Théorème de Dirichlet (nombres premiers dans les progressions arithmétiques)

Johan Dorian Koschall

Juillet 2025

Table des matières

Préface

Soit $0 < a \leq b$ deux entiers premiers entre eux. Il existe une infinité de nombres premiers dans la progression arithmétique de premier terme a et de raison b

*

C'est cette assertion portant sur les nombres premiers que nous cherchons à démontrer dans le présent document. Elle se lit bien, se comprend, et pourtant le lecteur sera sans doute bien surpris d'apprendre que, ici, la majorité des théorèmes, de leurs corollaires et de leurs démonstrations, ne portent pas sur les nombres entiers. En fait, il n'y aura que de très légères traces d'arithmétique dans tout ce qui sera fait.

Dans un premier temps, on voit bien que si a et b ne sont pas premiers entre eux, il y a au plus un nombre premier dans la progression arithmétique considérée. Un réflexe naturel est alors de tenter de démontrer cette assertion pour quelques cas particuliers, puis de trouver un schéma qui se répète, avant de le généraliser et d'en faire une preuve qui fera de cette assertion un théorème. Cependant, il est dur, très dur même, de trouver une telle preuve, dite « élémentaire », c'est-à-dire qui ne fait appel qu'à l'arithmétique. En 1949 le mathématicien norvégien Atle Selberg donne une telle preuve, utilisant ce qui sera nommé *« the theory of arithmetic linear transformations »* (eng), dont le cadre dépasse de loin celui qui est fixé dans ce document, à savoir le programme de licence en mathématiques.

La question de l'existence de preuves élémentaires des résultats les plus importants de la théorie des nombres se posait déjà au siècle dernier. Par exemple en 1896 Jean Jacques Hadamard et Charles-Jean de La Vallée Poussin démontrent le théorème des nombres premiers en utilisant des méthodes d'analyse complexe. À cette époque l'on chercha encore une démonstration élémentaire mais sans succès, ce qui conduira le grand mathématicien Godfrey Harold Hardy à déclarer : *« No elementary proof of the prime number theorem is known, and one may ask whether it is reasonable to expect one. [...] If anyone produces an elementary proof of the prime number theorem [...] it is time for the books to be cast aside and for the theory to be rewritten. »* (eng), traduisant l'idée que l'analyse complexe était pensée comme plus « profonde » que l'analyse réelle, et qu'elle devait être un outil (ou l'outil ?) privilégié en théorie des nombres. Mais en 1949 les mathématiciens Paul Erdős et Atle Selberg démontreront ce théorème de façon élémentaire, remettant en cause les considérations de l'époque.

On définit ici l'ensemble $\mathcal{P}_{a,b}$ des nombres premiers congrus à a modulo b. De plus, on appelle « Problème de Dirichlet » la question : « existe-t-il une infinité de nombres premiers congrus à a modulo b ? ». Au cours de l'histoire, de nombreux problèmes de Dirichlet ont été résolus, à commencer par Euclide et sa résolution (évidemment simultanée) des cas $(a, b) = (1, 1)$ et $(a, b) = (1, 2)$. Il est possible par ailleurs de résoudre de nombreux cas particuliers via des preuves similaires à celles d'Euclide, des preuves dites « euclidiennes », avec par exemple les cas $(a, b) = (2, 3)$, ou $(a, b) = (3, 8)$. En fait, un théorème dû à Schur en 1912 nous dit que si $a^2 \equiv 1 \mod b$, alors il existe une telle preuve euclidienne pour le cas (a, b). La réciproque a été démontrée(voir **[3]**) en 1988 par Murty, montrant alors que le monde des cas où il existe une preuve euclidienne est très restreint.

Dans ce document, nous explorerons dans un premier temps deux cas particuliers pour nous échauffer avec des preuves faisant usage de l'arithmétique. Par la suite, nous ferons un pas de plus dans les preuves arithmétiques en résolvant les cas $(a, b) = (1, n)$ où n est un entier plus grand que 1 (dit théorème faible de Dirichlet). Enfin nous démontrerons le théorème de la progression arithmétique non sans quelques prérequis, puis dans une ouverture en décrirons quelques conséquences et parlerons de quelques autres problèmes bien connus liés à celui-ci.

Partie 1

Cas élémentaires du problème de Dirichlet

Les epsilon deviennent des esclaves quand ils se mettent à courir après les patrons !

Paul Erdös

On se propose dans un premier temps de résoudre le problème de Dirichlet pour quelques cas, ce qui permet de faire le tour de quelques démonstrations élémentaires, c'est-à-dire, qui pour résoudre un problème sur les nombres entiers, font appel aux nombres entiers.

Le cas $4k+3$

Il y a un peu moins de quatre siècles, vers 1630, le mathématicien français Pierre de Fermat définit la suite de nombres $(F_n)_{n\in\mathbb{N}} = (2^{2^n}+1)_{n\in\mathbb{N}}$ et conjecture que tous les termes de cette suite sont premiers. Cependant en 1732 Leonhard Euler réfute cette conjecture en montrant que $F_5 = 4\,294\,967\,297$ est un multiple de 641, plus exactement $F_5 = 641 \times 6\,700\,417$.

Mais malgré le fait que cette conjecture soit fausse, les termes de cette suite qui seront plus tard nommés « nombres de Fermat » jouissent de certaines propriétés intéressantes, dont le fait qu'ils sont deux à deux premiers entre eux. Ceci découle d'une relation démontrable par récurrence sur les F_n qui est la suivante :

$$F_0 = 3 \quad \text{et} \quad \forall n \in \mathbb{N},\ F_{n+1} = 2 + \prod_{k=0}^{n} F_k. \tag{0.1}$$

Le fait que tous les F_n sont premiers entre eux entraîne qu'il existe une infinité de nombres premiers ! Nous pouvons en effet choisir de façon arbitraire un diviseur premier de chacun d'eux, qui ensemble seront alors tous différents et en nombre infini. Ceci résout donc le problème de Dirichlet pour les cas $(k+1)_{k\in\mathbb{N}}$ et $(2k+1)_{k\in\mathbb{N}}$ même si ces cas étaient déjà connus depuis au moins Euclide. Cependant, l'idée de généraliser les nombres de Fermat afin de trouver d'autres suites de nombres qui résolvent un cas particulier du problème de Dirichlet paraît ici naturelle, et c'est ce que nous ferons pour résoudre le cas $(4k+3)_{k\in\mathbb{N}}$. Considérons a, b deux entiers, ainsi que la suite $(F_n)_{n\in\mathbb{N}}$ définie par

$$F_0 = a \quad \text{et} \quad \forall n \in \mathbb{N},\ F_{n+1} = b + \prod_{k=0}^{n} F_k,$$

qui est de toute évidence une généralisation des nombres de Fermat une fois qu'on se remémore la relation (0.1). Nous nous proposons ici d'étudier cette suite en fonction de a et de b, étude qui nous mènera à la résolution - élémentaire *et* inédite - d'un cas du problème de Dirichlet.

Lemme 1. *La suite $(F_n)_{n\in\mathbb{N}}$ a les propriétés suivantes :*

(*i*) *$F_0 = a$, $F_1 = b$, et pour tout entier n supérieur ou égal à 1, $F_{n+1} = F_n^2 - bF_n + b$;*

(*ii*) *si a et b sont premiers entre eux, alors pour tous entiers naturels $m \neq n$, F_m et F_n sont premiers entre eux.*

Démonstration. Pour le premier point, prenons n un entier naturel supérieur ou égal à 1. Tout découle du calcul formel qui suit où l'on force l'apparition de F_n dans l'expression de F_{n+1}.

$$F_{n+1} \;:=\; b + \prod_{k=0}^{n} F_k \;=\; b + F_n\big(-b + b + \prod_{k=0}^{n-1} F_k\big) \;=\; b - bF_n + F_n^2.$$

Pour le second point raisonnons par récurrence et montrons que pour tout K dans $\mathbb{N}-\{0\}$, et pour tous $m \neq n$ inférieurs à K, F_m et F_n sont premiers entre eux. Notons H_K cette hypothèse de récurrence.

- L'hypothèse de coprimalité entre a et b implique directement H_1. Soit K un entier naturel plus grand que 1 tel que H_K soit vérifiée, et soit p un diviseur premier de F_{K+1}. Montrons que p ne divise pas b, ce qui permettra de conclure.

- Procédons par l'absurde, si p divise b alors il divise le produit $\prod_{l=0}^{K} F_l$. On sait par H_K que tous les F_l sont premiers entre eux, il existe par conséquent un et un seul indice i tel que $p \mid F_i$. Puisque $F_0 = a$, nécessairement $i \geq 1$, ce qui implique que $F_i = b + \prod_{j=0}^{i-1} F_j$. Étant donné que $p \mid b$, $p \mid \prod_{j=0}^{i-1} F_j$, et comme tous les F_j sont premiers entre eux, p en divise un et un seul. Il existe donc un indice k tel que $p \mid F_k$, ce qui est absurde puisque $k \neq i$. Ainsi p ne divise pas b, donc p ne divise pas $\prod_{l=0}^{K} F_l$ et a fortiori aucun des F_l pour $l \leq K$, ce qui montre H_{K+1}, et achève la démonstration de ce lemme. □

Dans ce qui va suivre, nous allons étudier le polynôme $P_b(X) = X^2 - bX + b$ qui a été mis en évidence dans le lemme précédent. Cette étude aura pour but de trouver les valeurs de a et de b pour lesquelles $P_b(X)$ admet des racines entières, ce qui nous permettra de factoriser $P_b(X)$ sur $\mathbb{Z}$. Cette factorisation nous permettra alors d'étudier les facteurs premiers de chaque terme de la suite $(F_n)_{n\in\mathbb{N}}$, dont certains d'entre eux seront congrus à a modulo b. Ceci impliquera que le cardinal de $\mathcal{P}_{a,b}$ est infini.

On voit facilement que le discriminant Δ de $P_b(X)$ est $b^2 - 4b$, et que ses racines sont $x_1 = \frac{b+\delta}{2}$ et $x_2 = \frac{b-\delta}{2}$, où $\delta = \sqrt{\Delta}$. Puisque $P_b(X)$ est à coefficient dans $\mathbb{Z}$ et *unitaire*, ses racines rationnelles sont en fait entières, et il est direct que ses racines sont rationnelles ssi δ est rationnel. Comme Δ est un entier, δ est rationnel ssi Δ est carré parfait. Malheureusement, ceci est rare.

Proposition 2. *Le discriminant Δ de $P_b(X)$ est un carré parfait si et seulement si $b \in \{0; 4\}$.*

Démonstration. Supposons qu'il existe un entier naturel c tel que $b^2 - 4b = c^2$. Cette expression se réduit en une équation de conique : $c^2 - (b-2)^2 = -4$, qui elle-même se factorise en $(c - b + 2)(c + b - 2) = -4$. Soit le couple d'entiers $(x; y) = (c - b + 2, c + b - 2)$, dont on sait qu'il vit dans $\{(2,-2), (4,-1), (-2,2), (-1,4), (-4,1), (1,-4)\}$. Puisque $x + y = 2c$ est pair x et y sont de même parité, ainsi $(x, y) \in \{(-2,2), (2,-2)\}$. Comme $y - x = 2b - 4$ on déduit que $b \in \{0, 4\}$, et que pour ces valeurs de b, $\Delta = 0$ est bien un carré parfait. □

Ainsi seul le cas $b = 4$ semble propice à l'application de notre stratégie (puisque pour $b = 0$, $(F_n)_{n\in\mathbb{N}} = (a^{n+1})_{n\in\mathbb{N}}$, ce qui ici n'est pas intéressant). Pour $b = 4$, $P_b(X) = X^2 - 4b + 4 = (X-2)^2$. En prenant $a \in \{1, 3\}$, on peut tenter de résoudre les cas $(4k+1)_{k\in\mathbb{N}}$ et $(4k+3)_{k\in\mathbb{N}}$ du problème de Dirichlet.

