Ordres moyens et le grand crible

J.J.T

Février 2026

Contents

Introduction et préliminaires

Ceci est un texte que j'ai écrit à l'issue de mes propres recherches sur les sujets de la théorie analytique des nombres et du grand crible. Il s'avère qu'il y a peu de littérature sur ce dernier sujet ; le livre de G. Tenenbaum ne prend que le point de vue du crible combinatoire de Brun. Heureusement, N. Tosel a écrit un super article d'un point de vue analytique sur le grand crible dans la RMS 135-4. Je remercie N. Tosel pour son aide et son temps.

On note $\mathcal{P}$ l'ensemble des nombres premiers et $\mathcal{Q}$ l'ensemble des entiers sans facteurs carrés (appelés les quadratfrei). Dans tout le texte, p désignera toujours un nombre premier. On note $\tau : \mathbb{N}^* \to \mathbb{N}$ la fonction qui à n associe son nombre de diviseurs et σ la fonction sommatoire associée. On note v_p

la valuation p-adique. Par des arguments de combinatoire élémentaire, on obtient les deux formules suivantes, valables pour tout $n \in \mathbb{N}^*$ et p :

$$\tau(n) = \prod_{p \in \mathcal{P}} (1 + v_p(n)) \text{ et } v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Ce dernier résultat étant la formule de Legendre. On admettra les deux premiers théorèmes de Mertens :

1. $\displaystyle\sum_{p \leq x} \frac{\ln(p)}{p} = \ln(x) + \mathcal{O}(1)$
2. $\displaystyle\sum_{p \leq x} \frac{1}{p} = \ln(\ln(x)) + M + \mathcal{O}\left(\frac{1}{\ln(x)}\right)$

Pour un certain $M > 0$ appelé constante de Meissel-Mertens. Ici, les indices signifient qu'on parcourt tous les nombres premiers inférieurs à x. Pour tout $A \subseteq \mathbb{N}^*$, on note $\Pi_A : [1, +\infty[\to \mathbb{R}$ la fonction de comptage associée :

$$\Pi_A(x) = \sum_{a \in A \cap [1,x]} 1$$

Et on note spécifiquement π la fonction de comptage associée aux nombres premiers. On dit que p est un nombre premier jumeau si $p+2$ est premier ; on note $\mathcal{P}_{\mathcal{J}}$ cet ensemble et $\Pi_{\mathcal{J}}$ la fonction de comptage associée. Un des buts centraux va être d'estimer cette quantité.

On définit $\mathcal{A} = \mathcal{F}(\mathbb{N}^*, \mathbb{C})$ l'ensemble des fonctions arithmétiques, où on définit le produit de convolution :

$$\forall (f,g) \in \mathcal{A}^2,\ f * g : n \mapsto \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Avec la notation $d|n$ indiquant qu'on parcourt les diviseurs positifs de n. Le lecteur se convaincra que $(\mathcal{A}, +, *)$ est alors un anneau commutatif. On note δ la fonction caractéristique du singleton $\{1\}$ et μ la fonction de Möbius, les deux vues comme des éléments de $\mathcal{A}$. On rappelle la relation fondamentale entre ces deux fonctions :

$$\delta = \mu * \mathbf{1}$$

Avec $\mathbf{1} \in \mathcal{A}$ la fonction constante égale à 1. Il s'ensuit trivialement qu'on a l'inversion de Möbius : si f, g sont deux fonctions arithmétiques, alors :

$$f = g * \mathbf{1} \Longrightarrow g = f * \mu$$

Si f et g sont des fonctions arithmétiques, on note F et G leurs fonctions sommatoires respectives, définies sur $\mathbb{R}$ et continues par morceaux sur ce dernier :

$$F(x) = \sum_{n \leq x} f(n) \text{ et } G(x) = \sum_{n \leq x} g(n)$$

On note φ la fonction indicatrice d'Euler, ω la fonction nombre de diviseurs premiers, γ la fonction qui à n associe le plus grand élément de $\mathcal{Q}$ qui divise n et Ω la fonction nombre de diviseurs comptés avec multiplicité ; pour tout $n \in \mathbb{N}^*$:

$$\omega(n) = \sum_{p|n} 1 \text{ et } \Omega(n) = \sum_{p^\nu \| n} \nu = \sum_{p \in \mathcal{P}} v_p(n)$$

Pour tout p et $x \in \mathbb{Z}$, on note $\overline{x}_p$ la classe d'équivalence de x dans $\mathbb{F}_p$. Finalement, pour $0 \leq a < b$, on écrit $[\![a, b]\!] = \mathbb{N} \cap [a, b]$. Avec tout ça compris, on peut continuer.

1 Ordres moyens

On va exhiber ici quelques résultats classiques et leurs applications immédiates. Il va d'abord falloir montrer deux lemmes qui vont nous être particulièrement utiles.

1.1 Lemme de sommation d'Abel

Le lemme qui suit est fondamental pour comprendre le lien entre fonction de comptage et somme d'inverses. La version originale est due à **Abel**, et a été modernisée pour mieux servir les buts de la théorie analytique des nombres.

Lemme 1.1 (Abel): soit $x \geq 1$ et $f \in \mathcal{A}$. Si $b : [1, x] \to \mathbb{C}$ est $\mathcal{C}^1$ alors:

$$\sum_{n \leq x} f(n)b(n) = F(x)b(x) - \int_1^x F(t)b'(t)\ dt$$

Preuve: Il suffit d'appliquer une transformée d'Abel classique pour conclure:

$$\sum_{n \leq x} f(n)b(n) = F(x)b(\lfloor x \rfloor) - \sum_{n \leq x-1} F(n)(b(n+1) - b(n))$$

Or, cette dernière somme peut se réécrire:

$$\sum_{n \leq x-1} F(n) \int_n^{n+1} b'(t)\ dt = \sum_{n \leq x-1} \int_n^{n+1} F(t)b'(t)\ dt = \int_1^{\lfloor x \rfloor} F(t)b'(t)\ dt$$

On a alors:

$$\sum_{n \leq x} f(n)b(n) = F(x)b(\lfloor x \rfloor) - \int_1^x F(t)b'(t)\ dt = F(x)b(n) + \int_{\lfloor x \rfloor}^x F(x)b'(t)\ dt - \int_1^x F(t)b'(t)\ dt$$

D'où le résultat. □

On peut immédiatement appliquer ce lemme pour montrer le résultat suivant:

Proposition 1.1: Soit $A \subset \mathbb{N}^*$. Alors les deux objets suivants ont la même nature:

$$\left(\sum_{a \in A \cap [1,n]} \frac{1}{a} \right)_{n \geq 1} \quad \text{et} \quad \int_1^x \frac{\Pi_A(t)}{t^2}\ dt$$

Preuve: Soit $x \geq 1$. Alors:

$$\sum_{a \in A \cap [1,x]} \frac{1}{a} = \sum_{k=1}^{n} \frac{\Pi_A(k) - \Pi_A(k-1)}{k}$$

En convenant que $\Pi_A(0) = 0$. On prend donc $f(n) = \Pi_A(n) - \Pi_A(n-1)$ et $b : x \mapsto 1/x$. En appliquant donc le lemme d'Abel:

$$\sum_{a \in A \cap [1,x]} \frac{1}{a} = \frac{\Pi_A(n)}{n} + \int_1^x \frac{\Pi_A(t)}{t^2}\ dt$$

En remarquant que la série est à termes positifs et que le terme en $\Pi_A(n)/n$ est borné, on arrive à conclure. □

On peut alors faire une première remarque intéressante concernant les nombres premiers ; une condition suffisante pour que la série évoquée à la proposition 1.1 converge est que $\Pi_A(t) \lesssim t^{1-\varepsilon}$ pour un certain $\varepsilon \in [0, 1[$. Par contraposée avec le second théorème de Mertens, on en déduit que pour tout $\alpha \in [0, 1[$:

$$\limsup_{x \to \infty} \frac{\pi(x)}{x^\alpha} = +\infty$$

Et par un encadrement simple, on peut même réduire la limite supérieure à une simple limite.

