CHAPTER 9

THE QUADRATIC RECIPROCITY LAW

The moving power of mathematical invention is not reasoning but imagination.
A. DEMORGAN

9.1 EULER'S CRITERION

As the heading suggests, the present chapter has as its goal another major contribution of Gauss: the Quadratic Reciprocity Law. For those who consider the theory of numbers "the Queen of Mathematics," this is one of the jewels in her crown. The intrinsic beauty of the Quadratic Reciprocity Law has long exerted a strange fascination for mathematicians. Since Gauss' time, over a hundred proofs of it, all more or less different, have been published (in fact, Gauss himself eventually devised seven). Among the eminent mathematicians of the 19th century who contributed their proofs appear the names of Cauchy, Jacobi, Dirichlet, Eisenstein, Kronecker, and Dedekind.

Roughly speaking, the Quadratic Reciprocity Law deals with the solvability of quadratic congruences. Therefore, it seems appropriate to begin by considering the congruence

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{1}$$

where p is an odd prime and $a \not\equiv 0 \pmod{p}$; that is, $\gcd(a, p) = 1$. The supposition that p is an odd prime implies that $\gcd(4a, p) = 1$. Thus, the quadratic congruence in Eq. (1) is equivalent to

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

By using the identity

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$$

the last-written quadratic congruence may be expressed as

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$$

Now put $y = 2ax + b$ and $d = b^2 - 4ac$ to get

$$y^2 \equiv d \pmod{p} \tag{2}$$

If $x \equiv x_0 \pmod{p}$ is a solution of the quadratic congruence in Eq. (1), then the integer $y \equiv 2ax_0 + b \pmod{p}$ satisfies the quadratic congruence in Eq. (2). Conversely, if $y \equiv y_0 \pmod{p}$ is a solution of the quadratic congruence in Eq. (2), then $2ax \equiv y_0 - b \pmod{p}$ can be solved to obtain a solution to Eq. (1).

Thus, the problem of finding a solution to the quadratic congruence in Eq. (1) is equivalent to that of finding a solution to a linear congruence and a quadratic congruence of the form

$$x^2 \equiv a \pmod{p} \tag{3}$$

If $p \mid a$, then the quadratic congruence in Eq. (3) has $x \equiv 0 \pmod{p}$ as its only solution. To avoid trivialities, let us agree to assume hereafter that $p \nmid a$.

Granting this, whenever $x^2 \equiv a \pmod{p}$ admits a solution $x = x_0$, there is also a second solution $x = p - x_0$. This second solution is not congruent to the first. For $x_0 \equiv p - x_0 \pmod{p}$ implies that $2x_0 \equiv 0 \pmod{p}$, or $x_0 \equiv 0 \pmod{p}$, which is impossible. By Lagrange's theorem, these two solutions exhaust the incongruent solutions of $x^2 \equiv a \pmod{p}$. In short: $x^2 \equiv a \pmod{p}$ has exactly two solutions or no solutions.

A simple numerical example of what we have just said is provided by the quadratic congruence

$$5x^2 - 6x + 2 \equiv 0 \pmod{13}$$

To obtain the solution, we replace this congruence by the simpler one

$$y^2 \equiv 9 \pmod{13}$$

with solutions $y \equiv 3, 10 \pmod{13}$. Next, solve the linear congruences

$$10x \equiv 9 \pmod{13} \qquad 10x \equiv 16 \pmod{13}$$

It is not difficult to see that $x \equiv 10, 12 \pmod{13}$ satisfy these equations and, by our previous remarks, also the original quadratic congruence.

The major effort in this presentation is directed toward providing a test for the existence of solutions of the quadratic congruence

$$x^2 \equiv a \pmod{p} \qquad \gcd(a, p) = 1 \tag{4}$$

To put it differently, we wish to identify those integers a that are perfect squares modulo p.

Some additional terminology will help us to discuss this situation concisely.

Definition 9.1. Let p be an odd prime and $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution, then a is said to be a *quadratic residue of* p. Otherwise, a is called a *quadratic nonresidue of* p.

The point to bear in mind is that if $a \equiv b \pmod{p}$, then a is a quadratic residue of p if and only if b is a quadratic residue of p. Thus, we only need to determine the quadratic character of those positive integers less than p to ascertain that of any integer.

Example 9.1. Consider the case of the prime $p = 13$. To find out how many of the integers $1, 2, 3, \ldots, 12$ are quadratic residues of 13, we must know which of the congruences

$$x^2 \equiv a \pmod{13}$$

are solvable when a runs through the set $\{1, 2, \ldots, 12\}$. Modulo 13, the squares of the integers $1, 2, 3, \ldots, 12$ are

$$\begin{aligned}
1^2 &\equiv 12^2 \equiv 1\\
2^2 &\equiv 11^2 \equiv 4\\
3^2 &\equiv 10^2 \equiv 9\\
4^2 &\equiv 9^2 \quad \equiv 3\\
5^2 &\equiv 8^2 \quad \equiv 12\\
6^2 &\equiv 7^2 \quad \equiv 10
\end{aligned}$$

Consequently, the quadratic residues of 13 are 1, 3, 4, 9, 10, 12, and the nonresidues are 2, 5, 6, 7, 8, 11. Observe that the integers between 1 and 12 are divided equally among the quadratic residues and nonresidues; this is typical of the general situation.

For $p = 13$ there are two pairs of consecutive quadratic residues, the pairs 3, 4 and 9, 10. It can be shown that for any odd prime p there are $\frac{1}{4}(p - 4 - (-1)^{(p-1)/2})$ consecutive pairs.

Euler devised a simple criterion for deciding whether an integer a is a quadratic residue of a given prime p.

Theorem 9.1 Euler's criterion. Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Proof. Suppose that a is a quadratic residue of p, so that $x^2 \equiv a \pmod{p}$ admits a solution, call it x_1. Because $\gcd(a, p) = 1$, evidently $\gcd(x_1, p) = 1$. We may therefore appeal to Fermat's theorem to obtain

$$a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1 \pmod{p}$$

For the opposite direction, assume that the congruence $a^{(p-1)/2} \equiv 1 \pmod{p}$ holds, and let r be a primitive root of p. Then $a \equiv r^k \pmod{p}$ for some integer k, with $1 \leq k \leq p - 1$. It follows that

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$$

By Theorem 8.1, the order of r (namely, $p - 1$) must divide the exponent $k(p-1)/2$. The implication is that k is an even integer, say $k = 2j$. Hence,

$$(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p}$$

making the integer r^j a solution of the congruence $x^2 \equiv a \pmod{p}$. This proves that a is a quadratic residue of the prime p.

Now if p (as always) is an odd prime and $\gcd(a, p) = 1$, then

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}$$

the last congruence being justified by Fermat's theorem. Hence, either

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}$$

but not both. For, if both congruences held simultaneously, then we would have $1 \equiv -1 \pmod{p}$, or equivalently, $p \mid 2$, which conflicts with our hypothesis. Because a quadratic nonresidue of p does not satisfy $a^{(p-1)/2} \equiv 1 \pmod{p}$, it must therefore satisfy $a^{(p-1)/2} \equiv -1 \pmod{p}$. This observation provides an alternate formulation of Euler's criterion: the integer a is a quadratic nonresidue of the prime p if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Putting the various pieces together, we come up with the following corollary.

Corollary. Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue or nonresidue of p according to whether

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}$$

Example 9.2. In the case where $p = 13$, we find that

$$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$$

Thus, by virtue of the last corollary, the integer 2 is a quadratic nonresidue of 13. Because

$$3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1^2 \equiv 1 \pmod{13}$$

the same result indicates that 3 is a quadratic residue of 13 and so the congruence $x^2 \equiv 3 \pmod{13}$ is solvable; in fact, its two incongruent solutions are $x \equiv 4$ and $9 \pmod{13}$.

There is an alternative proof of Euler's criterion (due to Dirichlet) that is longer, but perhaps more illuminating. The reasoning proceeds as follows. Let a be a quadratic nonresidue of p and let c be any one of the integers $1, 2, \ldots, p-1$. By the theory of linear congruences, there exists a solution c' of $cx \equiv a \pmod{p}$, with c' also in the set $\{1, 2, \ldots, p-1\}$. Note that $c' \not\equiv c$; otherwise we would have $c^2 \equiv a \pmod{p}$, which contradicts what we assumed. Thus, the integers between 1 and $p - 1$ can be divided into $(p-1)/2$ pairs, c, c', where $cc' \equiv a \pmod{p}$. This leads to $(p-1)/2$ congruences,

$$\begin{aligned} c_1c_1' &\equiv a \pmod{p} \\ c_2c_2' &\equiv a \pmod{p} \\ &\vdots \\ c_{(p-1)/2}c_{(p-1)/2}' &\equiv a \pmod{p} \end{aligned}$$

Multiplying them together and observing that the product

$$c_1c_1'c_2c_2'\cdots c_{(p-1)/2}c_{(p-1)/2}'$$

is simply a rearrangement of $1\cdot 2\cdot 3\cdots(p-1)$, we obtain

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}$$

At this point, Wilson's theorem enters the picture; for, $(p-1)! \equiv -1 \pmod{p}$, so that

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

which is Euler's criterion when a is a quadratic nonresidue of p.

