UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE APPLIQUÉES

PAR
HUGHES MOREAU

LA REPRÉSENTATION DES NOMBRES PREMIERS HYPERBOLIQUES DANS LE PLAN

AVRIL 2017

ÉVALUATEURS

Les personnes suivantes ont évalué le présent mémoire :

Dominic Rochon, directeur de recherche
Département de mathématiques et d'informatique

Sébastien Tremblay, juré
Département de mathématiques et d'informatique

Alain Chalifour, juré
Département de mathématiques et d'informatique

LA REPRÉSENTATION DES NOMBRES PREMIERS HYPERBOLIQUES DANS LE PLAN

Hughes Moreau

SOMMAIRE

L'intérêt actuel des nombres premiers est de recourir à des méthodes de cryptographie pour l'encodage de messages secrets militaires, de sécurisation des transactions bancaires en ligne, de protection de la vie privée, etc. Le but de ce mémoire est d'établir une nouvelle classe de nombres premiers : les nombres premiers hyperboliques. La théorie sur ces nombres premiers est comparée à celle dans les réels et les complexes.

L'ensemble des nombres hyperboliques est un anneau, et non un corps comme les réels ou les complexes. Suite à l'existence d'un isomorphisme entre la représentation cartésienne $z = x+yj$, où $j^2 = 1$, et la représentation matricielle $z = \left(\begin{smallmatrix} x & y \\ y & x \end{smallmatrix}\right)$, les propriétés sont démontrées en utilisant une base idempotente. Les éléments de cette base sont $e = \frac{1+i}{2}$ et $e^* = \frac{1-j}{2}$, où tout nombre $z = x + yj$ s'écrit, dans cette base, sous la forme $z = \alpha e + \beta e^*$. Cette représentation rend les opérations arithmétiques habituelles intuitives, ce qui permet de démontrer des théorèmes qui caractérisent les nombres premiers hyperboliques en utilisant des résultats de la théorie des nombres dans les réels. Pour la première fois, ces nombres premiers sont illustrés dans le plan cartésien.

THE REPRESENTATION OF THE HYPERBOLIC PRIME NUMBERS IN THE PLANE

Hughes Moreau

ABSTRACT

The current interest of the prime numbers is for cryptography purposes. Among other things, there is the encrypting of military messages, securing online bank account transactions, and protecting privacy. The goal of this master's thesis is to set a new class of prime numbers: the hyperbolic prime numbers. The theory about these prime numbers is compared to the one in the real and the complex numbers.

This set of hyperbolic numbers is a ring, and not a field like the real or complex numbers. Further to the existence of an isomorphism between the cartesian representation $z = x + yj$, where $j^2 = 1$, and the matrix representation $z = \left(\begin{smallmatrix} x & y \\ y & x \end{smallmatrix}\right)$, the properties are proved by using an idempotent basis. The elements of the basis are $e = \frac{1+i}{2}$ and $e^* = \frac{1-j}{2}$, where every single number $z = x + yj$ is written in that basis by $z = \alpha e + \beta e^*$. This representation makes the arithmetic operations more intuitive, and it allows to prove many theorems which characterize the hyperbolic prime numbers by using results from the number theory in the real field. For the first time, these prime numbers are shown in the Cartesian coordinate system.

AVANT-PROPOS

Au fil du temps, les mathématiques sont devenues une passion plus qu'« une matière dans laquelle j'avais moins de difficultés ». Je fais désormais des mathématiques parce que j'aime ça, par exemple dans le calcul de probabilités de jeux de société, ces derniers étant une passion pour moi. Quand vint le temps de choisir mon directeur de recherche (qui allait de pair avec le sujet), je me suis posé véritablement la question : « Maintenant que j'aime les mathématiques, qu'est-ce que j'aime le *plus* ? » Sans contredit, l'algèbre et la théorie des nombres. J'ai donc été voir mon actuel directeur de recherche Dominic Rochon et, bien qu'il fasse de l'analyse, il m'a proposé ce présent sujet de la théorie des nombres. Quand il m'expliquait ce qu'il en retournait, je ne comprenais rien du tout. Présentement, c'est tout le contraire : je comprends parfaitement où il voulait aller ! Au final, cela a donné cet ouvrage, qui a vu son lot de craintes, de calculs et de questionnements.

Je tiens personnellement à remercier Dominic Rochon. Merci pour ton support. Rencontre après rencontre, tu m'as guidé vers ce que tu attendais de moi. Merci pour ta confiance, car tu sais que je suis un bon petit garçon et que je fais toujours mes devoirs. Merci pour ta passion. Quand tu m'expliquais chaque petit détail, tu avais l'étincelle dans les yeux. Ne perds surtout pas ça, c'est ce qui fait que tu es un prof génial !

Comment pourrais-je passer à côté du soutien financier de l'ISM, l'Institut des Sciences Mathématiques, et le DMI, le Département de Mathématiques et d'Informatique. Vous m'avez donné la chance de me concentrer sur mon mémoire et d'avoir l'esprit tranquille. J'ai gagné le gros lot avec vous !

Merci à chacun de mes professeurs de l'UQTR. Vous m'avez fait rire, vous m'avez fait travailler et vous obtenez en retour un jeune professeur qui est prêt à tout affronter ! Et merci aux étudiants de l'association, je garde tellement de beaux souvenirs. Ce que l'on dit est vrai : l'université nous fait vivre les plus belles années de notre vie étudiante !

Finalement, merci à ma famille. Vous m'avez écouté raconter mes histoires de nombres premiers. Votre soutien a été seulement votre écoute, car vous n'avez rien compris de ce que je radotais... Mais vous pouvez quand même lire mon mémoire ! Maman : tu peux lire mon mémoire, c'est un livre avec des images !

Table des matières

Liste des tableaux

Table des figures

Introduction

La théorie des nombres est une des plus vieilles branches des mathématiques [17]. Les hommes de la préhistoire faisaient des correspondances un à un (des bijections), par exemple entre une roche dans un seau et un mouton pour savoir s'il restait des moutons dans les champs. Toutefois, ces enseignements se développèrent plus dans les civilisations babylonienne et égyptienne. Le mathématicien Pythagore de Samos et ses disciples ont jeté les bases de la théorie des nombres. Elle fut reprise par les Grecs, dû à la proximité (surtout maritime) de ces deux régions et de la Grèce. Les résultats des pythagoriciens touchaient principalement l'arithmétique (classification des nombres selon la parité ; types de nombres tels amicaux, parfaits... ; les nombres figurés tels les nombres triangulaires, carrés... ; les proportions et les nombres irrationnels), la géométrie (solides réguliers, la méthode d'application des aires), la musique, etc. Par la suite, Euclide, réunissant plusieurs résultats de la théorie des nombres, de la géométrie et plus encore, publia son livre *Éléments*, très célèbre à cette époque. Bon nombre de mathématiciens suivirent dans les siècles suivants tels que Dipohante, Fibonacci, Fermat, Goldbach, Euler, pour ne nommer que ceux-là, et plus récemment, Andrew Wiles, qui démontra le théorème de Fermat.

Les nombres premiers ont été grandement étudiés, plusieurs ouvrages témoignant des résultats fort impressionnants en lien avec ces nombres ([1], [6], [7], [22] et [23]). Un des résultats notables est le *théorème de l'arithmétique*, donnant l'existence d'une représentation de *n'importe quel nombre* en fonction de nombres uniquement premiers [1]. En guise de rappel, le chapitre 1 est dédié uniquement aux définitions et aux théorèmes menant au théorème de l'arithmétique réel.

Dans le livre de Kantor et de Solodovnikov [5], la multiplication complexe, donnée par la formule $(a + bi)(c + di) = ac + adi + bci + bdi^2$, est complètement déterminée par la valeur de l'unité imaginaire. C'est-à-dire que, en posant $i^2 = p + qi$, la multiplication devient $(a + bi)(c + di) = (ac + bdp) + (ad + bc + bdq)i$. Par des manipulations algébriques, on compte seulement trois systèmes de nombres différents que l'on peut obtenir : les complexes $(i^2 = -1)$, les hyperboliques $(i^2 = 1)$ et les duaux $(i^2 = 0)$. Toute combinaison de p et de q est équivalente à un de ces trois systèmes. Comme l'unité des nombres duaux n'est pas inversible $\left(\text{c'est-à-dire } \frac{1}{i} = \frac{i}{i^2} = \frac{i}{0}\right)$, cette catégorie de nombres perd de son intérêt dans le

présent ouvrage. Ainsi, il reste les nombres complexes et hyperboliques.

Le chapitre 2 est consacré aux nombres complexes ([4], [11] et [14]). On rappelle les définitions de base sur les nombres et les opérations sur les complexes. Repris principalement des ouvrages de Stan Wagon ([12], [13] et [18]), les propositions et les théorèmes sont à nouveau démontrés et expliqués rigoureusement dans le but d'obtenir cette décomposition en nombres complexes. Puis, on définit les entiers de Gauss, ensemble dénoté par le symbole $\mathbb{G}$, et on démontre quelques résultats. La norme complexe revêt un intérêt particulier dans $\mathbb{G}$. En effet, les nombres premiers complexes sont les $z \in \mathbb{G}$ tels que : z (ou iz) est un entier premier congru à 3 modulo 4, et $|z|^2$ est un entier premier. La norme est centrale dans l'expression des nombres premiers complexes.

Le chapitre 3 présente l'anneau des nombres hyperboliques et leurs propriétés de base ([9], [10] et [20]). Un nombre hyperbolique est un nombre $z = x+yj$ tel que $x, y \in \mathbb{R}$ et $j^2 = 1$. En effectuant un changement de base adéquat, cette base étant appelée « la base idempotente », le nombre $z = x+yj$ en coordonnées cartésiennes s'écrit $z = (x+y)e+(x-y)e^* = \alpha e+\beta e^*$ en coordonnées idempotentes, où $e = \frac{1+j}{2}$ et $e^* = \frac{1-j}{2}$. Les calculs sont intuitifs et simplifiés, car toute opération arithmétique est effectuée sur chaque composante idempotente respective.

N'ayant guère besoin de plus, le chapitre 4 présente les nombres premiers hyperboliques : $2^k e + 2e^*$, $2e + 2^k e^*$, $pe + 1e^*$ et $1e + pe^*$ et leurs associés, où $k \in \mathbb{N}$ et p est un entier premier impair. Ces nombres premiers sont dits *triviaux*, car leur primalité vient de la définition usuelle d'un nombre premier : « Tout nombre ayant seulement 1 et lui-même comme diviseur. »

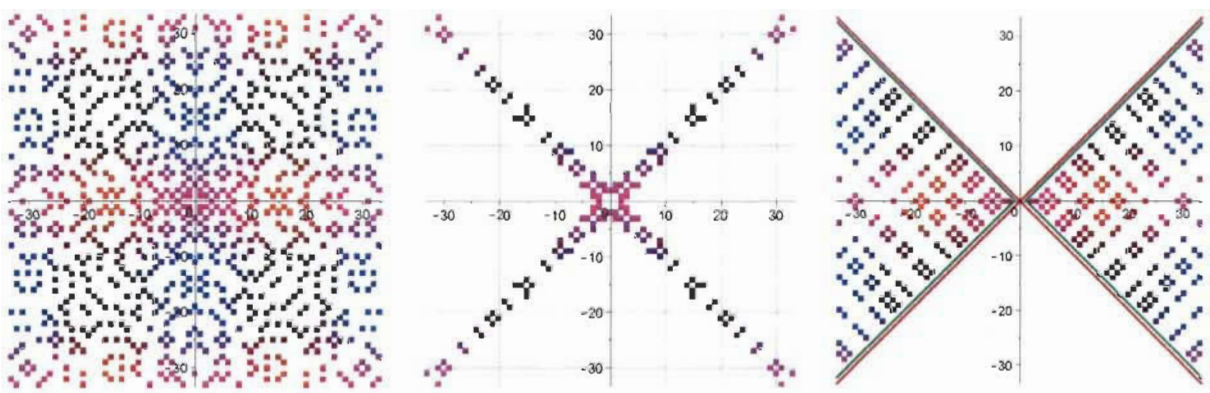


FIGURE 0.1 – Différentes classes de nombres premiers.
(A) Complexes. (B) Hyperboliques triviaux. (C) Hyperboliques non triviaux.

Par la suite, en considérant un module hyperbolique strictement positif, on introduit une nouvelle catégorie de nombres : les nombres $\mathbb{P}$ dont les deux composantes idempotentes α et β sont entières et premières. En modifiant la définition de la primalité par « tout nombre de

$\mathbb{P}$ ayant uniquement lui-même comme diviseur qui appartient à $\mathbb{P}$ », ces nouveaux nombres $\mathbb{P}$ s'avèrent être eux aussi premiers, dits *non triviaux* dû au changement de la définition de la primalité.

Exploitant cette nouvelle classe de nombres, les résultats de ce mémoire permettront de créer un lien entre les non triviaux et la conjecture de Goldbach ([8] et [24]). Pour cela, on exprime différemment les nombres hyperboliques : $z = x + yj = \frac{\alpha+\beta}{2} + \frac{\alpha-\beta}{2}j$. La conjecture de Goldbach sera valide si et seulement si l'ensemble des parties réelles $\frac{\alpha+\beta}{2}$ est l'ensemble $\mathbb{Z}\backslash\{-1, 0, 1\}$. De plus, la conjecture de Polignac, symétrique à celle de Goldbach, dit que *tout nombre pair est la différence de deux nombres premiers consécutifs d'une infinité de façons* [21]. Cette conjecture sera vérifiée si et seulement si l'ensemble des parties imaginaires $\frac{\alpha-\beta}{2}$ est l'ensemble $\mathbb{Z}$.

Chapitre 1

Les nombres premiers réels

Dans ce chapitre, nous revoyons la théorie des nombres premiers dans les réels. À l'aide de définitions et de propositions [1], nous présentons les résultats fondamentaux sur les nombres premiers. Nous supposons que les différents sous-ensembles de nombres (naturels, entiers, rationnels, irrationnels et réels) sont bien définis et que l'on maîtrise la théorie des ensembles. Voici un premier théorème que nous ne démontrerons pas.

Note : Dans le présent ouvrage, l'ensemble des entiers naturels est $\mathbb{N} = \{1, 2, 3, ...\}$.

Théorème 1.1 (Principe du bon ordre)**.** *Tout ensemble non vide* $S \subset \mathbb{N}$ *contient un plus petit élément.*

Le théorème suivant est connu sous le nom de « lemme d'Archimède ». Par contre, selon certaines sources [17], on peut croire que se serait Eudoxe de Cnide qui aurait d'abord utilisé ce lemme et qui fût repris par Euclide dans ses *Éléments* et puis par Archimède.

Théorème 1.2 (Propriété archimédienne)**.** *Soit* $a, b \in \mathbb{N}$. *Alors il existe un entier positif* n *tel que* $na \geq b$.

Démonstration. Procédons par contradiction. Supposons que pour tout entier positif n, on a $na < b$. Considérons l'ensemble $S = \{b - na : n \in \mathbb{N}\}$. Par la fermeture des entiers, $b - na \in \mathbb{Z}$ et $na < b \Rightarrow b - na > 0$, d'où $b - na \in \mathbb{N}$. Ainsi, $S \subset \mathbb{N}$. De plus, il est clair que $S \neq \varnothing$, car si $n \in \mathbb{N}$ alors il existe une infinité d'éléments de la forme $b - na$. Par le principe du bon ordre, il existe un plus petit élément $s_0 \in S$ tel que $s_0 \leq s$, pour tout $s \in S$. Posons $s_0 = b - n_0 s$. Or, comme $b - (n_0 + 1)s \in S$, on doit avoir

$$b - (n_0 + 1)a \geq b - n_0 s.$$

Ceci veut dire que $n_0 + 1 \leq n_0$, ce qui est une contradiction. ■

Définition 1.3. *Soit* $a, b \in \mathbb{Z}$ *avec* $a \neq 0$. *On dit que* a ***divise*** b *s'il existe* $q \in \mathbb{Z}$ *tel que* $b = aq$. *Dans un tel cas, on note* $a|b$

Si a **ne divise pas** b, alors on écrit $a \nmid b$. Cette notation sera privilégiée dans cet ouvrage.

Théorème 1.4. *Soit $a, b, c \in \mathbb{Z}$. Si $a|b$ et $a|c$, alors $a|(bx + cy)$, pour $x, y \in \mathbb{Z}$.*

Démonstration. Puisque $a|b$ et $a|c$, il existe $m, n \in \mathbb{Z}$ tels que $b = am$ et $c = an$. Or,

$$bx + cy = amx + any = a(mx + ny),$$

pour $x, y \in \mathbb{Z}$. Par la fermeture des entiers, on sait que $mx + ny \in \mathbb{Z}$. D'où $a|(bx + cy)$. ■

Les résultats précédents sont suffisants pour démontrer un théorème important de la théorie des nombres : la division euclidienne.

Théorème 1.5 (Division euclidienne)**.** *Soit $a, b \in \mathbb{Z}$ avec $a > 0$. Il existe $q, r \in \mathbb{Z}$ tels que $b = aq + r$, où $0 \leq r < a$. De plus, si $a \nmid b$, alors $0 < r < a$.*

Démonstration. Considérons l'ensemble $S = \{b - ma : b - ma \geq 0, m \in \mathbb{Z}\}$. Par la fermeture des entiers, on a $b - ma \in \mathbb{Z}$ et $S \subset \mathbb{N} \cup \{0\}$. De plus, une conséquence de la propriété archimédienne nous assure que $S \neq \varnothing$. Par le principe du bon ordre, on a que S contient un plus petit élément $r \geq 0$, d'où $r = b - qa$, avec $q \in \mathbb{Z}$. Dans ce cas, on a $b = aq + r$. Montrons que $r < a$. Supposons que $r \geq a$. On a $b - qa \geq a$, d'où $b - (q + 1)a \geq 0$. Ainsi, $b - (q + 1)a \in S$. Aussi, on sait que $b - (q + 1)a < b - qa = r$, ce qui contredit le fait que r est le plus petit élément de S. On conclut que $r < a$.

Pour la deuxième partie de la preuve, procédons par contraposition. Ainsi, si $r = 0$, alors $b = aq + r = aq \Rightarrow a|b$. ■

Définition 1.6. *Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Le **plus grand commun diviseur** de a et b est l'**entier positif** d qui satisfait :*

- *$d|a$ et $d|b$;*
- *si $c|a$ et $c|b$, alors $c \leq d$.*

On abrège souvent « plus grand commun diviseur » par pcgd. On note le pgcd de a et b par $\text{pgcd}(a, b)$ ou simplement (a, b) en l'absence de confusion. La notation utilisée dans cet ouvrage sera $\text{pgcd}(a, b)$.

Théorème 1.7. *Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Alors il existe $x_0, y_0 \in \mathbb{Z}$ tels que* $\text{pgcd}(a, b) = ax_0 + by_0$.

Démonstration. Considérons l'ensemble $S = \{ax + by : ax + by > 0, x, y \in \mathbb{Z}\}$. Par la fermeture des entiers, on a $ax + by \in \mathbb{Z}$ et comme $ax + by > 0$ alors $ax + by \in \mathbb{N}$. Par une conséquence de la propriété archimédienne, on a $S \neq \varnothing$. Ainsi, par le principe du bon ordre, S a un plus petit élément que l'on note d_0. Pour un certain choix $x_0, y_0 \in \mathbb{Z}$, on peut écrire $d_0 = ax_0 + by_0$. Il suffit de montrer que $d_0 = \text{pgcd}(a, b)$. On doit vérifier les deux conditions de la définition 1.6.

- Première condition. Supposons que $d_0 \nmid a$. D'après la division euclidienne, il existe $q, r \in \mathbb{Z}$ tels que $a = qd_0 + r$, où $0 < r < d_0$. On a

$$r = a - qd_0 = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) > 0.$$

  Ainsi, $r \in S$ et $r < d_0$. Ce qui contredit le fait que d_0 soit le plus petit élément de S. On conclut que $d_0|a$. On procède de la même façon pour conclure que $d_0|b$.

- Deuxième condition. Supposons que $d_1|a$ et $d_1|b$. Par le théorème 1.4, on a que $d_1|(ax + by)$, pour tout $x, y \in \mathbb{Z}$. En particulier $d_1|(ax_0 + by_0) \Rightarrow d_1|d_0$, et comme $d_0 > 0$, on a que $d_1 \leq d_0$.

■

Théorème 1.8. *Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Alors*

$$\text{pgcd}(a, b) = 1 \iff \text{il existe } x, y \in \mathbb{Z} \text{ tels que } ax + by = 1.$$

Démonstration.

$\Longrightarrow$) Si $\text{pgcd}(a, b) = 1$, d'après le théorème 1.7, il existe $x, y \in \mathbb{Z}$ tels que $ax + by = \text{pgcd}(a, b) = 1$.

$\Longleftarrow$) Soit $d = \text{pgcd}(a, b)$. D'après le théorème 1.4, il existe $x, y \in \mathbb{Z}$ tels que $d|(ax+by) \Rightarrow d|1$. Comme $1|a$ et $1|b$, par la définition 1.6, on a que $1 \leq \text{pgcd}(a, b) = d$. D'où $d = 1$. ■

Théorème 1.9 (Lemme d'Euclide)**.** *Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$.Si $a|bc$ et* $\text{pgcd}(a, b) = 1$, alors $a|c$.

Démonstration. D'après le théorème 1.8, il existe $x, y \in \mathbb{Z}$ tels que $ax+by = 1$. En multipliant par c, on a $axc + byc = c$. Il est évident que $a|ac$ et $a|bc$ par hypothèse. Par le théorème 1.4, a divise toute combinaison linéaire entre ac et bc. Ainsi, en particulier, $a|(axc + byc)$, d'où $a|c$. ■

Maintenant, résumons quelques propriétés des nombres premiers.

Définition 1.10. *Un entier $p > 1$ est un* ***nombre premier*** *si ses seuls diviseurs positifs sont 1 et p. Si un entier plus grand que 1 n'est pas premier, alors il est dit* ***composé****.*

Théorème 1.11. *Si p est premier et $p|ab$, alors $p|a$ ou $p|b$.*

Démonstration. Si $p|a$, on a le résultat. Supposons que $p \nmid a$ et démontrons que $p|b$. Comme $p \nmid a$, par la définition 1.6 et du fait que p est premier, on a que $\text{pgcd}(a, p) = 1$. On a ainsi les conditions du lemme d'Euclide et on conclut que $p|b$. ■

Corollaire 1.12. *Si p est premier et si $p|a_1a_2\cdots a_r$, alors il existe un entier $k \in \{1, 2, ..., r\}$ tel que $p|a_k$.*

Démonstration. On démontre ce corollaire par induction sur r.

- Cas $r = 1$. On a $p|a_1$, d'où $k = 1$.
- Cas $r > 1$. Supposons le corollaire vérifié jusqu'à $r - 1$. Démontrons qu'il est vrai pour r. Par l'hypothèse d'induction on a $p|a_1a_2\cdots a_{r-1}$, alors il existe $k_1 \in \{1, 2, ..., r-1\}$ tel que $p|a_{k_1}$. Si $p|a_1a_2\cdots a_{r-1}a_r$, alors, par le théorème 1.11, $p|a_1a_2\cdots a_{r-1}$ ou $p|a_r$. Si $p|a_1a_2\cdots a_{r-1}$, alors $p|a_{k_1}$. Si $p \nmid a_1a_2\cdots a_{r-1}$, alors $p|a_r$ et $k = r$.

Par le principe d'induction mathématique, on conclut que le résultat est vrai pour tout $r \in \mathbb{N}$. ■

Corollaire 1.13. *Si $p, q_1, q_2, ..., q_r$ sont des nombres premiers et si $p|q_1q_2\cdots q_r$, alors il existe $k \in \{1, 2, ..., r\}$ tel que $p = q_k$.*

Démonstration. On démontre ce corollaire par induction sur r.

- Cas $r = 1$. On a p et q_1 premiers et $p|q_1$. Comme $p|q_1$, il existe $n \in \mathbb{Z}$ tel que $q_1 = pn$. Ainsi, p et n sont des diviseurs de q_1. Or, les diviseurs de q_1 sont 1 et q_1. Comme $p \neq 1$, car il est premier, cela force $p = q_1$ et $n = 1$. Donc, on prend $k = 1$ pour obtenir la conclusion.
- Cas $r > 1$. Supposons le corollaire vérifié jusqu'à $r - 1$. Démontrons qu'il est vrai pour r. De l'hypothèse d'induction, si $p|q_1q_2\cdots q_{r-1}$, alors il existe $k_1 \in \{1, 2, ..., r-1\}$ tel que $p = q_{k_1}$. Par hypothèse, on a $p|q_1q_2\cdots q_{r-1}q_r$. Par le théorème 1.11, on a $p|q_1q_2\cdots q_{r-1}$ ou $p|q_r$. Si $p|q_1q_2\cdots q_{r-1}$, alors $p = q_{k_1}$. Par contre, si $p \nmid q_1q_2\cdots q_{r-1}$, alors $p|q_r$. Par l'argument utilisé dans le cas trivial, on a $p = q_r$, d'où $k = r$.

Par le principe d'induction mathématique, on conclut que le résultat est vrai pour tout $r \in \mathbb{N}$. ■

Théorème 1.14 (Théorème fondamental de l'arithmétique)**.** *Tout nombre naturel $n > 1$ peut s'écrire comme un produit de nombres premiers. La représentation est unique, à l'exception de l'ordre de présentation des facteurs premiers.*

Démonstration. Si n est premier, la démonstration est terminée. Supposons que n est composé. Considérons l'ensemble $D = \{d : d|n, 1 < d < n\}$. On sait que D est constitué de nombres naturels et, comme n est composé, il existe un nombre qui divise n, d'où $D \neq \varnothing$. Par le principe du bon ordre, il existe un plus petit élément $p_1 \in D$. On doit avoir que p_1

est premier, sinon il existerait d'autres nombres plus petits qui diviseraient p_1 et qui seraient dans D. On peut donc écrire $n = p_1 n_1$. Si n_1 est premier, la démonstration est terminée. Si n_1 est composé, on répète le même argument et on en déduit l'existence d'un nombre premier p_2 et d'un entier $n_2 < n_1$ tel que $n = p_1 p_2 n_2$. En poursuivant jusqu'à l'étape k, on a $n = p_1 p_2 \cdots p_k n_k$, où $n_1 > n_2 > \cdots > n_k > 1$. Comme les n_i sont des entiers strictement décroissants, le processus a une fin, ce qui force n_k à être premier à l'étape k, c'est-à-dire $n_k = p_{k+1}$. Ainsi, $n = p_1 p_2 \cdots p_{k+1}$, ce qui démontre l'existence de la représentation.

Supposons que la représentation n'est pas unique, c'est-à-dire que $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, où les p_i et les q_j sont tous des nombres premiers. Simplifions les p_i et les q_j qui apparaissent dans les deux membres de l'équation. Celle-ci devient $p_{i_1} p_{i_2} \cdots p_{i_\alpha} = q_{j_1} q_{j_2} \cdots q_{j_\beta}$, où $\alpha \leq r$ et $\beta \leq s$. Ainsi, dans la dernière équation, tous les p_i sont différents des q_j. Or, cela veut dire que $p_{i_1} | q_{j_1} q_{j_2} \cdots q_{j_\beta}$. Par le corollaire 1.13, il existe $k \in \{1, 2, ..., \beta\}$ tel que $p_{i_1} = q_{j_k}$. Nous avons une contradiction avec le fait que tous les p_i sont différents des q_j. Donc, la représentation de n est unique. ■

Ce chapitre fut un bref rappel des principaux théorèmes et définitions qui seront utilisés dans l'étude des nombres complexes et hyperboliques.

Chapitre 2

Les nombres premiers complexes

Les nombres imaginaires donnent tout particulièrement l'occasion de regarder le jeu croisé de l'algèbre et de la géométrie. (Jean-Pierre Cléro, [3])

La culture populaire moderne tend à expliquer l'apparition des nombres complexes par le besoin d'obtenir les racines d'un polynôme du second degré. Or, il n'en est rien. Les mathématiciens de l'an mil avaient la tendance à découler d'un problème géométrique une équation algébrique (sans nos symboles actuels, mais en mots) et vice versa. Pour eux, les mathématiques étaient utilitaires et non purement algébriques. Des problèmes comme la duplication du cube, la trisection de l'angle et la construction de polygones réguliers cachaient des équations du troisième degré de la forme $x^3 + px = q$. Leurs résolutions vinrent de Jérôme Cardan, vers 1545, qui a poussé plus loin les solutions de Nicolas Tartaglia (dit le bègue) dans son ouvrage *Ars Magna*. Or, dans les solutions proposées, les radicandes étaient positifs. Bien que certaines équations ne pouvaient être résolues par les techniques de Tartaglia et Cardan, on remarque que les radicandes devaient être négatifs.

C'est Raphael Bombelli qui calcula les produits entre 1, -1, $\sqrt{-1}$ et $-\sqrt{-1}$. Il fit cela dans *Algebra*, écrit en 1560, mais publié en 1572. Surnommées « imaginaires » par Descartes, ces quantités ne pouvaient pas être représentées par une « image », par quelque chose de « réel ». Euler désignera lui-même la notation i pour $\sqrt{-1}$. Gauss reprend cette notation pour éviter les erreurs de calcul, mais le symbole tarde à être repris par les mathématiciens de l'époque.

En 1799, Gauss donne une démonstration du théorème fondamental de l'algèbre, qui satisfait ses contemporains. Pendant près de 20 ans, il travaille sur le plan complexe, puis en 1831, Gauss utilise l'expression « nombre complexe » [3].

2.1 Rappels

Les nombres complexes (ou *nombres imaginaires* ou simplement *complexes*) sont des nombres ayant deux composantes. La *forme algébrique* d'un de ces nombres s'écrit $a+bi$, où $a, b \in \mathbb{R}$ et $i = \sqrt{-1} \notin \mathbb{R}$. Cette forme est la plus fréquemment utilisée pour l'introduction des nombres complexes et des propriétés de base.

Le plan complexe reprend essentiellement l'idée du plan euclidien, car $a, b \in \mathbb{R}$. Dans le plan complexe, l'axe des abscisses du plan euclidien devient l'*axe réel* tandis que l'axe des ordonnées devient l'*axe imaginaire*. Ce dernier axe est l'axe réel multiplié par le nombre i.

