Le théorème d'Erdös sur les fonctions multiplicatives monotones

G.Huvent

17 mai 2007

1 Avant propos

L'objet de ce document est de donner une preuve du théorème d'Erdös sur les fonctions multiplicatives monotones. Avant d'énoncer ce théorème il convient de donner la définition d'une fonction arithmétique multiplicative.

Définition 1 *Une fonction $f : \mathbb{N} \to \mathbb{N}$ est dite multiplicative si $f(1) = 1$ et si $(m, n) = 1 \Longrightarrow f(mn) = f(m) f(n)$, où $(m, n) = 1$ signifie que m et n sont premiers entre eux.*

On définit également les fonctions totalement multiplicative lorsque $f(mn) = f(m) f(n)$ ceci pour tous entiers m et n. Pour une fonction totalement multiplicative, la valeur en les nombres premiers de f définit complètement f. En effet si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ où les p_i sont des nombres premiers et si f est totalement multiplicative alors $f(n) = f(p_1)^{\alpha_1} \cdots f(p_n)^{a_n}$.
On peut maintenant énoncer le théorème d'Erdös :

Théorème 2 *Soit f multiplicative de $\mathbb{N}$ dans $\mathbb{N}$ et strictement croissante alors il existe $\alpha \in \mathbb{N}$ tel que $f(n) = n^{\alpha}$.*

Remarque 3 *Si on suppose simplement f à valeurs dans $\mathbb{R}$ au lieu de $\mathbb{N}$, la conclusion est remplacée par : il existe $\alpha \in \mathbb{R}$ tel que $f(n) = n^{\alpha}$.*

2 Preuve du théorème d'Erdös

La preuve se fait en deux temps et utilise deux résultats intermédiaires qui seront démontrés en annexes.
Premier acte : Si p est premier $f(p^n) = f(p)^n$.
Soit p un nombre premier et x tel que $(x, p) = 1$ alors pour $n \in \mathbb{N}$, on a $\left(x, p^{n+1}\right) = 1$ donc $f\left(xp^{n+1}\right) = f(x) f\left(p^{n+1}\right)$.
Puis $(p^n, (xp+1)) = 1$ (en effet un diviseur de p^n est de la forme p^a donc est divisible par p, il ne peut donc pas diviser $xp+1$). On en déduit que

$$f(p^n(xp+1)) = f(p^n) f(xp+1)$$

mais

$$f(p^n(xp+1)) = f\left(xp^{n+1} + p^n\right) > f\left(xp^{n+1}\right) = f(x) f\left(p^{n+1}\right)$$

d'où

$$f(p^n) f(xp+1) > f(x) f\left(p^{n+1}\right) \Longrightarrow \frac{f\left(p^{n+1}\right)}{f(p^n)} < \frac{f(xp+1)}{f(x)}$$

Mais puisque $(p, x+p) = 1$ on a $f\left(xp+p^2\right) = f(p) f(x+p) > f(xp+1)$ d'où

$$\frac{f\left(p^{n+1}\right)}{f(p) f(p^n)} < \frac{f(x+p)}{f(x)} \tag{E}$$

On pose alors $r = \dfrac{f\left(p^{n+1}\right)}{f(p) f(p^n)}$, si $(x, p) = 1$ alors $(x + jp, p) = 1$ pour $j \in \mathbb{N}$, ainsi avec $x = x$, puis $x+p, x+2p \cdots$ dans (E), on a en multipliant les inégalités, pour $k \in \mathbb{N}$

$$r^k < \frac{f(x+kp)}{f(x)}$$

Fixons k, on choisit x assez grand, premier avec p tel que $x+kp<2x$ (toujours possible, prendre x premier et supérieur à kp). alors

$$r^k < \frac{f(x+kp)}{f(x)} < \frac{f(2x)}{f(x)} = f(2)$$

donc $r^k < f(2)$ ceci quelque soit k ! Impossible si $r>1$, ainsi $r \leq 1$.
De la même manière,

$$f(p^n) f(px-1) = f(p^n(px-1)) = f\left(p^{n+1}x - p^n\right) < f\left(p^{n+1}x\right) = f\left(p^{n+1}\right) f(x)$$

On en déduit que $\dfrac{f\left(p^{n+1}\right)}{f(p^n)} > \dfrac{f(px-1)}{f(x)} > \dfrac{f\left(px-p^2\right)}{f(x)} = \dfrac{f(p)\, f(x-p)}{f(x)}$ en choisissant x assez grand, premier avec p et tel que $px-p^2 \geq 0$. On a donc

$$r > \frac{f(x-p)}{f(x)} \Longrightarrow \frac{1}{r} < \frac{f(x)}{f(x-p)} = \frac{f(x'+p)}{f(x')} \text{ où } x' = x-p$$

