LE Λ-CALCUL DE GOLOMB ET LA CONJECTURE DE BATEMAN-HORN

par

Marc Hindry et Tanguy Rivoal

« Les mathématiciens ont tâché jusqu'ici en vain à découvrir un ordre quelconque dans la progression des nombres premiers, et on a lieu de croire que c'est un mystère auquel l'esprit humain ne saurait jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers, que quelques personnes se sont donné la peine de continuer au-delà de cent-mille : et on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle. » – L. Euler [**20**].

1. Introduction

La répartition des nombres premiers et plus précisément la répartition de nombres premiers d'une forme déterminée est un sujet ancien et central en théorie des nombres. Un des premiers résultats obtenu par la voie de l'analyse complexe est le théorème de la progression arithmétique de Dirichlet [**19**] dont une version affinée due à de la Vallée-Poussin [**52**] s'énonce comme suit.

Théorème 1 (Dirichlet, de la Vallée-Poussin). — *Soient des entiers $a, b \geq 1$ tels que $(a, b) = 1$. On a*

$$\pi_{aX+b}(x) = \#\left\{n \leq x : an + b \text{ est premier}\right\} \sim \frac{a}{\varphi(a)} \cdot \frac{x}{\log(x)},$$

où $\varphi(a) = \left\{1 \leq n \leq a \ : (a, n) = 1\right\} = a \prod_{p \,|\, a} \left(1 - \frac{1}{p}\right)$ est la fonction indicatrice d'Euler.

Le fait que $\pi_{aX+b}(x)$ tende vers l'infini est dû à Dirichlet [**19**] et le théorème des nombres premiers (cas $a = 1$) a été prouvé simultanément et indépendamment par Hadamard [**25**]. Une variante du théorème indique que $\#\{p \text{ premier} \leq x : p = an + b,\ n \in \mathbf{N}\}$, a le même comportement asymptotique que $x/(\varphi(a)\log(x))$.

***Classification mathématique par sujets* (2000).** — Primaire 11N32 ; Secondaire 11M45, 11R42.

Ce résultat possède de nombreuses applications. Par exemple, bien avant que Dirichlet ne démontre son théorème, Legendre avait indiqué comment en déduire la loi de réciprocité quadratique, finalement démontrée inconditionnellement par Gauss. L'existence même d'un nombre premier du type $an+b$ (pour tout a, b premiers entre eux) est également un point clef de la preuve du théorème de Hasse-Minkowski : « *Une quadrique possède un point rationnel sur un corps de nombres* $\mathbf{K}$ *si et seulement si elle possède un point rationnel sur tous les complétés* $\mathbf{K}_v$*, lorsque* v *décrit les places de* $\mathbf{K}$ ». On dit qu'une famille de variétés algébriques vérifie le principe de Hasse si chacun de ses membres possède un point rationnel sur un corps de nombres $\mathbf{K}$ si et seulement s'il possède un point rationnel sur tous les complétés $\mathbf{K}_v$; il existe de nombreux contre-exemples au principe de Hasse, par exemple les courbes ou surfaces lisses cubiques.

Schinzel [**44**] a proposé une conjecture qualitative très générale concernant les valeurs premières simultanément prises par une famille finie des polynômes de $\mathbf{Z}[X]$. Cette conjecture permettrait notamment de faire de grands progrès sur les conditions de validité du principe de Hasse (voir par exemple [**12, 13**]). La conjecture de Schinzel a ensuite été précisée de façon quantitative par Bateman et Horn dans [**3**] à l'aide d'un raisonnement heuristique et leur estimation est très bien confirmée numériquement. En dehors du cas d'un seul polynôme de degré 1 (Théorème 1 ci-dessus), la conjecture de Schinzel semble totalement hors de portée à l'heure actuelle : pour situer son niveau de difficulté, indiquons que sa démonstration aurait comme corollaires l'infinité des nombres premiers jumeaux et celle des nombres premiers de la forme n^2+1.

Golomb [**24**] a développé une approche très intéressante et apparemment peu connue de la conjecture des nombres premiers jumeaux, basée sur le comportement au voisinage de $z=1$ de la série entière

$$\sum_{n=1}^{\infty} \Lambda(2n-1)\Lambda(2n+1)z^{2n},$$

où Λ désigne la fonction de von Mangolt, familière en théorie analytique des nombres. Une seule étape analytique (l'interversion d'une limite et d'une série) empêche Golomb de parvenir à son but. Néanmoins, en admettant cette étape, il esquisse comment obtenir l'estimation asymptotique, lorsque $x \to +\infty$,

$$\#\big\{1 \le n \le x \ : \ n \text{ et } n+2 \text{ sont premiers}\big\} \sim 2\prod_{p\ge 3}\left(1-\frac{1}{(p-1)^2}\right)\cdot\frac{x}{\log^2(x)},$$

conjecture bien connue et obtenue habituellement de façon heuristique (voir les références données au paragraphe 3). Dans [**14**], Conrad a adapté la méthode de Golomb, que pour des raisons évidentes nous appellerons Λ-calcul, au cas de la conjecture de Bateman-Horn. Pour cela, il n'a pas utilisé une série entière comme ci-dessus mais une série de Dirichlet, ce qui est la démarche classique en théorie analytique des nombres : par exemple dans le cas des nombres premiers jumeaux, il étudie le comportement de $\sum_{n=1}^{\infty}\Lambda(2n-1)\Lambda(2n+1)/n^s$ au voisinage de la droite $\mathrm{Re}(s)=1$.

L'analyse de Conrad est assez délicate et nous nous proposons ici de la reprendre dans le cadre des séries entières, qui nous semble un peu plus simple et plus frappant. Nous justifions autant que possible les diverses étapes du Λ-calcul, ce qui nous amènera à démontrer divers résultats, que nous espérons nouveaux pour certains, concernant les identités entre fonctions arithmétiques, la théorie algébrique des nombres et les fonctions zêta de Dedekind, la théorie analytique des nombres, les théorèmes taubériens, etc. Finalement, modulo une seule étape analytique non justifiée, on retrouvera exactement le comportement prédit par la conjecture de Bateman-Horn. Il est intéressant de noter que, bien que l'approche de Conrad par série de Dirichlet présente des similitudes avec celle que nous développons ici, il n'est pas du tout clair que les étapes non justifiées dans chaque cas soient logiquement équivalentes.

Nous agrémentons également l'article de discussions historiques. Il nous semble en effet intéressant de mettre en évidence la puissance heuristique du Λ–calcul, en particulier face aux heuristisques de nature probabiliste (dont on montrera qu'elles ont même pu suggérer des conjectures fausses) ou face à celles de nature analytique issues de la méthode du cercle de Hardy-Littlewood-Ramanujan (en général techniquement compliquées).

Le plan est le suivant. Au paragraphe 2, nous énonçons les conjectures de Schinzel et Bateman-Horn. Au paragraphe 3, nous reproduisons l'heuristique proposée dans [**3**] et la comparons à d'autres produites au fil du temps. Au paragraphe 4, nous réduisons la conjecture à un cas plus simple, qui nous permet de développer le Λ-calcul au paragraphe 5. À cet endroit, sont indiqués tous les paragraphes concernant les justifications nécessaires à la (presque) bonne marche de la méthode de Golomb : certains des résultats démontrés recoupent des travaux de Baier [**1**], Conrad [**14**] et Kurokawa [**34, 35**]. Cette démarche peut être complètement justifiée dans le cas du théorème des nombres premiers (Wiener) ou, plus généralement, dans le cas du théorème de de la Vallée-Poussin – ceci est exposé au paragraphe 12. Enfin, au paragraphe 13, nous concluons l'article en décrivant certaines heuristiques malheureuses produites au sujet de la conjecture de Goldbach : bien que la méthode de Golomb ne s'applique pas aussi élégamment à ce cas, nous montrons comment l'adapter et retrouvons une conjecture classique de Hardy et Littlewood [**28**].

2. Les conjectures de Schinzel et de Bateman-Horn

Considérons k polynômes $f_1, f_2, \dots, f_k$ de $\mathbf{Z}[X]$, de degrés respectifs $h_1, h_2, ..., h_k$. Notons $h = h_1 + h_2 + \cdots + h_k$, $f = f_1 f_2 \cdots f_k$, $\underline{f} = (f_1, \dots, f_k)$ et $\mathbf{K}_j$ le corps de nombres $\mathbf{Q}[X]/(f_j(X))$. Dans toute la suite, la notation « $a \,|\, b$ » signifie que a divise b et p désigne invariablement un nombre premier ≥ 2, ce qui vaut lorsqu'un produit infini porte sur p sans autre indication. On s'intéresse au comportement asymptotique de

$$\pi_{\underline{f}}(x) = \#\big\{1 \leq n \leq x \ : f_1(n), f_2(n), \dots, f_k(n) \text{ sont simultanément premiers}\big\},$$

ce qui conduit à chercher des conditions *a priori* nécessaires pour que $\pi_{\underline{f}}(x)$ ne soit pas bornée :

(*i*) Les polynômes f_j doivent tous être irréductibles sur $\mathbf{Q}$: si l'un ne l'est pas, il ne peut pas prendre une valeur première en n dès que n est assez grand. On suppose aussi qu'il n'existe pas deux entiers distincts i, j tels que $f_i = \pm f_j$.

(*ii*) Pour tout premier p, il existe un entier n tel que p ne divise pas $f(n)$.

(*iii*) En changeant au besoin un ou plusieurs f_j en $-f_j$ et par une translation de la variable commune aux f_j, on peut supposer que pour tout entier $n \geq 1$, les entiers $f_1(n), f_2(n), \ldots, f_k(n)$ sont tous > 1 : la valeur de $\pi_{\underline{f}}(x)$ n'est changée que d'une fonction bornée de x. Ces conditions sont commodes mais pas nécessaires. [(1)]

On qualifiera de *convenable* toute famille vérifiant ces conditions. La deuxième étant moins évidente, nous allons la motiver davantage. Supposons, au contraire, qu'il existe un premier p divisant $f(n)$ pour tout entier $n \geq 1$. Alors, pour tout (éventuel) entier $n \geq 1$ tel que tous les $f_j(n)$ sont premiers, au moins un des $f_j(n)$ vaut p, ce qui implique immédiatement qu'il y a au plus h entiers n tels que les $f_j(n)$ soient tous premiers simultanément. Pour tout entier $d \geq 1$ et tout $g \in \mathbf{Z}[X]$, posons $N_g(d) = \#\big\{1 \leq n \leq d \ : g(n) \equiv 0\,[d]\big\}$. On peut alors remplacer la condition (*ii*) par la suivante :

(*ii* bis) Pour tout nombre premier p, on a $N_f(p) < p$.

En effet, supposons qu'il existe un p tel que $N_f(p) = p$. Cela signifie alors que pour tout entier n dans l'une des classes de congruences $m + \mathbf{N}p$ (pour un $m = 0, \ldots, p-1$), p divise $f(n)$ puisque $f(n) \equiv f(m) \equiv 0[p]$. Donc pour tout entier $n \geq 1$, p divise $f(n)$. Et réciproquement. On remarque que $N_f(p) \leq \min(h, p)$ et qu'il suffit donc de faire un nombre fini de calculs pour les premiers $p \leq h$ pour vérifier la condition (*ii* bis).

Schinzel [**44**, p. 188] a conjecturé que, réciproquement, si une famille de polynômes est convenable, alors ces polynômes prennent une infinité de fois des valeurs premières simultanément.

Conjecture 1 (Schinzel). — *Soit $\underline{f}$ une famille convenable. Alors $\pi_{\underline{f}}(x)$ tend vers l'infini avec x.*

Dans le cas d'un seul polynôme, cette conjecture est due à Bouniakowsky [**6, 37**] ; dans le cas de plusieurs polynômes linéaires, elle est due à Dickson [**18**]. Si l'on remplace l'anneau $\mathbf{Z}$ par un anneau de polynômes sur un corps fini, alors la conjecture « trivialement » analogue à celle de Bouniakowsky est fausse : voir [**15**], ainsi que [**16**] pour une correction (conjecturale). Dans [**3**], Bateman et Horn ont proposé une heuristique précisant de façon quantitative la conjecture de Schinzel ; pour la formuler, on a besoin du produit

[(1)] La mise en oeuvre de la méthode de Golomb nécessite de se placer sous (*iii*) ainsi que de faire une autre hypothèse, *a priori* assez restrictive (voir paragraphe 4) ; on montrera a Théorème 3 que l'on ne perd en fait rien en généralité.

$$C(\underline{f}) = \prod_p \left(\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_f(p)}{p}\right) \right),$$

dont Bateman et Horn justifient la convergence, ce que nous ferons également au sous-paragraphe 7.3. Il en découle en particulier que $C(\underline{f})$ est non-nul si $N_f(p) < p$ pour tout p.

Conjecture 2 (Bateman-Horn). — *Soit $\underline{f}$ une famille convenable. Lorsque $x \to +\infty$, on a*

$$\pi_{\underline{f}}(x) \sim \frac{C(\underline{f})}{h_1 h_2 \cdots h_k} \cdot \frac{x}{\log^k(x)}.$$

On notera $\mathbf{BH}(\underline{f})$ la conjecture de Bateman-Horn pour la famille $\underline{f}$. Lorsque $k = 1$ et en notant a le coefficient dominant de $f_1 = f$, $\mathbf{BH}(\underline{f})$ implique que

$$\#\big\{p \leq x \ : p \in f(\mathbf{N})\big\} \sim \frac{C(\underline{f})}{a^{1/h}} \cdot \frac{x^{1/h}}{\log(x)}.$$

La conjecture de Bateman-Horn contient la conjecture des nombres premiers jumeaux, via la famille de polynômes $\underline{f} = (X, X+2)$. [(2)] Plus généralement, on peut s'intéresser aux couples de nombres premiers (p, q) tels que $q = p + 2k$, pour un entier $k \geq 1$ fixé, qui sont régis par $\mathbf{BH}(X, X + 2k)$. On a $N_{X(X+2k)}(p) = 1$ si $p \,|\, 2k$ et $N_{X(X+2k)}(p) = 2$ sinon. Après simplification de la constante $C(X(X + 2k))$, on obtient une conjecture de Hardy et Littlewood [**28**] (obtenue par une heuristique analytique issue de la méthode du cercle), qui précise celle de de Polignac [**41**] : « *Tout nombre pair peut s'écrire d'une infinité de façons différentes comme la différence de deux nombres premiers* ».

Conjecture 3 (Hardy-Littlewood). — *Soit un entier kge1 fix'e. Lorsque $x \to +\infty$,*

$$\#\big\{1 \leq n \leq x \ : \ n \text{ et } n + 2k \text{ premiers}\big\} \sim 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \cdot \prod_{\substack{p \mid k \\ p \geq 3}} \frac{p-1}{p-2} \cdot \frac{x}{\log^2(x)}.$$

Hardy et Littlewood [**28**] ont aussi prédit le comportement attendu des nombres premiers de la forme $n^2 + 1$, problème considéré par Landau dans une conférence à Cambridge. On retrouve cette prédiction en calculant la constante prévue par $\mathbf{BH}(X^2+1)$. Comme -1 est résidu, resp. non résidu, quadratique modulo $p \equiv 1\,[4]$, resp. $p \equiv 3\,[4]$ (voir [**29**, Theorem 82, p. 69]), on a $N_{X^2+1}(p) = 2$ si $p \equiv 1\,[4]$ et $N_{X^2+1}(p) = 0$ si $p \equiv 3\,[4]$. Comme $N_{X^2+1}(2) = 1$, après simplification de $C(X^2 + 1)$, on obtient donc la formulation suivante.

Conjecture 4 (Hardy-Littlewood). — *Lorsque $x \to +\infty$,*

$$\#\big\{1 \leq n \leq x \ : \ n^2 + 1 \text{ premier}\big\} \sim \frac{1}{2} \prod_{p \geq 3} \left(1 - \frac{(-1)^{(p-1)/2}}{p-1}\right) \cdot \frac{x}{\log(x)}.$$

(2) On utilise le choix classique $f_1(X) = X$ et $f_2(X) = X + 2$ à la place de $f_1(X) = X + 1$ et $f_2(X) = X + 3$, qui satisfont à la condition que les polynômes prennent des valeurs > 1 aux entiers positifs : en dehors du Λ-contexte, on néglige cette subtilité.

Hormis l'évidence numérique et le Théorème 1, on peut mentionner le résultat suivant prouvé dans [**4**] en utilisant le « Grand Crible ». On en donnera la preuve au paragraphe 11.

Théorème 2 (Bateman-Stemmler). — *On a la majoration*

$$\pi_{\underline{f}}(x) \leq k!\, 2^k\, C(\underline{f})\, x \log^{-k}(x)(1+o(1)).$$

Ainsi, on dispose d'une majoration qui, à la constante $h_1 \cdots h_k\, k!\, 2^k$ près, est équivalente à celle conjecturée. Bateman et Horn proposent également une extension de leur conjecture au cas plus général des polynômes qui envoient $\mathbf{Z}$ dans $\mathbf{Z}$. En suivant la présentation de Conrad [**14**], il suffit, au moins conjecturalement, de remplacer dans la formule définissant $C(\underline{f})$ les termes $N_f(p)/p$ par $\delta_f(p) = \text{mesure}\{x \in \mathbf{Z}_p : f(x) \equiv 0[p]\}$. Nous préférons nous limiter au cas des polynômes à coefficients entiers par soucis de clarté (voir néanmoins la remarque à la fin du paragraphe 4).

3. L'heuristique de Bateman et Horn

Nous reproduisons ici les raisons qui ont amené Bateman et Horn à formuler leur conjecture. En vertu du théorème des nombres premiers, la chance qu'un entier $m \geq 2$ soit premier est environ $1/\log(m)$. Comme $\log\big(f_j(n)\big)$ vaut environ $h_j \log(n)$, la chance que $f_1(n), f_2(n), \ldots, f_k(n)$ soient simultanément premiers est environ

$$\frac{1}{h_1 h_2 \cdots h_k} \cdot \frac{1}{\log^k(n)}. \tag{1}$$

Cette estimation est imprécise puisqu'elle suppose que les entiers $f_1(n), f_2(n), \ldots, f_k(n)$ sont « indépendants », ce qui n'est pas raisonnable. Pour chaque premier p, il semble en fait nécessaire de multiplier (1) par un facteur correctif r_p/s_p, où r_p est la chance que, pour un entier n aléatoire, aucun des entiers $f_1(n), f_2(n), \ldots, f_k(n)$ ne soit divisible par p et s_p est la chance qu'aucun des entiers constituant un k-uplet d'entiers aléatoires ne soit divisible par p. Or

$$r_p = 1 - \frac{N_f(p)}{p} \quad \text{et} \quad s_p = \left(1 - \frac{1}{p}\right)^k.$$

Avec cette correction, il est maintenant raisonnable d'estimer que pour n entier aléatoire, la chance que $f_1(n), f_2(n), \ldots, f_k(n)$ soient tous premiers est

$$\frac{C(\underline{f})}{h_1 h_2 \cdots h_k} \cdot \frac{1}{\log^k(n)}.$$

On en déduit que $\pi_{\underline{f}}(x)$ doit être de l'ordre de

$$\frac{C(\underline{f})}{h_1 h_2 \cdots h_k} \sum_{2 \leq n \leq x} \frac{1}{\log^k(n)},$$

ce qui est une façon d'écrire la conjecture de Bateman-Horn, puisque

$$\sum_{2\leq n\leq x}\frac{1}{\log^k(n)}\sim\int_2^x\frac{\mathrm{d}t}{\log^k(t)}\sim\frac{x}{\log^k(x)}.$$

Cette heuristique semble simple et naturelle mais elle a mis beaucoup de temps à être dégagée. Il existe dans la littérature de nombreux articles antérieurs qui exposent des arguments en faveur, par exemple, de la conjecture des nombres premiers jumeaux (Hardy et Wright [**29**, pp. 371–373]) ou des nombres premiers jumeaux généralisés (Cherwell [**10**], Cherwell et Wright [**11**], Pólya [**42**]). Ils se caractérisent en général par des arguments arithmético-probabilistes assez compliqués et on peut trouver au moins deux raisons théoriques à cela :

(i) Contrairement à ce que laisse espérer l'intuition, il n'existe aucune mesure de probabilité μ définie sur la tribu des parties de $\mathbf{N}$ telle que, pour tout entier $a\geq 1$, on ait $\mu(a\mathbf{N})=1/a$. On trouvera la preuve (facile et instructive) de ce résultat dans [**50**, p. 271]. Ceci explique peut-être pourquoi Bateman et Horn parlent de *chance* et non de *probabilité*; notons que lorsque $k=1$, Baier [**2**] a récemment construit un modèle assez fin de nombres premiers aléatoires dans lequel leur conjecture est vraie presque sûrement.

