Math. Ann. 305, 571–599 (1996)

Mathematische Annalen

Sommes des chiffres et nombres presque premiers

E. Fouvry[1], C. Mauduit[2]

[1] Département de Mathématiques, Bâtiment 425, Université de Paris-Sud, F-91405 Orsay Cedex, France (e-mail: etienne.fouvry@math.u-psud.fr)
[2] Laboratoire de Mathématiques Discrètes, 163, Avenue de Luminy, Case 930, F-13288 Marseille Cedex 09, France

Reçu le 1 Juin 1995

Mathematics Subject Classification (1991): 11A41, 11B85, 11N36

I Introduction

Un des problèmes centraux de la théorie analytique des nombres est de montrer qu'un ensemble $\mathscr{A}$ d'entiers naturels, défini de façon non artificielle, contient une infinité de nombres premiers. Suivant l'usage, la lettre p est réservée aux nombres premiers. Cette question, habituellement très difficile, peut revêtir différentes formes suivant la nature de la suite $\mathscr{A}$. Si celle-ci est par exemple $\mathscr{A} = \{p-2\}$, le problème est de nature *multiplicative*. Si $\mathscr{A} = \{P(n);\ n \in \mathbb{Z}\}$ avec $P(n)$ polynôme satisfaisant des hypothèses raisonnables, le problème devient alors de nature *algébrique*. Enfin, si $\mathscr{A}$ est l'ensemble des parties entières de 1^c, 2^c, 3^c,... avec c réel légèrement supérieur à 1, on peut qualifier ce problème d'*analytique*.

L'objet de cet article est de traiter le cas où $\mathscr{A}$ est de nature *automatique*, question, qui à notre connaissance, ne semble pas avoir été abordée dans la littérature. Notons, par exemple, $\mathscr{A}^+$ et $\mathscr{A}^-$ l'ensemble des entiers naturels n dont la somme des chiffres dans l'écriture en base 2, notée $s(n)$, est respectivement, paire et impaire. Chacune de ces suites est très dense, de densité asymptotique $\frac{1}{2}$, pourtant on ne sait pas démontrer que $\mathscr{A}^+$ et $\mathscr{A}^-$ contiennent chacune, une infinité de nombres premiers. Cette recherche de nombres premiers présente l'attrait de mélanger structures multiplicative et récursive. En effet, nous utiliserons explicitement ou implicitement la construction suivante de $\mathscr{A}^+$ et $\mathscr{A}^-$:

$$0 \in \mathscr{A}^+$$

$$n \in \mathscr{A}^{\pm} \Rightarrow 2n \in \mathscr{A}^{\pm} \text{et } 2n+1 \in \mathscr{A}^{\mp}.$$

Dans cette étude, les suites $\mathscr{A}^+$ et $\mathscr{A}^-$ jouent des rôles identiques; nous avons choisi de privilégier la première.

Le fait que la transformation $n \longmapsto 2n+1$ envoie $\mathscr{A}^+$ dans $\mathscr{A}^-$ et vice-versa, et que ces deux ensembles forment une partition de $\mathbb{N}$ donne

naissance à un jeu de *ping–pong* entre $\mathscr{A}^+$ et $\mathscr{A}^-$ qui conduit à la remarque suivante:

Remarque 0. Pour tout $x \geqq 1$ et tout $\mathscr{C} \subset N$, on a l'inégalité

$$|\{c;\ c \in \mathscr{C},\ c \in \mathscr{A}^+,\ c \leqq x\}| \geqq \frac{1}{2}|\{c;\ c \in \mathscr{C},\ 2c+1 \in \mathscr{C},\ 2c+1 \leqq x\}|\,.$$

En particulier, si l'équation $2c+1=c'$ admet une infinité de solutions avec c et c' dans $\mathscr{C}$, chacun des ensembles $\mathscr{A}^+ \cap \mathscr{C}$ et $\mathscr{A}^- \cap \mathscr{C}$ est infini.

Ce processus général peut être testé en prenant des suites $\mathscr{C}$ très particulières: par exemple si $\mathscr{C}$ est l'ensemble des valeurs d'un polynôme entier $P(n)$ du second degré, l'équation $2c+1=c'$ est du type Pell-Fermat, le résultat est tout de fois décevant, les solutions trouvées sont peu nombreuses et cet abord n'est guère plus efficace que l'abord direct, qui consiste à chercher dans $\mathscr{A}^+$ des éléments de la forme $P(n)$ où on part de n dont la forme est, suivant les cas 2^{k_1}, $2^{k_1}+2^{k_2}$,... avec les k_i judicieusement choisis. Mais, selon toute vraisemblance, les familles de solutions trouvées par ces deux méthodes, sont de nature différente.

Une application, à notre avis surprenante, concerne les entiers dont on a fixé l'ordre de grandeur du facteur premier de rang donné et passe par d'ingénieux arguments de combinatoire dus à Hildebrand ([Hi]) et Balog ([Ba]).

Corollaire 0. *Soit* $p_1(n) \geqq p_2(n) \cdots$ *la suite décroissante des diviseurs premiers ou égaux à* 1 *de l'entier* n. *Soit* $l \geqq 1$ *un entier fixé,* α *et* β *deux constantes vérifiant* $0 \leqq \alpha < \beta \leqq 1$. *Il existe alors une constante* $\delta = \delta(l,\alpha,\beta) > 0$, *telle qu'on ait, pour* x *assez grand la minoration*

$$|\{n \leqq x; n^\alpha < p_l(n) < n^\beta, n \in \mathscr{A}^+\}| \geqq \delta x\,.$$

Pour montrer ceci, on prend pour $\mathscr{C}$, l'ensemble

$$\mathscr{C} = \{n; n^\alpha < p_l(n) < n^\beta\}\,,$$

cet ensemble est de densité positive et est *k-stable* au sens de Balog et Hildebrand, par multiplication et division par tout nombre entier $k \geqq 1$, c'est-à-dire qu'on a les relations

$$k\mathscr{C} \dot{\subset} \mathscr{C} \text{ et } k^{-1}(\mathscr{C} \cap k\mathbb{N}) \dot{\subset} \mathscr{C}\,,$$

où $k\mathscr{C} = \{kc;\ c \in \mathscr{C}\}$ et $\mathscr{C} \dot{\subset} \mathscr{C}'$ signifie que $\mathscr{C}$ est quasiment inclus dans $\mathscr{C}'$ autrement dit que l'ensemble $\{c;\ c \in \mathscr{C},\ c \notin \mathscr{C}'\}$ est de densité nulle.

Balog avait conjecturé et Hildebrand ([Hi]) avait démontré qu'il suffit qu'une suite générale $\mathscr{A}$ d'entiers vérifie les conditions précédentes de densité et de stabilité pour que l'intersection $\mathscr{A} \cap (\mathscr{A}+1)$, soit de densité positive. Mais ici, nous devons traiter le cas de l'intersection $\mathscr{A} \cap (2\mathscr{A}+1)$ pour montrer qu'elle est de densité positive. Il faut donc adapter la preuve d'Hildebrand, mais cette modification n'est pas immédiate. Elle a été accomplie par Balog et Ruzsa ([B-R]) dans un récent travail, qui montrent ainsi que, toujours sous les

hypothèses précédentes, l'intersection $\mathscr{A} \cap (m\mathscr{A} + n)$ est de densité positive pour tous les entiers n et $m \geqq 1$.

Consacrons-nous à la recherche des nombres premiers dans $\mathscr{A}^+$ et dans $\mathscr{A}^-$. Grâce à ce qui précède, on peut énoncer:

Si l'équation $p' = 2p + 1$ a une infinité de solutions en nombres premiers p et p', chacun des ensembles $\mathscr{A}^+$ et $\mathscr{A}^-$ contient une infinité de nombres premiers.

Puisque les méthodes actuelles sont trop faibles pour montrer que l'équation précédente en nombres premiers a une infinité de solutions, on peut poursuivre ce jeu en se rabattant sur le théorème de Chen ([H-R], chapitre 11 par exemple) qui montre qu'il y a une infinité de p tels que $2p + 1$ ait au plus deux facteurs premiers. De façon précise, ce théorème (sans doute plus connu dans le cadre du problème de Goldbach et de la conjecture des nombres premiers jumeaux) affirme l'existence d'une constante positive α_0 telle que l'inégalité suivante soit vraie pour x suffisamment grand:

$$(1.1) \qquad |\{p; p \leqq x, 2p + 1 = p_1 \text{ ou } 2p + 1 = p_1 p_2\}| \geqq \alpha_0 \frac{x}{\log^2 x} .$$

Supposons qu'il n'y ait qu'un nombre fini de nombres premiers dans $\mathscr{A}^+$. L'inégalité (1.1) donne alors

$$|\{p \in \mathscr{A}^-; p \leqq x, 2p + 1 = p_1 p_2\}| \geqq \frac{\alpha_0}{2} \frac{x}{\log^2 x} ,$$

maintenant, dans l'expression précédente $2p + 1 \in \mathscr{A}^+$, d'où le

Théorème 0. *L'un au moins des énoncés suivants est correct*

i) *Il y a une infinité de nombres premiers dans $\mathscr{A}^+$.*

ii) *Il y a une infinité de couples de nombres premiers (p_1, p_2) de $(\mathscr{A}^-)^2$, tels que $p_1 p_2$ appartienne à $\mathscr{A}^+$.*

Puisque l'ensemble $\mathscr{A}^+$ est stable par multiplication par 2, on déduit la minoration asymptotique suivante, qui semble briser le phénomène de parité attaché au crible linéaire:

$$|\{p_1 p_2 \leqq x; p_1 p_2 \in \mathscr{A}^+\}| \gg x \log^{-2} x .$$

De même, si $\mathscr{B}^+$ et $\mathscr{B}^-$ désignent respectivement les ensembles d'entiers qui, écrits en base 2, ont un nombre pair de blocs 11 ou un nombre impair de tels blocs, on voit, en constatant que l'application $b \longmapsto 2b + 1$ envoie les impairs de $\mathscr{B}^{\pm}$ dans les impairs de $\mathscr{B}^{\mp}$, que le Théorème 0 est vrai en remplaçant $\mathscr{A}$ par $\mathscr{B}$. Bien entendu, le Théorème 0 et sa variante entraînent que $\mathscr{A}^+$ et $\mathscr{B}^+$ (connues respectivement dans la littérature sous le nom de suites de Thue-Morse et Rudin-Shapiro) contiennent une infinité d'entiers ayant au plus deux facteurs premiers.

Ce principe se transpose au cas plus général des suites automatiques, dont nous rappelons la définition. Soit r un entier supérieur ou égal à 2. On désigne par $[r]$ l'alphabet $\{0, 1, \ldots, r-1\}$, par $[r]^k$ l'ensemble des mots de

longueur $k \geqq 0$ et par $[r]^* = \cup_{k \geqq 0}[r]^k$ l'ensemble des mots de longueur finie sur l'alphabet $[r]$.

Définition 1. *Un r-automate* $\mathfrak{A}$ *est la donnée d'un quadruplet* $\mathfrak{A} = (A, a_0, \varphi, \tau)$ *avec*

i) A *alphabet fini*;
ii) $a_0 \in A$ (*état initial*);
iii) $\varphi : A \times [r] \longmapsto A$;
iv) $\tau : A \longmapsto \{0,1\}$ (*application de sortie*).

Pour tout $(a,s) \in A \times [r]$, on pose $\varphi(a,s) = a.s$. On prolonge par concaténation, φ en une application de $A \times [r]^*$ vers A. En particulier, si n est un entier positif dont la représentation en base r est $\tilde{n} = \varepsilon_g \varepsilon_{g-1} \cdots \varepsilon_0 \in [r]^{g+1}$, on pose pour tout $a \in A$:

$$\varphi(a, \tilde{n}) = a \cdot \tilde{n} = a \cdot \varepsilon_g \varepsilon_{g-1} \cdots \varepsilon_0 ,$$

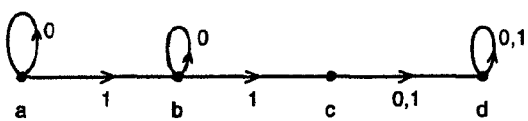
(à $n = 0$, on associe le mot vide $\emptyset$, avec $\varphi(a, \emptyset) = a$).

