武漢大學
WUHAN UNIVERSITY
Wuhan 430072, Hubei, P.R.China 中国·武汉 Tel.(027)

信安数基第4次作业-路不亨-2022302181149

(4) : 2-1: $y^2 = x^3-2x+3 \pmod 7$

$x=0, y^2=3 \pmod 7$，无解；$x=1, y^2=2 \pmod 7$，$y=3,4 \pmod 7$

$x=2, y^2=0 \pmod 7$，$y=0 \pmod 7$，$x=3, y^2=3 \pmod 7$，无解

$x=4, y^2=3 \pmod 7$，无解，$x=5, y^2=6 \pmod 7$，无解

$x=6, y^2=4 \pmod 7$，$y=2,5 \pmod 7$

共有5个点 分别是 $(0,3), (0,4), (6,2), (6,5), (2,0)$

(10) 求解同余式 $x^2 \equiv 79 \pmod{105}$

$$x^2 \equiv 79 \pmod{105} \Rightarrow \begin{cases} x^2 \equiv 79 \pmod 5 \equiv 4 \pmod 5 \\ x^2 \equiv 79 \pmod 3 \equiv 1 \pmod 3 \\ x^2 \equiv 79 \pmod 7 \equiv 2 \pmod 7 \end{cases}$$

$M_1=21, M_2=35, M_3=15$　　$x=x_1=\pm 2 \pmod 5$

$M_1' \equiv 1 \pmod 5$, $M_2' \equiv 2 \pmod 3$, $M_3' \equiv 4 \pmod 7$　　$x=x_2=\pm 1 \pmod 5$　$x=x_3=\pm 3 \pmod 7$

由中国剩余定理，原方程解为 $x=b_1\times 21+b_2\times 70+b_3\times 60 \pmod{105}$

$x_1 \equiv 2\times 21+1\times 70+3\times 60 \pmod{105} \equiv 82 \pmod{105}$

$x_2 \equiv 2\times 21+1\times 70-3\times 60 \pmod{105} \equiv 37 \pmod{105}$

$x_3 \equiv 2\times 21-70+3\times 60 \pmod{105} \equiv 47 \pmod{105}$

$x_4 \equiv 2\times 21-70-3\times 60 \pmod{105} \equiv 2 \pmod{105}$

$x_5 \equiv -2\times 21+70+3\times 60 \pmod{105} \equiv 103 \pmod{105}$

$x_6 \equiv -2\times 21-70+3\times 60 \pmod{105} \equiv 68 \pmod{105}$

$x_7 \equiv -2\times 21+70-3\times 60 \pmod{105} \equiv 58 \pmod{105}$

$x_8 \equiv -2\times 21-70-3\times 60 \pmod{105} \equiv 23 \pmod{105}$

20. $\left(\frac{151}{373}\right) = (-1)^{\frac{151^2-1}{2}\cdot\frac{373^2-1}{2}}\left(\frac{373}{151}\right) = (-1)^{(75\times152)(186\times372)} = 1\times\left(\frac{373}{151}\right) = \left(\frac{71}{151}\right)$

$= (-1)^{\frac{151^2-1}{2}\cdot\frac{71^2-1}{2}}\left(\frac{151}{71}\right) = (-1)^{75\times151\times35\times72} = \left(\frac{151}{71}\right) = \left(\frac{9}{71}\right) = 1$

$\left(\frac{911}{2003}\right) = (-1)^{\frac{911^2-1}{2}\cdot\frac{2003^2-1}{2}}\left(\frac{2003}{911}\right) = (-1)^{455\times912\cdot1001\times2004}\left(\frac{2003}{911}\right) = \left(\frac{181}{911}\right) = (-1)^{90\times182}\left(\frac{911}{181}\right)$

$= \left(\frac{6}{181}\right)$

$= \left(\frac{2}{181}\right)\left(\frac{3}{181}\right) = (-1)^{\frac{181^2-1}{8}}\left(\frac{1}{3}\right)(-1)^{\frac{3^2-1}{2}\cdot\frac{181^2-1}{2}} = (-1)^{48\times91} = -1$

$\left(\frac{37}{200723}\right) = \left(\frac{200723}{37}\right)(-1)^{\frac{37^2-1}{2}\cdot\frac{200723^2-1}{2}} = \left(\frac{200723}{37}\right)(-1)^{(36\times19)\times100362\times200722}$

$= \left(\frac{13}{37}\right) = (-1)^{\cancel{40}\times18\times18\times38} = \left(\frac{13}{19}\right)$

$= \left(\frac{-1}{13}\right) = -1^{\frac{13-1}{2}} = -1$

(22) ① $x^2 \equiv -2 \pmod{67}$

$\left(\frac{-2}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{-1}{67}\right) = (-1)^{\frac{67^2-1}{8}}(-1)^{\frac{67-1}{2}} = 1$，原方程有2个解

② $x^2 \equiv 2 \pmod{67}$ $\left(\frac{2}{67}\right) = (-1)^{\frac{67^2-1}{8}} = -1$，原方程无解

(26) ① $x^2 \equiv 7 \pmod{227}$ $\left(\frac{7}{227}\right) \equiv (-1)^{\frac{7^2-1}{2}\cdot\frac{227^2-1}{2}}\left(\frac{227}{7}\right) \equiv \left(\frac{3}{7}\right) = (-1)^{\frac{7^2-1}{2}\cdot\frac{3^2-1}{2}}\left(\frac{1}{3}\right) = 1$

有解

③ $11x^2 \equiv -6 \pmod{91}$

$\Rightarrow \begin{cases} 11x^2 \equiv -6 \pmod{7} \\ 11x^2 \equiv -6 \pmod{13} \end{cases}$

$\left(\frac{11}{7}\right) = \left(\frac{-6}{7}\right) = 1$,

$\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1 = \left(\frac{-6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{\frac{7-1}{2}} = -1$

有解

(33) $p = 401$，$q = 281$ 求解同余式 (1) $x^2 \equiv 11 \pmod{pq}$

$\Rightarrow \begin{cases} x^2 \equiv 11 \pmod{401} \\ x^2 \equiv 11 \pmod{281} \end{cases}$

$\left(\frac{11}{401}\right) = \left(\frac{401}{11}\right)(-1)^{\frac{11^2-1}{2}\cdot\frac{401^2-1}{2}} = \left(\frac{5}{11}\right) = \left(\frac{1}{5}\right) = 1$

$\left(\frac{11}{281}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)^{\frac{11^2-1}{8}}\left(\frac{2}{3}\right) = (-1)(-1) = -1$

故同余式无解