CHAPITRE 1

Arithmétique Algèbre générale

Sujets d'oraux

A Dénombrement

Ex. 1

Soit $n \in \mathbb{N}^*$, déterminer le nombre de surjections d'un ensemble à $n+1$ éléments sur un ensemble à n éléments.

Soit A de cardinal $n+1$: $A = \{a_1, \dots, a_{n+1}\}$, B de cardinal n : $B = \{b_1, \dots, b_n\}$, et S l'ensemble des surjections de A sur B.

Pour $f \in S$, il existe $i \in [\![1, n]\!]$, $(j, k) \in [\![1, n+1]\!]^2$, $j \neq k$, uniques tels que $f(a_j) = f(a_k) = b_i$ et alors $f_{|A \setminus \{a_j, a_k\}}$ est une bijection de $A \setminus \{a_j, a_k\}$ sur $B \setminus \{b_i\}$.

L'application Φ définie sur S par :

$$\Phi \ : \ f \mapsto b_i, \{a_j, a_k\}, f_{|A \setminus \{a_j, a_k\}}$$

est injective, donc :

$$\mathrm{Card}\, S = \mathrm{Card}\, \Phi(S) = n \times \mathrm{C}_{n+1}^2 \times (n-1)!.$$

En conclusion, $\mathrm{Card}\, S = \dfrac{n(n+1)!}{2}$.

B Nombres complexes – Identités algébriques

Ex. 2

Résoudre l'équation $e^{ix} + e^{iy} + e^{iz} = 0, \quad (x, y, z) \in \mathbb{R}^3$. $\qquad (E)$

Soit $\mathbb{U} = \{Z \in \mathbb{C} \ / \ |Z| = 1\}$, pour $(x, y, z) \in \mathbb{R}^3$, posons $X = e^{ix}$, $Y = e^{iy}$, $Z = e^{iz}$, l'équation proposée se lit :

$$X + Y + Z = 0, \quad (X, Y, Z) \in \mathbb{U}^3 \qquad (E')$$

> Il est bien connu que $1 + j + j^2 = 0$ avec $j = e^{2i\frac{\pi}{3}}$ donc $(1, j, j^2)$ est solution de (E'). Nous allons vérifier, qu'à une rotation près $\left((X, Y, Z) \mapsto (Xe^{i\alpha}, Ye^{i\alpha}, Ze^{i\alpha})\right)$, et une permutation près sur (X, Y, Z), c'est là l'unique solution de (E').

Remarquons d'abord que (E) est équivalente à :

$$1 + e^{i(y-x)} + e^{i(z-x)} = 0, \quad (x, y, z) \in \mathbb{R}^3$$

en posant $u = y - x$, $v = z - x$, on est donc ramené à étudier l'équation :

$$1 + e^{iu} + e^{iv} = 0, \quad (u, v) \in \mathbb{R}^2 \qquad (E_1)$$

qui s'écrit aussi : $1 + \cos u + \cos v = 0$, $\sin u + \sin v = 0$, $\quad (u, v) \in \mathbb{R}^2$.

$\sin v = -\sin u$ donne $v \equiv -u \mod 2\pi$ ou $v \equiv \pi + u \mod 2\pi$.

Pour $v \equiv \pi + u \bmod 2\pi$, on a $\cos v + \cos u = 0$, ce cas est donc à rejeter et (E_1) équivaut ainsi à :

$$v \equiv -u \bmod 2\pi \quad , \quad \cos u = -\frac{1}{2}.$$

Finalement les solutions des (E_1) sont les couples :

$$\left(\frac{2\pi}{3} + 2k\pi, -\frac{2\pi}{3} + 2\ell\pi\right) \quad \text{et} \quad \left(-\frac{2\pi}{3} + 2k\pi, \frac{2\pi}{3} + 2\ell\pi\right), \quad (k,\ell) \in \mathbb{Z}^2$$

et pour (E) on obtient les triplets :

$$\left(\alpha, \alpha + \frac{2\pi}{3} + 2k\pi, \alpha - \frac{2\pi}{3} + 2\ell\pi\right) \text{ et } \left(\alpha, \alpha - \frac{2\pi}{3} + 2k\pi, \alpha + \frac{2\pi}{3} + 2\ell\pi\right), \quad \alpha \in \mathbb{R}, (k,\ell) \in \mathbb{Z}^2$$

Ex. 3

Soit $N = 1\,0\,1\,0\,1\,0 \ldots 1\,0\,1$ écrit en base 10.
L'entier N est-il premier ?

