Équations diophantiennes et loi de réciprocité quadratique

Tom Wozniak

1 Introduction

L'objectif de ce stage est d'étudier, via quelques problèmes très classiques, une branche des mathématiques fondamentales qui n'est pas l'objet de beaucoup d'attention dans l'enseignement mathématique que j'ai reçu du lycée à la L3.

Pour cause, la théorie des nombres possède la particularité d'avoir des énoncés de problèmes très simples, qu'un non initié en mathématiques pourrait comprendre, mais dont les preuves font parfois appel à des outils pouvant être très compliqués d'analyse et d'algèbre.

Dans ce stage, j'ai commencé par étudier quelques équations diophantiennes avant de démontrer le théorème des deux carrés. Cela m'a permit de découvrir de nouvelles preuves et de connaître certains résultats que je serais amener à réétudier dans la suite de mes études.

J'ai ensuite poursuivi mon travail sur la loi de réciprocité quadratique qui est un résultat très riche de théorie des nombres par ses applications et par tous les outils que l'on peut développer pour le prouver. Ainsi, je me suis familiarisé avec les symboles de Legendre et Jacobi, les sommes de Gauss et une multitude de résultats intéressants sur les conditions pour que des entiers soient des carrés modulo d'autres entiers.

En bilan, ce stage m'a donné la possibilité d'appréhender de nombreuses notions qui m'étaient alors inconnues et que je serais sûrement amener à revoir dans la poursuite de mes études.

2 Pré-requis

On commence par rappeler quelques définitions élémentaires sur les anneaux.

2.1 Anneaux

Définition 1 *Un anneau est un ensemble A muni de deux lois de composition interne $+$ et $\times$ telles que :*
(i) $(A,+)$ est un groupe commutatif

(ii) Il existe $1_A \in A$ tel que pour tout $a \in A$:

$$a \times 1_A = 1_A \times a = a$$

(iii) Pour tout $a,b,c \in A$, on a :

$$(a \times b) \times c = a \times (b \times c)$$

(iv) Pour tout $a,b,c \in A$, on a :

$$a \times (b+c) = a \times b + a \times c \ , \ (b+c) \times a = b \times a + c \times a$$

Si de plus la loi $\times$ est commutative, c'est à dire

$$\forall a,b \in A, \ a \times b = b \times a$$

on dit que l'anneau est commutatif.

On continue par une définition capitale de la théorie des anneaux.

Définition 2 *Un anneau est dit intègre lorsque :*

$$\forall a, b \in A,\ a \times b = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Par exemple, $\mathbb{R}$ muni de l'addition et de la multiplication est un anneau commutatif intègre.

Dans la suite de cette section, $(A, +, \times)$ désigne un anneau commutatif intègre. On rappelle maintenant des définitions qui nous seront utiles pour faire de l'arithmétique.

Définition 3 *Un anneau A est dit principal lorsque chacun de ses idéaux est principal, c'est à dire engendré par un seul élément. Par exemple, $\mathbb{Z}$ est principal.*

La définition suivante permet de généraliser la division euclidienne dans un anneau quelconque.

Définition 4 *Un anneau A est dit euclidien lorsqu'il existe une fonction :*

$$\nu : A \setminus \{0_A\} \to \mathbb{N}^*$$

telle que pour tout $a \in A$ et $b \in A \setminus \{0_A\}$, il existe un couple $(q, r) \in A^2$ satisfaisant :

$$a = bq + r$$

avec

$$r = 0_A \text{ ou } \nu(r) < \nu(b).$$

Par exemple, les anneaux $\mathbb{Z}$ et $\mathbb{Z}[j]$ sont euclidiens.

La définition qui suit étend l'identité de Bézout à un anneau quelconque.

Définition 5 *Un anneau A est dit de Bézout lorsque la somme de deux idéaux principaux de A est un idéal principal.*

Enfin, la prochaine définition donne une généralisation du théorème fondamental de l'arithmétique à tout anneau.

Définition 6 *Un anneau A est dit factoriel lorsque :*
(1) Pour tout $a \in A \setminus \{0_A\}$, il existe $u \in A^\times$ et une famille $(p_i)_{i \in I}$ d'éléments irréductibles de A tels que

$$a = u \prod_{i \in I} p_i.$$

(2) La décomposition de a est unique à l'ordre des facteurs près. C'est à dire que s'il existe $p_1, ..., p_r$ et $q_1, ..., q_s$ deux familles décomposant a alors $r = s$ et il existe une permutation σ de l'ensemble $[\![1\ ;\ r]\!]$ telle que pour tout $i \in [\![1\ ;\ r]\!]$ on a

$$p_i = q_{\sigma(i)}.$$

On continue avec une généralisation du p.g.c.d à un anneau quelconque.

Définition 7 *Un anneau A est dit à p.g.c.d lorsque tout couple d'éléments non nuls admet un p.g.c.d, c'est à dire que pour tout $a, b \in A \setminus 0_A$, il existe $d \in A$ tel que d divise a et b et pour tout $d' \in A$ divisant a et b, d' divise d.*

On a aussi les implications suivantes :

Proposition 1

$$A \text{ euclidien} \Rightarrow A \text{ principal} \Rightarrow A \text{ de Bézout ,} A \text{ factoriel et } A \text{ à p.g.c.d}$$

Notons que le caractère euclidien d'un anneau n'entraîne pas le fait d'être principal. Par exemple, l'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais pas euclidien.

On note $\mathbb{Z}[i] = \{a + ib\ ,\ a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss. C'est un anneau euclidien. On pose l'application norme, noté N définie par :

$$N : \mathbb{Z}[i] \to \mathbb{N}\ ,\ N(z) = |z|^2.$$

Cette application est multiplicative, c'est à dire qu'elle vérifie pour $z, z' \in \mathbb{Z}[i]$:

$$N(zz') = N(z)N(z').$$

On rappelle maintenant quelques théorèmes et lemme d'arithmétique dans $\mathbb{Z}$.

2.2 Arithmétique

On commence par énoncer le théorème le plus important de l'arithmétique.

Théorème 1 (Théorème fondamental de l'arithmétique) *Tout entier strictement positif peut être écrit comme un produit de nombres premiers. Cette décomposition est unique à l'ordre des facteurs près.*

Démonstration. Cette preuve se déroule en deux temps, on commence par montrer l'existence d'une telle décomposition avant de prouver qu'elle est unique.

Existence On démontre l'existence de la décomposition par récurrence forte.

Déjà, 1 est le produit d'une famille finie de nombres premiers (la famille vide).

Soit $n > 1$ un entier fixé. Supposons que tout entier strictement inférieur à n puisse se décomposer comme produit de nombres premiers. Notons p le plus entier strictement supérieur à 1 divisant n. Alors, p est un nombre premier. En effet, tout entier qui divise p divise aussi n donc vaut p ou 1 par minimalité de p. On écrit alors $n = p \times \frac{n}{p}$. Puisque $\frac{n}{p} < n$, alors par hypothèse l'entier $\frac{n}{p}$ se décompose en produit de nombres premiers, on conclut donc que n peut aussi se décomposer comme produits de nombres premiers. On conclut que d'après le principe de raisonnement par récurrence, tous les entiers peuvent se décomposer en produits de nombres premiers.

Unicité L'unicité du théorème découle du lemme suivant :

Lemme 1 (Lemme d'Euclide) *Soient a, b deux entiers et p un nombre premier. Si p divise ab alors p divise a ou p divise b.*

Démonstration. On raisonne par l'absurde en supposant qu'il existe p un nombre premier et a, b des entiers tels que a et b ne soient pas divisibles par p mais le produit ab l'est. Pour a et p fixés, on choisit b le plus petit possible, c'est à dire que l'on réduit b modulo p de tel sorte à avoir $1 < b < p$. Notons maintenant b' le reste de la division euclidienne de p par b. Ainsi, il existe un entier m tel que $p = mb + b'$. Donc, $ab' = ap - mab$ est un multiple de p puisque ab l'est par hypothèse. Cela contredit la minimalité de b puisque $0 < b' < b < p$ et achève la preuve. ■

Supposons donc qu'il existe un entier qui possède deux décompositions en produits de nombres premiers. Soit p un nombre premier du premier produit. Il divise le premier produit et donc le second puisqu'ils sont égaux. Par le lemme d'Euclide, p divise donc un des nombres premiers du second produit, donc p est égal à un des facteurs du second produit. On peut donc diviser les deux produits par p, et continuer ce procédé pour voir que les facteurs premiers des deux produits coïncident. ■

On énonce maintenant un des théorèmes les plus importants pour caractériser la primalité de deux entiers.