De façon générale, un nombre imaginaire est noté z. La composante a est appelée la partie réelle $\mathrm{Re}(z)$ alors que la composante b est la partie imaginaire $\mathrm{Im}(z)$. Par exemple, les parties réelle et imaginaire du nombre $z = 2 - 3i$ sont $\mathrm{Re}(z) = \mathrm{Re}(2 - 3i) = 2$ et $\mathrm{Im}(z) = \mathrm{Im}(2-3i) = -3$. En ayant ces deux informations, il est possible de placer le nombre z dans le plan complexe, à la position du point $(2, -3)$.

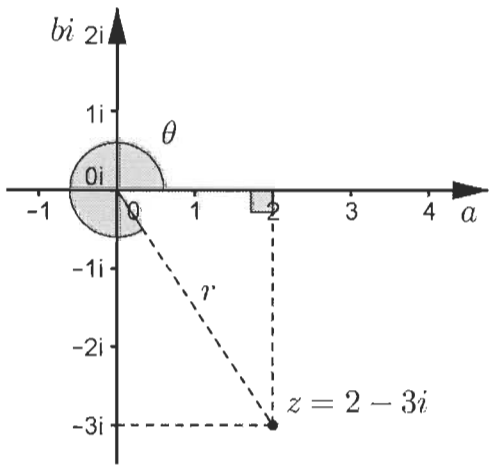


FIGURE 2.1 – Nombre complexe dans le plan.

En constatant qu'un complexe ayant sa partie imaginaire valant 0 est un réel, il est donc naturel de penser que les réels forment un sous-ensemble des complexes. En effet, les complexes sont une extension des réels. Il faut cependant savoir que les complexes perdent certaines propriétés des réels. Une de ces propriétés est la relation d'ordre qui était définie entre deux nombres réels et qui n'a plus lieu d'être chez les complexes. Il est évident que $2 < 5$, mais comment savoir si $2 + 4i < 5 - i$? La réponse est simple : il n'existe aucune relation d'ordre sur $\mathbb{C}$ qui corresponde aux opérations définies sur $\mathbb{C}$ ([4] et [16]).

Toutefois, bien que les complexes ne soient pas ordonnés, ces nombres respectent certaines propriétés généralisées de celles des réels [11].

Définition 2.2. *Soit $z = a + bi$ et $w = c + di$. Les quatre opérations arithmétiques de $\mathbb{C}$ sont définies par :*

$$\begin{aligned} z + w &= (a + bi) + (c + di) = (a + c) + (b + d)i; \\ z - w &= (a + bi) - (c + di) = (a - c) + (b - d)i; \\ zw &= (a + bi)(c + di) = (ac - bd) + (ad + bc)i; \\ \frac{z}{w} &= \frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i, \text{ si } w \neq 0. \end{aligned}$$

Définition 2.3. *Le **conjugué** de $z = a + bi$ est $\overline{z} = a - bi$.*

Le conjugué correspond au changement de signe de la partie imaginaire. Si $z \in \mathbb{R}$, alors $\overline{z} = z$ puisque z n'a pas de partie imaginaire. Graphiquement, $\overline{z}$ est la symétrie de z par rapport à l'axe réel $\mathbb{R}$.

Proposition 2.4. *Soit $z \in \mathbb{C}$. Alors $\overline{\overline{z}} = z$.*

Démonstration. Soit $z = a + bi \in \mathbb{C}$. Par la définition 2.3, on a

$$\begin{aligned} \overline{\overline{z}} &= \overline{\overline{a + bi}} \\ &= \overline{a - bi} \\ &= a + bi \\ &= z. \end{aligned}$$

■

Définition 2.5. *Le **module** (ou la **norme**) de $z = a + bi$ est $|z| = \sqrt{a^2 + b^2}$.*

Cette définition est en lien avec la relation de Pythagore. Puisque z correspond aux coordonnées (a, b) du plan, la distance de z à l'origine est $\sqrt{(a - 0)^2 + (b - 0)^2} = \sqrt{a^2 + b^2}$.

Une deuxième façon d'écrire un nombre complexe est sous la *forme polaire* [4]. Deux variables sont utilisées et bien plus visibles par la relation de Pythagore. Ce sont la norme r et l'angle θ. La norme est obtenue par la relation de Pythagore illustrée à la figure 2.1. La composante θ mesure l'angle entre l'axe des réels positifs et le vecteur $\overrightarrow{Oz}$. L'angle θ appartient à l'intervalle $[0, 2\pi)$. Le nombre complexe est alors exprimé par

$$z = re^{\theta i}.$$

Il est possible de convertir sous la forme polaire chacune des opérations arithmétiques définies à partie de la forme algébrique. Comme ce n'est pas l'objet de ce mémoire, je laisse la liberté au lecteur de consulter l'ouvrage [4] pour plus de détails.

Une troisième façon de représenter les nombres complexes est avec les matrices [6]. Le nombre complexe $z = a + bi$ devient $f(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ sous la forme matricielle, où f est un isomorphisme. L'addition et la multiplication matricielles sont les opérations usuelles. Soit $f(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ et $f(w) = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, alors

$$f(z+w) = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} = f(z) + f(w);$$

$$f(zw) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = f(z)f(w).$$

Les deux opérations sont donc bien définies par les matrices puisqu'une opération faite sur deux nombres complexes donne aussi un nombre complexe (fermeture). De plus, le neutre de l'addition est la matrice nulle, le neutre de la multiplication est la matrice identité et l'unité imaginaire est

$$f(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

2.2 Les entiers de Gauss

Si l'ensemble $\mathbb{C}$ est restreint à l'ensemble $\{a+bi : a, b \in \mathbb{Z}\}$, nous obtenons une extension des entiers $\mathbb{Z}$. Cet ensemble est appelé les *entiers de Gauss*. Il est noté $\mathbb{Z}[i]$ ou $\mathbb{G}$; c'est ce dernier symbole qui sera utilisé dans cet ouvrage. L'addition, la soustraction et la multiplication restent inchangées. Toutefois, la division est plus sensible. De la définition 2.2, les quotients $\frac{ac+bd}{c^2+d^2}$ et $\frac{bc-ad}{c^2+d^2}$ doivent être entiers, où $(a, b, c, d) \in \mathbb{Z}^4$. Il existe des combinaisons de quatre entiers tels que les quotients ne le sont pas, par exemple $(a, b, c, d) = (1, 2, 3, 4)$.

Définition 2.6. *Dans $\mathbb{G}$, les **unités imaginaires complexes** sont définies comme étant 1, -1, i et $-i$.*

Note : Dans les sections suivantes du présent chapitre, une unité est une unité imaginaire complexe.

Proposition 2.7. *Chaque entier de Gauss est divisible par les unités.*

Démonstration. Soit $z = a + bi \in \mathbb{G}$, où $a, b \in \mathbb{Z}$.

1. $\dfrac{z}{1} = \dfrac{a+bi}{1} = \dfrac{a}{1} + \dfrac{b}{1}i = a + bi \in \mathbb{G}$,
2. $\dfrac{z}{-1} = \dfrac{a+bi}{-1} = \dfrac{a}{-1} + \dfrac{b}{-1}i = -a - bi \in \mathbb{G}$,
3. $\dfrac{z}{i} = \dfrac{a+bi}{i} = \dfrac{a}{i} + \dfrac{b}{i}i = \dfrac{a}{i^2}i + b = b - ai \in \mathbb{G}$,
4. $\dfrac{z}{-i} = \dfrac{a+bi}{-i} = \dfrac{a}{-i} + \dfrac{b}{-i}i = \dfrac{a}{-i^2}i - b = -b + ai \in \mathbb{G}$.

■

L'ensemble des unités $\{1, -1, i, -i\}$ est clairement fermé sous la multiplication. Regardons la table de Cayley de la multiplication.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

TABLE 2.8 – Table de Cayley de la multiplication des unités imaginaires complexes.

Proposition 2.9. *Les unités sont inversibles.*

Démonstration. Il suffit de constater que le neutre multiplicatif 1 se retrouve une seule fois dans chaque ligne et dans chaque colonne de la table de Cayley. ■

Définition 2.10. *Soit $z, w \in \mathbb{G}$ et $w \neq 0$. S'il existe $n \in \mathbb{G}$ tel que $z = wn$, alors w **divise** z.*

Comme à la définition 1.3, on symbolise la relation par $|$. D'où w divise z s'abrège par la notation $w|z$.

Définition 2.11. *Soit $z, w \in \mathbb{G}$ et une unité notée par I. Si $z = wI$, alors z et w sont appelés des nombres **associés**.*

Exemple 2.12. Le nombre 4 est associé à -4, $4i$ et $-4i$. En effet, $4 \cdot 1 = -4 \cdot -1 = 4i \cdot -i = -4i \cdot i$.

Les propositions suivantes proviennent de [12] et chaque proposition est vérifiée pour tous les nombres dans $\mathbb{C}$.

Proposition 2.13. *Soit $z \in \mathbb{C}$. Alors $|z|^2 = z\overline{z}$.*

Démonstration. Soit $z = a + bi$. En partant du membre droit de l'égalité, on a

$$\begin{aligned} z\overline{z} &= (a+bi)\overline{(a+bi)} \\ &= (a+bi)(a-bi) \\ &= a^2 - abi + abi - b^2i^2 \\ &= a^2 - b^2i^2 \\ &= a^2 + b^2 \\ &= |z|^2. \end{aligned}$$

■

Proposition 2.14. *Soit $z \in \mathbb{C}$. Alors $|z| = |\overline{z}|$.*

Démonstration. En utilisant la proposition 2.13 et la commutativité du produit,

$$|\overline{z}|^2 = \overline{z}\,\overline{\overline{z}} = \overline{z}z = |z|^2.$$

Il suffit de prendre la racine carrée, car la norme élevée au carré est un réel positif ou nul. ■

Proposition 2.15. *Soit $z, w \in \mathbb{C}$. Alors $|zw| = |z| \cdot |w|$.*

Démonstration. Soit $z = a + bi$ et $w = c + di$. Évaluons le produit zw ;

$$\begin{aligned} zw &= (a+bi)(c+di) \\ &= ac + adi + bci + bdi^2 \\ &= ac + adi + bci - bd \\ &= (ac - bd) + (ad + bc)i. \end{aligned}$$

En évaluant le membre gauche de l'égalité,

$$\begin{aligned} |zw|^2 &= (ac-bd)^2 + (ad+bc)^2 \\ &= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2+d^2) + b^2(c^2+d^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &= |z|^2 \cdot |w|^2. \end{aligned}$$

Étant donné que $|zw|^2$, $|z|^2$ et $|w|^2 \in \mathbb{R}_+$, il suffit de prendre la racine carrée de chaque membre de l'égalité pour terminer la démonstration. ■

Proposition 2.16. *Soit $z, w \in \mathbb{C}$ et $w \neq 0$. Si $w|z$, alors $\overline{w}|\overline{z}$.*

Démonstration. Comme $w|z$ dans $\mathbb{C}$, il existe $n \in \mathbb{C}$ tel que $z = wn$, où $w \neq 0$. De cette égalité, on obtient

$$z = wn \Rightarrow \overline{z} = \overline{wn} \Rightarrow \overline{z} = \overline{w} \cdot \overline{n}.$$

Puisque $n \in \mathbb{C}$, alors $\overline{n} \in \mathbb{C}$. De la dernière égalité, on conclut que $\overline{w}|\overline{z}$. ■

Les propositions suivantes seront vérifiées dans le sous-ensemble $\mathbb{G}$ de $\mathbb{C}$. Rappelons que si $z \in \mathbb{G}$, alors $|z|^2 = a^2 + b^2$ est un entier non négatif, dû à la fermeture dans $\mathbb{Z}$.

Proposition 2.17. *Soit $z, w \in \mathbb{G}$ et $w \neq 0$. Si $w|z$ dans $\mathbb{G}$, alors $|w|^2 \mid |z|^2$ dans $\mathbb{Z}$.*

Démonstration. Comme $w|z$ dans $\mathbb{G}$, il existe $n \in \mathbb{G}$ tel que $z = wn$, où $w \neq 0$. Il découle de cette l'égalité que $|z|^2 = |wn|^2$. Par la proposition 2.15, $|z|^2 = |w|^2 \cdot |n|^2$. Puisque $|n|^2 \in \mathbb{Z}$, alors $|w|^2 \mid |z|^2$ dans $\mathbb{Z}$. ■

Proposition 2.18. *Les unités sont les seuls entiers de Gauss qui possèdent un inverse dans $\mathbb{G}$.*

Démonstration. Soit $z = a + bi \in \mathbb{G}$. Le nombre $z^{-1} \in \mathbb{G}$ est l'inverse de z si et seulement si $zz^{-1} = 1 = z^{-1}z$. Montrons que $zz^{-1} = 1$, où $z^{-1} = \dfrac{1}{z} \in \mathbb{G}$. Clairement 0 n'a pas d'inverse. Supposons $z \neq 0$. En réexprimant z^{-1}, on obtient

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z\overline{z}} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \in \mathbb{G}.$$

Ceci implique que $\dfrac{a}{a^2 + b^2} \in \mathbb{Z}$ et $\dfrac{-b}{a^2 + b^2} \in \mathbb{Z}$, où $a, b \in \mathbb{Z}$. Séparons la démonstration par cas.

Premier cas : $a = 0$ et $b \neq 0$. On obtient les valeurs suivantes : $\dfrac{a}{a^2 + b^2} = \dfrac{0}{b^2} = 0 \in \mathbb{Z}$ et $\dfrac{-b}{a^2 + b^2} = \dfrac{-b}{b^2} = \dfrac{-1}{b}$. Comme $\dfrac{-1}{b} \in \mathbb{Z}$, alors $b = \pm 1$.

Deuxième cas : $a \neq 0$ et $b = 0$. Similairement au premier cas, on obtient les deux expressions suivantes : $\dfrac{a}{a^2 + b^2} = \dfrac{a}{a^2} = \dfrac{1}{a}$ et $\dfrac{-b}{a^2 + b^2} = \dfrac{0}{a^2} = 0 \in \mathbb{Z}$. Comme $\dfrac{1}{a} \in \mathbb{Z}$, alors $a = \pm 1$.

Troisième cas : $a \neq 0$ et $b \neq 0$. On sait que $a^2 > 0$ et que $b^2 > 0$, ce qui implique $a^2 + b^2 > 0$. Or, $|a| = \sqrt{a^2} < \sqrt{a^2 + b^2} < a^2 + b^2 \Rightarrow \dfrac{|a|}{a^2 + b^2} < 1$.

De plus, $|-b| = |b| = \sqrt{b^2} < \sqrt{a^2 + b^2} < a^2 + b^2 \Rightarrow \dfrac{|-b|}{a^2 + b^2} < 1$. Par la définition de la valeur absolue,

$$-1 < \frac{a}{a^2 + b^2} < 1;$$
$$-1 < \frac{-b}{a^2 + b^2} < 1.$$

Comme $a \neq 0$ et $b \neq 0$, on a $\dfrac{a}{a^2+b^2} \neq 0$ et $\dfrac{-b}{a^2+b^2} \neq 0$. Donc, $\dfrac{a}{a^2+b^2} \notin \mathbb{Z}$ et $\dfrac{-b}{a^2+b^2} \notin \mathbb{Z}$ lorsque $a \neq 0$ et $b \neq 0$.

Finalement, selon les trois cas présentés, $\dfrac{a}{a^2+b^2} \in \mathbb{Z}$ et $\dfrac{-b}{a^2+b^2} \in \mathbb{Z}$ impliquent que soit $a = \pm 1$ et $b = 0$ ou soit $b = \pm 1$ et $a = 0$. Donc, les nombres de Gauss inversibles sont 1, -1, i et $-i$. Par la proposition 2.9, les unités sont les seuls nombres de Gauss inversibles. ■

Proposition 2.19. *Si $w|z$ et $z|w$, alors z et w sont des associés.*

Démonstration. Puisque $w|z$ et $z|w$, alors il existe $m, n \in \mathbb{G}$ tel que $z = wm$ et $w = zn$, où $z, w \neq 0$. En combinant ces deux dernières égalités, on obtient $z = wm = (zn)m = z(mn)$. En simplifiant, on obtient $mn = 1$, car $z \neq 0$. Clairement, $m, n \neq 0$. Puisque $mn = 1$, alors n est l'inverse de m, d'où $n = \dfrac{1}{m}$. Par la proposition 2.18, $m \in \{1, -1, i, -i\}$. Comme $z = wm$, où m est une unité, on a que z et w sont associés. ■

Proposition 2.20. *Si $z, w \in \mathbb{Z}$ et $w|z$ dans $\mathbb{G}$, alors $w|z$ dans $\mathbb{Z}$.*

Démonstration. Puisque $w|z$ dans $\mathbb{G}$, où $w \neq 0$, alors il existe $n \in \mathbb{G}$ tel que $z = wn$. On pose $n = a + bi$, où $a, b \in \mathbb{Z}$. Ainsi, $z = wn = w(a + bi) = wa + wbi$. On sait que $z = z + 0i$, car $z \in \mathbb{Z}$. Ainsi, $z = z + 0i = wa + wbi$. On obtient $z = wa$ et $0i = wbi \Rightarrow 0 = wb$. Cette dernière égalité implique que $w = 0$ ou $b = 0$. Par hypothèse, $w \neq 0$. Alors $b = 0$. En substituant b dans n, on obtient l'expression $n = a + bi = a + 0i = a$. Donc $n = a \in \mathbb{Z}$. Ainsi $z, w, n \in \mathbb{Z}$ et $z = wa = wn$. Par conséquent, $w|z$ dans $\mathbb{Z}$. ■

Proposition 2.21. *Soit $z, w \in \mathbb{G}$, où $z, w \neq 0$. Si $w|z$ et w n'est pas une unité ni un associé de z, alors $1 < |w|^2 < |z|^2$.*

Démonstration. Comme $w|z$, alors il existe $n \in \mathbb{G}$ tel que $z = wn$, où $w \neq 0$. Puisque $w \neq 0$, alors $|w|^2 \neq 0$. Comme w n'est pas une unité, alors $|w|^2 \neq 1$ et puisque $w \in \mathbb{G}$, on a

$$|w|^2 > 1 \Rightarrow |w|^2 \geq 2. \tag{2.1}$$

Par hypothèse, on sait que $z \neq 0$, donc $|z|^2 \neq 0$. Par la proposition 2.15, on sait que $|z|^2 = |wn|^2 = |w|^2 \cdot |n|^2$. Les facteurs sont des nombres entiers et comme $|z|^2 \neq 0$ et $|w|^2 \neq 0$, ceci implique $|n|^2 \neq 0$. Puisque z et w ne sont pas associés, alors n n'est pas une unité, d'où $|n|^2 \neq 1$. Donc $|n|^2 \geq 2$ et on a

$$|w|^2 \cdot |n|^2 = |z|^2 \Rightarrow |w|^2 = \frac{|z|^2}{|n|^2} \leq \frac{|z|^2}{2} < |z|^2 \Rightarrow |w|^2 < |z|^2. \tag{2.2}$$

Par conséquent, en combinant les équations (2.1) et (2.2), on obtient

$$1 < |w|^2 < |z|^2.$$

■

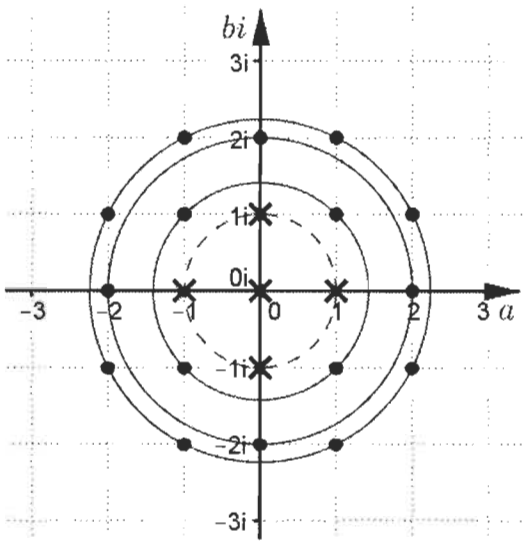


FIGURE 2.22 – Entiers de Gauss ayant une norme supérieure à 1.

Les entiers de Gauss ayant une norme supérieure à 1 ont une norme minimale à 2. Dans l'ordre croissant, le cercle pointillé détermine une norme de 1 unité, tandis que les autres sont de 2, 4 et 5 unités.

2.3 PGCD : Plus grand commun diviseur

À cette étape, introduisons la notion de *plus grand commun diviseur* dans $\mathbb{G}$.

Définition 2.23. *Soit $z, w \in \mathbb{G}$, où $zw \neq 0$. Le **plus grand commun diviseur** de z et de w, noté* $\text{pgcd}(z, w)$, est le nombre $d \in \mathbb{G}$ respectant les deux conditions suivantes :

- $d|z$ et $d|w$;
- $\forall c \in \mathbb{G}$ qui divise z et w, on a $c|d$.

Avant de montrer des résultats sur le pgcd, il convient de s'approprier un algorithme très utile apparu d'abord dans les entiers : l'algorithme d'Euclide. Cet algorithme vise à trouver le pgcd de deux nombres quelconques par opérations successives sur les deux nombres de départ. Le théorème de la division euclidienne dans les réels est possible à cause de la relation d'ordre existante dans ce corps. Toutefois, dans les complexes, il faut ajuster l'énoncé du théorème pour se ramener à des valeurs réelles ou entières. Ainsi, le théorème d'Euclide peut s'écrire de la façon suivante pour les entiers de Gauss.

Théorème 2.24 (Théorème d'Euclide). *Si $z, w \in \mathbb{G}$ et $w \neq 0$, alors il existe des entiers de Gauss q et r tels que $z = qw + r$ et $|r|^2 < |w|^2$. De plus, si $w \nmid z$, alors $0 < |r|^2 < |w|^2$. La quantité r est appelée le* ***résidu.***

Démonstration. Étant donné que la division de deux entiers de Gauss n'est pas toujours fermée dans $\mathbb{G}$, prenons la division de z et de w dans $\mathbb{C}$. Supposons que $\dfrac{z}{w} = u + vi$. Prenons m et n les arrondis de u et v aux entiers les plus près et tels que $u + vi = (m + s) + (n + t)i$, où $|s| \leq \dfrac{1}{2}$ et $|t| \leq \dfrac{1}{2}$.

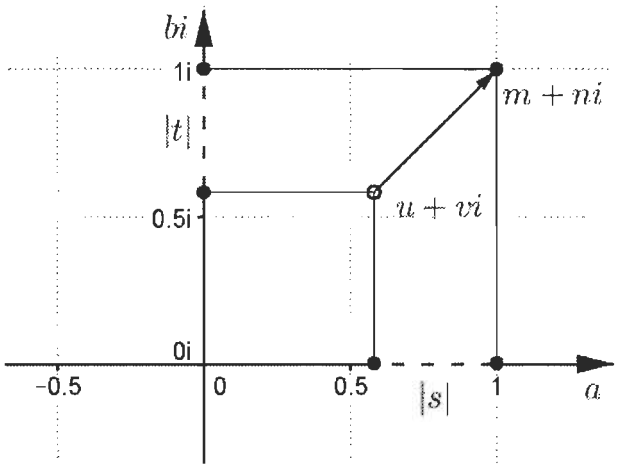


FIGURE 2.25 – Arrondissement du quotient $u + vi$ à l'entier de Gauss le plus près.

Si on pose $q = m + ni$, alors on a $r = z - qw = \left(\dfrac{z}{w} - q\right) w$. En utilisant la proposition 2.15, il s'en suit que

$$\begin{aligned} |r|^2 &= \left|\left(\frac{z}{w} - q\right) w\right|^2 = \left|\left(\frac{z}{w} - q\right)\right|^2 \cdot |w|^2 = |(u + vi) - (m + ni)|^2 \cdot |w|^2 = |s + ti|^2 \cdot |w|^2 \\ &\leq \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) \cdot |w|^2 = \frac{|w|^2}{2} \\ &< |w|^2. \end{aligned}$$

Pour la deuxième partie de la démonstration, nous procédons par contraposition. Notons $r = a + bi$. Supposons que $|r|^2 = 0$, alors $|r|^2 = a^2 + b^2 = 0$, avec $a, b \in \mathbb{Z}$. Étant donné que cette égalité est dans les entiers, alors $a = b = 0$. Ainsi $r = 0$ et $z = qw + r = qw \Rightarrow w|z$. ■

Exemple 2.26. Trouvons q et r en divisant $123 - 5i$ par $-2 + 9i$. On a

$$\begin{aligned} \frac{123 - 5i}{-2 + 9i} &= \frac{-291}{85} + \frac{-1097}{85} i \approx -3.42 - 12.91i \\ \Rightarrow \underbrace{123 - 5i}_{z} &= \underbrace{(-3 - 13i)}_{q}\underbrace{(-2 + 9i)}_{w} + \underbrace{(0 - 4i)}_{r}. \end{aligned}$$

On remarque que $|r|^2 = 16 < 85 = |w|^2$, ce qui est en accord avec le théorème d'Euclide. Par contre, le théorème affirme qu'il *existe* q et r. Ils ne sont pas uniques ! En effet, il est possible de choisir $q = -4 - 13i$ pour obtenir $r = -2 + 5i$.

$$\begin{aligned} qw + r &= (-4 - 13i)(-2 + 9i) + (-2 + 5i) \\ &= 8 - 36i + 26i - 117i^2 - 2 + 5i \\ &= 8 + 117 - 2 - 36i + 26i + 5i \\ &= 123 - 5i = z. \end{aligned}$$

On constate aussi que $|r|^2 = 29 < 85 = |w|^2$.

Lemme 2.27. *Soit $x, y, z \in \mathbb{G}$. Si $x|y$ et $x|z$, alors $x|(ys + zt)$, $\forall s, t \in \mathbb{G}$.*

Démonstration. Puisque $x|y$ et $x|z$, il existe $m, n \in \mathbb{G}$ tels que $y = xm$ et $z = xn$. Or,

$$ys + zt = xms + xnt = x(ms + nt),$$

$\forall s, t \in \mathbb{G}$. Par la fermeture des entiers de Gauss, on sait que $ms+nt \in \mathbb{G}$. D'où $x|(ys+zt)$. ■

Lemme 2.28. *Soit $d, m, w, z \in \mathbb{G}$ et une unité I. Si $d = \text{pgcd}(w, z)$, alors* $\text{pgcd}(w, z) = I \cdot \text{pgcd}(w, z + mw)$.

Démonstration. Soit $g = \text{pgcd}(w, z + mw)$. Comme $d|w$ et $d|z$, par le lemme 2.27, alors $d|(z + mw)$. D'où $d|g$. De la même façon, $g|w$ et $g|(z + mw)$ impliquent $g|z$, d'où $g|d$. Par la proposition 2.19, d et g sont des associés. ■

L'algorithme d'Euclide dans $\mathbb{G}$ consiste à appliquer le théorème d'Euclide successivement [18] pour construire une suite de résidus convergeant vers 0. Soit $z, w \in \mathbb{G}$, où $w \neq 0$. Soit $q_i, r_i \in \mathbb{G}$, $\forall i \in \{1, 2, 3, ...n\}$, où q_i et r_i sont obtenus à chaque itération par l'application du théorème d'Euclide. À l'étape $i = 1$, on a

$$\begin{aligned} z &= q_1 w + (z - q_1 w) \\ &= q_1 w + r_1, \text{ où } |r_1|^2 < |w|^2. \end{aligned}$$

Après l'application du théorème d'Euclide avec w et r_1, on obtient :

$$\begin{aligned} w &= q_2(z - q_1 w) + (w - q_2(z - q_1 w)) \\ &= q_2 r_1 + r_2, \text{ où } |r_2|^2 < |r_1|^2. \end{aligned}$$

Puis avec r_1 et r_2 :

$$\begin{aligned} r_1 &= z - q_1 w \\ &= q_3(w - q_2(z - q_1 w)) + ((z - q_1 w) - q_3(w - q_2(z - q_1 w))) \\ &= q_3 r_2 + r_3, \text{ où } |r_3|^2 < |r_2|^2, \end{aligned}$$

et ainsi de suite. À l'avant-dernière et dernière étapes, on retrouve

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \text{ où } |r_{n-1}|^2 < |r_{n-2}|^2, \text{ et} \\ r_{n-2} &= q_n r_{n-1}. \end{aligned}$$

Il faut noter que $r_{n-2} = q_n r_{n-1} + r_n$. Mais $r_n = 0$ puisque c'est la dernière étape de l'algorithme. On constate que les résidus vérifient la relation suivante :

$$0 = |r_n|^2 < |r_{n-1}|^2 < |r_{n-2}|^2 < \ldots < |r_2|^2 < |r_1|^2.$$

En fait, comme la norme au carré est un nombre positif et que la suite des résidus est strictement décroissante, on obtient un résidu valant 0 après un nombre fini d'itérations.

De plus, $r_{n-1} = \text{pgcd}(r_{n-1}, r_{n-2})$. On peut trouver une combinaison linéaire pour exprimer r_{n-1} en fonction de z et de w. Réécrivons l'algorithme à l'envers et isolons le pgcd. Les étapes de l'algorithme sont

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \\ r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2}, \\ r_{n-5} &= q_{n-3} r_{n-4} + r_{n-3}, \\ \vdots &= \quad \vdots \\ w &= q_2 r_1 + r_2, \\ z &= q_1 w + r_1. \end{aligned}$$

Ainsi,

$$\begin{aligned}
r_{n-1} &= r_{n-3} - q_{n-1}r_{n-2};\\
r_{n-1} &= r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2}r_{n-3}) = r_{n-3}(1 + q_{n-1}q_{n-2}) + r_{n-4}(-q_{n-1});\\
r_{n-1} &= (r_{n-5} - q_{n-3}r_{n-4})(1 + q_{n-1}q_{n-2}) + r_{n-4}(-q_{n-1});\\
&= r_{n-5}(1 + q_{n-1}q_{n-2}) + r_{n-4}(-q_{n-3} - q_{n-1}q_{n-2}q_{n-3} - q_{n-1})\\
\vdots &= \quad \vdots\\
r_{n-1} &= Aw + Br_1;\\
r_{n-1} &= Aw + B(z - q_1w)\\
&= w(A - q_1B) + z(B).
\end{aligned}$$

Nous sommes désormais en mesure de démontrer le théorème suivant.

