-5} = \binom{3}{1} = 3$， $|A_1 \cap A_3| = \binom{10-4-6+3-1}{10-4-6} = \binom{2}{0} = 1$，

$|A_2 \cap A_3| = 0$，$|A_1 \cap A_2 \cap A_3| = 0$。

而 a 的个数小于等于 3，b 的个数小于等于 4，c 的个数小于等于 5 的 10 组合全体为 $\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$，根据容斥原理知，它的元素个数为

$$|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| = |A| - (|A_1| + |A_2| + |A_3|) + (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_3|) - |A_1 \cap A_2 \cap A_3|$$
$$= 66 - (28+21+15) + (3+1+0) - 0 = 6$$

七、解 该递推关系的特征方程为 $x^4 + x^3 - 3x^2 - 5x - 2 = 0$，特征根为

$$x_1 = x_2 = x_3 = -1, x_4 = 2.$$

对应于 $x = -1$ 的解为 $f_1(n) = c_1(-1)^n + c_2 n(-1)^n + c_3 n^2 (-1)^n$；对应于 $x = 2$ 的解为 $f_2(n) = c_4 2^n$，因此递推关系的通解为

$$f(n) = f_1(n) + f_2(n) = c_1(-1)^n + c_2 n(-1)^n + c_3 n^2(-1)^n + c_4 2^n$$

代入初始值，得到方程组

$$\begin{cases} c_1 + c_4 = 1 \\ -c_1 - c_2 - c_3 + 2c_4 = 0 \\ c_1 + 2c_2 + 4c_3 + 4c_4 = 1 \\ -c_1 - 3c_2 - 9c_3 + 8c_4 = 2 \end{cases}$$

解这个方程组得

$$c_1 = \frac{7}{9}, c_2 = -\frac{1}{3}, c_3 = 0, c_4 = \frac{2}{9}$$

所以，原递推关系的解为

$$f(n) = (-1)^n \frac{7}{9} - (-1)^n \frac{1}{3} n + \frac{2}{9} \cdot 2^n.$$