a) Kako je 37 prost broj, ova kongruencija je rješiva ako i samo ako je $(132\,|\,37) = 1$. Stoga nađimo $(132\,|\,37)$:

$$(132\,|\,37) = (\mathrm{mod}(132, 37)\,|\,37) = (21\,|\,37) = (3\,|\,37)\,(7\,|\,37) =$$
$$= (37\,|\,3)\,(37\,|\,7)\,(-1)^{(37-1)\,(3-1)/4}\,(-1)^{(37-1)\,(7-1)/4} = (37\,|\,3)\,(37\,|\,7) =$$
$$= (\mathrm{mod}(37, 3)\,|\,3)\,(\mathrm{mod}(37, 7)\,|\,7) = (1\,|\,3)\,(2\,|\,7) = 1 \cdot (2\,|\,7) = (-1)^{(7^2-1)/8} = 1$$

Ovdje smo se poslužili faktorizacijom $21 = 3 \cdot 7$. Međutim, isti račun možemo obaviti i bez ove faktorizacije, pri čemu je u ovom konkretnom primjeru postupak čak i jednostavniji bez obavljene faktorizacije:

$$(132\,|\,37) = (\mathrm{mod}(132, 37)\,|\,37) = (21\,|\,37) = (37\,|\,21)\,(-1)^{(37-1)\,(21-1)/4} =$$
$$= (37\,|\,21) = (\mathrm{mod}(37, 21)\,|\,21) = (16\,|\,21) = (4^2\,|\,21) = 1$$

Može se postupiti i ovako:

$$(132\,|\,37) = (2^2 \cdot 33\,|\,37) = (2^2\,|\,37) \cdot (33\,|\,37) = (33\,|\,37) = (37\,|\,33) \cdot (-1)^{(37-1)\,(33-1)/4} =$$
$$= (37\,|\,33) = (\mathrm{mod}(37, 33)\,|\,33) = (4\,|\,33) = (2^2\,|\,33) = 1$$

Kongurencija je rješiva i ima dva tipična rješenja (rješive kongurencije sa prostim modulom uvijek imaju tačno dva tipična rješenja). Zaista, pokazuje se da su njena tipična rješenja $x = 13$ i $x = 24$.

b) Kako je $308 = 2^2 \cdot 7 \cdot 11$ i $\mathrm{NZD}(15, 308) = 1$, uvjeti rješivosti ove kongruencije su $(15\,|\,7) = 1$, $(15\,|\,11) = 1$ i $15 \equiv 1 \pmod 4$. Kako posljednji uvjet nije ispunjen, prva dva ne moramo niti provjeravati, nego odmah zaključujemo da kongurencija nije rješiva. Inače, napomenimo da su prva dva uvjeta ispunjena, jer je:

$$(15\,|\,7) = (\mathrm{mod}(15, 7)\,|\,7) = (1\,|\,7) = 1$$
$$(15\,|\,11) = (\mathrm{mod}(15, 11)\,|\,11) = (4\,|\,11) = (2^2\,|\,11) = 1$$

c) Kako je 31 prost broj, uvjet rješivosti je da je $(6\,|\,31) = 1$. Izračunajmo $(6\,|\,31)$:

$$(6\,|\,31) = (2 \cdot 3\,|\,31) = (2\,|\,31) \cdot (3\,|\,31) = (-1)^{(31^2-1)/8} \cdot (3\,|\,31) = (3\,|\,31) =$$
$$= (31\,|\,3) \cdot (-1)^{(31-1)\,(3-1)/4} = -(31\,|\,3) = -(\mathrm{mod}(31, 3)\,|\,3) = -(1\,|\,3) = -1$$

Slijedi da kongurencija nije rješiva.

