Préliminaire : réarrangement d'Abel

1. Soient $\sum_{n\geq 1} u_n$ et $\sum_{n\geq 1} v_n$ deux séries de nombres complexes, et $U_n = \sum_{k=1}^{n} u_k$. On a :

$$\begin{aligned}\sum_{k=1}^{n} u_k v_k &= U_1 v_1 + (U_2 - U_1)v_2 + \cdots + (U_n - U_{n-1})v_n \\ \sum_{k=1}^{n} u_k v_k &= U_1(v_1 - v_2) + \cdots + U_{n-1}(v_{n-1} - v_n) + U_n v_n \\ \sum_{k=1}^{n} u_k v_k &= U_n v_n + \sum_{k=1}^{n-1} U_k(v_k - v_{k+1})\end{aligned}$$

I Caractères des groupes abéliens finis

1. Soit G un groupe commutatif noté multiplicativement, $x \in G$ un élément autre que le neutre, et $gr(x)$ le sous-groupe engendré par x. Soit m son ordre. Alors $gr(x)$ est isomorphe au groupe $\mathbf{U}_m$ des racines m-ièmes de l'unité dans $\mathbf{C}^*$ (un isomorphisme étant par exemple donné par $\varphi : x^k \mapsto \exp(2ik\pi/m)$). Par conséquent, si l'on note $i : \mathbf{U}_m \to \mathbf{C}^*$ le morphisme d'inclusion, $\chi = i \circ \varphi$ est un caractère de $gr(x)$ tel que $\chi(x) = \exp(2i\pi/m) \neq 1$.

2. Soit $\mathcal{F}$ la famille des sous-groupes H de G contenant x tels que χ se prolonge en un caractère de H. $\{\operatorname{Card} H \ / \ H \in \mathcal{F}\}$ est une partie de $\mathbf{N}$ non vide (car contenant $\operatorname{Card} gr(x)$) et majorée, donc $\mathcal{F}$ a un élément G' de cardinal maximal. Supposons que $G' \neq G$ et soit $y \in G - G'$.

   En notant $|y|$ l'ordre de y dans G, on a $y^{|y|} = 1 \in G'$ donc il existe un entier $n \geq 1$ minimal tel que $z = y^n \in G'$. On considère G'' le sous-groupe de G engendré par G' et y. On a $G'' = \{ay^r \ / \ a \in G',\ r \in \mathbf{Z}\}$ puisque ce dernier ensemble est bien un sous-groupe de G, et que le sous-groupe engendré par G' et y le contient nécessairement. Soit alors α une racine n-ième de $\chi(z)$ dans $\mathbf{C}^*$. On prolonge χ à G'' en posant, pour tous $a \in G'$ et $r \in \mathbf{Z}$:

$$\chi(ay^r) = \chi(a)\alpha^r$$

   On définit bien ainsi une application. En effet, si $ay^r = a'y^{r'}$, on a $y^{r-r'} = a'a^{-1} \in G''$, donc $r' = nq + r$ pour un certain $q \in \mathbf{Z}$. Et alors $a = a'y^{nq} = a'z^q$, d'où :

$$\chi(a')\alpha^{r'} = \chi(a')\chi(z)^q\alpha^r = \chi(a'z^q)\alpha^r = \chi(a)\alpha^r$$

   De plus, on a, pour tous $(a,b) \in G'^2$ et $(r,s) \in \mathbf{Z}^2$:

$$\chi(ay^r)\chi(by^s) = \chi(a)\alpha^r\chi(b)\alpha^s = \chi(ab)\alpha^{r+s} = \chi((ay^r)(by^s))$$

   donc l'application prolongée est bien un caractère, d'où $G'' \in \mathcal{F}$, ce qui contredit la maximalité du cardinal de G'. Donc χ se prolonge en un caractère de G.

   Soit alors x un élément du noyau du morphisme $G \to \hat{\hat{G}}$ qui à u associe l'application $\phi_u : \chi \mapsto \chi(u)$. Pour tout caractère $\chi \in \hat{G}$, on a donc $\chi(x) = 1$. Or d'après ce qui précède, si $x \neq 1$, il existe un caractère de G vérifiant $\chi(x) \neq 1$. Donc $x = 1$, et le morphisme est injectif.

3. Soit $\chi' \in \hat{G}$ et $x \in G$. Alors $\chi \mapsto \chi\chi'$ est une permutation de $\hat{G}$. On a donc :

$$\sum_{\chi\in\hat{G}} \chi(x) = \sum_{\chi\in\hat{G}} \chi\chi'(x)$$

Si $x \neq 1$, considérons un caractère χ' tel que $\chi'(x) \neq 1$. On a :

$$\sum_{\chi\in\hat{G}} \chi(x) = \sum_{\chi\in\hat{G}} \chi(x)\chi'(x) = \chi'(x) \sum_{\chi\in\hat{G}} \chi(x)$$

