1. Da 19 er et primtal, eksisterer en primitiv rod i $\mathbb{F}_{19}$ ifølge sætning 2.4.4. Ifølge proposition 2.4.6 er da netop $\varphi\left(\varphi(19)\right) = \varphi\left(18\right) = \varphi(3^2 \cdot 2) = (3-1)3^{2-1}(2-1)2^{1-1} = 2 \cdot 3 = 6$ af sideklasserne $\overline{1}, \overline{2}, \ldots, \overline{18}$ primitive rødder modulo 19.
Nu finder vi

$$2^9 = 16 \cdot 32 \equiv -3 \cdot 13 \equiv -1 \pmod{19}, 2^2 \equiv 4 \pmod{19}.$$

.

Da $\mathbb{F}_p^\times$ er cyklisk ifølge korollar 2.4.5, må ordenen af 2 desuden gå op i $18 = 2 \cdot 3^2$, hvormed $\operatorname{ord}(2) = 18$.

Dermed er 2 en primitiv rod modulo 19, eller ækvivalent er 2 en generator for den cykliske gruppe $\mathbb{F}_{19}^\times$, hvormed vi har at alle andre generatorer er netop 2^a hvor $\gcd(a, 18) = 1$. Så vi har, at $2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$ er de resterende primitive rødder, som netop bliver

$$\begin{aligned}
2^5 &= 32 \equiv 13 \pmod{19} \\
2^7 &= 13 \cdot 4 \equiv 52 \equiv 14 \pmod{19} \\
2^{11} &= -5 \cdot 2^4 = (-5)(-3) = 15 \pmod{19} \\
2^{13} &= (-4) \cdot 4 \equiv -16 \equiv 3 \pmod{19} \\
2^{17} &= 3 \cdot (-3) \equiv 10 \pmod{19}.
\end{aligned}$$

Altså er $2, 3, 10, 13, 14, 15$ samtlige primitive rødder modulo 19.

2. Vi har

$$x^2 + 20x + 211 = \frac{1}{4}\left((2x+20)^2 - \left(20^2 - 4 \cdot 211\right)\right).$$

Så ligningen har løsninger hvis og kun hvis $20^2 - 4 \cdot 211 = -444 \equiv 82 \pmod{263}$ er en kvadratisk rod modulo 263, altså hvis og kun hvis $\left(\frac{82}{263}\right) = 1$. Ifølge kvadratisk reciprocitet (sætning 4.2.1) fås

$$\begin{aligned}
\left(\frac{82}{263}\right) &= \left(\frac{2}{263}\right)\left(\frac{41}{263}\right) \\
&= (-1)^{\frac{263^2-1}{8}} (-1)^{\frac{40 \cdot 262}{4}} \left(\frac{263}{41}\right).
\end{aligned}$$

Da $263^2 - 1 = 262 \cdot 264 = 262 \cdot 8 \cdot 33$ fås

$$\begin{aligned}
\left(\frac{82}{263}\right) &= \left(\frac{263}{41}\right) \\
&= \left(\frac{17}{41}\right) \\
&= (-1)^{\frac{16 \cdot 40}{4}} \left(\frac{41}{17}\right) \\
&= \left(\frac{7}{17}\right) \\
&= (-1)^{\frac{6 \cdot 16}{4}} \left(\frac{17}{7}\right) \\
&= \left(\frac{3}{7}\right) \\
&= (-1)^{\frac{2 \cdot 6}{4}} \left(\frac{7}{3}\right) \\
&= -1 \left(\frac{1}{3}\right) \\
&= -1.
\end{aligned}$$

Altså eksisterer ingen heltallige løsninger til ligningen ved en lokal obstruktion.

