À L'ASSAUT DE LA THÈSE DE TATE! (UN PETIT ASSAUT)

MATHIAS GARNIER

Les premières parties puisent dans le chapitre 8 du Tome 1 *Fourier analysis* de Stein & Shakarchi pour traiter le cas des groupes abéliens finis. Remarquons que pour l'introduction des séries de Fourier sur ces groupes, on pourrait ne pas suivre la convention de Stein & Shakarchi et c'est ce qui est parfois fait (cela a l'inconvénient de compliquer légèrement la formule de Parseval par exemple). Comme toujours, lorsque Tao écrit, c'est exactement ce qu'il fallait. On utilise donc quelques unes de ses notes de la classe 247B. Pour l'aspect harmonique, on suit *Aspects of harmonic analysis on locally compact abelian groups* de Gallier & Quantaince. Concernant la thèse de Tate, on se garde pour l'instant de la lire directement et l'on étudie ce qu'en dit Bjorn Poonen.

À reprendre et finir un jour.

TABLE DES MATIÈRES

On commence par quelques rappels généraux où l'on ne va pas ou peu dans le détail.

1. Groupes abéliens finis

Soit G un groupe abélien fini et $\mathbb{S}^1 \subset \mathbf{C}$ le cercle unité. On appelle caractère de G tout morphisme $\chi : G \to \mathbb{S}^1$ et l'on note $\widehat{G} = \mathrm{Hom}(G, \mathbb{S}^1)$ l'ensemble des caractères de G, également appelé dual de G. Pour la multiplication point par point, il est direct de remarquer que $\widehat{G}$ forme un groupe abélien.

Il est bon de noter que $\widehat{\mathbf{Z}/n\mathbf{Z}} = \mathbf{Z}/n\mathbf{Z}$. Par le théorème de classification des groupes abéliens finis, on en déduit automatiquement le dual de n'importe quel groupe abélien fini. Pour être tout à fait rigoureux et que ce résultat soit pleinement démontré, il convient de remarquer que $\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$.

Date: février 2025.

2. Propriétés à la Hilbert

On commet ici un abus de langage clair, nous sommes loin des Hilbert. Néanmoins, certaines propriétés du dual de G peuvent y faire penser. Soit E l'espace vectoriel $\mathrm{L}(G, \mathbf{C}) = \{f : G \to \mathbf{C}\}$. On y définit un produit scalaire hermitien comme suit : pour $f, g \in E$, on a $(f, g) = 1/|G| \sum_{a\in G} f(a)\overline{g(a)}$.

Proposition 1. *Les caractères de G forment une famille orthonormale.*

Démonstration. Soit $\chi \in \widehat{G}$, par définition on a $|\chi(x)| = 1$ pour tout x dans G. Il vient alors :

$$(\chi, \chi) = \frac{1}{|G|}\sum_{a\in G} \chi(a)\overline{\chi(a)} = \frac{1}{|G|}\sum_{a\in G} |\chi(a)|^2 = 1.$$

Il reste à prouver que $(\chi_1, \chi_2) = 0$ si χ_1 et χ_2 sont deux caractères distincts. Pour cela, rappelons que $\sum_{a\in G} \chi(a) = 0$ pour tout caractère χ non trivial, i.e. non identiquement égal à 1. Pour prouver ce résultat, multiplier par un caractère évalué (non égal à 1) et penser à chercher une bijection. Remarquons alors que le caractère $\chi_1\chi_2^{-1} = \chi_1\overline{\chi_2}$ ne peut pas être trivial par construction. On conclut alors directement par application du résultat rappelé. □

Plus précisément, on dispose du résultat suivant nous permettant alors d'affirmer que $|\widehat{G}| = |G|$. [1]

Proposition 2. *Les caractères de G forment une base orthonormale de E.*

Une preuve spectrale est possible, c'est celle présentée dans le Stein & Shakarchi. Pour une preuve alternative, nous avons donné tous les outils nécessaires plus haut.

3. Fourier ne meurt jamais

Nous sommes alors naturellement conduits à introduire les coefficients de Fourier de $f \in E$ par rapport à $\chi \in \widehat{G}$: $\hat{f}(\chi) = (f, \chi) = \frac{1}{|G|}\sum_{a\in G} f(a)\overline{\chi(a)}$. La série de Fourier de f est alors sans aucun doute : $f(x) = \sum_{\chi\in\widehat{G}} \hat{f}(\chi)\chi(x)$. Pour la norme dérivant du produit scalaire, on dispose logiquement de la formule de Parseval : $||f||^2 = \sum_{\chi\in\widehat{G}} |\hat{f}(\chi)|^2$. Enfin, comme dans le cas continu, le produit de convolution $(f * g)(x) = 1/|G| \sum_{y\in G} f(y)g(xy^{-1})$ vérifie $(\widehat{f * g})(\chi) = \hat{f}(\chi)\hat{g}(\chi)$ pour tout caractère χ. L'avantage de travailler sur des groupes abéliens finis se résume en ce qu'il n'existe aucun soucis de convergence de sommes.

4. Ce que l'on attend de Fourier

Avant d'étendre la théorie des caractères aux groupes abéliens localement compacts, arrêtons nous rapidement sur le cas classique de l'analyse de Fourier sur $\mathbf{R}^n$.

5. Extension aux localement compacts

Soit G un groupe abélien localement compact, i.e. un groupe abélien topologique dont l'espace topologique sous-jacent est localement compact. Un caractère est désormais un morphisme continu $\chi : G \to \mathbf{C}^\times$, l'ensemble des caractères de G se note $\mathrm{X}(G)$. On appelle alors caractère unitaire tout morphisme continu $\chi : G \to \mathbb{S}^1$. De nouveau, pour la multiplication point par point, le dual de Pontryagin $\widehat{G} = \mathrm{Hom}_c(G, \mathbb{S}^1)$ forme un groupe abélien localement compact (pour la topologie de la convergence compacte [2], i.e. celle engendrée par l'ensemble des applications continues qui envoient les compacts dans des ouverts) [3]. On a les identifications suivantes : $\widehat{\mathbf{Z}^n} \cong \mathbb{T}^n$, $\widehat{\mathbb{T}^n} \cong \mathbf{Z}^n$, $\widehat{\mathbf{R}^n} = \mathbf{R}^n$.

