Astérisque

ÉTIENNE FOUVRY

Quelques progrès récents en théorie analytique des nombre

Astérisque, tome 147-148 (1987), p. 79-93

<http://www.numdam.org/item?id=AST_1987__147-148__79_0>

Société Mathématique de France
Astérisque 147-148 (1987), p.79-93.

QUELQUES PROGRÈS RÉCENTS EN THÉORIE ANALYTIQUE DES NOMBRES

par

Etienne FOUVRY

I.- Rappel des résultats classiques du crible linéaire

En toute généralité, un problème de crible s'énonce ainsi :

Soient $\mathcal{A}$ *une suite finie d'entiers* $\geqslant 1$, $z \geqslant 2$, $\mathcal{P}$ *un ensemble de nombres premiers et* $P(z)$ *le produit* $\prod_{p<z,\, p\in\mathcal{P}} p$.

Que peut-on dire de la quantité

$$S(\mathcal{A}\,;\mathcal{P},z) \quad |\{a\in\mathcal{A}\,;\ (a,P(z))=1\}| \ ?$$

Les renseignements sur $\mathcal{A}$ concernent

$$\mathcal{A}_d = \{a\in\mathcal{A}\,;\ a\equiv 0[d]\}$$

et s'expriment par la formule d'approximation

$$|\mathcal{A}_d| = \omega(d)X/d + r(\mathcal{A};d) \qquad (1.1)$$

où X ne dépend pas de d , où $\omega(d)$, défini pour d , sans facteur carré, avec tous ses diviseurs premiers dans $\mathcal{P}$, vérifie la formule $\omega(d) = \prod_{p\mid d,\, p\in\mathcal{P}} \omega(p)$.

Dans la formule (1.1), on espère que $r(\mathcal{A};d)$ se comporte en terme d'erreur. Dans le cas linéaire, c'est-à-dire $\omega(p)$ valant 1 en moyenne, le crible de Selberg mène à la formule suivante (théorème de Jurkat-Richert) :

$$S(\mathcal{A};\mathcal{P},z) \begin{matrix} \leqslant \\ \\ \geqslant \end{matrix} XV(z) \begin{matrix} \{F(\log D/\log z)+E\}+ \\ \\ \{f(\log D/\log z)-E\}- \end{matrix} \sum_{\substack{d\mid P(z)\\ d<D}} 3^{\nu(d)}|r(\mathcal{A};d)| \qquad (1.2)$$

où $V(z)$ est le produit eulérien $\prod_{p\in\mathcal{P},\, p<z} (1-\omega(p)/p)$,

$\nu(d)$ le nombre de facteurs premiers de d

E un terme, négligeable en général,

F et f deux fonctions continues définies par

$$\begin{cases} F(s) = 2\, e^{\gamma} s^{-1} & (\gamma \text{ constante d'Euler}) \\ f(s) = 0 & \text{pour } 0 < s \leqslant 2 \end{cases}$$

et

$$\begin{cases} (sF(s))' = f(s-1) \\ (sf(s))' = F(s-1) & \text{pour } s > 2 \,. \end{cases}$$

(On se reportera à [12] pour un énoncé complet.) On montre que les fonctions F et f sont monotones, qu'elles tendent très rapidement vers 1 et qu'elles sont optimales, dans la formule (1.2).

Dans le cas linéaire, les formules du crible de Selberg sont maintenant dépassées par celles du crible de Rosser-Iwaniec, de nature combinatoire. On a les inégalités (volontairement schématisées) suivantes ([18]) :

$$S(\mathcal{A};\mathcal{P},z) \begin{matrix} \leqslant \\ \geqslant \end{matrix} XV(z) \begin{matrix} \{F(\log D/\log z) + E_1\} \\ \{f(\log D/\log z) - E_1\} \end{matrix} \pm \sum_{d\mid P(z)} \lambda^{\pm}(d) r(\mathcal{A};d) \quad (1.3)$$

Le terme principal de (1.3) coïncide avec celui de (1.2) (E_1 est une quantité négligeable) et le terme d'erreur contient les coefficients $\lambda^{\pm}(d)$ "bien factorisables de niveau D ". Par définition, une fonction arithmétique $\lambda(d)$ est *bien factorisable de niveau* $D > 1$, si, pour tout D_1 , $D_2 \geqslant 1$, $D_1 D_2 = D$, il existe deux fonctions $\lambda_1(d_1)$, $\lambda_2(d_2)$, nulles hors de $[1,D_1]$ et $[1,D_2]$, vérifiant

$$|\lambda_1(d_1)|, |\lambda_2(d_2)| \leqslant 1 \quad \text{pour tout } d_1 \text{ et tout } d_2$$

et

$$\lambda = \lambda_1 * \lambda_2 \,.$$

Le crible de Rosser-Iwaniec a déjà fourni des résultats apparemment inaccessibles, pour l'instant, par le crible de Selberg : équation $n^2+1 = P_2$, recherche de nombres premiers dans de petits intervalles,...

