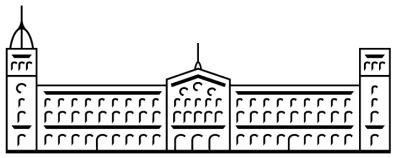

Treball final de màster

MÀSTER DE
MATEMÀTICA AVANÇADA

Facultat de Matemàtiques
Universitat de Barcelona

Fermat's Last Theorem:
Work of Kummer, Furtwängler and Terjanian

Autor:	**Adriana Moya Viñas**
Director:	**Dr. Victor Luis Dieulefait**
Realitzat a:	**Departament de Matemàtiques i Informàtica**

Barcelona, **27 de juny de 2018**

Abstract

As it is well-known, Fermat's Last Theorem states that the equation

$$x^n + y^n = z^n, \quad xyz \neq 0$$

has no integer solutions when the exponent n is greater or equal than 3. It was enunciated by Fermat around 1630 and stood unsolved for more than 350 years, until 1994 Andrew Wiles finally took that last step by proving the modularity conjecture for semistable elliptic curves.

This thesis highlights the first steps taken in proving the theorem, before the use of elliptic curves and modularity. Our objective is to resume all these results and try to give a general point of view of what was known before the use of modern methods.

Starting with elementary results, we move on to see Kummer's proof for regular primes. Afterwards, we see how Furtwängler uses class field theory to work on Fermat's problem, and give us more partial results of the theorem. Finally we study a generalization of Fermat's last theorem for even exponent, due to Hellegouarch, using again the techniques of class field theory.

Contents

Introduction

In the margin of his copy of the works of Diophantus, next to a problem on Pythagorean triples, Pierre de Fermat (1601 - 1665) wrote:

> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.

In modern language, Fermat's statement is the following:

Theorem (Fermat Last Theorem)**.** *The equation $x^n + y^n = z^n$, where n is a natural number larger than 2, has no solution in integers all different from 0.*

No proof of this statement was ever found among Fermat's papers. He did, however, write a proof for the particular case of $n = 4$ using the method which he called *infinite descent*. Briefly put, the method proves that certain properties or relations that satisfy positive natural numbers are impossible, by proving that if they held for any numbers they would hold for some smaller numbers; then, by the same argument, they would hold for some numbers that were smaller still, and so forth ad infinitum, which is impossible because a sequence of positive whole numbers cannot decrease indefinitely.

In trying to prove Fermat's theorem for every positive integer $n \geq 3$, one can observe that if the theorem holds for an integer m and $n = lm$ is a multiple on m,then it holds also for n. Since every integer $n \geq$ is a multiple of 4 or of a prime $p \neq 2$, it suffices to prove Fermat's conjecture for every odd prime. Another reduction that helps to find partial results on the theorem is to divide the statement in two cases:

> *First case*: The equation $x^p + y^p = z^p$ has no integer and non trivial solutions for which x, y, z are relatively prime to p.

> *Second case*: The equation $x^p + y^p = z^p$ has no integer and non trivial solutions for which one and only one of the three numbers is divisible by p.

A lot of mathematicians tried to aboard the problem. Some of them gave us partial results and actually we can thank to Fermat the amount of beautiful mathematics that have grown with the objective of proving his conjecture. A simple and elementary problem about whole numbers was stood unsolved for more than 350 years, but finally it was in 1994 when Andrew Wiles finally laid it to rest.

On these notes, we concentrate our attention in the techniques that were developed in order to prove FLT before the use of elliptic curves and modularity. These techniques only prove partial results of the general theorem, and our objective is to resume all these results and try to give a general point of view of what was known before the use of modern methods.

In Chapter 1 we start with the theorems that are proved without using any sophisticated methods, only arithmetic in $\mathbb{Z}$. This results include the particular cases that have an own proof and the first result that included a general kind of primes, the Sophie Germain primes. Finally, the first case on FLT but only for even exponent is also done with elementary techniques.

In Chapter 2 we give a background in the theory of cyclotomic fields and then prove Kummer's famous theorem: Fermat's last theorem is true for every exponent which is a regular prime.

Chapter 3 is devoted to two results that use class field theory to study Fermat's equation: Furtwängler's theorems and the generalization of FLT for even exponent, due to Hellegouarch. In order to understand how class fled theory derives these important criteria about Fermat's problem, we provide a short overview of the theory of reciprocity laws. Mainly we focus on Eisenstein's reciprocity law, which is crucial to relate class field theory with the Fermat's problem.

Finally, we present a short overview of what is the actual proof of Fermat's last theorem and how Andrew Wiles closed the problem that was more that 350 years open.

I would like to thank Dr. Luis Victor Dieulefait, my thesis advisor, his guidance and support throughout this work. I would also like to express my gratitude to Eduard Soto for his help and interest on this thesis.

Before Kummer

The methods that appear in this section only use elementary methods, i.e. they play with properties of the rational numbers. The case $n = 4$ had been settled by Fermat when he used his method of infinite descent to prove that the area of a right triangle with rational sides is never a perfect square, a condition that is equivalent to the claim that there are no integer solutions to $x^4 + y^4 = z^2$, and hence no solutions to $x^4 + y^4 = z^4$.

In 1770 Euler published a proof of FLT for $n = 3$, although the proof is now considered incomplete because one step involving the divisibility properties of integers of a special form was done without sufficient justification. Gauss also gave a proof for $n = 3$ using the quadratic field $\mathbb{Q}(\sqrt{-3})$, that was not published until after his death. In 1825 Legendre and Dirichlet proved the case of exponent 5, and in 1843 Lamé and Lebesgue solved the case $n = 7$.

While this special cases were being studied, Sophie Germain proved the first result that involved a general kind of primes.

2.1 The relations of Barlow and Abel

A natural way to attack the Fermat equation is to assume that there exist integers x, y, z different from 0 and satisfying the equation $x^p + y^p + z^p = 0$. And then try to derive relations involving these numbers x, y, z and p to reach a contradiction. The first idea to work with the equation is to factorize it as

$$x^n = x^n + y^n = (x + y)(x^{n-1} - x^{n-1}y + x^{n-2}y^2 - \cdots + y^{n-1}).$$

Note that $\frac{x^p+y^p}{x+y}$ is an integer and it is certainly of importance to study its divisibility properties. By this reason, we name the expression

$$Q_n(a, b) = \sum_{k=0}^{n-1} a^k(-b)^{n-k-1}, \quad a, b \in \mathbb{Z}.$$

Note that if $a + b \neq 0$ and n is odd then $Q_n(a, b) = \frac{a^n+b^n}{a+b} \in \mathbb{Z}$.

Barlow discovered in 1810 the following relations concerning the solutions x, y, z of the Fermat equation. These were also found later in 1823 by Abel. This relations were very useful in the future intents to prove the theorem. First see a property of the integer $Q_n(a, b)$.

Lemma 2.1. *If a and b are coprime with n then* $\gcd(Q_n(a,b), a+b) = \gcd(n, a+b)$.

Proof. Let d be a divisor of $a+b$, note that $a \equiv -b \pmod{d}$ and $Q_n(a,b) \equiv na^{n-1} \pmod{d}$. Since a is coprime with n, $d \mid n$ if and only if $d \mid Q_n(a,b)$. Therefore the $\gcd(Q_n(a,b), a+b)$ coincides with the $\gcd(n, a+b)$.

□

Proposition 2.1. *If $x^p + y^p + z^p = 0$ with $p \neq 2$ and $p \nmid z$, then there exist t and t_1 such that*

$$x + y = t^p, \quad \frac{x^p + y^p}{x+y} = t_1^p, \quad z = -tt_1.$$

Moreover, $p \nmid tt_1$, $\gcd(t, t_1) = 1$.

Proof. First observe that $p \nmid x+y$. By Fermat's theorem we have that $0 = x^p + y^p + z^p \equiv x + y + z \pmod{p}$ and then if p divides $x+y$ it also will divide z. Using the previous lemma we get that $\gcd(Q_p(x,y), x+y) = 1$. Now use the factorization of $(-z)^p$ as $Q_p(x,y)(x+y)$. Since we have unique factorization and $Q_p(x,y)$ and $x+y$ have non common factors, then there exist $t, t_1 \in \mathbb{Z}$ with $\gcd(t, t_1) = 1$ such that

$$x + y = t^p, \quad Q_p(x,y) = \frac{x^p + y^p}{x+y} = t_1^p.$$

Observe that $t^p t_1^p = (tt_1)^p = (x+y)Q_p(x,y) = (-z)^p$ therefore $tt_1 = -z$. □

Now suppose that we have x, y, z with $p \nmid xyz$ and $x^p + y^p + z^p = 0$. If we apply the previous proposition to y, z and z, x we get $t, r, s, t_1, r_1, s_1 \in \mathbb{Z}$ such that they satisfy the Barlow and Abel relations:

$$\begin{aligned}
x + y = t^p, &\qquad \frac{x^p + y^p}{x+y} = t_1^p, &\qquad z = -tt_1,\\
y + z = r^p, &\qquad \frac{y^p + z^p}{y+z} = r_1^p, &\qquad x = -rr_1,\\
z + x = s^p, &\qquad \frac{z^p + x^p}{z+x} = s_1^p, &\qquad y = -ss_1.
\end{aligned}$$

2.2 Sophie Germain

Germain's work led to Fermat's Last Theorem being broken into two cases:

> *First case*: $x^p + y^p = z^p$ has no integer solutions for which x, y, and z are relatively prime to p, i.e. in which none of x, y, and z are divisible by p.

> *Second case*: $x^p + y^p = z^p$ has no integer solutions for which one and only one of the three numbers is divisible by p.

Her theorem, brought by Legendre in an 1823 paper to the French Academy of Sciences, was greeted with great admiration.

Theorem 2.1 (Sophie Germain)**.** *Let p and q be odd primes satisfying:*

1. *p is not a p^{th} power residue* $\bmod q$.
2. *If x, y, z satisfy $x^p + y^p + z^p \equiv 0 \pmod q$ then q must divide one of x, y or z.*

Then first case of Fermat Last Theorem is true for p.

Proof. We assume that there exist x, y, z all coprime that are solution of the Fermat equation. By hypothesis 2, q divides x y or z. Suppose that $q \mid x$.

By the Barlow and Abel relations we have that

$$2x = -r^p + s^p + t^p \implies -r^p + s^p + t^p \equiv 0 \pmod q.$$

Again using 2 we have that $q \mid rst$. If $q \mid t$ then $q \mid x + y$ and so $q \mid y$. Similarly, if $q \mid s$ then $q \mid z + x$ and so $q \mid z$. Both cases are not possible because x, y and z are relatively prime. Therefore q divides r.

Now,

$$y + z = r^p \implies y \equiv -z \pmod q \implies y^p \equiv (-z)^p \pmod q \implies$$
$$y^p \equiv x^p + y^p = (x + y)Q_p(x, y) \pmod q \implies y^p \equiv xt_1^p + yt_1^p \equiv yt_1^p \pmod q \implies$$
$$y^{p-1} \equiv t_1^p \pmod q.$$

Moreover,

$$r_1^p = \frac{y^p + z^p}{y + z} = y^{p-1} - y^{p-2}z + \cdots + z^{p-1}$$

Since we have that $y \equiv -z \pmod q$ then $r_1^p \equiv pt_1^p \pmod q$. Let $t' \in \mathbb{Z}$ be the integer such that $t't_1 \equiv 1 \pmod q$ (this is possible because $q \nmid t_1$). Then, $(t'r_1)^p \equiv pt'^p t_1^p \equiv p \pmod q$. So we have found an pth power that is congruent to p modulo q, fact that contradicts with hypothesis 2. □

Theorem 2.2 (Sophie Germain)**.** *If p is an odd prime and $q = 2p+1$ is also prime, then first case of Fermat's Last Theorem is true for p.*

Proof. Let's see that p and q satisfy both hypothesis of the previous theorem. For the first one, suppose that there exist some $a \in \mathbb{Z}$ such that $p \equiv a^p \pmod{q}$. If we compute the Legendre symbol of $\left(\frac{a}{q}\right)$ we can observe that,

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

using Fermat's little theorem. Since $q = 2p + 1$, this is not possible so we get a contradiction. Now, for the second hypothesis let's suppose that there exist x, y, z such that $x^p + y^p + z^p \equiv 0 \pmod{q}$ and that $q \nmid xyz$. Since x, y, z are all coprime to q, Fermat's little theorem says that

$$\begin{aligned}
x^{q-1} \equiv 1 \pmod{q} &\implies x^p = x^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}, \\
y^{q-1} \equiv 1 \pmod{q} &\implies y^p = y^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}, \\
z^{q-1} \equiv 1 \pmod{q} &\implies z^p = z^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}.
\end{aligned}$$

And now we get a contradiction with the Fermat equation modulo q, since

$$0 \equiv x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \pmod{q}.$$

□

Germain actually proved much more than Theorem 2.2. She showed that if $a^p \not\equiv 2 \pmod{q}$ for all a and the auxiliary prime q is of the form $4p + 1$, $8p + 1$, $10p + 1$, $14p + 1$, or $16p + 1$, then condition 2 of her theorem holds. She then examined the exceptional cases where there is some $a^p \equiv 2 \pmod{q}$, and found the auxiliary primes of the form $2np + 1$ satisfying condition 2 for all n such that $1 \leq n \leq 10$ and all odd prime exponents $p \leq 100$. She also showed that all of these auxiliary primes found satisfy condition 1.

In his 1823 paper, Legendre, using different techniques than Germain, showed that conditions 1 and 2 hold whenever p is a prime and $4p + 1$, $8p + 1$, $10p + 1$, $14p + 1$, or $16p + 1$ is also a prime.

Germain and Legendre collectively showed that all odd prime exponents $p < 197$ satisfy First case of Fermat's Last Theorem, by explicitly finding an auxiliary prime

$q = 2np+1$ that satisfies Sophie Germain's theorem. See [15] for a table listing these auxiliary primes. This result was a large leap forward, even if it only showed that one of two cases holds true. Recall that previously, proofs had only been known for the exponents 3 and 4. Even a partial result relating to so many different primes was impressive.

2.3 Terjanian's theorem for even exponents

The best approximation of FLT concerning even exponents was published by Terjanian in 1977. It is quite surprising that his proof requires only very elementary considerations, nevertheless it covers the first case of FLT for all even exponents.