Dans quelques sections nous aurons tous les outils nécessaires pour pouvoir faire de l'analyse de Fourier sur un groupe abélien localement compact.

1. On obtient donc un isomorphisme $\widehat{G} \cong G$. Néanmoins, comme pour les espaces vectoriels de dimension finis, cet isomorphisme n'est pas naturel (en le sens qu'un choix arbitraire doit être fait lors de sa construction). En revanche, il existe un isomorphisme naturel entre G et son bidual : le morphisme d'évaluation en un élément de G. Ceci est un cas particulier de la dualité de Pontryagin.
2. Revenir sur ça !
3. Le *c* en indice signifie que l'on ne prend que les morphismes continus.

6. Motivations analytiques

Riemann a montré en 1860 que la fonction $\zeta(s)$ se prolongeait en une fonction méromorphe sur $\mathbf{C}$, holomorphe sur $\mathbf{C}$ excepté en le pôle simple $s = 1$ et qu'elle vérifiait l'équation fonctionnelle suivante : $\xi(s) = \xi(1-s)$ où $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Des constructions similaires sont possibles pour des fonctions L plus générales. L'apport de Tate semble constituer en une démonstration d'un genre nouveau. Avant d'y parvenir il va nous falloir démontrer une série de résultats relativement classiques.

Définition 3. *On appelle fonction* $\Gamma : \Omega \subset \mathbf{C} \to \mathbf{C}$ *la fonction suivante :*

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{\mathrm{d}t}{t}$$

où $\Omega = \{z \in \mathbf{C}, \mathrm{Re}(z) > 0\}$.

Une intégration par partie nous donne une propriété fondamentale de la fonction Γ, à savoir $\Gamma(s+1) = s\Gamma(s)$. Lorsque n est un entier, on trouve par une récurrence immédiate que $\Gamma(n+1) = n!$. Par holomorphie sous le signe intégral, on en déduit l'holomorphie de Γ sur Ω. On peut même prolonger méromorphiquement Γ à $\mathbf{C}$ tout entier privé de $0, -1, -2, \dots$.

À toute fin utile, on donne deux caractérisations de la fonction Γ.

Théorème 4 (Wielandt)**.** *La fonction* $\Gamma : \Omega \to \mathbf{C}$ *est l'unique fonction holomorphe vérifiant simultanément les trois propriétés suivantes :*
- $\Gamma(1) = 1$,
- $\Gamma(s+1) = s\Gamma(s)$,
- Γ *est bornée dans la bande* $1 \leq \mathrm{Re}(s) \leq 2$.

Théorème 5 (Bohr-Mollerup)**.** *La fonction* $\Gamma : \mathbf{R}_+^* \to \mathbf{R}_+^*$ *est l'unique fonction vérifiant simultanément les trois propriétés suivantes :*
- $\Gamma(1) = 1$,
- $\Gamma(x+1) = x\Gamma(x)$,
- Γ *est logarithmiquement convexe, i.e.* $\ln\Gamma$ *est convexe.*

7. Intégration sur un espace topologique localement compact X

Rappelons que la convention française considère que localement compact implique séparé (le monde anglo-saxon écrit donc *locally compact Hausdorff space*). On appelle $\mathscr{B}(X)$ l'ensemble des boréliens de X la σ-algèbre engendrée par les ouverts de X. Une mesure de Borel est une mesure sur l'espace mesurable $(X, \mathscr{B}(X))$.

Définition 6. *Une mesure extérieure de Radon sur* X *est une mesure de Borel* $\mu : \mathscr{B}(X) \to [0, \infty]$ *étant en outre :*
- *localement finie : pour tout point* $x \in X$*, il existe un voisinage ouvert* U *tel que* $\mu(U) < \infty$.
- *extérieurement régulière : tout borélien* $B \in \mathscr{B}(X)$ *vérifie* $\mu(S) = \inf_{S \subset U \text{ ouvert}} \mu(U)$,
- *intérieurement régulière sur les ouverts : tout ouvert* $U \subseteq X$ *vérifie* $\mu(U) = \sup_{K \text{ compact} \subseteq U} \mu(K)$.

Remarquons que Briane & Pagès appellent mesure de Radon ce que sera pour nous un cas particulier d'intégrale de Radon.

Définition 7. *Une intégrale de Radon sur* X *est une forme linéaire* $I : \mathcal{C}_c(X) \to \mathbf{C}$*, où* $\mathcal{C}_c(X)$ *désigne l'ensemble des fonctions continues à support compact, telle que* $I(f) \geq 0$ *lorsque* $f \geq 0$*. Pour toute mesure de Radon extérieure, on peut construire une intégrale de Radon associée* $I_\mu : \mathcal{C}_c(X) \to \mathbf{C}$ *définie par :*

$$I_\mu : f \mapsto \int_X f \mathrm{d}\mu.$$

Grâce à une généralisation aux espaces localement compacts du théorème de représentation de Riesz que l'on connaît, on a une identification entre intégrales de Radon sur X et mesures de Radon extérieures sur X.

8. Mesure de Haar

s

ANNEXE A. **DIRICHLET**

Le chapitre VI, *Théorème de progression arithmétique* dans le *Cours d'arithmétique* de J.-P. Serre, a pour objectif de démontrer le théorème de Dirichlet.

Théorème 8 (Dirichlet)**.** *Soient a et m deux entiers plus grands ou égaux à 1 et premiers entre eux. Il existe alors une infinité de nombres premiers p tels que $p \equiv a \mod m$.*

A.1. **Retour rapide sur les caractères.** On revient au formalisme des caractères introduit précédemment pour pouvoir définir et étudier une classe de fonctions L. Les propriétés de ces fonctions seront cruciales pour démontrer le théorème de la progression arithmétique de Dirichlet. Remarquons que Serre considère directement qu'un caractère est un morphisme de G dans $\mathbf{C}^\times$ et non restreint au cercle unité. On marque à la culotte (**de très près**) le texte de Serre en soulignant lorsqu'il peut exister des conflits avec nos notations ou bien ce que l'on a précédemment introduit. Notons qu'il conviendra de déployer un certain effort sur nombre de résultats dont la preuve est éludée par Serre. Attention, ce document est incomplet.

