SÉMINAIRE N. BOURBAKI

JEAN-MARC DESHOUILLERS

Progrès récents des petits cribles arithmétiques

Séminaire N. Bourbaki, 1979, exp. n° 520, p. 248-262

<http://www.numdam.org/item?id=SB_1977-1978__20__248_0>

Séminaire BOURBAKI 520-01
30e année, 1977/78, n° 520 Juin 1978

PROGRÈS RÉCENTS DES PETITS CRIBLES ARITHMÉTIQUES
[d'après CHEN, IWANIEC,...]

par Jean-Marc DESHOUILLERS

Pour un arithméticien, le terme cible évoque :

- soit la famille des méthodes (cribles arithmétiques) mises en oeuvre pour évaluer le nombre d'éléments qui subsistent dans un ensemble fini après qu'on lui ait retiré certains sous-ensembles réguliers (e.g. des progressions arithmétiques dans le cas d'un ensemble d'entiers),
- soit une famille de méthodes (crible analytique) utilisées en théorie analytique dans l'étude des séries de Dirichlet, qui conduisent à des résultats concernant la valeur moyenne des fonctions L ou la répartition des zéros de ces fonctions.

En regardant ces questions d'un peu plus près, on constate que la dichotomie précédente ne tient pas compte du développement historique de ces méthodes (ou, ce qui revient au même, des principes de base mis en jeu) ; cet aspect conduit à distinguer :

- les cribles arithmétiques adaptés au cas où les sous-ensembles soustraits à l'ensemble de départ sont "petits" : ce sont les petits cribles arithmétiques, sujet de l'exposé,
- le grand crible qui présente les deux facettes de crible arithmétique et analytique ; (nous recommandons la lecture de l'ouvrage de Richert [1976] pour une introduction à ce sujet et une vue d'ensemble).

Les cribles arithmétiques étant relativement peu connus en France, nous avons commencé cet exposé par un rappel des principes fondamentaux et de quelques résultats obtenus avant la fin des années mille neuf cent soixante ; (signalons ici l'excellente bible de Halberstam et Richert [1974]). La seconde partie de l'exposé a dû être amputée d'autant : nous nous sommes limité au crible de dimension 1 , délaissant à contrecoeur le travail d'Iwaniec [1976] sur le crible de dimension 1/2 (où il donne une démonstration élémentaire de la formule asymptotique du nombre de sommes de deux carrés dans l'intervalle $[1,x]$), les travaux récents consacrés au théorème de Brun-Titchmarsh...

1. Exemples ; formulation du crible

1.1. On s'intéresse ici à la question suivante (problème de crible) :

Evaluer le nombre $\mathcal{S}(\mathcal{A},\mathcal{P})$ d'éléments d'une collection finie $\mathcal{A}$ d'entiers relatifs non nécessairement distincts qui ne sont divisibles par aucun élément d'une famille finie $\mathcal{P}$ de nombres premiers.

1.2. Quelques exemples de tels problèmes (la lettre N désignera un entier supérieur à 2 et la lettre p un nombre premier).

1) Problème de Goldbach :

$$\mathcal{A} = \{2N - p \mid p < 2N\} \ , \quad \mathcal{P} = \{p \mid p \leq (2N)^{1/2}\}$$

2) Nombres premiers jumeaux :

a) $\mathcal{A} = \{p + 2 \mid p \leq N - 2\}$, $\mathcal{P} = \{p \mid p \leq N^{1/2}\}$

b) $\mathcal{A} = \{n(n+2) \mid n \leq N - 2\}$, $\mathcal{P} = \{p \mid p \leq N^{1/2}\}$

3) Nombres premiers dans un intervalle :

$$\mathcal{A} = \{n \mid N - M \leq n \leq N\} \quad \text{avec} \quad M < N - N^{1/2}$$

$$\mathcal{P} = \{p \mid p \leq N^{1/2}\}$$

4) Nombres premiers de la forme $n^2 + 1$:

$$\mathcal{A} = \{n^2 + 1 \mid n \leq N\} \ , \quad \mathcal{P} = \{p \mid p \leq N\}$$

5) Nombres au plus égaux à N qui sont résidus quadratiques modulo les nombres premiers au plus égaux à $N^{1/2}$:

$$\mathcal{P} = \{p \mid p \leq N^{1/2}\} \ , \quad \mathcal{A} = \{ \prod_{p \in \mathcal{P},\ (\frac{\nu}{p}) = -1} p \mid 1 \leq \nu \leq N\} \ .$$

1.3. Formulation du crible

Pour évaluer $\mathcal{S}(\mathcal{A},\mathcal{P})$, on commence par l'écrire sous la forme :

$$\mathcal{S}(\mathcal{A},\mathcal{P}) = \sum_{a \in \mathcal{A}} s^{o}(a) \ , \qquad \text{où} \quad s^{o}(a) = \begin{cases} 1 & \text{si } p \mid a \Rightarrow p \notin \mathcal{P} \\ 0 & \text{sinon} \ , \end{cases}$$

les propriétés élémentaires de la fonction de Möbius permettent d'écrire :

$$s^{o}(a) = \sum_{d \mid (a,P)} \mu(d) \ ,$$

où P désigne le produit des éléments de $\mathcal{P}$; en intervertissant les sommations, on obtient la relation

$$\mathcal{S}(\mathcal{A},\mathcal{P}) = \sum_{d \mid P} \mu(d) \ \mathrm{Card}\{a \in \mathcal{A} \mid a \equiv 0 \ [d]\} \ , \tag{1.1}$$

