Entiers d'Eisenstein

Marc Lorenzi

8 janvier 2026

1 Introduction

1.1 Racines 6èmes de l'unité

On note $\mathbb{U}_6$ le groupe des racines 6èmes de l'unité. Posons

$$\omega = e^{i\pi/3} = \frac{1}{2} + \imath\frac{\sqrt{3}}{2}$$

de sorte que

$$\mathbb{U}_6 = \{\omega^k : k \in [\![0, 5]\!]\} = \{\pm 1, \pm\omega, \pm\omega^2\}$$

Notons les égalités

$$\omega^3 = -1$$
$$\omega^2 = \omega - 1$$
$$\omega^{-1} = -\omega^2 = 1 - \omega$$
$$\omega^{-2} = -\omega$$
$$\overline{\omega} = 1 - \omega$$

Proposition 1. *Tout élément de $\mathbb{C}$ s'écrit de façon unique sous la forme $a + b\omega$ où $a, b \in \mathbb{R}$.*

Démonstration. $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2. Comme $\omega \notin \mathbb{R}$, la famille $(1, \omega)$ est une famille libre de $\mathbb{C}$. D'où le résultat puisque $\dim \mathbb{C} = 2$. □

Notation. $\mathcal{S} = \{z \in \mathbb{C}^* : \arg(z) \in [0, \pi/3[\}$, où l'argument appartient à $]-\pi, \pi]$. L'ensemble $\mathcal{S}$ est un sixième du plan complexe.

Proposition 2. *Soit $z = a + b\omega \in \mathbb{C}^*$ où $a, b \in \mathbb{R}$. On a $z \in \mathcal{S}$ si et seulement si $a > 0$ et $b \geq 0$.*

Démonstration. On a

$$z = \left(a + \frac{b}{2}\right) + ib\frac{\sqrt{3}}{2}$$

Soit $\theta = \arg(z) \in]-\pi, \pi]$.

Supposons $z \in \mathcal{S}$. On a $\theta \in [0, \pi/2[$, donc $2a + b > 0$ et $b \geq 0$. De plus,

$$\tan\theta = \frac{b\frac{\sqrt{3}}{2}}{a + \frac{b}{2}} = \frac{b\sqrt{3}}{2a+b} < \tan\frac{\pi}{3} = \sqrt{3}$$

et donc $b < 2a + b$. Ainsi, $a > 0$.

Inversement, supposons $a > 0$ et $b \geq 0$. On a alors $2a+b > 0$ et $0 \leq \tan\theta < \sqrt{3}$, donc $\theta \in [0, \pi/3[$. Ainsi, $z \in \mathcal{S}$. □

1.2 L'anneau des entiers d'Eisenstein

Définition 1. L'ensemble des *entiers d'Eisenstein* est $\mathbb{E} = \{a + b\omega : a, b \in \mathbb{Z}\}$.

On vérifie facilement que $\mathbb{E}$ est un sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$. Pour tous $a, b, a', b' \in \mathbb{Z}$,

$$(a + b\omega) + (a' + b'\omega) = (a + a') + (b + b')\omega$$

$$(a + b\omega) + (a' + b'\omega) = (aa' - bb') + (ab' + ba' + bb')\omega$$

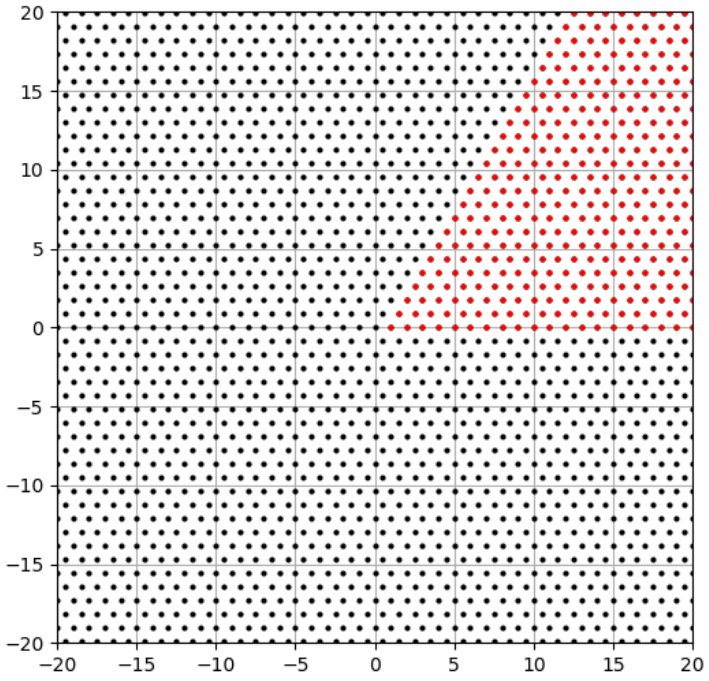

FIGURE 1 – L'ensemble $\mathbb{E}$. En rouge, les éléments de $\mathcal{S}$.

Remarquons que $\mathbb{E}$ est aussi stable par passage au conjugué : en effet, $\overline{\omega} = 1 - \omega$, donc pour tout $x = a + b\omega \in \mathbb{E}$,

$$\overline{x} = (a + b) - b\omega \in \mathbb{E}$$

Définition 2. Pour tout $x \in \mathbb{E}$, la *norme* de x est $N(x) = x\overline{x}$.

Si $x = a + b\omega$ où $a, b \in \mathbb{Z}$, on a

$$N(x) = (a + b\omega)(a + b\overline{\omega}) = a^2 + 2ab\mathrm{Re}(\omega) + b^2|\omega|^2 = a^2 + ab + b^2 \in \mathbb{N}$$

La norme étant un module au carré, on a immédiatement que $N(x) = 0$ si et seulement si $x = 0$. Également, pour tous $x, y \in \mathbb{E}$, $N(xy) = N(x)N(y)$. La norme va jouer un rôle important dans la suite. Elle remplace d'une certaine façon, dans l'arithmétique de l'anneau $\mathbb{E}$, la valeur absolue dans l'anneau $\mathbb{Z}$.

