Title: Gauss’s proofs of the quadratic reciprocity law

Author: Anna Febrer Galvany

Advisor: Jordi Quer Bosor

Department: Matemàtica Aplicada II

Academic year: 2012/2013
Gauss’s proofs of the quadratic reciprocity law

Anna Febrer Galvany

Advisor: Jordi Quer Bosor

Matemàtica Aplicada II
To all those people who had faith in me from the beginning and now can see how I become a mathematician.
# Contents

Introduction ................................................................. 1  

Chapter 1. Preliminaries .................................................... 3  
1.1. Historic introduction .............................................. 3  
1.2. Quadratic residues .................................................. 7  
1.3. Legendre symbol .................................................... 9  
1.4. Quadratic reciprocity law ......................................... 11  
1.5. Jacobi symbol ....................................................... 12  

Chapter 2. Gauss’s first proof ........................................... 15  
2.1. First and second supplementary laws ......................... 16  
2.2. Technical lemmas .................................................. 18  
2.3. Quadratic reciprocity law for odd integers .................. 22  
2.4. Quadratic reciprocity law for odd primes .................... 28  

Chapter 3. Proofs based on Gauss’s Lemma ......................... 43  
3.1. Gauss’s Lemma ...................................................... 43  
3.2. Gauss’s third proof ............................................... 44  
3.3. Gauss’s fifth proof ................................................. 48  

Chapter 4. Proofs based on trigonometric sums .................... 53  
4.1. Gauss’s fourth proof .............................................. 53  
4.2. Gauss’s sixth proof ............................................... 64  

References ................................................................. 71
Introduction

I find very interesting that a single statement can be proven in many different ways. For this reason I decided to dedicate my bachelor’s degree thesis to the study of the quadratic reciprocity law, probably the statement that admitted the greatest number of different proofs: up to now, several hundred proofs of the quadratic reciprocity law have been found. Franz Lemmermeyer, one of the leading experts on the subject maintains a web page [Lem1] with a list of published proofs that today contains 240 entries.

At the age of 19 Gauss proved for the first time the quadratic reciprocity law, that had stayed unproven for nearly 150 years, resisting the efforts of some of the best mathematicians including Fermat, Euler and Legendre. Gauss believed that the quadratic reciprocity law was a very important mathematical result, so important that he dared to call it “fundamental theorem”. Gauss was very proud of his proof of the fundamental theorem, so he tried to develop a bit more this field by looking for similar theorems for reciprocity of higher powers. His attempts to generalize the fundamental theorem to higher powers led him to found seven more proofs of the quadratic reciprocity law.

The goal of this thesis is to understand the quadratic reciprocity law, study the proofs that Gauss gave of it in its original sources (most of them written in Latin and not translated into other languages) and explain them in a more modern language. Due to time limitation, this project only presents five of the eight proofs of Gauss, which are the first, the third, the fourth, the fifth and the sixth.

We structured the thesis in four chapters. Chapter 1 introduces the topic, giving a bit of history of the development of the quadratic reciprocity law and basic notation, concepts and statement of quadratic reciprocity. Chapter 2, the largest chapter, presents the first proof which was made by induction and is by far the largest, tricky and more intricate proof found by Gauss. In Chapter 3 we show the third and the fifth proofs, the two ones based on Gauss’s Lemma. And finally in Chapter 4 we explain the proofs based on trigonometric sums, which are the fourth and the sixth.

All this project is sourced from Gauss’s original works, basically from the book Disquisitiones arithmeticae ([Gau1]) and the original papers of Gauss, collected in Werke Vol.2 ([Gau3],[Gau4],[Gau5] and [Gau6]). We tried to expose the five proofs using more modern notation in order to make them more understandable.
and easy to follow. However, sometimes we adopted Gauss notation which is not used any longer because it was useful in order to follow Gauss steps.
Chapter 1
Preliminaries

1.1. Historic introduction

The quadratic reciprocity law was born when Fermat became interested in the following problem:

Determine the primes \( p \) that can be written in the form:

\[
x^2 + ny^2 = p,
\]

where \( n \) is a fixed integer.

Since the first results were stated until the quadratic reciprocity law was proved, two hundred years later, there have been four mathematicians who played a key role in the development of the law.

**Fermat (1601-1665)**

Pierre de Fermat was the mathematician who started studying reciprocity questions. All we know about Fermat’s results is contained in his letters to other mathematicians (or in the margins of some books he read) since in Fermat’s time mathematical journals did not exist. The first result related with quadratic reciprocity appears in a letter to Mersenne, and it stated:

Tout nombre premier, qui surpassé de l’unité un multiple du quaternaire, est une seule fois la somme de deux carrés.\(^1\)

This statement is equivalent to say that for every prime number of the form \( 4n + 1 \), say \( p \), there exist two positive integers \( x \) and \( y \) such that \( p = x^2 + y^2 \). Using Bézouts’s identity, Fermat’s “little theorem” and some basic properties of congruences, it can be seen that a prime \( p \) is the sum of two squares \( (p = x^2 + y^2) \) if and only if the equation \( X^2 \equiv -1 \pmod{p} \) is solvable. Since Fermat knew that every prime number of the form \( 4n + 1 \) (and no other odd primes) can be expressed as a sum of two squares, it follows that the congruence \( X^2 \equiv -1 \pmod{p} \) is solvable if an

\(^1\)Every prime which is one more than a multiple of 4 is a sum of two squares in one and only one way.
only if \( p \) is congruent to 1 modulo 4. What Fermat stated and proved was what we nowadays know as the first supplementary law of quadratic reciprocity.

For other integers \( n \), the study of the primes of the form \( p = x^2 + ny^2 \) leads to the congruence \( X^2 \equiv -n \pmod{p} \), whose solutions for all \( p \) requires the quadratic reciprocity law.

Fermat was able to deduce and conjecture the quadratic character of \( \pm 2 \) and \( \pm 3 \) but he couldn’t prove them.

**Euler (1707-1783)**

Euler first steps in number theory were guided by Fermat’s work. He proved some of Fermat conjectures and he also refuted some of them. Euler used to correspond with Goldbach and to discuss with him themes related to number theory. In one of his letters to Euler, Goldbach asked:

\[
\text{P.S. Notane Tibi est Fermatii observatio omnes numeros hujus formulae 2}^{2^{x-1}} + 1, \text{ nempe 3,5,17, etc. esse primos, quam tamen ipse fatebatur se demonstrare non posse et post eum nemo, quod sciam, demonstravit.}\]

After that letter, Euler started to study Fermat numbers \( 2^{2^n} + 1 \) and Mersenne numbers \( 2^q - 1 \); and his work on divisors of these numbers and, more generally, on divisors of number represented by binary quadratic forms \( nx^2 + my^2 \) led Euler to realize the quadratic reciprocity law.

His first result directly connected with quadratic reciprocity law was:

**Euler’s criterion.** For integers \( a \) and odd primes \( p \) such that \( p \nmid a \) we have

\[
a^{\frac{p-1}{2}} = \begin{cases} 
+1 & \text{if } a \text{ is a quadratic residue modulo } p, \\
-1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. 
\end{cases}
\]

After some time working in other problems, the research of Lagrange in the years 1773/75 about quadratic reciprocity made Euler to take up the subject again, and this time he discovered the complete quadratic reciprocity law, that, translated into modern notation, he stated in the following form:

1. If \( p \equiv 1 \pmod{4} \) is prime and \( p \equiv x^2 \pmod{q} \) for some prime \( q \), then \( \pm q \equiv y^2 \pmod{p} \).
2. If \( p \equiv 3 \pmod{4} \) is prime and \( -p \equiv x^2 \pmod{q} \) for some prime \( q \), then \( q \equiv y^2 \pmod{p} \) but \( -q \not\equiv y^2 \pmod{p} \).
3. If \( p \equiv 3 \pmod{4} \) is prime and \( -p \not\equiv x^2 \pmod{q} \) for some prime \( q \), then \( -q \equiv y^2 \pmod{p} \) but \( q \not\equiv y^2 \pmod{p} \).
4. If \( p \equiv 1 \pmod{4} \) is prime and \( p \not\equiv x^2 \pmod{q} \) for some prime \( q \), then \( \pm q \not\equiv y^2 \pmod{p} \).

---

\(^2\text{P.S. Is Fermat’s observation known to you that all numbers of the form } 2^{2^{x-1}} + 1, \text{ namely } 3,5,17, \text{ etc. are primes, which he himself could not prove and which no one after him, to the best of my knowledge, has ever proved.}\)
This statement was finally published in 1783, after Euler’s death, without him having been able to produce a proof.

Euler also conjectured the following theorem:

**Theorem** Let $f, g \in \mathbb{Z}$ be coprime squarefree integers that are not both negative. If $h$ and $h'$ are positive primes such that $h \equiv h' \pmod{4fg}$, then the equation $fx^2 + gy^2 = hz^2$ is solvable if and only if the equation $fx^2 + gy^2 = h'z^2$ is also solvable.

The connection between this theorem and the quadratic reciprocity law comes by putting $g = -a$ and $f = 1$. Then Euler’s conjecture says that if $q \equiv q' \pmod{4a}$, then the equation $x^2 - ay^2 = qz^2$ is solvable if and only if $x^2 - ay^2 = q'z^2$.

**Legendre (1752-1833)**

The quadratic reciprocity law was published in a form that is more familiar to us in 1785 by Legendre. In his paper (see [Leg1]) he considers primes $a, A \equiv 1 \pmod{4}$ and $b, B \equiv 3 \pmod{4}$ and states:

- Théorème I. Si $b^{a-1} \equiv +1$, il s’ensuit $a^{b-1} \equiv +1$.
- Théorème II. Si $a^{b-1} \equiv -1$, il s’ensuit $b^{a-1} \equiv -1$.
- Théorème III. Si $a^{b-1} \equiv +1$, il s’ensuit $A^{b-1} \equiv +1$.
- Théorème IV. Si $a^{b-1} \equiv -1$, il s’ensuit $A^{b-1} \equiv -1$.
- Théorème V. Si $a^{b-1} \equiv +1$, il s’ensuit $b^{a-1} \equiv +1$.
- Théorème VI. Si $b^{a-1} \equiv -1$, il s’ensuit $a^{b-1} \equiv -1$.
- Théorème VII. Si $b^{a-1} \equiv +1$, il s’ensuit $B^{a-1} \equiv -1$.
- Théorème VIII. Si $b^{a-1} \equiv -1$, il s’ensuit $B^{a-1} \equiv +1$.

(Actually, Legendre wrote $=$ instead of $\equiv$ in order to denote equality up to certain multiples; the notion of congruence and the symbol $\equiv$ was later introduced by Gauss). It is worth to note that both the notation, using letters of the same type to denote primes $\equiv 1$ or $\equiv 3 \pmod{4}$ and also the way to state the result are the ones used by Gauss in the first proof. In later proofs Gauss moved to more compact and elegant ways to state the quadratic reciprocity law.

In 1798, Legendre introduces the “Legendre symbol” (see p. 186 of [Leg]):

$$(\frac{N}{c})$$

Comme les quantités analogues $N^{\frac{c-1}{2}}$ se rencontreront fréquemment dans le cours de nos recherches, nous emploierons le caractère abrégé $\left(\frac{N}{c}\right)$

pour exprimer le reste que donne $N^{\frac{c-1}{2}}$ divisé par $c$, reste qui suivant ce qu’on vient de voir ne peut être que $+1$ ou $-1$.\(^3\)

\(^3\)Since the analogous quantities $N^{\frac{c-1}{2}}$ will occur often in our researches, we shall employ the abbreviation $\left(\frac{N}{c}\right)$ for expressing the residue that $N^{\frac{c-1}{2}}$ gives upon division by $c$, and which, according to what we just have seen, only assumes the values $+1$ or $-1$.\(^3\)
And on page p. 214, he continues

Quels que soient les nombres premiers \( m \) et \( n \), s’ils ne sont pas tous deux de la forme \( 4x + 1 \), on aura toujours \( \left( \frac{n}{m} \right) = \left( \frac{m}{n} \right) \), et s’ils sont les deux de la forme \( 4x - 1 \), on aura \( \left( \frac{n}{m} \right) = -\left( \frac{m}{n} \right) \). Ces deux cas généraux sont compris dans la formule

\[
\left( \frac{n}{m} \right) = (-1)^{\frac{n-1}{2} - \frac{m-1}{2}} \left( \frac{m}{n} \right).
\]

Trying to prove the quadratic reciprocity law, Legendre found that the following statement must be true:

For each prime \( a \equiv 1 \pmod{4} \) there exists a prime \( \beta \equiv 3 \pmod{4} \) such that \( \left( \frac{\alpha}{\beta} \right) = -1 \).

However he could not rigorously prove the existence of such a prime \( \beta \), and this prevented him from proving the result. The first proof by Gauss in fact uses a technical nontrivial lemma similar to this result.

**Gauss (1777-1855)**

On 8 April 1796, Gauss finally could prove the quadratic reciprocity law at the age of 19. But his desire to find similar theorems for reciprocity of higher powers made him look for proofs which would generalize, and by 1818 he had published six different proofs, and two more were found in his unpublished papers and were published after his death.

But not only did Gauss give the first complete proofs of the quadratic reciprocity law, he also extended it to composite values of \( p \) and \( q \). This generalization can be stated using a generalization of the Legendre symbol for odd positive integers. This symbol was introduced by Jacobi in 1837 and is best known as Jacobi symbol.

Using Jacobi symbols, the Gauss generalization for the quadratic reciprocity law and its supplementary laws can be stated as follows:

**Generalization of the quadratic reciprocity for odd positive integers:** Let \( n, m \in \mathbb{N} \) be relatively prime and odd, then

\[
\left( \frac{m}{n} \right) = (-1)^{\frac{n-1}{2} - \frac{m-1}{2}} \left( \frac{n}{m} \right), \quad \left( \frac{-1}{n} \right) = (-1)^{\frac{n-1}{2}}, \quad \left( \frac{2}{n} \right) = (-1)^{\frac{n^2-1}{8}}.
\]

This was a great improvement on Euler’s and Legendre’s version of quadratic reciprocity, as far as the computation of residue symbols \( \left( \frac{m}{n} \right) \) was concerned: instead

---

\(^{4}\)Whatever the prime numbers \( m \) and \( n \) are, if they are both of the form \( 4x + 1 \), one always has \( \left( \frac{n}{m} \right) = \left( \frac{m}{n} \right) \); and if both are of the form \( 4x - 1 \), one has \( \left( \frac{n}{m} \right) = -\left( \frac{m}{n} \right) \). These two general cases are contained in the formula

\[
\left( \frac{n}{m} \right) = (-1)^{\frac{n-1}{2} - \frac{m-1}{2}} \left( \frac{m}{n} \right).
\]
of having to factor the residue of $m \pmod{n}$ before inverting the occurring Legendre symbols one could simply invert the Jacobi symbols and apply a computationally cheap Euclidean algorithm.

### 1.2. Quadratic residues

In the article 95 of *Disquisitiones Arithmeticae* (see [?] Gauss introduced the terminology “quadratic residue” and “nonquadratic residue” as follows:

**Definition 1.2.1.** An integer $q$ is called a *quadratic residue* modulo $n$ if it is congruent to a perfect square modulo $n$; i.e., if there is an integer $x$ such that:

$$x^2 \equiv q \pmod{n}.$$ 

Otherwise, $q$ is called a *quadratic nonresidue* modulo $n$.

When this can not cause any ambiguity, we will simply call them *residues* and *nonresidues*.

The modulo $n$ can be any integer, but for simplicity here we will only consider odd modulus.

**Proposition 1.2.2** Let $p$ be an odd prime number and $a$ a residue of $p$. Considering only the solutions smaller than $p$, the equation:

$$x^2 \equiv a \pmod{p}$$

has exactly two different solutions, one odd and one even.

**Proof.** Since $a$ is a residue of $p$, the equation $x^2 \equiv a \pmod{p}$ has at least a solution. Suppose that $m < p$ is a solution of the equation, i.e. $m^2 \equiv a \pmod{p}$. Then $-m$ is also a solution of the equation, because

$$(-m)^2 \equiv m^2 \equiv a \pmod{p}.$$ 

But $-m \equiv p - m \pmod{p}$, so $p - m$ is another solution of the equation and it is also smaller than $p$.

Note that $m + (p - m) = p$, so $m$ and $p - m$ must have different parity since their sum is an odd number.

Now we shall show that, apart from $m$ and $p - m$, the equation has no other solutions. Let us consider the set

$$A = \left\{ i^2 \pmod{p} \bigg| i = 1, \ldots, \frac{p-1}{2} \right\}.$$ 

Note that $|A| = \#\{\text{residues of } p \text{ less than } p\}$, and by Proposition 1.2.4 we know that $\#\{\text{residues of } p \text{ less than } p\} = \frac{p-1}{2}$. So $|A| = \frac{p-1}{2}$. Hence all elements of $A$ must be different, i.e. there isn’t any number $n < \frac{p-1}{2}$ different from $m$ and $p - m$ such that $m^2 \equiv n^2 \pmod{p}$. Consequently, there is not any number less than $p - 1$, apart from $m$ and $p - m$, satisfying the equation $x^2 \equiv a \pmod{p}$. Therefore we
proved that the only solutions of \(x^2 \equiv a \pmod{p}\) are \(m\) and \(p - m\), one odd and the other even. \(\square\)

Given a power of an odd prime \(p^n\), it is easy to count how many numbers less than \(p^n\) are a residue of it. The following Propositions 1.2.3 and 1.2.4 state this.

**Proposition 1.2.3** Let \(p\) be an odd prime number. Then half of the numbers less than \(p^n\) and not divisible by \(p\) are residue of \(p^n\). The other half are nonresidue of \(p^n\). I.e. there are \(\frac{1}{2}(p-1)p^{n-1}\) residues of \(p^n\) less than \(p^n\) and not divisible by \(p\) and \(\frac{1}{2}(p-1)p^{n-1}\) nonresidues of \(p^n\) less than \(p^n\) and not divisible by \(p\).

**Proof.** A residue \(r\) modulo \(p^n\) needs to be congruent to a square whose square root is less than \(p^n/2\). We have \(\frac{1}{2}(p-1)p^{n-1}\) numbers less than \(p^n/2\) and not divisible by \(p\) and their squares are all different modulo \(p^n\). Indeed, if we have \(a^2 - b^2 = (a-b)(a+b) \equiv 0 \pmod{p}\) then \(p^{n-m} \mid (a-b)\) and \(p^{n} \mid (a+b)\) for some \(m \in \{0, 1, \ldots, n\}\). If \(m = 0\) or \(m = n\) we have that \((a-b)\) or \((a+b)\) is divisible by \(p^n\) but this cannot be possible since \(a, b < p^n/2\). If \(m \neq 0, n\) both \((a+b)\) and \((a-b)\) are divisible by \(p\), so also the sum, \(2a\), and the difference, \(2b\), are divisible by \(p\), so \(a\) and \(b\) need to be divisible by \(p\) and that contradicts our hypothesis. So we can conclude that there are exactly \(\frac{1}{2}(p-1)p^{n-1}\) residues of \(p^n\) less than \(p^n\) and not divisible by \(p\). \(\square\)

**Corollary 1.2.4** Let \(p\) be an odd prime number. Then in the set \(\{1, 2, 3, \ldots, p-1\}\) there are \(\frac{1}{2}(p-1)\) residues of \(p\) and \(\frac{1}{2}(p-1)\) nonresidues of \(p\).

For odd composite numbers, \(P\), there exists a relation between the integers that are residues of \(P\) and the integers that are residues of all prime factors of \(P\). This relation is stated below, in Proposition 1.2.5 and Proposition 1.2.6.

**Proposition 1.2.5** Let \(p\) be an odd prime and \(M\) any number coprime to \(p\). Then \(M\) is a residue of \(p\) if and only if \(M\) is a residue of \(p^n\) for all \(n \in \mathbb{N}\).

**Proof.** Clearly if \(M\) is a residue of \(p^n\) then \(M\) is a residue of \(p\), since

\[x^2 \equiv M \pmod{p^n} \implies x^2 \equiv M \pmod{p}.\]

To prove the other implication let us suppose that \(M\) a residue of \(p^n\) for some \(n \in \mathbb{N}\) and we shall show that \(M\) is also a residue of \(p^{n+1}\). Since \(M\) is a residue of \(p^n\) there is a number \(x\) such that \(x^2 \equiv M \pmod{p^n}\). Let us take \(y = x + pn t\) and impose

\[M \equiv y^2 \equiv (x + pn t)^2 \equiv x^2 + p^2n^2 t^2 + 2xp^n t \pmod{p^{n+1}}.\]

Therefore:

\[M \equiv x^2 + 2xp^n t \pmod{p^{n+1}} \iff M - x^2 \equiv 2xp^n t \pmod{p^{n+1}} \iff M - x^2 \equiv 2x \pmod{p^n} \iff \frac{M - x^2}{p^n} \equiv t \pmod{p^n}.\]

Then, choosing \(t\) satisfying \(t \equiv \frac{M - x^2}{p^n} (2x)^{-1} \pmod{p}\) we obtain an integer \(y\) such that \(y^2 \equiv M \pmod{p^{n+1}}\), and this proves that \(M\) is residue of \(p\).
Hence, if \( M \) is a residue of \( p \) then \( M \) will be a residue of \( p^2 \). But \( M \) will also be a residue of \( p^3 \) and so on. In conclusion, if \( M \) is a residue of \( p \) then \( M \) will be a residue of \( p^n \) for all \( n \in \mathbb{N} \).

**Proposition 1.2.6** Let \( P \) be a composite odd number, and
\[
P = p_1^\alpha_1 p_2^\alpha_2 \cdots p_n^\alpha_n
\]
its prime factorization. Let \( M \) be any odd number. Then \( M \) is a residue of \( P \) if and only if \( M \) is a residue of all prime factors of \( P \), i.e. iff \( M \) is a residue of \( p_1, p_2, \ldots, p_n \).

**Proof.** If \( M \) is a residue of \( P \) then it is also a residue of every prime \( p_i \). Assume that \( M \) is a residue of each \( p_i \). Then, by the Proposition 1.2.5 we know that if \( M \) is a residue of \( p_i \) then \( M \) is also a residue of \( p_i^{\alpha_i} \) for \( i = 1, \ldots, n \). Hence:
\[
\begin{align*}
M \text{ residue of } p_1 &\implies M \text{ residue of } p_1^{\alpha_1} \implies \exists x_1 \text{ such that } x_1^2 \equiv M \pmod{p_1^{\alpha_1}}, \\
M \text{ residue of } p_2 &\implies M \text{ residue of } p_2^{\alpha_2} \implies \exists x_2 \text{ such that } x_2^2 \equiv M \pmod{p_2^{\alpha_2}}, \\
&\vdots \\
M \text{ residue of } p_n &\implies M \text{ residue of } p_n^{\alpha_n} \implies \exists x_n \text{ such that } x_n^2 \equiv M \pmod{p_n^{\alpha_n}}.
\end{align*}
\]
Let us consider the following equations on \( X \):
\[
\begin{align*}
x_1 &\equiv X \pmod{p_1^{\alpha_1}}, \\
x_2 &\equiv X \pmod{p_2^{\alpha_2}}, \\
&\vdots \\
x_n &\equiv X \pmod{p_n^{\alpha_n}}.
\end{align*}
\]
By the Chinese remainder theorem we know that there is an integer \( N \) such that \( N \equiv X \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}} \), i.e. \( N \equiv X \pmod{P} \). Hence:
\[
\begin{align*}
N &\equiv X \equiv x_1 \pmod{p_1^{\alpha_1}} & N^2 &\equiv x_1^2 \equiv M \pmod{p_1^{\alpha_1}}, \\
N &\equiv X \equiv x_2 \pmod{p_2^{\alpha_2}} & N^2 &\equiv x_2^2 \equiv M \pmod{p_2^{\alpha_2}}, \\
&\vdots & &\vdots \\
N &\equiv X \equiv x_n \pmod{p_n^{\alpha_n}} & N^2 &\equiv x_n^2 \equiv M \pmod{p_n^{\alpha_n}}.
\end{align*}
\]
Therefore \( N^2 \equiv M \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}} \), so \( M \) is a residue of \( P \).

1.3. Legendre symbol

The Legendre symbol was introduced by Legendre in 1798 in the book *Essai sur la théorie des nombres* (see [Leg]), in the course of his attempts at proving the quadratic reciprocity law.

**Definition 1.3.1** (Legendre symbol). Let \( p \) be an odd prime number and \( a \) an integer. The Legendre symbol is a function of \( a \) and \( p \) defined as follows:
\[
\left( \frac{a}{p} \right) = \begin{cases} 
0 & \text{if } p \mid a, \\
1 & \text{if } a \text{ is a quadratic residue modulo } p, \\
-1 & \text{if } a \text{ is a quadratic nonresidue modulo } p.
\end{cases}
\]

Legendre’s original definition was the explicit formula:

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

Nowadays this symbol is widely known and, in fact, is the one used when talking about the quadratic reciprocity law. But Legendre introduced the symbol two years later than the year Gauss proved the law for the first time (1796). So, in his papers, Gauss introduced another notation for defining a residue and a nonresidue. Gauss’s notation was the following:

\[
a Rp \quad \text{if } a \text{ is a residue of } p,
\quad a Np \quad \text{if } a \text{ is a nonresidue of } p.
\]

After being defined the Legendre symbol we will show some results related with it.

**Proposition 1.3.2** The Legendre symbol is multiplicative, i.e.

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

**Proof.** If \( ab \) is divisible by \( p \), \( \left( \frac{ab}{p} \right) = 0 \). Moreover, as \( p \) is prime, \( p \) has to divide \( a \), \( b \), or both. So we always have \( \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = 0 \). Then, if \( p \) divides \( ab \), the identity

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

is true.

Now we will study the case that \( p \nmid ab \). If \( a \) and \( b \) are residues modulo \( p \) then

\[
\alpha^2 \equiv a \pmod{p} \quad \text{and} \quad \beta^2 \equiv b \pmod{p} \]

\[
\implies (\alpha\beta)^2 \equiv ab \pmod{p}.
\]

So the product of two residues is a residue.

Note that if \( a \) is a residue modulo \( p \) then \( \frac{1}{a} \) will also be a residue modulo \( p \).

