ELEMENTARY NUMBER THEORY

W W L CHEN

Chapter 4

QUADRATIC RESIDUES

4.1. Introduction

In this chapter, we are concerned with quadratic congruences of the form

$$x^2 \equiv a \pmod{p}, \tag{1}$$

where p is an odd prime and $a \in \mathbb{Z}$. We are interested in determining whether for given p and a, the congruence (1) has a solution $x \in \mathbb{Z}$.

If $a \equiv 0 \pmod{p}$, then clearly (1) is soluble, with $x \equiv 0 \pmod{p}$ being the only solution. We therefore make the assumption that $a \not\equiv 0 \pmod{p}$. If (1) is soluble, then we say that a is a quadratic residue modulo p. If (1) is not soluble, then we say that a is a quadratic non-residue modulo p.

THEOREM 4A. *Suppose that p is an odd prime. Then there are precisely $(p-1)/2$ quadratic residues modulo p, and these are represented by the numbers*

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{2}$$

PROOF. Suppose that $p \nmid a$. Then it follows from Lagrange's theorem that the congruence (1) has at most two solutions. On the other hand, if $x \equiv b \pmod{p}$ is a solution, then it is easy to check that $x \equiv p-b \pmod{p}$ represents another solution. It follows that the congruence (1) has either two solutions or no solutions. Note next that any solution of the congruence (1) must be of the form $x \equiv b \pmod{p}$, with $1 \le b \le p-1$. It follows that there can be at most $(p-1)/2$ quadratic residues modulo p. It remains to show that there are at least $(p-1)/2$ quadratic residues modulo p. To do so, note that the $(p-1)/2$ numbers in (2) are clearly quadratic residues modulo p. It therefore suffices to show that they are incongruent modulo p. Suppose on the contrary that $x^2 \equiv y^2 \pmod{p}$, with $1 \le x < y \le (p-1)/2$. Then $p \mid (y-x)(y+x)$, a contradiction since p is prime and $0 < y-x < y+x < p$. ○

It is convenient to introduce the Legendre symbol, defined as follows. Suppose that p is an odd prime. Then we write

$$\left(\frac{a}{p}\right)_L = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

4.2. The Legendre Symbol

In this section, we analyze the Legendre symbol in a systematic way to provide some practical means of evaluating its value. Our first step is not particularly useful in itself, but provides a path towards results of a more practical nature.

THEOREM 4B. (EULER'S CRITERION) *Suppose that p is an odd prime. For every $a \in \mathbb{Z}$, we have*

$$\left(\frac{a}{p}\right)_L \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

PROOF. The result clearly holds if $p \mid a$, so we assume now that $p \nmid a$. If a is a quadratic residue modulo p, then there exists $x \in \mathbb{Z}$ such that $p \nmid x$ and $x^2 \equiv a \pmod{p}$. It follows from Fermat's little theorem that

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 = \left(\frac{a}{p}\right)_L \pmod{p}.$$

Consider next the congruence

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

By Fermat's little theorem, this has $p-1$ solutions. On the other hand, by Lagrange's theorem, neither

$$a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \tag{3}$$

nor

$$a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p} \tag{4}$$

has more than $(p-1)/2$ solutions. It follows that each of (3) and (4) has exactly $(p-1)/2$ solutions. The $(p-1)/2$ quadratic residues a modulo p all satisfy (3). It follows that all the quadratic non-residues a must satisfy (4). ○

We have immediately the following two consequences.

THEOREM 4C. *Suppose that p is an odd prime. Then*

$$\left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}}.$$

PROOF. Taking $a = 1$ in Theorem 4B, we obtain

$$\left(\frac{-1}{p}\right)_L \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Note, however, that

$$\left(\frac{-1}{p}\right)_L - (-1)^{\frac{p-1}{2}} \in \{-2, 0, 2\}.$$

The result follows. ○

THEOREM 4D. *Suppose that p is an odd prime. Then for every $a, b \in \mathbb{Z}$, we have*

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

PROOF. The result is trivial if $p \mid a$ or $p \mid b$, so we assume now that $p \nmid a$ and $p \nmid b$. It follows from Theorem 4B that

$$\left(\frac{ab}{p}\right)_L \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)_L \left(\frac{b}{p}\right)_L \pmod{p}.$$

Note, however, that

$$\left(\frac{ab}{p}\right)_L - \left(\frac{a}{p}\right)_L \left(\frac{b}{p}\right)_L \in \{-2, 0, 2\}.$$

The result follows. ○

In practice, Euler's criterion is not very useful when p is a rather large prime. The following represents a result of a more practical nature.