Exercice 1: Montrer que l'on peut remplacer la limite supérieure par une simple limite comme annoncé.

Ceci est bien sûr en concordance avec le théorème des nombres premiers, qui assure que:

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

Au voisinage de l'infini. On peut également montrer avec le lemme d'Abel que $\pi(x) \lesssim x/\ln(x)$.

Proposition 1.2: $\pi(x) \lesssim \dfrac{x}{\ln(x)}$

Preuve: On va mobiliser le premier théorème de Mertens:

$$\pi(x) = \sum_{p \leq x} 1 = \sum_{n \leq x} \frac{n}{\ln(n)}(S(n) - S(n-1)) + \mathcal{O}(1)$$

Avec pour tout $x \geq 0$, $S(x) = \displaystyle\sum_{p \leq x} \frac{\ln(p)}{p}$. En appliquant donc le lemme d'Abel:

$$\pi(x) = \frac{x}{\ln(x)}(\ln(x) + u(x)) - \int_1^x \frac{(\ln(t) + u(t))(\ln(t) - 1)}{\ln(t)^2}\, dt$$

Avec u une fonction bornée d'après le premier théorème de Mertens. Or:

$$\int_1^x \frac{(\ln(t) + u(t))(\ln(t) - 1)}{\ln(t)^2}\, dt = x - 1 + \mathcal{O}\left(\frac{x}{\ln(x)}\right)$$

Par des majorations triviales, d'où le résultat. □

On conclut que d'une certaine manière, le cas $\alpha = 1$ est un cas limite dans l'assertion précédente, sans avoir recours au théorème des nombres premiers.

1.2 Principe de l'hyperbole

On va maintenant regarder le principe de l'hyperbole, découvert en premier par Dirichlet pour obtenir une approximation asymptotique de σ. Comme l'indique son nom, il y a un lien intime entre cette méthode de sommation et la géométrie.

Lemme 1.2 (Dirichlet): Soit $(f, g) \in \mathcal{A}^2$ et $x \geq 1$. Alors pour tout $1 \leq y \leq x$:

$$\sum_{n \leq x}(f * g)(n) = \sum_{d \leq y} F\left(\frac{x}{d}\right) g(d) + \sum_{m \leq x/y} f(m) G\left(\frac{x}{m}\right) - F\left(\frac{x}{y}\right) G(y)$$

Preuve: Il suffit de l'écrire:

$$\sum_{n \leq x}(f * g)(n) = \sum_{md \leq x} f(m)g(d) = \sum_{\substack{md \leq x \\ d \leq y}} f(m)g(d) + \sum_{\substack{md \leq x \\ d > y}} f(m)g(d)$$

Remarquons que la première somme vaut simplement $\displaystyle\sum_{d \leq y} g(d) F\left(\frac{x}{d}\right)$ en factorisant à chaque fois par $g(d)$ à l'intérieur de la somme. Pour la somme à droite, on factorise par $f(m)$ afin de trouver:

$$\sum_{\substack{md \leq x \\ d > y}} f(m)g(d) = \sum_{m \leq x/y} f(m)(G\left(\frac{x}{m}\right) - G(y))$$

Et le résultat s'ensuit en développant. □

La question qui se pose est donc où est cachée l'hyperbole. Pour voir d'où vient ce découpage assez astucieux, on va se fier à un exemple. On va essayer d'estimer σ asymptotiquement ; une première manière de le faire est d'écrire naïvement :

$$\sigma(x) = \sum_{n \leq x} \tau(n) = \sum_{n \leq x} \sum_{d | n} 1 = \sum_{d \leq x} \left\lfloor \frac{x}{d} \right\rfloor$$

Et donc en encadrant la partie entière sans trop réfléchir :

$$xH(x) - \lfloor x \rfloor \leq \sigma(x) \leq xH(x)$$

Avec H la fonction sommatoire associée à la fonction arithmétique $n \mapsto 1/n$, appelée fonction harmonique. Puisque $H(x) = \ln(x) + \gamma + \mathcal{O}(1/x)$ avec γ la constante d'Euler-Mascheroni, on en tire que :

$$\sigma(x) \sim x\ln(x)$$

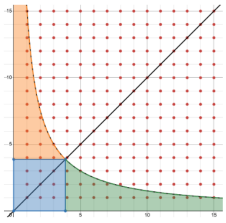
Il s'avère qu'on peut faire bien mieux grâce à Dirichlet.

Proposition 1.3: On a l'estimation $\sigma(x) = x\ln(x) + (2\gamma - 1)x + \mathcal{O}(\sqrt{x})$

Preuve: Il suffit de remarquer que $\tau = \mathbf{1} * \mathbf{1}$. On a alors en appliquant la méthode de l'hyperbole avec $f = g = \mathbf{1}$ et $y = \sqrt{x}$:

$$\sum_{n\leq x} \tau(n) = 2\sum_{n\leq\sqrt{x}} \left\lfloor \frac{x}{n} \right\rfloor - \lfloor\sqrt{x}\rfloor^2 =_{+\infty} 2x\sum_{n\leq\sqrt{x}} \frac{1}{n} - x + \mathcal{O}(\sqrt{x})$$

Or, $\displaystyle\sum_{n\leq\sqrt{x}} \frac{1}{n} =_{+\infty} \frac{1}{2}\ln(x) + \gamma + \mathcal{O}\left(\frac{1}{\sqrt{x}}\right)$ et le résultat s'ensuit. □



Ce qu'on a fait, c'est regrouper les termes en fonction de l'équation $md = k$ pour $k \leq x$. On veut compter tous les points à coefficients dans $\mathbb{N}^*$ sous la courbe $y = x/d$, c'est-à-dire les points rouges sous l'hyperbole dans l'image ci-dessus, qu'on peut partitionner en trois régions : les zones vertes et orange, qui ont le même nombre de points, et puis le carré bleu. On procède alors par un principe d'inclusion-exclusion : le nombre de points qu'on cherche est le nombre de points contenus dans bleu + vert, plus le nombre de points contenus dans bleu + orange, moins le nombre de points contenus dans bleu car on les a comptés en trop. Or, les points qui nous intéressent de vert + bleu correspondent à l'ensemble $\{(m,d) \in (\mathbb{N}^*)^2,\ md \leq x,\ d \leq \sqrt{x}\}$ et la zone orange + bleu correspond à l'ensemble $\{(m,d) \in (\mathbb{N}^*)^2,\ md \leq x,\ d > \sqrt{x}\}$, et la zone bleue va contenir exactement $\lfloor\sqrt{x}\rfloor^2$ points ; on retrouve bien le calcul qu'on vient d'effectuer. Le génie de Dirichlet est de remarquer que la symétrie axiale des hyperboles peut nous être utile et d'appliquer alors un principe d'inclusion-exclusion.