On note $\mathbb{P}$ l'ensemble des nombres premiers. Fixons un groupe abélien fini G d'ordre n et notons $\widehat{G} = \mathrm{Hom}(G, \mathbf{C}^\times)$ son dual. Supposons ici que G est engendré par un seul élément ζ, i.e. cyclique (hors sujet : tout groupe cyclique est abélien). Soit χ un caractère de G, notons $\omega = \chi(\zeta)$. On a $\omega^n = \chi(\zeta)^n = \chi(\zeta^n) = \chi(1) = 1$ puisque χ est un morphisme de groupes. Réciproquement, soit ω une racine de l'unité, en associant $\{1 \mapsto 1, \zeta \mapsto \omega, \zeta^2 \mapsto \omega^2, \dots, \zeta^{n-1} \mapsto \omega^{n-1}\}$ on définit un caractère. En effet, on vérifie immédiatement que l'on dispose d'un morphisme de G dans $\mathbf{C}^\times$. En conclusion, il existe un isomorphisme entre $\widehat{G}$ et $\mu_n \cong \mathbf{Z}/n\mathbf{Z}$ le groupe des racines de l'unité. En particulier, le groupe $\widehat{G}$ est cyclique d'ordre n.

Revenons à un groupe abélien fini quelconque. On dispose d'un théorème de relèvement des caractères, une sorte d'analogue de Hahn-Banach.

Proposition 9. *Soit H un sous-groupe de G. Tout caractère de H se prolonge en un caractère de G.*

Démonstration. On procède par récurrence sur l'indice $[G : H]$ de H dans G. Si $[G : H] = 1$, alors H et G s'identifient (revenir à la définition ou bien utiliser Lagrange si cela enchante), il n'y a rien à faire et l'initialisation est alors vérifiée.

Autrement, soit $x \in G \setminus H$ et n le plus petit entier strictement supérieur à 1 tel que $x^n \in H$. Soit χ un caractère de H et posons $t = \chi(x^n) = \chi(x)^n$. Il existe alors $\omega \in \mathbf{C}^\times$ tel que $\omega^n = t$. Notons $H' = \langle H, x\rangle$ le sous-groupe engendré. Tout élément h' de H' s'écrit alors sous la forme $h' = hx^a$ pour $h \in H$ et $a \in \mathbf{Z}$. Posons $\chi'(h') = \chi(h)\omega^a$. Ce complexe ne dépend pas de la décomposition de h' et $\chi' : H' \to \mathbf{C}^\times$ est un caractère de H' prolongeant χ. Par hypothèse de récurrence, puisque $[G : H'] < [G : H]$, on peut prolonger χ' en un caractère de G. □

Pour une présentation différente de la preuve, on peut se reporter au *blurb* de K. Conrad, thm. 3.2 et 3.3. Cette proposition permet de voir venir l'exactitude du foncteur contravariant dual de Pontryagin (thm. 3.8 de Poonen, mais il y a encore du travail). En effet, en conservant les notations de la proposition précédente, le morphisme de restriction $r : \widehat{G} \to \widehat{H}$ est surjectif. De plus, $\ker r$ est égal à l'ensemble des caractères de G triviaux sur H, à savoir le dual de G/H. On a donc la suite exacte suivante :

$$1 \to \widehat{\ker r} \to \widehat{G} \to \widehat{\mathrm{Im}\, r} \to 1.$$

On a plus précisément :

$$1 \to \widehat{G/H} \to \widehat{G} \to \widehat{H} \to 1.$$

On rappelle quelques résultats précédemment prouvés (ou bien dont la démonstration a déjà été esquissée).

Proposition 10. *Le dual de $\widehat{G}$ est un groupe abélien fini de même ordre que G. L'isomorphisme n'est pas canonique. En revanche, G est canoniquement isomorphe à son bidual.*

A.2. **Caractères modulaires.** Soit m un entier supérieur ou égal à 1. Notons $(\mathbf{Z}/m\mathbf{Z})^\times$ le groupe multiplicatif des inversibles de l'anneau $\mathbf{Z}/m\mathbf{Z}$. C'est un groupe abélien de cardinal $\phi(m)$, où ϕ est l'indicatrice d'Euler. On appelle caractère modulo m un élément du dual de $(\mathbf{Z}/m\mathbf{Z})^\times$. Quitte à poser $\chi(a) = 0$ pour a non premier avec m, ces caractères peuvent s'étendre à des fonctions de $\mathbf{Z}$ dans $\mathbf{C}^\times$.

Soit p un nombre premier différent de 2 et soit x un élément de $\mathbf{F}_p^*$. Le symbole de Legendre de x, noté $\left(\dfrac{x}{p}\right)$, est l'entier $x^{(p-1)/2} \in \{-1, 1\}$. On prend la convention que le symbole de Legendre de 0 est 0. Ce symbole est un caractère, il suffit de montrer que c'est un morphisme de groupe. En effet, automatiquement, on a pour x et y dans $\mathbf{F}_p$:

$$\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right).$$

À simple titre informatif, on donne un résultat sur les caractères d'ordre 2. Pour une application de ce résultat, cf. § 4.4 proposition 14 sur la densité des nombres premiers p tels que $\left(\dfrac{a}{p}\right) = 1$ pour a non carré.

Proposition 11. *Soit a un entier non nul sans facteur carré et posons $m = 4|a|$. Alors, il existe un unique caractère χ_a modulo m tel que $\chi_a(p) = \left(\dfrac{a}{p}\right)$ pour tout nombre premier p ne divisant pas m. On a de plus, $\chi_a^2 = 1$ et $\chi_a \neq 1$ si $a \neq 1$.*

A.3. **Séries de Dirichlet.** Soit $(\lambda_n)_n$ une suite croissante de nombres réels tendant vers $+\infty$. Limitons nous ici au cas où les λ_n sont tous positifs. Une série de Dirichlet est de la forme suivante $\sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ avec $a_n \in \mathbf{C}, s \in \mathbf{C}$. La série de Dirichlet associée à $a_n = 1$ et $\lambda_n = \ln n$, pour tout n, correspond à la fonction zêta de Riemann. Lorsque seulement $\lambda_n = \ln n$, on parle de série de Dirichlet ordinaire. Nous verrons ensuite comment la rencontre des caractères et des séries de Dirichlet nous permettent de considérer un objet d'une importance première pour démontrer le théorème de Dirichlet, à savoir les fonctions L.

