Chapter 4. Quadratic Residues

4.1 Note: Given $a \in \mathbb{Z}_n$ (or $a \in U_n$), how can we determine whether there exists $x \in \mathbb{Z}_n$ (or $x \in U_n$) such that $x^2 = a$? This is the problem that we address in this chapter.

4.2 Definition: For $a \in \mathbb{Z}_n$ (or U_n), we say that a is a **quadratic residue** (modulo n) when there exists $x \in \mathbb{Z}_n$ (or U_n) such that $x^2 = a$. Note that if $a \in U_n$ and $x \in \mathbb{Z}_n$ with $x^2 = a$, then we have $\gcd(x^2, n) = \gcd(a, n) = 1$, hence $\gcd(x, n) = 1$, so that $x \in U_n$. We denote the set of quadratic residues in $\mathbb{Z}_n$ and U_n by S_n and Q_n, respectively, so we have

$$S_n = \left\{a \in \mathbb{Z}_n \,\middle|\, a = x^2 \text{ for some } x \in \mathbb{Z}_n\right\},$$
$$Q_n = \left\{a \in U_n \,\middle|\, a = x^2 \text{ for some } x \in U_n\right\}.$$

Note that Q_n is a group, since $1 \in Q_n$ and if $a, b \in Q_n$ with, say $a = x^2$ and $y = b^2$ then we have $ab = (xy)^2$ and we have $a^{-1} = (x^{-1})^2$.

4.3 Theorem: *Let $k, \ell \in \mathbb{Z}$ with $\gcd(k, \ell) = 1$. The bijective map $F : \mathbb{Z}_{k\ell} \to \mathbb{Z}_k \times \mathbb{Z}_\ell$ given by $F(u) = (u, u)$ restricts to give a bijective map $F : S_{k\ell} \to S_k \times S_\ell$, and it restricts further to give a group isomorphism $F : Q_{k\ell} \to Q_k \times Q_\ell$.*

Proof: For $a \in \mathbb{Z}$, if $a = x^2 \bmod k\ell$ then we also have $a = x^2 \bmod k$ and $a = x^2 \bmod \ell$ and so F restricts to a map $F : S_{k\ell} \to S_k \times S_\ell$. On the other hand, if $b = y^2 \bmod k$ and $c = z^2 \bmod \ell$ and $F(a) = (b, c) = (y^2, z^2) = (y, z)^2$, then we have $a = x^2$ where $x = F^{-1}(y, z)$. Thus the map F restricts to give a bijective map $F : S_{k\ell} \to S_k \times S_\ell$. We have already seen that F restricts to give a group isomorphism $F : U_{k\ell} \to U_k \times U_\ell$ and the above argument shows that F restricts further to give a group isomorphism $F : Q_{k\ell} \to Q_k \times Q_\ell$.

4.4 Remark: In light of the above theorem, it suffices to understand the sets S_n and Q_n in the case that $n = p^k$ for some prime p and some $k \in \mathbb{Z}^+$. We shall focus our attention on the group Q_n with $n = p^k$.

4.5 Note: We point out some properties of quadratic residues which follow immediately from our understanding of the structure of the group of units U_n when n is a prime power.

(1) We have $Q_2 = \{1\}$, and $Q_4 = \{1\}$ and for $k \geq 3$, since $U_{2^k} = \left\{\pm 5^j \,\middle|\, 0 \leq j < 2^{k-2}\right\}$ we have

$$Q_{2^k} = \left\{x^2 \middle| x \in U_{2^k}\right\} = \left\{5^{2j} \middle| 0 \leq j < 2^{k-3}\right\} = \langle 25 \rangle$$

so that Q_{2^k} is cyclic with $|Q_{2^k}| = \frac{1}{4}|U_{2^k}| = 2^{k-3}$. Also note, in the case $k \geq 3$, that $U_{2^k} = \{\pm 5^j\}$ is equal to the disjoint union

