

Q3a, 7.12: First consider the case when $a = -3 \in Q_p$. We see by inspection that $-3 \in Q_2$ and $-3 \in Q_3$. So it is reasonable to assume that $p > 3$. By theorem 7.5, we have that

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

If it is the case that $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = 1$. By example 7.10, $\left(\frac{3}{p}\right) = 1$ when $p \equiv 1 \pmod{12}$. If $p \equiv 3 \pmod{4}$, then we have that $\left(\frac{-1}{p}\right) = -1$. Once again by example 7.10, $\left(\frac{3}{p}\right) = -1$ for $p \equiv 7 \pmod{12}$. Therefore, $p \equiv 1 \pmod{6}$. A similar argument can be made for $a = 5$. We get that $\left(\frac{p}{5}\right) = 1$ if $p \equiv \pm 1 \pmod{5}$. For $a = 6$, since $6 \notin Q_3, Q_2$ we can assume that $p > 3$. If $p \equiv 1 \pmod{4}$, then $\left(\frac{6}{p}\right) = 1$ when $\left(\frac{p}{2}\right) = \left(\frac{p}{3}\right)$. So, $p \equiv \pm 1 \pmod{24}$ or $p \equiv \pm 5 \pmod{24}$. When $a = 7$, $p = 2$, $p \equiv \pm 1 \pmod{28}$, $p \equiv \pm 3 \pmod{28}$, $p \equiv \pm 9 \pmod{28}$. When $a = 10$, we get that $p \equiv \pm 1, 3, 9, 13 \pmod{40}$. When $a = 169$, $p \neq 13$.

7.21: Notice that $-1 \in Q_n$ by theorem 7.15. This is only true iff $-1 \in Q_{p^e}$, for each $p^e \parallel n$. Note that by thm 7.14, $-1 \in Q_{2^e} \iff e = 0$ or 1 . If $p > 2$, $-1 \in Q_p \iff -1 \in Q_{p^e}$ by theorem 7.13. By cor. 7.7, this is true if and only if $p \equiv 1 \pmod{4}$. Therefore, $-1 \in Q_n$ if and only if 4 does not divide n or n is not divisible by a prime $p \equiv 3 \pmod{4}$.

7.22: We can observe that the quantities $\pm\sqrt{q}, \pm\sqrt{r}, \pm\sqrt{qr}$ are not integral. But at least one of $r, q, qr \equiv 1 \pmod{8}$. Therefore at least one belong to Q_{2^e} for all e , and so $\left(\frac{q}{r}\right) = 1$, and so $q \in Q_{r^e}$ for all e . Using the CRT, we want to show that for all prime p, p^e there exists some solution to $f(x) \equiv 0 \pmod{p^e}$. By LQR, $\left(\frac{r}{q}\right) = \left(\frac{q}{r}\right) = 1$ and so $r \in Q_{p^e}$. By theorem 7.5, if $p \neq 2, p \neq q, p \neq r$ then $\left(\frac{qr}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{r}{p}\right)$. So at minimum one of q, r, qr belong to Q_{p^e} for all e . So thus $h(x) \equiv 0 \pmod{n}$ has a solution for all n .

7.11. We factor $219 = 3 \cdot 73$ so by thm 7.5,

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)$$

We use the LQR to evaluate

$$\left(\frac{3}{383}\right) = \left(-\frac{383}{3}\right) = -\left(\frac{2}{3}\right) = 1$$

Similarly by applying cor. 7.10, we get that

$$\left(\frac{73}{383}\right) = 1$$

And so

$$\left(\frac{219}{383}\right) = 1$$

and so $219 \in Q_{383}$

7.25 We factor $923 = 13 \cdot 71$ So $43 \equiv 4 \pmod{13}$ and $43 \equiv 4 \pmod{13}$ and $43 \in Q_{13}$. Hence by LGR we can write

$$\left(\frac{43}{71}\right) = -\left(\frac{71}{43}\right) = -\left(\frac{28}{43}\right) = -\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right) = \left(\frac{1}{7}\right) = 1$$

And so $43 \in Q_{923}$