Proposition 3. *Pour* $(a\,,b) = (3\,,4)$ *la suite* $(F_n)_{n\in\mathbb{N}}$ *a les propriétés suivantes :*

(*i*) *pour tout entier* n *supérieur ou égal à* 2, F_n *est congru à* 1 *modulo* 4,

(*ii*) *pour tout entier* n *supérieur ou égal à* 3, F_n *a un diviseur premier congru à* 3 *modulo* 4.

Démonstration. Commençons par le premier point. On constate que $F_0 = 3$ et $F_1 = 7$ qui sont tous deux congrus à 3 modulo 4. Puisque $F_{n+1} = F_n^2 - 4F_n + 4$ pour tout entier n supérieur ou égal à 1, on déduit que $F_{n+1} \equiv F_n^2 \mod 4$, et on conclut par une récurrence immédiate.

Pour le second point, considérons n un entier supérieur ou égal à 2. Dans un premier temps, F_n est impair, donc tous ses facteurs premiers sont congrus à 1 ou à 3 modulo 4. Puisque $b = 4$, alors $F_{n+1} = (F_n - 2)^2$, et comme $F_n - 2 \equiv 3 \mod 4$ et que le produit d'entiers congrus à 1 modulo 4 est lui-même congru à 1 modulo 4 alors $F_n - 2$ doit admettre un diviseur premier congru à 3 modulo 4, il en va alors de même pour F_{n+1}. □

Théorème 4. *Il existe une infinité de nombres premiers congrus à* 3 *modulo* 4.

Démonstration. La démonstration est directe grâce à la proposition 3. En effet, pour i entier supérieur ou égal à 3, on peut choisir un p_i premier qui divise F_i et tel qu'il est congru à 3 modulo 4. On construit alors une suite $(p_i)_{i\geq 3}$ de nombres premiers congrus à 3 modulo 4, qui est injective par le lemme 1. On conclut qu'il y a une infinité de nombres premiers dans la suite arithmétique $(4k+3)_{k\in\mathbb{N}}$. □

Nous avons ainsi résolu comme annoncé un cas du problème de Dirichlet, malheureusement notre méthode ne semble pas s'appliquer au cas $(4k+1)_{k\in\mathbb{N}}$ puisque dans le cas où $b = 4$ et $a = 1$, décomposer les termes de la suite $(F_n)_{n\in\mathbb{N}}$ comme produit d'entiers congrus à 3 modulo 4 ne nous renseigne a priori pas sur leurs diviseurs premiers congrus à 1 modulo 4...

On peut même calculer les premiers termes de la suite dans ce cas, et voir que $F_2 = 9 = 3\times 3$ n'admet aucun diviseur premier de la forme $4k+1$... À ce jour nous n'avons pas encore trouvé une façon d'améliorer la « méthode Fermat » pour résoudre ce cas.

Le cas $3k+2$

Dans cette partie nous allons montrer avec des méthodes plus simples l'existence d'une infinité de nombres premiers congrus à 2 modulo 3. Nous allons toujours construire une suite de tels nombres premiers, qui seront les diviseurs d'une suite d'entiers que nous aurons construite en amont. Remarquons dans un premier temps que $2 \in \mathcal{P}_{2,3}$ qui par conséquent est non vide.

Lemme 5. *Pour tout entier naturel non nul a, les propriétés suivantes sont vérifiées :*

(*i*) *l'entier $3a-1$ admet un diviseur premier de la forme $3k+2$;*

(*ii*) *les entiers $3a-1$ et a sont premiers entre eux.*

Démonstration. Soit $a \in \mathbb{N} - \{0\}$. Pour le premier point, $3a-1$ est supérieur ou égal à 2 et est congru à 2 modulo 3. Comme il n'est pas divisible par 3, ses diviseurs premiers sont par conséquent tous congrus à 1 ou à 2 modulo 3. Étant donné que le produit d'entiers congrus à 1 modulo 3 est lui-même congru à 1 modulo 3, on déduit que $3a-1$ admet un diviseur premier congru à 2 modulo 3. Pour le second point, on voit que $3a-(3a-1)=1$, donc que $\mathrm{PGCD}(a, 3a-1)=1$ par le théorème de Bézout. □

Théorème 6. *Le cardinal de $\mathcal{P}_{2,3}$ est infini.*

Démonstration. Il manque un petit ingrédient à ajouter au lemme 5 pour pouvoir montrer ce théorème. On note $\widehat{\mathcal{P}}_1 = \{2\}$ et $p_1 = 2$. On dispose alors d'une partie à 1 élément de $\mathcal{P}_{2,3}$. Soit K un entier naturel plus grand que 1 tel qu'on a construit une partie à K éléments de $\mathcal{P}_{2,3}$. Notons $\widehat{\mathcal{P}}_K = \{p_1, p_2, p_3, ..., p_K\}$ cette partie, ordonnée avec les indices (i.e. $i \mapsto p_i$ est croissante). Notons $\Lambda = p_K!$ et $\Sigma = 3\Lambda - 1$. Par le lemme 5, Σ a un diviseur premier congru à 2 modulo 3 qu'on note p_{K+1} et qui est premier avec Λ. On déduit que $p_{K+1} \notin \mathcal{P}_K$. On note $\mathcal{P}_{K+1} = \mathcal{P}_K \cup \{p_{K+1}\}$, qui est bien une partie de $\mathcal{P}_{2,3}$ de cardinal $K+1$. Par récurrence, on conclut que le cardinal de $\mathcal{P}_{2,3}$ est infini. □

Le théorème faible de Dirichlet

Obsequium amicos, veritas odium parit.

Térence, dans l'*Andrienne*

Nous allons dans la suite montrer que les ensembles $\mathcal{P}_{1,n}$ sont infinis, ce qui traite une infinité de cas mais en laisse tout autant non résolus. Les méthodes utilisées seront élémentaires, c'est-à-dire qu'on ne fera que de l'arithmétique (et donc pas d'analyse complexe comme dans le cas général). Nos outils principaux dans les raisonnements qui vont suivre seront les *polynômes cyclotomiques*, auxquels nous allons nous intéresser maintenant.

Polynômes cyclotomiques

Les polynômes cyclotomiques nous seront utiles par la suite, notamment car ils donnent une condition suffisante facile à vérifier pour qu'un entier soit congru à 1 modulo b (b est un entier naturel non nul). Ils ont également beaucoup d'autres belles propriétés, et nous rendrons honneur à quelques-unes d'entre elles à la fin de ce paragraphe. Pour l'instant nous n'énoncerons que celles dont nous aurons besoin.

Définition. Soit $n \in \mathbb{N} - \{0\}$. On appelle *n-ième polynôme cyclotomique* le polynôme suivant.

$$\Phi_n(X) = \prod_{\substack{\zeta \in \mathbb{U}_n \\ \zeta \text{ primitive}}} (X - \zeta),$$

où les racines « primitives » sont les générateurs du groupe multiplicatif $\mathbb{U}_n$.

Lemme 7. *Soit n un entier naturel non nul. Le n-ième polynôme cyclotomique a les propriétés suivantes :*

(i) $\Phi_n(X)$ *est unitaire, et* $\deg(\Phi_n) = \phi(n)$ *;*

(ii) $X^n - 1 = \prod_{d|n} \Phi_d(X)$ *;*

(iii) $|\Phi_n(0)| = 1$ *;*

(iv) $\Phi_n(X) \in \mathbb{Z}[X]$ *;*

où ϕ désigne l'indicatrice d'Euler.

Démonstration. Le premier point est évident. Pour montrer le second point, il suffit de décomposer $X^n - 1$ en produit de $(X - \zeta)$ où ζ est une racine n-ième de l'unité, puis de regrouper selon l'ordre de ζ. Le troisième point est aussi immédiat que le premier. Pour le quatrième point, on peut facilement calculer $\Phi_1(X) = X - 1$, et se rendre compte que le résultat est vérifié pour $n = 1$. Soit $K \in \mathbb{N}$ tel que pour tous les $k \in \mathbb{N}$ inférieurs ou égaux à K, $\Phi_k(X)$ est dans $\mathbb{Z}[X]$. Comme

$$X^{K+1} - 1 = \prod_{d|K+1} \Phi_d(X) = \Phi_{K+1}(X)Q(X),$$

où $Q(X) \in \mathbb{Z}[X]$ par hypothèse, et que cette écriture est celle de la division euclidienne dans $\mathbb{Q}[X]$ de $X^{K+1} - 1$ par $Q(X)$ qui se réalise dans $\mathbb{Z}[X]$ puisque $Q(X)$ est unitaire, on déduit que $\Phi_{K+1}(X)$ est aussi dans $\mathbb{Z}[X]$ et on conclut avec le principe de récurrence. □

Les polynômes cyclotomiques sont en fait les facteurs irréductibles dans $\mathbb{Q}[X]$ du polynôme $X^n - 1$. De plus, quelques raisonnements faciles à partir de ce qui a été fait dans la preuve précédente permettent de montrer de jolis résultats d'arithmétique sur la fonction indicatrice ϕ d'Euler.

Corollaire 8. *Pour tout $n \geq 3$, $\phi(n)$ est pair.*

Démonstration. À partir de $n = 3$, 1 et -1 ne sont plus des racines n-ièmes primitives, ainsi toutes les racines primitives sont complexes. Comme on peut les regrouper selon que leur argument principal est dans l'intervalle $]0, \pi[$ ou $]-\pi, 0[$ mais que les racines du second regroupement sont en fait exactement les conjuguées de celles du premier, on peut les associer par paires. On déduit que le degré de $\Phi_n(X)$ est pair, or il vaut $\phi(n)$. □

Corollaire 9. *Pour tout $n \in \mathbb{N} - \{0\}$, $n = \sum_{d|n} \phi(d)$.*

Démonstration. Cela vient du lemme 7 (ii) et du fait que pour tout n, $\deg(\Phi_n) = \phi(n)$. □

Concernant certains aspects analytiques, ces polynômes se caractérisent grâce à la mesure de Mahler.

Définition. Soit P un polynôme de degré d et de coefficient dominant a_d. On appelle *mesure de Mahler de P*, notée $M(P)$, la quantité

$$M(P) = |a_d| \prod_{k=1}^{d} \max(1, |z_k|),$$

où les z_k sont les racines de P, ce qui se lit comme étant le produit du module du coefficient dominant et des modules des racines qui sont en-dehors du disque unité fermé.

Un théorème dû à Kronecker caractérise les polynômes cyclotomiques comme étant les seuls polynômes à coefficients entiers, unitaires et irréductibles dans $\mathbb{Q}[X]$ et de mesure de Mahler 1. On se demande aussi s'il est possible de générer des polynômes à coefficients dans $\mathbb{Z}$ de mesure de Mahler arbitrairement proche de 1 (et nécessairement plus grande). Cette interrogation constitue un problème encore ouvert.

Démonstration de la version faible du théorème de Dirichlet

Dans cette partie nous allons démontrer la version faible du théorème de Dirichlet en n'utilisant que des arguments d'arithmétique et d'algèbre sur les corps finis. Nous allons procéder en créant une « machine » à produire des nombres premiers dans les classes de congruence qui nous intéressent.

Théorème de la progression arithmétique (version faible) 10.
Soit $n \in \mathbb{N} - \{0\}$. Il existe une infinité de nombres premiers congrus à 1 modulo n.