$$U_{2^k} = \left\{5^0, 5^2, 5^4, \cdots\right\} \cup \left\{5^1, 5^3, 5^5, \cdots\right\} \cup \left\{-5^0, -5^2, -5^4, \cdots\right\} \cup \left\{-5^1, -5^3, -5^5, \cdots\right\}$$

and modulo 8, the elements in these sets are all equal to 1, 5, 7 and 3, respectively. Thus for $a \in U_{2^k}$, we have

$$a \in Q_{2^k} \iff a = 1 \bmod 8.$$

(2) Let p be an odd prime and let $k \in \mathbb{Z}^+$. Choose $u \in \mathbb{Z}$ so that $U_{p^k} = \langle u \rangle$. Then $\operatorname{ord}_{p^k}(u) = \varphi(p^k) = p^{k-1}(p-1)$, which is even, and $U_{p^k} = \left\{u^j \,\middle|\, 0 \leq j < p^{k-1}(p-1)\right\}$ so

$$Q_{p^k} = \left\{x^2 \,\middle|\, x \in U_{p^k}\right\} = \left\{u^{2j} \,\middle|\, 0 \leq j < \tfrac{1}{2}\, p^{k-1}(p-1)\right\} = \langle u^2 \rangle$$

and so Q_{p^k} is cyclic with $|Q_{p^k}| = \frac{1}{2}|U_{p^k}| = \frac{1}{2}\, p^{k-1}(p-1)$. Also note that for $a \in \mathbb{Z}$ with $p \nmid a$ we have

$$a \in Q_{p^k} \iff a = u^{2j} \text{ for some } j \iff a \in Q_p.$$

4.6 Remark: When $a \in \mathbb{Z}$ with $2 \not| a$ and $k \geq 3$, by the above note, $a \in Q_{2^k} \iff a = 1 \bmod 8$. When p is an odd prime, $a \in \mathbb{Z}$ with $p \not| a$ and $k \in \mathbb{Z}^+$, by the above note, $a \in Q_{p^k} \iff a \in Q_p$. It remains, then, to determine whether $a \in Q_p$ when p is an odd prime and $p \not| a$.

4.7 Definition: For an odd prime p and for $a \in \mathbb{Z}$, we define the **Legendre symbol**

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \text{ so } a \notin U_p\,, \\ 1 & \text{if } a \in Q_p\,, \\ -1 & \text{if } a \in U_p \setminus Q_p\,. \end{cases}$$

4.8 Note: When $a \in U_p = \langle u \rangle$ with say $a = u^k$, we have $a \in Q_p \iff k$ is even, and so

$$\left(\tfrac{a}{p}\right) = (-1)^k.$$

4.9 Theorem: *(Multiplicative Property) Let p be an odd prime and let $a, b \in \mathbb{Z}$. Then*

$$\left(\tfrac{ab}{p}\right) = \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right).$$

Proof: If $a \notin U_p$ or $b \notin U_p$, that is if $p \big| a$ or $p \big| b$, then we have $p \big| ab$ so that

$$\left(\tfrac{ab}{p}\right) = 0 = \left(\tfrac{a}{b}\right)\left(\tfrac{b}{p}\right).$$

If $a, b \in U_p = \langle u \rangle$, say $a = u^k$ and $b = u^\ell$, then we have $ab = u^{k+\ell}$ so

$$\left(\tfrac{ab}{p}\right) = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right).$$

4.10 Note: By the multiplicative property of the Legendre symbol, when $a = \prod_{i=1}^{\ell} {p_i}^{k_i}$ where $p_1, \cdots, p_\ell$ are distinct primes and $k_1, \cdots, k_\ell \in \mathbb{Z}^+$, we have $\left(\frac{a}{p}\right) = \prod_{i=1}^{\ell} \left(\frac{p_i}{p}\right)^{k_i}$. Thus to determine the value of $\left(\frac{a}{p}\right)$ it suffices to determine the value of $\left(\frac{q}{p}\right)$ when p and q are primes. We make a table, listing the values $\left(\frac{q}{p}\right)$ for some odd primes p and q .

