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 :

$$\text{Card } S = \text{Card } \Phi(S) = n \times \binom{2}{n+1} \times (n-1)!.$$

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

B Numération

Ex. 2

Montrer qu'il existe un entier N multiple de 1996 dont l'écriture en base 10 ne contient que le chiffre 4.

> Il faut commencer par analyser le problème en introduisant le nombre de chiffres de l'écriture de N.

Remarquons d'abord que $1996 = 4 \times 499$ avec 499 premier, et si l'écriture de N comporte n chiffres, $N = 4\left(1 + 10 + \dots + 10^{n-1}\right)$ c'est-à-dire :

$$N = 4\frac{10^n - 1}{9}.$$

Le problème se lit donc : il existe $n \in \mathbb{N}^*$ et $q \in \mathbb{N}^*$ tels que :

$$4 \cdot \frac{10^n - 1}{9} = 4 \times 499 \times q$$

soit aussi :

$$10^n - 1 = 9 \times 499 \times q.$$

> C'est le moment de penser au petit théorème de Fermat : si p est un entier premier, pour tout entier $x \not\equiv 0 \bmod p$, on a $x^{p-1} \equiv 1 \bmod p$.

499 est premier et $10 \not\equiv 0 \bmod 499$, donc $10^{498} \equiv 1 \bmod 499$.

D'autre part, $10 \equiv 1 \bmod 9$ donne, quel que soit $n \in \mathbb{N}$, $10^n \equiv 1 \bmod 9$.

Ainsi 9 et 499 divisent $10^{498} - 1$ et, puisqu'ils sont premiers entre eux, leur produit 9×499 divise $10^{498} - 1$. En conclusion, il existe $q \in \mathbb{N}^*$ tel que $10^{498} - 1 = 9 \times 499 \times q$ et le nombre :

$$N = 4\frac{10^{498} - 1}{9}$$

est solution du problème avec 498 chiffres 4.

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 :

$$N = \left(1 + 10 + \ldots + 10^{2n}\right)\left(1 - 10 + 10^2 + \ldots + (-1)^k 10^k + \ldots + 10^{2n}\right)$$

$$= \sum_{k=0}^{2n} 10^k \times \sum_{k=0}^{2n} (-1)^k 10^k$$

ce qui prouve que N n'est pas premier.

Ex. 4

Soit $abcdef$ l'écriture en base 10 d'un entier naturel divisible par 13. Montrer que l'entier naturel dont l'écriture en base 10 est $bcdefa$ est encore divisible par 13.

Dans le corps $\mathbb{Z}/13\mathbb{Z}$ les éléments étant notés $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{10}, \overline{11}, \overline{12}$, l'hypothèse se lit :

$$\overline{10}^5 a + \overline{10}^4 b + \overline{10}^3 c + \overline{10}^2 d + \overline{10} e + \overline{1} f = \overline{0} \qquad (1)$$

et il nous faut vérifier que :

$$\overline{10}^5 b + \overline{10}^4 c + \overline{10}^3 d + \overline{10}^2 e + \overline{10} f + \overline{1} a = \overline{0}. \qquad (2)$$

En multipliant les deux membres de (1) par $\overline{10}$, on obtient :

$$\overline{10}^5 b + \overline{10}^4 c + \overline{10}^3 d + \overline{10}^2 e + \overline{10} f + \overline{10}^6 a = \overline{0}. \qquad (3)$$

Or, avec $\overline{10} = -\overline{3}$, il vient successivement :

$$\overline{10}^2 = -\overline{30} = -\overline{4}, \quad \overline{10}^3 = -\overline{40} = -\overline{1} \quad \text{et} \quad \overline{10}^6 = (-\overline{1})^2 = \overline{1}.$$

En conséquence, (3) est identique à (2), ce qui montre que $bcdefa$ est divisible par 13.

C Identités algébriques Applications à l'arithmétique

Ex. 5

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 $\quad A(n) = n^2(n+1)^2 + 2n(n+1) + 1 - 2n$

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

L'égalité $A(n) = p^2$ donne :

$$2n = \big(n^2 + n + 1\big)^2 - p^2$$
$$= \big(n^2 + n + 1 - p\big)\big(n^2 + n + 1 + p\big)$$

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. 6

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 $n \notin \{2^k / k \in \mathbb{N}\}$. 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. 7

Trouver tous les couples (m, n) d'entiers naturels tels que :

$$3^m - 2^n = 1 \qquad (E)$$

> Après avoir écarté les cas particuliers liés aux solutions apparentes de cette équation, une démarche usuelle consiste en la recherche de conditions nécessaires. Pour ce faire, on pourra observer que, lorsque m et n sont pairs, $3^m - 2^n$ est factorisable au moyen de l'identité :
>
> $$a^2 - b^2 = (a-b)(a+b).$$

Notons d'abord que, la suite $\left(3^m\right)_{m\in\mathbb{N}}$ étant strictement croissante, pour $n \in \mathbb{N}$ donné il existe au plus une valeur de m telle que (m, n) soit solution de (E).