(ii) Si l'on persiste à employer des méthodes d'inspiration probabiliste, alors une contradiction peut rapidement survenir. En effet, par le théorème des nombres premiers, on peut estimer que la chance qu'un entier N soit premier est environ $1/\log(N)$. Mais, par ailleurs, on peut aussi estimer que la chance que N ne soit divisible par aucun nombre premier inférieur à N donc soit premier, vaut environ

$$\prod_{p<N}\left(1-\frac{1}{p}\right)\sim\frac{e^{-\gamma}}{\log(N)},\tag{2}$$

où l'équivalent asymptotique est un théorème de Mertens [**39**] et γ est la constante d'Euler. Bien que souvent utilisées au cours d'un même argument heuristique, ces deux estimations sont visiblement incompatibles puisque $e^{-\gamma}\neq 1$. Notons au passage que la divergence vers 0 du produit dans (2) intervient dans la démontration du résultat mentionné en (i).

Dans l'heuristique proposée par Hardy et Wright [**29**] concernant le comportement des nombres premiers jumeaux, il est amusant de lire « *But this is false* » en haut de la page 372 après une utilisation de l'équivalent (2), puis de voir, en haut de la page 373, ce même équivalent ponctuer la démarche tortueuse corrigeant la première utilisation fautive de (2). Quelles que soient les circonvolutions linguistiques employées pour faire « coller » heuristique et données numériques, ce qui rend plausible (conjecturalement) ce type d'argument est l'utilisation de probabilités conditionnelles : en effet, la bonne question n'est pas « Avec quelle fréquence deux nombres de la forme $n, n+2$ sont-ils simultanément premiers ? » mais plutôt « Avec quelle fréquence deux nombres sont-ils simultanément premiers sachant qu'ils

sont de la forme $n, n+2$? ». Cela sous-tend l'heuristique de [**29**] (malgré sa difficulté) et, de façon beaucoup plus claire, celle de Bateman et Horn.

Nous reviendrons au paragraphe 13 sur le sort de certaines heuristiques liées à la conjecture de Goldbach.

4. Une hypothèse simplificatrice

Afin d'appliquer la méthode de Golomb à la conjecture de Bateman-Horn, il est commode de supposer en plus que *pour tout entier $n \geq 1$ et pour tout couple d'entiers (i,j) tels que $1 \leq i < j \leq k$, les entiers $f_i(n)$ et $f_j(n)$ sont premiers entre eux.* Cette condition, que l'on dénommera hypothèse F, [(3)] est *a priori* contraignante puisqu'elle exclut le cas des polynômes $f_1(X) = X+1$ et $f_2(X) = X+3$. Cependant, elle s'avère innocente.

Théorème 3. — *Si* $\mathbf{BH}(\underline{f})$ *est vraie pour toute famille* $\underline{f}$ *convenable vérifiant l'hypothèse F, alors* $\mathbf{BH}(\underline{f})$ *est vraie pour toute famille* $\underline{f}$ *convenable.*

Démonstration. — Soient $f_1, f_2, \cdots, f_k$ des polynômes vérifiant les hypothèses de la conjecture de Bateman-Horn. Ces polynômes étant deux à deux premiers entre eux, pour tout couple d'entiers (i,j) tels que $1 \leq i < j \leq k$, il existe deux polynômes $u_{i,j}$ et $v_{i,j}$ de $\mathbf{Z}[X]$ et un entier $c_{i,j} \neq 0$ tels que

$$u_{i,j}(X)f_i(X) + v_{i,j}(X)f_j(X) = c_{i,j}. \tag{3}$$

Notons $\mathscr{P}$ l'ensemble des premiers divisant l'entier $\prod_{1\leq i<j\leq k} c_{i,j}$, posons $N_0 = \prod_{p\in\mathscr{P}} p$ et

$$\mathscr{N}_0 = \big\{1 \leq n \leq N_0 \ : f(n) \not\equiv 0 \ [p] \quad \text{pour tout } p \in \mathscr{P}\big\}.$$

Hormis un nombre fini d'exceptions, les entiers n pour lesquels $f_1(n)$, $f_2(n)$, ..., $f_k(n)$ sont tous premiers, sont dans les progressions arithmétiques de la forme $n \equiv n_0 \ [N_0]$, avec $n_0 \in \mathscr{N}_0$. En effet, si $n \equiv n_1 \ [N_0]$ avec $n_1 \notin \mathscr{N}_0$, alors il existe un nombre premier $p \in \mathscr{P}$ tel que $f(n) \equiv 0 \ [p]$ et donc p divise l'un des $f_j(n)$. Or si n est assez grand [(4)], celui des $f_j(n)$ divisible par p ne pourra pas être premier.

Fixons temporairement $n_0 \in \mathscr{N}_0$ et posons $f_{j,n_0}(X) = f_j(n_0 + N_0X)$, ainsi que $f_{n_0}(X) = f(n_0 + N_0X)$: la famille des polynômes $f_{1,n_0}, f_{2,n_0}, \ldots, f_{k,n_0}$ est toujours convenable et vérifie maintenant l'hypothèse F. En effet, pour tout entier $n \geq 1$ et tout $p \in \mathscr{P}$, on a $f_{n_0}(n) = f(n_0 + N_0n) \equiv f(n_0) \not\equiv 0 \ [p]$. Donc un $p \in \mathscr{P}$ ne divise aucun des $f_{j,n_0}(n)$. Or comme le pgcd de deux $f_{i,n_0}(n)$ et $f_{j,n_0}(n)$ ne peut être divisible que par un $p \in \mathscr{P}$ (conséquence de la relation de Bézout (3)), on en déduit que la famille $\underline{f_{n_0}}$ vérifie maintenant l'hypothèse F.

[(3)] La dénomination « hypothèse F » peut sembler à juste titre peu motivée aux yeux du lecteur mais elle l'est à ceux des auteurs.

[(4)] Ceci ne dépend que de la donnée des polynômes $f_1, f_2, \ldots, f_k$ et il y a au plus h exceptions.

Supposons maintenant que $\mathbf{BH}(\underline{f})$ soit vraie pour toute famille convenable $\underline{f}$ satisfaisant l'hypothèse F. Avec des notations évidentes, pour tout $n_0 \in \mathscr{N}_0$, on a donc

$$\pi_{\underline{f_{n_0}}}(x) \sim \frac{C(\underline{f_{n_0}})}{h_1 h_2 \cdots h_k} \cdot \frac{x}{\log^k(x)} \quad \text{et} \quad \pi_{\underline{f}}(x) = \sum_{n_0 \in \mathscr{N}_0} \pi_{\underline{f_{n_0}}}\left(\frac{x-n_0}{N_0}\right) + P(x),$$

où $P(x)$ est une fonction bornée de x. Remarquons que la constante $C(\underline{f_{n_0}})$ ne dépend pas de n_0, mais seulement de $N_0 = \prod_{p \in \mathscr{P}} p$. En fait, on a la relation

$$C(\underline{f_{n_0}}) \prod_{p \,|\, N_0} \left(1 - \frac{N_f(p)}{p}\right) = C(\underline{f}) \tag{4}$$

car $N_{\underline{f_{n_0}}}(p) = 0$ si $p \in \mathscr{P}$ et $N_{\underline{f_{n_0}}}(p) = N_f(p)$ si $p \notin \mathscr{P}$ puisqu'alors $(N_0, p) = 1$. On a donc

$$\pi_{\underline{f}}(x) \sim \frac{\#\mathscr{N}_0}{N_0} \cdot \frac{C(\underline{f_{n_0}})}{h_1 h_2 \cdots h_k} \cdot \frac{x}{\log^k(x)}.$$

Or le théorème des restes chinois assure que $\#\mathscr{N}_0 = \prod_{p \in \mathscr{P}} \big(p - N_f(p)\big)$. Ceci, comparé à (4), montre que $C(\underline{f_{n_0}}) \cdot \#\mathscr{N}_0/N_0 = C(\underline{f})$ et donc que

$$\pi_{\underline{f}}(x) \sim \frac{C(\underline{f})}{h_1 h_2 \cdots h_k} \cdot \frac{x}{\log^k(x)},$$

ce qui achève la démonstration de la proposition. □

Remarquons enfin que le même type d'argument permet de déduire la conjecture de Bateman-Horn généralisée aux polynômes prenant des valeurs entières de la conjecture étudiée dans ce texte : si $f(X) \in \frac{1}{N}\mathbf{Z}[X]$ et $\forall a \in \mathbf{N}$, $f(a) \in \mathbf{Z}$, on remarque que $f_a(X) = f(NX + a) \in \mathbf{Z}[X]$ et que, si la conjecture de Bateman-Horn est vraie pour les f_a, alors

$$\pi_{\underline{f}}(x) = \sum_{a=1}^{N} \pi_{\underline{f}_a}\left(\frac{x-a}{N}\right) \sim \left(\frac{1}{N}\sum_{a=1}^{N} C(\underline{f}_a)\right) \frac{1}{h_1 \ldots h_k} \cdot \frac{x}{\log^k x},$$

et on vérifie que la constante apparaissant à droite est égale à $C(\underline{f})$ ou encore que

$$\prod_{p \,|\, N} \left(1 - \frac{\delta_f(p)}{p}\right) = \frac{1}{N}\sum_{a=1}^{N} \prod_{p \,|\, N} \left(1 - \frac{N_{\underline{f}_a}(p)}{p}\right),$$

en appliquant deux fois le lemme chinois.

5. Le Λ-calcul et la conjecture de Bateman-Horn

Dans ce paragraphe, nous adaptons le Λ-calcul à la conjecture de Bateman-Horn. Dans un premier temps, nous suivons de près l'esquisse de Golomb dans [**24**], mais un certain nombre de détails seront donnés dans les paragraphes ultérieurs.

Étant donné un entier $n \geq 1$, on lui associe diverses fonctions définies à partir de la décomposition primaire de n. On définit ainsi $\omega(n)$ comme le nombre de facteurs premiers

distincts de n, $\Omega(n)$ comme le nombre de facteurs premiers distincts avec multiplicité de n, la fonction de von Mangolt $\Lambda(n)$ comme $\log(p)$ si n est une puissance de p, 0 sinon et enfin la fonction de Möbius $\mu(n)$ comme $(-1)^{\omega(n)}$ si n est sans facteur carré, $\mu(1) = 1$ et 0 sinon.

Donnons-nous des polynômes $f_j(X) \in \mathbf{Z}[X]$ $(j = 1, \ldots, k)$, vérifiant les hypothèses de la conjecture de Bateman-Horn, ainsi que l'hypothèse F (dont on a vu qu'elle n'était pas une condition restrictive). Considérons la série entière, convergente pour $|z| < 1$,

$$G_{\underline{f}}(z) = (-1)^k k! \sum_{n=1}^{\infty} \Lambda\big(f_1(n)\big)\Lambda\big(f_2(n)\big) \cdots \Lambda\big(f_k(n)\big) z^n, \tag{5}$$

dont nous allons étudier le comportement au voisinage de $z = 1$ afin d'en déduire des conséquences arithmétiques intéressantes. L'hypothèse F et une identité de Golomb (équation (13) au paragraphe 6) assurent que, pour tout entier $n \geq 1$, on a

$$\Lambda\big(f_1(n)\big)\Lambda\big(f_2(n)\big) \cdots \Lambda\big(f_k(n)\big) = \frac{(-1)^k}{k!} \sum_{\substack{d \geq 1 \\ d \mid \widetilde{f}(n)}} \mu(d) \log^k(d). \tag{6}$$

En injectant cette relation dans (5) et en intervertissant les deux sommations (ce qui est licite puisque $|z| < 1$ implique la convergence absolue des séries utilisées), on obtient

$$\begin{aligned} G_{\underline{f}}(z) &= \sum_{n=1}^{\infty} \Bigg(\sum_{\substack{d \geq 1 \\ d \mid \widetilde{f}(n)}} \mu(d) \log^k(d) \Bigg) z^n = \sum_{d=1}^{\infty} \mu(d) \log^k(d) \sum_{\substack{n=1 \\ f(n) \equiv 0\,[d]}}^{\infty} z^n \\ &= \sum_{d=1}^{\infty} \mu(d) \log^k(d) \sum_{\ell=0}^{\infty} \sum_{\substack{n=1 \\ f(n) \equiv 0\,[d]}}^{d} z^{n+\ell d} = \sum_{d=1}^{\infty} \frac{\mu(d) \log^k(d)}{1 - z^d} \sum_{\substack{n=1 \\ f(n) \equiv 0\,[d]}}^{d} z^n. \end{aligned}$$

La troisième égalité est conséquence du fait que l'ensemble des solutions positives de la congruence $f(n) \equiv 0\,[d]$ est l'union disjointe des ensembles $m + \mathbf{N}d$, où m est n'importe quelle solution particulière de cette congruence dans $\{1, \ldots, d\}$. Remarquons que la valeur en $z = 1$ du polynôme $\sum_{\substack{n=1,\ldots,d \\ f(n) \equiv 0\,[d]}} z^n$ est très exactement la quantité $N_f(d)$ introduite au début du paragraphe 2, même lorsque la somme est vide en convenant qu'elle vaut alors 0. En procédant à l'échange limite-série, ***qui demeure la seule étape non justifiée de cette approche,*** [5] on obtient donc

$$\lim_{z \to 1^-} (1 - z)\, G_{\underline{f}}(z) \stackrel{?}{=} \sum_{d=1}^{\infty} \mu(d) \log^k(d) \lim_{z \to 1^-} \left(\frac{\sum_{\substack{n=1,\ldots,d \\ f(n) \equiv 0\,[d]}} z^n}{\sum_{n=0,\ldots,d-1} z^n} \right) = \sum_{d=1}^{\infty} \mu(d) \log^k(d) \frac{N_f(d)}{d}. \tag{7}$$

Un point important est évidemment de s'assurer de la convergence et de la non-nullité de la série à droite de (7), que l'on notera $C'(\underline{f})$. Nous allons faire mieux que cela en donnant

[5] Voir cependant le paragraphe 12.

une expression très simple de $C'(\underline{f})$ à l'aide de la constante $C(\underline{f})$ de Bateman-Horn. Pour cela, introduisons la série de Dirichlet

$$L_{\underline{f}}(s) = \sum_{d=1}^{\infty} \frac{\mu(d) N_f(d)}{d^s}, \tag{8}$$

dont on montrera qu'elle converge absolument au moins pour $\mathrm{Re}(s) > 1$, l'encadrement $0 \leq N_f(d) \leq d$ impliquant seulement la convergence absolue pour $\mathrm{Re}(s) > 2$. En vertu du théorème des restes chinois, $N_f(d)$ est une fonction multiplicative, c'est-à-dire que $N_f(d_1 d_2) = N_f(d_1) N_f(d_2)$ si $(d_1, d_2) = 1$. On en déduit que, pour $\mathrm{Re}(s)$ assez grand (en fait, c'est vrai pour $\mathrm{Re}(s) > 1$),

$$L_{\underline{f}}(s) = \prod_p \left(1 - \frac{N_f(p)}{p^s}\right) = \frac{1}{\zeta^k(s)} \prod_p \left(\left(1 - \frac{1}{p^s}\right)^{-k} \left(1 - \frac{N_f(p)}{p^s}\right)\right).$$

Ici, on a utilisé, de façon triviale, la fonction zêta de Riemann définie pour $\mathrm{Re}(s) > 1$ par la série ou le produit

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - p^{-s}\right)^{-1}.$$

Voir les livres de Titchmarsh [**51**] ou de Tenenbaum [**50**] pour les propriétés de la fonction zêta qui seront utilisées sans référence ici. On montre au sous-paragraphe 7.4 que l'on peut prolonger analytiquement $L_{\underline{f}}(s)$ à un ouvert contenant le demi-plan $\mathrm{Re}(s) \geq 1$: il s'agit d'un cas particulier d'un résultat de Kurokawa [**34**]. Comme la fonction $\zeta(s)^{-k}$ s'annule à l'ordre k en $s = 1$ et que $\lim_{s \to 1}(s-1)\zeta(s) = 1$, on en déduira que

$$C'(\underline{f}) = (-1)^k L_{\underline{f}}^{(k)}(1) = (-1)^k \, k! \prod_p \left(\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_f(p)}{p}\right)\right) = (-1)^k \, k! \, C(\underline{f}). \tag{9}$$

Seule la première égalité nécessite quelques efforts, qui seront faits au paragraphe 8. Ce résultat inconditionnel est dû à Conrad [**14**] : nous en donnons une preuve plus détaillée que lui (notre fonction $L_{\underline{f}}(s)$ est sa fonction $G(s)$ lorsque son paramètre m vaut 1). À l'aide d'un théorème taubérien, que nous expliciterons au paragraphe 9, on traduit (7) et (9) par

$$\lim_{n \to +\infty} \frac{1}{n} \sum_{j=1}^{n} \Lambda\big(f_1(j)\big) \Lambda\big(f_2(j)\big) \cdots \Lambda\big(f_k(j)\big) = C(\underline{f}). \tag{10}$$

Un résultat relativement élémentaire montre que (10) équivaut à $\mathbf{BH}(\underline{f})$. L'existence d'une constante $D(\underline{f}) > 0$ telle que (10) ait lieu avec $D(\underline{f})$ à la place de $C(\underline{f})$ serait déjà un très beau résultat. Même en admettant l'existence de cette limite, nous ne voyons pas comment montrer que l'on aurait alors nécessairement $D(\underline{f}) = C(\underline{f})$, comme l'a fait Tchebichef [**49**, p. 352, Théorème III] en prouvant (un résultat équivalent à) l'implication

$$\lim_{x\to+\infty}\frac{1}{x}\sum_{n\le x}\Lambda(n)=C \implies C=1. \tag{11}$$

Enfin, il serait intéressant de considérer le cas des polynômes de plusieurs variables : bien qu'à notre connaissance il n'existe pas de conjecture similaire à celle de Bouniakowsky, rien n'interdit de s'intéresser au comportement au voisinage du point $(z_1,\dots,z_k)=(1,\dots,1)$ de séries telles que, par exemple,

$$\sum_{n_1,\dots,n_k\ge 0}\Lambda\big(P(n_1,\dots,n_k)\big)z_1^{n_1}\cdots z_k^{n_k},$$

où $P(X_1,\dots,X_k)\in\mathbf{Z}[X_1,\dots,X_k]$ prend des valeurs ≥ 1 aux entiers positifs.

Le cas d'un polynôme quadratique en deux variables est non trivial mais peut être résolu à l'aide du théorème de Dirichlet et de considération du groupe de classes d'un corps quadratique. L'exemple le plus simple est celui des nombres premiers (impairs) représentés par le polynôme X^2+Y^2 : d'après un résultat de Fermat, il s'agit des nombres premiers congrus à 1 modulo 4. Le cas d'un polynôme quadratique binaire général est traité en détail par Iwaniec [**31**]. On peut faire une partie de l'étude dans le cas des formes-normes « complètes » comme par exemple $F(X,Y,Z)=X^3+2Y^3+4Z^3-6XYZ=N_{\mathbf{Q}}^{\mathbf{K}}(X+Y\omega+Z\omega^2)$ avec $\omega^3=2$ et $\mathbf{K}=\mathbf{Q}(\omega)$: les premiers représentés par $F(X,Y,Z)$ sont les premiers non inertes dans $\mathbf{K}/\mathbf{Q}$ i. e. les premiers p congrus à 2 modulo 3 et les premiers congrus à 1 modulo 3 tels que 2 soit résidu cubique modulo p. Notons également que l'analogue naïf de l'hypothèse de Bouniakowsky – demander que pour tout n, il existe ℓ et m tels que $f(\ell,m)$ soit premier avec n – est insuffisant pour les polynômes à deux variables ou plus, comme le montre un exemple de Heath-Brown (voir l'introduction de [**30**]).

Citons enfin ici le fort beau résultat de Friedlander et Iwaniec [**21**] : le nombre de nombres premiers $\le x$ qui sont valeurs du polynôme X^2+Y^4 est équivalent à

$$\frac{\sqrt{2}\Gamma(1/4)^2}{3\pi^{3/2}}\cdot\frac{x^{3/4}}{\log(x)},$$

où Γ est la fonction Gamma d'Euler. Heath-Brown [**30**] a adapté leur méthode au cas du polynôme X^3+2Y^3.

6. L'identité de Golomb

Rappelons qu'une fonction arithmétique est une fonction définie sur $\mathbf{N}^\star$ et à valeur dans $\mathbf{C}$. Elle est dite multiplicative, resp. additive, si pour tout couple d'entiers (m,n) premiers entre eux, on a $f(mn)=f(m)f(n)$, resp. $f(mn)=f(m)+f(n)$; elle est dite totalement multiplicative, resp. totalement additive, si $f(mn)=f(m)f(n)$, resp. $f(mn)=f(m)+f(n)$, pour tous entiers m et n non nuls : μ est multiplicative, ω est additive et Ω est totalement additive, mais Λ n'a aucune propriété de la sorte.