THEOREM 4E. (GAUSS'S LEMMA) *Suppose that p is an odd prime, and the integer $a \in \mathbb{Z}$ satisfies $p \nmid a$. Let*

$$m = \#\left\{x \in \mathbb{N} : 1 \le x < \frac{p}{2} \text{ and } \frac{p}{2} < ax - p\left[\frac{ax}{p}\right] < p\right\};$$

in other words, m is the number of integers x satisfying $1 \le x < p/2$ for which the residue r_x of ax satisfies $p/2 < r_x < p$. Then

$$\left(\frac{a}{p}\right)_L = (-1)^m.$$

PROOF. By Euler's criterion, we have

$$\prod_{x=1}^{\frac{p-1}{2}} r_x \equiv \prod_{x=1}^{\frac{p-1}{2}} ax = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right)_L \left(\frac{p-1}{2}\right)! \pmod{p}. \tag{5}$$

Let $\alpha_1, \ldots, \alpha_m$ denote the m values of r_x for which $p/2 < r_x < p$, and let $\beta_1, \ldots, \beta_\ell$, where $\ell + m = (p-1)/2$, denote the ℓ values of r_x for which $0 < r_x < p/2$. Then

$$\prod_{x=1}^{\frac{p-1}{2}} r_x = \left(\prod_{i=1}^{m} \alpha_i\right) \left(\prod_{j=1}^{\ell} \beta_j\right) \equiv (-1)^m \left(\prod_{i=1}^{m} (p - \alpha_i)\right) \left(\prod_{j=1}^{\ell} \beta_j\right) \pmod{p}. \tag{6}$$

Clearly, for every $i = 1, \ldots, m$, we have $0 < p - \alpha_i < p/2$. Also, for every $j = 1, \ldots, \ell$, we have $0 < \beta_j < p/2$. Note also that the numbers $\alpha_1, \ldots, \alpha_m$ are distinct, and the numbers $\beta_1, \ldots, \beta_\ell$ are also distinct. Furthermore, for every $i = 1, \ldots, m$ and every $j = 1, \ldots, \ell$, the numbers $p - \alpha_i$ and β_j are different, for $p - \alpha_i = \beta_j$ would give $ax \equiv -ay \pmod{p}$, and hence $x + y \equiv 0 \pmod{p}$, for some $x, y \in \mathbb{Z}$ satisfying $1 \le x < y \le (p-1)/2$, clearly impossible. Hence

$$\left(\prod_{i=1}^{m} (p - \alpha_i)\right) \left(\prod_{j=1}^{\ell} \beta_j\right) = \left(\frac{p-1}{2}\right)!. \tag{7}$$

The result now follows on combining (5)–(7). ○

THEOREM 4F. *Suppose that p is an odd prime. Then*

$$\left(\frac{2}{p}\right)_L = (-1)^{[\frac{p}{2}]-[\frac{p}{4}]} = (-1)^{\frac{p^2-1}{8}}.$$

PROOF. The numbers $2, 4, 6, \ldots, p-1$ all lie between 0 and p, and so are their own residues modulo p. Moreover, $p/2 < 2x < p$ if and only if $p/4 < x < p/2$. Hence we must have $m = [p/2] - [p/4]$. The second equality is obtained by checking. ○

4.3. Quadratic Reciprocity

Suppose that $p, q \in \mathbb{N}$ are distinct odd primes. There is a beautiful result which links the solubility of the two quadratic congruences

$$x^2 \equiv q \pmod{p} \qquad \text{and} \qquad x^2 \equiv p \pmod{q},$$

in the sense that if we know whether one of these two congruences is soluble, then the determination of whether the other congruence is soluble involves only a simple calculation.

