1. Division med 4 ger den ekvivalenta kongruensen $187x \equiv 3 \pmod{498}$. Vi beräkar $\text{sgd}(498, 187)$ med Euklides algoritm:

$$\begin{aligned} 498 &= 3 \cdot 187 - 63 \\ 187 &= 3 \cdot 63 - 2 \\ 63 &= 31 \cdot 2 + 1. \end{aligned}$$

   Alltså är $\text{sgd}(498, 187) = 1$. Uträkning baklänges ger

$$\begin{aligned} 1 &= 63 - 31 \cdot 2 = 63 - 31(3 \cdot 63 - 187) = 31 \cdot 187 - 92 \cdot 63 \\ &= 31 \cdot 187 - 92(3 \cdot 187 - 498) = 92 \cdot 498 - 245 \cdot 187. \end{aligned}$$

   Alltså är $187 \cdot (-245) \equiv 1 \pmod{498}$, och kongruensen har lösning

$$x \equiv -245 \cdot 3 \equiv 261 \pmod{498}.$$

2. Systemet skrivs om som

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod 7. \end{cases}$$

   Vi har $M_1 = 5 \cdot 7 = 35$, $M_2 = 4 \cdot 7 = 28$ och $M_3 = 4 \cdot 5 = 20$. Kongruenserna $M_i x_i \equiv 1 \pmod{m_i}$ har lösningar $x_1 = 3$, $x_2 = 2$ och $x_3 = -1$. Enligt kinesiska restsatsen ges alla lösningar till systemet av

$$\begin{aligned} x &\equiv \sum b_i M_i x_i = 1 \cdot 35 \cdot 3 + 4 \cdot 28 \cdot 2 + 3 \cdot 20 \cdot (-1) \\ &= 105 + 224 - 60 = 269 \equiv 129 \pmod{140}. \end{aligned}$$

   Den minsta positiva lösningen är $x = 129$.

3. (a) Eftersom alla termer är positiva måste $y^2 \leq 30/7 < 5$ varav $|y| \leq 2$. Prövning ger att den enda möjligheten är $y = \pm 2$ och $x = \pm 1$.

   (b) Reduktion modulo 3 ger $-x^2 - y^2 \equiv 0 \pmod 3$. Då en kvadrat är kongruent med 0 eller 1 modulo 3 är den enda möjligheten att $x \equiv y \equiv 0 \pmod 3$. Då är $x^2 \equiv y^2 \equiv 0 \pmod{3^2}$ vilket medför att $9 | 2x^2 - 7y^2 = 30$, vilket är omöjligt. Alltså har ekvationen inga lösningar.

4. Faktorisering ger $2006 = 2 \cdot 17 \cdot 59$. Vi beräknar Legendresymbolen:

$$\begin{aligned}\left(\frac{2006}{2741}\right) &= \left(\frac{2}{2741}\right)\left(\frac{17}{2741}\right)\left(\frac{59}{2741}\right) \\ &= (-1)\left(\frac{2741}{17}\right)\left(\frac{2741}{59}\right) && \text{(Strayer 4.8 och 4.9)} \\ &= -\left(\frac{4}{17}\right)\left(\frac{27}{59}\right) = -\left(\frac{3}{59}\right)^3 = \left(\frac{59}{3}\right) && \text{(Strayer 4.9)} \\ &= \left(\frac{2}{3}\right) = -1.\end{aligned}$$

   Alltså är 2006 en kvadratisk icke-rest modulo 2741, och kongruensen saknar lösning.

5. Strayer avsnitt 2.6.

6. Om x och y båda är jämna så måste z också vara jämnt. Detta är uteslutet eftersom trippeln var primitiv, dvs $\text{sgd}(x, y, z) = 1$. Om x och y båda är udda så är $x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4$, men kongruensen $z^2 \equiv 2 \pmod 4$ har inga lösningar.

7. Eftersom $\text{ord}_m(a)$ delar $\phi(m)$ gäller $m - 1 | \phi(m)$. Men $\phi(m) \leq m - 1$ då $m > 1$, så vi måste ha $\phi(m) = m - 1$. Detta medför att m är ett primtal: Om $m = 2$ är detta klart, och om $m > 2$ och m vore sammansatt så skulle det finnas en delare k till m med $2 \leq k \leq m - 1$, och detta skulle medföra $\phi(m) < m - 1$.

8. För att få bort det obekanta k kan man dela s_1 med s_2. Detta ger

$$s_1 s_2^{-1} \equiv (m_1 - x r_1)(m_2 - x r_2)^{-1} \pmod{p-1}$$

   varav

$$\begin{aligned}& s_1 s_2^{-1}(m_2 - x r_2) \equiv m_1 - x r_1 \pmod{p-1} \\ \iff\ & s_1 s_2^{-1} m_2 - m_1 \equiv -x r_1 + x s_1 s_2^{-1} r_2 \\ \iff\ & x \equiv (s_1 s_2^{-1} m_2 - m_1)(s_1 s_2^{-1} r_2 - r_1)^{-1}.\end{aligned}$$

   Uppgiften visar att det är fatalt att använda samma k vid flera olika signeringar!