UNIVERSITÉ Grenoble Alpes

INSTITUT FOURIER

TRAVAIL D'ÉTUDE ET DE RECHERCHE

DEUXIÈME SEMESTRE 2020-2021

Loi de réciprocité quadratique

Liticia RENAULT

Professeurs référents :
MONSIEUR ESTANISLAO HERSCOVICH
MONSIEUR GREGORY MC SHANE

Remerciements

Je remercie Monsieur Estanislao Herscovich pour ses astuces précieuses en La Tex, pour son aide concernant les références, et pour ses conseils relatifs à la direction de mon Travail d'Étude et de Recherche.

Je remercie Moniseur Gregory Mc Shane pour l'élaboration de ce sujet qui m'a passionnée, et pour le temps qu'il m'a accordé.

Je remercie Madame Odile Garotta qui a bien voulu lire et annoter mon travail de remarques et corrections qui m'ont réellement permises d'améliorer la qualité de mon rendu.

Enfin, je remercie Monsieur Didier Piau qui a veillé à la bonne progression de mon Travail d'Étude et de Recherche au cours du Semestre.

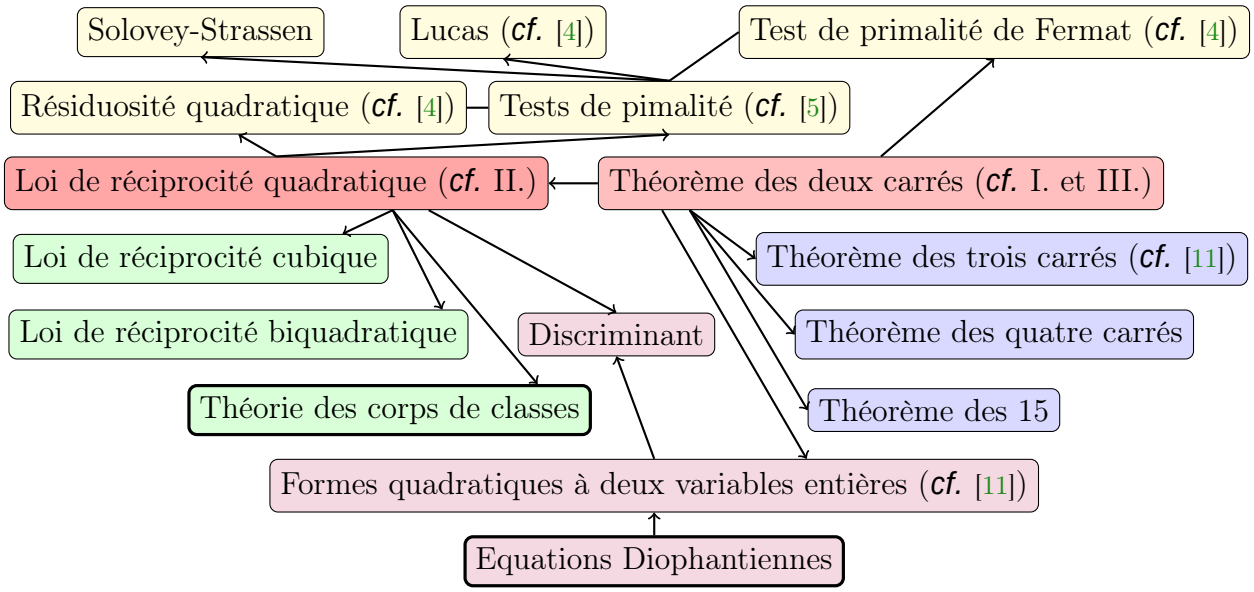
Sommaire

1 Introduction

Ce Travail d'Étude et de Recherche aborde dans un premier temps le Théorème des deux carrés de Fermat sous trois angles qui exposent respectivement une interprétation géométrique, un lien avec l'arithmétique modulaire puis un éclairage par les réseaux euclidiens. Dans un deuxième temps, on introduit la Loi de réciprocité quadratique par les sommes de Gauss et on utilise les résultats étudiés dans la première partie pour en construire la preuve. Enfin, dans une troisième partie, on complète les preuves d'existence d'une décompostion en somme de deux carrés (vues à la partie 1) par un algorithme permettant d'exhiber une telle décomposition en utilisant la Loi de réciprocité quadratique.

Ce choix est en outre chronologiquement cohérent avec l'Histoire puisque le Théorème des deux carrés est énoncé par Fermat en 1640, démontré dans les années 1740 par Euler (en extrayant au passage un test de primalité) qui, dans le même temps, conjecture la Loi de réciprocité quadratique, elle-même démontrée par Gauss en 1801.

On trouve de nombreuses applications à ces deux théorèmes (qui ne seront pas abordées dans ce document), notamment en cryptographie où la Loi de réciprocité quadratique simplifie les calculs dans la résolution du problème de résiduosité quadratique, et permet d'élaborer des tests de primalité (comme les tests de Lucas, ou Solovay-Strassen). Le Théorème des deux carrés a mené à des théorèmes tels que le Théorème des quatre carrés de Lagrange, le Théorème des trois carrés de Legendre, ou le Théorème des 15 de Conway. Lagrange, en repartant du Théorème des deux carrés, étend ses recherches aux formes quadratiques à deux variables puis, grâce à la loi de réciprocité quadratique, établit des résultats sur leur discriminant associé. De plus, la Loi de réciprocité quadratique se généralise, au-delà des Lois de réciprocité cubique et biquadratique, en la Théorie des corps de classe qui répond au 9ième problème de Hilbert. Se référer à [4] et [5] pour des applications détaillées. Voici un aperçu de quelques sujets (qu'on ne traitera pas ici) en lien étroit avec la Loi de réciprocité quadratique et le Théorème des deux carrés :



2 Théorème des deux carrés de Fermat

2.1 La preuve de Don Zagier et son interprétation géométrique par Alexander Spivak

2.1.1 La preuve de Don Zagier

Définition 2.1. *Soit E un nsemble quelconque. Une application* $f : E \longrightarrow E$ *est une involution de* E *si* $f \circ f = Id_E$.

Théorème 2.2 (Théorème des deux carrés)**.** *Tout nombre premier impair* p *peut s'écrire comme la somme de deux carrés d'entiers si et seulement si* p *est de la forme* $4k+1$*, avec* k *dans* $\mathbb{N}^*$.

Preuve de Don Zagier du Théorème des deux carrés. Se référer à [7] et [13].

Hypothèse : p est un nombre premier impair.

"L'involution sur l'ensemble fini $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ définie par :

$$(x, y, z) \longmapsto \begin{cases} (x + 2z, z, y - x - z) & \text{si } x < y - z \\ (2y - x, y, x - y + z) & \text{si } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{si } x > 2y \end{cases}$$

a exactement un point fixe, donc $|S|$ est impair et l'involution définie par $(x, y, z) \longmapsto (x, z, y)$ a aussi un point fixe." □

Remarque 2.3. *Si* $p = 2$*, on a :* $p = 1^2 + 1^2$ *et* p *peut s'écrire comme une somme de deux carrés d'entiers mais* p *n'est pas de la forme* $4k + 1$*. On exclut donc le cas* $p = 2$ *en demandant* p *impair.*

2.1.2 Interprétation géométrique de la preuve

On se réfère pour l'interprétation géométrique de la preuve de Don Zagier à [9].

Remarque 2.4. *Soit* p *un nombre premier impair. Alors* p *est de la forme* $4k+1$ *ou* $4k+3$*. En e et,* p *ne peut pas être de la forme* $4k$ *ou* $4k + 2$*.*

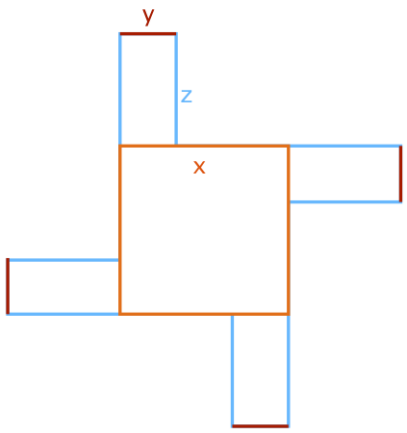
On procède en 2 temps :
1) Si p est de la forme $4k + 1$, p s'écrit comme une somme de deux carrés d'entiers.
2) Si p est de la forme $4k + 3$, il ne peut pas s'écrire comme une somme de deux carrés d'entiers.

1) Si p est de la forme $4k+1$, p s'écrit comme une somme de deux carrés d'entiers :

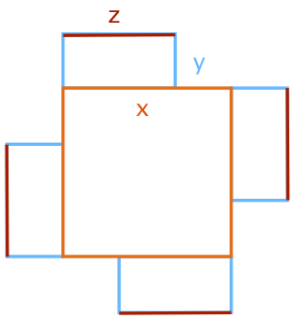
Existence Soit k, u, v des entiers positifs tels que : $p = 4k + 1 = u^2 + v^2$. p est impair, donc l'un des nombres u^2 ou v^2 est pair et l'autre est impair. Or le carré d'un nombre pair est pair et le carré d'un nombre impair est impair. Alors on peut réécrire : $p = x^2 + (2y)^2 = x^2 + 4y^2$, où $u = x$ et $v = 2y$.

On commence par chercher l'ensemble des solutions de : $p = x^2 + 4yz$.
Notons : $S := \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$. Soit $g : S \longrightarrow S$, l'involution $(x, y, z) \longmapsto (x, z, y)$. $Fix(g) = \{(x, y, z) \in S | y = z\}$ seront les solutions qui nous intéressent. En effet : $(x, y, z) \in Fix(g) \Rightarrow y = z$. Donc il suffit de montrer que $Fix(g)$ contient exactement un élément pour conclure que tout nombre premier de la forme $4k + 1$ s'écrit au moins d'une façon comme somme de deux carrés d'entiers.