On se limite ici aux résultats énoncés par Serre, pour quelques développement supplémentaires, on pourra consulter les *Éléments d'analyse, d'algèbre (et de théorie des nombres)* de Colmez. Montrons quelques résultats d'analyse sur les séries de Dirichlet.

Proposition 12. *Si la série $f(s) = \sum a_n e^{-\lambda_n s}$ converge en $s = s_0$, alors on a convergence uniforme sur tout domaine de la forme* $\mathrm{Re}(s - s_0) \geq 0$ *et* $\mathrm{Arg}(s - s_0) \leq \alpha$ *pour* $\alpha < \pi/2$.

Pour prouver ce résultat, nous avons besoin des deux lemmes suivants.

Lemme 13 (Transformation d'Abel). *Soient (a_n) et (b_n) deux suites complexes. Pour tous $N \in \mathbf{Z}$ et $M \in \mathbf{N}^*$, on a :*

$$\sum_{N<n\leq N+M} a_n b_n = A_{N,N+M} b_{N+M+1} + \sum_{N<n\leq N+M} A_{N,n}(b_n - b_{n+1})$$

où l'on a posé $A_{N,n} = \sum_{N<m\leq n} a_m$ pour $n \geq 0$.

L'énoncé provient du Tenenbaum et la preuve est un calcul direct.

Lemme 14. *Soient α et β deux nombres réels tels que $0 < \alpha < \beta$. Soit $s = x + iy$ avec x et y réels et $x > 0$. Alors, on a l'inégalité suivante :*

$$\left|e^{-\alpha s} - e^{-\beta s}\right| \leq \left|\frac{s}{x}\right| \left(e^{-\alpha x} - e^{-\beta x}\right).$$

Démonstration. Il suffit de remarquer l'identité suivante :

$$e^{-\alpha s} - e^{-\beta s} = s \int_\alpha^\beta e^{-ts} \mathrm{d}t.$$

De laquelle il vient :

$$\left|e^{-\alpha s} - e^{-\beta s}\right| \leq |s| \int_\alpha^\beta |e^{-ts}| \mathrm{d}t = |s| \int_\alpha^\beta |e^{-tx}| \mathrm{d}t = \left|\frac{s}{x}\right| \left(e^{-\alpha x} - e^{-\beta x}\right).$$

□

On peut donc en revenir à la preuve de la proposition.

Démonstration. Quitte à opérer un changement de variable et à modifier les coefficients sans perte de généralité, on se ramène au cas $s_0 = 0$. En effet, on a l'égalité formelle suivante :

$$f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s} = \sum_{n=1}^{\infty} \left(a_n e^{-\lambda_n s_0}\right) e^{-\lambda_n (s-s_0)}.$$

Prouvons que la convergence est uniforme sur tout domaine de la forme $\mathrm{Re}(s) \geq 0$, $\mathrm{Arg}(s) \leq \alpha < \pi/2$. On a donc convergence de la série $f(0) = \sum a_n$. Soit $\varepsilon > 0$. Par le critère de Cauchy uniforme, il existe alors $N_0 := N_0(\varepsilon)$ entier tel que, pour tout $N_2, N_1 > N_0$ avec $N_2 > N_1$, on ait :

$$\left| \sum_{n=N_1}^{N_2} a_n \right| \leq \varepsilon \frac{\cos(\alpha)}{2}$$

On conclut en appliquant le théorème 4.5 de chez Bordellès, qu'il faut convenablement modifier (à faire). $\square$

Noter que Colmez propose une preuve pour un cas particulier dans ses éléments (cela revient au même).
Par application immédiate et comme il y a convergence uniforme sur tout compact, on en déduit ceci.

Corollaire 15. *Si f converge en $s = s_0$, alors f converge pour $\mathrm{Re}(s) > \mathrm{Re}(s_0)$. La fonction f y est holomorphe.*

Lorsque les coefficients d'une série de Dirichlet sont tous réels positifs ou nuls, on obtient des propriétés de convergence plus fines. En particulier si les coefficients sont tous bornés par exemple (cf ci-dessous).

A.4. **Fonctions zêta et L.** On dit qu'une fonction $f : \mathbf{N} \to \mathbf{C}$ est multiplicative si $f(1) = 1$ et $f(mn) = f(m)f(n)$ pour n et m des entiers premiers entre eux. Soit f une fonction multiplicative bornée.

Lemme 16. *La série de Dirichlet $\sum_{n=1}^{\infty} f(n)/n^s$ converge absolument pour $\mathrm{Re}(s) > 1$ et sa somme sur ce domaine est égale à :*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 + f(p)p^{-s} + \cdots + f(p^m)p^{-ms} + \dots\right).$$

Démonstration. Puisque f est borné par C disons, la convergence absolue est une conséquence immédiate. En effet :

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{C}{n^s} = C\zeta(s) < \infty.$$

Pour redonner la raison, simplement penser à une comparaison série-intégrale ou rappeler le critère de Riemann (ce qui revient au même). De plus, on a, pour S un ensemble fini de nombres premiers et $N(S)$ l'ensemble des entiers supérieurs ou égaux à 1 tels que chacun de leurs facteurs premiers appartiennent à S :

$$\begin{aligned} \sum_{n \in N(S)} \frac{f(n)}{n^s} &= \sum_{0 \leq \alpha_1, \alpha_2, \dots, \alpha_r} \frac{f(p_1^{\alpha_1} \dots p_r^{\alpha_r})}{p_1^{\alpha_1 s} \dots p_r^{\alpha_r s}} = \sum_{0 \leq \alpha_1, \alpha_2, \dots, \alpha_r} \frac{f(p_1^{\alpha_1}) \dots f(p_r^{\alpha_r})}{p_1^{\alpha_1 s} \dots p_r^{\alpha_r s}} \\ &= \left(\sum_{\alpha_1=0}^{\infty} \frac{f(p_1^{\alpha_1})}{p_1^{\alpha_1 s}} \right) \dots \left(\sum_{\alpha_r=0}^{\infty} \frac{f(p_r^{\alpha_r})}{p_r^{\alpha_r s}} \right) = \prod_{p \in S} \left(\sum_{\alpha=0}^{\infty} \frac{f(p^\alpha)}{p^{\alpha s}} \right) \end{aligned}$$

où l'on a décomposé n sous la forme $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec les p_i des éléments de S. En faisant tendre S vers $\mathbb{P}$, on obtient le résultat désiré (en effet, $N(S)$ s'identifiera à $\mathbf{N}^*$). $\square$

