No: C4

Date:

T1. (1) $3x \equiv 2 \bmod 7$

解：①法一：模7的最小非负完全剩余系为 0, 1, 2, 3, 4, 5, 6. 逐个代入 x 验算得 方程有唯一解 $x \equiv 3 \bmod 7$.

②法二：$(3,7)=1$，故方程有唯一解 $x \equiv 2 \times 3^{\varphi(7)-1} \bmod 7 \equiv 2 \times 3^5 \pmod{7}$

得 $x \equiv 3 \bmod 7$.

(3) $23x \equiv 1 \bmod 140$

解：模因数140较大，使用中国剩余定理 将方程化为模数较小的同余方程组。$140 = 2^2 \cdot 5 \cdot 7$，方程等价于

$$\begin{cases} 23x \equiv 1 \bmod 2 \\ 23x \equiv 1 \bmod 5 \\ 23x \equiv 1 \bmod 7 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \bmod 2 \\ 3x \equiv 1 \bmod 5 \\ 2x \equiv 1 \bmod 7 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 5 \\ x \equiv 4 \bmod 7 \end{cases}$$

$M_1 = 35$，$M_2 = 14$，$M_3 = 10$，得

$e_1 \equiv M_1^{-1} \bmod 2 = 1$，$e_2 = M_2^{-1} \bmod 5 = 4$，$e_3 = M_3^{-1} \bmod 7 = 5$

所以，

$x \equiv (35 \times 1 \times 1 + 14 \times 4 \times 2 + 10 \times 5 \times 4) \bmod 140 \equiv 67 \bmod 140$

T4. 证明:(中国剩余定理的推广) 使用数学归纳法证明。由题意 $k\geq 2$.

① $k=2$ 时,存在性: 方程组为 $\begin{cases} x\equiv a_1 \bmod m_1 \\ x\equiv a_2 \bmod m_2 \end{cases}$ (1),由定义得

$\begin{cases} x = a_1+m_1q_1 \quad (q_1,q_2\in Z) \\ x = a_2+m_2q_2 \end{cases}$ $\Rightarrow$ $m_2q_2 = a_1-a_2+m_1q_1$

即 $m_2q_2 \equiv a_1-a_2 \bmod m_1$

该方程有解的充要条件为 $(m_2,m_1)\mid a_1-a_2$,此时 q_1,q_2 存在,
(变量为 q_2) 即使方程组成立的 x 存在,方程组有解.

② $k=2$ 时,解的唯一性: 设 (1) 的一个解为 A_1,假设存在其他解 $A_1' \neq A_1$,则 $A_1\equiv A_1' \bmod M_1$,其中 $M_1=[m_1,m_2]$,在中国剩余定理中已证明在 M_1 范围内解唯一,则 $A_1'=A_1$,方程组 (1) 解唯一.

③ 数学归纳法: 由①② 可将 (1) 等价于 $x\equiv A_1 \bmod M_1$,当 $k\geq 2$ 时,假设 k 个方程组已等效为一个方程 $x\equiv A_k \bmod M_k$,其中 $M_k=[m_1,\cdots m_k]$ $\forall i\in\{1,2,\cdots k\}$ 均满足 $A_k\equiv a_i \bmod m_i$,在此基础上添加一个方程 $x\equiv a_{k+1} \bmod m_{k+1}$,需满足有解条件,即 $\forall i\in\{1,2,\cdots k\}$ 均有 $(m_i,m_{k+1})\mid a_i-a_{k+1}$ $\Rightarrow$ $a_i\equiv a_{k+1} \bmod (m_i,m_{k+1})$

又 $A_k\equiv a_i \bmod m_i$,$(m_i,m_{k+1})\mid m_i$,得

$A_k\equiv a_{k+1} \bmod (m_i,m_{k+1})$ $\Rightarrow$ $A_k\equiv a_{k+1} \bmod [(m_1,m_{k+1}),\cdots(m_k,m_{k+1})]$

$\Rightarrow A_k\equiv a_{k+1} \bmod ((m_{k+1},[m_1,\cdots,m_k]))$ $\Rightarrow$ $A_k\equiv a_{k+1} \bmod (m_{k+1},M_k)$

$\Rightarrow (M_k,m_{k+1})\mid A_k-a_{k+1}$,则 $\begin{cases} x\equiv A_k \bmod M_k \\ x\equiv a_{k+1} \bmod m_{k+1} \end{cases}$ 有解,方程可等效为 $x\equiv A_{k+1} \bmod M_{k+1}$,$M_{k+1}=[m_1,\cdots,m_{k+1}]$

No:

Date:

综上，$n=k$时成立，则$n=k+1$时也成立，$k\geq 2$时题设结论均成立，证毕.（将中国剩余定理推广到m_i无两两互素限制）

T5. 求解 $3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\equiv 0 \mod 5$.

解：①法一：作多项式的欧几里得除法得

左边 $=(3x^9+4x^8+2x^6+3x^5+5x^4+2x^2+4x+5)(x^5-x)+3x^3+16x^2+6x$

方程等价于 $3x^3+16x^2+6x\equiv 3x^3+x^2+x \mod 5 \equiv 0$ 将 $0,\pm1,\pm2$ 代入验算得 $x\equiv 0,1,2 \mod 5$.

②法二：由Euler定理得 $x^4\equiv 1 \mod 5$，则有

$x^{14}\equiv x^{3\cdot 4+2} \mod 5\equiv x^2 \mod 5$，$x^{13}\equiv x \mod 5$，$x^{11}\equiv x^3 \mod 5$，

$x^9\equiv x \mod 5$，$x^6\equiv x^2 \mod 5$，原方程等价于

$3x^3+x^2+6x\equiv 0 \mod 5$，将 $0,\pm1,\pm2$ 代入验算得

$x\equiv 0,1,2 \pmod 5$