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

Now suppose that \( a \) is a residue and \( b \) is a nonresidue. The proposition says that \( \left( \frac{ab}{p} \right) = -1 \), i.e. \( ab \) has to be a nonresidue and we prove it by contradiction.

Let us suppose that \( ab \) is a residue so \( \alpha^2 \equiv ab \pmod{p} \). Multiplying both sides of the equation by \( \frac{1}{a} \) we get \( \alpha^2/a \equiv b \pmod{p} \). And since \( \frac{1}{a} \) is a residue and the product of two residues is a residue, we have that \( b \) must be a residue and this is a contradiction.
And finally, if $a$ and $b$ are nonresidues, then the product $ab$ has to be a residue. Let us prove it by contradiction. Let us suppose $ab$ is a nonresidue. Now multiply $a$ by all the residues $r$ modulo $p$ and we will get all the residues of the form $ar$. So it must exist $r$ such that $ab \equiv ar \mod p$. Multiplying both sides of the equation by $\frac{1}{a}$ we have $b \equiv r \mod p$. And this is a contradiction because $r$ is a residue and $b$ a nonresidue.

**Proposition 1.3.3** (Euler’s criterion) Let $p$ be a prime number and $a$ an integer, then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$ 

**Proof.** If $a$ is divisible by $p$ then $0 = \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv 0 \mod p$.

Now consider the case in which $a$ is not divisible by $p$. We will work with the elements $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Let $g$ be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, then $g$ is a nonresidue because if not all the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ would be residues and this cannot happen because we saw in Corollary 1.2.4 that half of the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ are residues and half are nonresidues.

$g$ has order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^*$, so $g^{(p-1)/2}$ has order 2 in $(\mathbb{Z}/p\mathbb{Z})^*$. Then $g^{(p-1)/2} = -1$ because this is the only element of order 2 in this group. Therefore, every element $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a power $g^e$ of the generator, and:

$$a^{(p-1)/2} = (g^e)^{(p-1)/2} = (g^{(p-1)/2})^e = (-1)^e = \left(\frac{g}{p}\right)^e = \left(\frac{g^e}{p}\right) = \left(\frac{a}{p}\right).$$

\[\square\]

### 1.4. Quadratic reciprocity law

The law of quadratic reciprocity is a law that gives conditions for the solvability of quadratic equations of the form $x^2 \equiv q \mod p$ where $p$ and $q$ are odd prime numbers. This law also includes two supplementary laws that give conditions for the solvability of quadratic equations of the form $x^2 \equiv -1$ and $x^2 \equiv 2$ both modulo an odd prime $p$.

**Theorem 1.4.1** (Quadratic reciprocity law) Let $p$ be an odd prime number. Then

- **(1st supplementary law)** $x^2 \equiv -1 \mod p$ is solvable $\iff p \equiv 1 \mod 4$.
- **(2nd supplementary law)** $x^2 \equiv 2 \mod p$ is solvable $\iff p \equiv \pm 1 \mod 8$.
- **(Quadratic reciprocity law)** Let $q > 2$ be another odd prime number different from $p$. Let $q^* = \pm q$ where the sign is plus if $q \equiv 1 \mod 4$ and minus if $q \equiv 3 \mod 4$. Then $x^2 \equiv p \mod q$ is solvable if and only if $x^2 \equiv q^* \mod p$ is solvable.
Using Legendre symbols, this theorem can be written as follows

**Theorem 1.4.2** (Quadratic reciprocity law) \( [\text{Written using the Legendre symbols}] \)

Let \( p \) and \( q \) be odd prime numbers. Then

- **(1st supplementary law)** \( \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} \).
- **(2nd supplementary law)** \( \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} \).
- **(Quadratic reciprocity law)** \( \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4} \left( \frac{p}{q} \right) \).

Indeed, Theorem 1.4.1 and Theorem 1.4.2 are equivalent.

- In the first supplementary law, \( x^2 \equiv -1 \pmod{p} \) if and only if \( \left( \frac{-1}{p} \right) = 1 \), and this is satisfied when \((p-1)/2\) is even.
  \((p-1)/2\) is even \iff \( p - 1 \equiv 0 \pmod{4} \iff p \equiv 1 \pmod{4} \).

- In the second supplementary law, \( x^2 \equiv 2 \pmod{p} \) if and only if \( \left( \frac{2}{p} \right) = 1 \), and this is satisfied when \((p^2-1)/8\) is even.
  \((p^2-1)/8\) is even \implies \((p^2-1)/8 \in \mathbb{Z} \implies p^2 \equiv 1 \pmod{8} \implies p \equiv \pm 1 \pmod{8} \).
  And conversely
  \( p \equiv \pm 1 \pmod{8} \implies \exists n \in \mathbb{N} \text{ such that } p = 8n \pm 1 \implies (p^2-1)/8 = ((64n^2 \pm 16n + 1) - 1)/8 = 2(4n^2 \pm n) \text{ is even.} \)

- The quadratic reciprocity law states \( \left( \frac{p}{q} \right) = (-1)^{(p-1)(q-1)} \left( \frac{q}{p} \right) \). Hence, when \( q \equiv 1 \pmod{4} \) we have that \( \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) \) and, indeed, \( x^2 \equiv p \pmod{q} \) is solvable if and only if \( x^2 \equiv q \pmod{p} \) is solvable. But when \( q \equiv 3 \pmod{4} \) we have:
  \( \left( \frac{p}{q} \right) = (-1)^{(p-1)(q-1)/2} \left( \frac{q}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q}{p} \right) = \left( \frac{-q}{p} \right) \).
  Therefore \( x^2 \equiv p \pmod{q} \) is solvable if and only if \( x^2 \equiv -q \pmod{p} \) is solvable.

### 1.5. Jacobi symbol

The Jacobi symbol is a generalization of the Legendre symbol. It was introduced by Jacobi in 1837 in the book *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie* (see [Jac]).
Definition 1.5.1. Let \( n \) be a positive odd integer with prime factorization \( n = \prod p_i^{r_i} \).
For every \( a \in \mathbb{Z} \) let us define the Jacobi symbol
\[
\left( \frac{a}{n} \right) = \prod \left( \frac{a}{p_i} \right)^{r_i}.
\]
I.e. the product of the Legendre symbols for the primes that divide \( n \), counted by multiplicity.

The main difference between the Legendre and the Jacobi symbol is that in this last one, the bottom number must be positive and odd, but does not need to be prime as in the Legendre symbol. If it is prime, the two symbols agree.

Using the Jacobi symbol, the quadratic reciprocity law can be generalized to positive odd integers.

Theorem 1.5.2 (Quadratic reciprocity law for the Jacobi symbol) Let \( n \) and \( m \) be two positive odd integers. Then

- (1st supplementary law)
  \[
  \left( \frac{-1}{n} \right) = (-1)^{(n-1)/2}.
  \]

- (2nd supplementary law)
  \[
  \left( \frac{2}{n} \right) = (-1)^{(n^2-1)/8}.
  \]

- (Quadratic reciprocity law)
  \[
  \left( \frac{m}{n} \right) = (-1)^{(n-1)(m-1)/4} \left( \frac{n}{m} \right).
  \]

Remark 1.5.3. When \( n \) is a prime number then the Jacobi symbol \( \left( \frac{m}{n} \right) \) agrees with the Legendre symbol.

Remark 1.5.4. The symbol \( \left( \frac{m}{n} \right) \) is 0 when \( \gcd(m, n) \neq 1 \).

Remark 1.5.5. When \( m \) is a residue of \( n \) then \( \left( \frac{m}{n} \right) = 1 \) but the converse is not true. In this case \( \left( \frac{m}{n} \right) = 1 \) means that there are an even number of prime factors of \( n \), counted with multiplicity, such that \( m \) is nonresidue of them.

Proposition 1.5.6 If either the top or the bottom argument is fixed, the Jacobi symbol is a completely multiplicative function in the other argument, i.e.

- Fixed \( n \), \( \left( \frac{ab}{n} \right) = \left( \frac{a}{n} \right) \left( \frac{b}{n} \right) \).

- Fixed \( a \), \( \left( \frac{a}{nm} \right) = \left( \frac{a}{n} \right) \left( \frac{a}{m} \right) \).

Proof. The Jacobi symbol is multiplicative in the bottom argument by definition and in the top argument by the multiplicativity of the Legendre symbol. \( \square \)
Chapter 2

Gauss’s first proof

In this chapter we will explain the first proof of the quadratic reciprocity law. This proof can be found in Gauss’s book *Disquisitiones arithmeticae* (see [Gau1]). Originally, Gauss called the quadratic reciprocity law “fundamental theorem” and he stated it, in the article 125 of [Gau1], as follows:

“If \( p \) is a prime number of the form \( 4n + 1 \), then +\( p \) will be a residue or a nonresidue of any prime number which, taken positively, is a residue or a nonresidue of \( p \). But if \( p \) is of the form \( 4n + 3 \), then it will be \( -p \) the one that will have the properties described above.”

Previously, in the articles 108 to 124 he had stated some particular cases, including the two supplementary laws. These had been stated as follows:

“\(-1\) is a quadratic residue of any prime number of the form \( 4n + 1 \), but is a nonresidue of any prime number of the form \( 4n + 3 \).”

“\(2\) is a residue of any prime number of the form \( 8n + 1 \) or \( 8n + 7 \), but is a nonresidue of any prime number of the form \( 8n + 3 \) or \( 8n + 5 \).”

Note that what Gauss stated is equivalent to the theorem in the form that we know it nowadays.

Indeed, by the first supplementary law we know that \( \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} \). Therefore, if \( p \) is of the form \( 4n + 1 \) then \( \left( \frac{-1}{p} \right) = (-1)^{2n} = 1 \), so \( -1 \) is a residue of \( p \).

But if \( p \) is of the form \( 4n + 3 \) then \( \left( \frac{-1}{p} \right) = (-1)^{2n+1} = -1 \), so \( -1 \) is a nonresidue of \( p \).

The second supplementary law states that \( \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} \). Therefore, if \( p \) is of the form \( 8n + 1 \) or \( 8n + 7 \), i.e. \( p \) is of the form \( 8n \pm 1 \), then \( \left( \frac{2}{p} \right) = (-1)^{8n^2 \pm 2n} = 1 \),
so 2 is a residue of p. While if p is of the form $8n + 3$ or $8n + 5$, i.e. $p$ is of the form $8n \pm 3$, then \( \left( \frac{2}{p} \right) = (-1)^{8n^2 \pm 6n + 1} = -1. \)

The quadratic reciprocity law says that \( \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4} \left( \frac{p}{q} \right) \) where p and q are two different odd prime numbers. Then, if p is of the form $4n + 1$,

\[
\left( \frac{q}{p} \right) = (-1) \frac{4n}{2} \frac{4n-1}{2} \left( \frac{p}{q} \right) = (-1)^{2n-1} \left( \frac{p}{q} \right) = \left( \frac{p}{q} \right).
\]

But if p is of the form $4n + 3$

\[
\left( \frac{q}{p} \right) = (-1) \frac{4n}{2} \frac{4n-1}{2} \left( \frac{p}{q} \right) = (-1)^{2n} \left( \frac{p}{q} \right) = \left( \frac{-1}{q} \right) \left( \frac{p}{q} \right) = \left( \frac{-p}{q} \right).
\]

Gauss’s aim was to prove the fundamental theorem for prime numbers, but in fact he ended proving the generalisation of it for any odd number in which the Legendre symbol is replaced by the Jacobi symbol.

### 2.1. First and second supplementary laws

In this section we shall prove the two supplementary laws of the quadratic reciprocity law as Gauss did in his book *Disquisitiones arithmeticae* (see [Gau1]).

**Theorem 2.1.1** (First supplementary law) $-1$ is a quadratic residue of any prime number of the form $4n + 1$, but is a nonresidue of any prime number of the form $4n + 3$.

**Proof.** This theorem can be easily proved using Euler’s criterion [Theorem 1.3.3]. If we have a prime number $p$ of the form $4n + 1$, then:

\[
\left( \frac{-1}{p} \right) \equiv (-1)^{(p-1)/2} = (-1)^{(4n+1-1)/2} = (-1)^{2n} = 1 \pmod{p}.
\]

But, if we have a prime number $p$ of the form $4n + 3$, then:

\[
\left( \frac{-1}{p} \right) \equiv (-1)^{(p-1)/2} = (-1)^{(4n+3-1)/2} = (-1)^{2n+1} = -1 \pmod{p}.
\]

**Theorem 2.1.2** (Second supplementary law) 2 is a residue of any prime number of the form $8n + 1$ or $8n + 7$, but is a nonresidue of any prime number of the form $8n + 3$ or $8n + 5$.

**Proof.** Let us start proving that 2 is a nonresidue of any prime number of the form $8n \pm 3$. We shall prove it by contradiction. Suppose that there exists a prime number of the form $8n \pm 3$ such that 2 is a residue of it. Let $t$ be the smallest prime number of the form $8n \pm 3$ satisfying \( \left( \frac{2}{t} \right) = 1 \), i.e. 2 is a nonresidue of all primes of the form $8n \pm 3$ less than $t$. Moreover 2 is a nonresidue of all $t' < t$ of the form $8n \pm 3$. Indeed, by the Proposition 1.2.6, 2 is a residue of $t'$ if and only if 2 is a
residue of all prime factors of \( t' \), but for being of the form \( 8n \pm 3 \), \( t' \) has at least a prime factor of the form \( 8n \pm 3 \), so 2 is a nonresidue of at least a prime factor of \( t' \), therefore 2 is a nonresidue of \( t' \). Then \( t \) is not only the smallest prime number of the form \( 8n \pm 3 \) such that 2 is nonresidue of \( t \) but also the smallest number of the form \( 8n \pm 3 \) such that 2 is nonresidue of it.

Hence there is an odd number \( a \) less than \( t \) (by Proposition 1.2.2) such that \( 2 \equiv a^2 \pmod{t} \). It implies that \( a^2 = 2 + tu \) with \( u < t \). Since \( a \) is odd, \( a^2 \) is of the form \( 8n + 1 \) because, putting \( a = 2m + 1 \), we have:

\[
a^2 = (2m + 1)^2 = 8(m(m + 1)/2) + 1.
\]

Then \( a^2 - 2 = tu \), and this equality modulo 8 becomes \( 1 - 2 \equiv \mp 3u \pmod{8} \) which implies that \( u \equiv \mp 3 \pmod{8} \). Note now that 2 is also a residue of \( u \), since \( a^2 \equiv 2 \pmod{u} \).

So we found a number \( u < t \) of the form \( 8n \pm 3 \) such that 2 is a residue of it and this contradicts the fact that \( t \) is the minimum number of the form \( 8n \pm 3 \) satisfying this. Hence 2 is nonresidue of any prime number of the form \( 8n \pm 3 \).

Now let us prove that 2 is a residue of any prime number of the form \( 8n + 7 \). In order to do that, we first prove the auxiliary case that states that \(-2\) is a nonresidue of any prime number of the form \( 8n + 5 \) or \( 8n + 7 \). As the previous case, we will prove it by contradiction. Suppose that there exists a prime number of the form \( 8n + 5 \) or \( 8n + 7 \) such that \(-2\) is a residue of it. Let \( t \) be the minimum prime number of the form \( 8n + 5 \) or \( 8n + 7 \) satisfying \( \left( \frac{-2}{t} \right) = 1 \), i.e. \(-2\) is a nonresidue of all primes of the form \( 8n + 5 \) or \( 8n + 7 \) less than \( t \). Moreover \(-2\) is a nonresidue of all \( t' < t \) of the form \( 8n + 5 \) or \( 8n + 7 \). Indeed, by the Proposition 1.2.6, \(-2\) is residue of \( t' \) if and only if \(-2\) is a residue of all prime factors of \( t' \), but all number of the form \( 8n + 5 \) or \( 8n + 7 \) has at least a prime factor of the form \( 8n + 5 \) or \( 8n + 7 \) respectively, so \(-2\) is a nonresidue of at least a prime factor of \( t' \), therefore \(-2\) is a nonresidue of \( t' \). Then \( t \) is not only the minimum prime number of the form \( 8n + 5 \) or \( 8n + 7 \) satisfying that \(-2\) is a residue of \( t \) but also the minimum number of the form \( 8n + 5 \) or \( 8n + 7 \) satisfying that \(-2\) is a residue of it.

Then there is an odd number \( a \) less than \( t \) such that \(-2 \equiv a^2 \pmod{t} \). This implies that \( a^2 = -2 + tu \) with \( u < t \). Since \( a \) is odd, \( a^2 \) is of the form \( 8n + 1 \). So \( a^2 + 2 = tu \), and this equality modulo 8 becomes \( 1 + 2 \equiv 5u \pmod{8} \) if \( t \) is of the form \( 8n + 5 \) or \( 1 + 2 \equiv 7u \pmod{8} \) if \( t \) is of the form \( 8n + 7 \). This implies that \( u \equiv 7 \pmod{8} \) or \( u \equiv 5 \pmod{8} \) respectively. Note that \(-2\) is also a residue of \( u \), since \( a^2 \equiv -2 \pmod{u} \).

So we found a number \( u < t \) of the form \( 8n + 5 \) or \( 8n + 7 \) such that \(-2\) is residue of it and this contradicts the fact that \( t \) is the minimum number of the form \( 8n + 5 \) or \( 8n + 7 \) satisfying this. Hence \(-2\) is a nonresidue of any prime number of the form \( 8n + 5 \) or \( 8n + 7 \). Using the first supplementary law and the multiplicativity property of the Legendre symbol we have

\[
-1 = \left( \frac{-2}{8n + 7} \right) = \left( \frac{-1}{8n + 7} \right) \left( \frac{2}{8n + 7} \right) = -1 \cdot \left( \frac{2}{8n + 7} \right) \Rightarrow \left( \frac{2}{8n + 7} \right) = 1
\]

This proves that 2 is a residue of any prime number of the form \( 8n + 7 \).
Proof. Let \( a \) be any primitive root of a prime number of the form \( 8n + 1 \). So \( a^{8n} \equiv 1 \pmod{8} \) and \( a^{4n} \equiv -1 \pmod{8} \). Indeed the last congruence may be expressed as \((a^{2n} + 1)^2 \equiv 2a^{2n} \pmod{8}\). Then \( 2a^{2n} \) is a residue of \( 8n + 1 \). As \( a^{2n} \) is a square not divisible by \( 8n + 1 \), \( a^{2n} \) is also a residue of \( 8n + 1 \). Hence, by the multiplicativity property of the Legendre symbols we can conclude

\[
1 = \left( \frac{2a^{2n}}{8n+1} \right) = \left( \frac{2}{8n+1} \right) \left( \frac{a^{2n}}{8n+1} \right) = \left( \frac{2}{8n+1} \right) \cdot 1 \implies \left( \frac{2}{8n+1} \right) = 1.
\]

\( \square \)

2.2. Technical lemmas

After having proved the first and the second supplementary laws, we want to prove the quadratic reciprocity law. The problem that for this proof we need to use that every prime number \( p \) of the form \( 4n + 1 \) (taken positively or negatively, except +1) is a nonresidue of some prime number, and if \( p > 5 \) then it is a nonresidue of some prime number less than \( p \). The aim of this section is to prove the above statement. This proof is based in some technical lemmas that we will state below.

Lemma 2.2.1 Let \( a_1, a_2, a_3, \ldots, a_n \) (I) and \( b_1, b_2, b_3, \ldots, b_m \) (II) be two series of numbers not necessarily with the same number of terms. If for every integer \( q \) that is a prime power, \( q \) divides at least as many terms in (I) as the number of terms in (II) that can be divided by \( q \) then:

\[
a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n \quad \text{and} \quad b_1 \cdot b_2 \cdot b_3 \cdot \ldots \cdot b_m \in \mathbb{Z}.
\]

Proof. Let \( A = \prod_{i=1}^{n} a_i \) and \( B = \prod_{i=1}^{m} b_i \). According to the hypothesis of the lemma, it is clear that any prime number \( p \) such that \( p \mid B \), also satisfies \( p \mid A \). Consequently we may express \( A \) and \( B \) as follows

\[
A = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r} \cdot M, \quad B = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r},
\]

where \( M \) is an integer such that \( \gcd(M, p_i) = 1 \) for \( i = 1, \ldots, r \).

Now we will prove that \( a_i \geq b_i \) for \( i = 1 \ldots r \). Let us denote \( c_{ij} \) to the number of terms in the series (I) that are divisible by \( p_i^j \), and \( c'_{ij} \) to the number of terms in the series (II) that are divisible by \( p_i^j \). We have that \( a_i = \sum_{j \geq 1} c_{ij} \) and \( b_i = \sum_{j \geq 1} c'_{ij} \).

By hypothesis we have that \( c_{ij} \geq c'_{ij} \) for every \( i, j \), hence \( a_i \geq b_i \) for \( i = 1, \ldots, r \).

And we have proved that \( A \) is divisible by \( B \). \( \square \)

Lemma 2.2.2 Let 1, 2, 3, \ldots, \( n \) (I) and \( a, a + 1, a + 2, \ldots, a + n - 1 \) (II) be two progressions of \( n \) terms. Then the number of terms in the progression (I) that are divisible by any number \( h \) needs to be greater than or equal to the number of terms in the progression (II) that are divisible by \( h \).
Proof. Let us distinguish two cases:

Case 1: \( n = hm \). In this case there are \( m \) terms in the progression \( (I) \) divisible by \( h \). Then if \( a = hs \) we have \( a + n - 1 = h(s + m) - 1 \), so \( h \cdot s, h(s + 1), \ldots, h(s + m - 1) \) are in \( (II) \) and these are the only ones in \( (II) \) which are divisible by \( h \). Consequently, if \( a = hs \) the progression \( (II) \) has \( m \) terms divisible by \( h \). If \( h(s + 1) > a > h \cdot s \) we have \( h(s + m) - 1 > a + n - 1 > h(s + m - 1) \), so \( h(s + 1), h(s + 2), \ldots, h(s + m) \) are in \( (II) \) and these are the only ones in \( (II) \) which are divisible by \( h \). Consequently, if \( a \neq h \cdot s \), there are \( m \) terms in the progression \( (II) \) divisible by \( h \).

Case 2: \( n = hm + r \), \( 0 < r < h \). In this case there are also \( m \) numbers divisible by \( h \) in the progression \( (I) \). Now if \( hs \geq a \geq hs - r + 1 \) we have \( h(s + m) + r - 1 \geq a + n - 1 \geq h(s + m) \), so the only terms divisible by \( h \) in the progression \( (II) \) are \( hs, h(s + 1), \ldots, h(s + m) \), in all \( m + 1 \) terms. But if \( h(s - 1) < a < hs - r + 1 \) we have \( h(s + m - 1) + r - 1 < a + n - 1 < h(s + m) \), so \( hs, h(s + 1), \ldots, h(s + m - 1) \) are the terms in \( (I) \) which are divisible by \( h \), in all, \( m \) terms.

The Lemma that we have just proved can be stated equivalently as follows:

Lemma 2.2.3 (Equivalent to Lemma 2.2.2) In the progression \( a, a+1, \ldots, a+n-1 \) there are at least as many terms congruent to any given number \( r \) modulo \( h \) as terms in the progression \( 1, 2, \ldots, n \) divisible by \( h \).

Lemma 2.2.4 Let \( a \) be any number of the form \( 8n + 1 \). Let \( p \) be any number such that \( (p,a) = 1 \) and \( \left( \frac{a}{p} \right) = 1 \). Given any integer \( m \) we take the progression \( a, \frac{1}{2}(a-1), 2(a-4), \frac{1}{2}(a-9), 2(a-16), \ldots, 2(a-m^2) \) if \( m \) is even or the progression \( a, \frac{1}{2}(a-1), 2(a-4), \frac{1}{2}(a-9), 2(a-16), \ldots, \frac{1}{2}(a-m^2) \) if \( m \) is odd. Then the number of terms of this progression that are divisible by \( p \) is greater than or equal to the number of terms of the progression \( 1, 2, 3, \ldots, 2m+1 \) that are divisible by \( p \).

Proof. In order to simplify the notation we will refer to the progression \( a, \frac{1}{2}(a-1), \ldots, 2(a-m^2) \) or \( \frac{1}{2}(a-m^2) \) as \( (I) \) and to the progression \( 1, 2, \ldots, 2m+1 \) as \( (II) \). Furthermore \( A \) will denote the number of terms in the progression \( (I) \) that are divisible by \( p \) and \( A' \) the number of terms in the progression \( (II) \) divisible by \( p \). Let us distinguish three cases:

Case 1: \( p=2 \). In this case \( A = m \) because all the terms in \( (I) \) are even except for \( a \). Indeed, if \( i \) is even then \( 2(a - i^2) \) is divisible by \( 2 \) and if \( i \) is odd then \( \frac{1}{2}(a - i^2) = \frac{1}{2}(8n + 1 - (2n' + 1)^2) = \frac{1}{2}(4(2n - n'^2 - n')) = 2(2n - n'(a' + 1)) \) is also divisible by \( 2 \). Now note that between \( 1 \) and \( 2m+1 \) we have \( m \) even numbers, then \( A' = m \). So in this case \( A = A' \).

Case 2: \( p \) is of the form \( p = 2^i(2t + 1) \) with \( i = 0, 1 \) or \( 2 \). We know that \( \left( \frac{a}{p} \right) = 1 \), so there is some \( r \) such that \( a \equiv r^2 \) (mod \( p \)). Now we take the progression \( -m, -(m - 1), -(m - 2), \ldots, -m, m \) which have the same number of terms as \( (II) \). Let us denote this progression as \( (III) \). Then, by Lemma 2.2.3, we have that the number of terms in \( (III) \) that are congruent to \( r \) modulo \( p \) is greater than or
equal to the number of terms in (II) divisible by \( p \). Now let us see that for each term in (III) congruent to \( r \) modulo \( p \) we have a term in (I) divisible by \( p \). First of all note that if \( b \) is a term of (III) such that \( b \equiv r \pmod{p} \) then \( -b \) can’t be congruent to \( r \) modulo \( p \). Suppose that \( b \equiv -b \equiv r \pmod{p} \), then \( 2b \equiv 0 \pmod{p} \) and consequently \( 2a \equiv 2rr \equiv 2bb \equiv 0 \pmod{p} \); but, as \( a \) and \( p \) are coprime, this only can occur when \( p = 2 \), and we discussed this case apart. Continuing with what we wanted to prove, we have that if \( b \) is a term of (III) congruent with \( r \) modulo \( p \) then \( a - bb \equiv rr - rr \equiv 0 \pmod{p} \), i.e. \( a - bb \) is divisible by \( p \). Therefore if \( b \) is even, the term \( 2(a - bb) \) of the progression (I) is divisible by \( p \), and if \( b \) is odd we have that \( b^2 \) is of the form

\[
b^2 = (2s + 1)^2 = 4s(s + 1) + 1 = 8\left(\frac{s(s + 1)}{2}\right) + 1
\]

so \( a - bb \) is divisible by \( 8 \) and, as \( p = 2^i(2t + 1) \) with \( i = 0, 1, 2 \), the quotient \( \frac{a - bb}{p} \) is even and we can conclude that \( \frac{1}{2}(a - bb) \) is an integer, i.e. the term \( \frac{1}{2}(a - b^2) \) of the progression (I) is divisible by \( p \).