Dans cet exposé, nous nous intéressons aux résultats récents sur le criblage de

$\mathcal{A} = \{p+2 \ ; \ p \leqslant x\}$ pour étudier les nombres premiers jumeaux c'est-à-dire la fonction

$$\pi_2(x) = |\{p+2 \leqslant x \ ; \ p+2 \text{ premier}\}|$$

et de

$\mathcal{A}^{(q)} = \{n \leqslant x \ ; \ n \equiv a[q]\}$ pour considérer la fonction

$$\pi(x;q,a) = |\{p \leqslant x \ ; \ p \equiv a[q]\}|$$

qui compte les nombres premiers dans une progression arithmétique. (La lettre p désigne toujours un nombre premier).

II.- Nombres premiers dans les progressions arithmétiques

L'équivalence

$$\pi(x;q,a) \sim (\text{li } x)/\varphi(q) \quad (x \to +\infty) \qquad (2.1)$$

bien que conjecturée avec uniformité pour $(a,q)=1$ et $q \leqslant x^{1-\varepsilon}$ (conséquence de la conjecture de Montgomery), n'est en fait démontrée que pour $q \leqslant (\log x)^A$ -A quelconque- (théorème de Siegel-Walfisz). Toutefois, on sait que l'équivalence (2.1) est vraie en moyenne, pour $q \leqslant x^{1/2}(\log x)^{-A}$. On démontre :

THÉORÈME O (Bombieri-Vinogradov).- *Pour tout* A , *on a :*

$$\sum_{q \leqslant x^{1/2}(\log x)^{-A}} \max_{y \leqslant x} \max_{(a,q)=1} \left|\pi(y;q,a) - \frac{\text{li } y}{\varphi(q)}\right| = O_A(x(\log x)^{-A+2}). \qquad (2.2)$$

Ce théorème, qui repose principalement sur l'inégalité de grand crible, a le mérite d'éviter le recours à l'hypothèse de Riemann généralisée, dans beaucoup d'applications, en particulier lorsqu'on crible la suite $\mathcal{A}$. Les choix $\omega(p) = p/(p-1)$ $(p \neq 2)$, $X = \text{li } x$ et $D = x^{(1/2)-\varepsilon}$, dans la formule (1.2) donnent, via la formule de Mertens, la majoration asymptotique :

COROLLAIRE O.- *Pour tout* $\varepsilon > 0$ *et* $x > x_0(\varepsilon)$, *on a*

$$\pi_2(x) \leqslant (4+\varepsilon) \, B \, x \log^{-2} x \ .$$

On a posé $B = 2 \prod_{p>2} (1-(p-1)^{-2})$, et on conjecture l'équivalence

$$\pi_2(x) \sim B \, x \log^{-2} x \quad (x \to \infty) \ .$$

On pense aussi que l'exposant $1/2$, dans (2.2), peut être remplacé par 1 (conjecture d'Elliott-Halberstam) et que le franchissement de la valeur critique $x^{1/2}$ est une question extrêmement difficile de théorie analytique des nombres (voir [6] pour des résulats partiels dans cette direction).

Le problème est plus aisé si on cherche des résultats en rapport avec le terme d'erreur de (1.3), autrement dit, des résultats où le signe de valeur absolue est remplacé par un coefficient bien factorisable. On va donner quelques idées de la démonstration du théorème de Bombieri, Friedlander et Iwaniec ([3]) :

THÉORÈME 1.- *Pour tout* $\varepsilon>0$, *tout* $A>0$, *tout* $x\geqslant 2$, *toute fonction bien factorisable de niveau* $x^{4/7-\varepsilon}$, *et tout entier* a, *on a :*

$$\sum_{\substack{q \\ (q,a)=1}} \lambda(q)(\pi(x;q,a)-(\mathrm{li}\ x)/\varphi(q)) = O_{a,\varepsilon,A}(x(\log x)^{-A}).$$

Iwaniec et l'auteur furent les premiers à donner une estimation de ce type avec un exposant supérieur à $1/2$, plus préciséent $9/17$ ([9]) et cette valeur fut portée à $17/32$ ([6]).

Le théorème 1, combiné avec la formule (1.3), mène au

COROLLAIRE 1.- *Pour tout* $\varepsilon>0$ *et* $x>x_0(\varepsilon)$, *on a*

$$\pi_2(x) \leqslant (7/2+\varepsilon)\ B\ x\ \log^{-2}x\ .$$

1.- Répartition du produit de convolution de deux suites

On transfère l'étude de la répartition des nombres premiers, via certaines identités combinatoires (Linnik, Vaughan ou Heath-Brown) à celle, plus générale, de la convolée de deux suites. Ainsi, la clé du théorème 1 est le lemme 1 ; il nécessite, pour son énoncé, plusieurs notations.