Comme $\chi'(x) \neq 1$, on a donc :

$$\sum_{\chi\in\hat{G}} \chi(x) = 0$$

Si maintenant $x = 1$, il vient :

$$\sum_{\chi\in\hat{G}} \chi(x) = \sum_{\chi\in\hat{G}} 1 = \operatorname{Card} \hat{G}$$

Soit maintenant $\chi \in \hat{G}$ fixé. Si $\chi \neq 1$, soit $y \in G$ tel que $\chi(y) \neq 1$. Il vient comme précédent :

$$\sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(xy) = \chi(y) \sum_{x\in G} \chi(x)$$

d'où $\sum_{x\in G} \chi(x) = 0$. Dans le cas $x = 1$, on a de même :

$$\sum_{x\in G} \chi(x) = \sum_{x\in G} 1 = \operatorname{Card} G$$

4. On considère la somme $S = \sum_{x,\chi} \chi(x)$. On a :

$$S = \sum_{x\in G} \sum_{\chi\in\hat{G}} \chi(x) = \sum_{\chi\in\hat{G}} \chi(1) + \sum_{x\neq 1} \sum_{\chi\in\hat{G}} \chi(x) = \operatorname{Card} \hat{G}$$

et de même :

$$S = \sum_{\chi\in\hat{G}} \sum_{x\in G} \chi(x) = \operatorname{Card} G$$

donc $\operatorname{Card} G = \operatorname{Card} \hat{G}$. Il en résulte que $\operatorname{Card} G = \operatorname{Card} \widehat{\hat{G}}$, donc le morphisme injectif $G \to \widehat{\hat{G}}$ décrit plus haut est un isomorphisme.

II Une évaluation asymptotique

1. p désignant un nombre premier, on a $v_p(xy) = v_p(x) + v_p(y)$ pour tout $(x,y) \in (\mathbf{N}^*)^2$, donc :

$$v_p(n!) = \sum_{m=1}^{n} v_p(m) = \sum_{m\leq n} \sum_{\substack{k\geq 1 \\ p^k|m}} 1 = \sum_{k\geq 1} \sum_{\substack{m\leq n \\ p^k|m}} 1$$

En effet, on peut échanger les signes de sommations car il n'y a qu'un nombre fini de termes non nuls. Précisément, les multiples de p^k inférieurs à n sont p^k,$2p^k$, …,$[n/p^k]p^k$, donc il y en a $[n/p^k]$, et :

$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

Or $\sum_{k=1}^{\infty} [n/p^k] \geq [n/p] > n/p - 1$ et :

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] \leq \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p} + \frac{n}{p^2}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)$$

donc on a l'encadrement :

$$\frac{n}{p} - 1 < v_p(n!) \leq \frac{n}{p} + \frac{n}{p^2}\frac{1}{1-1/p} = \frac{n}{p} + \frac{n}{p(p-1)}$$

2. Pour tout $m \in \mathbf{N}$, on a :

$$(1+1)^{2m+1} = 2\sum_{k=0}^{m} C_{2m+1}^{k} \geq C_{2m+1}^{m} + C_{2m}^{m} + 2\sum_{k=0}^{m-1} C_{2m}^{k} = C_{2m+1}^{m} + (1+1)^{2m}$$

Donc $C_{2m+1}^{m} \leq 2^{2m+1} - 2^{2m} = 4^m$.

Or si $m+1 < p \leq 2m+1$, on a $p|(2m+1)!$ et $p \not| \, m!(m+1)!$, d'où $p|C_{2m+1}^{m}$. Donc $\prod_{m+1<p\leq 2m+1} p$ divise C_{2m+1}^{m}, et :

$$\prod_{m+1<p\leq 2m+1} p \leq 4^m$$

3. Notons pour tout $n \in \mathbf{N}$, $\mathcal{P}(n) : \prod_{p\leq n} p \leq 4^n$. On a $\mathcal{P}(0)$, $\mathcal{P}(1)$, $\mathcal{P}(2)$. Soit alors $n > 2$. Supposons $\mathcal{P}(k)$ pour tout $k < n$. Si n est pair, il n'est pas premier, donc on a :

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p \leq 4^{n-1} \leq 4^n$$

Sinon, soit m tel que $n = 2m+1$. D'après ce qui précède, on a :

$$\prod_{p\leq n} p = \prod_{p\leq m+1} p \prod_{m+1<p\leq 2m+1} p \leq 4^{m+1}4^m = 4^n$$

donc on a bien $\mathcal{P}(n)$ pour tout $n \in \mathbf{N}$.

