Gauß, Eisenstein, and the "third" proof of the Quadratic Reciprocity Theorem: Ein kleines Schauspiel

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

[Mathematical Intelligencer **16** (1994), 67-72]

The year: 1844

The characters:

Carl Friedrich Gauß, Director of the Göttingen Observatory, and the most prominent mathematician of the 19th century (and, possibly, of all time).

Gotthold Eisenstein, 21-year old mathematics student at the Friedrich-Wilhelms University in Berlin.

Eisenstein: "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

[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.

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." [5]

Eisenstein (continuing): You, Herr Direktor, have described so eloquently the strange attractions of this science, and have given several proofs of its Fundamental Theorem.

Gauß: "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 Arithemeticae* 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 absorbed 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." [8, 11]

Gauß (continuing): The Quadratic Reciprocity Theorem compares the quadratic character of two primes with respect to each other. The quadratic character of q with respect to p is expressed by the Legendre symbol $\left(\frac{q}{p}\right)$, defined to be 1 if q is a quadratic residue (i.e., a square) modulo p, and -1 if not.

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

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

We also have the Ergänzungssatz

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

for the prime 2.

Note that the theorem says that p and q have the same quadratic character with respect to each other if either one of them is $\equiv 1 \pmod 4$, but not if both are $\equiv 3 \pmod 4$.

Why is this theorem so important? First, it can be used to solve the general problem of when a quadratic congruence has a solution, since the Fundamental Theorem, along with the multiplicativity of the Legendre symbol, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, enables one easily to compute its values, and thus to know exactly when square roots may be found modulo p. But it also represents an amazing and unexpected relationship between pairs of primes, a deep law governing prime numbers. Later in the century, Baumgart [2] will describe the role of the Fundamental Theorem within higher arithmetic:

> "The higher arithmetic in essence divides into two main parts, the theory of congruences and the theory of homogeneous forms. The theory of binomial congruences forms an integrating part of the general theory of congruences. 'The reciprocity laws are the cornerstone of the latter theory'[1]".

[1]Kummer, Berliner Abhandlungen, 1859, S. 19.

In my lifetime I will in fact present eight different proofs of the Fundamental Theorem, and other mathematicians will find many more. But my third published proof, which I will now present, is perhaps the most natural one I know. My proof begins with a theorem which in the future might be called

Gauß' Lemma *Let p be prime, and q any number not divisible by p. Then*

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

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 modulo p of the set $q\mathcal{A}$ which lie in $\mathcal{B}$.

> "Proof: Let $a, a', a'', \ldots$ be the residues belonging to the class $\mathcal{A}$ and $b, b', b'', \ldots$ be those belonging to $\mathcal{B}$. Then it is clear that the complements of the latter, $p-b, p-b', p-b'', \ldots$ are not equal to any of the numbers $a, a', a'', \ldots$ [for if, say, $qx \equiv a = p - b \equiv p - qy$ where x, y come from $\mathcal{A}$, then $q(x+y)$ would be divisible by p, which cannot occur since both x and y lie strictly between 0 and $\frac{p}{2}$], and together with them make up the class $\mathcal{A}$. Consequently we have
>
> $$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} = a \cdot a' \cdot a'' \cdots (p-b)(p-b')(p-b'') \cdots \ .$$
>
> The right-hand product evidently becomes, modulo p:
>
> $$\equiv (-1)^{\alpha} a a' a'' \cdots b b' b'' \cdots \equiv (-1)^{\alpha} q \cdot 2q \cdot 3q \cdots \frac{p-1}{2} q$$
>
> $$\equiv (-1)^{\alpha} q^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \ .$$
>
> Hence
>
> $$1 \equiv (-1)^{\alpha} q^{\frac{p-1}{2}} \ ,$$

that is $q^{\frac{p-1}{2}} \equiv \pm 1$ according as α is even or odd. Hence our theorem follows at once [from Euler's Criterion that $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}$]." [11]

Eisenstein: Hochgeehrtester Herr Hofrath, I too have devoted much effort to the study of the quadratic reciprocity law and have given four different proofs of it. My recently published geometric proof [7] is related to your third proof and, with all due modesty, represents something of an improvement in the exposition of the main ideas underlying it. My excitement is clear in the letter I wrote to my friend Moritz Stern in Göttingen:

> "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. 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." [9]

Instead, I begin my proof as follows, with what may hopefully someday be called Eisenstein's Lemma. Consider the set $a = 2, 4, 6, \ldots, p-1$. Let r denote the remainder (mod 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 the exponent. This formula is my replacement for your Lemma. Because the exponent is algebraic in nature, my proof will now proceed more easily than yours. Incidentally, the odd terms actually contributing to the parity of this exponent correspond exactly to the ones counted in your Lemma.