à ce stade, il convient d'introduire une hypothèse relative à la forme du cardinal

de l'ensemble $\mathcal{A}_d$ constitué par les éléments de $\mathcal{A}$ congrus à 0 modulo d ; les exemples du paragraphe 1.2 conduisent à supposer l'existence d'une relation de la forme :

$$\text{Card } \mathcal{A}_d = \frac{\omega(d)}{d} X + r(\mathcal{A},d)$$

où ω est une fonction multiplicative, X une approximation du cardinal de $\mathcal{A}$, le terme $r(\mathcal{A},d)$ devant être de la nature d'un terme d'erreur. La relation (1.1) s'écrit alors

$$(1.2) \qquad \mathcal{S}(\mathcal{A},\mathcal{P}) = X \prod_{p \in \mathcal{P}} (1 - \frac{\omega(p)}{p})) + \sum_{d \mid P} \mu(d)\, r(\mathcal{A},d) \ .$$

Remarquons que la formule (1.2), connue sous le nom de crible d'Eratosthene-Legendre, est de peu d'intérêt lorsque $\mathcal{P}$ n'est pas très petit, non seulement parce que le terme $\sum_{d \mid P} \mu(d)\, r(\mathcal{A},d)$ est malaisé à majorer, mais encore parce qu'il n'est pas toujours un terme d'erreur : si l'on considère le problème 3) avec $M := N^{1/2}$, le théorème des nombres premiers implique que chacun des trois termes de la relation (1.2) est du même ordre de grandeur !

Remarquons également que, dans les exemples 1) à 4) la fonction $\omega(p)$ est bornée, alors que dans l'exemple 5) la fonction $\omega(p)$ vaut $\frac{p-1}{2}$ (pour p impair dans $\mathcal{P}$) et n'est pas bornée, même en moyenne ; c'est sur ce point que l'on distingue un petit crible d'un grand ; plus précisément, on dit que le problème de crible $(\mathcal{A},\mathcal{P})$ est de dimension $\varkappa$ si le produit

$$\prod_{w \le p < z < \max \mathcal{P}} (1 - \frac{\omega(p)}{p})^{-1} \qquad \text{est équivalent à} \qquad \left(\frac{\text{Log } z}{\text{Log } w}\right)^{\varkappa} .$$

Ainsi, les exemples 1), 2 a), 3) et 4) sont de dimension 1, l'exemple 2 b) étant de dimension 2. Nous nous limiterons désormais aux cribles de dimension finie, et, pour les énoncés techniques, aux cribles linéaires, c'est-à-dire de dimension 1.

2. Les petits cribles jusqu'en 1970

2.1. Puisque la relation (1.2) peut ne pas conduire à une formule asymptotique, nous allons nous borner à chercher une majoration (resp. minoration) de la quantité $\mathcal{S}(\mathcal{A},\mathcal{P})$, notée désormais $\mathcal{S}(\mathcal{A})$; il suffit pour cela de construire une fonction s^+ (resp. s^-) qui majore (resp. minore) s^o . On connaît deux façons d'effectuer cela :

1) Chercher la fonction s de la forme

$$s(a) = \sum_{\substack{d \mid (a,P) \\ d \in \Delta}} \mu(d) \ ,$$

où Δ est une partie des diviseurs de P construite de manière combinatoire telle que :

(i) la fonction s majore (resp. minore) s^o ;

(ii) Δ ne soit pas trop gros, afin que la quantité $\sum_{\substack{d \mid P \\ d \in \Delta}} |r(\mathcal{A},d)|$ soit un terme d'erreur.

Cet abord combinatoire du problème a été développé en premier par Brun (vers 1920), puis raffiné par Rosser (vers 1950) ; le travail de Rosser n'a pas été publié et semblait alors donner des résultats surpassés par ceux de Selberg [1947] qui pose ainsi le problème :

2) Chercher la fonction s de la forme

$$s(a) = \sum_{\substack{d \mid (a,P) \\ d \leq z}} \lambda(d)$$

où la fonction λ et le nombre réel z sont tels que

(i) la somme s majore (resp. minore) s^o ;

(ii) le nombre z est suffisamment petit pour que la quantité

$\sum_{\substack{d \mid (a,P) \\ d \leq z}} |\lambda(d)\, r(\mathcal{A},d)|$ soit un terme d'erreur.

Il est relativement facile de construire une fonction s^+ : soit, en effet, Λ_d une famille de nombres réels tels que $\Lambda_1 = 1$ et $\Lambda_d = 0$ pour $d \nmid P$ ou $d > z^{1/2}$; la fonction

$$a \longmapsto \Big(\sum_{d \mid a} \Lambda_d\Big)^2 = \sum_{\substack{d \mid (a,P) \\ d \leq z}} \Big(\sum_{\substack{d_1, d_2 \\ [d_1,d_2] = d}} \Lambda_{d_1} \Lambda_{d_2} \Big)$$

est bien une fonction s^+, car elle vaut 1 quand s^o vaut 1 et elle est positive quand s^o vaut 0 ; il suffit alors de choisir les nombres réels (indépendants) Λ_d pour minimiser le terme principal de la majoration de $\mathcal{S}(\mathcal{A},\mathcal{P})$.