Il s'agit du même type d'inégalité que (E). Le même raisonnement conduit alors à $\dfrac{1}{r} \leq 1$. Conclusion $r=1$, fin de l'acte 1. On en déduit que f est totalement multiplicative. Si $m = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n}$, $n = p_1^{\beta_1} \times \cdots \times p_n^{\beta_n}$ alors

$$\begin{aligned} f(m) f(n) &= f(p_1)^{\alpha_1} \times \cdots \times f(p_n)^{\alpha_n} \times f(p_1)^{\beta_1} \times \cdots \times f(p_n)^{\beta_n} \\ &= f(mn) \end{aligned}$$

Second acte : $f(n) = n^\alpha$ pour un α réel a priori.
On veut prouver que $\dfrac{\ln f(n)}{\ln n}$ est constant. Si ce n'est pas le cas, il existe a et b tels que

$$\frac{\ln f(a)}{\ln a} \neq \frac{\ln f(b)}{\ln b}$$

par exemple

$$\frac{\ln a}{\ln b} < \frac{\ln f(a)}{\ln f(b)}$$

Par densité, il existe $\dfrac{p}{q}$ entre les deux, mais alors

$$\begin{aligned} \frac{\ln a}{\ln b} < \frac{p}{q} &\Longrightarrow a^q < b^p \\ \frac{p}{q} < \frac{\ln f(a)}{\ln f(b)} &\Longrightarrow f(b)^p < f(a)^q \end{aligned}$$

Or f est complètement multiplicative et croissante donc

$$f(a^q) = f(a)^q < f(b^p) = f(b)^p$$

absurde. On fait de même si c'est $\dfrac{\ln a}{\ln b} > \dfrac{\ln f(a)}{\ln f(b)}$.
On a donc prouvé que f est de la forme $f(n) = n^\alpha$ où $\alpha \in \mathbb{R}$. Pour montrer que $\alpha \in \mathbb{N}$, on va prouver le résultat général suivant.

Proposition 4 *Soit $\alpha \in \mathbb{R}$ tel que pour tout entier $n \in \mathbb{N}$ on a $n^\alpha \in \mathbb{N}$, alors α est entier.*

Preuve. *La suite $(n^\alpha)_n$ est à valeurs dans $\mathbb{N}$. On lui applique l'opérateur Δ d'Euler défini ainsi : si $u = (u_n)_{n\in\mathbb{N}}$ est une suite de réels, la suite $\Delta(u_n)$ a pour terme général $u_{n+1} - u_n$.*
Pour $p \in \mathbb{N}$ on a (voir preuve en annexe 1)

$$\Delta^p(u_n) = \sum_{i=0}^{p} (-1)^{p-i} \binom{p}{i} u_{n+i}$$

Supposons que $\alpha \in [0,p[$ *(par exemple* p *est égal à la partie entière de* $\alpha+1$*), on applique* $\Delta^p = \Delta \circ \cdots \circ \Delta$ *à la suite* $(n^\alpha)_n$*, alors*

$$\begin{aligned}
\Delta^p(n^\alpha) &= \sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}(n+i)^\alpha \\
&= n^\alpha \sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}\left(1+\frac{i}{n}\right)^\alpha \\
&= n^\alpha \sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}\sum_{k=0}^{+\infty}\binom{\alpha}{k}\left(\frac{i}{n}\right)^k \\
&= \sum_{k=0}^{+\infty}\left[\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^k\right]\binom{\alpha}{k}n^{\alpha-k}
\end{aligned}$$

Le développement en série entière n'étant valable que pour $n>p$*. Or (voir preuve en annexe 2)*

$$\begin{aligned}
&\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^k = 0 \text{ si } k<p \\
&\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^p = p!
\end{aligned}$$

ainsi

$$\Delta^p(n^\alpha) = p!\binom{\alpha}{p}n^{\alpha-p} + \sum_{k=p+1}^{+\infty}\left[\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^k\right]\binom{\alpha}{k}n^{\alpha-k}$$

d'où

$$\Delta^p(n^\alpha) \underset{n\to+\infty}{\sim} \frac{p!\binom{\alpha}{p}}{n^{p-\alpha}} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-p)}{n^{p-\alpha}} \xrightarrow[n\to+\infty]{} 0$$

car on a supposé $\alpha\in[0,p[$*. Mais puisque la suite* $(n^\alpha)_n$ *est à valeurs entières, elle est nulle pour* n *assez grand. On a donc*

$$\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-p)=0$$

et ainsi $\alpha\in\mathbb{N}$*.* ■

3 Annexe 1

Peuve de

$$\Delta^p(u_n) = \sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}u_{n+i}$$