Estimer l'erreur $E(x) = \left|\displaystyle\sum_{n\leq x} \tau(n) - x\ln(x) + (2\gamma - 1)x\right|$ est encore aujourd'hui un problème ouvert. On a montré que $E(x) = \mathcal{O}(\sqrt{x})$ mais on peut faire mieux ; le mathématicien russe Georgy Voronoï a montré en 1903 qu'en réalité $E(x) = \mathcal{O}(x^{1/3}\ln(x))$, et Hardy et Landau ont montré que ce n'était pas un $o(x^{1/4})$. On conjecture que la borne inférieure des α tels que $E(x) = \mathcal{O}(x^\alpha)$ est $1/4$, mais il s'avère que c'est toujours un problème ouvert et la meilleure majoration qu'on a de cette borne inférieure est $131/416$.

1.3 Quelques ordres moyens

Les ordres moyens sont les approximations asymptotiques de sommes de fonctions arithmétiques. En effet, la transformation d'Abel nous indique que les sommes vont avoir un comportement plus "lisse" que les termes des sommes en question. Il s'avère que la majorité des fonctions arithmétiques oscillent énormément (essayez, par exemple, de trouver une courbe représentative de la fonction φ). On arrive à avoir des approximations asymptotiques de certaines fonctions arithmétiques, mais elles sont souvent assez rudimentaires. Par exemple, on sait que pour tout $\varepsilon > 0$, $\tau(n) = \mathcal{O}(n^\varepsilon)$, mais on ne peut pas faire mieux. En effet, soit $\varepsilon > 0$. On constate à l'aide de la formule de décomposition en facteurs premiers que pour tout $n \geq 2$:

$$n = \prod_{p|n} p^{v_p(n)}$$

Ainsi:

$$\frac{\tau(n)}{n^\varepsilon} = \prod_{p|n} \frac{v_p(n)+1}{p^{\varepsilon v_p(n)}}$$

On est donc amené à étudier les fonctions $f_p : \mathbb{R} \to \mathbb{R}$:

$$f_p(x) = \frac{x+1}{p^{x\varepsilon}}$$

Pour tout $p \in \mathcal{P}$, $f_p \in \mathcal{C}^\infty(\mathbb{R})$ et de dérivée:

$$f_p'(x) = \frac{p^{x\varepsilon} - (x+1)\varepsilon \ln(p) p^{x\varepsilon}}{p^{2\varepsilon x}}$$

On vérifie donc que f_p est croissante puis décroissante sur $\mathbb{R}$ et atteint son maximum en $x = 1/\varepsilon \ln(p) - 1$. Or, puisque $\mathcal{P}$ est infini, il existe un certain $p_\varepsilon \in \mathcal{P}$ tel que pour tout $p \geq p_\varepsilon$ premier, $\sup_{x\geq 0} f_p(x) = f_p(0) = 1$ puisque $1/\varepsilon \ln(p) - 1 \to -1$ lorsque $p \to \infty$. Ainsi:

$$0 \leq \frac{\tau(n)}{n^\varepsilon} \leq \prod_{p \leq p_\varepsilon} f_p\left(\frac{1}{\varepsilon \ln(p)} - 1\right) = M_\varepsilon$$

D'où le résultat. On va donc s'intéresser aux séries de fonctions arithmétiques au lieu de se restreindre aux termes généraux.

Avant de continuer, montrons un résultat très classique, souvent mobilisé dans la théorie des fonctions L mais qui nous servira uniquement dans le cadre précis ici des ordres moyens.

Lemme 1.3: On note ζ la fonction zêta de Riemann, définie sur $]1, +\infty[$. Alors pour tout $s > 1$:

$$\frac{1}{\zeta(s)} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^s}$$

Preuve: Soit $s > 1$. Il suffit d'écrire le calcul:

$$\zeta(s) \sum_{d=1}^{\infty} \frac{\mu(d)}{d^s} = \sum_{d=1}^{\infty} \frac{(\mu * \mathbf{1})}{d^s} = 1$$

□

On va maintenant montrer quelques résultats classiques en théorie des nombres, ceux des ordres moyens ; ce sont des résultats du même type que la proposition 1.3. Regardons déjà le cas de φ:

Exercice 2: Soit $n \in \mathbb{N}^*$. Montrer l'identité de Gauss:

$$\sum_{d|n} \varphi(d) = n$$

Et en déduire que $\varphi = \mu * \mathrm{Id}_{\mathbb{N}}$.

Proposition 1.4: On a

$$\sum_{n\leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \ln(x))$$

Preuve: D'après l'exercice 2, on a:

$$\sum_{n\leq x} \varphi(n) = \sum_{n\leq x} \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{d\leq x} \frac{\mu(d)}{d} \sum_{dk\leq x} dk = \frac{1}{2} \sum_{d\leq x} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor \left(\left\lfloor \frac{x}{d} \right\rfloor + 1 \right)$$

On en tire:

$$\sum_{n\leq x} \varphi(n) = \frac{x^2}{2} \sum_{d\leq x} \frac{\mu(d)}{d^2} + \mathcal{O}(x \ln(x))$$

Et on conclut avec le lemme 1.3. □

Une application amusante de ce résultat est donnée dans *Introduction à la théorie analytique et probabiliste des nombres* de G. Tenenbaum ; pour tout $N \geq 1$, on définit $\mathcal{F}_N$ comme étant le nombre de rationnels de la forme p/q avec $1 \leq p \leq q \leq N$ et $p \wedge q = 1$. Par définition, on a alors:

$$\forall N \in \mathbb{N}^*,\ \mathcal{F}_N = \sum_{n \leq N} \varphi(n)$$

On en déduit alors avec le résultat qui précède que la suite $(\mathcal{F}_N)_{N \geq 1}$ vérifie:

$$\mathcal{F}_N = \frac{3}{\pi^2} N^2 + \mathcal{O}(N \ln(N))$$

Cette suite s'appelle la suite de Farey.

Proposition 1.5: On a le développement asymptotique:

$$\sum_{n \leq x} \omega(n) = x \ln(\ln(x)) + Mx + \mathcal{O}\left(\frac{x}{\ln(x)}\right)$$

Avec M la constante de Meissel-Mertens.

Preuve: Il suffit de l'écrire:

$$\sum_{n \leq x} \omega(n) = \sum_{n \leq x} \sum_{p | n} 1 = \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor = x \ln(\ln(x)) + Mx + \mathcal{O}\left(\frac{x}{\ln(x)}\right)$$

D'après le second théorème de Mertens. □

Exercice 3: Montrer que $\sum_{n \leq x} \Omega(n) \sim x \ln(\ln(x))$ par des arguments analogues. Peut-on faire mieux?

Regardons maintenant l'exemple des quadratfrei.

