CORRIGÉ

Terminale · maths expertes · CORRIGÉ

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

CHAPITRES

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

I Une base qui tourne

1

Avec $\beta = -1 + i$,

$$\beta^2 = (-1+i)^2 = -2i.$$

Puis

$$\beta^3 = (-2i)(-1+i) = 2 + 2i,$$

et

$$\beta^4 = (2+2i)(-1+i) = -4.$$

Ainsi

$$\boxed{\beta^4 = -4}.$$

En élevant cette égalité au carré,

$$\boxed{\beta^8 = 16}.$$

2

Par définition,

$$(10)_\beta = \beta = -1 + i, \qquad (11)_\beta = 1 + \beta = i.$$

Ensuite,

$$(1100)_\beta = \beta^3 + \beta^2 = (2+2i) - 2i = 2,$$
$$(1101)_\beta = \beta^3 + \beta^2 + 1 = 3,$$

et

$$(100000000)_\beta = \beta^8 = 16.$$

On obtient donc directement des entiers réels positifs à partir d'une base complexe :

$$\boxed{2 = (1100)_\beta, \qquad 3 = (1101)_\beta, \qquad 16 = (100000000)_\beta.}$$

II Quel doit être le dernier chiffre ?

3

On rationalise le dénominateur :

$$\frac{a+ib}{-1+i} = \frac{(a+ib)(-1-i)}{(-1+i)(-1-i)}.$$

Le dénominateur vaut 2, tandis que

$$(a+ib)(-1-i) = (b-a) - i(a+b).$$

Par conséquent,

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

Ce quotient appartient à $\mathbb{Z}[i]$ si et seulement si $b-a$ et $a+b$ sont pairs. Cela équivaut à dire que a et b ont la même parité. Ainsi,

$$\boxed{\frac{a+ib}{\beta} \in \mathbb{Z}[i] \iff a \text{ et } b \text{ ont la même parité.}}$$

4

(a) Si a et b ont la même parité, alors $z = a+ib$ est divisible par β au sens de la question, tandis que les coordonnées de

$$z - 1 = (a-1) + ib$$

ont des parités différentes.

Inversement, si a et b ont des parités différentes, alors z n'est pas divisible par β, mais $a-1$ et b ont la même parité : $z-1$ l'est.

Exactement l'un des deux nombres z et $z-1$ convient.

(b) Le chiffre des unités est donc imposé :

$$\boxed{\varepsilon_0 = \begin{cases} 0, & \text{si } a \text{ et } b \text{ ont la même parité,} \\ 1, & \text{sinon.} \end{cases}}$$

Alors

$$z_1 = \frac{z-\varepsilon_0}{\beta} \in \mathbb{Z}[i]$$

et

$$z = \varepsilon_0 + \beta z_1.$$

En utilisant la formule de la question 3 avec $z - \varepsilon_0 = (a-\varepsilon_0) + ib$, on obtient aussi

$$\boxed{z_1 = \frac{b-a+\varepsilon_0}{2} - i\,\frac{a+b-\varepsilon_0}{2}.}$$

5

Partons de $z_0 = 4 + 3i$. À chaque ligne, le chiffre est déterminé par la parité des deux coordonnées.

k	z_k	ε_k	z_{k+1}
0	$4+3i$	1	$-3i$
1	$-3i$	1	$-1+2i$
2	$-1+2i$	1	2
3	2	0	$-1-i$
4	$-1-i$	0	i
5	i	1	1
6	1	1	0

Les chiffres sont obtenus du rang le plus faible au rang le plus élevé :

$$\varepsilon_0, \dots, \varepsilon_6 = 1, 1, 1, 0, 0, 1, 1.$$

L'écriture se lit donc dans l'autre sens :

$$\boxed{4 + 3i = (1100111)_\beta}.$$

Pour la vérifier, on utilise

$$\beta^5 = -4\beta = 4 - 4i, \qquad \beta^6 = -4\beta^2 = 8i.$$

Alors

$$\begin{aligned}(1100111)_\beta &= \beta^6 + \beta^5 + \beta^2 + \beta + 1 \\ &= 8i + (4 - 4i) - 2i + (-1 + i) + 1 \\ &= 4 + 3i.\end{aligned}$$

III L'algorithme finit-il toujours ?

6

(a) À chaque étape,

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

En remplaçant successivement z_1, z_2 puis z_3, on obtient

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

Comme $\beta^4 = -4$,

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

(b) Avec

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

et

$$\beta = -1 + i, \qquad \beta^2 = -2i, \qquad \beta^3 = 2 + 2i,$$

il vient

$$\boxed{r = (\varepsilon_0 - \varepsilon_1 + 2\varepsilon_3) + i(\varepsilon_1 - 2\varepsilon_2 + 2\varepsilon_3).}$$