Théorème 2.29. *Chaque paire (z, w) d'entiers de Gauss, différents de 0, a un pgcd qui est unique aux associés près.*

Démonstration. Soit $I_j \in \{1, -1, i, -i\}$, où $j \in \{1, 2, ..., n-1\}$. En utilisant le lemme 2.28 successivement et en utilisant les notations de l'algorithme d'Euclide, on a

$$\begin{aligned}
\text{pgcd}(z, w) &= I_1\text{pgcd}(w, r_1),\\
&= I_1I_2\text{pgcd}(r_1, r_2),\\
&= ...\\
&= I_1I_2 \cdots I_{n-2}\text{pgcd}(r_{n-3}, r_{n-2}),\\
&= I_1I_2 \cdots I_{n-2}I_{n-1}\text{pgcd}(r_{n-2}, r_{n-1}).
\end{aligned}$$

Par la fermeture des unités (voir la table de Cayley 2.8), posons $I = I_1I_2 \cdots I_{n-1}$, d'où $\text{pgcd}(w, z) = I\text{pgcd}(r_{n-2}, r_{n-1}) = Ir_{n-1}$. Selon la définition 2.23, on conclut que r_{n-1} est un pgcd de z et de w.

L'unicité découle de la définition du pgcd. En effet, soit $d_1 \neq d_2$ deux $\text{pgcd}(z, w)$. Comme $d_1|z$, $d_1|w$ et d_2 est un $\text{pgcd}(z, w)$, alors $d_1|d_2$. Similairement, comme $d_2|z$, $d_2|w$ et d_1 est un $\text{pgcd}(z, w)$, alors $d_2|d_1$. Par la proposition 2.19, on a que d_1 et d_2 sont associés. ■

Le dernier résidu non nul de l'algorithme est le $\text{pgcd}\,(z, w)$. Voici un exemple pour illustrer l'algorithme.

Exemple 2.30. Trouvons le $\text{pgcd}(27+i, 73)$. Le nombre ayant la plus petite norme divisera celui qui a la plus grande norme. Ainsi, $|73|^2 = 5329$ et $|27+i|^2 = 730$. Le quotient vaut $\frac{73}{27+i} = 2.7 - 0.1i$ et on arrondit à $3 + 0i = 3$. On applique l'algorithme d'Euclide sur ces deux nombres :

$$73 = 3(27+i) + (-8-3i);$$
$$27+i = (-3+i)(-8-3i).$$

Puisque le résidu est nul, le $\text{pgcd}(27+i, 73) = -8-3i$.

Corollaire 2.31. *Si $d = \text{pgcd}(z, w)$, alors il existe x_0 et $y_0 \in \mathbb{G}$ tels que $d = zx_0 + wy_0$.*

Démonstration. La preuve découle essentiellement du calcul de la combinaison linéaire du pgcd détaillé lors de la présentation de l'algorithme d'Euclide. ■

Théorème 2.32. *Soit $z, w \in \mathbb{G}$ tels que $zw \neq 0$. Si I est une unité, alors*

$$\text{pgcd}(z, w) = I \iff \text{il existe } x, y \in \mathbb{G} \text{ tels que } zx + wy = I.$$

Démonstration.

$\Longrightarrow$) Si $\text{pgcd}(z, w) = I$, d'après le corollaire 2.31, il existe $x, y \in \mathbb{G}$ tels que $zx + wy = \text{pgcd}(z, w) = I$.

$\Longleftarrow$) On sait que $I|z$ et $I|w$. De plus, on a que $\text{pgcd}(z, w)|z$ et $\text{pgcd}(z, w)|w$. D'après le lemme 2.27, il existe $x, y \in \mathbb{Z}$ tels que $\text{pgcd}(z, w)|(zx + wy)$, et par hypothèse, ceci implique $\text{pgcd}(z, w)|I$. Par la définition 2.23, on a que $\text{pgcd}(z, w) = I$ est un pgcd de z et w. ■

Lemme 2.33. *Soit I une unité. Il existe une autre unité I_1 telle que $II_1 = 1$.*

Démonstration. Le résultat découle directement de la proposition 2.9. ■

Théorème 2.34. *Si $y|zw$ dans $\mathbb{G}$ et si* $\text{pgcd}(z, y) = I$, alors $y|w$.

Démonstration. Par la définition 2.23, on a $zy \neq 0$, car le $\text{pgcd}(z, y)$ existe. D'après le théorème 2.32, il existe $s, t \in \mathbb{G}$ tels que $I = zs + yt$. En multipliant par w, on a $Iw = zsw + ytw$. Il est évident que $y|yw$ et $y|zw$ par hypothèse. Par le lemme 2.27, y divise toute combinaison linéaire de yw et zw. En particulier, $y|(zsw + ytw) \Rightarrow y|Iw$. Ainsi, il existe $n \in \mathbb{G}$ tel que $Iw = yn$. Par le lemme 2.33, il existe une unité I_1 telle que $II_1 = 1$. Alors, $w = IwI_1 = ynI_1 = ym$, où $m = nI_1 \in \mathbb{G}$. On a donc $y|w$. ■

2.4 Premiers de Gauss

Définition 2.35. *Soit $z \in \mathbb{G}$ un entier différent de 0 et des unités. Alors z est* ***premier*** *s'il n'existe aucun produit de la forme $z = xy$, $\forall x, y \in \mathbb{G}\backslash\{1, -1, i, -i\}$. Si z n'est pas premier, alors on dit qu'il est* ***composé***.

Il est possible d'interpréter la définition 2.35 selon le concept des diviseurs. N'importe quel entier de Gauss est divisible par une unité ou un associé. Par contre, $z \neq 0$ sera premier si *les seuls diviseurs* de z sont les unités ou ses associés. Car s'il existe un produit de la forme $z = xy$ où, sans perte de généralité, $x \in \{1, -1, i, -i\}$, alors y est un associé de z.

Exemple 2.36. Les nombres 2 et 5 ne sont pas premiers dans $\mathbb{G}$, car $2 = (1+i)(1-i)$ et $5 = (2+i)(2-i)$. Ils ne sont pas uniquement le produit d'un entier de Gauss et d'une unité.

Exemple 2.37. Le nombre 3 est un nombre premier dans $\mathbb{G}$. Supposons que 3 n'est pas premier dans $\mathbb{G}$, alors il existe $w = a + bi \in \mathbb{G}$ tel que $w|3$. Selon la proposition 2.17, $|w|^2 \mid 9$. Les seuls diviseurs de 9 sont 1, 3 et 9. Si $|w|^2 = 1$, alors w est une unité, ou si $|w|^2 = 9$, alors w est un associé de 3, ce que l'on ne veut pas, car 3 est composé. Il faut donc que $|w|^2 = a^2 + b^2 = 3$. Si $a = 0$, alors $b^2 = 3$, mais 3 est premier dans $\mathbb{Z}$ et il n'existe aucun b. Si $a = \pm 1$, alors $b^2 = 2$, mais 2 est premier dans $\mathbb{Z}$, ainsi il n'existe aucun b. Lorsque $a \geq 2$ ou $a \leq -2$, $b^2 = 3 - a^2 < 0$. Alors il n'existe aucune combinaison de a et de b qui donne $a^2 + b^2 = 3$. Donc, pour que $w|3$ dans $\mathbb{G}$, w doit être une unité ou un associé de 3, c'est-à-dire que 3 est premier dans $\mathbb{G}$.

Définition 2.38. *Deux entiers de Gauss sont* ***relativement premiers*** *entre eux si leur* pgcd est une unité.

En effet, dans un tel cas, deux entiers ne sont pas associés et n'ont aucun facteur commun et les seuls nombres pouvant les diviser en même temps sont les unités. Il faut se rappeler que les unités divisent tout entier de Gauss.

Théorème 2.39. *Soit $w, z \in \mathbb{G}$. Si $p \in \mathbb{G}$ est premier et $p|wz$, alors $p|w$ ou $p|z$.*

Démonstration. Si $p|w$ ou $p|z$, la preuve est terminée. Sans perte de généralité, supposons que $p \nmid w$. Comme p est premier, ses seuls diviseurs sont ses associés et les unités. Or, aucun associé de p ne divisera w, ce qui ne laisse que les unités. Donc p et w sont relativement premiers et de la définition 2.38 on a que $\text{pgcd}(p, w) = I$. Du théorème 2.34, on a $p|z$. ■

Corollaire 2.40. *Si $p \in \mathbb{G}$ est premier et si $p|z_1 z_2 \cdots z_r$, alors il existe un entier $k \in \{1, 2, ..., r\}$ tel que $p|z_k$.*

Démonstration. Démontrons ce corollaire par induction sur r.

- Cas $r = 1$. On a $p|z_1$, d'où $k = 1$.
- Cas $r > 1$. Supposons le corollaire vérifié jusqu'à $r - 1$. Démontrons qu'il est vrai pour r. De l'hypothèse d'induction, si $p|z_1 z_2 \cdots z_{r-1}$, alors il existe $k_1 \in \{1, 2, ..., r-1\}$ tel que $p|z_{k_1}$. Par hypothèse, on a $p|z_1 z_2 \cdots z_{r-1} z_r$. Par le théorème 2.39, $p|z_1 z_2 \cdots z_{r-1}$ ou $p|z_r$. Si $p|z_1 z_2 \cdots z_{r-1}$, on a $p|z_{k_1}$. Par contre, si $p \nmid z_1 z_2 \cdots z_{r-1}$, alors $p|z_r$, d'où $k = r$.

Par le principe d'induction mathématique, on conclut que le résultat est vrai pour tout $r \in \mathbb{N}$. ■

Corollaire 2.41. *Si $p, z_1, z_2, ..., z_r \in \mathbb{G}$ sont des nombres premiers et si $p|z_1 z_2 \cdots z_r$, alors $pI = z_k$ pour un certain $k \in \{1, 2, ..., r\}$, où I est une unité.*

Démonstration. Procédons par induction sur r.

- Cas $r = 1$. Comme $p|z_1$, il existe $n \in \mathbb{G}$ tel que $pn = z_1$. Comme p est premier, il n'est pas une unité. En raisonnant par l'absurde à l'aide de la définition 2.35, on a que $n \notin \mathbb{G}\backslash\{1, -1, i-, i\}$. D'où $n = I \Rightarrow pI = z_1$, donc $k = 1$.
- Cas $r > 1$. Supposons le corollaire vérifié jusqu'à $r - 1$. De l'hypothèse d'induction, si $p|z_1 z_2 \cdots z_{n-1}$, alors il existe $k_1 \in \{1, 2, ..., n-1\}$ tel que $pI = z_{k_1}$. Comme $p|z_1 z_2 \cdots z_{r-1} z_r$, on utilise le théorème 2.39, d'où $p|z_1 z_2 \cdots z_{r-1}$ ou $p|z_r$. Si $p|z_1 z_2 \cdots z_{r-1}$, on a $pI = z_{k_1}$. Si $p \nmid z_1 z_2 \cdots z_{r-1}$, alors $p|z_r$. Avec l'argumentation du premier cas, on a que $pI = z_r$, d'où $k = r$.

Par le principe d'induction mathématique, on conclut que le résultat est vrai pour tout $r \in \mathbb{N}$. ■

Maintenant, il convient de démontrer un théorème dans $\mathbb{G}$ basé sur un résultat homologue dans $\mathbb{R}$ [1].

Théorème 2.42 (Théorème fondamental de l'arithmétique complexe)**.** *Tout nombre dans $\mathbb{G}$ différent de 0 et des unités peut s'écrire comme un produit de nombres premiers de Gauss et cette représentation est unique, à l'exception des associés et de l'ordre de présentation des facteurs.*

Démonstration. Soit $z \in \mathbb{G}$ différent de 0 et d'une unité. Posons $w_i \in \mathbb{G}\backslash\{1, -1, i, -i\}$, pour $i \in \{1, 2, ..., n\}$. Si z est premier, la preuve est terminée. Supposons que z est composé. Par la définition 2.35, il existe w_1 et w_2 tels que $z = w_1 w_2$. Comme w_1 et w_2 ne sont pas des unités, ils ne sont pas des associés de z. La proposition 2.21 nous donne $|w_1|^2 < |z|^2$ et $|w_2|^2 < |z|^2$. Si w_1 et w_2 sont premiers, on a terminé. Si au moins un des deux est composé, on le décompose en un produit de facteurs w_i. Prenons le cas où w_1 est composé. On pose $w_1 = w_3 w_4$ et on regarde la primalité de w_3 et w_4. Et ainsi de suite. La proposition 2.21 nous assure que chaque w_i subséquent vérifiera un emboitement de la forme $0 < |w_n|^2 < ... < |w_3|^2 < |w_1|^2 < |z|^2$. On note que tous les $w_i \neq 0$, car s'il existe un certain $w_k = 0$, où $k \in \{1, 2, 3, ...n\}$, on aurait $z = 0$, une contradiction avec l'hypothèse. Comme les normes sont des nombres entiers, le processus a un nombre fini d'itérations. On obtient z sous la forme d'un produit de nombres premiers de Gauss, soit $z = p_1 p_2 p_3 \cdots p_r$.

Supposons que cette représentation n'est pas unique, c'est-à-dire que $z = p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$ tel que les p_i et les q_j sont des nombres premiers et pas forcément distincts. On simplifie l'équation

$$p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$$

en éliminant tous les nombres premiers identiques qui sont dans les deux membres. De plus, si un p_i est l'associé d'un q_j, on les simplifie en conservant l'unité de l'associé. La simplification donne :

$$p_{i_1} p_{i_2} p_{i_3} \cdots p_{i_\alpha} = I q_{j_1} q_{j_2} q_{j_3} \cdots q_{j_\beta},$$

qui ne contient aucun doublon ni associé, où $\alpha \leq r$, $\beta \leq s$ et où I est la multiplication de toutes les unités restantes dû à la simplification. Or, par le théorème 2.39, on a $p_{i_1} | q_{j_1} q_{j_2} q_{j_3} \cdots q_{j_\beta}$. Comme p_{i_1}, q_{j_1}, q_{j_2}, q_{j_3}, ... sont tous des nombres premiers, on utilise le corollaire 2.41. Ainsi, il existe $\mu \in \{1, 2, ..., \beta\}$ et une unité I_1 tels que $p_{i_1} I_1 = q_{j_\mu}$. Nous obtenons une contradiction avec le fait qu'il ne doit pas y avoir d'associés. Ainsi, la représentation est unique, aux associés près. ■

Lemme 2.43. *Soit $x \in \mathbb{Z}$. Si x est pair, alors x^2 est pair et $x^2 \equiv 0$ (mod 4). Si x est impair, alors x^2 est impair et $x^2 \equiv 1$ (mod 4).*

Démonstration. Si x est pair, alors $x = 2k_1, k_1 \in \mathbb{Z}$. Donc $x^2 = 4k_1^2 = 2(2k_1^2)$, d'où x^2 est pair. De plus,

$$\begin{aligned} x^2 = 4k_1^2 &\Rightarrow x^2 - 0 = 4(k_1^2) \\ &\Rightarrow x^2 \equiv 0 \pmod 4. \end{aligned}$$

Si x est impair, alors $x = 2k_2 + 1, k_2 \in \mathbb{Z}$. Donc $x^2 = 4k_2^2 + 4k_2 + 1 = 2(2k_2^2 + 2k_2) + 1$, d'où x^2 est impair. De plus,

$$\begin{aligned} x^2 = 4k_2^2 + 4k_2 + 1 &\Rightarrow x^2 = 4(k_2^2 + k_2) + 1 \\ &\Rightarrow x^2 - 1 = 4(k_2^2 + k_2) \\ &\Rightarrow x^2 \equiv 1 \pmod 4. \end{aligned}$$

■

Le prochain théorème est très utile pour trouver les nombres premiers de Gauss. En jumelant les résultats sur la factorisation unique des nombres premiers de Gauss avec les congruences modulo dans les entiers, il est possible de démontrer le théorème suivant [18].

Théorème 2.44. *Un nombre premier $p \in \mathbb{Z}$ est la somme de deux entiers carrés si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$.*

Démonstration.

$\Longrightarrow$) Soit $p = x^2 + y^2$. Si l'on se réfère à la figure 2.22, il est évident que $(x, y) \in \{(1,1), (1,-1), (-1,1), (-1,-1)\}$ si et seulement si $p = 2$. Maintenant, supposons que $p \neq 2$, d'où $x \neq \pm 1$ ou $y \neq \pm 1$. Par le lemme 2.43, on obtient $x^2 + y^2$ est congru à 0, 1 ou 2 modulo 4. Or, comme p est premier et $p \neq 2$, alors p est impair. Étant donné que p est la somme de deux nombres, x et y doivent être de parité inverse. Ainsi, $x^2 + y^2 \equiv 0 + 1 = 1 \pmod 4$. Par conséquent, on a la conclusion recherchée.

$\Longleftarrow$) Si $p = 2$, alors $p = 1^2 + 1^2$, une somme de deux carrés. Supposons que $p \equiv 1 \pmod 4$. Nous utilisons le résultat suivant sur les résidus quadratiques [1] :

Soit $p \in \mathbb{Z}$ un nombre premier. Alors,
$x^2 \equiv -1 \pmod p$ possède des solutions si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$.

Puisque $p \equiv 1 \pmod 4$, alors il existe $k \in \mathbb{Z}$ tel que

$$x^2 \equiv -1 \pmod p \Rightarrow x^2 + 1 = pk.$$

Donc $p|(x^2 + 1)$ dans $\mathbb{Z}$. Or, dans $\mathbb{G}$, ceci voudrait dire que $p|(x + i)(x - i)$. Sans perte de généralité, par le théorème 2.39, supposons que $p|(x + i)$. Alors, il existe $a + bi \in \mathbb{G}$ tel que

$$\begin{aligned} p(a + bi) = x + i &\Rightarrow pa + pbi = x + i \\ &\Rightarrow pb = 1 \\ &\Rightarrow p = \frac{1}{b}. \end{aligned}$$

Puisque $p \in \mathbb{Z}$ est premier et $b \in \mathbb{Z}$, alors la dernière égalité est impossible. Alors p ne divise ni $x + i$ ni $x - i$. Or, l'unicité de la factorisation dans $\mathbb{G}$ et $x^2 + 1 = (x + i)(x - i) = pk$ impliquent que p n'est pas premier dans $\mathbb{G}$. On peut donc écrire $p = zw$, où $z, w \in \mathbb{G}$.

De plus, nous avons que $1 < |z|^2$ et $1 < |w|^2$. En effet, sans perte de généralité, supposons que $|w|^2 \leq 1$. Par la proposition 2.15, on a $|p|^2 = |z|^2 \cdot |w|^2 \leq |z|^2$, ce qui conduit à une contradiction avec la proposition 2.21. On observe que $|p|^2 = p^2 = |z|^2|w|^2$. Puisque p, $|z|^2$ et $|w|^2 \in \mathbb{Z}$ et que p est premier dans $\mathbb{Z}$, on a $|z|^2 = |w|^2 = p$. En posant $z = c + di$, où $c, d \in \mathbb{Z}$, alors $|z|^2 = c^2 + d^2 = p$. On a la conclusion recherchée. ■

En particulier, on tire du théorème précédent que si un nombre premier p dans $\mathbb{Z}$ s'écrit comme la somme de deux carrés, alors il n'est pas un nombre premier dans $\mathbb{G}$. En effet, 2 n'est pas premier dans $\mathbb{G}$ car $2 = (1 + i)(1 - i)$. Pour cela, il suffit de constater que $p = a^2 + b^2 = (a + bi)(a - bi)$.

Le prochain théorème fournit une catégorisation complète des nombres premiers de Gauss.

Théorème 2.45. *Un entier $z \in \mathbb{G}$ est un nombre premier dans $\mathbb{G}$ si et seulement si*

- *z (ou iz) est un entier premier congru à 3 modulo 4*

ou

- *$|z|^2$ est un entier premier.*

Démonstration.

$\Longrightarrow$) Soit z un nombre premier dans $\mathbb{G}$. Si z est un entier, alors z est premier dans $\mathbb{Z}$. Par le théorème 2.44, on a $z \neq 2$ ou $z \not\equiv 1 \pmod 4$. De plus, si $z \equiv 0 \pmod 4$ ou $z \equiv 2 \pmod 4$, alors z est un nombre pair, donc il n'est pas premier. La seule possibilité restante est $z \equiv 3 \pmod 4$. Le même raisonnement s'applique si iz est un entier.

Supposons que z n'est pas un entier ou un associé d'un entier, alors $z\overline{z} = |z|^2 \neq \pm z^2$. Par le théorème fondamental de l'arithmétique 1.14, on sait que $|z|^2 \in \mathbb{Z}$ peut être décomposé en un produit de nombres premiers. Alors, $z \in \mathbb{G}$ doit diviser un de ces nombres premiers, disons p. Comme z est un diviseur propre de p, alors, par la proposition 2.17, $|z|^2 \mid |p|^2 = p^2$. Comme p est un nombre premier, alors $|z|^2 = p$, d'où la conclusion.

$\Longleftarrow$) Supposons que, dans $\mathbb{Z}$, w est premier et que $w \equiv 3 \pmod 4$. Par contradiction, supposons que w n'est pas premier dans $\mathbb{G}$. Alors $w = xy$, où $x, y \in \mathbb{G}$ ne sont pas des unités. Par la proposition 2.15, ceci implique que $w^2 = |w|^2 = |x|^2 \cdot |y|^2$. Comme w est premier dans $\mathbb{Z}$, alors $w = |x|^2 = |y|^2 \neq 1$. Or, $x \in \mathbb{G}$ peut s'écrire $x = a + bi$. Alors $w = |x|^2 = a^2 + b^2$. Ceci contredit l'hypothèse affirmant que $w \equiv 3 \pmod 4$, en conformité avec le théorème 2.44.

Supposons que $|z|^2$ est un entier premier. Par contradiction, supposons que z n'est pas un premier dans $\mathbb{G}$. Ainsi, z peut s'écrire de la forme $z = xy$, où $x, y \in \mathbb{G}$ ne sont pas des unités. Par la proposition 2.21, $x|z$ où $1 < |x|^2 < |z|^2$. Par la proposition 2.15, $|z|^2 = |x|^2 \cdot |y|^2$. Comme $|x|^2 \neq 1$ et $|x|^2 \mid |z|^2$, ceci contredit l'hypothèse affirmant que $|z|^2$ est un entier premier. ■

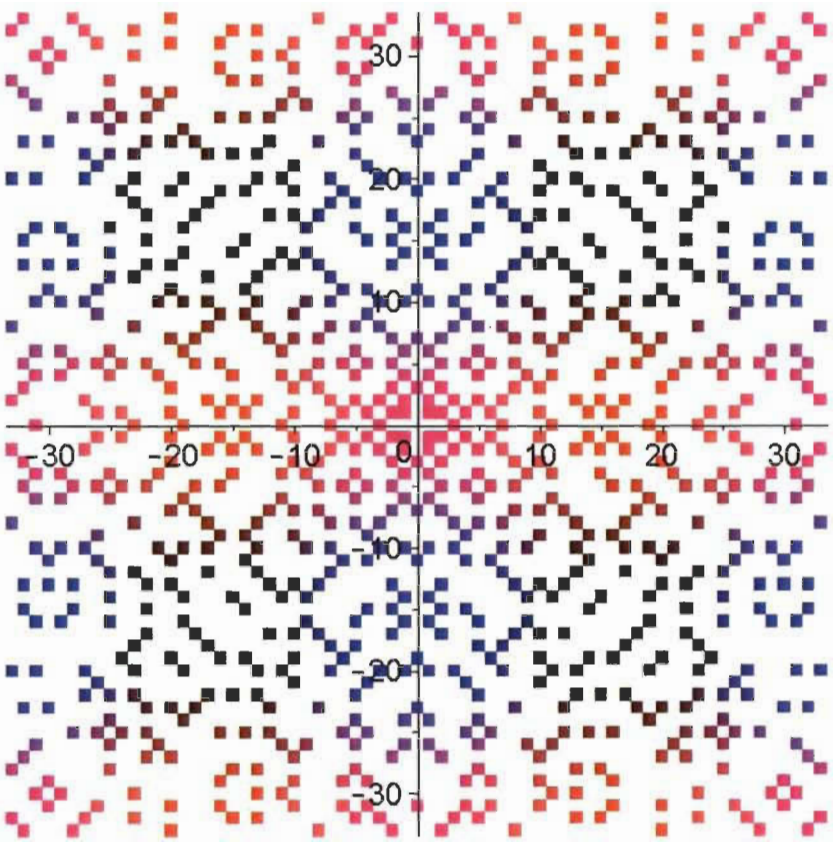


FIGURE 2.46 – Nombres premiers complexes.
Nombres premiers complexes dans le carré centré à l'origine de taille 67×67.

Du théorème précédent, nous sommes désormais en mesure d'afficher les nombres premiers complexes dans le plan. (Voir l'annexe B pour le code Maple).

Chapitre 3

Les nombres hyperboliques

Un nombre hyperbolique est analogue à un nombre complexe. La légère modification, et qui fait toute la différence, est que le carré de l'unité imaginaire vaut 1 au lieu de -1. Ce changement a des répercussions sur plusieurs définitions et propriétés, dont les hyperboliques inversibles et les premiers hyperboliques. La conséquence majeure de cette modification est la possibilité de trouver une base idempotente qui simplifiera les calculs. Les complexes n'ont pas de base équivalente, ce qui rend les hyperboliques plus faciles d'approche considérant les opérations élémentaires.

Débutons tout d'abord par la définition de l'ensemble des nombres hyperboliques. L'unité imaginaire hyperbolique de cet ensemble sera notée par j pour la différencier de i dans les complexes. L'ensemble des nombres hyperboliques est défini par

$$\mathbb{D} = \{x + yj : x, y \in \mathbb{R}, j^2 = 1\}.$$

La partie réelle d'un hyperbolique est notée $\mathrm{Re}(z)$ et la partie imaginaire est $\mathrm{Hy}(z)$. Par exemple, les composantes du nombre $z = -9 - 2\pi j$ sont $\mathrm{Re}(z) = \mathrm{Re}(-9 - 2\pi j) = -9$ et $\mathrm{Hy}(z) = \mathrm{Hy}(-9 - 2\pi j) = -2\pi$.

Définition 3.1. *Soit $z = x + yj$ et $w = u + vj$. On définit les deux opérations binaires :*

$$z + w = (x + u) + (y + v)j;$$
$$z \cdot w = (xu + yv) + (xv + yu)j.$$

Les réels sont un sous-ensemble des complexes obtenu en posant la composante imaginaire égale à 0. Or, les réels sont aussi un sous-ensemble des hyperboliques car

$$\mathbb{R} = \{x + yj : x, y \in \mathbb{R}, y = 0, j^2 = 1\}.$$

Définition 3.3. *Le **conjugué hyperbolique** de $z = x + yj$ est $z^* = x - yj$.*

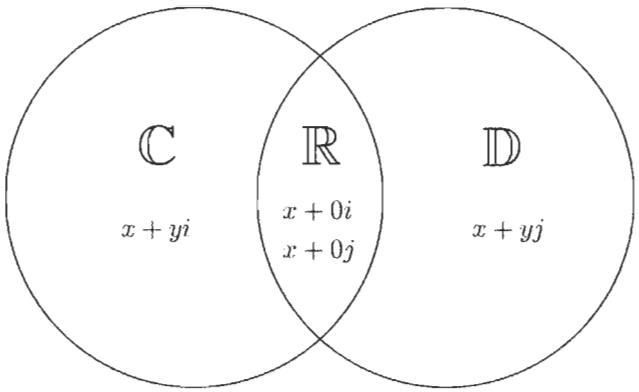


FIGURE 3.2 – Représentation des ensembles réels, complexes et hyperboliques.

Définition 3.4. *Le* ***module hyperbolique*** *d'un nombre* $z = x + yj$ *est* $|z|_h = \sqrt{x^2 - y^2}$.

On constate que $zz^* = (x + yj)(x - yj) = x^2 - y^2$, d'où $|zz^*|_h = \sqrt{x^2 - y^2}$. Il faut bien mettre en évidence que le module n'est pas une norme, car $\sqrt{x^2 - y^2} \not\geq 0, \forall z \in \mathbb{D}$. En effet, pour $x \in (-y, y)$, on a $x^2 - y^2 < 0$. Or la racine d'un nombre négatif n'est pas définie dans les hyperboliques. De plus, $|z|_h = 0 \not\Leftrightarrow z = 0$. Il suffit de choisir $x, y \in \mathbb{R}$ tels que $x = \pm y$ pour obtenir $x^2 = y^2 \Rightarrow \sqrt{x^2 - y^2} = 0$.

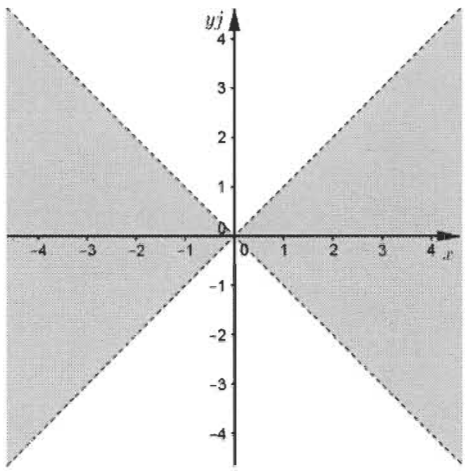


FIGURE 3.5 – Module hyperbolique.

Le module hyperbolique est $|z|_h = \sqrt{x^2 - y^2}$. En gris, $x^2 - y^2 > 0$. En pointillé, $x^2 - y^2 = 0$. En blanc, $x^2 - y^2 < 0$.

Nous savons que les complexes forment un corps. Mais qu'en est-il des hyperboliques ? Essayons de catégoriser cet ensemble en testant les conditions sur les ensembles [15].

Théorème 3.6. *Le triplet* $(\mathbb{D}, +, \cdot)$ *forme un anneau unitaire commutatif.*

Démonstration. Il faut montrer que $(\mathbb{D}, +)$ est un groupe commutatif, que $(\mathbb{D}, \cdot)$ est un semi-groupe commutatif avec unité et que les deux opérations binaires vérifient les propriétés de la distributivité. Soit $z, w, r \in \mathbb{D}$, où $z = x + yj, w = u + vj, r = s + tj$. Considérons $(\mathbb{D}, +)$.

- **Fermeture.** Comme $x + u, y + v \in \mathbb{R}$ par la fermeture de l'addition de $\mathbb{R}$, on a $z + w = (x + u) + (y + v)j \in \mathbb{D}$.