THEOREM 4G. (LAW OF QUADRATIC RECIPROCITY) *Suppose that $p, q \in \mathbb{N}$ are distinct odd primes. Then*

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

Theorem 4G will follow from the following three results.

THEOREM 4H. *Suppose that p is an odd prime, and the integer $a \in \mathbb{Z}$ satisfies $p \nmid a$. Then*

$$\left(\frac{a}{p}\right)_L = (-1)^n,$$

where

$$n = \sum_{y=1}^{\frac{p-1}{2}} \left[\frac{2ay}{p}\right].$$

PROOF. We shall use Gauss's lemma. In the notation of Theorem 4E, we have

$$m = \#\left\{x \in \mathbb{N} : 1 \le x \le \frac{p-1}{2} \text{ and } 1 < \frac{2ax}{p} - 2\left[\frac{ax}{p}\right] < 2\right\}.$$

Also, for any $x \in \mathbb{Z}$ satisfying $1 \le x \le (p-1)/2$, we must have

$$0 < \frac{2ax}{p} - 2\left[\frac{ax}{p}\right] < 2.$$

Hence

$$m = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p} - 2\left[\frac{ax}{p}\right]\right] \equiv n \pmod 2.$$

This completes the proof. ◯

THEOREM 4J. *Suppose that $p, q \in \mathbb{N}$ are distinct odd primes. Then*

$$\left(\frac{q}{p}\right)_L = (-1)^{\lambda(p,q)},$$

where

$$\lambda(p,q) = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right].$$

PROOF. Suppose that $a \in \mathbb{Z}$ is odd. Then $2 \mid (a+p)$, and

$$\left(\frac{\frac{1}{2}(a+p)}{p}\right)_L = \left(\frac{4}{p}\right)_L \left(\frac{\frac{1}{2}(a+p)}{p}\right)_L = \left(\frac{2(a+p)}{p}\right)_L = \left(\frac{2a}{p}\right)_L = \left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L,$$

in view of Theorem 4D. It follows from Theorem 4H that

$$\left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L = \left(\frac{\frac{1}{2}(a+p)}{p}\right)_L = (-1)^r,$$

where

$$r = \sum_{y=1}^{\frac{p-1}{2}} \left[\frac{(a+p)y}{p}\right].$$

Now

$$\sum_{y=1}^{\frac{p-1}{2}} \left[\frac{(a+p)y}{p}\right] = \sum_{y=1}^{\frac{p-1}{2}} \left(\left[\frac{ay}{p}\right] + y\right) = \sum_{y=1}^{\frac{p-1}{2}} \left[\frac{ay}{p}\right] + \frac{p^2-1}{8}.$$

Putting $a = 1$, we deduce (again) that

$$\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}.$$

It now follows that for odd prime q, we must have

$$\left(\frac{q}{p}\right)_L = (-1)^s, \qquad \text{where} \qquad s = \sum_{y=1}^{\frac{p-1}{2}} \left[\frac{qy}{p}\right].$$

This completes the proof. ◯

THEOREM 4K. *Suppose that $p,q\in\mathbb{N}$ are distinct odd primes. Then in the notation of Theorem 4J, we have*

$$\lambda(p,q)+\lambda(q,p)=\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right).$$

PROOF. We have

$$\lambda(p,q)=\sum_{1\le x<\frac{p}{2}}\left[\frac{qx}{p}\right]=\sum_{1\le x<\frac{p}{2}}\sum_{1\le y<\frac{qx}{p}}1=\sum_{1\le y<\frac{q}{2}}\sum_{\frac{py}{q}<x<\frac{p}{2}}1,$$

since $qx/p\notin\mathbb{Z}$ when $x<p$. Also,

$$\lambda(q,p)=\sum_{1\le y<\frac{q}{2}}\sum_{1\le x<\frac{py}{q}}1.$$

It follows that

$$\lambda(p,q)+\lambda(q,p)=\sum_{1\le y<\frac{q}{2}}\sum_{1\le x<\frac{p}{2}}1=\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right),$$