Gauß: Well, we shall see about that, Herr Student. I will begin the main part of my proof by deriving a few technical facts about the greatest integer function [ ] which are needed subsequently.

Let x be a non-integral quantity.

1. $[x] + [b - x] = b - 1$, whenever b is an integer.
2. If $x - [x]$ is a fraction less than $\frac{1}{2}$, then $[2x] - 2[x] = 0$. If on the other hand $x - [x]$ is greater than $\frac{1}{2}$, then $[2x] - 2[x] = 1$. Thus:
3. If the smallest positive residue of $b \pmod{p}$ is less than $\frac{p}{2}$, then $\left[\frac{2b}{p}\right] - 2\left[\frac{b}{p}\right] = 0$. If, however it is larger than $\frac{p}{2}$, then $\left[\frac{2b}{p}\right] - 2\left[\frac{b}{p}\right] = 1$.
4. From this it follows that

$$\begin{aligned} \alpha = &\left[\tfrac{2q}{p}\right] + \left[\tfrac{4q}{p}\right] + \left[\tfrac{6q}{p}\right] + \cdots + \left[\tfrac{(p-1)q}{p}\right] \\ &-2\left[\tfrac{q}{p}\right] - 2\left[\tfrac{2q}{p}\right] - 2\left[\tfrac{3q}{p}\right] - \cdots - 2\left[\tfrac{\frac{(p-1)}{2}q}{p}\right] . \end{aligned} \tag{2}$$

Eisenstein: But with all due respect, Herr Hofrath, the formula (1) in my Lemma already produces the essence of this more quickly and transparently. Clearly

$$\sum qa = p\sum\left[\frac{qa}{p}\right] + \sum r \ .$$

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 from (1) that

$$\left(\frac{q}{p}\right) = (-1)^{\sum\left[\frac{qa}{p}\right]} \ . \tag{3}$$

This is equivalent to what you have learned about α in (2), since only the parity is relevant.

Gauß: Well, Herr Eisenstein, that was indeed a clever shortcut to formula (3), leading now to the following necessary calculations. I transform the formula (2) as follows: From property 1 above, we have

$$\left[\tfrac{(p-1)q}{p}\right] = q - 1 - \left[\tfrac{q}{p}\right] \ , \ \left[\tfrac{(p-3)q}{p}\right] = q - 1 - \left[\tfrac{3q}{p}\right] \ ,$$
$$\left[\tfrac{(p-5)q}{p}\right] = q - 1 - \left[\tfrac{5q}{p}\right] \ , \ \ldots \ .$$

When we apply these substitutions to the last $\frac{p\mp1}{4}$terms of the top series in (2) we have:

first, when p is of the form $4n+1$,

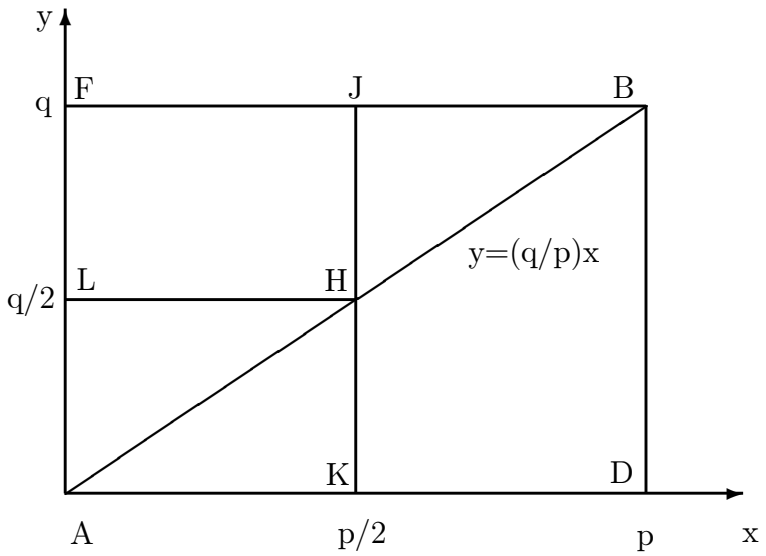
$$\alpha = \tfrac{(q-1)(p-1)}{4} - 2\left\{\left[\tfrac{q}{p}\right] + \left[\tfrac{3q}{p}\right] + \left[\tfrac{5q}{p}\right] + \cdots + \left[\tfrac{\frac{p-3}{2}q}{p}\right]\right\}$$
$$- \left\{\left[\tfrac{q}{p}\right] + \left[\tfrac{2q}{p}\right] + \left[\tfrac{3q}{p}\right] + \cdots + \left[\tfrac{\frac{p-1}{2}q}{p}\right]\right\} \ ,$$