Proposition 1.6: $\Pi_{\mathcal{Q}}(x) = \frac{6}{\pi^2} x + \mathcal{O}(\sqrt{x})$

Preuve: C'est plus délicat. Il faut remarquer que:

$$\Pi_{\mathcal{Q}}(x) = \sum_{n \leq x} \mu(n)^2$$

Remarquons que tout entier $n \in \mathbb{N}$ peut s'écrire qm^2, avec q le produit de tous les facteurs premiers de n dont la valuation est impaire et $m \in \mathbb{N}$. Ainsi, $\mu(n)^2 = \delta(m)$. Ainsi, en remarquant que $d|m$ est équivalent à l'assertion $d^2|n$:

$$\Pi_{\mathcal{Q}}(x) = \sum_{n \leq x} \sum_{d^2 | n} \mu(d) = \sum_{d \leq \sqrt{x}} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor$$

Et le résultat s'ensuit trivialement. □

Ce résultat rappelle un célèbre résultat de Dirichlet:

Proposition 1.6 bis: Soit $n \in \mathbb{N}^*$ et X, Y deux variables aléatoires suivant une loi uniforme dans $[\![1, n]\!]$. Alors:

$$\mathbb{P}(X \wedge Y = 1) \overset{n \to \infty}{\longrightarrow} \frac{6}{\pi^2}$$

Preuve: C'est assez similaire à l'ordre moyen des quadratfrei. À n fixé, on cherche à évaluer la quantité:

$$\mathbb{P}(X \wedge Y = 1) = \frac{1}{n^2} \sum_{(x,y) \in [\![1,n]\!]^2} \delta(x \wedge y) = \frac{1}{n^2} \sum_{(x,y) \in [\![1,n]\!]^2} \sum_{d | x} \sum_{d | y} \mu(d)$$

De ce fait:

$$\mathbb{P}(X \wedge Y = 1) = \frac{1}{n^2} \sum_{d \leq n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$$

Et un encadrement trivial de la partie entière permet de conclure. □

1.4 Ordre moyen de triplets Pythagoriciens et un équivalent classique

Un exercice classique de taupin consiste à montrer la proposition suivante :

Proposition 1.7 : On a l'équivalent suivant, au voisinage de 1^- :

$$\sum_{n=0}^{\infty} t^{n^2} \sim_{1^-} \frac{1}{2}\sqrt{\frac{\pi}{1-t}}$$

Souvent, ces exercices sont assez insatisfaisants ; l'explication pour l'apparition de π sort plus du calcul que du raisonnement géométrique. En effet, dans le tome d'Analyse de Xavier Gourdon, on utilise une approche avec les intégrales de Wallis. Heureusement, j'ai trouvé une démonstration qui me satisfait, et qui consiste à regarder l'ordre moyen du nombre de triplets pythagoriciens. Pour tout $r \geq 0$, on pose $Q(r) = \#\{(x,y) \in \mathbb{Z}^2,\ x^2+y^2 \leq r^2\}$ le nombre de points entiers contenus dans le cercle de centre $(0,0)$ et de rayon r. Alors on a le résultat suivant :

Proposition 1.8 : $Q(r) = \pi r^2 + \mathcal{O}(r)$

Preuve : Fixons un $r \in \mathbb{N}$, et soit $1 \leq k \leq r$ un entier fixé que l'on repère avec le point $(k,0)$. Sur la ligne perpendiculaire à l'axe des abscisses qui passe par $(k,0)$, on traverse forcément le cercle car $1 \leq k \leq r$.

Tous les points $(k,p) \in \mathbb{Z}^2$ qui appartiennent à cette droite et qui sont à l'intérieur du cercle vérifient $p^2 \leq r^2 - k^2$; puisque les p négatifs sont acceptés aussi, on en compte $1+2\lfloor\sqrt{r^2-k^2}\rfloor$, avec le $+1$ venant du cas $p=0$, que l'on ne veut pas compter deux fois. On en déduit que :

$$Q(r) = \sum_{k=-r}^{r} (1+2\lfloor\sqrt{r^2-k^2}\rfloor) = 1+2r+2\sum_{k=1}^{r}(1+2\lfloor\sqrt{r^2-k^2}\rfloor) = 4\sum_{k=1}^{r}\sqrt{r^2-k^2}+\mathcal{O}(r)$$

Or, on reconnaît l'expression d'une intégrale de Riemann de la fonction continue sur $[0,1]$ $x \mapsto \sqrt{1-x^2}$, dont la convergence est en $\mathcal{O}(1/r)$ malgré la singularité que présente la dérivée en $x=1$:

$$\frac{1}{r}\sum_{k=1}^{r}\sqrt{1-\frac{k^2}{r^2}} =_{+\infty} \frac{\pi}{4} + \mathcal{O}\left(\frac{1}{r}\right)$$

D'où l'estimation :

$$Q(r) = \pi r^2 + \mathcal{O}(r)$$

□

Exercice 4 : Justifier la convergence en $\mathcal{O}(1/r)$ malgré la singularité que présente la dérivée.

Ceci va nous permettre de montrer la proposition 1.7. En effet, posons pour tout $|t|<1$, $f(t) = \sum_{n=0}^{\infty} t^{n^2}$. Alors par des produits de Cauchy, on obtient :

$$\frac{1}{1-t}f(t)^2 = \sum_{n=0}^{\infty} Q^+(\sqrt{n})t^n$$

Avec $Q^+(n) = \{(x,y) \in \mathbb{N}^2,\ x^2+y^2 \leq n^2\}$ les points contenus dans le cercle résidant dans le premier quadrant de $\mathbb{R}^2$. Par un raisonnement analogue à la démonstration de la proposition 1.8, on trouve facilement que $Q^+(\sqrt{n}) \sim \frac{\pi}{4}n$. On va donc mobiliser le lemme classique suivant :

Lemme 1.4 : Soit (a_n), (b_n) deux suites positives dont les séries entières ont un rayon de convergence égal à 1, équivalentes au voisinage de l'infini et telles que la série des (a_n) diverge. Alors :

$$\sum_{n=0}^{\infty} a_n t^n \sim_{1^-} \sum_{n=0}^{\infty} b_n t^n$$

Preuve : Quitte à retrancher les sommes, on peut supposer que (a_n) et (b_n) sont strictement positives. Soit $\varepsilon > 0$. On note A et B les séries entières associées à (a_n) et (b_n) respectivement. Pour tout $n \in \mathbb{N}$ et $|t|<1$, on pose :

$$M_n = \sum_{k=0}^{n} a_k \text{ et } R_n(t) = \sum_{k=n+1}^{\infty} a_k t^k$$

Il existe un $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $|a_n - b_n| \leq \varepsilon a_n$. On en tire alors par l'inégalité triangulaire que :

$$|A(t) - B(t)| \leq M_N + \varepsilon R_N(t)$$

En divisant par $A(t)$, on obtient alors :

$$\left|\frac{B(t)}{A(t)} - 1\right| \leq \varepsilon + o(1)$$

Par positivité de (a_n), d'où le résultat en laissant tendre $t \to 1^-$. □

Il s'ensuit que :

$$\frac{f(t)^2}{1-t} \sim_{1^-} \frac{\pi}{4} \sum_{n=0}^{\infty} n t^n \sim_{1^-} \frac{\pi}{4(1-t)^2}$$

D'où le résultat. □

2 Initiation a la théorie analytique du crible

2.1 Qu'est-ce qu'un crible?

La théorie du crible est une des artilleries lourdes de la théorie analytique des nombres. C'est une manière assez "brute force" qui permet de donner des approximations asymptotiques de certains ensembles de nombres premiers, ou de parties de $\mathbb{N}$ qui vérifient une propriété imposée par le crible.