Commençons d'abord par démontrer un lemme central ; on travaillera avec $n \geq 3$ puisque les cas $n \in \{1, 2\}$ sont déjà connus.

Lemme 11. *Soit p un nombre premier qui ne divise pas n, et $a \in \mathbb{Z}$ tel que $\Phi_n(a) \equiv 0[p]$. Alors,*

(i) *a est d'ordre n dans $\mathbb{F}_p^\times$;*

(ii) $p \equiv 1 \mod n$.

Démonstration. Le point (ii) du lemme 7 donne immédiatement que l'ordre de a modulo p divise n. Raisonnons par l'absurde, et supposons qu'il existe d' diviseur strict de n tel que $a^{d'} \equiv 1[p]$. En réduisant modulo p la relation (ii) du lemme 7, $\bar{a}^n - 1 = \Phi_n(a) \prod_{d|n, d \neq n} \Phi_d(\bar{a})$. Puisque tous les diviseurs de d' sont diviseurs stricts de n on peut écrire $\bar{a}^n - 1 = \Phi_n(a)(\bar{a}^{d'} - 1)R(X)$ où $R(X)$ est un polynôme de $\mathbb{F}_p[X]$. On déduit que $\bar{a}$ est racine double du polynôme $X^n - 1$

dans $\mathbb{F}_p$, et que par conséquent $\bar{a}$ annule le polynôme dérivé qui est $\bar{n}X^{\bar{n}-1}$, ce qui implique par intégrité que $\bar{n} = 0$ ou $\bar{a} = 0$, ce qui est absurde puisque p ne divise pas n et que $\bar{a}^n = 1$. Ainsi l'ordre de $\bar{a}$ dans $\mathbb{F}_p^\times$ est bien n. □

Démonstration. (du théorème 10) Soit $\mathcal{F} \subset \mathcal{P}_{1,n}$ une partie finie. Indexons ses éléments de telle sorte que $\mathcal{F} = \{p_1, p_2, ... p_k\}$ où $k = \text{Card}(\mathcal{F})$. Soit $a = n\prod_{1\leq i\leq k} p_i$ (qui vaut n si $\mathcal{F} = \emptyset$) et $A = \Phi_n(a)$. On souhaite étudier les diviseurs premiers de A pour appliquer le lemme 11 sur l'un d'eux (on verra que ce diviseur ne peut pas diviser n). Pour cela, montrons d'abord que A est un entier plus grand que 2 en module. En effet $|A| = |\prod_{\zeta\in\mathbb{U}_n \text{ primitive}}(a-\zeta)| \geq \prod_{\zeta\in\mathbb{U}_n \text{ primitive}}(a-1)$ par la seconde inégalité triangulaire. Ainsi $|A| \geq 2^{\phi(n)} \geq 4$. On déduit que A est assez grand pour admettre un diviseur premier ; soit donc p un tel diviseur.

Nous allons maintenant réunir les conditions pour appliquer le lemme 11. Le point (*iii*) du lemme 7 nous dit que le terme constant de $\Phi_n(X)$ est ± 1. On sait donc que p ne divise pas a puisqu'il divise A et que s'il divisait a il diviserait aussi ± 1. A fortiori p ne divise pas n. En appliquant le lemme 11 on voit que p est dans $\mathcal{P}_{1,n}$, mais étant donné que p ne divise pas a, a fortiori p ne divise aucun des p_i, donc n'est pas dans $\mathcal{F}$.

Ainsi, étant donné une partie $\mathcal{F}$ de $\mathcal{P}_{1,n}$, on peut construire une partie à $\text{Card}(\mathcal{F}) + 1$ éléments. Par récurrence sur le nombre d'éléments de $\mathcal{F}$, on conclut que l'ensemble $\mathcal{P}_{1,n}$ est de cardinal infini. □

Partie 2

Quelques prérequis

Ab omni malo nos defendat

Devise de Saint-Didier-sous-Riverie

Dans cette partie nous nous aventurerons dans la preuve du théorème de progression arithmétique de Dirichlet, non sans quelques prérequis importants. Cette même preuve est un mélange d'algèbre et d'analyse complexe, et utilise fortement les propriétés des belles séries éponymes : les *séries de Dirichlet*. Un bagage de troisième année de licence est requis pour comprendre ces prérequis.

Caractères

Les caractères sont des objets algébriques appartenant à la *théorie des représentations*, il s'agit d'un cas particulier de ces représentations. Si G est un *groupe abélien fini* les caractères captent l'intégralité de sa structure (théorème 16), ce fait important (ou plutôt un corolaire immédiat) nous aidera dans la preuve du théorème de Dirichlet.

Définition. Soit G un *groupe abélien fini*. On appelle *caractère de* G tout morphisme de G vers le groupe $(\mathbb{C}^*, \times)$. L'ensemble des caractères de G est donc $\mathrm{Hom}(G, \mathbb{C}^*)$. On le note par convention $\widehat{G}$, et il est appelé le *dual* de G, dont on note souvent les éléments par des lettres grecques telles que χ. En particulier le caractère trivial de G dans $\mathbb{C}^*$ qui à tout g associe 1 est noté χ_0.

Proposition 12. *L'ensemble $\widehat{G}$ est non vide et forme un groupe pour la loi du produit des fonctions de G dans $\mathbb{C}^*$ dont l'élément neutre est χ_0.*

Démonstration. Nous invitons le lecteur à la faire de tête. □

Remarque 1. En réalité on n'a besoin d'aucune hypothèse sur G pour donner un sens à la notion de caractère. Le dual d'un groupe abélien fini se comporte de façon similaire au dual d'un $\mathbb{C}$-ev de dimension finie, mais dans le cas non abélien on perd beaucoup d'informations(voir exemple en bas de page).

Remarque 2. Un caractère est constant sur les classes de conjugaison (cela vient du fait que $\mathbb{C}^*$ est abélien), on dit qu'une telle application est *centrale*.

Exemple. Si $G = \mathfrak{S}_n$, $n \in \mathbb{N}^*$, on sait que G est engendré par les transpositions et qu'elles sont toutes conjuguées. Par la remarque 2 tout caractère est constant sur les transpositions et comme pour tout $i \neq j$ dans $\{1, ..., n\}$, $(i, j)^2 = \mathrm{Id}$, l'image d'une transposition par un caractère est 1 ou -1. On déduit de cela que les caractères de G sont χ_0 et la signature notée ε, d'où $\widehat{\mathfrak{S}} \simeq \mathbb{Z}/2\mathbb{Z}$.

Remarque 3. De façon générale, l'image par un caractère d'un groupe fini G est toujours un groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité (pour un $n \in \mathbb{N}^*$ convenable). En effet si m est l'exposant du groupe G, alors pour tout g dans G et pour tout caractère χ, $\chi(g)^m = \chi(g^m) = 1$. L'image de G par χ étant un sous-groupe de $\mathbb{U}_m$ il existe un diviseur n de m tel que $\mathrm{Im}(\chi) = \mathbb{U}_n$.

Par la suite nous allons nous restreindre au cas où G est un *groupe abélien fini*, puisque les groupes $(\mathbb{Z}/b\mathbb{Z})^\times$ nous serviront dans la preuve du théorème de Dirichlet. Voici un théorème sur la structure des groupes abéliens finis qui nous sera d'une grande utilité.

Théorème 13. *Soit G un groupe abélien fini. Alors G se décompose comme produit de groupes cycliques.*

Nous ne démontrerons pas ce théorème ici, mais il nous sera d'une grande aide. Nous allons établir un résultat important pour la suite(qui fait écho à l'algèbre linéaire). Tout d'abord montrons deux lemmes centraux.

Lemme 14. *Soit G_1, G_2 deux groupes. Alors $\widehat{G_1 \times G_2} \simeq \widehat{G_1} \times \widehat{G_2}$.*

Démonstration. Il suffit de trouver un isomorphisme entre les deux structures. Soit ϕ l'application de $\widehat{G_1} \times \widehat{G_2}$ dans $\widehat{G_1 \times G_2}$, qui à un couple de caractères (χ_1, χ_2) associe la fonction $\chi_1 \boxtimes \chi_2 : G_1 \times G_2 \to \mathbb{C}^*$, $(g_1, g_2) \mapsto \chi_1(g_1)\chi_2(g_2)$. On se convainc facilement du fait que $\chi_1 \boxtimes \chi_2 \in \widehat{G_1 \times G_2}$ et du fait que ϕ est un morphisme. Aussi si $\phi(\chi_1, \chi_2) = \chi_0$, alors pour tout g_1 dans G_1 et pour $g_2 = e_{G_2}$, on voit que $\phi(\chi_1, \chi_2)(g_1, g_2) = \chi(g_1) = 1$, donc χ_1 est trivial et de même pour χ_2, d'où l'injectivité de ϕ. Enfin si χ est un caractère de $\widehat{G_1 \times G_2}$, on peut regarder les « caractères partiels », $\chi_1 : g_1 \mapsto \chi(g_1, e_{G_2})$ et $\chi_2 : g_2 \mapsto \chi(e_{G_1}, g_2)$, qui sont évidemment des caractères de G_1 et de G_2. Puisque $\chi = \phi(\chi_1, \chi_2)$, on déduit la surjectivité de ϕ. □

Lemme 15. *Soit $n \in \mathbb{N}^*$. Le groupe cyclique d'ordre n est isomorphe à son dual.*

Démonstration. Il suffit encore de trouver un isomorphisme entre les deux structures. Soit C_n le groupe cyclique d'ordre n noté additivement. Soit g un générateur de C_n, et $\psi : C_n \longrightarrow \widehat{C_n}$, $\psi : kg \mapsto \chi_k$, où $\chi_k : lg \mapsto e^{\frac{2i\pi kl}{n}}$. D'une part, χ_k est un caractère bien défini puisque les mg où $n \mid m$ sont envoyés sur 1, d'autre part si $\psi(kg) = \chi_0$, alors pour tout l dans $\mathbb{Z}$, n divise kl, en particulier pour l premier avec n, on déduit par le lemme de Gauss que n divise k et que par conséquent $kg = 0$. Ainsi ψ est injective. Enfin si χ est un caractère de C_n, alors (cf. la remarque 3) $\chi(g)$ est un élément de $\mathbb{U}_n$ donc il existe k entier compris entre 0 et $n-1$ tel que $\chi(g) = e^{\frac{2i\pi k}{n}}$, d'où l'on déduit que $\chi = \psi(kg)$ et que ψ est surjectif. □

Théorème 16. *Soit G un groupe abélien fini. Alors $G \simeq \widehat{G}$. En particulier, $|G| = |\widehat{G}|$.*

Démonstration. Il existe une suite finie d'entiers strictement positifs $(a_1, ..., a_r)$ telle que $G \simeq \prod_i^r C_{a_i}$, où C_{a_i} désigne le groupe cyclique d'ordre a_i. Par récurrence immédiate et en utilisant le lemme 14, $\widehat{G} \simeq \widehat{\prod_i^r C_{a_i}} \simeq \prod_i^r \widehat{C_{a_i}}$ et par le lemme 15 $\widehat{C_{a_i}} \simeq C_{a_i}$ donc $G \simeq \widehat{G}$. □

Remarque 4. On remarque que tout comme un espace vectoriel de dimension finie, l'isomorphisme entre G et son dual n'est pas canonique puisqu'il fait appel aux isomorphismes entre ses facteurs directs externes cycliques et leur dual, qui eux-mêmes ne sont pas canoniques puisqu'ils font appel à un générateur.

