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

the time. Euler accepted, arriving in St. Petersburg in May of 1727. In spite of having been invited to study physiology, soon after his arrival he was given the opportunity to work in his true field of mathematics. During fourteen years in St. Petersburg, Euler published fifty-five works, making brilliant discoveries in such fields as analysis, number theory, and mechanics.

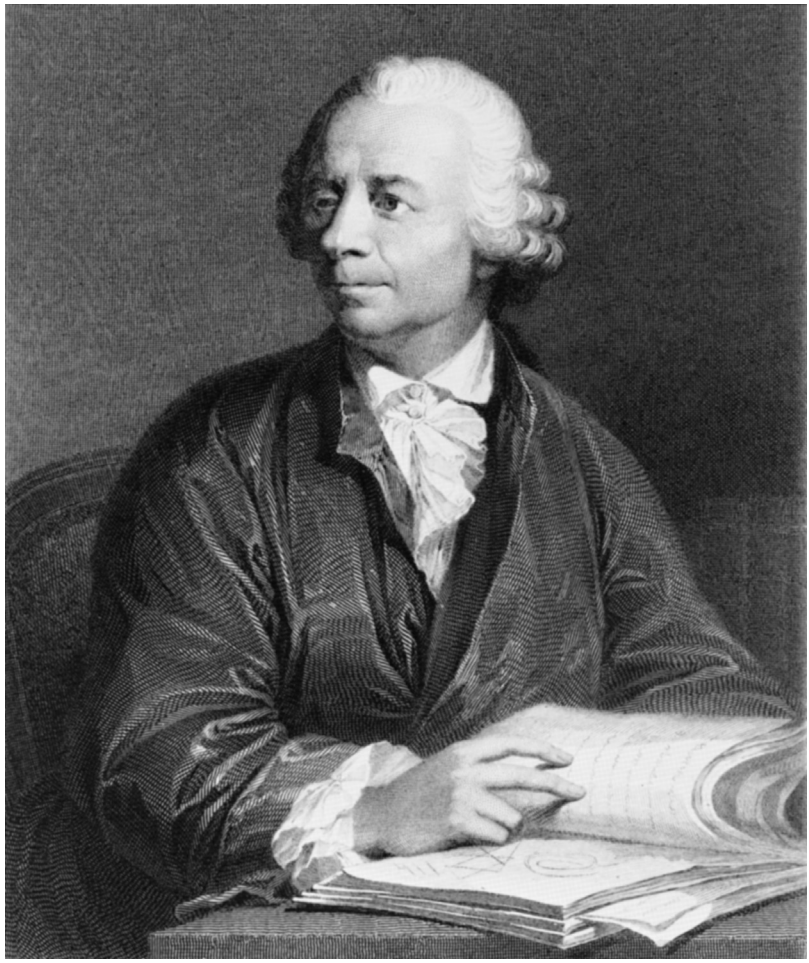

Photo 4.3. Euler.

In 1740, Euler was invited to join the Berlin Academy of Sciences and accepted, since the political situation in St. Petersburg had deteriorated by that time. During his tenure in Berlin, he remained an active member of the St. Petersburg Academy as well, publishing prolifically in both academies. In 1766, Euler returned to St. Petersburg, where he remained for the rest of his

life. Though he went blind shortly after his return, he was able to continue his work with the aid of assistants; indeed, he actually increased his output.

When Euler received a letter from Christian Goldbach (1690–1764) in December 1729, early in his first St. Petersburg period, little did he know that it was going to instill a new passion in him that would last the rest of his life. Continuing an initial exchange of letters earlier that fall, Goldbach mentions in a postscript the assertion of Fermat that every number of the form $2^{2^n}+1$ is a prime, and that nobody seemed to have a proof for it [65, p. 10]. Euler began to read Fermat's works and embarked on a long journey of providing proofs for and generalizing Fermat's number-theoretic insights. In 1735 he found the counterexample $2^{2^5}+1$ to the conjecture that initially aroused his interest. (What are the factors of this number, and how might Euler have discovered this [245]?)