We next examine the case in which a is a quadratic residue of p. In this setting the congruence $x^2 \equiv a \pmod{p}$ admits two solutions $x = x_1$ and $x = p - x_1$, for some x_1 satisfying $1 \leq x_1 \leq p-1$. If x_1 and $p - x_1$ are removed from the set $\{1, 2, \ldots, p-1\}$, then the remaining $p-3$ integers can be grouped into pairs c, c' (where $c \neq c'$) such that $cc' \equiv a \pmod{p}$. To these $(p-3)/2$ congruences, add the congruence

$$x_1(p-x_1) \equiv -x_1^2 \equiv -a \pmod{p}$$

Upon taking the product of all the congruences involved, we arrive at the relation

$$(p-1)! \equiv -a^{(p-1)/2} \pmod{p}$$

Wilson's theorem plays its role once again to produce

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

Summing up, we have shown that $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$ according to whether a is a quadratic residue or nonresidue of p.

Euler's criterion is not offered as a practical test for determining whether a given integer is or is not a quadratic residue; the calculations involved are too cumbersome unless the modulus is small. But as a crisp criterion, easily worked with for theoretic purposes, it leaves little to be desired. A more effective method of computation is embodied in the Quadratic Reciprocity Law, which we shall prove later in the chapter.

PROBLEMS 9.1

1. Solve the following quadratic congruences:
   (a) $x^2 + 7x + 10 \equiv 0 \pmod{11}$.
   (b) $3x^2 + 9x + 7 \equiv 0 \pmod{13}$.
   (c) $5x^2 + 6x + 1 \equiv 0 \pmod{23}$.

2. Prove that the quadratic congruence $6x^2 + 5x + 1 \equiv 0 \pmod{p}$ has a solution for every prime p, even though the equation $6x^2 + 5x + 1 = 0$ has no solution in the integers.

3. (a) For an odd prime p, prove that the quadratic residues of p are congruent modulo p to the integers

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

(b) Verify that the quadratic residues of 17 are 1, 2, 4, 8, 9, 13, 15, 16.

4. Show that 3 is a quadratic residue of 23, but a nonresidue of 31.

5. Given that a is a quadratic residue of the odd prime p, prove the following:

(a) a is not a primitive root of p.

(b) The integer $p - a$ is a quadratic residue or nonresidue of p according as $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

(c) If $p \equiv 3 \pmod{4}$, then $x \equiv \pm a^{(p+1)/4} \pmod{p}$ are the solutions of the congruence $x^2 \equiv a \pmod{p}$.

6. Let p be an odd prime and $\gcd(a\,, p) = 1$. Establish that the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is solvable if and only if $b^2 - 4ac$ is either zero or a quadratic residue of p.

7. If $p = 2^k + 1$ is prime, verify that every quadratic nonresidue of p is a primitive root of p.
[*Hint:* Apply Euler's criterion.]

8. Assume that the integer r is a primitive root of the prime p, where $p \equiv 1 \pmod{8}$.

(a) Show that the solutions of the quadratic congruence $x^2 \equiv 2 \pmod{p}$ are given by

$$x \equiv \pm(r^{7(p-1)/8} + r^{(p-1)/8}) \pmod{p}$$

[*Hint:* First confirm that $r^{3(p-1)/2} \equiv -1 \pmod{p}$.]

(b) Use part (a) to find all solutions to the two congruences $x^2 \equiv 2 \pmod{17}$ and $x^2 \equiv 2 \pmod{41}$.

9. (a) If $ab \equiv r \pmod{p}$, where r is a quadratic residue of the odd prime p, prove that a and b are both quadratic residues of p or both nonresidues of p.

(b) If a and b are both quadratic residues of the odd prime p or both nonresidues of p, show that the congruence $ax^2 \equiv b \pmod{p}$ has a solution.
[*Hint:* Multiply the given congruence by a' where $aa' \equiv 1 \pmod{p}$.]

10. Let p be an odd prime and $\gcd(a\,, p) = \gcd(b\,, p) = 1$. Prove that either all three of the quadratic congruences

$$x^2 \equiv a \pmod{p} \qquad x^2 \equiv b \pmod{p} \qquad x^2 \equiv ab \pmod{p}$$

are solvable or exactly one of them admits a solution.

11. (a) Knowing that 2 is a primitive root of 19, find all the quadratic residues of 19.
[*Hint:* See the proof of Theorem 9.1.]

(b) Find the quadratic residues of 29 and 31.

12. If $n > 2$ and $\gcd(a\,, n) = 1$, then a is called a quadratic residue of n whenever there exists an integer x such that $x^2 \equiv a \pmod{n}$. Prove that if a is a quadratic residue of $n > 2$, then $a^{\phi(n)/2} \equiv 1 \pmod{n}$.

13. Show that the result of the previous problem does not provide a sufficient condition for the existence of a quadratic residue of n; in other words, find relatively prime integers a and n, with $a^{\phi(n)/2} \equiv 1 \pmod{n}$, for which the congruence $x^2 \equiv a \pmod{n}$ is not solvable.

9.2 THE LEGENDRE SYMBOL AND ITS PROPERTIES

Euler's studies on quadratic residues were further developed by the French mathematician Adrien Marie Legendre (1752–1833). Legendre's memoir "Recherches d'Analyse Indéterminée" (1785) contains an account of the Quadratic Reciprocity Law and its many applications, a sketch of a theory of the representation of an integer as the sum of three squares, and the statement of a theorem that was later to become famous: Every arithmetic progression $ax + b$, where $\gcd(a, b) = 1$, contains an infinite number of primes. The topics covered in "Recherches" were taken up in a more thorough and systematic fashion in his *Essai sur la Théorie des Nombres*, which appeared in 1798. This represented the first "modern" treatise devoted exclusively to number theory, its precursors being translations or commentaries on Diophantus. Legendre's *Essai* was subsequently expanded into his *Théorie des Nombres*. The results of his later research papers, inspired to a large extent by Gauss, were included in 1830 in a two-volume third edition of the *Théorie des Nombres*. This remained, together with the *Disquisitiones Arithmeticae* of Gauss, a standard work on the subject for many years. Although Legendre made no great innovations in number theory, he raised fruitful questions that provided subjects of investigation for the mathematicians of the 19th century.

Before leaving Legendre's mathematical contributions, we should mention that he is also known for his work on elliptic integrals and for his *Éléments de Géométrie* (1794). In this last book, he attempted a pedagogical improvement of Euclid's *Elements* by rearranging and simplifying many of the proofs without lessening the rigor of the ancient treatment. The result was so favorably received that it became one of the most successful textbooks ever written, dominating instruction in geometry for over a century through its numerous editions and translations. An English translation was made in 1824 by the famous Scottish essayist and historian Thomas Carlyle, who was in early life a teacher of mathematics; Carlyle's translation ran through 33 American editions, the last not appearing until 1890. In fact, Legendre's revision was used at Yale University as late as 1885, when Euclid's *Elements* was finally abandoned as a text.

Our future efforts will be greatly simplified by the use of the symbol (a/p); this notation was introduced by Legendre in his *Essai* and is called, naturally enough, the Legendre symbol.

Definition 9.2. Let p be an odd prime and let $\gcd(a, p) = 1$. The *Legendre symbol* (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \end{cases}$$

For the want of better terminology, we shall refer to a as the *numerator* and p as the *denominator* of the symbol (a/p). Another standard notation for the Legendre symbol is $(\frac{a}{p})$, or $(a \mid p)$.

Example 9.3. Let us look at the prime $p = 13$, in particular. Using the Legendre symbol, the results of an earlier example may be expressed as

$$(1/13) = (3/13) = (4/13) = (9/13) = (10/13) = (12/13) = 1$$

and

$$(2/13) = (5/13) = (6/13) = (7/13) = (8/13) = (11/13) = -1$$

Remark. For $p \mid a$, we have purposely left the symbol (a/p) undefined. Some authors find it convenient to extend Legendre's definition to this case by setting $(a/p) = 0$. One advantage of this is that the number of solutions of $x^2 \equiv a \pmod{p}$ can then be given by the simple formula $1 + (a/p)$.

The next theorem establishes certain elementary facts concerning the Legendre symbol.