- **Associativité.** On a

$$\begin{aligned}
(z + w) + r &= ((x + yj) + (u + vj)) + (s + tj) \\
&= ((x + u) + (y + v)j) + (s + tj), \text{ par définition de l'addition ;} \\
&= ((x + u) + s) + ((y + v) + t)j, \text{ par définition de l'addition ;} \\
&= (x + (u + s)) + (y + (v + t))j, \text{ par l'associativité de } \mathbb{R} ; \\
&= (x + yj) + ((u + s) + (v + t)j), \text{ par définition de l'addition ;} \\
&= (x + yj) + ((u + vj) + (s + tj)), \text{ par définition de l'addition ;} \\
&= z + (w + r).
\end{aligned}$$

- **Neutre additif.** Le neutre est $0 = 0 + 0j$. En effet,

$$\begin{aligned}
z + 0 &= (x + yj) + (0 + 0j) \\
&= (x + 0) + (y + 0)j, \text{ par définition de l'addition ;} \\
&= x + yj, \text{ par le neutre additif de } \mathbb{R} ; \\
&= z.
\end{aligned}$$

- **Inverse additif.** L'inverse additif de z est $-z = -x + (-y)j$. En effet,

$$\begin{aligned}
z + (-z) &= (x + yj) + (-x + (-y)j) \\
&= (x + (-x)) + (y + (-y))j, \text{ par définition de l'addition ;} \\
&= 0 + 0j, \text{ par les inverses additifs de } \mathbb{R} ; \\
&= 0.
\end{aligned}$$

- **Commutativité.** On a

$$\begin{aligned} z + w &= (x + yj) + (u + vj) \\ &= (x + u) + (y + v)j, \text{ par définition de l'addition ;} \\ &= (u + x) + (v + y)j, \text{ par la commutativité de } \mathbb{R} ; \\ &= (u + vj) + (x + yj), \text{ par définition de l'addition ;} \\ &= w + z. \end{aligned}$$

Donc, $(\mathbb{D}, +)$ est un groupe commutatif. Considérons $(\mathbb{D}, \cdot)$.

- **Fermeture.** Comme $xu + yv, xv + yu \in \mathbb{R}$ par la fermeture de l'addition et de la multiplication de $\mathbb{R}$, alors $z \cdot w = (xu + yv) + (xv + yu)j \in \mathbb{D}$.

- **Associativité.** On a

$$\begin{aligned} (z \cdot w) \cdot r &= ((x + yj) \cdot (u + vj)) \cdot (s + tj) \\ &= ((xu + yv) + (xv + yu)j) \cdot (s + tj), \text{ par définition de la multiplication ;} \\ &= ((xu + yv)s + (xv + yu)t) + ((xu + yv)t + (xv + yu)s)j, \\ &\qquad \text{par définition de la multiplication ;} \\ &= (x(us + vt) + y(ut + vs)) + (x(ut + vs) + y(us + vt))j, \\ &\qquad \text{par distributivité et commutativité de } \mathbb{R} ; \\ &= (x + yj) \cdot ((us + vt) + (ut + vs)j), \text{ par définition de la multiplication ;} \\ &= (x + yj) \cdot ((u + vj) \cdot (s + tj)), \text{ par définition de la multiplication ;} \\ &= z \cdot (w \cdot r). \end{aligned}$$

- **Neutre multiplicatif.** Le neutre multiplicatif est $1 = 1 + 0j$. En effet,

$$\begin{aligned} z \cdot 1 &= (x + yj) \cdot (1 + 0j) \\ &= (x1 + y0) + (x0 + y1)j, \text{ par définition de la multiplication ;} \\ &= (x + 0) + (0 + y)j, \text{ par le neutre multiplicatif et l'élément absorbant de } \mathbb{R} ; \\ &= x + yj, \text{ par le neutre additif de } \mathbb{R} ; \\ &= z. \end{aligned}$$

- **Commutativité.** On a

$$\begin{aligned} z \cdot w &= (x + yj) \cdot (u + vj) \\ &= (xu + yv) + (xv + yu)j, \text{ par définition de la multiplication ;} \\ &= (ux + vy) + (uy + vx)j, \text{ par commutativité de } \mathbb{R} ; \\ &= (u + vj) \cdot (x + yj), \text{ par définition de la multiplication ;} \\ &= w \cdot z. \end{aligned}$$

Donc $(\mathbb{D}, \cdot)$ est bien un semi-groupe commutatif avec unité. Démontrons les deux propriétés de distributivité.

- **Distributivité à droite.** On a

$$\begin{aligned} z \cdot (w + r) &= (x + yj) \cdot ((u + vj) + (s + tj)) \\ &= (x + yj) \cdot ((u + s) + (v + t)j), \text{ par définition de l'addition ;} \\ &= (x(u + s) + y(v + t)) + (x(v + t) + y(u + s))j, \\ &\qquad \text{par définition de la multiplication ;} \\ &= ((xu + yv) + (xs + yt)) + ((xv + yu) + (xt + ys))j, \\ &\qquad \text{par distributivité et commutativité de } \mathbb{R} ; \\ &= ((xu + yv) + (xv + yu)j) + ((xs + yt) + (xt + ys))j, \\ &\qquad \text{par définition de l'addition ;} \\ &= ((x + yj) \cdot (u + vj)) + ((x + yj) \cdot (s + tj)), \\ &\qquad \text{par définition de la multiplication ;} \\ &= (z \cdot w) + (z \cdot r). \end{aligned}$$

- **Distributivité à gauche.** Il est facile de montrer que $(z + w) \cdot r = (z \cdot r) + (w \cdot r)$ d'une façon similaire à la distributivité à droite.

Ainsi, les deux propriétés sont respectées. Par conséquent, le triplet $(\mathbb{D}, +, \cdot)$ forme un anneau unitaire commutatif. ■

Dans la démonstration précédente, il est écrit que l'inverse additif est $-z = -x + (-y)j$. Par abus de notation, écrivons simplement que $-z = -x - yj$, ce qui conduit à l'opération de soustraction

$$z - w = (x + yj) - (u + vj) = (x - u) + (y - v)j.$$

Aussi, on simplifie la notation de la multiplication en écrivant $z \cdot w = zw$, ce qui est plus naturel. La paire $(\mathbb{D}, \cdot)$ est en fait un monoïde commutatif. De plus, comme les deux composantes d'un nombre hyperbolique sont réelles, il est normal que la fermeture vienne des réels. Plus encore, la majorité des propriétés démontrées dans le théorème précédent sont vraies par la commutativité et la distributivité des réels.

Dans le monoïde $(\mathbb{D}, \cdot)$, les inverses n'ont pas été abordés, car il fallait uniquement démontrer que $(\mathbb{D}, +, \cdot)$ était un anneau. Tentons de calculer l'inverse hyperbolique pour tout $z \in \mathbb{D}$. Soit $z, w \in \mathbb{D}$, où $z = x + yj$ et $w = u + vj$. Le neutre multiplicatif est 1. L'inverse de z est w si et seulement si $zw = 1$. Dans ce cas,

$$\begin{aligned} zw &= (x + yj)(u + vj) \\ &= (xu + yv) + (xv + yu)j \\ &= 1 + 0j \\ \Rightarrow\ & xu + yv = 1 \\ & xv + yu = 0. \end{aligned}$$

Sous forme matricielle, nous cherchons u et v tels que

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

La solution par la méthode de Cramer est

$$u = \frac{\begin{vmatrix} 1 & y \\ 0 & x \end{vmatrix}}{\begin{vmatrix} x & y \\ y & x \end{vmatrix}} = \frac{x}{x^2 - y^2} \qquad \text{et} \qquad v = \frac{\begin{vmatrix} x & 1 \\ y & 0 \end{vmatrix}}{\begin{vmatrix} x & y \\ y & x \end{vmatrix}} = \frac{-y}{x^2 - y^2}\ .$$

Or,

$$\begin{aligned} x^2 - y^2 \neq 0 &\Leftrightarrow x^2 \neq y^2 \\ &\Leftrightarrow x \neq \pm y. \end{aligned}$$

Si $x = \pm y$, alors z n'a pas d'inverse. Donc la paire $(\mathbb{D}, \cdot)$ ne forme pas un groupe. Ainsi, chaque élément sauf le neutre additif 0 n'a pas forcément un inverse (voir la figure 3.7). Donc $(\mathbb{D}, +, \cdot)$ ne forme pas un groupe.

À l'aide d'une construction similaire utilisée pour l'ensemble des complexes, les hyperboliques peuvent aussi s'écrire sous la forme matricielle. On a déjà obtenu cette matrice via l'équation matricielle résolue ci-dessus par la méthode de Cramer. Soit l'ensemble de matrices suivant :

$$A_2(\mathbb{R}) = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix} \;\middle|\; x, y \in \mathbb{R} \right\}.$$

Un nombre $z = x + yj$ pourra s'écrire aussi sous la forme matricielle

$$f(z) = \begin{pmatrix} x & y \\ y & x \end{pmatrix}$$

où $f : \mathbb{D} \longrightarrow A_2(\mathbb{R})$ est un isomorphisme.

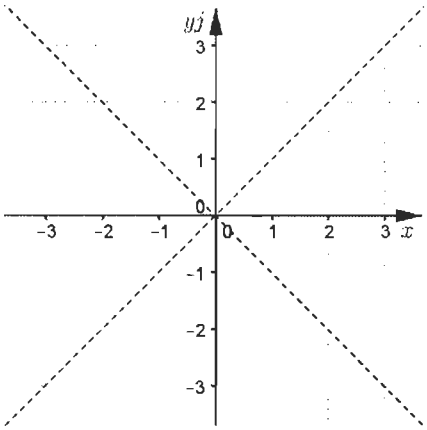


FIGURE 3.7 – Hyperboliques non inversibles.
Les non inversibles sont sur les droites $y = x$ et $y = -x$.

Théorème 3.8. *Soit les deux anneaux* $(\mathbb{D}, +, \cdot)$ *et* $(A_2(\mathbb{R}), *, \times)$. *L'application* f *définie par*

$$f : (\mathbb{D}, +, \cdot) \longrightarrow (A_2(\mathbb{R}), *, \times)$$
$$z = x + yj \longmapsto \begin{pmatrix} x & y \\ y & x \end{pmatrix}$$

est un isomorphisme.

Note : Le triplet $(A_2(\mathbb{R}), *, \times)$ *est un anneau. (Voir l'annexe A pour la démonstration.)*

Démonstration. Pour démontrer que f est un isomorphisme, il faut démontrer que f est un homomorphisme bijectif. Soit $z, w \in \mathbb{D}$, où $z = x + yj$ et $w = u + vj$. Démontrons que f est un homomorphisme.

- On montre que $f(z + w) = f(z) * f(w)$. En effet,

$$\begin{aligned} f(z+w) &= f((x+yj)+(u+vj)) \\ &= f((x+u)+(y+v)j) \\ &= \begin{pmatrix} x+u & y+v \\ y+v & x+u \end{pmatrix} \\ &= \begin{pmatrix} x & y \\ y & x \end{pmatrix} * \begin{pmatrix} u & v \\ v & u \end{pmatrix} \\ &= f(z) * f(w). \end{aligned}$$

- On montre que $f(z \cdot w) = f(z) \times f(w)$. En effet,

$$\begin{aligned} f(z \cdot w) &= f((x+yj) \cdot (u+vj)) \\ &= f((xu+yv)+(xv+yu)j) \\ &= \begin{pmatrix} xu+yv & xv+yu \\ xv+yu & xu+yv \end{pmatrix} = \begin{pmatrix} xu+yv & xv+yu \\ yu+xv & yv+xu \end{pmatrix} \\ &= \begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \begin{pmatrix} u & v \\ v & u \end{pmatrix} \\ &= f(z) \times f(w). \end{aligned}$$

Ainsi, l'application f est un homomorphisme. Montrons que f est une bijection.

- **Injection.** Supposons que $f(z) = f(w)$. Montrons que $z = w$. On a

$$\begin{aligned} f(z) = f(w) &\Rightarrow f(x+yj) = f(u+vj) \\ &\Rightarrow \begin{pmatrix} x & y \\ y & x \end{pmatrix} = \begin{pmatrix} u & v \\ v & u \end{pmatrix} \\ &\Rightarrow x = u \text{ et } y = v \\ &\Rightarrow x+yj = u+vj \\ &\Rightarrow z = w. \end{aligned}$$

- **Surjection.** Soit $A \in A_2(\mathbb{R})$. Montrons qu'il existe $r \in \mathbb{D}$ tel que $f(r) = A$. Comme $A \in A_2(\mathbb{R})$, alors

$$A = \begin{pmatrix} s & t \\ t & s \end{pmatrix},$$

pour $s, t \in \mathbb{R}$ quelconques. Il suffit de prendre $r = s + tj \in \mathbb{D}$ pour obtenir $f(r) = A$.

Ainsi, l'application f est bijective. Par conséquent, f est un isomorphisme. ■

Comme f est un isomorphisme, les triplets $(\mathbb{D}, +, \cdot)$ et $(A_2(\mathbb{R}), *, \times)$ sont isomorphes, donc la structure des nombres hyperboliques est la même que l'on soit dans $\mathbb{D}$ ou dans $A_2(\mathbb{R})$.

3.1 Une base idempotente

Une base idempotente de l'ensemble $\mathbb{D}$ sera constituée de deux nombres hyperboliques $e_1 = x_1 + y_1 j$ et $e_2 = x_2 + y_2 j$ qui respecteront les propriétés suivantes, où $k = 1, 2$:

- $e_k^2 = e_k \Leftrightarrow e_k^2 = (x_k + y_k j)^2 = (x_k^2 + y_k^2) + 2x_k y_k j = x_k + y_k j = e_k$. Si $y_k \neq 0$, alors $2x_k y_k = y_k \Rightarrow x_k = 1/2$. Puisque $x_k^2 + y_k^2 = x_k$, alors $y_k = \pm 1/2$;
- $e_1 \neq e_2 \Rightarrow e_1 = 1/2 + y_1 j \neq 1/2 + y_2 j = e_2 \Rightarrow y_1 \neq y_2$. Puisque $y_k = \pm 1/2$, alors $y_1 = 1/2$ et $y_2 = -1/2$, ou l'inverse.

On obtient

$$e_1 = \frac{1+j}{2} \text{ et } e_2 = \frac{1-j}{2}$$
$$\text{ou } e_1 = \frac{1-j}{2} \text{ et } e_2 = \frac{1+j}{2}.$$

Dans l'un ou l'autre des deux cas, on constate que $e_1^* = e_2$. Puisque seules les « étiquettes » e_1 et e_2 changent dans l'une ou l'autre des formes, posons $e = \dfrac{1+j}{2}$ et $e^* = \dfrac{1-j}{2}$.

Remarquons que ce n'est pas la seule base qui existe. Dans la première propriété, on a posé $y_k \neq 0$, pour $k = 1, 2$. Si l'on accepte $y_1 = 0$ et/ou $y_2 = 0$, on obtient de nouvelles bases idempotentes. Les nombres $e_1 = 1$ et $e_2 = \dfrac{1+j}{2}$ en sont un exemple.

Parmi les différentes bases idempotentes possibles dans $\mathbb{D}$, le choix de e et de e^* est fondé sur les propriétés suivantes.

Proposition 3.9. *La base idempotente* $\left\{ e = \dfrac{1+j}{2}, e^* = \dfrac{1-j}{2} \right\}$ *vérifie les cinq propriétés suivantes :*

- $e^2 = e$;
- $e^{*2} = e^*$;
- $e + e^* = 1$;
- $e - e^* = j$;
- $e \cdot e^* = 0$.

Démonstration. Il est facile de démontrer ces propriétés par des calculs directs. ■

Il est intéressant de constater que, au contraire de l'ensemble $\mathbb{D}$, les complexes n'ont pas de base idempotente. De façon générale, un corps commutatif K est assurément intègre, et comme un corps est un anneau, alors K est un anneau intègre. Les seuls éléments idempotents de K sont donc le neutre additif 0 et le neutre multiplicatif 1 [19]. Or, 0 et 1 ne forment pas une base de K sur $\mathbb{R}$, en particulier, lorsque $K = \mathbb{C}$; il n'existe donc aucune base idempotente dans les complexes.

Note : Dans le texte qui suit, un nombre est écrit en composantes « cartésiennes » s'il est de la forme $z = x + yj$ et il est écrit en composantes « idempotentes » s'il est de la forme $z = \alpha e + \beta e^*$.

Étant une base, n'importe quel nombre z pourra s'écrire comme une combinaison linéaire de e et e^*. Soit un nombre $z = \alpha e + \beta e^*$. De la représentation idempotente, on obtient l'écriture cartésienne qui suit :

$$z = \alpha e + \beta e^* = \alpha\left(\frac{1+j}{2}\right) + \beta\left(\frac{1-j}{2}\right) = \left(\frac{\alpha+\beta}{2}\right) + \left(\frac{\alpha-\beta}{2}\right) j = x + yj.$$

Quelle est l'opération inverse pour passer de $z = x + yj$ à $z = \alpha e + \beta e^*$? Pour cela, résolvons le système d'équations linéaires suivant :

$$\begin{aligned}
\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{-1}{2} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} &= \begin{bmatrix} x \\ y \end{bmatrix} \\
&\sim \left[\begin{array}{cc|c} \frac{1}{2} & \frac{1}{2} & x \\ \frac{1}{2} & \frac{-1}{2} & y \end{array}\right] \\
&\sim \begin{array}{r} L_1 \to 2L_1 \\ L_2 \to 2L_2 \end{array} \left[\begin{array}{cc|c} 1 & 1 & 2x \\ 1 & -1 & 2y \end{array}\right] \\
&\sim \begin{array}{r} \\ L_2 \to -L_1 + L_2 \end{array} \left[\begin{array}{cc|c} 1 & 1 & 2x \\ 0 & -2 & -2x + 2y \end{array}\right] \\
&\sim \begin{array}{r} \\ L_2 \to -\frac{1}{2}L_2 \end{array} \left[\begin{array}{cc|c} 1 & 1 & 2x \\ 0 & 1 & x - y \end{array}\right] \\
&\sim \begin{array}{r} L_1 \to -L_2 + L_1 \\ \\ \end{array} \left[\begin{array}{cc|c} 1 & 0 & x + y \\ 0 & 1 & x - y \end{array}\right].
\end{aligned}$$

Ainsi, on a

$$\alpha = x + y;$$
$$\beta = x - y.$$

Conséquemment, tout nombre hyperbolique $z = x + yj$ peut s'écrire comme suit :

$$z = (x + y)e + (x - y)e^*.$$

La représentation idempotente est unique. En effet, soit $z = \alpha_1 e + \beta_1 e^* = \alpha_2 e + \beta_2 e^*$. Pour $k = 1, 2$, on a

$$z = \left(\frac{\alpha_k + \beta_k}{2}\right) + \left(\frac{\alpha_k - \beta_k}{2}\right) j.$$

De par l'égalité des deux représentations cartésiennes, il s'ensuit

$$\frac{\alpha_1 + \beta_1}{2} = \frac{\alpha_2 + \beta_2}{2} \Rightarrow \alpha_1 + \beta_1 = \alpha_2 + \beta_2, \tag{3.1}$$
$$\frac{\alpha_1 - \beta_1}{2} = \frac{\alpha_2 - \beta_2}{2} \Rightarrow \alpha_1 - \beta_1 = \alpha_2 - \beta_2. \tag{3.2}$$

En additionnant (3.1) et (3.2) et en divisant par 2, on obtient $\alpha_1 = \alpha_2$. En substituant dans (3.1), on trouve que $\beta_1 = \beta_2$.

Exemple 3.10. Si $z = 2 + 3j$, alors $z = 5e - e^*$. En effet,

$$z = 2 + 3j = (2 + 3)e + (2 - 3)e^* = 5e - e^*.$$

Exemple 3.11. Si $w = (\pi + 1)e + (\pi - 1)e^*$, alors $w = \pi + j$. En effet,

$$w = (\pi + 1)e + (\pi - 1)e^* = \left(\frac{(\pi + 1) + (\pi - 1)}{2}\right) + \left(\frac{(\pi + 1) - (\pi - 1)}{2}\right) j = \pi + j.$$

De ce qui suit, nous présentons les opérations arithmétiques dans la base idempotente. Pour simplifier l'écriture lors des calculs, il convient de poser $\alpha = x + y$ et $\beta = x - y$, d'où

$$z = x + yj = (x + y)e + (x - y)e^* = \alpha e + \beta e^*.$$

Proposition 3.12. *Soit $z = x + yj = \alpha_1 e + \beta_1 e^*$ et $w = u + vj = \alpha_2 e + \beta_2 e^*$. Les quatre opérations arithmétiques sont données par :*

- ***Addition.*** *On a*

$$\begin{aligned} z + w &= (x + yj) + (u + vj) = (x + u) + (y + v)j \\ &= ((x + u) + (y + v))e + ((x + u) - (y + v))e^* \\ &= ((x + y) + (u + v))e + ((x - y) + (u - v))e^* \\ &= (\alpha_1 + \alpha_2)e + (\beta_1 + \beta_2)e^*. \end{aligned}$$

- ***Soustraction.*** *On a*

$$\begin{aligned} z - w &= (x + yj) - (u + vj) = (x - u) + (y - v)j \\ &= ((x - u) + (y - v))e + ((x - u) - (y - v))e^* \\ &= ((x + y) - (u + v))e + ((x - y) - (u - v))e^* \\ &= (\alpha_1 - \alpha_2)e + (\beta_1 - \beta_2)e^*. \end{aligned}$$

- ***Multiplication.*** *On a*

$$\begin{aligned} zw &= (x + yj)(u + vj) = (xu + yv) + (xv + yu)j \\ &= ((xu + yv) + (xv + yu))e + ((xu + yv) - (xv + yu))e^* \\ &= ((x + y)(u + v))e + ((x - y)(u - v))e^* \\ &= (\alpha_1\alpha_2)e + (\beta_1\beta_2)e^*. \end{aligned}$$

- ***Division.*** *Pour* $u^2 - v^2 = (u + v)(u - v) \neq 0 \Rightarrow \alpha_2, \beta_2 \neq 0$, *on a*

$$\begin{aligned} \frac{z}{w} = \frac{x + yj}{u + vj} &= \frac{(x + yj)(u - vj)}{(u + vj)(u - vj)} = \frac{xu - yv}{u^2 - v^2} + \frac{-xv + yu}{u^2 - v^2}j \\ &= \left(\frac{xu - yv}{u^2 - v^2} + \frac{-xv + yu}{u^2 - v^2}\right)e + \left(\frac{xu - yv}{u^2 - v^2} - \frac{-xv + yu}{u^2 - v^2}\right)e^* \\ &= \left(\frac{(x + y)(u - v)}{u^2 - v^2}\right)e + \left(\frac{(x - y)(u + v)}{u^2 - v^2}\right)e^* \\ &= \left(\frac{x + y}{u + v}\right)e + \left(\frac{x - y}{u - v}\right)e^* \\ &= \left(\frac{\alpha_1}{\alpha_2}\right)e + \left(\frac{\beta_1}{\beta_2}\right)e^*. \end{aligned}$$

On constate que les opérations deviennent plus naturelles dans la base idempotente, ce qui n'est pas le cas avec la représentation cartésienne.

La multiplication peut aussi être obtenue à l'aide de la distributivité habituelle. De la proposition 3.9, on a

$$\begin{aligned} zw &= (\alpha_1 e + \beta_1 e^*)(\alpha_2 e + \beta_2 e^*) \\ &= \alpha_1\alpha_2 ee + \alpha_1\beta_2 ee^* + \beta_1\alpha_2 e^* e + \beta_1\beta_2 e^* e^* \\ &= \alpha_1\alpha_2 e + \alpha_1\beta_2 0 + \beta_1\alpha_2 0 + \beta_1\beta_2 e^* \\ &= \alpha_1\alpha_2 e + \beta_1\beta_2 e^*. \end{aligned}$$

Aussi, nous avons la propriété suivante.

Proposition 3.13. *Soit $z = \alpha e + \beta e^*$, alors $z^n = \alpha^n e + \beta^n e^*$, pour $n \in \mathbb{N}$.*

Démonstration. Procédons par induction sur n.

- Cas $n = 1$. On a $z^1 = \alpha e + \beta e^* = \alpha^1 e + \beta^1 e^*$.
- Cas $n > 1$. Supposons le résultat vrai pour $n - 1$, c'est-à-dire $z^{n-1} = \alpha^{n-1} e + \beta^{n-1} e^*$. On a

$$\begin{aligned} z^n &= z^{n-1} z \\ &= (\alpha^{n-1} e + \beta^{n-1} e^*)(\alpha e + \beta e^*) \\ &= \alpha^{n-1} \alpha e + \beta^{n-1} \beta e^*, \text{ par la proposition 3.12} \\ &= \alpha^n e + \beta^n e^*. \end{aligned}$$

Par l'induction mathématique, le résultat est vérifié pour tout $n \in \mathbb{N}$. ■

Proposition 3.14. *Soit $z = \alpha e + \beta e^*$ et $P_n(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ un polynôme de degré n. Alors*

$$P_n(z) = P_n(\alpha) e + P_n(\beta) e^*.$$

Démonstration. Des propositions 3.9 et 3.13, on a

$$\begin{aligned} P_n(z) &= a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 \\ &= a_n(\alpha e + \beta e^*)^n + a_{n-1}(\alpha e + \beta e^*)^{n-1} + ... + a_1(\alpha e + \beta e^*) + a_0 \\ &= a_n(\alpha^n e + \beta^n e^*) + a_{n-1}(\alpha^{n-1} e + \beta^{n-1} e^*) + ... + a_1(\alpha e + \beta e^*) + a_0 \\ &= a_n \alpha^n e + a_{n-1} \alpha^{n-1} e + ... + a_1 \alpha e + a_0 e - a_0 e \\ &\quad + a_n \beta^n e^* + a_{n-1} \beta^{n-1} e^* + ... + a_1 \beta e^* + a_0 e^* - a_0 e^* + a_0 \\ &= (a_n \alpha^n + a_{n-1} \alpha^{n-1} + ... + a_1 \alpha + a_0) e \\ &\quad + (a_n \beta^n + a_{n-1} \beta^{n-1} + ... + a_1 \beta + a_0) e^* - a_0(e + e^*) + a_0 \\ &= P_n(\alpha) e + P_n(\beta) e^* - a_0 + a_0 \\ &= P_n(\alpha) e + P_n(\beta) e^*. \end{aligned}$$

■

Proposition 3.15. *Le conjugué hyperbolique de* $z = \alpha e + \beta e^*$ *est* $z^* = \beta e + \alpha e^*$.

Démonstration. Soit $z = \alpha e + \beta e^* = x + yj$, où $\alpha = x + y$ et $\beta = x - y$. On a

$$\begin{aligned} z^* &= x - yj \\ &= (x + (-y))e + (x - (-y))e^* \\ &= (x - y)e + (x + y)e^* \\ &= \beta e + \alpha e^*. \end{aligned}$$

■

Proposition 3.16. *Le module hyperbolique de* $z = \alpha e + \beta e^*$ *est* $|z|_h = \sqrt{\alpha\beta}$, *où* $\alpha\beta \geq 0$.

Démonstration. On obtient directement des propositions 3.9 et 3.12

$$|z|_h^2 = zz^* = (\alpha e + \beta e^*)(\beta e + \alpha e^*) = \alpha\beta e + \alpha\beta e^* = \alpha\beta(e + e^*) = \alpha\beta,$$

d'où en extrayant la racine carrée positive, on a le résultat. ■

Proposition 3.17. *Soit* $z = \alpha e + \beta e^*$ *un hyperbolique inversible. Alors* $z^{-1} = \frac{1}{\alpha}e + \frac{1}{\beta}e^*$, *où* $\alpha, \beta \neq 0$.

Démonstration. Comme z est inversible et que le neutre multiplicatif est 1, alors $zz^{-1} = 1$ et $z^{-1} = \frac{1}{z}$. De plus, on a $1 = e + e^*$ de la proposition 3.9. De la proposition 3.12, on a

$$z^{-1} = \frac{1}{z} = \frac{1e + 1e^*}{\alpha e + \beta e^*} = \frac{1}{\alpha}e + \frac{1}{\beta}e^*.$$

■

Il faut se rappeler qu'un hyperbolique $z = x + yj$ est inversible si et seulement si $x \neq \pm y$. L'analogie avec la base idempotente est évidente. Séparons en deux cas :

$$\begin{aligned} x \neq -y \Leftrightarrow x + y \neq 0 \Leftrightarrow \alpha \neq 0 \text{ et} \\ x \neq +y \Leftrightarrow x - y \neq 0 \Leftrightarrow \beta \neq 0. \end{aligned}$$

Les hypothèses de la proposition 3.17 nécessitent que $\alpha, \beta \neq 0$ car $1/\alpha$ et $1/\beta$ sont des nombres réels et la division par 0 est indéfinie.

Proposition 3.18. *(Caractérisation des hyperboliques non inversibles) Soit* $z = x + yj = \alpha e + \beta e^*$. *Alors* z *est non inversible si et seulement si* $\alpha = 0$ *ou* $\beta = 0$.

Démonstration. On a la double implication par la preuve directe.

$$\begin{aligned} z \text{ est non inversible} &\Leftrightarrow x^2 - y^2 = 0 \\ &\Leftrightarrow (x+y)(x-y) = 0 \\ &\Leftrightarrow \alpha = x + y = 0 \text{ ou} \\ &\quad\ \beta = x - y = 0. \end{aligned}$$

■

3.2 Les fonctions hyperboliques

L'hyperbole centrée à l'origine est une fonction réelle qui possède des propriétés similaires au cercle trigonométrique. Dans cette section, on mettra l'accent sur une équation de l'hyperbole dite équilatère. C'est entre autres avec l'hyperbole équilatère que l'on peut retrouver les fonctions $\cosh x$ et $\sinh x$, exprimées à l'aide des fonctions exponentielles. Puis on déduira quelques résultats de base sur ces fonctions.

3.2.1 L'hyperbole équilatère

Une hyperbole est le lieu géométrique de tous les points tels que la différence des distances entre ce point et deux points fixes, appelés les foyers, est constante. Nous sommes en mesure de construire géométriquement ce lieu où l'on obtient l'équation

$$\frac{(x-x_0)^2}{a^2} - \frac{(y-y_0)^2}{b^2} = 1. \tag{3.3}$$

Cette équation possède quatre paramètres : a la demi-longueur de l'axe transversal ; b la demi-longueur de l'axe conjugué ; x_0 et y_0 les coordonnées du centre de l'hyperbole, soit le point par lequel passent l'axe transversal, l'axe conjugué et les asymptotes. La différence constante des distances est en fait la longueur de l'axe transversal, c'est-à-dire $2a$. C'est aussi la distance entre les deux sommets $S_1(x_0+a, y_0)$ et $S_2(x_0-a, y_0)$ situés sur ce même axe. Les asymptotes, qui sont des droites affines, sont données par $y_1 = \frac{b}{a}(x - x_0) + y_0$ et $y_2 = -\frac{b}{a}(x - x_0) + y_0$. On obtient par l'équation (3.3) une hyperbole dite **horizontale**, car l'axe transversal est perpendiculaire à l'axe des abscisses. On dira d'une hyperbole qu'elle est **équilatère** si les asymptotes sont perpendiculaires entre elles, c'est-à-dire si $a = b$. De plus, les deux foyers sont situés aux points d'intersection du cercle d'équation $(x-x_0)^2 + (y-y_0)^2 = a^2 + b^2$ et de

la droite passant par les sommets. Il y a toujours deux branches à une hyperbole, qui sont le miroir l'une de l'autre. Il est possible de faire deux réflexions à l'aide des axes transversal et conjugué. La figure 3.19 donne un exemple de fonctions hyperboliques.