3.1 Première preuve (Par le binôme de Newton)

Soit T l'endomorphisme de E, espace vectoriel des suites réelles, défini par, si $u=(u_n)_n$ alors $T(u)=(u_{n+1})_n$. On a $\Delta = T - I_d$, puisque T et Id commutent, on peut appliquer le binôme de Newton. Donc

$$\Delta^p = (T-I_d)^p = \sum_{k=0}^{p}(-1)^{p-i}\binom{p}{i}T^i$$

Mais il est clair que $T^i(u) = (u_{n+i})_n$ d'où le résultat.

3.2 Seconde preuve (Par récurrence)

L'initialisation est immédiate, pour l'hérédité, on a

$$\begin{aligned}
\Delta^{p+1}(u_n) &= \Delta(\Delta^p(u_n)) = \sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}u_{n+i+1} - \sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}u_{n+i} \\
&= \sum_{i=1}^{p+1}(-1)^{p+1-i}\binom{p}{i-1}u_{n+i} + \sum_{i=0}^{p}(-1)^{p+1-i}\binom{p}{i}u_{n+i} \\
&= \binom{p}{p}u_{n+p+1} + \sum_{i=1}^{p}(-1)^{p+1-i}\left[\binom{p}{i-1}+\binom{p}{i}\right]u_{n+i} + (-1)^{p+1}\binom{p}{0}u_n
\end{aligned}$$

Avec la relation du triangle de Pascal, il vient

$$\begin{aligned}
\Delta^{p+1}(u_n) &= \binom{p+1}{p+1}u_{n+p+1} + \sum_{i=1}^{p}(-1)^{p+1-i}\binom{p+1}{i}u_{n+i} + (-1)^{p+1}\binom{p+1}{0}u_n \\
&= \sum_{i=0}^{p+1}(-1)^{p+1-i}\binom{p+1}{i}u_{n+i}
\end{aligned}$$

d'où l'hérédité et par récurrence la formule annoncée.

4 Annexe 2

Preuve de

$$\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^k = 0 \text{ si } k < p$$

$$\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^p = p!$$

4.1 Première preuve (par un développement limité)

On constate facilement que

$$\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^k = \left.\frac{d^k}{dx^k}\left[(e^x-1)^p\right]\right|_{x=0}$$

on peut donc obtenir sa valeur par le développement limité de $(e^x-1)^p$ en 0. Mais $(e^x-1)^p = x^p + \underset{x\to 0}{o}(x^p)$ d'où le résultat.

4.2 Seconde preuve (par une décomposition en éléments simples)

On considère la fraction rationnelle

$$F(x) = \frac{p!X^{k-1}}{\prod_{i=1}^{p}(X+i)}$$

que l'on décompose en éléments simples

$$F(X) = \sum_{i=1}^{p}\frac{\alpha_i}{(X+i)}$$

On a $\alpha_i = \dfrac{p!\,(-i)^{k-1}}{\prod\limits_{\substack{j=1\\ j\neq i}}^{p}(j-i)} = \dfrac{p!\,(-i)^{k}}{\prod\limits_{\substack{j=0\\ j\neq i}}^{p}(j-i)} = \dfrac{p!\,(-i)^{k}}{(-1)^{i}\,i!\,(p-i)!} = (-1)^{k-i}\dbinom{p}{i}i^{k}$. Puisque $\deg F = k-1-p$, on a

$$xF(x) \underset{x\to+\infty}{\longrightarrow} \begin{cases} 0 \text{ si } k<p \\ p! \text{ si } k=p \end{cases}$$

Or

$$xF(x) \underset{x\to+\infty}{\longrightarrow} \sum_{i=1}^{p}\alpha_i = (-1)^{k-p}\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^{k}$$

d'où le résultat.

