武汉大学计算机学院 2007-2008 学年第一学期

"信息安全数学基础（上）"(A 卷)答案

一 计算题（每题 10 分，共 60 分）。

1 求整数 s 和 t，使得 793s+2769t=(793,2769)。

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 31^{48413} mod 113。

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 求解同余式 $x^3+5x^2+9\equiv 0$（mod 27）。

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

$x_2\equiv 1+3t_1\equiv 4(\bmod 9)$，最后，计算 $t_2\equiv -\dfrac{f(x_2)}{3^2}f'(1)^{-1}\bmod 3\equiv 1(\bmod 3)$

$x_3\equiv x_2+3^2t_2\equiv 13(\bmod 27)$。因此，对应于 $x\equiv 1(\bmod 3)$ 的同余式 $f(x)\equiv 0(\bmod 27)$ 的解为 $x_3\equiv 13(\bmod 27)$；对于 $x\equiv 0(\bmod 3)$，因为 $f(0)\equiv 9\equiv 0(\bmod 9)$，所以 $x\equiv 0,3,6(\bmod 9)$ 都是同余式 $f(x)\equiv 0(\bmod 9)$ 的解。进一步，对于 $x\equiv 0(\bmod 9)$，因为 $f(0)\equiv 9\not\equiv 0(\bmod 27)$，所以 $f(x)\equiv 0(\bmod 27)$ 没有 $x\equiv 0(\bmod 9)$ 对应的解；对于 $x\equiv 3(\bmod 9)$，因为 $f(3)\equiv 0(\bmod 27)$，所以 $x\equiv 3,12,21(\bmod 27)$ 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 判断同余式 $x^2\equiv 37$(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$x \equiv 21,80(\bmod 101)$。

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（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。

`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）设 a, b 为异奇偶的正整数，且(a, b)=1，证明

$(a^2+b^2, a+b)=1$；

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）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。

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 $n=331\times359$。