4. Tout les facteurs premiers de $n!$ étant inférieurs à n, on a $n! = \prod_{p\leq n} p^{v_p(n!)}$, d'où :

$$\frac{\ln(n!)}{n} = \sum_{p\leq n} \frac{v_p(n!)}{n} \ln p$$

Donc d'après l'encadrement du 1, il vient :

$$\sum_{p\leq n} \left(\frac{1}{p} - \frac{1}{n}\right) \ln p < \frac{\ln(n!)}{n} \leq \sum_{p\leq n} \left(\frac{1}{p} + \frac{1}{p(p-1)}\right) \ln p$$

On a donc :

$$\sum_{p\leq n} \frac{\ln p}{p} < \frac{\ln(n!)}{n} + \frac{1}{n} \ln \prod_{p\leq n} p \leq \ln n - 1 + O\left(\frac{\ln n}{n}\right) + \frac{n \ln 4}{n}$$

et de même :

$$\sum_{p\leq n} \frac{\ln p}{p} \geq \frac{\ln(n!)}{n} + \frac{1}{n} \sum_{p\leq n} \frac{\ln p}{p(p-1)} \geq \ln n - 1 + O\left(\frac{\ln n}{n}\right) + O\left(\frac{1}{n}\right)$$

puisque $\sum_{p\leq n} (\ln p)/(p(p-1))$ est inférieure à $\sum_{m\geq 2} (\ln m)/(m^2 - m) < +\infty$. Il vient par conséquent :

$$\sum_{p\leq x} \frac{\ln p}{p} = \sum_{p\leq [x]} \frac{\ln p}{p} = \ln[x] + O(1) = \ln x + O(1)$$

car $\ln(x+1) - \ln(x) \leq 1/x \leq 1$ pour $x \geq 1$.

III Fonctions L de Dirichlet

Dorénavant, N est un entier non nul fixé, et les caractères considérés sont des caractères du groupe $G(N)$ des inversibles de $\mathbf{Z}/N\mathbf{Z}$, relevés à $\mathbf{N}$ tout entier en posant $\chi(m) = 0$ si m et N ne sont pas premiers entre eux.

1. Soit χ un caractère non trivial. Alors pour tout $k \in \mathbf{N}$:

$$\sum_{n=kN+1}^{(k+1)N} \chi(n) = \sum_{n \in \mathbf{Z}/N\mathbf{Z}} \chi(n) = \sum_{n \in G(N)} \chi(n) = 0$$

donc $\sum_{n=1}^{kN} \chi(n) = 0$ pour tout k, et la suite de terme général $U_n = \sum_{k=1}^{n} \chi(k)$ vérifie, si l'on note $n = Nq + r$:

$$|U_n| = \left| \sum_{n=Nq}^{Nq+r} \chi(n) \right| \leq \sum_{n \in \mathbf{Z}/N\mathbf{Z}} |\chi(n)| \leq N$$

et (U_n) est bornée. Par conséquent, si (v_n) est une suite de réels positifs décroissant vers 0 à partir d'un certain rang, $\sum_{n \geq 1} \chi(n) v_n$ converge d'après la règle d'Abel. En particulier, $\sum_{n \geq 1} \chi(n)/n$ converge, et de même pour $\sum_{n \geq 1} \chi(n) \ln(n)/n$, puisque :

$$\frac{d}{dx} \frac{\ln x}{x} = \frac{1 - \ln x}{x^2} \leq 0 \quad \text{pour } x \geq e$$

2. Dans la suite de cette partie, χ est à valeurs réelles. Soit $f : \mathbf{N}^* \to \mathbf{R}$ la fonction définie par $f(n) = \sum_{d|n} \chi(d)$. Si m et n sont des entiers ≥ 1 premiers entre eux et $d|mn$, il existe un unique couple $(a,b) \in (\mathbf{N}^*)^2$ (à savoir $(\mathrm{pgcd}(d,m), \mathrm{pgcd}(d,n))$) tel que $d = ab$, $a|m$ et $b|n$, donc :

$$f(mn) = \sum_{\substack{a|m \\ b|n}} \chi(ab) = \sum_{a|m} \sum_{b|n} \chi(a)\chi(b) = f(m)f(n)$$

Pour tout p premier et tout $\nu \in \mathbf{N}$, on a :

$$f(p^\nu) = \sum_{k=0}^{\nu} \chi(p^k) = \sum_{k=0}^{\nu} \chi(p)^k$$

Or $\chi(p) \in \{-1,0,1\}$. Si $\chi(p) = 0$ ou 1, on a donc $f(p^\nu) \geq \chi(p)^0 = 1$. Sinon, $\chi(p) = -1$ et $f(p^\nu) = (1 - (-1)^{\nu+1})/2 = 1$ ou 0 selon que ν est pair ou impair. Soit alors $n = p_1^{\nu_1} \dots p_r^{\nu_r}$. On a :

$$\chi(n) = \prod_{i=1}^{r} f(p_i^{\nu_i})$$

Si n est un carré, tous les ν_i sont pairs, donc $f(n) \geq 1$. Sinon, $f(n) \geq 0$.

Pour $x \in \mathbf{R}_+$, on pose $g(x) = \sum_{n \leq x} f(n)/\sqrt{n}$. Pour tout $x \geq 0$, on a, puisque $f(n) \geq 0$ pour tout n :

$$g(x) \geq \sum_{\substack{n \leq x \\ n \text{ carré}}} \frac{f(n)}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{f(m^2)}{\sqrt{m^2}} \geq \sum_{m \leq \sqrt{x}} \frac{1}{m}$$

Donc $\lim_{x \to +\infty} g(x) = +\infty$.