Clearly, if suffices to consider the exponent $2p$, where p is a odd prime. The equation that solved Terjanian and we will see is

$$x^{2p} + y^{2p} = z^{2p}, \quad 2p \nmid xyz.$$

Let's begin with some previous results:

Lemma 2.2. *Let y and z be different integers:*

1. *If $m = nq + r$, $0 \leq r < n < m$, then*

$$Q_m(z, -y) = z^r Q_q(z^n, -y^n) Q_n(z, -y) + y^{m-r} Q_r(z, -y).$$

2. *If $m = nq - r$, $0 \leq r < n < m$, then*

$$Q_m(z, -y) = (z^{n-r} Q_{q-1}(z^n, -y^n) + y^{m-n}) Q_n(z, -y) - y^{m-n} z^{n-r} Q_r(z, -y).$$

3. *If z and y are coprime odd integers, $z \equiv y \pmod 4$ and m is odd then*

$$Q_m(z, -y) \equiv m \pmod 4$$

and in particular $Q_m(z, -y)$ is odd.

4. *If z and y are coprime, $z \equiv y \pmod 4$ and m, n are odd, then*

$$\left(\frac{Q_m(z, -y)}{Q_n(z, -y)}\right) = \left(\frac{m}{n}\right)$$

where $\left(\frac{m}{n}\right)$ is the Jacobi symbol [1].

[1] If m, n are nonzero relatively prime integers, n odd, $n \geq 3$, the Jacobi symbol $\left(\frac{m}{n}\right)$ is defined $\left(\frac{m}{n}\right) = 1$ when m is a square modulo n and $\left(\frac{m}{n}\right) = -1$ otherwise.

Proof. Properties (1) and (2) follow from the definitions. For (3), let $z = y + 4t$. Then,

$$Q_m(z,-y) = \frac{(y+4t)^m - y^m}{4t} = \binom{m}{1}y^{m-1} + \binom{m}{2}y^{m-2}4t + \cdots \equiv my^{m-1} \equiv m \pmod 4.$$

(4) The assertion is proved by induction on $m+n$. It is trivial when $n = m = 1$. Let $m + n > 2$. If $m > n$, then there exists an integer r odd, $0 < r < n$ and q such that $m = qn + r$ or $m = qn - r$. In the first case, $m - r$ is even so by (1)

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{y^{m-r}Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{Q_r(z,-y)}{Q_n(z,-y)}\right).$$

Since $r + n < m + n$, by induction

$$\left(\frac{Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{r}{n}\right) = \left(\frac{m}{n}\right).$$

In the second case, $m - n$ and $n - r$ are even, so by (2)

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-y^{m-n}z^{n-r}Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-1}{Q_n(z,-y)}\right)\left(\frac{Q_r(z,-y)}{Q_n(z,-y)}\right).$$

Again by induction,

$$\left(\frac{-1}{Q_n(z,-y)}\right)\left(\frac{Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-1}{Q_n(z,-y)}\right)\left(\frac{r}{n}\right).$$

I claim that in fact $\left(\frac{-1}{Q_n(z,-y)}\right) = \left(\frac{-1}{n}\right)$. Indeed, by (3), $Q_n(z,-y) \equiv n \pmod 4$ and

$$\frac{Q_n(z,-y)-1}{2} \equiv \frac{n-1}{2} \pmod 2.$$

By quadratic reciprocity,

$$\left(\frac{-1}{Q_n(z,-y)}\right) = (-1)^{\frac{Q_n(z,-y)-1}{2}} = (-1)^{\frac{n-1}{2}} = \left(\frac{-1}{n}\right).$$

Thus

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-1}{n}\right)\left(\frac{r}{n}\right) = \left(\frac{m}{n}\right).$$

□

Theorem 2.3 (Terjanian)**.** *If x, y and z satisfy $x^{2p} + y^{2p} = z^{2p}$ for some odd prime p, then $2p \mid xy$.*

Proof. Note that x and y cannot be odd at the same time because if they were, $z^{2p} = x^{2p} + y^{2p} \equiv 1 + 1 \equiv 2 \pmod 4$ and 2 is not a square modulo 4. Let's suppose that x is even and y, z are odd. Then,

$$x^{2p} = z^{2p} - y^{2p} = (z^2 - y^2)\frac{z^{2p} - y^{2p}}{z^2 - y^2}$$

and there appears the element we defined before $Q_p(z^2, -y^2) = \frac{z^{2p}-y^{2p}}{z^2-y^2}$. By lemma 2.1, the gcd of $Q_p(z^2, -y^2)$ and $z^2 - y^2$ coincides with the gcd of p and $z^2 - y^2$ and it only can be p or 1. Note that if the gcd is p, then p divides x^{2p} therefore p divides x and since x is even, $2p$ divides x, so we are done.

Let's see that $Q_p(z^2, -y^2)$ and $z^2 - y^2$ are not coprime. Since p is not a square, there exists some prime q such that p is not a square modulo q, i.e. $\left(\frac{p}{q}\right) = -1$. On the other hand note that

$$x^{2p} = z^{2p} - y^{2p} = (z^2 - y^2)Q_p(z^2, -y^2).$$

If they are coprime, then both are squares and for any $m \in \mathbb{Z}$, $m \neq Q_p(z^2, -y^2)$, in particular $Q_p(z^2, -y^2)$ is a square modulo $Q_q(z^2, -y^2)$. Observe that $z^2 \equiv y^2 \pmod 4$ since they both are odd, so by the previous lemma,

$$1 = \left(\frac{Q_p(z^2, -y^2)}{Q_q(z^2, -y^2)}\right) = \left(\frac{p}{q}\right) = -1.$$

□

Fermat's Last Theorem for regular primes

3.1 Introduction

This chapter is devoted to Kummer's proof of Fermat's Last Theorem for a large class of prime number exponents p which are now known as the regular primes.

The first idea which has been used in the earlier chances to prove FLT is to express x^p+y^p as a product of integer factors which are pairwise relatively prime and therefore must themselves be pth powers, using unique prime factorization. Gabriel Lamé did make the breakthrough in attempting to decompose x^p+y^p using pth roots of 1 as

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

Lamé presented a proof in March of 1847 using this fact while assuming incorrectly that this was a unique decomposition into prime ideals. A few years before this, Kummer had already discovered that such unique factorization properties did not necessarily hold in the fields $\mathbb{Q}(\zeta_p)$ generated by these roots of unity. A few weeks after Lamé presented the incorrect proof, Kummer wrote a correct proof for a certain set of primes which had a property allowing for unique factorization to work in the step of Lamé's proof that went wrong.

All the work for Kummer was to give some sense to the field $\mathbb{Q}(\zeta_p)$ and of what are the integers in this field. Following the model of ordinary arithmetic, he could define a notion of divisibility and look for the integers which are prime. Here is where Lamé didn't realize that it is false, in general, that if α is a prime and α divides $\beta\gamma$ then $\alpha \mid \beta$ or $\alpha \mid \gamma$. And the fact is that if the cyclotomic integers had unique factorization in prime elements, then this would imply the property above.

To fix this, Kummer invented certain "ideal numbers" such that for these numbers, unique factorization holds, and then the factors would become pth powers of these ideal numbers.

We must first describe general notation and some basic facts on arithmetic of cyclotomic fields. Later on we will see how this ideas make a proof of FLT for a large class of prime exponents.

3.2 Arithmetic of cyclotomic fields

For any odd prime p, we denote a primitive pth root of unity as ζ_p, i.e. $\zeta_p \in \mathbb{C}$ has the property that $\zeta_p^k \neq 1$ for any $1 \leq k \leq p-1$ while $\zeta_p^p = 1$. It, along with all of its powers, is a root of the polynomial $X^p - 1$, hence it satisfies the equation $x^p = 1$, the motivation for its name. To find its minimal polynomial, we can factor $X^p - 1 = (X-1)\Phi(X)$ where

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

This is called the pth cyclotomic polynomial as it is the minimal polynomial for ζ_p. Note that the other pth roots of unity are powers of ζ_p, and are all roots of $\Phi_p(X)$ (except for $\zeta_p^p = 1$).

We can also talk about the field generated by pth roots of unity over $\mathbb{Q}$ known as the pth cyclotomic field. Note that this field, denoted $K = \mathbb{Q}(\zeta_p)$, is automatically the splitting field for $\Phi_p(X)$ over $\mathbb{Q}$ as we have seen before that the rest of the roots are just subsequent powers of ζ_p. This extension has degree $p-1$, coinciding with the degree of $\Phi_p(X)$.

One of the most fundamental properties of cyclotomic fields in terms of basic algebraic number theory is that its ring of integers is easy to describe.

Proposition 3.1. *We have*

$$\mathcal{O}_K = \mathbb{Z}[\zeta_p].$$

Galois groups of cyclotomic fields are similarly easy to handle.

Proposition 3.2. *The Galois group of $K|\mathbb{Q}$ is*

$$\mathrm{Gal}(K|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

with the isomorphism $(\sigma : \zeta \longrightarrow \zeta^a) \longmapsto a$.

Now let's focus on how are the elements of K. First we can observe the fact that $(1-\zeta) = (1-\zeta^i)$ is an equality of ideals for $1 \leq i \leq p-1$. This is evident because one can show that their quotient is a unit. Now, let's see how the ideal generated by p decomposes in prime ideals of $\mathcal{O}_K$.

Proposition 3.3. *Only the prime p ramifies in K, and*

$$p\mathcal{O}_K = (1-\zeta)^{p-1}\mathcal{O}_K$$

with $(1-\zeta)\mathcal{O}_K$ a prime ideal. Thus p is totally ramified in K.

Proof. Since the minimal polynomial of ζ_p is $\Phi_p(X) = \frac{X^p-1}{X-1}$, as a polynomial in $K[X]$, it can be decomposed as

$$\Phi_p(X) = \prod_{i=0}^{p-1}(x - \zeta_p^i)$$

Note that if we plug in $X = 1$ to $\Phi_p(X)$ we get from the polynomial in $\mathbb{Q}[X]$ and the polynomial in $K[X]$ that

$$p = \prod_{i=0}^{p-1}(1 - \zeta_p^i).$$

Note that $1 - \zeta_p$ is a unit away from $1 - \zeta_p^i$, i.e. $1 - \zeta_p^i = u(1 - \zeta_p)$ where u is the cyclotomic unit $\frac{\zeta_p^i-1}{\zeta_p-1}$. Thus we have an equality of ideals $(1 - \zeta_p) = (1 - \zeta_p^i)$. This, combined with the decomposition of p gives us $(p) = (1-\zeta_p)^{p-1}$. Furthermore, since $[K : Q] = p - 1$, from algebraic number theory we know that (p) can have at most $p - 1$ factors, hence the previous decomposition of (p) is in fact a prime decomposition, so we also get that $(1 - \zeta_p)$ is a prime ideal in $\mathcal{O}_K$. □

For simplify notation, we denote $\mathfrak{p}$ the ideal generated by $1 - \zeta$.

3.3 First case of FLT for regular primes

Like any other ring, $\mathcal{O}_K$ has ideals, and one property is that the ring of integers for any field K is a Dedekind domain, a type of integral domain with the added property that any ideal decomposes uniquely into a product of prime ideals. It is not necessarily true, however, that the elements of a Dedekind domain decompose uniquely into a prime or irreducible elements. Nevertheless, we can see that if all the ideals of a given $\mathcal{O}_K$ are principal, then the unique decomposition of prime ideals would give way to unique prime factorization of elements, as the factorization of any element $\alpha \in \mathcal{O}_K$ would be characterized by the decomposition of the ideal (α) into prime ideals generated by single irreducible elements. This motivates the construction of the ideal class group of K which is, loosely speaking, the quotient group of all the ideals in $\mathcal{O}_K$ modulo the principal ideals of $\mathcal{O}_K$. We are very lucky to find that this group is always finite, and in fact, when the order is 1, we are in the previously described case of all ideals of $\mathcal{O}_K$ are principal. The class number of K, denoted h_K is the order of this ideal class group, hence if $h_K = 1$, $\mathcal{O}_K$ has unique prime factorization of elements. If $h_K > 1$, then $\mathcal{O}_K$ does not have unique prime factorization.

The property of whether a prime p is regular can be characterized based on the class number of $K = \mathbb{Q}(\zeta_p)$. As described above, we think of the class number as a scalar quantity describing how close elements of $\mathcal{O}_K$ are to having unique factorization, but explicitly the class number h_K is the order of the ideal class group.

Definition 3.1. *A odd prime p is called regular if the class group of $K = \mathbb{Q}(\zeta_p)$ has no p-torsion, i.e. the class number h_K is prime to p.*

The usefulness for proving Fermat's last theorem of this assumption comes from the following easy fact: if an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is such that $\mathfrak{a}^p$ is a principal ideal, then so is $\mathfrak{a}$ itself.

We are now ready to present the proof when $p \nmid xyz$, also known as the first case of Fermat's last theorem for regular primes.

Theorem 3.1 (Kummer)**.** *Let p be a regular prime. If there is a non-trivial integer solution to*

$$x^p + y^p = z^p$$

then $p \mid xyz$.

A fact about the cyclotomic field K will need to be assembled before we can do the main proof of the theorem.

Lemma 3.1. *Let $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ the maximal real subfield of K. Then all unit of $\mathcal{O}_K$ is the product of a unit of $\mathcal{O}_{K^+}$ and a primitive pth root of unity.*

Proof. Suppose that u is a unit of $\mathcal{O}_K$ and consider the element $v := u/\overline{u}$ where $\overline{u}$ is the complex conjugate of u. Since complex conjugation belongs to $\mathrm{Gal}(K|\mathbb{Q})$, which is abelian, it commutes with all elements of $\mathrm{Gal}(K|\mathbb{Q})$. Thus if $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ we have

$$\sigma(v) = \sigma(u)/\sigma(\overline{u})$$

hence $|\sigma(v)| = 1$. Thus v is an algebraic integer all of whose conjugates have absolute value equal to 1. By Kronecker's theorem we deduce that it is a root of unity (see [3] Proposition 3.3.9 for Kroneker's theorem). □

Now we are capable to proof Kummer's theorem on the 1st case for FLT.

Proof. Since the case $p = 3$ it's already proved, we can suppose that $p \geq 5$. Let's take a solution x, y, z of the Fermat equation such that they are not divisible by p and pairwise coprime.

If we suppose that $x \equiv y \equiv -z \pmod{p}$, then we obtain that $z^p = x^p + y^p \equiv -2z^p \pmod{p}$, so p divides $3z$ and since $p \geq 5$ it is a contradiction with the fact that $p \nmid z$.

Therefore $x, y, -z$ can't be equivalent modulo p. So we can suppose for example that $x \not\equiv y \pmod{p}$.

We consider the usual factorization

$$x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y).$$

Observe that the ideals $(x + \zeta^i y)$ are coprime for all i: indeed if some prime ideal $\mathfrak{q}$ divides $(x + \zeta^i y)$ and $(x + \zeta^j y)$ for $i \neq j$, it divides also $(\zeta^i - \zeta^j)y$ and $(\zeta^j - \zeta^i)x$, hence $(\zeta^j - \zeta^i)$. Thus $\mathfrak{q} = (1-\zeta)\mathcal{O}_K$, so that since $\mathfrak{q} \mid z^p$, then $(1-\zeta)^p \mid z^p$ and then $(1-\zeta)^p \mid z$. therefore $p \mid z$ contrary to our hypothesis.