Nous allons maintenant munir l'espace vectoriel des fonctions complexes d'un groupe abélien fini G d'une structure *hermitienne*. Ce sont les informations fournies par cette même structure que nous utiliserons pour parcourir la première moitié du chemin lors de la preuve du théorème de Dirichlet.

Définition. Soit G un groupe abélien fini. On définit sur le $\mathbb{C}$-ev $\mathbb{C}^G$ une structure d'espace hermitien grâce au produit scalaire suivant :

$$\langle \cdot \mid \cdot \rangle : (x, y) \longmapsto \frac{1}{|G|} \sum_{g \in G} \overline{x(g)} y(g).$$

Remarque 5. En identifiant $\mathbb{C}^G$ à $\mathbb{C}^{|G|}$ au moyen de la base des indicatrices $\mathbf{1}_g$ d'un élément g de G (et d'une numérotation de ses éléments), on voit que l'application précédente est le produit scalaire canonique à constante près. De plus, l'identification montre que $\mathbb{C}^G$ est de dimension finie.

Proposition 17. *Les caractères de G forment une base orthonormée de l'espace $\mathbb{C}^G$.*

Démonstration. Soit χ_1, χ_2 deux caractères. On a toujours $\langle \chi_1 \mid \chi_2 \rangle = \langle \chi_0 \mid \overline{\chi_1} \chi_2 \rangle$, et puisque $\overline{\chi_1}\chi_2$ est un caractère, il suffit de montrer l'orthogonalité de tous les caractères non triviaux avec χ_0. Soit χ un caractère. On a $\sum_{g \in G} \overline{\chi_0(g)} \chi(g) = \sum_{g \in G} \chi(g)$, mais puisqu'il existe un entier positif n tel que $\chi(G) = \mathbb{U}_n$, et que $G/\ker(\chi) \sim \mathbb{U}_n$, alors en regroupant les éléments de G par classe d'équivalence modulo $\ker(\chi)$, on obtient que $\sum_{g \in G} \chi(g) = |\ker(\chi)| \sum_{\omega \in \mathbb{U}_n} \omega$. La dernière somme est 0 si χ est non trivial (i.e. $n > 1$), et $|G|$ si χ est trivial (i.e. $n = 1$). On déduit ainsi que la famille des caractères de G est libre, puis que c'est une base par le théorème 16. □

À constante multiplicative près, l'espace $\mathbb{C}^G$ admet une autre base orthonormée, plus naturelle, la base des indicatrices $\mathbf{1}_g$ d'un élément G. Nous allons établir une façon de passer d'une base à l'autre qui s'avère être particulièrement simple. Pour un élément g de G, on notera $\mathbf{1}_g$ l'indicatrice du singleton qui contient g.

Proposition 18. *On dispose des relations suivantes dans l'espace vectoriel $\mathbb{C}^G$ pour tout caractère χ et indicatrice $\mathbf{1}_g$:*

(i) $\chi = \sum_{g \in G} \langle \mathbf{1}_g \mid \chi \rangle \mathbf{1}_g = \sum_{g \in G} \chi(g) \mathbf{1}_g$,

(ii) $\mathbf{1}_g = \sum_{\chi \in \widehat{G}} \langle \chi \mid \mathbf{1}_g \rangle \chi = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{\chi(g)} \chi$.

Démonstration. On utilise simplement le fait que les deux bases sont orthonormées. □

Comme nous le verrons dans la preuve du théorème de Dirichlet, ces changements de base nous seront d'une grande utilité. En anticipant légèrement, nous verrons qu'ils nous permettent d'exhiber des contributions essentielles au voisinage d'un pôle d'une certaine fonction méromorphe. L'existence de ce pôle impliquera qu'il existe une infinité de nombres premiers congrus à a modulo b, où a et b sont premiers entre eux.

Introduisons maintenant une dernière notion liée aux caractères qui nous permettra d'écrire un grand nombre de lignes d'une façon plus simple et plus hygiénique.

Définition. Soit b un entier naturel non nul. On pose $B = \left(\mathbb{Z}/b\mathbb{Z}\right)^\times$, le groupe des inversibles de l'anneau quotient $\mathbb{Z}/b\mathbb{Z}$. Soit χ un élément de $\widehat{B}$. On appelle *caractère de Dirichlet modulo b associé à χ* l'application $\tilde{\chi}$ obtenue via un prolongement par 0 de χ à l'anneau $\mathbb{Z}/b\mathbb{Z}$, et relevée à $\mathbb{Z}$ par la surjection canonique (qu'on notera ici $\pi : \mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$) ; c'est-à-dire l'application :

$$\begin{aligned} \tilde{\chi} : \mathbb{Z} &\longmapsto \mathbb{C} \\ m &\longmapsto \begin{cases} \chi(\pi(m)) & \text{si } m \text{ est inversible modulo } b \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Exemple. Si b est un nombre premier et χ un caractère de B dont le noyau est l'image du morphisme $m \mapsto m^2$, le caractère de Dirichlet obtenu est en réalité le symbole de Legendre (qui permet de détecter les résidus quadratiques modulo b).

Proposition 19. *Les caractères de Dirichlet modulo b sont complètement multiplicatifs, c'est-à-dire que $\chi(1) = 1$ et $\chi(mn) = \chi(m)\chi(n)$ pour tous entiers m et n.*

Démonstration. La démonstration est une simple disjonction de cas selon que m et n sont premiers avec b ou non. □

Remarque 6. La coutume veut que le caractère de Dirichlet $\tilde{\chi}$ soit toujours noté χ avec un léger abus.

Dans la suite nous pourrons définir des fonctions particulières, les fonctions L, qui dépendent d'un caractère de Dirichlet et d'une variable complexe. Ces fonctions jouent un rôle très important dans la preuve du théorème de la progression arithmétique. Ces objets apparaissent dans bien d'autres situations, ils sont bien plus profonds que ce que leur apparition dans le présent document laissera suggérer. Commençons par d'importantes généralités.

Séries de Dirichlet

Les séries de Dirichlet sont ces bonnes amies des séries entières et des produits infinis qui, comme eux, permettent de définir des objets d'une certaine complexité. Les séries de Dirichlet ressemblent beaucoup aux séries entières, et certaines fonctions bien connues comme la fonction ζ de Riemann en sont des cas particuliers.

Définition. Soit $(a_n)_{n\in\mathbb{N}}$ une suite de nombres complexes. On appelle *série de Dirichlet associée à $(a_n)_{n\in\mathbb{N}}$* la série de fonctions de terme général $s \mapsto a_n n^{-s}$, où s est un nombre complexe.

Remarque 7. Pour élever un nombre réel x à une puissance complexe, on pose la définition suivante (qui nécessite que x soit strictement positif) : pour $z \in \mathbb{C}$, $x^z := e^{z\ln(x)}$.

Afin de démontrer quelques résultats essentiels concernant les séries de Dirichlet, nous aurons besoin d'une transformation d'Abel parfois appelée « intégration par parties discrète ».

Proposition 20. *Soit f une fonction de classe $\mathcal{C}^1$ sur $\mathbb{R}^+$ et $(a_n)_{n\in\mathbb{N}}$ une suite de nombres complexes. On note $A(t) := \sum_{k\leq t} a_k$ une « primitive » de $(a_n)_{n\in\mathbb{N}}$. Alors pour tous réels positifs $y < x$,*

$$\sum_{y<k\leq x} a_k f(k) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Démonstration. Dans un premier temps remarquons que $\int_k^{k+1} A(t)f'(t)dt = A(k)\int_k^{k+1} f'(t)dt = A(k)(f(k+1)-f(k))$. En posant $M = \lfloor y \rfloor$ et $N = \lfloor x \rfloor$, on a

$$\int_M^N A(t)f'(t)dt = \sum_{k=M}^{N-1}\int_k^{k+1} A(t)f'(t)dt = \sum_{k=M}^{N-1} A(k)(f(k+1)-f(k))$$

$$\overset{(*)}{=} \sum_{k=M+1}^{N} (A(k-1)-A(k))f(k) + A(N)f(N) - A(M)f(M)$$

$$= -\sum_{k=M+1}^{N} a_k f(k) + A(N)f(N) - A(M)f(M)$$

Et pour la formule générale on remarque que $\int_{\lfloor x \rfloor}^x A(t)f'(t)dt = A(x)f(x) - A(\lfloor x \rfloor)f(\lfloor x \rfloor)$.
$(*)$ Pour cette égalité il suffit de développer la somme précédente. □

Remarque 8. Cette transformation d'Abel est un outil remarquable pour passer d'une série à une représentation intégrale. Elle permet par exemple de donner (en étudiant $\ln(n!)$) l'estimation $\ln(n!) = n\ln(n) - n + O(\ln(n))$, ou bien $\sum_{p \text{ premier} \leq x} \frac{1}{p} \sim \ln(\ln(x))$.

Proposition 21. *Soit $\sum a_k k^{-s}$ une série de Dirichlet que l'on suppose convergente en un $s_0 \in \mathbb{C}$. La série converge alors uniformément sur tous les secteurs angulaires $S_{s_0,\theta} := \{s \in \mathbb{C} \text{ tq } \Re(s-s_0) \geq 0, |\mathrm{Arg}(s-s_0)| \leq \theta\}$ où $|2\theta| < \pi$.*

Démonstration. Pour un $M \geq 1$ et pour $x \geq M$ on note $A_M(x) = \sum_{M<k\leq x} a_k k^{-s_0}$. Par hypothèse, le reste à l'ordre M tend vers 0, ainsi $|A_M(x)| \leq \varepsilon(M)$ qui tend vers 0 quand M tend vers l'infini. Par la formule d'Abel,

$$\sum_{M\leq k\leq N} a_k k^{-s} = \sum_{M\leq k\leq N} a_k k^{-s_0}k^{-(s-s_0)} = A_M(N)N^{-(s-s_0)} + (s-s_0)\int_M^N A_M(t)t^{-(s-s_0+1)}dt.$$

On peut alors majorer la valeur absolue de la dernière intégrale par

$$\varepsilon(M)\int_M^N t^{-(\sigma-\sigma_0+1)}dt = \varepsilon(M)\frac{M^{-(\sigma-\sigma_0)} - N^{-(\sigma-\sigma_0)}}{(\sigma-\sigma_0)} \leq \frac{\varepsilon(M)}{\sigma-\sigma_0}$$

où $\sigma = \Re(s)$ et $\sigma_0 = \Re(s_0)$. En se plaçant dans un secteur $S_{s_0,\theta}$, $\Re(s-s_0) = \sigma - \sigma_0 \geq |s-s_0|\cos(\theta)$, donc $\frac{1}{\cos(\theta)} \geq \frac{|s-s_0|}{\sigma-\sigma_0}$. En injectant cette inégalité dans le dernier majorant, on a

$$\left|\sum_{M\leq k\leq N} a_k k^{-s}\right| \leq \varepsilon(M)\left(1 + \frac{1}{\cos(\theta)}\right),$$

ce qui suffit à montrer la convergence uniforme de la série sur le secteur considéré. □

Définition. On appelle *abscisse de convergence* d'une série de Dirichlet qui converge en au moins un $s_0 \in \mathbb{C}$ le réel $\inf\{\sigma \in \mathbb{R} \mid \sum a_k k^{-\sigma} \text{ converge}\}$.