Lemme 3. *Soit $x \in \mathbb{E}$. L'entier d'Eisenstein x est inversible si et seulement si $N(x) = 1$.*

Démonstration. Supposons x inversible, d'inverse $y \in \mathbb{E}$. On a $xy = 1$. En passant aux normes, $N(x)N(y) = 1$. Or, $N(y)$ et $N(y)$ sont des entiers naturels, donc $N(x) = N(y) = 1$.

Inversement, supposons $N(x) = 1$. On a $x\overline{x} = 1$, donc x est inversible dans $\mathbb{E}$, d'inverse $\overline{x}$. □

Proposition 4. *L'ensemble des inversibles de $\mathbb{E}$ est le groupe $\mathbb{U}_6$.*

Démonstration. Soit $x = a + b\omega \in \mathbb{E}$. Supposons x inversible. Par le lemme précédent,

$$(\star)\ a^2 + ab + b^2 = 1$$

ou encore

$$(2a + b)^2 + 3b^2 = 4$$

On en déduit que $3b^2 \leq 4$. Comme b est entier, $b = -1$, 0 ou 1.

- Cas 1, $b = -1$. En reportant dans $(\star)$, $a^2 - a = 0$ donc $a = 0$ ou $a = 1$. On a donc $x = -\omega$ ou $x = 1 - \omega = -\omega^2$.
- Cas 2, $b = 1$. En reportant dans $(\star)$, $a^2 + a = 0$ donc $a = 0$ ou $a = -1$. On a donc $x = \omega$ ou $x = -1 + \omega = \omega^2$.
- Cas 3, $b = 0$. En reportant dans $(\star)$, $a^2 = 1$ donc $a = 1$ ou $a = -1$. On a donc $x = 1$ ou $x = -1$.

Ainsi, l'ensemble des inversibles de $\mathbb{E}$ est inclus dans $\mathbb{U}_6$. Inversement, $\mathbb{U}_6$ est un groupe multiplicatif inclus dans $\mathbb{E}$, d'où l'inclusion réciproque. □

2 Divisibilité

2.1 Diviseurs, multiples

Définition 3. Soient $x, y \in \mathbb{E}$. x *divise* y lorsqu'il existe $z \in \mathbb{E}$ tel que $y = xz$.

Nous noterons $x \,|\, y$ lorsque x divise y. Dans le cas contraire, nous noterons $x \not| y$. Une ambiguïté apparaît. Si $x, y \in \mathbb{Z}$ et que x divise y, parlons-nous de divisibilité dans $\mathbb{Z}$ ou dans $\mathbb{E}$? En fait, il y a équivalence.

Proposition 5. *Soient $x, y \in \mathbb{Z}$. x divise y dans $\mathbb{Z}$ si et seulement si x divise y dans $\mathbb{E}$.*

Démonstration. Si x divise y dans $\mathbb{Z}$, il existe $z \in \mathbb{Z}$ tel que $y = zx$. Comme $z \in \mathbb{Z} \subset \mathbb{E}$, x divise aussi y dans $\mathbb{E}$. Inversement, si x divise y dans $\mathbb{E}$, il existe $z \in \mathbb{E}$ tel que $y = xz$. Posons $z = a + b\omega$ où $a, b \in \mathbb{Z}$. On a

$$y = y + 0\omega = xz = ax + bx\omega$$

Par unicité de l'écriture des éléments de $\mathbb{E}$, $y = ax$, donc x divise y dans $\mathbb{Z}$. □

Proposition 6. *La relation de divisibilité est réflexive et transitive. Pour tous $x, y \in \mathbb{E}$, x divise y et y divise x si et seulement si il existe $w \in \mathbb{U}_6$ tel que $y = wx$.*

Démonstration. Soit $x \in \mathbb{E}$. On a $x = 1x$ donc $x|x$, d'où la réflexivité.

Soient $x, y, z \in \mathbb{E}$. Supposons que $x|y$ et $y|z$. Soient $w, t \in \mathbb{E}$ tels que $y = wx$ et $z = ty$. On a $z = (tw)x$ donc $x|z$, d'où la transitivité.

Soient $x, y \in \mathbb{E}$. Supposons que $x|y$ et $y|x$. Soient $w, t \in \mathbb{E}$ tels que $y = wx$ et $x = ty$. Si $x = 0$, alors $y = w0 = 0$, donc $y = 1x$. Supposons $x \neq 0$. On a $x = (tw)x$ donc $1 = tw$. Ainsi, $w \in \mathbb{U}_6$. Inversement, supposons qu'il existe $w \in \mathbb{U}_6$ tel que $y = wx$. On a $x|y$ mais aussi, comme $x = w^{-1}y$, $y|x$. □

Définition 4. Les entiers d'Eisenstein x et y sont *associés* si x divise y et y divise x.

Tout élément x non nul de $\mathbb{E}$ possède ainsi 6 associés, qui sont les ux où $u \in \mathbb{U}_6$. Bien entendu, le seul associé de 0 est 0.

Le résultat suivant nous permet de choisir, pour chaque élément de $\mathbb{E}$ non nul, un associé remarquable.

Proposition 7. *Soit $x \in \mathbb{E}$ non nul. Un et un seul des associés de x appartient à $\mathcal{S}$.*

Démonstration. Soit $\theta = \arg(x) \in]-\pi, \pi]$. Les arguments des associés de x sont, modulo 2π, $\theta + k\pi/3$ où $k \in \mathbb{Z}$. On a

$$\begin{aligned} 0 \leq \theta + k\frac{\pi}{3} < \frac{\pi}{3} \quad &\iff \quad -\theta \leq k\frac{\pi}{3} < -\theta + \frac{\pi}{3} \\ &\iff \quad -\frac{3\theta}{\pi} \leq k < -\frac{3\theta}{\pi} + 1 \\ &\iff \quad k = \left\lfloor -\frac{3\theta}{\pi} \right\rfloor \end{aligned}$$

d'où l'existence et l'unicité. □

Par la caractérisation des éléments de $\mathcal{S}$, un et un seul des associés de x est donc de la forme $a + b\omega$ où $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$.