On a sensiblement les mêmes résultats si l'hyperbole est **verticale**, c'est-à-dire si son équation générale est de la forme

$$\frac{(y-y_0)^2}{b^2} - \frac{(x-x_0)^2}{a^2} = 1.$$

Il existe aussi des hyperboles obliques, mais elles ne seront pas étudiées ici.

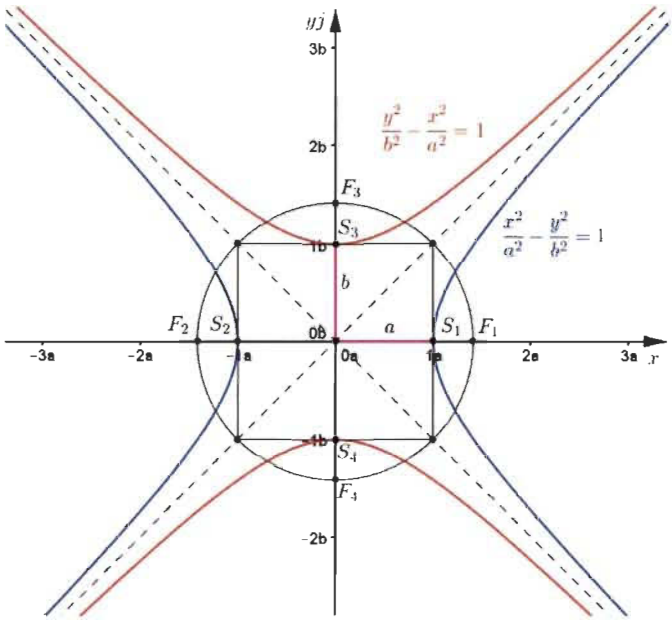


FIGURE 3.19 – Exemple d'hyperboles.

L'hyperbole $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ est centrée en $(0,0)$. L'axe transversal mesure $2a$ et l'axe conjugué mesure $2b$. Les sommets sont $S_1(a,0)$ et $S_2(-a,0)$ et les foyers sont $F_1(\sqrt{a^2+b^2},0)$ et $F_2(-\sqrt{a^2+b^2},0)$. L'hyperbole $\frac{y^2}{a^2} - \frac{x^2}{b^2} = 1$ a un axe transversal mesurant $2b$ et un axe conjugué mesurant $2a$. Ses sommets sont $S_3(0,b)$ et $S_4(0,-b)$ et ses foyers sont en $F_3(0,\sqrt{a^2+b^2})$ et en $F_4(0,-\sqrt{a^2+b^2})$. Dans les deux cas, les asymptotes sont $y = \frac{b}{a}$ et $y = -\frac{b}{a}$.

Dans le cas d'une hyperbole équilatère centrée à l'origine, si on pose dans l'équation (3.3) les valeurs $x_0 = 0$, $y_0 = 0$ et $p = a = b$, on obtient l'équation

$$x^2 - y^2 = p^2.$$

Un exemple simple d'une hyperbole équilatère est donnée par la fonction $y = \frac{1}{x}$, centrée à l'origine, dont ses asymptotes sont $y = 0$ et $x = 0$.

3.2.2 Les fonctions $\cosh t$ et $\sinh t$

Les fonctions hyperboliques sont obtenues comme combinaisons linéaires d'exponentielles. Les cosinus et sinus hyperboliques correspondront respectivement à la base et à la hauteur du triangle rectangle construit sur l'axe des abscisses ayant un sommet sur l'hyperbole. Trouvons les expressions de ces deux fonctions à l'aide de l'hyperbole $x^2 - y^2 = 1$.

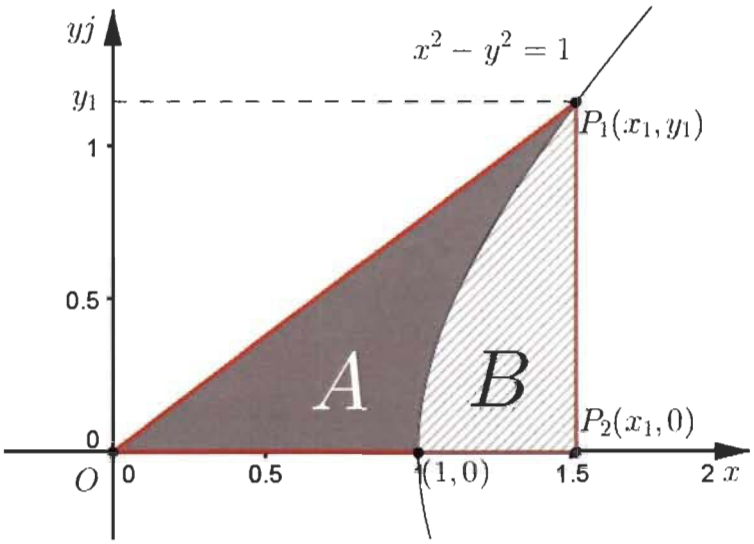


FIGURE 3.20 – Aire d'un triangle hyperbolique.

Tel qu'il est illustré à la figure 3.20, l'aire du $\triangle OP_1P_2$ égale l'aire de la région A plus l'aire de la région B. À des fins de compréhension, dans le texte qui suit, on désigne le contour et l'intérieur de la région A sous le nom de « triangle hyperbolique », car un côté de ce triangle est sur une courbe hyperbolique. Commençons d'abord par exprimer sous forme explicite l'équation de l'hyperbole

$$\begin{aligned} x^2 - y^2 = 1 &\Rightarrow y^2 = x^2 - 1 \\ &\Rightarrow y = \pm\sqrt{x^2 - 1}. \end{aligned}$$

Étant dans la partie supérieure du plan (à priori y_1 est positif), alors $y = \sqrt{x^2 - 1}$. Puisque $y_1 = \sqrt{x_1^2 - 1}$, alors

$$\text{Aire } \triangle OP_1P_2 = \frac{x_1 y_1}{2} = \frac{x_1\sqrt{x_1^2 - 1}}{2}.$$

L'aire de la région B est obtenue par le calcul de l'intégrale suivante :

$$\text{Aire } B = \int_1^{x_1} \sqrt{x^2 - 1}\mathrm{d}x.$$

Dans cette intégrale, posons le changement de variable $\cos\theta = 1/x$, d'où $x = \sec\theta \Rightarrow x^2 = \sec^2\theta$ et $\mathrm{d}x = \sec\theta\tan\theta\mathrm{d}\theta$. De plus, $\theta = \arccos\left(\frac{1}{x}\right)$. Lorsque $x = 1$ et $x = x_1$ respectivement, on a $\theta = \arccos(1) = 0$ et $\theta = \arccos\left(\frac{1}{x_1}\right)$.

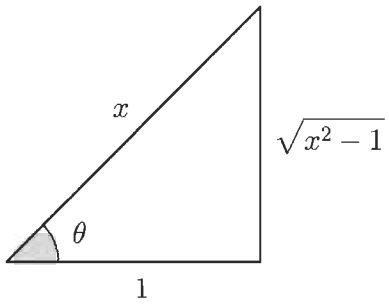


FIGURE 3.21 – Substitution trigonométrique.

Par des formules de réduction ou d'intégration par parties, on obtient

$$\begin{aligned}
\text{Aire } B = \int_1^{x_1} \sqrt{x^2-1}\mathrm{d}x &= \int_0^{\arccos(1/x_1)} \sqrt{\sec^2\theta - 1}\sec\theta\tan\theta\mathrm{d}\theta \\
&= \int_0^{\arccos(1/x_1)} \sqrt{\tan^2\theta}\sec\theta\tan\theta\mathrm{d}\theta \\
&= \int_0^{\arccos(1/x_1)} \tan^2\theta\sec\theta\mathrm{d}\theta \\
&= \frac{\sec\theta\tan\theta - \ln|\sec\theta+\tan\theta|}{2}\Bigg|_0^{\arccos(1/x_1)} \\
&= \frac{x_1\cdot x_1\sqrt{1-\frac{1}{x_1^2}} - \ln\left|x_1 + x_1\sqrt{1-\frac{1}{x_1^2}}\right|}{2} - \frac{0-\ln|1+0|}{2} \\
&= \frac{x_1\sqrt{x_1^2-1} - \ln\left|x_1+\sqrt{x_1^2-1}\right|}{2}.
\end{aligned}$$

Alors,

$$\begin{aligned}
\text{Aire } A &= \text{Aire } \triangle OP_1P_2 - \text{Aire } B \\
&= \frac{x_1\sqrt{x_1^2-1}}{2} - \frac{x_1\sqrt{x_1^2-1} - \ln\left|x_1+\sqrt{x_1^2-1}\right|}{2} \\
&= \frac{\ln\left|x_1+\sqrt{x_1^2-1}\right|}{2}.
\end{aligned}$$

Notre objectif est d'isoler les expressions de x_1 et de y_1 sachant que $x_1 \geq 0$, $y_1 \geq 0$ et $y_1 = \sqrt{x_1^2-1}$, fonction définie pour $|x_1| \geq 1$. Dans notre cas, $x_1 \geq 1$, d'où

$\left|x_1 + \sqrt{x_1^2 - 1}\right| = x_1 + \sqrt{x_1^2 - 1} > 0$. Ainsi,

$$\begin{aligned}
A &= \frac{\ln\left|x_1 + \sqrt{x_1^2 - 1}\right|}{2} \\
\Rightarrow 2A &= \ln\left(x_1 + \sqrt{x_1^2 - 1}\right) \\
\Rightarrow e^{2A} &= x_1 + \sqrt{x_1^2 - 1} \\
\Rightarrow \left(e^{2A} - x_1\right)^2 &= \left(\sqrt{x_1^2 - 1}\right)^2 \\
\Rightarrow e^{4A} - 2x_1 e^{2A} + x_1^2 &= x_1^2 - 1 \\
\Rightarrow e^{4A} + 1 &= 2x_1 e^{2A} \\
\Rightarrow \frac{e^{4A} + 1}{2e^{2A}} &= x_1 \\
\Rightarrow \frac{e^{2A} + e^{-2A}}{2} &= x_1.
\end{aligned}$$

Comme $y_1 = \sqrt{x_1^2 - 1} \geq 0$, alors

$$\begin{aligned}
y_1^2 &= x_1^2 - 1 \\
&= \left(\frac{e^{2A} + e^{-2A}}{2}\right)^2 - 1 \\
&= \frac{e^{4A} + 2 + e^{-4A}}{4} - \frac{4}{4} \\
&= \frac{e^{4A} - 2 + e^{-4A}}{4} \\
&= \left(\frac{e^{2A} - e^{-2A}}{2}\right)^2 \\
\Rightarrow |y_1| = y_1 &= \frac{e^{2A} - e^{-2A}}{2}.
\end{aligned}$$

Des expressions de $x_1 = \dfrac{e^{2A} + e^{-2A}}{2}$ et $y_1 = \dfrac{e^{2A} - e^{-2A}}{2}$, on constate que la variable indépendante est l'aire de la région A. Les coordonnées dépendent donc de l'aire du triangle hyperbolique. En comparant avec le cercle trigonométrique, par analogie, on appellera ces deux quantités le cosinus hyperbolique et le sinus hyperbolique. Par contre, au lieu de considérer $2A$, on posera t comme étant la variable. D'où

$$x = \frac{e^t + e^{-t}}{2} := \cosh t \qquad \text{et} \qquad y = \frac{e^t - e^{-t}}{2} := \sinh t,$$

où t représente le *double* de l'aire de la région A (voir la figure 3.22).

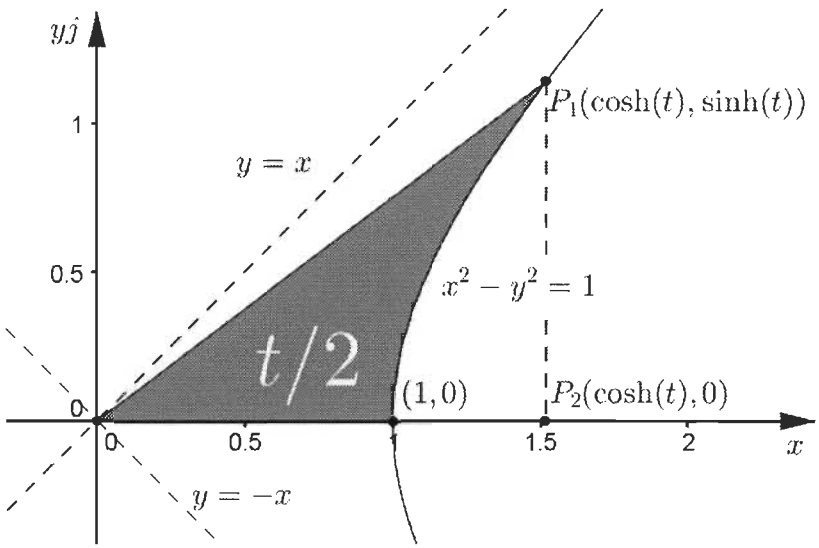


FIGURE 3.22 – Représentation d'un triangle hyperbolique.

Les résultats précédents sont obtenus dans le premier quadrant. On obtient des résultats similaires dans les autres quadrants sachant que l'aire est positive ou négative selon que le triangle hyperbolique est au-dessus ou au-dessous de l'axe des abscisses.

Proposition 3.23. *Les fonctions* $\cosh t$ *et* $\sinh t$ *vérifient les propriétés suivantes :*

- $\cosh^2 t - \sinh^2 t = 1$;
- $\cosh(-t) = \cosh t$;
- $\sinh(-t) = -\sinh t$;
- $\cosh t + \sinh t = e^t$;
- $\cosh t - \sinh t = e^{-t}$.

Démonstration. Il est facile de démontrer ces propriétés par des calculs directs. ■

3.2.3 Les fonctions $\cosh^{-1} x$ et $\sinh^{-1} y$

On a vu que la variable t des fonctions $x = \cosh t$ et $y = \sinh t$ représente le double de l'aire d'un triangle hyperbolique. Qu'en est-il si l'on exprime t en fonction des valeurs x et y ? Cela revient à trouver les fonctions inverses $\cosh^{-1} x$ et $\sinh^{-1} y$ [2]. Calculons dans un

premier temps la fonction $\cosh^{-1} x$. On a $x = \cosh t = \dfrac{e^t + e^{-t}}{2} > 0,\ \forall t \in \mathbb{R}$, d'où

$$\begin{aligned}
x &= \frac{e^t + e^{-t}}{2} \\
\Rightarrow x &= \frac{e^{2t} + 1}{2e^t} \\
\Rightarrow 2e^t x &= e^{2t} + 1 \\
\Rightarrow 0 &= e^{2t} - 2e^t x + 1 \\
\Rightarrow e^t &= \frac{-(-2x) \pm \sqrt{(-2x)^2 - 4 \cdot 1 \cdot 1}}{2(1)} \\
\Rightarrow e^t &= x \pm \sqrt{x^2 - 1}.
\end{aligned}$$

Puisque la fonction exponentielle est positive, il faut trouver les valeurs de x pour lesquelles $e^t > 0$. Pour que $\sqrt{x^2 - 1}$ soit définie, il faut que $|x| \geq 1$. Si $x \geq 1$, alors $x \pm \sqrt{x^2 - 1}$ est positive. Si $x \leq -1$, alors $x \pm \sqrt{x^2 - 1}$ est négative, et ce cas est à rejeter. Lorsque l'on applique le logarithme à $x \pm \sqrt{x^2 - 1}$, on obtient $t \geq 0$ en choisissant le signe « $+$ », et $t < 0$ pour le signe « $-$ ». On choisira le signe positif, autrement dit, nous privilégions la *branche principale* de la fonction $\cosh^{-1} x$. Lorsque $x \geq 1$, nous obtenons

$$e^t = x + \sqrt{x^2 - 1} \Rightarrow t = \ln\left(x + \sqrt{x^2 - 1}\right) := \cosh^{-1} x.$$

Calculons la fonction $\sinh^{-1} y$. Soit $y = \sinh t = \dfrac{e^t - e^{-t}}{2}$, alors

$$\begin{aligned}
y &= \frac{e^t - e^{-t}}{2} \\
\Rightarrow y &= \frac{e^{2t} - 1}{2e^t} \\
\Rightarrow 2e^t y &= e^{2t} - 1 \\
\Rightarrow 0 &= e^{2t} - 2e^t y - 1 \\
\Rightarrow e^t &= \frac{-(-2y) \pm \sqrt{(-2y)^2 - 4 \cdot 1 \cdot (-1)}}{2(1)} \\
\Rightarrow e^t &= y \pm \sqrt{y^2 + 1}.
\end{aligned}$$

Comme l'exponentielle est toujours positive, alors le signe négatif est à rejeter. D'où

$$e^t = y + \sqrt{y^2 + 1} \Rightarrow t = \ln\left(y + \sqrt{y^2 + 1}\right) := \sinh^{-1} y.$$

Puisque la fonction $y + \sqrt{y^2 + 1}$ est une fonction strictement positive, alors le logarithme est défini $\forall y \in \mathbb{R}$.

3.2.4 Développements en série

Le développement de Taylor autour de 0 de la fonction exponentielle est

$$e^t = 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \frac{t^4}{4!} + ... = \sum_{n=0}^{\infty} \frac{t^n}{n!},$$

et

$$e^{-t} = 1 - t + \frac{t^2}{2!} - \frac{t^3}{3!} + \frac{t^4}{4!} - ... = \sum_{n=0}^{\infty} \frac{(-1)^n t^n}{n!}.$$

Puisque l'argument des cosinus et sinus hyperboliques est un nombre réel, en particulier l'aire, on peut procéder à leur développement en série en utilisant les identités ci-dessus. Les résultats obtenus sont possibles grâce aux théorèmes sur les séries réelles.

Considérons la fonction $\cosh t$. Son développement est

$$\begin{aligned}
\cosh t = \frac{e^t + e^{-t}}{2} &= \frac{1}{2}\left(\sum_{n=0}^{\infty} \frac{t^n}{n!} + \sum_{n=0}^{\infty} \frac{(-1)^n t^n}{n!}\right) \\
&= \frac{1}{2} \sum_{n=0}^{\infty} \frac{t^n + (-1)^n t^n}{n!} \\
&= \frac{1}{2}\left(\sum_{n=0}^{\infty} \frac{t^{2n} + (-1)^{2n} t^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{t^{2n+1} + (-1)^{2n+1} t^{2n+1}}{(2n+1)!}\right) \\
&= \frac{1}{2}\left(\sum_{n=0}^{\infty} \frac{t^{2n} + t^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{t^{2n+1} - t^{2n+1}}{(2n+1)!}\right) \\
&= \frac{1}{2} \sum_{n=0}^{\infty} \frac{2t^{2n}}{(2n)!} \\
&= \sum_{n=0}^{\infty} \frac{t^{2n}}{(2n)!}.
\end{aligned}$$

Similairement, le développement de la fonction $\sinh t$ est

$$\begin{aligned}
\sinh t = \frac{e^t - e^{-t}}{2} &= \frac{1}{2}\left(\sum_{n=0}^{\infty}\frac{t^n}{n!} - \sum_{n=0}^{\infty}\frac{(-1)^n t^n}{n!}\right) \\
&= \frac{1}{2}\sum_{n=0}^{\infty}\frac{t^n - (-1)^n t^n}{n!} \\
&= \frac{1}{2}\left(\sum_{n=0}^{\infty}\frac{t^{2n} - (-1)^{2n}t^{2n}}{(2n)!} + \sum_{n=0}^{\infty}\frac{t^{2n+1} - (-1)^{2n+1}t^{2n+1}}{(2n+1)!}\right) \\
&= \frac{1}{2}\left(\sum_{n=0}^{\infty}\frac{t^{2n} - t^{2n}}{(2n)!} + \sum_{n=0}^{\infty}\frac{t^{2n+1} + t^{2n+1}}{(2n+1)!}\right) \\
&= \frac{1}{2}\sum_{n=0}^{\infty}\frac{2t^{2n+1}}{(2n+1)!} \\
&= \sum_{n=0}^{\infty}\frac{t^{2n+1}}{(2n+1)!}.
\end{aligned}$$

Par induction sur k, on a $j^k = \begin{cases} (1)^{\frac{k}{2}} & \text{si } k \text{ est pair} \\ (1)^{\frac{k-1}{2}} j & \text{si } k \text{ est impair} \end{cases}$. Ce résultat et les développements de $\cosh t$ et de $\sinh t$ permettent de retrouver le développement de l'exponentielle hyperbolique.

$$\begin{aligned}
e^{jt} &= \sum_{n=0}^{\infty}\frac{(jt)^n}{n!} \\
&= \sum_{n=0}^{\infty}\frac{j^n t^n}{n!} \\
&= \sum_{n=0}^{\infty}\frac{j^{2n}t^{2n}}{(2n)!} + \sum_{n=0}^{\infty}\frac{j^{2n+1}t^{2n+1}}{(2n+1)!} \\
&= \sum_{n=0}^{\infty}\frac{t^{2n}}{(2n)!} + j\sum_{n=0}^{\infty}\frac{t^{2n+1}}{(2n+1)!} \\
&= \cosh t + j\sinh t.
\end{aligned}$$

La séparation en deux sommes est permise, car les deux sommes convergent chacune $\forall t \in \mathbb{R}$.

3.2.5 Forme polaire hyperbolique

Le développement en série de l'exponentielle hyperbolique donne l'égalité suivante :

$$e^{jt} = \cosh t + j\sinh t.$$

Sachant que le cosinus est l'abscisse et que le sinus est l'ordonnée d'un point, l'exponentielle hyperbolique, au même titre que son homologue complexe, donne les coordonnées de tout point hyperbolique situé sur n'importe quelle hyperbole (voir la figure 3.24) [10]. Dans le premier quadrant, on a

$$pe^{jt} = p(\cosh t + j \sinh t) = p \cosh t + jp \sinh t = x + jy.$$

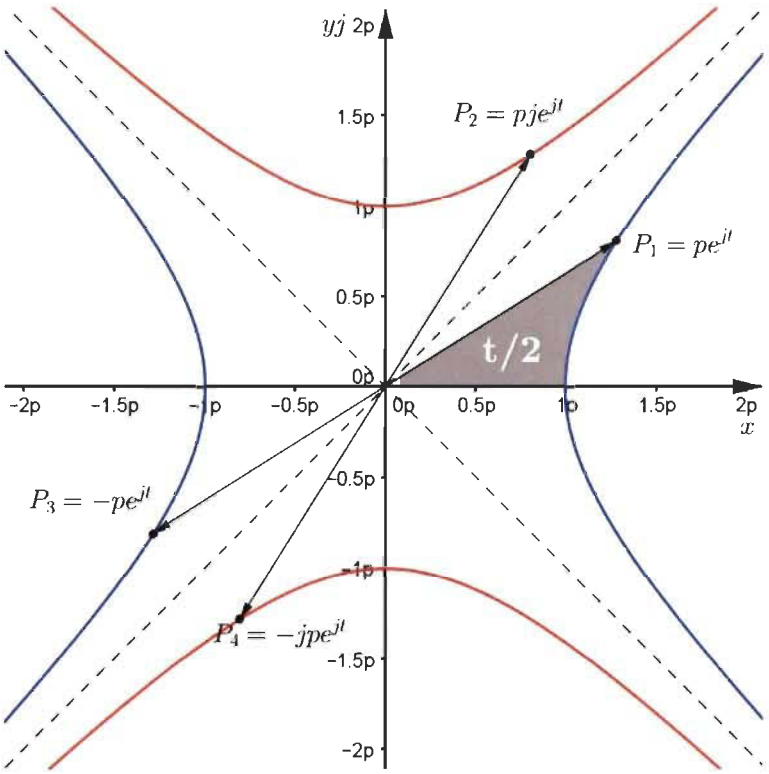


FIGURE 3.24 - Des points hyperboliques.
Les nombres P_1, P_2, P_3 et P_4 sont des associés, car ils sont multipliés par les unités hyperboliques $1, -1, j, -j$.

Exemple 3.25. Soit $z = 4 + j$. Puisque $4^2 - 1^2 = 15$, alors z est sur l'hyperbole horizontale $x^2 - y^2 = \left(\sqrt{15}\right)^2$. Comme $z = 4 + j$ est dans le premier quadrant, alors z est sur la branche droite. D'où $z = 4 + j = \sqrt{15}e^{jt} = \sqrt{15}\cosh t + \sqrt{15}j \sinh t$. Ainsi,

$$\begin{aligned} 4 = \sqrt{15}\cosh t \quad &\Rightarrow \quad \frac{4}{\sqrt{15}} = \cosh t \\ 1 = \sqrt{15}\sinh t \quad &\Rightarrow \quad \frac{1}{\sqrt{15}} = \sinh t. \end{aligned}$$

De la proposition 3.23, on a

$$e^t = \cosh t + \sinh t = \frac{4}{\sqrt{15}} + \frac{1}{\sqrt{15}} = \frac{5}{\sqrt{15}} \quad \Rightarrow \quad t = \ln\left(\frac{5}{\sqrt{15}}\right) = \frac{1}{2}\ln\left(\frac{5}{3}\right).$$

On vérifie que

$$4 = \sqrt{15}\cosh\left(\frac{1}{2}\ln\left(\frac{5}{3}\right)\right);$$

et

$$1 = \sqrt{15}\sinh\left(\frac{1}{2}\ln\left(\frac{5}{3}\right)\right).$$

Par conséquent, $z = 4 + j = \sqrt{15}e^{j\left(\frac{1}{2}\ln\left(\frac{5}{3}\right)\right)}$. Un associé de z serait $z_1 = -z = -4 - j = -\sqrt{15}e^{j\left(\frac{1}{2}\ln\left(\frac{5}{3}\right)\right)}$.

Exemple 3.26. Soit $z = -2 - 3j$. Comme $(-2)^2 - (-3)^2 = -5$, alors z n'est pas sur l'hyperbole horizontale $x^2 - y^2 = p^2$, car $p^2 > 0$. Par contre, $(-3)^2 - (-2)^2 = 5$, alors z est plutôt sur l'hyperbole verticale $y^2 - x^2 = \left(\sqrt{5}\right)^2$. Comme $z = -2 - 3j$ est dans le troisième quadrant, alors z est sur la branche du bas. D'où $z = -2 - 3j = -\sqrt{5}je^{jt} = -\sqrt{5}j\cosh t - \sqrt{5}\sinh t$.
Ainsi,

$$-2 = -\sqrt{5}\sinh t \quad \Rightarrow \quad \frac{2}{\sqrt{5}} = \sinh t$$
$$-3 = -\sqrt{5}\cosh t \quad \Rightarrow \quad \frac{3}{\sqrt{5}} = \cosh t.$$

De la proposition 3.23, on a

$$e^t = \sinh t + \cosh t = \frac{2}{\sqrt{5}} + \frac{3}{\sqrt{5}} = \sqrt{5} \quad \Rightarrow \quad t = \ln\left(\sqrt{5}\right) = \frac{1}{2}\ln 5.$$

On vérifie que

$$-2 = -\sqrt{5}\sinh\left(\frac{1}{2}\ln 5\right);$$

et

$$-3 = -\sqrt{5}\cosh\left(\frac{1}{2}\ln 5\right).$$

Par conséquent, $z = -2 - 3j = -\sqrt{5}je^{j\left(\frac{1}{2}\ln 5\right)}$. Un associé de z serait $z_1 = -jz = 3 + 2j = \sqrt{5}e^{j\left(\frac{1}{2}\ln 5\right)}$.

Chapitre 4

Les nombres premiers hyperboliques

4.1 Les premiers hyperboliques triviaux

Dans les complexes, les nombres premiers ont été obtenus dans l'ensemble des entiers de Gauss. Pour les nombres hyperboliques, on se ramène à un ensemble équivalent, c'est-à-dire les entiers hyperboliques

$$\mathbb{Z}[j] = \{x + yj : x, y \in \mathbb{Z}, j^2 = 1\}.$$

La suite de cette section portera sur cet ensemble.

Dans la base idempotente, il existe des valeurs de α et de β telles que $z = \alpha e + \beta e^* \notin \mathbb{Z}[j]$. Tentons de trouver pour quelles valeurs $z \in \mathbb{Z}$. On se rappelle que

$$z = \alpha e + \beta e^* = \frac{\alpha + \beta}{2} + \frac{\alpha - \beta}{2} j.$$

Les quantités $\alpha + \beta$ et $\alpha - \beta$ doivent être divisibles par 2 pour que $z \in \mathbb{Z}$. Affirmer que α et β sont divisibles par 2 dû à $\dfrac{\alpha + \beta}{2} = \dfrac{\alpha}{2} + \dfrac{\beta}{2}$ n'est pas un raisonnement valide. Voyons l'exemple suivant.

Exemple 4.1. Soit $z = 3e + 5e^*$. On calcule

$$3e + 5e^* = \left(\frac{3+5}{2}\right) + \left(\frac{3-5}{2}\right) j = \left(\frac{3}{2} + \frac{5}{2}\right) + \left(\frac{3}{2} - \frac{5}{2}\right) j = 4 - j.$$

Les nombres 3 et 5 ne sont pas divisibles par 2, mais $3 + 5$ et $3 - 5$ le sont.

Il faut donc considérer $\alpha + \beta$ et $\alpha - \beta$, et non chaque composante séparément. Ce qui nous conduit au théorème suivant.

Théorème 4.2. *Un entier hyperbolique $z = \alpha e + \beta e^* \in \mathbb{Z}[j]$ si et seulement si α et β sont de même parité.*

Démonstration. Soit $s, t \in \mathbb{Z}$.