La proposition 21 implique que l'ensemble des σ réels tels que $\sum_k a_k k^{-\sigma}$ converge est une demi-droite dont l'origine est l'abscisse de convergence. De la nature géométrique des secteurs $S_{s_0,\theta}$ et du fait que θ peut être pris dans $[0,\, \pi/2[$, on déduit que les séries de Dirichlet convergent sur des demi-plans. On considère désormais $D_\sigma := \{s \in \mathbb{C} \,|\, \Re(s) > \sigma\}$. Il est clair que la série converge sur D_σ et qu'elle ne converge pas sur le demi-plan $\Re(s) < \sigma$. Le comportement de la série sur la droite d'équation $\Re(s) = \sigma$ est par contre très imprévisible, autant que celui des séries entières sur leur cercle d'incertitude. La proposition 21 et le fait que $s \mapsto k^{-s}$ est entière impliquent la proposition suivante.

Proposition 22. *Soit $\sum_k a_k k^{-s}$ une série de Dirichlet d'abscisse de convergence σ. Soit $F : D_\sigma \mapsto \mathbb{C}$ sa somme. Alors F est holomorphe sur D_σ, et ses dérivées successives s'obtiennent en dérivant la série terme à terme.*

Démonstration. Il suffit de remarquer que tout compact de D_σ est inclus dans un secteur $S_{s_0,\theta}$, et on termine avec l'uniforme convergence de la série sur ce secteur en utilisant le théorème de convergence holomorphe de Weierstrass. □

Corollaire 23. *Si les sommes partielles de $\sum_n a_n$ sont bornées, alors la série de Dirichlet associée converge pour tout complexe s de partie réelle strictement positive.*

Démonstration. En reprenant la formule obtenue par la transformation d'Abel dans la preuve de la proposition 21 où on remplace s_0 par 0,

$$\sum_{1\leq k\leq N} a_k k^{-s} = \Big(\sum_{1<k\leq N} a_k\Big) N^{-s} + s\int_1^N \Big(\sum_{1<k\leq t} a_k\Big) t^{-(s+1)} dt$$

pour tout s de partie réelle strictement positive. Puisque les sommes partielles de la série de terme général $(a_k)_{k\in\mathbb{N}}$ sont bornées alors

$$\sum_{1\leq k\leq N} a_k k^{-s} = o(1) + s\int_1^N \Big(\sum_{1<k\leq t} a_k\Big) t^{-(s+1)} dt.$$

Il est clair que la dernière intégrale est absolument convergente, donc la série de Dirichlet converge pour $\Re(s) > 0$. □

Le corollaire précédent est un critère simple pour justifier qu'une série de Dirichlet admet une abscisse de convergence inférieure ou égale à 0, ce qui sera souvent nécessaire dans la preuve du théorème de la progression arithmétique.

Fonctions L

Définition. Soit b un entier naturel non nul et χ un caractère de Dirichlet modulo b. On définit la fonction L associée à χ comme la série de Dirichlet

$$L(\chi, s) = \sum_{n\geq 1} \chi(n) n^{-s}$$

Remarque 9. Si on choisit le caractère de Dirichlet associé au caractère trivial et si on prend $b = 1$, la fonction L obtenue est la fonction ζ de Riemann.

On va voir que les fonctions L ont plusieurs propriétés en commun avec la fonction ζ, propriétés qui font de ces objets de véritables ponts entre arithmétique et analyse complexe. Nous déterminons au passage l'abscisse de convergence des fonctions L.

Proposition 24. *On a l'égalité suivante pour toute fonction L et pour tout $\Re(s) > 1$,*

$$L(\chi, s) = \sum_{n\geq 1} \chi(n) n^{-s} = \prod_{p \text{ premier}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Cette égalité est appelée « formule d'Euler généralisée ».

Démonstration. Comme χ est bornée, le produit est normalement convergent sur tout compact de D_1. En particulier on peut voir le terme général comme une série géométrique, ce qui donne pour tout $x \geq 2$,

$$\prod_{p \text{ premier} \leq x} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p \text{ premier} \leq x} \sum_{m\geq 0} \chi(p)^m p^{-ms} = \lim_{N\to\infty} \prod_{p \text{ premier} \leq x} \sum_{m=0}^{N} \chi(p^m) p^{-ms}.$$

Le développement du produit sur la dernière somme donne

$$\prod_{p \text{ premier} \leq x} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \lim_{N\to\infty} \sum_{n\in\mathcal{E}_{x,N}} \chi(n) n^{-s},$$

où $\mathcal{E}_{x,N}$ est l'ensemble des entiers qui sont produits de facteurs premiers inférieurs à x et d'exposants inférieurs à N. Quand N tend vers l'infini, on couvrira l'ensemble des entiers dont les facteurs premiers sont inférieurs à x, et enfin quand on fait tendre x vers l'infini, on couvrira tous les entiers naturels. □

Corollaire 25. *Pour s dans D_1,*

$$\zeta(s) = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^s}\right)^{-1} \text{ et } L(\chi_0, s) = \prod_{\substack{p \text{ premier} \\ p \,|\, b}} \left(1 - \frac{1}{p^s}\right) \zeta(s),$$

où χ_0 est le caractère trivial modulo b.

Le corollaire suivant vient du fait que pour un produit normalement convergent, sa valeur est 0 ssi l'un des facteurs est nul.

Corollaire 26. *Pour tout caractère de Dirichlet χ, $L(\chi, s) \neq 0$ pour tout s de partie réelle strictement plus grande que 1.*

Proposition 27. *Si $\chi \neq \chi_0$, la fonction L associée à χ a pour abscisse de convergence 0. Si $\chi = \chi_0$ l'abscisse de convergence est 1.*

Démonstration. On sait bien que l'abscisse de convergence de la série de Dirichlet qui définit la fonction ζ de Riemann est 1. On étend cela aux $L(\chi_0, \,.\,)$ avec le corollaire 25. Enfin, soit χ un caractère modulo b différent du caractère trivial. D'après le corollaire 23, il suffit de montrer que les sommes partielles des $(\chi(n))_{n\geq 1}$ sont bornées. Par la proposition 18, on voit que $\sum_{k=r+1}^{r+m} \chi(k)$ $= \langle\, \chi_0 \mid \chi \,\rangle = 0$ pour tout entier naturel r. Par conséquent,

$$\left|\sum_{n\leq x} \chi(n)\right| = \left|\sum_{m\lfloor \frac{x}{m} \rfloor \leq n \leq x} \chi(n)\right| \leq m,$$

ce qui permet de dire que l'abscisse de convergence de la série est inférieure ou égale à 0. On conclut en remarquant que le terme général ne tend pas vers 0 si $\Re(s) \leq 0$. □

Logarithme des fonctions L

Nous allons désormais exhiber quelques dernières formules importantes avant de pouvoir attaquer la preuve du théorème de la progression arithmétique de Dirichlet. Définissons avant cela une fonction importante en théorie des nombres,

Définition. On définit la fonction de von Mangoldt $\Lambda : \mathbb{N} \to \mathbb{R}$ par

$$\Lambda(n) = \begin{cases} \ln(p) & \text{si } \exists m \geq 1 \mid n = p^m \\ 0 & \text{sinon.} \end{cases}$$

Autrement dit $\Lambda(n)$ vaut $\ln(p)$ si n est une puissance d'un nombre premier p et 0 sinon.

Nous allons construire une détermination holomorphe du logarithme principal d'une fonction L sur le demi-plan D_1, ce qui sera idéalement possible grâce au corollaire 26. Dans la suite $\mathrm{Log} : \mathbb{C} \setminus \mathbb{R}^- \to \mathbb{C}$ désigne la détermination principale du logarithme.

Proposition 28. *La fonction*

$$\mathrm{Log}(L(\chi, s)) = \sum_{p \text{ premier}} \sum_{m \geq 1} \frac{\chi(p)^m}{m} p^{-ms} = \sum_{p \text{ premier}} -\mathrm{Log}\left(1 - \frac{\chi(p)}{p^s}\right),$$

est une détermination principale du logarithme de $L(\chi, .)$ holomorphe sur D_1. De plus on dispose de l'égalité

$$\sum_{p \text{ premier}} \sum_{m \geq 1} \frac{\chi(p)^m}{m} p^{-ms} = \sum_{m \geq 1} \sum_{p \text{ premier}} \frac{\chi(p)^m}{m} p^{-ms}$$

Démonstration. Vérifions d'abord que cette fonction est bien définie. Dans un premier temps, comme $\Re(s) > 1$, la série sur m est absolument convergente pour tout p. Dans un second temps, on peut majorer le terme général de la série sur p par $-\ln(1-p^{-\Re(s)})$, et on est amené à calculer le produit d'Euler rencontré à la proposition 24 qui converge puisque $\Re(s) > 1$. Cette fonction est bien un logarithme de la fonction $L(\chi, .)$ puisque

$$e^{\mathrm{Log}(L(\chi,s))} = \prod_{p \text{ premier}} e^{\sum_{m \geq 1} \frac{\chi(p)^m}{m} p^{-ms}} = \prod_{p \text{ premier}} e^{-\mathrm{Log}(1 - \frac{\chi(p)}{p^s})},$$

et que pour tout z dans $\mathbb{C} \setminus \mathbb{R}^-$ l'égalité $\mathrm{Log}(z^{-1}) = -\mathrm{Log}(z)$ est vérifiée.

La fonction $-\mathrm{Log}(1-\chi(p)p^{-s})$ est évidemment holomorphe sur D_1. Puisque pour tout z dans le disque unité ouvert $|\mathrm{Log}(1+z)| \leq -\ln(1-|z|)$ alors le module du terme général est majoré par $-\ln(1-p^{-\Re(s)})$. Comme sur tout compact K de D_1 la partie réelle est minorée par un $\sigma > 1$,

$$-\ln(1 - \frac{1}{p^{\Re(s)}}) \leq -\ln(1 - \frac{1}{p^\sigma}) \sim \frac{1}{p^\sigma},$$

d'où la convergence normale de la série sur p, et uniforme sur tout compact K de D_1. On conclut que $\mathrm{Log}(L(\chi, .)$ est holomorphe sur D_1. Comme on a montré la convergence absolue de la double somme, la dernière égalité se déduit du théorème de Fubini. □

Corollaire 29. *On a de plus la formule suivante,*

$$-\frac{L'(\chi, s)}{L(\chi, s)} = \sum_{p \text{ premier}} \sum_{m \geq 1} \chi(p)^m \frac{\ln(p)}{p^{ms}} = \sum_{n \in \mathbb{N}^*} \chi(n) \frac{\Lambda(n)}{n^s}.$$

Démonstration. On ne fait que dériver terme à terme la détermination holomorphe précédente, ce que l'on sait possible grâce à la convergence normale. □

Théorème de la progression arithmétique

Le plus court chemin entre deux vérités réelles passe souvent par le domaine complexe.

Paul Painlevé

Après un si long chemin parcouru à travers certains paysages qui semble-t-il n'ont pas de liens directs avec l'arithmétique, nous allons enfin revenir dans cette si amicale forêt des nombres pour à nouveau s'émerveiller des chemins insoupçonnés qu'on y trouve. La preuve de Dirichlet est une carte qui décrit une route qui serpente dans les landes précédemment explorées, et qui finit dans les paysages de l'arithmétique que nous côtoyons depuis l'enfance. Les idées qu'elle contient rendent la randonnée qui va suivre d'autant plus surprenante.

La preuve

Dans cette section nous allons démontrer le théorème de Dirichlet en segmentant la preuve par « parties ». Nous invitons le lecteur à revenir aux prérequis s'il se sent perdu en cours de route ou à se munir d'un papier et d'un crayon pour raisonner en même temps qu'il lit.