$p \backslash q$	3	5	7	11	13	17	19	23	29
3	0	−1	1	−1	1	−1	1	−1	−1
5	−1	0	−1	1	−1	−1	1	−1	1
7	−1	−1	0	1	−1	−1	−1	1	1
11	1	1	−1	0	−1	−1	−1	1	−1
13	1	−1	−1	−1	0	1	−1	1	1
17	−1	−1	−1	−1	1	0	1	−1	−1
19	−1	1	1	1	−1	1	0	1	−1
23	1	−1	−1	−1	1	−1	−1	0	1
29	−1	1	1	−1	1	−1	−1	1	0

The table appears to be symmetric with $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ except when $p = q = 3 \bmod 4$ in which case $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. This pattern was conjectured to hold by Euler and Legendre and was first proven by Gauss.

4.11 Theorem: *(Euler's Criterion) Let p be an odd prime and let $a \in \mathbb{Z}$. Then*

$$\left(\tfrac{a}{p}\right) = a^{(p-1)/2} \bmod p.$$

Proof: If $a \notin U_p$, that is if $p\big|a$, then in Z_p we have $a = 0$, hence $a^{(p-1)/2} = 0 = \left(\frac{a}{p}\right)$. Suppose that $a \in U_p = \langle u \rangle$, say $a = u^k$. Note that, in U_p we have $u^{(p-1)/2} = -1$ because $u^{(p-1)/2} \neq 1$ and $\left(u^{(p-1)/2}\right)^2 = 1$ and -1 is the only element of order 2 in the cyclic group U_p. Thus

$$\left(\tfrac{a}{p}\right) = (-1)^k = \left(u^{(p-1)/2}\right)^k = (u^k)^{(p-1)/2} = a^{(p-1)/2}.$$

4.12 Theorem: *(Gauss' Lemma) Let p be an odd prime. Let $P = \left\{1, 2, 3, \cdots, \frac{p-1}{2}\right\}$ and let $N = \left\{-1, -2, -3, \cdots, -\frac{p-1}{2}\right\}$. Then for all $a \in U_p$ we have*

$$\left(\tfrac{a}{p}\right) = (-1)^{|aP \cap N|}$$

where $aP = \left\{a \cdot 1, a \cdot 2, a \cdot 3, \cdots, a \cdot \frac{p-1}{2}\right\} \subseteq U_p$.

Proof: For $k, \ell \in P$ we have

$$ak = a\ell \Longrightarrow a(k - \ell) = 0 \Longrightarrow k = \ell \in U_p.$$

Also, if $k, \ell \in P$ then

$$ak = -a\ell \Longrightarrow a(k + \ell) = 0 \Longrightarrow k = -\ell \in U_p$$

but this is not possible since $k \in P$ and $-\ell \in N$ and U_p is the disjoint union of P and Q. Thus the set aP consists of one element from each pair $\{\pm 1\}, \{\pm 2\}, \cdots, \{\pm \frac{p-1}{2}\}$. For each $k \in P$ choose $\varepsilon_k \in \{\pm 1\}$ so that $\varepsilon_k \cdot a \cdot k \in P$. Then we have

$$P = \left\{1, 2, \cdots, \tfrac{p-1}{2}\right\} = \left\{\varepsilon_1 \cdot a \cdot 1, \varepsilon_2 \cdot a \cdot 2, \cdots, \varepsilon_{(p-1)/2} \cdot a \cdot \tfrac{p-1}{2}\right\}$$

Multiply all the elements in theses sets to get

$$\left(\tfrac{p-1}{2}\right)! = \Big(\prod_{k \in P} \varepsilon_k\Big) \cdot a^{(p-1)/2} \cdot \left(\tfrac{p-1}{2}\right)!$$