Définition 2. *On dit qu'une suite d'entiers* $\mathscr{U}$ *est engendrée par le r-automate* $\mathfrak{A} = (A, a_0, \varphi, \tau)$, *si l'on a l'équivalence*

$$n \in \mathscr{U} \Longleftrightarrow \tau(a_0 \cdot \tilde{n}) = 1 .$$

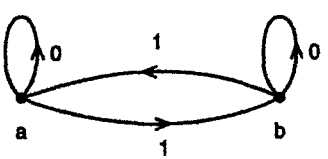
Définition 3. *On dit qu'un r-automate* $\mathfrak{A} = (A, a_0, \varphi, \tau)$ *est irréductible, s'il est toujours possible de passer d'un état à un autre par un certain chemin; en d'autres termes, pour tout a et a' de A, il existe* $l > 0$ *et* μ *dans* $[r]^l$, *tel que* $a \cdot \mu = a'$.

Exemple 1. *La suite des entiers* $2^n + 1$ *est engendrée par le 2-automate* $(\{a,b,c,d\}, a, \varphi, \tau)$ *avec* $a \cdot 0 = a$, $a \cdot 1 = b$, $b \cdot 0 = b$, $b \cdot 1 = c$, $c \cdot 0 = c \cdot 1 = d \cdot 0 = d \cdot 1 = d$ *et* $\tau(a) = \tau(b) = \tau(d) = 0$ *et* $\tau(c) = 1$:



Cet automate n'est pas irréductible.

Exemple 2. *La suite* $\mathscr{A}^+$ *est engendrée par le 2-automate* $(\{a,b\}, a, \varphi, \tau)$ *avec* $a \cdot 0 = a$, $a \cdot 1 = b$, $b \cdot 0 = b$, $b \cdot 1 = a$ *et* $\tau(a) = 1$, $\tau(b) = 0$:



Cet automate est irréductible et se généralise sans problème à la suite des entiers n tels que $s(n)$ appartienne à une certaine classe de congruence ou lorsqu'on passe à un développement dans une autre base.

Soit $\mathscr{U}$ une suite d'entiers engendrée par un r-automate irréductible $\mathfrak{A} = (A, a_0, \varphi, \tau)$ et $a \in A$ tel que $\tau(a) = 1$. Posons $\{a_1, \ldots, a_g\} = \tau^{-1}(\{0\})$. Par hypothèse, il existe des entiers strictement positifs l_i tels que, pour tout $1 \leqq i \leqq g$, il existe $\mu_i \in [r]^{l_i}$ tel que $a_i \cdot \mu_i = a$. En particulier, il existe $0 \leqq m_i < r^{l_i}$ pour $1 \leqq i \leqq g$ tels que, pour tout entier positif n, l'un au moins des entiers

$$n,\ r^{l_1}n + m_1, \ldots,\ r^{l_g}n + m_g\,,$$

appartient à la suite $\mathscr{U}$. Supposons tout d'abord que tous les m_i sont non nuls et que les facteurs $r^{l_i}X + m_i$ sont distincts. Soit $P_{\mathfrak{A}}(X)$ le polynôme

$$P_{\mathfrak{A}}(X) = X(r^{l}X + m_1)\cdots(r^{l_g}X + m_g)\,.$$

Ce polynôme est de degré $g+1$ et il existe $\kappa(\mathfrak{A})$ facteurs premiers p fixes, c'est-à-dire tels que, pour tout n, $p | P_{\mathfrak{A}}(n)$ (on a l'inégalité grossière: $\kappa(\mathfrak{A}) \leqq g + 1 + \omega((r, m_1 \cdots m_g))$, avec ω: fonction nombre de facteurs premiers). On se tourne maintenant vers [H-R] Theorem 10.5, il y a donc un entier G, une infinité de valeurs de n tels que $P_{\mathfrak{A}}(n)$ ait au plus G facteurs premiers. En fait ce théorème de [H–R] n'est énoncé que dans le cas où le polynôme en question n'a pas de facteur fixe, ce résultat continue d'être vrai dans le cas général, quitte à augmenter de $\kappa(\mathfrak{A})$ la valeur de G proposée dans ce théorème.

Dans le cas de nullité d'un des m_i ou d'égalité de deux facteurs $r^{l_i}X + m_i$, on se ramène au cas précédent en mettant de côté certains des facteurs de $P_{\mathfrak{A}}(X)$. Si on est intéressé par l'existence de G, le recours au crible pondéré est inutile; le crible de Brun, par exemple, suffit. Puisque pour $g = 1$ on retrouve le principe du ping-pong, l'énoncé suivant apparaît donc comme une généralisation du Théorème 0:

Théorème 0bis. *Soit $\mathscr{U}$ une suite d'entiers engendrée par un automate irréductible. Il existe une constante G et une infinité d'éléments de $\mathscr{U}$ ayant au plus G facteurs premiers.*

Notre démarche est beaucoup trop générale pour conduire à des valeurs optimales de G en fonction de l'automate $\mathfrak{A}$, mais fournit des exemples de suites non engendrées par un automate irréductible:

Corollaire 0. *Soit $\psi(n)$ une fonction tendant vers l'infini avec n. Alors aucune sous-suite non vide de l'ensemble*

$$\{n; \omega(n) \geqq \psi(n)\}$$

n'est engendrée par un automate irréductible.

Notre but est d'accéder à des petites valeurs de G dans le cas particulier des suites $\mathscr{A}_{q,b}$ des entiers n tels que $s(n)$ soit congru à b modulo q, (ainsi,

on a $\mathscr{A}^+ = \mathscr{A}_{2,0}$ et $\mathscr{A}^- = \mathscr{A}_{2,1}$). Volontairement, nous nous restreignons aux développements en base 2, les autres bases engendrent d'autres types de problèmes qui feront l'objet d'un prochain travail. L'un des objets de cet article est de montrer le

Théorème 1. *Pour tout choix des entiers $q \geqq 2$ et b, la suite $\mathscr{A}_{q,b}$ contient une infinité d'entiers ayant au plus deux facteurs premiers. Plus précisément, on a la minoration asymptotique*

$$|\{n; n \leqq x, s(n) \equiv b \pmod q,\ n = p_1 \text{ ou } n = p_1 p_2\}| \gg_q \frac{x}{\log x}.$$

Signalons que l'ordre de grandeur espéré du cardinal minoré précédemment est $x(\log\log x)/\log x$, et que, pour $q = 2$, l'application directe du principe du ping-pong et de ses améliorations conduisent à une minoration de moindre qualité.

Les techniques employées dans la preuve du Théorème 1 sont celles du crible linéaire appliqué à $\mathscr{A}_{q,b}$ et passent ainsi par une étude de la répartition en moyenne de $\mathscr{A}_{q,b}$ dans les progressions arithmétiques. Nous posons donc pour a et d entiers,

$$A_{q,b}(x; d, a) = |\{n < x; s(n) \equiv b \pmod q,\ n \equiv a \pmod d\}|,$$

les quantités $A^{\pm}(x; d, a)$ ayant une définition évidente. Nous verrons que la preuve du Théorème 2 ci-dessous repose sur la majoration de l'intégrale $I_N(\xi)$ définie par

$$I_N(\xi) = \int_0^1 \prod_{0 \leqq n < N} |\cos(\pi(2^n t + \xi))| dt,$$

et, en particulier, pour ξ fixé, sur les valeurs des constantes C vérifiant la relation

$$I_N(\xi) = O(C^N)\ (N \longrightarrow \infty). \tag{1.2}$$

Nous montrerons le

Théorème 2. *Soit C_q une constante vérifiant* (1.2) *pour tout $\xi \in \{\frac{1}{q}, \ldots, \frac{q-1}{q}\}$. On a, uniformément pour x et D supérieurs à* 1

$$\sum_{d \leqq D} \max_{y \leqq x} \max_{a} \left| A_{q,b}(y; d, a) - \frac{y}{qd} \right| = O\left(x^{1 + \frac{\log C_q}{\log 2}} D + x^{\gamma_q} (D^{3 - 2\gamma_q + 2\frac{\log C_q}{\log 2}} + \log x) \right), \tag{1.3}$$

pour une certaine constante $\gamma_q < 1$.

Pour rendre plus parlant le Théorème 2, il faut proposer des valeurs de C_q. Nous verrons au paragraphe IV.1, qu'on peut, pour tout q, prendre $C_q = 1/\sqrt{2}$, le second membre de (1.3) étant alors, pour tout A, en $O(x(\log x)^{-A})$, pour $D = x^{1/2}(\log x)^{-B(A)}$. Ceci est l'exact analogue du théorème de

Bombieri-Vinogradov pour les nombres premiers. Nous montrerons la

Proposition 1. *Pour tout réel ξ, on a*

$$I_N(\xi) = O\left(\left(\frac{\cos \pi/8}{2}\right)^{N/2}\right).$$

Autrement dit, (1.2) est vérifiée pour tout ξ, avec le choix $C = 0,679661...$ La Proposition 1 et le Théorème 2 entraînent immédiatement le

Corollaire 1. *On a*

$$\sum_{d \leqq D} \max_{y \leqq x} \max_{a} \left| A_{q,b}(y; d, a) - \frac{y}{qd} \right| = O_{q,A}(x(\log 2x)^{-A}),$$

pour tout A et $D = x^{0,55711}$.

Il est alors facile d'appliquer les formules du crible pondéré. La grande valeur de l'exposant de répartition, à savoir 0,55711 ne nous oblige pas à recourir à des systèmes de poids très sophistiqués: les poids de Richert sont suffisants. Le Théorème 9.3 et la page 258 de [H-R] fournissent la valeur $\Lambda_2 = 3 - (\log(18/5))/\log 3 = 1,8340$. Donc, puisque $0,55711 > 1/\Lambda_2$, le crible pondéré appliqué à la suite $\mathscr{A}_{q,b} \cap [1, x]$ donne directement le Théorème 1.

Une autre application du Corollaire 1 nous est fournie par la formule de majoration du crible linéaire. On a, de façon classique la majoration

$$|\{p;\ p \leqq x,\ s(p) \equiv b \pmod q\}| \leqq \frac{2}{0,5571} \cdot \frac{x}{q \log x},$$

pour x suffisamment grand; d'où, en sommant cette majoration sur les classes b n'appartenant pas à une ensemble $\mathscr{Q}$ de classes de congruences modulo q et en appliquant le théorème des nombres premiers, on obtient par soustraction le

Corollaire 2. *Soit q un entier au moins égal à 2 et $\mathscr{Q}$ un ensemble de classes de congruences modulo q. Il existe alors une infinité de nombres premiers p tels que $s(p) \in \mathscr{Q}$ dès que $|\mathscr{Q}| \geqq 0,722 \cdot q$.*

Ce Corollaire ne donne rien pour $q = 2$ ou $q = 3$ mais indique, par exemple, qu'il y a une infinité de p, et même une proportion positive, avec $s(p) \equiv 0$, 1 ou 2 (modulo 4). On verra par la suite, que q étant donné, on peut améliorer la valeur de C_q, et ainsi diminuer quelque peu la valeur de la constante apparaissant dans le Corollaire précédent.

Les intégrales $I_N(\xi)$ ont un intérêt intrinsèque. Par la théorie des opérateurs de transfert, nous en donnerons des équivalents asymptotiques sous la forme du.