2.2 Division euclidienne

Tout comme $\mathbb{Z}$, l'anneau $\mathbb{E}$ peut être muni d'une division euclidienne.

Proposition 8. *Soient $a, b \in \mathbb{E}$ tels que $b \neq 0$. Il existe $(q, r) \in \mathbb{E}^2$ tel que $a = bq + r$ et $N(r) < N(b)$.*

Remarquons que l'on n'affirme pas l'unicité du couple (q, r). Dans la suite, nous parlerons tout de même *du* quotient et *du* reste de la division euclidienne de a par b. On peut lever l'ambiguïté en décidant de choisir pour q et r les deux entiers d'Eisenstein définis dans la démonstration qui suit..

Démonstration. Soit $z = u + v\omega = a/b \in \mathbb{C}$. La partie réelle u et la partie imaginaire v de z sont deux rationnels. Posons $x = \lfloor u + 1/2 \rfloor$ et $y = \lfloor v + 1/2 \rfloor$. On a $x, y \in \mathbb{Z}$, $|x - u| \leq 1/2$ et $|y - v| \leq 1/2$. Soit $q = x + y\omega \in \mathbb{E}$. On a

$$\begin{aligned} |z - q|^2 &= |(u - x) + (v - y)\omega|^2 \\ &= (u - x)^2 + (u - x)(v - y) + (v - y)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4} \end{aligned}$$

De là, en multipliant par $N(b)$,

$$N(a - bq) \leq \frac{3}{4} N(b)$$

En posant $r = a - bq$, on a le résultat. On a même un peu mieux, puisque $N(r) \leq 3N(b)/4$. □

L'anneau $\mathbb{E}$ est ainsi un *anneau euclidien*. Il est donc aussi *principal*. La preuve est classique, c'est l'objet du paragraphe suivant.

2.3 Les idéaux de $\mathbb{E}$

Proposition 9. *Les idéaux de $\mathbb{E}$ sont les ensembles $a\mathbb{E}$ où $a \in \mathbb{E}$.*

Démonstration. Il est clair que pour tout $a \in \mathbb{E}$, $a\mathbb{E}$ est un idéal de $\mathbb{E}$. Inversement, soit $\mathfrak{I}$ un idéal de $\mathbb{E}$. Si $\mathfrak{I} = \{0\}$, alors $\mathfrak{I} = 0\mathbb{E}$. Supposons $\mathfrak{I} \neq \{0\}$. Soit

$$A = \{N(x) : x \in \mathfrak{I}, x \neq 0\}$$

L'ensemble A est une partie non vide de $\mathbb{N}$, il possède donc un plus petit élément. Soit $a \in \mathfrak{I}$ non nul tel que $N(a) = \min A$. Comme $\mathfrak{I}$ est un idéal, $a\mathbb{E} \subseteq \mathfrak{I}$. Inversement, soit $x \in \mathfrak{I}$. Effectuons la division euclidienne de x par a : il existe $(q, r) \in \mathbb{E}^2$ tel que $x = aq + r$ et $N(r) < N(a)$. On a $r = x - aq \in \mathfrak{I}$. Mais $N(r) < N(a) = \min A$, donc $N(r) \notin A$. Ainsi, $N(r) = 0$, d'où $r = 0$ et $x = aq \in a\mathbb{E}$. □

On vérifie facilement que pour tous $a, a' \in \mathbb{E}$, on a $a\mathbb{E} = a'\mathbb{E}$ si et seulement si a et a' sont associés. Explicitement,

$$a\mathbb{E} = (-a)\mathbb{E} = (a\omega)\mathbb{E} = (-a\omega)\mathbb{E} = (a\omega^2)\mathbb{E} = (-a\omega^2)\mathbb{E}$$

et ce sont les seules possibilités.

2.4 Plus grand diviseur commun

Proposition 10. *Soient $a, b \in \mathbb{E}$. Il existe $\delta \in \mathbb{E}$ tel que $a\mathbb{E} + b\mathbb{E} = \delta\mathbb{E}$. Un tel δ est unique à associé près.*

Démonstration. $a\mathbb{E} + b\mathbb{E}$ est un idéal de $\mathbb{E}$, d'où l'existence. Pour l'unicité, nous avons vu que $\delta\mathbb{E} = \delta'\mathbb{E}$ si et seulement si δ et δ' sont associés. □

Un tel δ est un *plus grand diviseur commun* (en abrégé pgcd) de a et b. Deux éléments a et b de $\mathbb{E}$ possèdent donc 6 pgcd, sauf si $a = b = 0$ (dans ce cas, le seul pgcd est 0). Lorsque δ est un pgcd de a et b, nous noterons $a \wedge b = \delta$. Cette égalité est à comprendre « à associé près ». Parmi les 6 pgcd de a et b, un et un seul appartient à $\mathcal{S}$. C'est celui que nous privilégierons. Remarquons, en particulier, que les entiers naturels non nuls appartiennent à $\mathcal{S}$.

Nous dirons que a et b sont *premiers entre eux* lorsque $a \wedge b = 1$.

L'anneau $\mathbb{E}$ étant euclidien, toutes les propriétés du pgcd bien connues dans $\mathbb{Z}$ y restent vérifiées : algorithme d'Euclide, théorème de Bézout, lemme de Gauss, etc. Nous ne les détaillerons pas ici, les preuves sont en tous points identiques à celles qui sont faites dans $\mathbb{Z}$. Signalons tout de même le résultat suivant.