3. Pour tout $x \geq 0$ on a :

$$g(x) = \sum_{\substack{n \leq x \\ d|n}} \frac{\chi(d)}{\sqrt{n}} = \sum_{dd' \leq x} \frac{1}{\sqrt{d'}} \frac{\chi(d)}{\sqrt{d}}$$

Soit alors $(d,d') \in (\mathbf{N}^*)^2$ tel que $dd' \leq x$. On a exactement l'une des deux situations : ($d' \leq \sqrt{x}$ et $d > \sqrt{x}$) ou $d \leq \sqrt{x}$. En effet, si l'on n'a pas $d > \sqrt{x}$, alors $d \leq \sqrt{x}$, et inversement, si l'on n'a pas $d \leq \sqrt{x}$, alors $d > \sqrt{x}$ et $d' \leq x/d \leq \sqrt{x}$. On ne peut bien sûr pas avoir les deux simultanément, donc :

$$\begin{aligned} g(x) &= \sum_{\substack{dd' \leq x \\ d' \leq \sqrt{x} \\ d > \sqrt{x}}} \frac{1}{\sqrt{d'}} \frac{\chi(d)}{\sqrt{d}} + \sum_{\substack{dd' \leq x \\ d \leq \sqrt{x}}} \frac{\chi(d)}{\sqrt{d}} \frac{1}{\sqrt{d'}} \\ g(x) &= \sum_{d' \leq \sqrt{x}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x} < d \leq x/d'} \frac{\chi(d)}{\sqrt{d}} + \sum_{d \leq \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{d' \leq x/d} \frac{1}{\sqrt{d'}} \\ g(x) &= g_1(x) + g_2(x) \end{aligned}$$

Pour évaluer $g(x)$, on aura besoin d'un développement asymptotique de :

$$h(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}}$$

Comme $t \mapsto 1/\sqrt{t}$ est décroissante, $h(x) - \int_1^x dt/\sqrt{t}$ tend vers une limite finie $(2+\alpha)$ quand $x \to +\infty$. On a donc :

$$h(x) = 2 + \alpha + \Big[2\sqrt{t}\Big]_1^x + o(1) = 2\sqrt{x} + \alpha + o(1)$$

En notant $h_n = h(n) - 2\sqrt{n}$, on a :

$$\begin{aligned} h_{n+1} - h_n &= \frac{1}{\sqrt{n+1}} - 2(\sqrt{n+1} - \sqrt{n}) = \frac{1}{\sqrt{n}} \left(\frac{1}{\sqrt{1+1/n}} - \frac{2\sqrt{n}}{\sqrt{n} + \sqrt{1+n}} \right) \\ h_{n+1} - h_n &\sim \frac{1}{\sqrt{n}} \left(\frac{1}{1+\frac{1}{2n}} - \frac{2}{2+\frac{1}{2n}} \right) = \frac{1}{\sqrt{n}} \left(\frac{2n(4n+1) - 4n(2n+1)}{(2n+1)(4n+1)} \right) \\ h_{n+1} - h_n &\sim -\frac{1}{4n^{3/2}} \end{aligned}$$

donc $-h_n \sim \int_n^{+\infty} -dt/(4t^{3/2}) = -1/(2\sqrt{n})$, d'où :

$$h(x) = 2\sqrt{x} + \alpha + O(\frac{1}{\sqrt{x}})$$

On remarque également que pour $0 < a < b$ et $\beta > 0$:

$$\left| \sum_{a < n \leq b} \frac{\chi(n)}{n^\beta} \right| \leq \frac{N}{[b]^\beta} + N \sum_{a < n \leq [b]-1} \frac{1}{n^\beta} - \frac{1}{(n+1)^\beta} \leq \frac{N}{a^\beta}$$

Il vient donc :

$$|g_1(x)| \leq \sum_{d' \leq \sqrt{x}} \frac{1}{\sqrt{d'}} \frac{N}{x^{1/4}} = N x^{-1/4} h(\sqrt{x}) = O(1)$$

et d'autre part :

$$g_2(x) - \sum_{d \leq \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \left(2\sqrt{\frac{x}{d}} + \alpha \right) = O\left(\sum_{d \leq \sqrt{x}} \frac{|\chi(d)|}{d} \sqrt{\frac{d}{x}} \right) = O(1)$$

donc :

$$\begin{aligned} g_2(x) - 2\sqrt{x}L(\chi) &= \alpha \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} - 2\sqrt{x} \sum_{d>\sqrt{x}} \frac{\chi(d)}{d} + O(1) \\ g_2(x) - 2\sqrt{x}L(\chi) &= \alpha\, O(1) - 2\sqrt{x}\, O(\frac{1}{\sqrt{x}}) + O(1) \end{aligned}$$

d'où finalement :

$$g(x) - 2\sqrt{x}L(\chi) = O(1)$$

4. Si $L(\chi) = 0$, on a donc $g(x) - 2\sqrt{x}L(\chi) = g(x) = O(1)$ quand x tend vers $+\infty$, ce qui contredit le résultat du 2. Donc pour tout caractère réel non trivial χ, $L(\chi) \neq 0$.