Theorem 9.2. Let p be an odd prime and let a and b be integers that are relatively prime to p. Then the Legendre symbol has the following properties:

(a) If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.
(b) $(a^2/p) = 1$.
(c) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.
(d) $(ab/p) = (a/p)(b/p)$.
(e) $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$.

Proof. If $a \equiv b \pmod{p}$, then the two congruences $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ have exactly the same solutions, if any at all. Thus, $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ are both solvable, or neither one has a solution. This is reflected in the statement $(a/p) = (b/p)$.

Regarding property (b), observe that the integer a trivially satisfies the congruence $x^2 \equiv a^2 \pmod{p}$; hence, $(a^2/p) = 1$. Property (c) is just the corollary to Theorem 9.1 rephrased in terms of the Legendre symbol. We use (c) to establish property (d):

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (a/p)(b/p) (\text{mod } p)$$

Now the Legendre symbol assumes only the values 1 or -1. If $(ab/p) \neq (a/p)(b/p)$, we would have $1 \equiv -1 \pmod{p}$ or $2 \equiv 0 \pmod{p}$; this cannot occur, because $p > 2$. It follows that

$$(ab/p) = (a/p)(b/p)$$

Finally, we observe that the first equality in property (e) is a special case of property (b), whereas the second one is obtained from property (c) upon setting $a = -1$. Because the quantities $(-1/p)$ and $(-1)^{(p-1)/2}$ are either 1 or -1, the resulting congruence

$$(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}$$

implies that $(-1/p) = (-1)^{(p-1)/2}$.

From parts (b) and (d) of Theorem 9.2, we may also abstract the relation

(f) $(ab^2/p) = (a/p)(b^2/p) = (a/p)$

In other words, a square factor that is relatively prime to p can be deleted from the numerator of the Legendre symbol without affecting its value.

Because $(p - 1)/2$ is even for a prime p of the form $4k + 1$ and odd for p of the form $4k + 3$, the equation $(-1/p) = (-1)^{(p-1)/2}$ permits us to add a small supplemental corollary to Theorem 9.2.

Corollary. If p is an odd prime, then

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

This corollary may be viewed as asserting that the quadratic congruence $x^2 \equiv -1 \pmod p$ has a solution for an odd prime p if and only if p is of the form $4k + 1$. The result is not new, of course; we have merely provided the reader with a different path to Theorem 5.5.

Example 9.4. Let us ascertain whether the congruence $x^2 \equiv -46 \pmod{17}$ is solvable. This can be done by evaluating the Legendre symbol $(-46/17)$. We first appeal to properties (d) and (e) of Theorem 9.2 to write

$$(-46/17) = (-1/17)(46/17) = (46/17)$$

Because $46 \equiv 12 \pmod{17}$, it follows that

$$(46/17) = (12/17)$$

Now property (f) gives

$$(12/17) = (3 \cdot 2^2/17) = (3/17)$$

But

$$(3/17) \equiv 3^{(17-1)/2} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1 \pmod{17}$$

where we have made appropriate use of property (c) of Theorem 9.2; hence, $(3/17) = -1$. Inasmuch as $(-46/17) = -1$, the quadratic congruence $x^2 \equiv -46 \pmod{17}$ admits no solution.

The corollary to Theorem 9.2 lends itself to an application concerning the distribution of primes.

Theorem 9.3. There are infinitely many primes of the form $4k + 1$.

Proof. Suppose that there are finitely many such primes; let us call them $p_1, p_2, \ldots, p_n$ and consider the integer

$$N = (2p_1p_2 \cdots p_n)^2 + 1$$

Clearly N is odd, so that there exists some odd prime p with $p \mid N$. To put it another way,

$$(2p_1p_2 \cdots p_n)^2 \equiv -1 \pmod p$$

or, if we prefer to phrase this in terms of the Legendre symbol, $(-1/p) = 1$. But the relation $(-1/p) = 1$ holds only if p is of the form $4k + 1$. Hence, p is one of the primes p_i, implying that p_i divides $N - (2p_1p_2 \cdots p_n)^2$, or $p_i \mid 1$, which is a contradiction. The conclusion: There must exist infinitely many primes of the form $4k + 1$.

We dig deeper into the properties of quadratic residues with Theorem 9.4.

Theorem 9.4. If p is an odd prime, then

$$\sum_{a=1}^{p-1} (a/p) = 0$$

Hence, there are precisely $(p - 1)/2$ quadratic residues and $(p - 1)/2$ quadratic nonresidues of p.

Proof. Let r be a primitive root of p. We know that, modulo p, the powers r, $r^2, \ldots, r^{p-1}$ are just a permutation of the integers $1, 2, \ldots, p - 1$. Thus, for any a lying between 1 and $p - 1$, inclusive, there exists a unique positive integer k $(1 \leq k \leq p - 1)$, such that $a \equiv r^k \pmod{p}$. By appropriate use of Euler's criterion, we have

$$(a/p) = (r^k/p) \equiv (r^k)^{(p-1)/2} = (r^{(p-1)/2})^k \equiv (-1)^k \pmod{p} \qquad (1)$$

where, because r is a primitive root of p, $r^{(p-1)/2} \equiv -1 \pmod{p}$. But (a/p) and $(-1)^k$ are equal to either 1 or -1, so that equality holds in Eq. (1). Now add up the Legendre symbols in question to obtain

$$\sum_{a=1}^{p-1} (a/p) = \sum_{k=1}^{p-1} (-1)^k = 0$$

which is the desired conclusion.

The proof of Theorem 9.4 serves to bring out the following point, which we record as a corollary.

Corollary. The quadratic residues of an odd prime p are congruent modulo p to the even powers of a primitive root r of p; the quadratic nonresidues are congruent to the odd powers of r.

For an illustration of the idea just introduced, we again fall back on the prime $p = 13$. Because 2 is a primitive root of 13, the quadratic residues of 13 are given by the even powers of 2, namely,

$$\begin{array}{ll} 2^2 \equiv 4 & 2^8 \equiv 9 \\ 2^4 \equiv 3 & 2^{10} \equiv 10 \\ 2^6 \equiv 12 & 2^{12} \equiv 1 \end{array}$$

all congruences being modulo 13. Similarly, the nonresidues occur as the odd powers of 2:

$$\begin{array}{ll} 2^1 \equiv 2 & 2^7 \equiv 11 \\ 2^3 \equiv 8 & 2^9 \equiv 5 \\ 2^5 \equiv 6 & 2^{11} \equiv 7 \end{array}$$

Most proofs of the Quadratic Reciprocity Law, and ours as well, rest ultimately upon what is known as Gauss' lemma. Although this lemma gives the quadratic character of an integer, it is more useful from a theoretic point of view than as a computational device. We state and prove it below.

Theorem 9.5 Gauss' lemma. Let p be an odd prime and let $\gcd(a, p) = 1$. If n denotes the number of integers in the set

$$S = \left\{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a\right\}$$

whose remainders upon division by p exceed $p/2$, then

$$(a/p) = (-1)^n$$

Proof. Because $\gcd(a, p) = 1$, none of the $(p-1)/2$ integers in S is congruent to zero and no two are congruent to each other modulo p. Let $r_1, \ldots, r_m$ be those remainders upon division by p such that $0 < r_i < p/2$, and let $s_1, \ldots, s_n$ be those remainders such that $p > s_i > p/2$. Then $m + n = (p-1)/2$, and the integers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are all positive and less than $p/2$.

To prove that these integers are all distinct, it suffices to show that no $p - s_i$ is equal to any r_j. Assume to the contrary that

$$p - s_i = r_j$$

for some choice of i and j. Then there exist integers u and v, with $1 \leq u, v \leq (p-1)/2$, satisfying $s_i \equiv ua \pmod{p}$ and $r_j \equiv va \pmod{p}$. Hence,

$$(u + v)a \equiv s_i + r_j = p \equiv 0 \pmod{p}$$

which says that $u + v \equiv 0 \pmod{p}$. But the latter congruence cannot take place, because $1 < u + v \leq p - 1$.

