The Law of Quadratic Reciprocity

From Fermat to Gauss

Author: Daniel Alkema (4025105)
Supervisor: Prof. Dr. Jan Hogendijk

University of Utrecht
January 2016

Contents

1 Introduction

In this thesis we will take a look at the development of the law of quadratic reciprocity. What is necessary to come up with such a theorem and what were the fundamental ideas connected to the quadratic reciprocity law which mathematicians came up with through out the years?

We will start our journey with Fermat, whose little theorem became very important in our story. Then we continue with Euler, the first mathematician who stated the complete law of quadratic reciprocity and Legendre who did some fundamental work, but eventually could not prove the quadratic reciprocity law. The first person who did was Gauss, he actually gave eight different proofs during his lifetime and we will study his third and fourth proof.

In this thesis we have made use of modern notation. The difference is not very large, because since the 17^{th} century, mathematicians used a notation that was similar to ours. Especially since the time of Euler (1707-1783) and most of this thesis is about the time during and after Euler's lifetime.

In this thesis we have tried to give a good overview of the development of the quadratic reciprocity law. Which also means that we have tried to clarify sources. It will be interesting to read if you are interested in number theory and the historical development of a mathematical law. It is written in such a way that first year mathematical students could understand it and even motivated secondary school pupils. The only important pre-knowledge someone must have is knowing how modulo calculations work. For Gauss' fourth proof, it is useful to know the binomial coefficient. An introduction in binomial series can be found in the book *Calculus*[1].

We have made use of secondary literary sources like historical and number theoretical source books, but the most important parts are based on the original works from Euler, Legendre and Gauss. Sometimes we will not give original proofs of theorem, because with modern mathematics there are much easier to understand proofs, especially for the target audience. If this is the case we will mention it.

Before we start, we will look at what the theorem is all about.
Quadratic reciprocity is a theorem about quadratic residues modulo a prime number p. Lets look at the equation

$$x^2 \equiv a \mod p$$

where p is a prime number and a is an integer coprime to p. We say that a is a quadratic residue modulo p if we can solve this equation for $x \in \mathbb{Z}$.

[1] R.A.Adams, C. Essex, *Calculus, a complete source*, 7^{th} edition, Toronto, 2003, p. 549-552

Example 1.1 Is 11 a quadratic residue modulo 53?
The question is; can we solve $x^2 \equiv 11 \mod 53$? By trying we can find that $x = 8$ will work. Because $8^2 \equiv 64 \equiv 11 \mod 53$. That means that 11 is a quadratic residue modulo 53.

To make things more clear in the first part of the thesis, we will introduce the law of quadratic reciprocity. But first, let us introduce the symbol of Legendre:

Definition (Legendre symbol) Let p be a prime number and a an integer not divisible by p. Then

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & if\ a\ is\ a\ quadratic\ residue\ modulo\ p \\ -1 & if\ a\ is\ a\ quadratic\ non-residue\ modulo\ p \end{cases}$$

The Legendre symbol is defined as zero if p divides a.

We are now ready to state the full law of quadratic reciprocity.
Take two prime numbers p and q to begin with. We can now ask the questions whether q is a quadratic residue modulo p or p is a quadratic residue modulo q. These two questions are very different and at first sight it seems that the answers can not be related to each other. But the law of quadratic reciprocity relates the Legendre symbols $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ in a very beautiful way:

Theorem 1.1 (Quadratic Reciprocity) Let p and q be different odd primes, then

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

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

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

Since the Legendre symbol is always +1 or -1, we can also write the last formula as

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

Example 1.2: Is 31 a quadratic residue modulo 43?
From theorem 3.1 below we can just try all $\frac{43-1}{2} = 21$ squares. But a faster method is to calculate the Legendre symbol.

$$\left(\frac{31}{43}\right) = \left(\frac{43}{31}\right)(-1)^{\frac{43-1}{2}\frac{31-1}{2}} = -\left(\frac{43}{31}\right) = -\left(\frac{12}{31}\right).$$

Because the Legendre symbol is multiplicative, we have

$$\left(\frac{12}{31}\right) = \left(\frac{4}{31}\right)\left(\frac{3}{31}\right).$$

We know that $\left(\frac{4}{31}\right) = 1$ because $2^2 = 4$. We go further with $\left(\frac{3}{31}\right)$

$$\left(\frac{3}{31}\right) = \left(\frac{31}{3}\right)(-1)^{\frac{3-1}{2}\frac{31-1}{2}} = -\left(\frac{1}{3}\right)$$

because $\left(\frac{1}{3}\right) = 1$, we have that $\left(\frac{3}{31}\right) = -1$ and

$$\left(\frac{31}{43}\right) = (-1)\cdot 1\cdot(-1) = 1$$

And we conclude that 31 is a quadratic residue modulo 43.

Example 1.3: For which prime p numbers is 7 a quadratic residue modulo p?
We want to know when $\left(\frac{7}{p}\right)$ equals 1.

$$\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}\frac{7-1}{2}} = \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}}$$

We want that $\left(\frac{p}{7}\right)$ and $(-1)^{\frac{p-1}{2}}$ have the same sign, then $\left(\frac{7}{p}\right) = 1$
We know that the quadratic residues modulo 7, are 1,2 and 4. That means that the $\left(\frac{p}{7}\right)$ equals 1 if $p \equiv 1, 2, 4 \mod 7$ and -1 if $p \equiv 3, 5, 6 \mod 7$. We also know that $(-1)^{\frac{p-1}{2}}$ equals 1 if $p \equiv 1 \mod 4$ and -1 is $p \equiv 3 \mod 4$.
The Chinese remainder theorem gives us the following:

- If $p \equiv 1 \mod 4$ and $p \equiv 1 \mod 7$, then $p \equiv 1 \mod 28$
- If $p \equiv 1 \mod 4$ and $p \equiv 2 \mod 7$, then $p \equiv 9 \mod 28$
- If $p \equiv 1 \mod 4$ and $p \equiv 4 \mod 7$, then $p \equiv 25 \mod 28$
- If $p \equiv 3 \mod 4$ and $p \equiv 3 \mod 7$, then $p \equiv 3 \mod 28$
- If $p \equiv 3 \mod 4$ and $p \equiv 5 \mod 7$, then $p \equiv 19 \mod 28$
- If $p \equiv 3 \mod 4$ and $p \equiv 6 \mod 7$, then $p \equiv 27 \mod 28$

We conclude that 7 is a quadratic residue modulo p if
$p \equiv 1, 3, 9, 19, 25, 27 \mod 28$.

As we will see, the law of quadratic reciprocity is a beautiful theorem that can be proven in many different ways.

2 Preliminaries

2.1 Pierre the Fermat

As we go back in time, the first mathematician who can be related to quadratic reciprocity was Pierre de Fermat[2] (1601-1665). Fermat was a French lawyer from Toulouse. He had an excellent educational background, spoke Latin, Greek, Italian and Spanish fluently and was also well known for his poetry in several languages. It is not known when Fermat became interested in mathematics, but he did some great discoveries. Fermat is most famous for his last theorem. Fermat stated in this theorem that there are no integers a, b, c and $n > 2$ such that $a^n + b^n = c^n$. For $n = 2$ we have infinitely many solutions; take $a = s^2 - t^2$, $b = 2st$ and $c = s^2 + t^2$, these are all the solutions to this problem, for which the greatest common divisor of a, b, c is 1
But for the proof that for all $n > 2$, there are no integer solutions, we had to wait until 1995 when Andrew Wiles first proofs Fermat's last theorem[3].

There is an age old tradition among mathematicians; they challenged each other with problems to get respect for the discoveries they had done. Fermat did the same in a letter to his friend Frenicle de Bessy,[4] from 1640, in which he stated that $a^{p-1} - 1$ is divisible by p if p is prime number and coprime to a. This is now known as Fermat's little theorem and was the first step towards quadratic reciprocity.
This theorem can be generalized as follows:

Theorem 2.1 (Fermat's little theorem) Let p be a prime number and a an integer, then p divides $a^p - a$. If p does not divide a, then p divides $a^{p-1} - 1$. In other words $a^{p-1} \equiv 1 \mod p$.