Goldbach was a well-traveled man whose main intellectual interests were languages and mathematics. In 1725 he became professor of mathematics and history at St. Petersburg, and in 1728 went to Moscow as tutor to Tsar Peter II. He knew many of the distinguished mathematicians of his time, including Nicolas and Daniel Bernoulli, who obtained their appointments to the academy in St. Petersburg thanks to his efforts, leading in turn to Euler's appointment there. Goldbach and Euler became lifelong friends and their correspondence provides the most vivid record of Euler's number-theoretic legacy, more so even than his published papers. Today Goldbach is best remembered for the conjecture, emerging from correspondence with Euler in 1742, that every even integer greater than 2 can be represented as the sum of two primes. This is still a famous open problem today.[7]

As discussed in the introduction, one of the many trails on Euler's journeys into questions raised by Fermat led him to look for patterns in the prime divisors of quadratic forms. By 1744 he could state some amazing patterns by "induction," i.e., extrapolation from experimental evidence (distinct from the proof technique we call the principle of "mathematical induction" today). He published his claims, without proof, in the paper *Theoremata circa divisores numerorum in hac forma contentorum* $paa \pm qbb$ [66, v. 2, pp. 194–222] (Theorems about the divisors of numbers expressed in the form $paa \pm qbb$). For each of a large variety of quadratic forms, he presented a list of arithmetic progressions whose primes he claimed were precisely all the nontrivial prime divisors of the quadratic form, i.e., solutions of the divisor problem. Most of the quadratic forms he considered were of the type a^2+Nb^2 or a^2-Nb^2, where N is a particular positive integer, usually prime. We shall present just a few of Euler's many examples, followed by excerpts from his extensive comments, in which he describes the patterns he noticed in a way that completely determines all the arithmetic progressions [57]. In his comments we will later recognize the

[7] Goldbach's conjecture was mentioned by David Hilbert as part of his famous problem about the distribution of prime numbers (recall the footnote in the introduction about Hilbert's problems).

discovery of the essence of quadratic reciprocity. The two cases $a^2 + Nb^2$ and $a^2 - Nb^2$ (recall $N > 0$) presented quite distinct patterns for Euler to decipher. Of course the claims we have seen by Fermat were all about forms of the type $a^2 + Nb^2$. While for future discussion we present some examples from both cases below, at this point in our story we will focus largely on the case $a^2 - Nb^2$, since it will lead to the simplest expression of patterns, and most directly to the quadratic reciprocity law as our story progresses. We strongly encourage the reader to pretend to be Euler, and try to conjecture exactly which arithmetic progressions are contained in Euler's experimental data for $a^2 - Nb^2$ (at least for N prime), before reading his comments spelling it all out (Exercise 4.20).

Leonhard Euler, from
Theorems
about the divisors of numbers expressed in the form $paa \pm qbb$

THEOREM 10

Numbers of the form $aa + 5bb$ have prime divisors that are always either 2 or 5 or contained in one of the 4 forms $20m + 1$, $20m + 3$, $20m + 7$, $20m + 9$.

THEOREM 11

If a number $20m+1$, $20m+3$, $20m+9$, $20m+7$ is prime, then it follows that

$$20m + 1 = aa + 5bb, \quad 2\,(20m + 3) = aa + 5bb,$$
$$20m + 9 = aa + 5bb, \quad 2\,(20m + 7) = aa + 5bb.$$

THEOREM 12

No number contained in a sequence of the form $20m - 1$, $20m - 3$, $20m - 9$, $20m - 7$ can be a divisor of a number of the form $aa + 5bb$.

...

THEOREM 44

All prime divisors of the form $aa - 5bb$ are either 2 or 5 or contained

in either the formulas	or in the single one
$20m \pm 1, \quad 20m \pm 9$	$10m \pm 1.$

Every prime number of this form is also contained in the divisors of the form $aa - 5bb$.

THEOREM 45

All prime divisors of the form $aa - 7bb$ are either 2 or 7 or contained in one of the following formulas:

$$28m \pm 1, \quad 28m \pm 3, \quad 28m \pm 9;$$

all prime numbers contained in these formulas are also contained in the divisors of the form $aa - 7bb$.

THEOREM 46

All prime divisors of the form $aa - 11bb$ are either 2 or 11 or contained in one of the following formulas:

$$44m \pm 1, \quad 44m \pm 5, \quad 44m \pm 7, \quad 44m \pm 9, \quad 44m \pm 19;$$

all prime numbers contained in these formulas are also contained in the divisors of the form $aa - 11bb$, and this reciprocation holds also in all succeeding theorems. . . .

THEOREM 49

All prime divisors of the form $aa - 19bb$ are either 2 or 19 or contained in the following formulas:

$$\begin{array}{lll} 76m \pm 1, & 76m \pm 3, & 76m \pm 9, \\ 76m \pm 27, & 76m \pm 5, & 76m \pm 15, \\ 76m \pm 31, & 76m \pm 17, & 76m \pm 25. \end{array}$$

. . .