Théorème 2 (Théorème de Bézout) *Soient $a, b \in \mathbb{Z}$ non nuls. a et b sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que $au+bv=1$.*

Démonstration. Notons E l'ensemble des entiers naturels strictement positifs décomposables sous la forme $au + bv$. L'ensemble E est non vide. En effet, si $a > 0$, on prend $u = 1, v = 0$ et on a $au + bv \in \mathbb{N}^*$ donc $au + bv \in E$. De même, si $a < 0$, on prend $u = -1, v = 0$.

Ainsi, E possède un plus petit élément, que l'on note d. On effectue la division euclidienne de a par d, il existe donc un couple d'entiers (q, r) tels que

$$a = qd + r$$

Par conséquent, en écrivant $d = au + bv$ il vient que

$$a = q(au + bv) + r \Leftrightarrow r = a(1 - qu) + b(-qv)$$

Si $r > 0$ alors $r \in E$ mais cela contredit la minimalité de d. Donc $r = 0$ ce qui montre que d divise a. On montre de même par symétrie des rôles joués par a et b que d divise b. Enfin, la minimalité de d permet de conclure qu'il s'agit d'un p.g.c.d de a et b.

Par conséquent, si a et b sont premiers entre eux, alors leur p.g.c.d est 1 ce qui donne l'existence d'un

couple d'entiers (u, v) tels que $au + bv = 1$ et réciproquement s'il existe un couple d'entiers (u, v) tels que $au + bv = 1$ alors 1 est un p.g.c.d de a et b donc ils sont premiers entre eux. ■

On introduit maintenant un lemme très utile démontré par Gauss dans son traité *Disquisitiones arithmeticae*.

Lemme 2 (Lemme de Gauss) *Soient $a, b, c \in \mathbb{Z}$ tel que a et b soient premiers entre eux et a divise bc. Alors a divise c.*

Démonstration. Soient a, b, c des entiers tels que a et b soient premiers entre eux et tel que a divise bc.
Puisque a divise ac et bc, a divise leur p.g.c.d.
Or, p.g.c.d(ac, bc)=p.g.c.d(a, b) c=c, ce qui achève la preuve. ■

On redonne maintenant un résultat classique du mathématicien Fermat.

Théorème 3 (Petit théorème de Fermat) *Soient p un nombre premier et a un entier non divisible par p. Alors, $a^{p-1} - 1$ est divisible par p.*

Démonstration. On commence par supposer sans perte de généralités que a est positif et on montre le résultat par récurrence sur a.
Si $a = 1$ le résultat est bien évidemment vrai.
Supposons maintenant pour a fixé que

$$a^p \equiv a \bmod p$$

ce qui est une écriture équivalente au fait que $a^{p-1} - 1$ soit divisible par p. Par la formule du binôme de Newton, on

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k.$$

De plus, pour $1 \leq k \leq p-1$, p divise $\binom{p}{k}$. En effet, d'après la formule du pion, on a

$$k\binom{p}{k} = p\binom{p-1}{k-1}.$$

Puisque p divise $p\binom{p-1}{k-1}$, p divise $k\binom{p}{k}$. D'après le lemme d'Euclide et puisque p ne divise pas k, on en déduit le résultat.
Par conséquent, il vient que

$$(a+1)^p \equiv a^p + 1 \bmod p.$$

Par hypothèse, il vient donc que

$$(a+1)^p \equiv a + 1 \bmod p.$$

ce qui achève la preuve par récurrence. ■

Enfin, on redonne quelques résultats sur la théorie des groupes.

2.3 Groupes

Définition 8 *Soient G un groupe et H un sous-groupe de G. On appelle indice de H dans G le cardinal du sous-groupe quotient G/H. On le note $[G : H]$.*

Théorème 4 (Théorème de Lagrange) *Soient G un groupe fini et H un sous-groupe de G. L'ordre de H divise celui de G.*

Démonstration. Pour prouver ce théorème, on va introduire un lemme qui nous permettra de rapidement conclure.

Lemme 3 (Lemme des bergers) *Soit $p : E \to F$ une application surjective et k un entier. On suppose de plus que tout élément de F possède k antécédents, c'est à dire que*

$$\forall y \in F,\ Card(p^{-1}(y)) = k.$$

Alors, on a

$$Card(E) = k\,Card(F).$$

Démonstration. Soit $y \in F$, on note $E_y = p^{-1}(y)$. Les parties E_y sont deux à deux disjointes.
En effet, pour $y, y' \in E$, si $x \in E_y \cap E_{y'}$ alors $y = p(x) = y'$. De plus, la réunion des E_y est E par surjectivité de p. Il vient donc

$$\mathrm{Card}(E) = \mathrm{Card}(\bigcup_{y \in F} E_y) = \sum_{y \in F} \mathrm{Card}(E_y) = \sum_{y \in F} k = k\mathrm{Card}(F)$$

ce qui achève la preuve du lemme. ■

Maintenant, si l'on choisit H un sous groupe d'un groupe fini G, alors les classes à gauche de H forment une partition de H, et leur cardinal est $[G : H]$. Ainsi, le lemme précédent assure que

$$\mathrm{Card}(G) = \mathrm{Card}(H) \times [G : H]$$

d'où le résultat. ■

3 L'équation $x^2 + y^2 = z^2$

On s'intéresse aux triplets $(x, y, z) \in \mathbb{Z}^3$ tels que $x^2 + y^2 = z^2$. Un tel triplet est appelé triplet pythagoricien et le but de cette section est d'en donner une définition explicite.

On commence évidemment par ramener le problème aux entiers naturels. En effet, si le triplet $(x, y, z) \in \mathbb{N}^3$ vérifie l'équation $x^2 + y^2 = z^2$ alors le triplet $(-x, -y, -z)$ est également solution. On note $\mathcal{P}$ l'ensemble des triplets pythagoriciens.

Soit $(x, y, z) \in \mathcal{P}$. Dans un premier temps, nous allons nous ramener au cas où x et y sont premiers entre eux.

Soit $(x, y, z) \in \mathcal{P}$. Sans pertes de généralités, nous pouvons supposer (quitte à diviser par p.g.c.d.(x, y)) que x et y sont premiers entre eux.

En effet, si ce n'est pas le cas, alors il existe un p.g.c.d de x et y noté d strictement supérieur à 1. On peut donc écrire $x = kd$ et $y = k'd$ où k et k' désignent des entiers naturels, premiers entre eux par définition du p.g.c.d.

L'équation $x^2 + y^2 = z^2$ se réécrit donc en

$$(kd)^2 + (k'd)^2 = z^2.$$

Ainsi, d^2 divise z^2 donc en divisant par d^2 les deux membres de l'équation, on se ramène au cas où x et y sont premiers entre eux.

Nous allons ensuite factoriser notre équation dans $\mathbb{Z}[i]$, il vient donc :

$$(x + iy)(x - iy) = z^2.$$

Commençons par prouver que $x + iy$ et $x - iy$ sont premiers entre eux dans $\mathbb{Z}[i]$.
Notons δ un p.g.c.d de $x + iy$ et $x - iy$. Par définition, on a donc

$$\delta \mid (x + iy + x - iy) = 2x \text{ et } \delta \mid (x + iy - (x - iy)) = 2iy.$$

Ensuite puisque x et y sont premiers entre eux dans $\mathbb{Z}$, le théorème de Bézout assure qu'ils le sont aussi dans $\mathbb{Z}[i]$ (car $\mathbb{Z} \subset \mathbb{Z}[i]$).
Ceci nous permet donc de conclure que δ divise 2.
Nous allons maintenant déterminer l'ensemble $\mathbb{Z}[i]^\times$, qui sont les inversibles de $\mathbb{Z}[i]$.
Soit $z \in \mathbb{Z}[i]^\times$. Alors, il existe $z' \in \mathbb{Z}[i]^\times$ tel que $zz' = 1$. Ainsi, on a en utilisant la fonction N définie précédemment :

$$N(z)N(z') = 1 \Leftrightarrow N(z) = N(z') = 1.$$

Il n'est alors pas difficile d'observer que :

$$\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i] : N(z) = 1\} = \{-1, 1, -i, i\}.$$

En écrivant $2 = (1+i)(1-i)$ et en observant que $N(1+i) = N(1-i) = 2$, on peut conclure que $(1+i)$ et $(1-i)$ sont irréductibles dans $\mathbb{Z}[i]$.
En effet si on écrit $1+i = zz'$ avec $z, z' \in \mathbb{Z}[i]$ alors on aurait :

$$2 = N(zz') = N(z)N(z')$$

par multiplicativité de la norme. Puisque 2 est premier cela force $N(z) = 1$ ou $N(z') = 1$ d'où l'irréductibilité de $1+i$. Le même raisonnement montre que $1-i$ est irréductible.