The first proof of this theorem was given by Leonard Euler in 1736 in his paper *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio,*[5] although Leibniz already gave a proof in 1680, but this proof was only found in 1863 among the manuscripts that Leibniz had left. We will prove this in a modern way, based on the proof given in *A Computational Introduction to Number Theory and Algebra.*[6]

[2] Article: P. de Fermat, in G. Gillispie, ed. Dictionary of Scientific Biography vol. 4, New York, 1971, p. 566-576
[3] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Cambridge, 1995
[4] A translation of this letter can be found in **[6]**, E.54, letter 2 (October 1640) from the Fermat-Frenicle correspondence.
[5] **[6]** L. Euler, *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio,* St. Petersburg, 1736
[6] V.Shoup, *A Computational Introduction to Number Theory and Algebra,* New York, 2008

Proof First assume that $p \mid a$, then for obvious reasons $p \mid a^p - a$, and we are done.
Lets assume that $p \nmid a$ and consider the first $p-1$ multiples of a

$$a, 2a, ..., (p-1)a$$

If we look at these numbers modulo p we have

$$\begin{aligned} a &\equiv r_1 \mod p \\ 2a &\equiv r_2 \mod p \\ &\vdots \\ (p-1)a &\equiv r_{p-1} \mod p \end{aligned}$$

Where $0 < r_i \leq p-1$. All $r_i \neq 0$ otherwise $p \mid a$. If we have that ra and sa are the same modulo p, we have that $r \equiv s \mod p$. Thus the $p-1$ multiples are all distinct and nonzero. This means that they must be congruent to $1, 2, ..., (p-1)$ in some order. If we multiply all these congruences together we find

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \mod p$$

we can write this as

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p$$

dividing by (p-1)! gives

$$a^{p-1} \equiv 1 \mod p$$

hence

$$a^p \equiv a \mod p$$

And we completed the proof.

Fermat was interested in the question wether you can write a prime number p as $p = x^2 + y^2$ for some integers x and y. Fermat knew that you can write a prime number as sum of
squares if and only if $p = 2$ or $p \equiv 1 \mod 4$, which is strongly related to what we now know as the first supplementary law of quadratic reciprocity:

$$x^2 \equiv -1 \mod p \text{ is solvable if and only if } p \equiv 1 \mod 4$$

Fermat's work can be seen as the first motivation for other mathematicians to study such problems.

3 Leonard Euler

The first mathematician who can be related to quadratic reciprocity after Fermat was Leonard Euler[7] (1707-1783). Euler started by studying a lot of Fermat's work. Because Fermat left plenty of theorems behind without proving them, Euler started by trying to prove some of Fermat's theorems. In 1736 Euler published his paper **[6]**, in which he proved Fermat's little theorem for the first time. Euler published a total of 530 books and articles during his lifetime, and after his death, this number increased to 886. It took the academy of St. Petersburg almost 50 years before they published all the work Euler left behind.[8]

Eventually Euler discovered the law of quadratic reciprocity. Unfortunately, he could not prove quadratic reciprocity, but he came up with some fundamental results that guided Legendre and Gauss.

Euler discovered that for any odd prime number p, exactly half of the numbers between 0 and p are perfect squares modulo p, and the other half are not. In other words, for any prime number p there are exactly $\frac{p-1}{2}$ perfect squares modulo p. The numbers that are perfect squares are called quadratic residues, the ones that are not, are called quadratic non-residues.

Theorem 3.1 Let p be an odd prime, then there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p.

Example 3.1 What are the quadratic residues modulo 11? We determine all $x^2 \mod p$ for $x = 1, 2, ..., 10$, and we find

$$1^2 \equiv 1 \mod 11 \quad 2^2 \equiv 4 \mod 11 \quad 3^2 \equiv 9 \mod 11 \quad 4^2 \equiv 5 \mod 11 \quad 5^2 \equiv 3 \mod 11$$

$$6^2 \equiv 3 \mod 11 \quad 7^2 \equiv 5 \mod 11 \quad 8^2 \equiv 9 \mod 11 \quad 9^2 \equiv 4 \mod 11 \quad 10^2 \equiv 1 \mod 11$$

Observe that the row of quadratic residues $1, 4, 9, 5, 3, 3, 5, 9, 4, 1$ is symmetric.

Proof Let us look at all the squares $1^2, 2^2, ..., (p-1)^2$ modulo p. Since $x^2 \equiv (-x)^2 \mod p$, the $p-1$ integers form $\frac{p-1}{2}$ congruent pairs modulo p. Therefore, there are at most $\frac{p-1}{2}$ quadratic residues and we just have to look at $x^2 \mod p$ for $x = 1, 2, ..., \frac{p-1}{2}$, because all quadratic residues are congruent to one of $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2 \mod p$. We have to prove that all $\frac{p-1}{2}$

[7] **[2]** Article: L. Euler, p. 467-484
[8] D.J. Struik, *Geschiedenis van de wiskunde,* Utrecht, 1965

quadratic residues are different, which means that if $x^2 \equiv y^2 \mod p$, for $x, y \leq \frac{p-1}{2}$, then $x = y$.

Assume that $x^2 \equiv y^2 \mod p$, for some $1 \leq x, y < \frac{p}{2}$. Then p divides $x^2 - y^2 = (x+y)(x-y)$, thus p must divide $(x+y)$ or $(x-y)$. Since p can not divide $(x+y)$, because $0 < (x+y) < \frac{p}{2} + \frac{p}{2} = p$, it means that p divides $(x-y)$. This implies that $x \equiv y \mod p$.
We conclude that there are exactly $\frac{p-1}{2}$ different quadratic residues.

Euler was the first person to discover that the product of two quadratic residues or the product of two non-residues is a quadratic residue, and that the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue. In Legendre symbols this means the following:

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

Once we know this, we can assume that a is a prime number,
otherwise we can just factorize a and consider the problem a factor at a time.

After proving Fermat's little theorem, Euler came up with his own theorem, which can be seen as an extensive form of Fermat's little theorem.

Theorem 3.2: (Euler's criterion) Let p be a prime number and a an integer not divisible by p. Then

$$a^{\frac{p-1}{2}} \equiv \begin{cases} +1 \mod p & if\ a\ is\ a\ quadratic\ residue\ modulo\ p \\ -1 \mod p & if\ a\ is\ a\ quadratic\ non-residue\ modulo\ p \end{cases}$$

In other words, we have the following for the Legendre symbol

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

Proof We can write Fermat's little theorem as $a^{p-1} - 1 \equiv 0 \mod p$, and observe that this is equivalent to

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p \quad (1)$$

Hence, at least one of the factors on the left hand side must be congruent to $0 \mod p$. We will break this proof down in two parts, $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a}{p}\right) = -1$.

First part

Let us first assume that $\left(\frac{a}{p}\right) = 1$. This means that a is a quadratic residue $\mod p$. Therefore there exists an $x \in \mathbb{N}$ such that $x^2 \equiv a \mod p$. We can raise both sides by $\frac{p-1}{2}$ and we find $\left(x^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \mod p$ which is equivalent to $x^{p-1} \equiv a^{\frac{p-1}{2}} \mod p$. We know from Fermat's little theorem that x^{p-1} is equal to $1 \mod p$. We can conclude that if a is a quadratic residue $\mod p$, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1$. And if a is a quadratic residue $\mod p$, the first part of equation (1) will be zero.

We know that the equation $x^{\frac{p-1}{2}} - 1 = 0$ has at most $\frac{p-1}{2}$ roots, and because there are $\frac{p-1}{2}$ quadratic residues, these are exactly the roots of $x^{\frac{p-1}{2}} - 1 = 0$.