COMMENT 13

Therefore, all the prime divisors of the numbers expressed in the form $aa - Nbb$ are either 2 or the divisors of the number N or can be expressed in the form $4Nm \pm \alpha$. But for one of the divisors to be in the form of $4Nm + \alpha$, then $4Nm - \alpha$ will also be the form of one of the divisors; and so this is unlike the case of the form $aa + Nbb$; in which if $4Nm + \alpha$ will be a divisor, then $4Nm - \alpha$ can never express a divisor for the same form.

COMMENT 14

Having established therefore $4Nm \pm \alpha$ as the general form of the divisors of the numbers described by the expression $aa - Nbb$, the letters α generally will represent many numbers, always including the number one; truly then, because this conversation is about prime divisors, no α itself will be among the values of the number N nor any of the divisors of N. Then it is also apparent, all these values of α can be arranged to be made less than $2N$. For if $4Nm + 2N + b$ is a divisor, then by substituting $m - 1$ in place of m, the divisor will be $4Nm - (2N - b)$. Therefore the values of α itself will be odd numbers [relatively] prime to N, less than $2N$, and of all these numbers which are odd and prime to N and less than $2N$, it will be seen that only one half are suitable values for α; the remaining will exhibit a form, in which plainly no divisor may be contained. It is always certain to have just as many forms of divisors, as there are that are not, except for the single case where $N = 1$.

...

COMMENT 16

But just as the number one is always found among the values of α, so also any squared number which is [relatively] prime to $4N$ will supply a suitable value for α.

Let us see what we can glean from these comments on the case $a^2 - Nb^2$. Euler claims from his observations that the nontrivial prime divisors of $a^2 - Nb^2$ $(N > 0)$ are all those found in certain arithmetic progressions having period $4N$, and that these progressions always occur in matched pairs of the form $4Nm \pm \alpha$. (He comments that this is quite contrary to the forms $a^2 + Nb^2$ $(N > 0)$, for which the relevant progressions never occur in matched pairs.) He then points out that one can always arrange for $0 < \alpha < 2N$. Next Euler points out that since we are seeking prime divisors, only progressions $4Nm \pm \alpha$ in which α is odd and relatively prime to N need be considered. He then claims that among these restricted possibilities, exactly half of them will be "suitable," i.e., will be those containing precisely the prime divisors of $a^2 - Nb^2$. Finally, Euler says that square numbers relatively prime to $4N$ will always supply suitable values.

Let us examine all these claims in the example $N = 7$ from Theorem 45 above. According to Euler, to find the prime divisors of numbers of the form $a^2 - 7b^2$, we should first consider only progressions of the form $28m \pm \alpha$, where $0 < \alpha < 14$ and α is odd and relatively prime to 7. This leads us to the possible values 1, 3, 5, 9, 11, 13 for α. Euler says that exactly half of these will produce the suitable progressions, and moreover that squares relatively prime to 28 will always produce suitable progressions. We wonder, will squares produce all the suitable pairs of progressions?

To examine the progressions arising from squares relatively prime to 28, we begin by listing the squares of odd numbers not divisible by 7, i.e., 1, 9, 25, 81, 121, 169, etc., and then express each of them in the form $28m \pm \alpha$, where $0 < \alpha < 14$, in order to find a suitable α. Thus we have

$$\begin{aligned} 1 &= 28 \cdot 0 + 1, \;\; 169 = 28 \cdot 6 + 1, \\ 9 &= 28 \cdot 0 + 9, \;\; 121 = 28 \cdot 4 + 9, \\ 25 &= 28 \cdot 1 - 3, \;\; 81 = 28 \cdot 3 - 3, \;\; \text{etc.} \end{aligned}$$

So the values for α produced so far are 1, 9, 3. Notice that these are exactly the three pairs of progressions Euler listed in Theorem 45, and according to Euler this list is complete, since he says that only half of the possible list $1, 3, 5, 9, 11, 13$ for α will be suitable. Notice that the three suitable values for α did all actually arise from our list of squares, and in fact occurred right away, from the first three squares, with the values arising thereafter simply repeating with a certain pattern. Although Euler does not say so, he was surely aware of these facts in general. We shall leave it to the reader to verify these latter phenomena in some other examples, and then to prove that it

always happens this way: For N an odd prime, the first $\frac{N-1}{2}$ odd squares will produce $\frac{N-1}{2}$ distinct suitable values for α, and will thus, according to Euler's claims, produce all the suitable progressions (Exercises 4.21, 4.22). This means that Euler discovered (without proof) a complete solution to the problem of determining the forms (arithmetic progressions) of nontrivial prime divisors of $a^2 - Nb^2$ $(N > 0)$! Euler also gave an analogous description for nontrivial prime divisors of $a^2 + Nb^2$ $(N > 0)$, which he claimed similarly lie in certain arithmetic progressions with periodicity $4N$. We shall not present that description here, but it will emerge in our second Euler source.