We thus have a product of pairwise coprime ideals that is equal to the pth power of an ideal, so that each of them is a pth power. Thus for each j we have $(x+\zeta^j y)\mathcal{O}_K = \mathfrak{a}_j$ for some ideal $\mathfrak{a}_j$. Now we use the hypothesis that p is regular. For all j, the ideal $\mathfrak{a}_j$ is principal, and since p doesn't divide the number of classes h_K, the ideal $\mathfrak{a}_j$ is itself is a principal ideal, say $\mathfrak{a}_j = \alpha_j \mathcal{O}_K$. In particular, there exist units $u_j \in \mathcal{O}_K^\times$ such that $x + \zeta^j y = u_j \alpha_j^p$ for all j.

We focus on the case of $j = 1$ and write $\alpha := \alpha_1$. Observe that

$$\overline{u_1 \alpha}^p = \overline{x + \zeta y} = x + \zeta^{-1} y.$$

By the lemma 3.1 the quotient $u/\overline{u}$ is a root of unity, it is of the form $\pm\zeta^i$ for some i so

$$x + \zeta y = u_1 \alpha^p = \pm\zeta^i \overline{u_1} \alpha^p.$$

On the other hand, we can write the element α as the sum $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$. Taking the pth power we obtain

$$\alpha^p \equiv a_0^p + a_1^p \zeta^p + \cdots + a_{p-2}^p \zeta^{(p-2)p} \equiv a_0 + \cdots + a_{p-2} \pmod{p\mathcal{O}_K}.$$

Thus $\alpha^p \equiv \overline{\alpha}^p \pmod{p\mathcal{O}_K}$ hence

$$x + \zeta y = u_1 \alpha^p = \pm\zeta^i \overline{u_1} \alpha^p \equiv \pm\zeta^i \overline{u_1 \alpha}^p = \pm\zeta^i (x + \zeta^{-1} y) \pmod{p\mathcal{O}_K}.$$

Finally we get

$$x + \zeta y \pm \zeta^i (x + \zeta^{-1} y) \in p\mathcal{O}_K.$$

Now let's see what value can take i and we'll get a contradiction in all of the possible cases. First if $3 \leq i \leq p-1$, and since $p \geq 5$, we have a lineal combination of elements of $\{1, \zeta, \ldots \zeta^{p-1}\}$ which is 0 in $\mathcal{O}_K/p\mathcal{O}_K$, hence all the coefficients are in $p\mathcal{O}_K$. This contradicts the fact that $p \not| xy$. Second, suppose that $i = 2$, then

$$x + \zeta y \pm \zeta^2 x \pm \zeta y \in p\mathcal{O}_K$$

and by the same argument above we can deduce that $p \mid x$. If $i = 0$,

$$x + \zeta y \pm x \pm \zeta^{p-1} y \in p\mathcal{O}_K$$

and then $p \mid y$. Finally the only case remaining is $i = 1$. Choosing the sign we get two possibilities

$$x + \zeta y + x\zeta + y = (x + y)(1 + \zeta) \in p\mathcal{O}_K,$$
$$x + \zeta y - x\zeta - y = (x - y)(1 - \zeta) \in p\mathcal{O}_K.$$

For the first one, since $1 + \zeta$ is a unit, $p \mid x + y$ and then

$$x + y \equiv 0 \pmod{p} \implies 0 \equiv x^p + y^p \equiv z^p \pmod{p} \implies p \mid z.$$

For the second one, since $p\mathcal{O}_K = (1 - \zeta)^{p-1}\mathcal{O}_K$, $x - y \in (1 - \zeta)^{p-2}\mathcal{O}_K$, but since $x - y \in \mathbb{Z}$, $x - y \in (1 - \zeta)^{p-2}\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$. Then p divides $x - y$ so $x \equiv y \pmod{p}$ contradicting the hypothesis that we made at the beginning of the proof. □

3.4 Second case of FLT for regular primes

The proof from this section is the reformulation of Kummer's original proof for the second case in modern language. This proof uses the same main argument as the first case, but also involves the method of infinite descent in which a contradiction is reached by showing that if there is one *smallest* counterexample, then we can continue to construct *smaller* counterexamples ad infinitum.

The following lemma allow us to relate the units in $\mathcal{O}_K$ with the rational integers in $\mathbb{Z}$.

Lemma 3.2. *Let p be a regular prime. If ε is a unit of $\mathcal{O}_K$ and $\varepsilon \equiv n \pmod{p}$, with n an integer, then ε is a pth power of some unit $u \in \mathcal{O}_K^\times$.*

Proof. Suppose ε is not a pth power, then we consider the field extension $L = K(\varepsilon^{1/p})$. Observe that the polynomial $f(X) = X^p - \varepsilon$ is irreducible: indeed if there is a polynomial of degree $k < p$ in $K[X]$ such that his roots are $\varepsilon^{1/p}\zeta^i$, then the coefficient of degree $k - 1$ is the sum of all roots of such polynomial. Since $\varepsilon^{1/p} \notin K$, the sum of the pth roots of unity must be 0, what contradicts the fact that the sum of less than $p - 1$ roots of units can't be 0 because they are linearly independent in K. So we can conclude that the extension $L|K$ is of degree p.

We will see that the extension $L|K$ is everywhere unramified. By class field theory, this extension must be contained in the Hilbert class field of K, which it's well known that is of degree h_K. Then the degree of $L|K$ has to divide h_K, contrary to the assumption that p is a regular prime.

We can suppose without lose of generality that $\varepsilon \equiv 1 \pmod{p}$. Note that

$$\varepsilon^{p-1} \text{ is a } p\text{th power } \iff \varepsilon \text{ is a } p\text{th power of a unit.}$$

Then taking the $p-1$ power of ε we get that $\varepsilon^{p-1} \equiv n^{p-1} \equiv 1 \pmod{p}$ and can suppose that $\varepsilon \equiv 1 \pmod{p}$.

Now let's see that $\varepsilon \equiv 1 \pmod{(1-\zeta)^p}$. Using the fact that any element of $\mathcal{O}_K$ can be seen as an integer modulo $(1-\zeta)$, we have that

$$\varepsilon = 1 + \alpha p = 1 + (a + x(1-\zeta))p = 1 + ap + x'(1-\zeta)^p, \quad \alpha, x, x' \in \mathcal{O}_K, a \in \mathbb{Z}.$$

If we compute the norm,

$$\pm 1 = N(\varepsilon) \equiv N(1+ap) \pmod{(1-\zeta)^p}.$$

Since $1 + ap \in \mathbb{Z}$, the norm coincides with the $p-1$th power. Reducing modulo $(1-\zeta)^p$ it only remains

$$\pm 1 \equiv N(1+ap) \equiv 1 + (p-1)ap \equiv 1 - ap \pmod{(1-\zeta)^p},$$

because $(1-\zeta)^p \mid p^2$. If $N(\varepsilon) = -1$ then $2 \equiv ap \pmod{(1-\zeta)^p}$ so $p \mid 2$. So we must have $N(\varepsilon) = 1$ and then we obtain

$$0 \equiv ap \pmod{(1-\zeta)^p} \implies \varepsilon \equiv 1 \pmod{(1-\zeta)^p}.$$

Consider now the polynomial $f(X) = \dfrac{((1-\zeta)X - 1)^p + \varepsilon}{(1-\zeta)^p}$. Note that in fact $f(X)$ is a monic polynomial with coefficients in $\mathcal{O}_K$, indeed

$$\frac{(1-\zeta)^p}{(1-\zeta)^p} \in \mathcal{O}_K, \quad \frac{\binom{p}{k}(1-\zeta)^k}{(1-\zeta)^p} \in \mathcal{O}_K \text{ if } 1 < k < p-1\ , \quad \frac{-1+\varepsilon}{(1-\zeta)^p} \in \mathcal{O}_K.$$

Moreover, the roots of $f(X)$ are $\dfrac{1-\zeta^i\varepsilon^{1/p}}{1-\zeta}$ with $1 \le i \le p$. So f generates the same extension $L|K$. Recall that the discriminant of f is the product of the square of the difference of the roots, so

$$\Delta(f) = \prod_{1 \le i < j \le p} \frac{(\zeta^i - \zeta^j)\varepsilon^{1/p}}{1-\zeta}.$$

Observe that for every i and j, $\frac{(\zeta^i - \zeta^j)}{1-\zeta} \in \mathcal{O}_K^\times$ since $\frac{1-\zeta^k}{1-\zeta} \in \mathcal{O}_K$ for every k. Thus the discriminant is a unit and therefore the extension $L|K$ is everywhere unramified. By the argument above we get a contradiction and therefore ε must be a pth power.

Finally note that if ε is a pth power of an element in $\mathcal{O}_K$, it must be of a unit since ε is already a unit.

□

We now begin the proof of 2nd case of FLT for regular primes. We will use Fermat's method of infinite descent. For this to work we need to study an equation that will descend to itself, so we will prove a stronger result.

Theorem 3.2 (Kummer)**.** *Let p be a regular prime and $K = \mathbb{Q}(\zeta)$ with ζ a primitive pth root of unity. There is no non-trivial solution of the equation*

$$z^p + y^p = \varepsilon z^p$$

with $x, y, z \in \mathcal{O}_K$, $\varepsilon \in \mathcal{O}_K^\times$ and such that $\mathfrak{p} \nmid x, y$ and $\mathfrak{p} \mid z$.

Proof. We will start with a solution of the equation that is minimal in $v_\mathfrak{p}(z)$. So suppose that there exist $x, y, z \in \mathcal{O}_K$ and $\varepsilon \in \mathcal{O}_K^\times$ that satisfy the Fermat equation with $\mathfrak{p} \mid z$ and $\mathfrak{p} \nmid x, y$.

We again use the factorization

$$\prod_{i=0}^{p-1}(z + \zeta^i y) = \varepsilon z^p.$$

Define the ideals $\mathfrak{a}_i = (x + \zeta^i y)\mathcal{O}_K$ for $0 \leq i \leq p-1$. Let's see that there is some i such that $\mathfrak{p}^2 \mid \mathfrak{a}_i$.

The ideas that we used in the proof of first case here don't work since the ideals are not necessarily coprime, but we can compute it's gcd and modify a little bit the idea.

I claim that for every $i \neq j$, the gcd of $\mathfrak{a}_i$ and $\mathfrak{a}_j$ is $\mathfrak{p}(x, y)$. Note that $\mathfrak{p}$ divides at least one of the factors of the factorization, and then, one of the ideals $\mathfrak{a}_k$. Moreover, since x and y aren't in $\mathfrak{p}$, if $\mathfrak{p}$ divides one of $(x + \zeta^i y)$, it divides to all. So $\mathfrak{p} \mid \mathfrak{a}_i$ for all i. Conversely, a common divisor $\mathfrak{d}$ of two ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ satisfies

$$x + \zeta^i y - (x + \zeta^j y) = (\zeta^i - \zeta^j)y \in \mathfrak{d} \implies (1 - \zeta)y \in \mathfrak{d},$$

$$x + \zeta^i y - \zeta^{i-j}(x + \zeta^j y) = (1 - \zeta^{i-j})x \in \mathfrak{d} \implies (1 - \zeta)x \in \mathfrak{d}.$$

Thus $\mathfrak{d} \mid \mathfrak{p}(x, y)$ and then the gcd of all the ideals $\mathfrak{a}_i$ is $\mathfrak{p}(x, y)$. We can write then $\mathfrak{a}_i = \mathfrak{p}(x, y)\mathfrak{c}_i$ with $\mathfrak{c}_i$ pairwise coprime ideals. Moreover,

$$\prod_{i=0}^{p-1} \mathfrak{a}_i = \mathfrak{p}^p(x, y)^p \prod_{i=0}^{p-1} \mathfrak{c}_i = (z)^p.$$

Since $\mathfrak{c}_i$ are pairwise coprime, by the relation above, every $\mathfrak{c}_i$ must be a pth power of an ideal in $\mathcal{O}_K$, say $\mathfrak{b}_i$.

Let $k := v_\mathfrak{p}(z)$, let's see that $k \geq 2$. A integral basis of $\mathcal{O}_K$ can be also $1-\zeta$ so all the elements in $\mathcal{O}_K/\mathfrak{p}^2$ can be written as $a_0 + a_1(1-\zeta)$ with $a_1, a_1 \in \mathbb{Z}$. Observe then that for any $0 \leq i \leq p-1$, $x+\zeta^i y$ is congruent to $a_0(1-\zeta)$ modulo $\mathfrak{p}^2$ for some $a_0 \in \mathbb{Z}$;

$$\mathfrak{p} \mid x+\zeta^i y \implies x+\zeta^i y \equiv (1-\zeta)(a_0+a_1(1-\zeta)) \equiv a_0(1-\zeta) \pmod{\mathfrak{p}^2}.$$

Note that if $x+\zeta^i y \equiv x+\zeta^j y \pmod{\mathfrak{p}^2}$ then $(\zeta^i-\zeta^j)y \equiv 0 \pmod{\mathfrak{p}^2}$ and so $\mathfrak{p} \mid y$ contrary to the assumption of $\mathfrak{p} \nmid x, y$, so all the elements $x+\zeta^i y$ define different classes in $\mathcal{O}_K/\mathfrak{p}^2$. Since $0 \leq i \leq p-1$, there is some b such that $b \equiv 0 \pmod{p}$ so $b(1-\zeta) \equiv 0 \pmod{\mathfrak{p}^2}$ i. e. $\mathfrak{p}^2 \mid x+\zeta^i y$ for some i, which tells us that k must be strictly greater than 1.

From above, since $(z)^p = \mathfrak{p}^p(x,y)^p \prod_{i=0}^{p-1} \mathfrak{b}_i^p$, one of the $\mathfrak{b}_i$ is a multiple of $\mathfrak{p}$. Suppose that $\mathfrak{p}^2 \mid x+\zeta^i y$, then we can obtain another solution

$$x^p + (\zeta^i y)^p = \varepsilon z^p$$

with $x, y' = \zeta^i y, z \in \mathcal{O}_K$ and now $\mathfrak{p}^2 \mid x+y'$. So we can suppose from the beginning that $\mathfrak{p}^2 \mid x+y$ and therefore $\mathfrak{p}$ is coprime with all $\mathfrak{b}_i$ except for $\mathfrak{b}_0$. In this case $v_\mathfrak{p}(\mathfrak{b}_0) = k-1$.