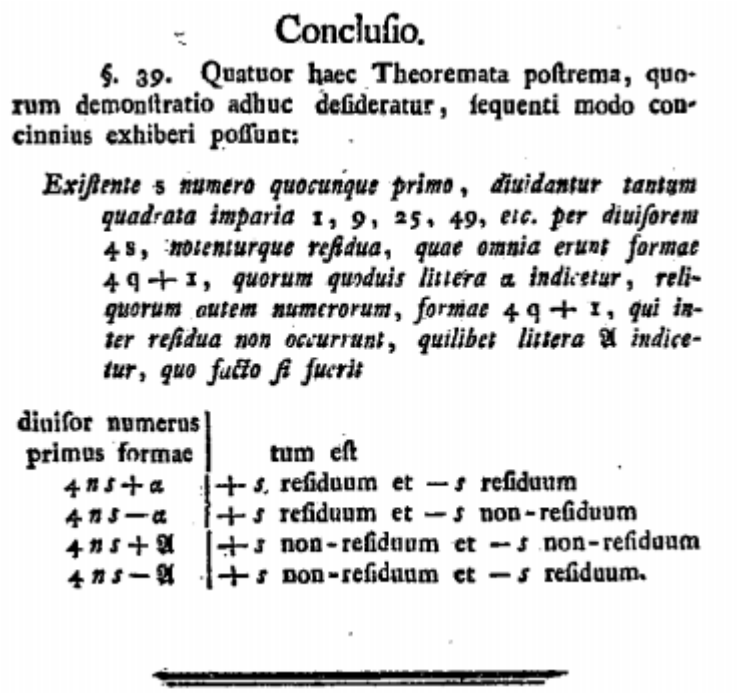
Second part

Let us now assume that $\left(\frac{a}{p}\right) = -1$. This means that a is not a quadratic residue modulo p. Since all these non-quadratic residues are roots of $x^{p-1} - 1 = 0$, but not from $x^{\frac{p-1}{2}} - 1 = 0$ because of the first part, they have to be roots of $x^{\frac{p-1}{2}} + 1 = 0$. By the same argument as in part 1, $x^{\frac{p-1}{2}} + 1 = 0$ has at most $\frac{p-1}{2}$ roots, and because there are $\frac{p-1}{2}$ quadratic non-residues, these are exactly the roots of $x^{\frac{p-1}{2}} + 1 = 0$. Thus all quadratic non-residues will make the second part of equation (1) zero.
We conclude that if a is not a quadratic residue modulo p,
$a^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$ and thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

We have completed the proof.

Eventually Euler discovered the law of quadratic reciprocity (figure 1), which was published in 1783[9] by the academy of St. Petersburg, afters Euler's death.

[9] L. Euler, *Observationes circa divisionem quadratorum per numeros primes*, 1783



Concluſio.

§. 39. Quatuor haec Theoremata poſtrema, quorum demonſtratio adhuc deſideratur, ſequenti modo concinnius exhiberi poſſunt:

Exiſtente s numero quocunque primo, diuidantur tantum quadrata imparia 1, 9, 25, 49, *etc. per diuiſorem* 4 s, *notenturque reſidua, quae omnia erunt formae* 4 q + 1, *quorum quiduis littera* a *indicetur, reliquorum autem numerorum, formae* 4 q + 1, *qui inter reſidua non occurrunt, quilibet littera* 𝔄 *indicetur, quo facto ſi fuerit*

diuiſor numerus primus formae	tum eſt
$4ns+a$	$+s$ reſiduum et $-s$ reſiduum
$4ns-a$	$+s$ reſiduum et $-s$ non-reſiduum
$4ns+\mathfrak{A}$	$+s$ non-reſiduum et $-s$ non-reſiduum
$4ns-\mathfrak{A}$	$+s$ non-reſiduum et $-s$ reſiduum.

Figure 1: The law of quadratic reciprocity by Euler[10]

Because Euler did not have the modern notation we have today, including the Legendre symbol, he distinguished four different cases, which together give the full law of quadratic reciprocity. Euler's four statements boil down to the following, where we assume that s is an odd prime:

1. If $p \equiv 1 \mod 4$ is prime and $p \equiv x^2 \mod s$ for some prime s, then there exists a $y \in \mathbb{Z}$ such that $s \equiv y^2 \mod p$ and there exists a $z \in \mathbb{Z}$ such that $-s \equiv z^2 \mod p$

2. If $p \equiv 3 \mod 4$ is prime and $-p \equiv x^2 \mod s$ for some prime s, then there exists a $y \in \mathbb{Z}$ such that $s \equiv y^2 \mod p$, but there is no $z \in \mathbb{Z}$ such that $-s \equiv z^2 \mod p$.

3. If $p \equiv 1 \mod 4$ is prime and $p \not\equiv x^2 \mod s$ for some prime s, then there is no $y \in \mathbb{Z}$ such that $s \equiv y^2 \mod p$ and there is no $z \in \mathbb{Z}$ such that $s \equiv z^2 \mod p$

4. If $p \equiv 3 \mod 4$ is prime and $-p \not\equiv x^2 \mod s$ for some prime s, then there exists a $y \in \mathbb{Z}$ such that $-s \equiv y^2 \mod p$ but there is no $z \in \mathbb{Z}$ such that $s \equiv z^2 \mod p$.

[10] **[6]** E. 552

To discuss the relationship of these four statements with the general law of quadratic reciprocity we first write them by means of Legendre symbols:

1. If $p \equiv 1 \mod 4$ the $\left(\frac{p}{s}\right) = +1 \Longrightarrow \left[\left(\frac{s}{p}\right) = +1 \; and \; \left(\frac{-s}{p}\right) = +1\right]$

2. If $p \equiv 3 \mod 4$ then $\left(\frac{-p}{s}\right) = +1 \Longrightarrow \left[\left(\frac{s}{p}\right) = +1 \; and \; \left(\frac{-s}{p}\right) = -1\right]$

3. If $p \equiv 1 \mod 4$ then $\left(\frac{p}{s}\right) = -1 \Longrightarrow \left[\left(\frac{s}{p}\right) = -1 \; and \; \left(\frac{-s}{p}\right) = -1\right]$

4. If $p \equiv 3 \mod 4$ then $\left(\frac{-p}{s}\right) = -1 \Longrightarrow \left[\left(\frac{s}{p}\right) = -1 \; and \; \left(\frac{-s}{p}\right) = +1\right]$

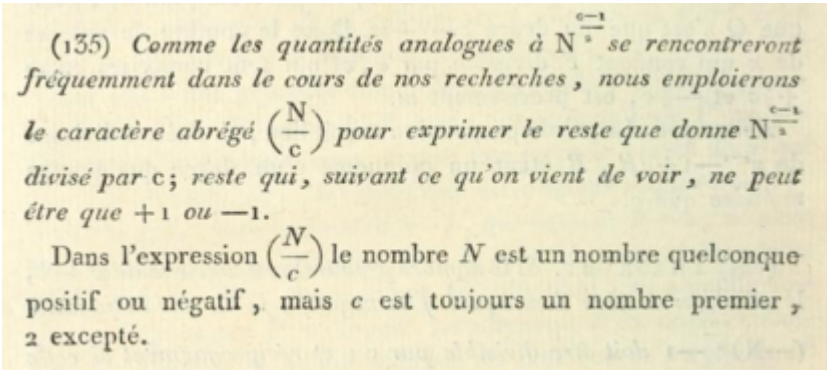
The following two facts were also known to Euler, and discussed in the same paper: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. From these two facts and Euler's four statements we can now immediately conclude the general reciprocity law $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

4 Adrien-Marie Legendre

Legendre[11] (1752-1833) was a French number theorist who studied a lot of discoveries made by Fermat and Euler. Legendre attempted to prove quadratic reciprocity, and in order to do that, he stated in his paper *Recherches d'analyse indéterminée* from 1785, the law of quadratic reciprocity in a very comprehensive way, in which he distinguished eight different cases[12]. Legendre tried to prove all these cases, but did not succeed. In particular because his proofs where based on a theorem, which we now know as Dirichlet's theorem:

Theorem 4.1 (Dirichtlet's theorem) Let a and b be positive integers with $gcd(a, b) = 1$, then there are infinitely many primes p such that $p \equiv a \mod b$

This theorem has the name of Dirichlet because he was the first man to give a proof in 1837.
A couple of years after Legendre successfully stated
the complete law of quadratic reciprocity, he wrote a book, named *Essai sur la theorie des nombres*[13] in which he introduced a new notation (Figure 2) to simplify discussions about quadratic reciprocity; the Legendre symbol.



(135) *Comme les quantités analogues à* $N^{\frac{c-1}{2}}$ *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.

Dans l'expression $\left(\frac{N}{c}\right)$ le nombre N est un nombre quelconque positif ou négatif, mais c est toujours un nombre premier, 2 excepté.

Figure 2: The introduction of the Legendre symbol.