Par ailleurs, on a

$$\Lambda(n) = \sum_{d\,|\,n} \mu(d)\log(n/d) = -\sum_{d\,|\,n} \mu(d)\log(d), \tag{12}$$

où la deuxième égalité utilise l'additivité totale de log et l'importante identité

$$\sum_{d\,|\,n} \mu(d) = \begin{cases} 1 \text{ si } n = 1\,; \\ 0 \text{ si } n \geq 2. \end{cases}$$

Nous montrons maintenant la propriété essentielle dont on a besoin pour le Λ-calcul et qui généralise (12) : l'identité (6) en découle.

Théorème 4 (Golomb). — *Soient un entier $k \geq 1$ et des entiers $a_1, \dots, a_k > 1$ deux à deux premiers entre eux. Alors, on a*

$$\prod_{j=1}^{k} \Lambda(a_j) = \frac{(-1)^k}{k!} \sum_{d\,|\,a_1\cdots a_k} \mu(d)\log^k(d). \tag{13}$$

Remarque. La démonstration ci-dessous utilise l'additivité de log mais pas son additivité totale ; le résultat d'ailleurs proposé par Golomb porte plus généralement sur des couples de fonctions similaires à $(\Lambda, \log)$, qu'il dénomme fonctions primaires et logarithmétiques, par exemple (indicatrice des nombres premiers, ω).

Démonstration. — Puisque les entiers $a_1, \dots, a_k$ sont deux à deux premiers entre eux, il y a bijection entre l'ensemble des diviseurs ≥ 1 du produit $a_1 \cdots a_k$ et l'ensemble des k-uplets $(d_1, \dots, d_k)$ tels $d_j \geq 1$ et $d_j \,|\, a_j$ pour $j = 1, \dots, k$. L'hypothèse que les a_j sont > 1 sera utilisée plus bas.

Comme les d_j sont en plus deux à deux premiers entre eux, on peut alors utiliser la multiplicativité de μ et l'additivité de log pour obtenir

$$\begin{aligned}
&\sum_{d\,|\,a_1\cdots a_k} \mu(d)\log^k(d) \\
&\quad= \sum_{d_1\,|\,a_1,\dots,d_k\,|\,a_k} \mu(d_1\cdots d_k)\log^k(d_1\cdots d_k) \\
&\quad= \sum_{d_1\,|\,a_1,\dots,d_k\,|\,a_k} \mu(d_1)\cdots\mu(d_k)\big(\log(d_1)+\cdots+\log(d_k)\big)^k \\
&\quad= \sum_{\substack{i_1,\dots,i_k\geq 0 \\ i_1+\cdots+i_k=k}} \frac{k!}{i_1!\cdots i_k!} \sum_{d_1\,|\,a_1,\dots,d_k\,|\,a_k} \mu(d_1)\cdots\mu(d_k)\log^{i_1}(d_1)\cdots\log^{i_k}(d_k) \\
&\quad= \sum_{\substack{i_1,\dots,i_k\geq 0 \\ i_1+\cdots+i_k=k}} \frac{k!}{i_1!\cdots i_k!} \prod_{j=1}^{k} \Big(\sum_{d_j\,|\,a_j} \mu(d_j)\log^{i_j}(d_j) \Big),
\end{aligned} \tag{14}$$

en convenant d'attribuer la valeur 1 à $\log^0(1)$. De plus, *stricto sensu*, pour utiliser le développement multinomial, il est préférable de supposer $k \geq 2$, ce qui est loisible puisque la formule à démontrer est vraie si $k = 1$ (par définition).

Or puisque $a_j > 1$, on a $\sum_{d_j \,|\, a_j} \mu(d_j) \log^{i_j}(d_j) = 0$ lorsque $i_j = 0$, ce qui annule le terme correspondant dans (14). Comme il n'y a qu'une seule façon d'écrire $k = i_1 + \cdots + i_k$ avec des entiers $i_1, \ldots, i_k \geq 1$, à savoir de les prendre tous égaux à 1, on déduit donc de (12) et (14) que

$$\sum_{d \,|\, a_1 \cdots a_k} \mu(d) \log^k(d) = \frac{k!}{1! \cdots 1!} \prod_{j=1}^{k} \Big(\sum_{d_j \,|\, a_j} \mu(d_j) \log(d_j) \Big) = (-1)^k k! \, \Lambda(a_1) \cdots \Lambda(a_k),$$

ce qui achève la preuve. □

Notons que la même démonstration donne le résultat suivant, puisqu'il n'y a aucune façon d'écrire $\ell = i_1 + \cdots + i_k$ avec des entiers $i_j \geq 1$ si $0 \leq \ell < k$.

Théorème 5. — *Soient un entier $k \geq 1$ et des entiers $a_1, \ldots, a_k > 1$ deux à deux premiers entre eux. Alors pour tout entier ℓ tel que $0 \leq \ell < k$, on a*

$$\sum_{d \,|\, a_1 \cdots a_k} \mu(d) \log^\ell(d) = 0.$$

On se servira de ce fait au sous-paragraphe 12.2.

7. Fonctions zêta de Dedekind et $L_{\underline{f}}(s)$

Dans ce paragraphe, nous indiquons comment lier la série de Dirichlet $L_{\underline{f}}(s)$ aux fonctions zêta de Dedekind associées aux corps de nombres $\mathbf{K}_1$, $\mathbf{K}_2$, ..., $\mathbf{K}_k$, ce qui permettra d'en faire le prolongement analytique : celui-ci a été apparemment fait dans ce contexte pour la première fois par Kurokawa [**35**], mais nous nous contentons de redémontrer la seule partie qui nous intéresse. Cette étude justifiera au passage que le produit de Bateman-Horn $C(\underline{f})$ est bien convergent. Les nombres f_j qui apparaissent dans les sous-paragraphes 7.1 et 7.2 sont des degrés résiduels et ne peuvent pas être confondus avec les polynômes f_j utilisés dans le reste de l'article (et pas dans ces deux paragraphes).

7.1. Racines d'un polynôme modulo p et idéaux premiers. — Soit g un polynôme unitaire et irréductible sur $\mathbf{Q}$, dont α est une racine. Notons $\mathbf{K} = \mathbf{Q}(\alpha)$ le corps de nombres associés à g. Supposons tout d'abord que l'anneau $\mathcal{O}_\mathbf{K}$ des entiers de $\mathbf{K}$ vérifie $\mathcal{O}_\mathbf{K} = \mathbf{Z}[\alpha]$. Dans ce cas, la factorisation dans $\mathcal{O}_\mathbf{K}$ de p en idéaux premiers entiers s'écrit $p\mathcal{O}_\mathbf{K} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$, avec $\mathrm{N}(\mathfrak{p}_j) = p^{f_j}$, où $\mathrm{N}(\mathfrak{a}) = \big[\mathcal{O}_\mathbf{K} : \mathfrak{a}\big]$ est l'indice d'un idéal $\mathfrak{a}$ de $\mathcal{O}_\mathbf{K}$. Cette factorisation correspond bijectivement à celle, dans $(\mathbf{Z}/p\mathbf{Z})[X]$, de la réduction du polynôme $\overline{g} = g \bmod p$, c'est-à-dire $\overline{g} = \overline{g}_1^{e_1} \overline{g}_2^{e_2} \cdots \overline{g}_r^{e_r}$ avec des $\overline{g}_j \in (\mathbf{Z}/p\mathbf{Z})[X]$ irréductibles, de degrés respectifs f_j : voir [**22**, p. 129]. En conséquence, en posant $A_{p,\mathbf{K}} = A_p = \#\{\mathfrak{p} \,\text{idéal premier de}\, \mathcal{O}_\mathbf{K} : \mathrm{N}(\mathfrak{p}) = p\}$, on a

$$A_p = N_g(p). \tag{15}$$

Bien entendu, il n'est pas toujours vrai que $\mathcal{O}_{\mathbf{K}} = \mathbf{Z}[\alpha]$, ni que g soit unitaire. Mais ce n'est pas un réel problème. En effet, si $g(X) = aX^d + \cdots$, on le remplace alors par $\tilde{g}(X) = a^{d-1}g(X/a) \in \mathbf{Z}[X]$, qui est unitaire, engendre le même corps de nombres $\mathbf{K}$ que g et possède la même décomposition modulo p que g pourvu que $p \nmid a$, ce qui est vrai pour tous sauf un nombre fini de p. De plus, si α est une racine de $\tilde{g}$, on a, de façon générale, seulement que $\mathbf{Z}[\alpha]$ est un sous-groupe d'indice fini de $\mathcal{O}_{\mathbf{K}}$: la factorisation indiquée ci-dessus de $p\mathcal{O}_{\mathbf{K}}$ en idéaux premiers et l'équation (15) restent vraies pourvu que $p \nmid \left[\mathcal{O}_{\mathbf{K}} : \mathbf{Z}[\alpha]\right]$ (c'est la généralisation proposée après l'énoncé du Theorem 23, p. 129, de [**22**]).

Il résulte de cette discussion que, hormis un nombre fini de nombres premiers qui ne dépendent que de g, on a toujours $A_p = N_g(p)$.

7.2. Quelques propriétés des fonctions zêta de Dedekind. — La fonction zêta de Dedekind associée à un corps de nombres $\mathbf{K}$ est par définition la série de Dirichlet (voir [**38**], chapter VIII) :

$$\zeta_{\mathbf{K}}(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

où $\mathfrak{a}$, resp. $\mathfrak{p}$, désigne les idéaux, resp. idéaux premiers, entiers non-nuls de $\mathcal{O}_{\mathbf{K}}$. L'abscisse de convergence de la série est 1 et la deuxième égalité est valable pour $\mathrm{Re}(s) > 1$. Notons que $\zeta_{\mathbf{Q}}$ est simplement la fonction zêta de Riemann. On se servira des propriétés suivantes :

(*i*) $\zeta_{\mathbf{K}}(s)$ peut être prolongée méromorphiquement à tout $\mathbf{C}$, avec un seul pôle simple en $s = 1$.

(*ii*) Il existe une constante explicite $C_{\mathbf{K}} > 0$ telle que $\zeta_{\mathbf{K}}(s)$ ne s'annule pas dans l'ouvert $\sigma > 1 - C_{\mathbf{K}}/\log(2 + |t|)$ (avec $s = \sigma + it$) qui contient le demi-plan $\mathrm{Re}(s) \geq 1$ et, sur ce même ouvert, on a également $|\zeta_{\mathbf{K}}(s)^{-1}| \ll \log(|t| + 2)$.

Remarque. En appliquant (*i*) et (*ii*) aux corps $\mathbf{Q}$ et $\mathbf{K}$, on voit qu'il existe une constante explicite $\tilde{C}_{\mathbf{K}} > 0$ telle que la fonction $\zeta_{\mathbf{K}}(s)/\zeta(s)$ est holomorphe et sans zéro sur l'ouvert $\sigma > 1 - \tilde{C}_{\mathbf{K}}/\log(|t| + 2)$. L'énoncé (*i*) est très classique (voir [**38**], chapter VIII, XIII) ; pour une preuve de (*ii*) dans le cas $\mathbf{K} = \mathbf{Q}$ (qui s'adapte aisément au cas général), voir la démonstration du Théorème 16, p.178 et suivantes, du livre de Tenenbaum [**50**].

Par ailleurs, avec la définition de A_p donnée au sous-paragraphe 7.1, on peut écrire (avec $\mathrm{N}(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$)

$$\zeta_{\mathbf{K}}(s) = \prod_{\mathfrak{p}, f_{\mathfrak{p}}=1} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1} \prod_{\mathfrak{p}, f_{\mathfrak{p}}\geq 2} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1} = \prod_{p} (1 - p^{-s})^{-A_p} R_{\mathbf{K}}(s),$$

où $R_{\mathbf{K}}(s) = \prod_{\mathfrak{p}, f_{\mathfrak{p}} \geq 2}(1 - \mathrm{N}(\mathfrak{p})^{-s})$ est holomorphe sans zéro sur le demi-plan $\mathrm{Re}(s) > 1/2$, de telle sorte que $\log(R_{\mathbf{K}}(s))$ est aussi holomorphe sur ce demi-plan. Donc pour $\mathrm{Re}(s) > 1$, on a

$$\log\big(\zeta_{\mathbf{K}}(s)\big) = \sum_p \frac{A_p}{p^s} + \sum_p \sum_{m \geq 2} \frac{A_p}{p^{ms}} + \log\big(R_{\mathbf{K}}(s)\big).$$

Comme la fonction $\zeta_{\mathbf{K}}(s)/\zeta(s)$ est holomorphe et sans zéro sur un ouvert contenant le demi-plan $\mathrm{Re}(s) \geq 1$, on en déduit que la série

$$\sum_p \frac{A_p - 1}{p^s} = \log\big(\zeta_{\mathbf{K}}(s)/\zeta(s)\big) - \sum_p \frac{A_p - 1}{p^s(p^s - 1)} + \log\big(R_{\mathbf{K}}(s)/R_{\mathbf{Q}}(s)\big)$$

est analytiquement prolongeable à ce même ouvert. La convergence de la série $\sum_p (A_p - 1)/p$ en découle grâce au résultat suivant, dû à Newman, qui s'applique ici car $0 \leq A_p \leq \deg(g)$:

« *Soit* $D(s) = \sum_{n=1}^{\infty} a_n/n^s$ *une série de Dirichlet convergente sur le demi-plan* $\mathrm{Re}(s) > 1$. *Supposons que* D *soit analytiquement prolongeable à un ouvert contenant le demi-plan fermé* $\mathrm{Re}(s) \geq 1$ *et que la suite des* a_n *soit bornée. Alors la série* $\sum_{n=1}^{\infty} a_n/n$ *est convergente, de somme* $D(1)$. »

Nous énoncerons et nous servirons d'une forme un peu plus générale de ce résultat au Théorème 10 du paragraphe 9.

7.3. Convergence du produit $C(\underline{f})$. — Rappelons qu'il existe deux polynômes $u_{i,j}$ et $v_{i,j}$ de $\mathbf{Z}[X]$ et un entier $c_{i,j} \neq 0$ tels que

$$u_{i,j}(X) f_i(X) + v_{i,j}(X) f_j(X) = c_{i,j}.$$

Soit p un premier ne divisant pas $\prod_{1 \leq i < j \leq k} c_{i,j}$. On déduit de cette relation de Bézout que pour tout entier $n \geq 1$ et tout couple (i, j) avec $1 \leq i < j \leq k$, le premier p ne divise pas le pgcd des entiers $f_i(n)$ et $f_j(n)$ et donc que $N_f(p) = N_{f_1}(p) + N_{f_2}(p) + \cdots + N_{f_k}(p)$. Notons $A_{p,\mathbf{K}_j}$ les entiers associés aux corps de nombres $\mathbf{K}_j$ $(j = 1, \ldots, k)$ au sous-paragraphe 7.1, où l'on a expliqué pourquoi l'équation $N_{f_j}(p) = A_{p,\mathbf{K}_j}$ est vraie, sauf pour un nombre fini de premiers p. Donc $N_f(p) - k = (A_{p,\mathbf{K}_1} - 1) + (A_{p,\mathbf{K}_2} - 1) + \cdots + (A_{p,\mathbf{K}_k} - 1)$, sauf pour un nombre fini de premiers p. De la convergence des séries $\sum_p (A_{p,\mathbf{K}_j} - 1)/p$, on déduit celle de $\sum_p (N_f(p) - k)/p$. Comme

$$\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_f(p)}{p}\right) = 1 + \frac{k - N_f(p)}{p} + \mathcal{O}\left(\frac{1}{p^2}\right),$$

le produit $C(\underline{f})$ est bien convergent.

De plus, en admettant les propriétés de $L_{\underline{f}}(s)$ qui seront démontrées dans le paragraphe ci-dessous (voir le Théorème 6), on a

$$C(\underline{f}) = \lim_{\sigma \to 1^+} \prod_p \left(\left(1 - \frac{1}{p^\sigma}\right)^{-k} \left(1 - \frac{N_f(p)}{p^\sigma}\right)\right) = \lim_{\sigma \to 1^+} \zeta(\sigma)^k L_{\underline{f}}(\sigma) = \lim_{\sigma \to 1^+} \frac{L_{\underline{f}}(\sigma)}{(\sigma - 1)^k}.$$

Comme la fonction $L_{\underline{f}}(s)$ est holomorphe en $s=1$, où elle admet un zéro d'ordre k, on en déduit que $C(\underline{f}) = k!\, L_{\underline{f}}^{(k)}(1)$.

Terminons ce paragraphe en remarquant que le produit $C(\underline{f})$ n'est en général pas absolument convergent. Dans [**17**], Davenport et Schinzel obtiennent une expression alternative de $C(\underline{f})$, qui, bien que particulièrement compliquée, a l'avantage de ne faire intervenir que des produits absolument convergents, ce qui permet donc de calculer plus facilement $C(\underline{f})$. Notons r_1 le nombre de racines réelles, r_2 le nombre de paires de racines complexes conjuguées et D le discriminant de f. Pour tout $j \in \{1,\dots,k\}$, au corps $\mathbf{K}_j$, on associe D_j son discriminant, h_j son nombre de classes, R_j son régulateur et w_j le nombre de ces racines de l'unité. Enfin, soient $A_i(p)$, resp. $A_{i,j}(p)$ le nombre de facteurs irréductibles de degré i de la réduction modulo p de f, resp. f_j. On a alors

$$C(\underline{f}) = 2^{-r_1-r_2}\pi^{-r_2}\prod_{j=1}^{k}\left(\frac{w_j|D_j|^{1/2}}{h_jR_j}\right)\cdot\prod_{p\mid D}\left(\left(1-\frac{N_f(p)}{p}\right)\prod_{j=1}^{k}\prod_{i\geq 2}\left(1-\frac{1}{p^i}\right)^{-A_{i,j}(p)}\right)$$
$$\times\prod_{p\nmid D}\left(\left(1-\frac{N_f(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-N_f(p)}\prod_{i\geq 2}\left(1-\frac{1}{p^i}\right)^{-A_i(p)}\right).$$

La démonstration de cette identité peut être reconstruite à partir des idées utilisées dans ce paragraphe et le suivant, jointes au fait que le résidu de $\zeta_{\mathbf{K}}(s)$ en $s=1$ s'exprime comme $2^{r_1+r_2}\pi^{r_2}h_{\mathbf{K}}R_{\mathbf{K}}/(w_{\mathbf{K}}|D_{\mathbf{K}}|^{1/2})$, avec des notations évidentes (voir [**22**, Theorem 61, p. 284]). En effet, avec les notations du théorème 6 du paragraphe suivant et en notant $\kappa_{\mathbf{K}_j}$ le résidu de la fonction zêta de Dedekind associée à $\mathbf{K}_j$, on a $C(\underline{f}) = M_{\underline{f}}(1)/\kappa_{\mathbf{K}_1}\dots\kappa_{\mathbf{K}_k}$.

7.4. Prolongement analytique de $L_{\underline{f}}(s)$. — On a défini, pour $\mathrm{Re}(s)>1$, la série de Dirichlet

$$L_{\underline{f}}(s) = \sum_{d=1}^{\infty}\frac{\mu(d)N_f(d)}{d^s} = \prod_{p}\left(1-N_f(p)p^{-s}\right).$$

Nous allons montrer ici le résultat suivant, qui recoupe un article de Kurokawa [**35**]. Celui-ci montre également que si $h\geq 2$, alors la fonction $L_{\underline{f}}(s)$ n'est pas prolongeable au delà de $\mathrm{Re}(s)>0$, nous en donnons un preuve dans un paragraphe ultérieur. Comme on sait, $L_{\underline{f}}(s)$ est en revanche méromorphiquement prolongeable à $\mathbf{C}$ lorsque $h=1$ mais il semble délicat d'en tirer des conclusions définitives.

Théorème 6. — *(i) L'abscisse de convergence absolue de la série de Dirichlet définissant $L_{\underline{f}}(s)$ est au plus* 1.

(ii) Il existe une constante explicite $\varepsilon_{\underline{f}}>0$ et une fonction $M_{\underline{f}}(s)$ holomorphe sur le demi-plan $\mathrm{Re}(s)>1/2$, *sans zéro sur* $\mathrm{Re}(s)>1-\varepsilon_{\underline{f}}$, *telle que*

$$L_{\underline{f}}(s) = \left(\zeta_{\mathbf{K}_1}(s)\zeta_{\mathbf{K}_2}(s)\cdots\zeta_{\mathbf{K}_k}(s)\right)^{-1}M_{\underline{f}}(s).$$

(*iii*) *Il existe une constante explicite* $B_{\underline{f}} > 0$ *telle que la fonction* $L_{\underline{f}}(s)$ *est analytiquement prolongeable à l'ouvert* $U_{\underline{f}}$ *défini par* $\sigma > 1 - B_{\underline{f}}/\log(|t|+2)$, *sur lequel elle n'a ni zéro ni pôle, sauf un zéro d'ordre* k *en* $s = 1$.