Now take the fractional ideal $\left(\frac{x+\zeta y}{x+y}\right)$ and observe that

$$\left(\frac{x+\zeta y}{x+y}\right) = \frac{\mathfrak{p}\mathfrak{a}\mathfrak{b}_1^p}{\mathfrak{p}\mathfrak{a}\mathfrak{b}_0^p} = \frac{\mathfrak{b}_1^p}{\mathfrak{b}_0^p} = \left(\frac{\mathfrak{b}_1}{\mathfrak{b}_o}\right)^p.$$

Now, since $p \nmid h_K$ and $\left(\frac{x+\zeta y}{x+y}\right)$ is principal, the ideal $\dfrac{\mathfrak{b}_1}{\mathfrak{b}_0}$ is also principal, i.e there exists some $\alpha_1 \in K$ such that

$$\frac{\mathfrak{b}_1}{\mathfrak{b}_0} = \alpha_1 \mathcal{O}_K,$$

The same argument works for the ideal $\left(\frac{x+\zeta^{-1}y}{x+y}\right)$. And we deduce that there exists some $\alpha_{-1} \in K$ such that

$$\frac{\mathfrak{b}_{-1}}{\mathfrak{b}_0} = \alpha_{-1} \mathcal{O}_K.$$

Therefore there exist units ε_1 and ε_{-1} such that

$$\frac{x+\zeta y}{x+y} = \varepsilon_1 \alpha_1^p, \quad \frac{x+\zeta^{-1} y}{x+y} = \varepsilon_{-1} \alpha_{-1}^p,$$

and they satisfy

$$\varepsilon_1\alpha_1^p + \zeta\varepsilon_{-1}\alpha_{-1}^p = \frac{x+\zeta y+\zeta x+y}{x+y} = \frac{(1+\zeta)(x+y)}{x+y} = 1+\zeta.$$

Multiplying by $(1-\zeta)^{p(k-1)}$ we obtain

$$\varepsilon_1((1-\zeta)^{k-1}\alpha_1)^p + \zeta\varepsilon_{-1}((1-\zeta)^{k-1}\alpha_{-1})^p = (1+\zeta)(1-\zeta)^{p(k-1)}.$$

Note that $(1-\zeta)^{k-1}\alpha_1 \in \mathcal{O}_K$ since we have seen before that $v_{\mathfrak{p}}(\mathfrak{b}_0) = k-1$. Similarly, $(1-\zeta)^{k-1}\alpha_{-1} \in \mathcal{O}_K$. Note also that $\mathfrak{p} \nmid (1-\zeta)^{k-1}\alpha_1$, $(1-\zeta)^{k-1}\alpha_{-1}$ since $\mathfrak{p} \nmid \mathfrak{b}_1, \mathfrak{b}_{-1}$. If we let $x := (1-\zeta)^{k-1}\alpha_1$, $y := (1-\zeta)^{k-1}\alpha_{-1}$ and $z := (1-\zeta)^{k-1}$ then we have a solution of the equation

$$\varepsilon_1 x^p + \zeta\varepsilon_{-1}y^p = (1+\zeta)z^p$$

with $x, y, z \in \mathcal{O}_K$, $\mathfrak{p} \nmid x, y$, $\mathfrak{p} \mid z$ such that $v_{\mathfrak{p}}(z) = k-1$. Dividing the equation by ε_1 we also get

$$x^p + \varepsilon_2 y^p = \varepsilon_3 z^p, \quad \varepsilon_2, \varepsilon_3 \in \mathcal{O}_K^\times.$$

This is not the equation that we had at the beginning of the proof, so in order to complete the infinite descent we only need to obtain a solution of $x^p + y^p = \varepsilon z^p$ with $v_{\mathfrak{p}}(z) < k$ and $\mathfrak{p} \nmid x, y$.

Observe that $\varepsilon_2 y^p = \varepsilon_3 z^p - x^p$, then since $\mathfrak{p}^{(k-1)p} \mid z^p$ we have also $p \mid z^p$ so

$$\varepsilon_2 \equiv -\left(\frac{z}{y}\right)^p.$$

Note that for any algebraic integer $\beta \in \mathcal{O}_K$, $\beta^p \equiv \beta_0 \pmod{p}$ with $\beta_0 \in \mathbb{Z}$. Then $\varepsilon_2 \equiv -\frac{a_1}{a_2} \pmod{p}$ with $a_1, a_2 \in \mathbb{Z}$. Since y is not divisible by p, $a_2 \neq 0 \pmod{p}$. So we can say that

$$\varepsilon_2 \equiv n \pmod{p}, \quad n \in \mathbb{Z}.$$

Kummer's lemma 3.2 then allows us to rewrite ε_2 as a pth power of some unit $u \in \mathcal{O}_K^\times$. Finally, we obtain the solution

$$x^p + (uy)^p = \varepsilon_3 z^p$$

with less valuation of $\mathfrak{p}$ in z than in the original solution, contrary to the fact that the first solution x, y, z was minimal in $v_{\mathfrak{p}}(z)$. This completes the proof for the second case, and thus Fermat's last theorem holds for regular primes.

□

3.5 Regular primes

In 1847 Kummer did not know whether every prime is regular. But in 1850 and 1851, he discovered that 37, 59, 67 are the only irregular primes less than 100. In 1874 he extended his computations up to 164. At that time and based on probabilistic arguments, Kummer advanced the conjecture that asymptotically there should be as many regular as irregular primes.

Today, despite the observed plurality of regular primes, it has not yet been shown that there exist infinitely many regular primes. On the other hand, quite surprisingly, it was proved in 1915 that there are infinitely many irregular primes (see [24], p. 63).

The power of class field theory

In 1912, Furtwängler used class field theory to derive two important criteria about the first case of Fermat's last theorem, As corollaries, he then gave new proofs of the theorems of Wieferich and Mirimanoff.

In this chapter our objective is to proof the Eisenstein reciprocity law. This result will help us to derive some theorems that are related with the first case FLT.

The Eisenstein reciprocity law talks about a relation that satisfies the power residue symbol. To see such result we will start with some background in class field theory and Kummer theory.

4.1 Local reciprocity law and the norm residue symbol

In this section, K will be a local field of characteristic 0, with $\mathcal{O}_K$ the ring of integers and $\mathfrak{p}$ the maximal ideal of $\mathcal{O}_K$. Let p be the characteristic of the residual field $\mathcal{O}_K/\mathfrak{p}$ and $q = \#\mathcal{O}_K/\mathfrak{p}$.

Recall that in local fields, if we have an unramified extension $L|K$ we have that the Galois group of the extension is the Galois group of the residual fields $\ell|\kappa$ which is cyclic and it is generated by the Frobenius automorphism $\varphi_{L|K}$ that sends $x \mapsto x^q$.

Now I will announce a very important result in local class field theory.

Theorem 4.1 (Artin reciprocity law)**.** *Let K be a local field and L a Galois extension, there exists a unique group homomorphism*

$$\phi : K^* \longrightarrow \mathrm{Gal}(L|K)^{ab}$$

such that

- $\phi(\pi) = \varphi_{K^{ur}|K}$ *where π is a uniformizer of $\mathfrak{p}_K$ and K^{ur} is the maximal unramified extension of K.*
- *If $L|K$ is a finite abelian extension then ϕ defines a isomorphism*

$$\phi_L : K^*/N_{L|K}(L^*) \xrightarrow{\cong} \mathrm{Gal}(L|K).$$

Given a finite abelian extension $L|K$, the map ϕ_L is a symbol which we denote by $(\cdot, L|K)$ taking values in $\mathrm{Gal}(L|K)$ and is called *local norm residue symbol* or *Artin symbol.*

Observe that if $L|K$ is an unramified extension, we have the following simple description of the norm residue symbol in the special cases π and u where π is a uniformizer of $\mathfrak{p}_K$ and u is a unit in $\mathcal{O}_K$,

$$(\pi, L|K) \quad \text{is the Frobenius automorphism of } \mathrm{Gal}(L|K),$$

and

$$(u, L|K) = 1.$$

In order to state the general reciprocity law in the next section, we need to define the local norm residue symbol at the archimedean local fields. So we define the symbol as

$$\begin{aligned}(\cdot, \mathbb{C}|\mathbb{R}) : \mathbb{R}^* &\longrightarrow \mathrm{Gal}(\mathbb{C}|\mathbb{R}) \\ a &\longmapsto (a, \mathbb{C}|\mathbb{R})(-1) = (-1)^{\mathrm{sign}(a)}.\end{aligned}$$

4.2 Hilbert symbol

To define Hilbert symbol in local fields we need to suppose that the local field K contains a primitive nth roots of unity, ζ_n, for some positive integer n. First we'll see some results of Kummer Theory.

Theorem 4.2. *Let K be a local field containing the nth roots of unity. Let Δ be a subgroup of K^* such that $K^{*n} \subset \Delta$ and $L = K(\sqrt[n]{\Delta})$. Then $L|K$ is an abelian extension of exponent n and there exists the isomorphism*

$$\Delta/K^{*n} \cong \mathrm{Hom}(\mathrm{Gal}(L|K), \langle\zeta_n\rangle).$$

Proof. Note that the extension is Galois since it is the decomposition field of the polynomials

$$x^n - a, \quad a \in \Delta.$$

To prove that the extension it is abelian, we need to see that the Galois group is abelian, it is that the action of every element of $\mathrm{Gal}(L|K)$ on the elements $\alpha \in \sqrt[n]{\Delta}$ is commutative. Let $\sigma \in \mathrm{Gal}(L|K)$ and $\alpha \in \sqrt[n]{\Delta}$,

$$\sigma(\alpha^n) = \alpha^n \quad \text{since } \alpha^n \in K^* \implies \sigma(\alpha) = \zeta_n^i \alpha.$$

Now, if $\tau \in \mathrm{Gal}(L|K)$, then

$$\tau(\sigma(\alpha)) = \zeta_n^i \tau(\alpha) = \zeta_n^i \zeta_n^j \alpha$$

so it is commutative. Here we've used that ζ_n^i is in the base field K. Observe that for every $\alpha \in \sqrt[n]{\Delta}$, and for all $\sigma \in \mathrm{Gal}(L|K)$, $\sigma^n(\alpha) = (\zeta_n^i)^n\alpha = \alpha$ thus the exponent is n.

Now let's define the map

$$\begin{aligned} \Delta \times \mathrm{Gal}(L|K) &\longrightarrow \langle \zeta_n \rangle \\ a, \quad \sigma &\longmapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}. \end{aligned}$$

Since $a \in \Delta$, $\sqrt[n]{a} \in L$ and it makes sense to talk about $\sigma(\sqrt[n]{a})$. Also note that

$$\left(\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\right)^n = \frac{\sigma(a)}{a} = 1$$

hence $\dfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$ is in $\langle \zeta_n \rangle$. It's trivially verified to be multiplicative, i.e. a pairing.

First observe that the kernel in he left is K^{*n} since

$$\sigma(\sqrt[n]{a}) = \sqrt[n]{a} \quad \forall \sigma \in \mathrm{Gal}(L|K) \iff \sqrt[n]{a} \in K^* \iff a \in K^{*n}.$$

Second, fix $\sigma \in \mathrm{Gal}(L|K)$, and assume that $\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = 1$ for all $a \in \Delta$. Thus, for every generator α of L such that $\alpha^n = a$ we have $\sigma(\alpha) = \alpha$. This implies that $\sigma(x) = x$ for all $x \in L$, hence $\sigma = 1$, so the left kernel is trivial.

We get two injective homomorphisms

$$\begin{aligned} 0 &\longrightarrow \Delta/K^{*n} \longrightarrow \mathrm{Hom}(\mathrm{Gal}(L|K), \langle \zeta_n \rangle), \\ 0 &\longrightarrow \mathrm{Gal}(L|K) \longrightarrow \mathrm{Hom}(\Delta/K^{*n}, \langle \zeta_n \rangle). \end{aligned}$$

In particular we obtain the inequalities

$$|\Delta/K^{*n}| \leq |\mathrm{Hom}(\mathrm{Gal}(L|K), \langle \zeta_n \rangle)|, \qquad |\mathrm{Gal}(L|K)| \leq |\mathrm{Hom}(\Delta/K^{*n}, \langle \zeta_n \rangle)|.$$

Using the fact that if A is a finite abelian group of exponent dividing n then $|\mathrm{Hom}(A, \langle \zeta_n \rangle)| = |A|$, we get that

$$|\Delta/K^{*n}| = |\mathrm{Hom}(\Delta/K^{*n}, \langle \zeta_n \rangle)|, \qquad |\mathrm{Gal}(L|K)| = |\mathrm{Hom}(\mathrm{Gal}(L|K), \langle \zeta_n \rangle)|.$$

In particular we have the equality

$$|\Delta/K^{*n}| = |\mathrm{Hom}(\mathrm{Gal}(L|K), \langle \zeta_n \rangle)|,$$

from which we deduce that the first injective homomorphism is also surjective and

$$\Delta/K^{*n} \cong \mathrm{Hom}(\mathrm{Gal}(L|K), \langle \zeta_n \rangle).$$

□

The above correspondence gives a bijection between subgroups $\Delta \subseteq K^*$ with $K^{*n} \subseteq \Delta$ and abelian extensions of exponent n. (For a proof of this statment see [12], Chapter I, §5.)

Now take a local field K satisfying the conditions of Kummer theory and let $L = K(\sqrt[n]{K^*})$ be the maximal abelian extension of exponent n. We have that

$$K^*/K^{*n} \cong \mathrm{Hom}(\mathrm{Gal}(L|K), \langle \zeta_n \rangle) \tag{4.1}$$

by the previous theorem. Since $L|K$ is abelian of exponent n, using Artin's reciprocity law

$$K^*/N_{L|K}L^* \cong \mathrm{Gal}(L|K)$$

we get that $K^*/N_{L|K}L^*$ has exponent n, so $K^{*n} \subseteq N_{L|K}L^*$. By the isomorphism 4.1 we obtain

$$|K^*/K^{*n}| = |\mathrm{Gal}(L|K)| = |K^*/N_{L|K}L^*|$$

what let us conclude that $K^{*n} = N_{L|K}L^*$. With this result, the isomorphism of the Artin's reciprocity law now is $K^*/K^{*n} \cong \mathrm{Gal}(L|K)$ and recall that the norm residue symbol $(\cdot, L|K)$ is defined with this isomorphism. Now we are capable to define the Hilbert symbol and see some properties.