Legendre introduced his symbol $\left(\frac{N}{c}\right)$ as $N^{\frac{c-1}{2}}$ after dividing by c, of which he already showed that it is equal to $+1$ or -1.

[11] **[2]** Article: A. M. Legendre, p. 135-143
[12] A. Legendre, *Recherches d'analyse indéterminée, Histoire de l'Académie*, Paris, 1785
[13] A. Legendre, *Essai sur la theorie des nombres*, Paris, 1798

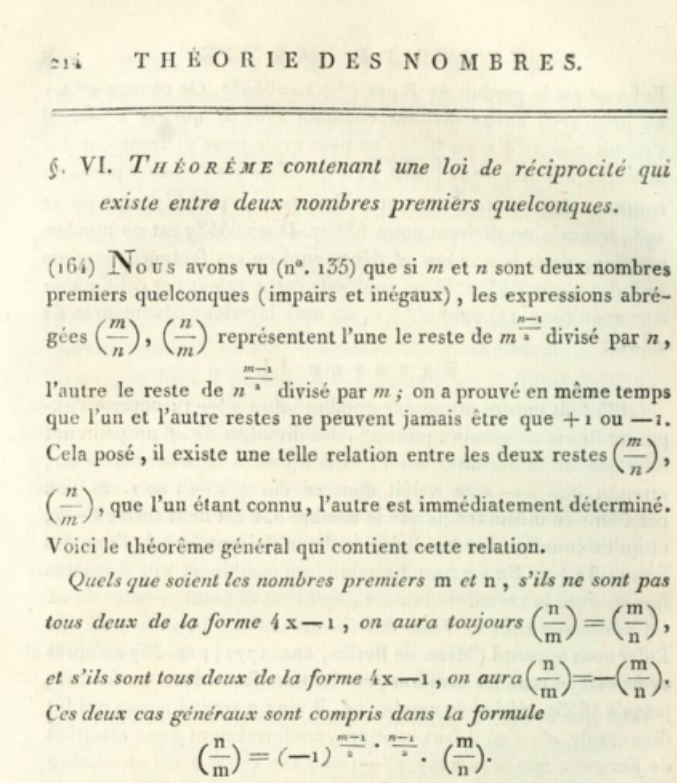
Today we define the Legendre symbol as follows:

Definition 4.1 (Legendre symbol) Let p be a prime number and a an integer not divisible by p. Then

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & if\ a\ is\ a\ quadratic\ residue\ modulo\ p \\ -1 & if\ a\ is\ a\ quadratic\ non-residue\ modulo\ p \end{cases}$$

The Legendre symbol is defined as zero if p divides a.

Legendre stated the law of quadratic reciprocity for the first time in history in its modern form (Figure 3).



214 THÉORIE DES NOMBRES.

§. VI. *Théorème contenant une loi de réciprocité qui existe entre deux nombres premiers quelconques.*

(164) Nous avons vu (n°. 135) que si m et n sont deux nombres premiers quelconques (impairs et inégaux), les expressions abrégées $\left(\frac{m}{n}\right)$, $\left(\frac{n}{m}\right)$ représentent l'une le reste de $m^{\frac{n-1}{2}}$ divisé par n, l'autre le reste de $n^{\frac{m-1}{2}}$ divisé par m; on a prouvé en même temps que l'un et l'autre restes ne peuvent jamais être que $+1$ ou -1. Cela posé, il existe une telle relation entre les deux restes $\left(\frac{m}{n}\right)$, $\left(\frac{n}{m}\right)$, que l'un étant connu, l'autre est immédiatement déterminé. Voici le théorême général qui contient cette relation.

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 tous 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*

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

Figure 3: Legendre's quadratic reciprocity law

If we have two primes m and n, and at least one of them is of the form $4x + 1$, for x an integer, then we have

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$$

If both m and n are of the form $4x - 1$ then we have

$$\left(\frac{n}{m}\right) = -\left(\frac{m}{n}\right)$$

These two general cases are included in the formula

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}$$

The notation that Legendre introduced was very important, it is the same notation we use today. Legendre was again trying to prove this theorem, but he did not succeed. His proof was not complete.

5 Carl Friedrich Gauss

Gauss[14] (1777-1855) was a German mathematician and by many people seen as the greatest mathematician who ever lived. He studied in Göttingen from 1795 until 1798 and it was in this time period that Gauss did some remarkable discoveries. In 1796, at the age of 19, Gauss figured out how to construct a regular heptadecagon (17-gon) using only a compass and a straightedge. In the same year, Gauss gave the complete proof of the law of quadratic reciprocity, which was published in his most famous work *Disquisitiones arithmeticae*[15] in 1801. This book, written in Latin, was a complete overview of the results in number theory discovered in the 17th and 18th century. Gauss also added some of his own important results, including his first proof of the law of quadratic reciprocity, and a second one. Gauss called the law of quadratic reciprocity a 'Fundamental Theorem' and by the time he wrote his *Disquisitiones arithmeticae*, he had already discovered two more proofs. These proofs where not published until 1863 after his death. During his lifetime, Gauss gave a total of eight different proofs.
His first proof is similar to what Legendre was trying to do, by separating eight different cases (Figure 4).

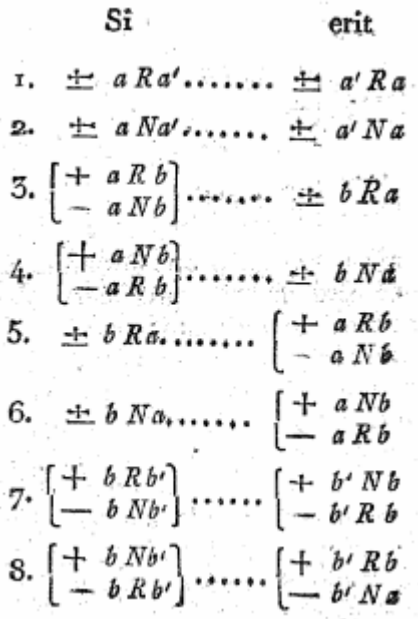


Figure 4: Eight different cases by Gauss[16].

[14] Article: C.F. Gauss, in G. Gillispie, ed. Dictionary of Scientific Biography vol. 5, New York, 1972, p. 298-315
[15] C.-F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801
[16] In latin 'Si' means 'if' and 'erit' means 'will be'

In figure 4, a and a' denote primes of the form $4n+1$ and b and b' denote primes of the form $4n+3$. xRy denotes that x is a quadratic residue of y and xNy denotes that x is not a quadratic residue of y.

For his third and fifth proof Gauss made use of a lemma which he introduced in his work *Theorematis arithmetici demonstratio nova*[17] to prove the law of quadratic reciprocity. We have used an English translation that can be found in *A Source book in mathematics*[18] by David Eugene Smith, for the proof of Gauss' lemma and Gauss' third proof of the quadratic reciprocity law.
We will first look at the lemma Gauss introduced and prove it.
Afterwards we will use this lemma to prove quadratic reciprocity.

Gauss' lemma looks at the remainders modulo p. We can list all these remainders as

$$1, 2, ..., \frac{p-1}{2}, \frac{p+1}{2}, ..., p-1 \mod p$$

where we will call all the remainders smaller then $\frac{p}{2}$ small residues and all the remainders bigger then $\frac{p}{2}$ big residues.

Lemma 5.1 (Gauss' lemma) Let p be an odd prime and a an integer coprime to p. Let u be the number of big residues in $1a, 2a, 3a, ..., \frac{p-1}{2}a$, then

$$\left(\frac{a}{p}\right) = (-1)^u$$

Let us first give an example before we prove this Lemma.
We want to know whether 5 is a quadratic residue modulo 7. We calculate the residues:

$$5 \cdot 1 \equiv 5 \equiv 5 \mod 7$$

$$5 \cdot 2 \equiv 10 \equiv 3 \mod 7$$

$$5 \cdot 3 \equiv 15 \equiv 1 \mod 7$$

We can count the residues that are bigger then $\frac{7}{2} = 3.5$, namely one.
So we know that $u = 1$ and

$$\left(\frac{5}{7}\right) = (-1)^1 = -1$$

[17] C.F. Gauss, *Theorematis arithmetici demonstratio nova*, Comment. Soc. regiae sci. Göttingen XVI (1808)
[18] D.E. Smith, *A source book in mathematics*, page 112-118, New York, 1929

We conclude that 5 is not a quadratic residue modulo 7.