d) Kako je $57 = 3 \cdot 19$, i $\mathrm{NZD}(32, 57) = 1$, uvjeti rješivosti su $(32\,|\,3) = 1$ i $(32\,|\,19) = 1$. Imamo

$$(32\,|\,3) = (\mathrm{mod}(32, 3)\,|\,3) = (2\,|\,3) = (-1)^{(3^2-1)/8} = -1$$

Stoga odmah zaključujemo da kongurencija nije rješiva, bez potrebe da računamo $(32\,|\,19)$. Čisto radi vježbe, izračunaćemo i ovu vrijednost:

$$(32\,|\,19) = (\mathrm{mod}(32, 19)\,|\,19) = (13\,|\,19) = (19\,|\,13) \cdot (-1)^{(19-1)\,(13-1)/4} = (19\,|\,13) =$$
$$= (\mathrm{mod}(19, 13)\,|\,13) = (6\,|\,13) = (2 \cdot 3\,|\,13) = (2\,|\,13) \cdot (3\,|\,13) = (-1)^{(13^2-1)/8} \cdot (3\,|\,13) =$$
$$= -(3\,|\,13) = -(13\,|\,3) \cdot (-1)^{(13-1)\,(3-1)/4} = -(13\,|\,3) = -(\mathrm{mod}(13, 3)\,|\,3) = -(1\,|\,3) = -1$$

Bitno je uočiti da je $(32\,|\,57) = 1$ (s obzirom da je $(32\,|\,57) = (32\,|\,3) \cdot (32\,|\,19)$) bez obzira što kongurencija nije rješiva. To je zato što 57 nije prost broj, odnosno $(32\,|\,57)$ nije Legendreov nego

Legendre-Jacobijev simbol. Neko bi se lako mogao prevariti i brzopleto zaključiti da je kongurencija rješiva nakon što izračuna da je $(32\,|\,57) = 1$ na sljedeći (ispravan) način:

$$(32\,|\,57) = (4^2 \cdot 2\,|\,57) = (4^2\,|\,57) \cdot (2\,|\,57) = (2\,|\,57) = (-1)^{(57^2-1)/8} = 1$$

e) Kako je $665 = 5 \cdot 7 \cdot 19$ i $\mathrm{NZD}(359, 665) = 1$, uvjeti rješivosti ove kongruencije su $(359\,|\,5) = 1$, $(359\,|\,7) = 1$ i $(359\,|\,19) = 1$. Imamo

$$(359\,|\,5) = (\mathrm{mod}(359, 5)\,|\,5) = (4\,|\,5) = (2^2\,|\,5) = 1$$

$$(359\,|\,7) = (\mathrm{mod}(359, 7)\,|\,7) = (2\,|\,7) = (-1)^{(7^2-1)/8} = 1$$

$$(359\,|\,19) = (\mathrm{mod}(359, 19)\,|\,19) = (17\,|\,19) = (19\,|\,17) \cdot (-1)^{(19-1)(17-1)/4} = (19\,|\,17) =$$
$$= (\mathrm{mod}(19, 17)\,|\,17) = (2\,|\,17) = (-1)^{(17^2-1)/8} = 1$$

Dakle, kongurencija je rješiva i ima $2^3 = 8$ tipičnih rješenja. Zaista, pokazuje se da su njena tipična rješenja $x = 32$, $x = 108$, $x = 158$, $x = 298$, $x = 367$, $x = 507$, $x = 557$ i $x = 633$.

f) Kako je $120 = 2^3 \cdot 3 \cdot 5$ i $\mathrm{NZD}(49, 120) = 1$ uvjeti rješivosti kongruencije su $(49\,|\,3) = 1$, $(49\,|\,5) = 1$ i $49 \equiv 1 \pmod 8$. Prvo ćemo provjeriti posljednji uvjet, jer je najlakši za provjeru. On je ispunjen, pa provjerimo i prva dva:

$$(49\,|\,3) = (\mathrm{mod}(49, 3)\,|\,3) = (1\,|\,3) = 1$$

$$(49\,|\,5) = (\mathrm{mod}(49, 5)\,|\,5) = (4\,|\,5) = (2^2\,|\,5) = 1$$

Dakle, kongurencija je rješiva i ima $2^{2+2} = 16$ tipičnih rješenja. Zaista, pokazuje se da su njena tipična rješenja $x = 7$, $x = 13$, $x = 17$, $x = 23$, $x = 37$, $x = 43$, $x = 47$, $x = 53$, $x = 67$, $x = 73$, $x = 77$, $x = 83$, $x = 97$, $x = 103$, $x = 107$ i $x = 113$.