$\Longrightarrow$) Soit $z = \alpha e + \beta e^* \in \mathbb{Z}[j]$, alors $z = \left(\frac{\alpha+\beta}{2}\right) + \left(\frac{\alpha-\beta}{2}\right) j \in \mathbb{Z}[j]$. On doit avoir $\frac{\alpha+\beta}{2} \in \mathbb{Z}$ et $\frac{\alpha-\beta}{2} \in \mathbb{Z}$. Par la définition 1.3, on a $2|(\alpha+\beta) \Rightarrow \alpha+\beta = 2k_1$ et $2|(\alpha-\beta) \Rightarrow \alpha-\beta = 2k_2$, où $k_1, k_2 \in \mathbb{Z}$. On a

$$\begin{cases} \alpha+\beta = 2k_1 \\ \alpha-\beta = 2k_2 \end{cases} \Rightarrow \begin{cases} \alpha = k_1+k_2 \\ \beta = k_1-k_2. \end{cases}$$

Vérifions la parité de α et de β.

- Si k_1 est pair et k_2 est pair, alors $k_1 = 2s$ et $k_2 = 2t$, avec $s, t \in \mathbb{Z}$. D'où

$$\begin{cases} \alpha = k_1+k_2 = 2s+2t = 2(s+t) \\ \beta = k_1-k_2 = 2s-2t = 2(s-t) \end{cases} \Rightarrow \alpha \text{ et } \beta \text{ sont pairs.}$$

- Si k_1 est pair et k_2 est impair, alors $k_1 = 2s$ et $k_2 = 2t+1$, avec $s, t \in \mathbb{Z}$. D'où

$$\begin{cases} \alpha = k_1+k_2 = 2s+2t+1 = 2(s+t)+1 \\ \beta = k_1-k_2 = 2s-2t-1 = 2(s-t)-1 \end{cases} \Rightarrow \alpha \text{ et } \beta \text{ sont impairs.}$$

- Si k_1 est impair et k_2 est pair, la preuve est similaire au cas précédent.

- Si k_1 est impair et k_2 est impair, alors $k_1 = 2s+1$ et $k_2 = 2t+1$, avec $s, t \in \mathbb{Z}$. D'où

$$\begin{cases} \alpha = k_1+k_2 = 2s+1+2t+1 = 2(s+t+1) \\ \beta = k_1-k_2 = 2s+1-2t-1 = 2(s-t) \end{cases} \Rightarrow \alpha \text{ et } \beta \text{ sont pairs.}$$

$\Longleftarrow$) Supposons que α et β sont de même parité.

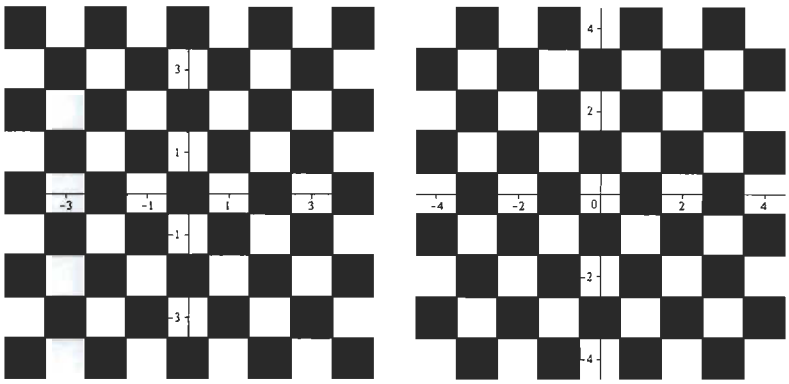
- Si α et β sont pairs, alors $\alpha = 2k_1$ et $\beta = 2k_2$, où $k_1, k_2 \in \mathbb{Z}$, et

$$z = \frac{\alpha+\beta}{2} + \frac{\alpha-\beta}{2} j = (k_1+k_2) + (k_1-k_2)j \in \mathbb{Z}[j].$$

- Si α et β sont impairs, alors $\alpha = 2k_1+1$ et $\beta = 2k_2+1$, où $k_1, k_2 \in \mathbb{Z}$, et

$$z = \frac{\alpha+\beta}{2} + \frac{\alpha-\beta}{2} j = (k_1+k_2+1) + (k_1-k_2)j \in \mathbb{Z}[j].$$

■



(A) (B)

FIGURE 4.3 – Parité des entiers hyperboliques.
(A) α et β sont pairs. (B) α et β sont impairs.

En produisant le graphique des entiers hyperboliques, on remarque un phénomène intéressant. Dans le carré 9×9 centré à l'origine, on peut regrouper les entiers hyperboliques en deux catégories : les entiers dont les composantes sont paires et ceux dont les composantes sont impaires. Superposés, les graphiques des deux catégories recouvrent le plan au complet (voir la figure 4.3). Ceci montre que les conditions du théorème précédent sont nécessaires et suffisantes pour produire $\mathbb{Z}[j]$.

Définition 4.4. *Les **unités imaginaires hyperboliques** sont* $1, -1, j, -j$.

Note : Dans les sections suivantes du présent chapitre, une unité est une unité imaginaire hyperbolique.

On note les unités imaginaires hyperboliques par le symbole J. Par exemple, si $z = J$, alors $z \in \{1, -1, j, -j\}$. La multiplication des unités est présentée à la table de Cayley 4.5. Remarquons que les unités sont obtenues avec des valeurs α et β impaires.

$\cdot$	1	-1	j	$-j$
1	1	-1	j	$-j$
-1	-1	1	$-j$	j
j	j	$-j$	1	-1
$-j$	$-j$	j	-1	1

TABLE 4.5 – Table de Cayley de la multiplication des unités imaginaires hyperboliques.

Proposition 4.6. *Les unités sont inversibles.*

Démonstration. Il suffit de remarquer que dans la diagonale de la table de Cayley on trouve le neutre multiplicatif 1. Ainsi, il existe un seul inverse pour chaque unité imaginaire. ■

Définition 4.7. *Soit $z, z_1 \in \mathbb{Z}[j]$ et $z_1 \neq 0$. Alors z_1 est un* ***diviseur*** *de z au sens hyperbolique s'il existe $z_2 \in \mathbb{Z}[j]$ tel que $z = z_1 z_2$*

Soit $z + \alpha e + \beta e^*$, $z_1 = \alpha_1 e + \beta_1 e^*$ et $z_2 = \alpha_2 e + \beta_2 e^*$. Le produit $z = z_1 z_2$ implique $\alpha = \alpha_1 \alpha_2$ et $\beta = \beta_1 \beta_2$. Par la proposition 3.12, α_1 et β_1 divisent respectivement au sens entier α et β.

Exemple 4.8. Le nombre $4e + 6e^*$ est un diviseur de $8e + 12e^*$. En effet, $8e + 12e^* = (4e + 6e^*)(2e + 2e^*)$. En notation cartésienne, $5 - j$ est un diviseur de $10 - 2j$. Par contre, $2e + 2e^*$ n'est pas un diviseur de $8e + 10e^*$, car $4e + 5e^* \notin \mathbb{Z}[j]$.

Définition 4.9. *Deux nombres hyperboliques z et w sont* ***associés*** *si $z = wJ$.*

Exemple 4.10. Les associés de 5 sont -5, $5j$ et $-5j$. Les associés de $4e + 2e^*$ sont $4e - 2e^*$, $-4e + 2e^*$ et $-4e - 2e^*$.

Autrement dit, les associés d'un nombre $z = \alpha e + \beta e^*$ sont obtenus par les combinaisons possibles des signes de α et de β. Ainsi, z et ses trois associés sont

$$\alpha e + \beta e^*,\ \alpha e - \beta e^*,\ -\alpha e + \beta e^* \text{ et } -\alpha e - \beta e^*.$$

Lemme 4.11. *Soit $z_1 = \alpha_1 e + \beta_1 e^*$ et $z_2 = \alpha_2 e + \beta_2 e^* \neq 0$. Alors z_1 et z_2 sont associés si et seulement si $\dfrac{\alpha_1}{\alpha_2} = \pm 1$ et $\dfrac{\beta_1}{\beta_2} = \pm 1$.*

Démonstration. Procédons par une double implication.

$$\begin{aligned} z_1 \text{ et } z_2 \text{ sont associés} &\Leftrightarrow z_1 = z_2 \cdot J \\ &\Leftrightarrow \frac{z_1}{z_2} = J, \text{ car } z_2 \neq 0 \\ &\Leftrightarrow \frac{\alpha_1}{\beta_1} = \pm 1 \text{ et } \frac{\alpha_2}{\beta_2} = \pm 1, \text{ par la proposition 3.12,} \end{aligned}$$

où $J \in \{1, -1, j, -j\}$. ■

Du lemme 4.11, on comprend que chaque associé d'un nombre z le divisera et que la division donnera une unité.

Les nombres premiers hyperboliques présentés dans cette section seront appelés les **nombres premiers triviaux**. On les dit triviaux car ils seront obtenus à partir de la définition usuelle de la primalité des nombres premiers.

Définition 4.12. *Soit $z \in \mathbb{Z}[j]$ un nombre différent de 0 et des unités. On dit que z est* ***premier*** *s'il n'existe aucun produit tel que $z = xy$, où $x, y \in \mathbb{Z}[j] \backslash \{1, -1, j, -j\}$. Si un tel produit existe, on dira que z est* ***composé****.*

De la négation d'un nombre composé, un nombre est premier s'il existe un produit xy où soit x ou soit y n'appartient pas à $\mathbb{Z}[j]\backslash\{1,-1,j,-j\}$. Sans perte de généralité, supposons que $x \notin \mathbb{Z}[j]\backslash\{1,-1,j,-j\}$. Ceci oblige $x = J$, d'où $z = xy = Jy$. Par définition, cela implique que z et y sont associés. Ainsi, z est premier si ses diviseurs sont les unités et ses associés. Comme chaque entier hyperbolique a une représentation unique en base idempotente, voyons de plus près le produit Jy dans cette base. Soit $z = s + tj = \alpha e + \beta e^*$, où $\alpha = s + t$ et $\beta = s - t$, où $s, t \in \mathbb{Z}$.

$$\begin{aligned}
z &= 1 \cdot y = (e + e^*)(\alpha e + \beta e^*);\\
z &= -1 \cdot y = (-e - e^*)(-\alpha e - \beta e^*);\\
z &= j \cdot y = (e - e^*)(\alpha e - \beta e^*);\\
z &= -j \cdot y = (-e + e^*)(\alpha e + \beta e^*).
\end{aligned}$$

Conséquemment, si on trouve un autre produit égal à z, on pourra affirmer que z est composé. Il convient de noter que z peut être premier que s'il est différent de 0 et des unités. On doit donc retirer les cas où $z = \alpha e + \beta e^*$ tel que $(\alpha, \beta) \in \{(0,0),(1,1),(1,-1),(-1,1),(-1,-1)\}$.

Exemple 4.13. Le nombre 3 n'est pas premier. En effet, on a $3 = (1 + 2j)(-1 + 2j)$. Le nombre $4 - 3j$ est premier car les seules possibilités sont

$$\begin{aligned}
4 - 3j = 1e + 7e^* &= (1e + 1e^*)(1e + 7e^*) = 1 \cdot (4 - 3j)\\
&= (1e - 1e^*)(1e - 7e^*) = j \cdot (-3 + 4j)\\
&= (-1e + 1e^*)(-1e + 7e^*) = -j \cdot (3 - 4j)\\
&= (-1e - 1e^*)(-1e - 7e^*) = -1 \cdot (-4 + 3j).
\end{aligned}$$

Lemme 4.14. *Un nombre hyperbolique est un premier trivial si et seulement si ses diviseurs hyperboliques sont ses associés ou les unités.*

Démonstration.

$\Longrightarrow$) Soit $z = \alpha e + \beta e^*$ un premier hyperbolique. Par contradiction, nous avons qu'il existe $z_1 = \alpha_1 e + \beta_1 e^*$ qui est un diviseur hyperbolique de z différent des associés de z et des unités. Par la définition 4.7, on a $\alpha_1 | \alpha$ et $\beta_1 | \beta$ au sens entier. Posons $z_2 = \alpha_2 e + \beta_2 e^*$, où $\alpha_2 = \alpha/\alpha_1$ et $\beta_2 = \beta/\beta_1$, de telle sorte que $z = z_1 z_2$. Comme z_1 n'est pas un associé de z, par le lemme 4.11, alors $\alpha_2 \neq \pm 1$ ou $\beta_2 \neq \pm 1$, donc z_2 n'est pas une unité. De la définition 4.9, comme z_1 n'est pas une unité, alors z_2 n'est pas un associé de z. Selon la définition 4.12, z est composé, ce qui est une contradiction. Donc, si un nombre hyperbolique est un premier trivial, alors ses diviseurs hyperboliques sont des associés ou des unités.

$\Longleftarrow$) Procédons par contraposition. On veut montrer que si un nombre hyperbolique est composé, alors il existe au moins un diviseur qui n'est pas un associé ni une unité. Par la définition 4.12, comme z est composé, alors il existe un produit $z = z_1 z_2$, où $z_1, z_2 \in \mathbb{Z}[j] \backslash \{1, -1, j, -j\}$. Comme z_1 n'est pas une unité, alors z_2 n'est pas un associé de z, et vice versa. Ainsi, il existe un produit de deux nombres qui ne sont ni des associés ni des unités. On a la conclusion souhaitée. ■

La puissance de la multiplication en base idempotente permet d'obtenir le théorème qui suit, lequel caractérise les nombres premiers triviaux dans $\mathbb{Z}[j]$.

Théorème 4.15. *Dans $\mathbb{Z}[j]$, les nombres premiers triviaux sont*

- $z = 2^k e + 2e^*$ *ou* $z = 2e + 2^k e^*$, *où* $k \in \mathbb{N}$,

et ceux de la forme

- $z = 1e + pe^*$ *ou* $z = pe + 1e^*$, *avec* $p \in \mathbb{Z} \backslash \{2\}$ *est un nombre premier,*

ainsi que tous leurs associés.

Démonstration. Soit un nombre $z \in \mathbb{Z}[j]$, différent de 0 et des unités. En base idempotente, $z = \alpha e + \beta e^*$, où $(\alpha, \beta) \notin \{(0,0), (1,1), (1,-1), (-1,1), (-1,-1)\}$. Le théorème 4.2 stipule que α et β sont de même parité. De plus, chaque diviseur doit aussi être dans $\mathbb{Z}[j]$, donc ses deux composantes idempotentes sont de même parité. Procédons par cas.

- Soit α et β pairs. Dans le cas où $(\alpha, \beta) \in \{(\alpha, 0), (0, \beta)\}$, alors $\alpha e + 0e^* = (\alpha e + 0e^*)(1e + \mu e^*)$ ou $0e + \beta e^* = (0e + \beta e^*)(\mu e + 1e^*)$, où μ est un entier impair sauf 1 ou -1. Donc z est composé par la définition 4.12. Excluons désormais toutes les possibilités avec 0, d'où $k_1 = \alpha/2 \neq 0$ et $k_2 = \beta/2 \neq 0$.

  - Soit k_1 et k_2 de même parité. Alors $z = \alpha e + \beta e^* = (2e + 2e^*)(k_1 e + k_2 e^*)$.

    1. Dans le cas où $(k_1, k_2) \notin \{(1,1), (1,-1), (-1,1), (-1,-1)\}$, on a $k_1 e + k_2 e^* \neq J$, une unité. Donc z est composé.
    2. Dans le cas où $(k_1, k_2) \in \{(1,1), (1,-1), (-1,1), (-1,-1)\}$, on a $\alpha = \pm 2$ et $\beta = \pm 2$. Sans considérer les signes, les diviseurs de 2 sont 1 et 2. On doit donc avoir $2e + 2e^* = (1e + 1e^*)(2e + 2e^*)$. On ne peut pas avoir $1e + 2e^*$ ou $2e + 1e^*$, car ils n'appartiennent pas à $\mathbb{Z}[j]$. En considérant les combinaisons de signes, on obtient que les diviseurs possibles sont le produit d'une unité et d'un associé de $\alpha e + \beta e^*$. Par le lemme 4.14, $2 = 2^1 e + 2^1 e^*$ et ses associés sont premiers.

- Soit k_1 et k_2 de parité opposée avec k_1 pair et k_2 impair.

  1. Si $k_2 \notin \{1, -1\}$, alors $z = \alpha e + \beta e^* = (1e + k_2 e^*)(\alpha e + 2e^*)$ est composé.
  2. Si $k_2 \in \{1, -1\}$, ou $\beta = \pm 2$, tout dépend des diviseurs de α.
     2.1. Si α admet un diviseur impair $k_3 \neq \pm 1$ tel que $\alpha = k_3 k_4$, où k_4 est pair, alors $\alpha e + \beta e^* = (k_3 e + k_2 e^*)(k_4 e + 2e^*)$. Et z est composé.
     2.2. Si α admet seulement ± 1 comme diviseur impair, alors $\alpha e + \beta e^* = (\pm 1e + k_2 e^*)(\pm \alpha e + 2e^*)$. Ainsi $\pm 1e + k_2 e^* = J$, et par le lemme 4.14, z est premier. Les seuls nombres ayant ± 1 comme diviseurs impairs sont les nombres de la forme $\pm 2^k$, $k \in \mathbb{N}$. Ainsi, les premiers sont $z = 2^k e + 2e^*$ et leurs associés.

  De façon similaire, en supposant k_1 impair et k_2 pair, on retrouve les nombres composés de la forme $(k_1 e + 1e^*)(2e + \beta e^*)$ et les premiers $z = 2e + 2^k e^*$ et leurs associés.

- Soit α et β impairs.

  - Si $\alpha, \beta \notin \{1, -1\}$, alors $z = \alpha e + \beta e^* = (1e + \beta e^*)(\alpha e + 1e^*)$, d'où z est composé.
  - Supposons $\alpha \in \{1, -1\}$.
    1. Si β est composé, c'est-à-dire $\beta = k_1 k_2$, avec $k_1, k_2 \notin \{1, -1\}$ et impairs, alors $z = \alpha e + \beta e^* = (1e + k_1 e^*)(\alpha e + k_2 e^*)$. Ainsi, z est composé.
    2. Si β est premier, ses seuls diviseurs sont ± 1 et $\pm \beta$. Or, $\alpha = \pm 1$. Les diviseurs hyperboliques de $\alpha e + \beta e^* = \pm 1e + \beta e^*$ sont $\{\pm 1e + 1e^*, \pm 1e - 1e^*, \pm 1e + \beta e^*, \pm 1e - \beta e^*\}$, c'est-à-dire les unités et ses associés. Conséquemment, par le lemme 4.14, z est premier.

  Si $\beta \in \{1, -1\}$, on procède de façon similaire, retrouvant les premiers de la forme $\alpha e + 1e^*$, avec α premier, et tous leurs associés.

■

Contrairement aux nombres complexes, le théorème sur les premiers hyperboliques triviaux ne requiert aucune notion préalable de la théorie des nombres (théorème des résidus, des modulos, etc.). C'est la propriété de la multiplication de la base idempotente qui permet de rapidement conclure sur l'expression de ces nombres premiers. La figure 4.16 illustre la répartition des premiers triviaux dans le plan. (Voir l'annexe C pour le code Maple.)

Puisque l'on est en mesure d'obtenir les nombres premiers hyperboliques triviaux, sommes-nous capables d'établir un théorème de l'arithmétique hyperbolique, comme c'est le cas dans les réels et les complexes ? La réponse est oui.

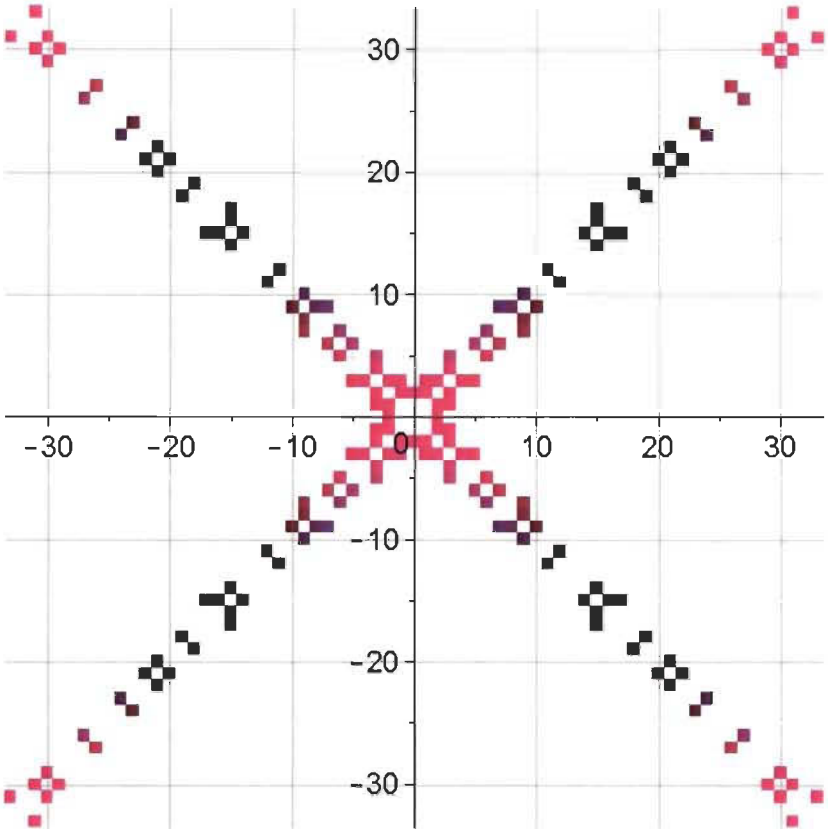


FIGURE 4.16 – Nombres premiers hyperboliques triviaux.
Les nombres premiers hyperboliques triviaux dans le carré 67×67 centré à l'origine.

Théorème 4.17 (Théorème fondamental de l'arithmétique hyperbolique)**.** *Tout nombre entier hyperbolique appartenant à $\mathbb{Z}[j]$, différent de 0 et des unités, peut s'écrire comme un produit de nombres premiers hyperboliques triviaux. Cette représentation est unique, à l'exception des associés et de l'ordre de présentation des facteurs.*

Démonstration. Soit $z = \alpha e + \beta e^*$. Selon le théorème 4.2, α et β doivent être de même parité. On applique le théorème fondamental de l'arithmétique 1.14 aux composantes α et β. Alors, les décompositions uniques en nombres premiers de α et de β peuvent s'écrire

$$\alpha = 2^t \alpha_1 \alpha_2 \cdots \alpha_r \text{ et}$$
$$\beta = 2^u \beta_1 \beta_2 \cdots \beta_s,$$

pour $t, u \in \mathbb{N} \cup \{0\}$. À noter que certains α_i ou β_i peuvent être identiques, pour $1 \leq i \leq r$ et $1 \leq j \leq s$. Posons

$$A = (\alpha_1 e + 1e^*)(\alpha_2 e + 1e^*) \cdots (\alpha_r e + 1e^*)(1e + \beta_1 e^*)(1e + \beta_2 e^*) \cdots (1e + \beta_s e^*).$$

- Si $t = 0$ et $u = 0$ (α et β sont impairs), alors $\alpha = \alpha_1\alpha_2\cdots\alpha_r$ et $\beta = \beta_1\beta_2\cdots\beta_s$, d'où

$$z = \alpha e + \beta e^* = A.$$

- Si $t = 1$ et $u = 1$ (α et β sont pairs), alors $\alpha = 2\alpha_1\alpha_2\cdots\alpha_r$ et $\beta = 2\beta_1\beta_2\cdots\beta_s$, d'où

$$z = A \cdot (2e + 2e^*).$$

- Si $t = 1$ et $u > 1$ (α et β sont pairs), alors $\alpha = 2\alpha_1\alpha_2\cdots\alpha_r$ et $\beta = 2^u\beta_1\beta_2\cdots\beta_s$, d'où

$$z = A \cdot (2e + 2^u e^*).$$

- Si $t > 1$ et $u = 1$ (α et β sont pairs), nous avons une décomposition similaire au cas précédent.

- Si $t > 1$ et $u > 1$ (α et β sont pairs), alors $\alpha = 2^t\alpha_1\alpha_2\cdots\alpha_r$ et $\beta = 2^u\beta_1\beta_2\cdots\beta_s$, d'où

$$z = A \cdot (2e + 2^{u-1}e^*) \cdot (2^{t-1}e + 2e^*).$$

Tous les α_i et β_j sont premiers et impairs, alors, en accord avec le théorème 4.15, on a décomposé $z = \alpha e + \beta e^*$ en un produit de nombres premiers hyperboliques triviaux.

L'unicité de la décomposition en nombres premiers hyperboliques triviaux vient de l'unicité de la représentation en base idempotente d'un nombre hyperbolique. S'il existe deux décompositions en premiers triviaux pour un même entier hyperbolique, en les multipliant, on obtient deux décompositions différentes pour un entier réel (soit pour α et/ou pour β). Cela contredit l'unicité de la décomposition en entiers premiers de α et/ou de β. La décomposition en premiers triviaux est donc unique. La seule différence est qu'en ajoutant les associés, on change le signe de certains α_i et/ou β_j. Cela ne change pas la primalité d'un nombre entier ou hyperbolique. Comme la multiplication est commutative, l'ordre des facteurs n'importe pas dans la décomposition. ■

4.2 Les premiers hyperboliques non triviaux

Y aurait-il une sous-classe de $\mathbb{Z}[j]$ qui admettrait des nombres premiers autres que triviaux ? Évidemment, il faut donner une définition de ces potentiels nouveaux nombres premiers. Regardons ce qui se produit lorsque l'on considère la classe des entiers tels que $|z|_h > 0$ avec $|z|_h^2 = x^2 - y^2 = \alpha\beta > 0$.

Définition 4.18. *En base idempotente, l'ensemble des hyperboliques ayant $\alpha, \beta > 0$ est noté $\mathbb{D}^+$ et l'ensemble des hyperboliques ayant $\alpha, \beta < 0$ est noté $\mathbb{D}^-$ de la façon suivante :*

$$\mathbb{D}^+ = \{\alpha e + \beta e^* : \alpha > 0, \beta > 0\};$$
$$\mathbb{D}^- = \{\alpha e + \beta e^* : \alpha < 0, \beta < 0\}.$$

Ainsi, $\{z = x+yj : x^2-y^2 > 0\} = \mathbb{D}^+ \cup \mathbb{D}^-$. Cet ensemble est fermé sous la multiplication. En effet, si $z_1 = \alpha_1 e + \beta_1 e^*$ et $z_2 = \alpha_2 e + \beta_2 e^*$, alors

$$z_1 \in \mathbb{D}^+, z_2 \in \mathbb{D}^+ \Rightarrow \alpha_1\alpha_2 > 0 \text{ et } \beta_1\beta_2 > 0 \Rightarrow z_1 z_2 \in \mathbb{D}^+;$$
$$z_1 \in \mathbb{D}^+, z_2 \in \mathbb{D}^- \Rightarrow \alpha_1\alpha_2 < 0 \text{ et } \beta_1\beta_2 < 0 \Rightarrow z_1 z_2 \in \mathbb{D}^-;$$
$$z_1 \in \mathbb{D}^-, z_2 \in \mathbb{D}^+ \Rightarrow \alpha_1\alpha_2 < 0 \text{ et } \beta_1\beta_2 < 0 \Rightarrow z_1 z_2 \in \mathbb{D}^-;$$
$$z_1 \in \mathbb{D}^-, z_2 \in \mathbb{D}^- \Rightarrow \alpha_1\alpha_2 > 0 \text{ et } \beta_1\beta_2 > 0 \Rightarrow z_1 z_2 \in \mathbb{D}^+.$$

Nous allons définir une nouvelle classe de nombres, appelés les **nombres premiers non triviaux** et qui appartiennent à $\mathbb{D}^+ \cup \mathbb{D}^-$. On motive le choix de l'appellation entre autres par leur définition.

Définition 4.19. *Un nombre entier hyperbolique $z = \alpha e + \beta e^* \in \mathbb{D}^+ \cup \mathbb{D}^-$ est un **premier non trivial** si α et β sont des entiers premiers.*

Il faut noter que la restriction de $\mathbb{Z}[j]$ à l'ensemble $\mathbb{D}^+ \cup \mathbb{D}^-$ entraîne quelques modifications. Il n'existe désormais plus que deux unités, à savoir $1e + 1e^* = 1$ et $-1e - 1e^* = -1$, car les signes doivent être identiques. Cela a aussi comme répercussion que chaque nombre a un seul associé (de signe contraire).

Exemple 4.20. Les nombres $3e + 5e^*$, $-7e - 23e^*$ et $-2e - 2e^*$ sont des premiers non triviaux.

L'ensemble contenant tous les premiers non triviaux, noté $\mathbb{P}$, sera

$$\mathbb{P} = \{z = \alpha e + \beta e^* : z \in \mathbb{D}^+ \cup \mathbb{D}^- \text{ et } \alpha, \beta \text{ sont premiers}\}.$$

La sélection de ce symbole reflète le caractère premier en chacune des deux composantes.

Regardons ce qui se produit pour des nombres de la forme $\pm\alpha e \pm 1e^*$ ou $\pm 1e \pm \beta e^*$, avec α, β impairs. Sans perte de généralité, concentrons-nous sur $\pm\alpha e \pm 1e^*$. Par le théorème fondamental de l'arithmétique 1.14, supposons $\alpha = 2^0\alpha_1^{\mu_1}\alpha_2^{\mu_2}\cdots\alpha_s^{\mu_s}$, où $\mu_i \in \mathbb{N}$. Les diviseurs de ± 1 sont ± 1 et les diviseurs de α sont toutes les combinaisons parmi les exposants et les signes des α_i. Tous les diviseurs de $\pm\alpha e \pm 1e^*$ sont donc de la forme

$$\pm\alpha_1^{\lambda_1}\alpha_2^{\lambda_2}\cdots\alpha_s^{\lambda_s} e \pm 1e^*,$$

où $0 \leq \lambda_i \leq \mu_i$. Comme ± 1 n'est pas un nombre premier, dès lors $\pm\alpha_1^{\lambda_1}\alpha_2^{\lambda_2}\cdots\alpha_s^{\lambda_s}e \pm 1e^* \notin \mathbb{P}$.

Pour cette raison, on enlèvera de l'ensemble $\mathbb{D}^+ \cup \mathbb{D}^-$ les nombres hyperboliques situés sur les droites $y = x + 1$, $y = x - 1$, $y = -x + 1$ et $y = -x - 1$ (en notation cartésienne), ou encore $\alpha = \pm 1$ et $\beta = \pm 1$ (en notation idempotente). L'ensemble actualisé donne

$$\bowtie := \{z = \alpha e + \beta e^* : z \in \mathbb{D}^+ \cup \mathbb{D}^-, \alpha \neq \pm 1, \beta \neq \pm 1\}.$$

Le symbole est apparenté à la forme des nombres z satisfaisant $x^2 - y^2 > 0$. La restriction de l'ensemble n'enlève aucun point de $\mathbb{P}$, c'est-à-dire que $\mathbb{P} \subset \bowtie \subset \mathbb{D}^+ \cup \mathbb{D}^-$. La figure 4.21 illustre les ensembles $\mathbb{P}$, $\bowtie$ et $\mathbb{D}^+ \cup \mathbb{D}^-$. (Voir l'annexe D pour le code Maple.)