IV Transformation de Moebius

1. Pour tout $n \in \mathbf{N}^*$, on pose $\mu(n) = 0$ si n est un carré, et $\mu(n) = (-1)^r$ si n est le produit de r nombres premiers distincts. Soit alors $n \geq 2$ quelconque, et $\{p_1, \ldots, p_r\}$ son support premier. On a :

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{r} C_r^k (-1)^k = (1-1)^r = 0$$

puisque n a C_r^k diviseurs qui sont le produits de k nombres premiers distincts.

2. Soit H une fonction non nulle $\mathbf{N}^* \to \mathbf{C}$ telle que pour tout $(m,n) \in (\mathbf{N}^*)^2$, $H(mn) = H(m)H(n)$. Il existe alors $n \in \mathbf{N}^*$ tel que $H(n) \neq 0$, et l'on a :

$$H(n) = H(n.1) = H(n)H(1) \quad \text{donc} \quad H(1) = 1$$

On se donne par ailleurs F, G deux fonctions $[1,\infty[\to \mathbf{C}$ vérifiant pour tout $x \geq 1$:

$$G(x) = \sum_{1\leq k\leq x} F(x/k)H(k)$$

On a alors, pour tout $x \geq 1$:

$$\begin{aligned} \sum_{1\leq k\leq x} \mu(k)G(x/k)H(k) &= \sum_{1\leq k\leq x} \mu(k)H(k) \sum_{1\leq l\leq x/k} F(\frac{x}{kl})H(l) \\ \sum_{1\leq k\leq x} \mu(k)G(x/k)H(k) &= \sum_{1\leq kl\leq x} \mu(k)F(\frac{x}{kl})H(kl) \\ \sum_{1\leq k\leq x} \mu(k)G(x/k)H(k) &= \sum_{1\leq n\leq x} F(x/n)H(n) \sum_{k|n} \mu(k) \\ \sum_{1\leq k\leq x} \mu(k)G(x/k)H(k) &= F(x/1)H(1) = F(x) \end{aligned}$$

3. Soit alors Λ la fonction $[1,+\infty[\to \mathbf{R}$ qui à p^n associe $\ln p$, et qui est nulle sur tous les réels qui ne sont pas une puissance de nombre premier. On considère alors $\Gamma : [1,+\infty[\to \mathbf{R}$ définie par :

$$\Gamma(x) = \sum_{1\leq k\leq x} \Lambda(x/k)$$

Si $x \notin \mathbf{N}^*$, $x/k \notin \mathbf{N}^*$ pour tout k, donc $\Gamma(x) = 0$. Soit alors $m = p_1^{\nu_1} \ldots p_r^{\nu_r}$. On a :

$$\Gamma(m) = \sum_{\substack{1\leq k\leq m \\ m/k \text{ puissance d'un } p}} \Lambda(m/k) = \sum_{i=1}^{r} \sum_{n=1}^{\nu_i} \Lambda(p_i^n) = \sum_{i=1}^{r} \nu_i \ln p_i = \ln m$$

donc d'après ce qui précède, on a :

$$\Lambda(m) = \sum_{\substack{1\leq k\leq m \\ m/k \text{ entier}}} \mu(k)\Gamma(m/k) = \sum_{d|m} \mu(d)\ln(m/d)$$

V Le théorème de Dirichlet

Soit χ un caractère non trivial.

1. Posons $G(x) = \sum_{1\leq n\leq x} \frac{x}{n}\chi(n)$. On a :

$$G(x) - xL(\chi) = x\sum_{n>x} \frac{\chi(n)}{n} = xO(\frac{1}{x})$$

d'après les résultats du III.3, et $G(x) - xL(\chi)$ est borné.

Supposons $L(\chi) \neq 0$. On a $G(x) = xL(\chi) + O(1)$, donc la transformation de Moebius donne :

$$x = \sum_{n\leq x} \mu(n)G(x/n)\chi(n) = \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n}(xL(\chi) + O(1))$$

d'où :

$$\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = \frac{x}{xL(\chi) + O(1)} = \frac{1}{L(\chi)} + O(1/x) = O(1)$$

2. Supposons $L(\chi) = 0$, et notons $G_1(x) = \sum_{1\leq n\leq x}(\frac{x}{n}\ln\frac{x}{n})\chi(n)$. On a :

$$G_1(x) = \sum_{1\leq n\leq x} \left(\frac{x\ln x}{n} - x\frac{\ln n}{n}\right)\chi(n) = G(x)\ln x - x\sum_{1\leq n\leq x} \frac{\chi(n)\ln n}{n}$$

Or $G(x) = O(1)$, et comme pour tout $m > x > e$:

$$\left|\sum_{x<n\leq m} \frac{\chi(n)\ln n}{n}\right| \leq \frac{N\ln m}{m} + N\left(\frac{\ln x}{x} - \frac{\ln m}{m}\right) = \frac{N\ln x}{x}$$

on a $\sum_{1\leq n\leq x} \frac{\chi(n)\ln n}{n} = L_1(\chi) + O(\frac{\ln x}{x})$, et :

$$G_1(x) = O(\ln x) - x\left(L_1(\chi) + O(\frac{\ln x}{x})\right) = -xL_1(\chi) + O(\ln x)$$