Théorème 3. *Soit ξ non entier. Il existe deux constantes absolues κ_ξ et $\lambda_\xi > 0$ telles que, pour $N \longrightarrow \infty$, on ait l'égalité*

$$I_N(\xi) = \kappa_\xi \lambda_\xi^N (1 + o(1)). \tag{1.4}$$

Signalons qu'un tel énoncé est faux pour ξ entier. En effet des manipulations élémentaires de trigonométrie conduisent à l'égalité

$$I_N(0) = 2^{-N} \int_0^1 \frac{|\sin 2^N \pi t|}{\sin \pi t} dt ,$$

puis des techniques simples de découpages d'intervalles, de changements de variables, de majorations et de minorations conduisent à la relation $I_N(0) \asymp N 2^{-N}$. Ce comportement différent de l'intégrale $I_N(\xi)$ pour ξ entier s'interprète, en terme de décomposition spectrale de l'opérateur P_0 (voir paragraphe V) par un bloc de Jordan de longueur 2 associé à la valeur propre 1.

L'étude de la fonction $\xi \mapsto \lambda_\xi$ peut donner lieu à d'intéressantes questions tant théoriques (comportement local, global, en moyenne...) que numériques (encadrement de λ_ξ, quotient de Rayleigh de l'opérateur de transfert qui lui est associé...). Ainsi dans ce travail, nous nous sommes restreints, par la minoration de $I_N(\xi)$ et par la Proposition 1, à l'encadrement général

$$\frac{1}{2} < \lambda_\xi < 0,679661...$$

pour ξ non entier.

La suite de notre travail sera uniquement consacrée au cas $q = 2$ que nous étudierons plus soigneusement. Nous poserons

$$I_N = I_N\left(\frac{1}{2}\right) = \int_0^1 \prod_{0 \leq n < N} |\sin(2^n \pi t)| dt .$$

La valeur numérique précise de $\lambda = \lambda_{1/2}$ nous semble quelque peu délicate à appréhender. Des calculs sur machine de l'intégrale I_N nous amènent à penser que $\lambda = 0,661..$ La méthode choisie, pour deviner cette valeur de λ consiste en un découpage de l'intervalle $[0, 1]$ en 2^N intervalles où le produit des fonctions sinus a un signe constant, en une intégration formelle sur chacun des intervalles, grâce au programme Mathematica, enfin, en un calcul exact par une différence des valeurs de ces primitives aux bornes. Il est facile de voir que le calcul précédent sature très vite, nous n'avons calculé qu'une douzaine de valeurs de I_N.

Nous montrerons à la Proposition 2, que, dans (1.3), on peut prendre

$$\gamma_2 = \log 3 / \log 4 .$$

Par une méthode directe, nous démontrerons l'encadrement

$$c_{21} < \lambda < C_{20} \tag{1.5}$$

où les constantes c_{21} et C_{20} seront définies comme minimum et maximum de certaines fonctions. Elles ont respectivement pour valeurs numériques $c_{21} = 0,654336...$ et $C_{20} = 0,663197...$ Étant donné le contexte, il n'y a guère de risque de confusion avec C_q apparaissant dans (1.3).

Le Théorème 3 permet d'évaluer la norme $\| \cdot \|_1$ de certains polynômes trigonométriques liés aux suites automatiques. En écrivant la fonction caractéristique de $\mathscr{A}^+$ sous la forme $(1 + (-1)^{s(n)})/2$ et en anticipant la technique qui sera développée au paragraphe II, on a l'égalité suivante (nous nous

restreignons au cas $x = 2^N$, pour raison de commodité):

$$\int_0^1 \left| \sum_{\substack{a \in \mathscr{A}^+ \\ a < x}} \exp(2\pi i a\alpha) \right| d\alpha$$

$$= \frac{1}{2} \int_0^1 \left| \sum_{n<x} (-1)^{s(n)} \exp(2\pi i n\alpha) \right| d\alpha + O\left(\int_0^1 \left| \sum_{n<x} \exp(2\pi i n\alpha) \right| d\alpha \right)$$

$$= \frac{1}{2} \cdot 2^N \cdot I_N + O(\log x) \sim \frac{\kappa_{1/2}}{2} x^{\Lambda},$$

où Λ est une constante absolue comprise entre 0,3881 et 0,4075.

La suite $\mathscr{A}^+$ se différencie totalement de la suite $\mathscr{B}^+$ de Rudin-Shapiro évoquée ci-dessus: soit ε_n le nombre de blocs 11 dans le développement en base 2 de $\mathscr{B}^+$. On a donc

$$\int_0^1 \left| \sum_{\substack{b \in \mathscr{B}^+ \\ b < x}} \exp(2\pi i b\alpha) \right| d\alpha$$

$$= \frac{1}{2} \int_0^1 \left| \sum_{n<x} (-1)^{\varepsilon_n} \exp(2\pi i n\alpha) \right| d\alpha + O(\log x) \ll x^{1/2},$$

par l'inégalité de Cauchy-Schwarz. Par contre, on a la minoration

$$\int_0^1 \left| \sum_{n<x} (-1)^{\varepsilon_n} \exp(2\pi i n\alpha) \right| d\alpha \geqq \left(\int_0^1 |\cdots|^2 d\alpha \right) \left\{ \sup_{0 \leqq \alpha \leqq 1} |\cdots| \right\}^{-1}.$$

Mais la suite de Rudin-Shapiro jouit de l'importante propriété que le sup précédent est $O(x^{1/2})$ ([Ru, Sh] et aussi [A-MF] pour des généralisations); en conclusion, on voit que, à la totale différence de $\mathscr{A}^+$, la suite $\mathscr{B}^+$ vérifie l'encadrement

$$\int_0^1 \left| \sum_{\substack{b \in \mathscr{B}^+ \\ b < x}} \exp(2\pi i b\alpha) \right| d\alpha \asymp x^{1/2}.$$

Pour revenir à notre propos principal, nous reportons dans (1.4) et dans (1.3) la majoration (1.5), nous obtenons alors directement le

Corollaire 3. *On a l'égalité*

$$\sum_{d \leqq D} \max_{y \leqq x} \max_{a} \left| A^{\pm}(y; d, a) - \frac{y}{2d} \right| = O(x(\log 2x)^{-A}), \tag{1.6}$$

pour tout A et $D = x^{0,5924}$.

Il est bon d'insister sur la valeur très élevée de l'exposant 0,5924, qui pourrait même être poussée au-delà de 0,595, si notre hypothèse sur la valeur numérique de λ était vérifiée. En fait, il nous suffirait d'avoir dans le Corollaire 3, un exposant quelque peu inférieur à 0,5 pour en déduire le Théorème 1, en combinant des méthodes renommées de théorie analytique des nombres: crible pondéré et principe d'inversion du rôle des variables d'Iwaniec-Chen, méthodes

qui menèrent à la preuve du Théorème de Chen cité auparavant. En d'autres termes, le Théorème 1 (avec $q = 2$) quoique très attrayant, est beaucoup moins profond que le Corollaire 3.

La puissance du crible sera augmentée en profitant du fait de la densité de $\mathscr{A}^+$. Ainsi, par le crible linéaire et le Corollaire 3, nous obtenons la minoration classique

$$|\{a \in \mathscr{A}^+; a \leqq x,\ p|a \Longrightarrow p \geqq x^{0,296}\}| \gg \frac{x}{\log x}. \tag{1.7}$$

En jouant sur la combinatoire qui est au départ des formules du crible de Rosser-Iwaniec, il est possible de tenir compte de termes systématiquement oubliés par le crible général ([I–J, Ha, Fo] par exemple); dans notre cas, ils sont alors traités par l'inversion du rôle des variables et une majoration absolument triviale (voir (7.1)). Ceci nous conduira au

Corollaire 4. *Soit D vérifiant pour tout A l'égalité* (1.6).
Alors, pour $z \longrightarrow \infty$ et $2 \leqq z \leqq D^{\frac{1}{2}}$, on a la minoration

$$|\{a \in \mathscr{A}^+; a < x, p|a \Longrightarrow p \geqq z\}|$$
$$\geqq (1 - o(1))\frac{xe^{-\gamma}}{2\log z}\left(F\left(\frac{\log x}{\log z}\right) + f\left(\frac{\log x}{\log z}\right) - F\left(\frac{\log D}{\log z}\right)\right).$$

Dans cette expression F et f sont les fonctions classiques du crible linéaire et γ est la constante d'Euler.

Signalons tout d'abord que la minoration standard de la quantité en question au Corollaire 4 est

$$(1 - o(1))\frac{xe^{-\gamma}}{2\log z} f\left(\frac{\log D}{\log z}\right), \tag{1.8}$$

qui implique directement (1.7), puisque $f(s) > 0$ pour $s > 2$. Pour illustrer le gain apporté par ce corollaire, il suffit de savoir que $F(s) = \frac{2e^{\gamma}}{s}$ pour $s \leqq 3$ et $f(s) = \frac{2e^{\gamma}\log(s-1)}{s}$ pour $2 \leqq s \leqq 4$; on voit alors que (1.7) est vrai avec un exposant légérement supérieur à la valeur critique 1/3 au lieu de 0,2951. Cette remarque redonne une démonstration du Théorème 1, toujours pour $q = 2$. Le gain par rapport à la formule (1.8) de minoration du crible linéaire est d'autant moindre que la valeur de $\log D/\log x$ est grande, ou encore $\log D/\log z$ est importante (lemme fondamental du crible).

Une autre façon de tendre vers la notion de nombre premier est de se situer dans un problème de crible, autant que possible assez naturel, dans lequel la dimension soit assez proche de 1. C'est ce qu'ont fait Iwaniec ([Iw2]) puis Iwaniec et Pomykala ([I-P]) qui se sont intéressés au problème de la représentation d'un entier grand, ou d'un entier fixé comme somme ou comme différence de deux normes d'idéaux d'une extension abélienne de $\mathbb{Q}$ de degré 3 ou 4. Les dimensions des cribles rencontrés sont alors 2/3 et 3/4. En nous inspirant de ces articles et en remplaçant le principe d'inversion du rôle des variables par l'inégalité (7.1), nous montrerons le

Corollaire 5. *Soit $K/\mathbb{Q}$ une extension abélienne de degré $k = 2$, 3 ou 4. On a alors la minoration*

$$|\{a \in \mathscr{A}^+;\ a \leqq x; a = N\mathfrak{A},\ \mathfrak{A} \text{ idéal de } K\}| \gg x(\log x)^{\frac{1}{k}-1}.$$

L'élaboration de cet article fut facilitée par des conversations avec Jean-Pierre Conze, Loïc Hervé, François Parreau et Joël Rivat. Qu'ils en soient remerciés !

II Passage aux sommes trigonométriques

Nous commençons par étudier le comportement de $\mathscr{A}_{q,b}$ dans une progression arithmétique fixée. Cette étude, qui a été déjà menée par Gelfond ([Ge]) (voir aussi [Fi]), présente un intérêt intrinsèque et est un passage obligé avant l'étude en moyenne faite au Théorème 2. Nous donnons une démonstration un peu différente de la

Proposition 2 ([Ge] Théorème 1). *Soit ζ un nombre complexe de module 1. Posons*

$$S_\zeta(x; d, a) = \sum_{\substack{0 \leqq n < x \\ n \equiv a (\mathrm{mod}\ d)}} \zeta^{s(n)}.$$

On a, uniformément pour $x \geqq 1$, a et d entiers ($d \geqq 1$),

$$S_\zeta(x; d, a) = O_\zeta(x^{\gamma(\zeta)}), \tag{2.1}$$

où $\gamma(\zeta) < 1$ si $\zeta \neq 1$,

et, dans le cas où $\zeta = -1$, l'inégalité plus précise

$$|S_{-1}(x; d, a)| \leqq (1 + \sqrt{3})\, x^{(\log 3/\log 4)}. \tag{2.2}$$

Uniformément pour a et $d \geqq 1$ entiers, on a l'égalité

$$A_{q,b}(x; d, a) = \frac{x}{qd} + O(x^{\gamma_q}). \tag{2.3}$$

avec $\gamma_q := \max\{\gamma(\zeta);\ \zeta^q = 1,\ \zeta \neq 1\} < 1$. En particulier, on a $\gamma_2 = \log 3/\log 4$.