We will give Gauss' proof but our notation will be adapted to that of Shoup.[19].

Proof of Gauss' lemma We have two types of residues; the small ones $\{1, 2, ..., \frac{p-1}{2}\}$ and the big ones $\{\frac{p+1}{2}, ..., p-1\}$. Note that we can write the big residues as $\{-1, -2, ..., -\frac{p-1}{2}\}$.Thus we can write all the residues as $\{\pm 1, \pm 2, ..., \pm\frac{p-1}{2}\}$. All these residues are different and if we multiply them by a they are still different. In fact, all the residues $\{\pm 1a, \pm 2a, ..., \pm\frac{p-1}{2}a\}$ are a rearrangement of $\{1, 2, ..., p-1\}$. This means that for all the values $\pm 1, \pm 2, ..., \pm\frac{p-1}{2} \mod p$ exactly half of them are a rearrangement of $1a, 2a, ..., \frac{p-1}{2}a \mod p$ and if $+s \in \{1a, 2a, ..., \frac{p-1}{2}a\}$, then $-s \notin \{1a, 2a, ..., \frac{p-1}{2}a\}$[20]. Now look at the product

$$A = a \cdot 2a \cdots \frac{p-1}{2}a = a^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

By our rearrangement we have found that

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

where u counts the big residues, because the number of big residues $\{-1, -2, ..., -\frac{p-1}{2}\}$ decides whether the sign will be positive or negative. We can now divide both sides by $\left(\frac{p-1}{2}\right)!$ to get

$$a^{\frac{p-1}{2}} = (-1)^u$$

Euler's criterion completes the proof.

[19]V.Shoup, *A Computational Introduction to Number Theory and Algebra,* New York, 2008, p.344

[20]This follows from $-s \equiv (p-s) \mod p$

5.1 Gauss' Third Proof

Gauss gave a total of eight proofs during his life. We will give Gauss' third proof that first appeared in his article[21], because it is considered by Gauss himself and many others to be the most elegant proof of all eight.
We have tried to make Gauss third proof better understandable then earlier published versions.

Gauss' third proof is based on Gauss' lemma which we just proved. Let us take a closer look at u, the number of big residues.
Take a prime number p and an integer a. Let r_i be the remainder such that $r_i \equiv ia \mod p$ for $i = 1, 2, ..., \frac{p-1}{2}$. Gauss introduced a new notation for u, which we would write in modern notation as:

$$u = (a, p) = \#\left\{ i \mid r_i > \frac{p-1}{2} \right\}$$

In Gauss' third proof, he made use of the floor function. The floor $\lfloor \frac{x}{y} \rfloor$ is defined as the smallest integer $\leq \frac{x}{y}$. For example, the floor of $\frac{7}{3}$ is 2.
Gauss used $[x]$ to refer to the floor function, but we will use the modern notation $\lfloor x \rfloor$ instead to avoid confusion.

We are starting with some properties of the floor function, where $x \in \mathbb{Q}$ but not an integer.

i. $\lfloor x \rfloor + \lfloor -x \rfloor = -1$. Note that this equals 0 if x is an integer.

ii. $\lfloor x \rfloor + h = \lfloor x + h \rfloor$. for h an integer

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

iv. If $x - \lfloor x \rfloor < \frac{1}{2}$ then $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 0$
and if $x - \lfloor x \rfloor \geq \frac{1}{2}$ then $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 1$.

v. Let $z \in \mathbb{Z}$ and $0 < r < p$ such that $z \equiv r \mod p$. If $r < \frac{p}{2}$ then $\lfloor \frac{2z}{p} \rfloor - 2\lfloor \frac{z}{p} \rfloor = 0$ and if $r \geq \frac{p}{2}$ then $\lfloor \frac{2z}{p} \rfloor - 2\lfloor \frac{z}{p} \rfloor = 1$.

vi. By v. and the definition of (a, p) we can write (a, p) as

$$(a,p) = \left(\lfloor \tfrac{2a}{p} \rfloor - 2\lfloor \tfrac{a}{p} \rfloor \right) + \left(\lfloor \tfrac{4a}{p} \rfloor - 2\lfloor \tfrac{2a}{p} \rfloor \right) + ... + \left(\lfloor \tfrac{2\left(\frac{p-1}{2}\right)a}{p} \rfloor - 2\lfloor \tfrac{\left(\frac{p-1}{2}\right)a}{p} \rfloor \right)$$

so

$$(a,p) = \lfloor \tfrac{2a}{p} \rfloor + \lfloor \tfrac{4a}{p} \rfloor + ... + \lfloor \tfrac{2\left(\frac{p-1}{2}\right)a}{p} \rfloor - 2\left(\lfloor \tfrac{a}{p} \rfloor + \lfloor \tfrac{2a}{p} \rfloor + ... + \lfloor \tfrac{\left(\frac{p-1}{2}\right)a}{p} \rfloor \right)$$

vii. Since (a, p) counts the big residues in $1a, 2a, 3a, ..., \frac{p-1}{2}a$ and $(-a, p)$ counts the big residues in $-1a, -2a, -3a, ..., -\frac{p-1}{2}a$, which modulo p is equal to $(p-1)a, (p-2)a, ..., \frac{p+1}{2}a$, we know that all the big residues are included

[21] **[16]** p. 71-74

in (a,p) and $(-a,p)$. Thus

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

Which we expected because of theorem 3.1.

Let us distinguish two different cases:

If $p\equiv 1 \mod 4$ then $(a,p)+(-a,p)=\frac{(4n+1)-1}{2}=2n$. Which means that (a,p) and $(-a,p)$ are both even or both odd. In Legendre symbols this is translated to $\left(\frac{-a}{p}\right)=\left(\frac{a}{p}\right)$.

If $p\equiv 3 \mod 4$ then $(a,p)+(-a,p)=\frac{(4n+3)-1}{2}=2n+1$. Which means that either (a,p) or $(-a,p)$ is even and the other is odd. In Legendre symbols this is translated to $\left(\frac{-a}{p}\right)=-\left(\frac{a}{p}\right)$.

If we take $a=1$, then $(1,p)=0$, because all $1\cdot 1, 1\cdot 2, ..., 1\cdot\frac{p-1}{2}$ are smaller then $\frac{p}{2}$, and because $\left(\frac{1}{p}\right)=1$ it follows that

$$\left(\frac{-1}{p}\right)=\begin{cases}+1 & if\ p=1 \mod 4\\ -1 & if\ p=3 \mod 4\end{cases}$$

which is the the first supplementary law of quadratic reciprocity.

viii. By iii we have

$$\lfloor\frac{ik}{p}\rfloor+\lfloor k-\frac{ik}{p}\rfloor=k-1$$

and

$$\lfloor\frac{(p-i)k}{p}\rfloor=\lfloor k-\frac{ik}{p}\rfloor=k-1-\lfloor\frac{ik}{p}\rfloor$$

Look at the first part of (a,p), which is $A=\lfloor\frac{2a}{p}\rfloor+\lfloor\frac{4a}{p}\rfloor+...+\lfloor\frac{2\left(\frac{p-1}{2}\right)a}{p}\rfloor$ and assume that $p\equiv 1 \mod 4$. Because $p-1$ is divisible by 4, we can replace the last $\frac{p-1}{4}$ terms of A to get

$$A=\lfloor\tfrac{2a}{p}\rfloor+\lfloor\tfrac{4a}{p}\rfloor+...+\lfloor\tfrac{\left(\frac{p-1}{2}\right)a}{p}\rfloor+\left((a-1)-\lfloor\tfrac{\left(\frac{p-3}{2}\right)a}{p}\rfloor\right)+$$
$$\left((a-1)-\lfloor\tfrac{\left(\frac{p-7}{2}\right)a}{p}\rfloor\right)+...+\left((a-1)-\lfloor\tfrac{3a}{p}\rfloor\right)+\left((a-1)-\lfloor\tfrac{a}{p}\rfloor\right)$$

or

$$A=\left(\sum_{i=1}^{\frac{p-1}{4}}\lfloor\frac{2ia}{p}\rfloor\right)+\frac{p-1}{4}(a-1)-\left(\sum_{i=1}^{\frac{p-1}{4}}\lfloor\frac{(2i-1)a}{p}\rfloor\right)$$