since both p and q are odd. ○

EXAMPLE. The numbers 8783 and 15671 are prime. We want to determine the number of solutions of the congruence $x^2\equiv 8783 \pmod{15671}$. We have

$$\begin{aligned}\left(\frac{8783}{15671}\right)_L&=(-1)^{\left(\frac{8783-1}{2}\right)\left(\frac{15671-1}{2}\right)}\left(\frac{15671}{8783}\right)_L=-\left(\frac{15671}{8783}\right)_L=-\left(\frac{6888}{8783}\right)_L\\&=-\left(\frac{2}{8783}\right)_L^3\left(\frac{3}{8783}\right)_L\left(\frac{7}{8783}\right)_L\left(\frac{41}{8783}\right)_L=-\left(\frac{2}{8783}\right)_L\left(\frac{3}{8783}\right)_L\left(\frac{7}{8783}\right)_L\left(\frac{41}{8783}\right)_L.\end{aligned}$$

Next, note that

$$\begin{aligned}\left(\frac{2}{8783}\right)_L&=-(-1)^{\left[\frac{8783}{2}\right]-\left[\frac{8783}{4}\right]},\\\left(\frac{3}{8783}\right)_L&=(-1)^{\left(\frac{3-1}{2}\right)\left(\frac{8783-1}{2}\right)}\left(\frac{8783}{3}\right)_L,\\\left(\frac{7}{8783}\right)_L&=(-1)^{\left(\frac{7-1}{2}\right)\left(\frac{8783-1}{2}\right)}\left(\frac{8783}{7}\right)_L,\\\left(\frac{41}{8783}\right)_L&=(-1)^{\left(\frac{41-1}{2}\right)\left(\frac{8783-1}{2}\right)}\left(\frac{8783}{41}\right)_L.\end{aligned}$$

It follows that

$$\begin{aligned}\left(\frac{8783}{15671}\right)_L&=-\left(\frac{8783}{3}\right)_L\left(\frac{8783}{7}\right)_L\left(\frac{8783}{41}\right)_L=-\left(\frac{2}{3}\right)_L\left(\frac{5}{7}\right)_L\left(\frac{9}{41}\right)_L=-(-1)^{\frac{9-1}{8}}\left(\frac{5}{7}\right)_L\left(\frac{3}{41}\right)_L^2\\&=\left(\frac{5}{7}\right)_L=(-1)^{\left(\frac{5-1}{2}\right)\left(\frac{7-1}{2}\right)}\left(\frac{7}{5}\right)_L=\left(\frac{7}{5}\right)_L=\left(\frac{2}{5}\right)_L=(-1)^{\frac{25-1}{8}}=-1.\end{aligned}$$

Hence the congruence has no solutions.

4.4. The Jacobi Symbol

To shorten many calculations involving the Legendre symbol, we introduce the Jacobi symbol which can be considered in some way to be a generalization of the Legendre symbol. For every $n \in \mathbb{Z}$, we write

$$\left(\frac{n}{1}\right)_J = 1.$$

If m is a positive odd integer with canonical decomposition $m = p_1^{u_1} \ldots p_r^{u_r}$, where $p_1, \ldots, p_r$ are distinct odd primes, then we write

$$\left(\frac{n}{m}\right)_J = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)_L^{u_i}.$$

Remark. We emphasize immediately that the Jacobi symbol is for calculation only. In particular, note that

$$\left(\frac{n}{m}\right)_J = 1$$

does not necessarily imply that the congruence $x^2 \equiv n \pmod{m}$ is soluble. Consider, for example, the case when $n = 2$ and $m = 15$.

The following observations can be deduced from the properties of the Legendre symbol. We leave the proof as an exercise for the reader.