Multiply both sides by the inverse of $\left(\frac{p-1}{2}\right)!$ then apply Euler's Criterion to get

$$1 = \Big(\prod_{k \in P} \varepsilon_k\Big) \cdot a^{(p-1)/2} = \Big(\prod_{k \in P} \varepsilon_k\Big) \cdot \left(\tfrac{a}{p}\right).$$

Note that by our choice of ε_k, the number of elements $k \in P$ such that $\varepsilon_k = -1$ is equal to the number of $k \in P$ such that $ak \in N$, which is equal to $|aP \cap N|$, and so

$$\prod_{k \in P} \varepsilon_k = (-1)^{|aP \cap N|}.$$

Thus $1 = (-1)^{|aP \cap N|} \cdot \left(\frac{a}{p}\right)$ and hence $\left(\frac{a}{p}\right) = (-1)^{|aP \cap N|}$, as required.

4.13 Theorem: *(Quadratic Reciprocity) Let p and q be distinct odd primes. Then*

$$\left(\tfrac{p}{q}\right) = \begin{cases} \left(\tfrac{q}{p}\right), & \text{if } p = 1 \bmod 4 \text{ or } q = 1 \bmod 4\,, \\ -\left(\tfrac{q}{p}\right), & \text{if } p = q = 3 \bmod 4\,. \end{cases}$$

Equivalently, we have

$$\left(\tfrac{p}{q}\right)\cdot\left(\tfrac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

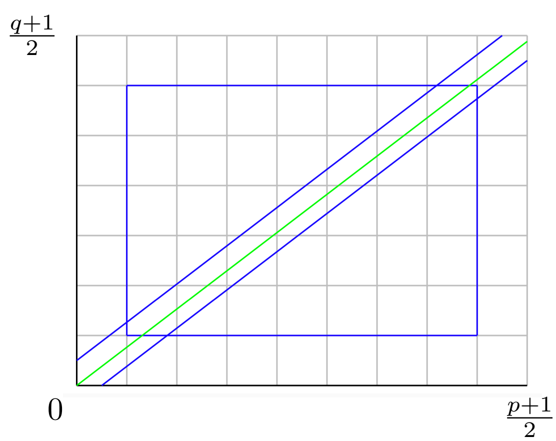
Proof: Let $P = \left\{1, 2, \cdots, \frac{p-1}{2}\right\}$ and $N = \left\{-1, -2, \cdots, -\frac{p-1}{2}\right\}$, and let $Q = \left\{1, 2, \cdots, \frac{q-1}{2}\right\}$ and $M = \left\{-1, -2, \cdots, -\frac{q-1}{2}\right\}$. By Gauss' Lemma, we have

$$\left(\tfrac{q}{p}\right)\cdot\left(\tfrac{p}{q}\right) = (-1)^{|qP\cap N|}(-1)^{|pQ\cap M|} = (-1)^{|qP\cap N| + |pQ+M|}$$

where $qP \cap N \subseteq U_p$ and $pQ \cap M \subseteq U_q$. Note that $|qP \cap N|$ is equal to the number of elements $x \in P$ with $qx \in N \bmod p$, which is equal to the number of $x \in P$ such that $qx - py \in N$ for some $y \in \mathbb{Z}$. Also note that

$$\begin{aligned} qx - py \in N &\iff py - qx \in P \iff 1 \le py - qx \le \tfrac{p-1}{2} \iff 0 < py - qx < \tfrac{p}{2} \\ &\iff qx < py < qx + \tfrac{p}{2} \iff \tfrac{q}{p}\,x < y < \tfrac{q}{p}\,x + \tfrac{1}{2} \end{aligned}$$

