Patterns in Prime Numbers: The Quadratic Reciprocity Law

4.1 Introduction

The ancient Greek philosopher Empedocles (c. 495–c. 435 B.C.E.) postulated that all known substances are composed of four basic elements: air, earth, fire, and water. Leucippus (fifth century B.C.E.) thought that these four were indecomposable. And Aristotle (384–322 B.C.E.) introduced four properties that characterize, in various combinations, these four elements: for example, fire possessed dryness and heat. The properties of compound substances were aggregates of these. This classical Greek concept of an element was upheld for almost two thousand years. But by the end of the nineteenth century, 83 chemical elements were known to exist, and these formed the basic building blocks of more complex substances. The European chemists Dmitry I. Mendeleyev (1834–1907) and Julius L. Meyer (1830–1895) arranged the elements approximately in the order of increasing atomic weight (now known to be the order of increasing atomic numbers), which exhibited a periodic recurrence of their chemical properties [205, 248]. This pattern in properties became known as the periodic law of chemical elements, and the arrangement as the periodic table. The periodic table is now at the center of every introductory chemistry course, and was a major breakthrough into the laws governing elements, the basic building blocks of all chemical compounds in the universe (Exercise 4.1).

The prime numbers can be considered numerical analogues of the chemical elements. Recall that these are the numbers that are multiplicatively indecomposable, i.e., divisible only by 1 and by themselves. The world in all its aspects is governed by whole numbers and their relationships, according to the Pythagoreans, a very influential group of philosophers and mathematicians gathered around Pythagoras during the sixth century B.C.E., after whom the Pythagorean theorem in geometry is named. One of the results about positive whole numbers known in antiquity is that every number can be written in essentially only one way as a product of prime numbers. This fact is now known as the fundamental theorem of arithmetic (see the Appendix). For instance, a consequence of the theorem is not only that 42 is a product of prime numbers,
namely 2, 3, and 7, but moreover that this is unique, in that it is the only way that 42 can be decomposed as a product of primes (Exercise 4.2). The uniqueness of the prime decomposition is incredibly important, underlying virtually all aspects of number theory.\footnote{For instance, we will often use without mention the fact that if a prime divides a product, then it divides one of its factors. This is a consequence of the uniqueness of prime factorization (Exercise 4.3), or can be proven separately and used to deduce the fundamental theorem of arithmetic. It is hard to overemphasize how often we use the fundamental theorem of arithmetic without even thinking about it.} Thus the prime numbers can be viewed as basic building blocks of whole numbers.\footnote{Note that the fundamental theorem of arithmetic builds numbers “multiplicatively” from primes. For an attempt at an “additive” analogy for numbers, see the later footnote about Lagrange’s “four squares” theorem, when we discuss his work under the heading Divisor plus Descent.} Like chemists, mathematicians too have striven to discover the laws that govern prime numbers, and to answer some of the most fundamental questions about them: How many prime numbers are there? Can we find them all?

The first question was already answered by the mathematicians of ancient Greece. The great Greek mathematician Euclid of Alexandria, who lived around 300 B.C.E., published a collection of results in geometry and number theory, *The Elements*[61], which went on to become one of the all-time best-sellers. One of the results, Proposition 20 in Book IX, states that “Prime numbers are more than any assigned multitude of prime numbers.” Today we would say that there are infinitely many prime numbers. Euclid’s very clever proof in fact provides a bit more information than that. A few hours of calculation will easily demonstrate to the reader that prime numbers seem to appear quite irregularly among all numbers. So one might ask the question whether, beginning with a given prime number, there is an estimate as to when we will encounter the next prime number. Euclid’s proof contains one such estimate, even though it is not a very good one.

Euclid proves the result by showing that if we take the first so many prime numbers, there has to be another one that is not among them. He concludes this from the observation that, if \(p_1, \ldots, p_n\) are the first \(n\) prime numbers, then the number \(x = (p_1 \cdot p_2 \cdots p_n) + 1\) can be written uniquely as a product of prime numbers, by the fundamental theorem of arithmetic. But none of the primes \(p_i\) divides this number, as the reader is invited to verify, so that there must be other primes. Furthermore, these other primes must appear between \(p_n\) and \(x\) (Exercise 4.4).

As to the second question, since the answer to the first question is “an infinite number,” no one can hope to write out all prime numbers any more than one can write out all positive integers. However, there are ways to find all prime numbers up to a certain size. The sieve of Eratosthenes is an ancient one (Exercise 4.5). One may also find the \(n\)th prime, for any \(n\), by simply extending the sieve far enough. No efficient closed formula to accomplish this
is known that invokes only elementary functions. However, Juri Matiyasević, as a by-product of showing that Hilbert’s tenth problem\textsuperscript{3} is unsolvable \cite{42, 43, 44, 130}, discovered a hefty polynomial (with integral coefficients and many variables) that, with positive integral inputs, outputs only primes and eventually any given prime (see also \cite{250} for other formulas). Since primes seem at first sight to occur totally irregularly among the natural numbers, it would be wonderfully surprising to find patterns in their appearance. This chapter is about exactly that: the discovery, proof, and applications of the first big pattern discovered in the occurrence of prime numbers, emerging from the ancient study of which numbers can be expressed as sums of squares.

Much of modern number theory revolves directly or indirectly around problems related to prime numbers. However, despite some ancient Greek interest in the subject, it was not until the work of the Frenchman Pierre de Fermat (1601–1665) that the foundations of the subject began to be laid. Most famous for his \textit{last theorem},\textsuperscript{4} Fermat worked on many problems, some of which had ancient origins, most notably in the \textit{Arithmetica} of Diophantus of Alexandria, who lived during the third century, one of the last great mathematicians of Greek antiquity. The \textit{Arithmetica} is a collection of 189 problems on the solution, using fractions, of equations in one or more variables, originally divided into thirteen “books,” of which only ten are preserved (four were rediscovered only in 1972) \cite{12, 189, 206}. The solutions are presented in terms of specific numerical examples. Studying a Latin edition of the \textit{Arithmetica} published in 1621 \cite{49} (see also \cite{109}), Fermat was inspired to begin his own number-theoretic researches. For instance, Problem 9 in Book V asks for an odd number to be expressed as a sum of two squares, with several side conditions. In the course of presenting a solution to this problem, Diophantus seems to assume that every integer can be written as a sum of at most four squares (Exercise 4.6). Another problem (Problem 19 in Book III) asserts that “It is in the nature of 65 that it can be written in two different ways as a sum of two squares, viz., as 16 + 49 and as 64 + 1; this happens because it is the product of 13 and 5, each of which is a sum of two squares” (Exercise 4.7).

\textsuperscript{3}David Hilbert (1862–1943), one of the most renowned mathematicians at the beginning of the twentieth century, proposed a list of 23 unsolved problems for consideration in the coming century, saying, “As long as a branch of science offers an abundance of problems, so long is it alive” \cite[p. 657]{18}. Hilbert’s problems have served as major inspiration and guideposts to mathematics now for more than a hundred years \cite{253}.