Rigoureusement, un crible $\mathcal{C} = (\mathcal{P}_\mathcal{C}, \Omega_\mathcal{C})$ est la donnée de deux objets mathématiques :

1. Une partie finie $\mathcal{P}_C \subset \mathcal{P}$
2. Une collection de parties $\Omega_\mathcal{C} = \bigcup_{p \in \mathcal{P}_\mathcal{C}} \{\Omega_{p,\mathcal{C}}\}$ avec pour tout $p \in \mathcal{P}_\mathcal{C}$, $\Omega_{p,\mathcal{C}}$ est une partie non vide de $\mathbb{F}_p$ différente de $\mathbb{F}_p$.

Pour tout $p \in \mathcal{P}$, on pose $\omega_\mathcal{C}(p) = |\Omega_{p,\mathcal{C}}| > 0$ si $p \in \mathcal{P}_\mathcal{C}$ et 0 dans le cas échéant. Pour une partie $I \subset \mathbb{Z}$, souvent finie, on définit alors :

$$\mathcal{C}(I) = \{x \in I, \forall p \in \mathcal{P}_C,\ \overline{x}_p \notin \Omega_{p,\mathcal{C}}\}$$

Il est évident que pour tout $p \in \mathcal{P}_\mathcal{C}$ on choisit $\Omega_{p,\mathcal{C}} \neq \emptyset$, car dans ce cas-là on n'a juste pas à considérer ce p en particulier. Il est également clair que $\Omega_{p,\mathcal{C}} \neq \mathbb{F}_p$ pour tout p, car sinon $\mathcal{C}(X) = \emptyset$ quel que soit $X \subset \mathbb{Z}$. Le but de la théorie du crible est alors d'estimer $\mathcal{C}(I)$ en termes de la taille de I et d'autres quantités. Regardons un exemple simple d'application du crible, le plus classique.

Définition 2.1: Le crible d'Ératosthène : Pour $N \in \mathbb{N}^*$, on pose $\mathcal{C}_N = (\mathcal{P} \cap [\![1, \sqrt{N}]\!], \Omega_{\mathcal{C}_N})$ avec pour tout $p \in \mathcal{P} \cap [\![1, \sqrt{N}]\!]$, $\Omega_{p,\mathcal{C}_N} = \{\overline{0}_p\}$. Regardons donc ce qui se passe lorsqu'on crible $[\![1, N]\!]$; soit $x \in [\![1, N]\!]$

- Si x n'est pas premier alors $x = ab$ avec $a, b \geq 2$. On en déduit que x admet un facteur premier plus petit que $\sqrt{N}$; il n'apparaît donc pas dans $\mathcal{C}_N([\![1, N]\!])$.
- Tous les nombres premiers plus petits que $\sqrt{N}$ sont enlevés.
- Tous les nombres premiers strictement plus grands que $\sqrt{N}$ et inférieurs à N restent.

On en déduit que $\mathcal{C}_N([\![1, N]\!]) = \mathcal{P} \cap]\!]\sqrt{N}, N]\!]$. Dans cette partie, on va démontrer une inégalité fondamentale portant sur le crible. Pour y parvenir, il va falloir passer par les polynômes trigonométriques.

2.2 Polynômes trigonométriques

Pour tout $k \in \mathbb{Z}$, on note $e_k : \mathbb{R} \to \mathbb{C}$ la fonction 1-périodique $x \mapsto \exp(2\pi ikx)$. On note E le $\mathbb{C}$-espace vectoriel engendré par toute combinaison linéaire finie des e_k, appelé l'ensemble des polynômes trigonométriques.

Dans le reste de cette partie, G désigne un groupe cyclique, et on note $\mathbb{C}^G$ l'ensemble des applications de $G \to \mathbb{C}$, que l'on munit d'une structure d'espace hermitien avec le produit scalaire hermitien suivant :

$$\forall (u,v) \in \mathbb{C}^G \times \mathbb{C}^G,\ \langle u, v\rangle = \frac{1}{|G|}\sum_{g\in G} \overline{u(g)}v(g)$$

On note $\widehat{G} = \hom(G, \mathbb{C}^*)$ l'ensemble des caractères sur G, appelé le dual de G. Il s'avère que cet ensemble forme une base orthonormée pour le produit scalaire $\langle \cdot, \cdot \rangle$. Montrons-le rapidement sous forme d'exercice :

Exercice 5 : Soit G un groupe cyclique d'ordre n, et g un générateur de G. Montrer successivement que :

1. Pour $\omega \in \mathbb{U}_n$, la formule $\chi_\omega(g^k) = \omega^k$ définit un caractère de G ;
2. On a $\widehat{G} = \{\chi_\omega,\ \omega \in \mathbb{U}_n\}$;
3. $\omega \to \chi_\omega$ est un isomorphisme de $\mathbb{U}_n$ sur $\widehat{G}$.

Et en déduire que $G \cong \widehat{G}$.

Pour conclure que cette famille est orthonormée (et donc libre) pour ce produit scalaire, il suffit de montrer le lemme suivant et de conclure par un argument de cardinalité :

Proposition 2.1 : Soit G un groupe fini et $\chi : G \to \mathbb{C}^*$ un morphisme non trivial. Alors :

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

Preuve : Il suffit de remarquer que puisque χ est non trivial, on dispose de $h \in G$ tel que $\chi(h) \neq 1$. De ce fait, puisque $g \mapsto hg$ définit une bijection :

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h)\sum_{g\in G}\chi(g)$$

D'où le résultat. □

On peut donc conclure :

Proposition 2.2 : Les éléments de $\widehat{G}$ forment une famille orthogonale pour $\langle \cdot, \cdot \rangle$. En particulier, la famille est libre dans $\mathbb{C}^G$.

Preuve : Si $\chi \neq \chi'$ sont deux caractères de G, alors $\overline{\chi}\chi' = \chi^{-1}\chi' \in \widehat{G}$ car tout caractère est à valeurs dans $\mathbb{U}$. Ainsi, en notant $\phi = \overline{\chi}\chi'$, $\phi \in \widehat{G}$ et est non trivial. On en tire :

$$\langle \chi, \chi' \rangle = \frac{1}{|G|}\sum_{g\in G}\phi(g) = 0$$

D'après la proposition précédente. Un calcul direct nous fournit :

$$\langle \chi, \chi \rangle = \frac{1}{|G|}\sum_{g\in G}|\chi(g)|^2 = \frac{1}{|G|}\sum_{g\in G} 1 = 1$$

D'où le résultat. □

On peut munir E d'une structure d'espace hermitien avec le produit scalaire classique :

$$\forall (f,g) \in E \times E,\ (f|g) = \int_0^1 \overline{f(x)}g(x)\ dx$$

Et le lecteur vérifiera facilement que la famille $(e_k)_{k\in\mathbb{Z}}$ forme ainsi une base orthonormée de E pour ce produit scalaire. Il s'ensuit qu'on a l'égalité de Parseval : si on note $(c_n(f))_{n\in\mathbb{Z}}$ les coefficients de f dans la base ci-dessus, on a :

$$\int_0^1 |f(x)|^2 \, dx = \sum_{n\in\mathbb{Z}} |c_n(f)|^2$$

Et on définit $\sigma(f) = \{n \in \mathbb{Z}, c_n(f) \neq 0\}$ le spectre de f. Avec ces résultats énoncés, montrons deux lemmes qui vont bien nous servir.