and so $|qP \cap N|$ is equal to the number of ordered pairs of integers (x, y) in the rectangle $R = \left[1, \frac{p-1}{2}\right] \times \left[1, \frac{q-1}{2}\right]$ such that $\frac{q}{p}\,x < y < \frac{q}{p}\,x + \frac{1}{2}$. Similarly, $|pQ \cap M|$ is equal to the number of ordered pairs of integers (x, y) in the rectangle R such that $\frac{p}{q}\,y < x < \frac{p}{q}\,y + \frac{1}{2}$. Note that since $\gcd(p, q) = 1$ there are no points (x, y) which lie on the line $y = \frac{q}{p}\,x$. To summarize, we have $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^m$ where $m = |qP + N| + |pQ + M|$ which is equal to the number of ordered pairs of integers $(x, y) \in R$ which lie strictly between the lines $y = \frac{q}{p}\,x + \frac{1}{2}$ and $x = \frac{p}{q}\,y + \frac{1}{2}$. Since these two lines are symmetric in the rectangle R, we also have $m = r - 2s$ where r is the number of $(x, y) \in R$ and s is the number of $(x, y) \in R$ with $y \ge \frac{q}{p}\,x + \frac{1}{2}$. Since $r = \frac{p-1}{2}\cdot\frac{q-1}{2}$ and $2s$ is even, we have $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$, as required.



4.14 Theorem: *Let p be an odd prime. Then*

(1) $-1 \in Q_p \iff p = 1 \bmod 4$,
(2) $\;\;2 \in Q_p \iff p = \pm 1 \bmod 8$,
(3) $-2 \in Q_p \iff p = 1$ *or* $3 \bmod 8$, *and*
(4) $\;\;3 \in Q_p \iff p = \pm 1 \bmod 12$.

Proof: To prove Part 1, note that by Euler's Criterion we have

$$\left(\tfrac{-1}{p}\right) = (-1)^{(p-1)/2} = \left\{ \begin{array}{r} 1 \text{ if } \frac{p-1}{2} \text{ is even} \\ -1 \text{ if } \frac{p-1}{2} \text{ is odd} \end{array} \right\} = \left\{ \begin{array}{r} 1 \text{ if } p = 1 \bmod 4 \\ -1 \text{ if } p = 3 \bmod 4 \end{array} \right\}.$$

To prove Part 2, note that by Gauss' Lemma we have $\left(\frac{2}{p}\right) = (-1)^{|2P\cap N|}$.

Case 1: suppose that $p = 1 \bmod 4$ so that $\frac{p-1}{2}$ is even. The sets P and $2P$ decompose as the disjoint unions

$$P = \left\{1, 2, \cdots, \tfrac{p-1}{4}\right\} \cup \left\{\tfrac{p+3}{4}, \cdots, \tfrac{p-1}{2}\right\},$$
$$2P = \left\{2, 4, \cdots, \tfrac{p-1}{2}\right\} \cup \left\{\tfrac{p+3}{2}, \cdots, p-1\right\}.$$

The first of the two sets which decompose $2P$ lies in P and the second set lies in N, so we have $|2P \cap P| = \frac{p-1}{4}$ and $|2P \cap N| = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$. Thus when $p = 1 \bmod 4$ we have

$$\left(\tfrac{2}{p}\right) = (-1)^{|2P\cap N|} = (-1)^{(p-1)/4} = \left\{ \begin{array}{r} 1 \text{ if } \frac{p-1}{4} \text{ is even} \\ -1 \text{ if } \frac{p-1}{4} \text{ is odd} \end{array} \right\} = \left\{ \begin{array}{r} 1 \text{ if } p = 1 \bmod 8 \\ -1 \text{ if } p = 5 \bmod 8 \end{array} \right\}.$$

Case 2: suppose that $p = 3 \bmod 4$ so that $\frac{p-1}{2}$ is odd. Then P and $2P$ are the disjoint unions

$$P = \left\{1, 2, \cdots, \tfrac{p-3}{4}\right\{ \cup \left\{\tfrac{p+1}{4}, \cdots, \tfrac{p-1}{2}\right\}$$
$$2P = \left\{2, 4, \cdots, \tfrac{p-3}{2}\right\} \cup \left\{\tfrac{p+1}{2}, \cdots, p-1\right\}.$$