Hilbert’s tenth problem was, “Does there exist a universal algorithm for solving Diophantine equations?” A Diophantine equation is a polynomial equation with integer coefficients for which only integer solutions are allowed, such as the Fermat equation in the next footnote.

\textsuperscript{4}See the chapter on Fermat’s last theorem in \cite{150}. Fermat claimed that the equation $x^n + y^n = z^n$ has no solution in positive whole numbers $x, y, z$ when $n > 2$. One of the greatest triumphs of twentieth-century mathematics was the proof of his famous long-standing claim.
Diophanti Alexandrini Arithmeticae

De Numeris Multangulosis

CVM COMMENTARIIS C. G. BACHEII V. C. 
& observationibus D. P. de FERMAT Senatoris Tolosani.

Accedit Doctrinae Analyticae inuentum nouum, collectum
ex variis eiusdem D. de FERMAT Epistolis.

Photo 4.1. Diophantus’s Arithmetica.
One of the well-known successors of Diophantus who also worked on sums of squares was Leonardo of Pisa (1180–1250), better known as Fibonacci, after whom the Fibonacci numbers are named [156].

Fermat, in a letter to Sir Kenelm Digby (an English adventurer and double agent) from June 1658, proudly presents some of his discoveries about sums of squares:

In most of the questions of volumes IV and V, Diophantus supposes that every whole number is either a square, or a sum of two, three, or four squares. In his commentary to Problem IV.31, Bachet admits that he was not able to completely prove this proposition. René Descartes himself, in a letter which will soon be published, and whose content I have learnt, ingeniously admits that he is ignoring the proof and declares that the road to obtaining it seems to him to be one of the most difficult and most obstructed. So I don’t see how one could doubt the importance of this proposition. Well, I am announcing to your distinguished correspondents that I have found a complete demonstration. I can add a number of very celebrated propositions for which I also possess irrefutable proof. For example:

Every prime number of the form \(4n + 1\) is the sum of two squares, such as 5, 13, 17, 29, 37, 41, etc.

Every prime number of the form \(3n + 1\) is the sum of a square and the triple of another square, for instance, 7, 13, 19, 31, 37, 43, etc.

Every prime number of the form \(8n + 1\) or \(8n + 3\) is the sum of a square and double another square, such as 3, 11, 17, 19, 41, 43, etc. [73, pp. 314–315].

No proofs of these results came forth to back up Fermat’s amazing claims, and it was not until over a hundred years later that all of them were shown to be true.

Fermat had a law degree and spent most of his life as a government official in Toulouse. There are many indications that he did mathematics partly as a diversion from his professional duties, solely for personal gratification. That was not unusual in his day, since a mathematical profession comparable to today’s did not exist. Very few scholars in Europe made a living through their research accomplishments. Fermat had one especially unusual trait: characteristically he did not divulge proofs for the discoveries he wrote of to others; rather, he challenged them to find proofs of their own. While he enjoyed the attention and esteem he received from his correspondents, he never showed interest in publishing a book with his results. He never traveled to the centers of mathematical activity, not even Paris, preferring to communicate with the scientific community through an exchange of letters, facilitated by the Parisian theologian Marin Mersenne (1588–1648), who served as a clearinghouse for scientific correspondence from all over Europe, in the absence as yet of scientific research journals. While Fermat made very important contributions to the development of the differential and integral calculus and to analytic geometry.
his life-long passion belonged to the study of properties of the integers, now known as number theory, and it is here that Fermat has had the most lasting influence on the subsequent course of mathematics.

In hindsight, Fermat was one of the great mathematical pioneers, who built a whole new paradigm for number theory on the accomplishments of his predecessors, and laid the foundations for a mathematical theory that would later be referred to as the “queen of mathematics.” But, as is the fate of some scientific pioneers, during his lifetime he tried in vain to kindle serious interest among the larger scientific community in pursuing his number-theoretic researches. Christiaan Huygens (1629–1695), the object of Fermat’s final effort to arouse interest in his work, commented in a 1658 letter [245, p. 119] to John
4.1 Introduction

Wallis (1616–1703), “There is no lack of better things for us to do.” Whether it was the sentiment of the times, or Fermat’s secretiveness about his methods of discovery and his lack of proofs, he was singularly unsuccessful in enticing the great minds among his contemporaries to follow his path. It was to be a hundred years before another mathematician of Fermat’s stature took the bait and carried on his work.

Leonhard Euler (1707–1783) was without doubt one of the greatest mathematicians the world has ever known. A native of Switzerland, Euler spent his working life at the Academies of Sciences in St. Petersburg and Berlin. His mathematical interests were wide-ranging, and included number theory, which he pursued almost as a diversion, in contrast to the more mainstream areas of mathematics to which he contributed [136]. A large part of Euler’s number-theoretic work consisted of a systematic program to provide proofs for all the assertions of Fermat, including Fermat’s last theorem. An excellent detailed description can be found in [245].

One of the first things that caught Euler’s attention in Fermat’s work, which he became aware of in 1730 through his correspondence with Christian Goldbach (1690–1764), was Fermat’s claim that every whole number was a square or a sum of two, three, or four squares. For the rest of his life he was to search for a proof of it, in vain. All he succeeded in showing is that every whole number is a sum of at most four rational squares. (An English translation of Euler’s proof can be found in [220, pp. 91–94].) After discovering proofs for many of Fermat’s claims about sums of squares, he turned his attention to the following more general question:

**Representation Problem.** For a given nonzero integer \( a \), which prime numbers can be represented in the form \( x^2 + ay^2 \) for a suitable choice of positive integers \( x \) and \( y \)?

As Euler certainly realized, this representability question is multiplicative in nature, in the sense that if \( m \) and \( n \) are of the form \( x^2 + ay^2 \), then so is \( mn \) (Exercise 4.8). So it makes sense first to pose and solve the problem of representing prime numbers in the form \( x^2 + ay^2 \). For the cases \( a = 1, 2, 3 \), a solution was essentially claimed by Fermat, as the letter to Digby, quoted above, shows. This is because, first, Fermat claims in each of these cases that every prime number of a certain “linear” form, i.e., lying in certain arithmetic progressions, will also be of the desired “quadratic” form \( x^2 + ay^2 \). For instance, for \( a = 2 \), Fermat asserts that every prime lying in the arithmetic progressions \( 8n + 1 \) or \( 8n + 3 \) (where \( n \) may be any nonnegative integer) can also be represented in the quadratic form \( x^2 + 2y^2 \). Second, the converse is easy to show in each case, namely that any (odd) prime represented in the desired quadratic form must also have the specified linear form (Exercise 4.9). Fermat’s assertions thus suggest that in general one look for certain linear

---

5 A *rational* number is one that can be expressed as a fraction.
forms (arithmetic progressions) whose primes are exactly those represented by certain quadratic forms.