On représente chaque triplet (x, y, z) de S par le moulin à vent $M_{(x,y,z)}$ suivant :

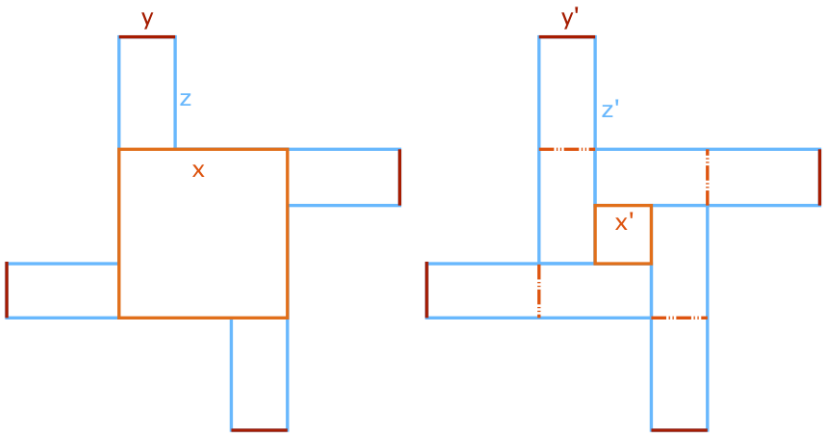


On constate que si $y \neq z$, le moulin à vent $M_{(x,z,y)}$ est différent de $M_{(x,y,z)}$:

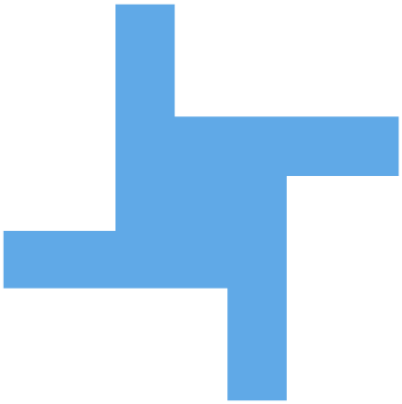


Et si $y = z$, $M_{(x,z,y)}$ est identique à $M_{(x,y,z)}$.

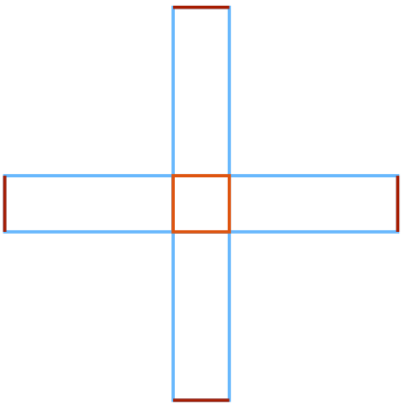
De plus un moulin à vent $M_{(x,y,z)}$ donne une autre solution de l'équation $x^2 + 4yz = p$, représentée par $M_{(x',y',z')}$:



Ces deux moulins à vent forment une paire et on les identifie l'un à l'autre puisque leur "ombre" est la même :

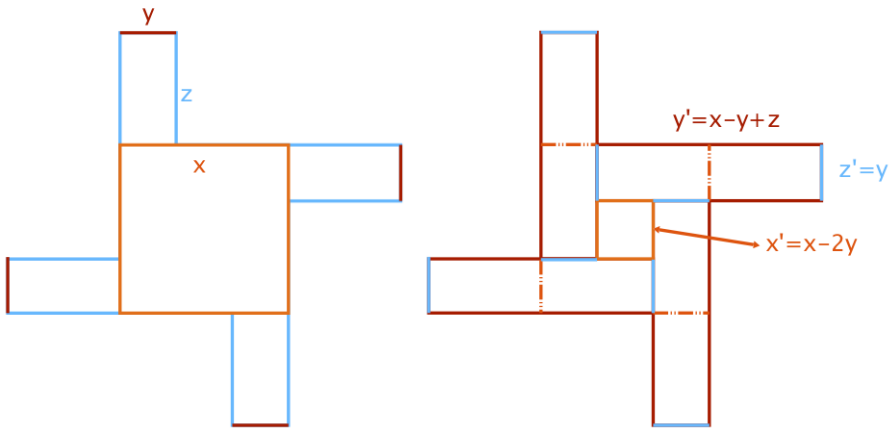


Enfin, on remarque que $M_{(1,1,z)}$ ne donne pas d'autre solution à $x^2 + 4yz = p$ que lui-même :



Idée 2.5. *Quand on considère la paire* $\{M_{(x,y,z)}, M_{(x',y',z')}\}$ *on cherche à expliciter* x', y', z' *en fonction de* x, y, z.

Exemple 2.6. *On a :*



Mais les longueurs doivent rester positives alors on a la contrainte :

$$\begin{cases} x-2y>0 \\ z+x-y>0 \end{cases} \Leftrightarrow \begin{cases} x>2y \\ x-y>0 \end{cases} \Leftrightarrow x>2y$$

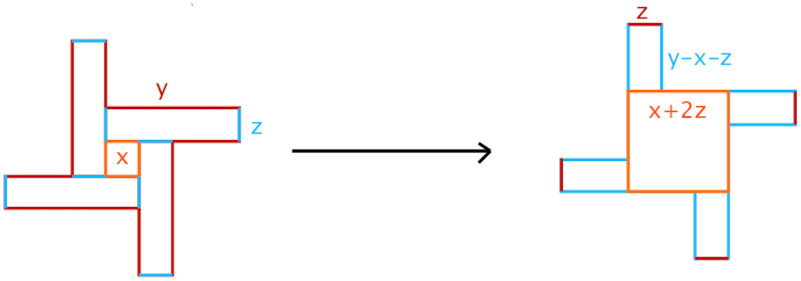
Idée 2.7. *On considère l'involution :*

$$I:(x,y,z)\longmapsto \begin{cases} (x+2z,z,y-x-z) & \text{si } x<y-z \\ (2y-x,y,x-y+z) & \text{si } y-z<x<2y \\ (x-2y,x-y+z,y) & \text{si } x>2y \end{cases}$$

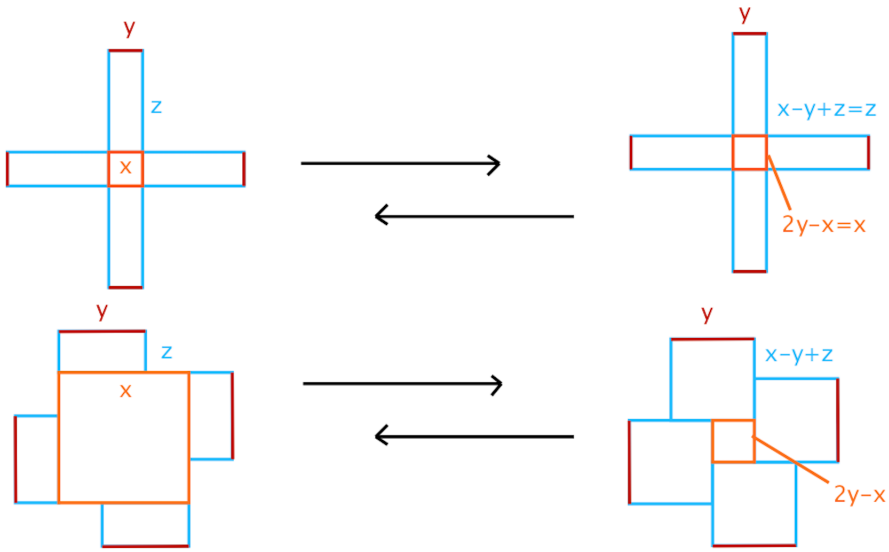
et on la traduit géométriquement en termes de moulins à vent : à chaque moulin à vent, elle associe l'autre moulin à vent qui constitue sa paire.

Illustration de l'involution par les moulins à vent :

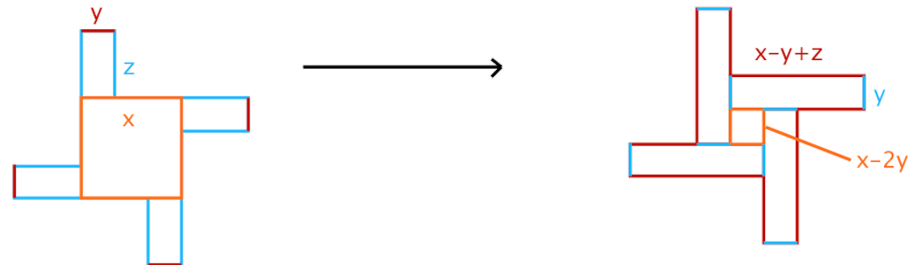
$(x+2z,z,y-x-z)$ si $x<y-z$



$(2y - x, y, x - y + z)$ si $y - z < x < 2y$



$(x - 2y, x - y + z, y)$ si $x > 2y$



Les seuls points fixes de I sont donc représentés par $M_{(x,x,z)}$. Ils vérifient : $p = x^2+4yz = x^2 + 4xz = x(x + 4z)$. Or p est premier impair et $x \leq x + 4z$ donc $x = y = 1$. De plus, p est de la forme $4k + 1$ donc l'unique point fixe de I sur S est $(1, 1, k)$. Finalement, pour tout entier premier impair congru à 1 modulo 4, il n'existe qu'un unique point fixe pour I, et tous les autres triplets de S sont associés en paires par l'involution. Donc $|S|$ est impair. Comme $|S|$ est impair, l'involution g sur S admet au moins un point fixe qui vérifie alors $p = x^2 + 4y^2 = x^2 + (2y)^2$. On a montré que si p est de la forme $4k + 1$ il s'écrit au moins d'une façon comme une somme de deux carrés d'entiers.

Unicité Il reste à montrer l'unicité de cette écriture. Par l'absurde, on suppose que p se décompose de deux manières en somme de deux carrés d'entiers. Soient a,b,c,d des entiers (avec $\{a, b\}$ distinct de $\{c, d\}$) tels que : $p = a^2 + b^2 = c^2 + d^2$. On a :

$$(*) \begin{cases} p^2 = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \\ p^2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \end{cases}$$

Donc p^2 admet aussi deux décompositions distinctes en somme de deux carrés.