Le nombre N s'écrit avec p fois le chiffre 1 et $p-1$ fois le chiffre 0 et on a :

$$N = 1 + 10^2 + \ldots + 10^{2(p-1)} = \frac{10^{2p} - 1}{10^2 - 1}.$$

> Une exploration numérique avec un logiciel de calcul formel montre que si 101 est premier, il n'en est pas de même pour $10101 = 3 \times 7 \times 13 \times 37$ ou pour $1010101 = 73 \times 101 \times 137$. En fait, nous allons prouver que N est non premier dès que $p \geqslant 3$. Ceci nécessite de faire apparaître une factorisation après la simplification par $10^2 - 1$ et, pour ce faire, nous allons procéder différemment selon que p est pair ou impair.

- Premier cas : p est pair, $p = 2n$ avec $n \geqslant 2$

Alors :

$$N = \frac{10^{4n} - 1}{10^2 - 1} = \frac{10^{2n} - 1}{10^2 - 1} \times \left(10^{2n} + 1\right) = \left(1 + 10^2 + \ldots + 10^{2(n-1)}\right)\left(10^{2n} + 1\right).$$

Puisque $n \geqslant 2$, on a $1 + 10^2 + \ldots + 10^{2(n-1)} > 1$, donc N n'est pas premier.

- Deuxième cas : p est impair, $p = 2n + 1$ avec $n \geqslant 1$

Alors :

$$N = \frac{10^{4n+2} - 1}{10^2 - 1} = \frac{10^{2n+1} - 1}{10 - 1} \times \frac{10^{2n+1} + 1}{10 + 1}$$

donc, en utilisant $a^{2n+1} + b^{2n+1} = (a+b)\sum_{k=0}^{2n} (-1)^k a^{2n-k} b^k$, il vient :

$$\begin{aligned} N &= \left(1 + 10 + \ldots + 10^{2n}\right)\left(1 - 10 + 10^2 + \ldots + (-1)^k 10^k + \ldots + 10^{2n}\right) \\ &= \sum_{k=0}^{2n} 10^k \times \sum_{k=0}^{2n} (-1)^k 10^k \end{aligned}$$

ce qui prouve que N n'est pas premier.

Ex. 4

Quels sont les entiers naturels n tels que $n^4 + 2n^3 + 3n^2 + 1$ soit le carré d'un entier ?

Posons $A(n) = n^4 + 2n^3 + 3n^2 + 1$.

Il est clair que $n = 0$ convient : $A(0) = 1^2$.
On se propose de démontrer que c'est la seule solution.

Supposons maintenant $n \geqslant 1$ donc $A(n) \geqslant 7$. S'il existe $p \in \mathbb{N}$ tel que $A(n) = p^2$, on a $p^2 \geqslant 7$ donc $p \geqslant 3$ et d'autre part :

$$n^4 + 2n^3 + 3n^2 + 1 = n^2(n+1)^2 + 2n^2 + 1 \quad \text{avec} \quad n \geqslant 1$$

donne $\quad p^2 < n^2(n+1)^2 + 2n(n+1) + 1$

c'est-à-dire $\quad p^2 < \big(n(n+1)+1\big)^2$

soit aussi $\quad p < n^2 + n + 1$

ou encore $\quad n^2 + n + 1 - p \geqslant 1.$

Écrivons alors $A(n) = n^2(n+1)^2 + 2n(n+1) + 1 - 2n$

$$= \left(n^2 + n + 1\right)^2 - 2n.$$

L'égalité $A(n) = p^2$ donne :

$$\begin{aligned} 2n &= \left(n^2+n+1\right)^2 - p^2 \\ &= \left(n^2+n+1-p\right)\left(n^2+n+1+p\right) \end{aligned}$$

et, avec $n^2 + n + 1 - p \geqslant 1$, il vient $2n \geqslant n^2 + n + 1 + p$, c'est-à-dire :

$$n^2 - n + 1 + p \leqslant 0$$

ce qui est évidemment absurde.