Another amazing claim of Fermat’s, that a sum $x^2 + y^2$, with $x$ and $y$ relatively prime positive integers, i.e., having no common prime divisors, can never have a divisor of the form $4n - 1$ no matter how $x$ and $y$ are chosen, suggested a related problem to Euler:

**Divisor Problem.** For a given nonzero integer $a$, find all nontrivial prime divisors, e.g., those in specified arithmetic progressions, of numbers of the form $x^2 + ay^2$, again with $x$ and $y$ running through all positive integers.

Let us begin by analyzing this second problem, which became a major focus for Euler. We begin by deciding what we mean by nontrivial divisors. First, any common divisor of $x$ and $y$ will trivially be a divisor of a number of the form $x^2 + ay^2$, so we may as well assume that $x$ and $y$ are relatively prime. Second, any divisor of $a$ will clearly also be a divisor of some number of this form. Third, 2 is always a divisor of some number of the form $x^2 + ay^2$. So to summarize, the nontrivial prime divisors $p$ of numbers of the form $x^2 + ay^2$ will be those for which $p$ is odd, $x$ and $y$ are relatively prime, and $p$ does not divide $a$. As a consequence we see that the divisor $p$ will also not divide $x$, nor therefore $y$.

Having set the stage, our nontrivial prime divisor satisfies

$$pm = x^2 + ay^2$$

for some integer $m$. From this point on we will freely use basic notation and properties of modern congruence arithmetic, outlined in the Appendix to this chapter, even though this did not come into use until around the beginning of the nineteenth century; it is amazing how helpful this notation and way of thinking is. Since $y$ is relatively prime to $p$, we can find an integer $z$ such that $yz \equiv 1 \pmod{p}$ (see the Appendix). Multiplying $x^2 + ay^2$ by $z^2$, we obtain

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

that is, $-a$ is a square or quadratic residue modulo $p$ (we reserve the term quadratic residue for nonzero squares modulo $p$).

Conversely, suppose that $-a \equiv n^2 \pmod{p}$ with $n$ not divisible by $p$. Then $-a = n^2 + mp$ for some integer $m$, and

$$(-m)p = n^2 + a \cdot 1^2.$$

Thus we have the following statement:

**Divisors and Quadratic Residues.** The nontrivial prime divisors $p$ of numbers of the form $x^2 + ay^2$ are precisely the odd primes $p$ for which $-a$ is a nonzero quadratic residue modulo $p$.

Therefore to solve the problem of finding nontrivial prime divisors of numbers of the form $x^2 + ay^2$ it is enough to find those odd primes for which $-a$ is
a nonzero quadratic residue. But of course this seems like an infinite task, to be calculated one prime at a time, with no pattern in sight! On the bright side, Fermat’s claims, both positive and negative, enticingly suggest that there may be an undiscovered pattern to the nontrivial prime divisors of such quadratic forms, namely that for each quadratic form its prime divisors might be precisely those in certain arithmetic progressions. For instance, if we put together Fermat’s two claims about the quadratic form $x^2 + y^2$, that odd primes of the form $4n + 1$ are always of the form $x^2 + y^2$, and that no number of the form $4n - 1$ can ever be a divisor of a number of the form $x^2 + y^2$, we see that the nontrivial prime divisors of numbers of the form $x^2 + y^2$ are precisely the primes in the arithmetic progression $4n + 1$, solving the divisor problem for $a = 1$. Rephrased in the language of congruences and quadratic residues, we can say that $-1$ is a quadratic residue modulo primes of the form $4n + 1$, and a quadratic nonresidue modulo primes of the form $4n + 3$.

Euler sought precisely such patterns, and amassed vast calculational evidence, enough that he was able to discover and state general patterns for the nontrivial prime divisors of all quadratic forms $x^2 + ay^2$, for arbitrary positive and negative values of $a$. Already in 1744, in the earlier part of his career, Euler published the paper *Theoremata circa divisores numerorum in hac forma contentorum paa ± qbb* (Theorems about the divisors of numbers expressed in the form $paa ± qbb$), in which he presents the results of his extensive experimental calculations, and displays and states what patterns he has observed for the prime divisors of such quadratic forms. In the next section, excerpts from this paper will form our first primary source, and in hindsight we can see in the general patterns he asserted in 1744 the essence of a fundamental law governing prime numbers [140]. One of the delightful aspects of reading Euler’s work is how transparently and expansively he shows us his train of investigation and exploration leading to the patterns that he conjectures to hold in general. Despite efforts spanning much of his life, though, he was able to prove these assertions in only a very few cases, essentially those of Fermat’s claims. He eventually managed to find proofs for the nontrivial prime divisors of numbers of the form $x^2 + ay^2$ for $a = 1, ±2, 3$, and in these cases he could even prove Fermat’s assertions above that prime numbers in certain arithmetic progressions are always actually represented by these forms, not merely divisors of them.

After a lifelong search for ways to settle the question of prime divisors of numbers of the form $x^2 + ay^2$, Euler published his final formulation of the still generally unproven magical property of primes he had discovered that provides the solution. We will also read excerpts from this later paper, *Observationes circa divisionem quadratorum per numeros primos* (Observations on the Division of Square Numbers by Primes), published in the year of his death. The property Euler discovered is a precursor of the quadratic reciprocity law (QRL), the cornerstone of our chapter. It enables one to answer the divisor problem. In more modern form and terminology, we shall see that it allows the determination of the quadratic character (quadratic residue or not) of $-a$ modulo $p$ in terms of the quadratic character of $p$ modulo primes
dividing \(-a\), i.e., with the roles of \(-a\) and \(p\) reversed! Note how this helps solve the original problem of finding all nontrivial prime divisors of a fixed form \(x^2 + ay^2\), which we already translated into the problem of finding the primes \(p\) for which \(-a\) is a quadratic residue modulo \(p\). Since the QRL will convert this into the question of which primes \(p\) are quadratic residues modulo each of the prime divisors of \(-a\), we are now dealing with finitely many fixed moduli, for which such calculations are highly tractable. Prior to this advance we needed to consider infinitely many prime moduli \(p\). We will illustrate this in detail as soon as we have a proper statement of the QRL in hand.

Let us now return to the representability problem, namely, which numbers are actually of the form \(x^2 + ay^2\), not merely divisors of such a form? It is of course still true, as above, that if a prime \(p\) is actually of the form \(x^2 + ay^2\), then \(-a\) must be a quadratic residue modulo \(p\). But this is only a necessary condition, and not always a sufficient one. For instance, 3 divides a number of the form \(x^2 + 5y^2\), since \(1^2 + 5 \cdot 2^2 = 21\); thus \(-5\) is a quadratic residue modulo 3. But clearly 3 is not of the form \(x^2 + 5y^2\). So while 3 is a nontrivial divisor of (a number of) the form \(x^2 + 5y^2\), it fails to be actually represented by it. This simple example shows that the representability problem is a related but in general much harder problem than the divisor problem, and it took a fresh paradigm to begin any real headway on it, established by the most distinguished of Euler’s young contemporaries, Joseph Louis Lagrange (1736–1813).