(*iv*) *Pour tout* $s \in U_{\underline{f}}$, *on a* $|L_{\underline{f}}(s)| \ll \log(|t|+2)^k$.

Démonstration. — (*i*) Rappelons que $0 \leq N_f(p) \leq h = \deg(f)$ pour tout nombre premier p. Il s'ensuit que pour tout entier $d \geq 1$, $|\mu(d)N_f(d)| \leq |\mu(d)|\, h^{\omega(d)}$ par multiplicativité de N_f (cette inégalité est en général fausse sans le facteur $\mu(d)$). Donc

$$\sum_{d=1}^{\infty} \left| \frac{\mu(d)N_f(d)}{d^s} \right| \leq \sum_{d=1}^{\infty} \frac{|\mu(d)|h^{\omega(d)}}{d^\sigma} = \prod_p \left(1 + \frac{h}{p^\sigma}\right).$$

Comme ce dernier produit converge pour tout $\sigma > 1$ et tout $h > 0$, on en déduit que l'abscisse de convergence absolue de la série de Dirichlet définissant $L_{\underline{f}}(s)$ est au plus 1. Pour référence future, notons que $\prod_p (1+hp^{-s}) = \zeta(s)^h T(s)$ avec $T(s) = \prod_p (1+hp^{-s})(1-p^{-s})^h$ holomorphe et bornée pour $\mathrm{Re}(s) \geq 1/2 + \varepsilon$ et, par conséquent,

$$\sum_{d=1}^{\infty} \left| \frac{\mu(d)N_f(d)}{d^s} \right| \ll \zeta(\sigma)^h \ll (\sigma - 1)^{-h}.$$

(*ii*) Pour tous sauf un nombre fini de premiers p, on a $N_f(p) = A_{p,\mathbf{K}_1} + A_{p,\mathbf{K}_2} + \cdots + A_{p,\mathbf{K}_k}$: notons $\mathscr{Q}$ l'ensemble des premiers où ceci a lieu et $\mathscr{R}$ l'ensemble fini des premiers « fautifs ». Comme par ailleurs, pour $\mathrm{Re}(s) > 1$ et tout entier $A \geq 1$

$$1 - \frac{A}{p^s} = \left(1 - \frac{1}{p^s}\right)^A - \sum_{m=2}^{A} \binom{A}{m} \frac{1}{p^{ms}} = \left(1 - \frac{1}{p^s}\right)^A \left(1 + \mathcal{O}\left(p^{-2\sigma}\right)\right),$$

on a donc, pour tout $p \in \mathscr{Q}$,

$$1 - \frac{N_f(p)}{p^s} = E_p(s) \left(1 - \frac{1}{p^s}\right)^{A_{p,\mathbf{K}_1} + A_{p,\mathbf{K}_2} + \cdots + A_{p,\mathbf{K}_k}}, \tag{16}$$

où $E_p(s)$ est une fonction holomorphe sur $\mathrm{Re}(s) > 1/2$ qui vérifie $E_p(s) = 1 + \mathcal{O}\left(p^{-2\sigma}\right)$. Le produit $E_{\mathscr{Q}}(s) = \prod_{p \in \mathscr{Q}} E_p(s)$ est donc convergent sur $\mathrm{Re}(s) > 1/2$, où il définit une fonction holomorphe. D'où

$$L_{\underline{f}}(s) = \left(\zeta_{\mathbf{K}_1}(s)\zeta_{\mathbf{K}_2}(s)\cdots\zeta_{\mathbf{K}_k}(s)\right)^{-1} E_{\mathscr{Q}}(s) \prod_{p \in \mathscr{R}} \frac{1 - N_f(p)p^{-s}}{(1-p^{-s})^{A_{p,\mathbf{K}_1} + \cdots + A_{p,\mathbf{K}_k}}}.$$

Posons

$$M_{\underline{f}}(s) = E_{\mathscr{Q}}(s) \prod_{p \in \mathscr{R}} \frac{1 - N_f(p)p^{-s}}{(1-p^{-s})^{A_{p,\mathbf{K}_1} + \cdots + A_{p,\mathbf{K}_k}}},$$

qui est holomorphe sur $\mathrm{Re}(s) > 1/2$ puisque les seuls pôles de $M_{\underline{f}}(s)$ ne peuvent provenir que de ceux des termes $\left(1 - p^{-s}\right)^{-1}$, c'est-à-dire lorsque $s \in i(2\pi/\log(p))\mathbf{Z}$. Compte-tenu de (16), les zéros de $M_{\underline{f}}(s)$ sont parmi ceux des termes $1 - N_f(p)p^{-s}$, c'est-à-dire lorsque $s \in \sigma_p + i(2\pi/\log(p))\mathbf{Z}$ avec $\sigma_p = \log(N_f(p))/\log(p)$. Or puisque $N_f(p) \leq \min(p-1, \deg(f))$,

on voit qu'il existe $\varepsilon_{\underline{f}} > 0$ tel que si $\mathrm{Re}(s) > 1 - \varepsilon_{\underline{f}}$, alors $M_{\underline{f}}(s) \neq 0$.

(*iii*) C'est maintenant une conséquence immédiate des propriétés analytiques des fonctions zêta de Dedekind et $M_{\underline{f}}(s)$.

(*iv*) La fonction $M_{\underline{f}}(s)$ est bornée sur tout demi-plan $\mathrm{Re}(s) \geq 1/2 + \varepsilon$ avec $\varepsilon > 0$. On conclut grâce à la majoration de la croissance des fonctions $\zeta_{\mathbf{K}}(s)^{-1}$ dans les ouverts de la forme $\sigma > 1 - C_{\mathbf{K}}/\log(|t| + 2)$, sur lesquels elles ne s'annulent pas. □

8. Valeur des dérivées de $L_{\underline{f}}(s)$ en $s = 1$

Le but de ce paragraphe est de justifier que pour tout entier $\ell \geq 0$, on a

$$\sum_{d=1}^{\infty} \mu(d) \log^{\ell}(d) \frac{N_f(d)}{d} = (-1)^{\ell} L_{\underline{f}}^{(\ell)}(1),$$

ce qui, pour $\ell = k$, est une égalité que nous avons promis de prouver. Ce résultat est prouvé par Conrad [**14**], essentiellement au moyen de la méthode maintenant décrite. Le Théorème 7 ci-dessous est légèrement plus fort que celui montré par Conrad mais les deux démonstrations utilisent la méthode de Selberg-Delange, qui semble le bon outil ici. Remarquons que le problème est de prouver la *convergence* de la série ; en effet, par les propriétés de base des séries de Dirichlet, si elle converge en un point s_0 et si la fonction définie sur le demi-plan $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ se prolonge (continûment ou analytiquement) en s_0, alors la valeur de la série est égale à la valeur de la fonction en s_0.

Pour montrer la convergence, nous allons appliquer de nouveau le théorème de Newman (dans la forme donnée au Théorème 10 au paragraphe 9 ci-dessous et non sous celle plus faible donnée à la fin du paragraphe 7.2) tandis que Conrad utilise un théorème de Riesz. La dérivée ℓ-ième de $L_{\underline{f}}(s)$ est donnée sur $\mathrm{Re}(s) > 1$ par

$$L_{\underline{f}}^{(\ell)}(s) = (-1)^{\ell} \sum_{d=1}^{\infty} \mu(d) \log^{\ell}(d) \frac{N_f(d)}{d^s}.$$

Puisque $L_{\underline{f}}(s)$ est analytiquement prolongeable à un ouvert contenant $\mathrm{Re}(s) \geq 1$, ses dérivées le sont également et pour appliquer le Théorème 10 à la série $L_{\underline{f}}^{(\ell)}(s)$, il nous reste à montrer que

$$S_{\ell}(x) = \sum_{1 \leq n \leq x} \mu(n) \log^{\ell}(n) N_f(n) = o(x).$$

Dans un premier temps, notons que la transformation d'Abel montre que, pour tous entiers $\ell \geq 1$ et $x \geq 2$, on a

$$S_\ell(x) = \sum_{1\leq n\leq x-1} S_0(n)\left(\log^\ell(n) - \log^\ell(n+1)\right) + S_0(x)\log^\ell(x+1)$$
$$\ll \sum_{1\leq n\leq x-1} \frac{\log^{\ell-1}(n)}{n}|S_0(n)| + |S_0(x)|\log^\ell(x).$$

Il nous suffit donc de montrer $S_0(x) \ll_N x/\log^N(x)$ pour tout entier $N \geq 0$ et le résultat suivant s'avère amplement suffisant.

Théorème 7. — *Il existe une constante explicite $c(\underline{f}) > 0$ telle que, lorsque $x \to +\infty$,*

$$|S_0(x)| \leq x\exp\left(-c(\underline{f})\sqrt{\log(x)}\right).$$

Démonstration. — La démarche est classique et est en fait un cas assez simple de la méthode de Selberg-Delange (voir [**50**, paragraphe II, 5.4]) : on utilise la formule sommatoire de Perron et les propriétés analytiques de la fonction $L_{\underline{f}}(s)$. Les constantes c_j et celles implicites dans les symboles $\ll$ et $\mathcal{O}$ ci-dessous sont effectives et ne dépendent au plus que de la famille $\underline{f}$.

Pour simplifier, posons $a_n = \mu(n)N_{\underline{f}}(n)$ et $A(x) = \sum_{1\leq n\leq x} a_n$, ainsi que $b_n = |\mu(n)|h^{\omega(n)}$ et $B(x) = \sum_{1\leq n\leq x} b_n$. Si on pose $M(s) = \sum_{n\geq 1} b_n/n^s$, on a vu que $|\sum_{n\geq 1} a_n/n^{\kappa+it}| \leq M(\kappa) \ll \zeta(\kappa)^h \ll (\kappa-1)^{-h}$. La formule de Perron « effective » nous donne

$$\int_1^x A(t)\mathrm{d}t = \frac{1}{2i\pi}\int_{\kappa-i\infty}^{\kappa+i\infty} L_{\underline{f}}(s)x^{s+1}\frac{\mathrm{d}s}{s(s+1)} = \frac{1}{2i\pi}\int_{\kappa-iT}^{\kappa+iT} L_{\underline{f}}(s)x^{s+1}\frac{\mathrm{d}s}{s(s+1)} + R(x,T),$$

où nous choisissons $\kappa = 1 + 1/\log(x)$ et où le reste $R(x,T)$ vérifie

$$|R(x,T)| \ll x^2\frac{\log^h(x)}{T}.$$

Sur le contour rectangulaire $\mathscr{C}$ de sommets $\kappa \pm iT, 1 - c_2/\log(T) \pm iT$ et contenu dans l'ouvert $U_{\underline{f}}$ sur lequel $L_{\underline{f}}(s)$ est holomorphe, on a

$$\int_{\mathscr{C}} L_{\underline{f}}(s)x^{s+1}\frac{\mathrm{d}s}{s(s+1)} = 0,$$

puisque l'intégrande n'a aucun pôle à l'intérieur. La propriété (iv) du Théorème 6 nous permet de contrôler l'intégrale sur les côtés $[\kappa - iT, 1 - c_2/\log(T) - iT]$, $[1 - c_2/\log(T) - iT, 1 - c_2/\log(T) + iT]$ et $[1 - c_2/\log(T) + iT, \kappa + iT]$ et on obtient finalement la majoration

$$\left|\frac{1}{2i\pi}\int_{\kappa-iT}^{\kappa+iT} L_{\underline{f}}(s)x^{s+1}\frac{\mathrm{d}s}{s(s+1)}\right| \ll x^2\left(\frac{\log^k(T)}{T^2} + \exp\big(-c_3\log(x)/\log(T)\big)\right).$$

En choisissant $T = \exp\left(\sqrt{\log(x)}\right)$ on obtient

$$\int_1^x A(t)\mathrm{d}t \ll x^2 \exp\left(-c_4\sqrt{\log(x)}\right)$$

Un calcul similaire, mais où apparaît un pôle en $s = 1$ avec résidu $\Phi(x)$, fournit

$$\int_1^x B(t)\mathrm{d}t = \Phi(x) + \mathcal{O}\left(x^2 \exp\left(-c_5\sqrt{\log x}\right)\right)$$

avec $\Phi(x) = x^2 Q(\log x)$ et Q polynôme explicite. Remarquons que $\Phi''(x) = \mathcal{O}\left(\log^a(x)\right)$, où l'exposant $a > 0$ ne dépend que de h.

Pour passer à $A(x)$ (voir [**50**, paragraphe II.5.4]), on écrit

$$A(x) = u^{-1}\int_x^{x+u} A(t)\mathrm{d}t + \mathcal{O}\left(u^{-1}L\right)$$

avec $L = \int_x^{x+u} |A(t) - A(x)|\mathrm{d}t$. On observe alors que $L \leq \int_x^{x+u}(B(t) - B(x))\mathrm{d}t$ et on en tire que

$$\begin{aligned} L &\leq \int_x^{x+u} B(t)\mathrm{d}t - \int_{x-u}^{x} B(t)\mathrm{d}t \\ &= \Phi(x+u) + \Phi(x-u) - 2\Phi(x) + \mathcal{O}\left(x^2\exp\left(-c_5\sqrt{\log x}\right)\right) \\ &\leq u^2 \max_{t\in[x-u,x+u]} \Phi''(t) + \mathcal{O}\left(x^2\exp\left(-c_5\sqrt{\log x}\right)\right). \end{aligned}$$

et enfin

$$L = \mathcal{O}\left(x^2\exp\left(-c_5\sqrt{\log(x)}\right)\right) + \mathcal{O}\left(u^2\log^a(x)\right).$$

En choisissant $u = x\exp\left(-c_6\sqrt{\log x}\right)$ et en reportant dans les majorations précédentes, on obtient bien $A(x) \ll x\exp\left(-c_7\sqrt{\log(x)}\right)$. □

9. Quelques théorèmes taubériens

Pour déduire (10) de (7) et (9), on dispose d'un outil puissant, dont on trouvera la preuve dans [**27**] : voir aussi [**32**] pour un historique des théorèmes taubériens démontrés au fil du siècle dernier.

Théorème 8 (Hardy-Littlewood). — *Soit $(A_n)_{n\geq 0}$ une suite de réels positifs satisfaisant à $\lim_{z\to 1^-}(1-z)\sum_{n=0}^{\infty} A_n z^n = 1$. Alors $\lim_{n\to+\infty}\frac{1}{n}\sum_{j=0}^{n} A_j = 1$.*

Il suffit donc d'appliquer ce théorème à la suite $(A_n)_{n\geq 0}$ définie par A_0 quelconque et $A_n = \Lambda\big(f_1(n)\big)\Lambda\big(f_2(n)\big)\cdots\Lambda\big(f_k(n)\big)/C(\underline{f}) \geq 0$ pour tout $n \geq 1$, pour déduire de

$\lim_{z\to 1^-}(1-z)G_{\underline{f}}(z) = (-1)^k\, k!\, C(\underline{f}) \neq 0$ que l'on a

$$\lim_{n\to+\infty}\frac{1}{n}\,\psi_{\underline{f}}(n) = \lim_{n\to+\infty}\frac{1}{n}\sum_{j=1}^{n}\Lambda\big(f_1(j)\big)\Lambda\big(f_2(j)\big)\cdots\Lambda\big(f_k(j)\big) = C(\underline{f}).$$

Notons $\Lambda_0(n) = |\mu(n)|\Lambda(n)$, $\theta_{\underline{f}}(x) = \sum_{j\le x}\Lambda_0\big(f_1(j)\big)\Lambda_0\big(f_2(j)\big)\cdots\Lambda_0\big(f_k(j)\big)$ et introduisons la variante :

$$\lim_{n\to+\infty}\frac{1}{n}\,\theta_{\underline{f}}(n) = \lim_{n\to+\infty}\frac{1}{n}\sum_{j=1}^{n}\Lambda_0\big(f_1(j)\big)\Lambda_0\big(f_2(j)\big)\cdots\Lambda_0\big(f_k(j)\big) = C(\underline{f}).$$

On a le résultat suivant.

Théorème 9 (Baier). — *Pour toute famille $\underline{f}$ convenable* [6]*, on a*

$$\pi_{\underline{f}}(x) \sim \frac{C(\underline{f})}{h_1\dots h_n}\frac{x}{\log^k(x)} \Longleftrightarrow \theta_{\underline{f}}(x) \sim C(\underline{f})x \Longleftrightarrow \psi_{\underline{f}}(x) \sim C(\underline{f})x.$$

Ceci est fait en détail dans [**1**] : la démonstration de la première équivalence est élémentaire et repose sur l'observation que la quantité $\Lambda_0\big(f_1(j)\big)\Lambda_0\big(f_2(j)\big)\cdots\Lambda_0\big(f_k(j)\big)$ est nulle si l'un des $f_i(j)$ n'est pas premier et équivalente à $h_1\dots h_k(\log j)^k$ sinon. La démonstration de la deuxième équivalence requiert un peu plus de travail : Baier utilise notamment le théorème de Siegel et montre que $0 \le \psi_{\underline{f}}(x) - \theta_{\underline{f}}(x) \le c\sqrt{x}\log^k(x)$. Ceci généralise l'équivalence classique

$$\pi(x) \sim \frac{x}{\log(x)} \Longleftrightarrow \theta(x) \sim x \Longleftrightarrow \psi(x) \sim x,$$

où $\pi(x)$ compte les nombres premiers $\le x$, $\theta(x) = \sum_{p\le x}\log(p)$ et $\psi(x) = \sum_{n\le x}\Lambda(n)$.

L'autre théorème taubérien (Riesz 1916, Ingham 1935, Newman 1980) que nous avons utilisé peut s'énoncer ainsi.

Théorème 10. — *Soit $D(s) = \sum_{n=1}^{\infty} a_n/n^s$ une série de Dirichlet convergente sur le demi-plan $\mathrm{Re}(s) > 1$. Supposons que D soit analytiquement prolongeable à un ouvert contenant le demi-plan fermé $\mathrm{Re}(s) \ge 1$ et que, lorsque $x \to +\infty$,*

(i) ou bien $a_n = \mathcal{O}(1)$ (Ingham-Newman),

(ii) ou bien $\sum_{1\le n\le x} a_n = o(x)$ (Riesz).

Alors la série $\sum_{n=1}^{\infty} a_n/n$ est convergente, de somme $D(1)$.

Démonstration. — (i) On trouve la preuve du théorème de Ingham-Newman (cas $a_n = \mathcal{O}(1)$) dans [**40**] ou [**32**, Theorem 6.1].

Notons $A(x) = \sum_{1\le n\le x} a_n$; sous l'hypothèse (ii), une variante de la méthode de Newman (voir [**32**, Theorem 7.1]) établit que l'intégrale $\int_1^{+\infty} A(t)t^{-2}dt$ est convergente, de valeur

[6] ne satisfaisant pas obligatoirement à l'hypothèse F

$D(1)$. Or cette intégrale vaut

$$\lim_{T\to+\infty}\left(\sum_{1\leq n\leq T}\frac{a_n}{n}+\frac{A(T)}{T}\right),$$

d'où le résultat énoncé. □

Remarquons qu'en fait le théorème de Riesz (correspondant à l'hypothèse (ii)) est plus fin car il ne requiert que le prolongement analytique au voisinage de $s=1$ (voir [**43**]).

Nous terminons ce paragraphe en citant le « prince » des théorèmes taubériens.

Théorème 11 (Ikehara-Wiener). — *Soit $(a_n)_{n\geq 1}$ une suite de réels positifs à laquelle on associe la série de Dirichlet $D(s)=\sum_{n=1}^{\infty}a_n/n^s$, que l'on suppose convergente pour $\mathrm{Re}(s)>1$. Supposons qu'il existe ρ tel que $D(s)-\rho(s-1)^{-1}$ soit analytiquement, ou même seulement continûment, prolongeable au demi-plan fermé $\mathrm{Re}(s)\geq 1$. Alors*

$$\lim_{x\to+\infty}\frac{1}{x}\sum_{1\leq n\leq x}a_n=\rho.$$

Remarque. Ce théorème suggère une approche plus classique de la conjecture de Bateman-Horn qui consiste à introduire la série de Dirichlet

$$D_{\underline{f}}(s)=\sum_{n=1}^{\infty}\frac{\Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big)}{n^s}.$$

C'est exactement l'approche développée par Conrad [**14**], auquel nous renvoyons pour plus de détails : indiquons seulement qu'il transforme cette série en utilisant lui aussi l'identité de Golomb. On voit aisément que la série converge pour $\mathrm{Re}(s)>1$ et que la conjecture de Schinzel pour la famille $\underline{f}$ est vraie si, et seulement si, l'abscisse de convergence est finie. De plus, si l'on savait que la fonction $D_{\underline{f}}(s)-C(\underline{f})\,(s-1)^{-1}$ se prolonge au demi-plan fermé $\mathrm{Re}(s)\geq 1$, le théorème de Ikehara-Wiener permettrait précisément de conclure que la conjecture de Bateman-Horn est vraie : ici aussi, la valeur exacte de $C(\underline{f})$ est plus qu'il ne faut puisqu'obtenir un prolongement avec une toute autre constante positive serait suffisant. Néanmoins, compte-tenu de l'expression pour $C(\underline{f})$, on voit qu'il serait équivalent de prouver que la série de Dirichlet $k!D_{\underline{f}}(s)-\zeta(s)L_{\underline{f}}^{(k)}(s)$, ou encore $k!D_{\underline{f}}(s)-\zeta^{(k)}(s)L_{\underline{f}}(s)$, se prolonge continûment à la droite $\mathrm{Re}(s)=1$. Dans cette direction, indiquons que Korevaar [**33**] a proposé une conjecture concernant le comportement analytique précis de $D_{X(X+2)}(s)$ au voisinage de $s=1$ et qui est équivalente à $\mathbf{BH}(X(X+2))$.

