Oswald Baumgart

The Quadratic Reciprocity Law

A Collection of Classical Proofs

Edited and Translated
by Franz Lemmermeyer

Birkhäuser

The Quadratic Reciprocity Law

Birkhäuser

Oswald Baumgart

The Quadratic Reciprocity Law

A Collection of Classical Proofs

Edited and Translated
by Franz Lemmermeyer

Birkhäuser

Oswald Baumgart

Translated by Franz Lemmermeyer
Jagstzell, Germany

ISBN 978-3-319-16282-9 ISBN 978-3-319-16283-6 (eBook)
DOI 10.1007/978-3-319-16283-6

Library of Congress Control Number: 2015938466

Mathematics Subject Classification (2010): 11A15, 11T22, 11T24

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG and Switzerland is part of Springer Science+Business Media (www.birkhauser-science.com)

Translator's Preface

This book contains a translation of Baumgart's thesis *Über das quadratische Reciprocitätsgesetz. Eine vergleichende Darstellung der Beweise* (On the Quadratic Reciprocity Law. A Comparative Presentation of its Proofs) written in Göttingen a hundred years after Legendre's publication of the reciprocity law. Its aim was to present and compare the proofs of the quadratic reciprocity law known to him in 1885. The introduction to this book, which was to give a detailed history of the number theory leading up to the statement and the first proofs of the quadratic reciprocity law, eventually evolved into a book of its own and will be published separately.

Baumgart's thesis consists of two parts. The first part gives a very brief history of the development up to Legendre and then presents some different proofs of the quadratic reciprocity law; Baumgart distinguished Gauss's first proof by induction, proofs by Gauss's Lemma, by complex analysis, by cyclotomy, and by quadratic forms. The last two chapters deal with supplementary laws and algorithms for computing Legendre symbols. In the second part, Baumgart compares the principles of these proofs.

Although Baumgart's thesis does not fill the gap left by the loss of Cooper's contribution to Dickson's history, the planned fourth volume[1] on the quadratic reciprocity law, it may perhaps serve as a stepping stone until such a history of quadratic residues is written.

A closer look at the proofs of the quadratic reciprocity law discussed by Baumgart reveals that only a few of them compare favorably – in terms of simplicity and elegance – with some of the proofs found in recent years. But this only emphasizes that we should continue striving for beauty even in time-honored subjects such as quadratic reciprocity. In addition I would like to call the readers' attention to the fact that only a few proofs so far have been transferred to the case of the (quadratic) reciprocity law in polynomial rings over finite fields.

[1] See [22].

Comments on the Translation

In general, I have corrected obvious mistakes without comment. In addition, I have filled a large gap in the presentation of one of Kummer's proofs. I have also collected the references in the bibliography at the end and have added references to collected works in order to give readers easier access to the original articles. Finally I added comments to the chapters of Part II ("Notes") in which I have briefly sketched the later developments.

In an appendix I have supplied detailed references to all the proofs of the quadratic reciprocity law in the integers that I was aware of at the time of writing.

Jagstzell, Germany
December 2014

Franz Lemmermeyer

Dedicated to

Dr. Phil. Joh. Eduard Böttcher
Teacher at the Realgymnasium in Leipzig
With Thankfulness and Admiration.

Oswald Baumgart, 1885

Contents

Introduction

Higher arithmetic in essence divides into two main parts, the theory of congruences and the theory of homogeneous forms.[2] An integral part of the theory of congruences is formed by the theory of binomial[3] congruences, whose pivotal point is the theory of power residues. “The reciprocity laws are the cornerstone of the latter theory” (see [47, p. 19]). Although finding these laws “of simply stated content” (see [31]) using induction[4] was comparatively easy, finding their proofs was connected with huge difficulties: to this end new methods had to be found, and proofs had to be sought in areas that seemed to have no connection with the number theory. And yet at first it was only possible to verify the correctness of the *quadratic* reciprocity law. But the principles found in the different proofs of the quadratic reciprocity law could be generalized to such a degree that they also could be used for deriving the general reciprocity laws.