**Divisor Plus Descent Can Produce Representability.** A solution to the divisor problem can often be combined with a method called descent, pioneered by Fermat, used by Euler, and vastly extended by Lagrange, to solve the representability problem.

We will sketch an initial illustration here, combining a divisor problem solution with a descent to prove Fermat’s most famous representation claim, that any prime \(p\) of the form \(4n + 1\) can be written as a sum of two squares. The first step is to have in hand a solution to the divisor problem for \(x^2 + y^2\), which we will obtain from our extract of Euler’s second paper: \(-1\) is a quadratic residue modulo the prime \(p = 4n + 1\), i.e., any prime \(p\) of the form \(4n + 1\) is a nontrivial divisor of some number of the form \(x^2 + y^2\). We also need a descent result, which will be provided by our extract from Lagrange’s work: If \(x^2 + y^2\) is a number with \(x\) and \(y\) relatively prime, then any divisor of this number is likewise a sum of two relatively prime squares. This is called descent because we have descended from one sum of squares to a smaller number of the same quadratic form. Now we combine these, following the divisor solution by the descent: Given a prime \(4n + 1\), by our divisor solution it must nontrivially divide a sum of two squares. But the descent solution says that any divisor of this sum of two squares is again a sum of two squares. Voilà, our original prime \(4n + 1\) is a sum of two squares.

To apply this two-step “divisor plus descent” technique to solve a representability problem, one would in general need a solution to the divisor problem (to be provided by the quadratic reciprocity law), and a descent result of
some kind. But we caution that from the example above, in which $x^2 + 5y^2$
nontrivially represents 21, but not its divisor 3, we see that descent does not always work as simply as one would wish. Lagrange’s analysis is what was needed next.

There was only a small number of scholars during the second half of the eighteenth century interested in pure mathematics. Fortunately, one of them, Lagrange, devoted part of his career to the pursuit of number theory. In 1766 Lagrange became the successor of Euler at the Academy of Sciences in Berlin, after Euler returned to St. Petersburg. Inspired by Euler’s work on number theory, Lagrange produced a string of publications on the subject during the following decade. Going beyond the scattered results of Fermat and Euler on sums of squares, Lagrange proposed a powerful abstraction, to make the representational forms themselves the object of study, rather than merely the integers represented by them. And he realized that in order to get a coherent theory, he needed to consider more general quadratic expressions than $x^2 + ay^2$.

In other words, Lagrange proposed to study formally general quadratic forms, expressions of the form $ax^2 + bxy + cy^2$,
as well as their properties and relationships, where $a, b, c$ are integers. In particular, he studied what the possible quadratic and linear forms could be for nontrivial divisors of a given quadratic form; this provides a basis for general descent results, as we shall see. Lagrange went on to lay the foundations of the theory of quadratic forms, which would be deepened and extended later by the great Carl Friedrich Gauss (1777–1855).

Amazingly, the general descent results Lagrange obtained, cleverly combined with just a few divisor problem solutions, produced a fountain of theorems about representability of primes by forms $x^2 + ay^2$, far beyond what Fermat and Euler had been able to show. To top it all off, Lagrange was able to find a proof for the long-standing claim that every positive integer is a sum of four integer squares.\footnote{This had become part of a much broader claim of Fermat’s, that every number is the sum of at most three triangular numbers (see the bridge chapter), or four squares, or five pentagonal numbers, etc. \cite{245}, indicating that these particular types of numbers are additive building blocks for all numbers in a certain sense.} Our next original source in the chapter will be an excerpt from Lagrange’s work on quadratic forms in \textit{Recherches d’Arithmétique} (Researches in Arithmetic), published in 1773–1775 as a Memoir of the Berlin Academy of Sciences \cite[vol. III, pp. 695–795]{141}, showing how his abstract analysis of quadratic forms enabled him to obtain many new representability results. The reader with some knowledge of algebraic number theory can find an extensive treatment of representations of integers as sums of squares in \cite{102}. The problem of representing primes as values of quadratic forms is discussed from a mathematically sophisticated point of view in the excellent exposition \cite{41}.
The next link in the precarious chain between Fermat and modern number theory was the French mathematician Adrien-Marie Legendre (1752–1833). After receiving an education in mathematics and physics in Paris, Legendre spent some time teaching at the military academy there. In 1782 he attracted the attention of Lagrange by winning the prize of the Berlin Academy of Sciences for a paper on applications of mathematics to ballistics. Legendre went on to a distinguished career at the Paris Academy of Sciences. He made significant contributions to several areas of mathematics, in particular number theory. In the tradition of his number-theoretic predecessors Fermat, Euler, and Lagrange, Legendre too studied the problem of representing prime numbers by quadratic forms, including some results on quadratic forms in more than two variables. In Part IV of the memoir Recherches d’Analyse Indéterminée (Researches in Indeterminate Analysis), published in 1788 (and submitted to the Paris Academy of Sciences in 1785), Legendre attempted a proof of what he called later “a law of reciprocity between primes,” now known as the quadratic reciprocity law. Curiously enough, there is no mention anywhere of Euler’s work on the QRL. Even though Legendre had carefully studied Euler [245, p. 326], he had apparently missed this gem. And Euler would certainly have deserved mention, even though he had not made major progress on providing a proof.

Later on, in his treatise Théorie des Nombres (Theory of Numbers) [153], one of the first books on number theory, Legendre reformulated the law using what is now called the Legendre symbol, and presented a proof of it. Unfortunately, his proof was not complete. In it he assumed, among other things, that in every arithmetic progression of the form

\[ \{an + b \mid n = 0, 1, 2, \ldots \}, \]

with \(a\) and \(b\) relatively prime, there exist infinitely many prime numbers. Despite Legendre’s certainty of this truth about arithmetic progressions, he had no proof for it. Proof was finally provided in 1837 by Lejeune Dirichlet (1805–1859) [135, p. 829f], and it stands now as one of the deep results about prime numbers. Our final original source on the discovery of the quadratic reciprocity law is excerpted from Legendre’s Theory of Numbers. In it not only will we see him state the law as a genuine reciprocity principle, but we will see that he uses it to prove many of the results that eluded Euler on divisors of quadratic forms and representation of primes via certain forms.