The second part of (a,p) is equal to $-2\left(\lfloor\frac{a}{p}\rfloor+\lfloor\frac{2a}{p}\rfloor+...+\lfloor\frac{\left(\frac{p-1}{2}\right)a}{p}\rfloor\right)$,

which together with A gives us the following expression.

$$(a,p) = \left(\sum_{i=1}^{\frac{p-1}{4}} \lfloor \frac{2ia}{p} \rfloor\right) + \frac{p-1}{4}(a-1) - \left(\sum_{i=1}^{\frac{p-1}{4}} \lfloor \frac{(2i-1)a}{p} \rfloor\right) - 2\left(\sum_{j=1}^{\frac{p-1}{2}} \frac{ja}{p}\right)$$

We assumed that $p \equiv 1 \mod 4$. But what if $p \equiv 3 \mod 4$? This is similar but we will replace the last $\frac{p+1}{2}$ terms of A to get the expression

$$(a,p) = \left(\sum_{i=1}^{\frac{p+1}{4}} \lfloor \frac{2ia}{p} \rfloor\right) + \frac{p+1}{4}(a-1) - \left(\sum_{i=1}^{\frac{p+1}{4}} \lfloor \frac{(2i-1)a}{p} \rfloor\right) - 2\left(\sum_{j=1}^{\frac{p-1}{2}} \frac{ja}{p}\right)$$

The case where $a = 2$ gives us the second supplementary law of quadratic reciprocity.

We are now almost ready to prove the law of quadratic reciprocity. We just need one more theorem.

Theorem 5.1.1 Let k and s be coprime positive odd numbers. Then:

$$\lfloor \frac{k}{s} \rfloor + \lfloor \frac{2k}{s} \rfloor + ... + \lfloor \frac{\frac{s-1}{2}k}{s} \rfloor + \lfloor \frac{s}{k} \rfloor + \lfloor \frac{2s}{k} \rfloor + ... + \lfloor \frac{\frac{k-1}{2}s}{k} \rfloor = \frac{(k-1)(s-1)}{4}$$

We will not give Gauss' algebraic proof of this theorem because we think that this proof is not very illuminating. An insightful geometric proof of the theorem can be found in *An introduction to the theory of numbers* by G.H.Hardy and E.M.Wright.[22]

Remember that we want to prove that for p and q two different primes

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

Take two numbers M and N defined as follows

$$M = (q,p) + \lfloor \frac{q}{p} \rfloor + \lfloor \frac{2q}{p} \rfloor + ... + \lfloor \frac{\frac{p-1}{2}q}{p} \rfloor$$
$$N = (p,q) + \lfloor \frac{p}{q} \rfloor + \lfloor \frac{2p}{q} \rfloor + ... + \lfloor \frac{\frac{q-1}{2}p}{q} \rfloor$$

From viii. we know that M and N are both even numbers, because (a,b) and $\lfloor \frac{a}{b} \rfloor + \lfloor \frac{2a}{b} \rfloor + ... + \lfloor \frac{\frac{b-1}{2}a}{b} \rfloor$ will always have the same sign for $a = p, q$ and $b = q, p$. That means $M + N$ will be even as well.

[22] G.H.Hardy and E.M.Wright, *An introduction to the theory of numbers,* fifth edition, Oxford, p 76

From theorem 5.1.1 we see that

$$M + N = (q, p) + (p, q) + \frac{(p-1)(q-1)}{4}$$

if $\frac{(p-1)(q-1)}{4}$ is even, (q, p) and (p, q) both need to be even or both need to be odd. Which gives us $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.
However, if $\frac{(p-1)(q-1)}{4}$ is odd, then one of (q, p) and (p, q) need to be even and the other odd. Which gives us $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. This gives us the following formula

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

This is exactly the quadratic reciprocity law and we completed the proof.

5.2 Jacobi and Gauss

Carl Gustav Jacob Jacobi introduced a new notation in his *Über die Kreisteilung und ihre Anwendung auf Zahlentheorie*[23] from1837, which is known as the Jacobi symbol. The Jacobi symbol is a generalization of the Legendre symbol and is defined as follows:

Definition (Jacobi symbol) Let n be an odd integer with prime factorization $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $m \in \mathbb{Z}$, such that $gcd(m, n) = 1$, then the Jacobi symbol $\left(\frac{m}{n}\right)$ is defined as

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{a_1} \left(\frac{m}{p_2}\right)^{a_2} \cdots \left(\frac{m}{p_r}\right)^{a_r} = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)^{a_i}$$

Where $\left(\frac{m}{p_i}\right)$ are Legendre symbols.

The important difference between the Legendre and Jacobi symbol is that in the Legendre symbol, the bottom number has to be prime, and in the Jacobi symbol it can be any odd number. If in the Jacobi symbol the bottom number is prime, then the Legendre and Jacobi symbols are equal.

Another difference between the two symbols can be found by looking at Euler's criterion.We have seen that we can write the Legendre symbol as $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \, mod \, p$, but what happens if we try to do this with the Jacobi symbol? Let us take a look at the following examples, where $\left(\frac{m}{n}\right)$ is the Jacobi symbol[24]:

i. $\left(\frac{19}{45}\right) = 1$ and $19^{\frac{45-1}{2}} \equiv 1 \mod 45$
ii. $\left(\frac{8}{21}\right) = -1$ but $8^{\frac{21-1}{2}} \equiv 1 \mod 21$
iii. $\left(\frac{7}{15}\right) = 1$ but $7^{\frac{15-1}{2}} \equiv 13 \mod 15$

We see that in some cases the Jacobi symbol is equal to what we would expect from Euler's criterion. But we also see that in other cases Euler's criterion does not even give us an answer equal to ± 1.

In Gauss' first proof, published in his *Disquisitiones Arithmeticae,* Gauss supposed that the quadratic reciprocity law is true until a certain prime number, and proved that it is still true for the next prime. But during his work, he figured out that if the law of quadratic reciprocity is true until a certain prime, then it is also true for all pairs of odd integers less then the next prime. Gauss ended up with a more general proof for odd prime numbers, where he used the Jacobi symbol.

[23] C.G.J. Jacobi, *Über die Kreisteilung und ihre Anwendung auf Zahlentheorie*, Berlin, 1837
[24] A tool to easy calculate the Jacobi symbol: http://math.fau.edu/richman/jacobi.htm

Theorem 5.2.1 (Quadratic reciprocity law for the Jacobi symbol) Let n and m be positive odd integers, with $gcd(m, n) = 1$, then

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

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

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

We will not prove this theorem because it is not necessary for our purpose.

5.3 A proof based on Gauss sums

The fourth and sixth proof that Gauss gave are based on what is now called Gauss sums. In his study to the equation $x^p - 1 = 0$, he invented these sums. In his article *Summatio quarumdam serierum singularium,* Gauss studied the sums:

$$G(k,p) = \sum_a (cos(ak\omega) + isin(ak\omega)) - \sum_b (cos(bk\omega) + isin(bk\omega))$$

Where p is an odd prime, k is an integer coprime to p, a denote the quadratic residues and b denote the and quadratic nonresidues in the set $1, 2, ..., p-1$, and $\omega = \frac{2\pi}{p}$. The goal of this article was not to prove the law of quadratic reciprocity, but to compute the sum. After the study of these sums, Gauss noticed that a new proof of the quadratic reciprocity law could be made. The sums are now called Gauss sums, and in modern notation we can write them as

$$G = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^j$$

Where $\left(\frac{j}{p}\right)$ is the Legendre symbol and $\zeta = e^{\frac{2\pi i}{p}}$ is the p-th root of unity[25], for which we know that $\zeta^p = e^{2\pi i} = 1$. Remember that $e^{ix} = \cos(x) + i\sin(x)$ and $\zeta^j = \zeta^k$ if $j \equiv k \mod p$.

The proof that we will give is inspired by Gauss' fourth and sixth proof of the quadratic reciprocity laws. However, we have changed the arguments where Gauss uses equations into arguments by means of p-th roots, following Legendre (in the third version of his Theorie des Nombres[26]) and Eisenstein, as explained in the translation by E. Netto[27]. As a result, our presentation resembles that in *Proofs from the Book*[28], but we have avoided all references to finite fields in order to make the proof better intelligible to readers who do not know field theory.