Enfin, pour tout $D \leqq x$ et pour tout A, on a l'égalité

$$\sum_{d \leqq D} \sum_{a=0}^{d-1} \left(A_{q,b}(x; d, a) - \frac{x}{qd} \right)^2 = O(Dx) + O_A(x^2(\log 2x)^{-A}). \tag{2.4}$$

1. Démonstration de la Proposition 2

Posons, pour α réel,

$$T_\zeta(x; \alpha, a) = \sum_{0 \leqq n < x} \zeta^{s(n)} e^{2i\pi(n-a)\alpha},$$

on déduit alors, par orthogonalité des caractères, l'égalité

$$S_\zeta(x;d,a) = \frac{1}{d}\sum_{0\leqq j<d} T_\zeta\left(x;\frac{j}{d},a\right). \tag{2.5}$$

Majorons $T_\zeta(x;\alpha,a)$ uniformément par rapport à α. Nous partons de l'égalité

$$|T_\zeta(x;\alpha,a)| = |T_\zeta(x,\alpha)|$$

avec

$$T_\zeta(x,\alpha) = T_\zeta(x;\alpha,0).$$

Nous divisons la démonstration en deux cas:

(i) $x = 2^N$ avec N entier. L'existence et l'unicité de l'écriture de tout entier en base 2, factorise $T_\zeta(2^N,\alpha)$ sous la forme

$$T_\zeta(2^N,\alpha) = \prod_{0\leqq n<N}(1+e^{2i\pi(2^n\alpha+\xi)}),$$

en ayant posé $\zeta = e^{2i\pi\xi}$, ce qui conduit à l'égalité

$$|T_\zeta(2^N,\alpha)| = 2^N \prod_{0\leqq n<N} |\cos(\pi(2^n\alpha+\xi))| = 2^N|F_N(\alpha,\xi)|,$$

avec

$$F_N(\alpha,\xi) = \prod_{0\leqq n<N}\cos(\pi(2^n\alpha+\xi)).$$

Dans le produit $F_N(\alpha,\xi)$, on regroupe les termes deux par deux, d'où l'égalité

$$|F_N(\alpha,\xi)| = O\left(\{\max_t |\cos(\pi(t+\xi))\cos(\pi(2t+\xi))|\}^{N/2}\right);$$

puisque ξ n'est pas un entier, le maximum ci-dessus est strictement inférieur à 1, d'où, dans ce cas, l'égalité

$$F_N(\alpha,\xi) = O(\beta(\xi)^N),\ (\beta(\xi)<1), \tag{2.6}$$

et enfin

$$T_\zeta(x,\alpha) = O(x^{\gamma(\zeta)}), \tag{2.7}$$

avec $\gamma(\zeta) := 1 + \log\beta(\xi)/\log 2\ (<1)$.

(ii) Cas général. On peut supposer que x est un entier qu'on écrit sous la forme $x = 2^{n_1}+\cdots+2^{n_k}$ avec $n_1 > \cdots > n_k$. La somme étudiée se décompose en

$$\begin{aligned} T_\zeta(x,\alpha) = {} & T_\zeta(2^{n_1},\alpha) + \zeta e^{2i\pi 2^{n_1}\alpha} T_\zeta(2^{n_2},\alpha) \\ & + \zeta^2 e^{2i\pi(2^{n_1}+2^{n_2})\alpha} T_\zeta(2^{n_3},\alpha) + \cdots \end{aligned} \tag{2.8}$$

une application répétée de (2.7) à chacun des éléments à droite de (2.8) montre alors que (2.7) est vraie dans tous les cas. Il suffit de regrouper (2.5) et (2.7) pour terminer la preuve de (2.1).

La preuve de (2.3) consiste à écrire l'égalité

$$A_{q,b}(x;d,a) = \frac{1}{q}\sum_{\zeta^q=1} \zeta^{-b} S_\zeta(x;d,a)\,; \tag{2.9}$$

le terme $\zeta = 1$ est le terme principal, il vaut donc $x/(qd) + O(1)$, dans les autres cas, on applique (2.1).

Enfin, puisque (2.3) implique que $\mathscr{A}_{q,b}$ vérifie le critère U de [Ho], par le Théorème 1 du même article, on voit que cette suite vérifie un théorème à la Barban-Davenport-Halberstam, d'où (2.4).

2. Le cas $q = 2$

Dans ce cas, on écrit

$$\begin{aligned}\left|F_N\left(\alpha, \frac{1}{2}\right)\right| &= |\sin(\pi\alpha)|^{1/3} |\sin(2^{N-1}\pi\alpha)|^{2/3} \\ &\quad \times \prod_{n=0}^{n=N-2} (|\sin(2^n\pi\alpha)|^{2/3} |\sin(2^{n+1}\pi\alpha)|^{1/3}) \\ &\leqq \prod_{n=0}^{n=N-2} \varphi(|\sin(2^n\pi\alpha)|)\,,\end{aligned}$$

où on a posé $\varphi(t) = t^{2/3}(2t\sqrt{1-t^2})^{1/3}$. Cette fonction est définie pour $t \in [0,1]$ et atteint son maximum en $t = \sqrt{3}/2$ où elle vaut $\sqrt{3}/2$.

On a donc montré l'inégalité

$$\left|F_N\left(\alpha, \frac{1}{2}\right)\right| \leqq \left(\frac{\sqrt{3}}{2}\right)^{N-1}, \tag{2.10}$$

valable pour tout α réel, on déduit alors l'inégalité

$$|T_{-1}(2^N, \alpha)| \leqq 2(\sqrt{3})^{N-1}\,.$$

Dans le cas général, on fait la même décomposition que dans (2.8) d'où l'inégalité

$$\begin{aligned}|T_{-1}(x,\alpha)| &\leqq \frac{2}{\sqrt{3}}((\sqrt{3})^{n_1} + \cdots + (\sqrt{3})^{n_k}) \leqq (1+\sqrt{3})(\sqrt{3})^{n_1} \\ &\leqq (1+\sqrt{3})(2^{n_1} + \cdots + 2^{n_k})^{\gamma_2} \leqq (1+\sqrt{3})x^{\gamma_2}\,,\end{aligned}$$

ce qui, grâce à (2.5), termine la démonstration de (2.2).

3. Remarques

Il nous faut signaler le caractère quasi-optimal de γ_2 dans (2.2) et (2.3), en effet en choisissant $\alpha = 2/3$ et en constatant que $2^n\pi\alpha = \pm 2\pi/3 \pmod{2\pi}$, on a l'égalité

$$|T_{-1}(2^N, 2/3)| = 2^N(\sqrt{3}/2)^N\,.$$

Cette quasi-optimalité se retrouve si on se reporte au résultat de Newman ([Ne]), raffiné par une autre méthode par Coquet ([Co]), qui a montré l'égalité

$$\frac{\overline{\lim} \sum_{n<N}(-1)^{s(3n)}}{N^{\gamma_2}} = 1,60195...$$

Autrement dit, dans l'énoncé de la Proposition 2, on ne peut remplacer la constante $1+\sqrt{3} = 2,732...$ de (2.2) par une constante inférieure à $\frac{1,60195...}{3^{\gamma_2}} = 0,67071...$ Au vu du choix précédent de α et des résultats de Newman et Coquet, on perçoit le rôle particulier le l'entier $d = 3$.

III Preuve du Théorème 2

L'objet de ce paragraphe est d'utiliser les techniques du grand crible qui ont montré toutes leurs forces dans le cadre de la répartition des nombres premiers dans les progressions arithmétiques (théorème de Bombieri–Vinogradov). Pour transformer la partie gauche de (1.3), on écrit, grâce à (2.5) et (2.9), les relations

$$(3.1)\qquad \max_a \left| A_{q,b}(y;d,a) - \frac{y}{qd} \right| \leqq \frac{1}{qd} \sum_{j=0}^{d} \sum_{\zeta^q=1,\zeta\neq 1} \left| T_\zeta\left(y, \frac{j}{d}\right)\right| + 1$$

$$= O\left(\frac{1}{qd} \sum_{j=1}^{d-1} \sum_{\zeta^q=1,\zeta\neq 1} \left| T_\zeta\left(y,\frac{j}{d}\right)\right| + \frac{x^{\gamma_q}}{d} + 1 \right),$$

la dernière étant impliquée par (2.7).

Soit 2^N la plus grande puissance de 2 inférieure ou égale à x. Par l'identité (2.8), on a, pour tout $y \leqq x$ et tout α réel, l'inégalité

$$|T_\zeta(y,\alpha)| \leqq \sum_{n\leqq N} |T_\zeta(2^n,\alpha)|,$$

puis, en utilisant (3.1), en faisant un découpage dyadique de l'intervalle $[1,D]$ et un changement de notations, on est ramené à prouver, pour tout D et tout ζ racine q-ème de l'unité différente de 1, la relation

$$(3.2)\qquad \mathscr{X}_\zeta(D) := \sum_{D/2<d\leqq D} \sum_{0<j<d} \left| T_\zeta\left(2^N, \frac{j}{d}\right)\right|$$

$$= O\left((2C_q)^N D^2 + 2^{\gamma_q N} (D^{2(2-\gamma_q+\frac{\log C_q}{\log 2})} + D\log x) \right).$$

Pour faire apparaître les fractions j/d sous forme irréductible, nous écrivons l'égalité:

$$(3.3)\qquad \mathscr{X}_\zeta(D) = \sum_{u\leqq D} \mathscr{X}^*_\zeta(Du^{-1}),$$

avec

$$\mathscr{X}^*_\zeta(z) = \sum_{z/2<d\leqq z} \sum_{\substack{0<j<d\\(j,d)=1}} \left| T_\zeta\left(2^N,\frac{j}{d}\right)\right|.$$

Nous voulons prendre en compte les effets de moyenne sur les fractions $\frac{j}{d}$, autrement dit ramener la somme double étudiée à $\int_0^1 |T_\zeta(2^N,t)|dt$. Pour ce faire, nous appliquons le lemme de Sobolev-Gallagher, célèbre dans le contexte du grand crible ([Mo] Lemma 1.2):

Lemme 1. *Soient T_0, $T \geqq \delta > 0$ des nombres réels, f une fonction de classe $\mathscr{C}^1$ sur l'intervalle $[T_0, T_0+T]$. Soit $\mathscr{I}$ un ensemble de nombres réels de l'intervalle $[T_0+\frac{\delta}{2}, T_0+T-\frac{\delta}{2}]$, vérifiant $|t-t'| \geqq \delta$ pour tous réels t et t' de $\mathscr{I}$. On a alors l'inégalité*

$$\sum_{t\in\mathscr{I}} |f(t)| \leqq \delta^{-1} \int_{T_0}^{T_0+T} |f(x)|dx + \frac{1}{2} \int_{T_0}^{T_0+T} |f'(x)|dx\,.$$