Proposition 11. *Soient $a, b \in \mathbb{Z}$. Le pgcd de a et b dans $\mathbb{Z}$ est aussi (à associé près) le pgcd de a et b dans $\mathbb{E}$.*

Démonstration. Soient $\delta_{\mathbb{E}} \in \mathbb{E}$ le pgcd de a et b dans $\mathbb{E}$ et $\delta_{\mathbb{Z}} \in \mathbb{Z}$ le pgcd de a et b dans $\mathbb{Z}$. Comme $\delta_{\mathbb{Z}}$ divise a et b dans $\mathbb{Z}$ il les divise aussi dans $\mathbb{E}$. De là, $\delta_{\mathbb{Z}}$ divise $\delta_{\mathbb{E}}$.

Par définition de $\delta_{\mathbb{Z}}$, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = \delta_{\mathbb{Z}}$. L'entier d'Eisenstein $\delta_{\mathbb{E}}$ divise a et b dans $\mathbb{E}$, donc il divise $ua + vb = \delta_{\mathbb{Z}}$ dans $\mathbb{E}$. Ainsi, $\delta_{\mathbb{E}}$ et $\delta_{\mathbb{Z}}$ sont associés dans $\mathbb{E}$. □

3 Primalité

3.1 Irréductibilité et primalité

Lorsqu'on cherche à définir la notion d'élément premier dans un anneau, on est amené à introduire deux concepts : l'*irréductibilité* et la *primalité*.

Définition 5. $p \in \mathbb{E}$ est *irréductible* si

- $p \notin \mathbb{U}_6$.
- Pour tous $a, b \in \mathbb{E}$, $p = ab \implies a \in \mathbb{U}_6$ ou $b \in \mathbb{U}_6$.

Définition 6. $p \in \mathbb{E}$ est *premier* si

- $p \neq 0$.
- $p \notin \mathbb{U}_6$.
- Pour tous $a, b \in \mathbb{E}$, $p|ab \implies p|a$ ou $p|b$.

Il s'avère que dans l'anneau $\mathbb{E}$, primalité et irréductibilité sont deux concepts équivalents. Commençons par un lemme facile.

Lemme 12. *Soient $a, p \in \mathbb{E}$. On suppose que p est irréductible et p ne divise pas a. Alors, p est premier avec a.*

Démonstration. Soit $\delta = a \wedge p$. Comme δ divise p, $\delta = 1$ ou $\delta = p$ (à associés près). Mais δ divise a et p ne divise pas a, donc $\delta \neq p$. Ainsi, $\delta = 1$. □

Proposition 13. *Un entier d'Eisenstein non nul est irréductible si et seulement si il est premier.*

Démonstration. Soit $p \in \mathbb{E}$ non nul. Supposons p premier. Soient $a, b \in \mathbb{E}$ tels que $p = ab$. On a $p|ab$ donc, comme p est premier, p divise a ou p divise b. Par exemple, $p|a$. Soit $c \in \mathbb{E}$ tel que $a = pc$. On a alors $p = ab = pcb$. Comme $p \neq 0$, $1 = cb$ donc $b \in \mathbb{U}_6$. Ainsi, p est irréductible.

Supposons p irréductible. Soient $a, b \in \mathbb{E}$ tels que $p|ab$. Supposons que p ne divise pas a. Par le lemme 12, a est premier avec p. Soit $c \in \mathbb{E}$ tel que $ab = pc$. On a $a|pc$ et a premier avec p donc, par le lemme de Gauss, a divise c. Soit $d \in \mathbb{E}$ tel que $c = ad$. On a alors $ab = pc = pad$. Comme p ne divise pas a, $a \neq 0$ et donc $b = pd$. Ainsi, p divise b. L'entier d'Eisenstein p est donc premier. □

Remarquons que primalité $\implies$ irréductibilité n'utilise que la définition de la relation de divisibilité et l'intégrité de l'anneau. En revanche, irréductibilité $\implies$ primalité utilise le lemme de Gauss, qui est vérifié dans $\mathbb{E}$ parce que $\mathbb{E}$ est un anneau principal.

Remarque. Si $p \in \mathbb{Z}$, deux questions se posent : p est-il premier en tant qu'élément de $\mathbb{Z}$? p est-il premier en tant qu'élément de $\mathbb{E}$? Nous allons voir que ces deux questions sont liées, mais aussi qu'il n'y a pas équivalence. Pour lever toute ambiguïté, nous insisterons si besoin en disant « p est premier dans $\mathbb{Z}$ » ou « p est premier dans $\mathbb{E}$ ».

Notation. On not $\mathcal{P}[\mathbb{Z}]$ l'ensemble des entiers relatifs premiers dans $\mathbb{Z}$ et $\mathcal{P}[\mathbb{E}]$ l'ensemble des entiers d'Eisenstein premiers dans $\mathbb{E}$. On note également $\mathcal{P}^+[\mathbb{Z}] = \mathcal{P}[\mathbb{Z}] \cap \mathbb{N}$ et $\mathcal{P}^+[\mathbb{E}] = \mathcal{P}[\mathbb{E}] \cap \mathcal{S}$.

Pour reformuler notre question, il s'agit de déterminer $\mathcal{P}[\mathbb{Z}] \cap \mathcal{P}[\mathbb{E}]$.

3.2 Une équation diophantienne

Nous allons voir dans ce qui suit que **la** clé pour l'étude des entiers d'Eisenstein premiers est la réponse à cette question : quels sont les entiers relatifs premiers dans $\mathbb{Z}$ qui sont de la forme $a^2 + ab + b^2$ où $a, b \in \mathbb{Z}$?

Proposition 14. *Soit $p \in \mathbb{N}$. On suppose qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + ab + b^2$. Alors, $p \equiv 0 \bmod 3$ ou $p \equiv 1 \bmod 3$.*

Démonstration. Le tableau ci-dessous donne $a^2 + ab + b^2 \bmod 3$ en fonction de $a \bmod 3$ et $b \bmod 3$.