We see in the Gauss sum G, that for a quadratic residue a modulo p, the sign of ζ will be positive, and for a quadratic non-residue b the sign will be negative. So we can write G as follows:

$$G = \sum_{x^2 \equiv a \mod p} \zeta^a - \sum_{x^2 \not\equiv b \mod p} \zeta^b = X_a - X_b$$

[25] A n-th root of unity, where n is an integer, is a number $z \in \mathbb{C}$ that satisfies the equation $z^n = 1$.

[26] Third version of **[14],** Paris, 1830, p. 391

[27] E. Netto, *Sechs beweise des fundamentaltheorems über quadratische reste von Carl Friedrich Gauss,* Leipzig, 1901

[28] M. Aigner, G.M. Ziegler, *Proofs from the Book*, Berlin, 1998, p. 25-31

Let us call the first sum X_a and the second sum X_b.
In order to prove the law of quadratic reciprocity with these sums, we want to find expressions for G^2 and G^{q-1} for a prime number q. We will first find these expressions and afterwards show how to use these expressions to proof quadratic reciprocity.

Let us start with G^2.
We can write this as $G^2 = (X_a - X_b)^2 = (X_a + X_b)^2 - 4X_aX_b$. In order to calculate G^2, we want to know how to calculate $X_a + X_b$ and X_aX_b. We will start with $X_a + X_b$. Since

$$X_a + X_b = \sum_{x^2 \equiv a \mod p} \zeta^a + \sum_{x^2 \not\equiv b \mod p} \zeta^b = \sum_{n \mod p \neq 0} \zeta^n$$

We want an expression for $\sum \zeta^n$.
We have already mentioned that Gauss studied the equation $x^p - 1$, and we will do the same. We know that all the roots of this equation are $x = 1$ and $x = \zeta^k = e^{\frac{2\pi i}{p}k}$ for $k = 1, 2, ..., p-1$. This means that we can factorize $x^p - 1$ as

$$x^p - 1 = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1})$$

and if we eliminate the brackets we find

$$x^p - 1 = x^p + x^{p-1}\left(-1 - \zeta - \zeta^2 - ... - \zeta^{p-1}\right) + ... + (-1)$$

(The last term is equal to (-1) because

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

From this equality it follows that, $-1 - \zeta - \zeta^2 - ... - \zeta^{p-1} = 0$. Which means that

$$\sum_{n \mod p \neq 0} \zeta^n = -1$$

And we conclude that $X_a + X_b = -1$

We will now look at X_aX_b. In order to do this we will introduce a theorem.

Theorem 5.3.1 if p is an odd prime, then there are numbers g such that $1, g, g^2..., g^{p-2}$ are incongruent modulo p.

We will not prove this theorem here, it was of course known to Gauss, but refer to a beautiful proof that can be found in the book *An introduction to the theory of numbers.***[21]**

Let say that we have a $g$as in theorem 5.3.1. We know that the quadratic residues modulo p are $\left\{g^0, g^2, g^4, ..., g^{p-3}\right\}$ and the quadratic non-residues

are $\left\{g^1, g^3, ..., g^{p-2}\right\}$. Note that these two sets both have $\frac{p-1}{2}$ elements. We can now write X_a and X_b in the following way

$$X_a = \sum_{x^2 \equiv a \mod p} \zeta^a = \zeta^{g^0} + \zeta^{g^2} + \zeta^{g^4} + ... + \zeta^{g^{p-3}}$$

$$X_b = \sum_{x^2 \not\equiv b \mod p} \zeta^b = \zeta^{g^1} + \zeta^{g^3} + \zeta^{g^5} + ... + \zeta^{g^{p-2}}$$

We want an expression for $X_a X_b$, and to get one, we will just multiply the sums of X_a and X_b in a smart way:

$$\begin{aligned} X_a X_b = &\left(\zeta^{g^0} + \zeta^{g^2} + \zeta^{g^4} + ... + \zeta^{g^{p-3}}\right)\left(\zeta^{g^1} + \zeta^{g^3} + \zeta^{g^5} + ... + \zeta^{g^{p-2}}\right) \\ &= \zeta^{g^0+g^1} + \zeta^{g^2+g^3} + \zeta^{g^4+g^5} + ... + \zeta^{g^{p-3}+g^{p-2}} \\ &+\zeta^{g^0+g^3} + \zeta^{g^2+g^5} + \zeta^{g^4+g^7} + ... + \zeta^{g^{p-3}+g^1} \\ &+\zeta^{g^0+g^5} + \zeta^{g^2+g^7} + \zeta^{g^4+g^9} + ... + \zeta^{g^{p-3}+g^3} \\ &\qquad\qquad\qquad\qquad\quad . \\ &\qquad\qquad\qquad\qquad\quad . \\ &\qquad\qquad\qquad\qquad\quad . \\ &+\zeta^{g^0+g^{p-2}} + \zeta^{g^2+g^1} + \zeta^{g^4+g^3} + ... + \zeta^{g^{p-3}+g^{p-4}} \end{aligned}$$

We can also write these expressions as

$$\begin{aligned} X_a X_b = &\zeta^{1+g^1} + \zeta^{g^2(1+g)} + \zeta^{g^4(1+g)} + ... + \zeta^{g^{p-3}(1+g)} \\ &+\zeta^{1+g^3} + \zeta^{g^2(1+g^3)} + \zeta^{g^4(1+g^3)} + ... + \zeta^{g^{p-3}(1+g^3)} \\ &+\zeta^{1+g^5} + \zeta^{g^2(1+g^5)} + \zeta^{g^4(1+g^5)} + ... + \zeta^{g^{p-3}(1+g^5)} \\ &\qquad\qquad\qquad\qquad\quad . \\ &\qquad\qquad\qquad\qquad\quad . \\ &\qquad\qquad\qquad\qquad\quad . \\ &+\zeta^{1+g^{p-2}} + \zeta^{g^2(1+g^{p-2})} + \zeta^{g^4(1+g^{p-2})} + ... + \zeta^{g^{p-3}(1+g^{p-2})} \end{aligned}$$

Let us first assume that $1+g$ is a quadratic residue modulo p. Then the first row consists of all quadratic residues and is equal to
$\zeta + \zeta^{g^2} + \zeta^{g^4} + ... + \zeta^{g^{p-3}} = X_a$. And because $1+g$ is a quadratic residue, if we look at the last row, $1 + g^{p-2} = g^{-1}\left(g + g^{p-1}\right) = g^{-1}(g+1)$[29] is not a quadratic residue. The last row consists of all quadratic non-residues and is equal to $\zeta^{g^1} + \zeta^{g^3} + \zeta^{g^5} + ... + \zeta^{g^{p-2}} = X_b$.

However, if $1+g$ is not a quadratic residue modulo p, in the same way we can show that the first row is equal to X_b and the last row equal to X_a. The same holds for the second and second last rows, third and third last row etc. We have already seen that $X_a + X_b = -1$, so all pairs of rows will add up to -1. Now there are two different cases, there is an even number

[29] By Fermat's little theorem $g^{p-1} \equiv 1 \mod p$

of rows or an odd number of rows. There is a total of $\frac{p-1}{2}$ rows; there is an even number of rows if $p \equiv 1 \mod 4$ and there is an odd number of rows if $p \equiv 3 \mod 4$.

Case 1:
If there is an even number of rows, we are quickly done because $X_a X_b = \frac{1}{2}\frac{p-1}{2}(-1) = -\frac{p-1}{4}$. Remember that $X_a + X_b = -1$. If we go back to our equation $G^2 = (X_a + X_b)^2 - 4X_aX_b$ we find

$$G^2 = (-1)^2 - 4\left(-\frac{p-1}{4}\right) = 1 + p - 1 = p$$

We conclude that if $p \equiv 1 \mod 4$, then $G^2 = p$.

