PEOPLE's DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf university of Msila
Faculty of Mathematics and computer sciences
Department of Mathematics

Master memory

Field : Mathematics and computer sciences
Branch : Mathematics
Option : Algebra and Discrete Mathematics

Theme

THE QUADRATIC RECIPROCITY LAW

Presented by :
M^s Elalia ALLAL

The jury composed of :

Lemnaouar ZADAM	Prof,	University of M'sila	**President**.
Moussa BENOUMHANI	MC,	University of M'sila	**Supervisor.**
Lahcene LADJLAT	MA,	University of M'sila	**Examiner.**

University year 2019/2020

الاهداء

مرت قاطرة البحث بكثير من العوائق , ومع ذلك حاولت أن أتخطاها بثبات بفضل من الله ومنه .

الى من وضع المولى سبحانه وتعالى الجنة تحت قدميها ووقرها في كتابه العزيز.

الى أم كانت سبب وجودي والتي وافتها المنية منذ24 عام.

والى أم وضعتني على طريق الحياة وضحت الكثير من أجلي ولم تدخر جهدا في سبيل اسعادي على الدوام والتي غادرتنا الى ديار الحق منذ ثلاثة أشهر طيب الله ثراهما.

نسير في دروب الحياة ويبقى من يسطر على أذهاننا في كل مسلك نسلكه صاحب الوجه الطيب (والدي العزيز)أطال الله في عمره.

الى أساتذتي ممن كان لهم الدور الأكبر في مساندتي وأخص بالذكر الأستاذ موسى بن أم هاني الذي لم يتوان في مساندتي وتزويدي بالمعلومات .

الى اخوتي واخواتي والى أصدقائي الذين أشهد لهم بأنهم نعم الاخوة ونعم الرفقاء في جميع الأمور .

أهدي لكم بحث تخرجي .....

داعيا المولى-عزوجل –أن يطيل أعماركم ويرزقكم الخيرات.

Table des matières

General Introduction

The Law of Quadratic Reciprocity deals with congruences of the second degree. More precisely, congruences of type $ax^2 + bx + c =\equiv 0 \mod p$, ($p$ is a prime number) which in turn, may be transformed to the simple equation $x^2 \equiv a \mod p$. If the previous equation has a solution, we say that a is a quadratic residue modulo p, and denote this by Legendre symbol :

$$\left(\frac{a}{p}\right) = 1,$$

if a is not a residue modulo p, we write

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

We can ask, if there is a relation between the two congruences $x^2 \equiv q \mod p$ and $x^2 \equiv p \mod q$?

The law of quadratic reciprocity answers this question and gives a relation between the solvability of the two equations. The basic relationship was conjectured experimentally by **Euler** in 1783. Two years later, **Legendre** gave an incomplete proof of it. Using this symbol (1798) , the first correct proof was given by **Gauss** in 1801.

This work is divided into three Chapters :

In the first Chapter, we state all the results we need in the sequel. The second chapter is devoted to the proof of the main result, namely, the Law of quadratic reciprocity. In the last chapter we give some applications, to illustrate the use of the law to solve some diophantine equations.

List of notation

$a \setminus b$: a divides b

$a \nmid b$: a does not divide b

$a \equiv b \mod n$: a is congruent to b modulo n

$\gcd(a, b)$: greatest common divisor of a and b

Icm(a,b) : least common multiple of a and b

(a/p) : Legendre symbol (p prime)

CHAPITRE 1

PRELIMINARIES

1.1 Euler's Criterion

In this chapter we state all the results we need in the sequel. The Quadratic Reciprocity Law is an important tool to solve quadratic diophantine equations. Before going far in the subject, let us see how to reduce quadratic equations to a simpler ones. For this, consider the equation of the second degree :

$$ax^2 + bx + c \equiv 0 \mod p, \tag{1}$$

where p is an odd prime and $p \nmid a$; that is, $\gcd(a, p) = 1$. The fact that p is an odd prime implies that $\gcd(4a, p) = 1$. The previous quadratic congruence becomes, after multiplying it by $4a$,

$$4a\left(ax^2 + bx + c\right) \equiv 0 \mod p.$$

$$\left(2ax^2\right) + 4abx + 4ac \equiv 0 \mod p.$$

By using the identity

$$(2ax)^2 + 4abx + 4ac = (2ax + b)^2 - \left(b^2 - 4ac\right)$$

that is, we obtain

$$(2ax + b)^2 \equiv \left(b^2 - 4ac\right) \mod p.$$

Now put

$$y = 2ax + b \quad \text{and} \quad d = b^2 - 4ac,$$

to get

$$y^2 \equiv d \mod p. \tag{2}$$

If

$$x \equiv x_0 \mod p$$

is a solution of the quadratic congruence in Eq (1), then the integer

$$y \equiv 2ax_0 + b \mod p$$

satisfies the quadratic congruence in Eq.(2).

Conversely, if

$$y \equiv y_0 \mod p$$

is a solution of the quadratic congruence in Eq.(2), then the linear

$$2ax \equiv y_0 - b \mod p$$

can be solved to obtain a solution of Eq.(1).

