Eisenstein's Misunderstood Geometric Proof of the Quadratic Reciprocity Theorem

Reinhard C. Laubenbacher
David J. Pengelley
Department of Mathematical Sciences
New Mexico State University
Las Cruces, NM 88003

[College Mathematics Journal **25** (1994), 29-34]

1 Introduction

The Quadratic Reciprocity Theorem has played a central role in the development of number theory, and formed the first deep law governing prime numbers. Its numerous proofs from many distinct points of view testify to its position at the heart of the subject. The theorem was discovered by Euler, and restated by Legendre in terms of the symbol now bearing his name, but was first proven by Gauss. The eight different proofs Gauss published in the early 1800s, for what he called the Fundamental Theorem, were followed by dozens more before the century was over, including four given by Gotthold Eisenstein in the years 1844–45. Our aim is to take a new look at Eisenstein's geometric proof, in which he presents a particularly beautiful and economical adaptation of Gauss' third proof, and to draw attention to all the advantages of his proof over Gauss', most of which have apparently heretofore been overlooked.

[0]The authors would like to thank Keith Dennis for his assistance in locating sources, Tom Hoeksema and Carol Walker for their enthusiastic support of the Honors courses which led to this work, and Joe Zund for telling us where to look.

It is hard to imagine today the sensation caused by Eisenstein when he burst upon the mathematical world. In the autumn of 1843, at age twenty, this self-taught mathematician had barely received his high school certificate and entered the Friedrich-Wilhelms University of Berlin, when he produced a flood of publications, instantly making him one of the leading mathematicians of the early nineteenth century. On July 14, 1844, Gauss wrote to C. Gerling, saying "I have recently made the aquaintance of a young mathematician, Eisenstein from Berlin, who came here with a letter of recommendation from Humboldt. This man, who is still very young, exhibits *very* excellent talent, and will certainly achieve great things" [4]. In 1844 Eisenstein contributed no less than 16 of the 27 mathematical articles in Volume 27 of Crelle's Journal, and by his third semester as a student he had received an honorary doctorate from Breslau [9]. Both Gauss and the great scientist and explorer Alexander von Humboldt made great efforts, for the most part in vain, to obtain recognition and financial security for the impoverished Eisenstein. Gauss wrote to Humboldt that Eisenstein's talent was "that which nature bestows upon only a few in each century" [3]. He did obtain a position as a Privatdozent (unsalaried lecturer) at the University in Berlin, and was eventually admitted to the Berlin Academy of Sciences in early 1852. But by then his lifelong poor health had seriously deteriorated, and later that same year he died, aged 29, of tuberculosis. Gotthold Eisenstein stands with Abel and Galois as another nineteenth century mathematical genius with a tragic and short life [3, 9].

Eisenstein's geometric proof appeared in Crelle's Journal under the title *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste* [5]. It is intimately connected to Gauss' third proof (published in [6] and translated in [10]). Many expositions of Eisenstein's proof, beginning with [1, 2], have observed only one of its three geometric aspects, and have overlooked the other important differences between the two proofs. The result has been a failure to recognize and fully appreciate all the ways in which Eisenstein greatly streamlines and illuminates Gauss' proof, and thereby reveals its essence. For instance, Gauss' third proof is based on a result known as Gauss' Lemma, and Eisenstein was particularly pleased with a shortcut he found to avoid the technicalities involved in applying it:

> "I did not rest until I freed my geometric proof ... from the Lemma on which it still depended, and it is now so simple that

it can be communicated in a couple of lines." [7, pp. 173–4]

We believe that the elegance of Eisenstein's proof deserves wide appreciation, and we present it here along with a comparison to Gauss' third proof.

2 Eisenstein's Proof

To set the stage, we recall a few consequences of the fact that the residue classes modulo a prime p form a field Z_p. Fermat's Little Theorem, that $b^{p-1} \equiv 1 \pmod{p}$ for any integer b not divisible by p, holds because the nonzero residue classes form a (cyclic) group of order $p-1$ under multiplication. When p is odd, the squaring map $x \to x^2$ has kernel $\{-1, 1\}$, so its image, the squares or *quadratic residues* modulo p, form a subgroup of order $\frac{p-1}{2}$ and the nonresidues form its coset. The quadratic character of a residue class $b \in Z_p^*$ is specified by the Legendre symbol: $\left(\frac{b}{p}\right) = 1$ if b is a quadratic residue mod p and $\left(\frac{b}{p}\right) = -1$ if not. From $\left(b^{\frac{p-1}{2}}\right)^2 = 1$, it follows that $b^{\frac{p-1}{2}} = \pm 1$ for any $b \in Z_p^*$. But if $b = c^2$, then $b^{\frac{p-1}{2}} = c^{p-1} = 1$, so the quadratic residues are all roots of the polynomial $x^{\frac{p-1}{2}} = 1$. Since this polynomial can have no more than $\frac{p-1}{2}$ roots in the field Z_p, we conclude that its roots are exactly the quadratic residues. That is, we have *Euler's Criterion*: $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}}$ for any integer b not divisible by p.