Enfin, si $1+i$ divise $x+iy$ et $x-iy$ alors $1-i$ divise $x+iy$ et $x-iy$ car $x+iy$ et $x-iy$ sont conjugués tout comme $1+i$ et $1-i$. Par conséquent, $(1+i)(1-i) = 2$ divise $x+iy$ et $x-iy$, impossible car x et y sont premiers entre eux, d'où le résultat.

Pour conclure quant à la structure des triplets pythagoriciens, on va utiliser le lemme suivant :

Lemme 4 *Soit A un anneau factoriel et soient a,$b \in A$ tels que a et b soient premiers entre eux et ab soit un carré. Alors, il existe α, $\beta \in A$ et $u \in A^\times$ tels que $a = u\alpha^2$ et $b = u^{-1}\beta^2$.*

Démonstration. Soit $c \in A$ tel que $ab = c^2$. Dans un anneau factoriel, le théorème fondamental de l'arithmétique reste valide. On écrit donc :

$$c = p_1 \times ... \times p_s$$

et par conséquent :

$$ab = p_1^2 \times ... \times p_s^2$$

Il découle directement que :

$$\forall i \in [\![1\ ;\ s]\!], ab = p_i \times p_1^2 \times ... \times p_i \times ... \times p_s^2$$

et donc que p_i divise ab. Par le lemme d'Euclide, on conclut que p_i divise a ou p_i divise b mais peut p_i ne peut pas diviser a et b car ils sont premiers entre eux. On pose :

$$\alpha = \prod_{p_i | a} p_i \text{ et } \beta = \prod_{p_i | b} p_i$$

de tel sorte à avoir :

$$ab = c^2 = \alpha^2\beta^2 \text{ et } \alpha^2 | a \text{ et } \beta^2 | b.$$

Ensuite, α et β on été construits de manière à ce que a et β^2 (respectivement b et α^2) n'aient aucun facteur premier commun, donc qu'ils soient premiers entre eux.
Donc, puisque $a|\alpha^2\beta^2$ et que a et β^2 sont premiers entre eux, le lemme de Gauss permet de conclure que $a|\alpha^2$.
Puisque l'on a déjà $\alpha^2|a$, on en déduit qu'il existe $u \in A^\times$ tel que $a = u\alpha^2$ et puisque $ab = \alpha^2\beta^2$, il vient directement que $b = u^{-1}\beta^2$. ■

On applique le lemme 4 dans $\mathbb{Z}[i]$. Il existe donc $u+iv \in \mathbb{Z}[i]$ et $\epsilon \in \{1, -1, i, -i\}$ tels que :

$$x + iy = \epsilon(u+iv)^2 = \epsilon(u^2 - v^2 + 2iuv).$$

Si $\epsilon = 1$, alors $x + iy = (u^2 - v^2 + 2iuv)$. On identifie partie réelle et partie imaginaire, on obtient :

$$x = u^2 - v^2, y = 2uv$$

et donc

$$z^2 = (u^2 + v^2)^2 \text{ d'où } z = u^2 + v^2$$

.
De même, si ϵ prend la valeur $-1, i$ ou $-i$ on obtient le même résultat au rôle près joué par x, y ou u, v. En reprenant les notations du début du paragraphe, on en déduit que l'ensemble des triplets pythagoriciens est :

$$\mathcal{P} = \{(d(u^2 - v^2), 2duv, d(u^2 + v^2)) : (u, v, d) \in \mathbb{Z}^3\}.$$

4 L'équation $x^4 + y^4 = z^4$

On commence par énoncer le théorème au cœur de l'équation que nous allons étudier.

Théorème 5 (Fermat-Wiles (1994)) *Il n'existe pas d'entiers naturels strictement positifs x, y et z tels que $x^n + y^n = z^n$ pour $n \geq 3$.*

Bien que ce théorème nous permet d'assurer que l'équation $x^4 + y^4 = z^4$ ne possède pas de solutions non triviale (c'est à dire différent de $x = y = z = 0$) dans $\mathbb{N}$, le résultat a en fait été démontré par Fermat lui-même en 1670.
Le but de cette partie est de le démontrer en utilisant l'argument de "descente infinie", qui consiste à supposer par l'absurde que cette équation possède une solution non triviale et dans ce cas qu'il est possible d'en trouver une encore plus petite.

Pour cela, nous allons montrer le résultat sur l'équation $x^4 + y^4 = z^2$. En effet, s'il n'existe pas $x, y, z \in \mathbb{Z}$ avec $xyz \neq 0$ vérifiant cette équation, alors il n'en n'existera pas non plus vérifiant $x^4 + y^4 = z^4$, il suffit en effet d'écrire $z^4 = (z^2)^2$ pour le voir.

Supposons donc par l'absurde que de tels nombres vérifient $x^4 + y^4 = z^2$. Alors, (x^2, y^2, z) est un triplet pythagoricien, dont on connaît la structure d'après la section précédente. Comme précédemment, nous allons nous ramener au cas où x et y sont premiers entre eux.
Si ce n'est pas le cas, notons d leur pgcd. Il existe donc $(k, k') \in \mathbb{Z}^2$ tel que

$$x = kd \text{ et } y = k'd$$

En remplaçant dans l'équation, il vient que

$$d^4(k^4 + k'^4) = z^2$$

Donc, $d^4 | z^2$, d'où l'existence de $l \in \mathbb{Z}$ tel que $z = ld^4$. On peut donc diviser chaque membre de l'égalité par d^4 et ainsi se ramener dans une situation où x et y sont premiers entre eux.

Ainsi, il existe $(u, v) \in \mathbb{Z}^2$ premiers entre eux tel que

$$x^2 = u^2 - v^2,\ y^2 = 2uv \text{ et } z = u^2 + v^2$$

.
Mais alors, on a $x^2 + v^2 = u^2$ donc (x, v, u) est un triplet pythagoricien. Puisque u et v sont premiers entre eux, x et v le sont aussi (tout diviseur de x et v divise u) donc on va utiliser à nouveau le résultat sur la structure des triplets pythagoriciens.

Il existe $(\alpha, \beta) \in \mathbb{Z}^2$ premiers entre eux tel que

$$x = \alpha^2 - \beta^2,\ v = 2\alpha\beta \text{ et } u = \alpha^2 + \beta^2$$

. On remplace cette expression de u et v dans celle de y obtenue précédemment et on obtient

$$b^2 = 4\alpha\beta(\alpha^2 + \beta^2)$$

On va maintenant montrer que $\alpha\beta$ et $\alpha^2 + \beta^2$ sont premiers entre eux, en montrant qu'aucun nombre premier ne divise ces deux nombres.

Par l'absurde, supposons qu'il existe $p \in \mathbb{N}^*$ premier tel que p divise $\alpha\beta$ et $\alpha^2 + \beta^2$.
Par le lemme d'Euclide, p divise donc α ou β (mais pas les deux car ils sont premiers entre eux par hypothèse). Si p divise α et qu'il divise donc $\alpha^2 + \beta^2$ alors il divise $\alpha^2 + \beta^2 - \alpha^2 = \beta^2$ donc il divise également β, ce qui est absurde. Donc, $\alpha\beta$ et $\alpha^2 + \beta^2$ sont premiers entre eux.

De plus, on a

$$\alpha\beta(\alpha^2 + \beta^2) = (\frac{b}{2})^2$$

donc $\alpha\beta(\alpha^2+\beta^2)$ est un carré et α et β sont de même signe. Supposons sans perte de généralité qu'ils soient positifs, alors le Lemme 4 assure que $\alpha\beta$ et $\alpha^2+\beta^2$ sont des carrés.

Puisque α et β sont premiers entre eux, alors ce sont tous deux des carrés donc il existe $m \in \mathbb{N}$ et $n \in \mathbb{N}$ tel que

$$\alpha = m^2 \text{ et } \beta = n^2$$

Il existe aussi $\gamma \in \mathbb{N}$ tel que $\alpha^2+\beta^2=\gamma^2$, donc en combinant on obtient

$$m^4+n^4=\gamma^2$$

Enfin, puisque $\gamma^2 = u$ et $z = u^2+v^2$, il vient que $|\gamma| < |z|$.
On vient donc de montrer qu'il est toujours possible de trouver une solution plus petite, donc par l'argument de descente infinie on conclut que l'équation $x^4+y^4=z^2$ n'a pas de solutions non triviale dans $\mathbb{Z}^3$ et il en est ainsi également le cas pour l'équation $x^4+y^4=z^4$.