This means that the problem of finding a solution to the quadratic congruence in Eq.(1) is equivalent to that of finding a solution to a linear congruence and a quadratic congruence of the form

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

If $p|a$, then the quadratic congruence in Eq.(3) has $x \equiv 0 \mod p$ as its only solution. From now on, we will assume that $p \nmid a$.

Once this supposition is done, whenever

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

has a solution $x = x_0$,there is also a second solution which is not congruent to the first. Indeed if

$$x_0 \equiv p - x_0 \mod p,$$

this implies that

$$2x_0 \equiv 0 \mod p$$

, or $x_0 \equiv 0 \mod p$, which is impossible.

By Lagrange's theorem, these two solutions are all the possible incongruent solutions of

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

In conclusion :

either

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

has exactly two solutions or no solutions at all.

Example Solve the quadratic congruences :

1) $x^2 + 7x + 10 \equiv 0 \mod 11.$

2) $5x^2 + 6x + 1 \equiv 0 \mod 23.$

Solution :

1) Since 11 is odd and $\gcd(1, 11) = 1$, the solution is given by

$$y^2 = (2x + 7)^2 \mod 11 \quad \text{and} \quad d = 9.$$

Then

$$(2x + 7)^2 \equiv 9 \mod 11.$$

We get $y \equiv \pm 3 \mod 11$. We solve the two equations :

$$y \equiv 3 \mod 11 \quad \text{and} \quad y \equiv -3 \mod 11$$

The first gives $x = 9$, and the second, $x = 6$.

2) For the second congruence, also, note that number 23 is an odd prime, and

$$\gcd(5, 23) = 1.$$

The equation is reduced to

$$y^2 = (10x + 6)^2 \quad and \quad d = 16.$$

Or, which is the same

$$(10x + 6)^2 \equiv 16 \,(mod 23)\,.$$

We obtain

$$y \equiv \pm 4 \mod 23.$$

Solving

$$y \equiv 4 \mod 23$$

gives

$$x = 9,$$

and solving

$$y \equiv -4 \mod 23,$$

gives

$$x = 22.$$

The aim goal of this work is to prove a test for the existence of solutions of the quadratic congruence,

$$x^2 \equiv a \mod p \qquad \gcd(a, p) = 1 \tag{4}$$

To put it differently, we wish to identify those integers a, that are perfect squares modulo p. Some additional and useful terminology will help us to investigate the subject easily.

Definition 1.1.1. *.Let p be an odd prime and* $\gcd(a, p) = 1$. *If the quadratic congruence* $x^2 \equiv a \mod p$ *has a solution, then* a *is said to be a quadratic residue of p .Otherwise,* a *is called a quadratic nonresidue of p .*

Example 1.1.1. *Consider the case of the prime* $p = 11$. *To find out how many of the integers* $1,\ 2\ , 3,\ ...,\ 10$ *are quadratic residues of 11, we must know which of the congruences*

$$x^2 \equiv a \mod 11,$$

are solvable when a *runs through the set* $\{1, 2, ..., 10\}$> . *Now* $mod 11$, *the squares of the integers* $1,\ 2\ , 3,\ ...,\ 10$ *are*

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

So ,the quadratic residues of 11 are 1,3,4,5 and 9 ;the integers 2,6,7,8 and 10 are quadratic nonresidues of 11.

Observe that the integers between 1 and 10 ar divided equally a mong the quadratic residues and nonresidues ;this is typical of the general situation
For $p = 11$ *there are two paires of consecutive quadratic residues ,the pairees 3,4 and 7,8 It can be shown that for any odd prime p there are* $1/4\left(p - 4 - (-1)^{(p-1)/2}\right)$ *consecutive pairs.*
Euler devised a simple criterion for deciding whether an integer a is a quadratic residue of agiven prime p.

Theorem 1.1.1. . ***Euler's Criterion.*** *Let p be an odd prime and* $\gcd(a, p) = 1$ *then a is a quadratic of p if and only if*

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

proof. *suppose that a is a quadratic residue of p, so that* $x^2 \equiv a \mod p$ *admits a solution, call it* x_1*.Because* $\gcd(a, p) = 1$*, evidently* $\gcd(x_1, p) = 1$*. we may therefore appeal to Fermat's theorem to obtain*

$$a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1 \mod p$$

For the opposite direction,assume that the congruence $a^{(p-1)/2} \equiv 1 \mod p$
holds,and let r be a primitive root of p. then $a \equiv r^k \mod p$ *for some integer k, with* $1 \leq k \leq p - 1$*. It follows that*

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \mod p$$

the order ofr(namely,$p - 1$*) must divide the exponent* $k(p-1)/2$*.the impllication is that k is even integer , say* $k = 2j$ *. hence ;*

$$(r^j)^2 = r^{2j} = r^k \equiv a \mod p$$

making the integer r^j *a solution of the congruence* $x^2 \equiv a\,(mod p)$*. This proves that a is a quadratic residue of the prime p .*
Now if p (as always) is an odd prime and $\gcd(a, p) = 1$*, then*