L'obtention de fonctions s^- est plus délicate et nous renvoyons le lecteur au chapitre IV de l'ouvrage de Halberstam et Roth [1966] pour ce point, ainsi que pour une introduction aux cribles de Brun et Selberg.

2.2. Appliqués aux exemples 1) à 4), les cribles que nous venons de présenter ne conduisent à aucun résultat (les termes d'erreur surpassant les termes "principaux"), et on doit donc se limiter à évaluer les quantités $\mathcal{S}(\mathcal{A},z)$ représentant le nombre des éléments de $\mathcal{A}$ qui ne sont divisibles par aucun élément de $\mathcal{P}$ inférieur à z. Pour ce qui est des majorations, cela est peu important : $\mathcal{S}(\mathcal{A},z)$ est en effet un majorant de $\mathcal{S}(\mathcal{A})$ et l'on arrive ainsi à des majorations satisfaisantes

(de l'ordre de grandeur de la valeur conjecturée). En ce qui concerne les minorations, mentionnons, à titre d'exemple, que Brun [1920] a obtenu une borne inférieure non triviale pour $\mathcal{S}(\mathcal{A},(N+1)^{1/10})$ dans le problème 2 b), ce qui implique l'existence d'une infinité d'entiers n tels que n et $(n+2)$ aient chacun au plus 9 facteurs premiers, ce que nous noterons :

$$P_9 + 2 = P_9 \quad \text{a une infinité de solutions .}$$

2.3. Bukhštab a remarqué que l'utilisation de la relation

$$(2.1) \qquad \mathcal{S}(\mathcal{A},z) = \mathcal{S}(\mathcal{A},z_1) - \sum_{\substack{z_1 \le p < z \\ p \in \mathcal{P}}} \mathcal{S}(\mathcal{A}_p, p)$$

permettait d'améliorer les estimations obtenues par le crible de Brun (ou celui de Selberg).

Dans le cas du crible linéaire, Jurkat et Richert [1965], utilisant de manière récurrente la relation (2.1), ont obtenu le résultat suivant :

Théorème 1.- Sous les conditions

$$0 \le \omega(p)/p \le B_1 < 1 ,$$

$$-L \le \sum_{w \le p < z} \frac{\omega(p) \operatorname{Log} P}{P} - \operatorname{Log} \frac{z}{w} \le B_2 \quad \text{pour} \quad 2 \le w \le z \le \max \mathcal{P} ,$$

pour tous nombres réels $\xi \ge z \ge 2$, on a

$$S(\mathcal{A},z) \le X V(z) \left\{ F\left(\frac{\operatorname{Log} \xi^2}{\operatorname{Log} z} \right) + \frac{cL}{(\operatorname{Log} \xi)^{1/14}} \right\} + R$$

$$S(\mathcal{A},z) \ge X V(z) \left\{ f\left(\frac{\operatorname{Log} \xi^2}{\operatorname{Log} z} \right) - \frac{cL}{(\operatorname{Log} \xi)^{1/14}} \right\} - R ,$$

où $R = \sum_{n < \xi^2 , n \mid P(z)} 3^{\nu(n)} |r(\mathcal{A},n)|$, $V(z) = \prod_{p \mid P(z)} \left(1 - \frac{\omega(p)}{p}\right)$,

$$P(z) = \prod_{p \in \mathcal{P}, p < z} p ,$$

et, où les fonctions F et f sont déterminées par :

$$uF(u) = 2e^{\gamma} , \qquad uf(u) = 0 \qquad \text{pour} \quad 0 < u \le 2$$

$$(uF(u))' = f(u-1) , \qquad (uf(u))' = F(u-1) \qquad \text{pour} \quad u \ge 2 .$$

Notons que Selberg a démontré (par un exemple) que ce résultat est le meilleur possible, en ce qui concerne les fonctions F et f pour $u \le 2$ et que Jurkat et Richert ont levé cette dernière restriction.

2.4. Il est instructif de revenir sur le pénultième paragraphe : à défaut de pou-

voir minorer $\mathcal{S}(\mathcal{A},(N+1)^{1/2})$, on minore $\mathcal{S}(\mathcal{A},(N+1)^{1/10})$ et on en déduit que l'équation $P_9 + 2 = P_9$ a une infinité de solutions ; mais, si l'on s'intéresse à l'équation $P_r + 2 = P_r$, on peut remarquer, avec Kuhn [1941], qu'il n'est pas nécessaire de minorer $\mathcal{S}(\mathcal{A},(N+1)^{1/(r+1)})$: une minoration (non triviale) de la quantité

$$\sum_{\substack{a \in \mathcal{A} \\ (a,\, P((N+1)^u)) = 1}} \Big\{ 1 - \frac{1}{t+1} \sum_{\substack{p \mid a \\ N^u \le p < N^{(1-u)/(s+1)}}} 1 \Big\} =$$