D'autre part : $\begin{cases} p = a^2 + b^2 \\ p = c^2 + d^2 \end{cases} \Leftrightarrow \begin{cases} p - a^2 = b^2 \\ p - c^2 = d^2 \end{cases} \Leftrightarrow \begin{cases} d^2(p - a^2) = b^2d^2 \\ b^2(p - c^2) = b^2d^2 \end{cases}$

D'où :

$$\begin{aligned} & d^2(p-a^2) = b^2(p-c^2) \\ \Leftrightarrow\ & d^2p - d^2a^2 = b^2p - b^2c^2 \\ \Leftrightarrow\ & d^2p - b^2p = d^2a^2 - b^2c^2 \\ \Leftrightarrow\ & p(d^2-b^2) = (da)^2 - (bc)^2 \\ \Leftrightarrow\ & p(d^2-b^2) = (da-bc)(da+bc) \end{aligned}$$

D'après le Lemme d'Euclide, p divise $(da-bc)$ ou p divise $(da+bc)$. Si p divise $(da-bc)$, il existe un entier non nul n tel que $da-bc=np$.
Par $(*)$ on obtient :
$p^2 = (ac+bd)^2 + (ad-bc)^2 = (ac+bd)^2 + (np)^2$
C'est impossible car $(ac+bd)^2 > 0$.
Si p divise $(da+bc)$, il existe un entier non nul n tel que $da+bc=np$.
Par $(*)$ on obtient :
$p^2 = (ac-bd)^2 + (ad+bc)^2 = (ac-bd)^2 + (np)^2$
Donc $(ac-bd)^2 = 0$. Donc $ac=bd$. Or comme p est premier et $p=a^2+b^2$, $PGCD(a,b) = PGCD(c,d) = 1$. Donc, par le Lemme de Gauss, a divise d et d divise a. De même b divise c et c divise b. Donc $a=d$ et $b=c$. C'est une contradiction.

2) Si p est de la forme $4k+3$, il ne peut pas s'écrire comme une somme de deux carrés d'entiers :

En fait, on va montrer qu'un entier n (pas forcément premier) congru à 3 modulo 4 ne peut pas s'écrire comme une somme de deux carrés.

Soit n un entier.

- $n \equiv 0 \pmod 4 \Rightarrow n^2 \equiv 0 \pmod 4$
- $n \equiv 1 \pmod 4 \Rightarrow n^2 \equiv 1 \pmod 4$
- $n \equiv 2 \pmod 4 \Rightarrow n^2 \equiv 4 \equiv 0 \pmod 4$
- $n \equiv 3 \pmod 4 \Rightarrow n^2 \equiv 9 \equiv 1 \pmod 4$

Finalement les carrés de $(\mathbb{Z}/4\mathbb{Z})$ sont 0 et 1.

Donc un entier qui s'écrit comme une somme de deux carrés est congru à 0, 1 ou 2 modulo 4 :

+	1	0
1	2	1
0	1	0

Donc les entiers qui sont de la forme $4k + 3$ ne s'écrivent pas comme une somme de deux carrés d'entiers.

2.2 Une preuve en passant par le Théorème de Wilson

Cf. [2] pour une référence concernant une preuve du Théorème des deux carrés utilisant le Théorème de Wilson. *Cf.* 2.2 pour l'énoncé du Théorème des deux carrés.

2.2.1 Si p est une somme de deux carrés alors p est de la forme $4k+1$

Soit x un entier. On a que x^2 est congru à 0 ou 1 modulo 4 (*cf.* 2.1.2). Soient x et y des entiers tels que $p = x^2 + y^2$. Comme p est impair on peut supposer sans perte de généralité que x^2 est pair et y^2 est impair. Donc p est congru à 1 modulo 4.

2.2.2 Si p est de la forme $4k+1$ alors p est une somme de deux carrés

Théorème 2.8 (Théorème de Wilson)**.** *Si p est un nombre premier (donc p>1) alors* $(p-1)! \equiv -1 \pmod{p}$.

preuve de Gauss. On se place dans $\mathbb{F}_p{}^*$. On considère le morphisme de groupes $\phi : x \longmapsto x^2$.
On a $x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow x = 1$ ou $x = -1$ (car $\mathbb{F}_p$ est un corps).
Si $p = 2$, $1 \equiv -1 \pmod 2$. On suppose pour la suite que $p \geq 3$.
Donc $Ker(\phi) = \{1, -1\}$.
Soit ψ l'involution $x \longmapsto x^{-1}$. On a : $Fix(\psi) = \{x | x = x^{-1}\} = Ker(\phi)$
Donc si $p \geq 3$, $\mathbb{F}_p{}^*$ contient $p-3$ éléments qu'on peut associer par paires $\{x, y\}$ telles que $x \neq y$ et $y = x^{-1}$.
Donc $1 \times 2 \times 3 ... \times (p-2) \times (p-1) = (1)^{\frac{p-3}{2}} \times -1 \times 1 = -1$.

□

Lemme 2.9. *Soit p un nombre premier impair. Si $p \equiv 1 \pmod 4$ alors -1 est un carré modulo p.*

Démonstration. On voit bien que :

$$
\begin{aligned}
& -1 \\
& \equiv (p-1)! \pmod p \text{ par le Théorème de Wilson (cf. Théorème 2.8)} \\
& \equiv \left(1.2.3 \ldots \frac{p-1}{2}\right)\left(\frac{p+1}{2}.\frac{p+3}{2} \ldots (p-2)(p-1)\right) \pmod p \\
& \equiv \left(1.2.3 \ldots \frac{p-1}{2}\right)\left((\frac{p+1}{2} - p)(\frac{p+3}{2} - p) \ldots (p-2-p)(p-1-p)\right) \pmod p \\
& \equiv \left(1.2.3 \ldots \frac{p-1}{2}\right)\left(\frac{-p+1}{2}.\frac{-p+3}{2} \ldots (-2)(-1)\right) \pmod p \\
& \equiv \left(1.2.3 \ldots \frac{p-1}{2}\right)\left(\frac{p-1}{2}.\frac{p-3}{2} \ldots 2.1\right).(-1)^{\frac{p-1}{2}} \pmod p \\
& \equiv \left(1.2.3 \ldots \frac{p-1}{2}\right)^2.(-1)^{\frac{p-1}{2}} \pmod p \\
& \equiv \left(1.2.3 \ldots \frac{p-1}{2}\right)^2 \pmod p \text{ car } p \text{ est de la forme } 4k+1 \text{ donc } \frac{p-1}{2} = \frac{4k}{2} = 2k.
\end{aligned}
$$

Finalement on a : $1 + (1.2.3 \ldots \frac{p-1}{2})^2 \equiv 0 \pmod p$. C'est-à-dire qu'il existe un multiple (non nul car $u^2 \neq -1$) de p qui s'écrit comme une somme de deux carrés d'entiers. □

Montrons par la méthode de descente de Fermat que p est une somme de deux carrés :

On va construire par récurrence une suite (m_n) strictement décroissante d'entiers supérieurs ou égaux à 1, qui aboutira en nombre fini N d'étapes à $m_N = 1$.

$(\mathcal{P}_n)$: $\exists x_n, y_n \in \mathbb{Z}$ avec $x_n y_n \neq 0$, $m_n \in \mathbb{N}^*$, $m_n < m_{n-1}$ tel que $m_n p = x_n^2 + y_n^2$

Initialisation : on a vu qu'il existe $u, m \in \mathbb{N}^*$, tels que $mp = u^2 + 1^2$.
On pose $x_0 = u$, $y_0 = 1$, et $m_0 = m$.
Donc $(\mathcal{P}_0)$ est vérifiée.

Récurrence : soit $n \in \mathbb{N}^*$ fixé quelconque. On suppose que $(\mathcal{P}_n)$ est vraie.
Montrons que si $m_n > 1$, $(\mathcal{P}_{n+1})$ est vraie.

Soient r et s tels que $x_n \equiv r \pmod{m_n}$, $\frac{-m_n}{2} < r \leq \frac{m_n}{2}$ et $y_n \equiv s \pmod{m_n}$, $\frac{-m_n}{2} < s \leq \frac{m_n}{2}$. On a : $r^2 + s^2 \equiv x_n^2 + y_n^2 \equiv 0 \pmod{m_n}$. Donc il existe m_{n+1} tel que $r^2 + s^2 = m_{n+1} m_n$.

On en déduit :
• $(r^2 + s^2)(x_n^2 + y_n^2) = (m_{n+1} m_n)(m_n p) = m_{n+1} m_n^2 p$
• $(rx_n + sy_n)^2 + (ry_n - sx_n)^2 = r^2 x_n^2 + 2rx_n sy_n + s^2 y_n^2 + r^2 y_n^2 - 2rx_n sy_n + s^2 x_n^2 = r^2(x_n^2 + y_n^2) + s^2(x_n^2 + y_n^2) = (r^2 + s^2)(x_n^2 + y_n^2)$
• $\exists a, b$ tels que
$$\begin{cases} rx_n + sy_n = r(am_n + r) + s(bm_n + s) = m_n(ra + sb) + r^2 + s^2 = m_n(ra + sb + m_{n+1}) \\ ry_n - sx_n = r(bm_n + s) - s(am_n + r) = m_n(rb - sa) + rs - sr = m_n(rb - sa) \end{cases}$$
D'où : $(rx_n + sy_n)^2 + (ry_n - sx_n)^2 = m_{n+1} m_n^2 p \Leftrightarrow (ra + sb + m_{n+1})^2 + (rb - sa)^2 = m_{n+1} p$.

Il reste à montrer que $0 < m_{n+1} < m_n$.
On suppose par l'absurde que $m_{n+1} = 0$.
$m_{n+1} = 0 \Rightarrow r^2 + s^2 = 0 \Rightarrow r = s = 0 \Rightarrow m_n | x_n$ et $m_n | y_n \Rightarrow m_n^2 | (x_n^2 + y_n^2) \Rightarrow m_n | p \Rightarrow m_n = 1$ ou $m_n = p$
Si $m_n = 1$, $x_n^2 + y_n^2 = p$ et on a fini. $(*)$
Si $m_n = p$, on a : $p | x_n$, $p | y_n$ et $p^2 = x_n^2 + y_n^2$ donc sans perte de généralité on a $x_n = p$ et $y_n = 0$ ce qui est impossible car par hypothèse $x_n y_n \neq 0$.

Montrons que $m_{n+1} < m_n$:
$r^2 + s^2 < 2(\frac{m_n}{2})^2 \Rightarrow m_{n+1} m_n < \frac{2m_n^2}{4} \Rightarrow m_{n+1} < \frac{m_n}{2} < m_n$.

$(\mathcal{P}_{n+1})$ est vraie. Par $(*)$ et comme $(m_n)_{n \geq 0}$ est strictement décroissante et minorée par 1, il existe un rang N tel que $m_N = 1$, où l'on s'arrête.

2.3 Une preuve en passant par les réseaux

Pour toute cette partie, se référer à [6].