Nous appliquons ce lemme avec $T_0 = 0$, $T = 1$,

$$\mathscr{I} = \{j/d; (j,d) = 1, 1 \leqq j < d, d \leqq Du^{-1}\}\,,$$

donc on peut choisir $\delta = u^2D^{-2}$. Le choix d'appliquer ce lemme avec

$$f(t) = 2^N \prod_{0\leqq n<N} \cos(\pi(2^n t + \xi)) = 2^N F_N(t,\xi)\,,$$

quoique naturel, a l'inconvénient de donner lieu à une dérivée $f'(t)$ d'ordre de grandeur trop élevé. Nous introduisons donc un entier N_1, compris entre 1 et N et nous décomposons $F_N(t,\xi)$ en

$$F_N(t,\xi) = F_{N_1}(t,\xi)\cdot F_{N-N_1}(2^{N_1}t,\xi)$$

ce qui donne, en utilisant (2.6), l'inégalité suivante valable pour tout t réel

$$|T_\zeta(2^N,t)| = O(2^N(\beta(\xi))^{N-N_1}|F_{N_1}(t,\xi)|)\,, \tag{3.4}$$

d'où la relation

$$\sum_{t\in\mathscr{I}} |T_\zeta(2^N,t)| = O\left(2^N\cdot(\beta(\xi))^{N-N_1} \sum_{t\in\mathscr{I}} |F_{N_1}(t,\xi)|\right)\,. \tag{3.5}$$

Par définition de C_q, on a la relation

$$\int_0^1 |F_{N_1}(t,\xi)|dt = O(C_q^{N_1})\,. \tag{3.6}$$

On majore trivialement $F'_{N_1}(t,\xi)$, d'où les relations

$$\begin{aligned} |F'_{N_1}(t,\xi)| &\leqq \sum_{i<N_1} 2^i\pi \prod_{j\neq i;\ j<N_1} |\cos(\pi(2^j t+\xi))| \\ &= O\left(\sum_{i<N_1} 2^i |F_i(t,\xi)|\right)\,, \end{aligned}$$

l'égalité (3.6) appliquée à $F_i(t,\xi)$ donne la relation

$$\int_0^1 |F'_\xi(N_1,t)|dt = O\left(\sum_{i<N_1} 2^i C_q^i\right) = O((2C_q)^{N_1}), \tag{3.7}$$

puisque nous verrons au paragraphe IV.1, que C_q vérifie nécessairement l'inégalité $C_q > 1/2$. On regroupe maintenant (3.4), (3.5), (3.6) et (3.7) dans le Lemme 1 pour écrire la relation

$$\mathscr{X}^*_\zeta(Du^{-1}) = O(2^N \cdot 2^{(\gamma_q-1)(N-N_1)}(D^2u^{-2}C_q^{N_1} + (2C_q)^{N_1})),$$

en ayant remarqué l'inégalité $\beta(\xi) \leqq 2^{\gamma_q-1}$.

On choisit pour N_1 le minimum de N et de la partie entière de $2\log(D/u)/\log 2$; on est donc conduit à la relation

$$\mathscr{X}^*(Du^{-1}) = O\left((2C_q)^N D^2u^{-2} + 2^{\gamma_q N}(D^2u^{-2})^{2-\gamma_q+\frac{\log C_q}{\log 2}}\right);$$

nous sommons par (3.3) sur u, puisque nous ignorons les tailles respectives de C_q et γ_q nous devons envisager les deux éventualités de convergence ou de divergence de la série en u, d'où la relation

$$\mathscr{X}_\zeta(D) = O\left((2C_q)^N D^2 + 2^{\gamma_q N}(D^{2(2-\gamma_q+\frac{\log C_q}{\log 2})} + D\log x)\right),$$

ce qui est exactement la formule (3.2) recherchée et termine la preuve du Théorème 2.

IV Étude asymptotique des intégrales $I_n(\xi)$

1. Premières observations

L'objet de ce paragraphe est d'avoir une première idée sur les constantes C vérifiant (1.2). En fait nous sommes interessés par une évaluation de $\|F_N(\cdot,\xi)\|_1$. La norme $\|F_N(\cdot,\xi)\|_2$ se calcule directement, c'est une conséquence du lemme suivant

Lemme 2. *Soit $n_1,\ldots,n_k$ une famille de k entiers tels que, si les ε_i sont des coefficients valant 0 ou ± 1, on ait l'implication*

$$\sum_{1\leqq i\leqq k} \varepsilon_i n_i = 0 \Rightarrow \varepsilon_i = 0 \ (1 \leqq i \leqq k).$$

Alors pour tout réel ξ, on a l'égalité

$$\int_0^1 \prod_{1\leqq i\leqq k} |\cos(\pi(n_i t + \xi))|^2 dt = 2^{-k}$$

Démonstration. Soit I l'intégrale étudiée. La trigonométrie entraîne

$$I = 2^{-k} \int_0^1 \prod_{1 \leqq i \leqq k} (1 + \cos(2\pi(n_i t + \xi)))\, dt\,,$$

on développe le produit sous l'intégrale, on utilise de façon répétée l'égalité $\cos a \cos b = (\cos(a+b) + \cos(a-b))/2$, pour se ramener à calculer les intégrales

$$\int_0^1 \cos\left(2\pi \cdot \sum_{i \leqq k} \varepsilon_i (n_i t + \xi)\right) dt\,,$$

avec $\varepsilon_i = 0, \pm 1$. Par hypothèse, seule l'intégrale avec tous les ε_i nuls est non nulle et vaut 1, d'où le résultat.

Puisque des puissances de 2 distinctes vérifient trivialement les hypothèses du Lemme 2, on a directement $\|F_N(\cdot, \xi)\|_2 = \left(\sqrt{2}\right)^{-N}$, puis par l'inégalité de Cauchy-Schwarz, l'inégalité $\|F_N(\cdot, \xi)\|_1 \leqq (\sqrt{2})^{-N}$, en d'autres termes on a montré que dans (1.2), on peut, pour tout ξ, choisir $C = \sqrt{2}/2 = 0,7071...$, valeur, qui, comme nous l'avons vu, conduit à un équivalent du Théorème de Bombieri-Vinogradov pour les suites $\mathscr{A}_{q,b}$. L'inégalité

$$\|F_N(\cdot, \xi)\|_1 \geqq \|F_N(\cdot, \xi)\|_2^2 \|F_N(\cdot, \xi)\|_\infty^{-1}$$

et la formule (2.6) entraînent que pour chaque ξ, on a, pour tout C vérifiant (1.2), l'inégalité $C \geqq (2\beta(\xi))^{-1} > 1/2$ pour ξ non entier. En particulier pour $\xi = 1/2$, on a toujours $C \geqq \sqrt{3}/3 = 0,5773...$

2. Un abord direct

Pour améliorer notre connaissance de $I_N(\xi)$, il faut éviter la norme $\|\cdot\|_2$ et profiter des changements de variable $x \longmapsto 2x$ et $x \longmapsto 2x - 1$. On écrit donc

$$\begin{aligned}
(4.1) \qquad I_N(\xi) &= \int_0^1 |\cos(\pi(x+\xi))| \cdot |F_{N-1}(2x, \xi)|\, dx \\
&= \int_0^{\frac{1}{2}} |\cos(\pi(x+\xi))| \cdot |F_{N-1}(2x, \xi)|\, dx \\
&\quad + \int_{\frac{1}{2}}^1 |\cos(\pi(x+\xi))| \cdot |F_{N-1}(2x, \xi)|\, dx \\
&= \int_0^1 \frac{1}{2} \left|\cos\left(\pi\left(\frac{x}{2} + \xi\right)\right)\right| \cdot |F_{N-1}(x, \xi)|\, dx \\
&\quad + \int_0^1 \frac{1}{2} \left|\sin\left(\pi\left(\frac{x}{2} + \xi\right)\right)\right| \cdot |F_{N-1}(x, \xi)|\, dx \\
&= \int_0^1 \varphi_1(x, \xi) \cdot |F_{N-1}(x, \xi)|\, dx\,;
\end{aligned}$$

où l'on a posé $\varphi_1(x, \xi) = \frac{1}{2}(|\cos(\pi(\frac{x}{2} + \xi))| + |\sin(\pi(\frac{x}{2} + \xi))|)$.

Construisons par récurrence la suite de fonctions $\varphi_k(x)$ $(k \geqq 1;\ 0 \leqq x \leqq 1)$, par la formule

$$\varphi_{k+1}(x,\xi) = \frac{1}{2}\left(\left|\cos\left(\pi\left(\frac{x}{2}+\xi\right)\right)\right| \cdot \varphi_k\left(\frac{x}{2},\xi\right) + \left|\sin\left(\pi\left(\frac{x}{2}+\xi\right)\right)\right| \cdot \varphi_k\left(\frac{x+1}{2},\xi\right)\right).$$

Enfin, par une récurrence évidente, la formule (4.1) s'étend en

$$I_N(\xi) = \int_0^1 \varphi_k(x,\xi) \cdot |F_{N-k}(x,\xi)|dx \quad (0 \leqq k \leqq N). \tag{4.2}$$

Posons

$$M_k(\xi) = \max_{0\leqq x\leqq 1} |\varphi_k(x,\xi)|^{\frac{1}{k}},$$

l'égalité (4.2) entraîne la majoration $I_N(\xi) \leqq (M_k(\xi))^k I_{N-k}(\xi)$ et par suite

$$I_N(\xi) = O_k(M_k(\xi)^N), \tag{4.3}$$

ce qui revient à dire que dans (1.2), on peut prendre $C = M_k(\xi)$.

Il reste à donner des valeurs intéressantes de $M_k(\xi)$. Il ne semble pas évident de donner, pour tout k, la valeur de $M_k = \sup_{0\leqq\xi\leqq 1} M_k(\xi)$, mais nous y sommes parvenus pour $k = 2$ en montrant l'égalité

$$M_2 = \left(\frac{\cos \pi/8}{2}\right)^{1/2}, \tag{4.4}$$

qui, par (4.3) conduit directement à la Proposition 1.

3. Preuve de (4.4)

Une récurrence facile conduit à la relation de symétrie

$$\varphi_k(x, 1-\xi) = \varphi_k(1-x,\xi),$$

valable pour tout $0 \leqq x \leqq 1$ et $0 \leqq \xi \leqq 1$, donc dans la définition de M_k, on peut se restreindre à l'intervalle $0 \leqq \xi \leqq 1/2$. Pour contourner la difficulté engendrée par les valeurs absolues dans les formules $\varphi_k(x,\xi)$, nous insérons dans les arguments des fonctions trigonométriques la fonction θ, définie sur $[0,1]$, par $\theta(t) = 0$ si $0 \leqq t < 1-2\xi$ et $\theta(t) = 1/2$ si $1-2\xi \leqq t \leqq 1$. On a donc

$$\begin{aligned}\varphi_1(x,\xi) &= \frac{1}{2}\left(\left|\cos\pi\left(\frac{x}{2}+\xi\right)\right| + \left|\sin\pi\left(\frac{x}{2}+\xi\right)\right|\right)\\ &= \frac{1}{2}\left(\cos\pi\left(\frac{x}{2}+\xi+2\theta(x)\right) + \sin\pi\left(\frac{x}{2}+\xi\right)\right)\\ &= \frac{\sqrt{2}}{2}\cos\pi\left(\frac{x}{2}+\xi-\frac{1}{4}-\theta(x)\right).\end{aligned}$$

(ce qui redonne évidemment l'égalité $M_1 = \sqrt{2}/2$).