Definition 4.1 (Hilbert symbol)**.** *Let K be a local field containing a nth primitive root of unity ζ_n. The Hilbert symbol $(\cdot,\cdot)$ is defined as*

$$\begin{aligned} K^*/K^{*n} \times K^*/K^{*n} &\longrightarrow \langle \zeta_n \rangle \\ a \qquad b \qquad &\longmapsto (a,b) = \frac{(a, K(\sqrt[n]{b})|K)\,\sqrt[n]{b}}{\sqrt[n]{b}}. \end{aligned}$$

where $(a, K(\sqrt[n]{b}|K)$ is de norm residue symbol. The Hilbert symbol in an archimedean field is defined as

$$\begin{aligned} (\cdot,\cdot)_\infty : \mathbb{R}^*/\mathbb{R}^{*2} \times \mathbb{R}^*/\mathbb{R}^{*2} &\longrightarrow \langle \zeta_2 \rangle \\ a \qquad b \qquad &\longmapsto (a,b)_\infty = (-1)^{\frac{\mathrm{sign}(a)-1}{2}\frac{\mathrm{sign}(b)-1}{2}}. \end{aligned}$$

It follows from the definition that the symbol is non degenerate:

$$(a,b) = 1 \quad \forall a \in K^* \implies \sqrt[n]{b} \in K^* \implies b \in K^{*n},$$

$$(a,b) = 1 \quad \forall b \in K^* \implies a \in K^{*n}.$$

We now state some properties of the Hilbert symbol which will be needed in next results.

Proposition 4.1. *Let $a, a', b, b' \in K^*$, and K as above:*

(a) (Bimultiplicativity) $(aa', b) = (a, b)(a', b)$ and $(a, bb') = (a, b)(a, b')$.

(b) (Inverse) $(a, b)^{-1} = (a, b^{-1}) = (a^{-1}, b)$.

(c) $(a, b) = 1$ if and only if a is a norm in $K(\sqrt[n]{b})|K$.

(d) $(a, 1 - a) = 1$ and $(a, -a) = 1$.

(e) $(a, b) = (b, a)^{-1}$.

Proof. The multiplicativity can be checked by the definition. To the inverse property observe that by multiplicativity we have $(a, 1) = 1$ and then,

$$(a, b)(a, b^{-1}) = (a, bb^{-1}) = (a, 1) = 1 \implies (a, b)^{-1} = (a, b^{-1}).$$

Similarly for (a^{-1}, b). The third property follows from the definition of the Hilbert symbol. For the $(a, 1 - a) = 1$ we write $1 - a$ as

$$1 - a = \prod_{i=0}^{n-1}(1 - \zeta_n^i \sqrt[n]{a}) \implies 1 - a = N_{K(\sqrt[n]{a})|K}(1 - \zeta_n \sqrt[n]{a}) \implies 1 - a \in K^{*n}.$$

Therefore $(a, 1 - a) = 1$. The second equality follows writing $-a = \frac{1-a}{1-a^{-1}}$ and using the inverse property and the equality $(a, 1-a) = 1$ that we've just proved. Finally, by (d) we have $(ab, -ab) = 1$. Finally, use bimultiplicativity and get $(a, b) = (b, a)^{-1}$. □

Let's see now how the Hilbert symbol acts on the units of $\mathcal{O}_K$, that we call U. First we need a standard fact of local theory.

Proposition 4.2. *If $u \in U$ and $(n, p) = 1$ then the extension $K(\sqrt[n]{u})|K$ is unramified.*

Proof. Consider the polynomial $X^n - u$ and observe that since n is coprime to the characteristic of $\mathcal{O}_K/\mathfrak{p}$, the polynomial is separable modulo $\mathfrak{p}$. Let $f(X)$ be the minimal polynomial of $\sqrt[n]{u}$ in $\mathcal{O}_K$, then $f(X)$ is also separable modulo $\mathfrak{p}$. Observe that $f(X)$ is irreducible in the residue field $\mathcal{O}_K/\mathfrak{p}$ because if it was reducible then by Hensel's lemma this factorization would lift to a factorization in $\mathcal{O}_K$, contradicting the irreducibility of $f(X)$. So the degree of the residual extension is at least $\deg f$ and the extension $K(\sqrt[n]{u})|K$ must be unramified.[2] □

[2]The ramification of a extension of local fields $L|K$ is characterized by the degree of the residual extension. If $f = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{q}]$ then:

- If $f = n$ then $L|K$ is unramified.
- If $f = 1$ then $L|K$ is totally ramified.

Now let's compute the Hilbert symbol (v,u) when v,u are units of $\mathcal{O}_K$. It follows from the definition and the relation of the norm residue symbol and the Frobenius automorphism that

$$(v,u)=\frac{(v,K(\sqrt[n]{u})|K))(\sqrt[n]{u})}{\sqrt[n]{u}}=\frac{\sqrt[n]{u}}{\sqrt[n]{u}}=1$$

since $K(\sqrt[n]{u})|K$ is unramified and then the symbol $(v,K(\sqrt[n]{u})|K)=1$ when v is a unit. Moreover, if π is a uniformizer of $\mathcal{O}_K$ then,

$$(\pi,u)=\frac{(\pi,K(\sqrt[n]{u})|K)(\sqrt[n]{u})}{\sqrt[n]{u}}=\frac{\varphi_{K(\sqrt[n]{u})|K}(\sqrt[n]{u})}{\sqrt[n]{u}}\equiv(\sqrt[n]{u})^{q-1}\pmod{\mathfrak{p}}.$$

4.3 Power residue symbol

In this section we generalize the symbols in a arbitrary number field by taking the completion with respect every prime ideal. So let K be a number field containing a primitive nth root of unity and let $\mathcal{O}_K$ be it's ring of integers. For every prime ideal $\mathfrak{p}$ we define the Hilbert Symbol at $\mathfrak{p}$ as

$$\begin{aligned}(\cdot,\cdot)_{\mathfrak{p}}: K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*n}\times K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*n}&\longrightarrow\langle\zeta_n\rangle\\ a\qquad b\qquad&\longmapsto(a,b)_{\mathfrak{p}}=\frac{(a,K_{\mathfrak{p}}(\sqrt[n]{b})|K_{\mathfrak{p}})\sqrt[n]{b}}{\sqrt[n]{b}}.\end{aligned}$$

where $K_{\mathfrak{p}}$ is the completion at $\mathfrak{p}$. And at the archimedean completion we have the symbol defined with the norm residue symbol $(\cdot,\mathbb{C}|\mathbb{R})_\infty$.

Remark. If $\mathfrak{p}$ does not divide a, b and n then $(a,b)_{\mathfrak{p}}=1$. Indeed, if $\mathfrak{p}\nmid a,b$ the elements a and b are units in $K_{\mathfrak{p}}$ and by the remark we saw above, $(a,b)_{\mathfrak{p}}=1$.

With this symbol, there is classical result of global class field theory, called Hilbert reciprocity and the statement is the following.

Theorem 4.3 (Hilbert's reciprocity law)**.** *Let K be a number field containing a primitive nth root of unity. If $a,b\in K^*$ then*

$$\prod_{\mathfrak{p}}(a,b)_{\mathfrak{p}}=1.$$

For a proof see [12], Capter IV, §9. Let's see how this generalization of Hilbert symbol can help us to find the next symbol called power residue symbol. Given a

prime ideal $\mathfrak{p}$ of K coprime with n and π a prime element above $\mathfrak{p}$, we saw before that

$$(\pi, u)_{\mathfrak{p}} \equiv (\sqrt[n]{u})^{N(\mathfrak{p})-1} \pmod{\mathfrak{p}}$$

where u is a unit in the completion of K at $\mathfrak{p}$. Therefore, the Hilbert symbol at $\mathfrak{p}$ is independent of the choice of the prime element π. We can define for every $\mathfrak{p}$ prime ideal coprime with n and for every $u \in \mathcal{O}_K$ such that $\mathfrak{p} \nmid u$ the *nth power residue symbol* of u and $\mathfrak{p}$ as

$$\left(\frac{u}{\mathfrak{p}}\right) := (\pi, u)_{\mathfrak{p}}$$

which is a nth root of unity determined by

$$\left(\frac{u}{\mathfrak{p}}\right) \equiv u^{\frac{N(\mathfrak{p})-1}{n}} \pmod{\mathfrak{p}}.$$

Definition 4.2. *For any fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ prime to n and any $a \in \mathcal{O}_K$ prime to $\mathfrak{b}$, we define the nth power residue symbol by*

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod_{\mathfrak{p}|\mathfrak{b}} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\mathfrak{b})}.$$

Clearly, the symbol is multiplicative in $\mathfrak{b}$. If $\mathfrak{b}$ is a principal ideal (b), then we simply write $\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a}{b}\right)$.

Proposition 4.3. *Let $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, the nth power residue symbol satisfies the following properties:*

(a) $\left(\frac{a}{\mathfrak{p}}\right) = \left(\frac{b}{\mathfrak{b}}\right)$ *if* $a \equiv b \pmod{\mathfrak{p}}$.

(b) $\left(\frac{a}{\mathfrak{p}}\right) = 1$ *if and only if* $a \equiv \alpha^n \pmod{\mathfrak{p}}$, *for some* $\alpha \in \mathcal{O}_K$.

Proof. The first property follows from the fact that there are not two different nth roots of unity in $\mathcal{O}_K/\mathfrak{p}$ if $\mathfrak{p}$ is coprime with n. For a proof of the second, assume that $a \equiv \alpha^n \pmod{\mathfrak{p}}$. Then,

$$a^{\frac{N(\mathfrak{p})-1}{n}} \equiv \alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{p}$$

hence by the first property $\left(\frac{a}{\mathfrak{p}}\right) = 1$. To prove the other direction, assume that $\left(\frac{a}{\mathfrak{p}}\right) = 1$. Then $1 \equiv a^{\frac{N(\mathfrak{p})-1}{n}}$. Since $(\mathcal{O}_K/\mathfrak{p})^\times$ is cyclic, there exists some γ such that $a \equiv \gamma^j \pmod{\mathfrak{p}}$. So,

$$1 \equiv a^{\frac{N(\mathfrak{p})-1}{n}} \equiv \gamma^{j\frac{N(\mathfrak{p})-1}{n}} \pmod{\mathfrak{p}}$$

which implies that $n \mid j$. Thus $\alpha \equiv \gamma^{n\lambda} \pmod{\mathfrak{p}}$ and therefore α is an nth power mod $\mathfrak{p}$.

□

We now are ready to prove the general reciprocity law of nth power residues.

Theorem 4.4 (General reciprocity law)**.** *Let $a, b \in K^*$ are prime to each other and to n, then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}|n,\infty} (a,b)_{\mathfrak{p}}.$$

Proof. From the definition of the nth power residue symbol we obtain

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}|(b)} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \prod_{\mathfrak{p}|(a)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_{\mathfrak{p}}(a)} = \prod_{\mathfrak{p}|(ab)} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_{\mathfrak{p}}(a)}.$$

Now observe that we can extend this product on all primes not dividing n nor ∞ because in this case $v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(a) = 1$. So,

$$\prod_{\mathfrak{p}|(ab)} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_{\mathfrak{p}}(a)} = \prod_{\mathfrak{p}\nmid n,\infty} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_{\mathfrak{p}}(a)}.$$

Now let's see how this product is related with the product of the Hilbert symbols. Recall from a remark above that if $\mathfrak{p} \nmid a, b, n, \infty$ then $(a,b)_{\mathfrak{p}} = 1$. Alternatively, if $\mathfrak{p} \nmid a, n, \infty$ then

$$\left(\frac{a}{\mathfrak{p}}\right) = (\pi, a)_{\mathfrak{p}}.$$

where π is a prime element of $K_{\mathfrak{p}}$. If $b = u\pi^{v_{\mathfrak{p}}(b)}$ with $v_{\mathfrak{p}}(b) > 0$ then

$$\left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} = (\pi, a)_{\mathfrak{p}}^{v_{\mathfrak{p}}(b)} = (b, a)_{\mathfrak{p}}$$

since $(u,a)_{\mathfrak{p}} = 1$. Similarly, if $\mathfrak{p} \nmid b, n, \infty$ and $a = u\pi^{v_{\mathfrak{p}}(a)}$ with $v_{\mathfrak{p}}(a) > 0$ then

$$\left(\frac{b}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)} = (\pi, b)_{\mathfrak{p}}^{v_{\mathfrak{p}}(a)} = (a,b)_{\mathfrak{p}}$$

and then

$$\left(\frac{b}{\mathfrak{p}}\right)^{-v_{\mathfrak{p}}(a)} = (\pi, b)_{\mathfrak{p}}^{-v_{\mathfrak{p}}(a)} = (a,b)_{\mathfrak{p}}^{-1} = (b,a)_{\mathfrak{p}}.$$

Therefore we obtain

$$\prod_{\mathfrak{p} \nmid n,\infty} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_{\mathfrak{p}}(a)} = \prod_{\mathfrak{p} \nmid n\infty} (b,a)_{\mathfrak{p}}.$$

By the Hilbert's reciprocity law (4.3) we finally get

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{p \mid n,\infty} (a,b)_{\mathfrak{p}}.$$

□

From this theorem one can deduce easily the quadratic reciprocity law taking $K = \mathbb{Q}$ and $n = 2$.

4.4 Eisenstein's reciprocity law

Let's move now to the cyclotomic field $K = \mathbb{Q}(\zeta)$ where ζ is a primitive pth root of unity. Let $\mathcal{O}_K = \mathbb{Z}[\zeta]$ be the ring of integers and $\mathfrak{p} = (1-\zeta)$ be the unique prime ideal above p. In order to state this reciprocity law we need to introduce the notion of a semi-primary integer.

Definition 4.3. *An element $\alpha \in \mathbb{Z}[\zeta]$ is said to be semi-primary if $\alpha \notin \mathfrak{p}$ but there exists an ordinary integer $q \in \mathbb{Z}$ such that $\alpha \equiv q \pmod{\mathfrak{p}^2}$.*

Whith this special type of integers we have the result:

Theorem 4.5 (Eisenstein's reciprocity law)**.** *Let m be an integer coprime with p and let $\alpha \in \mathcal{O}_K$ be a semi-primary integer relatively prime to the integer m. Then,*

$$\left(\frac{m}{\alpha}\right) = \left(\frac{\alpha}{m}\right).$$

Let's see now some lemmas that follow from the theory of the power residue symbol and will help us to prove Eisenstein's reciprocity law.

Lemma 4.1. *Let $\alpha, \beta \in K^*$ relatively prime and coprime with p. Then*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = (\alpha, \beta)_{\mathfrak{p}}.$$

Proof. From the General reciprocity law (Theorem 4.4) we have that

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{q}|p,\infty} (\alpha, \beta)_{\mathfrak{q}}.$$

Since the only prime ideal that lies above p is $\mathfrak{p}$,

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = (\alpha, \beta)_{\mathfrak{p}}.$$

□

Definition 4.4. *Let U denote the units of $K_{\mathfrak{p}}$ and $U_i = \{u \in U : u \equiv 1 \pmod{\mathfrak{p}^i}\}$ the i th higher principal units.*

Lemma 4.2. *Let $\alpha \in U_i$ and $\beta \in U_j$. If $i + j \geq p + 1$ we have*

$$(\alpha, \beta)_{\mathfrak{p}} = 1.$$

Proof. Let's see first that if $a \in K_{\mathfrak{p}}^{\times}$ is such that $a \equiv 1 \pmod{\mathfrak{p}^{p+1}}$ then the extension $K_{\mathfrak{p}}(\sqrt[n]{a})|K_{\mathfrak{p}}$ is trivial. In this case we say that a is hyperprimary.