(2.2)

$$= \mathcal{S}(\mathcal{A},(N+1)^u) - \frac{1}{t+1} \sum_{N^u \le p < N^{(1-u)/(s+1)}} \mathcal{S}(\mathcal{A}_p,(N+1)^u) ,$$

avec $t + s = r$ conduit aussi bien au résultat (en effet, un élément de $\mathcal{A}$ auquel est attaché un poids positif a : 0 facteur premier inférieur à N^u , au plus t entre N^u et $N^{(1-u)/(s+1)}$ et au plus s supérieurs à $N^{(1-u)/(s+1)}$) ; la seconde écriture ramène la minoration souhaitée, à la minoration de $\mathcal{S}(\mathcal{A},(N+1)^u)$ et à la majoration de $\mathcal{S}(\mathcal{A}_p,(N+1)^u)$, c'est-à-dire à une minoration où la précision est meilleure et à des majorations plus précises également, d'où résulte un gain global.

Par la suite, d'autres systèmes de poids que celui de Kuhn ont été introduits : citons ceux de Bukhštab [1967], optimisés (pour le crible linéaire dans le cas où le plus grand élément de $\mathcal{A}$ est de l'ordre de X) par une procédure de programmation linéaire, et les poids logarithmiques de Richert [1969] (qui étendent ceux d'Ankeny et Onishi), proportionnels à $(1 - \theta \frac{\text{Log } P}{\text{Log } X})$.

2.5. Résultats obtenus vers la fin des années 1960

On rappelle que l'on note P_k un entier ayant au plus k facteurs premiers (comptés avec multiplicité).

1) L'attaque de ce problème repose sur la connaissance de la répartition des nombres premiers dans les progressions arithmétiques, résultats généralement obtenus par le biais du grand crible ; Rényi [1947] a démontré l'existence d'un entier k tel que

$2N = P_1 + P_k$ est résoluble pour N assez grand.

Bukhštab [1967] a donné la valeur 3 comme valeur admissible pour k (outre son système de poids, sa démonstration utilise le théorème de Bombieri).

2) a) Le problème est tout-à-fait semblable au problème 1) ; Bukhštab [1967] a prouvé que

$P_1 + 2 = P_3$ a une infinité de solutions.

b) Le meilleur résultat est celui de Selberg :

$P_k + 2 = P_\ell$ a une infinité de solutions avec $k + \ell \leq 5$;

ce résultat est, bien entendu, inférieur au résultat obtenu par la formulation 2 a), mais il a le mérite d'être effectif.

3) (i) Rappelons pour mémoire que Huxley [1972] a démontré que pour N assez grand, il existe un nombre premier dans l'intervalle $[N - N^{7/12+\varepsilon}, N]$.

(ii) Dès que N est assez grand, il existe un P_2 dans l'intervalle $[N - N^{6/11}, N]$ (Richert [1969]).

2.6. Le théorème de Chen sur le problème de Goldbach

Chen a annoncé en 1966 et publié en 1973 une démonstration de l'infinité des solutions des équations

$$2N = P_1 + P_2 \qquad \text{et} \qquad P_1 + 2 = P_2 .$$

Il commence par obtenir (pour le second problème, le premier étant similaire) une minoration du nombre de P_3 de la forme $P_1 + 2$; en utilisant les poids de Kuhn il minore :

$$W := \sum_{\substack{p \leq N \\ (p+2,\, P(N^{1/10})) = 1}} \Big(1 - \frac{1}{2} \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \mid p+2}} 1\Big)$$

Son idée consiste alors à majorer la contribution des P_3 , c'est-à-dire la quantité :

$$U := \frac{1}{2} \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \mid p+2}} \; \sum_{\substack{N^{1/3} \leq p_2 < (N/p_1)^{1/2} \\ p_2 \mid p+2,\; p+2 = p_1 p_2 p_3}} 1$$

qui se réécrit

$$U = \frac{1}{2} \sum_{q \in \mathcal{Q}} \mathrm{Card}\{p' \mid p' < N/q \,,\; qp' - 2 = p\}$$

avec $\mathcal{Q} := \{p_1 p_2 : N^{1/10} \leq p_1 < N^{1/3} \leq p_2 < (N/p_1)^{1/2}\}$,

chaque terme de la somme sur $\mathcal{Q}$ peut être majoré par la méthode de Selberg : si l'on applique directement le Théorème 1, on obtient pour U une majoration supérieure à la minoration obtenue pour W ...

Chen reprend alors la méthode de Selberg, majorant

$$U \leq \frac{1}{2} \sum_{q \in \mathcal{Q}} \; \sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{p < N/q \\ qp \equiv 2 \;[D]}} 1 \,,$$

où $D = [d_1, d_2]$, $P(z) = \prod_{2 < p < z} p$ et où les paramètres λ_d sont choisis selon la procédure de Selberg et sont indépendants de q ; intervertissant les sommations, on a

$$U \leq \frac{1}{2} \sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{n < N \\ n \equiv 2 \ [D]}} b(n) \qquad \text{avec} \quad b(n) = \sum_{\substack{pq = n \\ p \in \mathcal{Q}}} 1 \ ,$$

le problème est alors justiciable des techniques analytiques, via la majoration de $\sum_D \Big| \sum_{\substack{n < N \\ n \equiv 2 \ [D]}} b(n) - \frac{1}{\varphi(D)} \sum_{n < N} b(n) \Big|$. Pour une démonstration complète, on pourra consulter Halberstam [1974].

