参考答案.

一. 1) $748 = 2\times357 + 34$. $357 = 10\times34 + 17$.

$34 = 2\times17 + 0$. 故 $(748, 357) = 17$

2. 也可用矩阵的方法

$$\begin{pmatrix} 1 & 748 \\ 1 & 357 \end{pmatrix} \to \begin{pmatrix} 1 & -2 & 34 \\ 1 & & 357 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & -2 & 34 \\ -10 & 21 & 17 \end{pmatrix} \to \begin{pmatrix} 21 & -43 & \\ -10 & 21 & 17 \end{pmatrix}$$

可得. 该不定方程的一个特解 $\begin{cases} x = -10 \\ y = 21 \end{cases}$

故其所有整数解为 $\begin{cases} x = -10 + 21t \\ y = 21 - 44t \end{cases}$ $t \in \mathbb{Z}$.

二. 所有小于等于20的素数为 2, 3, 5, 7, 11, 13, 17, 19

$\alpha(2, 20) = [\frac{20}{2}] + [\frac{20}{2^2}] + [\frac{20}{2^3}] + [\frac{20}{2^4}] = 18$.

$\alpha(3, 20) = [\frac{20}{3}] + [\frac{20}{3^2}] = 8$.

$\alpha(5, 20) = [\frac{20}{5}] = 4$

$\alpha(7, 20) = [\frac{20}{7}] = 2$

$[\frac{20}{11}] = [\frac{20}{13}] = [\frac{20}{17}] = [\frac{20}{19}] = 1$

故 $20! = 2^{18}\cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

三. 1) 由费马小定理.

$5^{16} \equiv 1 \pmod{17}$.

故 $5^{2022} = 5^{16\times126+6} \equiv 5^6 \equiv 8^3 \equiv 2 \pmod{17}$

2. $\varphi(10) = 4$. 由欧拉定理.

$7^4 \equiv 1 \pmod{10}$. 故.

$7^{1015} \equiv 7^{4\times253+3} \equiv 7^3 \equiv 3 \pmod{10}$

故 7^{1015} 的个位数为 3.

四. 方程组等价于 $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv -3 \pmod 2 \\ x \equiv -3 \pmod 7 \end{cases}$

$\Leftrightarrow$ $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv -3 \pmod 7 \end{cases}$ 则 $\begin{cases} M_1 = 42, & M_1^{-1} \equiv 3 \pmod 5 \\ M_2 = 35, & M_2^{-1} \equiv -1 \pmod 6 \\ M_3 = 30, & M_3^{-1} \equiv 4 \pmod 7 \end{cases}$

由孙子定理，解得 $x \equiv 2\times 42\times 3 + 1\times 35\times(-1) - 3\times 30\times 4$

$= -143 \equiv 67 \pmod{210}$.

四. ① $\begin{cases} x\equiv 2 \pmod 5 \\ x\equiv 1 \pmod 6 \\ x\equiv -3 \pmod{10} \end{cases} \Leftrightarrow \begin{cases} x\equiv 2 \pmod 5 \\ x\equiv 1 \pmod 2 \\ x\equiv 1 \pmod 3 \\ x\equiv -3 \pmod 2 \\ x\equiv -3 \pmod 5 \end{cases}$

$\Leftrightarrow \begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 1 \pmod 3 \\ x\equiv 2 \pmod 5 \end{cases}$ 取 $\begin{cases} M_1=15, & M_1^{-1}\equiv 1 \pmod 2 \\ M_2=10 & M_2^{-1}\equiv 1 \pmod 3 \\ M_3=6 & M_3^{-1}\equiv 1 \pmod 5 \end{cases}$

由孙子定理，解得 $x \equiv 1\times 15\times 1 + 1\times 10\times 1 + 2\times 6\times 1$

$= 37 \equiv 7 \pmod{30}$.

五. 计算 Legendre 符号 $\left(\frac{-110}{271}\right) = \left(\frac{-1}{271}\right)\cdot\left(\frac{2}{271}\right)\cdot\left(\frac{5}{271}\right)\cdot\left(\frac{11}{271}\right)$

$\left(\frac{-1}{271}\right) = (-1)^{\frac{271-1}{2}} = -1$. $\left(\frac{2}{271}\right) = (-1)^{\frac{271^2-1}{8}} = 1$

由二次互反律，$\left(\frac{5}{271}\right) = \left(\frac{271}{5}\right)\cdot(-1)^{\frac{271-1}{2}\cdot\frac{5-1}{2}}$

$= \left(\frac{1}{5}\right) = 1$.