5 Les sommes de deux carrés

Le but de cette partie est de déterminer l'ensemble des entiers pouvant s'écrire comme somme de deux carrés d'entiers :

$$\mathcal{C} = \{k \in \mathbb{N} : \exists (a,b) \in \mathbb{N}^2, k = a^2+b^2\}.$$

Nous débutons notre étude avec le résultat élémentaire suivant :

Lemme 5 *L'ensemble $\mathcal{C}$ est stable par multiplication, i.e.,*

$$kk' \in \mathcal{C} \quad \textit{pour tout } k, k' \in \mathcal{C}.$$

Démonstration. Soient $k, k' \in \mathcal{C}$. Il existe par définition de $\mathcal{C}$ des entiers a, b, c et d tels que $k = a^2+b^2$ et $k' = c^2+d^2$. En posant $z = a+ib$ et $z' = c+id$ et en exploitant le caractère multiplicatif de l'application norme N, on a

$$kk' = (a^2+b^2)(c^2+d^2) = |z|^2|z'|^2 = |zz'|^2 = (ac-bd)^2+(ad+bc)^2$$

et ceci traduit l'inclusion désirée $kk' \in \mathcal{C}$. ■

Maintenant, nous allons étudier une condition portant sur la décomposition primaire des entiers pour observer lesquels peuvent s'écrire comme somme de deux carrés.

Soit $n \geq 2$ un entier. D'après le théorème fondamental de l'arithmétique, on peut écrire que

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où les p_i sont des nombres premiers et α_i leur multiplicité.

Soit $s \in [\![1\ ;\ k]\!]$. On ordonne les facteurs de la décomposition pour avoir :

$$\forall i \in [\![1\ ;\ s]\!]\ \alpha_i \text{ impair et } \forall i \in [\![s+1\ ;\ k]\!]\ \alpha_i \text{ pair}$$

.
On peut alors écrire pour un certain $m \in \mathbb{N}$

$$n = m^2 \prod_{i=1}^{s} p_i.$$

On observe alors que si chaque p_i peut s'écrire comme somme de deux carrés alors n s'écrira également comme somme de deux carrés. Nous allons montrer que cette condition est une caractérisation des entiers pouvant s'écrire comme somme de deux carrés.

Pour cela nous allons prouver le résultat suivant :

Lemme 6 *Soient p un nombre premier impair et $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Il existe $x \in \mathbb{Z}/p\mathbb{Z})$ tel que $x^2 = a$ si et seulement si $a^{\frac{p-1}{2}} = \overline{1}$.*

Démonstration.

$\Rightarrow$, Supposons qu'il existe $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $x^2 = a$. Le fait que a soit non nul nous dit évidemment que x est non nul et ceci permet d'appliquer le petit théorème de Fermat (voir première partie) pour obtenir $\overline{1} = x^{p-1} = a^{\frac{p-1}{2}}$.
$\Leftarrow$, Supposons que $a^{\frac{p-1}{2}} = \overline{1}$. Commençons par introduire l'application $\Phi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par

$$\Phi(x) = x^2 \quad \text{pour tout } x \in (\mathbb{Z}/p\mathbb{Z})^*.$$

Soit $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $x = -x$. Alors $\overline{2}x = \overline{0}$ et puisque p est impair alors par intégrité de $\mathbb{Z}/p\mathbb{Z}$ on a $x = \overline{0}$. Par définition de Φ on en déduit que chaque élément de l'image Φ possède deux antécédents différents. Puisque Card $(\mathbb{Z}/p\mathbb{Z})^* = p - 1$, on en déduit que Card Im $\Phi = \frac{p-1}{2}$ et que chaque élément de l'image de Φ est solution de l'équation polynomiale $X^{\frac{p-1}{2}} - \overline{1} = \overline{0}$.

Enfin, comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, l'équation précédente possède au plus $\frac{p-1}{2}$ solutions et on les connaît tous, ce sont les carrés modulo p. Par conséquent, puisque a est solution de cette équation, on déduit directement qu'il existe $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $x^2 = a$. ■

Nous allons maintenant nous intéresser à une caractérisation des nombres premiers impairs pouvant s'écrire comme somme de deux carrés :

$$\exists (a, b) \in \mathbb{Z}^2, p = a^2 + b^2 \Leftrightarrow p \equiv 1 \ [4]$$

Supposons donc qu'il existe $(a, b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$. Dans $\mathbb{Z}/4\mathbb{Z}$ les carrés sont $\overline{0}$ et $\overline{1}$ donc les valeurs possibles prises par $a^2 + b^2$ sont $\overline{0}$, $\overline{1}$ ou $\overline{2}$. Puisque p est impair, $\overline{p} = \overline{0}$ et $\overline{p} = \overline{2}$ sont exclus d'où $\overline{p} = \overline{1}$ et donc le résultat.

Réciproquement, supposons que $p \equiv 1$ [4]. Il vient donc que $\frac{p-1}{2}$ est pair et donc que $(-\overline{1})^{\frac{p-1}{2}} = \overline{1}$.
Le lemme précédent nous donne l'existence de $x \in \mathbb{Z}$ tel que $\overline{x^2} = -\overline{1}$, ce qui se réécrit en

$$x^2 + 1 = kp$$

avec $k \in \mathbb{Z}$.

Dans $\mathbb{Z}[i]$, cette équation devient

$$(x + i)(x - i) = kp$$

ce qui implique que

$$p \mid (x + i)(x - i)$$

Or, p ne divise pas $(x + i)$ et $(x - i)$ car sinon il diviserait 1 ce qui est absurde.
Par conséquent, p n'est pas premier ni irréductible dans $\mathbb{Z}[i]$ ce qui donne l'existence de $z, z' \in \mathbb{Z}[i]$ tel que

$$p = zz'$$

Enfin, comme $N(p) = N(z)N(z') = p^2$ on en déduit, puisque $N(z) \neq 1$ et $N(z') \neq 1$, que $N(z) = N(z') = p$. Il ne reste plus qu'à poser $z = a + ib$ et donc $z' = a - ib$ pour avoir $p = a^2 + b^2$.

Enfin, nous allons montrer que si l'un des p_i de la décomposition en nombres premiers de n n'est pas somme de deux carrés alors n ne peut pas s'écrire comme somme de deux carrés. Pour cela, nous allons utiliser le lemme suivant :

Lemme 7 *Soit p un nombre premier qui ne soit pas un carré et soient $(a, b) \in \mathbb{Z}^2$. On a :*

$$p|(a^2 + b^2) \Rightarrow p|a \text{ et } p|b.$$

Démonstration. Supposons donc que

$$p|(a^2+b^2)$$

c'est à dire que

$$\overline{a^2+b^2} = \overline{0} \text{ dans } \mathbb{Z}/p\mathbb{Z}$$

Supposons que $b \neq \overline{0}$ alors b est inversible car $\mathbb{Z}/p\mathbb{Z}$ est un corps.
Donc puisque

$$\overline{a^2} = -\overline{b^2}$$

on a

$$\overline{(ab^{-1})^2} = \overline{-1}$$

et ainsi $\overline{-1}$ serait un carré modulo p. Or, en vertu du lemme précédent et puisque $p \equiv 3\ [4]$, on a $(-1)^{\frac{p-1}{2}} = -1$ d'où la contradiction. Ainsi, $\overline{b} = \overline{0}$ et donc $\overline{a} = \overline{0}$ par intégrité de $\mathbb{Z}/p\mathbb{Z}$. ■

On conclut donc que les entiers pouvant s'écrire comme somme de deux carrés sont les nombres dont les nombres premiers impairs de leur décomposition avec multiplicité impair sont congrus à 1 modulo 4.

6 La loi de réciprocité quadratique

Le but de cette partie est de démontrer la loi de réciprocité quadratique, démontré pour la première fois par Gauss en 1801.
Ce résultat est considéré comme fondamental dans la théorie des nombres car il permet de donner une condition pour qu'un nombre premier soit un carré modulo un autre nombre premier.
Il existe à ce jour plus de 220 preuves de ce résultat, Gauss est connu pour en avoir trouvé 6 d'entre elles et nous allons en étudier 2, une de Gauss reposant sur les sommes de Gauss que nous introduirons plus tard, et une proposée par Eisenstein reposant sur une formule trigonométrique et un lemme de Gauss sur la théorie des nombres.