The Quadratic Reciprocity Theorem compares the quadratic character of two primes with respect to each other.

Quadratic Reciprocity Theorem *If p and q are distinct odd primes, then*

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

Here is Eisenstein's proof, closely following both his own language and notation (which he conveniently and successfully abuses).

Consider the set $a = 2, 4, 6, \ldots, p-1$. Let r denote the remainder $\pmod{p}$ of an arbitrary multiple qa. Then it is apparent that the list of numbers $(-1)^r r$ agrees with the list of numbers a, up to multiples of p. (For

clearly each of the numbers $(-1)^r r$ has even least positive residue, and if there were duplication among these residues, e.g.

$$(-1)^{qa} qa \equiv (-1)^{qa'} qa',$$

then $a \equiv \pm a'$. Since the a's are distinct, it follows that $a + a' \equiv 0$, which cannot occur since $0 < a + a' < 2p$ and $a + a'$ is even.) Thus

$$q^{\frac{p-1}{2}} \prod a \equiv \prod r \pmod{p} \qquad \text{and} \qquad \prod a \equiv (-1)^{\sum r} \prod r \pmod{p},$$

from which it follows that $q^{\frac{p-1}{2}} \equiv (-1)^{\sum r} \pmod{p}$. Recalling Euler's Criterion that $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \pmod{p}$, this produces

$$\left(\frac{q}{p}\right) = (-1)^{\sum r}, \tag{1}$$

so one may focus solely on the parity of this exponent. Clearly

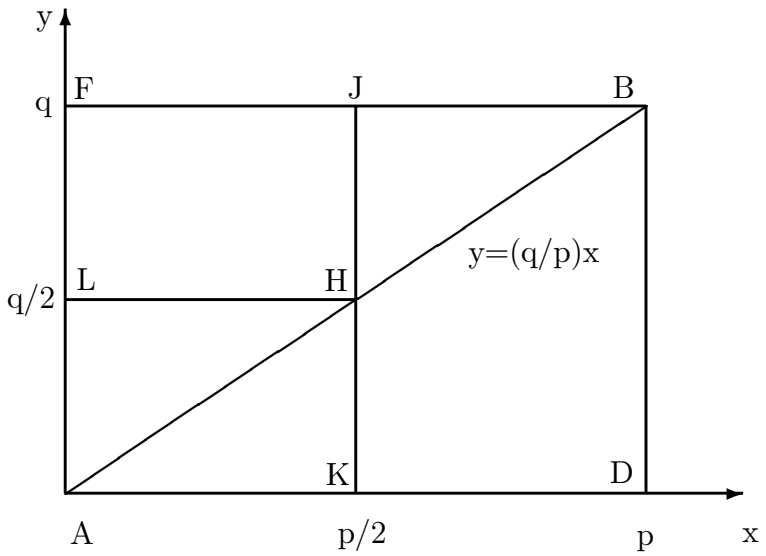
$$\sum qa = p \sum \left[\frac{qa}{p}\right] + \sum r, \tag{2}$$

where $[\ ]$ is the greatest integer function. Since the elements a are all even, and p is odd, it follows that $\sum r \equiv \sum \left[\frac{qa}{p}\right] \pmod{2}$, and thus

$$\left(\frac{q}{p}\right) = (-1)^{\sum \left[\frac{qa}{p}\right]}.$$

(Here Eisenstein remarks that since up to this point q need not have been an odd prime, but merely a number relatively prime to p, one can easily obtain the Ergänzungssatz $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ from the above formula. This we leave as an exercise for the reader.)

Eisenstein now uses a geometric representation of the exponent in this last equation to transform it twice while retaining its parity: This exponent is precisely the number of integer lattice points with even abscissas lying in the interior of triangle ABD in the Figure (note that no lattice points lie on the line AB). Consider an even abscissa $a > p/2$. Since the number of



lattice points on each abscissa in the interior of rectangle $ADBF$ is even, the number $\left[\frac{qa}{p}\right]$ of lattice points on the abscissa below AB has the same parity as the number of lattice points above AB. This in turn is the same as the number of points lying below AB on the odd abscissa $p-a$. This one-to-one correspondence between even abscissas in triangle BHJ and odd abscissas in AHK now implies that $\sum\left[\frac{qa}{p}\right] \equiv \mu \pmod 2$, where μ is the number of points inside triangle AHK, and thus $\left(\frac{q}{p}\right) = (-1)^{\mu}$.

