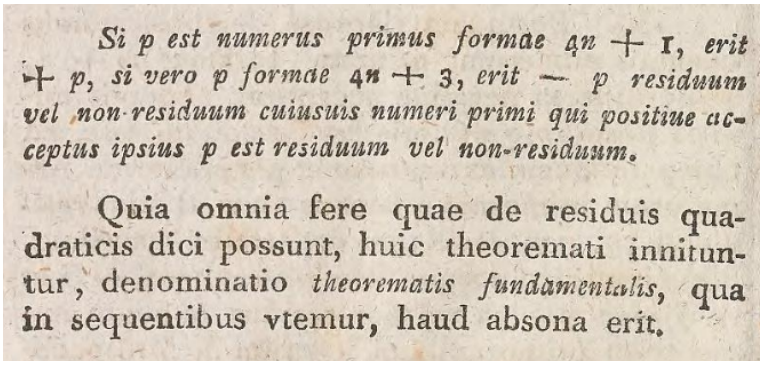
THE LAW OF QUADRATIC RECIPROCITY

NIELS KETELAARS

1. Introduction

The law of quadratic reciprocity is one of the most famous and important results from number theory. Known already to mathematicians like Euler and Legendre, it wasn't until the start of the 19th century when Gauss gave the first (complete) proof, who called it his *theorematis fundamentalis* (see also Figure 1). Near the end of the 19th century, many more proofs were known, and a large part of algebraic number theory was concerned with finding generalizations, to gain a deeper understanding of the theorem. Below we first give a short historical outline and motivation, after which we will give a proof based on one of Gauss's proofs. Finally we will discuss the theorem in the context of modern algebraic numebr theory, and mention a few generalizations.



Si p est numerus primus formae 4n + 1, erit + p, si vero p formae 4n + 3, erit — p residuum vel non-residuum cuiusuis numeri primi qui positiue acceptus ipsius p est residuum vel non-residuum.

Quia omnia fere quae de residuis quadraticis dici possunt, huic theoremati innituntur, denominatio *theorematis fundamentalis*, qua in sequentibus vtemur, haud absona erit.

FIGURE 1. Gauss's original formulation[1]from [Gau01].

2. Fermat, Euler and Legendre

This section is largely based on the first few chapters of David Cox's book [Cox13]. For proofs of the claims in this sections and additional information we point the reader to this book.

The history of quadratic reciprocity begins with a famous result of Fermat, that seems unrelated at first.

[1] "If p is a prime number of the form $4n + 1$, then p, or if p is of the form $4n + 3$, then $-p$, will be a residue, respectively a non-residue, of those primes, that are, when positive, a residue, respectively a non-residue of p itself."

Theorem 2.1 (Fermat)**.** *Let p be an odd prime. Then there exist integers x, y with $p = x^2 + y^2$ if and only is $p \equiv 1 \bmod 4$.*

It is fairly unexpected that the primes which can be written as a sum of squares can be characterized by their residue class modulo 4. A natural generalization is to consider for fixed $n \in \mathbf{Z}$, which primes can be written as $x^2 + ny^2$, and in particular we wonder if these primes can again be characterized by their residue class modulo some fixed number. This question was examined by Fermat and Euler among others. Euler quickly realized Fermat's original theorem had to do with the fact that -1 is a square in $\mathbf{Z}/p\mathbf{Z}$ if and only if $p \equiv 1 \bmod 4$. For our more general problem, is is therefore natural to consider for which primes we have that $-n$ is a square modulo p. This was Euler's motivation to study squares in $\mathbf{Z}/p\mathbf{Z}$, and it is how he eventually stumbled across the law of quadratic reciprocity. He noticed that for two odd primes p and q, there was a relation between whether p is a square modulo q, and whether q is a square modulo p. Before we state the theorem in full, we need some notation due to Legendre.

Definition 2.2. For $t \in \mathbf{Z}$ and p an odd prime, the *Legendre symbol* is

$$\left(\frac{t}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } p|t, \\ 1 & \text{if } p \nmid t \text{ and } t \text{ is a square mod } p, \\ -1 & \text{if } p \nmid t \text{ and } t \text{ is not a square mod } p. \end{cases}$$

Before we continue we note some nice properties of the Legendre symbol.

Proposition 2.3. *For $a, b \in \mathbf{Z}$, we have that*

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
(2) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$;
(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

These properties will become very important later on; in fact, the second is so fundamental that it was Legendre's original definition of the symbol.