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

the last congruence being justified by Fermat's theorem. hence ,either

$$a^{(p-1)/2} \equiv 1 \mod p \text{ or } a^{(p-1)/2} \equiv -1 \mod p$$

but not both. For,if both congruences held simultaneously, then we would have $1 \equiv -1\,(modp)$*,or equivalently ,*$p/2$*,which conflicts with our hypothesis.Because a quadratic nonresidue of p does not satisfy* $a^{(p-1)/2} \equiv 1 \mod p$*, it must therefore satisfy* $a^{(p-1)/2} \equiv -1\ modp$*. This observation provides an alternate formulation of Euler's criterion :the integer a is a quadratic nonresidue of the prime p if and only if* $a^{(p-1)/2} \equiv -1\ modp$*.*■

Corollary 1.1.1. *. Let p be an odd prime and* $\gcd(a, p) = 1$*. then a is a quadratic residue or nonresidue of p according to whether*

$$a^{(p-1)/2} \equiv 1 \mod p \text{ or } a^{(p-1)/2} \equiv -1 \mod p$$

Example 1.1.2. .

1) In the case where $p = 11$ *we find that*

$$2^{(11-1)/2} = 2^5 = 32 \equiv 10 \equiv -1 \mod 11$$

thus , by virtue of the last corollary , the integer 2 is a quadratic nonresidue of 11 .

Because

$$3^{(11-1)/2} = 3^5 = 243 \equiv 1 \mod 11$$

the same result indicates that 3 is a quadratic residue of 11 . 2) In the case where $p = 13$ *we find that*

$$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \mod 13$$

thus , by virtue of the last corollary , the integer 2 is a quadratic nonresidue of 13 .

Because

$$3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1 \mod 13$$

the same result indicates that 3 is a quadratic residue of 13 .

1.2 The Legendre Symbol and Its Properties

Solving diophantine equations will be highly simplified by the use of a symbol introduced by Legendre : $\left(\frac{a}{p}\right)$. It is called Legendre symbol. Here is its definition :

Definition 1.2.1. . *Let p be an odd prime and let* $\gcd(a,p)=1$.
The Legendre symbol (a/p) *is defined by*

$$\left(\frac{a}{p}\right)=\begin{cases} 1 \quad if \quad a \quad is \quad aquadraticresidueof \quad p \\ -1 \quad if \quad a \quad is \quad aquadraticnonresidueof \quad p \end{cases}$$

Remark. For $p \setminus a$, we have purposely left the symbol $\dfrac{a}{p}$ undefined. Some authors find it convenient to extend Legendre's definition to this case by setting $\left(\frac{a}{p}\right)=0$.

Example 1.2.1. .

$$\left(\frac{1}{11}\right)=\left(\tfrac{3}{11}\right)=\left(\frac{4}{11}\right)=\left(\tfrac{5}{11}\right)=\left(\tfrac{9}{11}\right)=1$$
$$\left(\tfrac{2}{11}\right)=\left(\tfrac{6}{11}\right)=\left(\tfrac{7}{11}\right)=\left(\tfrac{8}{11}\right)=\left(\tfrac{10}{11}\right)=-1$$

Theorem 1.2.1. . *Let p be an odd prime and let a and b be integers that are relatively prime to p . then the legendre symbol has the follwing properties :*

(a) *If* $a \equiv b \mod p, then\,(a/p)=(b/p)$.

(b) $(a^2/p)=1$.

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

(d) $(ab/p)=(a/p)\,(b/p)$.

(e) $(1/p)=1 \quad and \quad (-1/p)=(-1)^{(p-1)/2}$.

proof.

1) If $a \equiv b \mod p$*,then the two congruences* $x^2 \equiv a\ modp$ *and* $x^2 \equiv b\ modp$ *have exactly the same solution, if any at all. Thus,* $x^2 \equiv a\,(modp)$ *and*$x^2 \equiv b \mod p$ *are both solvable,or neither one has a solution. This is reflected in the statement* $\left(\dfrac{a}{p}\right)=\left(\frac{b}{p}\right)$.

2) observe that the integer a trivially satisfies the congruence $x^2 \equiv a^2 \mod p$*; hence,*$\left(\frac{a^2}{p}\right)=1$. *Property (c) is just the corollary to Theorem 1.1.1 rephrased in terms of the Legendre symbol. we use (c) to establish property (d) :*

$$\left(\tfrac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right) \mod p$$

Now the Legendre symbol assumesonly the values 1 or -1*.If* $\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*, we would have* $1 \equiv -1 \mod p$ *or*$2 \equiv 0 \mod p$*;this cannot occur,because* $p > 2$*.*

It follows that

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

Finally, we observe that the first equality in property (e) is a special case of property (b),whereas the second one is obtained from property (c)upon setting $a = -1$*.*

Because the quantities $\left(\frac{-1}{p}\right)$ *and* $(-1)^{(p-1)/2}$ *are either 1 or*-1*,the resulting congruence.*