6.1 Carrés modulo un entier

Le but de cette partie est d'étudier les entiers qui sont des carrés dans $\mathbb{Z}/N\mathbb{Z}$, avec N un entier. On commence donc par une définition :

Définition 9 *Soient $N \geq 2$ un entier et $a \in \mathbb{Z}$. On dit que a est un carré modulo N, ou un résidu quadratique modulo N, s'il existe $b \in \mathbb{Z}$ tel que :*

$$a \equiv b^2[N]$$

Cette propriété ne dépend bien évidemment que de la classe de a dans $\mathbb{Z}/N\mathbb{Z}$. De plus, s'il existe $M \in \mathbb{N}$ tel que M divise N alors a est un carré modulo M.
En effet, si a est un carré modulo N alors en reprenant les notations de la définition il existe $k \in \mathbb{N}$ tel que :

$$a - b^2 = kN$$

et donc puisque M divise N il existe $l \in \mathbb{N}$ tel que :

$$a - b^2 = klM \Leftrightarrow a \equiv b^2[M].$$

Nous allons donc commencer par étudier le cas où N est un nombre premier impair (car le cas $N = 2$ est trivial).

Proposition 2 *Soit p un nombre premier. On pose $C_p := \{x^2,\ x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$, l'ensemble des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$.*

(i) $|C_p| = \frac{p-1}{2}$

(ii) C_p est un sous groupe d'indice 2 de $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ de plus, le produit de deux éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ est un carré si et seulement si le deux éléments sont des carrés ou les deux éléments ne sont pas des carrés.

Démonstration.
(i) Nous avons déjà prouvé ce résultat dans le Lemme 6.

(ii) Il est clair que C_p est un sous groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$.
En effet, on évidement $C_p \subset (\mathbb{Z}/p\mathbb{Z})^\times$ et $\overline{1} \in C_p$. De plus si l'on prend $m, n \in C_p$ alors il existe $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que :

$$m = x^2 \text{ et } n = y^2$$

donc, il en découle que :

$$mn = (xy)^2 \text{ et } m^{-1} = (x^2)^{-1} = (x^{-1})^2$$

d'où le résultat.
Ensuite, puisque que $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, (i) nous assure que :

$$[(\mathbb{Z}/p\mathbb{Z})^\times : C_p] = 2.$$

On peut donc écrire $(\mathbb{Z}/p\mathbb{Z})^\times$ comme réunion de deux classes disjointes, c'est à dire qu'il existe $a \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus C_p$ tel que :

$$(\mathbb{Z}/p\mathbb{Z})^\times = C_p \bigsqcup aC_p.$$

Soient $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$. On sait déjà que si x et y sont des carrés alors xy est un carré. Cependant, si x et y ne sont pas des carrés alors il vient que :

$$xy \in a^2 C_p$$

donc xy est un carré. De même, si par exemple x est un carré mais y n'en n'est pas un alors on a :

$$xy \in aC_p$$

donc xy n'est pas un carré. ■

Nous allons maintenant introduire le symbole de Legendre qui va permettre de simplifier fortement les futurs énoncés.

Définition 10 (Symbole de Legendre) *Soient p un nombre premier impair et $a \in \mathbb{Z}$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre défini par :*
$\left(\frac{a}{p}\right) = 1$ *si a est premier avec p et a est un carré modulo p*
$\left(\frac{a}{p}\right) = -1$ *si a est premier avec p mais a n'est pas un carré modulo p*
$\left(\frac{a}{p}\right) = 0$ *si p divise a*

En particulier, cette notation permet de réécrire le point (ii) de la proposition précédente :

Corollaire 1 (Multiplicativité du symbole de Legendre) *Soient $a, b \in \mathbb{Z}$ et p un nombre premier impair. On a :*

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

Ainsi, grâce au théorème fondamental de l'arithmétique, pour $n \in \mathbb{Z}$ et p un nombre premier impair, $\left(\frac{n}{p}\right)$ est entièrement déterminé si l'on connaît $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ et $\left(\frac{p_i}{p}\right)$ où p_i désigne un nombre premier impair de la décomposition primaire de n.
Par conséquent, il est assez aisé connaissant p de trouver tous les $a \in \mathbb{Z}$ tel que $\left(\frac{a}{p}\right) = 1$ puisqu'il suffit de trouver les classes de k^2 avec $k \in [\![1\ ;\ \frac{p-1}{2}]\!]$.

Cependant, il est nettement plus compliqué d'effectuer le raisonnement inverse, c'est à dire connaissant $a \in \mathbb{Z}$ de trouver tous les nombres premiers p tel que $\left(\frac{a}{p}\right) = 1$.
Il n'existe pas de moyen simple sans ordinateur pour résoudre ce problème. Cependant, on dispose du critère suivant dû à Euler :

Proposition 3 (Critère d'Euler) *Soient p un nombre premier impair et $a \in \mathbb{Z}$. On a :*

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

Démonstration. Si a est divisible par p le résultat est évident. Supposons donc que a ne soit pas divisible par p.

Supposons que a soit un carré modulo p. Par le lemme 6, on a alors que :

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Supposons maintenant que a ne soit pas un carré modulo p. Par le petit théorème de Fermat, on sait que :

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

donc puisque $a^{p-1} = (a^{\frac{p-1}{2}})^2$, le lemme 4 nous assure que :

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p$$

ce qui achève la preuve. ■
De ce résultat découle directement le corollaire suivant :

Corollaire 2 (Fermat, Euler) *Soit p un nombre premier impair, -1 est un carré modulo p si et seulement si $p \equiv 1$ [4]. Autrement dit,*

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

Démonstration. On applique le critère d'Euler à $a = -1$. ■

Nous allons maintenant énoncer le résultat principal de ce chapitre et nous en proposerons deux preuves différentes.Nous terminerons ce chapitre par des applications de cette loi.

Théorème 6 (Loi de réciprocité quadratique) *Soient p, q deux nombres premiers impairs. On a :*

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

On a également la "loi supplémentaire" :

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

Avant de commencer la preuve, on peut observer que la "loi supplémentaire" peut aussi s'écrire : 2 est un carré modulo p si et seulement si $p \equiv \pm 1[8]$.

La première preuve de la loi de réciprocité quadratique que nous allons étudier repose sur les sommes de Gauss qui vont faire l'objet d'une étude dans la partie qui suit.

6.2 Sommes de Gauss

Dans toute cette partie, p désigne un nombre premier impair. On pose également $\zeta = e^{2i\pi/p}$.
On commence par définir les sommes de Gauss.

Définition 11 (Gauss) *On appelle somme de Gauss relativement à p le nombre complexe G défini par :*

$$G = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right)\zeta^a$$

La somme de Gauss relativement à 2 est définie par :

$$G = e^{2i\pi/8} + e^{-2i\pi/8}$$

Le nombre complexe G possède plusieurs propriétés que nous allons étudier. Commençons par énoncer un lemme qui nous servira par la suite.

Lemme 8 *Soit p un nombre premier impair. On a :*

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) = 0$$

Démonstration. La proposition 2 nous assure qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$, d'où le résultat. ■

Ce lemme va nous permettre de montrer une propriété remarquable des sommes de Gauss.

Proposition 4 (Gauss) *Soit p un nombre premier impair et G la somme de Gauss relative à p. On a :*

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

Démonstration. Par définition de G, on a

$$G^2 = \Big(\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right)\zeta^a\Big)\Big(\sum_{b \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{b}{p}\right)\zeta^b\Big)$$

donc par multiplicativité du symbole de Legendre, il vient que

$$G^2 = \sum_{(a,b) \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{ab}{p}\right)\zeta^{a+b}.$$

Si $a = 0$ ou $b = 0$, $\left(\frac{ab}{p}\right) = 0$. Par conséquent, on peut écrire que

$$G^2 = \sum_{(a,b)\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{ab}{p}\right)\zeta^{a+b}.$$

Soit $t \in \mathbb{Z}$. On sait que $\left(\frac{a^2t}{p}\right) = \left(\frac{t}{p}\right)$ par multiplicativité et définition du symbole de Legendre. Posons $b = at$. Il vient donc que

$$G^2 = \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right)\Big(\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)}\Big).$$

Ensuite, on remarque que si $t = -1$ alors

$$\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} = \text{ Card } (\mathbb{Z}/p\mathbb{Z})^\times = p - 1$$

Sinon, on observe que l'application $a \mapsto (a+t)a$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans lui-même. Par conséquent, il vient que

$$\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a} = -1$$

d'après une propriété bien connue sur les racines de l'unité. Finalement, on obtient que

$$G^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^\times\setminus\{1\}} \left(\frac{t}{p}\right)$$

Par le lemme précédent, on a donc

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

Le corollaire 2 permet alors de conclure. ■
On introduit maintenant une dernière propriété qui va nous permettre ensuite de démontrer la loi de réciprocité quadratique.