3. Progrès récents des petits cribles

3.1. La contribution de Chen au problème 3)

L'idée fondamentale de l'article de Chen [1975] relatif au problème 3) (et qui rappelle un argument de Chen [1973]) consiste à majorer globalement la somme $\sum_p \mathcal{S}(\mathcal{A}_p, z)$ qui apparaît dans la version pondérée du crible (cf. la relation (2.2)) ; avec $M = N^{1/2}$, il obtient un certain nombre de lemmes du type suivant :

Soient $\mathcal{A}$: $= [N - N^{1/2}, N]$, $\varepsilon > 0$; pour $\frac{5}{12} < \alpha < \frac{1}{2} - 2\sqrt{\varepsilon}$, on a :

$$N^{\alpha} < p < N^{\alpha+\varepsilon} \quad \mathcal{S}(\mathcal{A}_p, N^{1/7}) \leq \frac{N^{1/2} \ \mathrm{Log}(1 + \varepsilon/\alpha)}{(0{,}5 - \alpha - 2\sqrt{\varepsilon}) \ \mathrm{Log} \ N}$$

où le membre de droite est réduit de moitié par rapport à ce que l'on obtiendrait par application directe du Théorème 1 (borne supérieure) pour $\mathcal{S}(\mathcal{A}_p, N^{1/7})$ et cette amélioration se répercute de façon substantielle sur le problème de départ : Chen parvient ainsi à démontrer que,

pour tout entier N assez grand, il existe un P_2 dans l'intervalle $[N - N^{1/2}, N]$.

Soulignons qu'en raison de la présence de la valeur absolue de $r(\mathcal{A}, n)$ dans le terme reste du Théorème 1, celui-ci n'est pas exploitable pour démontrer le Lemme. Chen reprend donc le crible de Selberg au départ, écrivant pour une fonction λ_d convenable (indépendante de p) :

$$\sum_{N^\alpha < p < N^{\alpha+\varepsilon}} \mathcal{S}(\mathcal{A}_p, N^{1/7}) \leq \sum_{N^\alpha < p < N^{\alpha+\varepsilon}} \sum_{\substack{N - N^{1/2} < a < N \\ a \equiv 0 \ [p]}} \Big(\sum_{d \mid a} \lambda_d\Big)^2$$

$$= \sum_{d_1} \sum_{d_2} \lambda_{d_1} \lambda_{d_2} \sum_{N^\alpha < p < N^{\alpha+\varepsilon}} \left[\frac{N}{p[d_1,d_2]} \right] - \left[\frac{N - N^{1/2}}{p[d_1,d_2]} \right]$$

où $[u]$ désigne la partie entière du nombre réel u et $[d_1,d_2]$ le P.P.C.M. des entiers d_1 et d_2. L'évaluation de la dernière expression est alors ramenée à celle de sommes trigonométriques, lesquelles sont en fin de compte majorées par la méthode de van der Corput.

3.2. Le crible linéaire d'Iwaniec

En utilisant le crible de Rosser, Iwaniec [197? a] a récemment obtenu une version du Théorème 1 dont le terme reste fait intervenir $r(\mathcal{A},n)$ et non $|r(\mathcal{A},n)|$, ce qui permet de tenir compte des irrégularités de distribution (nous en verrons une application au paragraphe 4) :

Théorème 2.- *On conserve les notations du Théorème 1 ; sous l'hypothèse* $\frac{V(w)}{V(z)} \leq \frac{\text{Log } z}{\text{Log } w} \left(1 + O\left(\frac{1}{\text{Log } w}\right)\right)$, *on a, pour* $z \geq 2$, K *et* $L > \sqrt{2}$, *l'existence d'une constante positive* c *telle que pour tout* $\eta > 0$:

$$\mathcal{S}(\mathcal{A},z) \leq XV(z)\left\{F\left(\frac{\text{Log } KL}{\text{Log } z}\right) + cE\right\} + 2^{\eta^{-7}} R(\mathcal{A},K,L)$$

$$\mathcal{S}(\mathcal{A},z) \geq XV(z)\left\{f\left(\frac{\text{Log } KL}{\text{Log } z}\right) - cE\right\} - 2^{\eta^{-7}} R(\mathcal{A},K,L)$$

où $E << \eta(1 + \eta^{-8}(\text{Log } KL)^{-1/3})$ *et* $R(\mathcal{A},K,L) = \sum_{k<K} \sum_{\substack{\ell < L \\ k\ell \mid P(z)}} a_k b_\ell r(\mathcal{A},k\ell)$,

les termes a_k *et* b_ℓ *dépendant au plus de* K, L, z *et* η *et étant majorés en module par* 1.

3.3. Nouvelles pondérations

Laborde [1978] a repris l'étude de Bukhštab et a obtenu une description praticable de ses poids (cette description permet, entre autres, de vérifier la supériorité de ces poids sur les poids logarithmiques de Richert) ; il a également étendu les poids de Bukhštab pour le cas où le nombre d'éléments de la suite $\mathcal{A}$ est notablement différent du plus grand élément de $\mathcal{A}$.

