

Un petit exercice

Xavier Caruso

6 avril 2002

Énoncé :

Soit n un entier supérieur ou égal à 1. On considère X_1, \dots, X_{2^n-1} , $2^n - 1$ n -uplets d'entiers relatifs. Montrer qu'il existe un n -uplet d'entiers relatifs X tel que pour tout i , le segment ouvert qui relie X à X_i ne passe par aucun point à coordonnées entières.

Démonstration :

Remarquons en premier lieu que le cas $n = 1$ est trivial. On supposera donc $n \geq 2$.

Fixons tout d'abord quelques notations. On va noter $X = (x_1, \dots, x_n)$ et $X_i = (x_{i,1}, \dots, x_{i,n})$. La condition énoncée peut se redire de la façon suivante :

$$\forall i \in \{1, \dots, 2^n - 1\}, \quad \text{Pgcd}(x_1 - x_{i,1}, \dots, x_n - x_{i,n}) = 1$$

ce qui est encore équivalent à :

$$\forall i \in \{1, \dots, 2^n - 1\}, \forall p \text{ premier}, \quad (x_1, \dots, x_n) \not\equiv (x_{i,1}, \dots, x_{i,n}) \pmod{p}$$

Notons maintenant p_k le k -ième nombre premier et essayons de résoudre ce système de congruences en se limitant aux s premiers nombres premiers, avec $p_1 \dots p_s > \max |x_{i,j}|$. On obtient :

$$(S) : \begin{cases} (x_1, \dots, x_n) \equiv (y_{1,1}, \dots, y_{1,n}) \pmod{p_1} \\ (x_1, \dots, x_n) \equiv (y_{2,1}, \dots, y_{2,n}) \pmod{p_2} \\ \vdots \\ (x_1, \dots, x_n) \equiv (y_{s,1}, \dots, y_{s,n}) \pmod{p_s} \end{cases}$$

où $(y_{k,1}, \dots, y_{k,n}) \not\equiv (x_{i,1}, \dots, x_{i,n}) \pmod{p_k}$ pour tout k et pour tout i . À k fixé, il existe donc au moins $p_k^n - 2^n + 1$ possibilités différentes modulo p_k pour le choix de $(y_{k,1}, \dots, y_{k,n})$. Ainsi il existe au moins :

$$A_s = \prod_{k=1}^s (p_k^n - 2^n + 1)$$

systèmes de congruences classiques qui fournissent une solution de (S) . D'après le lemme chinois, à chacun d'entre eux correspond une solution telle que pour tout i , $1 \leq x_i \leq p_1 \dots p_s$.

La dernière inégalité prouve que si p est un nombre premier plus grand que $p_1 \dots p_s$, alors $(x_1, \dots, x_n) \not\equiv (x_{i,1}, \dots, x_{i,n}) \pmod{p}$ (car sinon il y aurait réellement égalité et il y aurait déjà égalité modulo 2 par exemple, ce qui est supposé faux).

Reste donc à étudier les nombres premiers compris entre p_s et $p_1 \dots p_s$. Soit donc p un nombre premier compris entre p_s et $p_1 \dots p_s$. Le nombre de n -uplets pour lesquels la condition de congruence modulo p n'est pas satisfaite est majoré par $(2^n - 1) \left(\frac{p_1 \dots p_s}{p} + 1 \right)$. Ainsi le nombre de n -uplets qui

vont être rejetés par les conditions de congruence modulo p , pour $p_s < p < p_1 \dots p_s$, sera majoré par :

$$B_s = (2^n - 1) \sum_{\substack{p \text{ premier} \\ p_s < p < p_1 \dots p_s}} \left(\frac{p_1 \dots p_s}{p} + 1 \right)$$

Il suffit pour conclure de prouver que $B_s < A_s$ pour s suffisamment grand. C'est ce que nous allons faire.

On a d'une part :

$$A_s = \prod_{k=2}^s (p_k^n - 2^n + 1) \geq \prod_{k=2}^s \left(\frac{p_k}{3} \right)^n = \frac{3}{2} \left(\frac{p_1}{3} \dots \frac{p_s}{3} \right)^n$$

et

$$B_s \leq 2(2^n - 1)(p_1 \dots p_s) \sum_{p=1}^{p_1 \dots p_s} \frac{1}{p} \leq 4(2^n - 1)(p_1 \dots p_s)^{3/2}$$

Ainsi :

$$\frac{A_s}{B_s} \geq C \frac{p_1^{n-3/2}}{3^n} \dots \frac{p_s^{n-3/2}}{3^n} \quad \text{où } C \text{ est une constante ne dépendant que de } n$$

et cette quantité peut être rendue arbitrairement grande dès que $n \geq 2$.