3. (a) Da p er et primtal, er $\mathbb{F}_p^\times$ cyklisk ifølge korollar 2.4.5, så lad $g \in \mathbb{F}_p^\times$ være en primitiv rod, dvs. $\operatorname{ord}(g) = p - 1 = 5k$ for $k \in \mathbb{Z}$ (hvor vi har brugt, at $p \equiv 1 \pmod 5 \implies p - 1 = 5k$ for et $k \in \mathbb{Z}$). Lad nu $c = g^k$. Da har vi $c^5 = g^{5k} = g^{p-1} \equiv 1 \pmod p$, så $\operatorname{ord}(c) \leq 5$. Antag nu, at $d = \operatorname{ord}(c) < 5$. Da har vi

$$1 \equiv c^d \equiv g^{kd},$$

hvormed $\operatorname{ord}(g) \leq kd < 5k = p-1$, som er i modstrid med, at g er en primitiv rod. Dermed må $\operatorname{ord}(c) = 5$.

(b) Lad $g = 2 \cdot \left(c + c^{-1}\right) + 1$. Da har vi

$$\begin{aligned} g^2 - 5 &= 4\left(c + c^{-1}\right)^2 + 4(c + c^{-1}) - 4 \\ &= 4\left[(c + c^{-1})^2 + (c + c^{-1}) - 1\right] \\ &\equiv 4\left[c^2 + c^{-2} + 2 + c + c^{-1} - 1\right] \\ &\equiv 4\left[c^2 + c + 1 + c^{-1} + c^{-2}\right] \\ &\equiv 4c^k\left[c^2 + c + 1 + c^{-1} + c^{-2}\right], \quad \forall k \in \mathbb{Z}. \end{aligned}$$

Hvor sidste ækvivalens følger af, at c har orden 5 og $c^2 + c + 1 + c^{-1} + c^{-2} \equiv 1 + c + c^2 + c^3 + c^4 \pmod p$. Dvs for alle $k \in \mathbb{Z}$ er $c^k\left(g^2 - 5\right) \equiv g^2 - 5 \pmod p$. Hvis $g^2 \not\equiv 5 \pmod p$, har $g^2 - 5$ en invers modulo p, hvormed vi får $c^k \equiv 1 \pmod p$ for alle k, dvs $c \equiv 1 \pmod p$, som er en modstrid med, at c er et element af orden 5. Dermed må $g^2 \equiv 5 \pmod p$.

(c) Da vi har fundet et element $g = 2 \cdot (c + c^{-1}) + 1$, med $g^2 \equiv 5 \pmod 5$, er 5 per definition en kvadratisk rod modulo p, så per definition er $\binom{5}{p} = 1$.
Ved kvadratisk reciprocitet har vi desuden, at

$$\begin{aligned} \binom{5}{p} &= (-1)^{\frac{4(p-1)}{4}} \binom{p}{5} \\ &= \binom{p}{5} && \text{(Da } p \equiv 1 \pmod 5 \implies p \neq 2\text{, så } p-1 \text{ er lige)} \\ &\overset{\alpha}{\equiv} \binom{5k+1}{5} \\ &= \binom{1}{5} \\ &= 1, \end{aligned}$$

hvor α følger af, at $p \equiv 1 \pmod 5 \implies p - 1 = 5k \implies p = 5k + 1$ for et $k \in \mathbb{Z}$.

4. Antag for modstrid, at n er en primitiv rod modulo p, dvs. $\operatorname{ord}(n) = p - 1 = 2k$ for et $k \in \mathbb{Z}$, da p var antaget at være ulige. Da $\binom{n}{p} = 1$, eksisterer $m \in \mathbb{Z}$, så $m^2 \equiv n \pmod p$. Bemærk, at da n er en primitiv rod, må $m \not\equiv 0 \pmod p$, da vi ellers ville have $n \equiv 0 \pmod p$. Dermed fås fra Fermats lille sætning, at

$$1 \equiv m^{p-1} = m^{2k} = \left(m^2\right)^k \equiv n^k \pmod p.$$

Men da har vi $\operatorname{ord}(n) \leq k < 2k = \operatorname{ord}(n)$, som er en modstrid.
Altså er n ikke en primitiv rod modulo p.