Iwaniec, dans son travail que nous analyserons par la suite, utilise un nouveau système de poids, dû à Richert (nous n'avons pas d'autre information concernant ce travail non publié de Richert : le cas particulier présenté par Iwaniec est plus simple à mettre en oeuvre que ce que donnerait la pondération de Bukhštab-Laborde,

mais moins précis).

Notre sentiment est que d'importantes améliorations soient à attendre d'une étude serrée des pondérations et que nous arrivons au moment où "it turns out that each sieve problem requires an optimization procedure of its own in order to reach the most precise results".

3.4. Résultats récents (fin Avril 1978)

1) $2N = P_1 + P_2$ (Chen, cf. § 2.6) ;

2) a) $P_1 + 2 = P_2$ (Chen, cf. § 2.6) ;

b) pas de progrès depuis le résultat de Selberg (cf. § 2.5) ;

3) (i) En combinant le crible linéaire d'Iwaniec avec les méthodes analytiques usuelles, Iwaniec et Jutila [197?] ont pu remplacer 7/12 par 13/23 .

(ii) Chen [1975] a remplacé 6/11 par 1/2 ; cette valeur a ensuite été réduite par Laborde, Halberstam, Heath-Brown, Iwaniec et Richert (la valeur actuelle est légèrement supérieure à 4/9).

4) L'équation $n^2 + 1 = P_2$ a une infinité de solutions (Iwaniec [197? b]).

4. Le théorème d'Iwaniec sur l'équation $n^2 + 1 = P_2$

On considère le crible $\mathcal{A} = \{n^2 + 1 , n \leq N\}$ et $\mathcal{P} = \{p \mid p \leq N\}$.

4.1. Pondération

Soit n un entier, p_n son plus petit facteur premier ; si l'on pose

$$w(n) := 1 - \sum_{p \mid n \, , \, p < N} w_p(n) \, ,$$

où $w_p(n) = \begin{cases} 1 - \text{Log } p / \text{Log } N & \text{pour } p = p_n \text{ ou } (p_n < p \text{ et } p \geq N^{1/2}) \\ \text{Log } p_n / \text{Log } N & \text{pour } p_n < p < N^{1/2} \end{cases}$

on a la minoration

$$\text{Card}\{a \in \mathcal{A} \, , \, a = P_2\} \geq \sum_{\substack{a \in \mathcal{A} \\ (a \, , \, P(N^{1/5})) = 1}} \mu^2(a) \, w(a)$$

on obtient sans peine la majoration

$$\sum_{\substack{a \in \mathcal{A} \\ (a \, , \, P(N^{1/5})) = 1}} (1 - \mu^2(a)) \leq \sum_{N^{1/5} \leq p \leq N^{9/10}} \sum_{\substack{n \leq N \\ n^2 + 1 \equiv 0 \, [p^2]}} 1 \leq 4 N^{0,9}$$

et il suffit de s'attacher à minorer

$$W(\mathcal{A},N^{1/5}) := \sum_{\substack{a \in \mathcal{A} \\ (a,P(N^{1/5}))=1}} w(a)$$

par la définition des poids $w(a)$, ceci est égal à

$$\mathcal{S}(\mathcal{A},N^{1/5}) - \sum_{N^{1/5} \le p < N^{1/2}} \left(1 - \frac{\text{Log } p}{\text{Log } N}\right) \mathcal{S}(\mathcal{A}_p, p) -$$

$$(4.1) \qquad - \sum_{N^{1/5} \le p_1 < p < N^{1/2}} \frac{\text{Log } p_1}{\text{Log } N} \mathcal{S}(\mathcal{A}_{pp_1}, p_1) -$$

$$- \sum_{N^{1/2} \le p \le N} \left(1 - \frac{\text{Log } p}{\text{Log } N}\right) \mathcal{S}(\mathcal{A}_p, N^{1/5}) \quad .$$

4.2. Utilisation du crible

On a réduit le problème à minorer la quantité $\mathcal{S}(\mathcal{A},N^{1/5})$ et à majorer les sommes $\mathcal{S}(\mathcal{A}_q, z)$, ce que nous effectuerons grâce au Théorème 2.

On note $\omega(d)$ le nombre de solutions de la congruence $n^2 + 1 \equiv 0 \ [d]$; la fonction ω est multiplicative, vaut 1 pour $d = 2$, zéro pour tout nombre premier congru à -1 modulo 4 et 2 pour tout nombre premier congru à 1 modulo 4 ; il en résulte que le produit $V(z)$ est de l'ordre de grandeur de $\frac{1}{\text{Log } z}$.

En appliquant le Théorème 2 pour majorer $\mathcal{S}(\mathcal{A}_q, z)$, on trouve un terme principal de la forme

$$V(z) \frac{\omega(q)}{q} N \left\{F\left(\frac{\text{Log } KL}{\text{Log } z}\right) + O(\eta)\right\}$$

qui est donc de l'ordre de grandeur de $\frac{\omega(q)}{q} \frac{N}{\text{Log } N}$, tant que KL et z sont des puissances de N .