In order to state the quadratic reciprocity law as presented by Legendre, we need first to mention a result discovered by Euler, which we shall see derived in our Legendre source. Euler derived a criterion, essentially a formula, for whether a given integer \(a\) is a quadratic residue modulo a given prime \(p\). Stated in modern congruence language, it says the following:

**Euler’s Criterion.** Let \(p\) be an odd prime and \(a\) not divisible by \(p\). Then \(a\) is a quadratic residue modulo \(p\) if and only if

\[ a^{(p-1)/2} \equiv 1 \pmod{p}. \]

While one could in principle actually use this formula to calculate whether a number is a quadratic residue, the calculations can be long, and Euler’s criterion is much more valuable for its theoretical use. In fact, everything from now on will be based on it. When we read Legendre, we shall see that even more is going on than is stated in the criterion above, namely that when \( p \) is an odd prime and \( a \) not divisible by \( p \), the expression \( a^{(p-1)/2} \) is always congruent to either 1 or \(-1\) modulo \( p \), according to whether or not \( a \) is a quadratic residue modulo \( p \). Legendre then introduces the symbolism \( \left( \frac{a}{p} \right) \) for this resulting value, so we have

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p, \\
-1 & \text{if not.}
\end{cases}
\]

For example, if \( p = 11 \), then \( \left( \frac{a}{11} \right) \) equals 1 for \( a = 1, 3, 4, 5, 9 \), and equals \(-1\) for \( a = 2, 6, 7, 8, 10 \). One can confirm this for each \( a \) by brute force by calculating and listing the squares of the ten nonzero residues modulo 11, or alternatively, using Euler’s criterion, by calculating for each \( a \) above whether \( a^{(p-1)/2} \) is congruent to 1 or \(-1\) modulo 11 (Exercise 4.10). Since

\[
\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right)
\]

if \( a \) and \( b \) have the same remainder modulo \( p \), as the reader should verify, evaluating other Legendre symbols with denominator 11 merely requires first calculating a remainder modulo 11.

We are now ready to state the QRL and actually use it to do a computation. Given two odd primes \( p \) and \( q \), it establishes an amazingly simple relationship between the Legendre symbol \( \left( \frac{p}{q} \right) \) and its “reciprocal” \( \left( \frac{q}{p} \right) \). But before reading further, the reader is encouraged to work Exercise 4.11 and guess the law.

**Quadratic Reciprocity Law.** If \( p, q \) are odd prime numbers, then

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.
\]

The reader is strongly encouraged to make this very compact formula more meaningful by reinterpreting it as a statement about how the two Legendre symbols \( \left( \frac{p}{q} \right) \) and \( \left( \frac{q}{p} \right) \), each of which is either 1 or \(-1\), compare with each other, depending on whether each of \( p \) or \( q \) has the form \( 4n + 1 \) or \( 4n + 3 \) (Exercise 4.12).

Two extremely useful supplementary results are commonly proven along with the reciprocity law, the first of which is a straightforward calculation if we allow ourselves to use Euler’s criterion (Exercise 4.13). We shall see Euler’s
242 4 Patterns in Prime Numbers: The Quadratic Reciprocity Law

proof of it later, too, and we will see how the second part follows from the same argument that proves the main QRL.

Supplementary Theorem. If \( p \) is an odd prime, then

1. \( \left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}, \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases} \)

2. \( \left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 
1 & \text{if } p \equiv 1, 7 \pmod{8}, \\
-1 & \text{if } p \equiv 3, 5 \pmod{8}.
\end{cases} \)

Let us illustrate the use of the QRL and the supplementary theorem to make computations with the example \( a = -6, p = 101 \). For this we need just one more tool (Exercise 4.14).

Multiplicativity of the Legendre Symbol. If \( a \) and \( b \) are integers relatively prime to \( p \), then

\[ \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right). \]

With all this we then easily calculate

\[
\left( \frac{-6}{101} \right) = \left( \frac{-1}{101} \right) \left( \frac{2}{101} \right) \left( \frac{3}{101} \right)
= (-1)^{50}(-1)^{\frac{1}{2}(101^2-1)}(-1)^{\frac{1}{2}(3-1)(101-1)} \left( \frac{101}{3} \right)
= -(-1) \left( \frac{101}{3} \right)
= -\left( \frac{2}{3} \right)
= -(-1)
= 1.
\]

Thus, \(-6\) is a quadratic residue modulo 101. Without the QRL we would have possibly had to compute all quadratic residues modulo 101, or calculate the remainder of \((-6)^{\frac{101-1}{2}} \mod 101\) (Exercise 4.15). Our example suggests that with the tools now at hand, it is easy to calculate Legendre symbols, and this is indeed the case, especially by using the QRL repeatedly as necessary during a calculation (Exercise 4.16).

Near the end of our discussion of the divisor problem, we promised that once we had the quadratic reciprocity law in hand, we would illustrate how it helps solve the original problem of finding all nontrivial prime divisors of a fixed quadratic form \( x^2 + ay^2 \). Let us take \( a = 6 \) as our example, so the question translates into asking for which odd primes \( p \) not dividing 6 is \( \left( \frac{-6}{p} \right) = 1 \) (recall “Divisors and Quadratic Residues” above). Euler claimed explicitly in his 1744 paper, based on his experimental evidence, that the nontrivial prime
divisors of numbers of the form \(x^2 + 6y^2\) are exactly those primes of the forms \(24n + 1, 24n + 5, 24n + 7, 24n + 11\). So let us see whether we can determine that these are exactly the odd primes not dividing 6 for which \((-\frac{6}{p}) = 1\). We calculate, as above, that

\[
\left( -\frac{6}{p} \right) = \left( -\frac{1}{p} \right) \left( \frac{2}{p} \right) \left( \frac{3}{p} \right) \quad = (-1)^{\frac{p-1}{2}} (-1)^{\frac{1}{2}(p^2-1)} (-1)^{(3-1) \frac{p-1}{2}} \left( \frac{p}{3} \right) \quad = (-1)^{\frac{1}{2}(p^2-1)} \left( \frac{p}{3} \right).
\]

We can now analyze each of the factors in this final product separately. By analyzing the parity of \(\frac{1}{2}(p^2-1)\), we see that the first factor is 1 if \(p \equiv 1, 7 \pmod{8}\), but is \(-1\) if \(p \equiv 3, 5 \pmod{8}\) (note that this covers all possibilities, since \(p\) is odd). And we see directly that the second factor is 1 if \(p \equiv 1 \pmod{3}\), but is \(-1\) if \(p \equiv 2 \pmod{3}\) (this too covers all possibilities, since \(p\) does not divide 6, so \(p \not\equiv 0 \pmod{3}\)). Now from this information we should be able to check that \((-\frac{6}{p})\), which is the product of these two factors, is 1 precisely for primes not dividing 6 that lie in one of the four arithmetic progressions given above by Euler, thereby proving his claimed identification of all the nontrivial prime divisors of numbers of the form \(x^2 + 6y^2\). We leave this final step to the reader, which amounts to melding the relevant congruences (Exercises 4.17 and 4.18).