Does this mean that Euler discovered the quadratic reciprocity law in 1744? Certainly it is not in the form stated in the introduction. But in hindsight we do see a strong glimmer of reciprocity here. Recall that in looking for prime divisors p of $a^2 - Nb^2$ (still always $N > 0$), we are asking whether N is a square modulo p. From Euler's claims we deduce that for N an odd prime, this happens precisely when p or $-p$, i.e., α or $-\alpha$, is itself a square modulo $4N$. Thus there is a "reciprocity" between N and p here, i.e., they exchange roles, from quadratic residue to modulus and vice versa, except that there is also an introduced $+$ or $-$ sign on p, and N gets multiplied by 4. The significance of all this will be clarified as we examine the evolution of the discovery of the quadratic reciprocity law in the hands of Euler's successors.

For almost another 40 years, Euler strove to prove his claims, and while he succeeded in a few special cases, especially those conjectured by Fermat, the general case eluded him. In the paper *Observationes circa divisionem quadratorum per numeros primos* (Observations on the Division of Squares by Prime Numbers) [66, v. 3, pp. 497–512], [232, pp. 40–46], presented to the St. Petersburg Academy in 1772, but not published until 1783, the year of his death, Euler did two important things. He gave proofs determining the quadratic character of -1 for all primes (this is the special case $a^2 + b^2$ of Euler's claims about divisors of quadratic forms, and was one of the results claimed by Fermat), and then gave a clear statement of his final vision of the role reversal between quadratic residues and moduli. Our second source consists of relevant excerpts from this paper.

Euler begins the paper by developing various basic properties of quadratic residues, some of which we will state here and leave to the reader to prove in exercises. By this time Euler's view had evolved considerably, and in particular he was thinking and writing partly in terms of quadratic residues. But he still lacked the full benefits of thinking and writing in terms of congruences, which we will rely on from our Appendix.

Key properties of quadratic residues. For p an odd prime:

1. There are exactly $\frac{p-1}{2}$ (nonzero) quadratic residues $\bmod p$ (by which we mean to count from among the equivalence classes modulo p not containing zero), obtained by squaring the numbers $1, \ldots, \frac{p-1}{2}$. Thus there are also $\frac{p-1}{2}$ (nonzero) nonquadratic residues $\bmod p$, since there is a total of $p - 1$ nonzero equivalence classes modulo p (Exercise 4.23).

2. Recall from the Appendix that every number that is nonzero mod p has a *reciprocal* mod p, i.e., we can divide by it mod p. Then (Exercise 4.24):
   a) A product or quotient of two quadratic residues mod p is also a quadratic residue mod p.
   b) A product or quotient of a quadratic residue with a quadratic nonresidue is a quadratic nonresidue.
   c) A product or quotient of two quadratic nonresidues is a quadratic residue.

Now we are ready to read from Euler's paper, with first a warning on three important matters of notation. Euler will use P for the prime divisor (modulus) in question, utilizing p for something else. He almost always uses the word *residue* to refer to what we call the *remainder*, i.e., a number congruent to P but chosen or restricted to be in the range from 0 to $P-1$. Finally, in this particular paper he always means "quadratic residue" when he says *residue*, i.e., the remainders only of squares mod P.

Leonhard Euler, from
Observations on the Division of Squares by Prime Numbers

23. *Theorem 4. If the divisor P is of the form $4q+3$, then -1 or $P-1$ is certainly a nonresidue.*

Demonstration. When we write $P = 2p+1$, then $p = 2q+1$, an odd number. Hence the number of all [quadratic] residues will be odd. If -1 were to appear in the sequence of residues, then to every residue α would correspond another residue $-\alpha$, and the sequence of residues could be written as follows:

$$+1,\ +\alpha,\ +\beta,\ +\gamma,\ +\delta,\ \text{etc.},$$

$$-1,\ -\alpha,\ -\beta,\ -\gamma,\ -\delta,\ \text{etc.},$$

and the number of residues would be even. But since this number is certainly odd, it is impossible that -1 or $P-1$ should appear in the sequence of residues; hence it belongs to the sequence of nonresidues ...