Si f est une fonction complètement multiplicative, i.e. sans condition de primalité, on a l'identité suivante :

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_{p \in \mathbb{P}} \frac{1}{1 - f(p)/p^s}.$$

En effet, la complète multiplicativité donne $f(p^m) = f(p)^m$. Le lemme précédent permet alors de conclure :

$$\begin{aligned}\sum_{n=1}^{\infty} f(n)/n^s &= \prod_{p\in\mathbb{P}} \left(1 + f(p)p^{-s} + \dots + f(p^m)p^{-ms} + \dots\right) = \prod_{p\in\mathbb{P}} \left(1 + f(p)p^{-s} + \dots + f(p)^m p^{-ms} + \dots\right) \\ &= \prod_{p\in\mathbb{P}} \left(1 + f(p)p^{-s} + \dots + \left(f(p)p^{-s}\right)^m + \dots\right) = \prod_{p\in\mathbb{P}} \frac{1}{1 - f(p)p^{-s}}.\end{aligned}$$

On a effectivement $|f(p)p^{-s}| < 1$. Autrement, par l'absurde, on obtiendrait $|f(n)| \geq n^s$ par décomposition en facteurs premiers et ainsi toute série de Dirichlet ayant pour coefficients les valeurs prises par une fonction complètement multiplicative serait divergente. Ce qui est absurde.

En particulier, lorsque f est identiquement égale à la fonction 1, on obtient la factorisation bien connue de la fonction zêta de Riemann pour $\mathrm{Re}(s) > 1$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1 - p^{-s}}.$$

Proposition 17. *La fonction zêta est holomorphe et ne s'annule plan dans le demi-plan* $\mathrm{Re}(s) > 1$. *On a :*

$$\zeta(s) = \frac{1}{s-1} + \phi(s)$$

pour $\phi(s)$ *une fonction holomorphe lorsque* $\mathrm{Re}(s) > 0$.

Démonstration. L'holomorphie et la non-annulation

Ensuite, commençons par remarquer l'identité suivante :

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s}\mathrm{d}t = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s}\mathrm{d}t.$$

De cela, on en déduit que :

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s}\mathrm{d}t\right) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(n^{-s} - t^{-s}\right)\mathrm{d}t.$$

Définissions alors les quantités suivantes :

$$\phi_n(s) = \int_n^{n+1} \left(n^{-s} - t^{-s}\right)\mathrm{d}t \quad \text{et} \quad \phi(s) = \sum_{n=1}^{\infty} \phi_n(s).$$

On souhaite donc montrer que $\phi(s)$ est bien définie et holomorphe sur le demi-plan $\mathrm{Re}(s) > 0$. Par holomorphie sous le signe intégral, les fonctions $\phi_n(s)$ sont bien définies et holomorphes pour $\mathrm{Re}(s) > 0$. Pour conclure, il suffit donc de prouver que la série $\sum \phi_n(s)$ converge normalement sur tout compact du demi-plan $\mathrm{Re}(s) > 0$. Par construction, on a :

$$|\phi_n(s)| \leq \sup_{n\leq t\leq n+1} |n^{-s} - t^{-s}| \leq \frac{|s|}{n^{\mathrm{Re}(s)+1}}$$

en appliquant l'inégalité des accroissements finis à la fonction $t \mapsto t^{-s}$. Ceci montre finalement l'holomorphie de $\phi(s)$ lorsque $\mathrm{Re}(s) > 0$. □

De cela, on déduit que la fonction zêta n'a qu'un pôle simple en $s = 1$. En effet, en regardant droit dans les yeux l'expression obtenue pour ζ dans la proposition précédente, on conclut directement (puisque $\phi(s)$ est holomorphe).

On peut même être un petit peu quantitatif sur le comportement de $\zeta(s)$ lorsque s tend vers 1. (Et c'est d'ailleurs un exercice du Pollack & Singha Roy.) On a $\sum_p p^{-s} = O(\ln(1/(s-1)))$ et $\sum_{p,k\geq 2} 1/p^{ks}$ reste borné lorsque s tend vers 1.

Pour quelques propriétés supplémentaires, on se reportera à la section portant sur les motivations analytiques dans le corps du texte.

Soit $m \geq 1$ un entier et χ un caractère modulo m. À ce caractère, on associe une fonction L définie par la série de Dirichlet $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$. Rappelons que nous avons étendus χ à **Z**, de fait $\chi(n) = 0$ si n et m ne sont pas premiers entre eux.

Proposition 18. *Soit χ le caractère trivial, noté $\mathbf{1}$, on a :*

$$L(s,\mathbf{1}) = \zeta(s) \prod_{p|m} \left(1 - p^{-s}\right).$$

En particulier, $L(s,\mathbf{1})$ se prolonge analytiquement pour $\mathrm{Re}(s) > 0$ et a un pôle simple en $s = 1$.

Démonstration. Les propriétés d'analyticité et le pôle de cette fonction L sont directement conséquences de propriétés de la fonction zêta vues précédemment. On obtient une expression de $L(s,\mathbf{1})$ en revenant au produit eulérien de la fonction zêta et en se rappelant que les termes contribuant dans la somme $\sum 1/n^s$ sont ceux pour lesquels n est premier avec m. Alors :

$$L(s,\mathbf{1}) = \sum_{\substack{n=1 \\ (n,m)=1}}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1-p^{-s}} \prod_{p|m} (1-p^{-s}) = \zeta(s) \prod_{p|m} (1-p^{-s}).$$

□

Pour étudier la convergence de $L(s,\chi)$ lorsque χ n'est pas le caractère trivial, nous aurons besoin du lemme suivant.