	0	1	2
0	0	1	1
1	1	0	1
2	1	1	0

d'où le résultat. □

Nous allons montrer la réciproque. C'est un peu plus délicat.

Lemme 15. *Soit $p \in \mathcal{P}^+[\mathbb{Z}]$. On suppose $p \equiv 1 \bmod 3$. Alors, -3 est un carré modulo p.*

Démonstration. Faute de mieux pour l'instant, j'utilise la loi de réciprocité quadratique. On a

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

Comme p est impair, $(-1)^{p-1} = 1$. Comme p est congru à 1 modulo 3,

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

Ainsi,

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

□

Lemme 16. *Soit $p \in \mathcal{P}^+[\mathbb{Z}]$. On suppose $p \equiv 1 \bmod 3$. Alors, il existe $r \in \mathbb{Z}$ tels que $r^2 + r + 1 \equiv 0 \bmod p$.*

Démonstration. Dans le corps $\mathbb{Z}/p\mathbb{Z}$, l'équation $r^2 + r + 1 = 0$ a pour discriminant -3. Comme -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, cette équation a une racine. Elle a même deux racines distinctes, puisque $-3 \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$. □

Proposition 17. *Soit $p \in \mathcal{P}^+[\mathbb{Z}]$. On suppose $p \equiv 1 \bmod 3$. Alors, il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + ab + b^2$.*

Démonstration. Soit $r \in [\![0, p-1]\!]$ tel que $r^2 + r + 1 \equiv 0 \bmod p$. Un tel r existe par le lemme 16. Soit $\delta = a + b\omega = p \wedge (r + \omega)$, où le pgcd est évidemment un pgcd dans $\mathbb{E}$.

Par définition de r, p divise $r^2 + r + 1$ dans $\mathbb{Z}$. Or,

$$r^2 + r + 1 = (r + \omega)(r + \overline{\omega})$$

L'entier d'Eisenstein p divise donc $(r+\omega)(r+\overline{\omega})$ dans $\mathbb{E}$. En supposant un court instant que p est premier avec $r+\omega$ dans $\mathbb{E}$ alors, par le lemme de Gauss, p divise $r+\overline{\omega}$. De là,

$$\frac{r}{p}+\frac{\overline{\omega}}{p}=\frac{r+1}{p}-\frac{1}{p}\omega\in\mathbb{E}$$

Contradiction car $1/p\notin\mathbb{Z}$. Ainsi, $\delta\neq 1$ (à associé près), donc $N(\delta)\neq 1$.

Comme δ divise $r+\omega$ dans $\mathbb{E}$, $N(\delta)$ divise $N(r+\omega)=r^2+r+1$ dans $\mathbb{Z}$. Remarquons que

$$(p-1)^2+(p-1)+1=p^2-p+1\equiv 1 \bmod p$$

donc $r\neq p-1$, donc $0\leq r<p-1$. De là,

$$N(\delta)|r^2+r+1<(p-1)^2+(p-1)+1=p^2-p+1<p^2$$

et donc $N(\delta)\neq p^2$.

Comme δ divise p dans $\mathbb{E}$, $N(\delta)=a^2+ab+b^2$ divise $N(p)=p^2$ dans $\mathbb{Z}$. Or, $N(\delta)\neq 1$ et $N(\delta)\neq p^2$, donc $N(\delta)=p$. Ainsi, $a^2+ab+b^2=p$. □

Bilan. Remarquons que $3=1^2+1^2+1\times 1$. Pour résumer ce qui précède, un entier naturel p premier dans $\mathbb{Z}$ est de la forme a^2+b^2+ab si et seulement si $p=3$ ou $p\equiv 1 \bmod 3$.

3.3 Entiers relatifs premiers dans $\mathbb{E}$

Proposition 18. *Soit $p\in\mathbb{Z}$. On a $p\in\mathcal{P}[\mathbb{E}]$ si et seulement si $p\in\mathcal{P}[\mathbb{Z}]$ et $|p|\equiv 2 \bmod 3$.*

Démonstration. Tout d'abord, si p est composé dans $\mathbb{Z}$ alors p l'est évidemment dans $\mathbb{E}$. Nous supposons dorénavant p premier dans $\mathbb{Z}$. On a p premier dans $\mathbb{E}$ si et seulement si $-p$ l'est. On peut donc supposer $p\geq 2$.

Supposons que p n'est pas premier dans $\mathbb{E}$. Il existe donc $x,y\in\mathbb{E}$ non inversibles tels que $p=xy$. En passant aux normes, il vient $p^2=N(x)N(y)$. Comme p est premier dans $\mathbb{Z}$ et $N(x),N(y)\geq 2$, on a $N(x)=N(y)=p$. De là $p=N(x)=x\overline{x}$. Posons $x=a+ib$ où $a,b\in\mathbb{Z}$. On a $a^2+b^2+ab=p$ et donc, par la proposition 14, $p=3$ ou $p\equiv 1 \bmod 3$.

Inversement, $3=(1+\omega)(1+\overline{\omega})$ donc 3 n'est pas premier dans $\mathbb{E}$. Supposons $p\equiv 1 \bmod 3$. Par la proposition 17, il existe $a,b\in\mathbb{Z}$ tels que $p=a^2+ab+b^2$. De là, $p=(a+b\omega)(a+b\overline{\omega})$ n'est pas premier dans $\mathbb{E}$. □

3.4 Se ramener aux entiers relatifs

Maintenant que nous connaissons les entiers relatifs qui sont premiers dans $\mathbb{E}$, nous pouvons examiner le cas général. Nous allons voir que si $x\in\mathbb{E}$, l'étude de la primalité de x se ramène à celle de $N(x)$.