Finally we conclude that in the progression (I) there are as many terms divisible by \( p \) as terms in (III) are congruent to \( r \) modulo \( p \), i.e. the number of terms divisible by \( p \) in the progression (I) is greater than or equal to the number of terms in the progression (II) divisible by \( p \).

Case 3: \( p \) is of the form \( p = 8n \). As \( a \equiv r^2 \pmod{p} \), it is also true that \( a \equiv r^2 \pmod{p} \). Now as in the previous case we have that the number of terms in the progression (III) congruent to \( r \) modulo \( p \) is greater than or equal to the number of terms in the progression (II). Note that the terms in (III) that are congruent to \( r \) modulo \( p \) are all different if we take them in absolute value, as it happened in the case 2. Now let us take a term in (III), \( b \), such that \( b \equiv r \pmod{p} \). Then \( b \) also satisfies \( bb \equiv rr \pmod{2p} \), because \( (b - r)(b + r) \) is divisible by \( 2p \) due to the fact that \( (b - r) \) is divisible by \( p \) and \( (b + r) \) is even for being the sum of two odd numbers. Therefore if \( b \) is odd

\[
\frac{1}{2}(a - bb) \equiv \frac{1}{2}(rr - bb) \equiv 0 \pmod{2p}.
\]

i.e. \( \frac{1}{2}(a - bb) \) is divisible by \( p \), and if \( b \) is even \( 2(a - bb) \) is also divisible by \( p \). So as in the previous case we proved that the number of terms in the progression (I) that can be divided by \( p \) is greater than or equal to the number of terms divisible by \( p \) in the progression (II). □

**Proposition 2.2.5** Every prime number \( p \) of the form \( 4n + 1 \) taken positively or negatively (except +1) is nonresidue of some prime number. Moreover, if \( p > 5 \) then it is a nonresidue of some prime less than \( p \).

**Proof.** We have seen in the first supplementary law that \( -1 \) is nonresidue of all primes of the form \( 4n + 3 \). 7 is a prime of the form \( 4n + 3 \) so the proposition is true for \(-1\).
Now let us discuss the case \( p = 5 \). Note that 1 is the only square modulo 3 and \( 5 \equiv 2 \pmod{3} \), so 5 a is nonresidue of 3. And \(-5\) is a nonresidue of 13, since the squares modulo 13 are \( 1, 3, 4, 9, 10, 12 \) but \(-5 \equiv 8 \pmod{13}\).

Now let us suppose that \( p > 5 \) and let us distinguish two different cases:

Case 1: Let \( p \) be a prime number of the form \( 4n + 1 \) taken negatively. Let \( 2a \) be the even number closest to \( \sqrt{p} \) with \( 2a > \sqrt{p} \). For \( p \neq 5, 17 \) it’s true that \( 4a^2 < 2p \). Indeed, expressing \( p \) as \( p = m^2 + k \) with \( m^2 \) the largest square less than \( p \), we have that \( 2a = m + 1 \) or \( 2a = m + 2 \) depending on \( m \) is odd or even. Hence

- If \( m \) is odd \( 4a^2 - 2p = (m + 1)^2 - 2(m^2 + k) = m^2 + 2m + 1 - 2m^2 - 2k = 2(1 - k) - (m - 1)^2 \)
- If \( m \) is even \( 4a^2 - 2p = (m + 2)^2 - 2(m^2 + k) = m^2 + 4m + 4 - 2m^2 - 2k = 2(4 - k) - (m - 1)^2 \).

If \( m \) is odd, since \( k \geq 1 \), it’s clear that \( 4a^2 - 2p < 0 \). While if \( m \) is even, \( m^2 \) is of the form \( 4n \) and \( k \) must be of the form \( 4n + 1 \) since \( p \) is of the form \( 4n + 1 \). Then \( 4a^2 - 2p \geq 0 \) when \( k < 4 \), that implies \( k = 1 \), and when \( (m - 1)^2 < 6 \), i.e. \( m = 2 \) and \( m = 4 \). So when \( p = 2^2 + 1 = 5 \) and when \( p = 4^2 + 1 = 17 \) we have that \( 4a^2 - 2p > 0 \), otherwise \( 4a^2 - 2p < 0 \). We have excluded 5 of this proof and note that \( \pm 17 \) is nonresidue of 5. Hence we can continue the proof for the rest of the primes using the statement \( 4a^2 - 2p < 0 \). It implies that \( 4a^2 - p < p \) with \( 4a^2 - p \) of the form \( 4n + 3 \). Note that \( p \) is a residue of \( 4a^2 - p \) because \( p \equiv 4a^2 \pmod{4a^2 - p} \). Then if \( 4a^2 - p \) is prime, by the first supplementary law and the property of multiplicativity of the Legendre symbol, we have that \( \left( \frac{-p}{4a^2 - p} \right) = -1 \).

And if \( 4a^2 - p \) is composite, since it is of the form \( 4n + 3 \), \( 4a^2 - p \) has at least a prime factor \( q \) of the form \( 4n + 3 \), because if not it would be of the form \( 4n + 1 \). Then \( p \) is a residue of \( q \) and \( -p \) is nonresidue of \( q < p \).

Case 2: Let \( p \) be a prime number taken positively. Now let us discuss two cases:

Case i): \( p \) is a prime number of the form \( 8n + 5 \). Let \( a \) be a positive number such that \( a < \sqrt{\frac{1}{2}p} \). Then it is easy to see that \( p - 2a^2 > 0 \). If \( a \) is even, \( p - 2a^2 \) is of the form:

\[ p - 2a^2 = 8n + 5 - 2(2m)^2 = 8n + 5 - 8m^2 = 8(n - m) + 5 = 8n' - 3, \]

and if \( a \) is odd, \( p - 2a^2 \) is of the form:

\[ p - 2a^2 = 8n + 5 - 2(2m + 1)^2 = 8n + 5 - 8m^2 - 8m - 2 = 8(n - m^2 - m) + 3 = 8n' + 3. \]

It shows to us that \( p - 2a^2 \) must have a prime factor, \( q \), of the form \( 8n \pm 3 \) because the product of numbers of the form \( 8n \pm 1 \) can’t be a number of the form \( 8n \pm 3 \). Then \( p - 2a^2 \equiv 0 \pmod{q} \), i.e. \( p \equiv 2a^2 \pmod{q} \) and it would be satisfied that \( \left( \frac{p}{q} \right) = \left( \frac{2a^2}{q} \right) \). By the second supplementary law (see Theorem 2.1.2) we know
Indeed contradiction. So we found some numbers less than 1 that multiplied are equal to 1, which is a divisible by 1.

II divisible by the product of the terms of (I). Now let us take the series $p, \frac{q}{2}(p - 1), 2(p - 4), \ldots, 2(p - m^2)$ or $2(p - m^2)$ (I) depending on if $m$ is odd or even and the series $1, 2, 3, \ldots, 2m + 1$ (II). By Lemma 2.2.4 we have that the number of terms in (I) which are divisible by any number less than $2\sqrt{p}$ is at least the number of terms in (II) divisible by that number. And by Lemma 2.2.1 we know that the product of the terms of the progression (I) is divisible by the product of the terms of (II). Note that the product of the terms of (I) is

$$p(p - 1)(p - 4)\ldots(p - m^2) \quad \text{if } m \text{ is even or}$$

$$\frac{p(p - 1)(p - 4)\ldots(p - m^2)}{2} \quad \text{if } m \text{ is odd.}$$

In both cases he have that

$$\frac{p(p - 1)(p - 4)\ldots(p - m^2)}{1 \cdot 2 \cdot 3 \ldots \cdot (2m + 1)} \in \mathbb{Z}.$$ 

As $p$ is prime, $p$ is coprime to all the terms in (II), therefore $(p - 1)(p - 4)\ldots(p - m^2)$ is also divisible by $1 \cdot 2 \cdot \ldots \cdot (2m + 1)$. Now note that the product of the terms of (II) can be expressed as follow

$$1 \cdot 2 \cdot \ldots \cdot (2m + 1) = (m + 1)((m + 1)^2 - 1) \ldots \cdot ((m + 1)^2 - m^2).$$

Indeed $(m + (n + 1))(m - (n - 1)) = m^2 + 2m + 1 - n^2 = (m + 1)^2 - n^2.$

Therefore we have that

$$\frac{1}{m + 1} \cdot \frac{p - 1}{(m + 1)^2 - 1} \cdot \frac{p - 4}{(m + 1)^2 - 4} \ldots \cdot \frac{p - m^2}{(m + 1)^2 - m^2} \in \mathbb{Z}.$$ 

Note that the factors of this product are all less than 1 because $p$ is prime, what implies that $\sqrt{p}$ is irrational, and we have taken $m$ as the number less than $\sqrt{p}$ closest to it, so it is true that $m + 1 > \sqrt{p}$ and consequently $(m + 1)^2 > p$. Hence we found some numbers less than 1 that multiplied are equal to 1, which is a contradiction. So $p$ is a nonresidue of some prime number less than $2\sqrt{p} + 1$. □

2.3. Quadratic reciprocity law for odd integers

In the original proof of the theorem Gauss introduced the following notation:
\* a, a', a'', \ldots denotes primes of the form 4n + 1.
\* b, b', b'', \ldots denotes primes of the form 4n + 3.
\* A, A', A'', \ldots denotes numbers, not necessarily primes, of the form 4n + 1.
\* B, B', B'', \ldots denotes numbers, not necessarily primes, of the form 4n + 3.
\* xRy denotes that x is residue of y.
\* xNy denotes that x is nonresidue of y.

And using this notation the fundamental theorem can be rewritten as follows:

\[
\begin{align*}
1. \quad aRa' \ldots & \quad a'Ra \\
2. \quad aNa' \ldots & \quad a'Na \\
3. \quad aRb \ldots & \quad -bRa \\
4. \quad aNb \ldots & \quad -bNa \\
5. \quad bRa \ldots & \quad aRb \\
6. \quad bNa \ldots & \quad aNb \\
7. \quad bRb' \ldots & \quad -b'Rb \\
8. \quad bNb' \ldots & \quad -b'Nb
\end{align*}
\]

Gauss proved the fundamental theorem by induction. He supposed that the theorem is true until a certain prime and he proved that the theorem is still true for the next prime. But in one of the steps of the proof, Gauss used that if the fundamental theorem is true until a certain prime then the fundamental theorem is also true for all pair of odd integers less than the next prime, since their factorization only involves primes such that the fundamental theorem is true for them. Hence, we will dedicate this section to prove that the "fundamental theorem" is true for every pair of integers supposing that the fundamental theorem is true for every pair of primes.

First of all we prove the following proposition:

**Proposition 2.3.1** Let a, b be odd prime numbers of the form 4n + 1 and 4n + 3 respectively, and let A, B be odd integers of the form 4n + 1 and 4n + 3 respectively. Then:

\[
\begin{align*}
1. \quad aRA \ldots & \quad ARa, \\
2. \quad aRB \ldots & \quad -BRa, \\
3. \quad bRA \ldots & \quad ARb, \\
4. \quad bRB \ldots & \quad -BRb.
\end{align*}
\]

**Proof.** Let us factorise A and B (we omitted the exponents so the factors may be repeated):

\[
A = a_1a_2 \ldots a_nb_1b_2 \ldots b_{2m}, \quad B = a'_1a'_2 \ldots a'_nb'_1b'_2 \ldots b'_{2m'+1}.
\]

By the Proposition 1.2.6 we know that if p is an odd prime number and P is an odd integer such that p is a residue of it, then p is residue of all prime factors of P.
2. GAUSS’S FIRST PROOF

In the first and the second case, \( a \) is a residue of all prime factors of \( A \) and \( B \) respectively. Suppose that the fundamental theorem is true, so we can assure that if \( a \) is a residue of \( A \), then all the prime factors of \( A \) are also residues of \( a \), and in the same way if \( a \) is a residue of \( B \), then all the prime factors of \( B \) are also residues of \( a \). Finally by the multiplicativity of the Legendre symbol we conclude that \( \left( \frac{A}{a} \right) = 1 \) and \( \left( -\frac{B}{a} \right) = \left( \frac{B}{a} \right) = 1 \).

In the third and the fourth case, \( b \) is a residue of all prime factors of \( A \) and \( B \) respectively. Suppose that the fundamental theorem is true, so we can assure that if \( b \) is a residue of \( A \), then the prime factors of \( A \) of the form \( 4n + 1 \) are residues of \( b \) and the prime factors of the form \( 4n + 3 \) are nonresidues of \( b \), in the same way if \( b \) is a residue of \( B \), then the prime factors of \( B \) of the form \( 4n + 1 \) are residues of \( b \) and the prime factors of the form \( 4n + 3 \) are nonresidues of \( b \). Remember \( A \) must have an even number of prime factors of the form \( 4n + 3 \) while \( B \) must have an odd number of them. So by the multiplicativity of the Legendre symbol we conclude that \( \left( \frac{A}{b} \right) = 1 \) and \( \left( -\frac{B}{b} \right) = -1 \), that implies \( \left( -\frac{B}{b} \right) = 1 \). \( \square \)

Let \( P \) and \( Q \) be two odd numbers and let us define the following notation:

\[
[P, Q] = \text{Number of prime factors of } Q, \text{ taken positively and counted with multiplicity, such that } P \text{ is nonresidue of them. (Note that } \left[ P, Q \right] = \left[ P, -Q \right] = \left[ P, |Q| \right] \text{ since the sign of } Q \text{ doesn’t matter.)}
\]

\[
[[P, Q]] = \text{The number of pairs } q_i, p_j, \text{ (prime factors of } Q \text{ and } P \text{ respectively), such that } \left( \frac{q_i}{p_j} \right) = -1.
\]

**Proposition 2.3.2** Let \( P, Q \) be two integers. Then

\[
\begin{align*}
\{ P = A \} & \cup \{ Q = A' \}, & \{ P = A \} & \cup \{ Q = -A' \} \\
\{ P = A \} & \cup \{ Q = B \}, & \{ P = A \} & \cup \{ Q = -B \} \\
\{ P = -A \} & \cup \{ Q = A' \}, & \{ P = B \} & \cup \{ Q = -B' \} \\
\end{align*}
\]

implies \([P, Q] \equiv [Q, P] \pmod{2} \), i.e. \([P, Q] \text{ and } [Q, P] \) have the same parity,

and

\[
\begin{align*}
\{ P = -A \} & \cup \{ Q = B \}, & \{ P = -A \} & \cup \{ Q = -B \} \\
\{ P = B \} & \cup \{ Q = A' \}, & \{ P = -B \} & \cup \{ Q = -B' \} \\
\end{align*}
\]

implies \([P, Q] \not\equiv [Q, P] \pmod{2} \), i.e. \([P, Q] \text{ and } [Q, P] \) have different parity.

**Proof.** Let us factorise \( P \) and \( Q \) in prime factors

\[
P = p_1 p_2 \ldots p_n, \quad Q = q_0 q_1 q_2 \ldots q_m,
\]

where \( q_0 = 1 \) when \( Q \) is positive and \( q_0 = -1 \) when \( Q \) is negative.
Therefore,\[ [[Q,P]] = \sum_{j=1}^{n} \left( \sum_{i=0}^{m} [q_i, p_j] \right), \]

Since \( q_i \) and \( p_j \) are prime, \([q_i, p_j] = 0\) when \( q_i \) is a residue of \( p_j \) and \([q_i, p_j] = 1\) when \( q_i \) is a nonresidue of \( p_j \). Hence \( k_j \) counts how many prime factors of \( Q \) are nonresidues of \( p_j \). If \( k_j \) is even, \( Q \) is a residue of \( p_j \), but if \( k_j \) is odd, \( Q \) is a nonresidue of \( p_j \). Then \([Q,P]\) counts how many \( k_j \) are odd.

Therefore \([Q,P] = k_1 + k_2 + \cdots + k_n\). Rearranging the summands we get:

\[
[[Q,P]] = 2k'_1 + \cdots + 2k'_{n-[Q,P]} + (2k'_{n-[Q,P]}+1) + \cdots + (2k'_n + 1)
\]

\[
= 2K + [Q,P]
\]

Hence \([Q,P]\) and \([Q,P]\) have the same parity.

Now let us consider \( P \) any odd positive integer and \( Q \) an integer of the form \( A \) or \( -B \). Factorise \( P \) and \( Q \) in prime factors:

\[
P = a_1a_2\ldots a_nb_1b_2\ldots b_{2m}, \quad Q = a'_1a'_2\ldots a'_mb'_1b'_2\ldots b'_{2m+1}.
\]

By the fundamental theorem \([[Q,P]] = [[P,Q]]\). Indeed,

\[
\left( \frac{a_i}{a'_i} \right) = \left( \frac{a'_j}{a_j} \right) = -1 \iff \left( \frac{a_i}{a'_i} \right) = -1,
\]

\[
\left( \frac{b_i}{b'_i} \right) = \left( \frac{b'_j}{b_j} \right) = -1 \iff \left( \frac{b_i}{b'_i} \right) = -1.
\]

And we saw before that \([Q,P] \equiv [[Q,P]] \pmod 2\) and \([P,Q] \equiv [[P,Q]] \pmod 2\).

Hence:

\[
[[Q,P]] = [[Q,P]] \equiv [P,Q] \equiv [P,Q] \pmod 2,
\]

and we can conclude that in the cases \( \{P = A, Q = A'\}, \{P = B, Q = A\}, \{P = A, Q = -B\} \) and \( \{P = B, Q = -B'\}, [P,Q] \) and \([Q,P]\) have the same parity.

Let \( P \) and \( Q \) be any odd integers, and let

\[
|P| = a_1a_2\ldots a_nb_1b_2\ldots b_{2m}, \quad Q = a'_1a'_2\ldots a'_mb'_1b'_2\ldots b'_{2m+1}
\]

be their prime factorization. Let us introduce the following notation:

- \( \theta : \# \left\{ a_i \mid a_i \text{ a prime factor of } |P| \text{ of the form } 4n+1 \text{ such that } \left( \frac{Q}{a_i} \right) = 1 \right\} \)
- \( \chi : \# \left\{ b_i \mid b_i \text{ a prime factor of } |P| \text{ of the form } 4n+3 \text{ such that } \left( \frac{Q}{b_i} \right) = 1 \right\} \)
\[2. \text{ GAUSS'S FIRST PROOF}\]

- \(\psi : \# \left\{ a_i \mid \text{a prime factor of } |P| \text{ of the form } 4n + 1 \text{ such that } \left( \frac{Q}{a_i} \right) = -1 \right\}\]
- \(\omega : \# \left\{ b_i \mid \text{a prime factor of } |P| \text{ of the form } 4n + 3 \text{ such that } \left( \frac{Q}{b_i} \right) = -1 \right\}\)

Then it is easy to see that \([Q,P] = \psi + \omega\) and \([-Q,P] = \chi + \psi\). Note that if \(P = A\) then \(\chi + \omega\) is even, since \(P = A\) must have an even number of prime factors of the form \(4n + 3\), and \(\chi - \omega\) is also even, since

\[
\chi - \omega = \frac{(\chi + \omega) - (2\omega)}{\text{even even}}.
\]

Then, when \(P = A\), by the equation:

\([-Q,P] = [Q,P] + \chi - \omega\),

we can conclude that \([Q,P]\) and \([-Q,P]\) have the same parity. Now let us consider the cases: \(\{P = A, Q = A'\}\) and \(\{P = A, Q = B\}\).

We saw before that in both cases \([P,Q]\) and \([Q,P]\) have the same parity. Moreover \([Q,P]\) and \([-Q,P]\) have also the same parity, since \(P = A\). Hence \([P,Q] = [P,-Q]\) and \([-Q,P]\) have the same parity, i.e.

\[
\begin{align*}
\{ P = A \\
Q = -A' \} & \implies [P,Q] \equiv [Q,P] \pmod{2}, \\
\{ P = A \\
Q = B \} & \implies [P,Q] \equiv [Q,P] \pmod{2}.
\end{align*}
\]

By the case \(\{P = -A, Q = A'\}\) (which is equivalent to the case \(\{P = A, Q = -A'\}\)) we have that \([Q,P]\) and \([P,Q]\) have the same parity. Moreover, since \(|P| = A\), we have that \([Q,P]\) and \([-Q,P]\) have the same parity. Hence:

\[
\begin{align*}
\{ P = -A \\
Q = -A' \} & \implies [P,Q] \equiv [Q,P] \pmod{2}.
\end{align*}
\]

Otherwise, when \(P = B\) then \(\chi + \omega\) is odd, since \(P = B\) must have an odd number of prime factors of the form \(4n + 3\), and \(\chi - \omega\) is also odd, since

\[
\chi - \omega = \frac{(\chi + \omega) - (2\omega)}{\text{odd even}}.
\]

By the equation

\([-Q,P] = [Q,P] + \chi - \omega\),

we can conclude that \([Q,P]\) and \([-Q,P]\) have the same parity. Now let us consider the cases: \(\{P = B, Q = A\}\) and \(\{P = B, Q = -B'\}\).

We saw before that in both cases \([P,Q]\) and \([Q,P]\) have the same parity, but since \(P = B\), we also have that \([Q,P]\) and \([-Q,P]\) have different parity. Hence \([P,Q] = [P,-Q]\) and \([-Q,P]\) have different parity, i.e.
2.3. QUADRATIC RECIPROCITY LAW FOR ODD INTEGERS

\[
\begin{align*}
\{ P = B \quad Q = -A \} & \quad \implies [P, Q] \neq [Q, P] \quad \text{(mod 2)}, \\
\{ P = B \quad Q = B' \} & \quad \implies [P, Q] \neq [Q, P] \quad \text{(mod 2)}. 
\end{align*}
\]

By the cases \( \{ P = -B, Q = A \} \) and \( \{ P = -B, Q = B' \} \) (which are equivalent to the cases \( \{ P = A, Q = -B \} \) and \( \{ P = -B, Q = B' \} \)) we have that in both cases \([Q, P]\) and \([P, Q]\) have the same parity. Moreover, since \(|P| = B\), we have that \([Q, P]\) and \([-Q, P]\) have different parity. Hence:

\[
\begin{align*}
\{ P = -B \quad Q = -A \} & \quad \implies [P, Q] \neq [Q, P] \quad \text{(mod 2)}, \\
\{ P = -B \quad Q = -B' \} & \quad \implies [P, Q] \neq [Q, P] \quad \text{(mod 2)}. 
\end{align*}
\]

\(\square\)

Note that, when \( P \) and \( Q \) are both positive, \((-1)^{[P,Q]}\) agrees with the Jacobi symbol \(\left(\frac{P}{Q}\right)\). Indeed, if \( \prod_{i=1}^{m} q_i \) is the prime factorization of \(Q\),

\[
\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right) \left(\frac{P}{q_2}\right) \cdots \left(\frac{P}{q_m}\right) = (-1)^{[P,Q]}.
\]

Remember that the quadratic reciprocity law for Jacobi symbols (Theorem 1.5.2) states:

\[
\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2} \frac{Q-1}{2}} \left(\frac{Q}{P}\right).
\]

Then \(\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)\) in the cases \( \{ P = A, Q = A' \} \), \( \{ P = A, Q = B \} \) and \( \{ P = B, Q = A \} \) (note that these last two cases are virtually the same, so it suffices to consider only one of them; we will only consider \( \{ P = A, Q = B \} \)), and \(\left(\frac{P}{Q}\right) = -\left(\frac{Q}{P}\right)\) in the case \( \{ P = B, Q = B' \} \). But in Proposition 2.3.2 we proved that in cases \( \{ P = A, Q = A' \} \) and \( \{ P = A, Q = B \} \), \([Q, P]\) and \([P, Q]\) have the same parity, and in the case \( \{ P = B, Q = B' \} \), \([Q, P]\) and \([P, Q]\) have different parity. Hence this proves the quadratic reciprocity law for positive integer numbers (using the Jacobi symbol). Notice that, in fact, Gauss proved something stronger than the quadratic reciprocity law for the Jacobi symbol, since the Proposition 2.3.2 involves positive and negative integers.

It is very important to remark that in the proof of the Proposition 2.3.2 we only used that the fundamental theorem is true for the prime factors of \( P \) and \( Q \), the proof didn’t involve any prime greater than \( P \) or \( Q \).
2.4. Quadratic reciprocity law for odd primes

In this section we shall prove the quadratic reciprocity law for odd primes, the one that Gauss called “fundamental theorem”. Using his notation, the fundamental theorem is stated as follows:

\[
\begin{align*}
1. & \ aR_a' \ \ldots \ a'R_a \\
2. & \ aN_a' \ \ldots \ a'Na \\
3. & \ aR_b \ \ldots \ -bRa \\
4. & \ aNb \ \ldots \ -bNa \\
5. & \ bRa \ \ldots \ aRb \\
6. & \ bNa \ \ldots \ aNb \\
7. & \ bRb' \ \ldots \ -b'Rb \\
8. & \ bNb' \ \ldots \ -b'Nb
\end{align*}
\]

(2.4.1)

Gauss proved the fundamental theorem by induction. So we will suppose that the theorem is true until a certain prime and we will prove that the theorem is still true until the next prime. But in order to apply this we need a base case. For the base case it is enough to prove that the theorem is true for all odd primes less than or equal to five:

\[\left(\frac{3}{5}\right) = -1 = (\frac{-1}{5})^{\frac{5-1}{2}} \cdot \left(\frac{5}{3}\right).\]

The case above is the only one that involves only odd primes \(\leq 5\) and it satisfies the fundamental theorem. Hence we can pass to the inductive step.