$\left(\frac{11}{271}\right) = \left(\frac{271}{11}\right)\cdot(-1)^{\frac{271-1}{2}\cdot\frac{11-1}{2}} = -\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right)(-1)^{\frac{11-1}{2}\cdot\frac{7-1}{2}}$

$= \left(\frac{4}{7}\right) = 1$.

故 $\left(\frac{-110}{271}\right) = -1$. 故此二次同余方程无解.

（判断二次剩余，还用 Legendre 符号）.

Legendre 符号二次互反律 P. 8 此证明方法参考.

三. 由题得同余方程.

$8y \equiv 6 \pmod{22}$.

解得 $y = 9, 20$. 故原方程化为求方

$x \equiv 5^9 = (5^2)^4\cdot 5 \equiv 2^4\cdot 5 \equiv 11 \pmod{23}$.

或 $x \equiv 5^{20} = (5^2)^{10} = 2^{10} = 12 \pmod{23}$

即 $x \equiv \pm 11 \pmod{23}$.

七. 解 $x^2 \equiv 10 \pmod{13}$ 的解.

$x \equiv \pm 6 \pmod{13}$.

令 $x = \pm 6 + 13y$. 则

$2\times(\pm 6)\,y \equiv -\frac{(\pm 6)^2 - 10}{13} \pmod{13}$.

即 $\pm 12y \equiv -2 \pmod{13}$.

解得. $y \equiv \pm 32 \pmod{13}$

故原方程的解为 $x \equiv \pm 32 \pmod{13^2}$.

八. $\sqrt{11} = 3 + \sqrt{11} - 3 = 3 + \frac{1}{\frac{\sqrt{11}+3}{2}} = 3 + \frac{1}{3 + \frac{\sqrt{11}-3}{2}}$

$= 3 + \frac{1}{3 + \frac{1}{6 + \sqrt{11} - 3}} = \cdots$

故 $\sqrt{11} = [3, 3, 6, 3, 6, \cdots]$.

则其渐近分数为

$3, \frac{10}{3}, \frac{63}{19}, \frac{199}{60}, \cdots$

$19 \times 60 = 1140 > 10^3$. 故其渐近分数为 $\frac{63}{19}$.

(写 $\frac{63}{19}, \frac{199}{60}, \cdots$ 之后说明也可以)

九. 反证法. 假设 $n \mid 2^n - 1$.

由 $2^n - 1$ 为奇数. 可知. n 为奇数.

设 p 为 n 的最小的素因子. 则 $p > 2$.

于是 $2^n - 1 \equiv 0 \pmod{p}$.

由费马小定理. $2^{p-1} - 1 \equiv 0 \pmod{p}$

设 2 模 p 的指数为 r. 则.

$r \mid n$. 且 $r \mid p-1$. 故 $r \mid (n, p-1)$.

又因为 p 为 n 的最小素因子. 所以 $r = 1$.

即 $2^1 \equiv 1 \pmod{p}$. 矛盾!

故 $n \nmid 2^n - 1$.

十. 反证法. 假设 $p \nmid a$.

由 $p \mid n$. $\Rightarrow$ $a^2 + b^2 \equiv 0 \pmod{p}$.

$\Rightarrow$ $1 + (\frac{b}{a})^2 \equiv 0 \pmod{p}$ $\Rightarrow$ $(\frac{b}{a})^2 \equiv -1 \pmod{p}$

$\Rightarrow -1$ 模 p 为二次剩余. $\Rightarrow p \equiv 1 \pmod{4}$. 矛盾!

故 $p \mid a$. 则 $b^2 = n - a^2$ 为 p 的倍数. $\Rightarrow p \mid b$.

$\Rightarrow p^2 \mid a^2 + b^2 = n$.

五. 也可利用 Jacobi 符号进行计算.

$$\left(\frac{-110}{271}\right)=\left(\frac{161}{271}\right)=\left(\frac{271}{161}\right)\cdot(-1)^{\frac{161-1}{2}\cdot\frac{271-1}{2}}$$

$$=\left(\frac{110}{161}\right)=\left(\frac{110}{23}\right)\cdot\left(\frac{110}{7}\right)$$

$$=\left(\frac{18}{23}\right)\cdot\left(\frac{5}{7}\right)$$

$$=\left(\frac{2}{23}\right)\cdot\left(\frac{3^2}{23}\right)\cdot\left(\frac{7}{5}\right)\cdot(-1)^{\frac{7-1}{2}\cdot\frac{5-1}{2}}$$

$$=\left(\frac{2}{23}\right)\cdot\left(\frac{2}{5}\right)=-1.$$