THEOREM 4L. *Suppose that m and m' are odd positive integers. Then for every $n, n' \in \mathbb{Z}$, we have*

(i) $\left(\frac{n}{m}\right)_J \left(\frac{n'}{m}\right)_J = \left(\frac{nn'}{m}\right)_J$;

(ii) $\left(\frac{n}{m}\right)_J \left(\frac{n}{m'}\right)_J = \left(\frac{n}{mm'}\right)_J$;

(iii) $\left(\frac{n}{m}\right)_J = \left(\frac{n'}{m}\right)_J$ *whenever* $n \equiv n' \pmod{m}$; *and*

(iv) $\left(\frac{a^2 n}{m}\right)_J = \left(\frac{n}{m}\right)_J$ *whenever* $(a, m) = 1$.

THEOREM 4M. *Suppose that m is an odd positive integer. Then*

$$\left(\frac{-1}{m}\right)_J = (-1)^{\frac{m-1}{2}} \qquad \text{and} \qquad \left(\frac{2}{m}\right)_L = (-1)^{\frac{m^2-1}{8}}.$$

Proof. It is convenient to write $m = p_1 \ldots p_s$, where the prime factors are not necessarily distinct. Then

$$m = \prod_{j=1}^{s}(1 + p_j - 1) = 1 + \sum_{j=1}^{s}(p_j - 1) + \sum_{\substack{j=1 \\ j \neq k}}^{s}\sum_{k=1}^{s}(p_j - 1)(p_k - 1) + \ldots \equiv 1 + \sum_{j=1}^{s}(p_j - 1) \pmod{4},$$

and so

$$\frac{m-1}{2} \equiv \sum_{j=1}^{s} \frac{p_j - 1}{2} \pmod{2}.$$

Thus

$$\left(\frac{-1}{m}\right)_J = \prod_{j=1}^{s} \left(\frac{-1}{p_j}\right)_L = \prod_{j=1}^{s} (-1)^{\frac{p_j-1}{2}} = (-1)^{\frac{m-1}{2}},$$

proving the first assertion. Similarly, we can write

$$m^2 = \prod_{j=1}^{s}(1+p_j^2-1) = 1 + \sum_{j=1}^{s}(p_j^2-1) + \sum_{j=1}^{s}\sum_{\substack{k=1 \\ j\neq k}}^{s}(p_j^2-1)(p_k^2-1) + \ldots \equiv 1 + \sum_{j=1}^{s}(p_j^2-1) \pmod{16},$$

and so

$$\frac{m^2-1}{8} \equiv \sum_{j=1}^{s} \frac{p_j^2-1}{8} \pmod{2}.$$

Thus

$$\left(\frac{2}{m}\right)_J = \prod_{j=1}^{s} \left(\frac{2}{p_j}\right)_L = \prod_{j=1}^{s} (-1)^{\frac{p_j^2-1}{8}} = (-1)^{\frac{m^2-1}{8}},$$

proving the second assertion. ○

We leave it as an exercise for the reader to prove the following reciprocity result.

THEOREM 4N. *Suppose that m and n are odd positive integers and $(m,n)=1$. Then*

$$\left(\frac{m}{n}\right)_J \left(\frac{n}{m}\right)_J = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}.$$

Example. Let us consider our earlier example again. Recall that we want to determine the number of solutions of the congruence $x^2 \equiv 8783 \pmod{15671}$, where the numbers 8783 and 15671 are prime. Omitting the details of a few steps from earlier, we have

$$\begin{aligned}
\left(\frac{8783}{15671}\right)_L &= -\left(\frac{6888}{8783}\right)_L = -\left(\frac{2}{8783}\right)_L^3 \left(\frac{861}{8783}\right)_L = -\left(\frac{861}{8783}\right)_L = -\left(\frac{861}{8783}\right)_J \\
&= -(-1)^{\left(\frac{861-1}{2}\right)\left(\frac{8783-1}{2}\right)} \left(\frac{8783}{861}\right)_J = -\left(\frac{8783}{861}\right)_J = -\left(\frac{173}{861}\right)_J \\
&= -(-1)^{\left(\frac{173-1}{2}\right)\left(\frac{861-1}{2}\right)} \left(\frac{861}{173}\right)_J = -\left(\frac{861}{173}\right)_L = -\left(\frac{-4}{173}\right)_L \\
&= -\left(\frac{-1}{173}\right)_L \left(\frac{2}{173}\right)_L^2 = -\left(\frac{-1}{173}\right)_L = -(-1)^{\frac{173-1}{2}} = -1.
\end{aligned}$$