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

implies that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$*.*

From parts (b) and (d) of Theorem 1.2.1, we may also abstract the relation

(f) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)$ *In other words ,a square factor that is relatively prime to p can be deleted from the numerator of the Legendre symbol Without affecting its value.*

Because $(p-1)/2$*is even for a prime p form* $4k+1$*and odd for p of the form* $4k+3$*, the equation* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ *permits us to add a small supplemental corollary to Theorem 1.2.1* ■

Corollary 1.2.1. *Let* p *be an odd prime number . then*

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

Equivalently

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

Example 1.2.2. *. Let the congruence*

$$x^2 \equiv -46 \mod 17.$$

To know if this equation is solvable or not, we evaluate Legendre symbol,

$$\left(\frac{-46}{17}\right).$$

First, we apply properties (d) *and* (e) *of Theorem 1.2.1, to write*

$$\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right) = \left(\frac{46}{17}\right).$$

Because $46 \equiv 12 \mod 17$*, it follows that*

$$\left(\tfrac{46}{17}\right) = \left(\tfrac{12}{17}\right)$$

Now property (f) *gives*

$$\left(\tfrac{12}{17}\right) = \left(\tfrac{3\cdot 2^2}{17}\right) = \left(\tfrac{3}{17}\right)$$

But

$$\left(\frac{3}{17}\right) \equiv 3^{(17-1)/2} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1\,(mod 17)\,,$$

where we have made appropriate use of property (c) *of Theorem* 1.2*; hence,*

$$\left(\frac{3}{17}\right) = -1.$$

So, since

$$\left(\frac{-46}{17}\right) = -1,$$

the quadratic congruence $x^2 \equiv -46 \mod 17$ *has no solution.*

Theorem 1.2.2. *There are infinitely many primes of the form* $4k+1$*.*

Proof. Suppose that there are finitely many such primes; let us call them

$$p_1, p_2, ..., p_n,$$

and consider the integer

$$N = (2p_1p_2...p_n)^2 + 1.$$

Clearly N is odd, so that there exists some odd prime$p$ with $p \setminus N$. Or, which is the same :

$$(2p_1p_2...p_n)^2 \equiv -1 \mod p.$$

This may be written, using the Legendre symbol;

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

But the relation $\left(\frac{-1}{p}\right) = 1$ holds only if p is of the form $4k+1$. Thus, p is one of the primes p_i. This implies that

$$p_i | N - (2p_1p_2...p_n)^2\,,$$

this means

$$p_i | 1.$$

Contradiction. In conclusion : There are infinitely many primes of the form $4k+1$. ■

We give more results and properties of quadratic residues with Theorem 1.2.3

Theorem 1.2.3. . *If p is an odd prime, then*

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

Hence, there are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues of p.

proof. Let r be a primitive root of p. We know that, $\mod p$, the powers

$$r, r^2, ..., r^{p-1},$$

are just a permutation of the integers $1, 2, ...p-1$. Thus, for any a lying between 1 and $p-1$, inclusive, there exists a unique positive integer

$$k\,(1 \leqslant k \leqslant p-1)\,,$$

such that $a \equiv r^k\,(modp)$. Using Euler's criterion, we have

$$\left(\frac{a}{p}\right)=\left(\frac{r^k}{p}\right)\equiv\left(r^k\right)^{(p-1)/2}=\left(r^{(p-1)/2}\right)^k\equiv(-1)^k\,(\mod p) \tag{1}$$

the number r is a primitive root of p, then

$$r^{(p-1)/2}\equiv -1 \mod p.$$

But $\left(\frac{a}{p}\right)$ and $(-1)^k$ are equal to either 1 or -1, so that equality. Now add up those Legendre symbols to obtain

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

which is the desired conclusion. ■ From the proof of Theorem 1.2.3, we deduce the corollary.

Corollary 1.2.2. *The quadratic residues of an odd prime p are congruent $\mod p$ to the even powers of a primitive root r of p; the quadratic nonresidues are congruent to the odd powers of r.*

Example 1.2.3. . *For $p=11$, 2 is a primitive root of 11, the quadratic residues modulo 11 are given by the even powers of 2,*

$$2^2\equiv 4$$
$$2^4\equiv 5$$
$$2^6\equiv 9$$
$$2^8\equiv 3$$
$$2^{10}\equiv 1$$

all congruences being modulo 11*, the non residues occur as the odd powers of 2 :*

$$2^1 \equiv 2$$
$$2^3 \equiv 8$$
$$2^5 \equiv 10$$
$$2^7 \equiv 7$$
$$2^9 \equiv 6$$

1.3 Gauss's lemma

The quadratic reciprocity theorem proof is based on the two following Lemmata, The first is commonly known as Gauss lemma, the second one is also important and will be used later in the proof of the law.