Lemme 19. *Soit f une série de Dirichlet ordinaire de coefficients a_n. Si la somme $A_{N,n} = \sum_{l=N}^{n} a_l$ est bornée, on a convergence simple de la série de Dirichlet sur le demi-plan $\mathrm{Re}(s) > 0$.*

Démonstration. Supposons que $|A_{N,n}|$ est borné par une constante $C > 0$. En faisant une transformation d'Abel, on obtient :

$$\left| \sum_{N < l \leq N+N'} \frac{a_l}{l^s} \right| \leq C \left(\left| \frac{1}{(N+N'+1)^s} \right| + \sum_{N < l \leq N+N'} \left| \frac{1}{l^s} - \frac{1}{(l+1)^s} \right| \right).$$

Par inégalité triangulaire répétée, on monte alors que :

$$\left| \sum_{N < l \leq N+N'} \frac{a_l}{l^s} \right| \ll C/|N^s|.$$

Puisque $\mathrm{Re}(s) > 0$, cela conclut. □

Proposition 20. *Pour $\chi \neq \mathbf{1}$, la série $L(s,\chi)$ converge (resp. converge absolument) dans le demi-plan $\mathrm{Re}(s) > 0$ (resp. $\mathrm{Re}(s) > 1$) et l'on a :*

$$L(s,\chi) = \prod_{p \in \mathbb{P}} \frac{1}{1-\chi(p)p^{-s}} \quad \textit{pour } \mathrm{Re}(s) > 1.$$

Démonstration. Le cas $\mathrm{Re}(s) > 1$ a été précédemment traité (un caractère est complètement multiplicatif). Il reste donc à montrer la convergence de la série $L(s,\chi)$ dans le demi-plan $\mathrm{Re}(s) > 0$. Pour ce faire, il suffit de montrer que la quantité $A_{N,n} = \sum_{l=N}^{n} \chi(l)$ est bornée. On a précédemment vu que $\sum_{l=N}^{N+m-1} \chi(l) = 0$. Rappelons, si ça ne saute pas aux yeux, que χ est un caractère modulo m non trivial et que l'ordre de $\mathbf{Z}/m\mathbf{Z}$ est m (et qu'il faut bien compter le nombre d'indices dans la somme !). Il suffit donc de majorer la somme $A_{N,n}$ pour $n - N < m$, ce qui est direct : $|A_{N,n}| \leq \phi(m)$. Ceci conclut la démonstration de la proposition. □

On voit donc que $L(1,\chi)$ est fini lorsque χ n'est pas trivial. Un point crucial pour la démonstration du théorème de Dirichlet est la non-annulation de $L(1,\chi)$. Montrons le. Rappelons que l'on a fixé m un entier supérieur ou égal à 1

Théorème 21. *Soit $\zeta_m(s) = \prod_\chi L(s,\chi)$ pour χ parcourant l'ensemble des caractères de $(\mathbf{Z}/m\mathbf{Z})^\times$. Il est alors équivalent que la fonction zêta ζ_m ait un pôle simple en $s = 1$ et que $L(1,\chi) \neq 0$ pour $\chi \neq \mathbf{1}$.*

Démonstration. Supposons que $L(1,\chi) \neq 0$ pour tout $\chi \neq 1$. Comme $L(s, \mathbf{1})$ admet un pôle simple en $s = 1$, il en est de même pour $\zeta_m(s)$.

Supposons désormais que $L(1,\chi) = 0$ pour un χ non trivial. On aurait alors que ζ_m serait holomorphe en $s = 1$ et ainsi sur tout le demi-plan $\mathrm{Re}(s) > 0$. **@TODO FINISH** $\square$

A.5. **Densité et théorème de Dirichlet.** Lorsque $s \to 1$, on a[4] :

$$\sum_{p \in \mathbb{P}} \frac{1}{p^s} = O\left(\ln\left(\frac{1}{s-1}\right)\right).$$

Pour $A \subset \mathbb{P}$, définissons la densité de A comme étant la limite lorsque s tend vers 1 de :

$$\left(\sum_{p \in A} \frac{1}{p^s}\right) \Bigg/ \left(\ln\left(\frac{1}{s-1}\right)\right)$$

On peut alors reformuler le théorème de Dirichlet sur les progressions arithmétiques comme suit.

Théorème 22. *Soient a et m deux entiers plus grands ou égaux que 1 et premiers entre eux. Notons $P_{a,m}$ l'ensemble des nombres premiers tels que $p \equiv a \mod m$. L'ensemble $P_{a,m}$ a pour densité $1/\phi(m)$.*

Puisqu'un ensemble fini est de densité nulle (il suffit de regarder dans le blanc des yeux le quotient ci-dessus), par contraposition, on en déduit le théorème de Dirichlet.

Corollaire 23. *L'ensemble $P_{a,m}$ est infini.*

Il nous faut donc désormais prouver que la densité de $P_{a,m}$ est $1/\phi(m)$. Soit χ un caractère de $(\mathbf{Z}/m\mathbf{Z})^\times$. Introduisons $f_\chi(s) = \sum_{p \nmid m} \chi(p)/p^s$, $g_a(s) = \sum_{p \in P_{a,m}} 1/p^s$.

La stratégie est la suivante : montrer que pour $\chi = \mathbf{1}$, on a $f_\chi(s) = O\left(\ln\left(\frac{1}{s-1}\right)\right)$ lorsque s tend vers 1 et pour χ non trivial, on a $f_\chi(s)$ borné lorsque s tend vers 1. Ensuite, en montrant la relation $g_a(s) = 1/\phi(m) \sum_\chi \chi(a)^{-1} f_\chi(s)$, comme la somme porte sur tous les caractères, on obtiendra immédiatement que $g_a(s) = O\left(1/\phi(m) \ln\left(\frac{1}{s-1}\right)\right)$. En effet, on a une partie bornée et une autre contrôlée lorsque s tend vers 1. Ceci nous assurera donc que la densité de $P_{a,m}$ est de $1/\phi(m)$.

Lemme 24. *Lorsque l'on prend la somme sur tous les caractères χ de $(\mathbf{Z}/m\mathbf{Z})^\times$, on a :*

$$g_a(s) = \frac{1}{\phi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s).$$

Démonstration. Par un calcul direct, on obtient :

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_\chi \chi(a)^{-1} \left(\sum_{p \nmid m} \chi(p)/p^s\right) = \sum_{p \nmid m} \left(\sum_\chi \chi(a)^{-1}\chi(p)\right) /p^{-s} = \sum_{p \nmid m} \left(\sum_\chi \chi(a^{-1}p)\right) /p^{-s}.$$

Or, $\sum_\chi \chi(a^{-1}p)$ est égal à $\phi(m)$ si $a^{-1}p \equiv 1 \mod m$, i.e. $p \equiv a \mod m$ et 0 autrement. Donc :

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \phi(m) g_a(s).$$

Ce qui conclut la preuve du lemme. $\square$

Pour être tout à fait rigoureux, il faudrait bien montrer que $g_a(s) = O\left(1/\phi(m) \ln\left(\frac{1}{s-1}\right)\right)$.