Lemme 2.1 : Soient $a < b$ deux réels et $f : [a, b] \to \mathbb{C}$ de classe $\mathcal{C}^1$. Alors pour tout $x \in [a, b]$:

$$|f(x)| \leq \frac{1}{b-a} \int_a^b |f(t)| \, dt + \int_a^b |f'(t)| \, dt$$

Preuve : Il suffit de l'écrire :

$$\left| f(x) - \frac{1}{b-a} \int_a^b f(t) \, dt \right| \leq \frac{1}{b-a} \int_a^b \left| \int_x^t f'(s) \, ds \right| \, dt \leq \int_a^b |f'(s)| \, ds$$

Et on conclut par l'inégalité triangulaire inverse. □

Lemme 2.2 : Soit $f \in E$ et $m \in \mathbb{N}$ tels que $\sigma(f) \subset [-m, m]$. Alors :

$$\int_0^1 |(|f(t)|^2)'| \, dt \leq 4\pi m \int_0^1 |f(t)|^2 \, dt$$

Preuve : Il suffit de l'écrire. On a :

$$\int_0^1 |(|f(t)|^2)'| \, dt = 2 \int_0^1 |\mathrm{Re}(f'\overline{f})(t)| \, dt \leq 2\sqrt{\int_0^1 |f(t)|^2 \, dt}\sqrt{\int_0^1 |f'(t)|^2 \, dt}$$

Or, pour tout $n \in \mathbb{Z}$, $|c_n(f')|^2 = 4\pi^2 n^2 |c_n(f)|^2$ et par l'identité de Parseval et une majoration de chaque $|n|$ par m, on obtient le résultat voulu. □

Introduisons une dernière définition qui va nous servir plus tard pour montrer l'inégalité analytique du grand crible.

Définition 2.2 : On pose $\Pi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ la projection canonique avec un système de représentants pris dans $[0, 1[$ et soit $X \subset \mathbb{R}$ finie, $\delta > 0$. On dit que X est δ-bien espacée modulo 1 si pour tout $(x, x') \in X^2$, $x \neq x'$:

$$|\Pi(x) - \Pi(x')| \geq \delta$$

Cette définition est surtout intéressante pour l'étude des intégrales de fonctions 1-périodiques. Appliquons-la pour montrer un résultat final qui va nous être la proposition la plus cruciale.

Proposition 2.3 : Soit $f \in E$ dont le spectre $\sigma(f)$ est inclus dans un segment entier de taille $N \geq 1$ et $X \subset \mathbb{R}$ δ-bien espacée modulo 1. Alors :

$$\sum_{x\in X} |f(x)|^2 \leq \left(2\pi N + \frac{1}{\delta}\right) \int_0^1 |f(t)|^2 \, dt$$

Preuve : Quitte à multiplier par un (e_k) pour tout recentrer, on peut supposer que $\sigma(f) \subset [\![-N/2, N/2]\!]$ sans que cela change les inégalités. Le lemme 2.1 nous fournit d'abord l'inégalité :

$$|f(x)|^2 \leq \frac{1}{\delta} \int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |f(t)|^2 \, dt + \int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |(|f(t)|^2)'| \, dt$$

En sommant et en remarquant que les intervalles $]x - \delta/2, x + \delta/2[$ sont tous disjoints modulo 1 :

$$\sum_{x\in X} |f(x)|^2 \leq \frac{1}{\delta} \int_0^1 |f(t)|^2 \, dt + \int_0^1 |(|f(t)|^2)'| \, dt$$

Et on applique le lemme 2.2 sur la deuxième intégrale pour conclure. □

2.3 Forme analytique du grand crible

Pour une famille X qui est δ-bien espacée modulo 1, on appelle forme analytique du grand crible toute inégalité de la forme :

$$\sum_{x\in X}|f(x)|^2 \leq \Delta(N,\delta)\int_0^1 |f(x)|^2$$

pour $f \in E$. La proposition 2.1 est bien une inégalité de cette forme, néanmoins loin d'être optimale. Selberg détermine la forme de $\Delta(N,\delta)$ optimale, où l'on perd le facteur 2π et l'on soustrait 1. Pourtant, l'inégalité de la proposition 2.1 va être largement suffisante pour nos besoins. Pour voir pourquoi ces inégalités vont nous intéresser, il va falloir poursuivre notre étude des polynômes trigonométriques dans le cadre spécifique où leur spectre est inclus dans $\mathcal{C}(\mathbb{Z})$.

Dans cette partie, fixons p un nombre premier et $\mathcal{C}$ un crible. On pose $\tilde{f} : x \mapsto f(x/p)$, qui est clairement une fonction p-périodique. Si on restreint alors notre étude à $\mathbb{F}_p$, il est clair qu'on peut la décomposer dans la base des caractères de ce dernier d'après la proposition 2.2. Ainsi, pour tout $x \in \mathbb{Z}$:

$$\tilde{f}(x) = \sum_{k=0}^{p-1} b_k\chi_k,\ b_k = \langle \chi_k, \tilde{f}\rangle$$

Avec un petit abus de langage où l'on traite les χ_k comme des applications de $\mathbb{Z} \to \mathbb{C}^*$ p-périodiques multiplicatives au lieu de morphismes de $\mathbb{F}_p \to \mathbb{C}^*$. Si $f \in E$ avec $(c_n(f))_{n\in\mathbb{Z}}$ ses coordonnées dans la base canonique, on a alors :

$$\forall k \in [\![0,p-1]\!],\ b_k = \frac{1}{p}\sum_{j=0}^{p-1}\overline{\chi_k}\left(\frac{j}{p}\right) f\left(\frac{j}{p}\right) = \sum_{n\in\mathbb{Z}} c_n(f)\langle\chi_k, e_j\rangle$$

Ici, il est clair que $\langle\chi_k, e_j\rangle = 1$ si $k \equiv j[p]$ et 0 sinon. On en tire donc le résultat suivant :

Proposition 2.4 : Soit $f \in E$ tel que $\sigma(f) \subset \mathcal{C}(\mathbb{Z})$. Alors :

$$\frac{\omega_{\mathcal{C}}(p)}{p-\omega_{\mathcal{C}}(p)}|f(0)|^2 \leq \sum_{j=1}^{p-1}\left|f\left(\frac{j}{p}\right)\right|^2$$

Preuve : Si $p \notin \mathcal{P}_{\mathcal{C}}$ le résultat est évident. Sinon, supposons que $p \in \mathcal{P}_{\mathcal{C}}$ et observons qu'avec la remarque précédente :

$$\tilde{f} = \sum_{k=0}^{p-1} b_k\chi_k,\ \text{avec } b_k = \sum_{n\in\mathbb{Z}, n\equiv k[p]} c_n(f)$$