Ex. 5

Soit $a_n = 2^n + 1$. On suppose que a_n est premier, que peut-on dire de n ?

> Une exploration numérique montre que pour $n \leqslant 20$, a_n est premier lorsque $n = 1, 2, 4, 8, 16$ c'est-à-dire lorsque n est de la forme $2^0, 2^1, 2^2, 2^3, 2^k$. On peut donc supposer qu'une condition nécessaire pour que a_n soit premier est que n soit de la forme 2^p.

Supposons que $n \notin \left\{2^k \mid k \in \mathbb{N}\right\}$. Alors en considérant la décomposition de n en facteurs premiers, il existe j impair, $j \geqslant 3$, et $k \in \mathbb{N}$ tels que $n = 2^k j$ donc aussi $n = 2^k(2i+1)$, $i \geqslant 1$. On en déduit $a_n = b^{2i+1} + 1$ où on a posé $b = 2^{2^k}$. L'identité :

$$x^{2n+1} + y^{2n+1} = (x+y)\sum_{k=0}^{2n}(-1)^k x^{2n-k} y^k$$

donne maintenant :

$$a_n = (b+1)\sum_{k=0}^{2i}(-1)^k b^{2i-k}$$

ce qui prouve que a_n est non premier.
En prenant la contraposée de cette implication, on en déduit que si a_n est premier, alors n est de la forme 2^k, $k \in \mathbb{N}$.

On note que cette condition n'est pas suffisante puisque $2^{2^5} + 1 = 641 \times 6\,700\,417$ (factorisation fournie par Maple).

> *Remarque*. Les nombres de la forme $2^{2^n} + 1$ sont appelés les nombres de Fermat. Les cinq premiers : 3 $(n = 1)$, 5 $(n = 2)$, 17 $\left(n = 2^2\right)$, 257 $\left(n = 2^3\right)$ et 65 537 $\left(n = 2^4\right)$ sont premiers mais au-delà, c'est-à-dire pour $n \geqslant 5$, on n'a, à ce jour, découvert aucun nombre premier.

Ex. 6

Montrer que pour tout $n \in \mathbb{N}$, 2^{2n+1} divise la partie entière de $\left(\sqrt{13}+3\right)^{2n+1}$.

> Il faut penser à introduire $\left(\sqrt{13}-3\right)^{2n+1}$ en remarquant que $0 < \sqrt{13}-3 < 1$.

D'après la formule du binôme, il existe a_n et b_n entiers naturels tels que :

$$\left(\sqrt{13}+3\right)^{2n+1} = a_n\sqrt{13} + b_n$$

$$\left(\sqrt{13}-3\right)^{2n+1} = a_n\sqrt{13} - b_n$$

en effet, on a :

$$\begin{aligned}\left(\sqrt{13}+3\right)^{2n+1} &= \sum_{k=0}^{2n+1} C_{2n+1}^{k}\, 13^{\frac{k}{2}} \cdot 3^{2n+1-k}\\ &= \sqrt{13}\sum_{j=0}^{n} C_{2n+1}^{2j+1}\, 13^{j} \cdot 3^{2(n-j)} + \sum_{j=0}^{n} C_{2n+1}^{2j}\, 13^{j} \cdot 3^{2(n-j)+1}\\ \left(\sqrt{13}-3\right)^{2n+1} &= \sum_{k=0}^{2n+1} C_{2n+1}^{k}\, 13^{\frac{k}{2}} \cdot (-3)^{2n+1-k}\\ &= \sqrt{13}\sum_{j=0}^{n} C_{2n+1}^{2j+1}\, 13^{j} \cdot 3^{2(n-j)} - \sum_{j=0}^{n} C_{2n+1}^{2j}\, 13^{j} \cdot 3^{2(n-j)+1}\end{aligned}$$

d'où :

$$a_n = \sum_{j=0}^{n} C_{2n+1}^{2j+1}\, 13^{j} \cdot 3^{2(n-j)} \quad \text{et} \quad b_n = \sum_{j=0}^{n} C_{2n+1}^{2j}\, 13^{j} \cdot 3^{2(n-j)+1}.$$