The first of the sets which decompose $2P$ lies in P and the second lies in N so we have $|2P \cap P| = \frac{p-3}{4}$ and $|2P \cap N| = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$. Thus when $p = 3 \bmod 4$ we have

$$\left(\tfrac{2}{p}\right) = (-1)^{|2P\cap N|} = (-1)^{(p-1)/4} = \left\{ \begin{array}{r} 1 \text{ if } \frac{p+1}{4} \text{ is even} \\ -1 \text{ if } \frac{p+1}{4} \text{ is odd} \end{array} \right\} = \left\{ \begin{array}{r} 1 \text{ if } p = 7 \bmod 8 \\ -1 \text{ if } p = 3 \bmod 8 \end{array} \right\}.$$

Combining the results from Cases 1 and 2 gives

$$\left(\tfrac{2}{p}\right) = \left\{ \begin{array}{r} 1 \text{ if } p = 1, 7 \bmod 8 \\ -1 \text{ if } p = 3, 5 \bmod 8 \end{array} \right\}.$$

Part 3 follows from Parts 1 and 2 using Theorem 7.9. Indeed, since

$$\left(\tfrac{-1}{p}\right) = \left\{ \begin{array}{rl} 1 & \text{if } p = 1, 5 \bmod 8 \\ -1 & \text{if } p = 3, 7 \bmod 8 \end{array} \right\} \quad \text{and} \quad \left(\tfrac{2}{p}\right) = \left\{ \begin{array}{rl} 1 & \text{if } p = 1, 7 \bmod 8 \\ -1 & \text{if } p = 3, 5 \bmod 8 \end{array} \right\}$$

It follows that

$$\left(\tfrac{-2}{p}\right) = \left(\tfrac{-1}{p}\right) \cdot \left(\tfrac{2}{p}\right) = \left\{ \begin{array}{r} 1 \text{ if } p = 1, 3 \bmod 8 \\ -1 \text{ if } p = 5, 7 \bmod 8 \end{array} \right\}.$$

Finally, we shall prove Part 4 using Quadratic Reciprocity. Fist note that $3 \notin Q_3$ so we can assume that $p > 3$ and hence that $p = 1, 2 \bmod 3$. By Quadratic Reciprocity, we have

$$\left(\tfrac{3}{p}\right) = \left\{ \begin{array}{r} \left(\frac{p}{3}\right) \text{ if } p = 1 \bmod 4 \\ -\left(\frac{p}{3}\right) \text{ if } p = 3 \bmod 4 \end{array} \right\}.$$

In the case that $p = 1 \bmod 4$, since $1 \in Q_3$ and $2 \notin Q_3$, we have $\left(\frac{p}{3}\right) = 1$ when $p = 1 \bmod 3$, that is when $p = 1 \bmod 12$, and we have $\left(\frac{p}{3}\right) = -1$ when $p = 2 \bmod 3$, that is when $p = 5 \bmod 12$. Similarly, in the case that $p = 3 \bmod 4$ we have $-\left(\frac{p}{3}\right) = 1$ when $p = 2 \bmod 3$, that is when $p = 11 \bmod 12$ and we have $-\left(\frac{p}{3}\right) = -1$ when $p = 1 \bmod 3$, that is when $p = 7 \bmod 12$. Part 4 follows by combing the results of both cases.