Remark 2.4. As a consequence of Proposition 2.3, the Legendre symbol induces a homomorphism $(\mathbf{Z}/p\mathbf{Z})^* \to \{\pm 1\}$ given by $a \bmod p \mapsto \left(\frac{a}{p}\right)$. It is surjective, and its kernel is precisely the set of squares. Thus the set of squares forms a subgroup of index 2, from which it follows that there are as many squares as non-squares in $(\mathbf{Z}/p\mathbf{Z})^*$. This will become important later in the proof of Lemma 3.3.

We can know present the theorem in its most common form.

Theorem 2.5 (Quadratic Reciprocity)**.** *Let p, q be distinct odd primes. Then we have that*

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

The fact that there is any relation at all between whether p is a square modulo q and whether q is a square modulo p is incredibly unexpected and remarkable. Paired with the fact that the theorem is incredibly easy to state, many consider it one of the most beuatiful theorems in number theory.

If we write

$$p^* \stackrel{\text{def}}{=} \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p,$$

it follows from Proposition 2.3 that the above formulation is equivalent to saying that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. This is the formulation that is most commonly found in algebraic number theory, and it is the one we will prove below.

3. Gauss and quadratic reciprocity

The proof we give in this section is largely based on Gauss's sixth proof, and can be found in the well-known book of Ireland and Rosen [IR90, Chapter 6, p. 70]. Recall that a *primitive n-th root of unity* is a complex number ζ satisfying $\zeta^n = 1$ and $\zeta^k \neq 1$ for $1 \leq k < n$. For the remainder of this article, ζ will be be a fixed primitve p-th root of unity. We start with a lemma about these roots of unity.

Lemma 3.1. *Let $c \in \mathbf{Z}$. Then*

$$\sum_{t=0}^{p-1} \zeta^{ct} = \begin{cases} p & \text{if } p|c, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $p|c$, we have $\zeta^{ct} = 1$ for all t, and hence the sum is equal to p. Otherwise we see that

$$\sum_{t=0}^{p-1} \zeta^{ct} = \frac{\zeta^{cp} - 1}{\zeta^c - 1} = 0. \qquad \square$$

Definition 3.2. For $a \in \mathbf{Z}$, the *quadratic Gauss sum* is

$$\tau_a \stackrel{\text{def}}{=} \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}.$$

We write $\tau = \tau_1$.

At first this may seem like a rather arbitrary definition. Intuitively one can think about it as a way of encoding all different Legendre symbols of p into a single number. This becomes more clear in the following lemma.

Lemma 3.3. $\tau_a = \left(\frac{a}{p}\right) \tau$.

Proof. In the case that a is a multiple of p, the right hand side is equal to 0. We also have that $\zeta^{at} = 1$ for all t, thus

$$\tau_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right),$$

and this is indeed 0 because of Remark 2.4, saying there are as many squares as non-squares in $(\mathbf{Z}/p\mathbf{Z})^*$.

If $p \nmid a$, we have $\left(\frac{a}{p}\right)^2 = 1$, so

$$\tau_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at} = \left(\frac{a}{p}\right)^2 \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at} = \left(\frac{a}{p}\right) \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at},$$

where the last equality follows from the multiplicativity of the Legendre symbol (Proposition 2.3). Now note the following: if t runs through a system of representatives of $\mathbf{Z}/p\mathbf{Z}$, then so does $s = at$. Thus

$$\left(\frac{a}{p}\right) \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \left(\frac{a}{p}\right) \sum_{s=0}^{p-1} \left(\frac{s}{p}\right) \zeta^{s} = \left(\frac{a}{p}\right) \tau. \qquad \square$$

We now arrive at what is probably the most important ingredient of the proof of quadratic reciprocity.

Proposition 3.4. $\tau^2 = p^*$.

Proof. The main idea is to write the sum $\sum_{a=0}^{p-1} \tau_a \tau_{-a}$ in two different ways, and then setting these two expressions equal. Using Lemma 3.3 we get that for $p \nmid a$, we have $\tau_a \tau_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right)\tau^2 = \left(\frac{-1}{p}\right)\tau^2$, and hence we see that

$$\sum_{a=0}^{p-1} \tau_a \tau_{-a} = \left(\frac{-1}{p}\right)(p-1)\tau^2.$$

On the other hand the definition of τ_a gives us that

$$\sum_{a=0}^{p-1} \tau_a \tau_{-a} = \sum_{a=0}^{p-1} \sum_{x,y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{ax} \zeta^{-ay} = \sum_{x,y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(x-y)}.$$

By Lemma 3.1 the inner sum is equal to 0 for $x \neq y$, and otherwise it is equal to p. Thus we can rewrite the double sum over x and y as a single sum over x, by replacing all instances of y with x, since the terms for which $x \neq y$ are zero. What remains is

$$\sum_{x,y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(x-y)} = \sum_{x=0}^{p-1} \left(\frac{x^2}{p}\right) p = (p-1)p.$$

From this we see that we must have $\left(\frac{-1}{p}\right)(p-1)\tau^2 = (p-1)p$, or put differently $\left(\frac{-1}{p}\right)\tau^2 = p$. Lastly we can multiply this equality by $\left(\frac{-1}{p}\right)$, to arrive at the fact that

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

At last, we are ready to give the proof of the law of quadratic reciprocity.