10. Une seconde façon de prolonger $L_{\underline{f}}(s)$

Ce paragraphe présente une esquisse de démonstration d'un théorème de Kurokawa [**34, 35**] ; ce résultat n'est pas utilisé dans la suite (et peut donc être omis en première lecture) mais éclaire peut-être une des raisons pour lesquelles, du point de vue analytique, le cas $\deg(f)=1$ est très particulier.

Théorème 12 (Kurokawa). — *La fonction $L_{\underline{f}}(s)$ admet un prolongement méromorphe au demi-plan* $\mathrm{Re}(s) > 0$. *De plus, hormis le cas où* $\deg(f) = 1$, *la droite* $\mathrm{Re}(s) = 0$ *constitue une frontière naturelle.*

Nous commençons par traiter le cas où f est produit de k facteurs linéaires puis passerons graduellement au cas d'un polynôme cubique de groupe de Galois $\mathfrak{S}_3$ avant d'esquisser le cas général. Dans le premier cas $L_{\underline{f}}(s) = P(s)Z_k(s)$ avec $P(s)$ est un produit fini de facteurs eulériens et $Z_k(s) = \prod_p (1 - kp^{-s})$. Il suffit donc de démontrer l'assertion du théorème pour $Z_k(s)$.

Lemme 1. — *Soit k entier ≥ 2. Il existe une unique suite d'entiers $a_j \geq 1$ tels que, pour tout $m \geq 1$, on ait*

$$1 - kT = (1-T)^{a_1}(1-T^2)^{a_2} \cdots (1-T^m)^{a_m}(1 + T^{m+1}R_{m+1}(T)), \tag{17}$$

avec $R_{m+1}(T)$ série convergente pour $|T| < 1$.

Démonstration. — On calcule

$$\begin{aligned}\prod_{j=1}^{m}(1-T^j)^{-a_j} &= \prod_{j=1}^{m}\sum_{n_j=0}^{\infty}\binom{n_j + a_j - 1}{a_j - 1}T^{jn_j} \\ &= \sum_{n=0}^{\infty}\sum_{n_1+2n_2+\cdots+mn_m=n}\prod_{j=1}^{m}\binom{n_j + a_j - 1}{a_j - 1}T^n = \sum_{n=0}^{\infty}B_n^{(m)}T^n \qquad \text{(disons)}\end{aligned}$$

On voit que, si $n \leq m-1$, on a $B_n^{(m)} = B_n^{(m-1)}$ et que $B_n^{(m)} = B_n^{(m-1)} + a_m$. Ainsi, si l'on veut que le produit soit égal à $(1-kT)^{-1} = \sum_{n\geq 0} k^n T^n$ modulo T^{m+1}, on obtient une définition par récurrence des a_j :

$$a_1 = k \quad \text{et} \quad a_m = k^m - \sum_{n_1+2n_2+\cdots+(m-1)n_{m-1}=m}\binom{n_1 + a_1 - 1}{a_1 - 1}\cdots\binom{n_{m-1} + a_{m-1} - 1}{a_{m-1} - 1}$$

qui prouve l'existence et l'intégralité des a_j. En prenant le logarithme de la relation (17), on trouve que $k^m = \sum_{j\,|\,m} j a_j$, ce qui permet de montrer que $a_j \geq 1$: on vérifie en effet par récurrence que $1 \leq m a_m \leq k^m$ (noter que $\sum_{j|m, j\neq m} j a_j \leq \sum k^j \leq (k^m - 1)/(k-1)$). □

Par exemple, on a $a_1 = k$, $a_2 = k(k-1)/2$ et $a_3 = k(k-1)(9k+1)/3$. On en déduit que la fonction $Z_k(s)$ admet un prolongement méromorphe à $\mathrm{Re}(s) > 0$, qui est donné, pour $\mathrm{Re}(s) > 1/(m+1)$, par $Z_k(s) = \prod_{j=1}^{m}\zeta(js)^{-a_j}\prod_p\left(1 + p^{-(m+1)s}R_{m+1}(p^{-s})\right)$. En particulier on voit que $Z_k(s)$ s'annule ou a un pôle lorsque

(a) $s = 1/j$ avec ordre a_j ;
(b) $s = \frac{\log k}{\log p} + \frac{2\pi i m}{\log p}$, pour p premier et $m \in \mathbf{Z}$ avec ordre 1 ;
(c) $s = \rho/j$ pour ρ zéro non trivial de $\zeta(s)$ et $j \geq 1$ avec ordre $-a_j$.

Corollaire 1. — *Si $k \geq 2$, la fonction $Z_k(s)$ ne peut pas se prolonger au delà de* $\mathrm{Re}(s) > 0$.

Démonstration. — L'hypothèse $k \geq 2$ assure que $a_j \neq 0$ pour tout $j \geq 1$, ce dont on va se servir pour produire une suite de zéros ou pôles de $Z_k(s)$ s'accumulant sur la droite $\mathrm{Re}(s) = 0$. Pour cela on observe que l'ensemble

$$S = \left\{ \frac{\log k}{\log p} + \frac{2\pi i m}{\log p} \;\middle|\; p \text{ premier},\ m \in \mathbf{Z} \right\}$$

admet comme ensemble d'accumulation la droite $\mathrm{Re}(s) = 0$. De même, les ensembles $S' = \{\rho/j \mid \rho \text{ zéro non trivial de } \zeta(s) \text{ et } j \geq 1\}$ et $S" = \{\frac{\rho}{j} \mid \rho = \frac{1}{2} + it, \text{ zéro de } \zeta(s) \text{ et } j \geq 1\}$ admettent aussi comme ensemble d'accumulation la droite $\mathrm{Re}(s) = 0$.

Remarquons aussi que $\frac{\log k}{\log p} \neq \frac{1}{2j}$ car sinon $p = k^{2j}$, ce qui est impossible. Donc, si l'on admet l'hypothèse de Riemann, il ne peut y avoir aucune compensation entre zéros (b) et (c) ; sinon on invoque l'infinité de zéros non triviaux de partie réelle $1/2$ pour voir que si on restreint S' à S'' donné par les zéros de partie réelle $1/2$, ils fournissent la même conclusion. La droite $\mathrm{Re}(s) = 0$ est donc bien une frontière. □

Dans le cas d'un ou plusieurs polynômes de degré ≥ 2, nous aurons besoin des fonctions L de Dirichlet et d'Artin (voir par exemple [**38**], chapter XII). Rappelons-en la définition et les propriétés que nous utiliserons. Soit $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ le groupe de Galois absolu du corps des rationnels et soit $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbf{C})$ une représentation continue ou, ce qui revient au même, qui se factorise à travers un quotient fini ($G = G_{\mathbf{Q}}/\mathrm{Ker}(\rho)$ par exemple). Notons encore $\rho : G \to \mathrm{GL}_n(\mathbf{C})$ la représentation et notons $\mathbf{F}$ le corps fixé par $\mathrm{Ker}\{G_{\mathbf{Q}} \to G\}$ de sorte que $G = \mathrm{Gal}(\mathbf{F}/\mathbf{Q})$. On pose également $\chi_\rho = \mathrm{Tr} \circ \rho$ qu'on appelle le *caractère* de la représentation. La théorie des représentations des groupes finis en caractéristique zéro (voir par exemple [**46**]) indique que la donnée de χ équivaut à celle de ρ à isomorphisme près. Sur les fonctions sur G, on dispose du produit scalaire défini par :

$$\langle f, f' \rangle = \langle f, f' \rangle_G = \frac{1}{|G|} \sum_{g \in G} f(g) \bar{f}'(g).$$

Pour p premier et $\mathfrak{B}$ premier de $\mathcal{O}_{\mathbf{F}}$ au dessus de p, notons $\mathbf{F}_{\mathfrak{B}} = \mathcal{O}_{\mathbf{F}}/\mathfrak{B}$ et $D_{\mathfrak{B}} = \{\sigma \in G \mid \sigma\mathfrak{B} = \mathfrak{B}\}$ le *groupe de décomposition* de $\mathfrak{B}$ (au dessus de p). On sait que la réduction modulo $\mathfrak{B}$ induit un homomorphisme surjectif $D_{\mathfrak{B}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{B}}/\mathbf{F}_p)$ dont le noyau est, par définition, le *groupe d'inertie* $I_{\mathfrak{B}} = \{\sigma \in D_{\mathfrak{B}} \mid \forall x \in \mathcal{O}_F,\ \sigma(x) - x \in \mathfrak{B}\}$. Pour presque tout $\mathfrak{B}$ (ou p), le groupe d'inertie est trivial, i.e. on est dans la situation non ramifiée. Dans tous les cas, l'existence d'un générateur canonique de $\mathrm{Gal}(\mathbf{F}_{\mathfrak{B}}/\mathbf{F}_p)$, le Frobenius $x \mapsto x^p$, induit l'existence d'un élément canonique $\mathrm{Frob}_{\mathfrak{B}} \in D_{\mathfrak{B}}/I_{\mathfrak{B}}$, appelé également Frobenius. Soit $\mathfrak{B}'$ un autre idéal au dessus de p, on a $\mathfrak{B}' = \sigma\mathfrak{B}$ pour un certain $\sigma \in G$ et on voit que $D_{\mathfrak{B}'} = \sigma D_{\mathfrak{B}} \sigma^{-1}$ et $I_{\mathfrak{B}'} = \sigma I_{\mathfrak{B}} \sigma^{-1}$. En particulier l'élément $\mathrm{Frob}_{\mathfrak{B}}$ ne dépend, modulo $I_{\mathfrak{B}}$ et à conjugaison près, que de p ; on se permettra donc de le noter Frob_p. Ceci permet de définir $L_p(\rho, s) = \det\left(Id - \rho(\mathrm{Frob}_{\mathfrak{B}}) p^{-s} \,|\, V^{I_{\mathfrak{B}}}\right)^{-1}$, que l'on note aussi $L_p(\chi, s)$ et, bien sûr, la *fonction L d'Artin* $L(\rho, s) = \prod_p L_p(\rho, s)$ que l'on note aussi $L(\chi, s)$ si $\chi = \chi_\rho$. Si $\lambda_1, \ldots, \lambda_n$ sont les valeurs propres de $\rho(\mathrm{Frob}_{\mathfrak{B}})$ (ce sont des racines de l'unité), on a

$\lambda_1^m + \cdots + \lambda_n^m = \operatorname{Tr}\rho\left((\mathrm{Frob}_{\mathfrak{B}})^m\right) = \chi\left((\mathrm{Frob}_{\mathfrak{B}})^m\right)$ et ainsi :

$$\log L(\rho, s) = \sum_p \sum_{j=1}^{n} \log(1 - \lambda_j p^{-s})^{-1} = \sum_p \sum_{j=1}^{n} \sum_{m\geq 1} \frac{\lambda_j^m}{m} p^{-ms} = \sum_p \sum_{m\geq 1} \chi\left((\mathrm{Frob}_{\mathfrak{B}})^m\right) \frac{p^{-ms}}{m}.$$

Ainsi les séries et le produit d'Euler convergent absolument pour $\mathrm{Re}(s) > 1$ (voir [**38**], chapter XII).

Proposition 1 (Artin-Brauer). — *La fonction $L(\rho, s)$ admet un prolongement méromorphe au plan complexe, sans zéros ni pôles sur $\mathrm{Re}(s) = 1$ hormis le point $s = 1$ où il y a un pôle d'ordre $\dim V^G$.*

Remarques. (*i*) La preuve est basée sur le théorème de Brauer (voir [**46**], théorème 20, page 95) : le caractère de toute représentation de G est somme à coefficients dans $\mathbf{Z}$ de caractères de représentations monomiales (i.e. induites de représentations de dimension 1 de sous-groupes de G).

(*ii*) On peut obtenir également une région sans zéro et pôle (sauf $s = 1$) du type $\mathrm{Re}(s) \geq 1 - c/\log \mathrm{Im}(s)$ et des bornes $\max\{|L(\chi, s)|, |L(\chi, s)|^{-1}\} \ll (\log|\mathrm{Im}(s)|)^C$ dans ce domaine.

(*iii*) L'hypothèse de Riemann généralisée permet évidemment d'améliorer ces estimations mais n'entraîne pas, semble-t-il, la *conjecture d'Artin* qui affirme que les $L(\rho, s)$ sont entières (hormis un pôle éventuel en $s = 1$).

(*iv*) Il existe une équation fonctionnelle reliant $L(\rho, s)$ et $L(\check{\rho}, 1-s)$ où $\check{\rho}$ est la contragrédiente de ρ.

Passons maintenant à notre deuxième exemple : le cas « typique » d'un polynôme cubique f de degré 3 engendrant une extension cubique $\mathbf{K} \cong \mathbf{Q}[X]/(f)$ non galoisienne. C'est-à-dire $[\mathbf{K} : \mathbf{Q}] = 3$, la clôture galoisienne $\mathbf{F}$ de $\mathbf{K}$ est de degré 6 sur $\mathbf{Q}$ et on a $G = \mathrm{Gal}(\mathbf{F}/\mathbf{Q}) \cong \mathfrak{S}_3$ et $H = \mathrm{Gal}(\mathbf{F}/\mathbf{K}) \cong \mathbf{Z}/2\mathbf{Z}$.

Lemme 2. — *Soit p non ramifié et $\mathfrak{B}$ un idéal de $\mathcal{O}_{\mathbf{F}}$ au dessus de p.*

(*i*) *Si $D_{\mathfrak{B}} = \{1\}$ alors $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ avec $N(\mathfrak{p}_i) = p$. En particulier $A_p = 3$.*

(*ii*) *Si $D_{\mathfrak{B}}$ est cyclique d'ordre 3, alors $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}$ avec $N(\mathfrak{p}) = p^3$. En particulier $A_p = 0$.*

(*iii*) *Si $D_{\mathfrak{B}}$ est cyclique d'ordre 2, alors $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}_1\mathfrak{p}_2$ avec $N(\mathfrak{p}_1) = p$ et $N(\mathfrak{p}_2) = p^2$. En particulier $A_p = 1$.*

On peut interpréter cela ainsi en notant $\mathbf{1} : \mathfrak{S}_3 \to \mathrm{GL}_1$, $\varepsilon : \mathfrak{S}_3 \to \mathrm{GL}_1$ et $\rho : \mathfrak{S}_3 \to \mathrm{GL}_2$ les trois représentations irréductibles de $\mathfrak{S}_3$ et $\mathbf{1}, \varepsilon, \chi$ les caractères associés. On a

$$A_p = 1 + \chi(\mathrm{Frob}_p) = \begin{cases} 3 & \text{si } \mathrm{Frob}_p \text{ est d'ordre 1} \\ 1 & \text{si } \mathrm{Frob}_p \text{ est d'ordre 2} \\ 0 & \text{si } \mathrm{Frob}_p \text{ est d'ordre 3.} \end{cases}$$

Ainsi, à un nombre fini de facteurs eulériens près, on a

$$L_{\underline{f}}(s) = \prod_p \left(1 - \frac{1 + \chi(\mathrm{Frob}_p)}{p^s}\right).$$

Les premières étapes du prolongement utilisent les fonctions $L(\varepsilon,s)=\prod_p L_p(\varepsilon,s)$ et $L(\chi,s)=\prod_p L_p(\chi,s)$, où $L_p(\varepsilon,s)=(1-\varepsilon(\mathrm{Frob}_p)p^{-s})^{-1}$, $L_p(\chi,s)=\det(1-\rho(\mathrm{Frob}_p)p^{-s})^{-1}$ $=(1-\chi(\mathrm{Frob}_p)p^{-s}+\varepsilon(\mathrm{Frob}_p)p^{-2s})^{-1}$. Ainsi$(1-T)(1-\chi T+\varepsilon T^2)=1-(1+\chi)T+O(T^2)$ permet d'écrire $L_{\underline{f}}(s)=\zeta^{-1}(s)L(\chi,s)^{-1}G_2(s)$ avec $G_2(s)$ holomorphe sur $\mathrm{Re}(s)>1/2$ et a ainsi obtenu un prolongement méromorphe à ce demi-plan.

Ensuite, la relation

$$(1-T)(1-\chi T+\varepsilon T^2)(1-\varepsilon T^2)(1-\chi T^2+\varepsilon T^4)=1-(1+\chi)T+(\chi+\varepsilon\chi+\chi^2)T^3+O(T^4)$$

permet d'écrire $L_{\underline{f}}(s)=\zeta^{-1}(s)L(\chi,s)^{-1}L(\varepsilon,2s)^{-1}L(\chi,2s)^{-1}G_3(s)$ avec $G(s)$ holomorphe sur $\mathrm{Re}(s)>1/3$ et a ainsi obtenu un prolongement méromorphe à ce demi-plan.

On ne s'arrête pas là ; en effet $\chi^2(\sigma)=\mathrm{Tr}(\rho\otimes\rho(\sigma))$ donc $L_p(\rho\otimes\rho;T)^{-1}=\det(1-\rho\otimes\rho(\mathrm{Frob}_p)T)=1-\chi^2(\mathrm{Frob}_p)T+O(T^2)$ et donc

$$\begin{aligned}(1-T)(1-\chi T+\varepsilon T^2)(1-\varepsilon T^2)(1-\chi T^2+\varepsilon T^4)(1-\chi^2(\mathrm{Frob}_p)T^3+O(T^4))\\ \times(1-\chi T^3+O(T^4))(1-\varepsilon\chi T^3+O(T^4))=1-(1+\chi)T+O(T^4)\end{aligned}$$

permet d'écrire

$$L_{\underline{f}}(s)=\zeta^{-1}(s)L(\chi,s)^{-1}L(\varepsilon,2s)^{-1}L(\chi,2s)^{-1}L(\rho\otimes\rho,3s)^{-1}L(\chi,3s)^{-1}L(\varepsilon\otimes\chi,3s)^{-1}G_4(s)$$

avec $G_4(s)$ holomorphe sur $\mathrm{Re}(s)>1/4$ et a ainsi obtenu un prolongement méromorphe à ce demi-plan.

Nous allons maintenant généraliser ce calcul à tout polynôme et tout ordre. De manière générale si $\mathbf{F}$ est la clôture galoisienne de $\mathbf{K}$, $G=\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ et $H=\mathrm{Gal}(\mathbf{F}/\mathbf{K})$, la décomposition de p dans $\mathcal{O}_{\mathbf{K}}$ est gouvernée par (la classe de conjugaison) du Frobenius au dessus de p et on pourra toujours exprimer A_p comme combinaison linéaire de caractères d'Artin.

Proposition 2. — *Il existe un caractère d'Artin $\chi=\chi_\tau$ (associé à une représentation τ) tel que, pour presque tout p, on ait $N_f(p)=\chi(\mathrm{Frob}_p)$. En particulier, la fonction $L_{\underline{f}}(s)$ est égale, à un produit eulérien fini près, à la fonction*

$$L^*_{\underline{f}}(s)=\prod_p\left(1-\frac{\chi(\mathrm{Frob}_p)}{p^s}\right).$$

La preuve de la proposition précédente s'appuie sur le lemme suivant qui a son intérêt propre.

Lemme 3. — *Soit $\mathbf{F}$ une extension galoisienne de $\mathbf{Q}$ de groupe G, H un sous-groupe et $\mathbf{K}=\mathbf{F}^H$ le sous-corps de $\mathbf{F}$ fixé par H. Notons A_p le nombre d'idéaux de $\mathbf{K}$ de norme p, on a alors*

$$A_p=\sum_\chi \dim V_\chi^H\chi(\mathrm{Frob}_p)=1+\sum_{\chi\neq 1}\dim V_\chi^H\chi(\mathrm{Frob}_p),$$

où la somme est prise sur les caractères χ des représentations irréductibles $\rho: G\to\mathrm{GL}(V)$.