Il est apparent que l'unique solution correspondant à $n = 1$ est le couple $(1, 1)$ $\left(3^1 - 2^1 = 1\right)$ et que celle correspondant à $n = 3$ est le couple $(2, 3)$ $\left(3^2 - 2^3 = 1\right)$. De même, il est facile de vérifier qu'il n'y a pas de solution correspondant à $n = 0$ ou $n = 2$. En conséquence, nous pouvons, dans la suite, nous limiter à $n \geqslant 4$.

- Recherche de conditions nécessaires

On suppose que (m, n) est solution de (E) avec $n \geqslant 4$.

En remarquant que $m \geqslant n$ donne :

$$3^m - 2^n \geqslant 3^n - 2^n = (3-2)\sum_{k=0}^{n-1} 3^{n-1-k}2^k$$

et donc $3^m - 2^n \geqslant n \geqslant 4$, on voit qu'une première condition nécessaire est $m < n$. (1)

L'égalité $3^m - 2^n = 1$ nous donne $3^m \equiv 1 \bmod 2^n$ soit aussi $\overline{3}^m = \overline{1}$ dans $\mathbb{Z}/2^n\mathbb{Z}$ et on en déduit que m est un mutiple de p, ordre de $\overline{3}$ dans le groupe des inversibles de $\mathbb{Z}/2^n\mathbb{Z}$.

Or on a $3 \equiv 1 \bmod 2$, $3^2 \equiv 1 \bmod 2^3$ et, en supposant $3^{2k} \equiv 1 \bmod 2^{k+2}$ c'est-à-dire $3^{2^k} = 2^{k+2}\,\ell + 1$ avec $\ell \in \mathbb{Z}$, on obtient :

$$3^{2^{k+1}} = \left(2^{k+2}\,\ell + 1\right)^2 = 2^{k+3}\left(2^{k+1}\,\ell^2 + \ell\right) + 1$$

donc $3^{2^{k+1}} \equiv 1 \bmod 2^{k+3}$, ce qui montre par récurrence que :

$$\forall k \in \mathbb{N}^*,\ 3^{2^k} \equiv 1 \bmod 2^{k+2}.$$

On en déduit $\overline{3}^{2^{n-2}} = \overline{1}$ dans $\mathbb{Z}/2^n\mathbb{Z}$ et l'ordre p de $\overline{3}$ est un diviseur de 2^{n-2} donc de la forme 2^α avec $0 \leqslant \alpha \leqslant n-2$. Sachant de plus que $\overline{3} \neq \overline{1}$ dès que $n \geqslant 2$, on a $p > 1$ c'est-à-dire $p = 2^\alpha$ avec $1 \leqslant \alpha \leqslant n-2$. Ainsi p est pair et m multiple de p est également pair :

$$m = 2a, \quad a \in \mathbb{N} \tag{2}$$

Remarquons maintenant que si n était pair : $n = 2b$, $b \geqslant 2$, on aurait :

$$3^m - 2^n = 3^{2a} - 2^{2b} = \left(3^a - 2^b\right)\left(3^a + 2^b\right)$$

donc $3^a + 2^b$ serait diviseur de 1, ce qui est impossible avec $3^a + 2^b \geqslant 5$. En conséquence, n est impair :

$$n = 2b + 1, \quad b \geqslant 2 \tag{3}$$

- Conditions suffisantes

> On recherche maintenant quels sont, parmi les couples (m, n) vérifiant les conditions (1), (2) et (3), ceux qui satisfont à $3^m - 2^n = 1$.

Les couples vérifiant (1), (2) et (3) sont de la forme $\left(2a, 2b+1\right)$ avec $(a, b) \in \mathbb{N}^2$, $b \geqslant 2$, $a \leqslant b$ et un tel couple est solution de (E) si et seulement si $3^{2a} - 1 = 2^{2b+1}$, c'est-à-dire :

$$\left(3^a - 1\right)\left(3^a + 1\right) = 2^{2b+1}.$$

Cette condition impose $a \neq 0$, donc $1 \leqslant a \leqslant b$, et elle donne l'existence de $c \in [\![1, 2b]\!]$ tel que :

$$3^a - 1 = 2^c \text{ et } 3^a + 1 = 2^{2b+1-c} \text{ soit aussi } 3^a = 2^{c-1} + 2^{2b-c} \text{ et } 1 = 2^{2b-c} - 2^{c-1}.$$

Il est facile de voir que l'équation $1 = 2^{2b-c} - 2^{c-1}$, $1 \leqslant c \leqslant 2b$, $b \geqslant 2$, n'a pas de solution. En effet, $c = 2b$ est à rejeter puisque l'on obtiendrait alors $0 = 2^{c-1}$ ce qui est irréalisable et, pour $c < 2b$, $1 + 2^{c-1} = 2^{2b-c}$ est un entier pair donc 2^{c-1} est impair ce qui exige $c = 1$, $1 + 2^{c-1} = 2$, $2b - 1 = 1$ donc $b = 1$, ce qui est exclu.

En conclusion, il n'existe aucun couple (m, n) solution de (E) avec $n \geqslant 4$ et, compte tenu de l'étude préliminaire, les seules solutions de (E) sont les deux couples $(1, 1)$ et $(2, 3)$.