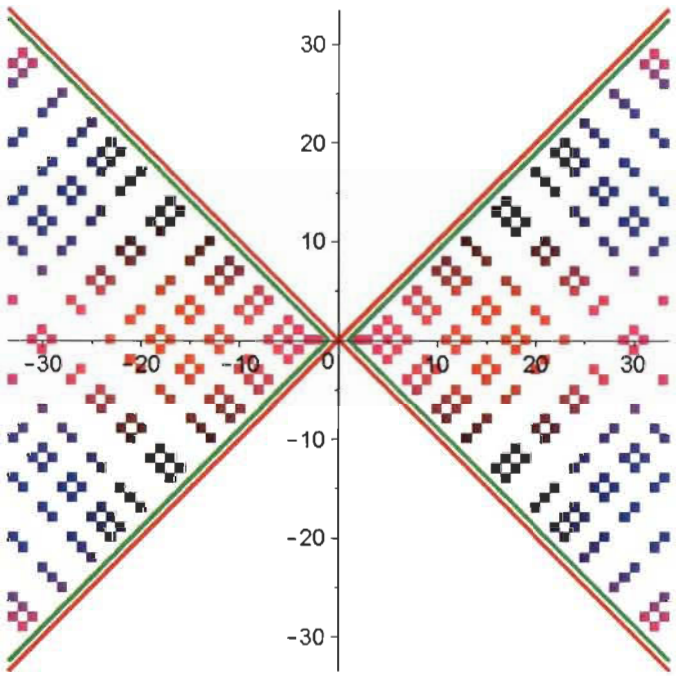


FIGURE 4.21 – Nombres premiers hyperboliques non triviaux.
Les droites $y = x$ et $y = -x$ sont les hyperboliques non inversibles.
Les demi-droites $y = x + 1$, $y = x - 1$, $y = -x + 1$ et $y = -x - 1$
sont les nombres hyperboliques de la forme $\pm\alpha e \pm 1e^*$ et $\pm 1e \pm \beta e^*$.

Être premier fait référence à avoir un produit d'une unité et d'un associé. Dans les premiers triviaux, on décomposait n'importe quel entier hyperbolique en facteurs de premiers triviaux. Est-il possible de faire des décompositions similaires en n'ayant que des facteurs appartenant à $\mathbb{P}$? Notons que la définition 4.7 sur les diviseurs reste la même dans les premiers non triviaux. Parmi les décompositions possibles, si le seul facteur appartenant à $\mathbb{P}$ est lui-même ou son associé, la définition est similaire à celle d'un nombre premier usuel. Cependant, dans $\mathbb{D}^+ \cup \mathbb{D}^-$, il y a les facteurs avec ± 1 que l'on ne veut pas considérer, mais qui sont enlevés de $\bowtie$. Conséquemment, les nombres seront premiers dans $\bowtie$ s'ils ont seulement

eux-mêmes et leur associé comme diviseur appartenant à $\mathbb{P}$. Ils sont dits non triviaux, car on modifie la définition même de la primalité, restreignant les diviseurs à $\mathbb{P}$ et non à l'ensemble en entier. Ci-dessous nous avons une caractérisation des premiers non triviaux qui permet de comprendre l'ampleur de l'appellation de ces nombres introduits dans ce mémoire.

Théorème 4.22. *Les nombres dans $\mathbb{P}$ sont les seuls nombres de l'ensemble $\bowtie$ à admettre comme diviseurs dans $\bowtie$ uniquement eux-mêmes et leur associé appartenant à $\mathbb{P}$.*

Démonstration. Soit $z = \alpha e + \beta e^* \in \bowtie$. Il est évident que $z|z$, ainsi z admet lui-même comme diviseur dans $\bowtie$. Par le lemme 4.11, tout associé de z le divisera aussi. Si $z \notin \mathbb{P}$, alors z est son propre diviseur, mais n'appartient pas à $\mathbb{P}$. Si $z \in \mathbb{P}$, alors α et β sont des entiers premiers de même signe.

- Si $\alpha = \beta = \pm 2$, les diviseurs sont $\pm 1e \pm 1e^*$ et $\pm 2e \pm 2e^*$. Dans $\bowtie$, seuls $\pm 2e \pm 2e^* \in \mathbb{P}$.
- Si α et β sont impairs, il n'y a que ± 1 et $\pm a$ ou ± 1 et $\pm\beta$ comme diviseurs entiers de α et de β. Puisque l'on a retiré de $\bowtie$ les hyperboliques de la forme $\pm\alpha e \pm 1e^*$ et $\pm 1e \pm \beta e^*$, il demeure seulement $\pm\alpha e \pm \beta e^* \in \mathbb{P}$ comme diviseurs de z.

■

Théorème 4.23. *Il n'existe pas de théorème fondamental de l'arithmétique hyperbolique avec les premiers non triviaux.*

Démonstration. Il faut montrer qu'il existe un nombre appartenant à $\mathbb{D}^+ \cup \mathbb{D}^-$ qui n'a pas de décomposition avec uniquement des premiers non triviaux. Prenons le nombre $2e + 6e^*$. Les diviseurs de 2 sont $\pm 1, \pm 2$ et ceux de 6 sont $\pm 1, \pm 2, \pm 3, \pm 6$. Les diviseurs de $2e + 6e^*$ sont :

$$\pm 1e \pm 1e^*, \qquad \pm 1e \pm 3e^*, \qquad \pm 2e \pm 2e^*, \qquad \pm 2e \pm 6e^*.$$

Le seul premier non trivial est $\pm 2e \pm 2e^*$. Il n'existe aucun $\mu e + \lambda e^* \in \mathbb{P}$ tel que $2e + 6e^* = (\pm 2e \pm 2e^*)(\mu e + \lambda e^*)$. Aucune décomposition en premiers non triviaux n'est possible. Ainsi, chaque nombre de $\mathbb{D}^+ \cup \mathbb{D}^-$ n'a pas forcément une décomposition en premiers non triviaux. ■

Il est même possible de compter le nombre de diviseurs hyperboliques appartenant à $\mathbb{P}$. Juste avant, montrons ce théorème.

Théorème 4.24. *Soit $z = \alpha e + \beta e^*$, où α et β sont pairs. Soit k_1 et k_2 les exposants du facteur 2 dans les décompositions en entiers premiers de α et de β. Si $k_1 = 1$ ou $k_2 = 1$, alors $2e + 2e^*$ ne sera pas un diviseur de z.*

Note : Dans ce théorème, le « ou » est exclusif.

Démonstration. Procédons par cas.

- Si $k_1 \geq 2$ et $k_2 \geq 2$, alors $\frac{\alpha}{2}$ et $\frac{\beta}{2}$ sont pairs, d'où $\alpha e + \beta e^* = (2e + 2e^*)\left(\frac{\alpha}{2}e + \frac{\beta}{2}e^*\right)$. Donc $2e + 2e^*$ est un diviseur de z.
- Si $k_1 = 1$ et $k_2 = 1$, alors $\frac{\alpha}{2}$ et $\frac{\beta}{2}$ sont impairs, d'où $\alpha e + \beta e^* = (2e + 2e^*)\left(\frac{\alpha}{2}e + \frac{\beta}{2}e^*\right)$. Donc $2e + 2e^*$ est un diviseur de z.
- Si $k_1 = 1$ et $k_2 \geq 2$, alors $\frac{\alpha}{2}$ est impair et $\frac{\beta}{2}$ est pair, alors $\frac{\alpha}{2}e + \frac{\beta}{2}e^* \notin \mathbb{Z}[j]$. Donc $2e + 2e^*$ n'est pas un diviseur de $\alpha e + \beta e^*$.
- Si $k_1 \geq 2$ et $k_2 = 1$, le cas est similaire au cas précédent.

■

Exemple 4.25. Trouvons le nombre de diviseurs hyperboliques de $100e + 120e^*$. Commençons par décomposer 100 et 120 en utilisant le théorème fondamental de l'arithmétique comme suit :

$$100 = 2^2 5^2;$$
$$120 = 2^3 3^1 5^1.$$

Par les théorèmes 4.2 et 4.24, sans compter les associés, le seul diviseur appartenant à $\mathbb{P}$ ayant ses composantes paires est $2e + 2e^*$. Les autres sont des combinaisons parmi les entiers premiers impairs. Ainsi, les diviseurs hyperboliques non triviaux sont :

$$2e + 2e^*, 5e + 3e^*, 5e + 5e^*.$$

En comptant maintenant les associés (le changement de signe), il y en a $3 \times 2 = 6$.

En fait, lorsque l'on veut trouver les diviseurs non triviaux, il faut utiliser chaque nombre entier premier et appliquer l'exposant 1, sinon on a un entier composé et le diviseur hyperbolique n'appartiendra pas à $\mathbb{P}$. Reprenons la démarche avec l'exemple donné dans le théorème 4.23.

Exemple 4.26. Soit le nombre $2e + 6e^*$. Le théorème de l'arithmétique nous donne

$$2 = 2^1;$$
$$6 = 2^1 3^1.$$

Ainsi, $2e + 2e^*$ est un diviseur hyperbolique appartenant à $\mathbb{P}$. Par contre, même si $3|6$, il n'y a pas de facteur premier impair dans la décomposition de 2. Il n'y a donc pas de diviseurs hyperboliques non triviaux avec des composantes impaires. Alors, en incluant les associés, $2e + 6e^*$ a deux diviseurs hyperboliques non triviaux : $2e + 2e^*$ et $-2e - 2e^*$.

4.3 La conjecture de Goldbach

Christian Goldbach est un mathématicien russe ayant vécu de 1690 à 1764. Il est né à Königsberg, la ville connue pour son fameux problème mathématique sur les ponts. Goldbach a correspondu avec d'autres grands mathématiciens [7]. Entre autres, il a écrit à Euler lui faisant mention dans une lettre envoyée en 1742 d'une conjecture qui allait semble-t-il traverser de nombreuses décennies sans être démontrée.

Conjecture 4.27 (Goldbach). *Tout nombre pair supérieur à 2 peut s'exprimer comme la somme de deux nombres premiers.*

Exemple 4.28. Les nombres 22, 112 et 236 respectent la conjecture, car $22 = 11 + 11$, $112 = 71 + 41$ et $236 = 233 + 3$.

Si l'on écrit les hyperboliques $\mathbb{P}$ en notation cartésienne, on trouve

$$z = \alpha e + \beta e^* = \left(\frac{\alpha + \beta}{2}\right) + \left(\frac{\alpha - \beta}{2}\right) j.$$

Le choix de l'ensemble $\mathbb{P}$ n'est pas dénué de sens. Les coordonnées x et y de $z = x + yj$ deviennent

$$\mathrm{Re}(z) = x = \frac{\alpha + \beta}{2} \Rightarrow 2x = \alpha + \beta;$$
$$\mathrm{Hy}(z) = y = \frac{\alpha - \beta}{2} \Rightarrow 2y = \alpha - \beta.$$

Comme α et β sont premiers et que $2x$ et $2y$ sont des nombres pairs, les résultats précédents font apparaître la conjecture de Goldbach ainsi que la conjecture symétrique appelée la conjecture de Polignac.

Vieille de près de 275 ans, si la conjecture de Goldbach s'avère être vraie, nous aurions que tout $x \geq 2$ possèderait une somme de deux entiers premiers équivalente à $2x$. Ce serait aussi valide pour tout entier $x \leq -2$. En effet, il suffit de multiplier la somme par -1. Si

$2x = \alpha + \beta > 0$, alors $-2x = 2 \cdot -x = -\alpha + (-\beta) < 0$. Donc pour tout $x \geq 2$ ou $x \leq -2$ donné, il existerait un nombre $z \in \mathbb{P}$ tel que $z = x + yj$. Ce qui conduit à un théorème faisant le lien entre les premiers hyperboliques non triviaux et la conjecture de Goldbach.

Théorème 4.29. *La conjecture de Goldbach est vraie si et seulement si*

$$\mathrm{Re}(\mathbb{P}) = \mathbb{Z}\backslash\{-1, 0, 1\}.$$

Démonstration.

$\Longrightarrow$) Supposons la conjecture vraie. Procédons par cas pour démontrer cette égalité d'ensemble.

- Soit $x \in \mathrm{Re}(\mathbb{P})$. Il existe $z = \alpha e + \beta e^* \in \mathbb{P} \subset \mathbb{D}^+ \cup \mathbb{D}^-$ tel que $\mathrm{Re}(z) = x = \dfrac{\alpha + \beta}{2} \in \mathbb{Z}$. On sait que α et β sont premiers, de même parité et de même signe. Si $\alpha, \beta \geq 2$, alors $x \geq 2$, et si $\alpha, \beta \leq -2$, alors $x \leq -2$. D'où $x \in \mathbb{Z}\backslash\{-1, 0, 1\}$.

- Soit $u \in \mathbb{Z}\backslash\{-1, 0, 1\}$. En multipliant par 2, $2u \in 2\mathbb{Z}\backslash\{-2, 0, 2\}$, et $2u$ respecte les conditions de la conjecture de Goldbach. Alors, il existe deux entiers premiers μ et λ tels que $2u = \mu + \lambda$, d'où $u = \dfrac{\mu + \lambda}{2}$. Ce qui implique que $u \in \mathrm{Re}(\mathbb{P})$, car il existe $w \in \mathbb{P}$ tel que $w = u + vj = \left(\dfrac{\mu + \lambda}{2}\right) + \left(\dfrac{\mu - \lambda}{2}\right) j$.

$\Longleftarrow$) Supposons que $\mathrm{Re}(\mathbb{P}) = \mathbb{Z}\backslash\{-1, 0, 1\}$. Soit un nombre pair $p > 2$ ou $p < -2$. On peut réécrire p en fonction d'un entier, en particulier $p = 2s$. C'est-à-dire que $p \in 2\mathbb{Z}\backslash\{-2, 0, 2\}$, ce qui implique $s \in \mathbb{Z}\backslash\{-1, 0, 1\}$. Par hypothèse, $s \in \mathrm{Re}(\mathbb{P})$. Donc il existe $r \in \mathbb{P}$ tel que $r = s + tj = \left(\dfrac{\eta + \xi}{2}\right) + \left(\dfrac{\eta - \xi}{2}\right) j$. D'où $s = \dfrac{\eta + \xi}{2}$ ou $2s = \eta + \xi$ et par définition de $\mathbb{P}$, $p = 2s$ est la somme de deux premiers. La conjecture de Goldbach est respectée, car p est arbitraire. ■

Tout nombre dans $\bowtie$ doit avoir ses composantes de même signe : positif s'il appartient à $\mathbb{D}^+$ et négatif s'il est dans $\mathbb{D}^-$. Ainsi, le graphique des premiers hyperboliques non triviaux illustre la conjecture. En prenant l'opposé de x, on applique une symétrie par rapport à l'axe y ; les coordonnés (x, y) de tout point $z \in \mathbb{P} \cap \mathbb{D}^+$ deviennent $(-x, y)$. La partie réelle ne peut pas être 0, 1, -1, en effet $2 \cdot 0 = 0$ et $2 \cdot \pm 1 = \pm 2$ ne sont pas des nombres pairs supérieurs à 2 ou inférieurs à -2.

La conjecture de Goldbach a été démontrée pour des entiers allant jusqu'à $4 \cdot 10^{18}$ [8]. En d'autres termes, le graphique des $z \in \bowtie$ contient assurément un point $z \in \mathbb{P}$ pour chaque x tel que $2 \leq x \leq 2 \cdot 10^{18}$ ou $-2 \cdot 10^{18} \leq x \leq -2$. Or, si l'on est capable de démontrer qu'il n'y pas de $z \in \mathbb{P}$ pour un certain $x \in \mathbb{Z}\backslash\{-1, 0, 1\}$ en dehors de ces deux intervalles, on aura démontré que la conjecture de Goldbach est fausse.

Regardons ce qui se produit avec la composante hyperbolique. Alphonse de Polignac est un mathématicien français ayant vécu dans les années 1800. Sa conjecture, symétrique à celle de Goldbach, est : « Tout nombre pair est la différence de deux nombres premiers consécutifs d'une infinité de façons » ([21] et [25]). Elle fut reprise par Hardy et Littlewood en 1923 [1]. Dans le présent ouvrage, nous utiliserons une conjecture plus faible que la conjecture de Polignac.

Conjecture 4.30 (Polignac faible)**.** *Chaque nombre pair est la différence de deux nombres premiers.*

Il a été calculé précédemment que $2y = \alpha - \beta$. Le nombre $2y$ étant pair pour tout $y \in \mathbb{Z}$, $2y$ est donc la différence de deux nombres premiers. Il faut faire attention, car dans la conjecture originale, deux entiers premiers peuvent respecter la différence voulue et ne pas être consécutifs ! Il y a un nom spécial pour les nombres premiers dont la différence vaut 2, 4 et 6 ; ce sont les premiers jumeaux [26], cousins et sexys respectivement lorsque $y = 1$, $y = 2$ et $y = 3$. Voyons quelques cas.

$$\begin{array}{lccccccccccc} \text{Jumeaux} & 2 & = & 5-3 & = & 7-5 & = & 13-11 & = & 19-17 & = & \ldots \\ \text{Cousins} & 4 & = & 7-3 & = & 11-7 & = & 17-13 & = & 23-19 & = & \ldots \\ \text{Sexys} & 6 & = & 11-5 & = & 13-7 & = & 17-11 & = & 19-13 & = & \ldots \end{array}$$

Les nombres 3 et 7 sont des premiers cousins, mais ils ne sont pas des premiers consécutifs, alors ils ne respectent pas la conjecture originale de Polignac.

Théorème 4.31. *Tout nombre pair est la différence de deux entiers premiers si et seulement si*

$$\mathrm{Hy}(\mathbb{P}) = \mathbb{Z}.$$

Ce théorème se démontre de la même façon que le théorème 4.29.

Tous les nombres pairs sont atteints lorsque $y \in \mathbb{Z}$ dans l'égalité $2y = \alpha - \beta$. Ceci implique $\mathrm{Hy}(\mathbb{P}) = \dfrac{\alpha - \beta}{2} = y \in \mathbb{Z}$. Si $\alpha \geq \beta$, alors $\dfrac{\alpha - \beta}{2} \geq 0$; on atteint des valeurs où $y \geq 0$. Inversement, si $\alpha < \beta$, alors $y < 0$. Similairement à la conjecture de Goldbach, si l'on est capable de trouver un y qui n'a aucune ou un nombre fini de différences, alors on aura démontré que la conjecture de Polignac est fausse.

D'un point de vue géométrique, les différences peuvent être représentées par des triangles isocèles dont les sommets sont les $z \in \mathbb{P}$. Les sommets de la base du triangle sont sur la droite $y = 0$, c'est-à-dire qu'ils sont des entiers premiers. Le troisième sommet se retrouve sur la droite $y = k$ et à ce sommet est formé un angle droit.

En prenant un x arbitraire, on sait qu'il existera au moins un point $z = x + yj \in \mathbb{P}$ par la conjecture de Goldbach tel que $\mathrm{Re}(z) = x$. Comme on veut une différence de $2y$ entre α et β, on doit considérer les sommets $(x + y, 0)$ et $(x - y, 0)$. Le sommet qui n'est pas sur la base

se retrouvera au point (x, y) si, en effet, $\alpha = x + y$ et $\beta = x - y$ sont deux nombres premiers. Pour respecter la conjecture de Polignac, il ne doit pas y avoir d'autres points $z \in \mathbb{P}$ *dans ou sur* le triangle isocèle. La figure 4.32 représente la conjecture de Polignac.

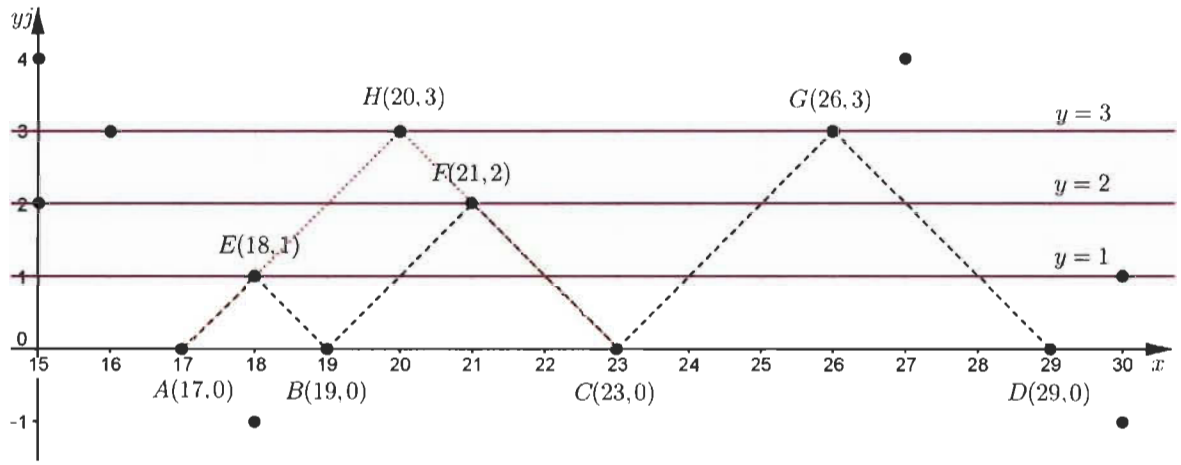


FIGURE 4.32 – Représentation de la conjecture de Polignac.
Les premiers jumeaux et cousins sont respectivement exemplifiés par les triangles AEB et BFC, tandis que les premiers sexys sont représentés par les triangles AHC et CGD. Seul AHC ne respecte pas la conjecture de Polignac, car 17 et 23 ne sont pas des premiers consécutifs. Le point $E(18, 1)$ est le nombre $19e + 17e^*$, $F(21, 2)$ est $23e + 19e^*$ et $G(26, 3)$ est $29e + 23e^*$.

En considérant la droite $y = 0$, on obtient les z tels que $0 = \alpha - \beta \Rightarrow \alpha = \beta$. Dans cette situation, on a, par exemple, $3e + 3e^* = 3$ et $7e + 7e^* = 7$. Ainsi, sur l'axe des abscisses, on retrouve la répartition des nombres entiers premiers au travers des nombres premiers non triviaux $\mathbb{P}$. Puisqu'il y a une infinité de nombres entiers premiers, alors il y a une infinité de $z \in \mathbb{P}$ sur la droite $y = 0$.

4.3.1 Suites particulières

Sans perte de généralité, attardons-nous au sous-ensemble tel que $\alpha > 1$ et $\beta > 1$ (le côté droit de $\bowtie$). On s'intéresse au nombre de points $z \in \mathbb{P}$ existants pour un x donné. On appelle une *partition de Goldbach* [24] d'un nombre pair $2x$ tout couple d'entiers premiers (α, β) tels que $2x = \alpha + \beta$. Si l'ordre de présentation de α et de β n'a pas d'importance, on a que $\alpha + \beta$ est aussi $\beta + \alpha$. On appelle ce dénombrement la fonction $r(2x)$ pour un x fixé. Par contre, si l'ordre de présentation est important, on doit considérer $\alpha + \beta$ différent de $\beta + \alpha$. C'est la fonction $R(2x)$, déductible à l'aide de $r(2x)$:

$$R(2x) = \begin{cases} 2 \cdot r(2x) - 1, & \text{si } x \text{ est premier ;} \\ 2 \cdot r(2x), & \text{si } x \text{ est composé.} \end{cases}$$

Sur le site *The On-Line Encyclopedia of Integer Sequences* de N. J. A. Sloane, on trouve une suite (A045917) créée à partir de la fonction $r(2x)$ [27] et une suite (A035026) pour la fonction $R(2x)$ [28]. En fait, A035026 est la suite A002372 (de titre « Goldbach conjecture: number of decompositions of 2n into ordered sums of two odd primes »).

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
$r(2x)$	1	1	1	2	1	2	2	2	2	3	3	3	2	3	2	4	4	2	3	...

TABLE 4.33 – Suite A045917 associée à la fonction $r(2x)$.

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
$R(2x)$	1	1	2	3	2	3	4	4	4	5	6	5	4	6	4	7	8	3	6	...

TABLE 4.34 – Suite A035026 associée à la fonction $R(2x)$.

Il est possible de dénombrer le nombre de points à la verticale, car on borne par $y = x$ pour la fonction $r(2x)$ et par $y = \pm x$ pour la fonction $R(2x)$. On ne peut pas dénombrer les points à l'horizontale, car $\alpha - \beta$ n'est pas borné. Il va sans dire que la soustraction peut autant donner 2, 4 ou bien 6, même si α et β sont de très grands entiers premiers consécutifs. S'il existe un nombre fini de soustractions, cela voudrait dire que la conjecture originale de Polignac est fausse.

Exemple 4.35. Le nombre 24 (ici $x = 12$) a 3 partitions : $19 + 5$, $17 + 7$ et $13 + 11$. Ainsi, $r(24) = 3$. Si on considère l'ordre, on a $R(24) = 2 \cdot r(24) = 6$. En effet, on inverse l'ordre de présentation des deux entiers : $5 + 19$, $7 + 17$ et $11 + 13$.

Exemple 4.36. Le nombre 34 (ici $x = 17$) a 4 partitions : $31 + 3$, $29 + 5$, $23 + 11$ et $17 + 17$. Ainsi, $r(34) = 4$. Si on considère l'ordre, on a $R(24) = 2 \cdot r(34) - 1 = 7$. En effet, on inverse l'ordre de présentation des deux entiers, mais $17 + 17$ est présent 2 fois, d'où le -1 dans la fonction $R(34)$.

Les figures 4.37 et 4.38 illustrent les exemples 4.35 et 4.36.

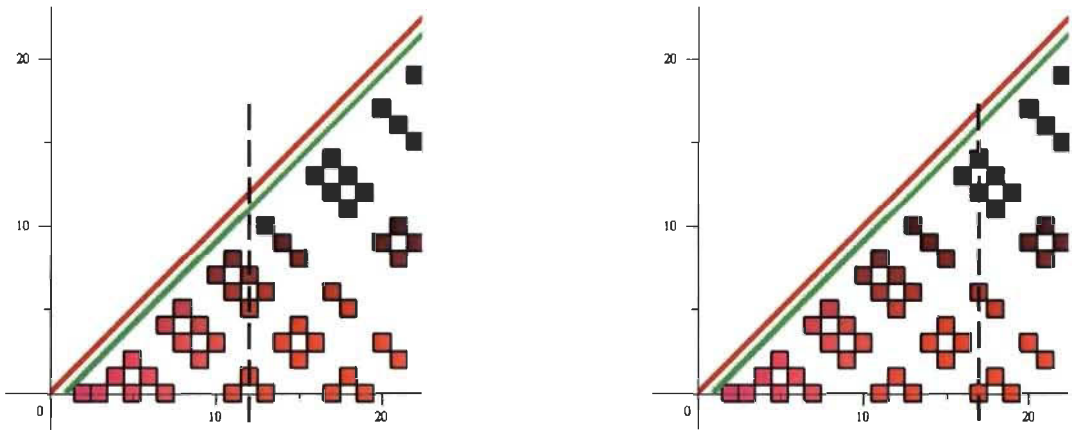


FIGURE 4.37 – Exemplifications des fonctions $r(24)$ et $r(34)$ avec l'ensemble $\mathbb{P}$.

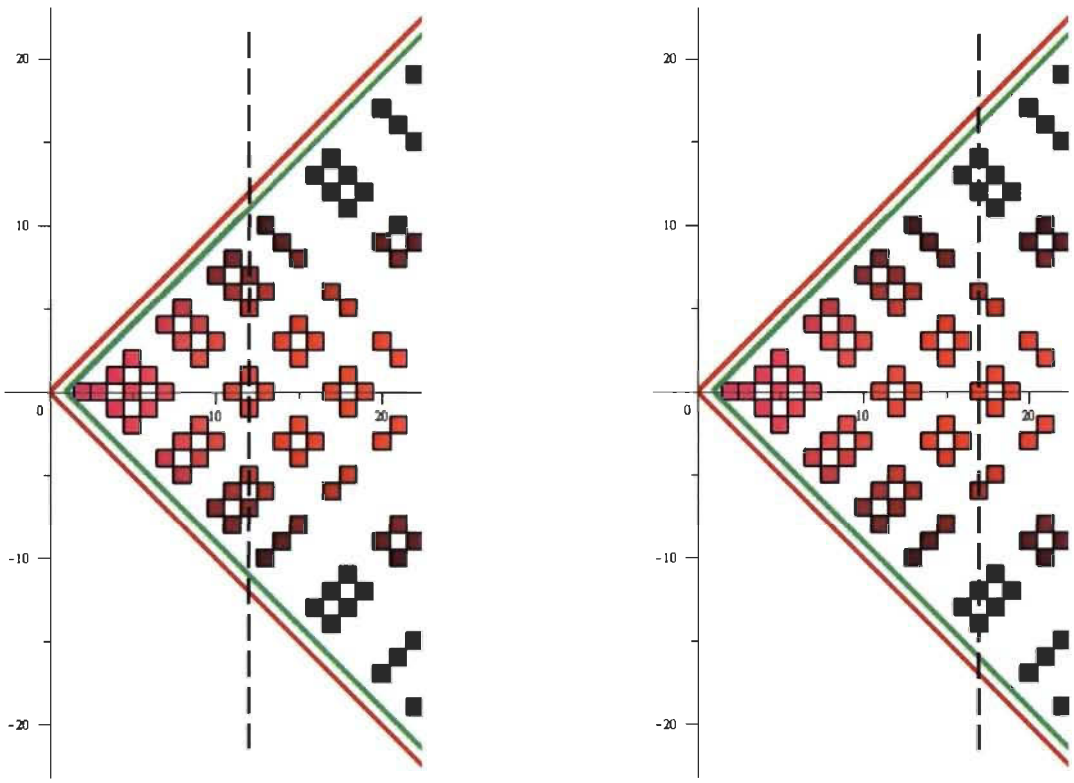


FIGURE 4.38 – Exemplifications des fonctions $R(24)$ et $R(34)$ avec l'ensemble $\mathbb{P}$.

Conclusion

L'objet de ce mémoire était de traiter des nombres premiers. Il a d'abord été sujet des nombres premiers réels dans le chapitre 1. Un retour aux définitions primaires et aux théorèmes était nécessaire pour comprendre leur utilité dans le *théorème fondamental de l'arithmétique* dans les réels. Ces mêmes définitions et théorèmes ont été au coeur d'une démarche qui s'est répétée dans les chapitres 2 et 3.