Remarque. On peut vérifier directement que A_p ne dépend que de $\mathbf{K}$ (et pas de la clôture galoisienne $\mathbf{F}$ choisie). On notera dans la suite $\mathscr{I}_G$ l'ensemble des représentations irréductibles de G et $\mathscr{I}_G^* = \mathscr{I}_G \setminus \{1\}$ l'ensemble des représentations irréductibles non triviales.

Corollaire 2. — *Soit $f = f_1 \dots f_k$ avec f_i irréductibles distincts à coefficients entiers. Posons $\mathbf{K}_i = \mathbf{Q}[X]/(f_i)$, choisissons $\mathbf{F}$ une extension galoisienne de groupe G avec des sous-groupes H_i, tels que $\mathbf{K}_i \cong \mathbf{F}^{H_i}$. Alors, pour presque tout p, on a*

$$N_f(p) = k + \sum_{i=1}^{k} \sum_{\chi \in \mathscr{I}_G^*} \dim \left(V_\chi^{H_i}\right) \chi(\mathrm{Frob}_p).$$

Démonstration du Lemme 3. — Soit $\mathfrak{B}$ un idéal de $\mathcal{O}_\mathbf{F}$ au dessus de p, de sorte que $N(\mathfrak{B}) = p^f$ avec $|D_\mathfrak{B}| = f$. On écrit les décompositions $p\mathcal{O}_\mathbf{K} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ et $\mathfrak{p}_j = \mathfrak{B}_1^{(j)} \cdots \mathfrak{B}_{h_j}^{(j)}$ avec $N(\mathfrak{p}_j) = p^{f/f_j}$ où $f_j = |D_{\mathfrak{B}_1^{(j)}/\mathfrak{p}_j}| = |D_{\mathfrak{B}_1^{(j)}} \cap H|$. On voit que $N(\mathfrak{p}_j) = p$ équivaut à $f_j = f$ ou encore à $D_{\mathfrak{B}_1^{(j)}} \subset H$. Par ailleurs, dans ce cas, en prenant les normes on obtient la valeur de h_j par $p^{|H|} = N_\mathbf{Q}^F(\mathfrak{p}_j\mathcal{O}_\mathbf{F}) = \prod_{i=1}^{h_j} N_\mathbf{Q}^F(\mathfrak{B}_i^{(j)}) = p^{fh_j}$. On en déduit alors que $A_p = |\{\sigma \in H\backslash G \,|\, \sigma D_\mathfrak{B} \sigma^{-1} \subset H\}| = |\{\sigma \in G \,|\, \sigma D_\mathfrak{B} \sigma^{-1} \subset H\}| \,/|H|$. Calculons maintenant la décomposition dans la base des caractères de la fonction centrale donnée par $\phi(g) = \#\{\sigma \in G \mid \sigma g \sigma^{-1} \in H\}$ (telle que $A_p = \phi(\mathrm{Frob}_p)/|H|$). Pour cela, on va utiliser le résultat classique suivant.

Fait 1. — *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation, $H \subset G$ et $\chi = \mathrm{Tr} \circ \rho$. Alors*

$$\sum_{g \in H} \chi(g) = \sum_{g \in H} \bar{\chi}(g) = |H| \dim V^H.$$

Démonstration. — La représentation restreinte $\rho_{|H}$ se décompose en $\rho_1 \oplus \cdots \oplus \rho_s$ avec ρ_i irréductibles. Or si χ irréductible, on a

$$\langle 1, \chi \rangle_H = \frac{1}{|H|} \sum_{g \in H} \bar{\chi}(g) = \begin{cases} 0 & \text{si } \chi \neq 1 \\ 1 & \text{si } \chi = 1, \end{cases}$$

d'où l'affirmation. □

Revenons à la preuve du Lemme 3. Il suffit de calculer

$$|G|\langle \phi, \chi \rangle = \sum_{g \in G} \phi(g)\bar{\chi}(g) = \sum_{\substack{g,\sigma \in G \\ \sigma g \sigma^{-1} \in H}} \bar{\chi}(g) = \sum_{\sigma \in G} \dim \left(V^{\sigma^{-1} H \sigma}\right) |\sigma^{-1} H \sigma| = |H|\,|G| \dim V^H.$$

Ainsi on a bien

$$\frac{\phi(g)}{|H|} = \sum_\chi \frac{\langle \phi, \chi \rangle \chi(g)}{|H|} = \sum_\chi \dim V_\chi^H \chi(g),$$

comme annoncé. □

Revenons au problème du prolongement analytique de $L_{\underline{f}}(s)$ dans le cas général. On voit donc que, toujours à un nombre fini de facteurs eulériens près et avec les conventions précédentes, on a

$$L_{\underline{f}}(s) = \prod_p \left(1 - \frac{(a_1\chi_1 + a_2\chi_2 + \cdots + a_t\chi_t)(\mathrm{Frob}_p)}{p^s}\right),$$

avec disons $\chi_1 = 1$ et $a_1 = r$ et les autres χ_i irréductibles et non triviaux. On utilisera que $\chi_1^{m_1} \cdots \chi_r^{m_r}$ est la trace de $\rho_1^{\otimes m_1} \otimes \cdots \otimes \rho_r^{\otimes m_r}$ donc

$$L(\rho_1^{\otimes m_1} \otimes \cdots \otimes \rho_r^{\otimes m_r}, s) = \prod_p (1 - \chi_1^{m_1} \cdots \chi_r^{m_r}(\mathrm{Frob}_p)p^{-s})^{-1}(1 + O(p^{-2s})).$$

La première étape du prolongement analytique (jusqu'à $\mathrm{Re}(s) > 1/2$) consiste à écrire

$$\begin{aligned} 1 - (a_1\chi_1 + \cdots + a_t\chi_t)T &= (1 - \chi_1 T)^{a_1} \cdots (1 - \chi_t T)^{a_t}(1 + O(T^2)) \\ &= L_p(\chi_1, T)^{-a_1} \cdots L_p(\chi_t, T)^{-a_t}(1 + O(T^2)) \end{aligned}$$

d'où l'on tire $L_{\underline{f}}(s) = L(\chi_1, s)^{-a_1} \cdots L(\chi_t, s)^{-a_t} G_2(s)$ avec $G_2(s)$ définie par un produit d'Euler convergent pour $\mathrm{Re}(s) > 1/2$. En se souvenant que $L(\chi_1, s)^{-a_1} = \zeta(s)^{-r}$ et que les autres $L(\chi_i, s)$ sont holomorphes sans zéros sur $\mathrm{Re}(s) = 1$, on retrouve le prolongement et le comportement de $L_{\underline{f}}(s)$ au voisinage de cette droite.

Lemme 4. — *Il existe une suite de représentation ρ_j telles que*

$$1 - \chi_\tau T = \prod_{1 \le j} \det\left(1 - \rho_j T^j\right) = \prod_{1 \le j \le m} \det\left(1 - \rho_j T^j\right)\left(1 + O\left(T^{m+1}\right)\right).$$

Pour le calcul nous utiliserons le fait classique suivant (Voir Serre [**46**], paragraphe 9.1, exercice 3).

Fait 2. — *Soit $\rho : G \to GL$ une représentation. Notons $\mathrm{Sym}^r \rho$ (resp. $\wedge^r \rho$) la r-ième puissance symétrique (resp. la r-ième puissance alternée). Pour un caractère χ, notons $\Psi^r\chi$ le caractère défini par $\Psi^r\chi(g) = \chi(g^r)$. On a les formules*

$$\begin{aligned} \det(1 - \rho(g)T)^{-1} &= \sum_{r \ge 0} \chi_{\mathrm{Sym}^r \rho}(g) T^r = \exp\left(\sum_{r \ge 1} \Psi^r \chi_\rho(g) \frac{T^r}{r}\right), \\ \det(1 - \rho(g)T) &= \sum_{r \ge 0} (-1)^r \chi_{\Lambda^r \rho}(g) T^r. \end{aligned}$$

Soient ρ_j une suite de représentations. On a

$$\begin{aligned}\prod_{j=1}^{m}\det\left(1-\rho_j T^j\right)^{-1} &= \prod_{j=1}^{m}\sum_{r_j\geq 0}\chi_{\mathrm{Sym}^{r_j}\rho_j}T^{jr_j}\\ &= \sum_{n\geq 0}\sum_{r_1+2r_2+\cdots+mr_m=n}\chi_{\mathrm{Sym}^{r_1}\rho_1}\cdots\chi_{\mathrm{Sym}^{r_m}\rho_m}T^n=\sum_{n\geq 0}\chi_n^{(m)}T^n \ \text{(disons)}.\end{aligned}$$

Observons que, pour $n\leq m-1$, on a $\chi_n^{(m)}=\chi_n^{(m-1)}$, alors que $\chi_m^{(m)}=\chi_m^{(m-1)}+\chi_{\rho_m}$. Si on veut que cette expression soit égale à $(1-\chi_\tau T)^{-1}=\sum_{n\geq 0}\chi_\tau^n T^n$, on trouve une définition par récurrence des ρ_j :

$$\chi_{\rho_1}=\chi_\tau \quad\text{et}\quad \chi_{\rho_m}=\chi_{\tau\otimes\cdots\otimes\tau}-\sum_{r_1+2r_2+\cdots+(m-1)r_{m-1}=m}\chi_{\mathrm{Sym}^{r_1}\rho_1\otimes\cdots\otimes\mathrm{Sym}^{r_{m-1}}\rho_{m-1}}$$

qui prouve le lemme avec $\rho_j\in R(G)$, i.e. ρ_j représentation « virtuelle ». En prenant le logarithme de la relation donnée par le lemme, on obtient :

$$\sum_{n\geq 1}\chi_\tau^n\frac{T^n}{n}=\sum_{j\geq 1}\sum_{r\geq 1}\Psi^r\chi_{\rho_j}\frac{T^{jr}}{r}=\sum_{n\geq 1}\left(\sum_{j\,|\,n}j\Psi^{n/j}\chi_{\rho_j}\right)\frac{T^n}{n}.$$

D'où la deuxième relation $\chi_{\tau\otimes\cdots\otimes\tau}=\sum_{j\,|\,n}j\Psi^{n/j}\chi_{\rho_j}$ qui permet de voir que $(\dim\tau)^n=\sum_{j\,|\,n}j\dim\rho_j$ et donc $\dim\rho_n=\frac{1}{n}\sum_{j\,|\,n}\mu(n/j)(\dim\tau)^j$. La fin de la preuve que les ρ_j sont effectives est laissée au lecteur ; par exemple si on note $\mathrm{T}^n\sigma$ la représentation telle que $\sigma\otimes\mathrm{Sym}^{n-1}\sigma=\mathrm{T}^n\sigma\oplus\mathrm{Sym}^n\sigma$, on a $\rho_2=\mathrm{T}^2\rho_1=\Lambda^2\rho_1$, $\rho_3=\mathrm{T}^3\rho_1$ et $\rho_4=\mathrm{T}^4\rho_1\oplus\mathrm{T}^2(T^2\rho_1)$, etc.

On peut donc écrire $L_{\underline{f}}(s)=\prod_{1\leq j\leq m}L(\chi_{\rho_j},js)^{-1}G_{m+1}(s)$ avec G_{m+1} holomorphe sur $\mathrm{Re}(s)>1/(m+1)$. Comme chacune des fonctions $L(\chi_{\rho_j},js)$ se prolonge (méromorphiquement) au plan complexe, on obtient bien ainsi un prolongement méromorphe de de $L_{\underline{f}}$ au demi-plan $\mathrm{Re}(s)>0$. De nouveau les pôles ou zéros vont s'accumuler vers la droite imaginaire ; c'est clair si l'on admet l'hypothèse de Riemann mais on peut s'en passer en examinant plus finement les résultats connus sur la densité des zéros (voir [**35**]).

11. Preuve du théorème de Bateman-Stemmler

L'argument donné ci-dessous pour prouver le Théorème 2 est essentiellement celui dans l'article de Bateman et Stemmler [**4**] : il nous semble cependant intéressant de le reproduire ici car il est court (une fois admise l'estimation générale du grand crible) et utilise les propriétés analytiques de la fonction $L_{\underline{f}}(s)$. Soit X un ensemble d'entiers contenu dans l'intervalle $[1,N]$. Si l'image de X dans $\overline{\mathbf{Z}}/p\mathbf{Z}$ a un cardinal borné par $p\,(1-\omega_p)$ (pour des « densités » $0\leq\omega_p\leq 1$) alors, pour tout $Q\geq 1$, l'application du grand crible (voir [**5**, Théorème 6, page 20] ou [**50**, I.4.5, Corollaire 6]) donne :

$$\mathrm{card}(X) \leq \frac{(N+Q^2)}{L(Q)} \quad \text{avec} \quad L(Q) = \sum_{n\leq Q} |\mu(n)| \prod_{p|n} \frac{\omega_p}{1-\omega_p}. \tag{18}$$

Dans le cas qui nous intéresse, on choisit pour X l'ensemble $X(\underline{f})$ des entiers n dans l'intervalle $[c\sqrt{N}, N]$ tels que les $f_i(n)$ soient tous premiers et on pose $Q = N^{1/2-\varepsilon}$. On remarque alors que si $p \leq Q$ et $n \in X$ alors, comme $f_i(n) \geq c' n^{h_i} \geq c'(c\sqrt{N})^{h_i} > Q$ et donc $p < f_i(n)$ (au moins si la constante c a été convenablement choisie) : p ne divise donc pas $f_i(n)$. On peut donc écarter $N_{\underline{f}}(p)$ valeurs mod p. En d'autres termes, on peut appliquer le crible à l'ensemble $X(\underline{f})$ avec les densités $\omega_p = N_f(p)/p$. Pour estimer $L(Q)$, posons $a_n = |\mu(n)| \prod_{p|n} \frac{\omega_p}{1-\omega_p}$ et introduisons la série de Dirichlet $P(s) = \sum_{n\geq 1} a_n/n^s$. On a

$$P(s) = \prod_p \left(1 + \frac{N_f(p)p^{-1-s}}{1 - N_f(p)p^{-1}}\right)$$

et on voit aisément que $P(s) = L_{\underline{f}}(s+1)^{-1} R(s)$, où $R(0) = 1$ et le produit définissant R est convergent pour $\mathrm{Re}(s) > -1$. On a vu (Théorème 6) que $L_{\underline{f}}(s)$ est équivalente à $C(\underline{f})(s-1)^k$ au voisinage de $s = 1$: la fonction $P(s)$ est donc équivalente à $C(\underline{f})^{-1} s^{-k}$ au voisinage de $s = 0$ et, hormis ce pôle, admet un prolongement holomorphe au demi-plan fermé $\mathrm{Re}(s) \geq 0$. En utilisant un théorème taubérien, on peut conclure que $L(Q) = \sum_{n\leq Q} a_n \sim (k!\, C(\underline{f}))^{-1} \log^k(Q)$.

L'inégalité de grand crible (18) donne donc $|X(\underline{f})| \leq k!\, 2^k\, C(\underline{f}) N \log^{-k}(N)(1+o(1))$ et finalement, comme $\pi_{\underline{f}}(N) \leq c\sqrt{N} + |X(\underline{f})|$, on obtient bien la majoration annoncée par le Théorème 2.

12. L'interversion limite et série

Le problème majeur et non résolu de la méthode de Golomb est de justifier l'interversion limite-série dans (7). Nous discutons de cette question dans ce paragraphe en montrant d'une part que cet obstacle peut être surmonté dans le cas d'un polynôme linéaire et en montrant d'autre part que l'analogue de cette interversion peut être justifiée dans d'autres situations.

12.1. Le cas d'un polynôme linéaire. — Lorsqu'on spécialise la conjecture de Bateman-Horn au cas $k = 1$ et $f = f_1$ linéaire, on obtient pour $f(X) = X$, resp. $f(X) = aX+b$, le théorème des nombres premiers, resp. le théorème de Dirichlet - de la Vallée-Poussin (Théorème 1). Un fait remarquable est que, dans ce cas, on sait justifier l'interversion limite-somme dans l'approche par le Λ-calcul, qui fournit donc une preuve du théorème des nombres premiers dans les progressions arithmétiques (dans le cas du théorème des nombres premiers, cette preuve est essentiellement celle donnée par Wiener). Il serait intéressant de démontrer le théorème de Dirichlet par l'étude de la série $\sum_{n=1}^{\infty} \Lambda(an+b)/n^s$.

Calculons d'abord la constante $C(aX+b)$. Pour cela, il nous faut déterminer $N_{aX+b}(p)$. Si p divise a, on a $N_{aX+b}(p)=0$ puisque $(a,b)=1$. Si p ne divise pas a, alors $(a,p)=1$ et il existe un entier c (unique modulo p) tel que $ac\equiv 1\,[p]$ et $-bc$ est alors l'unique solution (modulo p) de l'équation $an+b\equiv 0\,[p]$, d'où $N_{aX+b}(p)=1$ dans ce cas. On a donc

$$C(aX+b)=\prod_{p\,|\,a}\left(\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{0}{p}\right)\right)\prod_{p\nmid a}\left(\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{1}{p}\right)\right)=\frac{a}{\varphi(a)}.$$

Pour la démonstration du Théorème 1 nous utilisons un résultat prouvé dans le livre de Hardy [**26**, Theorem 5, p. 49, III.3.5] qui se traduit pour les séries ainsi.

Théorème 13 (Schur-Toeplitz). — *Soit une suite de fonctions $\Phi_n(z)$ définies au voisinage de $\omega\in\mathbf{C}\cup\{\infty\}$. Supposons qu'elles vérifient les deux conditions suivantes :*

$$\sum_{n=1}^{\infty}|\Phi_n(z)-\Phi_{n+1}(z)|\le H, \tag{$s1$}$$

$$\lim_{z\to\omega}\Phi_n(z)=1. \tag{$s2$}$$

Alors, si une série $\sum_{n=1}^{\infty}a_n$ est convergente, la série $\sum_{n=1}^{\infty}a_n\Phi_n(z)$ l'est également et on a

$$\lim_{z\to\omega}\sum_{n=1}^{\infty}a_n\Phi_n(z)=\sum_{n=1}^{\infty}a_n\lim_{z\to\omega}\Phi_n(z)=\sum_{n=1}^{\infty}a_n.$$

Remarques. (*i*) On peut montrer (*cf. loc. cit.*) que les conditions ($s1$), ($s2$) sont également nécessaires. Dans ces conditions, on dit que la transformation $\Phi_n(z)$ est *régulière*.

(*ii*) Si l'on sait que $\Phi_n(z)\ge 0$ et que la suite est décroissante (par rapport à n) alors

$$\sum_{n=1}^{N}|\Phi_n(z)-\Phi_{n+1}(z)|=\sum_{n=1}^{N}(\Phi_n(z)-\Phi_{n+1}(z))=\Phi_1(z)-\Phi_{N+1}(z)\le\Phi_1(z)\le H$$

donc ($s1$) est bien vérifiée et on observe au passage que la suite $\Phi_n(z)$ est uniformément bornée. Un peu plus généralement, si la suite est positive et uniformément bornée (disons $\Phi_n(z)\le H$) et est décroissante pour $n\ge n_0=n_0(z)$ et croissante auparavant (on pourrait autoriser un nombre fini borné de changements) alors

$$\begin{aligned}\sum_{n=1}^{N}|\Phi_n(z)-\Phi_{n+1}(z)| &= \sum_{n=1}^{n_0-1}(\Phi_{n+1}(z)-\Phi_n(z))+\sum_{n=n_0}^{N}(\Phi_n(z)-\Phi_{n+1}(z))\\ &= 2\Phi_{n_0}(z)-\Phi_1(z)-\Phi_{N+1}(z)\le 2\Phi_{n_0}(z)\le 2H.\end{aligned}$$

Pour appliquer le Théorème 13, on prend d'abord $\omega=1^-$ et [(7)]

$$\Phi_n(z)=\frac{nz^n(1-z)}{1-z^n}.$$

[(7)] Ce procédé de sommation est connu sous le nom de transformation de Lambert.