Il s'ensuit que $b_k = 0$ si $\overline{k}_p \notin \Omega_{p,\mathcal{C}}$. On en tire que :

$$|f(0)|^2 = |\tilde{f}(0)|^2 = \left|\sum_{k=0}^{p-1} b_k\mathbf{1}(\overline{k}_p \in \Omega_{p,\mathcal{C}})\right|^2 \leq (p-\omega_{\mathcal{C}}(p))\sum_{k=0}^{p-1}|b_k|^2$$

d'après l'inégalité de Cauchy-Schwarz. Or, cette dernière somme étant égale à $\langle\tilde{f},\tilde{f}\rangle$ par l'identité de Parseval, on en tire l'inégalité :

$$|f(0)|^2 \leq \frac{p-\omega_{\mathcal{C}}(p)}{p}\sum_{j=0}^{p-1}\left|f\left(\frac{j}{p}\right)\right|^2$$

Et en soustrayant le premier terme de la somme des deux côtés, on a le résultat. □

Il est important de remarquer une chose ici : cette inégalité est incroyablement flexible ! En effet, ce sont nous qui imposons les valeurs de $\omega_{\mathcal{C}}(p)$, quels p nous intéressent, et la seule restriction qui en réalité va nous servir est l'inclusion $\sigma(f) \subset \mathcal{C}(\mathbb{Z})$.

Généralisons cette inégalité pour $q \in \mathcal{Q}$. Posons :

$$g_{\mathcal{C}}(q) = \prod_{p|q}\frac{\omega_{\mathcal{C}}(p)}{p-\omega_{\mathcal{C}}(p)}$$

Ce produit, qui vaut 1 lorsque $q = 1$ et 0 si et seulement s'il existe un élément de $\mathcal{P}\backslash\mathcal{P}_\mathcal{C}$ qui divise q, va jouer un rôle central dans ce texte. En effet, on a alors la généralisation de la proposition précédente :

Proposition 2.5 : Soit $q \in \mathcal{Q}$ différent de 1. Alors, pour tout $f \in E$ tel que $\sigma(f) \subset \mathcal{C}(\mathbb{Z})$:

$$g_\mathcal{C}(q)|f(0)|^2 \leq \sum_{\substack{1\leq j\leq q-1\\ j\wedge q=1}} \left|f\left(\frac{j}{q}\right)\right|^2$$

Preuve : On va le montrer par récurrence sur le nombre de facteurs premiers de q, à savoir $\omega(q)$. On vient de traiter le cas $\omega(q) = 1$, c'est-à-dire $q \in \mathcal{P}$. Soit donc $n \in \mathbb{N}^*$ et supposons donc le résultat montré pour tout $\omega(q) \leq n$. Soit $q \in \mathcal{Q}$ tel que $\omega(q) = n$ et $p \in \mathcal{P}$ tel que $p \wedge q = 1$. On pose $q' = pq$. Alors on a l'égalité des deux ensembles suivants :

$$\{k \in [\![1, q'-1]\!], k \wedge q' = 1\} = \{kp + qj,\ j \in [\![1, p-1]\!], k \wedge q = 1\}$$

En effet, on vérifie immédiatement l'inclusion de l'ensemble à droite dans l'ensemble à gauche, et pour l'inclusion inverse on emploie un argument de cardinalité ; l'ensemble de gauche est de cardinal $\varphi(q') = \varphi(p)\varphi(q) = (p-1)\varphi(q)$, qui est le cardinal de l'ensemble de droite. Il s'ensuit que :

$$\sum_{\substack{1\leq k\leq q'-1\\ k\wedge q'=1}} \left|f\left(\frac{k}{q'}\right)\right|^2 = \sum_{j=1}^{p-1} \sum_{\substack{1\leq k\leq q-1\\ k\wedge q=1}} \left|f\left(\frac{k}{q}+\frac{j}{p}\right)\right|^2$$

On applique alors l'hypothèse de récurrence à $x \mapsto f\left(x + \dfrac{j}{p}\right)$, qui vérifie bien les hypothèses nécessaires. On en tire que pour tout $j \in [\![1, p-1]\!]$:

$$g_\mathcal{C}(q)\left|f\left(\frac{j}{p}\right)\right|^2 \leq \sum_{\substack{1\leq k\leq q-1\\ k\wedge q=1}} \left|f\left(\frac{k}{q}+\frac{j}{p}\right)\right|^2$$

On applique alors la proposition 2.4 en sommant sur $1 \leq j \leq p-1$ et la multiplicativité de $g_\mathcal{C}$ pour conclure. □

Toutes ces sommes devraient nous rappeler la proposition 2.3. Introduisons alors un nouvel espace qui va jouer le rôle de X dans cette proposition :

Définition 2.3 : Pour $Q \geq 1$, on pose $\mathcal{F}_Q$ l'ensemble des fractions irréductibles de la forme $0 \leq p < q \leq Q$ avec $q \in \mathcal{Q}$. On vérifie facilement que $\mathcal{F}_Q$ est un ensemble $1/Q^2$-bien espacé modulo 1.

On pose alors pour tout $Q \geq 1$:

$$\Lambda_\mathcal{C}(Q) = \sum_{\substack{q\in\mathcal{Q}\\ q\leq Q}} g_\mathcal{C}(q)$$

Alors on a le résultat suivant, conséquence directe des propositions 2.3 et 2.5 :

Proposition 2.6 : Soit $Q \geq 1$, I un intervalle de $\mathbb{Z}$ de longueur N et $f \in E$ tel que $\sigma(f) \subset \mathcal{C}(I)$. Alors :

$$\|f\|_\infty^2 \leq \frac{Q^2 + 2\pi N}{\Lambda_\mathcal{C}(Q)} \int_0^1 |f(t)|^2\ dt$$

Preuve : Quitte à considérer $t \mapsto f(x+t)$ pour un x bien choisi, on peut supposer que $\|f\|_\infty^2 = |f(0)|^2$. On applique la proposition précédente pour obtenir :

$$\sum_{\substack{q\in\mathcal{Q}\backslash\{1\}\\ q\leq Q}} g_\mathcal{C}(q)|f(0)|^2 \leq \sum_{k\in\mathcal{F}_Q\backslash\{0\}} |f(k)|^2$$

On rajoute alors $|f(0)|^2$ des deux côtés et on applique la proposition 2.3 pour conclure. □

On applique alors cette inégalité au cas particulier $f = \displaystyle\sum_{n\in\mathcal{C}(I)} e_n$ pour obtenir le théorème suivant, qui va être l'outil principal pour le reste de l'article :

Théorème 1 : forme analytique du grand crible : Soit $\mathcal{C}$ un crible et $I \subset \mathbb{Z}$ contenu dans un intervalle de longueur N. Alors, pour tout $Q \geq 1$:

$$|\mathcal{C}(I)| \leq \frac{Q^2 + 2\pi N}{\Lambda_{\mathcal{C}}(Q)}$$

Preuve : Il suffit de l'écrire. Avec la proposition 2.6 et en prenant f comme on vient de l'énoncer :

$$|\mathcal{C}(I)|^2 \leq \frac{Q^2 + 2\pi N}{\Lambda_{\mathcal{C}}(Q)}(f|f) = \frac{Q^2 + 2\pi N}{\Lambda_{\mathcal{C}}(Q)}|\mathcal{C}(I)|$$

