A VOS STYLOS

PROBLÈME 10

(proposé par D. DUMONT)

Soit l'ensemble $E = \{0, 1, 3, 4, 7, 9, 12, 13, 16, 19, \ldots\}$ dont on propose trois définitions :

Définition 1 : E est l'ensemble des entiers n pouvant s'écrire sous la forme

$$n = x^2 + xy + y^2 \text{ avec } x, y \text{ entiers } \geq 0.$$

Définition 2 : E est l'ensemble des entiers n pouvant s'écrire sous la forme

$$n = x^2 - xy + y^2 \text{ avec } x, y \text{ entiers } \geq 0.$$

Définition 3 : E est l'ensemble des entiers n pouvant s'écrire sous la forme

$$n = x^2 + 3y^2 \text{ avec } x, y \text{ entiers } \geq 0.$$

1°) Montrer que ces trois définitions sont bien équivalentes.

2°) Montrer que E est stable pour la multiplication, c'est-à-dire que $n_1 \in E$ et $n_2 \in E \Rightarrow n_1 n_2 \in E$.

3°) Soit $P = \{3, 7, 13, 19, 31, 37, \ldots\}$ l'ensemble des nombres premiers appartenant à E. Montrer que P se compose de 3 et de l'ensemble des nombres premiers de la forme $6k + 1$, et que pour ces nombres premiers la représentation sous la forme $x^2 + 3y^2$ est unique. En outre, si p est de la forme $6k + 1$ alors $4p$ s'écrit de manière unique comme suit :

$$4p = x^2 + 27y^2 \qquad (x, y \text{ entiers } > 0).$$

Solution :

Nous avons reçu quatre solutions, respectivement de Christian CUVIER, Jacques DAUTREVAUX, Thierry DOLLINGER et Pierre RENFER. C'est la solution de ce dernier que nous publions ci-après et à laquelle nous adjoignons la bibliographie proposée par J. DAUTREVAUX.

Pour tout nombre complexe z, posons : $N(z) = |z|^2 = z\bar{z}$. Alors : pour $x \in \mathbb{Z}, y \in \mathbb{Z}, j = e^{2i\pi/3}$,

$$\begin{aligned} N(x + i\sqrt{3}y) &= x^2 + 3y^2 \\ N(x + jy) &= (x + jy)(x + \bar{j}y) = x^2 + y^2 + (j + \bar{j})xy \\ &= x^2 - xy + y^2 \end{aligned}$$

Cela suggère deux autres définitions encore pour E.

Définition 4
E est l'ensemble des entiers n pouvant s'écrire : $n = N(z)$, où z appartient à l'anneau $\mathbb{Z}(i\sqrt{3})$, $(\mathbb{Z}(i\sqrt{3}) = \{x + i\sqrt{3}y | x \in \mathbb{Z}, y \in \mathbb{Z}\})$.

Définition 5
E est l'ensemble des entiers n pouvant s'écrire : $n = N(z)$, où z appartient à l'anneau $\mathbb{Z}(j)$, $(\mathbb{Z}(j) = \{x + jy | x \in \mathbb{Z}, y \in \mathbb{Z}\})$.

1) Montrons l'équivalence des cinq définitions

- $3 \iff 4$ est évident (les signes de x et y n'interviennent pas)
- $2 \implies 5$ est évident
- $1 \implies 5$ car $x^2 + xy + y^2 = N(x - jy)$
- Pour démontrer $5 \implies 1$ et $5 \implies 2$, il suffit de prouver que $N(x + jy)$, avec $x > 0$, peut être égalé à $N(x' + jy')$ tel que xy et $x'y'$ aient des signes différents.
L'anneau $\mathbb{Z}(j)$ possède six éléments inversibles : ce sont les racines sixièmes de l'unité : $1, j, 1 + j$ et leurs opposés.
Un tel élément u vérifie : $N(u) = 1$ et pour tout z dans $\mathbb{Z}(j)$: $N(uz) = N(u)N(z) = N(z)$.
On calcule :

$$j(x + jy) = -y + (x - y)j$$
$$(1 + j)(x + jy) = (x - y) + xj.$$

Si $x \geq y > 0$ alors $j(x + jy) = x' + iy'$, avec $x'y' \leq 0$.
Si $y \geq x > 0$ alors $(1 + j)(x + jy) = x' + iy'$, avec $x'y' \leq 0$.
Si $x > 0 > y$ alors $j(x + jy) = x' + iy'$, avec $x'y' > 0$.