On a bien sûr $\lim_{z\to 1^-}\Phi_n(z)=1$ (condition $(s2)$) et un calcul direct donne

$$\Phi_n(z)-\Phi_{n+1}(z)=\frac{z^n\,(n-z(1+z+\cdots+z^{n-1}))}{(1+z+\cdots+z^{n-1})(1+z+\cdots+z^n)}\geq 0.$$

Donc

$$\sum_{n=1}^{\infty}|\Phi_n(z)-\Phi_{n+1}(z)|=\sum_{n=1}^{\infty}(\Phi_n(z)-\Phi_{n+1}(z))=\Phi_1(z)\leq 1,$$

et la condition $(s2)$ est également vérifiée. On conclut donc que, pour toute série $\sum_n a_n$ convergente, on a :

$$\lim_{z\to 1^-}(1-z)\sum_{n=1}^{\infty}\frac{na_nz^n}{(1-z^n)}=\sum_{n=1}^{\infty}a_n.$$

Plus généralement, soit $c>0$ et z tel que $|z^c|<1$; on choisit

$$\Phi_n(z)=\frac{nz^{cn}(1-z)}{1-z^n}$$

qui vérifie trivialement $(s2)$ et est uniformément bornée : c'est évident pour $c\geq 1$ et si $c<1$, choisissons $m>1/c$ et posons $n=qm+r$ avec $r<m$, alors $1+z+\cdots+z^{n-1}\geq qz^{q-1}$ et $\Phi_n(z)\leq nz^{cn}/qz^{q-1}=(m+r/q)z^{(cm-1)q+rc+1}\leq 2m$. On vérifie ensuite par *calculus* que, pour $c\geq 1/2$, la suite $\Phi_n(z)$ est décroissante et que, pour $c<1/2$, elle est croissante puis décroissante. On conclut donc que, pour toute série $\sum_n a_n$ convergente, on a :

$$\lim_{z\to 1^-}(1-z)\sum_{n=1}^{\infty}\frac{na_nz^{cn}}{1-z^n}=\sum_{n=1}^{\infty}a_n.$$

Nous sommes maintenant en position de justifier l'interversion limite-série (7) :

$$\lim_{z\to 1^-}(1-z)\sum_{d=1}^{\infty}\frac{\mu(d)\log^k(d)}{1-z^n}\sum_{\substack{n=1\\ d|f(n)}}^{d}z^n\stackrel{?}{=}\sum_{d=1}^{\infty}\frac{\mu(d)\log^k(d)N_f(d)}{d}$$

dans le cas des théorèmes des nombres premiers et de la progression arithmétique (c'est-à-dire lorsque $k=1$ et $f=f_1$ est linéaire).

Dans le cas du théorème des nombres premiers, on a $f(n)=n$ et donc $\sum_{1\leq n\leq d,d|f(n)}z^n=z^d$, $\Phi_d(z)=dz^d(1-z)/(1-z^d)$ et l'interversion limite-série est donc justifiée par la regularité de la transformation de Lambert (12.1) :

$$\lim_{z\to 1^-}\sum_{d=1}^{\infty}\frac{\mu(d)\log(d)\,z^d(1-z)}{1-z^d}=\sum_{d=1}^{\infty}\frac{\mu(d)\log(d)}{d}=-1.$$

Dans le cas du théorème de la progression arithmétique, on a $f(n)=an+b$. L'équation $an+b\equiv 0[d]$ possède une unique solution $n_0(d)$ dans l'intervalle $[1,d]$ si $(a,d)=1$ et aucune solution si $(a,d)>1$. Supposons donc $(a,d)=1$ et soit $\delta\in(\mathbf{Z}/a\mathbf{Z})^*$ la classe de congruence de d. Soit $\ell(\delta)$ le représentant dans l'intervalle $[1,a]$ de $b\delta^{-1}\in(\mathbf{Z}/a\mathbf{Z})^*$.

Lemme 5. — *Avec les notations précédentes, on a $n_0(d)=(\ell(\delta)d-b)/a$ pour tout $d>b$.*

Démonstration. — Tout d'abord $\ell(\delta)d - b \equiv \ell(\delta)\delta - b \equiv 0[a]$ donc n_0 est bien entier. Ensuite $an_0 + b = \ell(\delta)d \equiv 0[d]$ et enfin, comme $1 \leq \ell(\delta) \leq a$ et $d > b$, on a bien $0 < (d-b)/a \leq n_0 \leq d - b/a < d$. □

On a donc $\sum_{1\leq n\leq d, d|f(n)} z^n = z^{n_0(d)} = z^{-b/a}\left(z^{\ell(\delta)/a}\right)^d$ pour $d > b$: on commettra l'abus de notation sans conséquence que cette identité reste valable pour $d \leq b$. Par ailleurs, posons $G = (\mathbf{Z}/a\mathbf{Z})^*$ et $\hat{G}$ son groupe des caractères et étendons tout caractère $\chi \in \hat{G}$ en un caractère de Dirichlet en posant $\chi(d) = \chi(d \bmod a)$ si $(a,d) = 1$ et $\chi(d) = 0$ si $(a,d) > 1$. Rappelons que

$$\frac{1}{\varphi(a)}\sum_{\chi\in\hat{G}} \bar{\chi}(b)\chi(x) = \begin{cases} 1 \text{ si } x \equiv b[a], \\ 0 \text{ si } x \not\equiv b[a]. \end{cases}$$

En fait, si χ est un caractère de Dirichlet, modulo a disons, on a

$$L(\chi,s)^{-1} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{d=1}^{\infty} \frac{\chi(d)\mu(d)}{d^s}$$

et donc

$$\sum_{d=1}^{\infty} \frac{\chi(d)\mu(d)\log(d)}{d^s} = -\frac{L'(\chi,s)}{L(\chi,s)^2}.$$

Le cas du caractère unité doit être traité séparément et correspond à $\zeta(s)^{-1}$ sauf pour les facteurs eulériens en p divisant a.

D'après les propriétés classiques des $L(\chi,s)$, la fonction $\sum_{d=1}^{\infty}\chi(d)\mu(d)\log(d)/d^s$, a priori définie pour $\mathrm{Re}(s) > 1$, admet un prolongement analytique au demi-plan $\mathrm{Re}(s) \geq 1$ et même à un ouvert du type $\sigma > 1 - c/\log(|t|+2)$. Par le théorème de Newman ou des calculs classiques dans ce cas, on conclut que

$$\sum_{d=1}^{\infty} \frac{\chi(d)\mu(d)\log(d)}{d} \text{ est convergente et vaut } -\frac{L'(\chi,1)}{L(\chi,1)^2}.$$

Dans le cas du caractère unité modulo a, si l'on note $\zeta_a(s) = \zeta(s)\prod_{p\,|\,a}(1-p^{-s})$, on a

$$\sum_{d=1,(d,a)=1}^{\infty} \frac{\mu(d)\log(d)}{d} = \left[\frac{-1}{\zeta_a(s)}\right]'_{|\,s=1} = -\frac{a}{\varphi(a)}.$$

On obtient donc en utilisant le lemme 5 et les équations (12.1) et (6) :

$$\begin{aligned}
\lim_{z\to 1^-}\sum_{d=1}^{\infty}\frac{\mu(d)\log(d)\,z^{n_0(d)}(1-z)}{1-z^d} &= \lim_{z\to 1^-}\sum_{\delta\in G}\sum_{d=1,d\equiv\delta[a]}^{\infty} z^{\frac{-b}{a}}\frac{\mu(d)\log(d)\,z^{\ell(\delta)d/a}(1-z)}{1-z^d}\\
&= \frac{1}{\varphi(a)}\sum_{\delta\in G}\sum_{\chi\in\hat{G}}\bar{\chi}(\delta)\lim_{z\to 1^-}\sum_{d=1}^{\infty} z^{\frac{-b}{a}}\frac{\chi(d)\mu(d)\log(d)\,z^{\frac{\ell(\delta)d}{a}}}{1+z+\cdots+z^{d-1}}\\
&= \frac{1}{\varphi(a)}\sum_{\delta\in G}\sum_{\chi\in\hat{G}}\bar{\chi}(\delta)\sum_{d=1}^{\infty}\frac{\chi(d)\mu(d)\log(d)}{d}\\
&= \sum_{d=1,(d,a)=1}^{\infty}\frac{\mu(d)\log(d)}{d} = -\frac{a}{\varphi(a)}
\end{aligned}$$

et l'interversion limite-série est donc justifiée.

Remarque. Revenons au cas général de Bateman-Horn et posons, si $N_f(d)\neq 0$,

$$\Phi_d(z)=\frac{d(1-z)\sum_{1\le n\le d, d|f(n)} z^n}{N_f(d)(1-z^d)}$$

qui vérifie $(s2)$ mais probablement pas $(s1)$ en général. Noter que le choix de la valeur de $\Phi_d(z)$ lorsque $N_f(d)=0$ n'a *a priori* aucune incidence sur le résultat à démontrer, mais qu'il peut être déterminant pour une éventuelle preuve. La généralisation ou variante suivante du Théorème 13 (qui correspond au cas $r(n)=1$) pourrait être utile.

Variante. *Soit une suite de fonctions $\Phi_n(z)$ définies au voisinage de $\omega\in\mathbf{C}\cup\{\infty\}$ et soit $r(n)$ une suite positive décroissante. Supposons qu'elles vérifient les deux conditions suivantes :*

$$\sum_{n=1}^{\infty} r(n)\,|\Phi_n(z)-\Phi_{n+1}(z)|\le H, \tag{$s1_r$}$$

$$\lim_{z\to\omega}\Phi_n(z)=1. \tag{$s2$}$$

Si une série $\sum_{n=1}^{\infty}a_n$ est convergente et telle que $\sum_{n>N}a_n=o(r(N))$, alors la série $\sum_{n=1}^{\infty}a_n\Phi_n(z)$ l'est également et on a

$$\lim_{z\to\omega}\sum_{n=1}^{\infty}a_n\Phi_n(z)=\sum_{n=1}^{\infty}a_n\lim_{z\to\omega}\Phi_n(z)=\sum_{n=1}^{\infty}a_n.$$

Démonstration. — Quitte à remplacer a_n par $a'_n=a_n$ pour $n\ge 2$ et $a'_1=a_1-\sum_{n=1}^{\infty}a_n$ pour $n=1$, on peut supposer $\sum_{n=1}^{\infty}a_n=0$ et donc $S_N=\sum_{n=1}^{N}a_n=o(r(N))$. Alors si $\varepsilon>0$ est donné, il existe N tel que, pour $n\ge N$ on ait $|S_n|\le\varepsilon r(n)$. Par ailleurs, d'après

$(s2)$, si z est suffisamment proche de ω, on aura $\sum_{n=1}^{N} |S_n|\,|\Phi_n(z)-\Phi_{n+1}(z)| \le \varepsilon$ et donc, en utilisant également $(s1_r)$ on obtient

$$\left|\sum_{n=1}^{\infty} a_n\Phi_n(z)\right| = \left|\sum_{n=1}^{\infty} S_n(\Phi_n(z)-\Phi_{n+1}(z))\right| \le \varepsilon + \left|\sum_{n>N}^{\infty} S_n(\Phi_n(z)-\Phi_{n+1}(z))\right| \le \varepsilon+\varepsilon H,$$

ce qui achève la preuve. □

Choisissons une fonction $r(n)$ telle que $\sum_{d\ge n}\mu(d)\log^k(d)N_f(d)/d = o(r(n))$. Pour que la condition $(s1_r)$ soit vérifiée, il suffirait donc que

$$\sum_{n=1}^{\infty} r(n)\,|\Phi_n(z)-\Phi_{n+1}(z)| \le H.$$

Remarquons que la majoration que nous avons prouvée au paragraphe 8 concernant la somme $\sum_{d\le n}\mu(d)\log^k(d)N_f(d)$ permet de prendre $r(n)=\exp(-c\sqrt{\log n})$, cette estimation pouvant bien sûr être améliorée modulo l'hypothèse de Riemann (pour les fonctions zêta de Dedekind). Cependant nous ne sommes pas parvenus à des majorations satisfaisantes, hormis les cas cités.

12.2. Deux exemples de passage à la limite. — Nous donnons maintenant deux exemples liés aux transformations de Golomb et où le passage à la limite est justifiable rigoureusement. Le premier exemple est particulièrement surprenant, mais la preuve que nous en donnons est trop spéciale pour éclairer le seul cas qui nous importe, $\ell = k$.

Théorème 14. — *Soit $(f_1,\dots,f_k)$ une famille convenable vérifiant l'hypothèse F. Alors, pour tout entier ℓ tel que $0\le\ell<k$, on a*

$$\lim_{z\to1^-}\sum_{d=1}^{\infty}\mu(d)\log^\ell(d)\frac{\sum_{\substack{n=1,\dots,d\\ f(n)\equiv0\,[d]}} z^n}{\sum_{n=0,\dots,d-1} z^n} = \sum_{d=1}^{\infty}\mu(d)\log^\ell(d)\lim_{z\to1^-}\frac{\sum_{\substack{n=1,\dots,d\\ f(n)\equiv0\,[d]}} z^n}{\sum_{n=0,\dots,d-1} z^n},$$

la valeur commune étant 0.

Démonstration. — On a

$$\sum_{d=1}^{\infty}\mu(d)\log^\ell(d)\lim_{z\to1^-}\frac{\sum_{\substack{n=1,\dots,d\\ f(n)\equiv0\,[d]}} z^n}{\sum_{n=0,\dots,d-1} z^n} = \sum_{d=1}^{\infty}\mu(d)\log^\ell(d)\frac{N_f(d)}{d}$$

et les résultats du paragraphe 8 justifient que ces deux séries sont égales à $(-1)^\ell L_{\underline{f}}^{(\ell)}(1)$. On a aussi vu que la fonction $L_{\underline{f}}(s)$ admet un zéro d'ordre k en $s=1$. D'où

$$\sum_{d=1}^{\infty}\mu(d)\log^\ell(d)\lim_{z\to1^-}\frac{\sum_{\substack{n=1,\dots,d\\ f(n)\equiv0\,[d]}} z^n}{\sum_{n=0,\dots,d-1} z^n} = 0 \quad \text{pour } 0\le\ell<k.$$

Pour justifier que la fonction

$$F_{\underline{f},\ell}(z) = \sum_{d=1}^{\infty} \mu(d) \log^{\ell}(d) \frac{\sum_{\substack{n=1,\dots,d \\ f(n)\equiv 0\,[d]}} z^n}{\sum_{n=0,\dots,d-1} z^n}$$

tend vers 0 quand $z \to 1^-$, nous allons montrer beaucoup plus, à savoir que $F_{\underline{f},\ell}(z)$ est identiquement nulle ! En effet, en effectuant à l'envers le calcul fait au paragraphe 5, on obtient

$$F_{\underline{f},\ell}(z) = (1-z) \sum_{n=1}^{\infty} \Bigg(\sum_{\substack{d\geq 1 \\ d \mid f(n)}} \mu(d) \log^{\ell}(d) \Bigg) z^n.$$

Or par le Théorème 5, on a

$$\sum_{\substack{d\geq 1 \\ d \mid f(n)}} \mu(d) \log^{\ell}(d) = 0 \quad \text{pour } n \geq 1 \text{ et } 0 \leq \ell < k,$$

ce qui conclut la démonstration. □

Un des problèmes techniques auquel on se heurte avec la méthode de Golomb est le fait que l'on doive manipuler des séries non absolument convergentes. La situation se simplifie notablement lorsque les séries considérées sont absolument convergentes et que l'on peut utiliser, par exemple, le théorème de convergence dominée, comme dans l'illustration suivante.

Posons

$$F(z) = \sum_{n=1}^{\infty} \frac{\varphi(f(n))}{f(n)} z^n,$$

où $f(X) \in \mathbf{Z}[X]$ est tel que $f(n) \geq 1$ pour tout $n \geq 1$. Pour tout entier $m \geq 1$, on a $\varphi(m)/m = \sum_{d|m} \mu(d)/d$, d'où

$$F(z) = \sum_{d=1}^{\infty} \frac{\mu(d)}{d(1-z^d)} \sum_{\substack{n=1 \\ f(n)\equiv 0\,[d]}}^{d} z^n.$$

Il est possible de justifier l'interversion limite-série suivante :

$$\lim_{z\to 1^-} (1-z)\, F(z) = \sum_{d=1}^{\infty} \frac{\mu(d)}{d} \lim_{z\to 1^-} \left(\frac{\sum_{\substack{n=1,\dots,d \\ f(n)\equiv 0\,[d]}} z^n}{\sum_{n=0,\dots,d-1} z^n} \right) = \sum_{d=1}^{\infty} \frac{\mu(d) N_f(d)}{d^2} = L_f(2). \qquad (19)$$

En effet, notons h le degré de f et $s(d)$ le plus petit entier $n \in \{1, \dots, d\}$ tel que $d | f(n)$ lorsqu'il existe et $s(d) = d$ s'il n'existe pas. Pour tout z tel que $0 < z < 1$ et pour tout $d \geq 1$, on a

$$0 \leq \sum_{\substack{n=1,\dots,d \\ f(n)\equiv 0\,[d]}} z^n \leq N_f(d) z^{s(d)} \quad \text{et} \quad \sum_{n=0}^{d-1} z^n \geq \sum_{n=0}^{s(d)-1} z^n \geq s(d) z^{s(d)-1}.$$

D'où

$$\left|\frac{\mu(d)}{d}\frac{\sum_{\substack{n=1,\dots,d\\ f(n)\equiv 0\,[d]}} z^n}{\sum_{n=0,\dots,d-1} z^n}\right| \le z\frac{|\mu(d)|N_f(d)}{d\,s(d)} \le \frac{|\mu(d)|h^{\omega(d)}}{d\,s(d)} \ll \frac{|\mu(d)|h^{\omega(d)}}{d^{1+1/h}},$$

car $d \mid f(s(d))$ implique que $s(d) \gg d^{1/h}$. Comme la série de terme $|\mu(d)|h^{\omega(d)}/d^{1+1/h}$ est convergente (de valeur $\prod_p(1+hp^{-1-1/h})$), on peut appliquer le théorème de convergence dominée pour montrer (19). Le théorème taubérien d'Hardy-Littlewood et la transformation d'Abel nous permettent d'en déduire le :

Théorème 15. — *Pour tout polynôme $f(X) \in \mathbf{Z}[X]$ tel que $f(n) \ge 1$, on a*

$$\sum_{n\le x} \varphi(f(n)) \sim \frac{L_f(2)}{h+1}\, xf(x).$$

Remarques. (*i*) La minoration $s(d) \gg d^{1/h}$ ne peut pas être améliorée en général puisque pour tout entier $m \gg 1$, on $s(f(m)) \le m \ll f(m)^{1/h}$. Ce fait est une des raisons de la difficulté de justifier l'interversion limite-série lorsque $h \ge 2$.

(*ii*) Il existe des expressions absolument convergentes de $\sum_{d\ge1}\mu(d)\log^k(d)N_f(d)/d$. Parmi diverses possibilités, la transformation d'Abel montre que cette série est égale à

$$\sum_{d=1}^{\infty}(\log^k(d)-\log^k(d+1))\sum_{j=1}^{d}\frac{\mu(j)N_f(j)}{j},$$

qui est bien absolument convergente puisque $\log^k(d)-\log^k(d+1) = \mathcal{O}(\log^{k-1}(d)/d)$ et $\sum_{j=1}^d \mu(j)N_f(j)/j = \mathcal{O}(\exp(-c\sqrt{\log(d)}) = \mathcal{O}(\log^{-k-1}(d))$.

La série de fonctions correspondante

$$\sum_{d=1}^{\infty}(\log^k(d)-\log^k(d+1))\sum_{j=1}^{d}\frac{\mu(j)}{1+z+\cdots+z^{j-1}}\sum_{\substack{n=1\\ f(n)\equiv 0\,[j]}}^{j} z^n.$$

est malheureusement moins facile à étudier, bien que l'on dispose ici de l'intéressante propriété

$$\sum_{j=1}^{\infty}\frac{\mu(j)}{1+z+\cdots+z^{j-1}}\sum_{\substack{n=1\\ f(n)\equiv 0\,[j]}}^{j} z^n = 0$$

pour tout z (en vertu de la démonstration du Théorème 14, cas $\ell = 0$).

13. La conjecture de Goldbach

Dans ce paragraphe, on considère le cas de la conjecture de Goldbach [**23**] « *Tout nombre pair est la somme de deux nombres premiers* », qui ne rentre pas dans le cadre de celle de Schinzel-Bateman-Horn. On s'intéresse tout d'abord à divers raffinements quantitatifs dans l'esprit de Bateman et Horn, puis on montre comment adapter le Λ-calcul à ce cas.

13.1. Le difficile art de la conjecture. — Les estimations numériques de la conjecture de Goldbach indiquent que non seulement tout nombre pair n est apparemment la somme de deux nombres premiers, mais que le nombre d'écriture différente de n sous cette forme croit avec n. Il est donc naturel de s'intéresser au comportement asymptotique de la quantité

$$G(n) = \#\{(p,q) : \ n = p+q \text{ et } p,\, q \text{ sont premiers}\}$$

lorsque $n \to +\infty$. Le premier à l'avoir fait est, semble-t'il, Sylvester [**48**] en 1872 dans un article de trois pages particulièrement surprenant. En effet, on n'y trouvera que les onze expressions mathématiques suivantes (comptées avec multiplicité) : $\frac{p-2}{p-1}$, n, $\sqrt{n}$ et $x+y=n$. Une traduction de l'anglais vers les mathématiques fournit néanmoins une conjecture, qui a provoqué ce commentaire de Hardy et Littlewood [**28**, p. 33] : « *There is no sufficient evidence to show how he was led to this result* ».