Proposition 5 *Soit q un nombre premier impair distinct de p. On a :*

$$G^q \equiv \left(\frac{q}{p}\right) G \ mod\ q.$$

Si p=2 on a :

$$G^q \equiv (-1)^{\frac{q^2-1}{8}} G \ mod\ q.$$

Démonstration. Puisque $\mathbb{Z}/q\mathbb{Z}$ est un anneau de caractéristique q, on a

$$G^q = \Big(\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right)\zeta^a\Big)^q \equiv \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right)^q \zeta^{aq}.$$

Puisque q est impair, il vient que

$$G^q \equiv \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right)\zeta^{aq}$$

De plus, puisque q est inversible modulo p, l'application $a \mapsto aq$ est une bijection de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même. Il en découle par multiplicativité du symbole de Legendre que

$$\left(\frac{q}{p}\right)G^q \equiv \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \left(\frac{aq}{p}\right)\zeta^{aq} = G$$

ce qui achève la preuve dans le cas où p est premier impair.
Si $p = 2$ on conclut de manière similaire en remarquant que $(e^{2i\pi/8})^q + (e^{-2i\pi/8})^{-q} = G$ si $q \equiv \pm 1 \bmod 8$ et $-G$ sinon. ■

Nous allons maintenant proposer une première démonstration de la loi de réciprocité quadratique.

6.3 Une première démonstration de la loi de réciprocité quadratique

Démonstration. On garde les notations de la partie précédente. L'idée de cette preuve est de calculer G^q d'une manière différente que précédemment.
Par la proposition 4, on a :

$$G^q = (G^2)^{\frac{q-1}{2}} G = ((-1)^{\frac{p-1}{2}} p)^{\frac{q-1}{2}} G = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}} G$$

Le critère d'Euler assure que

$$G^q \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) G \bmod q.$$

On remplace maintenant G^q par l'expression que l'on a déterminé dans la proposition précédente, il vient donc que

$$(-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) G \equiv \left(\frac{q}{p}\right) G \bmod q.$$

On multiplie chaque membre de l'équation par $(-1)^{\frac{p-1}{2}} G$ et on applique une nouvelle fois la proposition 4 pour obtenir

$$(-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) p \equiv \left(\frac{q}{p}\right) p \bmod q.$$

En divisant chaque membre de l'égalité par p qui est inversible dans $\mathbb{Z}/q\mathbb{Z}$, on obtient alors la loi de réciprocité quadratique, ce qui achève la preuve. ■

6.4 Une seconde démonstration de la loi de réciprocité quadratique

Dans cette partie, nous allons étudier une seconde démonstration de la loi de réciprocité quadratique due à Eisenstein et proposée en 1845. Elle se base pour cela sur deux lemmes que nous allons énoncer.

Lemme 9 *Soit m un entier naturel impair et soit $x \in \mathbb{R} \setminus \pi\mathbb{Z}$, on a*

$$\frac{\sin(mx)}{\sin(x)} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} (\sin^2(x) - \sin^2(\frac{2\pi j}{m})).$$

Démonstration. Soit $n \in \mathbb{N}$. On pose $m = 2n+1$ et on se donne $x \in \mathbb{R} \setminus \pi\mathbb{Z}$. D'après la formule du binôme de Newton, on peut écrire que

$$(\cos(x) + i\sin(x))^{2n+1} = \sum_{k=0}^{2n+1} \binom{2n+1}{k} i^k \sin^k(x) \cos^{2n+1-k}(x)$$

D'après la formule de Moivre, il vient donc que

$$\cos((2n+1)x) + i\sin((2n+1)x) = \sum_{k=0}^{2n+1} \binom{2n+1}{k} i^k \sin^k(x) \cos^{2n+1-k}(x)$$

On va maintenant identifier la partie imaginaire de cette somme. On remarque que lorsque l'entier k est impair, $\binom{2n+1}{k} i^k \sin^k(x) \cos^{2n+1-k}(x) \notin \mathbb{R}$. On réindexe, il vient alors que

$$\sin((2n+1)x) = \sum_{j=0}^{n} \binom{2n+1}{2j+1} (-1)^j \sin^{2j+1}(x) \cos^{2(n-j)}(x).$$

En utilisant la formule $\cos^2(x) + \sin^2(x) = 1$ et en divisant par $\sin(x)$ il vient

$$\frac{\sin((2n+1)x)}{\sin(x)} = \sum_{j=0}^{n} \binom{2n+1}{2j+1} (-1)^j \sin^{2j}(x)(1 - \sin^2(x))^{n-j}.$$

Ceci nous amène à considérer le polynôme $P \in \mathbb{Z}[X]$ défini par

$$P = \sum_{j=0}^{n} \binom{2n+1}{2j+1} (-1)^j X^j (1-X)^{n-j}.$$

Ce polynôme est clairement de degré au plus n et il a été défini de tel sorte à avoir

$$P(\sin^2(x)) = \frac{\sin(mx)}{\sin(x)}.$$

Soit $j \in [\![1, n]\!]$, on observe que les éléments $\sin^2(\frac{2\pi j}{m})$ sont n racines distinctes de P. Par conséquent, ce sont donc toutes ses racines. On peut alors scinder P en racines simples, c'est à dire qu'il existe $\lambda \in \mathbb{R}$ tel que

$$P = \lambda \prod_{j=1}^{\frac{m-1}{2}} (X - \sin^2(\frac{2\pi j}{m})).$$

Donc par définition de P, on obtient que

$$\frac{\sin(mx)}{\sin(x)} = \lambda \prod_{j=1}^{\frac{m-1}{2}} (\sin^2(x) - \sin^2(\frac{2\pi j}{m})).$$

Il ne reste maintenant plus qu'à déterminer λ. Pour cela, on va commencer par évaluer $\frac{\sin(mx)}{\sin(x)}$ en $x = \frac{\pi}{2}$. En effet, on a

$$\frac{\sin(m\frac{\pi}{2})}{\sin(\frac{\pi}{2})} = \cos(\frac{m-1}{2}\pi) = (-1)^{\frac{m-1}{2}}.$$

On a toujours $n = \frac{m-1}{2}$. Par conséquent, il vient que

$$(-1)^n = \lambda \prod_{j=1}^{n} (1 - \sin^2(\frac{2\pi j}{2n+1})) = \lambda \prod_{j=1}^{n} \cos^2(\frac{2\pi j}{2n+1}).$$

De plus, on évidemment

$$\prod_{j=1}^{n} \cos^2(\frac{2\pi j}{2n+1}) = (\prod_{j=1}^{n} \cos(\frac{2\pi j}{2n+1}))^2.$$

Il ne reste plus qu'à déterminer la valeur de ce produit. Pour cela, on va utiliser la relation trigonométrique valable pour tout $x \in \mathbb{R} \setminus \pi\mathbb{Z}$

$$\cos(x) = \frac{\sin(2x)}{2\sin(x)}.$$

Il vient alors que

$$\prod_{j=1}^{n} \cos(\frac{2\pi j}{2n+1}) = \frac{1}{2^n} \prod_{j=1}^{n} \frac{\sin(\frac{4\pi j}{2n+1})}{\sin(\frac{2\pi j}{2n+1})}.$$

Il ne reste plus qu'à remarquer que, modulo 2π, les quantités $\frac{4\pi j}{2n+1}$ et $\frac{2\pi j}{2n+1}$ sont les mêmes, d'où on déduit directement que

$$\forall n \in \mathbb{N}, \quad \frac{\sin(\frac{4\pi j}{2n+1})}{\sin(\frac{2\pi j}{2n+1})} = 1.$$

Par conséquent, on obtient le résultat remarquable suivant

$$\prod_{j=1}^{n} \cos^2(\frac{2\pi j}{2n+1}) = \frac{1}{4^n}.$$

Il vient alors que $\lambda = (-4)^n$ ce qui achève la preuve. ■
Nous allons maintenant énoncer un lemme dû à Gauss qui va nous permettre de démontrer la loi de réciprocité quadratique.

Lemme 10 (Gauss) *Soient p un nombre premier impair et a un entier non divisible par p. On a*

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

où l'entier n désigne le nombre de résidus plus grand que $\frac{p}{2}$ parmi les entiers a, $2a$,..., $a\frac{p-1}{2}$.