Let \(3, 5, 7, 11, \ldots, P_t, P_{t+1}, \ldots\) be the sequence of odd prime numbers. And let us suppose that the fundamental theorem is true until \(P_t\), i.e. the theorem is true for all pairs of primes \(p, q\) less than or equal to \(P_t\). Note that from Proposition 2.3.2 we have that the fundamental theorem is true for all positive odd integer less than \(P_{t+1}\).

Now let us take a pair of odd prime numbers, \(p \leq P_t\) and \(q = P_{t+1}\); and try to prove that the theorem is also true for them.

Now we shall prove the fundamental theorem itself:

**Cases 1, 3, 5 and 7 of (2.4.1).** In all cases \(p\) is a residue of \(q = P_{t+1}\), i.e. there exists \(e\) such that \(p \equiv e^2 \mod q\). Since \(q\) is odd, \(p \equiv x^2 \mod q\) has two solutions smaller than \(q\), one odd and one even, so let us take \(e < q\) and even. Now we distinguish two subcases:

**Subcase 1:** \(p \mid e\) (that implies \(p \mid e^2\)). We have \(e^2 = p + qf\) with \(f > 0, f < q\) since \(e < q\) and \(p \mid f\) since \(p \mid e^2\). Then \(f\) is of the form \(4n + 1\) when

\[
\begin{align*}
\{ p = 4n + 3 \\
q = 4n + 1
\}
\end{align*}
\]

or

\[
\begin{align*}
\{ p = 4n + 1 \\
q = 4n + 3
\}
\end{align*}
\]
and \( f \) is of the form \( 4n + 3 \) when

\[
\begin{align*}
\begin{cases}
p = 4n + 1 \\
q = 4n + 1 \\
f = 4n + 3
\end{cases}
\quad \text{or} \quad
\begin{cases}
p = 4n + 3 \\
q = 4n + 3
\end{cases}
\end{align*}
\]

It is true that \( e^2 \equiv p \pmod{f} \), so \( \left( \frac{p}{f} \right) = 1 \). Since \( p \) and \( f \) are both smaller than \( q \), the fundamental theorem is true for them, hence:

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

Therefore, \( \left( \frac{f}{p} \right) = -1 \) when both \( f \) and \( p \) are of the form \( 4n + 3 \), otherwise \( \left( \frac{f}{p} \right) = 1 \). But it is also true that \( e^2 \equiv qf \pmod{p} \), so \( \left( \frac{qf}{p} \right) = 1 \). By the multiplicity of the Legendre symbol \( \left( \frac{qf}{p} \right) = \left( \frac{q}{p} \right) \left( \frac{f}{p} \right) \). And for the four different cases we have:

1. \( \begin{cases} p = 4n + 1 \\
q = 4n + 1 \\
f = 4n + 3 \end{cases} \quad \Rightarrow \quad \left( \frac{q}{p} \right) \left( \frac{f}{p} \right) = 1 \quad \Rightarrow \quad \left( \frac{q}{p} \right) \cdot 1 = 1 \quad \Rightarrow \quad \left( \frac{q}{p} \right) = 1,
\]

2. \( \begin{cases} p = 4n + 1 \\
q = 4n + 3 \\
f = 4n + 3 \end{cases} \quad \Rightarrow \quad \left( \frac{-q}{p} \right) \left( \frac{f}{p} \right) = 1 \quad \Rightarrow \quad \left( \frac{-q}{p} \right) \cdot 1 = 1 \quad \Rightarrow \quad \left( \frac{-q}{p} \right) = 1,
\]

3. \( \begin{cases} p = 4n + 3 \\
q = 4n + 1 \\
f = 4n + 3 \end{cases} \quad \Rightarrow \quad \left( \frac{q}{p} \right) \left( \frac{f}{p} \right) = 1 \quad \Rightarrow \quad \left( \frac{q}{p} \right) \cdot 1 = 1 \quad \Rightarrow \quad \left( \frac{q}{p} \right) = 1,
\]

4. \( \begin{cases} p = 4n + 3 \\
q = 4n + 3 \\
f = 4n + 3 \end{cases} \quad \Rightarrow \quad \left( \frac{-q}{p} \right) \left( \frac{f}{p} \right) = -1 \quad \Rightarrow \quad \left( \frac{-q}{p} \right) \cdot (-1) = -1 \quad \Rightarrow \quad \left( \frac{-q}{p} \right) = 1.
\]

**Subcase 2:** \( p \mid e \) (that implies \( p \mid e^2 \)). We have \( e = pq \) and \( e^2 = p^2 q^2 = p + qh \). Hence simplifying \( p \) in the equation we obtain \( pq^2 = 1 + qh \), where \( h \) is smaller than \( q \) and prime with \( p \) and \( g^2 \). Then \( h \) is of the form \( 4n + 1 \) when

\[
\begin{cases}
p = 4n + 3 \\
q = 4n + 1
\end{cases}
\quad \text{or} \quad
\begin{cases}
p = 4n + 3 \\
q = 4n + 3
\end{cases}
\]

and \( h \) is of the form \( 4n + 3 \) when

\[
\begin{cases}
p = 4n + 1 \\
q = 4n + 1
\end{cases}
\quad \text{or} \quad
\begin{cases}
p = 4n + 3 \\
q = 4n + 1
\end{cases}
\]

It is true that \( pg^2 \equiv 1 \pmod{h} \), so \( \left( \frac{pg^2}{h} \right) = 1 \) that implies \( \left( \frac{p}{h} \right) = 1 \) because

\[
\left( \frac{g^2}{h} \right) = 1.
\]

Since \( p \) and \( h \) are both smaller than \( q \), the fundamental theorem is true for them, hence:

\[
\left( \frac{h}{p} \right) = (-1)^{\frac{h-1}{2}} \frac{p}{h} = (-1)^{\frac{h-1}{2}} \frac{p}{h}.
\]
Therefore, \((h/p) = -1\) when both \(h\) and \(p\) are of the form \(4n + 3\), otherwise \((h/p) = 1\). But is also true that \(-qh \equiv 1 \pmod{p}\), so \((-qh/p) = 1\). By the multiplicity of the Legendre symbol \((-qh/p) = (1/p)(q/p)(h/p)\). And for the four different cases we have:

\[
\begin{align*}
(1) \quad & \begin{cases} p = 4n + 1 \\ q = 4n + 1 \\ h = 4n + 3 \end{cases} \implies (qh/p) = 1 \implies 1 \cdot (q/p) \cdot 1 = 1 \implies (q/p) = 1, \\
(3) \quad & \begin{cases} p = 4n + 1 \\ q = 4n + 3 \\ h = 4n + 1 \end{cases} \implies (qh/p) = 1 \implies (q/p) \cdot 1 = 1 \implies (q/p) = 1, \\
(5) \quad & \begin{cases} p = 4n + 3 \\ q = 4n + 1 \\ h = 4n + 3 \end{cases} \implies (qh/p) = 1 \implies (-1) \cdot (q/p) \cdot (-1) = 1 \implies (q/p) = 1, \\
(7) \quad & \begin{cases} p = 4n + 3 \\ q = 4n + 3 \\ h = 4n + 1 \end{cases} \implies (qh/p) = 1 \implies (q/p) \cdot 1 = 1 \implies (q/p) = 1.
\end{align*}
\]

**Cases 4 and 8 of (2.4.1).** In both cases \(p\) is nonresidue of \(q = P_{t+1}\), which is of the form \(4n + 3\). Hence:

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

We saw that \(-p\) is a residue of \(q\), so there exists an \(e\) such that \(-p \equiv e^2 \pmod{q}\). As \(q\) is odd, \(p \equiv x^2 \pmod{q}\) has two solutions smaller than \(q\), one odd and one even, so let us take \(e < q\) and even. Now distinguish two subcases:

**Subcase 1:** \(p \not| e\). We have \(e^2 = -p + qf\) where \(f\) is a positive number, coprime to \(p\) and smaller than \(q\). Moreover \(f\) is of the form \(4n + 3\) when \(p = 4n + 1\) and of the form \(4n + 1\) when \(p = 4n + 3\). By the equation \(e^2 = -p + qf\) we deduce that \((h/p) = 1\) and since \(p\) and \(f\) are both less than \(q\), the fundamental theorem is true for them. So when \(f\) is of the form \(4n + 1\) then \((f/p) = 1\), and when is of the form \(4n + 3\) then \((f/p) = -1\). We also deduce that \((qf/p) = 1\), so considering the two cases we are studying we have:

\[
\begin{align*}
(4) \quad & \begin{cases} p = 4n + 1 \\ q = 4n + 3 \\ f = 4n + 3 \end{cases} \implies (qf/p) = 1 \implies (q/p) \cdot (f/p) = 1 \implies (q/p) = -1, \\
(8) \quad & \begin{cases} p = 4n + 3 \\ q = 4n + 3 \\ f = 4n + 1 \end{cases} \implies (qf/p) = -1 \implies (q/p) \cdot (f/p) = -1 \implies (q/p) = -1.
\end{align*}
\]
Subcase 2: $p \mid e$. We have $e = pg$ and $e^2 = p^2g^2 = -p + qph$. Hence simplifying $p$ in the equation we obtain $pg^2 = -1 + qh$, where $h$ is a positive number less than $q$, coprime to $p$ and $g^2$, and of the form $4n + 3$. From $e^2 = -p + qph$ we deduce \( \left( \frac{-p}{h} \right) = 1 \), that implies \( \left( \frac{p}{h} \right) = -1 \). Since $p$ and $h$ are both less than $q$, the fundamental theorem is true for them, so we have \( \left( \frac{-h}{p} \right) = -1 \) in both cases ($p = 4n + 1$ and $p = 4n + 3$). Now from $pg^2 = -1 + qh$ we deduce $1 \equiv qh \pmod{p}$, so \( \left( \frac{qh}{p} \right) = 1 \), and considering the two cases we are studying we have:

\[
\begin{align*}
\{ p = 4n + 1, q = 4n + 3, h = 4n + 3 \} & \implies \left( \frac{qh}{p} \right) = 1 \implies \left( \frac{-q}{p} \right) \cdot \left( \frac{-h}{p} \right) = 1 \implies \left( \frac{-q}{p} \right) = -1, \\
\{ p = 4n + 3, q = 4n + 3, h = 4n + 3 \} & \implies \left( \frac{qh}{p} \right) = 1 \implies \left( \frac{-q}{p} \right) \cdot \left( \frac{-h}{p} \right) = 1 \implies \left( \frac{-q}{p} \right) = -1.
\end{align*}
\]

Cases 2 and 6. In both cases $p$ is a nonresidue of $q$ which is of the form $4n + 1$. By the Proposition 2.2.5 there is a prime number less than $q$, say $q'$, such that \( \left( \frac{q}{q'} \right) = -1 \). $q'$ could be of the form $4n + 1$ or $4n + 3$ and by the reciprocal of the cases 1 and 5, that we have already proved, we have that also $\left( \frac{q'}{q} \right) = -1$. Hence

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

So $q'p$ is a residue of $q$ and there is an even number $e$, $e < q$, such that $e^2 \equiv q'p \pmod{q}$. Now let us consider four subcases:

Subcase 1: $p \nmid e$ and $q' \nmid e$. Then $e^2 = q'p \pm qf$, with $f$ a positive number less than $q$ and coprime to $p$ and $q'$. Note that as we have defined $e^2$ we will take the positive sign when $q'p < e^2$ and the negative otherwise. Let us study these different cases separately.

- **Case (1.A).** $q'p < e^2$, so $e^2 = q'p + qf$. In this case, $f$ will be of the form $4n + 1$ when

\[
\begin{cases}
p = 4n + 1 \\
q' = 4n + 3
\end{cases}
\text{ or } \begin{cases}
p = 4n + 3 \\
q' = 4n + 1
\end{cases},
\]

and of the form $4n + 3$ when

\[
\begin{cases}
p = 4n + 1 \\
q' = 4n + 1
\end{cases}
\text{ or } \begin{cases}
p = 4n + 3 \\
q' = 4n + 3
\end{cases}.
\]

Note that $q'p \equiv e^2 \pmod{f}$, so $q'p$ is a residue of $f$ and by the Proposition 1.2.6 $q'p$ is a residue of all prime factors of $f$. Hence $[q'p, f] = 0$. Now let us study the value of $[f, q'p]$. Note that, since $q'p$ has only two prime factors,
[f, q′p] = 0, 1 or 2. Therefore, studying the different cases and according to the Proposition 2.3.2 we have:

\[
\begin{align*}
\begin{cases}
  p = 4n + 1 \\
  q' = 4n + 3 \\
  f = 4n + 1
\end{cases} \quad \Rightarrow \quad \begin{cases}
  q'p = B \\
  f = A
\end{cases} \quad \Rightarrow \quad [f, q′p] = 0 \text{ or } 2, \\
\begin{cases}
  p = 4n + 3 \\
  q' = 4n + 1 \\
  f = 4n + 1
\end{cases} \quad \Rightarrow \quad \begin{cases}
  q'p = B \\
  f = A
\end{cases} \quad \Rightarrow \quad [f, q′p] = 0 \text{ or } 2, \\
\begin{cases}
  p = 4n + 1 \\
  q' = 4n + 1 \\
  f = 4n + 3
\end{cases} \quad \Rightarrow \quad \begin{cases}
  q'p = A \\
  f = B
\end{cases} \quad \Rightarrow \quad [f, q′p] = 0 \text{ or } 2, \\
\begin{cases}
  p = 4n + 3 \\
  q' = 4n + 3 \\
  f = 4n + 3
\end{cases} \quad \Rightarrow \quad \begin{cases}
  q'p = A \\
  f = B
\end{cases} \quad \Rightarrow \quad [f, q′p] = 0 \text{ or } 2.
\end{align*}
\]

Then, \( \left( \frac{f}{p} \right) = \left( \frac{f}{q'} \right) = 1 \) or \( \left( \frac{f}{p} \right) = \left( \frac{f}{q'} \right) = -1 \). But \( f q \equiv e^2 \pmod{q'} \), hence:

\[
1 = \left( \frac{f q}{q'} \right) = \left( \frac{f}{p} \right) \left( \frac{q}{q'} \right) = \left( \frac{f}{q} \right) \cdot (-1) \Rightarrow \left( \frac{f}{q} \right) = -1.
\]

Then it must be \( \left( \frac{f}{p} \right) = -1 \). We have that \( f q \equiv e^2 \pmod{p} \), hence

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

- **Case (1.B).** \( q'p > e^2 \), so \( e^2 = q′p - qf \). In this case, \( f \) will be of the form \( 4n + 1 \) when

\[
\begin{align*}
\begin{cases}
  p = 4n + 1 \\
  q' = 4n + 1
\end{cases} \quad \text{or} \quad \begin{cases}
  p = 4n + 3 \\
  q' = 4n + 3
\end{cases}
\end{align*}
\]

and of the form \( 4n + 3 \) when

\[
\begin{align*}
\begin{cases}
  p = 4n + 1 \\
  q' = 4n + 3
\end{cases} \quad \text{or} \quad \begin{cases}
  p = 4n + 3 \\
  q' = 4n + 1
\end{cases}
\end{align*}
\]

Note that \( q'p \equiv e^2 \pmod{-f} \), so \( q′p \) is a residue of \(-f\) and by the Proposition 1.2.6 \( q′p \) is a residue of all prime factors of \( f \). Hence \( [q′p, -f] = 0 \). Therefore, studying the different cases and according to the Proposition 2.3.2 we have:

\[
\begin{align*}
\begin{cases}
  p = 4n + 1 \\
  q' = 4n + 1 \\
  -f = -(4n + 1)
\end{cases} \quad \Rightarrow \quad \begin{cases}
  q'p = A \\
  -f = -A'
\end{cases} \quad \Rightarrow \quad [-f, q′p] = 0 \text{ or } 2, \\
\begin{cases}
  p = 4n + 3 \\
  q' = 4n + 3 \\
  -f = -(4n + 1)
\end{cases} \quad \Rightarrow \quad \begin{cases}
  q'p = A \\
  -f = -A'
\end{cases} \quad \Rightarrow \quad [-f, q′p] = 0 \text{ or } 2.
\end{align*}
\]
2.4. Quadratic Reciprocity Law for Odd Primes

\[ \begin{align*}
\{ p = 4n + 1 \\ q' = 4n + 3 \\ -f = -(4n + 3) \} & \implies \{ q'p = B \\ -f = -B' \} \implies [-f, q'p] = 0 \text{ or } 2, \\
\{ p = 4n + 3 \\ q' = 4n + 1 \\ -f = -(4n + 3) \} & \implies \{ q'p = B \\ -f = -B' \} \implies [-f, q'p] = 0 \text{ or } 2.
\end{align*} \]

Then \( \left( \frac{-f}{p} \right) = \left( \frac{-f}{q'} \right) = 1 \) or \( \left( \frac{-f}{p} \right) = \left( \frac{f}{q} \right) = -1 \). We know that \(-fq \equiv e^2 \pmod{q'}\), hence:

\[ 1 = \left( \frac{-f}{q'} \right) = \left( \frac{-f}{q} \right) \left( \frac{q}{q'} \right) = \left( \frac{f}{q'} \right) \cdot (-1) \implies \left( \frac{f}{q'} \right) = -1. \]

Then it must be \( \left( \frac{-f}{p} \right) = -1 \). We have that \(-fq \equiv e^2 \pmod{p}\), hence

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

**Subcase 2:** \( p \mid e \) but \( q' \nmid e \). We have \( e = pg \) and \( e^2 = (p q)^2 = q'p \pm p q h \). Hence simplifying \( p \) in the equation we obtain \( p q^2 = q'q \pm qh \), where \( g \) is an even integer and \( h \) is a positive number, smaller than \( q \) and coprime to \( p \), \( q^2 \) and \( q' \). Note that as we have defined \( e^2 \) we will take the positive sign when \( q'p < e^2 \) and the negative otherwise. Let us study these different cases separately.

- **Case (2.A).** \( q'p < e^2 \), so \( e^2 = q'p + p q h \) and \( p q^2 = q' + q h \). In this case, \( h \) will be of the form \( 4n + 1 \) when

\[ \begin{align*}
\{ p = 4n + 1 \\ q' = 4n + 3 \} \text{ or } & \{ p = 4n + 3 \\ q' = 4n + 3 \},
\end{align*} \]

and of the form \( 4n + 3 \) when

\[ \begin{align*}
\{ p = 4n + 1 \\ q' = 4n + 1 \} \text{ or } & \{ p = 4n + 3 \\ q' = 4n + 1 \}.
\end{align*} \]

Of the equation \( e^2 = q'p + p q h \) we obtain that \( q'p \equiv e^2 \pmod{h} \), i.e. \( q'p \) is a residue of \( h \) and by the Proposition 1.2.6 we know that \( q'p \) is a residue of all prime factors of \( h \). Hence \([q', h] = 0\). Studying the different cases and according to the Proposition 2.3.2 we get:

\[ \begin{align*}
\{ p = 4n + 1 \\ q' = 4n + 3 \\ h = 4n + 1 \} & \implies \{ q'p = B \\ h = A \} \implies [h, q'p] = 0 \text{ or } 2, \\
\{ p = 4n + 3 \\ q' = 4n + 3 \\ h = 4n + 1 \} & \implies \{ q'p = A \\ h = A' \} \implies [h, q'p] = 0 \text{ or } 2, \\
\{ p = 4n + 1 \\ q' = 4n + 1 \\ h = 4n + 1 \} & \implies \{ q'p = A \\ h = B \} \implies [h, q'p] = 0 \text{ or } 2, \\
\{ p = 4n + 1 \\ q' = 4n + 1 \\ h = 4n + 3 \} & \implies \{ q'p = A \\ h = B \} \implies [h, q'p] = 0 \text{ or } 2.
\end{align*} \]
Therefore, in the first and the third case, where $p > e^2$, we have:

\[
\begin{align*}
\begin{cases}
p = 4n + 3 \\
q' = 4n + 1 \\
h = 4n + 3
\end{cases}\implies \begin{cases}
q'p = B \\
h = B'
\end{cases} \implies [h, q'p] = 1.
\end{align*}
\]

Then, in the three first cases, $p$ and $q'$ are less than $q$, the "fundamental theorem" is true for them. Therefore $\left(\frac{pqh}{q'}\right) = 1$.

Multiplying the equation $pg^2 = q' + qh$ by $p$ we get $(pg)^2 = q'p + pqh$, and we can deduce $\left(\frac{pqh}{q'}\right) = 1$. Hence

\[
1 = \left(\frac{pqh}{q'}\right) = \left(\frac{pq}{q'}\right) \left(\frac{q'}{q}\right) \left(\frac{q}{h}\right) = \left(\frac{p}{q}\right) \left(\frac{q}{q'}\right) \left(\frac{q'}{h}\right) = \left(\frac{p}{q}\right) \left(\frac{q}{q'}\right) \left(\frac{q'}{h}\right) = \left(\frac{p}{q}\right).
\]

Note that, since $p$ and $q'$ are less than $q$, the "fundamental theorem" is true for them. Therefore $\left(\frac{p}{q}\right) = -1$.

Multiplying the equation $pg^2 = q' + qh$ by $q'$ we get $q'p g^2 = q'^2 + q'h g$, and we can deduce $\left(\frac{-q'qh}{p}\right) = 1$.

Therefore, in the first and the third case, where $p$ is of the form $4n + 1$, we have:

\[
1 = \left(\frac{-q'qh}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{q}{p}\right) \left(\frac{h}{p}\right) = 1 \cdot \left(\frac{q'}{p}\right) \left(\frac{q}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{h}{p}\right).
\]

In the second case, where $p$ and $q'$ are of the form $4n + 3$, we have:

\[
1 = \left(\frac{-q'qh}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{q}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right).
\]

And in the last case, where $p$ is of the form $4n + 3$ and $q'$ of the form $4n + 1$, we have:

\[
1 = \left(\frac{-q'qh}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{q}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{h}{p}\right).
\]

**Case (2.B).** $q'p > e^2$, so $e^2 = q'p - pqh$ and $pg^2 = q' - qh$. In this case, $h$ will be of the form $4n + 1$ when

\[
\begin{cases}
p = 4n + 1 \\
q' = 4n + 1
\end{cases}
\]

or

\[
\begin{cases}
p = 4n + 3 \\
q' = 4n + 1
\end{cases}
\]

and of the form $4n + 3$ when

\[
\begin{cases}
p = 4n + 1 \\
q' = 4n + 3
\end{cases}
\]

or

\[
\begin{cases}
p = 4n + 3 \\
q' = 4n + 3
\end{cases}
\]
Of the equation \( c^2 = q'p - pqh \) we obtain that \( q'p \equiv c^2 \) (mod \(-h\)), i.e. \( q'p \) is a residue of \(-h\) and by the Proposition 1.2.6 we know that \( q'p \) is a residue of all prime factors of \(-h\). Hence \([q'p, -h] = 0\). Studying the different cases and according to the Proposition 2.3.2 we get:

\[
\begin{align*}
\begin{cases}
p = 4n + 1 \\
q' = 4n + 1 \\
-h = -(4n + 1)
\end{cases}
\implies \begin{cases}
q'p = A \\
-h = -A'
\end{cases} \implies [-h, q'p] = 0 \text{ or } 2,
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
p = 4n + 3 \\
q' = 4n + 1 \\
-h = -(4n + 1)
\end{cases}
\implies \begin{cases}
q'p = B \\
-h = -A
\end{cases} \implies [-h, q'p] = 1,
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
p = 4n + 1 \\
q' = 4n + 3 \\
-h = -(4n + 3)
\end{cases}
\implies \begin{cases}
q'p = B \\
-h = -B'
\end{cases} \implies [-h, q'p] = 0 \text{ or } 2,
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
p = 4n + 3 \\
q' = 4n + 3 \\
-h = -(4n + 3)
\end{cases}
\implies \begin{cases}
q'p = A \\
-h = -B
\end{cases} \implies [-h, q'p] = 0 \text{ or } 2.
\end{align*}
\]

Then, in the first and the two last cases, \((-h/q) = (-h/p) = \pm 1\) but in the second case, \((-h/q) = (-h/p) = \pm 1\).

Multiplying the equation \( pq^2 = q' - qh \) by \( p \) we get \((pq)^2 = q'p - pqh\), and we can deduce \((-pqh/q) = 1\). Hence

\[
1 = \left(\frac{-pqh}{q}\right) = \left(\frac{p}{q}\right) \left(\frac{q}{q'}\right) \left(\frac{-h}{q'}\right) = \left(\frac{p}{q}\right) (-1) \left(\frac{-h}{q'}\right) \implies \left(\frac{-h}{q'}\right) = -\left(\frac{p}{q}\right).
\]

Since \( p \) and \( q' \) are less than \( q \), the fundamental theorem is true for them and we can use \(\frac{p}{q'} = -1 \frac{(p-1)(q'-1)}{4} \left(\frac{q'}{p}\right)\).

Multiplying the equation \( pq^2 = q' - qh \) by \( q' \) we get \(q'pq^2 = q'^2 - q'qh\), and we can deduce \((-pqh/p) = 1\).

Therefore, in the first and the third case, where \( p \) is of the form \(4n+1\), we have:

\[
1 = \left(\frac{pqh}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{q'}\right) \left(\frac{q}{p}\right) \left(\frac{-h}{p}\right) = \left(\frac{q'}{p}\right) \left(\frac{q}{p}\right) \left(\frac{-1}{p}\right) \left(\frac{p}{q'}\right) = \left(\frac{-1}{p}\right) \left(\frac{p}{q'}\right) = -1.
\]

In the fourth case, where \( p \) and \( q' \) are of the form \(4n+3\), we have:

\[
1 = \left(\frac{pqh}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{q}{p}\right) \left(\frac{-h}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q'}{p}\right) \left(\frac{q}{p}\right) \left(\frac{-1}{p}\right) \left(\frac{p}{q'}\right) = \left(\frac{-1}{p}\right) \left(\frac{p}{q'}\right) = -1.
\]
Subcase 3:

where \( p \) is of the form \( 4n + 3 \) and \( q \) of the form \( 4n + 1 \), we have:

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

**Subcase 3:** \( p \not| e \) but \( q' | e \). We have \( e = q'g \) and \( e^2 = (q'g)^2 = q'p \pm q'qh \). Hence simplifying \( q' \) in the equation we obtain \( q'g^2 = p \pm qh \), where \( g \) is an even integer and \( h \) is a positive number, less than \( q \) and coprime to \( p \), \( g^2 \) and \( q' \). Note that as we have defined \( e^2 \) we will take the positive sign when \( q'p < e^2 \) and the negative otherwise. Let us study these different cases separately.