Conjecture 5 (Sylvester). — *Lorsque l'entier pair $n \to +\infty$,*

$$G(n) \sim \frac{2n}{\log(n)} \cdot \prod_{\substack{3 \leq p < \sqrt{n} \\ p \nmid n}} \left(\frac{p-2}{p-1}\right).$$

Stäckel [**47**] s'est intéressé à ce problème [(8)] en 1896, de façon un peu plus vague.

Conjecture 6 (Stäckel). — *Lorsque l'entier pair $n \to +\infty$, le nombre $G(n)$ vaut approximativement*

$$\mathfrak{G}(n) = \frac{n}{\log^2(n)} \cdot \prod_{p \mid n} \left(\frac{p}{p-1}\right) = \frac{n^2}{\log^2(n)\varphi(n)}.$$

On peut enfin mentionner l'approche de Brun [**7**], datant de 1915.

Conjecture 7 (Brun). — *Lorsque l'entier pair $n \to +\infty$,*

$$G(n) \sim 2n \cdot \prod_{3 \leq p < \sqrt{n}} \left(1 - \frac{2}{p}\right) \cdot \prod_{\substack{p \geq 3 \\ p \mid n}} \left(\frac{p-1}{p-2}\right).$$

Comme Sylvester, il n'est pas facile de réellement comprendre ce qui a guidé Stäckel et Brun. Bien que les trois estimations soient en apparence assez éloignées, les produits eulériens suggèrent pour les trois des arguments heuristiques utilisant le « fait » que la chance que N soit premier vaut environ $\prod_{p<N}(1-1/p)$. Quoi qu'il en soit, Landau a montré en 1900 que

Théorème 16 (Landau). — *Lorsque $x \to +\infty$, on a*

$$\sum_{n \leq x} G(n) \sim \frac{x^2}{2\log^2(x)} \quad \text{et} \quad \sum_{n \leq x} \mathfrak{G}(n) \sim \frac{\zeta(2)\zeta(3)}{3\zeta(6)} \cdot \frac{x^2}{2\log^2(x)}.$$

(8) On apprend dans [**47**] que Cantor [**8**] fut lui aussi suffisamment intéressé par la conjecture de Goldbach pour la vérifier jusqu'à $n = 1000$.

Comme $\zeta(2)\zeta(3)/3\zeta(6) \approx 0,6478$*, la conjecture de Stäckel est fausse.*

Hardy et Littlewood [**28**] se sont eux penchés sur les conjectures de Sylvester et Brun que, grâce au théorème de Mertens, ils ont reformulées ainsi :

$$G(n) \sim \ 2e^{-\gamma} \cdot 2\prod_{p\geq 3}\left(1-\frac{1}{(p-1)^2}\right)\cdot\frac{n}{\log^2(n)}\cdot\prod_{\substack{p\geq 3\\ p|n}}\left(\frac{p-1}{p-2}\right) \qquad \text{(Sylvester)}$$

$$G(n) \sim \ 8e^{-2\gamma} \cdot 2\prod_{p\geq 3}\left(1-\frac{1}{(p-1)^2}\right)\cdot\frac{n}{\log^2(n)}\cdot\prod_{\substack{p\geq 3\\ p|n}}\left(\frac{p-1}{p-2}\right) \qquad \text{(Brun).}$$

Il en découle que ces conjectures ne peuvent pas être vraies simultanément, bien qu'elles ne différent finalement que d'un facteur constant.

Théorème 17 (Hardy-Littlewood). — *Si* $G(n) = o(n/\log^2(n))$ *pour* n *impair et si, lorsque* n *pair* $\to +\infty$*,*

$$G(n) \sim A\cdot\frac{n}{\log^2(n)}\cdot\prod_{\substack{p\geq 3\\ p|n}}\left(\frac{p-1}{p-2}\right),$$

alors nécessairement, $A = 2\prod_{p\geq 3}\left(1-\frac{1}{(p-1)^2}\right)$*. Les conjectures de Brun et Sylvester sont donc fausses.*

Cette caractérisation de la constante A est similaire au résultat de Tchebichef rappelé à l'équation (11). Obtenir une telle caractérisation pour les constantes de Bateman-Horn $C(\underline{f})$ semble difficile : les démonstrations des Théorèmes 16 et 17 reposent sur le fait qu'il est assez facile d'analyser le comportement en moyenne de $G(n)$ (ou de fonctions similaires), malgré son comportement erratique. Par exemple, Landau a remarqué que, lorsque $x \to +\infty$, on a

$$\sum_{n\leq x} G(n) = \sum_{p\leq x}\pi(x-p) \sim \int_2^{x-2}\frac{\pi(x-t)}{\log(t)}\,\mathrm{d}t \sim \int_2^{x-2}\frac{x-t}{\log(x-t)\log(t)}\,\mathrm{d}t \sim \frac{x^2}{2\log^2(x)},$$

tandis que Hardy et Littlewood ont exploité le comportement au voisinage de $z=1$ de la série

$$\sum_{n=1}^{\infty}\left(\sum_{p+q=n}\log(p)\log(q)\right)z^n = \left(\sum_p \log(p)\,z^p\right)^2 \sim \frac{1}{(1-z)^2}.$$

Malheureusement, nul ne sait si l'on peut adapter ce type d'arguments au cas de $C(\underline{f})$.

Encouragés par les divers résultats obtenus avec leur méthode du cercle, Hardy et Littlewood ont également conjecturé que le Théorème 17 décrit correctement le comportement de $G(n)$. De son côté, Schinzel [**45**] est parvenu à adapter l'heuristique de Bateman et Horn aux problèmes de type Goldbach. On reprend les notations du début du paragraphe 2 : soit $f_1, f_2, \ldots, f_k$ une famille convenable de polynômes et posons $f = f_1 f_2 \cdots f_k$. Soit $f_0(X) \in \mathbf{Z}[X]$ de terme dominant positif. Posons $N(n) = \#\{m \geq 1 : n - f_0(m) > 0\}$, $\omega(n,p) = \#\{1 \leq m \leq p : f(m)(n-f_0(m)) \equiv 0\,[p]\}$ et $h_0 = \deg(f_0)$.

Conjecture 8 (Schinzel). — *Lorsque $n \to +\infty$ de sorte que $n - f_0(X)$ soit irréductible et que, pour tout premier p, il existe $m \geq 1$ tel que p ne divise pas $f(m)(n - f_0(m))$, on a*

$$\#\{m \leq n : f_1(m), \dots, f_k(m) \text{ et } n - f_0(m) \text{ premiers}\} \sim \frac{1}{h_0 h_1 \cdots h_k} \prod_p \left(\left(1 - \frac{1}{p}\right)^{-k-1} \left(1 - \frac{\omega(n,p)}{p}\right) \right) \cdot \frac{N(n)}{\log^{k+1}(N(n))}.$$

Le cas $k = 1$, $f_0(X) = f_1(X) = X$ correspond à la conjecture de Goldbach.

13.2. Goldbach et Golomb. — Pour obtenir une version quantitative de la conjecture de Goldbach, Hardy et Littlewood [**28**, p. 38] notent que la fonction

$$g(n) = \sum_{k=1}^{n-1} \Lambda(k)\Lambda(n-k)$$

est celle qui s'impose le plus naturellement. Cependant, en raison de la dépendance en n du sommande, la méthode fonctionnelle de Golomb ne peut pas être utilisée de la même manière que pour la conjecture de Bateman-Horn. De plus, pour appliquer l'identité (13), il faut restreindre la sommation aux seuls entiers k tels $(k, n) = 1$ et étudier

$$\mathscr{G}(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n-1} \Lambda(k)\Lambda(n-k) = \frac{1}{2} \sum_{d=1}^{\infty} \mu(d) \log^2(d) \sum_{\substack{k=1 \\ (k,n)=1,\, d \mid k(n-k)}}^{n-1} 1. \tag{20}$$

Nous donnons maintenant un argument analytique permettant d'estimer $\mathscr{G}(n)$ d'une manière certes moins élégante que dans le cas de Bateman-Horn mais que nous espérons assez plausible. Nous montrons en fin de paragraphe pourquoi, conjecturalement, $g(n)$ et $\mathscr{G}(n)$ ont le même comportement asymptotique.

Notons $A(n, d)$ la somme finie tout à droite de (20) : on a évidemment $A(n, d) = 0$ si $(d, n) > 1$ ou si $d > \max_k k(n-k) = n^2/4$. De plus, si $d = p$ est premier et si $(n, p) = 1$, on a

$$A(n,p) = 2 \sum_{r \mid n} \mu(r) \left[\frac{n}{rp}\right] = \frac{2\varphi(n)}{p} + R(n,p) = \frac{N(p)\,\varphi(n)}{p} + R(n,p).$$

avec $R(n,p) = 2\sum_{r|n} \mu(r)\big(\left[\frac{n}{rp}\right] - \frac{n}{rp}\big) \ll \tau(n)$ (= le nombre de diviseurs de n) et $N(d) = N_{X(n-X)}(d)$. On peut espérer que pour d quelconque, la fonction $R(n, d)$ définie par

$$A(n,d) = \frac{N(d)\,\varphi(n)}{d} + R(n,d) \tag{21}$$

soit petite [(9)] en un certain sens. Notons que l'écriture (21) est typique des méthodes de crible, où l'on cherche à approcher une fonction arithmétique compliquée par des fonctions

[(9)] Il s'agit évidemment du cœur du problème : prouver que l'effet de $R(n, d)$ se dilue finalement dans un terme d'erreur correspond au problème de l'inversion limite-série dans le cas de la conjecture de Bateman-Horn.

plus simples, multiplicatives par exemple : ici, cela revient à quantifier le fait que les conditions $(k,n)=1$ et $d \mid k(n-k)$ sont plus ou moins « indépendantes » pour un entier générique k lorsque $(d,n)=1$.

Si l'on pouvait négliger la contribution due à $R(n,d)$, on obtiendrait alors l'approximation

$$\mathscr{G}(n) \overset{?}{\sim} \frac{\varphi(n)}{2} \sum_{\substack{d \leq n^2/4 \\ (d,n)=1}} \frac{\mu(d)\log^2(d)N(d)}{d} = \frac{\varphi(n)}{2} \sum_{\substack{d=1 \\ (d,n)=1}}^{\infty} \frac{\mu(d)\log^2(d)N(d)}{d} + o(\varphi(n)),$$

puisque la série est convergente. Or on montre que

$$\sum_{\substack{d=1 \\ (d,n)=1}}^{\infty} \frac{\mu(d)\log^2(d)N(d)}{d} = \frac{n}{\varphi(n)} \prod_p \left(\left(1-\frac{1}{p}\right)^{-2} \left(1-\frac{N(p)}{p}\right)\right)$$

et $N(p)=1$ si $p \mid n$ tandis que $N(p)=2$ si $p \nmid n$. Si n est impair, on a donc $N(2)=2$ et le produit est nul, ce qui va dans le bon sens. Si n est pair, des manipulations immédiates donnent alors

$$\mathscr{G}(n) \overset{?}{\sim} 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \cdot \prod_{\substack{p \mid n \\ p \geq 3}} \frac{p-1}{p-2} \cdot n + o(n), \tag{22}$$

en utilisant le fait que $o(\varphi(n)) = o(n)$.

Estimons maintenant $g(n) - \mathscr{G}(n)$ lorsque n est pair. Puisque $(k,n) > 1$, pour que $\Lambda(k)\Lambda(n-k) \neq 0$, le nombre k doit être une puissance d'un diviseur premier de n donc doit lui-même diviser n. En majorant simplement $\Lambda(k)\Lambda(n-k)$ par $\log^2(n)$, on a donc

$$0 \leq g(n) - \mathscr{G}(n) = \sum_{\substack{k=1 \\ (k,n)>1}}^{n-1} \Lambda(k)\Lambda(n-k) \leq \sum_{k \mid n} \Lambda(k)\Lambda(n-k) \leq \log^2(n)\,\tau(n) \ll n^{\varepsilon} \tag{23}$$

pour tout $\varepsilon > 0$ (par la majoration classique $\tau(n) \ll n^{\varepsilon}$: voir [**50**, p. 83, Corollaire 11]). Comme (22) suggère que $\mathscr{G}(n) \overset{?}{\gg} n$, on déduit donc de (22) et (23) que

$$\sum_{k=1}^{n-1} \Lambda(k)\Lambda(n-k) \overset{?}{\sim} 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \cdot \prod_{\substack{p \mid n \\ p \geq 3}} \frac{p-1}{p-2} \cdot n,$$

qui est l'une des variantes de l'estimation prédite par Hardy et Littlewood [**28**]. De tels arguments s'appliquent probablement à la conjecture de Schinzel énoncée au paragraphe 13.1. Enfin, rappelons que le théorème le plus proche de la conjecture de Goldbach est celui de Chen [**9**] : « *Tout entier pair suffisamment grand est la somme d'un nombre premier et d'un entier produit d'au plus deux nombres premiers* ».

Remerciements. Ils vont à K. Conrad pour ses commentaires pertinents qui nous ont permis d'améliorer une version préliminaire de ce texte.

Bibliographie

[1] S. Baier, *On the Bateman-Horn conjecture*, J. Num. Theory **96**.2 (2002), 432–448.

[2] S. Baier, *A probabilistic model for primes in random sets*, prépublication (2002).

[3] P. T. Bateman et R. A. Horn, *A Heuristic Asymptotic Formula Concerning the Distribution of Prime Numbers*, Math. Comp. **16** (1962), 363–367.

[4] P. T. Bateman et R. M. Stemmler, *Waring's problem for algebrai numbers and primes of the form* $(p^r-1)/(p^d-1)$, Illinois J. Math. **6** (1962), 142–156.

[5] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18** (1974).

[6] V. Bouniakowsky, *Sur les diviseurs numériques invariables des fonctions rationnelles entières*, Mémoires sc. math. et phys. **6** (1854),306–329.

[7] V. Brun, *Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare*, Arch. f. Math. og Naturv. **34** (1915), 3–19.

[8] G. Cantor, *Vérification jusqu'à* 1000 *du théorème empirique de Goldbach*, Assoc. Franç. Caen XXIII (1894), 117–134.

[9] J. R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sin. **16** (1973), 157–176.

[10] Lord Cherwell, *Note on the distribution of the intervals between prime numbers*, Quaterly J. Math. (Oxford) **17** (1946), 46–62.

[11] Lord Cherwell et E. M. Wright, *The frequency of primes patterns*, Quaterly J. Math. (Oxford II) **11** (1960), 60–63.

[12] J-L. Colliot-Thélène et J-J. Sansuc, *Sur le principe de Hasse et l'approximation faible, et sur une conjecture de Schinzel*, Acta Arith. **41** (1982), 33–53.

[13] J-L. Colliot-Thélène, A. Skorobogatov et P. Swinnerton-Dyer, *Hasse principle for pencils of curves of genus one whose jacobian have rational 2-division points*, Inv. Math. **134** (1998), 579–650.

[14] K. Conrad, *Hardy-Littlewood constants*, Mathematical properties of sequences and other combinatorial structures (Los Angeles, CA, 2002), 133–154, Kluwer Acad. Publ., Boston, MA, 2003.

[15] B. Conrad et K. Conrad, *The Möbius function and the residue theorem*, J. Num. Theory **110** (2005), 22–36.

[16] B. Conrad, K. Conrad et R. Gross, *Irreducible specialization in genus* 0, prépublication (2005).

[17] H. Davenport et A. Schinzel, *A note on certain arithmetical constants*, Illinois. J. Math. **10** (1966), 181–185.

[18] L. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Math. **33** (1904), 155–161.

[19] G. L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sing, unendlich viele Primzahlen erhält*, Abh. Akad. Berlin (1837), 45–71.

[20] L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Bibliothèque impartiale **3** (1751), 10–31. La citation reproduite ici se trouve dans la réédition de l'article dans les *Opera Posthuma* **1** (1862), 76–84 et disponible sur le site `http://math.dartmouth.edu/~euler/docs/originals/E175.pdf`.

[21] J. Friedlander et H. Iwaniec, *The polynomial X^2+Y^4 captures its primes*, Ann. Math. **148**.3 (1998), 945–1040.

[22] A. Frölich et M. J. Taylor, *Algebraic number theory*, Cambridge studies in advanced mathematics **27**, 1991.

[23] C. Goldbach, lettre à L. Euler datée du 7 juin 1742. Facsimilé disponible sur le site `http://www.mathstat.dal.ca/~joerg/pic/g-letter.jpg`.

[24] S. Golomb, *The Lambda Method in Prime Number Theory*, J. Num. Theory **2** (1970), 193–198.

[25] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. S.M.F. **24**, 199–220.

[26] G. H. Hardy, *Divergent Series*, Oxford University Press, First Edition, 1949.

[27] G. H. Hardy et J. E. Littlewood, *Tauberian theorem concerning power series and Dirichlet's series whose coefficients are positive*, Proc. Lond. Math. Soc. **13**.2 (1914), 174–191.

[28] G. H. Hardy et J. E. Littlewood, *Some Problems of 'Partitio Numerorum.' III. On the Expression of a Number as a Sum of Primes*, Acta Math. **44** (1923), 1–70.

[29] G. H. Hardy et E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, Fifth Edition, 1979.

[30] D. R. Heath-Brown, *Primes represented by x^3+2y^3*, Acta Math. **186**.1 (2001), 1–84.

[31] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Acta Arith. **24** (1974), 435–459.

[32] J. Korevaar, *A century of complex tauberian theory*, Bull. A.M.S. **39**.4 (2002), 475–531.

[33] J. Korevaar, *Distributional Wiener-Ikehara theorem and twin primes*, Indag. Mathem., N.S., **16**.1 (2005), 37–49.

[34] N. Kurokawa, *Special values of Euler products and Hardy-Littlewood constants*, Proc. Japan Acad. Ser. A Math. Sci. **60**.1 (1984), 325–338.

[35] N. Kurokawa, *On the meromorphy of Euler products I, II*, Proc. Lond. Math. Soc. **53** (1986), 1–47 et 209–236.

[36] E. Landau, *Ueber die zahlentheoretische Function $\varphi(n)$ und ihre Beziehung zum Goldbach'schen Satz*, Gött. Nachr. (1900), 177–186.

[37] S. Lang, *La conjecture de Bateman-Horn*, Gaz. Math. **67** (1996), 82–84.

[38] S. Lang, *Algebraic Number Theory*, Addison-Wesley (1970).

[39] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie. Ueber die Vertheilung der Primzahlen*, Borchardts J. für Math. (J. reine angew. Math.) **78** (1874), 46–63.

[40] D. J. Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), 693–696.

[41] A. de Polignac, *Six propositions arithmologiques déduites du crible d'Ératosthène*, Nouv. Ann. Math. **8** (1849), 423–429.

[42] G. Pólya, *Heuristic reasoning in the theory of numbers*, Am. Math. Mon. **66** (1959), 375–384.

[43] M. Riesz, *Ein Konvergenzsatz für Dirichletsche Reihen*, Acta Matematica **40** (1916), 349–61.

[44] A. Schinzel et W. Sierpinski, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208.

[45] A. Schinzel, *A remark on a paper of Bateman and Horn*, Math. Comput. **17** (1963), 445–447.

[46] J-P. Serre, *Représentations linéaires des groupes finis*, Herman (1967).

[47] P. Stäckel, *Ueber Goldbach's empirisches Theorem*, Gött. Nachr. (1896), 292–299.

[48] J. J. Sylvester, *On the partition of an even number into two primes*, Proc. Lond. Math. Soc. IV. (1872), 4–6.

[49] P. L. Tchebichef, *Sur la totalité des nombres premiers inférieurs à une limite donnée*, J. de Liouville **17** (1852), 341–365.

[50] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Publication de l'Institut Élie Cartan **13**, Université de Nancy, 1990.

[51] E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, Oxford Science Publications, Second Edition, 1986.

[52] C. de la Vallée-Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Brux. S. sc. 21 B (1897), 251–342 et 343–368.

Certaines des références anciennes peuvent être difficile à trouver. Des versions scannées des articles [**25, 36, 47, 49**] sont accessibles sur certaines bibliothèques numériques recensées sur `http://www.library.cornell.edu/math/digitalization.php`. De plus, la base de données *Jahrbuch über die Fortschritte der Mathematik* donne un lien direct vers la version scannée de nombreux articles datés d'avant 1942 : `http://www.emis.de/MATH/JFM/`.

Institut de Mathématiques de Jussieu, Université Denis Diderot - Paris VII, Boîte 7012, 2 place Jussieu, 75251 Paris cedex 05, France.
`hindry@math.jussieu.fr`

Institut Fourier, CNRS UMR 5582 - Université Grenoble 1, 100 rue des Maths, BP 74, 38402 Saint-Martin d'Hères cedex, France,
`rivoal@ujf-grenoble.fr`

---

version révisée le 12 décembre