The point we wish to bring out is that the $(p-1)/2$ numbers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are simply the integers $1, 2, \ldots, (p-1)/2$, not necessarily in order of appearance. Thus, their product is $[(p-1)/2]!$:

$$\begin{aligned} \left(\frac{p-1}{2}\right)! &= r_1 \cdots r_m(p - s_1) \cdots (p - s_n) \\ &\equiv r_1 \cdots r_m(-s_1) \cdots (-s_n) \pmod{p} \\ &\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p} \end{aligned}$$

But we know that $r_1, \ldots, r_m, s_1, \ldots, s_n$ are congruent modulo p to $a, 2a, \ldots, [(p-1)/2]a$, in some order, so that

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a \pmod{p}$$
$$\equiv (-1)^n a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p}$$

Because $[(p-1)/2]!$ is relatively prime to p, it may be canceled from both sides of this congruence to give

$$1 \equiv (-1)^n a^{(p-1)/2} \pmod{p}$$

or, upon multiplying by $(-1)^n$,

$$a^{(p-1)/2} \equiv (-1)^n \pmod{p}$$

Use of Euler's criterion now completes the argument:

$$(a/p) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod{p}$$

which implies that

$$(a/p) = (-1)^n$$

By way of illustration, let $p = 13$ and $a = 5$. Then $(p-1)/2 = 6$, so that

$$S = \{5, 10, 15, 20, 25, 30\}$$

Modulo 13, the members of S are the same as the integers

$$5, 10, 2, 7, 12, 4$$

Three of these are greater than 13/2; hence, $n = 3$, and Theorem 9.5 says that

$$(5/13) = (-1)^3 = -1$$

Gauss' lemma allows us to proceed to a variety of interesting results. For one thing, it provides a means for determining which primes have 2 as a quadratic residue.

Theorem 9.6. If p is an odd prime, then

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8} \\ -1 & \text{if } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8} \end{cases}$$

Proof. According to Gauss' lemma, $(2/p) = (-1)^n$, where n is the number of integers in the set

$$S = \left\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \ldots, \left(\frac{p-1}{2}\right) \cdot 2\right\}$$

which, upon division by p, have remainders greater than $p/2$. The members of S are all less than p, so that it suffices to count the number that exceed $p/2$. For $1 \leq k \leq (p-1)/2$, we have $2k < p/2$ if and only if $k < p/4$. If [ ] denotes the greatest integer function, then there are $[p/4]$ integers in S less than $p/2$; hence,

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$$

is the number of integers that are greater than $p/2$.

Now we have four possibilities; for, any odd prime has one of the forms $8k+1$, $8k+3$, $8k+5$, or $8k+7$. A simple calculation shows that

$$\text{if } p = 8k+1, \text{ then } n = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k$$

$$\text{if } p = 8k+3, \text{ then } n = 4k+1 - \left[2k + \frac{3}{4}\right] = 4k+1-2k = 2k+1$$

$$\begin{aligned}\text{if } p = 8k+5, \text{ then } n &= 4k+2 - \left[2k+1+\frac{1}{4}\right] \\ &= 4k+2-(2k+1) = 2k+1\end{aligned}$$

$$\begin{aligned}\text{if } p = 8k+7, \text{ then } n &= 4k+3 - \left[2k+1+\frac{3}{4}\right] \\ &= 4k+3-(2k+1) = 2k+2\end{aligned}$$

Thus, when p is of the form $8k+1$ or $8k+7$, n is even and $(2/p) = 1$; on the other hand, when p assumes the form $8k+3$ or $8k+5$, n is odd and $(2/p) = -1$.

Notice that if the prime p is of the form $8k \pm 1$ (equivalently, $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$), then

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$$

which is an even integer; in this situation, $(-1)^{(p^2-1)/8} = 1 = (2/p)$. On the other hand, if p is of the form $8k \pm 3$ (equivalently, $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$), then

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1$$

which is odd; here, we have $(-1)^{(p^2-1)/8} = -1 = (2/p)$. These observations are incorporated in the statement of the following corollary to Theorem 9.6.

Corollary. If p is an odd prime, then

$$(2/p) = (-1)^{(p^2-1)/8}$$

It is time for another look at primitive roots. As we have remarked, there is no general technique for obtaining a primitive root of an odd prime p; the reader might, however, find the next theorem useful on occasion.

Theorem 9.7. If p and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2}2$ is a primitive root of $2p+1$.

Proof. For ease of discussion, let us put $q = 2p+1$. We distinguish two cases: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

If $p \equiv 1 \pmod 4$, then $(-1)^{(p-1)/2}2 = 2$. Because $\phi(q) = q - 1 = 2p$, the order of 2 modulo q is one of the numbers 1, 2, p, or $2p$. Taking note of property (c) of Theorem 9.2, we have

$$(2/q) \equiv 2^{(q-1)/2} = 2^p \pmod q$$

But, in the present setting, $q \equiv 3 \pmod 8$; whence, the Legendre symbol $(2/q) = -1$. It follows that $2^p \equiv -1 \pmod q$, and therefore 2 cannot have order p modulo q. The order of 2 being neither 1, 2, ($2^2 \equiv 1 \pmod q$ implies that $q \mid 3$, which is an impossibility) nor p, we are forced to conclude that the order of 2 modulo q is $2p$. This makes 2 a primitive root of q.

We now deal with the case $p \equiv 3 \pmod 4$. This time, $(-1)^{(p-1)/2}2 = -2$ and

$$(-2)^p \equiv (-2/q) = (-1/q)(2/q) \pmod q$$

Because $q \equiv 7 \pmod 8$, the corollary to Theorem 9.2 asserts that $(-1/q) = -1$, whereas once again we have $(2/q) = 1$. This leads to the congruence $(-2)^p \equiv -1 \pmod q$. From here on, the argument duplicates that of the last paragraph. Without analyzing further, we announce the decision: -2 is a primitive root of the prime q.

Theorem 9.7 indicates, for example, that the primes 11, 59, 107, and 179 have 2 as a primitive root. Likewise, the integer -2 serves as a primitive root for 7, 23, 47, and 167.

Before retiring from the field, we should mention another result of the same character: if both p and $4p + 1$ are primes, then 2 is a primitive root of $4p + 1$. Thus, to the list of prime numbers having 2 for a primitive root, we could add, say, 13, 29, 53, and 173.

An odd prime p such that $2p + 1$ is also a prime is called a Germain prime, after the French number theorist Sophie Germain (1776–1831). An unresolved problem is to determine whether there exist infinitely many Germain primes. The largest such known today is $p = 2540041185 \cdot 2^{114729} - 1$, which has 34547 digits.

There is an attractive proof of the infinitude of primes of the form $8k - 1$ that can be based on Theorem 9.6.

Theorem 9.8. There are infinitely many primes of the form $8k - 1$.

Proof. As usual, suppose that there are only a finite number of such primes. Let these be $p_1, p_2, \ldots, p_n$ and consider the integer

$$N = (4p_1p_2 \cdots p_n)^2 - 2$$

There exists at least one odd prime divisor p of N, so that

$$(4p_1p_2 \cdots p_n)^2 \equiv 2 \pmod p$$

or $(2/p) = 1$. In view of Theorem 9.6, $p \equiv \pm 1 \pmod 8$. If all the odd prime divisors of N were of the form $8k + 1$, then N would be of the form $8a + 1$; this is clearly impossible, because N is of the form $16a - 2$. Thus, N must have a prime divisor q of the form $8k - 1$. But $q \mid N$, and $q \mid (4p_1p_2 \cdots p_n)^2$ leads to the contradiction that $q \mid 2$.

The next result, which allows us to effect the passage from Gauss' lemma to the Quadratic Reciprocity Law (Theorem 9.9), has some independent interest.

Lemma. If p is an odd prime and a an odd integer, with $\gcd(a, p) = 1$, then

$$(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2}[ka/p]}$$

Proof. We shall employ the same notation as in the proof of Gauss' lemma. Consider the set of integers

$$S = \left\{a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\right\}$$

Divide each of these multiples of a by p to obtain

$$ka = q_k p + t_k \qquad 1 \leq t_k \leq p - 1$$

Then $ka/p = q_k + t_k/p$, so that $[ka/p] = q_k$. Thus, for $1 \leq k \leq (p-1)/2$, we may write ka in the form

$$ka = \left[\frac{ka}{p}\right]p + t_k \tag{1}$$

If the remainder $t_k < p/2$, then it is one of the integers $r_1, \ldots, r_m$; on the other hand, if $t_k > p/2$, then it is one of the integers $s_1, \ldots, s_n$.

Taking the sum of the $(p-1)/2$ equations in Eq. (1), we get the relation

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right]p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k \tag{2}$$

It was learned in proving Gauss' lemma that the $(p-1)/2$ numbers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are just a rearrangement of the integers $1, 2, \ldots, (p-1)/2$. Hence

$$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n}(p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \tag{3}$$

Subtracting Eq. (3) from Eq. (2) gives

$$(a-1)\sum_{k=1}^{(p-1)/2} k = p\left(\sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right] - n\right) + 2\sum_{k=1}^{n} s_k \tag{4}$$

Let us use the fact that $p \equiv a \equiv 1 \pmod 2$ and translate this last equation into a congruence modulo 2:

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left(\sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right] - n\right) \pmod 2$$

or

$$n \equiv \sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right] \pmod 2$$

The rest follows from Gauss' lemma; for,

$$(a/p) = (-1)^n = (-1)^{\sum_{k=1}^{(p-1)/2}[ka/p]}$$

as we wished to show.