g) U ovom slučaju imamo $\mathrm{NZD}(4, 378) = 2 \neq 1$, što donekle komplicira postupak. Prvo je potrebno $d = \mathrm{NZD}(4, 378)$ prikazati u obliku $p\,q^2$ gdje su p i q prirodni brojevi takvi da se u rastavi broja p na proste faktore ne javlja niti jedan prosti faktor sa eksponentom većim od 1. U ovom slučaju očigledno imamo $p = 2$ i $q = 1$. Sada, polazna kongruencija $x^2 \equiv a \pmod m$ je rješiva ako i samo ako vrijedi $\mathrm{NZD}(a/q^2, m/d) = 1$ i ako je pored toga rješiva kongruencija $y^2 \equiv a/q^2 \pmod{m/d}$. U konkretnom slučaju, polazna kongruencija je rješiva ako i samo ako je $\mathrm{NZD}(4/1^2, 378/2) = 1$ i ako je pored toga rješiva kongruencija $y^2 \equiv 4/1^2 \pmod{378/2}$. Prvi uvjet je ispunjen, s obzirom je $\mathrm{NZD}(4, 189) = 1$. Preostaje da ispitamo rješivost kongruencije $y^2 \equiv 4 \pmod{189}$. Kako je $189 = 3^3 \cdot 7$, uvjeti rješivosti ove kongruencije su $(4\,|\,3) = 1$ i $(4\,|\,7) = 1$. Oba uvjeta su očigledno ispunjena, zbog $(4\,|\,3) = (2^2\,|\,3) = 1$ i $(4\,|\,7) = (2^2\,|\,7) = 1$. Dakle, kongruencija $y^2 \equiv 4 \pmod{189}$ je rješiva, a samim tim je rješiva i polazna kongruencija.

Kako posljednja kongruencija ima $2^2 = 4$ tipična rješenja, polazna kongruencija ima također $4\,q = 4$ tipičnih rješenja (broj tipičnih rješenja nije se promijenio zbog činjenice da je $q = 1$). Zaista, pokazuje se da su njena tipična rješenja $x = 2$, $x = 110$, $x = 268$ i $x = 376$.

h) Kako je $900 = 2^2 \cdot 3^2 \cdot 5^2$ i $\mathrm{NZD}(17, 900) = 1$ uvjeti rješivosti postaju $(17\,|\,3) = 1$, $(17\,|\,5) = 1$ i $17 \equiv 1 \pmod 4$. Odmah vidimo da je posljednji uvjet ispunjen, pa provjerimo i prva dva uvjeta:

$$(17\,|\,3) = (\mathrm{mod}(17, 3)\,|\,3) = (2\,|\,3) = (-1)^{(9-1)/8} = -1$$

Dakle, kongurencija nije rješiva. Lako je vidjeti i da je $(17\,|\,5) = -1$.

Napomena: Treba primijetiti da $(17\,|\,900)$ nije definiran čak ni u smislu Legendre-Jacobijevog simbola, jer je 900 paran broj (ali jeste u smislu Kroneckerovog simbola).

