1. Strayer 1.19.

2. Vi använder Euklides algoritm för att finna $\text{sgd}(1290, 348)$.

$$\begin{aligned} 1290 &= 3 \cdot 348 + 246 \\ 348 &= 1 \cdot 246 + 102 \\ 246 &= 2 \cdot 102 + 42 \\ 102 &= 2 \cdot 42 + 18 \\ 42 &= 2 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 \end{aligned}$$

   Alltså är $\text{sgd}(1290, 348) = 6$. Eftersom $6 \mid 24$ har ekvationen lösning. Vi uttrycker 6 som en linjärkombination av 1290 och 348:

$$\begin{aligned} 6 &= 42 - 2 \cdot 18 \\ &= 42 - 2(102 - 2 \cdot 42) = 5 \cdot 42 - 2 \cdot 102 \\ &= 5(246 - 2 \cdot 102) - 2 \cdot 102 = 5 \cdot 246 - 12 \cdot 102 \\ &= 5 \cdot 246 - 12(348 - 246) = 17 \cdot 246 - 12 \cdot 348 \\ &= 17(1290 - 3 \cdot 348) - 12 \cdot 348 \\ &= 17 \cdot 1290 - 63 \cdot 348. \end{aligned}$$

   Multiplikation med 4 ger

$$24 = 68 \cdot 1290 - 252 \cdot 348,$$

   och en partikulärlösning till den givna ekvationen är därför $(x_0, y_0) = (68, -252)$. Samtliga lösningar ges därför av

$$\begin{cases} x = 68 + \dfrac{348}{6} n = 68 + 58n \\ y = -252 - \dfrac{1290}{6} n = -252 - 215n \end{cases}$$

   för alla $n \in \mathbb{Z}$. Genom att substituera $n - 1$ för n kan vi få en ekvivalent lösning med mindre tal:

$$\begin{cases} x = 68 + \dfrac{348}{6} n = 10 + 58n \\ y = -252 - \dfrac{1290}{6} n = -37 - 215n. \end{cases}$$

3. Villkoren innebär att vi ska lösa systemet

$$\begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

Enligt kinesiska restsatsen har detta en entydig lösning modulo 140. De två sista ekvationerna är ekvivalenta med $x \equiv 2 \pmod{35}$. Vi behöver nu bara se till att den första ekvationen också är uppfylld, och finner lätt att $x = 2 \cdot 35 + 2 = 72$ fungerar. Lösningen är därför $x \equiv 72 \pmod{140}$.

4. $s^2 \equiv t^2 \pmod{m} \iff m \mid (s+t)(s-t)$. Om m vore ett primtal eller 1, så skulle detta medföra att $m \mid s+t$ eller $m \mid s-t$ (Strayer 1.14). Men detta strider mot att $s \not\equiv \pm t \pmod{m}$. Alltså måste m vara sammansatt.

5. $a \equiv r \pmod{b} \iff a = qb + r$ för något $q \in \mathbb{Z}$. Då är
$$2^a - 1 = 2^{qb+r} - 1 = (2^b)^q 2^r - 1 \equiv 2^r - 1 \pmod{2^b - 1}$$
ty $2^b \equiv 1 \pmod{2^b - 1}$. (Jämför även Strayer övning 1.9.)

6. Strayer 3.5.

7. Villkoret $a^m \equiv 1 \pmod{n}$ är enligt kinesiska restsatsen ekvivalent med systemet
$$\begin{cases} a^m \equiv 1 \pmod{p} \\ a^m \equiv 1 \pmod{q}. \end{cases}$$
För den första ekvationen räcker det enligt Fermats sats att ta $m = p - 1$, och för den andra ekvationen duger $m = q - 1$. Ett m som fungerar för båda ekvationerna är därför $m = \operatorname{mgm}(p-1, q-1)$. Det återstår att visa att detta är det minsta värde som fungerar. För detta räcker det att hitta ett a med $\operatorname{ord}_n(a) = m$. Låt r vara en primitiv rot modulo p, och låt s vara en primitiv rot modulo q. Enligt kinesiska restsatsen finns ett x sådant att
$$\begin{cases} x \equiv r \pmod{p} \\ x \equiv s \pmod{q} \end{cases}$$
och ett sådant x är relativt primt med n eftersom r och s är det. Det är nu lätt att se att $\operatorname{ord}_n(x) = \operatorname{mgm}(p-1, q-1)$, ty
$$x^t \equiv 1 \pmod{n} \iff \begin{cases} x^t \equiv 1 \pmod{p} \\ x^t \equiv 1 \pmod{q} \end{cases} \iff \begin{cases} p-1 \mid t \\ q-1 \mid t \end{cases} \iff \operatorname{mgm}(p-1, q-1) \mid t.$$

8. Räknereglerna för Legendresymbolen visar att
$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{\left((p-1)/2\right)\left((3-1)/2\right)} \quad \text{enligt Strayer 4.6 och 4.9} \\ &= (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right). \end{aligned}$$
Eftersom den enda kvadratiska resten modulo 3 är 1, så är
$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{om } p \equiv 1 \pmod{3} \\ -1 & \text{om } p \equiv 2 \pmod{3} \end{cases}$$
varav påståendet följer.