Définition 2.10. *Soit R un réseau d'un espace vectoriel V. On définit une norme N sur R par :* $N(R) := \min_{x \in R \setminus \{0\}} ||x||$

Théorème 2.11 (Inégalité de Hermite)**.** *Si R est un réseau euclidien, il existe une base $(e_1, ..., e_n)$ telle que* $||e_1|| \cdot ||e_2|| \cdot ... \cdot ||e_n|| \leq (\frac{4}{3})^{\frac{n(n-1)}{4}} \cdot |det(R)|$.

Corollaire 2.12. $N(R) \leq (\frac{4}{3})^{\frac{n-1}{4}} \cdot |det(R)|^{\frac{1}{n}}$.

Preuve du théorème des deux carrés de Fermat. Comme p est congru à 1 modulo 4, on a que 4 divise $(p-1)$.
Donc 4 divise l'ordre du groupe $(\mathbb{Z}/p\mathbb{Z})^*$.
De plus $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique donc il contient un élément n_0 d'ordre 4.
En particulier, n_0 vérifie : $\begin{cases} n_0^4 \equiv 1 \pmod{p} \\ n_0^2 \not\equiv 1 \pmod{p} \end{cases}$
Donc : $n_0^2 \equiv -1 \pmod{p}$ $(\star)$

Soit R le réseau de $\mathbb{R}^2$ engendré par $\begin{pmatrix} 1 \\ n_0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ p \end{pmatrix}$ qui forment une base B de R.
On a : $|det(R)| = p$.
Alors d'après le corollaire avec $n = 2$ on a : $\exists x \in R$, $||x|| = N(R) \leq (\frac{4}{3})^{\frac{1}{4}} \cdot |det(R)|^{\frac{1}{2}} = (\frac{4}{3})^{\frac{1}{4}} \cdot \sqrt{p}$. Ainsi en majorant $\sqrt{\frac{4}{3}}$ par 2 on a : $0 < ||x||^2 < 2p$ $(\star\star)$.
Ecrivons x dans la base B, soient u et v des entiers relatifs tels que :
$x = u \begin{pmatrix} 1 \\ n_0 \end{pmatrix} + v \begin{pmatrix} 0 \\ p \end{pmatrix}$.
On obtient : $||x||^2 = || \begin{pmatrix} u \\ u \cdot n_0 + v \cdot p \end{pmatrix} ||^2 = u^2 + (u \cdot n_0 + v \cdot p)^2$.
D'où :
$(\star\star)$
$\Leftrightarrow 0 < u^2 + (u \cdot n_0 + v \cdot p)^2 < 2p$
$\Leftrightarrow 0 < u^2(1 + n_0^2) + p(2 \cdot u \cdot n_0 \cdot v + v^2 \cdot p) < 2p$.

Or : $\begin{cases} p(2 \cdot u \cdot n_0 \cdot v + v^2 \cdot p) \equiv 0 \pmod{p} \\ u^2(1 + n_0^2) \equiv 0 \pmod{p} \end{cases}$ par $(\star)$

Donc $||x||^2 \equiv 0 \pmod{p}$, donc $||x||^2 = p$ par $(\star\star)$.

Finalement, on a bien exprimé p comme une somme de deux carrés d'entiers :
$p = u^2 + (u \cdot n_0 + v \cdot p)^2$. □

3 Loi de réciprocité quadratique par les sommes de Gauss

3.1 Sommes de Gauss, symbole de Legendre-Jacobi et ses propriétés

Définition 3.1. *Soient a et n des entiers $(n > 1)$. On dit que a est un résidu quadratique modulo n si il existe un entier x tel que $a \equiv x^2 \pmod{n}$.*

Définition 3.2. *Soient p un nombre premier impair et a un entier relatif. Le symbole de Legendre est tel que :*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p|a \\ 1 & \text{si } p \nmid a \text{ et } a \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } p \nmid a \text{ et } a \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

Critère 3.3 (Critère d'Euler)**.** $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Démonstration.

$$\begin{aligned} & a \text{ est un résidu quadratique modulo } p \\ \Leftrightarrow\ & \exists x \text{ tq } a \equiv x^2 \pmod{p} \\ \Leftrightarrow\ & x \not\equiv 0 \pmod{p} \text{ et } a \text{ racine de } X^{\frac{p-1}{2}} - 1 \text{ dans } \mathbb{Z}/p\mathbb{Z}, \text{ ou } x \equiv 0 \pmod{p} \\ \Leftrightarrow\ & a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ ou } p|a \text{ (et } a^{\frac{p-1}{2}} \equiv 0 \pmod{p}) \end{aligned}$$

De plus, le petit théorème de Fermat nous dit que $a^{p-1} \equiv 1 \pmod{p}$. Donc a n'est pas un carré modulo p si et seulement si $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Proposition 3.4. *$\mathbb{F}_p{}^*$ contient $\frac{p-1}{2}$ carrés.*

Démonstration. On considère le morphisme : $\begin{array}{ccccc} f & : & \mathbb{F}_p{}^* & \to & \mathbb{F}_p{}^* \\ & & x & \mapsto & x^2 \end{array}$, car $Im(f)$ est l'ensemble des carrés de $\mathbb{F}_p{}^*$.
$Ker(f) = \{x \in \mathbb{F}_p{}^* | x^2 = 1\} = \{-1, 1\}$ car $X^2 - 1 = 0$ admet au plus deux racines distinctes sur un corps.
Comme $Im(f) \simeq \mathbb{F}_p{}^*/Ker(f)$ on a $|Im(f)| = |\mathbb{F}_p{}^*/Ker(f)| = \frac{p-1}{2}$ □

Propriété 3.5. *Soient a et b deux entiers relatifs. Alors : $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, et le symbole de Legendre vu comme un morphisme de $(\mathbb{F}_p)^*$ dans $\mathbb{C}^*$ est un caractère multiplicatif de $(\mathbb{F}_p)^*$.*

Démonstration. Soit p un entier premier impair,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \begin{cases} 0 & \text{si } p|a \text{ ou si } p|b \\ 1 & \text{si } p \nmid a \text{ et } p \nmid b \text{ et } \exists x, y \text{ tq } a \equiv x^2 \pmod{p},\ b \equiv y^2 \pmod{p} \\ -1 & \text{si } p \nmid a \text{ et } p \nmid b \text{ et } \nexists x \text{ ou } \nexists y \text{ tq } a \equiv x^2 \pmod{p},\ b \equiv y^2 \pmod{p} \end{cases}$$

$$= \begin{cases} 0 & \text{si } p|ab \\ 1 & \text{si } p\nmid ab \text{ et } \exists x,y \text{ tq } ab \equiv (xy)^2 \pmod p \\ -1 & \text{si } p\nmid ab \text{ et } \nexists x \text{ ou } \nexists y \text{ tq } ab \equiv (xy)^2 \pmod p \end{cases}$$

par le Lemme d'Euclide et les propriétés de la congruence

$$= \begin{cases} 0 & \text{si } p|ab \\ 1 & \text{si } p\nmid ab \text{ et } \exists z \text{ tq } ab \equiv z^2 \pmod p \\ -1 & \text{si } p\nmid ab \text{ et } \nexists z \text{ tq } ab \equiv z^2 \pmod p \end{cases}$$

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

□

Définition 3.6. *Soient $n := \prod_{i=0}^{d} p_i^{\alpha_i}$ un entier écrit dans sa décomposition en facteurs premiers et a un entier relatif. Le symbole de Jacobi est la généralisation du symbole de Legendre tel que :*

$\left(\frac{a}{n}\right) = \left(\frac{a}{\prod_{i=0}^{d} p_i^{\alpha_i}}\right) = \prod_{i=0}^{d} \left(\frac{a}{p_i}\right)^{\alpha_i}$

Définition 3.7. *Soient p et l deux nombres premiers distincts. Soit Ω une clôture algébrique de $\mathbb{F}_p$. Soit ξ une racine primitive $l^{ième}$ de l'unité dans Ω.*
On définit la somme de Gauss par : $y := \sum_{a\in(\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{a}{l}\right)\xi^a$.

Proposition 3.8. $y^2 = \left(\frac{-1}{l}\right) l$ *(avec y définit à la Définition 3.7, donc y est dans $\mathbb{F}_p$)*

Se référencer à [8] pour cette preuve.

Démonstration. On a :

$$y^2$$

$$= \left(\sum_{a\in\mathbb{F}_l{}^*} \left(\frac{a}{l}\right)\xi^a\right)^2$$

$$= \sum_{(a,b)\in(\mathbb{F}_l{}^*)^2} \left(\frac{a}{l}\right)\left(\frac{b}{l}\right)\xi^a\xi^b$$

$$= \sum_{(a,b)\in(\mathbb{F}_l{}^*)^2} \left(\frac{ab}{l}\right)\xi^{a+b} \quad \text{par la Propriété 3.5 de multiplicativité du symbole de Legendre}$$

$$= \sum_{(a,c)\in(\mathbb{F}_l{}^*)^2} \left(\frac{a^2c}{l}\right)\xi^{a+ac} \quad \text{en posant } c = a^{-1}b$$

$$= \sum_{(a,c)\in(\mathbb{F}_l{}^*)^2} \left(\frac{c}{l}\right)\left(\frac{a}{l}\right)^2\xi^{a(1+c)} \quad \text{par la Propriété 3.5 de multiplicativité du symbole de Legendre}$$

$$= \sum_{c\in\mathbb{F}_l{}^*} \left(\left(\frac{c}{l}\right)\sum_{a\in\mathbb{F}_l{}^*}\left(\frac{a}{l}\right)^2\xi^{a(1+c)}\right)$$

$$= \sum_{c\in\mathbb{F}_l{}^*} \left(\left(\frac{c}{l}\right)\sum_{a\in\mathbb{F}_l{}^*}\xi^{a(1+c)}\right) \quad \text{car } \left(\frac{a}{l}\right)^2 = (\pm 1)^2 = 1$$

$$= \left(\frac{-1}{l}\right)(l-1) + \sum_{c\in\mathbb{F}_l{}^*\setminus\{-1\}}\left(\frac{c}{l}\right)(-1) \text{ car } \sum_{a\in\mathbb{F}_l{}^*}\xi^{a(1+c)} = \begin{cases} (l-1) & \text{si } c=-1 \\ -(\xi^{1+c})^0 = (-1) & \text{si } c\neq -1 \end{cases}$$

$$= \left(\frac{-1}{l}\right)(l-1) - \left(\frac{-1}{l}\right)(-1) + \sum_{c\in\mathbb{F}_l{}^*}\left(\frac{c}{l}\right)(-1)$$

$$= \left(\frac{-1}{l}\right) l - \sum_{c\in\mathbb{F}_l{}^*}\left(\frac{c}{l}\right)$$