On en déduit :

$$\left(\sqrt{13}+3\right)^{2n+1} - \left(\sqrt{13}-3\right)^{2n+1} = 2b_n$$

et, compte tenu de $3 < \sqrt{13} < 4$, donc $0 < \sqrt{13}-3 < 1$, il vient :

$$E\left(\left(\sqrt{13}+3\right)^{2n+1}\right) = 2b_n\,.$$

Nous sommes donc ramenés à prouver que 2^{2n} divise b_n .

> Il suffit maintenant de prouver que les suites $\left(a_n\right)_{\mathbb{N}}$ et $\left(b_n\right)_{\mathbb{N}}$ vérifient une relation de récurrence simple pour mettre en place une démonstration par récurrence.

Avec $\begin{aligned}\left(\sqrt{13}+3\right)^{2n+3} &= a_{n+1}\sqrt{13} + b_{n+1}\\ &= \left(\sqrt{13}+3\right)^{2n+1}\left(\sqrt{13}+3\right)^{2}\\ &= \left(a_n\sqrt{13}+b_n\right)\left(22+6\sqrt{13}\right)\\ &= \left(22a_n+6b_n\right)\sqrt{13} + 78a_n + 22b_n\end{aligned}$

puisque le couple $\left(1, \sqrt{13}\right)$ est libre dans $\mathbb{R}$ considéré comme $\mathbb{Q}$-espace vectoriel, il vient :

$$a_{n+1} = 22a_n + 6b_n \quad , \quad b_{n+1} = 78a_n + 22b_n\,.$$

En écrivant $\left(\sqrt{13}+1\right)^{1} = 1 \cdot \sqrt{13} + 3$, on a $a_0 = 1$ et $b_0 = 3$, donc 2^0 divise a_0 et b_0 et les quotients (encore égaux à a_0 et b_0) sont de même parité.

Soit maintenant la propriété $\mathcal{P}(n)$: 2^{2n} divise a_n et b_n et les quotients a'_n et b'_n $\left(a_n = 2^n a'_n,\ b_n = 2^n b'_n\right)$ sont de même parité.

En supposant $\mathscr{P}(n)$ vraie, on a donc :

$$a_{n+1} = 2^{2n+1}\left(11a'_n + 3b'_n\right) \quad , \quad b_{n+1} = 2^{2n+1}\left(39a'_n + 11b'_n\right).$$

Les entiers a'_n et b'_n étant de même parité, $11a'_n + 3b'_n$ et $39a'_n + 11b'_n$ sont pairs, c'est-à-dire qu'il existe a'_{n+1} et b'_{n+1} entiers tels que $11a'_n + 3b'_n = 2a'_{n+1}$ et $39a'_n + 11b'_n = 2b'_{n+1}$ d'où aussi :

$$a_{n+1} = 2^{2(n+1)}a'_{n+1} \quad \text{et} \quad b_{n+1} = 2^{2(n+1)}b'_{n+1}.$$

Formons enfin $2\left(b'_{n+1} - a'_{n+1}\right) = 28a'_n + 8b'_n = 4\left(7a'_n + 2b'_n\right)$, on en déduit :

$$b'_{n+1} - a'_{n+1} = 2\left(7a'_n + 2b'_n\right),$$

ce qui montre que a'_{n+1} et b'_{n+1} sont de même parité.

On a ainsi prouvé que la propriété $\mathscr{P}(n)$ est héréditaire et, puisque $\mathscr{P}(0)$ est vraie, le principe de récurrence montre que $\mathscr{P}(n)$ est vraie quel que soit $n \in \mathbb{N}$, ce qui achève la démonstration.