Entiers de Gauss : $\mathbb{Z}[i]$

Damien Mégy

26 octobre 2023

Table des matières

1 **Rappels rapides sur $\mathbb{Z}$** 1

2 **Entiers de Gauss : $\mathbb{Z}[i]$** 2

1 Rappels rapides sur $\mathbb{Z}$

1. $\mathbb{Z}$ est ce qu'on appelle un anneau commutatif : il y a une addition et une multiplication, qui vérifient les propriétés attendues (distributivité, commutativité c'est-à-dire $ab = ba$, je ne fais pas la liste complète).
2. Dans $\mathbb{Z}$, on dit que a divise b s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. Par exemple -2 divise 6.
3. Les *unités* sont les éléments inversibles dans $\mathbb{Z}$. Ce sont 1 et -1 (aucun autre nombre relatif n'est inversible dans $\mathbb{Z}$ (être inversible dans $\mathbb{Z}$ c'est posséder un inverse qui est lui aussi dans $\mathbb{Z}$). Deux éléments qui se déduisent l'un de l'autre par multiplication par un inversible sont dits *associés*. Dans le cas de $\mathbb{Z}$, n est associé à $-n$. Pour les entiers de Gauss, tout ceci sera moins simple.
4. Un élément est dit irréductible si, modulo multiplication par un inversible, il ne possède que deux diviseurs : 1 et lui-même. Par exemple, à proprement parler, -3 possède quatre diviseurs dans $\mathbb{Z}$: ± 1 et ± 3. Mais justement, si on néglige la multiplication par un inversible, il n'y a que deux diviseurs. Traditionnellement on appelle nombre premier un irréductible positif. Tout nombre entier relatif peut être écrit comme le produit d'irréductibles. Quitte à groupe les éventuels signes, on peut dire que tout nombre relatif est le produit de nombres premiers et d'un inversible. Là encore, avec les entiers de Gauss il y a plus d'inversibles donc il faudra faire attention.
5. On a une division euclidienne : pour tout couple (a, b) d'entiers avec b non nul, on peut diviser a par b avec reste, c'est-à-dire qu'il existe un couple (q, r) avec $|r| < |b|$ (inégalité stricte) tel que $a = bq + r$. On dit que l'anneau est *euclidien*. De là on déduit la plupart des propriétés de $\mathbb{Z}$, dont :
6. L'anneau $\mathbb{Z}$ est un anneau *factoriel* : la décomposition en produit d'irréductibles est unique modulo permutation des termes et modulo multiplication par des inversibles. Une façon moins alambiquée de le dire est qu'un nombre positif est produit de nombres premiers de manière unique modulo permutations.
7. L'anneau $\mathbb{Z}$ est un anneau *principal* : en particulier, si on prend deux éléments, ils possèdent un pgcd (unique modulo multiplication par des inversibles, c'est-à-dire dans notre cas, unique modulo le signe). Mais on pourrait dire que 6 et 4 ont en fait deux PGCD : 2 et -2, qui sont associés. Dans les entiers de Gauss, là aussi on aura plusieurs pgcd, tous associés entre eux, mais ça sera moins simple d'en choisir un spécial (ici, on choisit le positif). Il y a aussi un ppcm (ou *des* ppcms, tous associés). Et on a des théorèmes sur les pgcd, comme $a \wedge b = a \wedge (a + b)$ ou des choses comme ça. Ceci est la base pour faire tourner l'algorithme d'Euclide et trouver les pgcd en pratique.
8. Deux éléments sont premiers entre eux si leur pgcd est 1.

9. Et enfin, si on fixe n, on peut calculer modulo n, avec des congruences. Comme on travaille avec des congruences modulo des entiers, on peut multiplier les congruences [1]. Ça aussi, on pourra faire dans $\mathbb{Z}[i]$ mais ça sera un peu différent.

