

Stage de Vendôme

Corrigé du test du 5 juillet 2002

Exercice 1

Existe-t-il deux puissances de 2 distinctes mais dont l'écriture décimale comporte exactement les mêmes chiffres (avec multiplicité) ?

Solution:

Nous allons prouver que deux telles puissances n'existent pas. Supposons que ce soit le cas et disons qu'un exemple soit 2^n et 2^m avec $m > n$. Alors 2^n et 2^m ont le même nombre de chiffres, ce qui implique que le quotient $2^{m-n} < 10$. Ainsi soit $m = n + 1$, soit $m = n + 2$, soit $m = n + 3$.

On remarque à présent que si l'on note pour un entier k , $S(k)$ la somme des chiffres de k , on a toujours la congruence :

$$S(k) \equiv k \pmod{9}$$

Comme les chiffres de 2^n et de 2^m sont les mêmes, on va avoir $S(2^n) = S(2^m)$ et donc $2^n \equiv 2^m \pmod{9}$. Mais, en étudiant les puissances successives de 2 modulo 9, on voit directement que cela implique que n soit congru à m modulo 6.

Des deux remarques précédentes, on déduit directement une contradiction.

Exercice 2

Soit n un entier naturel. Montrer qu'il existe une *unique* suite $(a_i)_{i \geq 1}$ d'entiers telle que :

i) la suite (a_i) soit nulle à partir d'un certain rang

ii) $0 \leq a_i \leq i$

iii) $n = \sum_{i=1}^{\infty} a_i \cdot i!$

On rappelle que par définition $i! = 1 \times 2 \times \dots \times i$.

Solution:

On copie plus ou moins la démonstration du cours pour la décomposition en base n .

Si une telle décomposition existe, on remarque que a_1 est forcément le reste de la division euclidienne de n par 2, le quotient de cette division euclidienne est quant à lui égal à :

$$a_2 \cdot \frac{2!}{2!} + \dots + a_n \cdot \frac{n!}{2!} + \dots$$

Ainsi on voit que a_2 est forcément égal au reste de la division euclidienne de ce quotient par 3, le nouveau quotient étant ce coup-ci égal à :

$$a_3 \cdot \frac{3!}{3!} + \dots + a_n \cdot \frac{n!}{3!} + \dots$$

Ainsi de suite, on détermine a_3, a_4, \dots . Il ne reste plus qu'à voir que cette construction s'arrête au bout d'un nombre fini d'étapes, mais cela est clair car les quotients successifs diminuent strictement à chaque étape.

Note : Une telle décomposition s'appelle la décomposition d'un entier en *base factorielle*.

Exercice 3

- a) Montrer que si $p^2 + q^2$ est un multiple de 7, alors il en est de même de p et q .
- b) Montrer que cela reste vrai si l'on remplace 7 par un nombre premier quelconque congru à 3 modulo 4.

Solution:

Nous allons traiter directement la deuxième question. Appelons par exemple n ce nombre premier congru à 3 modulo 4. Le fait que $p^2 + q^2$ soit un multiple de n s'écrit :

$$p^2 + q^2 = 0$$

dans $\mathbb{Z}/n\mathbb{Z}$.

Supposons un instant que q ne soit pas un multiple de n , c'est-à-dire que \dot{q} soit non nul dans $\mathbb{Z}/n\mathbb{Z}$. Comme n est premier, il est inversible, appelons \dot{q}' un inverse et multiplions la relation précédente par \dot{q}'^2 . On obtient :

$$\dot{q}'^2 p^2 + \dot{1} = \dot{0}$$

puis

$$(\dot{q}'p)^2 = -\dot{1}$$

Il s'agit donc de voir si $-\dot{1}$ est un carré dans $\mathbb{Z}/n\mathbb{Z}$ mais on a un critère pour cela, c'est le critère d'Euler. Il s'agit de calculer $(-\dot{1})^{\frac{n-1}{2}}$. Mais n est congru à 3 modulo 4 et donc cette quantité vaut $-\dot{1}$, et donc $-\dot{1}$ n'est pas un carré dans $\mathbb{Z}/n\mathbb{Z}$.

Cela prouve que l'équation n'a pas de solution si \dot{q} est non nul. Maintenant si $\dot{q} = \dot{0}$, on obtient $\dot{p}^2 = \dot{0}$ et encore parce que n est premier, cela implique $\dot{p} = \dot{0}$.

On vient donc de prouver que la seule solution de l'équation est $\dot{p} = \dot{q} = \dot{0}$ et donc de résoudre le problème.