i) U ovom slučaju imamo $\mathrm{NZD}(25, 3750) = 25 \neq 1$, što slično kao u slučaju pod g) komplicira postupak. Kako je $25 = 1 \cdot 5^2$, ova kongruencija je rješiva ako i samo ako je ispunjeno da je $\mathrm{NZD}(25/5^2, 3750/25) = 1$ i ako je pored toga rješiva kongruencija $y^2 \equiv 25/5^2 \pmod{3750/25}$. Prvi uvjet je očigledno ispunjen jer je $\mathrm{NZD}(1, 150) = 1$. Preostaje da ispitamo rješivost kongruencije $y^2 \equiv 1 \pmod{150}$. Kako je $150 = 2 \cdot 3 \cdot 5^2$, uvjeti rješivosti ove kongruencije su $(1 \mid 3) = 1$ i $(1 \mid 5) = 1$. Međutim, ovi uvjeti su trivijalno ispunjeni, jer je $(1 \mid n) = 1$ za svaki neparan broj n. Dakle, kongruencija $y^2 \equiv 1 \pmod{150}$ je rješiva, pa je samim tim rješiva i polazna kongruencija.

Kako posljednja kongruencija ima $2^2 = 4$ tipična rješenja, polazna kongruencija ima $4q = 20$ tipičnih rješenja. Zaista, pokazuje se da su njena tipična rješenja $x = 5$, $x = 245$, $x = 505$, $x = 745$, $x = 755$, $x = 995$, $x = 1255$, $x = 1495$, $x = 1505$, $x = 1745$, $x = 2005$, $x = 2245$, $x = 2255$, $x = 2495$, $x = 2755$, $x = 2995$, $x = 3005$, $x = 3245$, $x = 3505$ i $x = 3745$.

j) Kako je $1064 = 2^3 \cdot 7 \cdot 19$ i $\mathrm{NZD}(25, 1064) = 1$, uvjeti rješivosti ove kongruencije postaju $(25 \mid 7) = 1$, $(25 \mid 19) = 1$ i $25 \equiv 1 \pmod 8$. Posljednji uvjet je očito ispunjen, stoga nađimo $(25 \mid 7)$ i $(25 \mid 19)$:

$$(25 \mid 7) = (\mathrm{mod}(25, 7) \mid 7) = (4 \mid 7) = (2^2 \mid 7) = 1$$

$$\begin{aligned}(25 \mid 19) &= (\mathrm{mod}(25, 19) \mid 19) = (6 \mid 19) = (2 \cdot 3 \mid 19) = (2 \mid 19) \cdot (3 \mid 19) = (3 \mid 19) \cdot (-1)^{(19^2-1)/8} = \\ &= -(3 \mid 19) = -(19 \mid 3) \cdot (-1)^{(19-1)(3-1)/4} = (19 \mid 3) = (\mathrm{mod}(19, 3) \mid 3) = (1 \mid 3) = 1\end{aligned}$$

Svi neophodni uvjeti su ispunjeni tako da je kongruencija rješiva, pri čemu je broj njenih tipičnih rješenja $2^{2+2} = 16$. Zaista, pokazuje se da njena tipična rješenja glase $x = 5$, $x = 33$, $x = 233$, $x = 261$, $x = 271$, $x = 299$, $x = 499$, $x = 527$, $x = 537$, $x = 565$, $x = 765$, $x = 793$, $x = 803$, $x = 831$, $x = 1031$ i $x = 1059$.

k) Kako je $2717 = 11 \cdot 13 \cdot 19$, uvjeti rješivosti ove kongruencije su $(15 \mid 11) = 1$, $(15 \mid 13) = 1$ i $(15 \mid 19) = 1$. Nađimo vrijednosti $(15 \mid 11)$, $(15 \mid 13)$ i $(15 \mid 19)$:

$$(15 \mid 11) = (\mathrm{mod}(15, 11) \mid 11) = (4 \mid 11) = (2^2 \mid 11) = 1$$

$$(15 \mid 13) = (\mathrm{mod}(15, 13) \mid 13) = (2 \mid 11) = (-1)^{(11^2-1)/8} = -1$$