We have already seen how the QRL was discovered in pursuit of questions about representability and divisibility of quadratic forms. We can see the utility of the QRL from another perspective as well. The algorithm provided by the quadratic formula for finding the solutions of a quadratic equation is almost as old as mathematics itself. A natural generalization of quadratic equations are quadratic congruences

\[ ax^2 + bx + c \equiv 0 \pmod{n}, \]

for various values of \(n\), and integers \(a, b, c\). One might ask whether there is an analogue of the quadratic formula. Let us explore the case in which the modulus \(n\) is an odd prime, and we may as well assume that \(a\) is not divisible by \(n\), since otherwise the congruence is a linear one. (The case of a more general modulus can be reduced to this one; see [96, Section 9.4].) We can then complete the square and rearrange to obtain the equivalent

\[ (2ax + b)^2 \equiv b^2 - 4ac \pmod{n}. \]

To solve this equation for \(x\) modulo \(n\), we need to be able to find a square root for \(b^2 - 4ac\) and to divide by \(2a\), both modulo \(n\). Division by \(2a\) is possible modulo \(n\) from our assumption that \(a\) is an odd prime not dividing \(n\) (see Appendix). Thus the original quadratic congruence is solvable if and only if its “discriminant” \(d = b^2 - 4ac\) is a square modulo \(n\), that is, if and only if \((-\frac{d}{n}) = 1\). The situation is similar to our example above. If we vary \(n\), it
seems that for every choice of \( n \) we need to check whether \( d \) is a square, an infinite process to accomplish for all \( n \). However, if \( d \) is prime, we can use the QRL to translate the computation of \( \left( \frac{d}{n} \right) \) into calculating \( \left( \frac{n}{d} \right) \) instead (if \( d \) is composite, we simply first split the calculation up multiplicatively, as in the example calculation above, in terms of the prime factors of \( d \)). Now since computing \( \left( \frac{n}{d} \right) \) requires only that we know \( \left( \frac{r}{d} \right) \) for the remainder of \( n \) modulo \( d \), we see that we need only compute these \( d \) values once and for all, and can then easily determine whether the original congruence is solvable modulo any given \( n \). So the QRL saves the day again (Exercise 4.19).

As to congruences of higher degree, the natural question arises whether there are higher reciprocity laws that help us solve these congruences. It was Gauss who first formulated one such higher law, namely a fourth-degree, or so-called biquadratic, reciprocity law (its proof was left to Gotthold Eisenstein (1823–1852)). In his first memoir on biquadratic residues Gauss makes it clear that he believes these higher laws to be a whole new ball game:

The theory of quadratic residues can be reduced to the most beautiful jewel among the fundamental theorems of higher arithmetic, which, as is known, were first discovered easily by inductive methods and then were proved in so many ways that nothing remains to be desired. However, the theory of cubic and biquadratic residues is more difficult by far. In 1805, as we began to investigate these, except for the first results which gave several special theorems that stand out both because of their simplicity and because of the difficulty of their proofs, we soon recognized that the principles of arithmetic which were usable until then were in no way sufficient to build a general theory. Rather such a theory necessarily required an infinite enlargement to some extent of the field of higher arithmetic . . . [96, p. 224].

This is still one of the important unsolved problems in modern number theory: the search for further higher reciprocity laws [155]. (See Wyman [252] for a beautiful exposition of general reciprocity laws.) Of course, a similar generalization is suggested by quadratic form theory when one asks what happens if the forms are allowed to have degree higher than two.

For the quadratic reciprocity law itself, it was the genius of Carl Friedrich Gauss that finally provided a complete rigorous proof, in his *Disquisitiones Arithmeticae* (Arithmetical Investigations), published in 1801 [80]. An unbelievable tour de force, this book of the twenty-four-year-old Gauss opened up number theory as a full-fledged mathematical subject, established notation that is still standard today, provided an extensive set of tools and methods, and proved a plethora of astounding results, with the QRL being one of them. Another of Gauss’s major achievements was a new theory of quadratic forms, comprising a vast extension of Lagrange’s foundational work (for a detailed discussion of the contents of the *Disquisitiones* see [26, Chapter 3]).

In our first section on Gauss’s work, we shall read excerpts showing how he stated the QRL (which he calls the “fundamental theorem”), as well as
his assessment of the work of his predecessors. Interestingly, Gauss considers Euler’s work as falling short of an actual discovery of the QRL, and Legendre complained bitterly about not receiving enough credit from Gauss (see Kronecker [140] on the history of the QRL for details concerning this priority issue). At that juncture in the chapter we shall summarize by providing a unified mathematical view connecting the various claims of Euler, Legendre, and Gauss that we have read up to that point.

Gauss gave altogether six different proofs of the QRL, the first one in the *Disquisitiones Arithmeticae*. In introducing his third published proof in 1808, he says:

The questions of higher arithmetic often present a remarkable characteristic which seldom appears in more general analysis, and increases the beauty of the former subject. While analytic investigations lead to the discovery of new truths only after the fundamental principles of the subject (which to a certain degree open the way to these truths) have been completely mastered; on the contrary in arithmetic the most elegant theorems frequently arise experimentally as the result of a more or less unexpected stroke of good fortune, while their proofs lie so deeply embedded in the darkness that they elude all attempts and defeat the sharpest inquiries. Further, the connection between arithmetical truths which at first glance seem of widely different nature, is so close that one not infrequently has the good fortune to find a proof (in an entirely unexpected way and by means of quite another inquiry) of a truth which one greatly desired and sought in vain in spite of much effort. These truths are frequently of such a nature that they may be arrived at by many distinct paths and that the first paths to be discovered are not always the shortest. It is therefore a great pleasure after one has fruitlessly pondered over a truth and has later been able to prove it in a round-about way to find at last the simplest and most natural way to its proof.

The theorem which we have called in sec. 4 of the *Disquisitiones Arithmeticae* the fundamental theorem, because it contains in itself all the theory of quadratic residues, holds a prominent position among the questions of which we have spoken in the preceding paragraph. We must consider Legendre as the discoverer of this very elegant theorem, although special cases of it had previously been discovered by the celebrated geometers Euler and Lagrange. I will not pause here to enumerate the attempts of these men to furnish a proof; those who are interested may read the above mentioned work. An account of my own trials will suffice to confirm the assertions of the preceding paragraph. I discovered this theorem independently in 1795 at a time when I was totally ignorant of what had been achieved in higher arithmetic, and consequently had not the slightest aid from the literature on the subject. For a whole year this theorem tormented me and ab-
sorbed my greatest efforts until at last I obtained a proof given in the fourth section of the above-mentioned work. Later I ran across three other proofs which were built on entirely different principles. One of these I have already given in the fifth section, the others, which do not compare with it in elegance, I have reserved for future publication. Although these proofs leave nothing to be desired as regards rigor, they are derived from sources much too remote, except perhaps the first, which however proceeds with laborious arguments and is overloaded with extended operations. I do not hesitate to say that until now a natural proof has not been produced. I leave it to the authorities to judge whether the following proof which I have recently been fortunate enough to discover deserves this description [82], [220, pp. 112–118].