Première partie

Fixons une bonne fois pour toutes a et b deux entiers strictement positifs premiers entre eux tels que $a < b$ et notons $\mathcal{P}_{a,b}$ l'ensemble des nombres premiers congrus à a modulo b. La première idée de Dirichlet est de montrer que la série

$$\sum_{p \in \mathcal{P}_{a,b}} \frac{1}{p}$$

diverge, ce qui implique clairement que le cardinal de $\mathcal{P}_{a,b}$ est infini. Pour étudier la divergence de cette série, nous allons étudier le comportement au voisinage de 1 de la série de Dirichlet

$$\sum_{p \in \mathcal{P}_{a,b}} p^{-s}, \tag{0.2}$$

qui est bien définie pour $\Re(s) > 1$ par le critère de Riemann. La seconde idée de Dirichlet est de transformer cette somme en remarquant que, modulo b, on somme des représentants premiers de la classe de a. Ceci revient à écrire

$$\sum_{p \in \mathcal{P}_{a,b}} p^{-s} = \sum_{p \text{ premier}} \mathbf{1}_{\pi(a)}(\pi(p)) p^{-s} \ ,$$

où $\pi : \mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ désigne la surjection canonique. La transformation en question est en fait le changement de base exhibé dans la proposition 18 qui passe de la base des indicatrices à celle des caractères (qui a un sens puisque les termes sont nuls en dehors de $\left(\mathbb{Z}/b\mathbb{Z}\right)^\times$). C'est ici qu'on utilise que a et b sont premiers entre eux, puisque la fonction $\mathbf{1}_{\pi(a)}$ est bien un élément de $\mathbb{C}^{\mathbb{Z}/b\mathbb{Z}^\times}$. En l'appliquant à l'égalité précédente, on obtient

$$\sum_{p \text{ premier}} \mathbf{1}_{\pi(a)}(\pi(p)) p^{-s} = \sum_{p \text{ premier}} p^{-s} \frac{1}{\phi(b)} \sum_{\chi} \overline{\chi(a)} \chi(p),$$

où ϕ désigne l'indicatrice d'Euler. La seconde somme porte sur les caractères de Dirichlet modulo b puisque le changement de base ne peut s'appliquer pour tous les p (ils ne sont pas tous inversibles modulo b). En reprenant les notations de la proposition 18, $G = \mathbb{Z}/b\mathbb{Z}$, donc $|G| = \phi(b)$, d'où le facteur $\frac{1}{\phi(b)}$.

Puisque la somme sur les caractères de Dirichlet est finie, on peut procéder à une interversion et obtenir que

$$\sum_{p\in\mathcal{P}_{a,b}} p^{-s} = \frac{1}{\phi(b)}\sum_{\chi}\overline{\chi(a)}\sum_{p \text{ premier}} p^{-s}\chi(p).$$

Seconde partie

La transformation précédente, de nature algébrique, décrit la série de Dirichlet (0.2) comme une somme finie de fonctions qui « ressemblent » aux fonctions L de Dirichlet. Nous allons voir que celle qui est associée au caractère trivial va apporter la contribution principale dans le comportement au voisinage de 1 de (0.2). En mettant de côté la somme où $\chi = \chi_0$, on obtient

$$\sum_{p\in\mathcal{P}_{a,b}} p^{-s} = \frac{1}{\phi(b)}\sum_{\substack{p \text{ premier}\\ p\nmid b}} p^{-s} + \frac{1}{\phi(b)}\sum_{\chi\neq\chi_0}\overline{\chi(a)}\sum_{p \text{ premier}} p^{-s}\chi(p).$$

Admettons temporairement deux résultats que nous démontrerons plus tard (Log désigne le logarithme principal).

Proposition 30. *On a* $\sum_{p \text{ premier}} p^{-s} = -\mathrm{Log}(s-1) + O(1)$ quand $s \to 1$ *avec* $s \in D_1$.

Proposition 31. *Si* χ *est différent du caractère trivial,* $L(\chi, 1) \neq 0$.

Le premier de ces deux résultats nous permet de contrôler la première somme, c'est-à-dire de montrer qu'elle diverge comme $-\mathrm{Log}(s-1)/\phi(b)$ au voisinage de 1. Pour contrôler la seconde somme, nous allons utiliser le second résultat ainsi que l'égalité

$$\begin{aligned}\mathrm{Log}(L(\chi,s)) &= \sum_{p \text{ premier}}\sum_{m\geq 1}\frac{\chi(p)^m}{m}p^{-ms} = \sum_{m\geq 1}\sum_{p \text{ premier}}\frac{\chi(p)^m}{m}p^{-ms}\\ &= \sum_{p \text{ premier}}\chi(p)p^{-s} + \sum_{m\geq 2}\sum_{p \text{ premier}}\frac{\chi(p)^m}{m}p^{-ms},\end{aligned}$$

où la première interversion est justifiée par la seconde partie proposition 28. On déduit alors que

$$\sum_{p \text{ premier}}\chi(p)p^{-s} = \mathrm{Log}(L(\chi,s)) + H_\chi(s)$$

où H_χ est une fonction holomorphe pour $\Re(s) > \frac{1}{2}$. En effet, si $\Re(s) > \frac{1}{2}$ et $m \geq 2$ alors $\Re(ms) > 1$, et la somme qui définit H_χ converge absolument par le critère de Riemann. On peut donc récrire

$$\sum_{p\in\mathcal{P}_{a,b}} p^{-s} = -\frac{\ln(s-1)}{\phi(b)} + \sum_{\chi\neq\chi_0}\mathrm{Log}(L(\chi,s)) + H_\chi(s)$$

Comme les fonctions H_χ sont holomorphes sur $D_{\frac{1}{2}}$, elles sont bornées au voisinage de 1 et comme $L(\chi, 1) \neq 0$ pour $\chi \neq \chi_0$, on déduit que

$$\sum_{p\in\mathcal{P}_{a,b}} p^{-s} = -\frac{\ln(s-1)}{\phi(b)} + O(1) \text{ quand } s \to 1^+,$$

ce qui termine la preuve du théorème de la progression arithmétique.

Derniers points

Lemme 32. *Pour $\Re(s) > 1$, $\zeta(s) = \frac{1}{s-1} + O(1)$ quand s tend vers 1 avec $s \in D_1$.*

Démonstration. Soit x un réel plus grand que 2. En appliquant la formule d'Abel (proposition 21) pour $y = 1$, x, $(a_k)_k$ constante égale à 1 et $f : t \mapsto t^{-s}$,

$$\sum_{1\leq k\leq x} k^{-s} = 1 + \sum_{1<k\leq x} a_k f(k) = \lfloor x \rfloor x^{-s} + s\int_1^x \frac{\lfloor t \rfloor}{t^{s+1}} dt.$$

L'intégrale peut être scindée en deux en écrivant $\lfloor t \rfloor = t - \{t\}$, où $\{t\}$ désigne la partie fractionnaire de t, ce qui donne

$$\sum_{1\leq k\leq x} k^{-s} = \lfloor x \rfloor x^{-s} + s\left(\frac{x^{1-s}}{1-s} - \frac{1}{1-s} - \int_1^x \frac{\{t\}}{t^{s+1}} dt\right).$$

Puisque la dernière intégrale converge quand x tend vers l'infini (en effet $\{t\} \leq 1$),

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{t\}}{t^{s+1}} dt = \frac{1}{s-1} + 1 - s\int_1^\infty \frac{\{t\}}{t^{s+1}} dt. \tag{0.3}$$

La dernière intégrale est majorée par $\frac{1}{s}$, ce qui permet d'écrire :

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

achevant ainsi la preuve du lemme. □

Remarque 10. Puisque l'intégrale de (0.3) définit une fonction holomorphe pour $s > 0$, elle permet de prolonger ζ en une fonction méromorphe sur le domaine $D_0 \setminus \{1\}$. Le principe du prolongement analytique permet de dire qu'un tel prolongement est unique.

Proposition 30. *On a l'estimation suivante,*

$$\sum_{p \text{ premier}} p^{-s} = -\mathrm{Log}(s-1) + O(1)$$

quand s tend vers 1 avec $s \in D_1$.

Démonstration. On sait via la remarque 9 page 15 que pour le caractère de Dirichlet trivial modulo 1, la fonction L associée n'est autre que la fonction ζ. Avec la détermination holomorphe de son logarithme principal on peut écrire

$$\mathrm{Log}(\zeta(s)) = \sum_{p \text{ premier}} \sum_{m\geq 1} \frac{\chi(p)^m}{m} p^{-ms} = \sum_{p \text{ premier}} p^{-s} + \sum_{p \text{ premier}} \sum_{m\geq 2} \frac{\chi(p)^m}{m} p^{-ms}.$$

La deuxième somme définit une fonction H holomorphe sur $D_{\frac{1}{2}}$, donc bornée au voisinage de 1. On déduit que

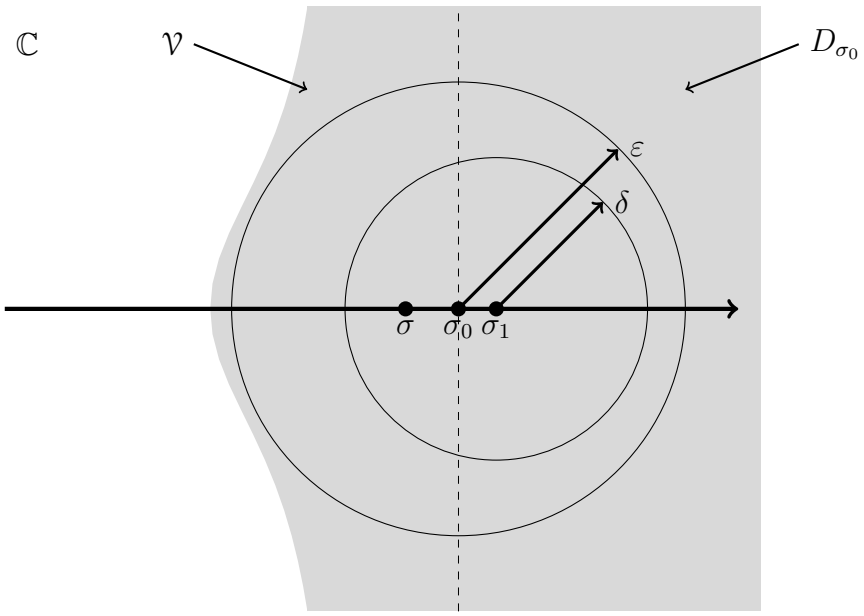
$$\sum_{p \text{ premier}} p^{-s} = \mathrm{Log}(\zeta(s)) + O(1) = \mathrm{Log}\left(\frac{1}{s-1}\Big(1 + o(1)\Big)\right) + O(1)$$

Puisque $\Re(s) > 1$, $(s-1)^{-1} \in D_0$, son argument principal est donc strictement inférieur à $\pi/2$ en valeur absolue. Pour s suffisamment proche de 1, le terme en $1+o(1)$ est aussi dans D_0, et on déduit que son argument principal est aussi strictement inférieur à $\pi/2$ en valeur absolue. Par conséquent, le logarithme principal de leur produit est la somme des logarithmes principaux, ce qui termine la preuve. □

Nous allons maintenant démontrer la proposition 31. Pour cela, commençons par démontrer un théorème dû à Landau sur les séries de Dirichlet à termes positifs, qui dit qu'elles ne peuvent être prolongées analytiquement au voisinage de leur abscisse de convergence (si elle est finie).

