1. Vi bestämmer först $\text{sgd}(4048, 3864)$ med Euklides algoritm:

$$4048 = 1 \cdot 3864 + 184$$
$$3864 = 21 \cdot 184.$$

Alltså är $\text{sgd}(4048, 3864) = 184$. Vi bestämmer nu $\text{sgd}(11270, 184)$. Här kan vi faktorisera $184 = 8 \cdot 23$ och $11270 = 2 \cdot 5 \cdot 7^2 \cdot 23$, varav vi ser att den största gemensamma delaren är $2 \cdot 23 = 46$.

2. (a) Enligt Strayer 6.13 kan varje positivt tal skrivas som summan av fyra kvadrater. Vi faktoriserar $2660 = 2^2 \cdot 5 \cdot 7 \cdot 19$. Vi börjar med att skriva $5 \cdot 7 \cdot 19$ som summan av fyra kvadrater. Eftersom

$$5 \cdot 7 = 1^2 + 3^2 + 5^2 \quad \text{och} \quad 19 = 1^2 + 3^2 + 3^2$$

ger Eulers formel (Strayer 6.10) att

$$5{\cdot}7{\cdot}19 = (1{\cdot}1{+}3{\cdot}3{+}5{\cdot}3)^2{+}(1{\cdot}3{-}3{\cdot}1)^2{+}(1{\cdot}3{-}5{\cdot}1)^2{+}(3{\cdot}3{-}5{\cdot}3)^2 = 25^2{+}2^2{+}6^2$$

varav

$$2660 = 2^2 \cdot 5 \cdot 7 \cdot 19 = 50^2 + 4^2 + 12^2 + 0^2.$$

(Observera att det finns många andra lösningar.)

(b) Eftersom $7 \equiv 3 \pmod 4$ och 7 endast förekommer en gång i primfaktoriseringen av 2660, kan detta tal inte skrivas som summan av två kvadrater (Strayer 6.8).

3. Eftersom $10 \equiv 128 = 2^7 \pmod{59}$ är $\text{ind}_2(10) = 7$. Vidare är $2^{29} \equiv -1 \pmod{59}$ (se Strayer övn 5.12a), så $\text{ind}_2(-4) = 29 + 2 = 31$. Genom att applicera index på den givna kongruensen får vi

$$7 + 5\,\text{ind}_2(x) \equiv 31 \pmod{58} \iff 5\,\text{ind}_2(x) \equiv 24 \pmod{58}.$$

Euklides algoritm ger $58 = 12 \cdot 5 - 2$ och $5 = 2 \cdot 2 + 1$ varav

$$1 = 5 - 2 \cdot 2 = 5 - 2(12 \cdot 5 - 58) = 2 \cdot 58 - 23 \cdot 5,$$

så kongruensen blir

$$\text{ind}_2(x) \equiv -23 \cdot 24 \equiv 28 \pmod{58}.$$

Alltså är lösningen

$$x \equiv 2^{28} = 2^{29} \cdot 2^{-1} \equiv -1 \cdot 30 \equiv 29 \pmod{59}.$$

4. Eftersom $a_0 = 2^0 - 1$ gäller påståendet för $n = 0$. Antag att påståendet är sant för $n = k \geq 0$. Då är

$$a_{2(k+1)} = a_{2k+2} = 2a_{2k} + 1 = 2(2^k - 1) + 1 = 2^{k+1} - 1$$

där vi använt induktionsantagandet i den näst sista likheten. Alltså är påståendet sant även för $n = k + 1$. Enligt induktionsprincipen gäller påståendet för alla $n \geq 0$.

5. Strayer 2.11 och 2.12.

6. Låt $d = \text{sgd}(a, b, c)$ och $e = \text{sgd}(a, \text{sgd}(b, c))$. Eftersom $d|b$ och $d|c$ måste $d|\,\text{sgd}(b, c)$ (se t ex inlämningsuppgiften!). Eftersom $d|a$ och $d|\,\text{sgd}(b, c)$ måste likaså $d|e$.

   Vidare gäller $e|\,\text{sgd}(b, c)$ varav $e|b$ och $e|c$. Eftersom även $e|a$ följer att $e|\,\text{sgd}(a, b, c) = d$. Detta visar att $d = e$.

7. Eftersom $\phi(17) = 16$ gäller att $\text{ord}_{17}(3)|16$. Det räcker därför att kontrollera att $3^8 \not\equiv 1 \pmod{17}$, vilket kan göras genom direkt uträkning. Alternativt kan man använda kvadratisk reciprocitet vilket ger att

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

   och enligt Eulers kriterium (Strayer 4.4) är då $3^8 \equiv -1 \pmod{17}$. Således är $\text{ord}_{17}(3) = 16$, och 3 är därför en primitiv rot.

   Alla primitiva rötter ges enligt Strayer 5.5 av 3^i där $\text{sgd}(i, 16) = 1$. Dessa i är alla udda tal mellan 1 och 15, och vi har $3^1 = 3$, $3^3 = 27 \equiv 10$, $3^5 \equiv 90 \equiv 5$, $3^7 \equiv 45 \equiv 11$ samt $3^i = -3^{i-8}$ om $8 \leq i \leq 16$. Alltså är de primitiva rötterna 3, 10, 5, 11, 14, 7, 12 och 6.

8. Dekrypteringsmetoden är $M = C^d$. Alltså är

$$M_3 \equiv C_3^d = (C_1 C_2)^d = C_1^d C_2^d \equiv M_1 M_2 = 253 \cdot 1358 = 343574 \equiv 42237 \pmod{m}.$$