Démonstration. On commence par évaluer le produit

$$Z = a \times 2a \times ...a\frac{p-1}{2} = a^{\frac{p-1}{2}}(\frac{p-1}{2})!$$

On définit maintenant une application f sur $\mathbb{Z}/p\mathbb{Z}$ par

$$f(x) = \begin{cases} x & \text{si } 1 \leq x \leq \frac{p-1}{2} \\ -x & \text{si } \frac{p+1}{2} \leq x \leq p-1 \end{cases}$$

Soit $k \in [\![1, \frac{p-1}{2}]\!]$. Par définition de l'entier n, il s'agit du nombre de multiple ka lorsque $ka \in [\![\frac{p+1}{2}, p-1]\!]$. Par définition de la congruence modulo p, pour ces multiples on a donc $-ka \in [\![1, \frac{p-1}{2}]\!]$. On peut donc évaluer d'une autre façon Z, il vient que

$$Z = (-1)^n(f(a) \times f(2a) \times ... \times f(a\frac{p-1}{2}))$$

Observons maintenant que pour les $f(ka)$ sont distincts. En effet, supposons qu'il existe $k' \in [\![1, \frac{p-1}{2}]\!]$ tel que $f(ka) = f(k'a)$. Alors, il vient que $ka = \pm k'a$ et donc $k = \pm k'$ car a est inversible dans $\mathbb{Z}/p\mathbb{Z}$. Il vient directement que $k = k'$ puisque $k, k' \in [\![1, \frac{p-1}{2}]\!]$.
Ainsi, l'application $k \mapsto f(ka)$ est une bijection de $[\![1, \frac{p-1}{2}]\!]$ dans lui-même, c'est donc une permutation des entiers $1, 2, ..., \frac{p-1}{2}$, ce qui nous permet d'écrire, toujours modulo p, que

$$Z = (-1)^n(1 \times 2 \times ... \times \frac{p-1}{2}) = (-1)^n(\frac{p-1}{2})!$$

On simplifie par $(\frac{p-1}{2})!$, il vient que

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

Le critère d'Euler permet alors de conclure la preuve. ■

Nous allons maintenant commencer la preuve de la loi de réciprocité quadratique.

Démonstration. Soient p, q deux nombres premiers distincts. Posons $S = [\![1, \frac{p-1}{2}]\!]$. En reprenant le même type de raisonnement que dans la preuve du lemme de Gauss, on peut observer que

$$\forall k \in S,\ \exists! k_q \in S : qk = \pm k_q$$

En multipliant par $\frac{2\pi}{p}$ les deux membres de l'égalité et en composant par la fonction sin, on a donc

$$\sin(\frac{2\pi}{p}qk) = \pm\sin(\frac{2\pi}{p}k_q).$$

Notons que, comme précédemment le "$\pm$" provient de la valeur de qk modulo p.
Par conséquent, lorsque l'on fait le produit des deux membres précédent lorsque k décrit S et puisque l'application $k \mapsto k_q$ est bijective, on obtient que

$$\prod_{k\in S}\sin(\frac{2\pi}{p}qk) = \prod_{k\in S}\pm\sin(\frac{2\pi}{p}k) \Leftrightarrow (-1)^n = \prod_{k\in S}\frac{\sin(\frac{2\pi}{p}qk)}{\sin(\frac{2\pi}{p}k)}.$$

On applique maintenant le lemme de Gauss, il vient que

$$\left(\frac{q}{p}\right) = \prod_{k\in S}\frac{\sin(\frac{2\pi}{p}qk)}{\sin(\frac{2\pi}{p}k)}$$

Posons $T = [\![1, \frac{q-1}{2}]\!]$. On applique le lemme 9 à $m = q$ et $x = \frac{2\pi k}{p}$, il en découle que

$$\left(\frac{q}{p}\right) = \prod_{k\in S}(-4)^{\frac{q-1}{2}}\prod_{t\in T}(\sin^2(\frac{2\pi k}{p}) - \sin^2(\frac{2\pi t}{q})).$$

En factorisant par $(-4)^{\frac{q-1}{2}}$, il vient que

$$\left(\frac{q}{p}\right) = (-4)^{\frac{(q-1)(p-1)}{4}}\prod_{k\in S, t\in T}(\sin^2(\frac{2\pi k}{p}) - \sin^2(\frac{2\pi t}{q})).$$

Par symétrie entre p et q on a également

$$\left(\frac{p}{q}\right) = (-4)^{\frac{(q-1)(p-1)}{4}} \prod_{k\in S, t\in T} (\sin^2(\frac{2\pi k}{q}) - \sin^2(\frac{2\pi t}{p})).$$

On a donc directement

$$\left(\frac{q}{p}\right) = (-1)^{\mathrm{Card}(S\times T)} \left(\frac{p}{q}\right).$$

Le cardinal de $S \times T$ étant précisément $\frac{(q-1)(p-1)}{4}$, on obtient donc

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

ce qui achève la preuve. ■

Cette preuve, qui utilise de la trigonométrie suggère qu'il serait possible de prouver la loi de réciprocité quadratique de manière géométrique.
C'est effectivement possible et Eisenstein l'a prouvé en trouvant une relation entre $\left(\frac{q}{p}\right)$ et le nombre de points à coordonnées entières à l'intérieur du triangle dont les coordonnées des points sont $O(0,0)$, $S(\frac{q}{2}, \frac{p}{2})$ et $P(0, \frac{p}{2})$.

Dans la partie qui suit, nous allons étudier des applications de la loi de réciprocité quadratique afin de mieux comprendre sa puissance et son utilité en théorie des nombres.

6.5 Applications de la loi de réciprocité quadratique

On va commencer par étudier quelques exemples découlant directement de la loi.
Sachant que 691 et 41 sont des nombres premiers, est-ce que 41 est un carré modulo 691 ? Si l'on essaie de répondre à ce problème naïvement, on doit alors lister tous les carrés modulo 691 ce qui est très fastidieux. Si l'on utilise le critère d'Euler on peut facilement résoudre le problème avec un ordinateur mais c'est encore une fois compliqué à la main puisqu'il faut calculer le résidu de 41^{345} modulo 691. Utilisons la loi de réciprocité quadratique, il vient que

$$\left(\frac{41}{691}\right) = \left(\frac{691}{41}\right)$$

Le seul calcul à faire consiste à trouver le résidu de 691 modulo 41, qui reste relativement simple sans l'aide de l'ordinateur, et on trouve $691 \equiv 35\ [41]$. Par conséquent, on a

$$\left(\frac{41}{691}\right) = \left(\frac{35}{41}\right)$$

On utilise ensuite la multiplicativité du symbole de Legendre pour obtenir

$$\left(\frac{41}{691}\right) = \left(\frac{7}{41}\right)\left(\frac{5}{41}\right)$$

On réutilise la loi de réciprocité quadratique et il vient que

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

Par conséquent, 41 n'est pas un carré modulo 691.

Un autre corollaire puissant de la loi de réciprocité quadratique est, connaissant q, de pouvoir déterminer $\left(\frac{q}{p}\right)$ facilement. Détaillons cela pour $q = 3$ et $q = 5$.

Corollaire 3 *Soit p un nombre premier impair.*

3 est un carré modulo p si et seulement si $p = 3$ ou $p \equiv \pm 1\ [12]$

5 est un carré modulo p si et seulement si $p = 5$ ou $p \equiv \pm 1\ [5]$

Démonstration. La loi de réciprocité quadratique nous donne directement

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

Par conséquent, 3 est un carré modulo p si et seulement si

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

Maintenant, si $\left(\frac{p}{3}\right) = 1$ alors on a

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p \equiv 1\ [12]$$

De même, si $\left(\frac{p}{3}\right) = -1$, on a

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} = -1 \Leftrightarrow p \equiv -1\ [12]$$

d'où le résultat.
Pour 5, on écrit d'après la loi de réciprocité quadratique

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

Les carrés modulo 5 étant 0,1 et -1 le résultat découle directement. ■

6.5.1 Le symbole de Jacobi

On va maintenant introduire le symbole de Jacobi qui est un extension du symbole de Legendre permettant de calculer plus facilement ces derniers.

Définition 12 (Symbole de Jacobi) *Soient m, n des entiers avec n impair positif. On pose*

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\left(\frac{m}{p_i}\right)$$

où les p_i sont les nombres premiers non distincts de la décomposition primaire de n.

Par convention, pour tout entier m, on pose $\left(\frac{m}{1}\right) = 1$.
On observe que lorsque n est premier, les symboles de Legendre et Jacobi coïncident.
Cependant, il faut aussi remarquer que $\left(\frac{m}{n}\right) = 1$ n'entraîne pas nécessairement que m et un carré modulo n.
Par exemple, on a

$$\left(\frac{2}{15}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{3}\right) = (-1) \times (-1) = 1$$

et pourtant 2 n'est pas un carré modulo 15.