30. *Theorem 5. If the divisor P is a prime of the form $4q+1$, then the number -1 or $P-1$ is certainly a residue. ...*

Conclusion. These ... theorems,[8] of which the demonstration from now on is desired, can be nicely formulated as follows:

Let s be some prime number, let only the odd squares 1, 9, 25, 49, etc. be divided by the divisor $4s$, and let the residues be noted, which will all be of the form $4q+1$, of which any may be denoted by the letter α, and the other numbers

[8] That is, several theorems succeeding number 30.

of the form $4q+1$, which do not appear among the residues, be denoted by some letter $\mathfrak{U}$, then we shall have

divisor a prime number $[P]$ of the form	then [modulo P]
$4ns+\alpha$	$+s$ is a residue, and $-s$ is a residue;
$4ns-\alpha$	$+s$ is a residue, and $-s$ is a nonresidue;
$4ns+\mathfrak{U}$	$+s$ is a nonresidue, and $-s$ is a nonresidue;
$4ns-\mathfrak{U}$	$+s$ is a nonresidue, and $-s$ is a residue.

The text is quite detailed and requires only a little explanation. In Theorem 4 the reader should confirm why all the residues listed and counted are distinct. In proving Theorem 5 Euler matches residues with their reciprocals, rather than their negatives as in Theorem 4, and we leave this interesting proof to the reader (Exercise 4.25). As we explained when discussing the divisor problem in the introduction, Theorem 4 ensures that no sum of two relatively prime squares can have a prime divisor of the form $4q+3$, and Theorem 5 tells us that every prime of the form $4q+1$ is a divisor of a sum of two relatively prime squares. Recall that in the language of quadratic residues, this solution to the divisor problem for $a=1$ proves the first part of the supplementary theorem to the quadratic reciprocity law stated in the introduction (Exercise 4.26):

The quadratic character of negative one. -1 is a quadratic residue for every prime of form $4q+1$, but not for any prime of form $4q+3$.

This is an extremely important result, and we shall find it useful shortly. In the full text, Euler comments after Theorem 5 that he can use it to solve the harder problem of representation of the quadratic form in this case, the one claimed by Fermat: Every prime of the form $4q+1$ actually is a sum of two squares. As discussed in the introduction, to do this Euler also needed a descent result, that every nontrivial divisor of a sum of two relatively prime squares is again a sum of two squares. We shall have this in hand shortly, from the source by Lagrange that we will read next.

Finally, let us look at the four statements in Euler's *Conclusion*. While the notation is very different from his earlier paper[9] of 1744, what Euler writes here in 1772 is just a crystallized statement of what he already claimed earlier, now phrased partly in the language of (quadratic) residues, a major step toward the congruence viewpoint. This latter paper was Euler's final formulation of the patterns he saw in quadratic residues modulo prime divisors, which will metamorphose into the modern formulation of quadratic reciprocity. The statements about $+s$ above correspond to the forms a^2-Nb^2 $(N>0)$ we read about in detail in the earlier paper, while the statements about $-s$ correspond

[9] From the 1744 paper to the 1772 paper, his notation changes as follows: $N \to s$, $m \to n$. And α has a subtly different meaning: while in the earlier paper he arranges for α always to satisfy $|\pm\alpha| < 2N$, in this later paper he chooses $0 < \alpha < 4s$, i.e., α becomes, as he says, simply the remainder of an odd square upon division by $4s$.

to the forms $a^2 + Nb^2$ $(N > 0)$, of which we presented only a single excerpt. We leave it to the reader to confirm detailed agreement between what Euler claims in the papers of 1744 and 1772 (Exercises 4.27, 4.28). Interestingly, using what we know about the quadratic character of -1, and the key property above about products of quadratic residues and nonresidues, it is easy to see that Euler's statements about $+s$ are equivalent to those about $-s$ (Exercise 4.29), so the distinction between the nature of divisors of the forms $a^2 - Nb^2$ and $a^2 + Nb^2$ is now explained.