- Il ne reste plus qu'à démontrer : $4 \iff 5$. $4 \implies 5$ est facile, car $x + i\sqrt{3}y = (x + y) + 2yj$.
Pour $5 \implies 4$, on remarque $x + jy \in \mathbb{Z}(i\sqrt{3})$, si y est pair. Sinon, on remplace $x + jy$ par :

$$(1 + j)(x + jy) = (x - y) + xj, \quad \text{si } x \text{ est pair}$$
$$\text{ou } j(x + jy) = -y + (x - y)j, \text{ si } x \text{ et } y \text{ sont impairs}$$

2) Grâce à la définition 4 ou 5,il est facile de prouver que E reste stable par la multiplication.
Si

$$n_1 \in E \quad \text{et} \quad n_2 \in E$$

alors

$$n_1 n_2 = N(z_1)N(z_2) = N(z_1 z_2) \in E.$$

3) Soit p un nombre premier de E, distinct de 3 :

$$p \equiv x^2 \pmod 3.$$

Donc $p \equiv 0$ ou $p \equiv 1 \pmod 3$.
Mais p n'étant pas divisible par 3, $p \equiv 1 \pmod 3$.
Donc $p \equiv 1 \pmod 6$ ou $p \equiv 4 \pmod 6$.
Mais p n'étant pas divisible par 2, $p \equiv 1 \pmod 6$.

Réciproquement si $p \equiv 1 \pmod 6$ et si p est premier, il faut prouver que p appartient à E.
Soit $p = 6k + 1$.

• D'après le théorème de FERMAT, l'équation $x^{6k} - 1 = 0$ admet comme solutions les $6k$ éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$.
Or $x^{6k} - 1 = (x^{2k} + 1)(x^{4k} - x^{2k} + 1)$. L'équation $x^{4k} - x^{2k} + 1 = 0$ admet donc au moins une solution $x = a$ dans $\mathbb{Z}/p\mathbb{Z}$, ce qui signifie que p divise $a^{4k} - a^{2k} + 1 = N(a^{2k} + j)$ (élément de E).

• On peut démontrer (voir annexe) que $\mathbb{Z}(j)$ est un anneau principal. Les résultats usuels d'arithmétique y sont donc valables : notamment l'existence et l'unicité (aux éléments inversibles près) de la décomposition en facteurs premiers.

• Considérons une décomposition en facteurs premiers de $a^{2k} + j$:

$$a^{2k} + j = u\alpha_1\alpha_2 \dots \alpha_l,$$

où u est inversible et $\alpha_1, \alpha_2, \dots \alpha_l$ sont premiers.
Alors $p | N(a^{2k} + j) = u\bar{u}\alpha_1\bar{\alpha}_1\alpha_2\bar{\alpha}_2 \dots \alpha_l\bar{\alpha}_l$.
L'un des facteurs, par exemple α_1, divise p; son conjugué $\bar{\alpha}_1$ divise p aussi.
Mais p ne saurait admettre un autre facteur encore, par exemple α_2, sinon : $p^2 = N(p) = N(\alpha_1)N(\bar{\alpha}_1)N(\alpha_2)N(\bar{\alpha}_2)$ aurait quatre facteurs entiers non triviaux.
Donc : $p = \alpha_1\bar{\alpha}_1 = N(\alpha_1) \in E$.
Le choix de α_1 est unique, à un élément inversible de $\mathbb{Z}(j)$ près, ce qui conduit, d'après les calculs de 1), à une expression unique de p sous la forme $x^2 + 3y^2$, avec x, y entiers naturels.

La décomposition de $4p$ en facteurs premiers dans $\mathbb{Z}(j)$ est : $4p = 2 \times \alpha_1 \times 2 \times \bar{\alpha}_1$.
Les facteurs sont uniques à un élément inversible près.
Soit $\alpha_1 = x + jy$ alors

$$\begin{aligned} 2\alpha_1 &= (2x - y) + i\sqrt{3}y \\ 2j\alpha_1 &= -(x + 3y) + i\sqrt{3}(x - y) \\ 2(1 + j)\alpha_1 &= (x - 3y) + i\sqrt{3}(x + y). \end{aligned}$$

De ces trois éléments associés, un et un seul a pour seconde composante un multiple de 3, (y, $x - y$ ou $x + y$). D'où l'unicité de l'écriture : $4p = X^2 + 27Y^2$, avec $X \in \mathbb{N}, Y \in \mathbb{N}$.