Théorème 33. *Soit $F(s) = \sum a_n n^{-s}$ une série de Dirichlet où tous les a_n sont positif et σ_0 un réel. Si la série converge pour tout réel strictement plus grand que σ_0, et si elle peut être prolongée analytiquement au voisinage de σ_0, alors son abscisse de convergence est strictement inférieure à σ_0.*

Démonstration. Soit $\varepsilon > 0$ tel que le disque ouvert centré en σ_0 et de rayon ε soit inclus dans le voisinage $\mathcal{V}$ de σ_0 où F se prolonge analytiquement. Il est clair que ce disque intersecte D_{σ_0} et $\mathcal{V} \cap \complement_{\mathbb{C}} D_{\sigma_0}$. Soit alors $\sigma_1 > \sigma_0$ vérifiant $|\sigma_1 - \sigma_0| < \varepsilon$, et $0 < \delta < \varepsilon$ tel que le disque de centre σ_1 et de rayon δ intersecte D_{σ_0} et $\mathcal{V} \cap \complement_{\mathbb{C}} D_{\sigma_0}$. Soit $\sigma < \sigma_0$ un réel qui se trouve dans cette intersection.



Construction de σ

Nous allons utiliser les développements en série entière et en série de Dirichlet de F en σ_1 pour montrer que la série de Dirichlet qui définit F converge en σ, ce qui achèvera la preuve de ce théorème. D'une part, on sait grâce à la proposition 22 que pour tout $k \geq 0$ entier,

$$F^{(k)}(\sigma_1) = \sum_{n \geq 1} a_n (-\ln(n))^k n^{-\sigma_1}.$$

Comme F se prolonge analytiquement au voisinage de σ_0, elle se développe en série entière en σ_1, développement dont le rayon de convergence est plus grand que δ. On peut donc évaluer la série entière de F au point σ_1 en σ ce qui donne

$$F(\sigma) = \sum_{k \geq 0} \frac{F^{(k)}(\sigma)}{k!} (\sigma - \sigma_1)^k = \sum_{k \geq 0} \sum_{n \geq 1} \frac{1}{k!} (\sigma - \sigma_1)^k a_n (-\ln(n))^k n^{-\sigma_1}$$

$$= \sum_{k \geq 0} \sum_{n \geq 1} \frac{1}{k!} (\sigma_1 - \sigma)^k a_n (\ln(n))^k n^{-\sigma_1}.$$

Comme $\sigma_1 > \sigma$ et que $a_n \geq 0$ pour tout n, les termes de cette double somme sont tous positifs, on utilise le théorème de Fubini pour intervertir les sommes, ce qui donne

$$F(\sigma) = \sum_{n\geq 1} a_n n^{-\sigma_1} \sum_{k\geq 0} \frac{1}{k!}((\sigma_1 - \sigma)(\ln(n)))^k.$$

Comme on reconnait en la seconde somme le développement en série entière de l'exponentielle, on peut alors écrire :

$$F(\sigma) = \sum_{n\geq 1} a_n n^{-\sigma_1} \exp(\ln(n)(\sigma_1 - \sigma)) = \sum_{n\geq 1} a_n n^{-\sigma}.$$

On déduit que la série de Dirichlet converge en σ, et que par conséquent l'abscisse de convergence de la série de Dirichlet qui définit F est strictement inférieure à σ_0. □

Remarque 11. Rappelons que si f est une fonction holomorphe définie sur un ouvert U du plan complexe, et si a est un point de U, le rayon de convergence de la série entière de f au point a ne dépend que de la *géométrie* de U. Pour $r > 0$ tel que le disque de centre a et de rayon r est contenu dans U, on sait que le rayon de convergence de la série entière de f au point a est alors plus grand que r, chose qui se voit quand on démontre qu'une fonction holomorphe est analytique. C'est cet argument qui nous permet de dire que le rayon de convergence de la série entière de F au point σ_1 dans la preuve précédente est plus grand que δ.

Proposition 31. *Soit χ un caractère de Dirichlet modulo b non trivial. Alors $L(\chi, 1) \neq 0$.*

Démonstration. On introduit dans un premier temps la fonction

$$\Xi(s) = \prod_{\chi} L(\chi, s) = \prod_{\chi} \prod_{p \text{ premier}} \left(1 - \chi(p)p^{-s}\right)^{-1} = \prod_{\chi} \prod_{p\nmid b} \left(1 - \chi(p)p^{-s}\right)^{-1},$$

définie et holomorphe sur D_1. L'idée de la preuve est de remarque que, comme il existe une fonction entière $C(s) = \prod_{p|b}\left(1 - p^{-s}\right)$ telle que $L(\chi_0, s) = C(s)\zeta(s)$ pour tout s dans D_1 (cela grâce au corollaire 25), par le lemme 32,

$$L(\chi_0, s) = \frac{C(s)}{s-1} + O(1) \tag{0.4}$$

quand s tend vers 1 avec $\Re(s) > 1$. Supposons qu'il existe χ_1 tel que la fonction $L(\chi_1, .)$ s'annule en 1. Dans ce cas, par le lemme de factorisation, on aurait qu'il existe une fonction g_{χ_1} holomorphe sur D_0 qui ne s'annule pas au voisinage de 1 et $m \in \mathbb{N}^*$ tels que pour tout s dans D_1,

$$\Xi(s) = g_{\chi_1}(s)(s-1)^m L(\chi_0, s) \prod_{\chi_0 \neq \chi \neq \chi_1} L(\chi, s).$$

En remplaçant $L(\chi_0, s)$ par (0.4), on obtient

$$\Xi(s) = \left(C(s)g_{\chi_1}(s)(s-1)^{m-1} + O(1)\right) \prod_{\chi_0 \neq \chi \neq \chi_1} L(\chi, s).$$

Cette expression de $\Xi(s)$ est bien définie pour $\Re(s) > 0$, laissant dire que Ξ se prolonge analytiquement sur D_0 (en effet, par la remarque 10 page 20, le $O(1)$ dans (0.4) est une fonction holomorphe sur D_0). Il suffit donc de montrer que Ξ ne se prolonge pas analytiquement sur D_0 pour montrer qu'aucun des $L(\chi, .)$ ne s'annule pour $\chi \neq \chi_0$. Pour cela, on va écrire Ξ comme une série de Dirichlet à termes positifs et appliquer le théorème 33 de Landau.

Comme $\Xi(s)$ est produit fini de fonctions L, on peut intervertir les deux produits et obtenir que

$$\Xi(s) = \prod_{p\nmid b} \prod_{\chi} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

Considérons alors $\phi_p : \widehat{\mathbb{Z}/b\mathbb{Z}^\times} \to \mathbb{C}^*$, $\chi \mapsto \chi(p)$ (où ici χ désigne avec abus le caractère de $\mathbb{Z}/b\mathbb{Z}^\times$ et le caractère de Dirichlet modulo b associé). On voit clairement que c'est un morphisme (un élément du bidual de $\mathbb{Z}/b\mathbb{Z}^\times$). Notons $\iota(p)$ l'entier naturel tel que $\mathrm{Im}(\phi_p)$ est isomorphe au groupe des racines $\iota(p)$-ièmes de l'unité. Notons $\kappa(p)$ le cardinal d'une classe modulo $\ker(\phi_p)$ (un sous-ensemble de $\widehat{\mathbb{Z}/b\mathbb{Z}^\times}$de la forme $\chi.\ker(\phi_p)$, qui sont tous de même cardinal par la preuve du théorème de Lagrange).

On peut ainsi regrouper les termes du produit qui porte sur les caractères en $\kappa(p)$ produits de la forme $\prod_{\omega^{\iota(p)}=1} \left(1 - \omega p^{-s}\right)^{-1}$. En utilisant la (quasi-évidente) identité polynomiale $\prod_{\omega^n=1} \left(1 - \omega X\right) = 1 - X^n$, on obtient que

$$\Xi(s) = \prod_{p\nmid b} \left(1 - p^{-\iota(p)s}\right)^{-\kappa(p)}.$$

Comme $p^{-\iota(p)s}$ est strictement inférieur à 1 en module, on peut remplacer le facteur général du produit par son développement en série géométrique, évaluée en $p^{-\iota(p)s}$, ce qui donne

$$\Xi(s) = \prod_{p\nmid b} \left(\sum_{j=0}^{\infty} p^{-\iota(p)js}\right)^{\kappa(p)}.$$

On voit bien que, en développant (par des arguments similaires à ceux de la proposition 24), on obtient une série de Dirichlet à coefficients positifs. De plus, étant donné que, par définition, $\iota(p) \leq \phi(b)$ et $\kappa(p) \geq 1$, alors pour σ réel tel que le produit qui définit $\Xi(\sigma)$ converge,

$$\Xi(\sigma) = \prod_{p\nmid b} \left(\sum_{j=0}^{\infty} p^{-\iota(p)j\sigma}\right)^{\kappa(p)} \geq \prod_{p\nmid b} \left(1 + p^{-\phi(b)\sigma}\right).$$

Le minorant exhibé diverge [1] en $\sigma = \frac{1}{\phi(b)}$, ce qui implique que la série de Dirichlet a une abscisse de convergence plus grande que $\frac{1}{\phi(b)}$, qui est strictement positive. Comme cette série de Dirichlet est à coefficients positifs, on déduit par le théorème 33 qu'elle ne se prolonge pas analytiquement au voisinage de son abscisse de convergence qui est plus grande que $\frac{1}{\phi(b)}$ et *a fortiori* sur D_0. De cela on déduit qu'aucune des fonctions $L(\chi, .)$ pour χ non trivial ne s'annule en 1.

□

1. il suffit de transformer le produit avec une exponentielle et un logarithme, puis de savoir que la série de terme général $\frac{1}{p}$ avec p premier diverge.

Conséquences et problèmes en théorie des nombres

« Een, twee, drie... », de rij dezer klanken kennen we uit ons hoofd als een reeks zonder einde [...].

Over de grondslagen der wiskunde – Luitzen Egbertus Jan Brouwer

Le théorème de la progression arithmétique amène bien des questions. Dans cette partie nous proposons d'en survoler certaines, sans preuves, dans le but de renseigner le lecteur sur les résultats récents qui entourent les nombres premiers dans les progressions arithmétiques. Nous mentionnerons aussi certains problèmes bien connus, tels que *l'hypothèse de Riemann* ou la conjecture *BSD*.

Question. Peut-on estimer le plus petit nombre premier congru à a modulo b ?

En 1944 le mathématicien Yuri Linnik démontre qu'il existe une façon de contrôler la valeur d'un tel nombre premier. Pour a, b deux entiers naturels premiers entre eux, soit $p_{a,b}$ le plus petit nombre premier congru à a modulo b.

Théorème (Linnik). *Il existe deux constantes strictement positives c et L telles que pour tous entiers naturels a et b premiers entre eux, $p_{a,b} < cb^L$.*

Les constantes qui interviennent dans cette majoration sont universelles, ce qui les rend particulièrement importantes d'autant plus qu'à l'heure actuelle nous ne disposons pas d'un majorant plus précis. Linnik démontra également que les constantes c et L sont calculables, mais ne donna pas de valeurs précises. En 1957 le mathématicien Pan Chengdong démontre que la valeur de L est inférieure à 10^4, puis à partir de là la borne a été abaissée jusqu'en 2018 où le mathématicien Trian Xylouris démontre qu'il existe une borne strictement inférieure à 5 (voir [**5**]).

Les problèmes liés aux nombres premiers dans les suites arithmétiques sont aussi connectés à des problèmes plus généraux et bien connus. Dans la suite, on note ζ la fonction méromorphe sur le demi-plan des parties réelles strictement positives privé de 1 obtenue par prolongement de la série de Dirichlet $\sum_n n^{-s}$ (voir remarque 10 page 20). On note aussi que par le corollaire 25, les fonctions L associées au caractère trivial modulo b se prolongent elles aussi sur ce domaine, ce qui donne un sens aux (très importantes) conjectures suivantes.

Conjecture (Hypothèse de Riemann). Soit s un nombre complexe de partie réelle strictement positive tel que $\zeta(s) = 0$, alors $\Re(s) = \frac{1}{2}$.