- **Case (3.A).** \( q'p < e^2 \), so \( e^2 = q'p + q'qh \) and \( q'g^2 = p + qh \). In this case, \( h \) will be of the form \( 4n + 1 \) when

\[
\begin{align*}
\{ & p = 4n + 3 \\
& q' = 4n + 1 \}
\end{align*}
\]

and of the form \( 4n + 3 \) when

\[
\begin{align*}
\{ & p = 4n + 1 \\
& q' = 4n + 1 \}
\end{align*}
\]

Of the equation \( e^2 = q'p + q'qh \) we obtain that \( q'p \equiv e^2 \mod h \), i.e. \( q'p \) is a residue of \( h \) and by the Proposition 1.2.6 we know that \( q'p \) is a residue of all prime factors of \( h \). Hence \( \{ q'h, h \} = 0 \). Studying the different cases and according to the Proposition 2.3.2 we get:

\[
\begin{align*}
\{ & p = 4n + 3 \\
& q' = 4n + 1 \\
& h = 4n + 1 \} \implies \{ & q'p = B \\
& h = A \} \implies [h, q'p] = 0 \text{ or } 2, \\
\{ & p = 4n + 3 \\
& q' = 4n + 3 \\
& h = 4n + 1 \} \implies \{ & q'p = A \\
& h = A' \} \implies [h, q'p] = 0 \text{ or } 2, \\
\{ & p = 4n + 1 \\
& q' = 4n + 1 \\
& h = 4n + 1 \} \implies \{ & q'p = A \\
& h = B \} \implies [h, q'p] = 0 \text{ or } 2, \\
\{ & p = 4n + 1 \\
& q' = 4n + 1 \\
& h = 4n + 3 \} \implies \{ & q'p = B \\
& h = B' \} \implies [h, q'p] = 1.
\end{align*}
\]

Then, in the three first cases, \( \left( \frac{h}{p} \right) = \left( \frac{h}{q'} \right) = 1 \) or \( \left( \frac{h}{p} \right) = \left( \frac{h}{q'} \right) = -1 \), but in the last case, \( -\left( \frac{h}{p} \right) = \left( \frac{h}{q'} \right) = 1 \) or \( -\left( \frac{h}{p} \right) = \left( \frac{h}{q'} \right) = -1 \).
Multiplying the equation $q' q^2 = p + qh$ by $p$ we get $q' p q^2 = p^2 + p qh$, and we can deduce \[ \left( \frac{-p qh}{q'} \right) = 1. \] Hence
\[
1 = \left( \frac{-p qh}{q'} \right) = \left( \frac{-1}{q'} \right) \left( \frac{p}{q} \right) \left( \frac{q}{q'} \right) \left( \frac{h}{q} \right) = \left( \frac{-1}{q'} \right) \left( \frac{p}{q} \right) \left( -1 \right) \left( \frac{h}{q} \right).
\]
\[
\downarrow
\]
\[
\left( \frac{h}{q} \right) = - \left( \frac{p}{q} \right) \left( \frac{-1}{q'} \right).
\]
Since $p$ and $q'$ are less than $q$, the fundamental theorem is true for them and we can use \( \left( \frac{p}{q'} \right) = (-1)^{\frac{p-1}{2} \left( \frac{q'}{q} \right)} \) and \( \left( \frac{-1}{q'} \right) = (-1)^{\frac{q'-1}{2}}. \)

Multiplying the equation $q' q^2 = p + qh$ by $q'$ we get $(q' q)^2 = q' p + q' qh$, and we can deduce \( \left( \frac{q' q h}{p} \right) = 1. \)

Therefore, in the first and the third case, where $q'$ is of the form $4n + 1$, we have:
\[
1 = \left( \frac{q' q h}{p} \right) = \left( \frac{q'}{p} \right) \left( \frac{q}{p} \right) \left( \frac{h}{p} \right) = \left( \frac{q'}{p} \right) \left( \frac{q}{p} \right) \left( -1 \right) \left( \frac{p}{q} \right) \left( \frac{-1}{q'} \right) =
\]
\[
= (-1) \cdot (\frac{p-1}{2} \left( \frac{q'}{q} \right)) \left( \frac{q'}{p} \right)^2 \left( \frac{q}{p} \right) = (-1) \left( \frac{q}{p} \right) \Rightarrow \left( \frac{q}{p} \right) = -1.
\]

In the second case, where $p$ and $q'$ are of the form $4n + 3$, we have:
\[
1 = \left( \frac{q' q h}{p} \right) = \left( \frac{q'}{p} \right) \left( \frac{q}{p} \right) \left( \frac{h}{p} \right) = \left( \frac{q'}{p} \right) \left( \frac{q}{p} \right) \left( -1 \right) \left( \frac{p}{q} \right) \left( \frac{-1}{q'} \right) =
\]
\[
= (-1) \cdot \left( \frac{p+1}{2} \left( \frac{q'}{q} \right) \right) \left( \frac{q'}{p} \right)^2 \left( \frac{q}{p} \right) = (-1) \left( \frac{q}{p} \right) \Rightarrow \left( \frac{q}{p} \right) = -1.
\]

And in the fourth case, where $p$ is of the form $4n + 1$ and $q'$ of the form $4n + 3$, we have:
\[
1 = \left( \frac{q' q h}{p} \right) = \left( \frac{q'}{p} \right) \left( \frac{q}{p} \right) \left( \frac{h}{p} \right) = \left( \frac{q'}{p} \right) \left( \frac{q}{p} \right) \left( -1 \right) \left( \frac{p}{q} \right) \left( \frac{-1}{q'} \right) =
\]
\[
= (-1) \cdot (-1) \left( \frac{p+1}{4} \left( \frac{q'}{q} \right) \right) \left( \frac{q'}{p} \right)^2 \left( \frac{q}{p} \right) = (-1) \left( \frac{q}{p} \right) \Rightarrow \left( \frac{q}{p} \right) = -1.
\]

- **Case (3.B).** $q' p > e^2$, so $e^2 = q' p - q' qh$ and $q' q^2 = p - qh$. In this case, $h$ will be of the form $4n + 1$ when
\[
\left\{ \begin{array}{ll}
    p = 4n + 1 \\
    q' = 4n + 1
\end{array} \right. \quad \text{or} \quad \left\{ \begin{array}{ll}
    p = 4n + 1 \\
    q' = 4n + 3
\end{array} \right.,
\]
and of the form $4n + 3$ when
\[
\left\{ \begin{array}{ll}
    p = 4n + 3 \\
    q' = 4n + 1
\end{array} \right. \quad \text{or} \quad \left\{ \begin{array}{ll}
    p = 4n + 3 \\
    q' = 4n + 3
\end{array} \right..
\]

Of the equation $e^2 = q' p - q' qh$ we obtain that $q' p \equiv e^2 \pmod{-h}$, i.e. $q' p$ is a residue of $-h$ and by the Proposition 1.2.6 we know that $q' p$ is a residue
2. GAUSS’S FIRST PROOF

of all prime factors of \(-h\). Hence \([q'p, -h] = 0\). Studying the different cases and according to the Proposition 2.3.2 we get:

\[
\begin{align*}
\begin{cases}
p = 4n + 1 \\
q' = 4n + 1 \\
-h = -(4n + 1)
\end{cases} \implies \begin{cases}
q'p = A \\
-h = -A'
\end{cases} \implies [-h, q'p] = 0 \text{ or } 2,
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
p = 4n + 1 \\
q' = 4n + 1 \\
-h = -(4n + 1)
\end{cases} \implies \begin{cases}
q'p = B \\
-h = -A
\end{cases} \implies [-h, q'p] = 1,
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
p = 4n + 3 \\
q' = 4n + 1 \\
-h = -(4n + 3)
\end{cases} \implies \begin{cases}
q'p = B \\
-h = -B'
\end{cases} \implies [-h, q'p] = 0 \text{ or } 2,
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
p = 4n + 3 \\
q' = 4n + 3 \\
-h = -(4n + 3)
\end{cases} \implies \begin{cases}
q'p = A \\
-h = -B
\end{cases} \implies [-h, q'p] = 0 \text{ or } 2.
\end{align*}
\]

Then, in the first and the two last cases, \(\left(\frac{-h}{p}\right) = \left(\frac{-h}{q'}\right) = \pm 1\), but in the second case, \(-\left(\frac{-h}{p}\right) = \left(\frac{-h}{q'}\right) = \pm 1\).

Multiplying the equation \(q'g^2 = p - qh\) by \(p\) we get \(q'pg^2 = p^2 - pqh\), and we can deduce \(\left(\frac{pqh}{q'}\right) = 1\). Hence

\[
1 = \left(\frac{pqh}{q'}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q'}\right)\left(\frac{q'}{q}\right)\left(\frac{-h}{q'}\right) = \left(\frac{-1}{q'}\right)\left(\frac{p}{q'}\right)(-1)\left(\frac{-h}{q'}\right)
\]

\[
\downarrow
\]

\[
\left(\frac{-h}{q'}\right) = -\left(\frac{p}{q'}\right)\left(\frac{-1}{q'}\right).
\]

Since \(p\) and \(q'\) are smaller than \(q\), the fundamental theorem is true for them and we can use \(\left(\frac{p}{q'}\right) = (-1)^{\frac{q'-1}{4}(q'-1)}\left(\frac{q}{p}\right)\) and \(\left(\frac{-1}{q'}\right) = (-1)^{\frac{q'-1}{2}}\).

Multiplying the equation \(q'g^2 = p - qh\) by \(q'\) we get \((q'q)^2 = q'q - q'qh\), and we can deduce \(\left(\frac{-q'qh}{p}\right) = 1\).

Therefore, in the first and the third case, where \(q'\) is of the form \(4n + 1\), we have:

\[
1 = \left(\frac{-q'qh}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p}\right)\left(\frac{-h}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p}\right)\left(\frac{-1}{p}\right) = (-1) \cdot (-1)^{\frac{q'-1}{4}(q'-1)}\left(\frac{q}{p}\right)^2\left(\frac{q}{p}\right) = (-1)\left(\frac{q}{p}\right) = -1.
\]

In the second case, where \(p\) is of the form \(4n + 1\) and \(q'\) of the form \(4n + 3\), we have:

\[
1 = \left(\frac{-q'qh}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p}\right)\left(\frac{-h}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p}\right)\left(\frac{p}{q'}\right)\left(\frac{-1}{q'}\right) =
\]
Subcase 4: $p \mid e$ and $q' \mid e$. We have $e = q'p g$ and $e^2 = (q'p g)^2 = q'p \pm q'p qh$. Hence simplifying $q'p$ in the equation we obtain $q'p g^2 = 1 \pm qh$, where $g$ is an even integer and $h$ is a positive number, less than $q$ and coprime to $p$, $q'^2$ and $q'$. Note that as we have defined $e^2$ we will take the positive sign when $q'p < e^2$ and the negative otherwise. Let us study these different cases separately.

- Case (4.A). $q'p < e$, so $e^2 = q'p + q'p qh$ and $q'p g^2 = 1 + qh$. In this case, $h$ is of the form $4n + 3$. Of the equation $e^2 = q'p + q'p qh$ we obtain that $q'p = e^2 \pmod{h}$, i.e. $q'p$ is a residue of $h$ and by the Proposition 1.2.6 we know that $q'p$ is a residue of all prime factors of $h$. Hence $[q'p, h] = 0$. Studying the different cases and according to the Proposition 2.3.2 we get:

\[
\begin{align*}
\begin{cases}
p = 4n + 1 \\
q' = 4n + 1 \\
h = 4n + 3
\end{cases} \implies \begin{cases}
q'p = A \\
h = B
\end{cases} \implies [h, q'p] = 0 \text{ or } 2, \\
\begin{cases}
p = 4n + 1 \\
q' = 4n + 3 \\
h = 4n + 3
\end{cases} \implies \begin{cases}
q'p = B \\
h = B'
\end{cases} \implies [h, q'p] = 1, \\
\begin{cases}
p = 4n + 3 \\
q' = 4n + 1 \\
h = 4n + 3
\end{cases} \implies \begin{cases}
q'p = B \\
h = B
\end{cases} \implies [h, q'p] = 1, \\
\begin{cases}
p = 4n + 3 \\
q' = 4n + 3 \\
h = 4n + 3
\end{cases} \implies \begin{cases}
q'p = A \\
h = B
\end{cases} \implies [h, q'p] = 0 \text{ or } 2.
\end{align*}
\]

Then, in the first and in the last case, $\left(\frac{h}{p}\right) = \left(\frac{h}{q'}\right) = \pm 1$, but in the other cases, $\left(\frac{h}{p}\right) = \left(\frac{h}{q'}\right) = \pm 1$.

Multiplying the equation $q'p g^2 = 1 + qh$ by $p^2$ we get $q'p^3 g^2 = p^2 + p^2 qh$, and we can deduce $\left(\frac{-p^2 qh}{q'}\right) = 1$. Hence

\[
1 = \left(\frac{-p^2 qh}{q'}\right) = \left(\frac{-1}{q'}\right) \left(\frac{p^2}{q'}\right) \left(\frac{q}{q'}\right) \left(\frac{h}{q'}\right) = \left(\frac{-1}{q'}\right) \left(\frac{h}{q'}\right) = \left(\frac{-1}{q'}\right).
\]
Since $q'$ is smaller than $q$, the fundamental theorem is true for it and we can use 
\[ (-1) \frac{q' - 1}{q'} \].

Multiplying the equation $q' g^2 = p + qh$ by $q'^2$ we get $q'^3 p g^2 = q'^2 + q'^2 qh$, and we can deduce 
\[ (-q'^2 qh) p = 1. \]

Therefore, in the first and the last case, where $q' + p$ is of the form $4n + 2$, we have:

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

And in the other cases, where $q' + p$ is of the form $4n$, we have:

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

○ Case (4.b). $q'p > e$, so $e^2 = q'p - q'pqh$ and $q'p g^2 = 1 - qh$. In this case, $h$ is of the form $4n + 1$. Of the equation $e^2 = q'p - q'pqh$ we obtain that $q'p \equiv e^2 \pmod{-h}$, i.e. $q'p$ is a residue of $-h$ and by the Proposition 1.2.6 we know that $q'p$ is a residue of an odd prime factors of $-h$. Hence $[q'/p, -h] = 0$. Studying the different cases and according to the Proposition 2.3.2 we get:

\[
\begin{align*}
\{ p = 4n + 1, q' = 4n + 1, -h = -(4n + 1) \} & \implies \{ q'p = A, -h = -A' \} \implies [-h, q'p] = 0 \text{ or } 2, \\
\{ p = 4n + 1, q' = 4n + 3, -h = -(4n + 1) \} & \implies \{ q'p = B, -h = -A \} \implies [-h, q'p] = 1, \\
\{ p = 4n + 3, q' = 4n + 1, -h = -(4n + 1) \} & \implies \{ q'p = B, -h = -A \} \implies [-h, q'p] = 1, \\
\{ p = 4n + 3, q' = 4n + 3, -h = -(4n + 1) \} & \implies \{ q'p = A, -h = -A' \} \implies [-h, q'p] = 0 \text{ or } 2.
\end{align*}
\]

Then, in the first and in the last case, \[ \left( \frac{h}{p} \right) = \left( \frac{h}{q} \right) = \pm 1 \], but in the other cases, \[ -\left( \frac{h}{p} \right) = \left( \frac{h}{q} \right) = \pm 1. \]
Multiplying the equation \( q'p \ g^2 = 1 - qh \) by \( p^2 \) we get \( q'p^3 \ g^2 = p^2 - p^2 qh \), and we can deduce \( \left( \frac{p^2 qh}{q'} \right) = 1 \). Hence

\[
1 = \left( \frac{p^2 qh}{q'} \right) = \left( \frac{-1}{q'} \right) \left( \frac{p^2}{q} \right) \left( \frac{q}{q'} \right) \left( \frac{-h}{q'} \right) = \left( \frac{-1}{q'} \right) \left( -1 \right) \left( \frac{-h}{q'} \right)
\]

\[\downarrow\]

\[
\left( \frac{-h}{q'} \right) = -\left( \frac{-1}{q'} \right).
\]

Since \( q' \) is less than \( q \), the fundamental theorem is true for it and we can use \( \left( \frac{-1}{q'} \right) = (-1)^{2-1} \).

Multiplying the equation \( q' \ g^2 = p - qh \) by \( q'^2 \) we get \( q'^3 \ g^2 = q'^2 - q'^2 qh \), and we can deduce \( \left( \frac{q'^2 qh}{p} \right) = 1 \).

Therefore, in the first and the last case, where \( q' + p \) is of the form \( 4n + 2 \), we have:

\[
1 = \left( \frac{q'^2 qh}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q'^2}{p} \right) \left( \frac{q}{p} \right) \left( \frac{-h}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q}{p} \right) \left( -1 \right) \left( \frac{-1}{q'} \right) =
\]

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

And in the other cases, where \( q' + p \) is of the form \( 4n \), we have:

\[
1 = \left( \frac{q'^2 qh}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q'^2}{p} \right) \left( \frac{q}{p} \right) \left( \frac{-h}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q}{p} \right) \left( -1 \right) \left( \frac{-1}{q'} \right) =
\]

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

\[\square\]
Chapter 3
Proofs based on Gauss’s Lemma

3.1. Gauss’s Lemma

In some of his papers, Gauss stated the following a lemma, which is nowadays known as Gauss’s Lemma.

**Lemma 3.1.1 (Gauss’s Lemma)** Let $p$ be a prime number and let $M$ be an integer not divisible by $p$. Let us take the series:

1, 2, 3, ..., $\frac{1}{2}(p-1)$, \hspace{1cm} (A)

$\frac{1}{2}(p+1), \frac{1}{2}(p+3), \ldots, (p-1)$. \hspace{1cm} (B)

For all $i \in A$, let us denote $r_i$ the remainder of the division of $iM$ by $p$. Since $A \cup B = \{1, 2, 3, \ldots, p-1\}$ and $0 < r_i < p$, we note that $r_i \in A \cup B$. Let $\mu$ denote the number of remainders $r_i$ that are in $B$. If $\mu$ is even then $M$ is a residue of $p$ and if $\mu$ is odd then $M$ is a nonresidue of $p$.

This Lemma appears in the papers [Gau3] and [Gau5], both collected in Gauss’s Werke Vol.2. In fact, these papers contain the third and the fifth proofs that Gauss gave of the quadratic reciprocity law. These two proofs are based on Gauss’s Lemma and in this chapter we will present and explain them.

But first of all, let us prove the Gauss’s Lemma:

**Proof.** (Gauss’s Lemma) First of all note that $r_i \neq r_j$ for all $i \neq j$. Indeed, if $r_i = r_j$ for some $i \neq j$ then

$$iM - jM \equiv r_i - r_j \equiv 0 \pmod{p},$$

that implies $(i - j)M \equiv 0 \pmod{p}$. By hypothesis $p \nmid M$, hence it is necessary that $p \mid (i - j)$, but this is impossible because $0 < i, j < p$.

Now let us denote $a_1, a_2, a_3, \ldots, a_{\frac{1}{2}(p-1)-\mu}$ the remainders $r_i$ that are in $A$, and $b_1, b_2, b_3, \ldots, b_{\mu}$ the remainders $r_i$ that are in $B$. Note that $p-b_1, p-b_2, \ldots, p-b_\mu \in A$ and moreover $a_t \neq p - b_s$ for all $t \in \{1, 2, \ldots, \frac{1}{2}(p-1) - \mu\}$ and $s \in \{1, 2, \ldots, \mu\}$. Indeed, if $a_t = p - b_s$ for some $t, s$ then $p = a_t + b_s$. By the definition of $a_t$ and $b_s$
there exist some \( i, j \), \( i \neq j \) such that
\[
a_t = r_i \equiv i M \pmod{p} \quad \text{and} \quad b_s = r_j \equiv j M \pmod{p}.
\]
Hence \( 0 \equiv a_t + b_s \equiv i M + j M \pmod{p} \). By hypothesis \( p \nmid M \), hence it is necessary that \( p \mid (i + j) \) but this is impossible because \( 0 < i, j < \frac{1}{2}(p-1) \).

Therefore we found \( \frac{1}{2}(p-1) \) different numbers in \( A \), and the series \( A \) is made of \( \frac{1}{2}(p-1) \) numbers, hence the series \( a_1, a_2, \ldots, a_{\frac{1}{2}(p-1)-\mu}, p-b_1, p-b_2, \ldots, p-b_\mu \) is a rearrangement of the series \( A \). Then:
\[
1 \cdot 2 \cdot 3 \cdots (\frac{1}{2}(p-1)) = a_1 a_2 \cdots a_{\frac{1}{2}(p-1)-\mu} (p-b_1)(p-b_2) \cdots (p-b_\mu)
\equiv a_1 a_2 \cdots a_{\frac{1}{2}(p-1)-\mu} b_1 b_2 \cdots b_\mu (-1)^\mu
\equiv M(2M)(3M) \cdots (\frac{1}{2}(p-1)M) (-1)^{\mu}
\equiv (-1)^\mu M^{\frac{1}{2}(p-1)} \cdot 1 \cdot 2 \cdot 3 \cdots (\frac{1}{2}(p-1)) \pmod{p}.
\]

Therefore:
\[
1 \equiv (-1)^\mu M^{\frac{1}{2}(p-1)} \pmod{p}.
\]

Remember that Euler's criterion (see Proposition 1.3.3) says that \( \left( \frac{a}{p} \right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p} \), hence we can rewrite the above congruence as follows:
\[
1 \equiv (-1)^\mu \left( \frac{M}{p} \right) \pmod{p}.
\]

Therefore \( \left( \frac{M}{p} \right) = 1 \) if and only if \( \mu \) is even and \( \left( \frac{M}{p} \right) = -1 \) if and only if \( \mu \) is odd. \( \square \)

Nowadays, using the Legendre symbol notation, we can find the following modern statement of the Gauss’s Lemma.

**Lemma 3.1.2** (Gauss’s Lemma. Modern version) For any odd prime number \( p \) let \( a \) be an integer coprime to \( p \). Consider the integers
\[
a, 2a, 3a, \ldots, (\frac{p-1}{2})a,
\]
and their least positive residues modulo \( p \). These residues are all distinct, so there are \( \frac{1}{2}(p-1)a \) of them. Let \( n \) denote the number of these residues that are greater than \( \frac{p}{2} \). Then:
\[
\left( \frac{a}{p} \right) = (-1)^n.
\]

### 3.2. Gauss’s third proof

In this section we will present the Gauss’s third proof of the quadratic reciprocity law. This proof is based on Gauss’s Lemma and on some properties of \( \lfloor x \rfloor \), the largest integer not greater than \( x \). Originally, in his paper [Gau3], Gauss used the notation \( \lfloor x \rfloor \) to refer to the floor function, but in this section we will use the modern notation \( \lfloor x \rfloor \) for this concept. Because the one that Gauss used is nowadays used in any other contexts and it could lead to confusion.
Let us start stating some properties of $\lfloor x \rfloor$. Let $p$ be an odd prime number, as usual, and $k$ a positive integer coprime to $p$. Let $r_i$ be the remainder of $ik$ divided by $p$ for $i = 1, 2, \ldots, \frac{1}{2}(p - 1)$. Now let us introduce the following notation:

$$(k, p) = \# \left\{ i, \text{ such that } r_i > \frac{1}{2}(p - 1) \right\}.$$ 

Note that $(k, p)$ agrees with the $\mu$ defined in Theorem 3.1.1. Note also that $x - \lfloor x \rfloor \in [0, 1)$ and $\lfloor -x \rfloor = -\left( \lfloor x \rfloor + 1 \right)$.

Below we will enumerate some properties of $(k, p)$ and of $\lfloor x \rfloor$, which will help us to prove the two supplementary laws of the quadratic reciprocity law and will give us some tips for proving the quadratic reciprocity law itself:

I. $\lfloor x \rfloor + \lfloor -x \rfloor = -1$.

II. $\lfloor x \rfloor + h = \lfloor x + h \rfloor$, where $h$ is an integer.

III. $\lfloor x \rfloor + \lfloor h - x \rfloor = h - 1$.

IV. If $x - \lfloor x \rfloor < \frac{1}{2}$ then $2 \lfloor x \rfloor - 2 \lfloor x \rfloor = 0$, but if $x - \lfloor x \rfloor \geq \frac{1}{2}$ then $2 \lfloor x \rfloor - 2 \lfloor x \rfloor = 1$.

V. Let $h$ be an integer such that $h \equiv r \pmod{p}$ with $0 < r < p$. If $r < \frac{1}{2}p$ then $2h \left( \frac{h}{p} \right) = 0$, but if $r \geq \frac{1}{2}p$ then $2h \left( \frac{h}{p} \right) = 1$.

VI. According to V and to the definition of $(k, p)$ we can express $(k, p)$ as follows:

$$(k, p) = \left\lceil \frac{2k}{p} \right\rceil - 2 \left\lceil \frac{k}{p} \right\rceil + \left\lceil \frac{4k}{p} \right\rceil - 2 \left\lceil \frac{2k}{p} \right\rceil + \cdots + \left\lceil \frac{2(\frac{p-1}{2})k}{p} \right\rceil - 2 \left( \left\lceil \frac{k}{p} \right\rceil + \left\lceil \frac{2k}{p} \right\rceil + \cdots + \left\lceil \frac{2(\frac{p-1}{2})k}{p} \right\rceil \right).$$

VII. From I and VI we deduce:

$$(k, p) + (-k, p) = \frac{1}{2}(p - 1).$$

Notice that if $p$ is of the form $4n + 1$ then $(k, p) + (-k, p) = \frac{1}{2} \left( 4n + 1 - 1 \right) = 2n$, hence:

$$(k, p) \text{ even } \iff (k, p) \text{ even, } \quad (-k, p) \text{ odd } \iff (k, p) \text{ odd, } \quad \text{i.e. } \quad \left( \frac{-k}{p} \right) = \left( \frac{k}{p} \right).$$

But if $p$ is of the form $4n + 3$ then $(k, p) + (-k, p) = \frac{1}{2} \left( 4n + 3 - 1 \right) = 2n + 1$, hence:

$$(k, p) \text{ even } \iff (k, p) \text{ odd, } \quad (-k, p) \text{ odd } \iff (k, p) \text{ even, } \quad \text{i.e. } \quad \left( \frac{-k}{p} \right) = -\left( \frac{k}{p} \right).$$

In the particular case $k = 1$, $(1, p) = 0$ for all primes $p$, so $\left( \frac{1}{p} \right) = 1$. Then:

$$\left( \frac{-1}{p} \right) = 1 \text{ if } p = 4n + 1 \quad \text{and} \quad \left( \frac{-1}{p} \right) = -1 \text{ if } p = 4n + 3.$$
This is the first supplementary law of the quadratic reciprocity law.