4.15 Example: Determine whether $7 \in Q_{43}$.

Solution: We provide 4 solutions. First we make a table showing the values of k^2, 7^k and $7k$ for half of the values of $k \in U_{43}$ (that is the values $k \in P$).

k	k^2	7^k	$7k$	k	k^2	7^k	$7k$
1	1	7	7	12	1	1	-2
2	4	6	14	13	40	7	5
3	9	-1	21	14	24	6	12
4	16	-7	-15	15	10	-1	19
5	25	-6	-8	16	41	-7	-17
6	36	1	-1	17	31	-6	-10
7	6	7	6	18	23	1	-3
8	21	6	13	19	17	7	4
9	38	-1	20	20	13	6	11
10	14	-7	-16	21	11	-1	18
11	35	-6	-9				

For the first solution, note that since the column listing the values of k^2 does not include 7, it follows from the definition of Q_{43} that $7 \notin Q_{43}$.

For the second solution, we apply Euler's Criterion, using the column listing the values of 7^k, to obtain $\left(\frac{7}{43}\right) = (-1)^{(43-1)/2} = (-1)^{21} = -1$ so that $7 \notin Q_{43}$, hence $7 \notin Q_{43}$.

For the third solution, we apply Gauss' Lemma, using the column which lists the values of $7k$ for $k \in P$. Note that this column indicates, for each $k \in P$, whether $7k \in P$ or $7k \in N$. Since 9 of the entries in this column are negative, we have $|7P \cap N| = 9$ and so $\left(\frac{7}{43}\right) = (-1)^{|7P \cap N|} = (-1)^9 = -1$.

For the fourth solution, we use Quadratic Reciprocity. Since $7 = 3 \bmod 4$ and $43 = 3 \bmod 4$ we have $\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) = -\left(\frac{1}{7}\right) = -1$ and so $7 \notin Q_{43}$.

4.16 Example: Determine whether $136 \in Q_{421}$.

Solution: First we determine whether 421 is prime. Since $\lfloor\sqrt{421}\rfloor = 20$, it suffices to check each of the primes $2, 3, 5, 7, 11, 13, 17, 19$ to see whether they are factors. We find that none of those primes are factors, and so 421 is prime. Since $136 = 2^3 \cdot 17$ we have

$$\left(\frac{136}{421}\right) = \left(\frac{2}{421}\right)^2 \cdot \left(\frac{2}{421}\right) \cdot \left(\frac{17}{421}\right) = \left(\frac{2}{421}\right) \cdot \left(\frac{17}{421}\right).$$

Since for an odd prime p we have $2 \in Q_p \iff p = 1 \bmod 8$, and since $421 = 5 \bmod 8$, we have $2 \notin Q_{421}$ so that $\left(\frac{2}{421}\right) = -1$. Also, by applying Quadratic Reciprocity twice, since $421 = 1 \bmod 4$ and $13 = 1 \bmod 4$ we have $\left(\frac{17}{421}\right) = \left(\frac{421}{17}\right) = \left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1$. Thus

$$\left(\frac{136}{421}\right) = \left(\frac{2}{421}\right) \cdot \left(\frac{17}{421}\right) = (-1)(1) = -1 \text{ , and so } 136 \notin Q_{421}.$$

4.17 Example: Determine whether $468 \in Q_{697}$.

First we determine whether 697 is prime. Since $\lfloor\sqrt{697}\rfloor = 26$, it suffices to check each of the primes $2, 3, 5, 7, 11, 13, 17, 19, 23$ to see whether they are factors. We find that in fact 17 is a factor and that $697 = 17 \cdot 41$, and so we need to determine whether $468 \in Q_{17}$ and whether $468 \in Q_{41}$. Since $468 = 9 = 3^2 \bmod 17$ we have $468 \in Q_{17}$. Reducing modulo the denominator and applying Quadratic Reciprocity three times gives

$$\left(\frac{468}{41}\right) = \left(\frac{17}{41}\right) = \left(\frac{41}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

so $468 \notin Q_{41}$ hence $468 \notin Q_{697}$.

4.18 Example: Find a polynomial $f(x) \in \mathbb{Z}[x]$ which has a root in $\mathbb{Z}_n$ for every $n \in \mathbb{Z}^+$ but which has no root in $\mathbb{Z}$.