Proposition 19. *Soit $x=a+b\omega\in\mathbb{E}$, où $a,b\in\mathbb{Z}$.*

- *Si x est associé à un entier relatif, alors $x \in \mathcal{P}[\mathbb{E}]$ si et seulement si $|x| \in \mathcal{P}[\mathbb{Z}]$ et $|x| \equiv 2 \bmod 3$.*
- *Sinon, $x \in \mathcal{P}[\mathbb{E}]$ si et seulement si $N(x) \in \mathcal{P}[\mathbb{Z}]$.*

Démonstration.

- Supposons x associé à un entier relatif p. On a $x = \pm p$ ou $x = \pm p\omega$ ou $x = \pm p\omega^2$, et donc $|x| = |p|$. Il suffit d'appliquer la proposition 18.
- Supposons que x n'est pas associé à un entier relatif.

  Supposons x composé dans $\mathbb{E}$. Soient $a, b \in \mathbb{E}$ non inversibles tels que $x = ab$. En passant aux normes, $N(x) = N(a)N(b)$. Comme $N(a)$ et $N(b)$ sont différents de 1, $N(x)$ est composé dans $\mathbb{Z}$.

  Inversement, supposons x premier dans $\mathbb{E}$. On a $N(x) = x\overline{x}$, donc x divise $N(x)$ dans $\mathbb{E}$. Par le lemme d'Euclide, x divise l'un des facteurs premiers de $N(x)$ dans $\mathbb{Z}$. Soit p un tel facteur premier. On a $x|p$, donc aussi $\overline{x}|\overline{p} = p$, d'où $N(x) = x\overline{x}|p^2$. De là, $N(x) = 1$, p ou p^2. Comme x est premier, $N(x) \neq 1$. Il reste à voir que $N(x) \neq p^2$. Supposons le contraire. Écrivons $p = xy$ où $y \in \mathbb{E}$. En passant aux normes,

  $$p^2 = N(p) = N(x)N(y) = p^2N(y)$$

  donc $N(y) = 1$, c'est à dire y est inversible. De là, x et p sont associés, contradiction.

□

Pour prendre les choses « à l'envers » soit p un entier naturel premier.

- Si $p \equiv 2 \bmod 3$, alors $\pm p$, $\pm p\omega$ et $\pm p\omega^2$ sont premiers dans $\mathbb{E}$.
- Si $p \equiv 1 \bmod 3$, alors $p = a^2 + ab + b^2$ où $a, b \in \mathbb{Z}$. L'entier d'Eisenstein $a + b\omega$ et ses associés sont alors premiers dans $\mathbb{E}$.
- Tous les entiers d'Eisenstein premiers sont obtenus de cette façon.

Donnons quelques détails sur l'unicité dans le cas numéro 2.

Proposition 20. *Soit $p \in \mathcal{P}^+[\mathbb{Z}]$ congru à 1 modulo 3. Il existe exactement deux couples $(a, b) \in \mathbb{N}^2$ tels que $p = a^2 + ab + b^2$. Si (a, b) est l'un des deux couples, l'autre est (b, a).*

Démonstration. supposons $p = x\overline{x} = y\overline{y}$ où x et y sont premiers dans $\mathbb{E}$. x divise $y\overline{y}$ et x est premier, donc x divise y ou x divise $\overline{y}$. Par exemple, x divise y. Soit $z \in \mathbb{E}$ tel que $y = xz$. On a $x\overline{x} = z\overline{z}x\overline{x}$, d'où $N(z) = z\overline{z} = 1$. Ainsi, x et y sont associés. Inversement, si x et y sont associés, alors $N(x) = N(y)$.

À associé près, il y a donc une unique factorisation de p sous la forme $x\overline{x}$. Or, un et un seul des associés de x (et de même pour $\overline{x}$) appartient à $\mathcal{S}$. Il y a donc exactement deux couples $(a, b) \in \mathbb{N}^2$ tels que $p = a^2 + ab + b^2$. Pour terminer, si (a, b) convient alors, par symétrie, (b, a) convient aussi. De plus, $a \neq b$ sinon $p = 3a^2$, impossible puisque $p \equiv 1 \bmod 3$. □

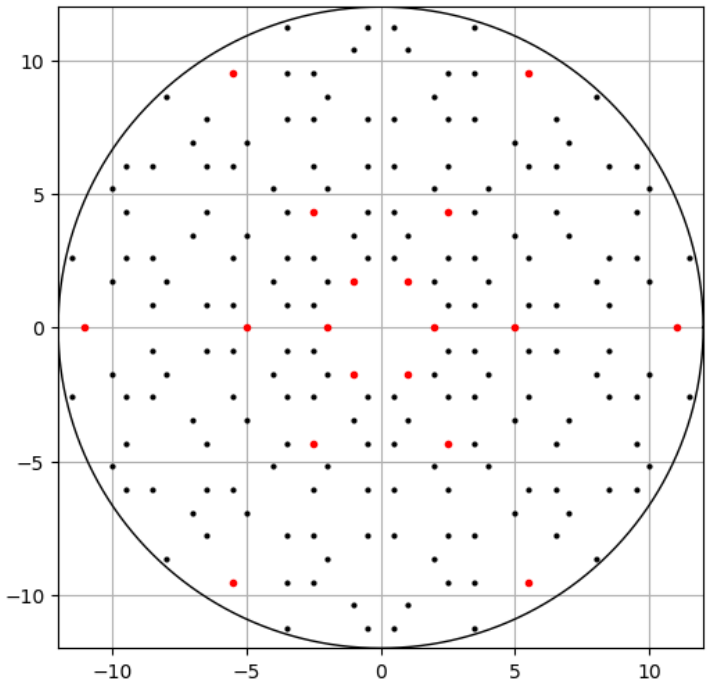

FIGURE 2 – Quelques entiers d'Eisenstein premiers. En rouge, les éléments associés à un entier naturel premier congru à 2 modulo 3.