Alternatively, try to fill in the missing details in the argument below. We have

$$\begin{aligned}
\left(\frac{8783}{15671}\right)_L &= -\left(\frac{15671}{8783}\right)_L = -\left(\frac{-1895}{8783}\right)_L = -\left(\frac{8783}{1895}\right)_J \\
&= -\left(\frac{8783}{5}\right)_J \left(\frac{8783}{379}\right)_J = -\left(\frac{379}{33}\right)_J = -\left(\frac{16}{33}\right)_J = -1.
\end{aligned}$$

4.5. The Distribution of Quadratic Residues

Suppose that the prime p satisfies $p \equiv 1 \pmod{8(k!)}$, where $k \in \mathbb{N}$. Then it is not difficult to see that 2 is a quadratic residue modulo p. Furthermore, for any odd prime $q \in \mathbb{N}$ such that $q \leq k$ and $q \neq p$, we have

$$\left(\frac{q}{p}\right)_L = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\left(\frac{p}{q}\right)_L = \left(\frac{1}{q}\right)_L = 1,$$

so that q is a quadratic residue modulo p. Suppose now that $n \in \mathbb{N}$ satisfies $n \leq k$. Then all the prime factors of n do not exceed k. It follows from Theorem 4D that n is a quadratic residue modulo p.

Now let n_p denote the least positive quadratic non-residue modulo p. For the prime p above, we have $n_p > k$. It follows that

$$\limsup_{p\to\infty} n_p = \infty.$$

In 1919, Vinogradov conjectured that for any $\epsilon > 0$, we have $n_p \ll_\epsilon p^\epsilon$ as $p \to \infty$. Here we prove the following weaker result.

THEOREM 4P. *For every odd prime p, we have*

$$n_p \leq \frac{1}{2} + \left(p + \frac{1}{4}\right)^{1/2}. \tag{8}$$

PROOF. Let $h = [p/n_p] + 1$. Then $p < hn_p < p + n_p$, so that $(hn_p/p)_L = 1$. Since $(n_p/p)_L = -1$, it follows from Theorem 4D that $(h/p)_L = -1$. Note now that since $0 < h < p/2 + 1 < p$, we must have $1 \leq h < p$, so that $h \geq n_p$. We therefore conclude that

$$n_p \leq \left[\frac{p}{n_p}\right] + 1 \leq \frac{p}{n_p} + 1.$$

The inequality (8) follows. ○

Problems for Chapter 4

1. How many solutions does the congruence $x^2 \equiv 3 \pmod{71}$ have?

2. (i) Show that 3 is a quadratic residue for primes of the form $12k \pm 1$ and a quadratic non-residue for primes of the form $12k \pm 5$.
   (ii) Deduce that -3 is a quadratic residue for primes of the form $6k+1$ and a quadratic non-residue for primes of the form $6k - 1$.
   (iii) By considering $x^2 + 3$, show that there are infinitely many primes of the form $6k + 1$.

3. Suppose that p is an odd prime. Suppose further that the set $\{1, 2, \ldots, p-1\}$ can be expressed as the union of two non-empty subsets $\mathcal{S}$ and $\mathcal{T}$ such that
   - $\mathcal{S} \neq \mathcal{T}$;
   - the product modulo p of any two elements in the same set lies in $\mathcal{S}$; and
   - the product modulo p of any element in $\mathcal{S}$ with any element in $\mathcal{T}$ lies in $\mathcal{T}$.

   Prove that $\mathcal{S}$ consists of the quadratic residues modulo p, and that $\mathcal{T}$ consists of the quadratic non-residues modulo p.

