Terminale · maths expertes · DM

# DM n°04 — Peut-on compter en binaire avec un nombre complexe ?

CHAPITRES

Nombres complexes · Divisibilité et parité · Algorithmique · Raisonnement par descente

> *En base 2, la position d'un chiffre indique la puissance de 2 qui lui est associée. Ici, on remplace 2 par le nombre complexe $\beta = -1 + i$. À chaque changement de rang, les puissances changent à la fois de taille et de direction dans le plan. Rien ne garantit donc a priori que les deux seuls chiffres 0 et 1 suffisent encore.*

On appelle **entier de Gauss** tout nombre complexe de la forme

$$a + ib, \qquad a, b \in \mathbb{Z},$$

et l'on note

$$\mathbb{Z}[i] = \{a + ib : \ a, b \in \mathbb{Z}\}.$$

Dans toute la suite, on fixe

$$\boxed{\beta = -1 + i}.$$

Pour des chiffres $\varepsilon_0, \dots, \varepsilon_n \in \{0, 1\}$, on pose

$$(\varepsilon_n \cdots \varepsilon_1 \varepsilon_0)_\beta = \sum_{k=0}^{n} \varepsilon_k \beta^k.$$

Le chiffre situé tout à droite correspond donc à la puissance $0$. Comme en numération usuelle, des zéros ajoutés à gauche ne changent pas la valeur représentée.

## I Une base qui tourne

1 Calculer $\beta^2$, $\beta^3$ et $\beta^4$, puis en déduire $\beta^8$.

2 Calculer les nombres complexes représentés par

$$(10)_\beta, \qquad (11)_\beta, \qquad (1100)_\beta, \qquad (1101)_\beta, \qquad (100000000)_\beta.$$

Que peut-on déjà remarquer à propos des trois dernières écritures ?

## II Quel doit être le dernier chiffre ?

Soit

$$z = a + ib \in \mathbb{Z}[i].$$

3 Montrer que

$$\frac{z}{-1+i} = \frac{b-a}{2} - i\,\frac{a+b}{2}.$$

En déduire une condition nécessaire et suffisante, portant seulement sur la parité de $a$ et $b$, pour que $z/\beta$ appartienne encore à $\mathbb{Z}[i]$.

**4** **(a)** Montrer que parmi les deux nombres $z$ et $z-1$, exactement l'un a un quotient par $\beta$ qui appartient à $\mathbb{Z}[i]$.

**(b)** En déduire qu'il existe un unique chiffre $\varepsilon_0 \in \{0,1\}$ tel que

$$z_1 = \frac{z-\varepsilon_0}{\beta}$$

soit encore un entier de Gauss. Exprimer $\varepsilon_0$ en fonction de la parité de $a$ et $b$.

On peut alors recommencer avec $z_1$, puis avec $z_2$, etc. À chaque étape,

$$z_k = \varepsilon_k + \beta z_{k+1}.$$

**5** Appliquer cet algorithme à $z = 4+3i$. Présenter les valeurs successives de $z_k$ et des chiffres $\varepsilon_k$, jusqu'à atteindre éventuellement $0$.

En déduire une écriture de $4+3i$ en base $\beta$, puis la vérifier directement à l'aide des puissances de $\beta$.

## III L'algorithme finit-il toujours ?

Trouver un chiffre à chaque étape ne suffit pas : pour obtenir une véritable numération, il faut encore démontrer que le procédé ne peut pas se poursuivre indéfiniment.

Partons d'un entier de Gauss $z = z_0$ et effectuons quatre étapes. Si $0$ est atteint plus tôt, on peut prolonger le procédé en prenant ensuite uniquement des chiffres nuls. On obtient ainsi des chiffres $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3$ et un entier de Gauss $z_4$.

**6** **(a)** Montrer que

$$z = \varepsilon_0 + \varepsilon_1\beta + \varepsilon_2\beta^2 + \varepsilon_3\beta^3 - 4z_4.$$

**(b)** On pose

$$r = \varepsilon_0 + \varepsilon_1\beta + \varepsilon_2\beta^2 + \varepsilon_3\beta^3.$$

Montrer que

$$r = (\varepsilon_0 - \varepsilon_1 + 2\varepsilon_3) + i(\varepsilon_1 - 2\varepsilon_2 + 2\varepsilon_3),$$

puis établir

$$|\operatorname{Re}(r)| \leq 3, \qquad |\operatorname{Im}(r)| \leq 3.$$

**7** Pour $w = x + iy \in \mathbb{Z}[i]$, on pose

$$M(w) = \max(|x|, |y|).$$

Écrire $z = a+ib$ et $z_4 = A+iB$. À l'aide de la question précédente, montrer que

$$M(z_4) \leq \frac{M(z)+3}{4}.$$

En déduire que

$$M(z) > 1 \quad \Longrightarrow \quad M(z_4) < M(z).$$

Expliquer pourquoi, après un nombre fini de blocs de quatre étapes, l'algorithme atteint nécessairement un entier de Gauss $w$ tel que $M(w) \leq 1$.

**8** Il n'existe que huit entiers de Gauss non nuls vérifiant $M(w) \leq 1$. Les déterminer, puis appliquer à chacun la règle de la partie II pour montrer que l'algorithme finit par atteindre $0$.

Conclure que tout entier de Gauss possède au moins une écriture finie en base $\beta$ avec les seuls chiffres $0$ et $1$.

## IV Peut-il y avoir deux écritures ?

**9** Supposons qu'un même entier de Gauss $z$ possède deux écritures finies

$$z = (\varepsilon_n \cdots \varepsilon_0)_\beta = (\delta_m \cdots \delta_0)_\beta.$$

Montrer que $\varepsilon_0 = \delta_0$.

Après avoir retiré ce chiffre commun et divisé par $\beta$, expliquer pourquoi le même raisonnement peut être recommencé. En déduire que les deux suites de chiffres coïncident, une fois les éventuels zéros initiaux supprimés.

**10** Formuler précisément le résultat obtenu sur l'existence et l'unicité de l'écriture des entiers de Gauss dans cette base.

## V Un signe moins devenu inutile

**11** Déterminer les écritures en base $\beta$ de

$$i, \qquad -i, \qquad -1.$$

Vérifier également que

$$-2 + 3i = (11011)_\beta$$

et que la règle d'addition

$$1 + 1 = (1100)_\beta$$

est correcte.

Expliquer en quelques phrases pourquoi cette numération n'a besoin ni d'un symbole séparé pour la partie imaginaire, ni d'un symbole « $-$ » pour représenter des entiers négatifs.

### Repère historique

En 1965, Walter Penney publie un court article consacré à un système « binaire » pour les nombres complexes fondé sur la base $-1+i$ et les deux chiffres $0$ et $1$. Le système permet de traiter un nombre complexe à coordonnées entières comme une seule quantité, sans coder séparément ses parties réelle et imaginaire.