second, when p is of the form $4n+3$,

$$\alpha = \tfrac{(q-1)(p+1)}{4} - 2\left\{\left[\tfrac{q}{p}\right] + \left[\tfrac{3q}{p}\right] + \left[\tfrac{5q}{p}\right] + \cdots + \left[\tfrac{\frac{p-1}{2}q}{p}\right]\right\}$$
$$- \left\{\left[\tfrac{q}{p}\right] + \left[\tfrac{2q}{p}\right] + \left[\tfrac{3q}{p}\right] + \cdots + \left[\tfrac{\frac{p-1}{2}q}{p}\right]\right\} \ .$$

From these the Ergänzungssatz follows for $q = 2$, and we assume henceforth that q is an odd prime.

Eisenstein: Firstly, Herr Direktor, the Ergänzungssatz also follows easily from my (3). And, secondly, the results of your substitutions can all be interpreted geometrically for q odd. Let us use a simple geometric representation of the exponent $\sum\left[\frac{qa}{p}\right]$ in (3) to transform it 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 $q - 1$, which 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

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

In each of your expressions above for α, the first line is even, and the second line counts precisely the lattice points in triangle AHK. Your substitutions are realized simply by these geometric transformations when we focus specifically on the parity.

Gauß (aside): Darn, my calculations really do seem clumsy compared

with this youngster's geometric methods.

Gauß (to Eisenstein again): Very well Herr Eisenstein, there does seem to be some merit to your approach. But now your geometry has reached its limit, and we must compare the reciprocal roles of p and q as follows.

Considering the second line in each of the expressions above for α, and comparing it with the same expression when the roles of p and q are interchanged, I will prove that

$$\begin{gathered}\left[\tfrac{q}{p}\right]+\left[\tfrac{2q}{p}\right]+\left[\tfrac{3q}{p}\right]+\cdots+\left[\tfrac{\frac{p-1}{2}q}{p}\right]\\ +\left[\tfrac{p}{q}\right]+\left[\tfrac{2p}{q}\right]+\left[\tfrac{3p}{q}\right]+\cdots+\left[\tfrac{\frac{q-1}{2}p}{q}\right]\\ =\tfrac{(p-1)(q-1)}{4}\ .\end{gathered}$$

This is somewhat technical and lengthy, but we begin as follows: ...

Eisenstein (agitated): But Herr Hofrath, please, this is immediately obvious from the geometric representation, for it is merely the sum of the number of lattice points μ in triangle AHK with the number ν in triangle AHL, which clearly equals the total number $\frac{p-1}{2}\cdot\frac{q-1}{2}$ inside the rectangle.

Gauß (after some hesitation): Indeed, verehrter Herr Eisenstein, this is impressive! For the sake of completeness, though, I will now finish my argument by letting

$$\begin{aligned}L&=\alpha+\left[\tfrac{q}{p}\right]+\left[\tfrac{2q}{p}\right]+\left[\tfrac{3q}{p}\right]+\cdots+\left[\tfrac{\frac{p-1}{2}q}{p}\right],\\ M&=\beta+\left[\tfrac{p}{q}\right]+\left[\tfrac{2p}{q}\right]+\left[\tfrac{3p}{q}\right]+\cdots+\left[\tfrac{\frac{q-1}{2}p}{q}\right],\end{aligned}$$

where β has the same definition as α does but with the roles of p and q interchanged. Then from the expressions above for α we see that L, and likewise M, are even, and moreover

$$L+M=\alpha+\beta+\frac{(p-1)(q-1)}{4}\ .$$

Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\alpha}(-1)^{\beta}=(-1)^{\alpha+\beta}=(-1)^{\frac{(p-1)(q-1)}{4}}$$

and the proof is complete.