Ce qui est équivalent à ce qu'on voulait montrer. □

Prenons du recul. Cette majoration, valable pour tout $Q \geq 1$, est à nous de raffiner ; en effet, on choisit le crible, on choisit la valeur de Q la plus adaptée ; en outre, la seule chose qui reste un mystère là-dedans est la quantité $\Lambda_{\mathcal{C}}(Q)$, qu'on va voir être calculable dans la majorité des cas qui nous intéressent, ou qui au moins admet des développements asymptotiques faciles lorsque $Q \to +\infty$. Il va être assez naturel de choisir $Q = \sqrt{N}$ et d'observer ce qui se passe lorsque ce dernier tend vers l'infini. N. Tosel dit qu'il vaut mieux choisir Q légèrement inférieur à $\sqrt{N}$ pour obtenir des résultats encore plus pertinents (Q de l'ordre de $\sqrt{N/\ln(N)}$ par exemple). Il s'avère que le théorème 1 ne permet malheureusement pas d'améliorer l'approximation de $\pi(x)$ qu'on a obtenue à la proposition 1.2 (j'encourage le lecteur à essayer d'appliquer le théorème 1 au crible d'Ératosthène défini au début de cette section). Cependant, il va être particulièrement utile pour montrer le théorème de Brun sur les nombres premiers jumeaux

2.4 Le théorème de Brun

Théorème 2 (Brun) : On a l'approximation suivante :

$$\Pi_{\mathcal{J}}(x) = \mathcal{O}\left(\frac{x}{\ln(x)^2}\right)$$

Corollaire : On a $\displaystyle\sum_{p \in \mathcal{P}_{\mathcal{J}}} \frac{1}{p} < +\infty$

Avec le corollaire provenant de la proposition 1.1. D'une manière assez frustrante, ceci ne permet pas de conclure quant au nombre de nombres premiers jumeaux (qui reste aujourd'hui un problème ouvert). Montrer ce résultat est étonnamment facile avec le formalisme du crible.

Preuve : Appliquons le crible tout bêtement avec la première chose qui nous passe par la tête. On fixe $Q \geq 2$ et on pose $\mathcal{C}_Q = (\mathcal{P}_Q, \Omega_Q)$ avec $\mathcal{P}_Q = \mathcal{P} \cap [2, Q]$ et pour tout $p \in \mathcal{P}_Q$, $\Omega_{p,\mathcal{C}_Q} = \{\overline{0}_p, \overline{-2}_p\}$ si $p > 2$ et $\{\overline{0}_2\}$ sinon. Soit donc $N > Q$. Il est alors clair qu'on a l'inclusion $\mathcal{P}_{\mathcal{J}} \cap]Q, N] \subset \mathcal{C}(\llbracket 1, N \rrbracket)$. On en tire avec le théorème 1 que :

$$\Pi_{\mathcal{J}}(N) - \Pi_{\mathcal{J}}(Q) \leq \frac{Q^2 + 2\pi N}{\Lambda_{\mathcal{C}_Q}(Q)} \Longrightarrow \Pi_{\mathcal{J}}(N) \leq Q + \frac{Q^2 + 2\pi N}{\Lambda_{\mathcal{C}_Q}(Q)}$$

Il reste donc à choisir le bon Q pour conclure. Comme annoncé, le travail qui reste à faire est d'estimer la quantité $\Lambda_{\mathcal{C}_Q}(Q)$. Puisque $g_{\mathcal{C}_Q}(2) = 1$, on peut écrire :

$$\Lambda_{\mathcal{C}_Q}(Q) = \sum_{\substack{q \leq Q \\ 2 \nmid q \in \mathcal{Q}}} \prod_{p|q} \frac{2}{p-2}$$

Soit donc $q \in \mathcal{Q} \cap [1, Q]$ tel que $2 \nmid q$ et remarquons que :

$$\prod_{p|q} \frac{2}{p-2} = \prod_{p|q} \left(\sum_{n_p=1}^{\infty} \frac{2^{n_p}}{p^{n_p}} \right) = \sum_{\substack{n \in \mathbb{N}^* \\ \gamma(n) = q}} \frac{2^{\Omega(n)}}{n}$$

Ainsi :

$$\Lambda_{\mathcal{C}_Q}(Q) = \sum_{\substack{n \in \mathbb{N}^* \\ \gamma(n) \leq Q, n \equiv 1[2]}} \frac{2^{\Omega(n)}}{n} \geq \sum_{\substack{1 \leq n \leq Q \\ n \equiv 1[2]}} \frac{\tau(n)}{n}$$

Car $2^x \geq x+1$ pour tout $x \geq 1$ et d'après la formule de τ donnée dans les préliminaires. Or, on sait estimer cette somme. Définissons pour tout $x \geq 1$:

$$D(x) = \sum_{1 \leq n \leq x} \frac{\tau(n)}{n} \text{ et } D'(x) = \sum_{\substack{1 \leq n \leq x \\ n \equiv 1[2]}} \frac{\tau(n)}{n}$$

Alors, en utilisant encore la formule donnée dans les parties préliminaires, on a pour tout $x \geq 1$:

$$D(x) = \sum_{r=0}^{+\infty} \sum_{\substack{1 \leq n \leq x \\ v_2(n)=r}} \frac{\tau(n)}{n} = \sum_{r=0}^{+\infty} \frac{r+1}{2^r} D'\left(\frac{x}{2^r}\right) \leq D'(x) \sum_{r=0}^{+\infty} \frac{r+1}{2^r} = 4D'(x)$$

Par un calcul élémentaire. Il s'ensuit que :

$$\forall Q \geq 1,\ \Lambda_{\mathcal{C}_Q}(Q) \geq \frac{D(Q)}{4}$$

Or, il est facile d'estimer $D(Q)$ avec les techniques développées dans la partie 1. En effet, en effectuant une transformation d'Abel toute bête :

$$D(x) = \frac{\sigma(x)}{x} + \int_1^x \frac{\sigma(t)}{t^2}\, dt$$

Or, on sait très bien estimer σ grâce à la proposition 1.3 : il existe une fonction $u : [1, +\infty[\to \mathbb{R}$ vérifiant $|u(x)| \leq M\sqrt{x}$ pour un certain $M > 0$ tel que $\sigma(x) = x\ln(x) + (2\gamma - 1)x + u(x)$. Tout calcul fait, on retrouve l'existence d'une constante $C \in \mathbb{R}$ vérifiant :

$$D(x) = \frac{\ln(x)^2}{2} + 2\gamma \ln(x) + C + o(1)$$

On en tire notamment qu'après un certain rang, on a $4D(x) \geq 2\ln(x)^2$. Donc pour Q et N assez grands, on a :

$$\Pi_{\mathcal{J}}(N) \leq Q + \frac{Q^2 + 2\pi N}{2\ln(Q)^2}$$

Il suffit de choisir $Q = \sqrt{N}$ pour conclure. □