Le théorème de Dirichlet est finalement démontré. Pour une preuve plus analytique, voir sans doute le chapitre 9, *Complex Analysis with applications to Number Theory* de Tarlok Nath Shorey.

4. L'exercice 3.24 du Pollack & Singha Roy nous mettait déjà sur cette voie.

ANNEXE B. **BOMBIERI-VINOGRADOV**

On suit l'article de R.C. Vaughan, *The Bombieri-Vinogradov theorem*. L'objectif est de comprendre la démonstration du théorème éponyme. Ce théorème quantifie l'erreur commise UTILISER LE DOCUMENT DE KEDLAYA PLUTÔT ? ? ?

Théorème 25 (Bombieri-Vinogradov)**.** *Soit A constante positive, on a uniformément pour $Q \geq 1$, $x \geq 1$:*

$$\sum_{q \leq Q} \max_{(a,q)=1} \sup_{y \leq x} \left| \psi(y; a, q) - \frac{y}{\varphi(q)} \right| \ll_A \frac{x}{(\ln x)^A} + x^{1/2} (\ln(Qx))^4 .$$

On suit la preuve donnée par Newman et présentée par Zagier dans son article *Newman's short proof of the Prime Number Theorem*. Lorsque Zagier n'est pas clair, on se réfère à Hindry. On n'hésite pas à capitaliser sur des résultats déjà rencontrés précédemment (tout particulièrement dans la partie sur le théorème Dirichlet sur les progressions arithmétiques). Un nombre complexe sera noté $s = \sigma + it$.

Soit $\pi(x)$ la fonction de compte des nombres premiers. On montre le théorème des nombres premiers (abrégé en TNP) avec et sans terme d'erreur.

Théorème 26 (TNP)**.** *On a la relation asymptotique suivante :*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

On donnera plus tard une meilleure estimation.

Introduisons les fonctions $\Phi(s) = \sum_p \ln(p)/p^s$ et $\vartheta(x) = \sum_{p\leq x} \ln(p)$ pour s complexe et x réel. La fonction $\Phi(s) - 1/(s-1)$ est holomorphe pour $\mathrm{Re}(s) \geq 1$. On rappelle quelques propriétés de la fonction zêta de Riemann $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ pour $s = \sigma + it$ avec $\sigma > 1$. On en connaît l'holomorphie et le produit eulérien $\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}$ sur le demi-plan $\sigma > 1$. on a automatiquement la non annulation de la fonction $\zeta(s)$ pour $\sigma > 1$. Le cas $\sigma = 1$ est fondamental.

Proposition 27. *La fonction zêta ne s'annule pas en $s = 1$.*

Démonstration. Soit $\sigma > 1$. Commençons par considérer l'inégalité suivante :

$$0 \leq 2(1+\cos(t))^2 = 3 + 4\cos(t) + \cos(2t).$$

On obtient donc :

$$\begin{aligned}\ln\left(\zeta(\sigma)^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)|\right) &= 3\ln\zeta(\sigma) + 4\ln|\zeta(\sigma+it)| + \ln|\zeta(\sigma+2it)| \\ &= \sum_{p,m} \frac{1}{mp^{m\sigma}}\left(3 + 4\cos(mt\ln p) + \cos(2mt\ln p)\right) \geq 0.\end{aligned}$$

Ceci est équivalent, en prenant l'exponentielle, à :

$$\zeta(\sigma)^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)| \geq 1.$$

Le théorème de Mertens (Tenenbaum, 3.11) généralise cette situation au cas des séries de Dirichlet à coefficients positifs ou nuls. Enfin, notons l_1 (resp. l_2) l'ordre du zéro de $\zeta(s)$ en $s = \sigma + it$ (resp. $\sigma + 2it$) et faisons tendre σ vers 1 supérieurement. Alors $|\zeta(\sigma)|^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)|$ se comporte comme $\alpha(\sigma-1)^{-3+4l_1+l_2}$, $\alpha > 0$. Ceci implique que $-3 + 4l_1 + l_2 \leq 0$ ce qui n'est possible que si $l_1 = 0$. $\square$

Le théorème ci-dessous ramène la preuve du TNP à la convergence d'intégrales (transformées de Laplace) bien choisies.

Théorème 28 (Analytique)**.** *Soit $t \geq 0$ et $f(t)$ une fonction bornée, localement intégrable et supposons que $g(s) = \int_0^\infty f(t)e^{-st}\mathrm{d}t$ définie pour* $\mathrm{Re}(s) > 0$ *se prolonge holomorphiquement sur* $\mathrm{Re}(s) \geq 0$. *Alors $\int_0^\infty f(t)\mathrm{d}t$ existe et est égale à $g(0)$.*

Pour la démonstration du TNP, on peut affaiblir les hypothèses nécessaires sur f en la demandant seulement bornée et continue par morceau.

Démonstration. Pour T réel, il est clair que $g_T(s) = \int_0^T f(t)e^{-st}\mathrm{d}t$ est holomorphe pour $s \in \mathbf{C}$. Montrons que $g_T(0)$ tend vers $g(0)$ lorsque T tend vers l'infini. Soit $\delta > 0$, considérons le contour $\gamma(R,\delta) = \partial\{s \in \mathbf{C} \mid \mathrm{Re}(s) \geq -\delta,\ |s| \leq R\}$. Comme l'écrit Hindry, *the trick lies in introducing the function :*

$$G_T(s) = (g(s) - g_T(s))\, e^{sT}\left(1 + \frac{s^2}{R^2}\right).$$

Remarquons que $G_T(0) = g(0) - g_T(0)$. Le théorème des résidus nous donne :

$$G_T(0) = \frac{1}{2i\pi} \int_{\gamma(R,\delta)} (g(s) - g_T(s))\, e^{sT} \left(1 + \frac{s^2}{R^2}\right) \frac{\mathrm{d}s}{s}.$$