$= \left(\frac{-1}{l}\right) l$ car d'après 3.4, $\mathbb{F}_l{}^*$ contient autant d'éléments carrés que d'éléments non carrés. □

Proposition 3.9. $y^p = \left(\frac{p}{l}\right) y$ *(avec y définit à la Définition 3.7, donc y est dans $\mathbb{F}_p$)*

Démonstration. Cf. [8] pour une référence à cette preuve.

$$
\begin{aligned}
& y^p \\
&= \left(\sum_{a \in (\mathbb{Z}/l\mathbb{Z})*} \left(\frac{a}{l}\right) \xi^a \right)^p \\
&= \sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{a}{l}\right)^p \xi^{ap} \text{ car } \mathbb{F}_p \text{ est un corps de caractéristique } p \\
&= \sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{a}{l}\right) \xi^{ap} \text{ car } p \text{ est impair (si } \left(\frac{a}{l}\right) \text{ vaut 0,1 ou } -1, \left(\frac{a}{l}\right)^p \text{ vaut bien respectivement 0,1 ou } -1) \\
&= \sum_{b \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{bp^{-1}}{l}\right) \xi^b \text{ par le changement de variable } ap = b, \text{ et } b \in (\mathbb{Z}/l\mathbb{Z})^* \text{ car on est dans } (\mathbb{Z}/l\mathbb{Z})^* \\
&= \sum_{b \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{b}{l}\right) \left(\frac{p^{-1}}{l}\right) \xi^b \text{ par la Propriété 3.5 de multiplicativité du symbole de Legendre} \\
&= \left(\frac{p^{-1}}{l}\right) \sum_{b \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{b}{l}\right) \xi^b \\
&= \left(\frac{p^{-1}}{l}\right) y \\
&= \left(\frac{p}{l}\right) y \text{ car } \begin{cases} p^{-1} \equiv x^2 \pmod{l} \Rightarrow p = p^2 p^{-1} \equiv p^2 x^2 \equiv (px)^2 \pmod{l} \\ p \equiv x^2 \pmod{l} \Rightarrow p^{-1} = p^{-2} p \equiv p^{-2} x^2 \equiv (p^{-1}x)^2 \pmod{l} \end{cases}
\end{aligned}
$$

□

3.2 Enoncés de la Loi de réciprocité quadratique et ses lois complémentaires

Les énoncés 1 et 2 sont équivalents.

Enoncé A :

Loi 3.10 (Première loi complémentaire)**.** *Soit p un nombre premier impair.*
$\exists x$ *tel que* $-1 \equiv x^2 \pmod{p} \Leftrightarrow p \equiv 1 \pmod{4}$

Loi 3.11 (Deuxième loi complémentaire)**.** *Soit p un nombre premier impair.*
$\exists x$ *tel que* $2 \equiv x^2 \pmod{p} \Leftrightarrow p \equiv 1$ *ou* $-1 \pmod{8}$

Théorème 3.12 (Théorème fondamental)**.** *Soient p, q deux nombres premiers impairs distincts.*
•Si p ou $q \equiv 1 \pmod{4}$, alors p est un carré modulo q si et seulement si q est un carré modulo p
•Si p et $q \equiv 3 \pmod{4}$, alors p est un carré modulo q si et seulement si q n'est pas un carré modulo p

Enoncé B :

Loi 3.13 (Première loi complémentaire)**.** *Soit p un nombre premier impair.*
$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Loi 3.14 (Deuxième loi complémentaire)**.** *Soit p un nombre premier impair.*
$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Théorème 3.15 (Théorème fondamental)**.** *Soient p, l deux nombres premiers impairs distincts.*
$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}}$

3.3 Preuve de la Loi de réciprocité quadratique

Pour toute cette partie, se référer à [1], [8] et [11].

3.3.1 Preuve de la première loi complémentaire

Preuve de l'énoncé B 3.13. On rappelle l'énoncé : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, p nombre premier impair.

Si $p \equiv 1 \pmod 4$, alors $(-1)^{\frac{p-1}{2}} = 1$ et $\left(\frac{-1}{p}\right) = 1$ car -1 est un carré modulo p par le Lemme 2.9 du Théorème de Wilson.

Si $p \equiv 3 \pmod 4$, alors $(-1)^{\frac{p-1}{2}} = -1$.
Montrons par l'absurde que -1 n'est pas un carré modulo p :
$-1 \equiv x^2 \pmod p$, alors $(-1)^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod p$ dénote une contradiction.
Donc $\left(\frac{-1}{p}\right) = -1$.

On a bien l'égalité voulue.

□

Remarque 3.16. *On a montré au passage la réciproque du Lemme 2.9 du Théorème de Wilson.*

Proposition 3.17 (équivalence des énoncés A 3.10 et B 3.13)**.** *On a :*

$$\begin{aligned} &(1)\ \exists x, x^2 \equiv -1 \pmod p \\ \Leftrightarrow\ &(2)\ p = 2 \text{ ou } p \equiv 1 \pmod 4 \\ \Leftrightarrow\ &(3)\ \left(\frac{-1}{p}\right) = 1 \end{aligned}$$

Démonstration. On procède en trois temps.
Montrons que (1) $\Rightarrow$ (2)
$x^2 \equiv -1 \pmod p \Rightarrow \begin{cases} x^4 \equiv 1 \pmod p \\ x^2 \not\equiv 1 \pmod p \quad \text{si } p \neq 2 \end{cases} \Rightarrow p = 2$ ou $4|(p-1)$ par Lagrange pour

$(\mathbb{F}_p)^*$.

Montrons que (1) $\Leftarrow$ (2)
$p \equiv 1 \pmod 4 \Rightarrow \exists x$, tq $x^2 \equiv -1 \pmod p$ par le Lemme 2.9.

Montrons que (1) $\Leftrightarrow$ (3)
Par définition de $\left(\frac{-1}{p}\right)$. □

3.3.2 Preuve de la deuxième loi complémentaire

Preuve de l'énoncé B 3.14. On rappelle l'énoncé : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, où p est un nombre premier impair.

On considère le polynôme $P(X) = X^4 + 1$ à coefficients dans le corps $\mathbb{F}_p$. Si x est une racine de P, elle vérifie $x^4 = -1$ (et en particulier x est dans $(\mathbb{F}_p)^*$). Alors on a :
$(x + x^{-1})^4 = x^4 + 4x^2 + 6 + 4x^{-2} + x^{-4} = 4x^2 + 4 + 4x^{-2} = 4(x^2 + xx^{-1} + x^{-2}) = 4((x + x^{-1})^2 - xx^{-1}) = 4((x + x^{-1})^2 - 1)$
Donc le polynome $X^2 - 4X + 4 = (X - 2)^2$ admet pour racine double $(x + x^{-1})^2$. Donc $x + x^{-1}$ est une racine carrée de 2.

Soit $z := x + x^{-1}$. Comme on est sur un corps de caractéristique p, $z^p = x^p + x^{-p}$.

Comme p est premier impair :
$p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4 \Leftrightarrow p \equiv 1$ ou $5 \pmod 8$ ou $p \equiv -5$ ou $-1 \pmod 8$.

Si $p \equiv \pm 1 \pmod 8$
$z^p = x^{\pm 1 + 8k} + x^{\mp 1 - 8k} = x^{\pm 1}x^{8k} + x^{\mp 1}x^{-8k} = x^{\pm 1} + x^{\mp 1} = z$ car $x^4 = -1$. Or $z^2 = 2$, donc $z \neq 0$. Donc $z^{p-1} = 1$. (On trouve donc que $z \in (\mathbb{F}_p)^*$.)
Donc $(\frac{2}{p}) = 2^{\frac{p-1}{2}} = (x + x^{-1})^{p-1} = z^{p-1} = 1$.

Si $p \equiv \pm 5 \pmod 8$
$z^p = x^{\pm 5 + 8k} + x^{\mp 5 - 8k} = x^{\pm 5}x^{8k} + x^{\mp 5}x^{-8k} = x^5 + x^{-5}$ (car $x^4 = -1$).
Or :

$$
\begin{aligned}
& 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 = 0 \\
\Leftrightarrow\ & 1 + x + x^3 - 1 + x^5 + x^7 = 0 && \text{car } x^2 + x^6 = x^2(1 + x^4) = 0 \\
\Leftrightarrow\ & x + x^3 + x^5 + x^7 = 0 \\
\Leftrightarrow\ & x + x^{-5} + x^5 + x^{-1} = 0 \\
\Leftrightarrow\ & x^{-5} + x^5 = -(x + x^{-1}) = -z
\end{aligned}
$$

Donc $z^p = -z$, $z \neq 0$ d'où $z^{p-1} = -1$.
Donc $(\frac{2}{p}) = 2^{\frac{p-1}{2}} = (x + x^{-1})^{p-1} = z^{p-1} = -1$.

On a :

•$p \equiv \pm 1 \pmod 8 \Leftrightarrow \frac{p^2-1}{8}$ est pair $\Leftrightarrow (-1)^{\frac{p^2-1}{8}} = 1$
•$p \equiv \pm 5 \pmod 8 \Leftrightarrow \frac{p^2-1}{8}$ est impair $\Leftrightarrow (-1)^{\frac{p^2-1}{8}} = -1$
Cela achève la preuve et montre l'équivalence entre les énoncés A 3.11 et B 3.14 de la deuxième loi complémentaire. □

3.3.3 Preuve du Théorème fondamental

Preuve de l'énoncé B 3.15. Rappel de l'énoncé : $\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}}$, pour tous nombres premiers impairs distincts p et l. Dans $\mathbb{F}_p$:

$$\begin{aligned}
\left(\frac{p}{l}\right) &= y^{p-1} && \text{par la Proposition 3.9}\\
&= \left(y^2\right)^{\frac{p-1}{2}} &&\\
&= \left(\left(\frac{-1}{l}\right)l\right)^{\frac{p-1}{2}} && \text{par la Proposition 3.8}\\
&= (-1)^{\frac{l-1}{2}\frac{p-1}{2}} l^{\frac{p-1}{2}} && \text{d'après la première loi complémentaire, } \textit{cf.} \text{ Loi 3.13}\\
&= (-1)^{\frac{l-1}{2}\frac{p-1}{2}}\left(\frac{l}{p}\right) && \text{par le critère d'Euler, } \textit{cf.} \text{ Critère 3.3}
\end{aligned}$$

L'égalité $\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\frac{p-1}{2}}\left(\frac{l}{p}\right)$ est vraie dans $\mathbb{F}_p$, $p \geq 3$ donc elle est vraie dans $\mathbb{Z}$ (car p>2 implique $1 \neq -1$ dans $\mathbb{F}_p$).