Let $a = 1 + c\pi^{p+1}$ with $c \in K_{\mathfrak{p}}^{\times}$ and $\alpha^p = a$ with $\alpha = 1 + x\pi$ with $x \in K_{\mathfrak{p}}(\sqrt[n]{a})$. We obtain that

$$\begin{aligned}
(1 + x\pi)^p &= 1 + c\pi^{p+1}, \\
1 + xp\pi + p\pi^2(\cdots) + x^p\pi^p &= 1 + c\pi^{p+1}, \\
xp\pi + x^p\pi^p &\equiv 0 \pmod{\mathfrak{p}^{p+1}}, \\
\pi^p(-x + x^p) &\equiv 0 \pmod{\mathfrak{p}^{p+1}}, \\
x^p - x &\equiv 0 \pmod{\mathfrak{p}}.
\end{aligned}$$

Here we have used that $p\pi^2 \equiv 0 \pmod{\mathfrak{p}^{p+1}}$ and that $p\pi \equiv -\pi^p \pmod{\mathfrak{p}^{p+1}}$. The first one follows from the fact that $\pi^{p-1} \mid p$ and the second one from:

$$0 = (1 - \pi)^p - 1 \equiv 1 - p\pi + p\pi^2(\cdots) + -\pi^p - 1 \equiv -p\pi - \pi^p \pmod{\mathfrak{p}^{p+1}}.$$

Now if $f(X)$ is the minimal polynomial of the element x, it satisfies that

$$f(X) \equiv X^p - X \pmod{\mathfrak{p}}$$

So the polynomial splits and by Hensel's lemma it also splits in $K_\mathfrak{p}(\sqrt[n]{a})|K_\mathfrak{p}$. Therefore, the extension $K_\mathfrak{p}(\sqrt[n]{a})|K_\mathfrak{p}$ is trivial.

We now will see that π generates the group $K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p U_1$. Observe that we have the exact sequence

$$0 \longrightarrow (1+\mathfrak{p}) \longrightarrow \mathcal{O}_{K_\mathfrak{p}}^\times \longrightarrow \mathbb{F}_p^\times \longrightarrow 0$$

and since $\mathbb{F}_p^\times \cong \langle \zeta_{p-1} \rangle$, we can deduce that $K_\mathfrak{p}^\times = \mathfrak{p}^\mathbb{Z} \cdot \mathcal{O}_{K_\mathfrak{p}}^\times = \mathfrak{p}^\mathbb{Z} \cdot \langle \zeta_{p-1} \rangle \cdot (1+\mathfrak{p})$. Therefore,

$$(K_\mathfrak{p}^\times)^p \cong p\mathbb{Z} \times \langle \zeta_{p-1} \rangle \times (1+\mathfrak{p})^p.$$

If we consider the quotient $K_\mathfrak{p}^\times$ modulo $(K_\mathfrak{p}^\times)^p$ we obtain

$$K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p \cong \mathbb{Z}/p\mathbb{Z} \times U_1/U_1^p \implies K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p U_1 \cong \mathbb{Z}/p\mathbb{Z}.$$

Let $\pi^r \cdot \zeta_{p-1}^s \cdot (1+\alpha)$ an element of $K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p U_\mathfrak{p}^1$, then

$$\pi^r \cdot \zeta_{p-1}^s \cdot (1+\alpha) = \pi^a \cdot \gamma$$

with $\gamma = xy$ and $x \in (K_\mathfrak{p}^\times)^p$ and $y \in U_\mathfrak{p}^1$. If $r = ap + b$ then

$$\pi^b \cdot (\pi^a \zeta_{p-1}^{s'})^p \cdot (1+\alpha).$$

Therefore $K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p U_\mathfrak{p}^1 = \langle \pi \rangle$.

Now let's see that for all i the group U_i/U_{i+1} is a cyclic group with order p and generated by $\eta_i = 1 - \pi^i$. Let $x \in U_i/U_{i+1}$, then $x \equiv 1 \pmod{\mathfrak{p}^i}$ so we can write $x = 1 + \alpha\pi^i$ for some $\alpha \in K_\mathfrak{p}^\times$. Then $x^p \equiv 1 \pmod{\mathfrak{p}^{i+1}}$, so the group has order p. Note that $\eta_i = 1 - \pi^i \in U_i$, and note that η_i has order p since if $j \neq p$

$$(\eta_i)^j = (1-\pi^i)^j \not\equiv 1 \pmod{\mathfrak{p}^{i+1}}.$$

Therefore U_i/U_{i+1} is a cyclic group generated by η_i.

Using the fact that we've seen above, we note that $U_{p+1} \subseteq (K_\mathfrak{p}^\times)^p$. Summing up we get

$$K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p \cong \mathbb{Z}/p\mathbb{Z} \times U_1/(U_1)^p \cong \mathbb{Z}/p\mathbb{Z} \times U_1/U_2 \times U_2/U_3 \times \cdots \times U_p/U_{p+1}.$$

And every group is generated by $\pi, \eta_1, \ldots, \eta_p$ respectively.

Now, take $\alpha \in U_i$ and $\beta \in U_j$ such that $i + j \geq p + 1$. By the result above, we can write $\alpha = \eta_i^{a_i} x_{i+1}$ with $x_{i+1} \in U_{i+1}$. Doing the same with x_{i+1}, we obtain

$$\alpha = \eta_i^{a_i} \eta_{i+1}^{a_{i+1}} \cdots \eta_p^{a_p} x_{p+1}$$

with $x_{p+1} \in U_{p+1}$. Similarly,

$$\beta = \alpha = \eta_j^{b_j} \eta_{j+1}^{b_{j+1}} \cdots \eta_p^{b_p} y_{p+1}$$

with $y_{p+1} \in U_{p+1}$. Observe that if $k \neq l$

$$(\eta_k, \eta_l) = (\pi^l, \eta_l)(\eta_k, \eta_l) = (\pi^l \eta_k, \eta_l) = \left(\frac{\pi^l \eta_k}{\eta_{k+l}}, \eta_k\right)(\eta_{k+l}, \eta_k)$$
$$\left(\frac{\pi^l \eta_k}{\eta_{k+l}}, \eta_{k+l}\right)\left(\frac{\pi^l \eta_k}{\eta_{k+l}}, \frac{\eta_l}{\eta_{k+l}}\right)(\eta_{k+l}, \eta_l).$$

Note that $((\eta_{k+l})^{-1}, \eta_{k+l}) = 1$, and that $(\pi^l \eta_k + \eta_l = \eta_{k+l}$ hence $(\frac{\pi^l \eta_k}{\eta_{k+l}}, \frac{\eta_l}{\eta_{k+l}}) = 1$, then

$$(\eta_k, \eta_l) = (\pi^l \eta_k, \eta_{k+l})(\eta_{k+l}, \eta_l) = (\pi^l, \eta_{k+l})(\eta_k, \eta_{k+l})(\eta_{k+l}, \eta_l). \tag{4.2}$$

and for all k,

$$(\eta_k, x_{p+1}) = 1 \text{ if } x_{p+1} \in U_{p+1}.$$

Since $i+j \geq p+1$, we have $U_{i+j} \subseteq (K_\mathfrak{p}^\times)^p$ so for all $a \in K_\mathfrak{p}^\times$, $(a, \eta_{i+j}) = (\eta_{i+j}, a) = 1$. And by the expression of (η_i, η_j) in 4.2, if $i + j \geq p + 1$, $(\eta_i, \eta_j) = 1$. Finally, by the expression of α and β as product of η_k's we can deduce that

$$(\alpha, \beta)_\mathfrak{p} = 1.$$

□

Proof of Eisenstein's reciprocity law. By lemma 4.1 we only need to prove that the Hilbert symbol at the completion on the ideal $\mathfrak{p}$ is $(\alpha, m)_\mathfrak{p} = 1$. The fact that α is semi-primary is equivalent with the existence of an integer $q \in \mathbb{Z}$ coprime with p such that $\frac{\alpha}{q} \in U_\mathfrak{p}^2$. And observe that if using Fermat's little theorem,

$$m^{p-1} \equiv 1 \pmod{p} \implies m^{p-1} \equiv 1 \pmod{\mathfrak{p}^{p-1}} \implies m^{p-1} \in U_\mathfrak{p}^{p-1}.$$

By the previous lemma we have

$$\left(\frac{\alpha}{q}, m\right)^{p-1} = \left(\frac{\alpha}{q}, m^{p-1}\right)_\mathfrak{p} = 1.$$

Now, $\left(\frac{\alpha}{q}, m\right)_{\mathfrak{p}}$ is a p^{th} root of unity, by definition of the Hilbert symbol. Since p and $p-1$ are coprime we obtain

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

and then

$$1 = \left(\frac{\alpha}{q}, m\right)_{\mathfrak{p}} = (\alpha, m)_{\mathfrak{p}}(q, m)_{\mathfrak{p}}^{-1} \implies (\alpha, m)_{\mathfrak{p}} = (q, m)_{\mathfrak{p}}.$$

Since q is also coprime with p we can apply again Fermat's little theorem and get $q^{p-1} \in U_{\mathfrak{p}}^{p-1}$. Again using the previous lemma we get

$$1 = (q^{p-1}, m^{p-1})_{\mathfrak{p}} = (q, m)_{\mathfrak{p}}^{2p-2}.$$

And by the same argument as before we can deduce that

$$(q, m)_{\mathfrak{p}} = 1 \implies (\alpha, m)_{\mathfrak{p}} = 1.$$

□

4.5 Furtwängler theorems on FLT

In 1912, Furtwängler noticed that the Eisenstein's reciprocity law for the pth power residue symbol can be used to get interesting sufficient conditions for the 1st case on FLT. In the following we keep notation of section 4.4.

The following corollary of Eisenstein's reciprocity law is required in Furtwängler's theorems.

Corollary 4.1. *Let m be an integer, $p \nmid m$, let $\alpha \in \mathcal{O}_K$ be a semi-primary integer coprime with m. If $\alpha\mathcal{O}_K$ is the pth power of some ideal of $\mathcal{O}_K$ then $\left(\frac{\alpha}{m}\right) = 1$.*

Proof. Using Eisenstein's law we get

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

and since there exist some ideal I such that $\alpha\mathcal{O}_K = I^p$, we obtain

$$\left(\frac{m}{\alpha}\right) = \left(\frac{m}{I^P}\right) = \left(\frac{m}{I}\right)^p = 1.$$

□

Theorem 4.6 (First theorem of Furtwängler)**.** *Let $p \geq 3$ be prime, let x, y, and z be pairwise coprime nonzero integers such that $x^p + y^p = z^p$, and assume that $p \nmid x$. Then for every $r \mid x$ we have $r^{p-1} \equiv 1 \pmod{p^2}$.*

Proof. Since x, y and z are pairwise coprime, we can suppose that $p \nmid z$. Observe first that

$$\prod_{i=1}^{p} \zeta^i x + \zeta^{-x} y = \prod_{i=1}^{p} \zeta^{-x}(\zeta^{i+x} x + y) = \prod_{i=1}^{p} \zeta^{-x}(\zeta^i x + y) = x^p + y^p = z^p.$$

Since x and y are coprime and $p \nmid z$, the elements $\zeta^i x + \zeta^{-x} y$ are pairwise coprime as we saw in the proof of Kummer 1st case. Then the ideals $(\zeta^i x + \zeta^{-x} y)\mathcal{O}_K$ are pth powers of ideals for all i. In particular, if $\alpha = \zeta^y x + \zeta^{-x} y$, the ideal $\alpha\mathcal{O}_K$ is a pth power of an ideal in $\mathcal{O}_K$.

Now observe that α is a semi-primary integer since

$$\begin{aligned} \zeta^y &= (1 - (1-\zeta))^y \equiv 1 - y(1-\zeta) \pmod{\mathfrak{p}^2}, \\ \zeta^{-x} &= (1 - (1-\zeta))^{-x} \equiv 1 - (-x)(1-\zeta) \pmod{\mathfrak{p}^2}, \end{aligned}$$

so $\alpha \equiv x(1 - y(1-\zeta)) + y(1 + x(1-\zeta)) \equiv x + y \pmod{\mathfrak{p}^2}$. Let $r \mid x$, note that r and y are coprime and they are also r and α. We are in the hypothesis of the corollary above, so we obtain

$$\left(\frac{\alpha}{r}\right) = \left(\frac{r}{\alpha}\right)$$

and this is 1 by the corollary above.

Recall a property of the power residue symbol that states that if $\alpha, \beta \notin I$, and I is an ideal of $\mathcal{O}_K$ then

$$\alpha \equiv \beta \pmod{I} \implies \left(\frac{\alpha}{I}\right) = \left(\frac{\beta}{I}\right).$$

Observe that

$$\alpha = \zeta^y x + \zeta^{-x} y = \zeta^{-x}(\zeta^{y+x} x + y) = \zeta^{-x}(x + y + x(\zeta^{y+x} - 1))$$

and since $r \mid x$, we get $\alpha \equiv \zeta^{-x}(x+y) \pmod{r\mathcal{O}_K}$. So

$$1 = \left(\frac{\alpha}{r}\right) = \left(\frac{\zeta^{-x}(x+y)}{r}\right) = \left(\frac{\zeta^{-x}}{r}\right)\left(\frac{x+y}{r}\right).$$

Now let's see that $\left(\frac{x+y}{r}\right) = 1$. Since $p \nmid z$, $p \nmid x+y$, so $(x+y)$ is semi-primary. Since $(x+y)$ and r are coprime, and the ideal $(x+y)\mathcal{O}_K$ is a pth power of an ideal of $\mathcal{O}_K$, by the previous corollary we get $\left(\frac{x+y}{r}\right) = 1$. With this claim we obtain

$$1 = \left(\frac{\zeta^{-x}}{r}\right) = \left(\frac{\zeta}{r}\right)^{-x} \implies \left(\frac{\zeta}{r}\right) = 1.$$

Recall that the only primes of $\mathbb{Z}$ that don't ramify in $\mathcal{O}_K$ are those who divide the discriminant of $K|\mathbb{Q}$ which is $(-1)^{\frac{p-1}{2}}p^{p-2}$. So the prime factors of r are ramified in $\mathcal{O}_K$. Let $r\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{r}_i$ be the prime decomposition of the ideal $r\mathcal{O}_K$, with g such that $N(\mathfrak{r}_i) = r^f$ and $fg = p-1$. By definition of the power residue symbol we have $\left(\frac{\zeta}{\mathfrak{r}_i}\right) \equiv \zeta^{\frac{N(\mathfrak{r}_i)-1}{p}} \pmod{\mathfrak{r}_i}$ and in this case we have an equality because both sides are roots of unity and mod $\mathfrak{r}_\mathfrak{i}$ have to be the same since $\mathfrak{r}_i \nmid p$. Thus,

$$1 = \left(\frac{\zeta}{r}\right) = \prod_{i=1}^{g}\left(\frac{\zeta}{\mathfrak{r}_i}\right) = \prod_{i=1}^{g}\zeta^{\frac{N(\mathfrak{r}_i)-1}{p}} = \prod_{i=1}^{g}\zeta^{\frac{r^f-1}{p}} = \zeta^{\frac{g(r^f-1)}{p}},$$

$$\frac{g(r^f-1)}{p} \equiv 0 \pmod{p} \implies g(r^f-1) \equiv 0 \pmod{p^2}$$

and since $g \mid p-1$, $p \nmid g$ so $r^f \equiv 1 \pmod{p^2}$. Since $f \mid p-1$ we also have

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

□

Furtwängler then extended the result for divisors of $x-y$.