Theorem 1.3.1. . ***Gauss's lemma .*** *Let* p *be an odd prime and let* $\gcd(a,p) = 1$*. If* n *denotes the number of integers in the set*

$$S = \left\{a, 2a, 3a, ..., \left(\tfrac{p-1}{2}\right) a\right\}$$

whose remainders upon division by p *exceed* $p/2$*, then*

$$\left(\tfrac{a}{p}\right) = (-1)^n$$

Proof . *Because*

$$\gcd(a,p) = 1,$$

none of the integers in S *is congruent to zero and no two are congruent to each other modulo* p*. Let*

$$r_1, ..., r_m,$$

be those remainders upon division by p *such that* $0 < r_i < p/2$*, and let*

$$s_1, ..., s_n,$$

be those remainders such that $p > s_i > p/2$ *.*
Then

$$m + n = (p-1)/2,$$

and the integers

$$r_1, ..., r_m \quad p - s_1, ..., p - s_n$$

are all positive and less than $p/2$.

It suffices to show that no $p - s_i$ *is equal to any* r_j. *Assume to the contrary that*

$$p - s_i = r_j,$$

for some of i *and* j. *Then there exist integers* u *and* v, *with* $1 \leqslant u, v \leqslant (p-1)/2$, *satisfying*

$$s_i \equiv ua \mod p \text{ and } r_j \equiv va \mod p.$$

Hence,

$$(u+v)\, a \equiv s_i + r_j = p \equiv 0 \mod p,$$

which says that

$$u + v \equiv 0 \mod p.$$

But the latter congruence cannot be true, because

$$1 < u + v \leqslant p - 1.$$

The point we arrive at, is that the $(p-1)/2$ *numbers*

$$r_1, ..., r_m \quad p - s_1, ..., p - s_n$$

are just the integers $1, 2, ..., (p-1)/2$, *not necessarily in the natural order. Thus, their product is*

$$[(p-1)/2]!.$$

Or, which is the same

$$\left(\frac{p-1}{2}\right)! = r_1, ..., r_m\, (p - s_1), ..., (p - s_n) \equiv (-1)^n\, r_1, ..., r_m\, (-s_1), ..., (-s_n) \mod p \equiv (-1)^n\, r_1, ..., r_m s$$

But we know that

$$r_1, ..., r_m, s_1, ..., s_n$$

are congruent $\mod p$ *to*

$$a, 2a, ..., [(p-1)/2]$$

a, in a certain order, so that

$$\left(\tfrac{p-1}{2}\right)! \equiv (-1)^n a_1.2a...\left(\tfrac{p-1}{2}\right) a \mod p$$
$$\equiv (-1)^n a^{(p-1)/2}\left(\tfrac{p-1}{2}\right)! \mod p$$

Because $[(p-1)/2]!$ *is relatively to p, it may be canceled from both sides of this congruence to give*

$$1 \equiv (-1)^n a^{(p-1)/2} \mod p$$

or upon multiplying by $(-1)^n$*,*

$$a^{(p-1)/2} \equiv (-1)^n \mod p$$

Use of Euler's criterion completes the proof :

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

and because these previous numbers are just 1 *or* -1*, we deduce*

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

The proof is complete. ■

Let us illustrate by the following example the previous Lemma.

Example 1.3.1. *. Let* $p = 17$*,* $a = 7$*,* $(p-1)/2 = 8$*,* $\gcd(17, 7) = 1$*. So that*

$$S = \{7, 14, 21, 28, 35, 42, 49, 56\} .$$

Modulo 17*, the members of* S *are the same as the integers*

$$7, 14, 4, 11, 1, 8, 15, 5.$$

Three of these are greater than $17/2$*. Hence,* $n = 3$ *and Theorem 1.3.1 says that*

$$(7/17) = (-1)^3 = -1.$$

Lemma 1.3.1. *If* p *is an odd prime and* a *an odd integer, with* $\gcd(a, p) = 1$*,then*

$$\left(\tfrac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}[ka/p]}$$

Example 1.3.2. *.we consider* $P = 13$ *and* $a = 5$*. Because* $(p-1)/2 = 6$ *, it is necessary to calculate* $[ka/p]$ *for* $k = 1, ..., 6$:

$$[5/13] = [10/13] = 0$$
$$[15/13] = [20/13] = [25/13] = 1$$
$$[30/13] = 2$$

But the lemma just proven , we have
$(5/13) = (-1)^{1+1+1++2} = (-1)^5 = -1$

The following result, gives us, the conditions for the number 2 to be a quadratic residue modulo an odd prime p.

Theorem 1.3.2. *. If p is an odd prime,then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & ,if \quad p \equiv 1 \mod 8 \quad or \quad p \equiv 7 \mod 8 \\ -1 & ,if \quad p \equiv 3 \mod 8 \quad or \quad p \equiv 5 \mod 8 \end{cases}$$