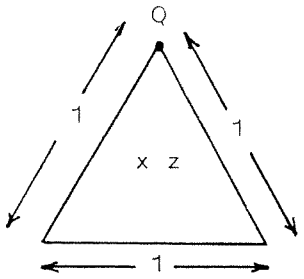
Annexe

Pour prouver que $\mathbb{Z}(j)$ est un anneau principal, il suffit de montrer qu'il est euclidien, c'est-à-dire que pour tout élément A de $\mathbb{Z}(j)$ et tout élément B non

nul de $\mathbb{Z}(j)$, il existe Q et R dans $\mathbb{Z}(j)$, tels que

$$A = BQ + R, \quad \text{avec} \quad N(R) < N(B).$$

$\mathbb{Z}(j)$ est un réseau de triangles équilatéraux dans le plan, de côtés 1.
Soit $z = A/B$. C'est un élément du corps $\mathbb{Q}(j)$.
S'il appartient à $\mathbb{Z}(j)$, on choisit $Q = z$ et $R = 0$. Sinon, il est à l'intérieur d'une maille triangulaire du réseau $\mathbb{Z}(j)$; on choisit Q égal à l'un des sommets de cette maille et $R = A - BQ$.



$$N(\frac{A}{B} - Q) < 1$$

$$\text{Donc} : N\big(A - BQ\big) = N\big(B \times (\frac{A}{B} - Q)\big) < N(B).$$

Par contre, il est intéressant de noter que $\mathbb{Z}(i\sqrt{3})$ n'est pas un anneau principal! En effet : 4 admet, par exemple, deux décompositions en facteurs premiers distincts :

$$4 = 2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3}).$$

Bibliographie

GAUSS C.-F.– *Recherches arithmétiques.*– Paris 1807 (rééd. Blanchard).
LEGENDRE A.-M.– *Théorie des nombres.*– 2 vol., Paris 1830 (rééd. Blanchard).
HUMBERT E.– *Traité d'arithmétique.*– Paris, Vuibert 1948.
TANNERY J.– *Leçons d'arithmétique.*– Paris, A. Colin 1911.

PROBLÈME 11

Enoncé

Trouver le plus petit entier positif k pour lequel il existe un polynôme à coefficients entiers, de degré k, de la forme

$$P(x) = x^k + a, x^{k-1} + \cdots + a_k$$

et tel que, pour tout entier $x \in \mathbb{Z}$, $P(x)$ soit divisible par un milliard.

Indication

Coefficients binomiaux.

PROBLÈME 12

Enoncé

Soit Ω un ouvert non vide du plan. Deux points C (chat) et S (souris) sont mobiles dans Ω et choisissent chacun à chaque instant leur vitesse, le module de cette dernière étant toutefois limité à un intervalle $[O, V]$, où la vitesse maximale V est la même pour C et S. On demande, selon la forme de Ω, si C a une stratégie imparable pour finir par rattraper S, si au contraire S a un moyen certain de toujours échapper à C, ou si ni l'un ni l'autre de ces deux cas ne se présente.

PROBLÈME 13

Enoncé

Un réel x est algébrique si et seulement s'il existe des polynômes à coefficients entiers $P(u, v)$ et $Q(u, v)$ et des entiers u_o, v_o tels que, en posant

$$u_{n+1} = P(u_n, v_n) \quad ; \quad v_{n+1} = Q(u_n, v_n)$$

on ait $v_n \neq 0$ pour tout n et $(u_n/v_n) \longrightarrow_\infty x$.

Voici une liste de personnes. Pour chacune dis-moi si pour toi, elle ressemble ou pas à un chercheur scientifique, par exemple, est-ce qu'un professeur ressemble ou ne ressemble pas à un chercheur scientifique ...

	ressemble	*ne ressemble pas*	*SR*
Un professeur	*39*	*60*	*1*
et un médecin	*71*	*29*	*0*
et un explorateur	*74*	*25*	*1*
et un ingénieur	*62*	*37*	*1*
et un artiste	*18*	*81*	*1*
et un inventeur	*88*	*12*	*0*

Je vais te lire des phrases à propos de tes parents et de toi. Pour chaque phrase, je voudrais que tu me dises si c'est vrai ou si ce n'est pas vrai ...

	vrai	*pas vrai*	*SR*
Veulent que tu sois surtout bon en maths	*45*	*54*	*1*
Veulent que tu sois bon surtout en français	*57*	*41*	*2*
Veulent que tu sois bon en sciences (physique, chimie, biologie, géologie)	*36*	*62*	*2*