4. (i) Prove that 3 is a primitive root of any prime of the form 2^n+1, where $n>1$ is an integer.
 (ii) Prove that 2 is a primitive root of any prime of the form $2p+1$, where p is a prime of the form $4n+1$.
 (iii) Prove that -2 is a primitive root of any prime of the form $2p+1$, where p is a prime of the form $4n+3$.
 (iv) Prove that 2 is a primitive root of any prime of the form $4p+1$, where p is a prime.
 (v) Prove that 3 is a primitive root of any prime of the form 2^np+1, where $n>1$ is an integer and the prime $p>(3^{2^n}-1)/2^n$.

5. Suppose that q is an odd prime, and that $p=4q+1$ is also a prime.
 (i) Prove that the congruence $x^2\equiv -1 \pmod{p}$ has exactly two solutions, each of which is a quadratic non-residue modulo p.
 (ii) Prove that every quadratic non-residue modulo p is a primitive root modulo p, with the exception of the two quadratic non-residues in part (i).
 (iii) Find all the primitive roots of 29.

6. Suppose that $n\in\mathbb{N}$ and p is prime. Prove that if $(n/p)_L=-1$, then $\displaystyle\sum_{d\mid n} d^{\frac{p-1}{2}}\equiv 0 \pmod{p}$.

7. Suppose that the prime $p\equiv 3 \pmod 4$, and that a is a quadratic residue modulo p. Show that the solutions of the congruence $x^2\equiv a \pmod{p}$ are given by $x=\pm a^{\frac{p+1}{4}} \pmod{p}$.

8. Suppose that the prime $p\equiv 5 \pmod 8$, and that a is a quadratic residue modulo p.
 (i) Suppose that $a^{\frac{p-1}{4}}\equiv 1 \pmod{p}$. Show that the solutions of the congruence $x^2\equiv a \pmod{p}$ are given by $x\equiv \pm a^{\frac{p+3}{8}} \pmod{p}$.
 (ii) Suppose that $a^{\frac{p-1}{4}}\equiv -1 \pmod{p}$. Show that the solutions of the congruence $x^2\equiv a \pmod{p}$ are given by $x\equiv \pm 2^{\frac{p-1}{4}}a^{\frac{p+3}{8}} \pmod{p}$.

9. Prove Theorem 4L.

10. Prove Theorem 4N.

11. Suppose that p is an odd prime. Suppose further that $a,b\in\mathbb{Z}$ and $p\nmid a$. Prove that

$$\sum_{n=1}^{p}\left(\frac{an+b}{p}\right)_L=0.$$

12. Suppose that p is an odd positive prime. Suppose further that $k\in\mathbb{Z}$ and $p\nmid k$.
 (i) Prove that

$$\sum_{n=1}^{p-1}\left(\frac{n(n+k)}{p}\right)_L=\sum_{\substack{n=1\\ nn'\equiv 1 \pmod{p}}}^{p-1}\sum_{n'=1}^{p-1}\left(\frac{n(n+knn')}{p}\right)_L=\sum_{n'=1}^{p-1}\left(\frac{1+kn'}{p}\right)_L.$$

 (ii) Deduce that

$$\sum_{n=1}^{p-2}\left(\frac{n(n+k)}{p}\right)_L=\sum_{\substack{n=1\\ nn'\equiv 1 \pmod{p}}}^{p-2}\sum_{n'=1}^{p-2}\left(\frac{n(n+knn')}{p}\right)_L=\sum_{n'=1}^{p-2}\left(\frac{1+kn'}{p}\right)_L.$$

13. Suppose that p is an odd prime.
   (i) Let $A(R,R)$ denote the number of integers n satisfying $1 \le n \le p-2$ such that both n and $n+1$ are quadratic residues modulo p. Show that

$$A(R,R) = \frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)_L\right)\left(1+\left(\frac{n+1}{p}\right)_L\right) = \frac{1}{4}\left(p-4-\left(\frac{-1}{p}\right)_L\right).$$

   (ii) Let $A(R,N)$ denote the number of integers n satisfying $1 \le n \le p-2$ such that n is a quadratic residue and $n+1$ is a quadratic non-residue modulo p. By first considering the sum $A(R,R)+A(R,N)$, find $A(R,N)$.
   (iii) Let $A(N,R)$ denote the number of integers n satisfying $1 \le n \le p-2$ such that n is a quadratic non-residue and $n+1$ is a quadratic residue modulo p. By first considering the sum $A(R,R)+A(N,R)$, find $A(N,R)$.
   (iv) Hence determine $A(N,N)$, the number of integers n satisfying $1 \le n \le p-2$ such that both n and $n+1$ are quadratic non-residues modulo p.