Eisenstein: Herr Hofrath, thank you for your kind words. Of course my proof was already finished before, since I have

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

As I wrote to my friend Stern,

> "How lucky good Euler would have considered himself, had he possessed these lines about seventy years ago." [9]

Eisenstein (aside): I wonder if Gauß already had my geometric view of his transformations when he published his third proof in 1808, and if the old fox has merely been humoring me all along in our conversation.

EPILOGUE

Gauß: I have just today, July 14, 1844, written a letter to C. Gerling, saying "I have recently made the acquaintance 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]. By the end of this year he will have contributed no less than 16 of the 27 mathematical articles in volume 27 of Crelle's Journal, including his geometric proof of the Fundamental Theorem. Next year, as a third semester student, he will receive an honorary doctorate from the University of Breslau [10]. I will write to the great scientist and explorer Alexander von Humboldt that Eisenstein's talent is "that which nature bestows upon only a few in each century". Both von Humboldt and I will make great efforts, for the most part in vain, to obtain recognition and financial security for the impoverished Eisenstein. He will obtain a position as a Privatdozent (unsalaried lecturer) at the University in Berlin, and will eventually be admitted to the Berlin Academy of Sciences in early 1852. But by then his lifelong poor health will have seriously deteriorated, and he will die later that same year, at the age of 29, of tuberculosis [3, 10]. How tragic that, like Abel and Galois in

the same period, we will lose the genius of Gotthold Eisenstein to so early a death.

The brilliance and power of Eisenstein's work will remain unappreciated for a long time in part because it will be almost 125 years before the publication of his Collected Works. In the foreword to their second edition [6], the eminent twentieth century mathematician André Weil reviews Eisenstein's mathematical contributions, in particular

> "the impressive series of papers on elliptic functions and their application to the higher reciprocity laws . . . . [The] series ends up with a great paper, the *Genaue Untersuchung* of 1847, which excited Kronecker's enthusiasm when he discovered it late in life, and which still deserves ours; it is nothing less than the sketch of a complete theory of elliptic and modular functions, based on principles essentially distinct from those of Jacobi and from those of Weierstraß (while anticipating him by nearly fifteen years), but, as I have more amply demonstrated elsewhere, its principles can be profitably applied to important current problems."

Late in the 19th century, Baumgart [2] will write a survey of the many different proofs of the Fundamental Theorem given by then. Unfortunately, he will misunderstand and overlook most of the beautiful features of Eisenstein's geometric proof, mentioning only how he counts the points in a rectangle to avoid my technical argument above for adding the two series with interchanged roles for p and q. Sadly, he will miss Eisenstein's algebraic form of my Lemma, as well as his geometric way of representing my transformations. Subsequent mathematicians, probably relying on Baumgart's survey rather than reading Eisenstein's original paper, will perpetuate this oversight. Let me just mention Bachmann's early 20th century book on number theory [1] as an example.

Only shortly before the dawn of the 21st century will this injustice be rectified, when mathematicians of the distant future rediscover and fully appreciate the neglected and spectacular parts of Eisenstein's geometric proof of the Fundamental Theorem of higher arithmetic.

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., 1989, pp. 919–929.

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

[5] G. Eisenstein, Berlin Academy of Sciences membership acceptance speech (1852), in *Mathematische Werke*, Chelsea Publ., New York, second edition, 1989, pp. 762–763.

[6] G. Eisenstein, *Mathematische Werke*, Chelsea Publ., New York, second edition, 1989, p. ix.

[7] G. Eisenstein, *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste*, Crelle Journal **28** (1844), 246–249; also in *Mathematische Werke*, pp. 164–166.

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

[9] A. Hurwitz and F. Rudio (Eds.), *Briefe von G. Eisenstein an M. Stern*, supplement to Zeitschrift für Mathematik und Physik **40** (1895), 169–203, pp. 173–4; also G. Eisenstein, *Mathematische Werke*, pp. 789–823.

[10] F. Rudio (Ed.) *Eine Autobiographie von Gotthold Eisenstein. Mit Ergänzenden Biographischen Notizen*, Zeitschrift für Mathematik und Physik **40** (1895), 143–168; also G. Eisenstein, *Mathematische Werke*, pp. 879–904.

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