On va maintenant énoncer quelques propriétés du symbole de Jacobi.

Proposition 6 *Soient $m, m', n, n' \in \mathbb{Z}$ avec n, n' impairs positifs. On a*

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

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

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

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

De plus, si m est impair positif on a

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(n-1)(m-1)}{4}}$$

Démonstration. La première propriété découle directement de la multiplicativité du symbole de Legendre. Pour la seconde propriété, on écrit

$$n = \prod_{i=1}^{r} p_i \text{ et } n' = \prod_{i=1}^{r'} p'_i$$

de sorte à avoir

$$nn' = \prod_{i=1}^{q} p_i p'_i$$

mais alors, par définition du symbole de Jacobi et d'après la décomposition primaire du nombre $\prod_{i=1}^{q} p_i p'_i$, on a

$$\left(\frac{m}{nn'}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right) \prod_{k=1}^{r'} \left(\frac{m}{p'_k}\right)$$

d'où le résultat.
On va maintenant introduire un lemme qui va nous permettre de prouver les autres propriétés.

Lemme 11 *Soient $m, n \in \mathbb{Z}$ des entiers impairs. On a :*

(i) $\frac{n-1}{2} + \frac{m-1}{2} \equiv \frac{nm-1}{2}$ [2]

(ii) Si $n = \prod_i n_i$ *et* $m = \prod_j m_j$, *alors* $\sum_{i,j} \frac{n_i-1}{2}\frac{m_j-1}{2} \equiv \frac{n-1}{2}\frac{m-1}{2}$ [2]

(iii) $n^2 \equiv 1$ [8]

(iv) $\frac{n^2-1}{8} + \frac{m^2-1}{8} \equiv \frac{n^2m^2-1}{8}$ [2]

Démonstration. Pour prouver (i), il suffit d'écrire $n = 2k+1$ et $m = 2k'+1$, il vient alors que :

$$\frac{n-1}{2} + \frac{m-1}{2} = k + k' \text{ et } \frac{nm-1}{2} = 2kk' + k + k'$$

d'où on déduit aisément le résultat.
Pour le point (ii), on utilise remarque que chaque n_i et m_j sont impairs puisque n et m le sont. D'après le point (i) et puisque les deux sommes sont finies, on a

$$\sum_i \sum_j \frac{n_i-1}{2}\frac{m_j-1}{2} = \sum_i (\frac{n_i-1}{2})(\frac{m_1-1}{2} + \frac{m_2-1}{2} + ...)$$

d'où vu (i)

$$\sum_i \sum_j \frac{n_i-1}{2}\frac{m_j-1}{2} \equiv \sum_i (\frac{n_i-1}{2})(\frac{\prod_j m_j - 1}{2}) \text{ [2]}$$

donc il vient que

$$\sum_i \sum_j \frac{n_i-1}{2}\frac{m_j-1}{2} \equiv \sum_i (\frac{n_i-1}{2})(\frac{m-1}{2}) \text{ [2]}$$

en réutilisant le point (i) on trouve finalement que

$$\sum_i \sum_j \frac{n_i-1}{2}\frac{m_j-1}{2} \equiv \frac{n-1}{2}\frac{m-1}{2} \text{ [2]}$$

Pour prouver le point (iii), on commence par écrire $n = 2k+1$ et donc $n^2 = 4k^2 + 4k + 1$.
Si le nombre k est pair alors on écrit $k = 2p$ et il vient que

$$n^2 = 16p^2 + 16p + 1 \equiv 1 \text{ [8]}$$

Si k est impair, on écrit $k = 2p+1$ et on a de même

$$n^2 = 16p^2 + 24p + 9 \equiv 1 \text{ [8]}$$

Enfin, pour le point (iv), il suffit de refaire le même calcul que dans le point (i) en posant $n = 2k + 1$ et $m = 2k' + 1$ et le résultat découle directement. ■ Ainsi, pour prouver la troisième propriété, il suffit d'écrire

$$\left(\frac{-1}{n}\right) = \prod_i \left(\frac{-1}{p_i}\right)$$

d'après le critère d'Euler, il vient que

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

On utilise alors le point (i) du lemme pour conclure.
De la même manière, en utilisant la loi supplémentaire et le point (iv) du lemme, on prouve la quatrième propriété, et en utilisant la loi de réciprocité quadratique et le point (ii) on prouve la dernière propriété. ■

Comme dit précédemment, le symbole de Jacobi permet de calculer plus facilement les symboles de Legendre. En effet, il permet de fournir un algorithme efficace pour calculer $\left(\frac{m}{n}\right)$ pour tout $m \in \mathbb{Z}$ et pour tout entier n impair positif premier avec m :

(1) On cherche m' tel que $-\frac{n-1}{2} \leq m' \leq \frac{n-1}{2}$ et $m \equiv m'$ mod n
(2) On factorise m' sous la forme $m' = \epsilon 2^q m''$ avec m'' impair positif, q un entier et $\epsilon = \pm 1$
(3) On utilise les propriétés d symbole de Jacobi :

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right) = \epsilon^{\frac{n-1}{2}} \left(\frac{2}{n}\right)^q (-1)^{\frac{(n-1)(m''-1)}{4}} \left(\frac{n}{m''}\right)$$

(4) Si $m'' = 1$ c'est terminé, sinon on retourne à l'étape (1) en remarquant que $m'' < n$ et que n et m'' sont premiers entre eux.

D'un point de vu algorithmique, ce procédé est avantageux car il n'est pas nécessaire de décomposer m'' en facteur premiers (ce qui est très coûteux) mais seulement de trouver la plus grande puissance de 2 dans sa décomposition, ce qui est rapide à faire par ordinateur.

Illustrons cet algorithme par un exemple. Est-ce que 3763 est un carré modulo 20353 ?
A l'aide d'une machine, on calcule que $20353 \equiv 1538$ [3763]. De plus, $1538 = 2 \times 769$. On recommence, on a $3763 \equiv -82$ [769] et $82 = 2 \times 41$. Enfin, on a $769 \equiv -10$ [41]
On résume tout ça à l'aide du symbole de Jacobi :

$$\left(\frac{3763}{20353}\right) = \left(\frac{1538}{3763}\right) = -\left(\frac{769}{3763}\right)$$

d'où

$$\left(\frac{3763}{20353}\right) = -\left(\frac{-82}{769}\right) = -\left(\frac{41}{769}\right) = -\left(\frac{-10}{41}\right)$$

finalement, il vient que

$$\left(\frac{3763}{20353}\right) = -\left(\frac{-2}{41}\right)\left(\frac{5}{41}\right) = -1$$

donc on peut conclure que 3763 n'est pas un carré modulo 20353.
Nous allons maintenant conclure cette étude, nous allons étudier une application de la loi de réciprocité quadratique sur un test de primalité.

6.5.2 Test de primalité de Solovay-Strassen

Le test de primalité de Solovay-Strassen est un test dit probabiliste, c'est à dire qu'il donne avec une certaine probabilité la chance qu'un entier donné soit premier.
Le principe du test repose sur le critère d'Euler et le symbole de Jacobi. On choisit un entier n impair et un nombre (aussi grand que l'on veut) d'entiers a. On vérifie alors pour chaque entier a si l'égalité

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

est vérifiée. S'il existe a tel que l'égalité ne soit pas vérifiée alors n n'est pas premier.
Dans la pratique, cet algorithme a été utilisé jusqu'en 1980, où il a alors été remplacé par le test de primalité de Miller-Rabin.
Notons finalement en remarque que la nature probabiliste du test provient du fait qu'il existe des entiers a qui vérifient l'égalité dans les cas où n n'est pas premier. De tels nombres sont appelés des "menteurs d'Euler".

7 Conclusion

Cette étude de quelques équations diophantiennes et de la loi de réciprocité quadratique m'a permis de découvrir non seulement de nouveaux résultats très intéressants, mais aussi de nouvelles techniques de preuves, comme par exemple la méthode de descente infinie.

Grâce à la loi de réciprocité quadratique, j'ai également pu travailler sur les sommes de Gauss et sur des formules trigonométriques surprenantes qui n'ont a priori pas de lien direct avec le résultat, ce qui m'a donné la chance d'établir des liens entre différentes domaines des mathématiques, ce qui est à mon sens un des aspects les plus formidables de la théorie des nombres.

8 Bibliographie

-Alain Kraus : *Loi de réciprocité quadratique*, Cours de Master Université Pierre et Marie Curie