Le terme d'erreur $R(\mathcal{A}_q, K, L)$ prend la forme

$$\sum_{\ell < L} \sum_{\substack{k < K \\ k\ell \mid P(z)}} a_\ell \, b_k \, r(\mathcal{A}_q, k\ell) = \sum_{\ell < L} \sum_{\substack{k < K \\ k\ell \mid P(z)}} a_\ell \, b_k \, r(\mathcal{A}, k\ell q)$$

et la résolution du problème initial est réduite à la détermination de K et L tels que le produit KL soit maximal et $|R(\mathcal{A}_q, K, L)|$ soit $o\left(\frac{\omega(q)}{q} \frac{N}{\text{Log } N}\right)$.

4.3. Traitement du terme d'erreur

Posons $B(\ell,K) := \sum^{(k)} b_k\, r(\mathcal{A},k\ell)$, où la sommation est effectuée sur les entiers k inférieurs à K et premiers à ℓ . Nous esquisserons la démonstration de la relation

$$\sum_{L<\ell<2L} B^2(\ell,K) \ll (1 + K^{7/2} L^{-5/4} N)N^{1+\varepsilon} \qquad \text{pour } K \text{ et } L \leq N .$$

En utilisant l'inégalité de Cauchy-Schwarz et en sommant par parties, on obtient la majoration, valable pour $\varepsilon > 0$:

$$(4.2) \qquad \sum_{\ell < N^{1-4\varepsilon}} \left|B(\ell,N^{1/15-\varepsilon})\right| \ll N^{1-\varepsilon}$$

que nous utiliserons dans la partie 4.4.

4.3.1. De la relation

$$\text{Card}\ \mathcal{A}_{k\ell} = \sum^{(v)} \sum^{(s)} 1 ,$$

où v et s satisfont les conditions

(v) $\quad 0 < v < \ell \qquad v^2 + 1 \equiv 0 \ [\ell]$

(s) $\quad s < N \qquad s \equiv v \ [\ell] \qquad s^2 + 1 \equiv 0 \ [k]$

on déduit

$$B(\ell,K) = \sum^{(v)} \left\{ \sum^{(k)} b_k \sum^{(s)} 1 - \frac{N}{\ell} \sum^{(k)} b_k \frac{\omega(k)}{k} \right\}$$

par l'inégalité de Cauchy-Schwarz, on a :

$$B^2(\ell,K) \leq \omega(\ell) \sum^{(v)} \left\{ \sum^{(k)} b_k \sum^{(s)} 1 - \frac{N}{\ell} \sum^{(k)} b_k \frac{\omega(k)}{k} \right\}^2$$

pour $\ell \leq N$, on majore $\rho(\ell)$ par N^{ε} ; nous allons maintenant évaluer la somme

$$\sum_{L<\ell<2L} B^2(\ell,K) \qquad \text{pour } L \leq N$$

nous nous limiterons ici au terme diagonal qui apparaît dans le développement du carré :

$$V(N,K,L) := \sum_{L<\ell<2L} \sum^{(v)} \frac{1}{\ell} \left(\sum^{(k_1)} b_{k_1} \sum^{(s)} 1 \right) \left(\sum^{(k_2)} b_{k_2} \frac{\omega(k_2)}{k_2} \right)$$

$$= \sum^{(k_1)} \sum^{(k_2)} b_{k_1} b_{k_2} \frac{\omega(k_2)}{k_2} \sum^{(*)} \ell^{-1} ,$$

où la dernière somme est étendue aux triplets (ℓ,v,s) satisfaisant les conditions $(\ell) := (L < \ell < 2L ,\ (\ell,k_1,k_2) = 1)$, (v) et (s)

on effectue alors le changement de variables $\ell = \ell$, $v = v$, $t = \frac{s - v}{\ell}$, les

conditions sur (s) devenant

$$(t') \qquad t < \frac{N - v}{\ell} \quad , \qquad (\ell t + v)^2 + 1 \equiv 0 \ [k_1] \ .$$

La contribution à V des triplets pour lesquels $\frac{N - v}{t} \leq \ell < \frac{N}{t}$ est aisément majorée par N^{ε}, et on peut se restreindre à considérer les triplets (ℓ,v,t) satisfaisant les conditions (ℓ), (v) et

$$(t) \qquad t < \frac{N}{\ell} \quad , \qquad (\ell t + v)^2 + 1 \equiv 0 \ [k_1] \ ,$$

soit alors c le reste de t modulo k_1 ; en posant $\Omega = c\ell + v$, on a :

$$\Sigma^{(*)} \ell^{-1} = \sum_{t < N/\ell} \sum^{(\ell,\Omega)} \ell^{-1} + O(N^{\varepsilon})$$

où la somme intérieure est effectuée sur les couples (ℓ,Ω) tels que

$$(\ell,\Omega) \quad \begin{cases} L < \ell < \min(2L, N/t) & (\ell, k_1 k_2) = 1 \\ c\ell \leq \Omega < (c+1)\ell & \Omega^2 + 1 \equiv 0 \ [\ell k_1] \ . \end{cases}$$