For an example of this last result, again consider $p = 13$ and $a = 5$. Because $(p - 1)/2 = 6$, it is necessary to calculate $[ka/p]$ for $k = 1, \ldots, 6$:

$$\begin{aligned} [5/13] &= [10/13] = 0 \\ [15/13] &= [20/13] = [25/13] = 1 \\ [30/13] &= 2 \end{aligned}$$

By the lemma just proven, we have

$$(5/13) = (-1)^{1+1+1+2} = (-1)^5 = -1$$

confirming what was earlier seen.

PROBLEMS 9.2

1. Find the value of the following Legendre symbols:
   (a) $(19/23)$.
   (b) $(-23/59)$.
   (c) $(20/31)$.
   (d) $(18/43)$.
   (e) $(-72/131)$.
2. Use Gauss' lemma to compute each of the Legendre symbols below (that is, in each case obtain the integer n for which $(a/p) = (-1)^n$):
   (a) $(8/11)$.
   (b) $(7/13)$.
   (c) $(5/19)$.
   (d) $(11/23)$.
   (e) $(6/31)$.
3. For an odd prime p, prove that there are $(p - 1)/2 - \phi(p - 1)$ quadratic nonresidues of p that are not primitive roots of p.
4. (a) Let p be an odd prime. Show that the Diophantine equation

   $$x^2 + py + a = 0 \qquad \gcd(a\,, p) = 1$$

   has an integral solution if and only if $(-a/p) = 1$.
   (b) Determine whether $x^2 + 7y - 2 = 0$ has a solution in the integers.
5. Prove that 2 is not a primitive root of any prime of the form $p = 3 \cdot 2^n + 1$, except when $p = 13$.
   [*Hint:* Use Theorem 9.6.]
6. (a) If p is an odd prime and $\gcd(ab\,, p) = 1$, prove that at least one of a, b, or ab is a quadratic residue of p.
   (b) Given a prime p, show that, for some choice of $n > 0$, p divides

   $$(n^2 - 2)(n^2 - 3)(n^2 - 6)$$

7. If p is an odd prime, show that

   $$\sum_{a=1}^{p-2} (a(a + 1)/p) = -1$$

   [*Hint:* If a' is defined by $aa' \equiv 1 \pmod{p}$, then $(a(a + 1)/p) = ((1 + a')/p)$. Note that $1 + a'$ runs through a complete set of residues modulo p, except for the integer 1.]

8. Prove the statements below:
(a) If p and $q = 2p + 1$ are both odd primes, then -4 is a primitive root of q.
(b) If $p \equiv 1 \pmod 4$ is a prime, then -4 and $(p - 1)/4$ are both quadratic residues of p.

9. For a prime $p \equiv 7 \pmod 8$, show that $p \mid 2^{(p-1)/2} - 1$.
[*Hint:* Use Theorem 9.6.]

10. Use Problem 9 to confirm that the numbers $2^n - 1$ are composite for $n = 11, 23, 83, 131, 179, 183, 239, 251$.

11. Given that p and $q = 4p + 1$ are both primes, prove the following:
(a) Any quadratic nonresidue of q is either a primitive root of q or has order 4 modulo q.
[*Hint:* If a is a quadratic nonresidue of q, then $-1 = (a/q) \equiv a^{2p} \pmod q$; hence, a has order $1, 2, 4, p, 2p$, or $4p$ modulo q.]
(b) The integer 2 is a primitive root of q; in particular, 2 is a primitive root of the primes 13, 29, 53, and 173.

12. If r is a primitive root of the odd prime p, prove that the product of the quadratic residues of p is congruent modulo p to $r^{(p^2-1)/4}$ and the product of the nonresidues of p is congruent modulo p to $r^{(p-1)^2/4}$.
[*Hint:* Apply the corollary to Theorem 9.4.]

13. Establish that the product of the quadratic residues of the odd prime p is congruent modulo p to 1 or -1 according as $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 4$.
[*Hint:* Use Problem 12 and the fact that $r^{(p-1)/2} \equiv -1 \pmod p$. Or, Problem 3(a) of Section 9.1 and the proof of Theorem 5.5.]

14. (a) If the prime $p > 3$, show that p divides the sum of its quadratic residues.
(b) If the prime $p > 5$, show that p divides the sum of the squares of its quadratic nonresidues.

15. Prove that for any prime $p > 5$ there exist integers $1 \le a, b \le p - 1$ for which

$$(a/p) = (a + 1/p) = 1 \qquad \text{and} \qquad (b/p) = (b + 1/p) = -1$$

that is, there are consecutive quadratic residues of p and consecutive nonresidues.

16. (a) Let p be an odd prime and $\gcd(a, p) = \gcd(k, p) = 1$. Show that if the equation $x^2 - ay^2 = kp$ admits a solution, then $(a/p) = 1$; for example, $(2/7) = 1$, because $6^2 - 2 \cdot 2^2 = 4 \cdot 7$.
[*Hint:* If x_0, y_0 satisfy the given equation, then $(x_0 y_0^{p-2})^2 \equiv a \pmod p$.]
(b) By considering the equation $x^2 + 5y^2 = 7$, demonstrate that the converse of the result in part (a) need not hold.
(c) Show that, for any prime $p \equiv \pm 3 \pmod 8$, the equation $x^2 - 2y^2 = p$ has no solution.

17. Prove that the odd prime divisors p of the integers $9^n + 1$ are of the form $p \equiv 1 \pmod 4$.

18. For a prime $p \equiv 1 \pmod 4$, verify that the sum of the quadratic residues of p is equal to $p(p - 1)/4$.
[*Hint:* If $a_1, \dots, a_r$ are the quadratic residues of p less than $p/2$, then $p - a_1, \dots, p - a_r$ are those greater than $p/2$.]

9.3 QUADRATIC RECIPROCITY

Let p and q be distinct odd primes, so that both of the Legendre symbols (p/q) and (q/p) are defined. It is natural to enquire whether the value of (p/q) can be determined if that of (q/p) is known. To put the question more generally, is there any connection at all between the values of these two symbols? The basic relationship was conjectured experimentally by Euler in 1783 and imperfectly proved by Legendre two years thereafter. Using his symbol, Legendre stated this relationship in the elegant form that has since become known as the Quadratic Reciprocity Law:

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Legendre went amiss in assuming a result that is as difficult to prove as the law itself, namely, that for any odd prime $p \equiv 1 \pmod 8$, there exists another prime $q \equiv 3 \pmod 4$ for which p is a quadratic residue. Undaunted, he attempted another proof in his *Essai sur la Théorie des Nombres* (1798); this one also contained a gap, because Legendre took for granted that there are an infinite number of primes in certain arithmetical progressions (a fact eventually proved by Dirichlet in 1837, using in the process very subtle arguments from complex variable theory).

At the age of 18, Gauss (in 1795), apparently unaware of the work of either Euler or Legendre, rediscovered this reciprocity law and, after a year's unremitting labor, obtained the first complete proof. "It tortured me," says Gauss, "for the whole year and eluded my most strenuous efforts before, finally, I got the proof explained in the fourth section of the *Disquisitiones Arithmeticae*." In the *Disquisitiones Arithmeticae*—which was published in 1801, although finished in 1798—Gauss attributed the Quadratic Reciprocity Law to himself, taking the view that a theorem belongs to the one who gives the first rigorous demonstration. The indignant Legendre was led to complain: "This excessive impudence is unbelievable in a man who has sufficient personal merit not to have the need of appropriating the discoveries of others." All discussion of priority between the two was futile; because each clung to the correctness of his position, neither took heed of the other. Gauss went on to publish five different demonstrations of what he called "the gem of higher arithmetic," and another was found among his papers. The version presented below, a variant of one of Gauss' own arguments, is due to his student, Ferdinand Eisenstein (1823–1852). The proof is challenging (and it would perhaps be unreasonable to expect an easy proof), but the underlying idea is simple enough.