La traduction de l'énoncé B en termes de congruences donne directement l'énoncé A. □

4 Décomposition en somme de deux carrés

On se pose la question suivante : comment peut-on écrire un agorithme efficace qui trouve les valeurs de α et β pour un entier p premier donné de la forme $4k+1$ tels que $p = \alpha^2 + \beta^2$. Pour toute cette partie se référer à [12].

4.1 Algorithme

Algorithme 4.1. *Soit p un entier congru à 1 modulo 4.*
1) On trouve un x tel que $x^2 \equiv -1 \pmod{p}$.
2) On applique l'algorithme d'Euclide à p et x jusqu'à trouver les deux premiers restes α et β inférieurs à $\sqrt{p}$. On aura bien α et β qui vérifient $p = \alpha^2 + \beta^2$.

Pour rendre efficace l'algorithme, on aura besoin des propriétés suivantes :

Propriété 4.2. *Si p est premier de la forme $4k+1$, $\left(\frac{2}{p}\right) \equiv -1 \pmod{p} \Leftrightarrow p \equiv 5 \pmod{8}$*

Démonstration.

$$\left(\frac{2}{p}\right) \equiv -1 \pmod{p}$$
$$\Leftrightarrow (-1)^{\frac{p^2-1}{8}} \equiv -1 \pmod{p} \quad \text{par la deuxième loi complémentaire, } \textit{cf.} \text{ Loi 3.14}$$
$$\Leftrightarrow (-1)^{\frac{16k^2+8k}{8}} \equiv -1 \pmod{p}$$
$$\Leftrightarrow (-1)^{k(2k+1)} \equiv -1 \pmod{p}$$
$$\Leftrightarrow \exists k' \text{ tq } k = 2k'+1$$
$$\Leftrightarrow \exists k' \text{ tq } p = 4(2k'+1)+1 = 8k'+5$$
$$\Leftrightarrow p \equiv 5 \pmod{8}$$

□

Propriété 4.3. *Si p est premier de la forme $4k+1$, $\left(\frac{3}{p}\right) \equiv -1 \pmod{p} \Leftrightarrow p \equiv 2 \pmod{3}$*

Démonstration.

$$\left(\frac{3}{p}\right) \equiv -1 \pmod{p}$$
$$\Leftrightarrow (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} \left(\frac{p}{3}\right) \equiv -1 \pmod{3} \quad \text{par le Théorème fondamental } \textit{cf.} \text{ Théorème 3.15}$$
$$\Leftrightarrow p^{\frac{3-1}{2}} \equiv 2 \pmod{3} \quad \text{par le Critère 3.3 d'Euler}$$
$$\Leftrightarrow p \equiv 2 \pmod{3}$$

□

Le logiciel utilisé pour cette partie programmation est SageMath 9.1 notebook, pour les références *cf.* [3] et [10].
On implémente un algorithme de décomposition en somme de deux carrés dans une version simplifiée.

Programme 4.4 (Euclide). *On commence par implémenter une fonction Euclide utile pour la suite qui e ectue la division euclidienne de a par b et renvoie la liste des restes successifs.*

```
In [38]: def Euclide(a, b, restes):
             if b ==0 : return restes
             else :
                 restes.append(a%b)
                 #print(restes)
                 return(Euclide(b, a % b, restes))
```

Programme 4.5 (Decompose). *On implémente ensuite une fonction Decompose qui prend en entrée un entier p premier de la forme 4k+1, et trouve a et b tels que $p=a^2+b^2$.*

```
In [47]: def Decompose(p) :
             if ((p%4)!=1)or(is_prime(p)==False) :
                 return "erreur p n'est pas un nombre premier de la forme 4k+1"
             c=5
             L=[]
             borne=int(sqrt(p))
             k=int((p-1)/4)
         # Etape 1 : on cherche x tq x^2 congru à 1 modulo p
         # a) c^((p-1)/2)=-1[p] <=> c^(2k)=-1[p] donc on cherche un tel c
             if ((p%8)==5) : #par la Propriété 4.1
                 c=2
             elif ((p%3)==2) : #par la Propriété 4.2
                 c=3
             else :
                 while(((c^(2*k))%p)!=p-1) :
                     c=next_prime(c)
         #par a) :
             x=c^k
         # Etape 2 :
         # a) on applique l'algorithme d'Euclide à p et x
             restes=Euclide(p,x,[])
             i=0
         # b) les 2 premiers restes < sqrt(p) sont les a et b recherchés
             while(restes[i]>borne):
                 i=i+1
             return(restes[i],restes[i+1])
```

Tests 4.6 (Série de tests pour le Programme Decompose). *On a :*

```
In [48]: Decompose(5)
```

```
Out[48]: (2, 1)
```

```
In [49]: Decompose(13)

Out[49]: (3, 2)

In [50]: Decompose(17)

Out[50]: (4, 1)

In [51]: Decompose(97)

Out[51]: (9, 4)

In [52]: 9^2+4^2

Out[52]: 97

In [53]: Decompose(3)

Out[53]: "erreur p n'est pas un nombre premier de la forme 4k+1"

In [54]: Decompose(9)

Out[54]: "erreur p n'est pas un nombre premier de la forme 4k+1"
```

Ce programme pose problème pour des nombres premiers trop grands :

```
In [32]: Decompose(848654483879497562821)

---------------------------------------------------------------------------
OverflowError                             Traceback (most recent call last)

<ipython-input-32-87086fe65a7d> in <module>()
----> 1 Decompose(Integer(848654483879497562821))


<ipython-input-26-3d5ff09baeeb> in Decompose(p)
     13         c=Integer(3)
     14     else :
---> 15         while(((c**(Integer(2)*k))%p)!=p-Integer(1)) :
     16             c=next_prime(c)
     17 #par a) :


[...]
2220
```

```
   2221         if type(left) is type(right):
-> 2222             return (<Integer>left)._pow_(right)
   2223         elif isinstance(left, Element):
   2224             return coercion_model.bin_op(left, right, operator.pow)


[...]
   2300                 r = smallInteger(1)
   2301         else:
-> 2302             raise OverflowError(f"exponent must be at most {LONG_MAX}")
   2303         if mpz_sgn(exp) >= 0:
   2304             return r


OverflowError: exponent must be at most 9223372036854775807
```

Remarque 4.7. *Pour pallier au problème d'"Overflow" on peut utiliser la loi de réciprocité quadratique :*
$\left(\frac{c}{p}\right) \equiv -1 \pmod{p} \Leftrightarrow \left(\frac{p}{c}\right) \equiv -1 \pmod{c} \Leftrightarrow \left(\frac{d}{c}\right) \equiv -1 \pmod{c}$, *où* d *est le reste de la division de* p *par* c. *On recommence ce procédé jusqu'à trouver c. Pour éviter l'"Overflow" on a aussi besoin d'utiliser :* $a^b \equiv a^{k \cdot ord(a)+r} \equiv a^r \pmod{p}$. *Pour permettre des calculs en temps raisonnable avec de grands exposants (dont on a besoin pour calculer* x^k, *i.e. quand* k *est grand donc quand* p *est grand) on utilise un algorithme d'exponentiation rapide.*

On introduit l'algorithme d'exponentiation rapide suivant :

Programme 4.8 (Exp_LR_mod). *On a :*

```
#renvoie x^n mod(p), attention n doit être de type ring.integer.Integer,
# x et p de type int
In [38]: def Exp_LR_mod(x,n,p):
             if n==0 :
                 return 1
             res=x
             t=int(log(n,2))
             B=n.digits(2) #B=(b_0, b_1,...b_k)
             #on n'écrit pas B.reverse() car on parcourt la liste B de droite à gauche
             while t>0 :
                 t=t-1
                 res=(res^2)%p
                 if B[t]==1 :
                     res=(res*x)%p
             return res
```

Tests 4.9 (Série de tests pour le programme Exp_LR_mod). *Un test sur un très grand nombre premier p=84865448387949756282l dont on sait que c=2 :*

```
In [39]: 848654483879497562820//4 #calcul de k

Out[39]: 212163620969874390705

# c=2, k=212163620969874390705, p=848654483879497562821
In [40]: Exp_LR_mod(2,212163620969874390705,848654483879497562821)

Out[40]: 354060813206257083018

In [88]: #On trouve x=354060813206257083018, on verifie qu'on a bien x^2≡-1[p]
         (354060813206257083018^2)%848654483879497562821

Out[88]: 848654483879497562820
```

Programme 4.10 (Bordre). *On conçoit un programme qui permet de calculer l'ordre d'un élément dans* $(\mathbb{Z}/N\mathbb{Z})^*$ *afin d'accélérer les calculs dans une partie du programme amélioré de Decompose (cf. 4.5) :*

```
# Bordre renvoie 1 pour vrai si ordre(n)=k et 0 pour faux sinon dans (Z/NZ)*
In [42]: def Bordre(n,k,N):
             f=factor(k)
             F=list(f)
             b=1
             if(exp_LR_mod(n,k,N)!=1):
                 b=0
             for i in range(len(F)):
                 d=F[i][0]
                 if (is_prime(d)):
                     if(exp_LR_mod(n,Integer(k/d),N)==1):
                         b=0
             return b
```

Programme 4.11 (Ordre). *A l'aide du Programme 4.10 on calcule l'ordre d'un élément n dans un groupe* $(\mathbb{Z}/N\mathbb{Z})^*$

```
In [43]: def Ordre (n,N):
             i=1
             while(Bordre(n,i,N)==0):
                 i=i+1
             return i
```

Tests 4.12 (Série de tests pour les Programmes 4.10 Bordre et 4.11 Ordre). *On a :*

```
In [44]: Bordre(2,4,4)

Out[44]: 0
```

```
In [45]: Bordre(3,2,4)

Out[45]: 1

In [46]: Ordre(3,4)

Out[46]: 2
```

Enfin on a tous les éléments pour programmer la version améliorée de Decompose.