Proof. We apply Gauss's Lemma (Theorem 1.3.1) to the set

$$S = \{1, 2, 3, ..., (p-1)/2\}.$$

Then

$$\{2s : s \in S\} = \{2, 4, 6, ..., p-1\},$$

and

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

which, upon division by p, have remainders greater than $p/2$. The members $2s$ are all less than p , so it is enough to count the number that exceed $p/2$ for $1 \leqslant k \leqslant (p-1)/2$. We have $2k < p/2$ if and only if $k < p/4$. If [ ] denotes the floor function, then there are $[p/4]$ integers in $2s$ less than $p/2$. Hence,

$$n = \tfrac{p-1}{2} - \left[\tfrac{p}{4}\right]$$

is the number of integers that are greater than $p/2$.
Since every odd prime p is congruent to $1, 3, 5, or 7$ modulo 8, there are four cases to consider.
1) If $p = 8k+1$, then $n = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k$
and so $n = 2k$ and $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$.
2) If $p = 8k+3$, then $n = 4k+1 - \left[2k + \frac{3}{4}\right] = 4k+1-2k = 2k+1$
and so $n = 2k+1$ and $\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1$

3) If $p = 8k + 5$, then $n = 4k + 2 - \left[2k + 1 + \frac{1}{4}\right] = 4k + 2 - (2k + 1) = 2k + 1$
and so $n = 2k + 1$ and $\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1$
4) If $p = 8k + 7$, then $n = 4k + 3 - \left[2k + 1 + \frac{3}{4}\right] = 4k + 3 - (2k + 1) = 2k + 2$
and so $n = 2k + 2$ and $\left(\frac{2}{p}\right) = (-1)^{2k+2} = 1$
Thus, when p is of the form $8k + 1$ or $8k + 7$, n is even and $\left(\frac{2}{p}\right) = 1$; on the other hand, when p assumes the form $8k + 3$ or $8k + 5$, n is odd and $\left(\frac{2}{p}\right) = -1$. This completes the proof. ■
It is possible to write the previous result in a more elegant and closed form :

Corollary 1.3.1. *.If p is an odd prime, then*

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

***Proof**. In fact, if the prime p is of the form $8k \pm 1$ (equivalently, $p \equiv 1 \mod 8$ or $p \equiv 7 \mod 8$, then*

$$\frac{p^2 - 1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$$

which is even integer ; in this situation,

$$(-1)^{\left(p^2-1\right)/2} = 1 = (2/p)\,.$$

On the other hand, if p has the form $8k \pm 3$ (equivalently, $p \equiv 3 \mod 8$ or $p \equiv 5 \mod 8$, then

$$\frac{p^2 - 1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1$$

which is odd ; here, we have

$$(-1)^{\left(p^2-1\right)/2} = -1 = (2/p)\,.$$

This completes the proof. ■
Another application of of the previous Gauss Lemma, is to apply it as a technique to find primitive roots. As we know, there is no general procedure for find a primitive root of the an odd prime p, bur in certain cases, it is possible to know whether a number is a primitive root or not.

Theorem 1.3.3. *.If p and $2p + 1$ are both odd primes, then the integer $(-1)^{(p-1)/2}\, 2$ is a primitive root of $2p + 1$.*

Proof. Let

$$q = 2p + 1.$$

There are two cases : $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$. In the first case, $(-1)^{(p-1)/2} = 2$. Since $\phi(q) = 2p$, the order of 2 modulo q must be $1, \ , 2\ p$, or $2p$. We have

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

But, since $q = 8k + 3$, it follows that

$$2^p \equiv -1 \mod q.$$

So, the order of 2, can not be p modulo q. Also, the order of 2 can not be 1 or 2, Because

$$2^2 \equiv 1 \mod q,$$

means that $q|3$, and that is impossible. So, the only possibility is that the order of 2 modulo q is $2p$.

Now, let $p \equiv 3 \mod 4$. In this case

$$(-1)^{(p-1)/2} = -2,$$

and

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

Now, because $q \equiv 3 \mod 8$, then

$$\left(\frac{-1}{q}\right) = -1 \text{ and } \left(\frac{2}{q}\right) = 1.$$

This gives the congruence

$$(-2)^p = \equiv -1.$$

We deduce then, that the order of 2 modulo q is $2p$. This completes the proof. ■

Theorem 1.3.4. *.There are infinitely many primes of the form $8k - 1$.*

Proof. As usual, suppose that there are only a finite number of such primes. Call them

$$p_1, p_2, ..., p_n,$$

and consider the integer

$$N = (4p_1, p_2, ..., p_n)^2 - 2$$

There exists at least one odd prime divisor p of N, so that

$$(4p_1, p_2, ..., p_n)^2 \equiv 2 \mod p$$

or $(2/p) = 1$. By Theorem 1.3.2, $p \equiv \pm 1 \mod 8$. If all the odd prime divisors of N were of the form $8k+1$, then N would be of the form $8k+1$, this is clearly impossible, because N is of the form $16a-2$. Furthermore, N must have a prime divisor q having the form $8k-1$. But $q|N$, and

$$q| (4p_1, p_2, ..., p_n)^2$$

this leads to the contradiction that $q|2$. The proof is finished. ■

CHAPITRE 2

QUADRATIC RECIPROCITY

In this chapter,we will prove the main result of the dissertation. The general idea is a relation between the two symbols

$$(p/q) \text{ and } (q/p)$$

2.1 QUADRATIC RECIPROCITY Law

Let p and q be distinct odd primes. If q is a quadratic residue $\mod p$, then the congruence