In the following we will present all known proofs of the quadratic reciprocity law and carefully compare the principles on which they are based. The author believes that such a first comparison is not completely useless, because this law is the fundamental result in the theory of quadratic residues and nonresidues, moreover because the principles on which they are built allow us to find new and very general methods, and finally because the proofs of this law have induced a very welcome interaction between some, until then almost or completely isolated, areas

[2] [FL] Jacobi also divided the number theory into these two areas, as did H.J. Smith in his report; notably absent from this list is cyclotomy, which both authors apparently subsumed into the theory of congruences.

[3] [FL] In modern terms: polynomial equations in two variables over residue class rings, i.e., solutions of $f(X, Y) = 0$ over finite fields

[4] [FL] Clearly he is not talking about mathematical induction; finding something by induction in those days simply meant making a conjecture based on empirical evidence.

of mathematics. In addition, the history of this theorem is a faithful reflection of the simultaneous history of mathematics in the small.[5]

It was Professor SCHEIBNER who notified me of this remarkable and attractive fact. I would like to thank my highly respected teacher for this as well as for the support and the stimulation I have received from him.

In the first part I have presented all known proofs, as far as they were accessible to me, ordered in chapters in such a way that the proofs of one chapter are based on the same main idea. Within each chapter, the proofs are given in chronological order. The principles themselves are developed in the second part. Historical notes are given at the beginning and the end of this thesis.

For the convenience of the reader, and also in order to highlight the similarities and the differences of the proofs, I have tried to choose a common notation and presentation. It goes without saying that not only the main idea but also the individual structure of the different proofs has remained untouched.

[5] [FL] This seems to be an allusion to Haeckel's "Biogenetic Law" first published in 1866, according to which ontogeny recapitulates phylogeny, i.e., an embryo repeats in its development the evolutionary history of its species as it passes through stages in which it resembles its remote ancestors.

Part I
Presentation of the Proofs of the Quadratic Reciprocity Law

Chapter 1
From Fermat to Legendre

After BACHET DE MÉZIRIAC [1] had brought the theory of linear diophantine equations to a certain closure, mathematicians were faced with the question of solving equations of the second degree, in particular the binomial congruence of degree 2. In other words, the problem was to find simple conditions for the solvability of the congruence

$$x^2 \equiv p \bmod q,$$

where p and q are given integers.

At first only special cases were investigated.

It transpires from a letter of FERMAT to the Englishman KENELM DIGBY (see [72, vol. II, p. 857]) in 1658 that already FERMAT knew the conditions for which odd primes q the numbers ± 1, 2, ± 3, 5 are quadratic residues or nonresidues; it is also clear from a letter of FRENICLE (see [23, p. 168]) to FERMAT in 1641 that already FRENICLE knew when -2 is quadratic residue or nonresidue of some prime number. Probably, however, as also LAGRANGE [49, p. 337] assumes, this had been known to FERMAT before and was FRÉNICLE's answer to a question of FERMAT.

All these results were found by induction and given without proofs. For -1, the theorem was first proved by EULER [21, p. 135] (see also p. 71 of this report) using associated residues (*residua socia*); his method did not succeed for ± 2. This gap was closed by LAGRANGE [49, p. 349, 351]. It is a remarkable fact that EULER did not succeed in finding the proof for ± 2, because he actually knew (see [19]) the proof of the law for ± 3. As for ± 5, it was again LAGRANGE [49, p. 352] who first succeeded in proving under which conditions this number is a quadratic residue or nonresidue of a given prime number.

These results, which were without influence on the actual presentation of the law, are presented for the sake of completeness and in order to make clear with which difficulties mathematicians had to deal here. Although it cannot be denied

O. Baumgart, *The Quadratic Reciprocity Law*,
DOI 10.1007/978-3-319-16283-6_1

that the invention of infinitesimal calculus has essentially diverted mathematicians from number theory, it is nevertheless a remarkable fact that simple results such as those mentioned above could remain without proofs for more than 100 years.