As mentioned earlier, it was the *Disquisitiones* that finally established number theory, or higher arithmetic as it was called then, as a full-fledged mathematical subject. One of those inspired by the new subject was Gotthold Eisenstein, who gives his view of the subject:

Already early in my youth I was attracted by the beauty of a subject which differs from other subjects not only in its content but, most importantly, in the nature and variety of its methods. In it, it is not enough to just lay out the consequences of a single idea in a long sequence of deductions; almost each step requires one to conquer new difficulties and apply new principles.

A little over fifty years ago, number theory consisted only of a collection of isolated facts, unknown to most mathematicians, and practiced only occasionally by a few, even though Euler already found in it leisure from his other activities. It was through Gauss and some of his successors that number theory has reached such heights that now it is not inferior to any other mathematical discipline in depth and breadth, and has had a fruitful influence on many of them. A school has arisen which counts the most eminent mathematical talents among its disciples, and which I too proudly am a part of, if only one of its lowliest [60, pp. 762–763].

Naturally, Eisenstein too worked on the QRL and higher laws. Among the many contributions he made to number theory during his very short life were several new proofs of the QRL, including a version of Gauss’s third proof that used a tool from geometry. Writing to a friend, he says:

I did not rest until I freed my geometric proof, which delighted you so much, and which also, incidentally, particularly pleased Jacobi, from the Lemma [of Gauss] on which it still depended, and it is now so simple that it can be communicated in a couple of lines [60, pp. 879–904].

It is this proof of Eisenstein’s that we shall study in our section on the proof of the quadratic reciprocity law, after reading Gauss’s own short original
statement of his version of the QRL in the *Disquisitiones*, and his discussion of previous work by others. While Eisenstein’s proof takes a bit more than “a couple of lines,” it is very accessible, quite ingenious, and beautiful in its elegance and economy. Gauss’s own proofs often tended to obscure the paths by which he obtained his insights, in stark contrast to Euler and Lagrange wanting to show us their paths. For instance, the opaqueness of motivation and context for many aspects of Gauss’s third proof of the QRL even make it hard to see that Eisenstein’s geometric proof apparently evolved from it (see [148, 149] for a comparison of the Gauss and Eisenstein proofs).

Since the time of Gauss, many different proofs of the QRL have been given and its role has evolved with the subject itself. (See [11] for a comprehensive review of different proofs of the QRL.) In fact, together with the Pythagorean theorem, the QRL probably qualifies as the theorem with the largest collection of different proofs to its name (and which seems to be growing; see, e.g., [90]). The reader might wonder why mathematicians would bother re-proving over and over again something already known. One could give a number of technical answers to this question, but the likely essence is that, like a complex and challenging mountain peak, it provides many possible routes for an ascent, each with its unique difficulties and rewards. It appears in many different guises, and its modern formulations are hardly recognizable. It is now properly a result that is formulated in abstract algebra terms as part of a subject called class field theory. And the theory of quadratic forms is now intimately connected with the theory of quadratic number fields. In fact we can see in our excerpts from Lagrange and Gauss on quadratic forms that mathematics was already changing significantly, from limited concrete problems to a more global, structurally oriented, and abstract approach. Gauss, in many ways, opened the door from classical to modern mathematics. In our final section, we shall read a bit from Gauss’s development in his *Disquisitiones Arithmeticae* of a modern theory of quadratic forms, to see how the subject developed as it entered the nineteenth century, when modern abstract algebra would transform much of mathematics.

Gauss considered number theory the *queen of the mathematical sciences*, and for the last two hundred years it has stood as one of the most pure and abstract disciplines, fundamental to our understanding of the mathematical world. At the same time, number theory seemed to be totally removed from the concerns of everyday life. In his famous *A Mathematician’s Apology*, the distinguished British mathematician G. H. Hardy (1877–1947) opines:

It is undeniable that a good deal of elementary mathematics ... has considerable practical utility. These parts of mathematics are, on the whole, rather dull; they are just the parts which have least aesthetic value. The “real” mathematics of the “real” mathematicians, the mathematics of Fermat and Euler and Gauss and Abel and Riemann, is almost wholly “useless” (and this is as true of “applied” as of “pure” mathematics). It is not possible to justify the life of any
genuine professional mathematician on the ground of the “utility” of his work [107, pp. 119–120].

Poor Hardy would be in for quite a surprise had he lived just a little longer. Ironically, in the last twenty-five years, number theory in general, and the theory of quadratic residues in particular, has found its way into our daily lives in some of the most surprising ways. So-called public key cryptography was invented in 1978 [195] as a means to exchange encrypted messages without having to exchange decryption keys first. The subsequent emergence of the World Wide Web and the ensuing revolution in commerce and information exchange made public key cryptography essential for the protection of information traveling over the Internet. The encryption key in this scheme is based on the product of two prime numbers (and, interestingly, on an application of Fermat’s little theorem, which is included in the Appendix). The product is made public and the two primes are kept secret. Anyone can encrypt, but only the person who knows the two primes can decrypt. The security of the method relies on the fact that the factoring of integers into their prime factors is computationally very expensive (at least no one seems to know how to factor cheaply, i.e., quickly). Given the present state of computing, it is essentially impossible to factor a product of two prime numbers of approximately 150 digits each into its factors. Large-scale application of this process and ever faster computers require a constant supply of ever larger prime numbers, or at least numbers that are prime “for all practical purposes.” A generalization of the QRL is at the heart of one of the most commonly used probabilistic primality tests [229, Chapter 4.5]. Somewhat more esoteric uses of the theory of quadratic residues, such as for the design of concert hall ceilings, can be found in [203, Chapter 15].

At the end of this chapter, the reader familiar with the topics discussed will surely complain, and justly so, that many important related topics have not been mentioned. Pell’s equation does not appear, continued fractions are completely absent, no discussion of a modern field-theoretic presentation of quadratic form theory is given, and many more topics are left unmentioned. The choices of what to include were guided by space considerations, as well as the background and motivation of the intended audience of this book. The reader interested in a more detailed discussion of issues raised by the work of Lagrange and Legendre can consult the excellent source [245]. For a reader with some background in abstract algebra we recommend [25] for a bird’s eye view of quadratic form theory, as seen from the vantage point of quadratic number fields, as well as the historically motivated treatment [200]. And, of course, there is [102], mentioned earlier.

Exercise 4.1. Read about the periodic law in [177, vol. 2, pp. 910–932]. In 1829, well before Dmitry Mendeleyev (1834–1907) began arranging the elements to produce a periodic table, Johann W. Döbereiner discovered, among the elements then known, triads of similar elements: for example, lithium (Li, atomic weight 6.9), sodium (Na, 23.0) and potassium (K, 39.1). What is striking is that the atomic weight of sodium is the average of those of lithium
and potassium. We now know that these are the elements 3, 11, and 19 in the periodic table. Another triad noticed by him is chlorine (Cl), bromine (Br), and iodine (I). In mathematics, in the same spirit, there is a triad of primes: 3, 5, and 7. We pose the following questions for exploration. Are there any other triads of primes? What about the pattern 11, 13, 17, and 19? When does such a prime pattern occur again? Does either pattern occur infinitely often?