Theorem 9.9 Quadratic Reciprocity Law. If p and q are distinct odd primes, then

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

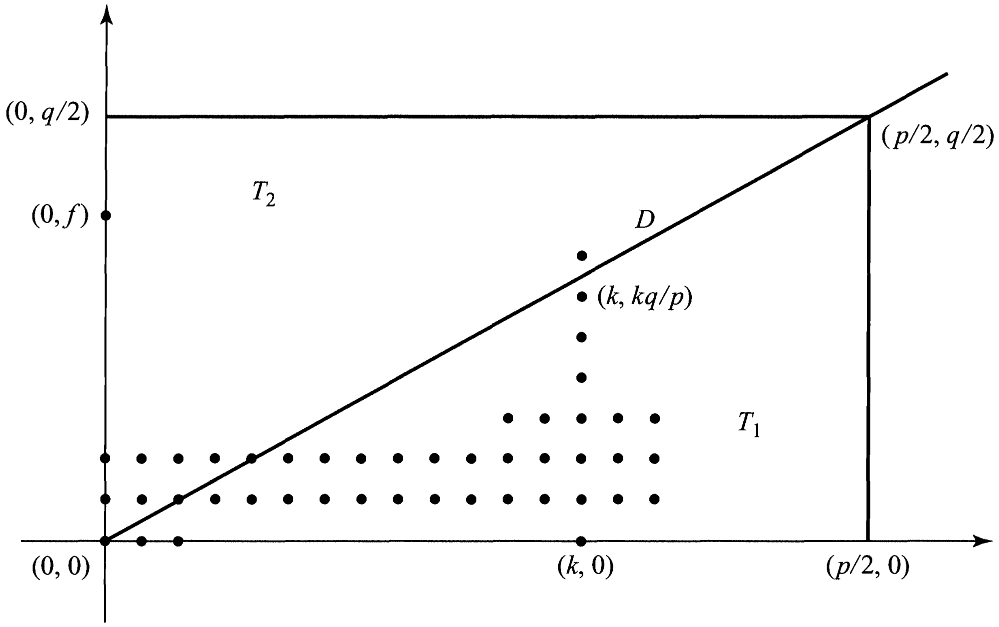
Proof. Consider the rectangle in the xy coordinate plane whose vertices are $(0, 0)$, $(p/2, 0)$, $(0, q/2)$, and $(p/2, q/2)$. Let R denote the region within this rectangle, not including any of the bounding lines. The general plan of attack is to count the number of lattice points (that is, the points whose coordinates are integers) inside R in two different ways. Because p and q are both odd, the lattice points in R consist of all points (n, m), where $1 \leq n \leq (p-1)/2$ and $1 \leq m \leq (q-1)/2$; clearly, the number of such points is

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

Now the diagonal D from $(0, 0)$ to $(p/2, q/2)$ has the equation $y = (q/p)x$, or equivalently, $py = qx$. Because $\gcd(p, q) = 1$, none of the lattice points inside R will lie on D. For p must divide the x coordinate of any lattice point on the line $py = qx$, and q must divide its y coordinate; there are no such points in R. Suppose that T_1 denotes the portion of R that is below the diagonal D, and T_2 the portion above. By what we have just seen, it suffices to count the lattice points inside each of these triangles.

The number of integers in the interval $0 < y < kq/p$ is equal to $[kq/p]$. Thus, for $1 \leq k \leq (p-1)/2$, there are precisely $[kq/p]$ lattice points in T_1 directly above the point $(k, 0)$ and below D; in other words, lying on the vertical line segment from $(k, 0)$ to $(k, kq/p)$. It follows that the total number of lattice points contained in T_1 is

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]$$



A similar calculation, with the roles of p and q interchanged, shows that the number of lattice points within T_2 is

$$\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right]$$

This accounts for all of the lattice points inside R, so that

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right]$$

The time has come for Gauss' lemma to do its duty:

$$\begin{aligned}(p/q)(q/p) &= (-1)^{\sum_{j=1}^{(q-1)/2}[jp/q]} \cdot (-1)^{\sum_{k=1}^{(p-1)/2}[kq/p]} \\ &= (-1)^{\sum_{j=1}^{(q-1)/2}[jp/q]+\sum_{k=1}^{(p-1)/2}[kq/p]} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\end{aligned}$$

The proof of the Quadratic Reciprocity Law is now complete.

An immediate consequence of this is Corollary 1.

Corollary 1. If p and q are distinct odd primes, then

$$(p/q)(q/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

Proof. The number $(p-1)/2 \cdot (q-1)/2$ is even if and only if at least one of the integers p and q is of the form $4k+1$; if both are of the form $4k+3$, then the product $(p-1)/2 \cdot (q-1)/2$ is odd.

Multiplying each side of the equation of the Quadratic Reciprocity Law by (q/p) and using the fact that $(q/p)^2 = 1$, we could also formulate this as Corollary 2.

Corollary 2. If p and q are distinct odd primes, then

$$(p/q) = \begin{cases} (q/p) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -(q/p) & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

Let us see what this last series of results accomplishes. Take p to be an odd prime and $a \neq \pm 1$ to be an integer not divisible by p. Suppose further that a has the factorization

$$a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where the p_i are distinct odd primes. Because the Legendre symbol is multiplicative,

$$(a/p) = (\pm 1/p)(2/p)^{k_0}(p_1/p)^{k_1} \cdots (p_r/p)^{k_r}$$

To evaluate (a/p), we have only to calculate each of the symbols $(-1/p)$, $(2/p)$, and (p_i/p). The values of $(-1/p)$ and $(2/p)$ were discussed earlier, so that the one stumbling block is (p_i/p), where p_i and p are distinct odd primes; this is where the Quadratic Reciprocity Law enters. For Corollary 2 allows us to replace (p_i/p) by a new Legendre symbol having a smaller denominator. Through continued inversion and division, the computation can be reduced to that of the known quantities

$$(-1/q) \qquad (1/q) \qquad (2/q)$$

This is all somewhat vague, of course, so let us look at a concrete example.

Example 9.5. Consider the Legendre symbol $(29/53)$, for instance. Because both $29 \equiv 1 \pmod{4}$ and $53 \equiv 1 \pmod{4}$, we see that

$$(29/53) = (53/29) = (24/29) = (2/29)(3/29)(4/29) = (2/29)(3/29)$$

With reference to Theorem 9.6, $(2/29) = -1$, while inverting again,

$$(3/29) = (29/3) = (2/3) = -1$$

where we used the congruence $29 \equiv 2 \pmod{3}$. The net effect is that

$$(29/53) = (2/29)(3/29) = (-1)(-1) = 1$$

The Quadratic Reciprocity Law provides a very satisfactory answer to the problem of finding odd primes $p \neq 3$ for which 3 is a quadratic residue. Because $3 \equiv 3 \pmod 4$, Corollary 2 of Theorem 9.9 implies that

$$(3/p) = \begin{cases} (p/3) & \text{if } p \equiv 1 \pmod 4 \\ -(p/3) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Now $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. By Theorems 9.2 and 9.6,

$$(p/3) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

the implication of which is that $(3/p) = 1$ if and only if

$$p \equiv 1 \pmod 4 \qquad \text{and} \qquad p \equiv 1 \pmod 3 \tag{1}$$

or

$$p \equiv 3 \pmod 4 \qquad \text{and} \qquad p \equiv 2 \pmod 3 \tag{2}$$

The restrictions in the congruencies in Eq. (1) are equivalent to requiring that $p \equiv 1 \pmod{12}$ whereas those congruencies in Eq. (2) are equivalent to $p \equiv 11 \equiv -1 \pmod{12}$. The upshot of all this is Theorem 9.10.

Theorem 9.10. If $p \neq 3$ is an odd prime, then

$$(3/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Example 9.6. For an example of the solution of a quadratic congruence with a composite modulus, consider

$$x^2 \equiv 196 \pmod{1357}$$

Because $1357 = 23 \cdot 59$, the given congruence is solvable if and only if both

$$x^2 \equiv 196 \pmod{23} \qquad \text{and} \qquad x^2 \equiv 196 \pmod{59}$$

are solvable. Our procedure is to find the values of the Legendre symbols $(196/23)$ and $(196/59)$.

The evaluation of $(196/23)$ requires the use of Theorem 9.10:

$$(196/23) = (12/23) = (3/23) = 1$$

Thus, the congruence $x^2 \equiv 196 \pmod{23}$ admits a solution. As regards the symbol $(196/59)$, the Quadratic Reciprocity Law enables us to write

$$(196/59) = (19/59) = -(59/19) = -(2/19) = -(-1) = 1$$

Therefore, it is possible to solve $x^2 \equiv 196 \pmod{59}$ and, in consequence, the congruence $x^2 \equiv 196 \pmod{1357}$ as well.

To arrive at a solution, notice that the congruence $x^2 \equiv 196 \equiv 12 \pmod{23}$ is satisfied by $x \equiv 9, 14 \pmod{23}$, and $x^2 \equiv 196 \equiv 19 \pmod{59}$ has solutions $x \equiv 14, 45$

(mod 59). We may now use the Chinese Remainder Theorem to obtain the simultaneous solutions of the four systems:

$$\begin{array}{lcl} x \equiv 14 \pmod{23} & \text{and} & x \equiv 14 \pmod{59} \\ x \equiv 14 \pmod{23} & \text{and} & x \equiv 45 \pmod{59} \\ x \equiv 9 \pmod{23} & \text{and} & x \equiv 14 \pmod{59} \\ x \equiv 9 \pmod{23} & \text{and} & x \equiv 45 \pmod{59} \end{array}$$

The resulting values $x \equiv 14, 635, 722, 1343 \pmod{1357}$ are the desired solutions of the original congruence $x^2 \equiv 196 \pmod{1357}$.