La transformation de Moebius donne donc :

$$x\ln x = \sum_{n\leq x} \mu(n)G_1(x/n)\chi(n) = \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n}(-xL_1(\chi) + O(\ln x))$$

Par conséquent :

$$\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = \frac{x\ln x}{-xL_1(\chi) + O(\ln x)} = -\frac{\ln x}{L_1(\chi)} + O(1/x)$$

et $L_1(\chi)\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} + \ln x$ est borné.

3. Pour tout $x > e$, on a :

$$\begin{aligned} L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} &= \sum_{d\leq x}\frac{\mu(d)\chi(d)}{d}\left[\sum_{1\leq k\leq x/d}\frac{\chi(k)\ln k}{k}+\sum_{k>x/d}\frac{\chi(k)\ln k}{k}\right] \\ L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} &= \sum_{kd\leq x}\frac{\chi(kd)}{kd}\mu(d)\ln k+O\left(\sum_{d\leq x}\mu(d)\frac{\ln(x/d)}{x/d}\frac{\chi(d)}{d}\right) \end{aligned}$$

Si l'on pose $F(x)=\sum_{d\leq x}\mu(d)\frac{\ln(x/d)}{x/d}\frac{\chi(d)}{d}$, on a :

$$\left|\frac{\ln x}{x}\right|\geq\sum_{1\leq k\leq x}|F(x/k)|\frac{|\chi(k)|}{k}\geq|F(x)|$$

donc :

$$\begin{aligned} L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} &= \sum_{m\leq x}\frac{\chi(m)}{m}\sum_{d|m}\mu(d)\ln(m/d)+O(\frac{\ln x}{x}) \\ L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} &= \sum_{m\leq x}\frac{\chi(m)}{m}\Lambda(m)+O(1) \\ L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} &= \sum_{p\leq x}\frac{\chi(p)\ln p}{p}+\sum_{\substack{k\geq 2\\ p^k\leq x}}\frac{\chi(p)^k\ln p}{p^k}+O(1) \\ L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} &= \sum_{p\leq x}\frac{\chi(p)\ln p}{p}+O(1) \end{aligned}$$

car on a :

$$\left|\sum_{\substack{k\geq 2\\ p^k\leq x}}\frac{\chi(p)^k\ln p}{p^k}\right|\leq\sum_{k\geq 2}\sum_{p}\frac{\ln p}{p^k}\leq\sum_{k\geq 2}\int_1^{+\infty}\frac{\ln t}{t^k}dt=\sum_{k\geq 2}\frac{1}{(k-1)^2}<+\infty$$

4. D'après ce qui précède, on a donc :

$$\sum_{p\leq x}\frac{\chi(p)\ln p}{p}=L_1(\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n}+O(1)=\begin{cases} O(1) & \text{si } L(\chi)\neq 0\\ -\ln x+O(1) & \text{si } L(\chi)=0\end{cases}$$

5. Soit T le nombre de caractères non triviaux tels que $L(\chi)=0$. On a :

$$\begin{aligned} \sum_{\chi\in\widehat{G(N)}}\sum_{p\leq x}\frac{\chi(p)\ln p}{p} &= \sum_{p\leq x}\frac{\ln p}{p}+\sum_{\substack{\chi\in\widehat{G(N)}-\{1\}\\ L(\chi)=0}}\sum_{p\leq x}\frac{\chi(p)\ln p}{p}+\sum_{\substack{\chi\in\widehat{G(N)}-\{1\}\\ L(\chi)\neq 0}}\sum_{p\leq x}\frac{\chi(p)\ln p}{p} \\ \sum_{\chi\in\widehat{G(N)}}\sum_{p\leq x}\frac{\chi(p)\ln p}{p} &= (\ln x+O(1))+(-T\ln x+O(1))+O(1) \\ \sum_{\chi\in\widehat{G(N)}}\sum_{p\leq x}\frac{\chi(p)\ln p}{p} &= (1-T)\ln x+O(1) \end{aligned}$$

Or, comme $G(N)$ est fini, on peut sommer par paquets :

$$\sum_{\chi\in\widehat{G(N)}}\sum_{p\leq x}\frac{\chi(p)\ln p}{p}=\sum_{p\leq x}\left(\sum_{\chi\in\widehat{G(N)}}\chi(p)\right)\frac{\ln p}{p}=\sum_{\substack{p\leq x\\ p\equiv 1 \bmod N}}\operatorname{Card}G(N)\frac{\ln p}{p}$$

puisque $\sum_{\chi\in\widehat{G(N)}}\chi(p)=0$ pour $p\not\equiv 1 \bmod N$. On trouve donc bien :

$$\operatorname{Card} G(N)\sum_{\substack{p\leq x\\ p\equiv 1 \bmod N}}\frac{\ln p}{p}=(1-T)\ln x+O(1)$$

Comme le membre de gauche est positif pour tout x, on a $T\leq 1$, puisque pour x grand, $(1-T)\ln x+O(1)$ est négatif si $T>1$.