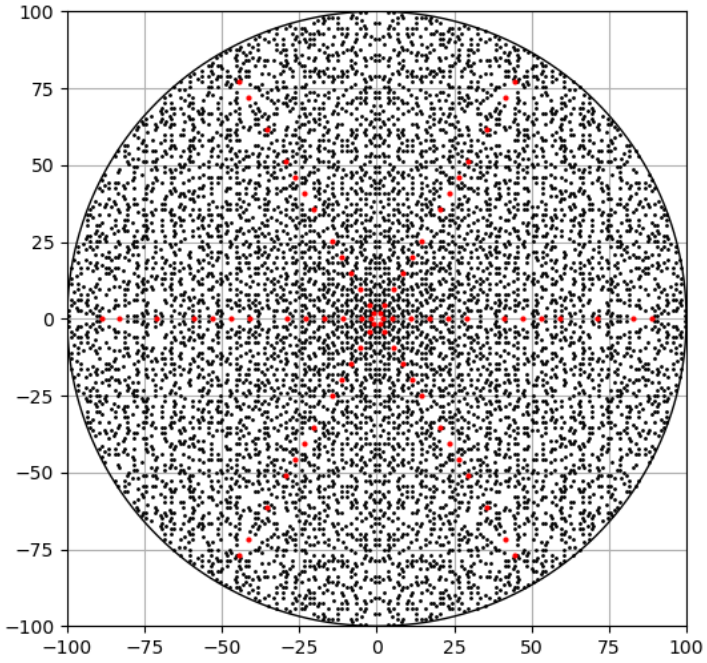

FIGURE 3 – Une vue élargie de $\mathcal{P}[\mathbb{E}]$.

4 Factorialité

4.1 Le théorème de décomposition unique

L'anneau $\mathbb{E}$ est un anneau principal, il est donc aussi *factoriel* : tout élément non nul de $\mathbb{E}$ s'écrit de façon « unique » comme un produit d'entiers de Gauss premiers. Nous allons préciser un peu la question de l'unicité.

Rappelons que

$$\mathcal{S} = \{z \in \mathbb{C} \setminus \{0\} : 0 \leq \arg(z) < \pi/3\} = \{a + b\omega : a \in \mathbb{R}_+^*, b \in \mathbb{R}_+\}$$

et

$$\mathcal{P}^+[\mathbb{E}] = \mathcal{P}[\mathbb{E}] \cap \mathcal{S}$$

Lemme 21. *Soit $x \in \mathbb{E} \setminus \mathbb{U}_6$. L'entier d'Eisenstein x possède un diviseur $p \in \mathcal{P}^+[\mathbb{E}]$.*

Démonstration. Procédons par récurrence sur $n = N(x)$. La propriété est trivialement vérifiée pour $n = 1$ puisque'il n'y a aucun entier d'Einsenstein non inversible de norme 1. Soit maintenant $n \geq 2$. Supposons la propriété vérifiée pour tous les entiers de Gauss non inversibles de norme strictement inférieure à n. Soit $x \in \mathbb{E} \setminus \mathbb{U}_6$ de norme n. Si x est premier, alors, par le lemme précédent, un (et un seul) des associés de x appartient à $\mathcal{P}^+[\mathbb{E}]$. Cet associé divise x. Si x n'est pas premier, alors $x = ab$ où $a, b \in \mathbb{E}$ ne sont pas inversibles. On a $n = N(x) = N(a)N(b) > N(a)$. Par l'hypothèse de récurrence, il existe $p \in \mathcal{P}^+[\mathbb{E}]$ tel que p divise a. Comme a divise x, p divise x. □

Proposition 22. *Soit $x \in \mathbb{E}$ non nul. L'entier d'Eisenstein x s'écrit de façon unique*

$$x = u \prod_{p \in \mathcal{P}^+[\mathbb{E}]} p^{\nu_p}$$

où $u \in \mathbb{U}_6$ et les ν_p sont des entiers naturels presque tous nuls.

Démonstration. Montrons l'existence par récurrence forte sur $N(x)$. Si $N(x) = 1$, il suffit de poser $u = x \in \mathbb{U}_6$ et pour tout $p \in \mathcal{P}^+[\mathbb{E}]$, $\nu_p = 0$. Soit $n > 1$. Supposons l'existence de la décomposition assurée pour tous les entiers d'Eisenstein non nuls de norme strictement inférieure à n. Soit $x \in \mathbb{E}$ de norme n. Par le lemme précédent, il existe $p_0 \in \mathcal{P}^+[\mathbb{E}]$ qui divise x. On a $x = p_0 x'$ où $x' \in \mathbb{E}$, $x' \neq 0$ et $N(x') < N(x)$. Par l'hypothèse de récurrence,

$$x' = u \prod_{p \in \mathcal{P}^+[\mathbb{E}]} p^{\nu'_p}$$

où $u \in \mathbb{U}_6$ et les ν'_p sont des entiers naturels presque tous nuls. On a alors

$$x = u \prod_{p \in \mathcal{P}^+[\mathbb{E}]} p^{\nu_p}$$

où $\nu_p = \nu'_p$ si $p \neq p_0$ et $\nu_{p_0} = \nu'_{p_0} + 1$.

Passons à l'unicité. Supposons

$$(\star)\ u \prod_{p\in\mathcal{P}^+[\mathbb{E}]} p^{\nu_p} = u' \prod_{p\in\mathcal{P}^+[\mathbb{E}]} p^{\nu'_p}$$

où $u, u' \in \mathbb{U}_6$ et les ν_p, ν'_p sont des entiers naturels presque tous nuls. Soit $p_0 \in \mathcal{P}^+[\mathbb{E}]$. L'entier d'Eisenstein p_0 est premier avec tous les $p \neq p_0$, donc $p_0^{\nu_{p_0}}$ est premier avec le produit des $p^{\nu'_p}$, $p \neq p_0$. En appliquant le lemme de Gauss, on en déduit que $p_0^{\nu_{p_0}}$ divise $p_0^{\nu'_{p_0}}$. De même, $p_0^{\nu'_{p_0}}$ divise $p_0^{\nu_{p_0}}$. Ainsi, il existe $v \in \mathbb{U}_6$ tel que

$$p_0^{\nu'_{p_0}} = v p_0^{\nu_{p_0}}$$

En passant aux normes,

$$N(p_0)^{\nu'_{p_0}} = N(p_0)^{\nu_{p_0}}$$

Cette égalité entre entiers naturels entraîne $\nu'_{p_0} = \nu_{p_0}$. Ainsi, pour tout $p \in \mathcal{P}^+[\mathbb{E}]$, $\nu'_p = \nu_p$. En reportant dans $(\star)$, on obtient pour terminer $u' = u$. □