De même on peut écrire

$$\varphi_2(x,\xi)=\frac{\sqrt{2}}{4}\left[\cos\pi\left(\frac{x}{4}+\xi-\frac{1}{4}-\theta\left(\frac{x}{2}\right)\right)\ \cos\pi\left(\frac{x}{2}+\xi+2\theta(x)\right)\right.$$
$$\left.+\cos\pi\left(\frac{x}{4}+\xi-\theta\left(\frac{x+1}{2}\right)\right)\ \cos\pi\left(\frac{x}{2}+\xi-\frac{1}{2}\right)\right],$$

soit encore, en utilisant la formule

$$(4.5)\quad \cos a\cos b+\cos c\cos d=\cos\frac{a+b+c+d}{2}\cos\frac{a+b-c-d}{2}$$
$$+\cos\frac{a-b+c-d}{2}\cos\frac{a-b-c+d}{2},$$

on parvient à l'égalité

$$\varphi_2(x,\xi)=\frac{\sqrt{2}}{4}\left[\cos\pi\left(\frac{1}{8}-\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)-\theta\left(\frac{x+1}{2}\right)\right)+\theta(x)\right)\right.$$
$$\times\cos\pi\left(\frac{3x}{4}+2\xi-\frac{3}{8}-\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)+\theta\left(\frac{x+1}{2}\right)\right)+\theta(x)\right)$$
$$+\cos\pi\left(\frac{3}{8}+\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)-\theta\left(\frac{x+1}{2}\right)\right)+\theta(x)\right)$$
$$\left.\times\cos\pi\left(\frac{x}{4}-\frac{1}{8}+\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)+\theta\left(\frac{x+1}{2}\right)\right)+\theta(x)\right)\right].$$

En majorant certains |cos| par 1, on a l'inégalité

$$\varphi_2(x,\xi)\leqq\frac{\sqrt{2}}{4}\left[\left|\cos\pi\left(\frac{1}{8}-\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)-\theta\left(\frac{x+1}{2}\right)\right)+\theta(x)\right)\right|\right.$$
$$\left.+\left|\cos\pi\left(\frac{3}{8}+\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)-\theta\left(\frac{x+1}{2}\right)\right)+\theta(x)\right)\right|\right],$$

maintenant, en utilisant l'égalité $|a|+|b|=\max(|a+b|,|a-b|)$ et la trigonométrie, on parvient à l'inégalité

$$\varphi_2(x,\xi)$$
$$\leqq\frac{\sqrt{2}}{2}\max\left\{\left|\cos\pi\left(\frac{1}{4}+\theta(x)\right)\cos\pi\left(\frac{1}{8}+\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)-\theta\left(\frac{x+1}{2}\right)\right)\right)\right|,\right.$$
$$\left.\left|\sin\pi\left(\frac{1}{4}+\theta(x)\right)\sin\pi\left(\frac{1}{8}+\frac{1}{2}\left(\theta\left(\frac{x}{2}\right)-\theta\left(\frac{x+1}{2}\right)\right)\right)\right|\right\}$$
$$\leqq\frac{1}{2}\cos\frac{\pi}{8},$$

puisque, on a constamment l'égalité

$$\left|\cos\pi\left(\frac{1}{4}+\theta(x)\right)\right| = \left|\sin\pi\left(\frac{1}{4}+\theta(x)\right)\right| = \frac{\sqrt{2}}{2}$$

et

$$\theta\left(\frac{x}{2}\right) - \theta\left(\frac{x+1}{2}\right) \in \left\{-\frac{1}{2};0\right\},$$

(vérification élémentaire, en distinguant la place de ξ par rapport à 1/4). La valeur M_2 est effectivement atteinte par $\varphi_2(\frac{1}{2},\frac{1}{2})$, ceci termine la preuve de (4.4).

V Preuve du Théorème 3

L'objet de ce paragraphe est de donner le développement asymptotique de $I_N(\xi)$ en faisant appel à des techniques plus profondes que celles rencontrées au paragraphe IV.2.

Sur l'espace E des fonctions f lipschitziennes sur $[0,1]$ muni de la norme

$$|||f||| = \sup_{0\leqq x\leqq 1}|f(x)| + \sup_{0\leqq x<y\leqq 1}\left|\frac{f(x)-f(y)}{x-y}\right|,$$

on considère l'opérateur Q_ξ défini par

$$Q_\xi f(x) = 2|\cos\pi(x+\xi)|\ f(2x).$$

On a donc les égalités

$$I_N(\xi) = 2^{-N}\int_0^1 (Q_\xi^N\ 1)\ dx = 2^{-N}\int_0^1 (P_\xi^N\ 1)\ dx,$$

où $P_\xi = Q_\xi^*$ est l'opérateur adjoint de Q_ξ:

$$P_\xi\ f(x) = f\left(\frac{x}{2}\right)\left|\cos\left(\pi\left(\frac{x}{2}+\xi\right)\right)\right| + f\left(\frac{x+1}{2}\right)\left|\cos\left(\pi\left(\frac{x}{2}+\xi+\frac{1}{2}\right)\right)\right|.$$

L'opérateur P_ξ est l'opérateur de transfert associé à la fonction positive $|\cos\pi(x+\xi)|$ (pour cette définition, voir par exemple le paragraphe 3 de [Her2]). La décomposition spectrale de P_ξ sur E est résolue par la série de résultats suivants. Tout d'abord, on rappelle la définition de *quasi-compacité*:

Définition 4. *Soit $(L, |||\cdot|||_L)$ un espace de Banach complexe; un opérateur T borné sur L, de rayon spectral $\rho(T)$, est dit* quasi-compact *s'il existe un nombre réel $r \geqq 0$ et deux sous-espaces F et G supplémentaires dans L, stables par T, tels que*

i) *F est fermé et le rayon spectral de $T_{|F}$ est strictement inférieur à r,*

ii) *$1 \leqq \dim G < +\infty$ et $T_{|G}$ n'a que des valeurs propres de module $\geqq r$.*

Le point crucial est la

Proposition 3 ([Her2]). *Pour ξ non entier, l'opérateur de transfert P_ξ de E est quasi-compact. Il admet*

$$\rho(P_\xi) = \lim_{k \longrightarrow \infty} \|P_\xi^k \ 1\|_\infty^{1/k}$$

comme rayon spectral et unique valeur propre de module $\rho(P_\xi)$ et possède une fonction propre associée ψ strictement positive sur $[0,1]$ avec $\psi(0) = \psi(1)$.

On a la décomposition spectrale suivante de P_ξ:

$$E = \mathrm{Ker}\left(P_\xi - \rho(P_\xi)\mathrm{Id}\right) \oplus F_\xi \,,$$

où F_ξ est un sous-espace de E, stable par P_ξ, tel que le rayon spectral de $P_{\xi|F_\xi}$ soit strictement inférieur à $\rho(P_\xi)$.

Ce résultat obtenu par Hervé (Théorèmes 3.1 et 4.2 de [Her2]) lors de l'étude des fonctions d'échelle dans le cadre de la théorie des ondelettes, résulte de la théorie spectrale des opérateurs de transition, développée par de nombreux auteurs à la suite des travaux de Ionescu Tulcea et Marinescu ([IT-M]).

Pour pouvoir appliquer le théorème 4.2 de [Her2], on vérifie que si $\xi \notin \mathbb{Z}$, il n'existe pas de cycles périodiques invariants pour la fonction $|\cos \pi(x + \xi)|$, c'est-à-dire qu'il n'existe pas de nombre entier $q \geqq 1$, tel que

$$\forall n \in \{1, \ldots, q\}, \ \forall k < 2^n, \cos \pi \left(\frac{k}{2^n - 1} + \xi + \frac{1}{2} \right) = 0 \,.$$

Mais puisque la fonction $\cos \pi t$ n'a qu'un seul zéro sur $[0,1]$, il suffit de vérifier cette condition pour $q = 1$.

Notons que la décomposition spectrale de P_ξ résulte d'un théorème plus général dû à Hennion, qui montre en particulier:

Proposition 4 ([Hen]). *Supposons qu'il existe une norme $\|\cdot\|$ sur L telle que T soit un opérateur compact de $(L, |||\cdot|||_L)$ dans $(L, \|\cdot\|)$* (i.e. *telle que l'image par T de la boule fermée unité soit compacte pour la topologie forte*) *et que, pour chaque nombre entier $n \geqq 1$, il existe des nombres réels positifs R_n et r_n tels qu'on ait*

i) *pour tout f de L, $|||T^n f|||_L \leqq R_n \|f\| + r_n |||f|||_L$,*

ii) $\underline{\lim}\ r_n^{1/n} < \rho(T)$.

Alors, T est quasi-compact et on peut prendre $r = \underline{\lim}\ r_n^{1/n}$ dans la définition précédente.

Cette Proposition s'applique avec $L = E$, $|||\cdot|||_L = |||\cdot|||$ et $\|\cdot\| = \|\cdot\|_\infty$, voir par exemple [Her1] et [Her2].

La stricte positivité de ψ fonction propre résulte de l'étude effectuée par Conze et Raugi ([C-R]) des compacts invariants associés aux transformations $x \longmapsto \frac{x}{2}$ et $x \longmapsto \frac{x+1}{2}$ de $[0,1]$ et de la description des zéros des fonctions propres de l'opérateur P donnée par Hervé ([Her1]). Enfin, le fait que $\rho(P_\xi)$ soit l'unique valeur propre de P_ξ de module $\rho(P_\xi)$ découle de la démonstration du Théorème 4.2 de [Her2]. Ces résultats généralisent l'étude effectuée par

Keane dans le cadre des g-mesures ([Ke]). Signalons, pour terminer, une conséquence directe de la Proposition 3 à savoir que pour tout $0 \leqq x \leqq 1$, la suite $\varphi_{k+1}(x,\xi)/\varphi_k(x,\xi)$ converge vers $\frac{1}{2}\rho(P_\xi)$ (rappelons l'égalité $\varphi_k(\cdot,\xi) = 2^{-k}P_\xi^k\ 1$).

Maintenant, il suffit d'écrire la fonction 1, selon la décomposition spectrale de P_ξ présentée dans la Proposition 3, à savoir $1 = \alpha\psi + f$, avec α constante et f dans F_ξ, pour conclure que pour $N \longrightarrow \infty$, on a

$$I_N(\xi) = 2^{-N} \cdot \alpha \cdot (\rho(P_\xi))^N \int_0^1 \psi(t)\,dt(1 + O(\theta^{-N}))\,,$$

où $\theta > 1$ est le rapport de $\rho(P_\xi)$ sur le rayon spectral de $P_{\xi|F_\xi}$ et $\lambda_\xi = \rho(P_\xi)/2$. Ceci termine la démonstration du Théorème 3.

VI Le cas particulier $\xi = 1/2$

Chacune des fonctions $\varphi_k(x,\frac{1}{2})$ est symétrique par rapport à $x = 1/2$ et nous montrerons, au Lemme 3, qu'elle jouit de l'importante propriété de concavité. On a donc l'égalité

$$M_k\left(\frac{1}{2}\right) = \varphi_k\left(\frac{1}{2},\frac{1}{2}\right),$$

le maximum de cette fonction est donc immobile, ce qui facilite énormément son calcul sur machine. On a le

Lemme 3. *Pour tout k, la fonction $\varphi_k(x,\frac{1}{2})$ est concave sur $[0,1]$. Plus précisément, il existe une suite $(a_k(n))_{0\leqq n<2^{k-1}}$ de réels positifs telle que*

$$\varphi_k\left(x,\frac{1}{2}\right) = \frac{\sqrt{2}}{2^k} \sum_{n<2^{k-1}} a_k(n)\cos\left(\frac{2n+1}{2^k}\pi x - \frac{2n+1}{2^{k+1}}\pi\right).$$

L'énoncé est vrai pour $k = 1$ puisque $\varphi_1(x,\frac{1}{2}) = \frac{\sqrt{2}}{2}\cos(\frac{\pi}{2}x - \frac{\pi}{4})$. Nous nous proposons de montrer, par récurrence les formules plus précises suivantes (qui entraînent aussitôt la positivité des $a_k(n)$, $n < 2^{k-1}$)

$$(6.1)\qquad a_{k+1}(2^{k-1}+i) = a_k(i)\cos\left(\frac{2^k+2i+1}{2^{k+2}}\pi\right) \qquad (i < 2^{k-1})\,,$$

$$(6.2)\qquad a_{k+1}(2^{k-1}-i-1) = a_k(i)\cos\left(\frac{2^k-2i-1}{2^{k+2}}\pi\right) \qquad (i < 2^{k-1})\,.$$