2 Entiers de Gauss : $\mathbb{Z}[i]$

Il existe énormément d'anneaux : anneaux de nombres (quadratiques, algébriques), de polynômes (à une ou plusieurs variables), anneaux plus étonnants , par exemple les entiers p-adiques (des nombres entiers écrits en base p, mais où on autorise une infinité de chiffres!). Tous ne sont pas euclidiens, ni factoriels, ni principaux etc. L'étude des anneaux en général est faite après le bac, c'est le début de la théorie algébrique des nombres et de la géométrie algébrique, et c'est magnifique! Ici on ne regarde qu'un exemple très spécial d'anneau : l'anneau $\mathbb{Z}[i]$ des entiers de Gauss. Il est extrêmement spécial car comme $\mathbb{Z}$, il est euclidien :

1. Définition : $\mathbb{Z}[i]$ est l'ensemble des nombres complexes de la forme $a+ib$ avec a et b entiers relatifs. Par exemple $2+3i$, 1, 2, 5, $4i$, $7i$, $5-7i$ etc. Les éléments de $\mathbb{Z}[i]$ sont appelés *entiers de Gauss*.
2. On peut additionner et multiplier comme les nombres complexes. On obtient un anneau commutatif.
3. Nouveauté : on dispose de la conjugaison et du module! Le module va un peu ressembler à la valeur absolue sur $\mathbb{Z}$, mais la conjugaison est vraiment quelque chose de nouveau que l'on va exploiter.
4. Notation : si $\alpha = a+ib$ est un entier de Gauss, on note $N(\alpha) = |\alpha|^2 = \alpha\bar{\alpha} = a^2+b^2$. On l'appelle la *norme* de α. Montrer que la norme est multiplicative : $N(\alpha\beta) = N(\alpha)N(\beta)$. La norme est un entier positif, c'est une des façons standard de repasser des entiers de Gauss aux entiers relatifs usuels. Par exemple si l'entier de Gauss α divise l'entier de Gauss β, alors l'entier usuel $N(\alpha)$ divise l'entier $N(\beta)$.
5. La définition de divisibilité est la même que dans $\mathbb{Z}$, mais en remplaçant $\mathbb{Z}$ par $\mathbb{Z}[i]$: si α et β sont deux entiers de Gauss, on dit que α divise β s'il existe un entier de Gauss γ tel que $\beta = \alpha\gamma$. Par exemple, $1+i$ divise 2, car $2 = (1+i)(1-i)$. On voit en passant que $1-i$ divise également 2. On commence à voir des choses intéressantes.
6. Mais auparavant, les inversibles : comme dans $\mathbb{Z}$, les inversibles sont les entiers de Gauss qui possèdent un inverse qui est un entier de Gauss. Par exemple, 1 et -1 sont inversibles bien sûr. Mais aussi i, puisque $\frac{1}{i} = -i$ est un entier de Gauss. Exercice : les entiers de Gauss inversibles sont ± 1 et $\pm i$. Il y en a donc quatre. ceci va un peu compliquer les choses, mais aussi les embellir.
7. Deux entiers de Gauss qui se déduisent l'un de l'autre par multiplication par un inversible sont dits associés. Donc par exemple 2 et -2 sont associés. Mais ils sont également associés à $2i$ et $-2i$. Les associés vont donc par paquets de quatre (à part zéro). Noter que $1+2i$ et $-2+i$ sont associés. Voir l'association est un peu moins immédiat, il faut faire attention.
8. Il y a les analogues de nombres premiers : on dit qu'un entier de Gauss est irréductible si, modulo inversible, il possède exactement deux diviseurs : 1 et lui-même. ATTENTION : 2 n'est pas irréductible dans les entiers de Gauss, comme on l'a vu plus haut : $2 = (1+i)(1-i)$ et 5 non plus car $5 = (2+i)(2-i)$. Par contre, 3 est toujours irréductible. Donc attention, les nombres premiers dans $\mathbb{Z}$ ne sont plus forcément « premiers ». dans $\mathbb{Z}[i]$. Un entier de Gauss irréductible est appelé *premier de Gauss*. De la même façon que 1 n'est pas premier, les entiers de Gauss ± 1 et $\pm i$ ne sont pas des premiers de Gauss.

1. La multiplication de congruences et quelque chose de miraculeux et profond et surtout, faux pour des congruences générales, par exemple pour des congruences modulo 2π. En effet on a $\pi \equiv 3\pi\ [2\pi]$ et $\pi \equiv 5\pi\ [2\pi]$ mais on n'a absolument pas $\pi^2 \equiv 15\pi^2\ [2\pi]$!!

9. Attention il existe des premiers de Gauss qui ne sont pas des nombres premiers. Par exemple $1+i$ (et donc ses associés : $-1+i$, $-1-i$ et $1-i$). (Exercice)
10. Il existe une division euclidienne, le module joue le rôle de la valeur absolue. Essayer de deviner comment marche cette division euclidienne : comment diviser $5+3i$ par 2, par exemple ? Attention, le quotient et le reste ne sont pas uniques, cette fois, mais ce n'est pas très gênant.
11. Les conséquences sont les mêmes : existence de pgcd et unicité à inversible près, existence et unicité de la décomposition en irréductibles !! Tous les lemmes classiques restent grosso-modo les mêmes.
12. Deux éléments sont premiers entre eux si 1 est un de leurs pgcds.