Example 9.7. Let us turn to a quite different application of these ideas. At an earlier stage, it was observed that if $F_n = 2^{2^n} + 1, n > 1$, is a prime, then 2 is not a primitive root of F_n. We now possess the means to show that the integer 3 serves as a primitive root of any prime of this type.

As a first step in this direction, note that any F_n is of the form $12k + 5$. A simple induction argument confirms that $4^m \equiv 4 \pmod{12}$ for $m = 1, 2, \ldots$; hence, we must have

$$F_n = 2^{2^n} + 1 = 2^{2m} + 1 = 4^m + 1 \equiv 5 \pmod{12}$$

If F_n happens to be prime, then Theorem 9.10 permits the conclusion

$$(3/F_n) = -1$$

or, using Euler's criterion,

$$3^{(Fn-1)/2} \equiv -1 \pmod{F_n}$$

Switching to the phi-function, the last congruence says that

$$3^{\phi(F_n)/2} \equiv -1 \pmod{F_n}$$

From this, it may be inferred that 3 has order $\phi(F_n)$ modulo F_n, and therefore 3 is a primitive root of F_n. For if the order of 3 were a proper divisor of

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

then it would also divide $\phi(F_n)/2$, leading to the contradiction

$$3^{\phi(F_n)/2} \equiv 1 \pmod{F_n}$$

PROBLEMS 9.3

1. Evaluate the following Legendre symbols:
   (a) $(71/73)$.
   (b) $(-219/383)$.
   (c) $(461/773)$.
   (d) $(1234/4567)$.
   (e) $(3658/12703)$.
   [*Hint:* $3658 = 2 \cdot 31 \cdot 59$.]
2. Prove that 3 is a quadratic nonresidue of all primes of the form $2^{2n} + 1$, and all primes of the form $2^p - 1$, where p is an odd prime.
   [*Hint:* For all n, $4^n \equiv 4 \pmod{12}$.]
3. Determine whether the following quadratic congruences are solvable:
   (a) $x^2 \equiv 219 \pmod{419}$.

(b) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$.
(c) $2x^2 + 5x - 9 \equiv 0 \pmod{101}$.

4. Verify that if p is an odd prime, then

$$(-2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \quad \text{or} \quad p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8 \quad \text{or} \quad p \equiv 7 \pmod 8 \end{cases}$$

5. (a) Prove that if $p > 3$ is an odd prime, then

$$(-3/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$$

(b) Using part (a), show that there are infinitely many primes of the form $6k + 1$.
[*Hint:* Assume that $p_1, p_2, \ldots, p_r$ are all the primes of the form $6k + 1$ and consider the integer $N = (2p_1p_2 \cdots p_r)^2 + 3$.]

6. Use Theorem 9.2 and Problems 4 and 5 to determine which primes can divide integers of the forms $n^2 + 1$, $n^2 + 2$, or $n^2 + 3$ for some value of n.

7. Prove that there exist infinitely many primes of the form $8k + 3$.
[*Hint:* Assume that there are only finitely many primes of the form $8k + 3$, say $p_1, p_2, \ldots, p_r$, and consider the integer $N = (p_1p_2 \cdots p_r)^2 + 2$.]

8. Find a prime number p that is simultaneously expressible in the forms $x^2 + y^2$, $u^2 + 2v^2$, and $r^2 + 3s^2$.
[*Hint:* $(-1/p) = (-2/p) = (-3/p) = 1$.]

9. If p and q are odd primes satisfying $p = q + 4a$ for some a, establish that

$$(a/p) = (a/q)$$

and, in particular, that $(6/37) = (6/13)$.
[*Hint:* Note that $(a/p) = (-q/p)$ and use the Quadratic Reciprocity Law.]

10. Establish each of the following assertions:
(a) $(5/p) = 1$ if and only if $p \equiv 1, 9, 11$, or $19 \pmod{20}$.
(b) $(6/p) = 1$ if and only if $p \equiv 1, 5, 19$, or $23 \pmod{24}$.
(c) $(7/p) = 1$ if and only if $p \equiv 1, 3, 9, 19, 25$, or $27 \pmod{28}$.

11. Prove that there are infinitely many primes of the form $5k - 1$.
[*Hint:* For any $n > 1$, the integer $5(n!)^2 - 1$ has a prime divisor $p > n$ that is not of the form $5k + 1$; hence, $(5/p) = 1$.]

12. Verify the following:
(a) The prime divisors $p \neq 3$ of the integer $n^2 - n + 1$ are of the form $6k + 1$.
[*Hint:* If $p \mid n^2 - n + 1$, then $(2n - 1)^2 \equiv -3 \pmod p$.]
(b) The prime divisors $p \neq 5$ of the integer $n^2 + n - 1$ are of the form $10k + 1$ or $10k + 9$.
(c) The prime divisors p of the integer $2n(n + 1) + 1$ are of the form $p \equiv 1 \pmod 4$.
[*Hint:* If $p \mid 2n(n + 1) + 1$, then $(2n + 1)^2 \equiv -1 \pmod p$.]
(d) The prime divisors p of the integer $3n(n + 1) + 1$ are of the form $p \equiv 1 \pmod 6$.

13. (a) Show that if p is a prime divisor of $839 = 38^2 - 5 \cdot 11^2$, then $(5/p) = 1$. Use this fact to conclude that 839 is a prime number.
[*Hint:* It suffices to consider those primes $p < 29$.]
(b) Prove that both $397 = 20^2 - 3$ and $733 = 29^2 - 3 \cdot 6^2$ are primes.

14. Solve the quadratic congruence $x^2 \equiv 11 \pmod{35}$.
[*Hint:* After solving $x^2 \equiv 11 \pmod 5$ and $x^2 \equiv 11 \pmod 7$, use the Chinese Remainder Theorem.]

15. Establish that 7 is a primitive root of any prime of the form $p = 2^{4n} + 1$.
[*Hint:* Because $p \equiv 3$ or $5 \pmod 7$, $(7/p) = (p/7) = -1$.]

16. Let a and $b > 1$ be relatively prime integers, with b odd. If $b = p_1 p_2 \cdots p_r$ is the decomposition of b into odd primes (not necessarily distinct) then the *Jacobi symbol* (a/b) is defined by

$$(a/b) = (a/p_1)(a/p_2)\cdots(a/p_r)$$

where the symbols on the right-hand side of the equality sign are Legendre symbols. Evaluate the Jacobi symbols

$$(21/221) \qquad (215/253) \qquad (631/1099)$$

17. Under the hypothesis of the previous problem, show that if a is a quadratic residue of b, then $(a/b) = 1$; but, the converse is false.

18. Prove that the following properties of the Jacobi symbol hold: If b and b' are positive odd integers and $\gcd(aa', bb') = 1$, then

(a) $a \equiv a' \pmod b$ implies that $(a/b) = (a'/b)$.
(b) $(aa'/b) = (a/b)(a'/b)$.
(c) $(a/bb') = (a/b)(a/b')$.
(d) $(a^2/b) = (a/b^2) = 1$.
(e) $(1/b) = 1$.
(f) $(-1/b) = (-1)^{(b-1)/2}$.
[*Hint:* Whenever u and v are odd integers, $(u-1)/2 + (v-1)/2 \equiv (uv-1)/2 \pmod 2$.]
(g) $(2/b) = (-1)^{(b^2-1)/8}$.
[*Hint:* Whenever u and v are odd integers, $(u^2-1)/8 + (v^2-1)/8 \equiv [(uv)^2-1]/8 \pmod 2$.]

19. Derive the Generalized Quadratic Reciprocity Law: If a and b are relatively prime positive odd integers, each greater than 1, then

$$(a/b)(b/a) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

[*Hint:* See the hint in Problem 18(f).]

20. Using the Generalized Quadratic Reciprocity Law, determine whether the congruence $x^2 \equiv 231 \pmod{1105}$ is solvable.

9.4 QUADRATIC CONGRUENCES WITH COMPOSITE MODULI

So far in the proceedings, quadratic congruences with (odd) prime moduli have been of paramount importance. The remaining theorems broaden the horizon by allowing a composite modulus. To start, let us consider the situation where the modulus is a power of a prime.

Theorem 9.11. If p is an odd prime and $\gcd(a, p) = 1$, then the congruence

$$x^2 \equiv a \pmod{p^n} \qquad n \geq 1$$

has a solution if and only if $(a/p) = 1$.