**Exercise 4.2.** Prove the fundamental theorem of arithmetic, or look up a proof in a book on elementary number theory, e.g., [27].

**Exercise 4.3.** Show that if a prime divides a product, then it divides one of its factors.

**Exercise 4.4.** Find the theorem on the infinitude of primes in Euclid’s *Elements* [61] and compare his proof with the sketch given in this section.

**Exercise 4.5.** Look up the sieve of Eratosthenes and find the first 25 primes. Notice the irregular and elusive spacing of these first few primes. Do you see any patterns?

**Exercise 4.6.** Problem 29 in Book IV of Diophantus’s *Arithmetica* states, “To find four square numbers such that their sum added to the sum of their sides makes a given number.” Diophantus provides the following solution (by way of a numerical example) [109].

\[
\text{Given the number } 12. \text{ Now } x^2 + x + 1/4 = \text{ a square. Therefore the sum of four squares } + \text{ the sum of their sides } +1 = \text{ the sum of four other squares } = 13, \text{ by hypothesis. Therefore we have to divide 13 into four squares; then, if we subtract } 1/2 \text{ from each of their sides, we shall have the sides of the required squares. Now }
\]

\[
13 = 4 + 9 = \left( \frac{64}{25} + \frac{36}{25} \right) + \left( \frac{144}{25} + \frac{81}{25} \right),
\]

and the sides of the required squares are

\[
11/10, \quad 7/10, \quad 19/10, \quad 13/10,
\]

the squares themselves being

\[
121/100, \quad 49/100, \quad 361/100, \quad 169/100.
\]

Use Diophantus’s example to construct a more general solution, one that applies whenever the given number plus one is a sum of two rational squares. Hint: Notice how Diophantus’s illustration shows us how to write any rational square as a sum of two rational squares, by paying attention to the role of the 25.
Exercise 4.7. Show that if \( n \) is a product of two integers each of which is a sum of two squares, then \( n \) can be written as a sum of two squares in two different ways. (Hint: use the hint in Exercise 4.8.)

Exercise 4.8. Show that if \( m \) and \( n \) are whole numbers, both of the form \( x^2 + ay^2 \), then \( mn \) is also of this form. Hint: Verify and use “Brahmagupta’s identity”

\[
(x^2 + ay^2)(z^2 + aw^2) = (xz \pm ayw)^2 + a(xw \mp yz)^2.
\]

Exercise 4.9. Show the converse of Fermat’s claims made to Digby. In other words, show in each case \( a = 1, 2, 3 \) that any odd prime represented by the given quadratic form \( x^2 + ay^2 \) must belong to the claimed arithmetic progressions.

Exercise 4.10. Calculate the values of \( \left( \frac{a}{11} \right) \) for all \( a = 1, \ldots, 10 \), by both the methods suggested in the illustration in the text. Hint: To calculate whether \( a^{n+1} \) is congruent to 1 or \(-1\) in each case, use everything you know about arithmetic modulo \( p \) to shorten your calculation (see the Appendix). You should never have to actually work with very large numbers.

Exercise 4.11. Make an array whose rows and columns are labeled by the first ten odd prime numbers 3, 5, 7, 11, \ldots, 31. In position \((p, q)\) put the value of the Legendre symbol \( \left( \frac{p}{q} \right) \). Use the entries of this array to conjecture a relationship between \( \left( \frac{p}{q} \right) \) and the “reciprocal” symbol \( \left( \frac{q}{p} \right) \). Before you can do all this you will need to find quadratic residues. Make an auxiliary table of squares of integers modulo \( p \). What additional properties of quadratic residues do you discover?

Exercise 4.12. Reinterpret the equality of the quadratic reciprocity law as saying whether \( \left( \frac{p}{q} \right) \) and \( \left( \frac{q}{p} \right) \) agree or disagree, depending on whether each of \( p, q \) has the form \( 4n + 1 \) or \( 4n + 3 \).

Exercise 4.13. Prove the first part of the supplementary theorem.

Exercise 4.14. Let \( p \) be an odd prime, and \( a, b \) integers that are relatively prime to \( p \). Prove that

\[
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right).
\]

Hint: Use Euler’s criterion.

Exercise 4.15. Calculate \( \left( \frac{-6}{101} \right) \) using Euler’s criterion by doing a calculation modulo 101. How does this compare in difficulty with the calculation in the text using the quadratic reciprocity law?
Exercise 4.16. Calculate various Legendre symbols by repeatedly using only the QRL, the supplementary theorem, and the multiplicativity of the Legendre symbol. You should never have to check a quadratic residue by brute force or Euler’s criterion.

Exercise 4.17. Complete the verification in the text that the odd primes not dividing 6 for which \(-6\) is a quadratic residue are precisely those in the four arithmetic progressions given by Euler.

Exercise 4.18. In the next section we shall read Euler’s claim in his paper of 1744 that the nontrivial prime divisors of numbers of the form \(x^2 - 5y^2\) are precisely those of the form \(10m \pm 1\), and that the nontrivial prime divisors of numbers of the form \(x^2 - 7y^2\) are precisely those of the form \(28m \pm 1, 28m \pm 3, 28m \pm 9\). Use the QRL to verify this.

Exercise 4.19. Find all solutions of the congruence

\[x^2 + x + 1 \equiv 0 \pmod{31}.

4.2 Euler Discovers Patterns for Prime Divisors of Quadratic Forms

Without doubt Leonhard Euler was one of the world’s mathematical giants, whose work profoundly transformed mathematics. He made extensive contributions to many mathematical subjects, including number theory, and was so prolific that the publication of his collected works, begun in 1911, is still underway, and is expected to fill more than 100 large volumes.

Born in Basel, Switzerland, in 1707, Euler’s mathematical career spanned almost the whole eighteenth century, and he was at the heart of all its great accomplishments. His father, a Protestant minister interested in mathematics, was responsible for his son’s earliest education. Later, Euler attended the Gymnasium in Basel, a high school that did not provide instruction in mathematics, however. At fourteen, Euler entered the University of Basel, where Johann Bernoulli (1667–1748) had succeeded his brother Jakob (1654–1705) in the chair of mathematics. Though Bernoulli declined to give Euler private lessons (and Bernoulli’s public lectures at the university were limited to elementary mathematics), he was willing to help Euler with difficulties in the mathematical texts that Euler studied on his own.

Euler received a degree in philosophy and joined the Department of Theology in 1723, but his studies in theology, Greek, and Hebrew suffered from his devotion to mathematics. Eventually he gave up the idea of becoming a minister. In autumn of 1725, Johann Bernoulli’s sons Nikolaus (1687–1759) and Daniel (1700–1782) went to Russia to join the newly organized St. Petersburg Academy of Sciences; at their behest, the following year the academy invited Euler to serve as adjunct of physiology, the only position available at