5 Annexe 3

L'équivalent de $\Delta^{p}(n^{\alpha})$ obtenu à la proposition 4 mérite d'être complétement justifié. On a montré que

$$\begin{aligned}\Delta^{p}(n^{\alpha}) &= \sum_{k=0}^{+\infty}\left[\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^{k}\right]\binom{\alpha}{k}n^{\alpha-k} \\ &= n^{\alpha}\sum_{k=0}^{+\infty}\left[\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^{k}\right]\binom{\alpha}{k}\left(\frac{1}{n}\right)^{k}\end{aligned}$$

pour $n>p$ par des développements en séries entières de rayon de convergence non nul. Si on introduit la série entière

$$S(x) = \sum_{k=0}^{+\infty}\left[\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^{k}\right]\binom{\alpha}{k}x^{k} = \sum_{k=0}^{+\infty}a_k x^{k}$$

cette série entière a un rayon de convergence non nul. On a également prouvé qu'elle s'exprime sous la forme

$$S(x) = p!\binom{\alpha}{p}x^{p} + \sum_{k=p+1}^{+\infty}a_k x^{k}$$

i.e. que sa valuation vaut p ($a_0 = \cdots = a_{p-1} = 0$ et $a_p \neq 0$). L'équivalent vient alors du fait que

$$\frac{S(x)}{x^{p}} = p!\binom{\alpha}{p} + \sum_{k=1}^{+\infty}a_{k+p}x^{k}$$

est une série entière qui tend vers $p!\dbinom{\alpha}{p}$ quand x tend vers 0. Ainsi

$$S(x) \underset{x\to0}{\sim} p!\binom{\alpha}{p}x^{p}$$

et

$$\Delta^{p}(n^{\alpha}) = n^{\alpha}S\left(\frac{1}{n}\right) \underset{n\to+\infty}{\sim} \frac{p!\binom{\alpha}{p}}{n^{p-\alpha}}$$

6 Deux exercices simples liés

6.1 Une olympiade de St Petersbourg

Exercice 5 *Soit* $f : \mathbb{N} \to \mathbb{N}$ *telle que* $f(2) = 2$, *pour tout* $(m, n) \in \mathbb{N}^2$, $m > n \Longrightarrow f(m) > f(n)$ *et si* m *et* n *n'ont pas de facteurs communs alors* $f(mn) = f(m) f(n)$. *Que vaut* $f(3)$ *?*

Solution 6 *Pour résoudre cette exercice, nul besoin d'invoquer le théorème d'Erdos. On peut raisonner autrement. On a alors*

$$f(15) = f(3 \times 5) = f(3) f(5) \leq f(18) = 2f(9) < 2f(10) = 2f(2 \times 5) = 4f(5)$$

donc

$$2 = f(2) < f(3) < 4$$

Ainsi

$$f(3) = 3$$

6.2 Une version faible du théorème d'Erdös

Le résultat suivant est une illustration intéressante de la récurrence forte et constitue une version faible du théorème d'Erdös.

Exercice 7 *Soit* $f : \mathbb{N} \to \mathbb{N}$ *strictement croissante telle que* $f(2) = 2$ *et* $\forall (p, q) \in \mathbb{N}^2$, $f(pq) = f(p) f(q)$. *Montrer que* $\forall n \in \mathbb{N}$, $f(n) = n$.

Solution 8 *Par récurrence forte sur* n. *On définit* $P(n) =$ " $f(n) = n$".
On sait que $f(2 \times 0) = f(2) \times f(0) = 2 \times f(0) = f(0)$ *donc* $f(0) = 0$ *ce qui prouve* $P(0)$. *Puis* $0 < 1 < 2$ *donc par stricte croissance* $0 = f(0) < f(1) < f(2) = 2$. *Mais* f *est à valeurs entières donc* $f(1) = 1$. *Ceci prouve* $P(1)$.
On vient d'exposer les deux grandes idèes de la démonstration.
Supposons $P(0), P(1), ..., P(n)$ *vraies à* $n \geq 0$ *fixé. Montrons* $P(n+1)$. *Si* $n + 1 = 2p$ *est pair alors* $f(n+1) = f(2) \times f(p) = 2p$ *car* $P(p)$ *vraie.*
Si $n + 1 = 2p + 1$ *est impair alors* $2p \leq 2p + 1 < 2(p+1) \Longrightarrow f(2p) < f(n+1) < f(2p+2)$. *Mais* $f(2p) = 2p$ *(car* $P(n)$ *vraie),* $f(2p+2) = f(2) f(p+1) = 2(p+1)$ *car* $p + 1 \leq 2p + 1$ *(dès que* $p \geq 0 \Longleftrightarrow n \geq 1$ *).et donc* $P(p+1)$ *vraie.*