VIII. In VI we saw that \((k, p) = A - B\), where:

\[
A = \left\lfloor \frac{2k}{p} \right\rfloor + \left\lfloor \frac{4k}{p} \right\rfloor + \ldots + \left\lfloor \frac{2(p-1)k}{2p} \right\rfloor,
\]

\[
B = 2 \left\lfloor \frac{k}{p} \right\rfloor + 2 \left\lfloor \frac{2k}{p} \right\rfloor + \ldots + 2 \left\lfloor \frac{(p-1)k}{2p} \right\rfloor.
\]

By III we have:

\[
\left\lfloor \frac{ik}{p} \right\rfloor + \left\lfloor \frac{k - ik}{p} \right\rfloor = k - 1 \iff \left\lfloor \frac{(p - i)k}{p} \right\rfloor = k - 1 - \left\lfloor \frac{ik}{p} \right\rfloor.
\]

Now if \(p\) is of the form \(4n + 1\), we replace the \(\frac{p-1}{4}\) last terms of \(A\) getting

\[
A = \left\lfloor \frac{2k}{p} \right\rfloor + \left\lfloor \frac{4k}{p} \right\rfloor + \ldots + \left\lfloor \frac{p-1}{4}k \right\rfloor + \left( (k-1) - \left\lfloor \frac{p-3}{2}k \right\rfloor \right) +
\]

\[
\left( (k-1) - \left\lfloor \frac{p-7}{4}k \right\rfloor \right) + \ldots + \left( (k-1) - \left\lfloor \frac{3}{2}k \right\rfloor \right) + \left( (k-1) - \left\lfloor \frac{k}{p} \right\rfloor \right).
\]

Hence:

\[
(k, p) = \left( \frac{p - 1}{4} \right) (k - 1) + \sum_{i=1}^{\frac{p-1}{4}} \left( - \left\lfloor \frac{(2i-1)k}{p} \right\rfloor + \frac{2ik}{p} \right) - 2 \sum_{j=1}^{\frac{p-1}{4}} \left\lfloor \frac{jk}{p} \right\rfloor.
\]

Similarly we can get an analogous expression for \(p\) of the form \(4n + 3\), but this time we replace the \(\frac{p+1}{4}\) last terms of \(A\) instead of the \(\frac{p-1}{4}\) ones, and we get the expression

\[
(k, p) = (k - 1) \left( \frac{p + 1}{4} \right) - 2 \left( \sum_{i=1}^{\frac{p-1}{4}} \left\lfloor \frac{(2i-1)k}{p} \right\rfloor \right) - \left( \sum_{j=1}^{\frac{p+1}{4}} \left\lfloor \frac{jk}{p} \right\rfloor \right).
\]

IX. Let us study the special case \(k = 2\). Using the formula of VIII, since in this case \(\left\lfloor \frac{2(p-1)}{p} \right\rfloor = \left\lfloor \frac{p-1}{p} \right\rfloor = 0\), we have that \((2, p) = \frac{1}{2}(p \pm 1)\); taking the positive sign if \(p\) is of the form \(4n + 3\) and the negative if \(p\) is of the form \(4n + 1\). Then \((2, p)\) is even, which is equivalent to say that \(2\) is residue of \(p\), when \(p\) is of the form \(8n \pm 1\), and \((2, p)\) is odd, which is equivalent to say that \(2\) is nonresidue of \(p\), when \(p\) is of the form \(8n \pm 3\).

To sum up we have proved that:

\[
\left( \frac{2}{p} \right) = 1 \text{ if } p = 8n \pm 1 \quad \text{and} \quad \left( \frac{2}{p} \right) = -1 \text{ if } p = 8n \pm 3.
\]

And this is the second supplementary law of the quadratic reciprocity law.
After having proved the two supplementary laws, let us state two theorems which will enable us to prove the quadratic reciprocity law.

**Theorem 3.2.1** Let \( x \) be a non-integer positive number such that \( kx \notin \mathbb{Z} \) for \( k = 1, 2, \ldots, n \), and define \( h = \lfloor nx \rfloor \). Then:

\[
\lfloor x \rfloor + \lfloor 2x \rfloor + \cdots + \lfloor nx \rfloor + \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{2}{2} \right\rfloor + \cdots + \left\lfloor \frac{h}{2} \right\rfloor = nh.
\]

**Proof.** Note that, for \( i \leq h \), the value \( \left\lfloor \frac{i}{2} \right\rfloor \) counts how many terms of the form \( kx \), for \( k = 1, 2, \ldots, n \), satisfy \( \lfloor kx \rfloor < i \). But when \( i = h + 1 \), then \( n \) denotes the number of terms of the form \( kx \) that satisfies \( \lfloor kx \rfloor < h + 1 \). Hence the number of summands equal to 0 in the sum \( \lfloor x \rfloor + \lfloor 2x \rfloor + \cdots + \lfloor nx \rfloor \) is \( \left\lfloor \frac{1}{2} \right\rfloor \), the number of summands equal to 1 in the same sum is \( \left\lfloor \frac{2}{2} \right\rfloor - \left\lfloor \frac{1}{2} \right\rfloor \), and so on. Then we can rewrite the sum \( \lfloor x \rfloor + \lfloor 2x \rfloor + \cdots + \lfloor nx \rfloor \) as follows:

\[
\lfloor x \rfloor + \lfloor 2x \rfloor + \cdots + \lfloor nx \rfloor = 0 \left\lfloor \frac{1}{2} \right\rfloor + 1 \left( \left\lfloor \frac{2}{2} \right\rfloor - \left\lfloor \frac{1}{2} \right\rfloor \right) + 2 \left( \left\lfloor \frac{3}{2} \right\rfloor - \left\lfloor \frac{2}{2} \right\rfloor \right) + \cdots + (h-1) \left( \left\lfloor \frac{h}{2} \right\rfloor - \left\lfloor \frac{h-1}{2} \right\rfloor \right) + h \left( n - \left\lfloor \frac{h}{2} \right\rfloor \right) = nh - \left\lfloor \frac{1}{2} \right\rfloor - \left\lfloor \frac{2}{2} \right\rfloor - \left\lfloor \frac{3}{2} \right\rfloor - \cdots - \left\lfloor \frac{h}{2} \right\rfloor.
\]

\[\square\]

**Theorem 3.2.2** Let \( k \) and \( p \) be coprime positive odd numbers, then:

\[
\left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{2k}{p} \right\rfloor + \cdots + \left\lfloor \frac{k(p-1)k}{p} \right\rfloor + \left\lfloor \frac{p}{k} \right\rfloor + \left\lfloor \frac{2p}{k} \right\rfloor + \cdots + \left\lfloor \frac{p(k-1)}{k} \right\rfloor = \frac{(k-1)(p-1)}{4}.
\]

**Proof.** Wlog, suppose \( k < p \). Then \( \frac{1}{2}(k-1) < \frac{1}{2}(p-1)k < \frac{1}{2}k \), that implies \( \left\lfloor \frac{1}{2}(p-1)k \right\rfloor = \frac{1}{2}(k-1) \). Taking \( x = \frac{k}{p} \), \( n = \frac{1}{2}(p-1) \) and \( h = \frac{1}{2}(k-1) \), this theorem is an immediate consequence of the previous theorem (Theorem 3.2.1). \( \square \)

After all these preliminaries we shall proceed to prove the quadratic reciprocity law itself.

Let \( p, q \) be two different odd primes. Let us define

\[
L = (q, p) + \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{3q}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2} q \right\rfloor, \\
M = (p, q) + \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \left\lfloor \frac{3p}{q} \right\rfloor + \cdots + \left\lfloor \frac{q-1}{2} p \right\rfloor.
\]

By VIII we know that \( L \) and \( M \) are always even numbers. Combining this with Theorem 3.2.2 we have

\[
\frac{L + M}{2} = (q, p) + (p, q) + \frac{1}{4}(q-1)(p-1).
\]
So if \( \frac{1}{4}(q-1)(p-1) \) is even then \((q,p)\) and \((p,q)\) need to be both even or both odd, i.e. \( \left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) \). But if \( \frac{1}{4}(q-1)(p-1) \) is odd then \((q,p)\) and \((p,q)\) need to be one even and the other odd, i.e. \( \left( \frac{q}{p} \right) = -\left( \frac{p}{q} \right) \).

Note that this last paragraph is equivalent to the formula
\[
\left( \frac{q}{p} \right) = (-1)^{\frac{1}{2}(q-1)(p-1)} \left( \frac{p}{q} \right),
\]
which is the statement of the quadratic reciprocity law. \(\square\)

### 3.3. Gauss’s fifth proof

In Gauss’s fifth proof, the other one based on Gauss’s Lemma, Gauss stated the quadratic reciprocity law as a corollary of the following theorem:

**Theorem 3.3.1.** Let \( n \) and \( m \) be two positive odd integers relatively prime. Let \( r_i \) be the remainder of the division of \( i \cdot m \) by \( n \) for all \( i \in \{1, 2, 3, \ldots, \frac{1}{2}(n-1)\} \), and let \( r'_j \) be the remainder of the division of \( j \cdot n \) by \( m \) for all \( j \in \{1, 2, 3, \ldots, \frac{1}{2}(m-1)\} \).

Let \( N \) denote the number of reminders \( r_i \) greater than \( \frac{1}{2}n \), and let \( M \) denote the number of reminders \( r'_j \) greater than \( \frac{1}{2}m \). Then, if \( \frac{1}{4}(n-1)(m-1) \) is even, \( N \) and \( M \) are simultaneously odd or even, but if \( \frac{1}{4}(n-1)(m-1) \) is odd, \( N \) and \( M \) have different parity, i.e. one is even and the other odd.

**Proof.** Let us take the sets:
\[
\{1, 2, 3, \ldots, \frac{1}{2}(n-1)\}, \quad (F)
\]
\[
\left\{ \frac{1}{2}(n+1), \frac{1}{2}(n+3), \ldots, (n-1) \right\}, \quad (F')
\]
\[
\{1, 2, 3, \ldots, \frac{1}{2}(m-1)\}, \quad (G)
\]
\[
\left\{ \frac{1}{2}(m+1), \frac{1}{2}(m+3), \ldots, (n-1) \right\}. \quad (G')
\]

Note that \( N \) denotes how many remainders obtained from the division of the numbers of the set \( mF \) by \( n \) are in \( F' \), and \( M \) denotes how many remainders obtained from the division of the numbers of the set \( nG \) by \( m \) are in \( G' \).

Now let us take the two sets:
\[
\{1, 2, 3, \ldots, \frac{1}{2}(nm-1)\}, \quad (\varphi)
\]
\[
\left\{ \frac{1}{2}(nm+1), \frac{1}{2}(nm+3), \ldots, (nm-1) \right\}. \quad (\varphi')
\]

Note that every number divisible by \( n \) has a least positive residue modulo \( n \) in \( F \) or \( F' \), and every number not divisible by \( m \) has a least positive residue modulo \( m \) in \( G \) or \( G' \). Since in the set \( \varphi \) there isn’t any number divisible simultaneously by \( n \) and by \( m \), the terms of \( \varphi \) can be separated in eight different classes:
I: Numbers in \(\phi\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F\) and their least positive residue modulo \(m\) in \(G\). Let \(\alpha\) denote how many numbers are in this class.

II: Numbers in \(\phi\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F\) and their least positive residue modulo \(m\) in \(G'\). Let \(\beta\) denote how many numbers are in this class.

III: Numbers in \(\phi\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F'\) and their least positive residue modulo \(m\) in \(G\). Let \(\gamma\) denote how many numbers are in this class.

IV: Numbers in \(\phi\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F'\) and their least positive residue modulo \(m\) in \(G'\). Let \(\delta\) denote how many numbers are in this class.

V: Numbers in \(\phi\) divisible by \(n\) but not by \(m\) such that their least positive residue modulo \(m\) is in \(G\). Let \(\zeta\) denote how many numbers are in this class.

VI: Numbers in \(\phi\) divisible by \(n\) but not by \(m\) such that their least positive residue modulo \(m\) is in \(G'\). Let \(\eta\) denote how many numbers are in this class.

VII: Numbers in \(\phi\) divisible by \(m\) but not by \(n\) such that their least positive residue modulo \(n\) is in \(F\). Let \(\theta\) denote how many numbers are in this class.

VIII: Numbers in \(\phi\) divisible by \(m\) but not by \(n\) such that their least positive residue modulo \(n\) is in \(F'\). Let \(\nu\) denote how many numbers are in this class.

Note that the classes V and VI together are the set \(nG\). Hence:

\[
\eta = M \quad \text{and} \quad \zeta = \frac{(m - 1)}{2} - M. \tag{3.3.1}
\]

In the same way, the classes VII and VIII together are the set \(mF\). Therefore:

\[
\nu = N \quad \text{and} \quad \theta = \frac{(n - 1)}{2} - N. \tag{3.3.2}
\]

By an analogous argument we can also separate \(\phi'\) in eight different classes:

I': Numbers in \(\phi'\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F\) and their least positive residue modulo \(m\) in \(G\). Let \(\alpha'\) denote how many numbers are in this class.

II': Numbers in \(\phi'\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F\) and their least positive residue modulo \(m\) in \(G'\). Let \(\beta'\) denote how many numbers are in this class.

III': Numbers in \(\phi'\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F'\) and their least positive residue modulo \(m\) in \(G\). Let \(\gamma'\) denote how many numbers are in this class.

IV': Numbers in \(\phi'\) not divisible by \(n\) nor by \(m\) such that their least positive residue modulo \(n\) is in \(F'\) and their least positive residue modulo \(m\) in \(G'\). Let \(\delta'\) denote how many numbers are in this class.

V': Numbers in \(\phi'\) divisible by \(n\) but not by \(m\) such that their least positive residue modulo \(m\) is in \(G\). Let \(\zeta'\) denote how many numbers are in this class.
VIII: Numbers in \( \varphi' \) divisible by \( n \) but not by \( m \) such that their least positive residue modulo \( m \) is \( G' \). Let \( \eta' \) denote how many numbers are in this class.

VII': Numbers in \( \varphi' \) divisible by \( m \) but not by \( n \) such that their least positive residue modulo \( n \) is in \( F \). Let \( \theta' \) denote how many numbers are in this class.

VIII': Numbers in \( \varphi' \) divisible by \( m \) but not by \( n \) such that their least positive residue modulo \( n \) is in \( F' \). Let \( \nu' \) denote how many numbers are in this class.

Since \( nm - r \equiv -r \equiv n - r \pmod{n} \) and \( nm - r \equiv -r \equiv m - r \pmod{m} \), if \( r \) is in \( F \) then \( n - r \) is in \( F' \) and vice versa, and if \( r \) is in \( G \) then \( m - r \) is in \( G' \) and vice versa. Hence we can find a relation between the cardinals of the eight classes of \( \varphi \) and \( \varphi' \):

\[
\begin{align*}
\alpha &= \delta', \quad \delta = \alpha', \quad \beta = \gamma', \quad \gamma = \beta', \\
\zeta &= \eta', \quad \eta = \zeta', \quad \theta = \nu', \quad \nu = \theta'.
\end{align*}
\] (3.3.3)

Since \( F \) has \( \frac{n-1}{2} \) elements and \( G \) has \( \frac{m-1}{2} \) elements, by the Chinese Remainder Theorem we see that \( I \cup I' \) has \( \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right) \) elements, i.e.

\[
\alpha + \alpha' = \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right).
\]

In the same way we can see \( \beta + \beta' = \gamma + \gamma' = \delta + \delta' = \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right) \). Hence from these equalities and from (3.3.3) we have:

\[
\begin{align*}
\alpha + \delta &= \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right), \\
\gamma + \beta &= \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right).
\end{align*}
\] (3.3.4)

Note that \( II \cup IV \cup VI \) is the set of numbers smaller than \( \frac{nm}{2} \) such that their least residue modulo \( m \) is in \( G' \). I.e. \( II \cup IV \cup VI \) is composed of the numbers of the form:

\[ G', m + G', 2m + G', \ldots, \frac{m-3}{2} + G'. \]

Then the cardinal of the set \( II \cup IV \cup VI \) is \( \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right) \), i.e.

\[
\beta + \delta + M = \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right).
\] (3.3.5)

And in a similar way we can see that the cardinal of the set \( III \cup IV \cup VIII \) is also \( \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right) \), then:

\[
\gamma + \delta + N = \left( \frac{n-1}{2} \right) \left( \frac{m-1}{2} \right).
\] (3.3.6)

Hence from (3.3.4), (3.3.5) and (3.3.6), and letting \( R \) denote \( \frac{(n-1)(m-1)}{4} \), we deduce:

\[
\begin{align*}
2\alpha &= 2R - 2\delta = (\beta + M) + (\gamma + N) = R + N + M, \\
2\beta &= (R - \gamma) + (R - M - \delta) = R + N - M, \\
2\gamma &= (R - \beta) + (R - N - \delta) = R - N + M, \\
2\delta &= (R - M - \beta) + (R - N - \gamma) = R - N - M.
\end{align*}
\] (3.3.7)
Hence
\[
2\alpha = \frac{(n-1)(m-1)}{4} + N + M,
\]
\[
2\beta = \frac{(n-1)(m-1)}{4} + N - M,
\]
\[
2\gamma = \frac{(n-1)(m-1)}{4} - N + M,
\]
\[
2\delta = \frac{(n-1)(m-1)}{4} - N - M.
\]

Each of these equalities implies that if \( \frac{(n-1)(m-1)}{4} \) is even then \( M \) and \( N \) need to have the same parity but if \( \frac{(n-1)(m-1)}{4} \) is odd, then the parity of \( M \) and \( N \) needs to be different.

\[\square\]

The theorem stated above, Theorem 3.3.1, is true for any pair of coprime positive odd integers. But this theorem in the particular case of two different odd primes is, in fact, the quadratic reciprocity law.

**Corollary 3.3.2 (Quadratic Reciprocity Law)** Let \( p \) and \( q \) be two different odd prime numbers. Then
\[
\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).
\]

**Proof.** By Theorem 3.3.1 and by Gauss’s Lemma (Lemma 3.1.1) we know that if \( \frac{(p-1)(q-1)}{4} \) is even, then
\[
\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1 \text{ or } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1,
\]
but if \( \frac{(p-1)(q-1)}{4} \) is odd, then
\[
\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = 1 \text{ or } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -1.
\]
And the corollary immediately follows. \(\square\)
Chapter 4
Proofs based on trigonometric sums

In this chapter we are going to show the two proofs that Gauss found based on trigonometric sums, and more concretely, in some special type of trigonometric sums nowadays known as Gauss sums.

4.1. Gauss’s fourth proof

In his article *Summatio quarumdam serierum singularium* [Gau4], Gauss studied the sums

\[ G(k, p) = \sum_a \left( \cos(ak\omega) + i\sin(ak\omega) \right) - \sum_b \left( \cos(bk\omega) + i\sin(bk\omega) \right), \]  

(4.1.1)

where \( p \) is an odd prime number, \( k \) is an integer coprime to \( p \), \( a \) and \( b \) denote the quadratic residues and nonresidues modulo \( p \) in the set \( \{1, 2, \ldots, p-1\} \), respectively, and \( \omega = \frac{2\pi}{p} \). In that article, his aim was not to prove the quadratic reciprocity law, but the computation of the sum itself and, especially, of the sign of the sum (see article 356 of [Gau1]). After the study of these sums he noticed that a new proof of the quadratic reciprocity law could follow from them. This proof is the one that we will show in this section.

Nowadays these sums are known as Gauss sums, and we can express them in a more modern way:

\[ G(k, p) = \sum_{\lambda=1}^{p-1} \left( \lambda \middle| p \right) \zeta^{\lambda k}, \]

(4.1.2)

where \( \zeta = e^{\frac{2\pi i}{p}} \) is a primitive \( p \)-th root of unity and \( \left( \lambda \middle| p \right) \) denotes the Legendre symbol.

Let us begin by showing some other expressions of these sums.
Since $\zeta^{\lambda k} = \cos(\lambda k \omega) + i \sin(\lambda k \omega)$ we know that:

$$\sum_{a} \left( \cos(ak \omega) + i \sin(ak \omega) \right) + \sum_{b} \left( \cos(bk \omega) + i \sin(bk \omega) \right) = \sum_{\lambda=1}^{p-1} \left( \cos(\lambda k \omega) + i \sin(\lambda k \omega) \right) = \sum_{\lambda=1}^{p-1} \zeta^{\lambda k} = -1.$$ 

Hence:

$$\sum_{b} \left( \cos(bk \omega) + i \sin(bk \omega) \right) = -1 - \sum_{a} \left( \cos(ak \omega) + i \sin(ak \omega) \right) \quad (4.1.3)$$

Applying (4.1.3) to (4.1.1) we get an expression of $G(k,p)$ depending only on the residues of $p$:

$$G(k,p) = 1 + 2 \sum_{a} \left( \cos(ak \omega) + i \sin(ak \omega) \right) = 1 + 2 \sum_{a} \zeta^{ak}. \quad (4.1.4)$$

By Corollary 1.2.4 we know that in the set $\{1, 2, 3, \ldots, p-1\}$ there are exactly $\frac{p-1}{2}$ residues of $p$. These $\frac{p-1}{2}$ residues are congruent to $1, 2^2, 3^2, \ldots, (\frac{p-1}{2})^2$ modulo $p$, but they are also congruent to $(\frac{p-1}{2} + 1)^2, (\frac{p-1}{2} + 2)^2, \ldots, (p-1)^2$. Hence:

$$\sum_{a} \zeta^{ak} = \zeta^k + \zeta^{2^2k} + \cdots + \zeta^{(\frac{p-1}{2})^2k}, \quad (4.1.5)$$

$$\sum_{a} \zeta^{ak} = \zeta^{(\frac{p-1}{2} + 1)^2k} + \zeta^{(\frac{p-1}{2} + 2)^2k} + \cdots + \zeta^{(p-1)^2k}. \quad (4.1.6)$$

And from the equations (4.1.4), (4.1.5) and (4.1.6) we get:

$$G(k,p) = 1 + \sum_{\lambda=1}^{p-1} \zeta^{\lambda^2k}.$$

Now note that, since $p$ and $k$ are coprime, from the equation (4.1.2) we have:

$$G(k,p) = \sum_{\lambda=1}^{p-1} \left( \frac{\lambda}{p} \right) \zeta^{\lambda k} = \left( \frac{k}{p} \right) \sum_{\lambda=1}^{p-1} \left( \frac{\lambda k}{p} \right) \zeta^{\lambda k} = \left( \frac{k}{p} \right) \sum_{\lambda=1}^{p-1} \left( \frac{\lambda}{p} \right) \zeta^{\lambda} = \left( \frac{k}{p} \right) G(1,p).$$

Then it is enough to study the Gauss sum

$$G(1,p) = 1 + \zeta + \zeta^4 + \zeta^9 + \cdots + \zeta^{(p-1)^2}.$$

### 4.1.1. Some polynomial identities

In this part of the section we will spend some time in showing some results that will help us to proceed with the proof itself.

Let us begin introducing the following notation:

$$\frac{(m, \mu) = \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})}{(1-x)(1-x^2)(1-x^3)\ldots(1-x^\mu)}, \quad (4.1.7)}{(m, \mu) = \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})}{(1-x)(1-x^2)(1-x^3)\ldots(1-x^\mu)},$$
where \(m\) and \(\mu\) are two positive integers, \(0 < \mu \leq m\). Note that when \(m = \mu\), the factors of the numerator and on the denominator are the same but in the inverse order, hence \((\mu,\mu) = 1\). For \(\mu = 0\), we define \((m, 0) = 1\).