14. Consider the sum

$$S(k) = \sum_{n=1}^{p}\left(\frac{n^2-k}{p}\right)_L,$$

where p is an odd prime, and $k \in \mathbb{Z}$.
   (i) Show that if $p \mid k$, then $S(k) = p-1$.
   (ii) Show that if $p \nmid k$, then

$$S(k) = \sum_{m=1}^{p}\left(\frac{m-k}{p}\right)_L\left(1+\left(\frac{m}{p}\right)_L\right) = -1.$$

15. Consider the sum

$$T(a,b,c) = \sum_{n=1}^{p}\left(\frac{an^2+bn+c}{p}\right)_L,$$

where p is an odd prime, and $a,b,c \in \mathbb{Z}$ satisfy $p \nmid a$. By considering the sum

$$\left(\frac{4a}{p}\right)_L T(a,b,c),$$

show that

$$T(a,b,c) = \begin{cases} -\left(\frac{a}{p}\right)_L & \text{if } p \nmid (b^2-4ac), \\ (p-1)\left(\frac{a}{p}\right)_L & \text{if } p \mid (b^2-4ac). \end{cases}$$

16. Suppose that $f(x)$ is a polynomial with integer coefficients. Suppose further that $a,b \in \mathbb{Z}$ and p is a prime, and $\mathcal{R}$ denotes a complete set of residues modulo p.
   (i) Suppose that $(a,p)=1$. Prove that

$$\sum_{x\in\mathcal{R}}\left(\frac{f(ax+b)}{p}\right)_L = \sum_{x\in\mathcal{R}}\left(\frac{f(x)}{p}\right)_L.$$

(ii) Prove that

$$\sum_{x\in\mathcal{R}}\left(\frac{af(x)}{p}\right)_L=\left(\frac{a}{p}\right)_L\sum_{x\in\mathcal{R}}\left(\frac{f(x)}{p}\right)_L.$$

(iii) Suppose that $(a,p)=1$. Prove that

$$\sum_{x\in\mathcal{R}}\left(\frac{ax+b}{p}\right)_L=0.$$

(iv) Suppose that $(a,p)=(b,p)=1$. Prove that

$$\sum_{x=1}^{p-1}\left(\frac{x(ax+b)}{p}\right)_L=-\left(\frac{a}{p}\right)_L.$$

[Hint: Begin by multiplying the sum by $(4a/p)_L$.]

17. Suppose that the primes $p\equiv 1 \pmod 4$ and $q\equiv 3 \pmod 4$. Prove each of the following:

(i) $\displaystyle\sum_{n=1}^{p-1}n\left(\frac{n}{p}\right)_L=0.$

(ii) $\displaystyle\sum_{\substack{n=1\\(n/p)_L=1}}^{p-1}n=\frac{p(p-1)}{4}.$

(iii) $\displaystyle\sum_{n=1}^{q-1}n^2\left(\frac{n}{q}\right)_L=q\sum_{n=1}^{q-1}n\left(\frac{n}{q}\right)_L.$

(iv) $\displaystyle\sum_{n=1}^{p-1}n^3\left(\frac{n}{p}\right)_L=\frac{3p}{2}\sum_{n=1}^{p-1}n^2\left(\frac{n}{p}\right)_L.$

(v) $\displaystyle\sum_{n=1}^{q-1}n^4\left(\frac{n}{q}\right)_L=2q\sum_{n=1}^{q-1}n^3\left(\frac{n}{q}\right)_L-q^2\sum_{n=1}^{q-1}n^2\left(\frac{n}{q}\right)_L.$