Case 2
If there is an odd number of rows, we know that there will be $\frac{p-3}{4}$ pairs formed. We have to look at the middle row that does not form a pair. Let us call the middle row x_m. Then we know that $X_aX_b = -\frac{p-3}{4} + x_m$
We know that x_m is equal to

$$x_m = \zeta^{1+g^{\frac{p-1}{2}}} + \zeta^{g^2(1+g^{\frac{p-1}{2}})} + \zeta^{g^4(1+g^{\frac{p-1}{2}})} + ... + \zeta^{g^{p-3}(1+g^{\frac{p-1}{2}})}$$

Because $1 + g^{\frac{p-1}{2}} \equiv 0 \mod p$, we can write all powers of x_m as a multiple of p, for example sp. Thus $x_m = \zeta^{sp} + \zeta^{sp} + ... + \zeta^{sp} = \frac{p-1}{2}\zeta^{sp}$. We also know that

$$\zeta^{sp} = \left(e^{\frac{2\pi i}{p}}\right)^{sp} = \left(e^{2\pi i}\right)^s = 1^s = 1$$

Thus $x_m = \frac{p-1}{2}$ and $X_aX_b = -\frac{p-3}{4} + \frac{p-1}{2} = -\frac{p-3}{4} + \frac{2p-2}{4} = \frac{p+1}{4}$. We can again look at $G^2 = (X_a + X_b)^2 - 4X_aX_b$ and we find

$$G^2 = (-1)^2 - 4\left(\frac{p+1}{4}\right) = 1 - p - 1 = -p$$

We conclude that if $p \equiv 3 \mod p$, then $G^2 = -p$.

If we take the cases 1 and 2 together we find $G^2 = (-1)^{\frac{p-1}{2}}p$.

In order to complete the proof, we also need an expression for G^{q-1} where q is an odd prime number and not equal to p.

Let us first look at $(a+b)^q$, where a and b are integers and q is a prime number. We know that this is equal to

$$(a+b)^q = a^q + b^q + \binom{q}{1}a^{q-1}b + \binom{q}{2}a^{q-2}b^2 + ... + \binom{q}{q-1}ab^{q-1}$$

Where $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ is the binomial coefficient for $0 \leq m \leq n$. Since q is prime, it will divide all $\binom{q}{i}$ for $i = 1, 2, ..., q-1$ and we will denote $(a+b)^q$ as

$$(a+b)^q = a^q + b^q + q\sum_i a_i a b^i$$

Where a_i are all integers coming from dividing the the binomial coefficients by q.

We can do the same with our Gauss sum

$$G^q = \left(\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\zeta^j\right)^q = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)^q\zeta^{jq} + q\sum_j a_j\zeta^j$$

Let us first concentrate on the first sum in this equation. Since q is a prime number, the sign of the Legendre symbol $\left(\frac{j}{p}\right)$ will not change. Therefore

$$\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)^q\zeta^{jq} = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\zeta^{jq}$$

By a little trick, the Legendre symbol is equivalent to
$\left(\frac{j}{p}\right) = \left(\frac{q^2}{p}\right)\left(\frac{j}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{jq}{p}\right)$, which gives us

$$\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\zeta^{jq} = \left(\frac{q}{p}\right)\sum_{j=1}^{p-1}\left(\frac{jq}{p}\right)\zeta^{jq}$$

Now we realize that jq runs with j through all nonzero residues $\mod p$. Thus $\sum_{j=1}^{p-1}\left(\frac{jq}{p}\right)\zeta^{jq} = G$ and we find an expression for G^q, namely

$$G^q = \left(\frac{q}{p}\right)G + q\sum_j a_j\zeta^j$$

If we divide both sides by G, we have found our expression for G^{q-1}

$$G^{q-1} = \left(\frac{q}{p}\right) + \frac{q}{G}\sum_j a_j\zeta^j$$

The proof of the law of quadratic reciprocity follows from an other very easy to find expression of G^{q-1} with the help of G^2.

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

The last expression follows from Euler's criterion.

We have found two expressions for G^{p-1} and if we set them equal we find

$$\left(\frac{q}{p}\right) + \frac{q}{G}\sum_j a_j \zeta^j = p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

If we put $T = \sum_j a_j \zeta^j$ it follows from the identity which we have just proved that $\frac{T}{G}$ is a rational number. Now put $k = p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} - \left(\frac{q}{p}\right)$, then k is an integer and $q\frac{T}{G} = k$, so $q^2\frac{T^2}{G^2} = k^2$. Since $G^2 = \pm p$, as we proved above, it follows that T^2 is a rational number. Because $T^2 = \sum_j b^j \zeta^j$ for integers b, and because T^2 is a rational number, we can easily show that T^2 is an integer.

[The argument depends on the irreducibility of the polynomial $1 + x + x^2 + .. + x^p = 0$ of which all the ζ^j are the roots; we will not give the details here.]

So $\frac{T^2}{G^2} = \frac{m}{p}$ for an integer number m. Then $q^2\frac{m}{p} = k^2$ so $q^2 m = k^2 p$. Since p does not divide q, p must divide m. Therefore $\frac{T^2}{G^2}$ is an integer, and since $\frac{T}{G}$ is rational, it must be an integer as well, say $\frac{T}{G} = n$.

We conclude $qn = p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} - \left(\frac{q}{p}\right)$ and by taking the remainders modulo q, we conclude $0 \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} - \left(\frac{q}{p}\right) \mod q$. Because both terms can only be $+1$ and -1, the law of quadratic reciprocity follows

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

We have completed the proof.

6 After Gauss

After the time Gauss gave his first six proofs of the quadratic reciprocity law, a lot of other mathematicians came up with different proofs. By the time Gauss' seventh and eight proof where published in 1863, the number of different proofs was already raised to 31. Five of were them done by Eisenstein, but also Dirichlet, Cauchy and Dedekind gave different proofs. During the years, mathematics has developed and new techniques were born, this leads to more different proofs of the quadratic reciprocity law and nowadays there are as many as 246 different proofs. The German mathematician Franz Lemmermeyer keeps a list of all different proofs.[30] Of course the question is whether all these proofs are really different, because some proofs are very lookalike.

The importance of Gauss' work can be seen by looking at the different proofs that were found after Gauss. Not only did he give eight different proofs himself, he has also led other mathematicians to find different proofs based on his work. A lot of proofs are based on Gauss' lemma and other proofs made use of Gauss sums.

The last proof of the quadratic reciprocity law was given in 2013, but since the beginning of the new century, already 30 new proofs appeared. We probably will not have to wait long for a new proof to appear, and maybe the discovery of new proofs will never stop.

[30] http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

References

[1] R.A.Adams, C. Essex, *Calculus, a complete source*, Toronto, 2003
[2] G. Gillispie, ed. Dictionary of Scientific Biography vol. 4, New York, 1971
[3] G. Gillispie, ed. Dictionary of Scientific Biography vol. 5, New York, 1972
[4] V.J. Katz, *A history of mathematics, An introduction*
[5] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Cambridge, 1995
[6] Commentarii academiae scientiarum Petropolitanae 8, St. Petersburg, 1741, pp. 141-146
[7] A. Adler, J.E. Coury, *The Theory of numbers, a text and source book of problems,* London, 1995
[8] V.Shoup, *A Computational Introduction to Number Theory and Algebra,* New York, 2008
[9] L. Euler, *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio*, St. Petersburg, 1736
[10] L. Euler, *Observationes circa divisionem quadratorum per numeros primes*, 1783.
[11] D.J. Struik, *Geschiedenis van de wiskunde,* Utrecht, 1965
[12] F. Lemmermeyer, *Recipiprocity Laws, from Euler to Eisenstein*, New York, 2000
[13] A. Legendre, *Recherches d'analyse indéterminée, Histoire de l'Académie*, Paris, 1785
[14] A. Legendre, *Essai sur la theorie des nombres*, Paris, 1798
[15] C.F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801
[16] C.F. Gauss, *Theorematis arithmetici demonstratio nova*, Comment. Soc. regiae sci. Göttingen XVI (1808)
[17] D.E. Smith, *A source book in mathematics*, New York, 1929
[18] C.G.J. Jacobi, *Über die Kreisteilung und ihre Anwendung auf Zahlentheorie*, Berlin, 1837
[19] M. Aigner, G.M. Ziegler, *Proofs from the Book*, Berlin, 1998
[20] W. Engelmann*, Sechs beweise des fundamentaltheorems über quadratische reste von Carl Friedrich Gauss,* Leipzig, 1901
[21] G.H.Hardy and E.M.Wright, *An introduction to the theory of numbers,* fifth edition, Oxford, 1979