Proof. As is common with many "if and only if" theorems, half of the proof is trivial whereas the other half requires considerable effort: If $x^2 \equiv a \pmod{p^n}$ has a solution, then so does $x^2 \equiv a \pmod p$—in fact, the same solution—whence $(a/p) = 1$.

For the converse, suppose that $(a/p) = 1$. We argue that $x^2 \equiv a \pmod{p^n}$ is solvable by inducting on n. If $n = 1$, there is really nothing to prove; indeed, $(a/p) = 1$ is just another way of saying that $x^2 \equiv a \pmod p$ can be solved. Assume that the result holds for $n = k \geq 1$, so that $x^2 \equiv a \pmod{p^k}$ admits a solution x_0. Then

$$x_0^2 = a + bp^k$$

for an appropriate choice of b. In passing from k to $k + 1$, we shall use x_0 and b to write down explicitly a solution to the congruence $x^2 \equiv a \pmod{p^{k+1}}$.

Toward this end, we first solve the linear congruence

$$2x_0 y \equiv -b \pmod p$$

obtaining a unique solution y_0 modulo p (this is possible because $\gcd(2x_0, p) = 1$). Next, consider the integer

$$x_1 = x_0 + y_0 p^k$$

Upon squaring this integer, we get

$$\begin{aligned}(x_0 + y_0 p^k)^2 &= x_0^2 + 2x_0 y_0 p^k + y_0^2 p^{2k} \\ &= a + (b + 2x_0 y_0)p^k + y_0^2 p^{2k}\end{aligned}$$

But $p \mid (b + 2x_0 y_0)$, from which it follows that

$$x_1^2 = (x_0 + y_0 p^k)^2 \equiv a \pmod{p^{k+1}}$$

Thus, the congruence $x^2 \equiv a \pmod{p^n}$ has a solution for $n = k + 1$ and, by induction, for all positive integers n.

Let us run through a specific example in detail. The first step in obtaining a solution of, say, the quadratic congruence

$$x^2 \equiv 23 \pmod{7^2}$$

is to solve $x^2 \equiv 23 \pmod 7$, or what amounts to the same thing, the congruence

$$x^2 \equiv 2 \pmod 7$$

Because $(2/7) = 1$, a solution surely exists; in fact, $x_0 = 3$ is an obvious choice. Now x_0^2 can be represented as

$$3^2 = 9 = 23 + (-2)7$$

so that $b = -2$ (in our special case, the integer 23 plays the role of a). Following the proof of Theorem 9.11, we next determine y so that

$$6y \equiv 2 \pmod 7$$

that is, $3y \equiv 1 \pmod 7$. This linear congruence is satisfied by $y_0 = 5$. Hence,

$$x_0 + 7y_0 = 3 + 7 \cdot 5 = 38$$

serves as a solution to the original congruence $x^2 \equiv 23 \pmod{49}$. It should be noted that $-38 \equiv 11 \text{ mod } (49)$ is the only other solution.

If, instead, the congruence

$$x^2 \equiv 23 \pmod{7^3}$$

were proposed for solution, we would start with

$$x^2 \equiv 23 \pmod{7^2}$$

obtaining a solution $x_0 = 38$. Because

$$38^2 = 23 + 29 \cdot 7^2$$

the integer $b = 29$. We would then find the unique solution $y_0 = 1$ of the linear congruence

$$76y \equiv -29 \pmod 7$$

Then $x^2 \equiv 23 \pmod{7^3}$ is satisfied by

$$x_0 + y_0 \cdot 7^2 = 38 + 1 \cdot 49 = 87$$

as well as $-87 \equiv 256 \pmod{7^3}$.

Having dwelt at length on odd primes, let us now take up the case $p = 2$. The next theorem supplies the pertinent information.

Theorem 9.12. Let a be an odd integer. Then we have the following:

(a) $x^2 \equiv a \pmod 2$ always has a solution.
(b) $x^2 \equiv a \pmod 4$ has a solution if and only if $a \equiv 1 \pmod 4$.
(c) $x^2 \equiv a \pmod{2^n}$, for $n \geq 3$, has a solution if and only if $a \equiv 1 \pmod 8$.

Proof. The first assertion is obvious. The second depends on the observation that the square of any odd integer is congruent to 1 modulo 4. Consequently, $x^2 \equiv a \pmod 4$ can be solved only when a is of the form $4k + 1$; in this event, there are two solutions modulo 4, namely, $x = 1$ and $x = 3$.

Now consider the case in which $n \geq 3$. Because the square of any odd integer is congruent to 1 modulo 8, we see that for the congruence $x^2 \equiv a \pmod{2^n}$ to be solvable a must be of the form $8k + 1$. To go the other way, let us suppose that $a \equiv 1 \pmod 8$ and proceed by induction on the exponent n. When $n = 3$, the congruence $x^2 \equiv a \pmod{2^n}$ is certainly solvable; indeed, each of the integers 1, 3, 5, 7 satisfies $x^2 \equiv 1 \pmod 8$. Fix a value of $n \geq 3$ and assume, for the induction hypothesis, that the congruence $x^2 \equiv a \pmod{2^n}$ admits a solution x_0. Then there exists an integer b for which

$$x_0^2 = a + b2^n$$

Because a is odd, so is the integer x_0. It is therefore possible to find a unique solution y_0 of the linear congruence

$$x_0 y \equiv -b \pmod 2$$

We argue that the integer

$$x_1 = x_0 + y_0 2^{n-1}$$

satisfies the congruence $x^2 \equiv a \pmod{2^{n+1}}$. Squaring yields

$$\begin{aligned}(x_0 + y_0 2^{n-1})^2 &= x_0^2 + x_0 y_0 2^n + y_0^2 2^{2n-2}\\ &= a + (b + x_0 y_0)2^n + y_0^2 2^{2n-2}\end{aligned}$$

By the way y_0 was chosen, $2 \mid (b + x_0 y_0)$; hence,

$$x_1^2 = (x_0 + y_0 2^{n-1})^2 \equiv a \pmod{2^{n+1}}$$

(we also use the fact that $2n - 2 = n + 1 + (n - 3) \geq n + 1$). Thus, the congruence $x^2 \equiv a \pmod{2^{n+1}}$ is solvable, completing the induction step and the proof.

To illustrate: The quadratic congruence $x^2 \equiv 5 \pmod 4$ has a solution, but $x^2 \equiv 5 \pmod 8$ does not; on the other hand, both $x^2 \equiv 17 \pmod{16}$ and $x^2 \equiv 17 \pmod{32}$ are solvable.

In theory, we can now completely settle the question of when there exists an integer x such that

$$x^2 \equiv a \pmod n \qquad \gcd(a, n) = 1 \qquad n > 1$$

For suppose that n has the prime-power decomposition

$$n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad k_0 \geq 0, k_i \geq 0$$

where the p_i are distinct odd primes. Since the problem of solving the quadratic congruence $x^2 \equiv a \pmod n$ is equivalent to that of solving the system of congruences

$$\begin{gathered} x^2 \equiv a \pmod{2^{k_0}} \\ x^2 \equiv a \pmod{p_1^{k_1}} \\ \vdots \\ x^2 \equiv a \pmod{p_r^{k_r}} \end{gathered}$$

our last two results may be combined to give the following general conclusion.

Theorem 9.13. Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of $n > 1$ and let $\gcd(a, n) = 1$. Then $x^2 \equiv a \pmod n$ is solvable if and only if

(a) $(a/p_i) = 1$ for $i = 1, 2, \ldots, r$;
(b) $a \equiv 1 \pmod 4$ if $4 \mid n$, but $8 \nmid n$; $a \equiv 1 \pmod 8$ if $8 \mid n$.

PROBLEMS 9.4

1. (a) Show that 7 and 18 are the only incongruent solutions of $x^2 \equiv -1 \pmod{5^2}$.
   (b) Use part (a) to find the solutions of $x^2 \equiv -1 \pmod{5^3}$.
2. Solve each of the following quadratic congruences:
   (a) $x^2 \equiv 7 \pmod{3^3}$.
   (b) $x^2 \equiv 14 \pmod{5^3}$.
   (c) $x^2 \equiv 2 \pmod{7^3}$.
3. Solve the congruence $x^2 \equiv 31 \pmod{11^4}$.
4. Find the solutions of $x^2 + 5x + 6 \equiv 0 \pmod{5^3}$ and $x^2 + x + 3 \equiv 0 \pmod{3^3}$.
5. Prove that if the congruence $x^2 \equiv a \pmod{2^n}$, where a is odd and $n \geq 3$, has a solution, then it has exactly four incongruent solutions.
   [*Hint:* If x_0 is any solution, then the four integers $x_0, -x_0, x_0 + 2^{n-1}, -x_0 + 2^{n-1}$ are incongruent modulo 2^n and comprise all the solutions.]