Theorem 4.7 (Second theorem of Furtwängler)**.** *Let $p \geq 3$ be prime, let x, y and z be pairwise coprime nonzero integers such that $x^p + y^p = z^p$, and assume that $p \nmid x^2 - y^2$. Then for every $r \mid x-y$ we have $r^{p-1} \equiv 1 \pmod{p^2}$.*

Proof. Since $p \nmid x^2 - y^2$ then $p \nmid x+y$ and then $p \nmid z$. Similarly to the previous proof, the element $\alpha = \zeta^y x + \zeta^{-x} y$ generates an ideal which is a pth power of an ideal of $\mathbb{Z}[\zeta]$, and α is again semi-primary, therefore the symbol

$$\left(\frac{\zeta^y x + \zeta^{-x} y}{r}\right) = 1.$$

Now observe that

$$\alpha = \zeta^y x + \zeta^{-x} y = \zeta^{y-x}(\zeta^{-y}x + \zeta^x y + (x-y)(\zeta^x - \zeta^{-y})) \equiv \zeta^{y-x}(\zeta^{-y}x + \zeta^x y) \pmod{r\mathcal{O}_K}.$$

Then

$$1 = \left(\frac{\zeta^y x + \zeta^{-x} y}{r}\right) = \left(\frac{\zeta^{y-x}(\zeta^{-y} x + \zeta^x y)}{r}\right) = \left(\frac{\zeta^{y-x}}{r}\right)\left(\frac{\zeta^{-y} x + \zeta^x y}{r}\right).$$

Now $\zeta^{-y} x + \zeta^x y$ is semi-primary since

$$\zeta^{-y} x + \zeta^x y \equiv x(1 - (1-\zeta)(-y)) + y(1 - (1-\zeta)x) \equiv x + y \pmod{\mathfrak{p}^2}$$

and it is also a pth power and coprime with r, thus

$$\left(\frac{\zeta^{-y} x + \zeta^x y}{r}\right) = \left(\frac{r}{\zeta^{-y} x + \zeta^x y}\right) = 1.$$

Therefore we have

$$\left(\frac{\zeta^{y-x}}{r}\right) = 1 \implies \left(\frac{\zeta}{r}\right) = 1$$

and by the same argument as in the first theorem we deduce

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

□

With these theorems, Furtwängler obtained both theorems of Wieferich criteria and Mirmanoff in a very natural way.

Theorem 4.8 (Wieferich)**.** *If the first case of FLT fails for p then it satisfies the congruence*

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Proof. Let x, y and x such that $x^p + y^p + z^p = 0$ with $p \nmid xyz$. Note that one of x y or z must be even, suppose that it is x. We also have that $p \nmid x$, so by the first theorem of Furtwängler, $2^{p-1} \equiv 1 \pmod{p^2}$. □

Theorem 4.9 (Mirimanoff)**.** *If the first case of FLT fails for p then $3^{p-1} \equiv 1 \pmod{p^2}$.*

Proof. If $3 \mid xyz$ then by Furtwängler's first theorem (4.6) we have $3^{p-1} \equiv 1 \pmod{p^2}$. Now is $3 \nmid xyz$ then

$$0 = x^p + y^p + z^p \equiv x + y + z \equiv \pm 1 \pm 1 \pm 1 \pmod 3 \implies x \equiv y \equiv z \pmod 3$$

Note that $3 \mid x-y, x-z, y-z$. Now p can't divide the three numbers because

$$0 = x^p + y^p + z^p \equiv x + y + z \equiv 3x \pmod{p} \implies p \mid x.$$

So we can suppose that $p \nmid x-y$. Since $x + y \equiv -z \pmod{p}$ then $p \nmid x+y$ and then $p \nmid x^2 - y^2$ so we are in the hypothesis of Furtwängler's second theorem (4.7) and we can deduce that

$$3^{p-1} \equiv 1 \pmod{p^2}.$$

□

In view of their importance, the theorems of Furtwängler were proved again, extended and generalized by Inkeri, McDonell and Vandiver and they got the same result for

$$r \mid x^2 - yz, y^2 - xz, z^2 - xy, x^2 + yz, y^2 + xz, z^2 + xy.$$

Hellegouarch showed that if the Fermat equation has solution for $n = p^t$ then p^{2t} divides both $2^p - 2$ and $3^p - 3$. As a consequence, for every prime p the first case of FLT holds for some exponent p^n and therefore the first case is true for infinitely many prime exponents.

4.6 Generalization of Terjanian's theorem

Here in this section we will talk about the 2-power residue symbol in a arbitrary number field K. First note that every number field contains a primitive 2-th root of unit, -1, so all the class field theory we studied in number fields containing pth roots of unity is true in K for $p = 2$.

The Hilbert symbol can be characterized by the study of a quadratic form.

Proposition 4.4. *For every $\alpha, \beta \in K$ and $\mathfrak{p}$ a prime ideal, the Hilbert symbol at $\mathfrak{p}$ is*

$$(\alpha, \beta)_{\mathfrak{p}} = \begin{cases} 1 \text{ if } \alpha X^2 + \beta Y^2 = Z^2 \text{ has a non-zero solution in } K_{\mathfrak{p}}, \\ -1 \text{ otherwise.} \end{cases}$$

Proof. Recall that $(\alpha, \beta)_{\mathfrak{p}} = 1$ if and only if $\alpha \in N_{K_{\mathfrak{p}}(\sqrt{\beta})|K_{\mathfrak{p}}}$. So if $(\alpha, \beta)_{\mathfrak{p}} = 1$, $\alpha = N_{K_{\mathfrak{p}}(\sqrt{\beta})|K_{\mathfrak{p}}}(z + \sqrt{\beta}y)$ for some $y, z \in K_{\mathfrak{p}}$. Then $\alpha = z^2 - \beta y^2$ and $\alpha + \beta y^2 = z^2$ so the equation $\alpha X^2 + \beta Y^2 = Z^2$ has a solution $(1, y, z)$ in $K_{\mathfrak{p}}$. Now suppose that there exist $x, y, z \in K_{\mathfrak{p}}$ such that $\alpha x^2 + \beta y^2 = z^2$. If $x \neq 0$ then

$$\alpha = \frac{z^2}{x^2} - \beta \frac{y^2}{x^2} = N_{K_{\mathfrak{p}}(\sqrt{\beta})|K_{\mathfrak{p}}}(\frac{z}{x} + \sqrt{\beta}\frac{y}{x}) \implies (\alpha, \beta)_{\mathfrak{p}} = 1.$$

If $x = 0$ and $y \neq 0$ we have $\beta = \frac{z^2}{y^2}$, so β is a square in $K_\mathfrak{p}$ and $(\alpha, \beta)_\mathfrak{p} = 1$. Note that the case of $x = y = 0$ is not a non-zero solution, so we are done. $\square$

With this characterization, it's clear that if $K_\mathfrak{p}$ is complex, then the Hilbert symbol is 1. So the only archimedean places that the Hilbert symbol sees are those where the completion $K_\mathfrak{p}$ is $\mathbb{R}$, and they correspond to the real embeddings of K. There are a special kind of integers where the Hilbert symbol is always trivial, they are the primary elements of K.

Definition 4.5. *We say that an element $\alpha \in \mathcal{O}_K$ is primary if it is coprime with 2 and α is congruent to a square modulo $4\mathcal{O}_K$.*

Note that if α or β is primary, one of α or β is a square modulo $4\mathcal{O}_K$, and then the equation

$$\alpha X^2 + \beta Y^2 = Z^2$$

has a nonzero solution modulo $4\mathcal{O}_K$. Therefore by Hensel's lemma it also has a solution in $K_\mathfrak{p}$ for every $\mathfrak{p}$ prime ideal dividing 2. So the Hilbert symbol in the primes that divide 2 are 1 in this case.

Now let's see how the general reciprocity law acts when $n = 2$.

Proposition 4.5. *Let $\alpha, \beta \in \mathcal{O}_K$ be coprime and coprime with 2. If α or β is primary then*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \prod_{i=1}^{r} (-1)^{\frac{\operatorname{sgn}(\sigma_i(\alpha))-1}{2}\frac{\operatorname{sgn}(\sigma_i(\beta))-1}{2}}$$

where σ_i, $1 \leq i \leq r$ are the real embeddings of K.

Proof. The general reciprocity law states that

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{p}|2,\infty} (\alpha, \beta)_\mathfrak{p}.$$

Note that since α or β is primary, $\prod_{\mathfrak{p}|2}(\alpha, \beta)_\mathfrak{p} = 1$. We observed before that the only archimedean places that the Hilbert symbol can be different from 1 are those where the completion is $\mathbb{R}$, and they correspond to the real embeddings of K. Moreover, if σ is a real embedding, the Hilbert symbol is defined as

$$(\alpha, \beta) = (-1)^{\frac{\operatorname{sgn}(\sigma(\alpha))-1}{2}\frac{\operatorname{sgn}(\sigma(\beta))-1}{2}}.$$

If $\sigma_i : K \longrightarrow \mathbb{R}$ are the real embeddings, with $1 \leq i \leq r$, we get

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \prod_{i=1}^{r}(-1)^{\frac{\operatorname{sgn}(\sigma_i(\alpha))-1}{2}\frac{\operatorname{sgn}(\sigma_i(\beta))-1}{2}}.$$

□

The generalization of Hellegouarch on Fermat Last Theorem for even degree follows from two theorems.

Theorem 4.10. *Let K be a number field of odd degree and $\mathcal{O}_K$ it's ring of integers. If $y, z \in \mathcal{O}_K$ are coprime, coprime with 2 and they satisfy $y^2 \equiv z^2 \pmod{4\mathcal{O}_K}$, then for every odd prime $p \in \mathbb{Z}$ the ideal*

$$\left(\frac{z^{2p} - y^{2p}}{z^2 - y^2}\right)\mathcal{O}_K$$

is not a square.

The idea for proving the theorem is to relate the 2th power residue symbol to the Jacobi symbol. To do this we give first a characterization of the Jacobi symbol, but only in the primary integers. Let $\mathcal{P}$ be the set of primary integers in $\mathbb{Z}$ and let Δ be the set of $\mathcal{P} \times \mathcal{P}$ of the couples (n, m) where n and m are not coprime.

Lemma 4.3. *Let $f : \mathcal{P} \times \mathcal{P} \setminus \Delta \longrightarrow \{+1, -1\}$ be a map satisfying*

1. $f(1, 1) = 1$.
2. $f(n, m) = (-1)^{\frac{\operatorname{sgn}(n)-1}{2}\frac{\operatorname{sgn}(m)-1}{2}} f(m, n)$
3. $f(m_1, n) = f(m_2, n)$ *if* $m_1 \equiv m_2 \pmod{n}$.
4. $f(m_1, n) = (-1)^{\frac{\operatorname{sgn}(n)-1}{2}} f(m_2, n)$ *if* $m_1 + m_2 \equiv 0 \pmod{n}$.

Then f is the Jacobi symbol.

With this characterization we are capable to proof the first theorem of Hellegouarch.

Proof of theorem 4.10. Let $a, b \in \mathcal{O}_K$ be different and $m \in \mathcal{P}$, we define $Q_m(a, b)$ similarly to the proof of Terjanian

$$Q_m(a, b) = \operatorname{sgn}(m)\frac{a^{2|m|} - b^{2|m|}}{a^2 - b^2}.$$

Observe that $Q_m(a,b) = \operatorname{sgn}(m)\sum_{i=1}^{|m|} a^{2(|m|-i)}b^{2(i-1)} \in \mathcal{O}_K$. If $y, z \in \mathcal{O}_K$ satisfy the hypothesis of the theorem, and $(n,m) \in \mathcal{P}\times\mathcal{P}\setminus\Delta$, let's see that the map

$$f(n,m) = \left(\frac{Q_n(z,y)}{Q_m(z,y)}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the 2th power residue symbol in K, is also the Jacobi symbol. First let's see that f is well defined. The 2th power residue symbol is only defined in coprime elements, so we first have to prove that $Q_m(z,y)$ and $Q_n(z,y)$ are coprime.

Claim: If $\gcd(n,m) = d$ then $\gcd(Q_n(z,y), Q_m(a,b)) = Q_d(a,b)$ for all a, b relatively coprime.

Proof: Suppose that $|m| > |n|$, then the claim follows from the equality

$$Q_m(a,b) = a^r Q_q(a^{|n|}, b^{|n|})Q_n(a,b) + b^{2(|m|-r)}Q_r(a,b), \tag{4.3}$$

where $|m| = q|n| + r$ and the Euclid's Algorithm.

Note that since $(n,m) \in \mathcal{P}\times\mathcal{P}\setminus\Delta$, then n and m are coprime and $\gcd(Q_n(z,y), Q_m(z,y)) = Q_1(z,y) = 1$. By the previous lemma we only have to check the conditions (1) to (4). The first one is trivial.

(2) For the condition (2) we see first that $Q_n(z,y)$ and $Q_m(z,y)$ are primary in K. Since $y^2 \equiv z^2 \pmod{4\mathcal{O}_K}$ then

$$\begin{aligned} Q_n(z,y) =& \operatorname{sgn}(n)\sum_{i=1}^{|n|} z^{2(|n|-i)}y^{2(i-1)} \equiv \operatorname{sgn}(n)\sum_{i=1}^{|n|} z^{2(|n|-i)}z^{2(i-1)} \pmod{4\mathcal{O}_K} \\ \equiv& \operatorname{sgn}(n)|n|z^{2(|n|-1)} \equiv nz^{2(|n|-1)} \pmod{4\mathcal{O}_K} \end{aligned}$$

and since n is primary, $n \equiv x^2 \pmod 4$ so $Q_n(z,y) \equiv x^2 z^{2(|n|-1)} \pmod{4\mathcal{O}_K}$ and it is primary. The same argument works for $Q_m(z,y)$.