Problème 1. Montrer que si deux entiers relatifs sont premiers entre eux dans $\mathbb{Z}$, alors ils sont premiers entre eux dans $\mathbb{Z}[i]$.

Problème 2. Montrer que $1+2i$, $1-2i$, 7, $2+3i$ sont des premiers de Gauss.

Problème 3. Parmi les dix premiers nombres premiers, lesquels sont des premiers de Gauss ? Que peut-on conjecturer ? Tester la conjecture sur les nombres nombres premiers suivants.

Problème 4. Trouver tous les entiers de Gauss qui divisent 2, 3, 4, 5, pousser jusqu'à 10. En déduire « la » factorisation en produit de premiers de Gauss de ces nombres. (Guillemets car la décomposition est unique uniquement modulo inversibles.)

Problème 5. Parmi les entiers de Gauss $a+ib$ avec $1 \leq a, b \leq 10$ trouver tous les premiers de Gauss. Faire comme lorsqu'on cherche les nombres premiers entre 1 et 100 (ou 1000) : crible. (Mais avec des multiples complexes. Utiliser la norme pour borner la « taille » des diviseurs possibles.)

Problème 6. Que dire la norme de ces éléments irréductibles ? Que peut-on conjecturer ?

Problème 7. Trouver un exemple de couple d'entiers de Gauss (a, b) pour lequel la division euclidienne de a par b n'est pas unique. (En général, il y a au maximum quatre choix pour b : pourquoi ?)

Problème 8. Montrer que si un nombre premier n'est pas irréductible dans $\mathbb{Z}[i]$, alors il est somme de deux carrés.

Problème 9. Montrer que si un ombre premier p est somme de deux carrés, il n'est pas irréductible dans $\mathbb{Z}[i]$ et que cette décomposition en somme de deux carrés est unique.

Problème 10. On suppose que le nombre premier p est congru à 1 modulo 4. Montrer qu'il n'est pas irréductible à l'aide du théorème de Wilson.

Problème 11. Soit p un nombre premier. Montrer que si $p \equiv 3[4]$, alors il est irréductible dans $\mathbb{Z}[i]$.

Problème 12. Trouver une condition nécessaire et suffisante sur un entier naturel n pour qu'il soit somme de deux carrés.

Problème 13. Quel est le (ou les) pgcd de $11+7i$ et $18-i$?

Problème 14. Montrer (avec des entiers de Gauss, mais trouver également d'autres preuves) que si $n > 3$ et k sont des entiers, alors $n!$ ne peut pas être égal à k^2+1.

Problème 15. Trouver tous les triplets pythagoriciens $x^2+y^2=z^2$ lorsque $x \wedge y = 1$ grâce aux entiers de Gauss. (C'est-à-dire, trouver une façon de paramétrer tous les triplets pythagoriciens.)

Problème 16. Résoudre sur $\mathbb{Z}$ l'équation

$$x^2+4=y^3.$$

Indication : montrer que $x+2i$ et $x-2i$ doivent être des cubes dans $\mathbb{Z}[i]$. Écrire $x+2i=(a+ib)^3$ et continuer...

Problème 17. Résoudre sur $\mathbb{Z}$:

$$ab + cd = 34, \quad ac - bd = 19$$

Une partie des exos de `www.fen.bilkent.edu.tr/~franz/nt/mid2a.pdf` et les autres dans les questions d'agreg!

Problème 18.

Problème 19.

Problème 20.

Problème 21.

Problème 22.

Indications

Exercice 17. Identités de ??? Celles que l'on obtient avec les nombres complexes.
Exercice 18.
Exercice 19.
Exercice 20.
Exercice 21.
Exercice 22.

Correction

Correction de l'exercice 17.
Avec des entiers de Gauss :

$$(a+id)(c+ib) = 19+34i$$

Il s'agit donc de factoriser cet entier de Gauss.

Sinon, il va s'agir d'écrire des entiers comme somme de deux carrés...

Source : `https://www.youtube.com/watch?v=gUh4dkfQ1pU`

Correction de l'exercice 18.

Correction de l'exercice 19.

Correction de l'exercice 20.

Correction de l'exercice 21.

Correction de l'exercice 22.