U ovom trenutku već znamo da kongruencija nije rješiva, jer je $(15 \mid 13) \neq 1$. Čisto radi ilustracije, nađimo i $(15 \mid 19)$:

$$\begin{aligned}(15 \mid 19) &= (19 \mid 15) \cdot (-1)^{(19-1)(15-1)/4} = -(19 \mid 15) = -(\mathrm{mod}(19, 15) \mid 15) = \\ &= -(4 \mid 15) = -(2^2 \mid 15) = -1\end{aligned}$$

Ovaj primjer još jednom ilustrira da uvjet $(a \mid m) = 1$ u slučaju kada je m složen broj nije dovoljan za rješivost kongruencije $x^2 \equiv a \pmod m$. Zaista, u ovom primjeru imamo kongruenciju $x^2 \equiv 15 \pmod{2717}$ koja nije rješiva, bez obzira što je $(15 \mid 2717) = 1$, što je lako provjeriti:

$$\begin{aligned}(15 \mid 2717) &= (2717 \mid 15) \cdot (-1)^{(2717-1)(15-1)/4} = (2717 \mid 15) = (\mathrm{mod}(2717, 15) \mid 15) = \\ &= (2 \mid 15) = (-1)^{(15^2-1)/8} = 1\end{aligned}$$

l) U ovom slučaju imamo $\mathrm{NZD}(144, 630) = 18 \neq 1$, što slično kao u slučajevima pod g) i i) komplicira postupak. Kako je $18 = 2 \cdot 3^2$, ova kongruencija je rješiva ako i samo ako vrijedi $\mathrm{NZD}(144/3^2, 630/18) = 1$ i ako je pored toga rješiva kongruencija $y^2 \equiv 144/3^2 \pmod{630/18}$. Prvi uvjet je ispunjen, s obzirom da je $\mathrm{NZD}(16, 35) = 1$. Preostaje da ispitamo rješivost kongruencije $y^2 \equiv 16 \pmod{35}$. Kako je $35 = 5 \cdot 7$, uvjeti rješivosti ove kongruencije su $(16 \mid 5) = 1$ i $(16 \mid 7) = 1$. Nađimo sada $(16 \mid 5)$ i $(16 \mid 7)$:

$$(16\,|\,5) = (\mathrm{mod}(16,5)\,|\,5) = (1\,|\,5) = 1$$

$$(16\,|\,7) = (\mathrm{mod}(16,7)\,|\,7) = (2\,|\,7) = (-1)^{(7^2-1)/8} = 1$$

Svi neophodni uvjeti su ispunjeni, tako da je polazna kongruencija rješiva. Kako kongruencija $y^2 \equiv 16 \pmod{35}$ ima $2^2 = 4$ tipična rješenja, polazna kongruencija ima $4 \cdot 3 = 12$ tipičnih rješenja. Zaista, pokazuje se da su njena tipična rješenja $x = 12$, $x = 72$, $x = 138$, $x = 198$, $x = 222$, $x = 282$, $x = 348$, $x = 408$, $x = 432$, $x = 492$, $x = 558$ i $x = 618$.

m) Kako je $715 = 5 \cdot 11 \cdot 13$ i $\mathrm{NZD}(31, 715) = 1$, kongruencija je rješiva ako i samo ako je $(31\,|\,5) = 1$, $(31\,|\,11) = 1$ i $(31\,|\,13) = 1$. Nađimo vrijednosti $(31\,|\,5)$, $(31\,|\,11)$ i $(31\,|\,13)$:

$$(31\,|\,5) = (\mathrm{mod}(31,5)\,|\,5) = (1\,|\,5) = 1$$

$$(31\,|\,11) = (\mathrm{mod}(31,11)\,|\,11) = (9\,|\,11) = (11\,|\,9) \cdot (-1)^{(11-1)(9-1)/4} = (11\,|\,9) =$$
$$= (\mathrm{mod}(11,9)\,|\,9) = (2\,|\,9) = (-1)^{(9^2-1)/8} = 1$$

$$(31\,|\,13) = (\mathrm{mod}(31,13)\,|\,13) = (5\,|\,13) = (13\,|\,5) \cdot (-1)^{(13-1)(5-1)/4} = (13\,|\,5) = (\mathrm{mod}(13,5)\,|\,5) =$$
$$= (3\,|\,5) = (5\,|\,3) \cdot (-1)^{(5-1)(3-1)/4} = (5\,|\,3) = (\mathrm{mod}(5,3)\,|\,3) = (2\,|\,3) = (-1)^{(3^2-1)/8} = -1$$