Until now, only special cases were treated. The first to try to recognize and formulate our law in its full generality was EULER. And he succeeded in making an important step forward. In [20] he gives four theorems that completely contain the quadratic reciprocity law. They read[1]:

1. Si divisor primus fuerit formae $4ns + (2x + 1)^2$, existente s numero primo, tum in residuis occurent numeri $+s$ et $-s$.
2. Si divisor primus fuerit formae $4ns - (2x + 1)^2$, existente s numero primo, tum in residuis occuret numerus $+s$, at $-s$ in non-residuis.
3. Si divisor primus fuerit formae $4ns - 4z - 1$ excludendo omnes valores in forma $4ns - (2x + 1)^2$ contentos, existente s numero primo, tum in residuis occuret numerus $-s$; at s erit non-residuum.
4. Si divisor primus fuerit formae $4ns + 4z + 1$ excludendo omnes valores in forma $4ns + (2x + 1)^2$ contentos, existente s numero primo, tum tam $+s$ quam $-s$ in non-residuis occuret.

As a simple calculation shows, Euler has made a mistake in the formulation of 3. Indeed, the second part of this theorem has to be stated as follows: *If s has the form $4n + 1$, then $+s$ is nonresidue and $-s$ residue; for $s = 4n - 1$, the opposite happens.*[2]

These four theorems, also stated without proof, completely contain, as we have already remarked and as will be shown later on without effort by comparison, the quadratic reciprocity law. GAUSS seems to have been unaware of EULER's article just discussed and therefore credits LEGENDRE (see [25, Art. 151]) with the discovery of our law.

It was this famous number theorist, however, who for the first time clearly and explicitly enunciated the fundamental theorem using formulas, namely 1785 in [53, pp. 516–517], and who gave a partial proof. In the fourth section of the work just mentioned he stated eight theorems, in which A, a are primes of the form $4n + 1$,

[1] [FL] Using modern notation, this can be translated as follows:

1. A prime has the form $p = 4ns + (2x + 1)^2$ if and only if $p \equiv 1 \bmod 4$ and $p \equiv y^2 \bmod s$. Thus the first statement claims that if $p \equiv 1 \bmod 4$ is prime and $p \equiv x^2 \bmod s$ for some prime s, then $\pm s \equiv y^2 \bmod p$. In other words: if $p \equiv 1 \bmod 4$ then $(\frac{p}{s}) = +1 \Rightarrow (\frac{\pm s}{p}) = +1$.
2. If $p \equiv 3 \bmod 4$ is prime and $-p \equiv x^2 \bmod s$ for some prime s, then $s \equiv y^2 \bmod p$ and $-s \not\equiv y^2 \bmod p$. In other words: if $p \equiv 3 \bmod 4$ then $(\frac{-p}{s}) = +1 \Rightarrow (\frac{s}{p}) = +1$, $(\frac{-s}{p}) = -1$.
3. If $p \equiv 3 \bmod 4$ is prime and $-p \not\equiv x^2 \bmod s$ for some prime s, then $-s \equiv y^2 \bmod p$ and $s \not\equiv y^2 \bmod p$. In other words: if $p \equiv 3 \bmod 4$ then $(\frac{-p}{s}) = -1 \Rightarrow (\frac{-s}{p}) = +1$, $(\frac{s}{p}) = -1$.
4. If $p \equiv 1 \bmod 4$ is prime and $p \not\equiv x^2 \bmod s$ for some prime s, then $\pm s \not\equiv y^2 \bmod p$. In other words: if $p \equiv 1 \bmod 4$ then $(\frac{p}{s}) = -1 \Rightarrow (\frac{\pm s}{p}) = -1$.

[2] [FL] It seems that Baumgart is wrong here. I cannot see anything wrong with Euler's formulation.