Conjecture (Hypothèse de Riemann généralisée). Soit χ un caractère de Dirichlet modulo b et s un nombre complexe de partie réelle strictement positive tel que $L(\chi, s) = 0$, alors $\Re(s) = \frac{1}{2}$.

On notera pour simplifier *RH* la première conjecture, et *GRH* la seconde.

Sous l'hypothèse que *GRH* est vraie, on peut démontrer que

$$p_{a,b} < \phi(b)^2 \ln(b)^2, \tag{0.5}$$

où ϕ désigne l'indicatrice d'Euler. Étant donné que pour tout entier naturel non nul n, $\phi(n) \leq n$ et que $\ln(n) \leq n$, $p_{a,b} < b^4$, ce qui est bien pire que (0.5), certes, mais ce qui renseigne considérablement sur les valeurs minimales de c et de L. Il est même conjecturé bien mieux sur ces deux constantes.

Conjecture. Les constantes c et L de Linnik vérifient $c \leq 1$ et $L \leq 2$.

Question. Comment les nombres premiers se répartissent-ils dans une classe de congruence modulo b ?

Soit $\mathcal{P}$ l'ensemble des nombres premiers. Étant donné un sous-ensemble $\mathcal{A}$ de nombres premiers, on définit deux notions de densité.

Définition. On appelle *densité analytique* de $\mathcal{A}$ la limite suivante (quand elle existe) :

$$d(A) := \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{A}} p^{-s}}{\sum_{p \in \mathcal{P}} p^{-s}}.$$

Définition. On appelle *densité naturelle* de $\mathcal{A}$ la limite suivante (quand elle existe) :

$$\hat{d}(A) := \lim_{n \to \infty} \frac{\mathrm{Card}(\{p \in \mathcal{A}, p \leq n\})}{\mathrm{Card}(\{p \in \mathcal{P}, p \leq n\})}.$$

Il est clair que le théorème de la progression arithmétique équivaut à l'inégalité $d(\mathcal{P}_{a,b}) > 0$ quand a et b sont premiers entre eux (et on sait qu'elle vaut $\frac{1}{\phi(b)}$). Introduisons maintenant la fonction de comptage des nombres premiers.

Définition. On appelle *fonction de comptage des nombres premiers* la fonction $\pi : \mathbb{R}^+ \to \mathbb{N}$ définie par

$$\pi : x \to \mathrm{Card}\{p \in \mathcal{P}, p \leq x\}.$$

Définition. Soit a et b des entiers naturels premiers entre eux. On appelle *fonction de comptage des nombres premiers congrus à a modulo b* la fonction $\pi(\,.\,, a, b) : \mathbb{R}^+ \to \mathbb{N}$ définie par

$$\pi(\,.\,, a, b) : x \to \mathrm{Card}\{p \in \mathcal{P}_{a,b}, p \leq x\}.$$

Théorème (Dirichlet quantitatif). On a l'équivalent suivant quand x tend vers l'infini :

$$\pi(x, a, b) \sim \frac{\pi(x)}{\phi(b)}.$$

En d'autres termes, il y a environ un nombre premier sur $\phi(b)$ qui est congru à a modulo b, ou encore, $\hat{d}(\mathcal{P}_{a,b}) = \frac{1}{\phi(b)}$.On peut encore être plus précis, et utiliser le théorème suivant.

Théorème (des nombres premiers). On a l'équivalent suivant quand x tend vers l'infini :

$$\pi(x) \sim \frac{x}{\ln(x)}.$$

On obtient alors l'équivalent quand x tend vers l'infini :

$$\pi(x, a, b) \sim \frac{x}{\phi(b)\ln(x)}.$$

Question. Quels rôles les fonctions L ont-elles encore à jouer ?

Cette question est d'un ordre plutôt philosophique, mais elle a tout autant sa place que les autres dans la mesure où, dans leur intégralité, les résultats énoncés dans cette partie se démontrent tous avec des techniques d'analyse complexe poussées et avec les fonctions L associées aux caractères de Dirichlet modulo b. Les fonctions L se démarquent ainsi dans de nombreux résultats liés au théorème de la progression arithmétique. Elles font même l'objet d'un problème du millénaire !

Il ne semble pas exister de consensus (et *a fortiori* de définition) sur ce qu'est une fonction L, mais la terminologie est utilisée dans d'autres domaines où de telles fonctions sont ainsi nommées, mais où leur comportement diffère quelque peu des fonctions L de Dirichlet. Par exemple dans l'étude des courbes elliptiques l'on rencontre de telles fonctions qui font l'objet d'un (autre) problème du millénaire.

Conjecture (Birch et Swinnerton-Dyer). Le rang d'une courbe elliptique est égal à l'ordre d'annulation en 1 de la fonction L associée.

La conjecture BSD tente de faire un lien entre un objet analytique (une fonction L) et un objet algébrique (un groupe abélien de type fini), tous deux reliés à une même courbe elliptique. Nous ne nous épancherons cependant pas sur le sujet au vu de son incroyable complexité qui dépasse (de très loin) l'objectif initial de ce document. De même nous ne ferons que mentionner l'existence de la *théorie des motifs* dans laquelle interviennent de telles fonctions. Tout cela pour mettre en avant l'idée que tous les objets introduits dans ce document possèdent une myriade d'apparitions dans d'autres domaines et d'autres théories, même si nous n'avons pas non plus mentionné une application importante des caractères qui est la *transformée de Fourier discrète*, ou l'utilisation de la fonction ζ dans les problèmes qui concernent la cryptographie et les nombres premiers, par exemple.

Notes

Quand j'étais au collège et que pour la première fois j'étudiai les nombres premiers, notre professeur nous donna un jeu à réaliser à deux. Nous devions tour à tour construire une suite finie et injective de nombres entiers $(a_n)_{n\in\mathbb{N}}$ compris entre 1 et 100 dont le premier terme a_0 est choisi arbitrairement, et tel que pour tout n, $a_{n+1} \mid a_n$ ou $a_n \mid a_{n+1}$. L'objectif est de bloquer l'autre joueur en choisissant un entier naturel qui respecte les critère de construction de la suite et tel qu'aucun autre ne pourra compléter la suite. Par exemple : $1 \to 2 \to 6 \to 3 \to 9 \to 27 \to 81$ est une suite pour laquelle le joueur rouge est gagnant. Notre professeur nous mit au défi d'imaginer la partie la plus longue possible, c'est-à-dire la plus longue suite d'entiers valide (selon les règles imposées ci-dessus). Je tentai de résoudre ce problème de façon irréfléchie dans un premier temps afin de tester sa difficulté. À mesure que je continuais à chercher la plus longue suite possible, je me rendis compte que les nombres premiers jouaient un rôle central dans ce problème. Je décidai donc d'en retenir par cœur le plus possible, ceci me permit de construire une suite longue de 58 termes. Je commençais alors à nourrir un intérêt pour ces nombres, car bien que loin d'être insurmontable, ce problème faisait preuve d'une difficulté exotique qui lui suscita tout mon intérêt.

J'appris d'ailleurs plus tard que ce jeu se nomme le *Juniper Green*.

Plus tard, au lycée, j'appris l'existence de la fonction ζ et des problèmes connus qui l'entourent notamment grâce au travail de très respectables vulgarisateurs sur internet [2]. Je fus d'abord fasciné par ma quasi-totale incompréhension de ces objets, ce qui me poussa dans une forme de recherche personnelle qui visait à mieux les comprendre (mes investigations personnelles me poussèrent à trouver des résultats « faux » dont j'étais convaincu d'une forme de véracité tels que $\sum_{k=0}^{\infty} 2^k = -1$ ou encore $\sum_{k=1}^{\infty} k = -1/12$). Je fus également ébahi quand j'appris certains résultats de probabilités (dont l'énoncé ici présent est ambigu) tels que : *la probabilité que deux entiers tirés au hasard soient premiers entre eux est de* $6/\pi^2$ et sa généralisation pour n entiers naturels tirés au hasard (où la « probabilité » devient $1/\zeta(n)$). Quand je tombai sur une vidéo de Numberphile où la constante $\zeta(3)$ (dite constante d'Apéry) était calculée par une expérience menée sur le réseau social (feu) Twitter, je commençai naïvement à tenter de trouver une forme explicite pour cette constante (travail qui me conduisit à la somme déjà connue : $\sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^3} = \frac{\pi^3}{32}$).

En classe de première je cherchai à trouver une formule pour calculer le n-ième nombre premier ($n \in \mathbb{N}$ donné). Je commençai par étudier la suite des différences entre deux nombres premiers consécutifs, sans succès. Par la suite j'eus l'idée d'étudier la suite des différences de leurs carrés, et me rendis assez vite compte que pour un nombre premier p plus grand que 5, et pour p' son suivant, la différence $p'^2 - p^2$ est toujours un multiple de 6. Je réalisai que cela était vrai pour tous les nombres premiers inférieurs à 10^5 par ordinateur, puis je notai cette conjecture, sans parvenir à montrer qu'elle était vraie. Une des conséquences que j'avais remarquée est que pour p un nombre premier plus grand que 5, il suffit d'ajouter 6 un certain nombre de fois à p ou à $-p$ pour retomber sur p'. Je tentai alors d'étudier ce fameux « nombre de fois » afin de voir s'il n'avait pas un comportement prévisible, mais j'abandonnai vite face au chaos numérique auquel je fis face.

L'histoire reprend son cours il y a 8 mois quand je me suis remémoré ma conjecture. Je décidai donc d'écrire un mail à M. Germoni (qui eut toujours répondu à mes questions depuis le début de l'année) afin de lui demander ce qu'il pensait de ma conjecture. Il me répondit le soir même en me donnant une démonstration rapide de ladite conjecture, tout en me renseignant sur le fait que c'était quelque chose de connu.

2. Jérôme COTTANCEAU, Lê Nguyên Hoang, David LOUAPRE pour citer ceux qui m'ont le plus marqué.

Soit p un nombre premier plus grand que 5 et p' son suivant. Comme les seuls inversibles modulo 6 sont 1 et 5, p est congru à 1 ou 5 modulo 6, et il en va de même pour p'. De cela on déduit que l'un des deux nombres $p + p'$ ou $p' - p$ est un multiple de 6, donc *a fortiori* le nombre $(p + p')(p' - p) = p'^2 - p^2$.

C'est suite à cette question et aux interrogations qui en découlèrent que M. Germoni me proposa d'effectuer ce stage de recherche, au cours duquel nous travaillâmes sur les questions qui entourent les nombres premiers dans les progressions arithmétiques, et qui aboutit à la démonstration du théorème de Dirichlet. Il a été difficile de ne pas ajouter toutes les digressions qui ont eu lieu lors de nos nombreuses discussions. C'est ici que je tiens à remercier M. Germoni pour l'intérêt qu'il a accordé à mes nombreuses questions ainsi que pour le temps qu'il m'a accordé, mais encore et surtout pour toutes les choses qu'il m'a apprises, sur le plan mathématique principalement mais aussi sur le plan rédactionnel et sur celui de la réflexion.

Juin 2025

Références

[1] Marc Hindry (2008) *Arithmétique*, Calvage et Mounet.

[2] Martin Aigner & Günter M. Ziegler (2010) *Raisonnements Divins*, Springer.

[3] Keith Konrad, *Euclidian proofs of Dirichlet's theorem*, [link].

[4] D.R. Heath-Brown, *Zero-Free Regions for Dirichlet L-Functions, and the Least Prime in an Arithmetic Progression*, [link].

[5] Wikipedia, *Linnik's theorem*, [link].