6. On a vu que pour les caractères réels non triviaux, on avait $L(\chi)\neq 0$. Supposons alors que χ soit un caractère non trivial tel que $L(\chi)=0$. χ ne prend donc pas que des valeurs réelles, d'où $\bar\chi\neq\chi$. Or $L(\bar\chi)=\overline{L(\chi)}=0$, donc $T\geq 2$, ce qui est absurde. On a donc $T=0$.

7. Soit l un entier premier à N. On a alors $\bar 1(l)=1$, d'où :

$$\sum_{\chi\in\widehat{G(N)}}\sum_{p\leq x}\bar\chi(l)\frac{\chi(p)\ln p}{p}=\sum_{p\leq x}\frac{\ln p}{p}+\sum_{\chi\in\widehat{G(N)}-\{1\}}\bar\chi(l)O(1)=\ln x+O(1)$$

Or, comme précédemment :

$$\sum_{\chi\in G(N)}\sum_{p\leq x}\bar\chi(l)\frac{\chi(p)\ln p}{p}=\sum_{p\leq x}\left(\sum_{\chi\in G(N)}\bar\chi(l)\chi(p)\right)\frac{\ln p}{p}=\sum_{\substack{p\leq x\\ p/l\equiv 1 \bmod N}}\operatorname{Card} G(N)\frac{\ln p}{p}$$

Donc :

$$\sum_{\substack{p\leq x\\ p\equiv l \bmod N}}\frac{\ln p}{p}\sim\frac{\ln x}{\operatorname{Card} G(N)}$$

n'est pas borné. Il en résulte que $\{p \text{ premier } / \ p\equiv l \bmod N\}$ est infini.

VI Polynômes cyclotomiques

Pour P un polynôme non nul à coefficients entiers, on note $c(P)$ le plus grand diviseur commun de ses coefficients.

1. Soient P et Q deux polynômes non nuls à coefficients entiers. Posons $P_1=P/c(P)$, $Q_1=Q/c(Q)$. On a $c(P_1)=c(Q_1)=1$. Soit alors p un éventuel diviseur premier de $c(P_1Q_1)$. Il vient $P_1Q_1\equiv 0 \bmod p$. Or $\mathbf{Z}/p\mathbf{Z}[X]$ est un anneau intègre, donc on a $p|P_1$ ou $p|Q_1$, ce qui est absurde. Par conséquent :

$$c(P_1Q_1)=\frac{c(PQ)}{c(P)c(Q)}=1 \quad \text{d'où} \quad c(PQ)=c(P)c(Q)$$

2. Soit ζ une racine n-ième de l'unité, et P_ζ le polynôme unitaire de $\mathbf{Q}[X]$ de plus petit degré qui annule ζ. Comme $\mathbf{Q}[X]$ est principal, P_ζ est le générateur canonique de l'idéal des polynômes annulateurs de ζ. En particulier, il existe $Q\in\mathbf{Q}[X]$ tel que $X^n-1=QP_\zeta$. Soient m, n les plus grands communs multiples des dénominateurs des coefficients de P_ζ et Q respectivement. mP_ζ et nQ sont à coefficients entiers et primitifs. Or :

$$c(mnQP_\zeta)=c(mn(X^n-1))=mn$$

donc $mn=c(mP_\zeta)c(nQ)=1$, et $P_\zeta\in\mathbf{Z}[X]$.

3. Soit d le degré de P_ζ et $\mathcal{B} = (1,\zeta,\ldots,\zeta^{d-1}) \in \mathbf{Q}[\zeta]^d$. Considérons l'application $\varphi : \mathbf{Q}[X]/(P_\zeta) \to \mathbf{Q}[\zeta]$ définie par $\phi(P) = P(\zeta)$. Elle est bien définie, car si $P \equiv 0 \bmod P_\zeta$, on a $P(\zeta) = 0$. Elle est $\mathbf{Q}$-linéaire, et surjective, car le sous-anneau de $\mathbf{C}$ engendré par $\mathbf{Q}$ et ζ est formé des valeurs des polynômes de $\mathbf{Q}[X]$ en ζ. De plus, si $\varphi(P) = 0$, on a $P(\zeta) = 0$ donc $P \in (P_\zeta)$ d'après ce qui précède. φ est donc un isomorphisme, et $\mathcal{B}$ est l'image par φ de la base $(1,X,\ldots,X^{d-1})$ de $\mathbf{Q}[X]/(P_\zeta)$, donc c'est une base de $\mathbf{Q}[\zeta]$.

4. Soit $P = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_0$ un polynôme à coefficients entiers. On a :

$$P(X^p) \equiv \sum_{i=0}^{m} a_i^p (X^p)^i \equiv \sum_{i=0}^{m} (a_i X^i)^p \equiv P(X)^p \bmod p$$

d'après le petit théorème de Fermat. Donc il existe $G_p \in \mathbf{Z}[X]$ tel que $P(X^p) = P(X)^p + pG_p(X)$.