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

has two solutions. Also, if p is a quadratic residue $\mod q$, then the congruence

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

has also a solution. Using the Legendre symbol, this relationship may be written in the following form, known as the Quadratic Reciprocity Law :

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Theorem 2.1.1. ***Quadratic Reciprocity Law.*** *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Proof. Consider the rectangle in the xy coordinate plane whose vertices are $(0,0), (p/2,0), (0,q/2),$
$and\,(p/2,q/2)$. Let R indicates the region within this rectangle,not including any of the surrounding lines. The general attack plan is to calculate the number of lattice points (the points having coordinates of whole numbers), within R in two different ways. Because p and q are odd, the grid points in R consist of all points (n,m), where

$$1 \leqslant n \leqslant (p-1)/2 \text{ and } 1 \leqslant m \leqslant (q-1)/2.$$

Clearly, the number of such points is

$$\tfrac{p-1}{2} \cdot \tfrac{q-1}{2}.$$

Now, the diagonal D from $(0,0)$ $(p/2, q/2)$ has the equation has the equation

$$y = (q/p)\, x,$$

or equivalently

$$py = qx.$$

Because

$$\gcd(p,q) = 1,$$

none of the lattice points inside R will lie on D. If so, then p must divide the x coordinate of any lattice point on the line $py = qx$, and q must divide its y coordinate. This is not possible for such points in R. Suppose that T_1 denotes the portion of R that is below the diagonal D, and T_2 the portion above.

By what we have just seen, it suffices to count the lattice points inside each of these triangles. The number of integers in the interval $0 < y < kq/p$ is equal to $[kq/p]$. thus, for $1 \leqslant k \leqslant (p-1)/2$, there are precisely

$$[kq/p]$$

lattice points in T_1 directly above the point $(k,0)$ and below D; in other words, lying on the vertical line segment from $(k,0)\, to\, (k, kq/p)$. If follows that the total number of lattice points contained in T_1 is

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right].$$

By the same, the roles of p and q interchanged, we find the number of lattice points within T_2 :

$$\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right].$$

This is the total number of all the lattice points inside R, then

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right]$$

Now, by Gauss's lemma :

$$(p/q)(q/p) = (-1)^{\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right]} \cdot (-1)^{\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]} = (-1)^{\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right] + \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

This completes the proof. ■ It is possible to write the quadratic reciprocity law as follows :

Corollary 2.1.1. *If p and q are distinct odd primes,then*

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

Proof. *For p and q odd primes, $(p-1)/2 \cdot (q-1)/2$ is an even number if and only if p or q has the form $4k+1$,then*

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

If both are of the from $4k+3$, then $(p-1)/2 \cdot (q-1)/2$ is an odd number, and

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

This is what we wanted to prove. ■

It is also possible to write it as follows :

Corollary 2.1.2. *If p and q are distinct odd primes, then*

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

This means that if p and q are odd primes, then

$$(p/q) = (q/p),$$

unless both p and q are congruent to 3 modulo 4, and in that case,

$$(p/q) = -(q/p).$$

Proof.

If $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$ then

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

from (Corollarly 2.1.1). Hence

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

We have $\left(\frac{q}{p}\right)^2 = 1$. *So* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. *If* $p \equiv q \equiv 3 \mod 4$ *then*

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

from (Corollarly 2.1.1). We deduce

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

we have $\left(\frac{q}{p}\right)^2 = 1$ *then* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ ■

Example 2.1.1. *Let us evaluate* $\left(\frac{7}{19}\right)$. *Because* $p = q = 3 \mod 4$, *by the Law of Quadratic Reciprocity, we know that*

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right).$$

From part (a) *of Theorem 1.2.1, we see that*

$$\left(\frac{19}{7}\right) = \left(\frac{5}{7}\right).$$

Again, using the Law of Quadratic Reciprocity, and because $5 \equiv 1 \mod 4$ *and* $7 \equiv 3 \mod 4$, *we have*

$$\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right).$$

By part (a) *of Theorem 1.2.1, we know*

$$\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Hence, we deduce

$$\left(\frac{7}{19}\right) = 1.$$

Adapting the proof of the value of $\left(\frac{2}{p}\right)$, or using the quadratic law directly, we have

Theorem 2.1.2. *If* $p \neq 3$ *is an odd prime, then*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & if\ p \equiv \pm 1 \mod 12 \\ -1 & if\ p \equiv \pm 5 \mod 12 \end{cases}$$

Proof. By the quadratic reciprocity law, we have

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

Now, $p \equiv 1 \mod 3$ or $p \equiv 2 \mod 3$. So, using the previous results, we obtain

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & if\ p \equiv 1 \mod 3 \\ -1 & if\ p \equiv 2 \mod 3. \end{cases}$$

So,

$$\left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \mod 4 \text{ and } p \equiv 1 \mod 3$$

$$p \equiv 3 \mod 4 \text{ and } p \equiv 2 \mod 3.$$

The first condition is equivalent to

$$p \equiv 1 \mod 12,$$

while the second is equivalent to

$$p \equiv -1 \mod 12.$$

This completes the proof. ■

CHAPITRE 3

APPLICATIONS

In this chapter, we give some applications of the quadratic reciprocity law. First, we start by applying it to see whether the number 41 is a quadratic residue modulo 691 ? then we apply it to solve some diophantine equations.