De manière générale, on a : en considérant le pire cas possible, i.e. $|s| = R$, i.e. $S = Re^{i\theta}$:

$$\left| e^{sT} \left(1 + \frac{s^2}{R^2}\right) \frac{1}{s} \right| = 2e^{\sigma T} \sigma / R^2.$$

$$|g(s) - g_T(s)| = \left| \int_T^\infty f(t) e^{-st} \mathrm{d}t \right| \leq \max |f(t)| \int_T^\infty |e^{-st}| \mathrm{d}t = \max |f(t)| \frac{e^{-\sigma T}}{\sigma}$$

pour $\sigma > 0$. Subdivisons le contour $\gamma(R, \delta)$ en deux parties γ_1 pour la partie dans le demi plan $\mathrm{Re}(s) > 0$ et γ_2 celle dans le demi plan $\mathrm{Re}(s) < 0$. Ainsi :

$$\begin{aligned} \left| \frac{1}{2i\pi} \int_{\gamma_1} (g(s) - g_T(s))\, e^{sT} \left(1 + \frac{s^2}{R^2}\right) \frac{\mathrm{d}s}{s} \right| &\leq \frac{1}{2i\pi} \int_{\gamma_1} \max |f(t)| \frac{e^{-\mathrm{Re}(s)T}}{\mathrm{Re}(s)} 2e^{\mathrm{Re}(s)T} \mathrm{Re}(s)/R^2 \mathrm{d}s \\ &\leq \frac{\max |f(t)|}{i\pi R^2} \int_{\gamma_1} \mathrm{d}s \\ &\leq \alpha / R \end{aligned}$$

avec α une constante positive non nulle. En prenant R suffisamment grand, l'intégrale sur γ_1 peut être donc rendue arbitrairement petite. Pour contrôler l'intégrale sur γ_2, on découpe l'intégrale en deux parties par linéarité de la somme. Pour l'une on revient à la définition de la convergence (rq. $g(s)e^{st}(1 + s^2/R^2)/s$ tend vers 0 lorsque T tend vers l'infini, rappelons que $\mathrm{Re}(s) < 0$). Pour l'autre partie, on effectue le même raisonnement que pour γ_1. Mis bout à bout, ceci permet de conclure que $|g(0) - g_T(0)|$ tend vers 0 lorsque T tend vers l'infini. □

Proposition 29. *L'intégrale* $\int_1^\infty (\vartheta(x) - x)/x^2 \mathrm{d}x$ *est convergente.*

Démonstration. Introduisons la fonction $F(s)$:

$$g(s) = \int_1^\infty \frac{\vartheta(x) - x}{x^{s+2}} \mathrm{d}x = \int_0^\infty \frac{\vartheta(e^t) - e^t}{e^{t(s+2)}} e^t \mathrm{d}t = \int_0^\infty \left(\theta(e^t) e^{-t} - 1\right) e^{-ts} \mathrm{d}t.$$

On peut alors appliquer le théorème analytique puisque la fonction $f(t) = \theta(e^t)e^{-t} - 1$ est bornée et continue par morceau. Ainsi, $g(0)$ est convergente et égale à l'intégrale dont nous cherchions à déterminer la nature. □

Proposition 30. *On a* $\vartheta(x) = O(x)$*, i.e.* $\vartheta(x)$ *est borné par un multiple de* x*.* [5]

Démonstration. Soit n un entier. Remarquons les majorations suivantes :

$$2^{2n} = (1+1)^{2n} = \binom{2n}{0} + \dots \binom{2n}{2n} \geq \binom{2n}{n} = \frac{(2n)!}{n!n!} \geq \prod_{n<p\leq 2n} p = \exp\left(\sum_{n<p\leq 2n} \ln(p)\right) = \exp\left(\vartheta(2n) - \vartheta(n)\right).$$

En somme, on a obtenu $\vartheta(2n) - \vartheta(n) \leq n \ln 4$. Cette inégalité est plus généralement vrai pour x réel supérieur ou égal à 2. En effet, $\vartheta(\lfloor 2n \rfloor) - \vartheta(\lfloor n \rfloor) = \vartheta(2n) - \vartheta(n)$ et $\lfloor x \rfloor \leq x$ pour x positif. Remarquons alors que l'on a :

$$\begin{aligned} \vartheta(x) &= \vartheta(x) - \vartheta(x/2) + \vartheta(x/2) - \vartheta(x/4) + \vartheta(x/4) + \dots \\ &\leq \left(x + x/2 + x/2^2 \dots\right) \ln 4 = 2x \ln 4. \end{aligned}$$

Ceci conclut. □

Proposition 31. *Plus précisément, on a* $\vartheta(x) \sim x$*, i.e.* $\vartheta(x)/x$ *tend vers* 1.

5. Attention aux notations.

Démonstration. Par l'absurde, soit $\lambda > 1$, supposons qu'il existe un x suffisamment grand tel que $\vartheta(x) \geq \lambda x$. Par croissance de ϑ, on a :

$$\int_x^{\lambda x} \frac{\vartheta(t) - t}{t^2} \mathrm{d}t \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2} \mathrm{d}t = \int_1^{\lambda} \frac{\lambda - u}{u^2} \mathrm{d}u > 0.$$

Ceci contredit la convergence de l'intégrale $\int_1^\infty (\vartheta(x) - x)/x^2 \mathrm{d}x$. On raisonne identiquement pour $\lambda < 1$ et en supposant que $\vartheta(x) \leq \lambda x$. Donc $\lambda = 1$,[6] ce qui conclut. □

De là, on en déduit le théorème des nombres premiers. En effet, on a :

$$\vartheta(x) = \sum_{p \leq x} \ln p \leq \sum_{p \leq x} \ln x = \pi(x) \ln(x).$$

De plus, pour tout $\varepsilon > 0$:

$$\vartheta(x) \geq \sum_{x^{1-\varepsilon} \leq p \leq x} \ln p \geq \sum_{x^{1-\varepsilon} \leq p \leq x} \ln\left(x^{1-\varepsilon}\right) = (1 - \varepsilon) \sum_{x^{1-\varepsilon} \leq p \leq x} \ln x \geq (1 - \varepsilon) \ln(x) \left[\pi(x) + O\left(x^{1-\varepsilon}\right)\right].$$

Donc $\pi(x)/(x/\ln x)$ tend vers 1 lorsque x tend vers l'infini (puisque $\vartheta(x) \sim x$). Cette preuve manque de naturel, il conviendrait donc d'en chercher (au moins) une autre. Plus, j'ai l'impression de louper quelque chose... voir Garrett.

6. Mieux rédiger ça. C'est étrange écrit comme ça.