Par linéarité, il nous suffit de transformer, sous la forme recherchée, l'expression suivante (voir la définition de φ_{k+1} en fonction de φ_k)

$$X_k(n) = \cos\left(\frac{2n+1}{2^k}\pi\left(\frac{x}{2}\right) - \frac{2n+1}{2^{k+1}}\pi\right)\sin\frac{\pi x}{2}$$
$$+ \cos\left(\frac{2n+1}{2^k}\pi\left(\frac{x+1}{2}\right) - \frac{2n+1}{2^{k+1}}\pi\right)\cos\left(\frac{\pi x}{2}\right)$$

$$= \cos\left(\frac{2n+1}{2^{k+1}}\pi x - \frac{2n+1}{2^{k+1}}\pi\right)\cos\left(\frac{\pi x}{2} - \frac{\pi}{2}\right)$$

$$+ \cos\left(\frac{2n+1}{2^{k+1}}\pi x\right)\cos\left(\frac{\pi x}{2}\right) .$$

Puis on utilise de nouveau la formule (4.5) avec, pour choix des variables, $a = \frac{2n+1}{2^{k+1}}\pi x - \frac{2n+1}{2^{k+1}}\pi$, $b = \frac{\pi x}{2} - \frac{\pi}{2}$, $c = \frac{2n+1}{2^{k+1}}\pi x$ et $d = \frac{\pi x}{2}$. L'expression étudiée devient alors

$$X_k(n) = \cos\left(\frac{\pi}{4} + \frac{2n+1}{2^{k+2}}\pi\right)\cos\left(\frac{\pi x}{2} + \frac{2n+1}{2^{k+1}}\pi x - \frac{\pi}{4} - \frac{2n+1}{2^{k+2}}\pi\right)$$

$$+ \cos\left(\frac{\pi}{4} - \frac{2n+1}{2^{k+2}}\pi\right)\cos\left(\frac{\pi x}{2} - \frac{2n+1}{2^{k+1}}\pi x - \frac{\pi}{4} + \frac{2n+1}{2^{k+2}}\pi\right) .$$

Il suffit maintenant de regrouper les termes à l'intérieur des fonctions cos, c'est-à-dire écrire $X_k(n)$ sous la forme

$$X_k(n) = \cos\left(\frac{2^k+2n+1}{2^{k+2}}\pi\right)\cos\left(\frac{2^k+2n+1}{2^{k+1}}\pi x - \frac{2^k+2n+1}{2^{k+2}}\pi\right)$$

$$+ \cos\left(\frac{2^k-2n-1}{2^{k+2}}\pi\right)\cos\left(\frac{2^k-2n-1}{2^{k+1}}\pi x - \frac{2^k-2n-1}{2^{k+2}}\pi\right) ,$$

et ainsi retrouver les formules (6.1) et (6.2).

Il reste à calculer des valeurs de $C_k := M_k(\frac{1}{2}) = \varphi_k(\frac{1}{2}, \frac{1}{2})$. Ainsi, trouve-t-on $C_1 = \sqrt{2}/2 = 0,7071\ldots$, $C_2 = \frac{\sqrt{2}}{2}\sqrt{\cos\frac{\pi}{8}} = 0,6796\ldots$, résultats déjà trouvés. Le calcul de C_3 est moins direct et conduit à la valeur

$$C_3 = \frac{\sqrt{2}}{2}\left(\frac{\sin\frac{\pi}{8}\ \cos\frac{3\pi}{16} + \cos\frac{\pi}{8}\cos\frac{\pi}{16}}{\sqrt{2}}\right)^{\frac{1}{3}} = 0,6739\ldots$$

Le calcul devient de plus en plus délicat à la main, puisque à chaque pas, le nombre de valeurs considérées est multiplié par deux. Il faut alors faire appel au programme Mathematica, on parvient aux valeurs approchées : $C_{12} = 0,6644\ldots$, $C_{13} = 0,664199\ldots,\ldots, C_{20} = 0,663197\ldots$ Il est possible d'accéder à quelques autres valeurs des C_k avec un peu plus de soins, mais le calcul sur machine sature très vite. Ceci termine la preuve du Corollaire 3.

Pour minorer $I_N(\frac{1}{2})$, on écrit

$$I_N\left(\frac{1}{2}\right) \geqq \min_{0\leqq x\leqq 1} \varphi_k\left(x, \frac{1}{2}\right) \int_0^1 \left|F_{N-k}\left(x, \frac{1}{2}\right)\right| \, dx ,$$

en posant $c_k = \min_{0\leqq x\leqq 1} |\varphi_k(x, 1/2)|^{\frac{1}{k}}$, on parvient à

$$I_N\left(\frac{1}{2}\right) \geqq c_k^k \int_0^1 \left|F_{N-k}\left(x, \frac{1}{2}\right)\right| \, dx \gg c_k^N .$$

Puisque φ_k est concave et symétrique, on a $c_k = (\varphi_k(0))^{1/k}$. Par la relation de récurrence, on a $\varphi_{k+1}\left(0, \frac{1}{2}\right) = \frac{1}{2}\varphi_k\left(\frac{1}{2}, \frac{1}{2}\right)$, ce qui conduit à

$$c_{k+1} = C_k \frac{1}{(2C_k)^{\frac{1}{k+1}}} .$$

Avec la valeur numérique de C_{20} trouvée précédemment, on déduit la minoration

$$I_N \gg (c_{21})^N = (0,654336\ldots)^N ,$$

ce qui termine la preuve de (1.5).

VII Preuve du Corollaire 4

On note $\mathscr{A}^+(x)$ l'ensemble des entiers de $\mathscr{A}^+$ plus petits que x, de même $\mathbb{N}(x)$ désigne l'ensemble des entiers inférieurs à x. Les performances du crible seront améliorées par l'inégalité évidente suivante

$$|\mathscr{A}^+(x) \cap \mathscr{E}| \leqq |\mathbb{N}(x) \cap \mathscr{E}| . \tag{7.1}$$

valable pour tout ensemble infini $\mathscr{E}$ d'entiers. Si l'ensemble $\mathscr{E}$ est assez régulier et, par sa définition n'a rien à voir avec $\mathscr{A}^+$, on peut penser que le membre de gauche de (7.1) est asymptotiquement égal à la moitié du membre de droite. Maintenant, si $\mathscr{E}$ est, par sa définition, lié à une question générale de crible linéaire, où le phénomène de parité entre en jeu, on sait que, pour majorer la partie gauche de (7.1), on ne pourra pas, par le crible, faire mieux, dans certaines situations, que deux fois la valeur espérée. Autrement dit, on a tout intérêt à recourir à la majoration (7.1).

Pour mettre en place les formules générales du crible, $\mathscr{A}_d^+(x)$ et $\mathbb{N}_d(x)$ désignent l'ensemble des entiers de $\mathscr{A}^+(x)$ et $\mathbb{N}(x)$ divisibles par l'entier positif d. Le plus petit diviseur premier de l'entier d est désigné par $p(d)$ et $S(\mathscr{A}^+(x), z)$ est le cardinal de l'ensemble des éléments de $\mathscr{A}^+(x)$ dont tous les diviseurs premiers sont supérieurs ou égaux à z. Nous travaillons avec le crible de Rosser, comme l'a présenté Iwaniec ([Iw1]). Associées au paramètre D, Iwaniec construit, dans le cadre de la dimension 1, deux suites de coefficients λ_d^+ (valant 0, 1 et -1) et σ_d^+ (valant 0 et 1), tels que nous ayons l'égalité suivante

$$S(\mathscr{A}^+(x), z) = \sum_{d|P(z)} \lambda_d^+ |\mathscr{A}_d^+(x)| - \sum_{d|P(z)} \sigma_d^+ S(\mathscr{A}_d^+(x), p(d)) , \tag{7.2}$$

obtenue par itération de l'identité de Buchstab ([Iw] pages 178 et 179). Nous appliquons la même identité à la suite $\mathbb{N}$; par division par 2 et par soustraction, on a

$$\begin{aligned} S(\mathscr{A}^+(x), z) = \frac{1}{2} S(\mathbb{N}(x), z) &+ \sum_{d|P(z)} \lambda_d^+ \left(|\mathscr{A}_d^+| - \frac{1}{2} |\mathscr{N}_d| \right) \\ &- \sum_{d|P(z)} \sigma_d^+ \left(S(\mathscr{A}_d^+(x), p(d)) - \frac{1}{2} S(\mathbb{N}_d(x), p(d)) \right) . \end{aligned} \tag{7.3}$$

En associant l'égalité évidente

$$|\mathbb{N}_d(x)| = \frac{x}{d} + O(1)\,, \tag{7.4}$$

le Corollaire 3 et le fait que $\lambda_d^+ = 0$ pour $d > D$, on transforme (7.3) en

$$\begin{aligned} S(\mathscr{A}^+(x), z) = \frac{1}{2} S(\mathbb{N}(x), z) \\ - \sum_{d|P(z)} \sigma_d^+ \left(S(\mathscr{A}_d^+(x), p(d)) - \frac{1}{2} S(\mathbb{N}_d(x), p(d)) \right) \\ + O(x(\log x)^{-2})\,. \end{aligned} \tag{7.5}$$

Maintenant, nous insérons la majoration triviale, qui n'est qu'une illustration de (7.1)

$$S(\mathscr{A}_d^+(x), p(d)) \leqq S(\mathbb{N}_d(x), p(d))\,,$$

et (7.5) devient l'inégalité

$$S(\mathscr{A}^+(x), z) \geqq \frac{1}{2} S(\mathbb{N}(x), z) - \frac{1}{2} \sum_{d|P(z)} \sigma_d^+ S(\mathbb{N}_d(x), p(d)) + O(x(\log x)^{-2})\,. \tag{7.6}$$

L'égalité (7.2) écrite avec $\mathscr{A}^+(x)$ remplacé par $\mathbb{N}(x)$ exprime $\sum \sigma_d^+ S(\mathbb{N}_d(x), p(d))$ en fonction des $|\mathbb{N}_d(x)|$; en reportant dans (7.6), on a

$$S(\mathscr{A}^+(x), z) \geqq S(\mathbb{N}(x), z) - \frac{1}{2} \sum_{d|P(z)} \lambda_d^+ |\mathbb{N}_d(x)| - O(x(\log x)^{-2})\,. \tag{7.7}$$

On utilise maintenant (7.4) et la majoration suivante du terme principal de la formule du crible linéaire (voir formule (1.4) de [Iw1]):

$$\sum_{d|P(z)} \frac{\lambda_d^+}{d} \leqq \prod_{p<z} \left(1 - \frac{1}{p}\right) \left\{ F\left(\frac{\log D}{\log z}\right) + O((\log D)^{-1/3}) \right\}\,, \tag{7.8}$$

uniformément pour $2 \leqq z \leqq D$. La fonction $S(\mathbb{N}(x), z)$ a été intensivement étudiée, voir par exemple le chapitre III.6 de [Te]. Cette fonction est notée $\Phi(x, z)$, nous n'aurons besoin que d'une forme très faible du Théorème 3, page 445 de [Te], à savoir

$$S(\mathbb{N}(x), z) \sim \frac{x\omega(\log x/\log z)}{\log z}\,, \tag{7.9}$$

avec ω fonction de Buchstab. Cette fonction définie par une équation différentielle aux différences, vérifie entre autres, l'égalité

$$\omega(u) = \frac{F(u) + f(u)}{2e^{\gamma}} \quad (u \geqq 1)\,.$$

Il reste à insérer dans (7.7), les relations (7.8) et (7.9), à utiliser la formule de Mertens, pour conclure la preuve du Corollaire 4.