4.2 La décomposition en pratique

Dans ce paragraphe, nous allons voir que pour décomposer un entier d'Eisenstein en produit d'entiers d'Eisenstein premiers, il suffit de savoir décomposer un entier relatif en produit d'entiers relatifs premiers.

Soit $x \in \mathbb{E} \setminus \{0\}$. Écrivons

$$x = u \prod_{p\in\mathcal{P}^+[\mathbb{E}]} p^{\nu_p}$$

où $u \in \mathbb{U}_6$ et les ν_p sont des entiers naturels presque tous nuls. On a

$$N(x) = \prod_{p\in\mathcal{P}^+[\mathbb{E}]} N(p)^{\nu_p}$$

Comme $N(x) \in \mathbb{N}^*$, on peut décomposer $N(x)$ en produit d'entiers naturels premiers. Supposons connue cette décomposition :

$$N(x) = \prod_{q\in\mathcal{P}^+[\mathbb{Z}]} q^{\mu_q}$$

où les μ_q sont des entiers naturels presque tous nuls.

Il s'agit de déterminer les ν_p en fonction des μ_q. Discutons sur $q \in \mathcal{P}^+[\mathbb{Z}]$.

- Tout d'abord, $\nu_{1+\omega} = \mu_3$.
- Si $q \in \mathcal{P}^+[\mathbb{Z}]$ est congru à 2 modulo 3, alors $q \in \mathcal{P}^+[\mathbb{E}]$ et $2\nu_q = \mu_q$.
- Si q est un entier naturel premier congru à 1 modulo 3, alors q s'écrit de façon quasi-unique $q = a^2 + ab + b^2$ où $a, b \in \mathbb{N}^*$. Nous avons vu qu'il y a 2 couples (a, b) d'entiers naturels qui conviennent. Ces 2 couples correspondent à 2 éléments p et p' distincts de $\mathcal{P}^+[\mathbb{E}]$ dont q est la norme. On a dans ce cas $\nu_p + \nu_{p'} = \mu_q$. Si $\mu_q \neq 0$, on peut, algorithmiquement, effectuer des divisions successives de x par p pour obtenir ν_p. On en déduit alors $\nu_{p'}$.

Une fois déterminés les ν_p, on obtient u par une simple division.

Exemple. Soit $x = 54929 - 21217\omega$. On a

$$N(x) = 2301927537 = 3 \times 7^4 \times 13^2 \times 31 \times 61$$

La méthode que nous venons de décrire permet d'obtenir la décomposition

$$x = \omega(1+\omega)(1+2\omega)^2(2+\omega)^2(1+3\omega)^2(5+\omega)(5+4\omega)$$

La figure ci-dessous représente les diviseurs premiers de x. En rouge, les diviseurs qui appartiennent à $\mathcal{S}$ (et donc apparaissent dans la décomposition de z). Remarquons les deux diviseurs $2+\omega$ et $1+2\omega$ qui ont même norme.

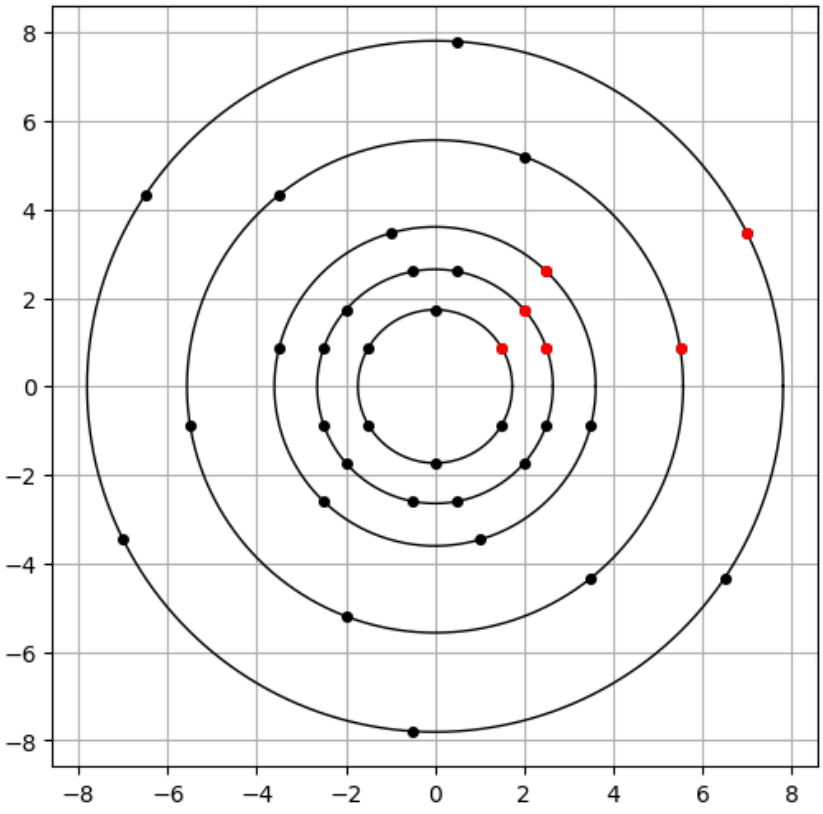

FIGURE 4 – Les diviseurs premiers de $54929 - 21217\omega$