Reversing the roles of p and q yields $\left(\frac{p}{q}\right) = (-1)^{\nu}$, where ν is the number of points inside triangle AHL. Since the total number of points inside both triangles is simply $\frac{p-1}{2} \cdot \frac{q-1}{2}$, one may now conclude that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\nu+\mu} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \qquad \square$$

Even the normally modest Eisenstein could not restrain his pleasure with this proof:

> "How lucky good Euler would have considered himself, had he possessed these lines about seventy years ago." [7, p. 174]

3 Eisenstein versus Gauss

Gauss himself considered his third proof to be the most direct and natural of his demonstrations. In introducing it he said:

> "For a whole year this theorem tormented me and absorbed my greatest efforts until at last I obtained a proof .... Later I came across three other proofs which were built on entirely different principles. ... 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." [10, p. 113]

While Eisenstein essentially follows the same outline as Gauss, each feature of his approach displays great clarity and insight, and offers an elegant view while shortening the path taken by Gauss.

Gauss' third proof begins with his Lemma, which says that

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}, \tag{3}$$

with α obtained as follows: Let

$$\mathcal{A} = \{1, 2, \ldots, \frac{p-1}{2}\} \quad \text{and} \quad \mathcal{B} = \{\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1\}.$$

Then α is defined to be the number of least positive residues of the set $q\mathcal{A}$ which lie in $\mathcal{B}$.

Instead of using Gauss' Lemma, Eisenstein derives equation (1), with the algebraic expression $\sum r$ in the exponent, which is then more easily converted into the key equation

$$\left(\frac{q}{p}\right) = (-1)^{\sum\left[\frac{qa}{p}\right]}, \tag{4}$$

common to both proofs, than is equation (3). While Eisenstein's algebraic exponent is easily transformed into the exponent in (4) via (2), Gauss must establish a number of technical properties of the greatest integer function and apply them to relate α to the exponent in (4). Eisenstein's use of the set $a = 2, 4, 6, \ldots, p-1$, as opposed to Gauss' $\mathcal{A}$, allows him to count the same elements as Gauss' Lemma, but via the expression $\sum r$, leading quickly to (4):

> "The main difference between my argument and that of Gauss is that I do not divide the numbers less than p into those less than $p/2$ and those greater than $p/2$, but rather into even and odd ones." [7]

Eisenstein now applies his two clever geometric transformations to convert the exponent $\sum \left[\frac{qa}{p}\right]$ into the number of lattice points in triangle AHK (mod 2). After doing the same for $\left(\frac{p}{q}\right)$, yielding the number of lattice points in AHL, the proof is completed simply by counting the lattice points in rectangle $AKHL$.[1] Gauss, on the other hand, in essence performs the same two transformations, and counting, without availing himself of the geometric presentation. He actually counts the lattice points using algebraic properties of the greatest integer function. This makes the remainder of his proof lengthy and nonintuitive, and forces him to consider separate cases depending on the congruence classes of p and q (mod 4). (For a more detailed comparison, see [8].)

References

[1] P. G. Bachmann, *Niedere Zahlentheorie*, Teubner, Leipzig, 1902–1910, republished by Chelsea, New York, 1968.

[2] O. Baumgart, Über das Quadratische Reciprozitätsgesetz, *Zeitschrift für Mathematik und Physik* **30** (1885), Historisch-literarische Abtheilung, 169–277.

[3] K.-R. Biermann, Gotthold Eisenstein: Die Wichtigsten Daten seines Lebens und Wirkens, *Mathematische Werke; Gotthold Eisenstein*, New York, Chelsea Publ. Co., 1975, pp. 919–929.

[4] K.-R. Biermann, *Carl Friedrich Gauß*, Verlag C.H. Beck, München, 1990, p. 177.

[5] G. Eisenstein, Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste, *Crelle's Journal* **28** (1844), 246–249.

[1] Most modern expositions of Eisenstein's proof present only this final counting argument, replacing his two geometric transformations by algebra.

[6] C. F. Gauss, *Commentationes Societatis Regiae Scientiarum Gottingensis* **16** (1808), Göttingen; also *Werke*, Göttingen, 1876, Band 2, pp. 1–8.

[7] A. Hurwitz and F. Rudio (Eds.), Briefe von G. Eisenstein an M. Stern, supplement to *Zeitschrift für Mathematik und Physik* **40** (1895), 169–203.

[8] R. Laubenbacher and D. Pengelley, Gauss, Eisenstein, and the "third" proof of the Quadratic Reciprocity Theorem: Ein kleines Schauspiel, *Mathematical Intelligencer*, to appear.

[9] F. Rudio (Ed.) Eine Autobiographie von Gotthold Eisenstein. Mit Ergänzenden Biographischen Notizen, *Zeitschrift für Mathematik und Physik* **40** (1895), 143–168.

[10] D. E. Smith, *A Source Book in Mathematics*, Dover, New York, 1959, pp. 112–118.