4.3.2. Pour illustrer la méthode employée dans l'évaluation de la dernière somme, nous évaluerons la somme

$$T(L,\beta) := \sum_{\substack{L < \ell < 2L \\ 0 \leq \Omega < \beta\ell \ , \ \Omega^2 + 1 \equiv 0 \ [\ell]}} 1 = \sum_{\substack{L < \ell < 2L \\ \Omega^2 + 1 \equiv 0 \ [\ell]}} \chi_\beta(\Omega/\ell)$$

où χ_β est la fonction périodique de période 1 qui coïncide sur $[0,1[$ avec la fonction caractéristique de l'intervalle $[0,\beta[$; en encadrant cette fonction entre deux fonctions dérivables, ou en utilisant directement un résultat de Erdös-Turán [1948] sur la répartition modulo 1, on a pour tout H une majoration de la forme

$$\left| T(L,\beta) - \beta T(L,1) \right| << \frac{T(L,1)}{H} + \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{\substack{L < \ell < 2L \\ \Omega^2 + 1 \equiv 0 \ [\ell]}} e\left(\frac{h\Omega}{\ell} \right) \right| .$$

Le terme principal T(L,1) ne soulève pas de difficulté particulière. Pour évaluer les sommes trigonométriques intervenant dans le membre de droite, on commence par utiliser la correspondance, due à Lagrange, entre les solutions de

$$D = r^2 + s^2 \qquad (r,s) = 1 \qquad |r| < s$$

et les solutions de $\Omega^2 + 1 \equiv 0 \ [D]$ donnée par

$$\Omega = \frac{\bar{r}}{s}(r^2 + s^2) - \frac{r}{s} \ ,$$

où $\bar{r}$ est l'inverse de r modulo Ω. On en déduit la majoration

$$\left| \sum_{\ell,\Omega} e\left(\frac{h\Omega}{\ell} \right) \right| \leq \sum_{s = (L/2)^{1/2}}^{(2L)^{1/2}} \sup_{\substack{r_1, r_2 \\ 0 < r_2 - r_1 < 2s}} \left| \sum_{\substack{(r,s) = 1 \\ r_1 < r < r_2}} e\left(\frac{h\bar{r}}{s} - \frac{hr}{r^2 + s^2} \right) \right|$$

et on a ainsi réduit le problème à l'estimation d'une somme de Kloosterman tronquée ; dans le cas général, on doit évaluer des sommes du type

$$\sum_{\substack{(r,s)=1 \\ r_1 < r < r_2 \\ r \equiv \lambda \ [\Lambda]}} e\left(\frac{h\bar{r}}{s} - \frac{hr}{r^2+s^2} \right) \quad ,$$

sommes que Hooley [1967] a majorées en partant des estimations de Weil pour les sommes de Kloosterman.

4.4. Fin de la démonstration

Il résulte de la relation (4.2) que l'expression Log KL / Log N peut prendre la valeur $\frac{16}{15} - \varepsilon$, alors qu'un traitement direct conduirait à la valeur 1 . L'application du Théorème 2 et de la relation (4.1), conduit, après un calcul numérique pénible (cf. la définition des fonctions f et F en terme d'équations différence - différentielles) à la positivité de la quantité $W(\mathcal{A}, N^{1/5})$.

Remarquons pour conclure que la même méthode permet de démontrer que pour tout polynôme $G(n) \equiv an^2 + bn + c$ avec $a > 0$ et c impair, il existe une infinité d'entiers n tels que $G(n) = P_2$.

BIBLIOGRAPHIE

Ouvrages et exposés d'intérêt général

BOMBIERI [1974] - Le grand crible dans la théorie analytique des nombres, Astérisque 18, 1974.

HALBERSTAM - ROTH [1966] - Sequences, vol. 1, Oxford at the Clarendon Press, Chapitre IV pour une introduction aux cribles arithmétiques.

HALBERSTAM-RICHERT [1974] - Sieve methods, Academic Press London, La bible du petit crible !

HALBERSTAM [1974] - A proof of Chen's Theorem, Astérisque 24-25, 1975, 281-293, Présentation du théorème de Chen.

MONTGOMERY [1971] - Topics in multiplicative Number Theory, Springer Verlag, Lecture Notes in Maths. 227, Le grand crible en 1971.

RICHERT [1976] - Sieve methods, Edité par le Tata Institute Bombay, Introduction au grand crible et au crible de Selberg ; on visitera avec profit sa bibliographie.

Articles spécialisés

BRUN [1920] - Skr. Norske Vid.-Akad. Kristiania I (1920) n° 3, 36 pp.

BUKHŠTAB [1967] - Russian Math. Surveys, 22 (1967), 205-233.

CHEN [1973] - Sci. Sinica, 16 (1973), 157-176.

CHEN [1975] - Sci. Sinica, 18 (1975), 611-627.

ERDÖS - TURÂN [1948] - Indag. Math., 10 (1948), 370-378 et 406-413.

HOOLEY [1967] - Acta Math., 117 (1967), 281-299.

HUXLEY [1972] - The distribution of prime numbers, Oxford, x + 128 pp.

IWANIEC [1976] - Acta Arith., 29 (1976), 69-95.

IWANIEC [197? a] - A new form of the error term in the linear sieve (preprint), à paraître dans Acta Arith.

IWANIEC [197? b] - Almost-primes represented by polynomials (preprint).

IWANIEC - JUTILA [197?] - Primes in short intervals (preprint).

KÜHN [1941] - Norske Vid. Selsk. Forh., Trondhejm, 14 (1941), 145-148.

LABORDE [1978] - Thèse de 3ème Cycle ; à paraître dans Mathematika.

RICHERT [1969] - Mathematika, 16 (1969), 1-22.