We have the following results:

**Proposition 4.1.1** Let \(m\) and \(\mu\) be two different positive odd integers, and let us define \((m, \mu)\) as in (4.1.7). Then

\[
(m, \mu + 1) = (m - 1, \mu + 1) + x^{m-\mu-1}(m - 1, \mu). \tag{4.1.8}
\]

**Proof.** Indeed

\[
(m - 1, \mu + 1) + x^{m-\mu-1}(m - 1, \mu) = \\
= \frac{(1 - x^{m-1}) \cdots (1 - x^{m-\mu-1})}{(1 - x) \cdots (1 - x^{\mu+1})} + \frac{x^{m-\mu-1}(1 - x^{m-1}) \cdots (1 - x^{m-\mu})}{(1 - x) \cdots (1 - x^{\mu})} \\
= \frac{(1 - x^{m-1}) \cdots (1 - x^{m-\mu})}{(1 - x) \cdots (1 - x^{\mu})} \left(1 - x^{m-\mu-1}\right) + x^{m-\mu-1}\left(1 + x^{\mu+1}\right) \\
= \frac{(1 - x^m)(1 - x^{m-1}) \cdots (1 - x^{m-\mu})}{(1 - x) \cdots (1 - x^{\mu})} = (m, \mu + 1). \\
\]

\(\Box\)

And applying recursively the proposition above we get:

**Corollary 4.1.2** Let \(m\) and \(\mu\) be two positive odd integers such that \(m > \mu\) and let us define \((m, \mu)\) as in (4.1.7). Then \((m, \mu + 1)\) can be alternatively expressed as follows:

\[
(m, \mu + 1) = (\mu, \mu) + x(\mu + 1, \mu) + x^2(\mu + 2, \mu) + \cdots + x^{m-\mu-1}(m - 1, \mu). 
\]

**Proof.** By Proposition 4.1.1 we have:

\[
(m - 1, \mu + 1) = (m - 2, \mu + 1) + x^{m-\mu-2}(m - 2, \mu), \\
(m - 2, \mu + 1) = (m - 3, \mu + 1) + x^{m-\mu-3}(m - 3, \mu), \\
(m - 3, \mu + 1) = (m - 4, \mu + 1) + x^{m-\mu-4}(m - 4, \mu), \\
\vdots \\
(\mu + 2, \mu + 1) = (\mu + 1, \mu + 1) + x(\mu + 1, \mu) = (\mu, \mu) + x(\mu + 1, \mu). \\
\]

And applying these equations we get:

\[
(m, \mu + 1) = (\mu, \mu) + x(\mu + 1, \mu) + x^2(\mu + 2, \mu) + \cdots + x^{m-\mu-1}(m - 1, \mu). \\
\]

\(\Box\)

Let us define \(f(x, m)\) as a function which depends on \((m, i), i = 1, 2, \ldots, m\), as follows:
\textbf{Definition 4.1.3.} Let \( m \) be a positive integer. Let us define the following function in \( x \):

\[ f(x, m) = 1 - (m, 1) + (m, 2) - (m, 3) + \cdots + (-1)^m(m, m). \quad (4.1.9) \]

The function \( f(x, m) \) defined above can be also expressed in a recursive way:

\textbf{Proposition 4.1.4} The function \( f(x, m) \) satisfies the recursive expression

\[ f(x, m) = (1 - x^{m-1}) f(x, m - 2). \]

\textbf{Proof.} By the equation (4.1.8) we have:

\begin{align*}
1 &= 1, \\
-(m, 1) &= -((m - 1), 1) - x^{m-1}(m - 1, 0), \\
+(m, 2) &= +((m - 1), 2) + x^{m-2}(m - 1, 1), \\
-(m, 3) &= -((m - 1), 3) - x^{m-3}(m - 1, 2), \\
\vdots
\end{align*}

Thus, \((-1)^m(m, m) = (-1)^m(m - 1, m) + (-1)^m(m - 1, m - 1).

Hence, applying these equations to (4.1.9), we get:

\[ f(x, m) = 1 - x^{m-1} - (1 - x^{m-2})(m - 1, 1) + (1 - x^{m-3})(m - 1, 2) - (1 - x^{m-4})(m - 1, 3) + (1 - x^{m-5})(m - 1, 4) - \cdots \]

(4.1.10)

Note that the identity

\[ \left(1 - x^{m-(n+1)}\right)(m - 1, n) = (1 - x^{m-1})(m - 2, n), \quad \forall n < m. \]

holds for all \( n \) smaller than \( m \). Indeed:

\begin{align*}
\left(1 - x^{m-(n+1)}\right)(m - 1, n) &= \left(1 - x^{m-(n+1)}\right) \frac{(1 - x^{m-1})\cdots(1 - x^{m-n})}{(1 - x)\cdots(1 - x^n)} \\
&= \frac{(1 - x^{m-1})(1 - x^{m-2})\cdots(1 - x^{m-n})(1 - x^{m-(n+1)})}{(1 - x)\cdots(1 - x^n)} \\
&= (1 - x^{m-1})\frac{(1 - x^{m-2})\cdots(1 - x^{m-(n+1)})}{(1 - x)\cdots(1 - x^n)} \\
&= (1 - x^{m-1})(m - 2, n).
\end{align*}

Therefore

\begin{align*}
(1 - x^{m-2})(m - 1, 1) &= (1 - x^{m-1})(m - 2, 1), \\
(1 - x^{m-3})(m - 2, 1) &= (1 - x^{m-1})(m - 2, 2), \\
(1 - x^{m-4})(m - 3, 1) &= (1 - x^{m-1})(m - 2, 3), \\
\vdots
\end{align*}
And applying these formulae to the equation (4.1.10), we get the recursive expression
\[
f(x, m) = (1 - x^{m-1})f(x, m - 2).
\]
\[\blacksquare\]

**Corollary 4.1.5** By Proposition 4.1.4 we get that if \(m\) is even, since \(f(x, 0) = 1\), then:
\[
f(x, m) = (1 - x^{m-1}) f(x, m - 2)
= (1 - x^{m-1}) (1 - x^{m-3}) f(x, m - 4) = \ldots \tag{4.1.11}
= (1 - x^{m-1})(1 - x^{m-3}) \ldots (1 - x)f(x, 0)
= (1 - x)(1 - x^3) \ldots (1 - x^{m-3})(1 - x^{m-1}).
\]
But if \(m\) is odd, since \(f(x, 1) = 1 - (1, 1) = 0\), then:
\[
f(x, m) = (1 - x^{m-1}) f(x, m - 2)
= (1 - x^{m-1}) (1 - x^{m-3}) f(x, m - 4) = \ldots
= (1 - x^{m-1})(1 - x^{m-3}) \ldots (1 - x^2)f(x, 1)
= 0.
\]

### 4.1.2. Proof itself

Now we return to the study of the Gauss sums \(G(1, n)\) that we introduced at the beginning of this section, but this time \(n\) is more generally any odd integer, not necessarily prime. I.e., we want to compute the sum:
\[
G(1, n) = \sum_{\lambda=0}^{n-1} \zeta^{\lambda^2},
\]
where \(\zeta = e^{2\pi i/n}\) is a primitive \(n\)-th root of unity.

Now, for any odd integer \(n > 0\), let us replace \(m\) with \(n - 1\) and \(x\) with \(\zeta\), in the equation (4.1.7) getting:
\[
(n - 1, \mu) = \left(\frac{1 - \zeta^{n-1}}{1 - \zeta}\right) \left(\frac{1 - \zeta^{n-2}}{1 - \zeta^2}\right) \ldots \left(\frac{1 - \zeta^{n-\mu}}{1 - \zeta^\mu}\right).
\]
Note that, since \(\zeta^n = 1\), for all positive integer \(t\) such that \(\gcd(t, n) = 1\), we have:
\[
\frac{1 - \zeta^{n-t}}{1 - \zeta^t} = \frac{1 - \zeta^n \zeta^{-t}}{1 - \zeta^t} = \frac{\zeta^{-t}}{1 - \zeta^t} = -\zeta^{-t},
\]
therefore
\[
(n - 1, \mu) = \left(\frac{1 - \zeta^{n-1}}{1 - \zeta}\right) \left(\frac{1 - \zeta^{n-2}}{1 - \zeta^2}\right) \ldots \left(\frac{1 - \zeta^{n-\mu}}{1 - \zeta^\mu}\right)
= (-\zeta^{-1})(-\zeta^{-2}) \ldots (-\zeta^{-\mu}) = (-1)^\mu \zeta^{-\frac{(n+1)\mu}{2}}.
\]
Hence
\[ f(\zeta, n - 1) = 1 - (n - 1, 1) + (n - 1, 2) - (n - 1, 3) + \cdots + (n - 1, n - 1) \]
\[ = 1 - (-1)^{\frac{n-1}{2}} + (-1)^2\zeta^{-\frac{3}{2}} - (-1)^3\zeta^{-\frac{5}{2}} + \cdots + (-1)^{n-1}\zeta^{-\frac{n(n-1)}{2}} \]
\[ = 1 + \zeta^{-1} + \zeta^{-3} + \zeta^{-6} + \zeta^{-10} + \cdots + \zeta^{-\frac{n(n-1)}{2}}. \] (4.1.12)

But, since \( n - 1 \) is even, from the equation (4.1.11), we also have:
\[ f(\zeta, n - 1) = (1 - \zeta)(1 - \zeta^3)(1 - \zeta^5) \cdots (1 - \zeta^{n-2}). \] (4.1.13)

Consequently, by equations (4.1.12) and (4.1.13) we get the identity:
\[ (1-\zeta)(1 - \zeta^3)(1 - \zeta^5) \cdots (1 - \zeta^{n-2}) = 1+\zeta^{-1}+\zeta^{-3}+\zeta^{-6}+\cdots+\zeta^{-\frac{n(n-1)}{2}} \] (4.1.14)

Note that, since \(-2\) and \( n \) are coprime, the identity above still holds putting \( \zeta^{-2} \) instead of \( \zeta \). Hence we get:
\[ (1 - \zeta^{-2})(1 - \zeta^{-6})(1 - \zeta^{-10}) \cdots (1 - \zeta^{-2(n-2)}) = 1 + \zeta^2 + \zeta^6 + \zeta^{12} + \cdots + \zeta^{n(n-1)} \] (4.1.15)

Now note that
\[ 1 + 3 + 5 + \cdots + (n - 2) = \left( \sum_{i=1}^{n-1} \frac{i - n - 1}{2} \right) = \frac{n(n - 1)}{4} - \frac{n - 1}{4} = \frac{n^2 - n - n + 1}{4} = \left( \frac{n - 1}{2} \right)^2 \]
\[ \text{Hence} \]
\[ \zeta^{\left( \frac{n-1}{2} \right)^2} = \zeta^1 \zeta^3 \zeta^5 \cdots \zeta^{n-2}. \]

Therefore multiplying the right side of the equation (4.1.15) by \( \zeta^{\left( \frac{n-1}{2} \right)^2} \) and the left side by \( \zeta^1 \zeta^3 \zeta^5 \cdots \zeta^{n-2} \), we have:
\[ \zeta^1 \zeta^3 \cdots \zeta^{n-2} (1 - \zeta^{-2}) (1 - \zeta^{-6}) \cdots (1 - \zeta^{-2(n-2)}) = \zeta^{\left( \frac{n-1}{2} \right)^2} \left( 1 + \zeta^2 + \zeta^6 + \cdots + \zeta^{n(n-1)} \right). \]

Which is equivalent to
\[ (\zeta - \zeta^{-1}) (\zeta^3 - \zeta^{-3}) (\zeta^5 - \zeta^{-5}) \cdots (\zeta^{n-2} - \zeta^{-(n-2)}) = \zeta^{\left( \frac{n-1}{2} \right)^2} + \zeta^{2+\left( \frac{n-1}{2} \right)^2} + \zeta^{6+\left( \frac{n-1}{2} \right)^2} + \cdots + \zeta^{n(n-1)+\left( \frac{n-1}{2} \right)^2}. \] (4.1.16)

Note that, since \( \zeta^n = 1 \),
\[ \zeta^{\left( t(t+1)+\frac{n-1}{2} \right)^2} = \zeta^{\left( \frac{n-(2t+1)}{2} \right)^2}, \quad \forall t \in \mathbb{Z}. \] (4.1.17)

Indeed,
\[ \zeta^{t(t+1)+\frac{n-1}{2}} = \zeta^{\frac{4t(t+1)+n^2-2n+1}{4}} = \zeta^{\frac{4t^2+4t+1+n^2-2n}{4}} = \zeta^{\frac{(2t+1)^2+n^2-2n}{4}} = \zeta^{(\frac{n-(2t+1)}{2})^2}. \]
Applying the equation (4.1.17) to (4.1.16) we get:

\[
(\zeta - \zeta^{-1}) (\zeta^3 - \zeta^{-3}) (\zeta^5 - \zeta^{-5}) \ldots (\zeta^{n-2} - \zeta^{-(n-2)}) = \\
= \zeta\left(\frac{n+1}{2}\right)^2 + \zeta\left(\frac{n+3}{2}\right)^2 + \zeta\left(\frac{n+5}{2}\right)^2 + \ldots + \zeta \left(\frac{n-3}{2}\right)^2 + \zeta \left(\frac{n-1}{2}\right)^2.
\]

Then, rearranging the terms of the equation (4.1.18), we get the following equation:

\[
(\zeta - \zeta^{-1}) (\zeta^3 - \zeta^{-3}) \ldots (\zeta^{n-2} - \zeta^{-(n-2)}) = 1 + \zeta + \zeta^4 + \ldots + \zeta^{(n-1)^2}.
\]

Now notice that the right side of the last equation is the Gauss sum \( G(1, n) \), hence the discussion above leads to the following theorem, that will be the key for the computation of \( G(1, n) \).

**Theorem 4.1.6** Let \( n \) be a positive odd integer and let \( \zeta \) be a primitive \( n \)-th root of unity. Hence the Gauss sum \( G(1, n) \) can be expressed as follows:

\[
G(1, n) = (\zeta - \zeta^{-1}) (\zeta^3 - \zeta^{-3}) \ldots (\zeta^{n-2} - \zeta^{-(n-2)}).
\]

Note that, since \( \zeta^n = 1 \), it is true:

\[
\zeta - \zeta^{-1} = - (\zeta^{n-1} - \zeta^{-n+1}), \\
\zeta^3 - \zeta^{-3} = - (\zeta^{n-3} - \zeta^{-n+3}), \\
\zeta^5 - \zeta^{-5} = - (\zeta^{n-5} - \zeta^{-n+5}), \\
\vdots
\]

\[
\zeta^{n-2} - \zeta^{-(n-2)} = - (\zeta^2 - \zeta^{-2}).
\]

Therefore \( G(1, n) \) can be rewritten in the following way:

\[
G(1, n) = (-1)^{n-1} (\zeta^2 - \zeta^{-2}) (\zeta^4 - \zeta^{-4}) (\zeta^6 - \zeta^{-6}) \ldots (\zeta^{n-1} - \zeta^{-(n-1)}).
\]

Multiplying the equation (4.1.19) by the equation (4.1.20) we get:

\[
G(1, n)^2 = (-1)^{\frac{n(n+1)}{2}} (\zeta^1 - \zeta^{-1}) (\zeta^2 - \zeta^{-2}) (\zeta^3 - \zeta^{-3}) \ldots (\zeta^{n-1} - \zeta^{-(n-1)})
\]

\[
= (-1)^{\frac{n(n+1)}{2}} \frac{n(n-1)}{2} (1 - \zeta^{-2}) (1 - \zeta^{-4}) (1 - \zeta^{-6}) \ldots (1 - \zeta^{-2(n-1)}).
\]

Since \( \gcd(-2, n) = 1 \), \( \zeta^{-2} \) generates the group of \( n \)-th roots of unity. Hence

\[
1, \zeta^{-2}, \zeta^{-4}, \ldots, \zeta^{-2(n-1)}
\]

are all roots of the equation \( x^n - 1 = 0 \). I.e.

\[
x^n - 1 = (x - 1) (x - \zeta^{-2}) (x - \zeta^{-4}) \ldots (x - \zeta^{-2(n-1)}),
\]
that implies:

\[ x^{n-1} + x^{n-2} + \cdots + x + 1 = (x - \zeta^{-2})(x - \zeta^{-4}) \cdots (x - \zeta^{-2(n-1)}) \].

Evaluating the above equation in \( x = 1 \) we have:

\[ n = (1 - \zeta^{-2})(1 - \zeta^{-4}) \cdots (1 - \zeta^{-2(n-1)}) \]. \hspace{1cm} (4.1.22)

Therefore, mixing the equations (4.1.21) and (4.1.22) we get the following identity:

\[ G(1, n)^2 = (-1)^{\frac{n-1}{2}} n. \]

This implies

\[ G(1, n) = \begin{cases} \pm \sqrt{n} & \text{if } n \equiv 1 \pmod{4}, \\ \pm i \sqrt{n} & \text{if } n \equiv 3 \pmod{4}. \end{cases} \]

Now we return to the equation (4.1.19) in order to find the sign of \( G(1, n) \). Notice that

\[ \zeta^t - \zeta^{-t} = 2 i \sin(t \omega), \quad \forall t \in \mathbb{Z} \]

Indeed,

\[ \zeta^t - \zeta^{-t} = (\cos(t \omega) + i \sin(t \omega)) - (\cos(-t \omega) + i \sin(-t \omega)) = (\cos(t \omega) + i \sin(t \omega)) - (\cos(t \omega) - i \sin(t \omega)) = 2 i \sin(t \omega). \]

Applying these equations to (4.1.19) we find:

\[ G(1, n) = (2i)^{\frac{n-1}{2}} \sin(\omega) \sin(3\omega) \sin(5\omega) \cdots \sin((n-2)\omega). \]

Let us count how many sines in this product are negative. First of all note that, since \( \omega = \frac{2\pi}{n} \) and \( q \) is odd, the values \( \omega, 3\omega, \ldots, (n-2)\omega \) are all less than \( 2\pi \). Hence:

\[ \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid \sin t \omega < 0 \right\} = \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid \pi < t \omega < 2\pi \right\} = \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid \frac{n}{2} < t < n \right\} = \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid \frac{n-1}{2} \leq t \leq n-2 \right\}, \]

and

\[ \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid \sin t \omega > 0 \right\} = \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid 0 < t \omega < \pi \right\} = \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid 0 < t < \frac{n}{2} \right\} = \# \left\{ t \in \{1, 3, \ldots, n-2\} \mid 1 \leq t \leq \frac{n-1}{2} \right\}. \]

Now let us distinguish the following two cases:

Case 1: \( n \) is of the form \( 4\mu + 1 \). \( \frac{n-1}{2} \) is even, then there are \( \frac{n-1}{4} \) positive sines and \( \frac{n-1}{4} \) negative sines. Hence

\[ G(1, n) = i^{\frac{n-1}{2}} (-1)^{\frac{n-1}{2}} 2^{\frac{n-1}{2}} \left\{ \sin(\omega) \cdots \sin(\frac{n-3}{2}\omega) \sin(-\frac{n-1}{2}\omega) \cdots \sin(-(n-2)\omega) \right\}, \]
where $K$ denotes a positive constant. Therefore the sign of $G(1, n)$ is determined by the sign of $i^{\frac{n-1}{2}}(-1)^{\frac{n-3}{4}}$, but
\[ i^{\frac{n-1}{2}}(-1)^{\frac{n-3}{4}} = i^{\frac{(4n+1)-1}{2}}(-1)^{\frac{(4n+3)-1}{4}} = i^{2\mu}(-1)^{\mu} = (-1)^{\mu} = (-1)^{2\mu} = 1. \]
Hence, in the case $n = 4\mu + 1$,
\[ G(1, n) = i^{\frac{n-1}{2}}(-1)^{\frac{n-3}{4}} K = K. \]

Case 2: $n$ is of the form $4\mu + 3$. $\frac{n-1}{2}$ is odd, then there are $\frac{n+1}{4}$ positive sines and $\frac{n-3}{4}$ negative sines. Hence
\[ G(1, n) = i^{\frac{n-1}{2}}(-1)^{\frac{n-3}{4}} \frac{2^{\frac{n-1}{2}}}{\sqrt{n}} \sin(\omega) \ldots \sin(-\frac{n-1}{2}\omega) \ldots \sin(-(n-2)\omega), \]
where $K$ denotes a positive constant. Therefore the sign of $G(1, n)$ is determined by the sign of $i^{\frac{n-1}{2}}(-1)^{\frac{n-3}{4}}$, but
\[ i^{\frac{n-1}{2}}(-1)^{\frac{n-3}{4}} = i^{\frac{(4n+3)-1}{2}}(-1)^{\frac{(4n+1)-3}{4}} = i^{2\mu+1}(-1)^{\mu} = i(-1)^{\mu} = i(-1)^{2\mu} = i. \]
Hence, in the case $n = 4\mu + 3$,
\[ G(1, n) = i^{\frac{n-1}{2}}(-1)^{\frac{n-3}{4}} K = iK. \]

Combining these two cases we finally get
\[ G(1, n) = \begin{cases} \sqrt{n} & \text{if } n \equiv 1 \pmod{4}, \\ i\sqrt{n} & \text{if } n \equiv 3 \pmod{4}. \end{cases} \] (4.1.23)

Now let us show the multiplicity of these sums given by $G(b, a)G(a, b) = G(1, ab)$.

**Theorem 4.1.7** Let $n = ab$ be the product of two positive relatively prime integers. Let $\zeta$ be an $n$-th root of unity and
\[ G(1, n) = 1 + \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{(n-1)^2}. \]
Then we can express
\[ G(a, b) = 1 + \zeta^{a^2} + \zeta^{4a^2} + \zeta^{9a^2} + \cdots + \zeta^{(b-1)^2a^2}, \]
\[ G(b, a) = 1 + \zeta^{b^2} + \zeta^{4b^2} + \zeta^{9b^2} + \cdots + \zeta^{(a-1)^2b^2}, \]
and they satisfy $G(1, n) = G(a, b)G(b, a)$.

**Proof.** First of all let us show that the sum $1 + \zeta^{a^2} + \zeta^{4a^2} + \zeta^{9a^2} + \cdots + \zeta^{(b-1)^2a^2}$ agrees with $G(a, b)$. We know that
\[ G(a, b) = 1 + \varrho^a + \varrho^{4a} + \varrho^{9a} + \cdots + \varrho^{(b-1)^2a}, \]
where $\varrho = e^{\frac{2\pi i}{n}}$ is a root of the equation $x^n - 1 = 0$. But, since $\zeta^n = 1$,
\[ (\zeta^a)^b - 1 = \zeta^{ab} - 1 = \zeta^n - 1 - 1 - 1 = 0, \]
is $\zeta^a$ is a root of the equation $x^b - 1 = 0$. Then replacing $\varrho$ with $\zeta^a$ we get:
\[ G(a, b) = 1 + \zeta^{a^2} + \zeta^{4a^2} + \zeta^{9a^2} + \cdots + \zeta^{(b-1)^2a^2}. \]
In the same way, since \( \zeta^b \) is a root of the equation \( x^a - 1 = 0 \) we find that the sum \( 1 + \zeta^{b^2} + \zeta^{4b^2} + \zeta^{9b^2} + \cdots + \zeta^{(a-1)b^2} \) agrees with \( G(b, a) \). Let us express \( G(a, b), G(b, a) \) and \( G(1, n) \) in a compact way:

\[
G(a, b) = \sum_{\beta=0}^{b-1} \zeta^{\beta^2 a^2}, \quad G(b, a) = \sum_{\alpha=0}^{a-1} \zeta^{\alpha^2 b^2} \quad \text{and} \quad G(1, n) = \sum_{\nu=0}^{n-1} \zeta^{\nu^2}.
\]

Hence:

\[
G(a, b)G(b, a) = \left( \sum_{\beta=0}^{b-1} \zeta^{\beta^2 a^2} \right) \left( \sum_{\alpha=0}^{a-1} \zeta^{\alpha^2 b^2} \right) = \sum_{\beta=0}^{b-1} \sum_{\alpha=0}^{a-1} \zeta^{\beta^2 a^2 + \alpha^2 b^2}.
\]

Note that \( \zeta^{2ab} = \zeta^{2\beta n} = 1 \), therefore:

\[
G(a, b)G(b, a) = \sum_{\beta=0}^{b-1} \sum_{\alpha=0}^{a-1} \zeta^{\beta^2 a^2 + \alpha^2 b^2} = \sum_{\beta=0}^{b-1} \sum_{\alpha=0}^{a-1} \zeta^{\beta^2 a^2 + \alpha^2 b^2} \zeta^{2ab} = \sum_{\beta=0}^{b-1} \sum_{\alpha=0}^{a-1} \zeta^{\beta^2 a^2 + 2\alpha \beta a + \alpha^2 b^2} = \sum_{\beta=0}^{b-1} \sum_{\alpha=0}^{a-1} \zeta^{(\beta a + \alpha b)^2}.
\]

Now notice that, when \( \alpha \) takes the values \( 0, 1, 2, \ldots, a - 1 \) and \( \beta \) takes the values \( 0, 1, 2, \ldots, b - 1 \), the numbers \( \beta a + \alpha b \mod n \) take the values \( 0, 1, 2, \ldots, n - 1 \). Indeed if there exist \( \alpha, \overline{\alpha} \in \{0, 1, \ldots, a - 1\} \) and \( \beta, \overline{\beta} \in \{0, 1, \ldots, b - 1\} \) such that \( (\beta a + \alpha b) \equiv (\overline{\beta} a + \overline{\alpha} b) \mod n \) then:

\[
(\beta a + \alpha b) \equiv (\overline{\beta} a + \overline{\alpha} b) \mod n \implies a(\beta - \overline{\beta}) \equiv b(\overline{\alpha} - \alpha) \mod n
\]

\[
\implies ab(\beta - \overline{\beta}) \equiv b^2(\overline{\alpha} - \alpha) \mod n
\]

\[
\implies 0 \equiv b^2(\overline{\alpha} - \alpha) \mod n
\]

Since \( b^2 \not\equiv 0 \mod n \), it implies \( \overline{\alpha} - \alpha \equiv 0 \mod n \), and this is only true when \( \overline{\alpha} = \alpha \) because \( \alpha, \overline{\alpha} \in \{0, 1, \ldots, a - 1\} \). Similarly we find that \( \beta \) must be equal to \( \overline{\beta} \).

Then, for each \( \alpha b + \beta a \) there exist a number \( \nu, 0 \leq \nu \leq n - 1 \), such that \( \alpha b + \beta a = \nu \), hence

\[
\zeta^{(\alpha b + \beta a)^2} = \zeta^{\nu^2}.
\]

Therefore the set \( \{ \alpha b + \beta a \mid \alpha \in \{0, 1, \ldots, a - 1\}, \beta \in \{0, 1, \ldots, b - 1\} \} \) is equal to the set \( \{ \nu \mid \nu \in \{0, 1, \ldots, n - 1\} \} \) and we can say:

\[
G(a, b)G(b, a) = \sum_{\beta=0}^{b-1} \sum_{\alpha=0}^{a-1} \zeta^{(\beta a + \alpha b)^2} = \sum_{\nu=0}^{n-1} \zeta^{\nu^2} = G(1, n).
\]

\( \square \)

Gauss noticed that this result can be generalized as follows:

**Theorem 4.1.8** Let \( n = a_1 a_2 \ldots a_k \) where \( a_1, a_2, \ldots, a_k \) are \( k \) different integers relatively prime to each other. Then \( G(1, n) = 1 + \zeta + \zeta^4 + \zeta^9 + \cdots + \zeta^{n-1} \) is the
product of:

\[ G\left(\frac{n}{a_1}, a_1\right) = 1 + \zeta^{a_1^2} + \zeta^{\frac{a_1}{n}} + \zeta^{\frac{a_1}{p_1}} + \cdots + \zeta^{\left(a_1-1\right)^2 n^2}, \]

\[ G\left(\frac{n}{a_2}, a_2\right) = 1 + \zeta^{a_2^2} + \zeta^{\frac{a_2}{n}} + \zeta^{\frac{a_2}{p_2}} + \cdots + \zeta^{\left(a_2-1\right)^2 n^2}, \]

\[ \vdots \]

\[ G\left(\frac{n}{a_k}, a_k\right) = 1 + \zeta^{a_k^2} + \zeta^{\frac{a_k}{n}} + \zeta^{\frac{a_k}{p_k}} + \cdots + \zeta^{\left(a_k-1\right)^2 n^2}. \]

I.e. \( G(1, n) = \prod_{i=1}^{k} G\left(\frac{n}{a_i}, a_i\right). \)

And as a consequence Gauss stated the following theorem:

**Theorem 4.1.9** Let \( p_1, p_2, \ldots, p_k \) be \( k \) different odd prime numbers and let \( n = p_1 p_2 \ldots p_k \). Let \( m \) denote the number of \( p_i \) which are of the form \( 4\mu + 3 \) and let \( s \) denote the number of \( p_i \) which satisfy that \( \frac{n}{p_i} \) is nonresidue of \( p_i \). Hence, if \( s \) is even, \( m \) must be of the form \( 4\mu + 3 \) or \( 4\mu + 1 \), but if \( s \) is odd, \( m \) must be of the form \( 4\mu + 2 \) or \( 4\mu + 4 \).