Solution: Note that $13 \in Q_{17}$ (indeed $13 = 8^2 \bmod 17$), and $17 \in Q_{13}$ ($17 = 2^2 \bmod 13$), and $17 = 1 \bmod 8$, and $13 \cdot 17 = 221$, and consider the polynomial

$$f(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221).$$

Note that $f(x)$ has real roots $\pm\sqrt{13}$, $\pm\sqrt{17}$, $\pm\sqrt{221}$ so it has no roots in $\mathbb{Z}$ (or $\mathbb{Q}$). Since $17 = 1 \bmod 8$ we have $17 \in Q_{2^k}$ for all $k \in \mathbb{Z}^+$ and hence $f(x)$ has a root in $\mathbb{Z}_{2^k}$ for all $k \in \mathbb{Z}^+$. Since $13 \in Q_{17}$ we also have $13 \in Q_{17^k}$ for all $k \in \mathbb{Z}^+$, and it follows that $f(x)$ has a root in $\mathbb{Z}_{17^k}$ for all $k \in \mathbb{Z}^+$. Since $17 \in Q_{13}$ we also have $17 \in Q_{13^k}$ for all $k \in \mathbb{Z}^+$, and it follows that $f(x)$ has a root in $\mathbb{Z}_{13^k}$ for all $k \in \mathbb{Z}^+$. For any prime $p \neq 2, 13, 17$ we have $\left(\frac{221}{p}\right) = \left(\frac{13}{p}\right) \cdot \left(\frac{17}{p}\right)$ and it follows that one of the three Legendre symbols $\left(\frac{13}{p}\right)$, $\left(\frac{17}{p}\right)$ or $\left(\frac{221}{p}\right)$ must be equal to 1, and so either $13 \in Q_p$ or $17 \in Q_p$ or $221 \in Q_p$, and hence for every $k \in \mathbb{Z}^+$, either $f(13) = 0$ or $f(17) = 0$ or $f(221) = 0$ in $\mathbb{Z}_{p^k}$. Thus $f(x)$ has a root in $\mathbb{Z}_{p^k}$ for every prime p and every $k \in \mathbb{Z}^+$. Finally, suppose that $n = \prod {p_i}^{k_i}$, where $p_1, \cdots, p_\ell$ are distinct primes and $k_1, \cdots, k_\ell \in \mathbb{Z}^+$. For each index i, choose $a_i \in \mathbb{Z}$ such that $f(a_i) = 0 \in \mathbb{Z}_{{p_i}^{k_i}}$. By the Chinese Remainder Theorem, we can choose $x \in \mathbb{Z}$ so that $x = a_i \bmod {p_1}^{k_i}$ for all indices i. Then, for all indices i, we have $f(x) = f(a_i) = 0 \bmod {p_i}^{k_i}$ and hence, by the Chinese Remainder Theorem, we have $f(x) = 0 \bmod n$.

4.19 Remark: We can extend the Legendre symbol to the **Jacobi symbol** $\left(\frac{a}{b}\right)$, defined for $a, b \in \mathbb{Z}^+$ with b odd, by defining

$$\left(\frac{a}{\prod {p_i}^{k_i}}\right) = \prod \left(\frac{a}{p_i}\right)^{k_i}.$$

As an optional exercise, you can verify that the Jacobi symbol satisfies the following properties.

(1) $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right) \cdot \left(\frac{b}{c}\right)$,
(2) $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{c}\right)$,
(3) $\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right)$ when $a = b \bmod c$,
(4) $\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}$,
(5) $\left(\frac{-1}{a}\right) = \left\{ \begin{array}{r} 1 \text{ if } a = 1 \bmod 4 \\ -1 \text{ if } a = 3 \bmod 4 \end{array} \right\}$ and $\left(\frac{2}{a}\right) = \left\{ \begin{array}{r} 1 \text{ if } a = 1, 7 \bmod 8 \\ -1 \text{ if } a = 3, 5 \bmod 8 \end{array} \right\}$.