Now observe that if σ is a real embedding of K, the sign of $\sigma(Q_n(z,y))$ coincides with the sign of n because

$$\sigma\left(\frac{z^{2|n|}-y^{2|n|}}{z^2-y^2}\right) = \frac{\sigma(z)^{2|n|}-\sigma(y)^{2|n|}}{\sigma(z)^2-\sigma(y)^2} = \sum_{i=1}^{|n|}\sigma(z)^{2(|n|-1)}\sigma(y)^{2(i-1)} > 0.$$

Using this fact and the general reciprocity law on primary elements (Proposition 4.5), we get

$$\left(\frac{Q_n(z,y)}{Q_m(z,y)}\right)\left(\frac{Q_m(z,y)}{Q_n(z,y)}\right) = \prod_{i=1}^{r}(-1)^{\frac{\operatorname{sgn}(n)-1}{2}\frac{\operatorname{sgn}(m)-1}{2}}$$

and since r is odd we also get the condition (2).

(3) We use again the equality 4.3 to observe that if $m_1 \equiv m_2 \pmod{n}$ then $Q_{m_1}(z,y) \equiv Q_{m_2}(z,y) \pmod{Q_n(z,y)}$. By a property of the power residue symbol we get the condition (3).

(4) If $m_1 + m_2 \equiv 0 \pmod{n}$ then $m_1 \equiv -m_2 \pmod{n}$ and by (3) we get

$$\left(\frac{Q_{m_1}(z,y)}{Q_n(z,y)}\right) = \left(\frac{Q_{-m_2}(z,y)}{Q_n(z,y)}\right) = \left(\frac{-Q_{m_2}(z,y)}{Q_n(z,y)}\right) = \left(\frac{-1}{Q_n(z,y)}\right)\left(\frac{Q_{m_2}(z,y)}{Q_n(z,y)}\right).$$

Since the 2-power residue symbol is multiplicative. Using (2) we obtain

$$\left(\frac{-1}{Q_n(z,y)}\right) = \left(\frac{Q_{-1}(z,y)}{Q_n(z,y)}\right) = (-1)^{\frac{\mathrm{sgn}(-1)-1}{2}\frac{\mathrm{sgn}(n)-1}{2}}\left(\frac{Q_n(z,y)}{Q_{-1}(z,y)}\right) = (-1)^{\frac{\mathrm{sgn}(n)-1}{2}}$$

since $\left(\frac{Q_n(z,y)}{Q_{-1}(z,y)}\right) = \left(\frac{Q_n(z,y)}{-1}\right) = 1$. Finally,

$$\left(\frac{Q_{m_1}(z,y)}{Q_n(z,y)}\right) = (-1)^{\frac{\mathrm{sgn}(n)-1}{2}}\left(\frac{Q_{m_2}(z,y)}{Q_n(z,y)}\right).$$

Once we've checked all the conditions of lemma 4.3, we obtain that

$$f(n,m) = \left(\frac{Q_n(z,y)}{Q_m(z,y)}\right) = \left(\frac{n}{m}\right)$$

is the Jacobi symbol of n and m.

Now let $p \in \mathbb{Z}$ be an odd prime, we want to see that the ideal generated by $Q_p(z,y)$ is not a square. Since p is not a square, $p^* = (-1)^{\frac{p-1}{2}}p = \pm p$ is also not square and now it is primary (a square modulo 4). Then there exists some prime primary number $l \in \mathbb{Z}$ such that p^* is not a square modulo l and the Jacobi symbol is $\left(\frac{p^*}{l}\right) = -1$. Then,

$$-1 = \left(\frac{p^*}{l}\right) = (-1)^{\frac{\mathrm{sgn}(p*)-1}{2}\frac{\mathrm{sgn}(l)-1}{2}}\left(\frac{l}{p^*}\right) = \left(\frac{l}{p^*}\right) = \left(\frac{Q_l(z,y)}{Q_{p^*}(z,y)}\right).$$

Therefore, by the power residue symbol theory, the ideal $Q_{p^*}(z,y)\mathcal{O}_K$, which coincides with the ideal $Q_p(z,y)\mathcal{O}_K$, is not the square of any ideal in $\mathcal{O}_K$.

□

With this strong result we can extend Terjanian's theorem in a number field of odd degree and odd class number with the following theorem of Hellegouarch.

Theorem 4.11 (Hellegouarch)**.** *Let K be a number field of odd degree and odd class number, if $x, y, z \in \mathcal{O}_K$ and y or z coprime with 2, $\epsilon \in \mathcal{O}_K^*$, $\gamma \in \mathbb{Z}$ satisfy*

$$\epsilon 4^\gamma x^{2p} + y^{2p} = z^{2p}$$

with $p > C(K, \gamma)$, then p and x are not coprime.

In the proof of this theorem we use the existence of a field called Hilbert class field H which is the maximal abelian unramified extension of K. Its degree over K is the class number of K and every ideal of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_H$.

Proof. Suppose that we have x, y, z, ϵ and γ satisfying the hypothesis, then

$$z^{2p} - y^{2p} = \epsilon 4^\gamma x^{2p}. \tag{4.4}$$

Consider the ideal generated by y and z in $\mathcal{O}_H$, which is principal, generated by some element $d \in \mathcal{O}_H$. Then divide the equation (4.4) by d^{2p} and obtain

$$z'^{2p} - y'^{2p} = \epsilon 4^\gamma x'^{2p} \tag{4.5}$$

with $y' = \frac{y}{d}$, $z' = \frac{z}{d}$ and $x' = \frac{x}{d}$. It's clear that $y', z' \in \mathcal{O}_H$ and they are coprime. A priori $x' \notin \mathcal{O}_H$ but since $d^{2p} \mid 4^\gamma x^{2p}$ then $d^p \mid 2^\gamma x^p$ and $2^\gamma x' \in \mathcal{O}_H$. Observe that taking p big enough $d^p \mid x^p$ and then we'll have $x' \in \mathcal{O}_H$ also. This is because if $\mathfrak{q}_i$ with $1 \leq i \leq s$, are the prime ideals in 2 and $v_i(2)$ its valuation, then taking $p > \gamma v_i(2)$ for all i then if $d^p \mid 2^\gamma$,

$$d^p \mid \mathfrak{q}_1^{\gamma v_1(2)} \cdots \mathfrak{q}_r^{\gamma v_s(2)} \implies d^p \mid \mathfrak{q}_1^{\gamma \sup_i v_i(2)} \cdots \mathfrak{q}_r^{\gamma \sup_i v_i(2)} \implies d \mid \mathfrak{q}_1 \cdots \mathfrak{q}_s \implies d \mid 2$$

and this is a contradiction since d is the generator of the ideal $(y, z)\mathcal{O}_H$ and one of y or z is coprime with 2.

Now we have $y', z' \in \mathcal{O}_H$ coprime, coprime with 2 (by the equation), and a number field H with degree

$$[H : \mathbb{Q}] = [H : K][K : \mathbb{Q}]$$

which is odd. In order to use theorem 4.10 it remains to see the $y'^2 \equiv z'^2 \pmod{4\mathcal{O}_H}$.

Since $z'^{2p} - y'^{2p} \equiv 0 \pmod{4\mathcal{O}_H}$ and supposing that z' is coprime with 2, we obtain

$$\left(\frac{y'^2}{z'^2}\right)^p \equiv 1 \pmod{4\mathcal{O}_H}.$$

If p is big enough such that it doesn't divide the degree of the finite group $(\mathcal{O}_H/4\mathcal{O}_H)^*$, then $\frac{y'^2}{z'^2}$ is a pth root of unity in the ring $\mathcal{O}_H/4\mathcal{O}_H$ and if p is coprime with the degree of the group,

$$\frac{y'^2}{z'^2} \equiv 1 \pmod{4\mathcal{O}_H} \implies y'^2 \equiv z'^2 \pmod{4\mathcal{O}_H}.$$

By theorem 4.10, the ideal $\left(\frac{z'^{2p}-y'^{2p}}{z'^2-y'^2}\right)\mathcal{O}_H$ is not a square of any ideal of $\mathcal{O}_H$. On the other hand, the equation (4.5) implies that the ideal

$$(z'^{2p}-y'^{2p})\mathcal{O}_H = \left(\frac{z'^{2p}-y'^{2p}}{z'^2-y'^2}\right)\mathcal{O}_H(z'^2-y'^2)\mathcal{O}_H$$

is a square. Where we can deduce that the ideals $\left(\frac{z'^{2p}-y'^{2p}}{z'^2-y'^2}\right)\mathcal{O}_H$ and $(z'^2-y'^2)\mathcal{O}_H$ must be non-coprime. Let $\mathfrak{q}$ be a common prime divisor of both ideals, then by the expression of $\frac{z'^{2p}-y'^{2p}}{x'^2-y'^2}$ we obtain

$$0 \equiv \frac{z'^{2p}-y'^{2p}}{x'^2-y'^2} \equiv pz'^{2(p-1)} \equiv py'^{2(p-1)} \pmod{\mathfrak{q}}$$

and since y', z' are coprime, $\mathfrak{q}$ must divide p. Since $\mathfrak{q} \mid z'^{2p}-y'^{2p}$ then $\mathfrak{q} \mid 4^\gamma x'^{2p}$ and since $\mathfrak{q}$ is prime and not dividing 2 we get also $\mathfrak{q} \mid x$. Finally, since p and x are also in $\mathcal{O}_K$, the ideal can be considered in $\mathcal{O}_K$, so p and x are not coprime.

□

The actual proof of Fermat Last Theorem

All of the results we've seen above are based on work in algebraic number theory, none of it uses elliptic curves. The first person to suggest a connection between elliptic curves and Fermat's Last Theorem was Yves Hellegouarch. In his 1972 doctoral thesis, Hellegouarch associates to any non-trivial solution (a, b, c) of $a^l + b^l = c^l$ with l an odd prime, the elliptic curve

$$E_{a,b,c} : y^2 = x(x - a^l)(x + b^l).$$

Hellegouarch did not make much progress with this, but in 1986, Gerhard Frey had the insight that these construction might provide a precise link between Fermat's Last Theorem and deep questions in the theory of elliptic curves, most notably the Shimura Taniyama conjecture.

Given a solution $a^l + b^l = c^l$ to the Fermat equation of prime degree l, we may assume without loss of generality that a $a^l \equiv -1 \pmod 4$ and $b^l \equiv 0 \pmod{32}$ (note that p is odd so we multiply both sides by -1 if necessary to achieve this). Frey considered the elliptic curve (following Hellegouarch)

$$E_{a,b,c} : y^2 = x(x - a^l)(x + b^l)$$

which can be seen that it is semistable. Proving Fermat's Last Theorem then amounted to showing that no such elliptic curve $E_{a,b,c}$ can exist. Frey suggested that the elliptic curve $E_{a,b,c}$ if it existed, could not possibly be modular.

Shortly thereafter, Jean-Pierre Serre reduced Frey's conjecture to a much more precise statement about modular forms and Galois representations, known as the epsilon conjecture, which was proved by Ken Ribet a few years later. Applied in the case of the curve $E_{a,b,c}$, Serre's conjecture predicted that the Galois respresentation associated to $E_{a,b,c}$ would correspond to a modular form mod l of weight two and level two. Such modular forms, which correspond to differentials on the modular curve $X_0(2)$, do not exist because $X_0(2)$ has genus 0.

The final and most difficult step was to show that if the elliptic curve $E_{a,b,c}$ exists, then in fact it is modular, yielding a contradiction. Andrew Wiles, with the assistance of Richard Taylor, proved the stronger statement that every semistable elliptic curve over $\mathbb{Q}$ is modular (Shimura-Taniyama conjecture for semistable elliptic curves, see [25]), providing the final missing step and proving Fermat's Last Theorem.

References

[1] Artin, E., Tate, J., *Class field theory.* Reprinted with corrections from the 1967 original. AMS Chelsea Publishing, Providence, RI, 2009.

[2] Cassels J.W.S. and Frohlich A., *Algebraic Number Theory*, Academic Press, New York (1967).

[3] Cohen H., *Number theory. Vol. I. Tools and Diophantine equations.* Graduate Texts in Mathematics, 239. Springer, New York, 2007.

[4] Darmon H., Diamond F., Taylor R., Fermat's Last Theorem, September 9, 2007.

[5] Hellegouarch Y., Théorème de Terjanian généralisé. Sém. Théor. Nombres Bordeaux (2) 2 (1990), no. 2, 245–254.

[6] Ireland K. and Rosen M., *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[7] Lang S., *Cyclotomic Fields I and II*, Springer-Verlag, New York, 1994.

[8] Lang S., *Algebraic number theory.* Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[9] Lemmermeyer F., *Reciprocity laws. From Euler to Eisenstein.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[10] Lorenz F., *Algebra. Vol. II. Fields with structure, algebras and advanced topics.* Translated from the German by Silvio Levy. With the collaboration of Levy. Universitext. Springer, New York, 2008.

[11] Milne J. S., Class field theory. 2013. `http://www.jmilne.org/math/CourseNotes/CFT.pdf`.

[12] Neukirch J., *Class field theory.* Springer-Verlag, Heidelberg, 2013.

[13] Neukirch J., *Algebraic number theory.* Springer-Verlag, Berlin, 1999.

[14] Quême R., On Furtwängler's theorems and second case of Fermat's Last Theorem. 2013.

[15] Riddle, L., Sophie Germain and Fermat's Last Theorem, Agnes Scott College, 2009. http://www.agnesscott.edu/Lriddle/women/germain-FLT/SGandFLT.htm.

[16] Riehl E., Kummer's Special Case of Fermat's Last Theorem. May 18, 2005.

[17] Ribenboim P., *13 lectures on Fermat's last theorem*. Springer-Verlag, New York-Heidelberg, 1979.

[18] Shastri P., Reciprocity laws: Artin-Hilbert. Cyclotomic fields and related topics, Bhaskaracharya Pratishthana, Pune, 2000.

[19] Shmid P., On Eisenstein reciprocity. April 2015. https://www.researchgate.net/publication/273916477_On_Eisenstein_reciprocity.

[20] Sukumar Das A., The early reciprocity laws: from Gauss to Eisenstein. Cyclotomic fields and related topics, Bhaskaracharya Pratishthana, Pune, 2000.

[21] Travesa A., Teoria de nombres. https://atlas.mat.ub.edu/personals/travesa/.

[22] Terjanian G., Sur l'équation $x^{2p} + y^{2p} = z^{2p}$. C. R. Acad. Sci. Paris Sér. A-B 285 (1977).

[23] Varma I., Kummer, regular primes, and Fermat's las theorem, California institute of technology.

[24] Washington L., *An Introduction to Cyclotomic Fields*. 2nd ed., Springer-Verlag, New York, 1997.

[25] Wiles A., Modular elliptic curves and Fermat's Last Theorem, *Annals of Math.* 141 (1995), 443–551.