Programme 4.13 (Decompose1). *Implémentation d'un algorithme de décomposition en somme de deux carrés dans une version améliorée :*

```
In [47]: #prend en entrée un nombre premier p et renvoie x et y tq x^2+y^2=p
         def Decompose1(p) :
             if ((p%4)!=1)or(is_prime(p)==False) :
                 return "erreur p n'est pas un nombre premier de la forme 4k+1"
         #Initialisation des variables
             c=5
             borne=int(sqrt(p))
             k=int((p-1)/4)

         # Etape 1 : on cherche x tq x^2≡1[p]
         # a) c^((p-1)/2)≡-1[p] <=> c^(2k)≡-1[p] donc on cherche un tel c
             if ((p%8)==5) :  #Par la Prop 4.1
                 c=2
             elif ((p%3)==2) :  #Par la Prop 4.2
                 c=3
         #b) utiliser la loi de réciprocité quadratique :
         #(c/p)≡-1[p] <=> (p/c)≡-1[c] <=> (d/c)≡-1[c],où d est le reste de
         la division de p par c
             else :
                 tmp=c
                 d=p%tmp
                 l=int((tmp-1)/4)
                 o=Ordre(d,tmp)
                 puiss=(2*l)%o
                 #on ré-utilise la loi de réciprocité quadratique jusqu'à
                 trouver c
                 while(((d^puiss)%tmp)!=tmp-1) :
                     tmp=next_prime(tmp)
                     d=p%tmp
                     l=int((tmp-1)/4)
                     o=Ordre(d,tmp)
                     puiss=(2*l)%o
                     if ((tmp%8)==5)and(d==2) :  #Par la Prop 4.1
```

```
                c=tmp
            elif ((tmp%3)==2)and(d==3) :  #Par la Prop 4.2
                c=tmp
    #par a) :
        #On utilise l'algorithme d'exponentiation rapide pour calculer x^k,
        sinon le temps de calcul est trop long
        x=Exp_LR_mod(c,ZZ(k),p)
        #ZZ(k) fait passer k du type int au type rings.integer.Integer

    # Etape 2 :
    #a)on applique l'algorithme d'Euclide à p et x
        restes=Euclide(p,x,[])
        i=0
    #b)les deux premiers restes plus petits que sqrt(p) sont les a et b
    recherchés
        while(restes[i]>borne):
            i=i+1
        return(restes[i],restes[i+1])
```

Tests 4.14 (Série de tests pour le programme Decompose1). *On a bien les résultats attendus :*

```
In [48]: Decompose1(97)

Out[48]: (9, 4)

In [49]: Decompose1(73)

Out[49]: (8, 3)

In [50]: Decompose1(848654483879497562821)

Out[50]: (28440994650, 6305894639)

In [51]: 28440994650^2+6305894639^2==848654483879497562821

Out[51]: True

In [52]: Decompose1(5903)

Out[52]: "erreur p n'est pas un nombre premier de la forme 4k+1"

In [70]: 5903%4

Out[70]: 3

In [53]: Decompose1(5981)

Out[53]: (59, 50)
```

```
In [54]: 59^2+50^2==5981

Out[54]: True

In [55]: Decompose1(29989)

Out[55]: (170, 33)

In [56]: 170^2+33^2==29989

Out[56]: True

In [58]: Decompose1(49993)

Out[58]: (213, 68)

In [59]: 213^2+68^2==49993

Out[59]: True

In [66]: Decompose1(3203431780337)

Out[66]: (1742624, 408281)

In [67]: 1742624^2+408281^2==3203431780337

Out[67]: True

In [75]: Decompose1(618509)

Out[75]: (778, 115)

In [76]: 778^2+115^2==618509

Out[76]: True
```

4.2 Preuve de l'algorithme

Notation 4.15. *On garde les notations suivantes pour toute cette partie. Soient a et b des entiers naturels avec a plus grand que b. Dans l'algorithme d'Euclide appliqué à a et b, on note (q_i) la liste de longueur $n+1$ des quotients successifs avec $q_1 = [a/b]$, $q_2 = [b/r_2], \ldots$ On note (r_i) la liste de longueur $n+2$ des restes successifs avec $r_0 = a$, $r_1 = b$, $r_n = pgcd(a,b)$ et $r_{n+1} = 0$. Ainsi la $i^{ème}$ étape de l'algorithme d'Euclide s'écrit*

$$r_i = r_{i+1}q_{i+1} + r_{i+2} \quad (1)$$

Pour la preuve de l'Algorithme on prendra $a = p$ un entier premier congru à 1 modulo 4 et $b = x$ tel que x^2 soit congru à -1 modulo p.

Définition 4.16. *On définit les suites (s_i) et (t_i) de l'algorithme de Bézout, $i = 0, 1, \ldots, n$, telles que :*

$$r_i = as_i + bt_i \quad (2)$$

On construit ces suites en prenant $t_0 = 0$, $t_1 = 1$ (de sorte qu'on ait bien $r_0 = a$ et $r_1 = b$) et $r_{i+1} = as_{i+1} + bt_{i+1}$ (et par construction s_i et t_i sont définis de manière unique). On pose $t_{n+1} = t_{n-1} - q_n t_n$ pour obtenir un terme supplémentaire sur la suite (t_i) qui nous sera utile.

Propriété 4.17. *On a : $\forall i \in [\![0, n]\!]$, $t_{i+1} = t_{i-1} - q_i t_i$.*

Démonstration. Montrons que la suite (t_i) vérifie la propriété $(\mathcal{P}_i) : t_{i+1} = t_{i-1} - q_i t_i$.
$t_0 = 0$
$t_1 = 1$
$t_2 = t_0 - q_1 t_1 = -q_1$
Soit i un entier naturel fixé quelconque entre 0 et n. On sait que $r_{i-1} = r_i q_i + r_{i+1} = bt_{i-1} + as_{i-1}$ et $r_i = r_{i+1}q_{i+1} + r_{i+2} = bt_i + as_i$.
On a :

$$\begin{aligned} r_{i+1} &= bt_{i+1} + as_{i+1} \\ &= r_{i-1} - r_i q_i \\ &= bt_{i-1} + as_{i-1} - q_i(bt_i + as_i) \\ &= b(t_{i-1} - q_i t_i) + a(s_{i-1} - q_i s_i) \end{aligned}$$

Donc $t_{i+1} = t_{i-1} - t_i q_i$. □

Exemple 4.18. *On prend $a = p = 89$, $b = x = 34$. On a bien que p est premier congru à 1 modulo 4, et x^2 est congru à -1 modulo p. On a :*

$$\begin{aligned} 89 &= 34 \times 2 + 21 & t_2 &= 0 - 2 \times 1 = -2 \\ 34 &= 21 \times 1 + 13 & t_3 &= 1 - 1 \times (-2) = 3 \\ 21 &= 13 \times 1 + 8 & t_4 &= -2 - 1 \times 3 = -5 \\ 13 &= 8 \times 1 + 5 & t_5 &= 3 - 1 \times (-5) = 8 \\ 8 &= 5 \times 1 + 3 & t_6 &= -5 - 1 \times 8 = -13 \\ 5 &= 3 \times 1 + 2 & t_7 &= 8 - 1 \times (-13) = 21 \\ 3 &= 2 \times 1 + 1 & t_8 &= -13 - 1 \times (21) = -34 \end{aligned}$$

Donc on a :

i	q_i	r_i	t_i
0		89	0
1	2	34	1
2	1	21	-2
3	1	13	3
4	1	8	-5
5	1	5	8
6	1	3	-13
7	1	2	21
8	1	1	-34
9	2	0	89

On remarque qu'on a $n = 8$, que la suite $(|t_i|)$ renversée est identique à la suite (r_i), que la suite (t_i) est alternée, que la suite (q_i) est symétrique par rapport à son centre, et que $r_{\frac{n}{2}}$ est le premier reste strictement inférieur à $\sqrt{p}$. Ici on trouve que $89 = 8^2 + 5^2$.

Propriété 4.19. *La suite (t_i) est de signes alternés.*

Démonstration. Montrons par récurrence que la suite (t_i) est alternée :
$t_0 = 0$
$t_1 = 1$
$t_2 = t_0 - q_1 t_1 = -q_1 \leq 0$
Soit la propriété $(\mathcal{P}_i) : sgn(t_i) = (-1)^{i+1}$.
Soit i un entier naturel fixé quelconque entre 1 et n, on suppose que $(\mathcal{P}_i)$ et $(\mathcal{P}_{i-1})$ sont vraies.
Montrons que $(\mathcal{P}_{i+1})$ est vraie :
$sgn(t_{i+1}) = sgn(t_{i-1} - q_i t_i) = sgn(-t_{i-1})$ car q_i est positif et t_{i-1} et t_i sont de signes opposés.
Donc : $sgn(t_{i+1}) = -1 \times (-1)^{i+1} = (-1)^{i+2}$.

□

Propriété 4.20. *On a : $\forall i \in [\![0, n]\!]$, $|t_{i+1}| = |t_{i-1}| + q_i|t_i|$.*

Démonstration. D'après la Propriété 4.17, on a : $|t_{i+1}| = |t_{i-1} - q_i t_i|$. Or d'après la Propriété 4.19, les t_i sont alternés et par ailleurs les q_i sont positifs. Donc t_{i-1} est de même signe que $-q_i t_i$. Donc on a le résultat voulu. □

Propriété 4.21. *La suite $(|t_i|)$ est strictement croissante pour $i \geq 2$.*

Démonstration. On sait que : $\forall i \in [\![1, n+1]\!]$, $q_i \geq 1$. En particulier on a : $|t_2| = q_1$, $|t_1| = 1$, $|t_0| = 0$ donc $|t_2| \geq |t_1| > |t_0|$. De plus : $\forall i \in [\![1, n+1]\!]$, $t_i \geq 1$ car $r_i = as_i$ est impossible. Par ailleurs : $\forall i \in [\![1, n+1]\!]$, $q_i \geq 1$. La Propriété 4.20 nous donne $|t_{i+1}| = |t_{i-1}| + q_i|t_i|$, donc pour $i \geq 2$, $|t_{i+1}| \geq 1 + |t_i|$ donc $|t_{i+1}| > |t_i|$. □

Propriété 4.22. *$\{|t_i|, i = n+1, n, \ldots, 1\}$ est la suite des restes successifs pour l'algorithme d'Euclide qui commence par les termes t_{n+1} et t_n.*

Démonstration. Cela découle directement des Propriétés 4.20 et 4.21. □

A l'aide des propriétés précédentes, on montre cinq nouvelles propriétés qui nous permettront de construire la preuve de l'algorithme de décomposition en somme de deux carrés d'un nombre premier p congru à 1 modulo 4. Comme annoncé en début de partie, on se place maintenant dans le cas particulier où $a = p$ et $b = x$.