Proof of Theorem 2.5. We will use the same general idea as the previous proof, and express τ^{q+1} in two ways. On one hand,

$$\tau^{q+1} = (\tau^2)^{\frac{q-1}{2}}\tau^2 = (p^*)^{\frac{q-1}{2}}p^* \equiv \left(\frac{p^*}{q}\right)p^* \bmod q,$$

where we used Proposition 3.4 for the second equality, and part 2 of Proposition 2.3 for the last congruence.

On the other hand, we can write out that

$$\tau^{q+1} = \left(\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\zeta^t\right)^q \tau.$$

If we were to expand this using repeated binomial expansion, we would certainly get all the individual terms of the sum raised to the power q, plus a number of cross terms. Since q is prime, one can easily show are binomial coefficients $\binom{q}{k}$ are divisible by q for $1 < k < q$. Hence the coefficients of the cross terms are divisible by q. If we therefore consider the entire expression modulo q, we are left with

$$\tau^{q+1} \equiv \left(\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)^q\zeta^{qt}\right)\tau = \tau_q\tau = \left(\frac{q}{p}\right)\tau^2 = \left(\frac{q}{p}\right)p^* \bmod q,$$

where the last two equalities follow from Lemma 3.3 and Proposition 3.4 respectively. Thus we see that $\left(\frac{q}{p}\right)p^* \equiv \left(\frac{p^*}{q}\right)p^* \bmod q$, and because p and q are distinct, p^* is invertible mod q, and hence $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \bmod q$. Finally, because -1 and 1 are never congruent modulo an odd prime, we get that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. □

The careful reader may have noticed we are working modulo q while our expressions can contain complex numbers. Using facts about rings one can easily show that this is still valid.[2]

4. Artin and Langlands

After Gauss had given this proof in 1818, many number theorists were convinced there was something deeper going on in the proof. The connection with roots of unity in particular, that is nowhere to be found in the theorem itself, is plainly clear in the proof. This was one of the main reasons for the beginning of *class field theory*, a subfield of algebraic numebr theory, dealing mainly with so called Abelian extensions of number fields and generalizations of the classical reciprocity law. One of the highlights of class field theory was the proof at the start of the 20th century of the *Artin reciprocity law*. This theorem, which to this day is still one of the most important results in number theory, makes it possible to place quadratic reciprocity and Gauss's proof in a broader context, making it possible to gain a much more deep

[2]We are in fact working in the ring $\mathbf{Z}[\zeta]/(q)$.

understanding. We refer the interested reader to the accessible article of Lenstra and Stevenhagen [LS00].

In modern number theory, the Langlands program is a central object of study. It is a collection of conjectures that can in a way be seen as the 'ultimate' generalization of quadratic reciprocity. Both the aforementioned theorem of Artin, but also the modularity theorem, which was the basis for Wiles's proof of Fermat's Last Theorem, are special cases of Langlands's conjectures. In 2018 Robert Langlands won the Abel prize for his work. See for instance [Sle18] for a short and accessible introduction.

The law of quadratic reciprocity thus may seem simple, and is probably nothing more than a cool party trick at first. Nevertheless, there is a lot of beautiful mathematics behind it, and it would be difficult to say were number theory as a whole would currently be if it hadn't been discovered.

References

[Cox13] David Cox. *Primes of the form $x^2 + ny^2$*. 2nd ed. John Wiley & Sons, Inc., 2013.

[Gau01] Carl Friedrich Gauss. *Disquisitiones Arithmaticae*. 1801.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. 2nd ed. Springer-Verlag, New York, 1990.

[LS00] Hendrik W. Lenstra and Peter Stevenhagen. "Artin Reciprocity and Mersenne Primes". *Nieuw Archief voor Wiskunde* 5.1 (2000), pp. 44–54. URL: http://websites.math.leidenuniv.nl/algebra/artin.pdf (visited on 03/01/2020).

[Sle18] Arne Sletsjøe. *From quadratic reciprocity to Langlands' program*. 2018. URL: https://www.abelprize.no/c73016/binfil/download.php?tid=73038 (visited on 01/23/2020).