3.1 Application 1

Is 41 a quadratic residue modulo 691 ?

Solution :

First, we have $\gcd(41, 691) = 1$. Let us evaluate the legendre symbol.

$$\left(\frac{41}{691}\right) = \left(\frac{691}{41}\right)(-1)^{\frac{691-1}{2}\cdot\frac{41-1}{2}} = \left(\frac{691}{41}\right) = \left(\frac{35}{41}\right).$$

Because the legendre symbol is multiplicative, we have

$$\left(\frac{7}{41}\right)\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right)\left(\frac{41}{7}\right) = \left(\frac{1}{5}\right)\left(\frac{6}{7}\right).$$

We know that $\left(\frac{1}{5}\right) = 1$.

So, with $\left(\frac{6}{7}\right)$.

$$\left(\frac{6}{7}\right) = -1.$$

Hence

$$\left(\frac{41}{691}\right) = \left(\frac{1}{5}\right)\left(\frac{6}{7}\right) = 1\,(-1) = -1$$

It follows then that 41 is a quadratic non residue of 691 and the only calculation actually done shows that

$$691 \equiv 35 \mod 41$$

3.2 Application 2

Find the solution (if it exists) of the diophantine equation :

$$103x + 78 = y^2.$$

Solution :

The number 103 is prime, so

$$y^2 = 78 \,(\mod 103)\,.$$

Also, note that

$$\gcd(103, 78) = 1.$$

The existence of a solution is equivalent to the fact that 78 is a quadratic residue modulo 103 .

The first step is to see if this is true in order to determine whether a solution exists.

The symbol $\left(\frac{78}{103}\right)$ must be calculated.

Before the Law of Quadratic Reciprocity can be used, the numerator must be first.

Let us decomposing 78 into prime factors, and using the formula

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

previously mentioned, we obtain

$$\left(\frac{78}{103}\right) = \left(\frac{2}{103}\right)\left(\frac{3}{103}\right)\left(\frac{13}{103}\right).$$

We already know that $\left(\frac{2}{103}\right) = 1$.

Also $103 \equiv -1 \,(\mod 8)$ (see formula in case $a = 2$).

Now use the Law of Quadratic Reciprocity for each of the two terms.

Since 3 and 103 are both equal to 3 modulo 4. This gives :

$$\left(\frac{78}{103}\right) = -\left(\frac{103}{3}\right)\left(\frac{103}{13}\right) = -\left(\frac{1}{3}\right)\left(\frac{12}{13}\right),$$

where 13 can be replaced by its modulo value 3in the first symbol and by its modulo value 13 in the second, as the value of a symbol depends only on the value of the numerator modulo the denominator were clearly $\left(\frac{1}{3}\right) = 1$, and hence

$$\left(\frac{78}{103}\right) = -\left(\frac{12}{13}\right) = -\left(\frac{-1}{13}\right).$$

Because $13 \equiv 1 \pmod 4$, we get $a\left(\frac{-1}{13}\right) = 1$.

So we have proved that

$$\left(\frac{78}{103}\right) = -1.$$

Hence 78 is a quadratic non residue of 103, and our equation has no integer solutions

3.3 Application

Does the following diophantine equation have a solution ?

$$43x + 31 = y^2$$

Solution :

$$y^2 \equiv 31 \mod 43$$

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

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 $2^2 = 4$.

Also

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

Now 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, and the equation does have a solution. $\frac{31}{43} = (-1)(1)(-1) = 1$. Therfore it is possible to solve $y^2 = 31(mod 43)$

$$y \equiv 17, 26(mod 43)$$

it is mong these solutions $y \equiv 17$and $y \equiv 26$

General Conclusion

In this work, we have given the proof of the Quadratic Reciprocity Law, as well as some of its applications in Number Theory.

We have seen how to know, whether a number is a quadratic residue modulo a prime or a non residue. Also, we saw how to solve congruence equations of the form square of the type $ax^2 + bx + c = 0 \mod p$, where p is a prime number

Bibliographie

[1] Daniel Alkema, The Law of Quadratic Reciprocity From Fermat to Gauss, University of Utrecht, January 2016.

[2] David M. Burton, Elementary Number Theory, University of New Hampshire , Fifth Edition .

[3] Hadj D.Oussama, Finite Arithmetic and Quadratic Reciprocity, Master's thesis, University Mohamed Boudiaf, M'sila, Algeria, 2017.

[4] M. B. Nathanson, Elementary Methods in Number Theory, Springer-Verlag, New yark, 2000.

[5] P. Daniel, Cours D'algèbre, Ellipses, 1996.

[6] S. Y. Yan, Elementary Number Theory, Springer, Berlin, 2002.

[7] K. Rosen, Elementary Number Theory and Its Applications, 4th Edition, Addison Wesley, 2000.

[8] Mathraining at https ://www.mathraining.be