Note that, if instead of \( k \) primes we only take 2, the previous theorem states the same that the quadratic reciprocity law.

**Theorem 4.1.10** (Equivalent to the quadratic reciprocity law) Let \( p \) and \( q \) be two different odd prime numbers and let \( n \) be their product. Let \( m \) denote how many prime factors of \( n \) are of the form \( 4\mu + 3 \) and let

\[
 s = \begin{cases} 
 0 & \text{if } p \text{ and } q \text{ are both residues of each other,} \\
 2 & \text{if } p \text{ and } q \text{ are both nonresidues of each other,} \\
 1 & \text{otherwise.} 
\end{cases}
\]

Then, if \( s \) is even, i.e. \( \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1 \), \( m \) must be 0 or 1, but if \( s \) is odd, i.e. \( \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = -1 \), \( m \) must be 2.

In [Gau4], Gauss proved the general theorem (Theorem 4.1.9), but since the case that is of our interest is \( k = 2 \) we will only prove Theorem 4.1.10. The proof of Theorem 4.1.9 is analogous.

**Proof.** By Theorem 4.1.7 we know that \( G(p, q)G(q, p) = G(1, pq) \). And by equation (4.1.23) we have:

\[
 G(p, q) = \begin{cases} 
 \left(\frac{p}{q}\right)^{\sqrt{q}}, & \text{if } q \equiv 1 \pmod{4}, \\
 \left(\frac{p}{q}\right)^{\sqrt{q}}, & \text{if } q \equiv 3 \pmod{4}, 
\end{cases} \quad G(q, p) = \begin{cases} 
 \left(\frac{q}{p}\right)^{\sqrt{p}}, & \text{if } q \equiv 1 \pmod{4}, \\
 i\left(\frac{q}{p}\right)^{\sqrt{p}}, & \text{if } q \equiv 3 \pmod{4}, 
\end{cases}
\]
and

\[ G(1, pq) = G(1, n) = \begin{cases} \sqrt{n}, & \text{if } n \equiv 1 \pmod{4}, \\ i\sqrt{n}, & \text{if } n \equiv 3 \pmod{4}. \end{cases} \]

Hence let us distinguish four different cases:

\[ G(1, pq) = G(p, q)G(q, p) \]

\[ \begin{align*}
\{ & p = 4\mu + 1 \\ & q = 4\mu + 1 \} \rightarrow \sqrt{pq} = \left( \frac{p}{q} \right) \sqrt{q} \cdot \left( \frac{q}{p} \right) \sqrt{p} \implies \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = 1 \\
\{ & p = 4\mu + 1 \\ & q = 4\mu + 3 \} \rightarrow i\sqrt{pq} = i \left( \frac{p}{q} \right) \sqrt{q} \cdot \left( \frac{q}{p} \right) \sqrt{p} \implies \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = 1 \\
\{ & p = 4\mu + 3 \\ & q = 4\mu + 1 \} \rightarrow i\sqrt{pq} = \left( \frac{p}{q} \right) \sqrt{q} \cdot i \left( \frac{q}{p} \right) \sqrt{p} \implies \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = -1 \\
\{ & p = 4\mu + 3 \\ & q = 4\mu + 3 \} \rightarrow \sqrt{pq} = \left( \frac{p}{q} \right) \sqrt{q} \cdot i \left( \frac{q}{p} \right) \sqrt{p} \implies \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = -1 
\end{align*} \]

Note that \( s \) is even in the three first cases, and in these cases \( m \) is 0 or 1. And \( s \) is odd in the last case where \( m \) is 2.

\[ \square \]

4.2. Gauss’s sixth proof

In this section we will show Gauss’s sixth proof, proved in his article *Theorematis fundamentalis in theoria residuorum quadraticorum demonstratio sexta* (see [Gau6]).

First of all, let us state a theorem and its corollary that will be used during the whole proof.

**Theorem 4.2.1** Let \( p \) be an odd prime number and let \( n \) be a positive integer not divisible by \( p \). Then

\[
\frac{1 + x^n + x^{2n} + x^{3n} + \cdots + x^{(p-1)n}}{1 + x + x^2 + x^3 + \cdots + x^{p-1}} \in \mathbb{Z}[x],
\]

i.e. \( 1 + x^n + x^{2n} + x^{3n} + \cdots + x^{(p-1)n} \) is divisible by \( 1 + x + x^2 + x^3 + \cdots + x^{p-1} \).

**Proof.** Since \( p \) and \( n \) are coprime, by Bézout’s identity we know that there exist \( g \) and \( h \) positive integers such that \( gn - hp = 1 \) or, which is equivalent, \( gn = 1 + hp \).

Hence:

\[
\frac{1 + x^n + x^{2n} + x^{3n} + \cdots + x^{(p-1)n}}{1 + x + x^2 + x^3 + \cdots + x^{p-1}} = \left( \frac{1 - x^{np}}{1 - x^n} \right) \left( \frac{1 - x}{1 - x^p} \right)
= \left( \frac{1 - x^{np}}{1 - x^n} \right) \left( 1 - x^{gn} + x^{1+hp} - x \right)
= \frac{1 - x^{np}}{1 - x^p} \cdot \frac{1 - x^{gn}}{1 - x^n} \cdot \frac{1 - x^{np}}{1 - x^n} \cdot \frac{x(1 - x^{hp})}{1 - x^p}.
\]
4.2. GAUSS'S SIXTH PROOF

Since \( \frac{1-x^n}{1-x} = 1 + x^2 + x^3 + \cdots + x^{(b-1)a} \), the above expression belongs to \( \mathbb{Z}[z] \), so we can conclude that \( 1 + x^n + x^{2n} + x^{3n} + \cdots + x^{(p-1)n} \) is divisible by \( 1 + x + x^2 + x^3 + \cdots + x^{p-1} \). \( \square \)

**Corollary 4.2.2** Every polynomial \( p(x) \in \mathbb{Z}[x] \) that is divisible by \( \frac{1-x^n}{1-x} \) is also divisible by \( \frac{1-x^p}{1-x} \).

**Proof.** Since by hypothesis \( p(x) \) is divisible by \( \frac{1-x^n}{1-x} \) we have:

\[
p(x) = q(x) \in \mathbb{Z}[x].
\]

Therefore, by Theorem 4.2.1,

\[
\frac{p(x)}{1 + x + x^2 + \cdots + x^p} = \frac{q(x)}{1 + x + x^2 + \cdots + x^p} \in \mathbb{Z}[x].
\]

\( \square \)

Now let us start the proof itself. This proof could be separated in two parts. The first part of the proof mostly consists in study the divisibility of certain polynomials in \( \mathbb{Z}[x] \).

4.2.1. First part of Gauss’s sixth proof

**Lemma 4.2.3** Let \( p \) be an odd prime number and let \( \alpha \) be a primitive root modulo \( p \), i.e. an integer such that their powers \( 1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p-2} \) modulo \( p \) agree with the set \( \{1, 2, 3, \ldots, p-1\} \). In other words, let \( \alpha \) be a generator of the multiplicative group of integers modulo \( p \). Let us define

\[
f(x) = 1 + x + x^2 + x^3 + \cdots + x^{p-1}.
\]

Then \( f(x) \) is divisible by \( 1 + x + x^2 + x^3 + \cdots + x^{p-1} \).

**Proof.** First of all note that \( f(x) - 1 - x - x^2 - x^3 - \cdots - x^{p-1} \) is divisible by \( \frac{1-x^p}{1-x} \). Indeed

\[
f(x) - 1 - x - x^2 - x^3 - \cdots - x^{p-1} = x + x^2 + x^3 + \cdots + x^{p-2} - 1 - x - x^2 - \cdots - x^{p-1}
\]

and note that the first \( p - 1 \) exponents are powers of \( \alpha \), which modulo \( p \) agree with the last \( p - 1 \) exponents. So, for each \( i \in \{0, 1, 2, \ldots, p-1\} \) there exists \( j_i \in \{1, 2, 3, \ldots, p-1\} \) (different for each \( i \)) such that \( \alpha^{j_i} \equiv j_i \pmod{p} \) or, which is the same, \( \alpha^{i} \equiv j_i + h_i \pmod{p} \). Then:

\[
\frac{x^{\alpha^i} - x^{j_i}}{1 - x} = \frac{-x^{j_i}(1 - x^{h_i}p)}{1 - x} = -x^{j_i}(1 + x^p + x^{2p} + \cdots + x^{(h_i-1)p}) \in \mathbb{Z}[x].
\]

So we have

\[
f(x) - 1 - x - x^2 - x^3 - \cdots - x^{p-1} = (1 - x) \sum_{i=0}^{p-2} -x^{j_i} \frac{1 - x^{h_i}p}{1 - x} \in \mathbb{Z}[x]
\]
Theorem 4.2.5

Proof. Let us study the two cases separately.

- \( n \) is coprime to \( p \). By Lemma 4.2.3, replacing \( x \) with \( x^n \), we have that \( f(x^n) \) is divisible by \( \frac{1 - x^n}{1 - x} \). And by Corollary 4.2.2 we can conclude that \( f(x^n) \) is divisible by \( \frac{1 - x^n}{1 - x} \).

- \( n \) is a multiple of \( p \), i.e. \( n = hp \). We know that

\[
\begin{align*}
    f(x^n) - p &= 1 + x^n + x^{na} + x^{na^2} + \cdots + x^{na^{p-2}} - p \\
    &= x^n + x^{na} + x^{na^2} + \cdots + x^{na^{p-2}} - (p - 1) \\
    &= (x^n - 1) + (x^{na} - 1) + (x^{na^2} - 1) + \cdots + (x^{na^{p-2}} - 1) \\
    &= (x^{hp} - 1) + (x^{hpa} - 1) + (x^{hp^2} - 1) + \cdots + (x^{hp^{p-2}} - 1).
\end{align*}
\]

Note that each summand is divisible by \( 1 - x^p \), hence \( \frac{f(x^n) - p}{1 - x^p} \in \mathbb{Z}[x] \). Consequently \( (f(x^n) - p) \frac{1 - x}{1 - x^p} \) also belongs to \( \mathbb{Z}[x] \), so \( f(x^n) - p \) is divisible by \( \frac{1 - x^p}{1 - x} \).

\[ \square \]

Lemma 4.2.4 Let us take \( p, \alpha \) and \( f(x) \) defined as in Lemma 4.2.3 and let \( n \) be a positive integer. Then, if \( n \) is coprime to \( p \), \( f(x^n) \) is divisible by \( \frac{1 - x^n}{1 - x} \), but if \( n \) is a multiple of \( p \), is \( f(x) - p \) that is divisible by \( \frac{1 - x^p}{1 - x} \).

Proof. Let us study the two cases separately.

- \( n \) is coprime to \( p \). By Lemma 4.2.3, replacing \( x \) with \( x^n \), we have that \( f(x^n) \) is divisible by \( \frac{1 - x^n}{1 - x} \). And by Corollary 4.2.2 we can conclude that \( f(x^n) \) is divisible by \( \frac{1 - x^n}{1 - x} \).

- \( n \) is a multiple of \( p \), i.e. \( n = hp \). We know that

\[
\begin{align*}
    f(x^n) - p &= 1 + x^n + x^{na} + x^{na^2} + \cdots + x^{na^{p-2}} - p \\
    &= x^n + x^{na} + x^{na^2} + \cdots + x^{na^{p-2}} - (p - 1) \\
    &= (x^n - 1) + (x^{na} - 1) + (x^{na^2} - 1) + \cdots + (x^{na^{p-2}} - 1) \\
    &= (x^{hp} - 1) + (x^{hpa} - 1) + (x^{hp^2} - 1) + \cdots + (x^{hp^{p-2}} - 1).
\end{align*}
\]

Note that each summand is divisible by \( 1 - x^p \), hence \( \frac{f(x^n) - p}{1 - x^p} \in \mathbb{Z}[x] \). Consequently \( (f(x^n) - p) \frac{1 - x}{1 - x^p} \) also belongs to \( \mathbb{Z}[x] \), so \( f(x^n) - p \) is divisible by \( \frac{1 - x^p}{1 - x} \).

\[ \square \]

Theorem 4.2.5 Let us define the polynomial

\[ \xi = \xi(x) = x - x^\alpha + x^{\alpha^2} - x^{\alpha^3} + x^{\alpha^4} - \cdots - x^{\alpha^{p-2}}. \]

Then \( \xi^2 - (-1)^{\frac{p + 1}{2}} p \) is divisible by \( \frac{1 - x^p}{1 - x} \).

Note that replacing \( x \) with an \( n \)-th root of unity, \( \zeta \), then \( \xi(\zeta) = G(1, p) \) where \( G(1, p) \) is the Gauss sum defined in section 4.1.

Proof. Let us take the following \( p - 1 \) polynomials:

\[
\begin{align*}
    +x\xi - x^2 &+ x^{\alpha+1} - x^{\alpha^2+1} + \cdots + x^{\alpha^{p-2}+1} \\
    -x^\alpha\xi - x^{2\alpha} + x^{\alpha^2+\alpha} - x^{\alpha^3+\alpha} + \cdots + x^{\alpha^{p-1}+\alpha} \\
    +x^{\alpha^2}\xi - x^{2\alpha^2} + x^{\alpha^3+\alpha^2} - x^{\alpha^4+\alpha^2} + \cdots + x^{\alpha^{p-1}+\alpha^2} \\
    -x^{\alpha^3}\xi - x^{2\alpha^3} + x^{\alpha^4+\alpha^3} - x^{\alpha^5+\alpha^3} + \cdots + x^{\alpha^{p+1}+\alpha^3}
\end{align*}
\]
Hence $\Omega$ is divisible by $(1 - x^p)$, and so their sum. Note that the sum of these polynomials, $\Omega$, can be expressed as follows:

$$
\Omega = \xi^2 - (f(x^2) - \ell) + (f(x^{p+1}) - \ell) - \left( f(x^{p^2+1}) - \ell \right) + \cdots + \left( f(x^{p^{p-2}+1}) - \ell \right).
$$

Hence $\Omega$ is divisible by $(1 - x^p)$ and, consequently, $\Omega$ is also divisible by $\frac{1-x^p}{1-x}$. Note that from all the exponents of $x$ in the expression of $\Omega$ (i.e., $2, \alpha + 1, \alpha^2 + 1, \ldots, \alpha^{(p-2) + 1}$) only one of them is a multiple of $p$, and it will be the exponent $\frac{1}{2}(p-1) + 1$. Indeed:

$$
\left( \alpha^{\frac{1}{2}(p-1)} \right)^2 \equiv 1 \pmod{p} \implies \alpha^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p} \\
\implies \alpha^{\frac{1}{2}(p-1)} + 1 \equiv 0 \pmod{p}.
$$

Hence, by Lemma 4.2.3 and Corollary 4.2.2, we have that every summand $f(x^2)$ of $\Omega$ with $\beta \neq \alpha^{\frac{1}{2}(p-1) + 1}$ are divisible by $\frac{1-x^p}{1-x}$. Therefore $\xi^2 - (-1)^{\frac{p+1}{2}} f(x^{\alpha^{\frac{1}{2}(p-1) + 1}})$ is divisible by $\frac{1-x^p}{1-x}$. But, by Lemma 4.2.3, we also have that $f(x^{\alpha^{\frac{1}{2}(p-1) + 1}}) - p$ is divisible by $\frac{1-x^p}{1-x}$.

From this it follows that

$$
\xi^2 - (-1)^{\frac{p+1}{2}} f\left(x^{\alpha^{\frac{1}{2}(p-1) + 1}}\right) + (-1)^{\frac{1}{2}(p-1)} f\left(x^{\alpha^{\frac{1}{2}(p-1) + 1}}\right) = \xi^2 - (-1)^{\frac{p+1}{2}} p
$$

must be divisible by $\frac{1-x^p}{1-x}$.

**Definition 4.2.6.** Since in Theorem 4.2.5 we proved that $\xi^2 - (-1)^{\frac{p-1}{2}}$ divided by $\frac{1-x^p}{1-x}$ is a polynomial in $\mathbb{Z}[x]$, let us define the following polynomial:

$$
Z = Z(x) = \frac{(1-x) \left( \xi^2 - (-1)^{\frac{p+1}{2}} p \right)}{1-x^p}. \tag{4.2.1}
$$

Now let us take a positive odd integer, say $q$. Then we have that

$$
\frac{(\xi^2)^{\frac{1}{2}(q-1)} - \left( (-1)^{\frac{p+1}{2}} p \right)^{\frac{1}{2}(q-1)}}{\xi^2 - (-1)^{\frac{p+1}{2}} p} \in \mathbb{Z}[x].
$$

So, by Theorem 4.2.5, we have that $\xi^{q-1} - (-1)^{\frac{(p-1)(q-1)}{2}} p^{\frac{q-1}{2}}$ is also divisible by $\frac{1-x^p}{1-x}$.

**Definition 4.2.7.** Since we have seen that $\xi^{q-1} - (-1)^{\frac{(p-1)(q-1)}{2}} p^{\frac{q-1}{2}}$ divided by $\frac{1-x^p}{1-x}$ is a polynomial in $\mathbb{Z}[x]$, let us define the following polynomial:

$$
Y = Y(x) = \frac{(1-x) \left( \xi^{(q-1)} - \left( (-1)^{\frac{(p-1)(q-1)}{2}} p^{\frac{q-1}{2}} \right) \right)}{1-x^p}. \tag{4.2.2}
$$
Now let us suppose that \( q \) is an odd prime (different to \( p \)). Hence, in the article 51 of *Disquisitiones Arithmeticae* it is proved that

\[
\xi^q \equiv \left(x - x^\alpha + x^{p-2} - \cdots - x^{(p-2)\alpha} \right)^q \equiv x^q - x^{q\alpha} + x^{q(p-2)} - \cdots - x^{q(p-2)^2} \quad (\text{mod } q).
\]

Hence

\[
\xi^q - \left(x^q - x^{q\alpha} + x^{q(p-2)} - \cdots - x^{q(p-2)^2} \right) \equiv 0 \quad (\text{mod } q).
\]

This implies that \( \xi^q - \left(x^q - x^{q\alpha} + x^{q(p-2)} - \cdots - x^{q(p-2)^2} \right) \) is divisible by \( q \).

**Definition 4.2.8.** Since \( \xi^q - \left(x^q - x^{q\alpha} + x^{q(p-2)} - \cdots - x^{q(p-2)^2} \right) \) is divisible by \( q \), let us define the following polynomial:

\[
X = X(x) = \frac{\xi^q - \left(x^q - x^{q\alpha} + x^{q(p-2)} - \cdots - x^{q(p-2)^2} \right)}{q} \quad (4.2.3)
\]

Since \( \alpha \) is a primitive root modulo \( p \), there exist a \( \mu \) such that \( \alpha^\mu \equiv q \) (mod \( p \)). Hence set of numbers

\[q, q\alpha, q\alpha^2, \ldots, q\alpha^{p-2}\]

are congruent modulo \( p \) with

\[\alpha^\mu, \alpha^{\mu+1}, \ldots, \alpha^{p-2}, 1, \alpha, \alpha^2, \ldots, \alpha^{\mu-1}.
\]

Therefore, the polynomials

\[
x^q - x^{\alpha^\mu}, x^{q\alpha} - x^{\alpha^{\mu+1}}, x^{q\alpha^2} - x^{\alpha^{\mu+2}}, \ldots, x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}},
\]

\[
x^{q\alpha^{p-\mu}} - x^{\alpha^{p-1}}, x^{q\alpha^{p-\mu+1}} - x^{\alpha^{p-2}}, \ldots, x^{q\alpha^{p-2}} - x^{\alpha^{p-1}}
\]

are all divisible by \( 1 - x^p \). Applying the alternate sum at these polynomials we get that the resulting polynomial

\[
x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \cdots - x^{q(p-2)^2} - (-1)^\mu \xi
\]

is also divisible by \( 1 - x^p \).

Note that \( q \) is a residue of \( p \) if and only if \( \mu \) is even, then \((-1)^\mu = \left(\frac{q}{p}\right)\).

**Definition 4.2.9.** Since \( x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \cdots - x^{q(p-2)^2} - (-1)^\mu \xi \) is divisible by \( 1 - x^p \) and \((-1)^\mu \) agrees to the Legendre symbol, let us define the following polynomial:

\[
W = W(x) = \frac{x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \cdots - x^{q(p-2)^2} - \left(\frac{q}{p}\right) \xi}{1 - x^p} \quad (4.2.4)
\]
4.2. GAUSS’S SIXTH PROOF

After being defined the polynomials $\xi, Z(x), Y(x), W(x)$ and $X(x)$ we can find an identity containing in its expression the five polynomials and playing with it we will finally find the quadratic reciprocity law. We shall prove that the identity

$$q\xi = q\left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \left(\frac{q}{p}\right)\right) + \frac{1-x^p}{1-x} \left(Z \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} \right) - \left(\frac{q}{p}\right)\right) + Y\xi^2 - W\xi(1-x)$$  (4.2.5)

holds, where $\varepsilon = (-1)^{\frac{p-1}{2}}$ and $\delta = (-1)^{\frac{(p-1)(q-1)}{4}}$. Indeed, from the expressions:

$$q\xi = \xi^{q+1} - \xi^{(x^q - x^q \alpha + x^{q \alpha^2} - \cdots - x^{q \alpha^{q-2}})}$$

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

$$\frac{1-x^p}{1-x} \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \left(\frac{q}{p}\right)\right) = \xi^2 - (-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} + \varepsilon \left(\frac{q}{p}\right)$$

$$\frac{1-x^p}{1-x} (Y\xi^2) = \xi^2 = -\xi^{(x^q - x^q \alpha + x^{q \alpha^2} - \cdots - x^{q \alpha^{q-2}})}$$

we can check that the equality follows.

Now let us consider the division of $\xi X$ by $\frac{1-x^p}{1-x}$, getting

$$\xi X = \frac{1-x^p}{1-x} U + T$$  (4.2.6)

where $U = U(x)$ is the quotient of the division and $T = T(x)$ the remainder. Replacing what we got in the equation (4.2.6) to the equation (4.2.5) we have:

$$qT - \varepsilon \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \left(\frac{q}{p}\right)\right) = \frac{1-x^p}{1-x} \left(Z \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} \right) - \left(\frac{q}{p}\right)\right) + Y\xi^2 - W\xi(1-x) - qU$$

For this equation to hold, both sides of the equation need to have the same degree. Note that the degree of the left side of the equation is smaller than $p - 1$, since $T$ is the only factor depending on $x$ and $\deg T < p - 1$ because is the remainder of the division of $\xi X$ by $1 + x + x^2 + \cdots + x^{p-1}$. Hence, if

$$\frac{1-x^p}{1-x} \left(Z \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} \right) + Y\xi^2 - W\xi(1-x) - qU\right) \neq 0$$

the degree of the right side of the equation is greater than or equal to $p - 1$. Hence, it is necessary that

$$\frac{1-x^p}{1-x} \left(Z \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} \right) + Y\xi^2 - W\xi(1-x) - qU\right) = 0$$

and this implies that both sides of the equation must be $0$. Then

$$qT - \varepsilon \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \left(\frac{q}{p}\right)\right) = 0 \Rightarrow qT = \varepsilon \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \left(\frac{q}{p}\right)\right)$$

so $\varepsilon \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \left(\frac{q}{p}\right)\right)$ is divisible by $q$. Since $p$ and $q$ are coprime, $q \nmid \varepsilon$, hence $q \mid \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \left(\frac{q}{p}\right)\right)$, what implies $q \mid \left(\frac{p^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}} - \delta \left(\frac{q}{p}\right)\right)$ since $\delta^2 = 1$. 

By Euler’s criterion (Proposition 1.3.3) we have that
\[ p^{\frac{q-1}{2}} \equiv \left( \frac{p}{q} \right) \pmod{q}, \]
i.e. we have that \( p^{\frac{q-1}{2}} - \left( \frac{p}{q} \right) \) is divisible by \( q \). Hence
\[ \left( p^{\frac{q-1}{2}} - \delta \left( \frac{q}{p} \right) \right) - \left( p^{\frac{q-1}{2}} - \left( \frac{p}{q} \right) \right) = \left( \frac{p}{q} \right) - \delta \left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) - (-1)^{\frac{p-1}{2}(q-1)} \left( \frac{q}{p} \right) \]
is also divisible by \( q \). But \( \left( \frac{p}{q} \right) - (-1)^{\frac{p-1}{2}(q-1)} \left( \frac{q}{p} \right) \) can only take the values \(-2, -1, 0, 1, 2\). Then, since \( q \) is an odd prime and \( q \) divides (4.2.7), the only value that \( \left( \frac{p}{q} \right) - (-1)^{\frac{p-1}{2}(q-1)} \left( \frac{q}{p} \right) \) can take is 0. Hence we get:
\[ \left( \frac{p}{q} \right) = (-1)^{\frac{p-1}{2}(q-1)} \left( \frac{q}{p} \right), \]
which is the statement of the quadratic reciprocity law.
References


[Lem1] [http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html](http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html)