Kako je $(31\,|\,13) \neq 1$, kongruencija nije rješiva.

n) Kako je $1232 = 2^4 \cdot 7 \cdot 11$ i $\mathrm{NZD}(25, 1232) = 1$, kongruencija je rješiva ako i samo ako je $(25\,|\,7) = 1$, $(25\,|\,11) = 1$ i $25 \equiv 1 \pmod{8}$. Posljednji uvjet je ispunjen, tako da treba naći $(25\,|\,7)$ i $(25\,|\,11)$:

$$(25\,|\,7) = (\mathrm{mod}(25,7)\,|\,7) = (4\,|\,7) = (2^2\,|\,7) = 1$$

$$(25\,|\,11) = (\mathrm{mod}(25,11)\,|\,11) = (3\,|\,11) = (11\,|\,3) \cdot (-1)^{(11-1)(3-1)/4} = -(11\,|\,3) =$$
$$= -(\mathrm{mod}(11,3)\,|\,3) = -(2\,|\,3) = -(-1)^{(3^2-1)/8} = 1$$

Svi uvjeti su ispunjeni, te je kongruencija rješiva. Broj njenih tipičnih rješenja je $2^{2+2} = 16$. Zaista, može se pokazati da njena tipična rješenja glase $x = 5$, $x = 61$, $x = 93$, $x = 149$, $x = 467$, $x = 523$, $x = 555$, $x = 611$, $x = 621$, $x = 677$, $x = 709$, $x = 765$, $x = 1083$, $x = 1139$, $x = 1171$ i $x = 1227$.

o) Kako je $17325 = 3^2 \cdot 5^2 \cdot 7 \cdot 11$, $2871 = 3^2 \cdot 11 \cdot 29$ i $\mathrm{NZD}(17325, 2871) = 3^2 \cdot 11 = 99$, postupak se komplicira jer je $d = \mathrm{NZD}(17325, 2871) \neq 1$. Na osnovu rastave $d = 11 \cdot 3^2$ slijedi je kongruencija rješiva ako i samo ako vrijedi $\mathrm{NZD}(2871/3^2, 17325/99) = 1$ i ako je pored toga rješiva kongruencija $y^2 \equiv 2871/3^2 \pmod{17325/99}$ odnosno $y^2 \equiv 319 \pmod{175}$. Kako je $\mathrm{NZD}(319, 175) = 1$, prvi uvjet je ispunjen. Testirajmo sada rješivost kongruencije $y^2 \equiv 319 \pmod{175}$. Kako je $175 = 5^2 \cdot 7$, ona je rješiva ako i samo ako vrijedi $(319\,|\,5) = 1$ i $(319\,|\,7) = 1$. Imamo:

$$(319\,|\,5) = (\mathrm{mod}(319,5)\,|\,5) = (4\,|\,5) = (2^2\,|\,5) = 1$$

$$(319\,|\,7) = (\mathrm{mod}(319,7)\,|\,7) = (4\,|\,7) = (2^2\,|\,7) = 1$$

Dakle, posljednja kongruencija je rješiva i ima $2^2 = 4$ tipična rješenja. Stoga, broj tipičnih rješenja polazne kongruencije iznosi $4 \cdot 3 = 12$. Zaista, može se pokazati da su njena tipična rješenja $x = 561$, $x = 2211$, $x = 3564$, $x = 5214$, $x = 6336$, $x = 7986$, $x = 9339$, $x = 10989$, $x = 12111$, $x = 13761$, $x = 15114$ i $x = 16764$.