5. Pour tout $x \in \mathbf{Z}[\zeta]$, on note $M(x)$ la matrice de l'application $y \mapsto xy$ dans la base $\mathcal{B}$. Pour tout $(x,y) \in \mathbf{Z}[\zeta]^2$, on a $(M(x)^k)(y) = x^k y$, donc si $P \in \mathbf{Z}[X]$:

$$P(M(x))(y) = P(x)y = M(P(x))(y) \quad \text{donc} \quad P(M(x)) = M(P(x))$$

Posons $M = M(\zeta)$. M est la matrice :

$$M = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & \vdots & 0 \\ & \ddots & 0 & \vdots \\ 0 & & 1 & 0 \end{bmatrix} \in \mathbf{M}_d(\mathbf{Z})$$

Donc pour tout $k \in \mathbf{Z}$, $M^k \in \mathbf{M}_d(\mathbf{Z})$.

Soit l un entier premier à n. Il existe une suite $(p_i)_{i\in\mathbf{N}}$ de nombres premiers tels que $p_i \equiv l \bmod n$. En particulier, on a $M^l = M^{p_i}$ pour tout i. Donc :

$$P_\zeta(M^l) \equiv P_\zeta(M)^{p_i} \equiv 0 \bmod p_i$$

et p_i divise tous les coefficients de $P_\zeta(M^l)$ pour tout $i \in \mathbf{N}$. Comme un entier non nul a un support premier fini, il en résulte que $P_\zeta(M^l) = 0$, donc :

$$P_\zeta(\zeta^l) = P_\zeta(M^l)(1) = 0$$

6. On note pour tout $d \in \mathbf{N}$, $E_d = \{k/d,\ \text{pgcd}(k,d) = 1 \text{ et } 1 \le k \le d\}$. Soit alors a un entier tel que $1 \le a \le n$, et $\delta = \text{pgcd}(a,n)$, $a = \delta k$, $n = \delta d$. On a :

$$\frac{a}{n} = \frac{k}{d} \quad \text{avec} \quad \text{pgcd}(k,d) = 1 \text{ et } 1 \le k \le n/\delta = d$$

donc $a/n \in E_d$ où $d|n$. Par conséquent :

$$\left\{\frac{k}{n},\ k = 1,\ldots,n\right\} = \bigcup_{d|n} E_d$$

et la réunion est disjointe, car si $a/n = k/d$ avec $\text{pgcd}(k,d) = 1$, on a :

$$\frac{a}{k} = \text{pgcd}(k,\frac{ad}{k}) = \text{pgcd}(a,n)$$

qui ne dépend que de a.

On note alors pour tout $d \in \mathbf{N}$:

$$\Phi_d(X) = \prod_{\substack{\text{pgcd}(k,d)=1 \\ 1 \leq k \leq d}} \left(X - \exp(\frac{2ik\pi}{d}) \right)$$

On a donc :

$$X^n - 1 = \prod_{k=1}^{n} \left(X - \exp(\frac{2ik\pi}{n}) \right) = \prod_{d|n} \prod_{k/d \in E_d} \left(X - \exp(\frac{2ik\pi}{d}) \right) = \prod_{d|n} \Phi_d(X)$$

Montrons alors par récurrence que $\Phi_n \in \mathbf{Z}[X]$ pour tout $n \in \mathbf{N}^*$. C'est le cas pour $n = 1$. Soit alors $n > 1$, et supposons $\Phi_d \in \mathbf{Z}[X]$ pour tout $d < n$. On a :

$$\Phi_n(X) = \frac{X^n}{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)} \in \mathbf{C}[X] \cap \mathbf{Q}(X) = \mathbf{Q}[X]$$

Notons donc m le p.p.c.m. des dénominateurs coefficients de Φ_n. On a :

$$c\left(m \prod_{d|n} \Phi_d \right) = c(m\Phi_n) \prod_{\substack{d|n \\ d<n}} c(\Phi_d) = 1$$

puisque les Φ_d sont unitaires. Or :

$$c\left(m \prod_{d|n} \Phi_d \right) = c(m(X^n - 1)) = m$$

d'où $m = 1$ et $\Phi_n \in \mathbf{Z}[X]$.

7. P_ζ divise $X^n - 1 = \prod_{d|n} \Phi_d(X)$ donc, comme P_ζ est irréductible dans $\mathbf{Q}[X]$, il divise l'un des Φ_d. Les polynômes Φ_d étant unitaires, il en résulte qu'il existe $d|n$ tel que $P_\zeta = \Phi_d$. Quand ζ parcourt l'ensemble des racines de l'unité, d parcourt $\mathbf{N}^*$, donc tous les Φ_d sont irréductibles dans $\mathbf{Q}[X]$ (et également dans $\mathbf{Z}[X]$, car $c(\Phi_d) = 1$).