Au chapitre 2, tout ce qui a été fait dans le chapitre 1 a été considéré dans les complexes. Entre autres, l'accent est mis sur les théorèmes 2.24 et 2.42.

Par la suite, au chapitre 3, de nouveaux nombres similaires aux complexes (de par leur construction et leurs opérations arithmétiques) ont été étudiés : les nombres hyperboliques. Le théorème de l'arithmétique hyperbolique a été démontré et simplifié grâce à l'artifice de calcul qu'est la base idempotente. Tout comme dans les complexes, une étude sommaire des fonctions hyperboliques a conduit à la représentation polaire d'un nombre. Un travail ultérieur permettrait d'accroître la compréhension de ces fonctions hyperboliques, ainsi que l'application de ces fonctions aux nombres hyperboliques.

Finalement, au chapitre 4, de nouvelles opérations avec la base idempotente ont permis de trouver les nombres premiers hyperboliques triviaux d'une façon bien plus directe que cela a été fait dans les complexes. Puis, en définissant les non triviaux, un lien intéressant est apparu entre ces nombres, la conjecture de Goldbach et la conjecture de Polignac.

En comparaison des premiers réels, les premiers complexes n'ont pas de formule de répartition connue à ce jour. Ils suivent deux règles bien définies présentées au théorème 2.45, mais semblent être « aléatoires » dans le plan complexe. Bien que les premiers réels ne suivent pas de règle autre que la définition usuelle de la primalité, il est toutefois possible d'estimer le nombre de nombres premiers. J. Hadamard et C. J. de la Vallée-Poussin ont indépendamment démontré par des méthodes d'analyse complexe un théorème concernant la distribution asymptotique des nombres premiers [1]. Ce théorème porte le nom de « théorème des nombres premiers » et consiste à approximer le nombre de premiers précédant un entier x. La fonction donnant le nombre exact de nombres premiers avant x est notée $\pi(x)$. Le théorème lie cette fonction à son approximation de la façon suivante : $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$. Autrement dit, plus x est grand, plus $\frac{x}{\ln x}$ donne une meilleure approximation du nombre de

premiers avant x. Dans les hyperboliques, cette répartition est tout autant inconnue dans les triviaux que dans les non triviaux. Cependant, étant donné que les premiers non triviaux sont en fait les premiers réels en deux dimensions (une composante α et une autre β), il pourrait être intéressant de voir comment il est possible d'appliquer les résultats de la distribution des nombres premiers sur cette nouvelle classe de nombres introduite dans cet ouvrage.

Bibliographie

[1] DE KONINCK, Jean-Marie, et Armel MERCIER. *Introduction à la théorie des nombres*, Mont-Royal (Québec), Modulo, 1994, 254 p.

[2] OUELLET, Gilles. *Calcul 3 : théorie, exemples, problèmes*, Sainte-Foy (Québec), Le Griffon d'argile, 1984, 430 p.

[3] BOYE, Anne, et Commision Inter-IREM épistémologie (France) et al. *Images, imaginaires, imaginations : une perspective historique pour l'introduction des nombres complexes*, Paris (France), Ellipses-Marketing, 1998, 400 p.

[4] AGARWAL, Ravi P., Kanishka PERERA et Sandra PINELAS. *An introduction to complex analysis*, New-York (USA), Springer, 2011, 331 p.

[5] KANTOR, I. L., et A. S. SOLODOVNIKOV. *Hypercomplex numbers: an elementary introduction to algebras*, New-York (USA), Springer-Verlag, 1989, 169 p.

[6] COPPEL, W. A. *Number theory: an introduction to mathematics*, New-York (USA), Springer, 2009, 610 p.

[7] ROSEN, Kenneth H. *Elementary number theory and its applications*, 5^{e} éd., Boston (USA), Pearson/Addison Wesley, 2005, 721 p.

[8] SILVA, Tomás Olivera e, Siegfried HERZOG et Silvio PARDI. « Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$ », *Mathematics of Computation*, American Mathematical Society, vol. 83, no 288 (2014), p. 2033-2060.

[9] SHAPIRO, M., D. C. STRUPPA, A. VAJIAC et M. B. VAJIAC. « Hyperbolic numbers and their functions », *Anal. Univ. Oradea*, Fasc. Matematica, vol XIX, no 1 (2012), p. 265-283.

[10] SOBCZYK, Garret. « The hyperbolic number plane », *The College Mathematics Journal*, Mathematical Association of America vol 26, no 4 (1995), p. 268-280.

[11] ANDREESCU, Titu et Dorin ANDRICA. *Complex numbers from A to... Z*, Boston (USA), Birkhäuser, 2006, 321 p.

[12] WAGON, Stan. « Imaginary primes and prime imaginaries », *Mathematica in action*, New-York (USA), W. H. Freeman, 1991, p. 287-324.

[13] BRESSOUD, David et Stan WAGON. « The gaussian integers », *A course in computational number theory*, New-York (USA), Key College Pub. en coopération avec Springer, 2000, p. 302-324.

[14] FLANIGAN, F. J. *Complex variables: harmonic and analytic functions*, Boston (USA), Allyn and Bacon, 1972, 353 p.

[15] BURTON, D. M. *Introduction to modern abstract algebra*, Reading (USA), Addison-Wesley Pub. Co., 1967, 310 p.

[16] GUININ, Daniel et Bernard JOPPIN. « Réels - Suites réelles », *Analyse MPSI*, Rosny-sous-Bois (France), Bréal, 2003, p. 109-148.

[17] COLLETTE, Jean-Paul. *Histoire des mathématiques*, Montréal (Québec), Éditions du Renouveau Pédagogique, 1973, 228 p.

[18] JEANNERET, Alain et Daniel LINES. *Invitation à l'algèbre : théorie des groupes, des anneaux, des corps et des modules*, Toulouse (France), Cépaduès, 2008, 394 p.

[19] ASSEM, Ibrahim et Pierre Yves LEDUC. « Anneaux », *Cours d'algèbre : groupes, anneaux, modules et corps*, Montréal (Québec), Presses internationales Polytechnique, 2009, p. 239-264.

[20] ROCHON, Dominic et M. SHAPIRO. « On algebraic properties of bicomplex and hyperbolic numbers », *Anal. Univ. Oradea*, Fasc. Matematica, vol. 11 (2004), p. 71-110.

[21] DICKSON, Leonard E. *History of the theory of numbers. Vol. 1, Divisibility and primality*, Washington (USA), Carnegie Institution of Washington, 1919, 486 p.

[22] BURTON, David M. *Elementary number theory*, 7^{e} éd., New-York (USA), McGraw-Hill, 2011, 436 p.

[23] ROVIRA, Patrice. *Mathématiques générales : pour 1er cycle universitaire et formation continue*, Toulouse (France), Cépaduès, 2003, 464 p.

[24] WEISSTEIN, Eric W. *Goldbach Partition*, de MathWorld-A Wolfram Web Resource, [En ligne], `http://mathworld.wolfram.com/GoldbachPartition.html` (Page consultée le 8 mars 2016)

[25] WEISSTEIN, Eric W. *De Polignac's Conjecture*, de MathWorld-A Wolfram Web Resource, [En ligne], `http://mathworld.wolfram.com/dePolignacsConjecture.html` (Page consultée le 9 mars 2016)

[26] WEISSTEIN, Eric W. *Twin Primes*, de MathWorld-A Wolfram Web Resource, [En ligne], `http://mathworld.wolfram.com/TwinPrimes.html` (Page consultée le 9 mars 2016)

[27] RUSSO, Felice. « From Goldbach problem: number of decompositions of 2n into unordered sums of two primes », 11 décembre 1999, dans N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, [En ligne], `https://oeis.org/A045917` (Page consultée le 12 juin 2016)

[28] BOWER, Gordon R. « Number of times that i and 2n-i are both prime, for i=1,...2n-1 », 11 décembre 1999, dans N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, [En ligne], `https://oeis.org/A035026` (Page consultée le 12 juin 2016)

Annexe A

L'anneau des matrices $A_2(\mathbb{R})$

Soit l'ensemble

$$A_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

On constate que $A_2(\mathbb{R}) \subset \mathbf{M}_2(\mathbb{R})$, l'ensemble de toutes les matrices de format 2×2. Démontrons que $(A_2(\mathbb{R}), *, \times)$ forme un anneau, où $*$ et $\times$ sont respectivement l'addition et la multiplication matricielles.

Soit $A, B, C \in A_2(\mathbb{R})$ trois matrices telles que

$$A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \qquad B = \begin{pmatrix} c & d \\ d & c \end{pmatrix}, \qquad C = \begin{pmatrix} f & g \\ g & f \end{pmatrix}.$$

- **Fermeture.** Comme $a + b, c + d \in \mathbb{R}$ lorsque $a, b, c, d \in \mathbb{R}$, alors

$$A * B = \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix} \in A_2(\mathbb{R}).$$

- **Associativité.** On a

$$\begin{aligned}(A*B)*C &= \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} c & d \\ d & c \end{pmatrix}\right) * \begin{pmatrix} f & g \\ g & f \end{pmatrix} \\ &= \begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix} * \begin{pmatrix} f & g \\ g & f \end{pmatrix} \\ &= \begin{pmatrix} (a+c)+f & (b+d)+g \\ (b+d)+g & (a+c)+f \end{pmatrix} \\ &= \begin{pmatrix} a+(c+f) & b+(d+g) \\ b+(d+g) & a+(c+f) \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} c+f & d+g \\ d+g & c+f \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \left(\begin{pmatrix} c & d \\ d & c \end{pmatrix} * \begin{pmatrix} f & g \\ g & f \end{pmatrix}\right) \\ &= A*(B*C).\end{aligned}$$

- **Neutre additif.** Le neutre additif est la matrice $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. En effet,

$$A * O_2 = \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+0 & b+0 \\ b+0 & a+0 \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} = A.$$

- **Inverse additif.** L'inverse additif de la matrice A est $-A = \begin{pmatrix} -a & -b \\ -b & -a \end{pmatrix}$. En effet,

$$A * (-A) = \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} -a & -b \\ -b & -a \end{pmatrix} = \begin{pmatrix} a+(-a) & b+(-b) \\ b+(-b) & a+(-a) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O_2.$$

- **Commutativité.** On a

$$\begin{aligned}A*B &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix} \\ &= \begin{pmatrix} c+a & d+b \\ d+b & c+a \end{pmatrix} = \begin{pmatrix} c & d \\ d & c \end{pmatrix} * \begin{pmatrix} a & b \\ b & a \end{pmatrix} = B*A.\end{aligned}$$

Donc, la paire $(A_2(\mathbb{R}), *)$ est un groupe commutatif. Considérons $(A_2(\mathbb{R}), \times)$.

- **Fermeture.** Comme $ac+bd, ad+bc \in \mathbb{R}$ lorsque $a, b, c, d \in \mathbb{R}$, alors

$$A \times B = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{pmatrix} \in A_2(\mathbb{R}).$$

- **Associativité.** On a

$$\begin{aligned}
(A \times B) \times C &= \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & d \\ d & c \end{pmatrix} \right) \times \begin{pmatrix} f & g \\ g & f \end{pmatrix} \\
&= \begin{pmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{pmatrix} \times \begin{pmatrix} f & g \\ g & f \end{pmatrix} \\
&= \begin{pmatrix} (ac+bd)f + (ad+bc)g & (ac+bd)g + (ad+bc)f \\ (bc+ad)f + (bd+ac)g & (bc+ad)g + (bd+ac)f \end{pmatrix} \\
&= \begin{pmatrix} a(cf+dg) + b(df+cg) & a(cg+df) + b(dg+cf) \\ b(cf+dg) + a(df+cg) & b(cg+df) + a(dg+cf) \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} cf+dg & cg+df \\ df+cg & dg+cf \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \left(\begin{pmatrix} c & d \\ d & c \end{pmatrix} \times \begin{pmatrix} f & g \\ g & f \end{pmatrix} \right) \\
&= A \times (B \times C).
\end{aligned}$$

- **Neutre multiplicatif.** Le neutre multiplicatif est la matrice identité $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

  En effet,

$$A \times I_2 = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a1+b0 & a0+b1 \\ b1+a0 & b0+a1 \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} = A.$$

- **Inverse multiplicatif.** Lorsque $\det(A) \neq 0$, on sait que l'inverse de la matrice A est

$$A^{-1} = \frac{1}{a^2-b^2} \begin{pmatrix} a & -b \\ -b & a \end{pmatrix}.$$

  En effet ,

$$A \times A^{-1} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \frac{1}{a^2-b^2} \begin{pmatrix} a & -b \\ -b & a \end{pmatrix} = \frac{1}{a^2-b^2} \begin{pmatrix} a^2-b^2 & -ab+ab \\ ab-ab & a^2-b^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

- **Commutativité.** On a

$$\begin{aligned} A \times B &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{pmatrix} \\ &= \begin{pmatrix} ca+db & cb+da \\ da+cb & db+ca \end{pmatrix} = \begin{pmatrix} c & d \\ d & c \end{pmatrix} \times \begin{pmatrix} a & b \\ b & a \end{pmatrix} = B \times A. \end{aligned}$$

Pour que $(A_2(\mathbb{R}), \times)$ soit un groupe commutatif, seul le neutre additif O_2 doit ne pas avoir d'inverse. OR, si $\det(A) = a^2 - b^2 = 0$, alors A n'a pas d'inverse. Dans ce cas, $(A_2(\mathbb{R}), \times)$ est un monoïde commutatif. Vérifions les deux lois de distributivité.

- **Distributivité à droite.** On a

$$\begin{aligned} A \times (B * C) &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \left(\begin{pmatrix} c & d \\ d & c \end{pmatrix} * \begin{pmatrix} f & g \\ g & f \end{pmatrix} \right) = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} c+f & d+g \\ d+g & c+f \end{pmatrix} \\ &= \begin{pmatrix} a(c+f)+b(d+g) & a(d+g)+b(c+f) \\ b(c+f)+a(d+g) & b(d+g)+a(c+f) \end{pmatrix} \\ &= \begin{pmatrix} (ac+bd)+(af+bg) & (ad+bc)+(ag+bf) \\ (bc+ad)+(bf+ag) & (bd+ac)+(bg+af) \end{pmatrix} \\ &= \begin{pmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{pmatrix} * \begin{pmatrix} af+bg & ag+bf \\ bf+ag & bg+af \end{pmatrix} \\ &= \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & d \\ d & c \end{pmatrix} \right) * \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} f & g \\ g & f \end{pmatrix} \right) \\ &= (A \times B) * (A \times C). \end{aligned}$$

- **Distributivité à gauche.** On montre $(A * B) \times C = (A \times C) * (B \times C)$ d'une façon similaire à la distributivité à droite.

Ainsi, les deux lois sont respectées. Par conséquent, le triplet $(A_2(\mathbb{R}), *, \times)$ forme un anneau unitaire commutatif.

Annexe B

Code pour les premiers complexes

Suite au théorème 2.45, nous avons les deux conditions pour représenter les nombres premiers de Gauss dans le plan complexe. On constate que le motif créé est symétrique horizontalement, verticalement et diagonalement.

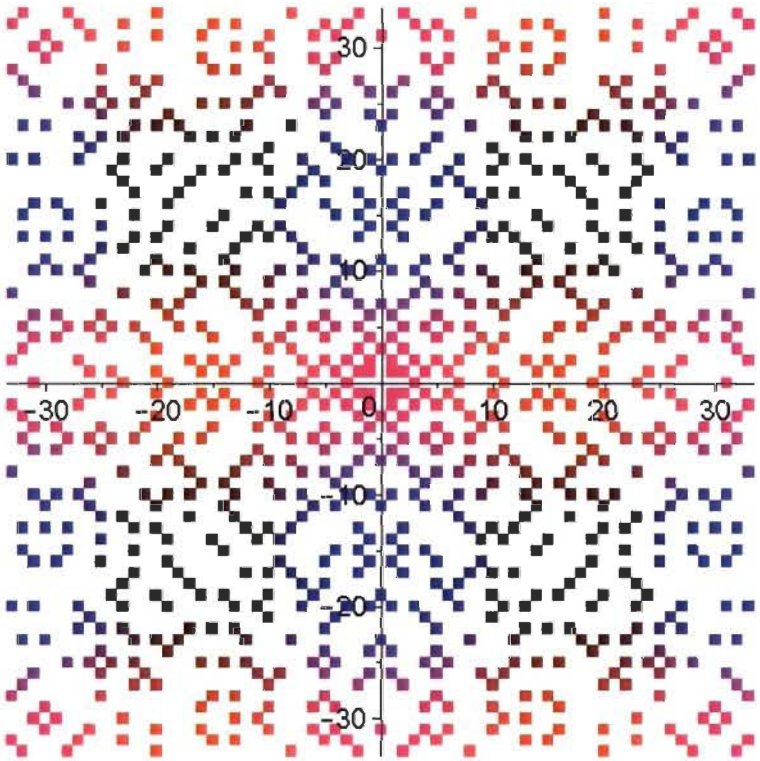


FIGURE B.1 – Nombres premiers complexes.

La condition « z est un entier premier congru à 3 modulo 4 » donne les nombres premiers complexes situés sur les axes x et y. Étant donné que l'associé d'un nombre premier est lui aussi premier, il suffit de reproduire la portion de l'axe $[0, +\infty[$ sur les demi-axes $]-\infty, 0]$, $[0, +\infty \cdot i[$ et $]-\infty \cdot i, 0]$.

La condition « $|z|^2$ est un entier premier » donne tous les autres nombres premiers qui ne sont pas sur les axes, car s'il est sur un axe, il est considéré dans la première condition.

Voici le code utilisé pour générer les nombres premiers de Gauss à l'aide du programme Maple 16.

```
> restart;
> with(plottools):
> with(plots):
> with(ColorTools):
> gauss := proc(n)
  local i, j, A, L, P;
  L := [0,0];
  P := [0,0];
   for i from -n to n do #Compteur pour les rangées.
    for j from -n to n do #Compteur pour les colonnes.

     #Deuxième condition du théorème.

     if isprime(i^2+j^2) = true then L := L, [i,j];

     #Première condition du théorème.

     elif (is(i+j*I, integer) = true and isprime(i+j*I) = true and
      i+j*I mod 4 = 3) then L := L, [i,j];
     elif (is(i+j*I, integer) = true and isprime(-i+j*I) = true and
      -i+j*I mod 4 = 3) then L := L, [i,j];
     elif (is((i+j*I)/I, integer) = true and isprime((i+j*I)/I) = true and
      (i+j*I)/I mod 4 = 3) then L := L, [i,j];
     elif (is((i-j*I)/I, integer) = true and isprime((i-j*I)/I) = true and
      (i-j*I)/I mod 4 = 3) then L := L, [i,j];
     end if;
    end do;
   end do;
  L := [L];
  L := remove(x->x[1] = 0 and x[2] = 0, L);

   #Faire les carrés aux nombres premiers [i,j] en mettant de la couleur.
```

```
    for i from 1 to nops(L) do
    A := rectangle([op(1, op(i, L)) - 0.5, op(2, op(i, L)) + 0.5],
     [op(1, op(i, L)) + 0.5, op(2, op(i, L)) - 0.5], color = ColorTools:-Color(
     [round((255/2)*cos(((2*Pi)/n)*op(2, op(i, L)))+(255/2)),
     round((255/8)*cos(((2*Pi)/n)*op(2, op(i, L)))+(255/8)),
     round((255/2)*cos(((2*Pi)/n)*op(1, op(i, L)))+(255/2))]));
    P := P, A;
    end do;
   P := [P];
   P := subsop(1 = NULL, P);
   display(P, scaling = constrained, font = ["Arial", 18], labels = [" ", " "]);
   end proc:
 > gauss(33);
```

La couleur du graphique n'a aucun lien avec les nombres premiers ; c'est plutôt un choix esthétique. On remarque l'utilisation de fonctions cosinus pour déterminer les teintes, c'est ce qui donne les dégradés de couleurs. Dans Maple, le premier argument de la couleur est le rouge. La variable est la valeur de la partie réelle (compteur pour les colonnes) pour la fonction

$$f(x) = \frac{255}{2} \cdot \cos\left(\frac{2\pi}{n}x\right) + \frac{255}{2}, \text{ où } n = 33.$$

Le deuxième élément est le vert. La fonction est

$$g(x) = \frac{255}{8} \cdot \cos\left(\frac{2\pi}{n}x\right) + \frac{255}{8}, \text{ où } n = 33.$$

Il y a moins de vert que de rouge, car l'amplitude et l'ordonnée à l'origine sont plus petites. Finalement, le bleu est généré par la valeur de la partie imaginaire (compteur pour les rangées). Sa fonction est aussi $f(x)$. On a donc l'effet d'une « vague » verticale de bleu, alors que le rouge et le vert génèrent une « vague » horizontale. De plus, toutes ces fonctions sont arrondies à l'entier le plus près et ont leurs images bornées entre $[0, 255]$.

Annexe C

Code pour les premiers hyperboliques triviaux

Pour faire suite au théorème 4.15, nous avons les conditions pour représenter les nombres premiers hyperboliques triviaux dans le plan. Le motif créé est symétrique à l'horizontale, à la verticale et à la diagonale.

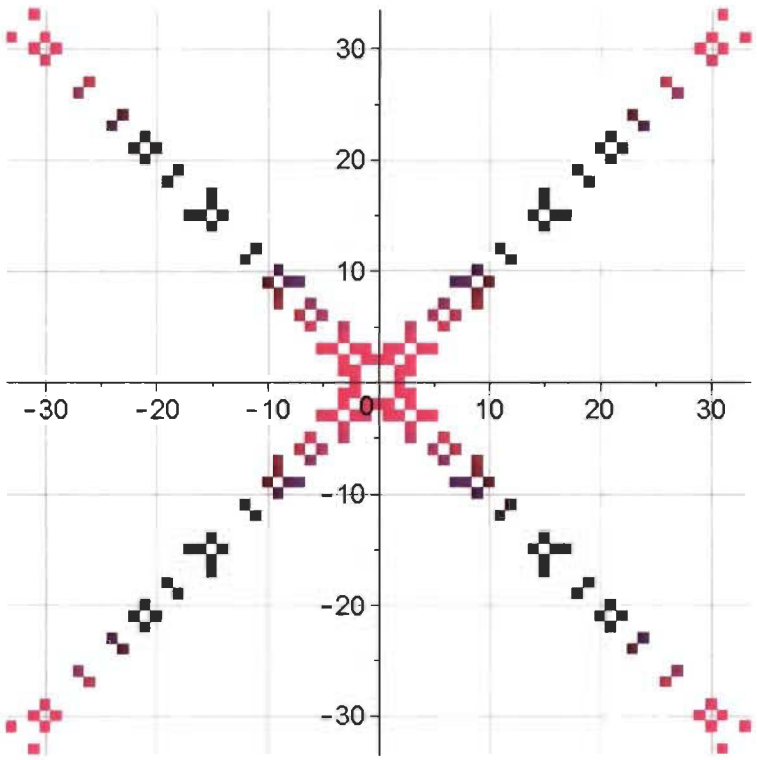


FIGURE C.1 – Nombres premiers hyperboliques triviaux.

Voici le code utilisé dans Maple 16 pour générer les nombres premiers hyperboliques triviaux.

```
> restart:
> with(plottools):
> with(plots):
> with(ColorTools):
> hypprime := proc(n)
  local i, j, k, A, L, P;
  L := [0,0];
  P := [0,0];
  k := 1;
  while 2^k<2*n do
   for i from -2*n to 2*n do
    for j from -2*n to 2*n do
     if ((i=2^k and j=2) or (i=2^k and j=-2) or (i=2 and j=2^k) or
      (i=2 and j=-2^k) or (i=-2^k and j=2) or (i=-2^k and j=-2) or
      (i=-2 and j=2^k) or (i=-2 and j=-2^k)) or (i mod 2 =1 and j mod 2 = 1
      and ((isprime(i)=true and j=1 and i<>1 and i<>-1) or (isprime(-i)=true
      and j=1 and i<>1 and i<>-1) or (isprime(i)=true and j=-1 and i<>1 and
      i<>-1) or (isprime(-i)=true and j=-1 and i<>1 and i<>-1) or
      (i=1 and isprime(j)=true and j<>1 and j<>-1) or (i=-1 and isprime(j)=true
      and j<>1 and j<>-1) or (i=1 and isprime(-j)=true and j<>1 and j<>-1) or
      (i=-1 and isprime(-j)=true and j<>1 and j<>-1)))
      then L:=L, [(i+j)/2,(i-j)/2];
     end if;
    end do;
   end do;
  k:=k+1;
  end do;
  L := [L];
  L := remove(x->x[1] = 0 and x[2] = 0, L);
  for i from 1 to nops(L) do
   A := rectangle([op(1, op(i, L)) - 0.5, op(2, op(i, L)) + 0.5],
    [op(1, op(i, L)) + 0.5, op(2, op(i, L)) - 0.5], color = ColorTools:-Color(
    [round((255/2)*cos(((2*Pi)/n)*op(2, op(i, L)))+(255/2)),
    round((255/8)*cos(((2*Pi)/n)*op(2, op(i, L)))+(255/8)),
    round((255/2)*cos(((2*Pi)/n)*op(1, op(i, L)))+(255/2))]));
   P := P, A;
```

```
    end do;
  P := [P];
  P := subsop(1 = NULL, P);
  display(P, scaling = constrained, gridlines = true, font = ["Arial", 18],
  labels = [" ", " "]);
  end proc:
> hypprime(33);
```

La couleur du graphique est identique à celle du graphique des nombres premiers complexes de l'annexe B.

Annexe D

Code pour les premiers hyperboliques non triviaux

La définition 4.19 implique que chaque composante idempotente des nombres $\mathbb{P}$ est un nombre premier de même parité. Il suffit de créer toutes les paires de premiers possibles.

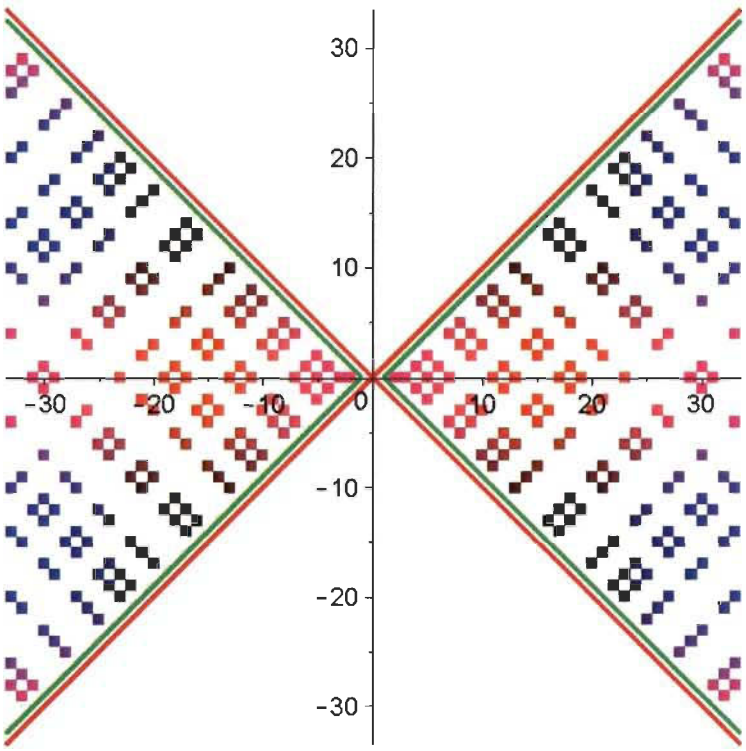


FIGURE D.1 – Nombres premiers hyperboliques non triviaux.

Voici le code généré à partir de Maple 16. Dans le code, l'ensemble $\bowtie$ est appelé « le papillon ».

```
> restart;
> with(plottools):
> with(plots):
> with(ColorTools):
> hypprimenontrivial := proc(n)
  local i, j, y, L, P, A, M, z1, z2, z3, z4, z5, z6;
  L := [0,0];
  P := [0,0];
  for i from -2*n to 2*n do
   for j from -2*n to 2*n do
    if (((i mod 2 = 0 and j mod 2 = 0) or (i mod 2 = 1 and j mod 2 = 1)) and
     (isprime(i) = true or isprime(-i) = true) and (isprime(j) = true
     or isprime(-j) = true) and ((i+j)/2)^2 >= ((i-j)/2)^2 and
     (i+j)/2 >= -n and (i+j)/2 <= n)
     then L := L, [(i+j)/2, (i-j)/2];
    end if;
   end do;
  end do;
  L := [L];
  L := remove(x->x[1] = 0 and x[2] = 0, L);
  for i from 1 to nops(L) do
   A := rectangle([op(1, op(i, L)) - 0.5, op(2, op(i, L)) + 0.5],
    [op(1, op(i, L)) + 0.5, op(2, op(i, L)) - 0.5], color = ColorTools:-Color(
    [round((255/2)*cos(((2*Pi)/n)*op(2, op(i, L)))+(255/2)),
    round((255/8)*cos(((2*Pi)/n)*op(2, op(i, L)))+(255/8)),
    round((255/2)*cos(((2*Pi)/n)*op(1, op(i, L)))+(255/2))]));
   P := P, A;
  end do;
  P := [P];
  P := subsop(1 = NULL, P);

  #Ajouter les fonctions délimitant le papillon, sinon les omettre.

  z1 := display(plot(x+1, x = -n-0.5..-1, y = -n-0.5..-1, thickness = 4,
   color = 'green'));
  z2 := display(plot(x-1, x = 1..n+0.5, y = 0..n+0.5, thickness = 4,
   color = 'green'));
```

```
z3 := display(plot(-x+1, x = 1..n+0.5, y = -n-0.5..0, thickness = 4,
 color = 'green'));
z4 := display(plot(-x-1, x = -n-0.5..-1, y = 0..n+0.5, thickness = 4,
 color = 'green'));
z5 := display(plot(x, x = -n-0.5..n+0.5, y = -n-0.5..n+0.5, thickness = 4,
 color = 'red'));
z6 := display(plot(-x, x = -n-0.5..n+0.5, y = -n-0.5..n+0.5, thickness = 4,
 color = 'red'));
M := display(P, scaling = constrained, view = [-n-0.5..n+0.5, -n-0.5..n+0.5]);
display(M, z1, z2, z3, z4, z5, z6, font = ["Arial", 18], labels = [" ", " "]);
end proc:
> hypprimenontrivial(33);
```

La couleur du graphique est identique à celle du graphique des nombres premiers complexes de l'annexe B.