We make one last comment about Euler's *Conclusion*. At first it appears from his wording that Euler is making claims in only one direction, namely that $+s$ $(-s)$ is or is not a quadratic residue modulo prime divisors of certain types, but not necessarily solely of these types. However, the reader may check that the four prime divisor types he lists actually encompass, mutually exclusively, all odd primes. Thus his four claims actually cover all possibilities, and so provide a complete characterization of the relationship between types of prime divisors and quadratic residues modulo those divisors.

Exercise 4.20. Looking just at the lists of arithmetic progressions Euler presents in his Theorems 44, 45, 46, and 49, conjecture a general description of exactly what those arithmetic progressions might be for any quadratic form $a^2 - Nb^2$ where N is an odd prime. Hint: Which values of α appear for all N?

Exercise 4.21. Check Euler's general claims in his Comments 13, 14, 16, and our further observations, against his Theorems 46 and 49 in the same way we did for $N = 7$ against Theorem 45. In other words, carry out his prescription for finding the arithmetic progressions providing all prime divisors of $a^2 - 11b^2$ and $a^2 - 19b^2$, and see whether the suitable progressions are all provided by the first $\frac{N-1}{2}$ odd squares.

Exercise 4.22. Prove that for N an odd prime, the first $\frac{N-1}{2}$ odd squares provide distinct values of α in Euler's analysis. (Be careful: sometimes a square produces α modulo $4N$, sometimes $-\alpha$.) Thus, according to Euler, the odd squares provide all the suitable values.

Exercise 4.23. Prove that for p an odd prime, there are exactly $\frac{p-1}{2}$ nonzero quadratic residues $\bmod p$ (by which we mean to count among the equivalence classes modulo p not containing zero), obtained by squaring the numbers $1, \ldots, \frac{p-1}{2}$. Thus there are also $\frac{p-1}{2}$ nonzero nonquadratic residues $\bmod p$, since there is a total of $p - 1$ nonzero equivalence classes modulo p.

Exercise 4.24. Prove that:

1. A product or quotient of quadratic residues $\bmod p$ is also a quadratic residue $\bmod p$.
2. A product or quotient of a quadratic residue with a quadratic nonresidue is a quadratic nonresidue.
3. A product or quotient of two quadratic nonresidues is a quadratic residue. (Hint: Count the possible products of a nonresidue with all the residues.)

Exercise 4.25. Give a proof of Euler's Theorem 5. (Hint: First show that 1 and -1 are the only remainders that are their own reciprocals mod p. Then use the idea of his proof of Theorem 4, but match numbers with their reciprocals instead of their negatives.)

Exercise 4.26. Prove the first part of the supplementary theorem to the quadratic reciprocity law stated in the introduction.

Exercise 4.27. Compare Euler's claims in his *Conclusion* of 1772 about the quadratic character of $+s$ ($s > 0$) with what we read in Comments 13, 14, 16 of his paper of 1744. Verify that they agree.

Exercise 4.28. Compare Euler's claims in his *Conclusion* of 1772 about the quadratic character of $-s$ with what he claims in his paper of 1744. You will have to find the relevant parts of the earlier paper, and you may need to read some Latin. Verify that they agree.

Exercise 4.29. Show that Euler's claims for $+s$ are equivalent to his claims for $-s$, using the characterization of the quadratic character of -1 that he just proved, along with the key property about multiplicativity of quadratic residues and nonresidues proven in Exercise 4.24.

4.3 Lagrange Develops a Theory of Quadratic Forms and Divisors

Even though the second half of the eighteenth century was not very favorably disposed toward pure mathematics, in the 1770s the torch of studying quadratic reciprocity was being passed to two younger men, Lagrange and Legendre. Since the time of Newton and Leibniz in the late seventeenth century, the geometers, as mathematicians called themselves, were primarily busy working on the development of the calculus, not number theory. Here too Euler's genius and phenomenal output defined the central problems and lines of development. The astonishing practical applications of the new theory left little time to catch one's breath and worry about the somewhat shaky foundations on which people juggled derivatives, integrals, and infinite series. But this shaky foundation was adequate to most eighteenth-century developments, and there was much political and economic gain from solving applied problems, such as accurate navigation at sea (see our chapter on curvature). Thus, there was neither livelihood nor prestige to be found in working primarily on problems such as the nature of patterns in prime numbers.

To be a professional mathematician in the eighteenth century meant to have a wealthy sponsor and be part of the scientific academy of a country, or be independently wealthy. There was no instruction in higher mathematics at universities, leaving only private tutors if one wanted to be led to the edge of mathematical research. That is how Euler earned a living for a while, and so did several of the Bernoullis. The two leading academies during the second half