VIII Preuve du Corollaire 5

Comme dans l'article de Iwaniec et Pomykala ([I–P]), soit $K/\mathbb{Q}$ une extension abélienne de degré k valant 2, 3 ou 4, dont le conducteur est noté Δ. Il existe un sous-groupe $\mathscr{H}$ d'indice k de $(\mathbb{Z}/\Delta\mathbb{Z})^*$, ayant la propriété suivante

Soit a un entier premier avec Δ. Alors, on a l'équivalence
a est la norme d'un idéal de $K/\mathbb{Q} \Longleftrightarrow \{p|a \Longrightarrow p(\mathrm{mod}\,\Delta) \in \mathscr{H}\}$.
Notons maintenant

$$\mathscr{X} = \{a \in \mathscr{A}^+;\ a \leqq x,\ a \equiv 1(\mathrm{mod}\,\Delta)\}\,,$$
$$\mathscr{Y} = \{a \in \mathbb{N}^*;\ a \leqq x,\ a \equiv 1(\mathrm{mod}\,\Delta)\}\,,$$
$$\mathscr{P} = \{p;\ p \nmid \Delta,\ p \notin \mathscr{H}(\mathrm{mod}\,\Delta\}\,,$$
$$P(z) = \prod_{p<z,\, p\in\mathscr{P}} p\,,$$

et

$$S(\mathscr{X};\mathscr{P},z) = |\{a \in \mathscr{X},\ p|a \text{ et } p \in \mathscr{P} \Longrightarrow p \geqq z\}|\,.$$

Puisqu'un élément de $\mathscr{X}$ ne peut pas posséder exactement un diviseur premier, compté avec multiplicité, dans $\mathscr{P}$, on voit, grâce à la propriété précédente de $\mathscr{H}$, que $S(\mathscr{X};\mathscr{P},z)$, pour $z = x^{1/2} + 1$, minore le cardinal étudié dans l'énoncé du Corollaire 5.

L'étude de $S(\mathscr{X};\mathscr{P},z)$ est un problème de crible de dimension $\kappa = 1 - 1/k$ et se mène, comme au paragraphe VII, en criblant en parallèle $\mathscr{X}$ et $\mathscr{Y}$. La formule (7.2) se transforme en

$$S(\mathscr{X};\mathscr{P},z) = \sum_{d|P(z)} \lambda_d^+ |\mathscr{X}_d| - \sum_{d|P(z)} \sigma_d^+ S(\mathscr{X}_d;\mathscr{P},p(d))\,,$$

les coefficients λ_d^+ et σ_d^+ étant alors relatifs à la dimension κ.

Nous travaillons avec les formules d'approximation

$$|\mathscr{X}_d| = \frac{x}{2d\Delta} + \left(A^+(x;d\Delta,a_d) - \frac{x}{2d\Delta}\right)\,, \tag{8.1}$$
$$|\mathscr{Y}_d| = \frac{x}{d\Delta} + O(1)\,,$$

pour $d|P(z)$ et a_d étant défini par les congruences $a_d \equiv 1(\mathrm{mod}\,\Delta)$ et $a_d \equiv 0(\mathrm{mod}\,d)$.

On suit la même démarche qu'au paragraphe VII, on arrive donc à l'analogue de (7.7) à savoir

$$S(\mathscr{X};\mathscr{P},z) \geqq S(\mathscr{Y};\mathscr{P},z) - \frac{1}{2}\sum_{d|P(z)} \lambda_d^+ |\mathscr{Y}_d| - O(x(\log x)^{-2})\,, \tag{8.2}$$

le terme d'erreur venant de l'application du Corollaire 3.

Pour évaluer le premier terme à gauche de (8.2), nous remarquons, toujours pour $z = x^{1/2} + 1$, qu'on a l'égalité

$$S(\mathscr{Y};\mathscr{P},z) = |\{n \leqq x;\ n \equiv 1(\mathrm{mod}\,\Delta), p|n \Longrightarrow p \in \mathscr{H}\}|\,,$$

dont nous connaissons un équivalent grâce à la formule (26) de [I-P]:

(8.3)
$$S(\mathscr{Y};\mathscr{P},z) \sim \frac{k}{\varphi(\Delta)}\Gamma^{-1}\left(\frac{1}{k}\right)\left(\prod_{p\in\mathscr{H}}\left(1-\frac{1}{p}\right)^{-1}\cdot\prod_{p}\left(1-\frac{1}{p}\right)^{\frac{1}{k}}\right)\cdot x(\log x)^{-\kappa},$$

le produit des deux produits infinis étant naturellement interprété comme étant convergent.

En utilisant le Théorème 1 de [Iw1], déjà évoqué auparavant, on a la majoration

$$(8.4)\quad \sum_{d|P(z)}\frac{\lambda_d^+}{d} \leqq \prod_{\substack{p<z,\,(p,\Delta)=1\\ p\notin\mathscr{H}(\mathrm{mod}\,\Delta)}}\left(1-\frac{1}{p}\right)\left(F_\kappa\left(\frac{\log D}{\log z}\right)+O\left((\log D)^{-1/3}\right)\right);$$

avec D ayant la valeur du Corollaire 3. Sur l'intervalle considéré, la fonction de crible F_κ a pour expression

$$F_\kappa(s)=\frac{A_\kappa}{s^\kappa},$$

avec A_κ est une constante absolue, dont certaines valeurs sont tabulées dans ([Iw1], page 176).

Quant au produit eulérien apparaissant dans (8.4), on le transforme en

$$W(z)=\frac{\Delta}{\varphi(\Delta)}\prod_{p<z}\left(1-\frac{1}{p}\right)^{\kappa}\left(\prod_{p<z,\,p\in\mathscr{H}}\left(1-\frac{1}{p}\right)^{-1}\cdot\prod_{p<z}\left(1-\frac{1}{p}\right)^{\frac{1}{k}}\right),$$

d'où l'équivalence asymptotique, conséquence de la formule de Mertens

$$(8.5)\qquad W(z)\sim\frac{\Delta}{\varphi(\Delta)}\cdot\frac{\mathrm{e}^{-\gamma\kappa}}{(\log z)^\kappa}\left(\prod_{p\in\mathscr{H}}\left(1-\frac{1}{p}\right)^{-1}\cdot\prod_{p}\left(1-\frac{1}{p}\right)^{\frac{1}{k}}\right).$$

En regroupant (8.1), (8.2), (8.3), (8.4) et (8.5), on voit, que pour obtenir la minoration

$$S(\mathscr{X};\mathscr{P},z)\gg x(\log x)^{-\kappa},$$

il suffit de vérifier l'inégalité

$$(8.6)\qquad k\Gamma^{-1}\left(\frac{1}{k}\right)-\frac{1}{2}\cdot A_\kappa\cdot\mathrm{e}^{-\gamma\kappa}\cdot\left(\frac{\log x}{\log D}\right)^{\kappa}>0\cdot$$

Pour $k=2$, il n'est pas nécessaire de faire appel à tout ce qui précède. En effet, on voit que, dans le cas présent, on a $\log D/\log z = 1,1848\ldots > 1$, et 1 est la *sieving limit* du crible de dimension 1/2. Autrement dit, puisque la fonction $f_{1/2}(s)$ est positive pour $s>1$, on a directement la minoration recherchée en appliquant la formule de minoration du crible à la fonction $S(\mathscr{X};\mathscr{P},z)$. Signalons que si nous choisissons $K=\mathbb{Q}(i)$, nous obtenons, avec le bon ordre de grandeur, une minoration du cardinal

$$|\{n\leqq x; s(n)\text{ pair},\ n=a^2+b^2\}|.$$

Dans le cas des extensions cubiques, le raisonnement précédent ne s'avère pas suffisant, puisque la fonction $f_{2/3}(s)$ est positive pour $s > \beta_{2/3} = 1,2242$ alors que nous sommes au point $s = 1,1848$. On en est réduit à vérifier (8.6), ce qui se fait sans peine lorsqu'on sait que $A_{2/3} = 1,9134\ldots$, $\gamma = 0,5772\ldots$, $\Gamma(1/3) = 2,6789\ldots$ Le membre de gauche de (8.6) vaut au moins 0,196 et l'inégalité recherchée est vérifiée.

Enfin, dans le cas où $k = 4$, on utilise les valeurs $A_{3/4} = 2,2020\ldots$, $\Gamma(1/4) = 3,6256\ldots$, le membre de gauche de (8.6) vaut au moins 0,045, ce qui termine la preuve du Corollaire 5.

Bibliographie

[A-MF] Allouche, J.-P., Mendès France, M.: On an extremal property of the Rudin-Shapiro sequence. Mathematika **32** (1985), 33–38

[B-R] Balog, A., Ruzsa, I.: On an additive property of stable sets. Proceedings of the Conference in honour of C. Hooley (Cardiff 1995) (à paraître)

[C-R] Conze, J.-P., Raugi, A.: Fonctions harmoniques pour un opérateur de transition et applications. Bull. Soc. Math. France **118** (1990), 273–310

[Co] Coquet, J.: A summation formula related to the binary digits. Invent. Math. **73** (1983), 107–115

[Fi] Fine, N.J.: The distribution of the sum of digits (mod p). Bull. Amer. Math. Soc. **71** (1965), 651–652

[Fo] Fouvry, E.: Théorème de Brun-Titchmarsh; application au théorème de Fermat. Invent. Math. **79** (1985), 383–407

[Ge] Gelfond, A.O.: Sur les nombres qui ont des propriétés additives et multiplicatives données, Acta Arith. **13** (1968), 259–265

[Ha] Harman, G.: The distribution of αp modulo one. J. London Math. Soc. (2) **27** (1983), 9–18

[H-R] Halberstam, H., Richert, H.E.: Sieve Methods. Academic Press, New York 1974

[Hen] Hennion, H.: Sur un théorème spectral et son application aux noyaux lipschitziens. Proc. of the A.M.S. **118**(2) (1993), 627–634

[Her1] Hervé, L.: Étude d'opérateurs quasi-compacts positifs. Applications aux générateurs de transfert. Ann. Inst. Henri Poincaré **30**(3) (1994), 437–466

[Her2] Hervé, L.: Construction et régularité des fonctions d'échelle. SIAM J. Anal. Math. **26** (1995), 1361–1385

[Hi] Hildebrand, A.: On a conjecture of Balog. Proc. of the A.M.S. **95** (1985), 517–523

[Ho] Hooley, C.: On the Barban–Davenport–Halberstam Theorem. III, J. London Math. Soc. (2) **10** (1975), 249–256

[IT-M] Ionescu-Tulcea, C.T., Marinescu, G.: Théorie ergodique pour une classe d'opérations non complètement continues. Annals Math. **52** (1950), 140–147

[I-J] Iwaniec, H., Jutila, M.: Primes in short intervals. Arkiv Math. **17** (1979), 167–176

[I-P] Iwaniec, H, Pomykala, J.: Sums and differences of quartic norms. Mathematika **40** (1993), 233–245

[Iw1] Iwaniec, H.: Rosser's Sieve. Acta Arith. **36** (1980), 171–202

[Iw2] Iwaniec, H.: On sums of two norms of cubic fields. Journées de Théorie additive des nombres (1977) Bordeaux, 71–89

[Ke] Keane, M.: Strongly Mixing g-Measures. Invent. Math. **16** (1972), 309–324

[Mo] Montgomery, H.L.: Topics in Multiplicative Number Theory, Lecture Notes in Mathematics **227**, Springer, Berlin 1971

[Ne] Newman, D.J.: On the number of binary digits in a multiple of three. Proceedings of the A.M.S. **21** (1969), 719–721

[Ru] Rudin, W.: Some Theorems on Fourier Coefficients. Proceedings of the A.M.S. **10** (1959), 855–859

[Sh] Shapiro, H.S.: Extremal Problems for Polynomials and Power Series, Doctoral Thesis, M.I.T. (1951)

[Te] Tenenbaum, G.: Introduction à la théorie analytique et probabiliste des nombres. Cours Spécialisés 1 Société Mathématique de France (1995)