Comme chaque ε_j vaut 0 ou 1,

$$-1 \leq \varepsilon_0 - \varepsilon_1 + 2\varepsilon_3 \leq 3$$

et

$$-2 \leq \varepsilon_1 - 2\varepsilon_2 + 2\varepsilon_3 \leq 3.$$

Donc

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

7

Écrivons

$$z = a + ib, \qquad z_4 = A + iB, \qquad r = u + iv.$$

La relation $z = r - 4z_4$ donne

$$a = u - 4A, \qquad b = v - 4B,$$

donc

$$A = \frac{u - a}{4}, \qquad B = \frac{v - b}{4}.$$

Puisque $|u| \leq 3$ et $|v| \leq 3$,

$$|A| \leq \frac{|a| + 3}{4}, \qquad |B| \leq \frac{|b| + 3}{4}.$$

Ainsi,

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

Si $M(z) > 1$, alors

$$M(z) + 3 < 4M(z),$$

d'où

$$\boxed{M(z_4) < M(z).}$$

Les coordonnées des z_k étant entières, $M(z_k)$ est un entier naturel. Tant que $M > 1$, chaque bloc de quatre étapes fait donc strictement diminuer cet entier. Une descente stricte dans $\mathbb{N}$ ne peut pas durer indéfiniment : après un nombre fini de blocs, on atteint nécessairement un entier de Gauss w tel que

$$\boxed{M(w) \leq 1}.$$

8

Les huit entiers de Gauss non nuls tels que $M(w) \leq 1$ sont

$$1,\ -1,\ i,\ -i,\ 1+i,\ 1-i,\ -1+i,\ -1-i.$$

La règle de la partie II donne les transitions suivantes :

$$1-i \longrightarrow -1 \longrightarrow 1+i \longrightarrow -i \longrightarrow i \longrightarrow 1 \longrightarrow 0,$$
$$-1+i \longrightarrow 1 \longrightarrow 0, \qquad -1-i \longrightarrow i \longrightarrow 1 \longrightarrow 0.$$

Ces trois chaînes contiennent les huit valeurs possibles et atteignent toutes 0.

Tout entier de Gauss finit donc par atteindre 0. En remontant les relations

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

on obtient une écriture finie

$$z = \varepsilon_0 + \varepsilon_1\beta + \cdots + \varepsilon_n\beta^n, \qquad \varepsilon_k \in \{0,1\}.$$

Ainsi,

$$\boxed{\text{tout entier de Gauss possède au moins une écriture finie en base } \beta.}$$

IV Peut-il y avoir deux écritures ?

9

Supposons

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

Dans la première écriture, $z - \varepsilon_0$ a un quotient par β dans $\mathbb{Z}[i]$. Dans la seconde, il en va de même pour $z - \delta_0$.

Or la question 4 a montré qu'il existe un *unique* chiffre parmi 0 et 1 ayant cette propriété. Par conséquent,

$$\boxed{\varepsilon_0 = \delta_0}.$$

Retirons ce chiffre commun puis divisons par β :

$$\frac{z - \varepsilon_0}{\beta} = (\varepsilon_n \cdots \varepsilon_1)_\beta = (\delta_m \cdots \delta_1)_\beta.$$

Le même raisonnement impose alors $\varepsilon_1 = \delta_1$, puis $\varepsilon_2 = \delta_2$, et ainsi de suite.

Si l'une des écritures est plus courte, on peut la compléter à gauche par des zéros sans en changer la valeur. Tous les chiffres coïncident donc. Une fois les zéros initiaux supprimés, l'écriture est unique.

10

On obtient le résultat suivant :

Tout entier de Gauss $a+ib$, avec $a,b\in\mathbb{Z}$, possède une unique représentation finie normalisée

$$a+ib=\sum_{k=0}^{n}\varepsilon_k(-1+i)^k,\qquad \varepsilon_k\in\{0,1\}.$$

Pour un nombre non nul, le chiffre de plus haut rang est 1 ; le nombre 0 est représenté par 0.

V Un signe moins devenu inutile

11

Comme

$$1+\beta=1+(-1+i)=i,$$

on a

$$\boxed{i=(11)_\beta}.$$

De même,

$$1+\beta+\beta^2=1+(-1+i)-2i=-i,$$

donc

$$\boxed{-i=(111)_\beta}.$$

Enfin,

$$\begin{aligned}(11101)_\beta&=\beta^4+\beta^3+\beta^2+1\\&=-4+(2+2i)-2i+1\\&=-1,\end{aligned}$$

d'où

$$\boxed{-1=(11101)_\beta}.$$

Par ailleurs,

$$\begin{aligned}(11011)_\beta&=\beta^4+\beta^3+\beta+1\\&=-4+(2+2i)+(-1+i)+1\\&=-2+3i,\end{aligned}$$

et

$$1+1=2=(1100)_\beta.$$

Les puissances de $-1+i$ changent elles-mêmes de signe et de direction dans le plan complexe. Les chiffres n'ont donc pas à porter séparément ces informations : une seule chaîne de 0 et de 1 peut coder simultanément la partie réelle, la partie imaginaire et leurs signes.

Repère historique

Dans son article de 1965 *A "Binary" System for Complex Numbers*, Walter Penney présente la base $-1+i$ avec les seuls chiffres 0 et 1, et met en avant la possibilité de représenter en une seule écriture les nombres complexes à coordonnées entières. L'argument de terminaison par blocs de quatre utilisé aux questions 6 à 8 est une démonstration élémentaire distincte.

SOURCES

Walter Penney — A "Binary" System for Complex Numbers, Journal of the ACM, vol. 12, no 2, 1965, p. 247-248. Lien direct