Formule 4.23. *(Formule d'Euler, admise.) Soient a et b deux entiers tels que $pgcd(a, b) = 1$. Il existe une fonction f qui vérifie $a = f(q_1, \dots, q_n)$, $b = f(q_2, \dots, q_n)$, $r_2 = f(q_3, \dots, q_n)$ avec $a = q_1 b + r_2$. La fonction f prenant en argument une suite $(q_1, q_2, \dots, q_n)$est définie de la façon suivante : on prend le produit des q_i, qu'on ajoute à tous les produits possibles des q_i en omettant un couple de q_i consécutifs, qu'on ajoute à tous les produits possibles des q_i en ommettant deux couples de q_i consécutifs disjoints, qu'on ajoute en omettant trois couples de q_i consécutifs deux à deux disjoints, etc.*
Par exemple :
$f(q_1, q_2, q_3, q_4, q_5, q_6) = q_1q_2q_3q_4q_5 + q_3q_4q_5 + q_1q_4q_5 + q_1q_2q_5 + q_1q_2q_3 + q_5 + q_1 + q_3$
$f(q_1, q_2, q_3, q_4, q_5, q_6) = q_1q_2q_3q_4q_5q_6 + q_3q_4q_5q_6 + q_1q_4q_5q_6 + q_1q_2q_5q_6 + q_1q_2q_3q_6 + q_1q_2q_3q_4 + q_5q_6 + q_1q_6 + q_1q_2 + q_3q_6 + q_3q_4 + q_1q_4$
On remarque que $f(q_1, q_2, \dots, q_n) = f(q_n, q_{n-1}, \dots, q_1)$, puisque les couples d'éléments consécutifs sont préservés.

Propriété 4.24. *La suite $(|t_i|)$ est la suite inversée (c'est à dire en remontant les indices à l'envers) de la suite (r_i).*

Démonstration. On a : $|t_{i+1}| = |t_{i-1}| + q_i|t_i|$ et $r_i = r_{i+1}q_{i+1} + r_{i+2}$. Les suites (r_i) et $(|t_i|)$ suivent un algorithme d'Euclide associé à la même suite q_i, mais tandis que les indices de la suite (r_i) sont croissants, ceux de la suite $(|t_i|)$ sont décroissants. Donc si les deux premiers termes des $(|t_i|)$ inversés coïncident avec les deux premiers termes de la suite (r_i), alors la suite $(|t_i|)$ inversée coïncide avec la suite (r_i).
On a que $t_{n+1} = \pm p$, car par la formule d'Euler : $p = f(q_1, \dots, q_n) = f(q_n, \dots, q_1) = |t_{n+1}|$ (car la fonction d'Euler est stable par inversion de la suite). Donc $|t_{n+1}| = p$. Par ailleurs, $t_i b \equiv r_i \pmod{a}$ (découle directement de la Définition 4.16), donc $t_n x \equiv 1 \pmod{p}$. Comme $x^2 \equiv -1 \mod p$ on a $t_n \equiv -x \pmod{p}$, or $|t_n| < |t_{n+1}| = p$, donc $t_n = -x$ ou $t_n = p - x$. Si $t_n = p - x$, la suite $(|t_i|)$ inversée commence par les termes $(p, p - x, x, \dots)$, mais comme la suite (r_i) comence par $(p, x, \dots)$, on aurait que (r_i) et $(|t_i|)$ ne sont pas de même longueur, ce qui est impossible. Donc $t_n = -x$, et la suite $(|t_i|)$ inversée commence par les termes $(p, x, \dots)$ qui coïncident avec les deux premiers termes de la suite (r_i). □

Propriété 4.25. *n est pair.*

Démonstration. On sait que $t_1 = 1$ donc positif, et d'après la preuve de la Propriété 4.24, on sait que t_n est négatif. Or par la Propriété 4.19 la suite (t_i) est alternée. Donc n est pair. □

Propriété 4.26. *La suite (q_i) est symétrique par rapport à son centre. C'est à dire que $q_i = q_{n+1-i}$.*

Démonstration. Par la Propriété 4.24, la suite des quotients associée à la suite $(|t_i|)$ inversée est (q_i), donc $|t_{n-i}| = |t_{n-i+2}| + q_i|t_{n-i+1}|$. Par la Propriété 4.20, $|t_{i+1}| = |t_{i-1}| + q_i|t_i|$ c'est à dire $|t_{n-i}| = |t_{n-i+2}| + q_{n+1-i}|t_{n+1-i}|$. Donc $q_i = q_{n+1-i}$. □

Propriété 4.27. *Pour tout i, p divise ${r_i}^2 + {t_i}^2$.*

Démonstration. Par la Définition 4.16, on a : $t_i b \equiv r_i - s_i a \equiv r_i \pmod{a}$.

$$\begin{aligned} & t_i x \equiv r_i \pmod{p} \\ \Rightarrow & {t_i}^2 \equiv {r_i}^2 \pmod{p} \\ \Rightarrow & -{t_i}^2 - {r_i}^2 \equiv 0 \pmod{p} \\ \Rightarrow & {t_i}^2 + {r_i}^2 \equiv 0 \pmod{p} \end{aligned}$$

□

Propriété 4.28. *$r_{\frac{n}{2}}$ est le premier reste strictement inférieur à $\sqrt{p}$.*

Démonstration.

$$\begin{aligned} & {r_{\frac{n}{2}}}^2 \\ = & f(q_{\frac{n}{2}+1}, \ldots, q_n)^2 && \text{par la Formule 4.23} \\ = & f(1, \ldots, q_{\frac{n}{2}}) f(q_{\frac{n}{2}+1}, \ldots, q_n) && \text{par la Propriété 4.26} \\ = & f(q_1, \ldots, q_n) - A \\ = & p - A \end{aligned}$$

A est la somme des produits que l'on peut construire avec le couple $(q_{\frac{n}{2}}, q_{\frac{n}{2}+1})$ comme vu dans la Formule d'Euler.
Donc comme p est premier on a ${r_{\frac{n}{2}}}^2 < p$. Il reste à montrer que $(r_{\frac{n}{2}-1})^2 > p$.

$$\begin{aligned} & {r_{\frac{n}{2}-1}}^2 \\ = & f(q_{\frac{n}{2}}, \ldots, q_n)^2 && \text{par la Formule 4.23} \\ = & f(1, \ldots, q_{\frac{n}{2}}, q_{\frac{n}{2}+1}) f(q_{\frac{n}{2}}, q_{\frac{n}{2}+1}, \ldots, q_n) && \text{par la Propriété 4.26} \\ = & f(q_1, \ldots, q_n) + A \\ = & p + A \end{aligned}$$

□

Preuve finale :

Démonstration. Par la Propriété 4.24 $C := (r_{\frac{n}{2}})^2 + (t_{\frac{n}{2}})^2 = (r_{\frac{n}{2}})^2 + (r_{\frac{n}{2}+1})^2$. D'après 4.28 $(r_{\frac{n}{2}})^2 < p$ et $(r_{\frac{n}{2}+1})^2 < p$, d'où $C < 2p$, or par la Propriété 4.27 p divise C, donc $C = p$. □

Références

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, 6th, Springer Publishing Company, Incorporated, 2009. ↑17

[2] Blogdemaths, *Le théorème des deux carrés de Fermat* (25 Décembre 2014 [online]), 4 pp., available at https://blogdemaths.files.wordpress.com/2014/12/theoreme_des_deux_carres_de_fermat.pdf. organisation worldpress publié sur Blogdemaths, blog. ↑11

[3] A. Casamayou, N. Cohen, G. Connan, T. Dumont, L. Fousse, F. Maltey, M. Meulien, M. Mezzarobba, C. Pernet, N.M. Thiéry, and P. Zimmermann, *Calcul Mathématique avec SAGE*, CreateSpace Independent Publishing Platform, 30 Mai 2013. ISBN : 9781481191043. ↑20

[4] Jean-Luc Chabert, *Histoire d'algorithmes Du caillou à la puce*, Editions Belin, 1994 (French). ISBN 10 : 2-7011-1346-6. ↑3

[5] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Spinger-Verlag, 1993 (English). ISBN 10 : 3-540-55640-0. ↑3

[6] François Dahamani, *Commentaires et une application en théorie des nombres* (19 Janvier 2021 [online]), available at https://videos.univ-grenoble-alpes.fr/video/15492-reseaux-commentaires/. Université Grenoble Alpes, Cours magistral vidéo Algèbre 2, Partie 2, Réseaux et groupes cristallographiques. ↑13

[7] Christian Elsholtz, *A combinatorial approach to sums of two squares and related problems*, Additive number theory, Springer, New York, 2010, pp. 115–140. doi : 10.1007/978-0-387-68361-4_8. MR2744747 ↑4

[8] Gabriel Pallier, *Réciprocité quadratique par les sommes de Gauss*, 3 pp., available at https://www.imo.universite-paris-saclay.fr/~pallier/pdfs/Devagreg/rqGauss.pdf. ↑15, 16, 17

[9] Burkard Polster, *Why was this visual proof missed for 400 years ? (Fermat's two square theorem)* (20 Janvier 2020), available at https://www.youtube.com/watch?v=DjI1NICfjOk&t=861s. Youtube, Matholodger's channel. ↑4

[10] William Stein, *SageMath* (January 2020), available at https://www.sagemath.org. version 9.1, licence GPL. ↑20

[11] Jean-Pierre Serre, *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1977 (French). Deuxième édition revue et corrigée ; Le Mathématicien, No. 2. MR0498338 ↑3, 17

[12] Stan Wagon, *Editor's Corner : The Euclidean Algorithm Strikes Again*, The American Mathematical Monthly **97** (1990), no. 2, 125–129. ↑20

[13] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), no. 2, 144, DOI 10.2307/2323918. MR1041893 ↑4