On note (α_m) et (β_n) deux suites vérifiant

$$|\alpha_m| \leqslant \tau_K(m) \qquad |\beta_n| \leqslant \tau_K(n) \tag{2.3}$$

où K est un entier fixé et $\tau_K(m)$ est le nombre de représentations de l'entier m en produit de K entiers $\geqslant 1$. On demande aussi que la suite (β_n) se répartisse bien dans les progressions arithmétiques (condition analogue à l'énoncé du théorème de Siegel-Walfisz) :

$\forall n_0 \quad \forall q \geqslant 1 \ (n_0,q) = 1 \ , \ \forall d \geqslant 1 \quad \forall y \geqslant 2 \ , \ \forall A$ *on a*

$$\sum_{\substack{n \equiv n_0 [q] \\ (n,d)=1 \\ n \leqslant y}} \beta_n = \frac{1}{\varphi(q)} \sum_{\substack{(n,dq)=1 \\ n \leqslant y}} \beta_n + O_A\left(y \tau_K(d) (\log y)^{-A}\right) \tag{2.4}$$

et que β_n s'annule si n a un petit facteur premier :

$$p \mid n \quad \text{et} \quad p < \exp(\log^{1/10} n) \Rightarrow \beta_n = 0 \tag{2.5}$$

(cette dernière condition, purement technique, peut parfois être omise). On définit maintenant la quantité

$$\Delta(\ldots) = \Delta((\alpha_m),(\beta_n);x,N,q,a) = \sum_{\substack{m \leqslant xN^{-1} \\ n \leqslant N \\ mn \equiv a [q]}} \alpha_m \beta_n - \frac{1}{\varphi(q)} \sum_{\substack{m \leqslant xN^{-1} \\ n \leqslant N \\ (mn,q)=1}} \alpha_m \beta_n$$

qui décrit la répartition de $\alpha_m * \beta_n$ dans une progression arithmétique, et pour finir, la fonction $\vartheta(t)$ par les formules :

$$0 \leqslant t \leqslant \frac{1}{10} : \vartheta(t) = \frac{1}{2} + \frac{t}{2} \quad ; \quad \frac{1}{10} \leqslant t \leqslant \frac{1}{6} : \vartheta(t) = \frac{13}{24} + \frac{t}{12}$$

$$\frac{1}{6} \leqslant t \leqslant \frac{1}{4} : \vartheta(t) = \frac{1}{2} + \frac{t}{3} \quad ; \quad \frac{1}{4} \leqslant t \leqslant \frac{2}{7} : \vartheta(t) = \frac{2}{3} - \frac{t}{3}$$

$$\frac{2}{7} \leqslant t \leqslant \frac{2}{5} : \vartheta(t) = \frac{1}{2} + \frac{t}{4} \quad ; \quad \frac{2}{5} \leqslant t \leqslant \frac{1}{2} : \vartheta(t) = 1 - t$$

$$\frac{1}{2} \leqslant t \leqslant 1 : \vartheta(t) = \frac{1}{2} \ .$$

En posant $\upsilon = (\log N)/\log x$, on énonce

LEMME 1.- *Sous les conditions* (2.3), (2.4) *et* (2.5), *on a, pour tout* $\varepsilon > 0$, *tout* A , *tout* υ $(\varepsilon \leqslant \upsilon \leqslant 1-\varepsilon)$, *tout* $x \geqslant 2$, *tout entier* a *et toute fonction* λ *bien factorisable de niveau* $x^{\vartheta(\nu)-\varepsilon}$, *la relation*

$$\sum_{\substack{q \\ (q,a)=1}} \lambda(q) \, \Delta(\ldots) = O_{a,\varepsilon,K,A}\left(x (\log x)^{-A}\right) \ .$$

On trouve le lemme 1 sous cette forme dans [8] ; il rassemble en un seul énoncé les différents résultats de [3], [6] et [9] et montre que la valeur critique $x^{1/2-\varepsilon}$ du "niveau de répartition" est franchie pour $\varepsilon < \upsilon < 1/2 - \varepsilon$. La démonstration, très longue et très déli-

cate, de ce lemme s'appuie sur un calcul de dispersion et des majorations en moyenne de sommes de Kloosterman ([4]) qui, dans ce contexte, sont plus efficaces que la majoration classique de Weil. Evidemment, on décompose $\lambda=\lambda_1*\lambda_2$ au mieux de ses intérêts.

Les identités combinatoires, déjà évoquées, amènent à envisager le cas particulier où $\beta_n=1$, pour tout n. On montre :

LEMME 2.- *Dans le cas particulier où* $\beta_n\equiv 1$, *l'estimation du lemme* 1 *susbiste en remplaçant* $\vartheta(\upsilon)$ *par* $\vartheta_1(\upsilon)$ *où la fonction* $\vartheta_1(t)$ *est définie comme suit :*

$$\vartheta_1(t) = \begin{cases} \vartheta(t) & \text{pour} \quad 0\leqslant t\leqslant \frac{2}{5} \\ \frac{3}{2}\,t & \text{pour} \quad \frac{2}{5}\leqslant t\leqslant \frac{1}{2} \\ \frac{1}{2}+\frac{1}{2} & \text{pour} \quad \frac{1}{2}\leqslant t\leqslant 1 \end{cases} .$$

Ce lemme se trouve dans [3], [5] et [9] et améliore la valeur du niveau de répartition pour $\upsilon \geqslant 2/5$ (voir figure). Sa démonstration utilise la technique de Fourier et, une fois encore, les majorations de [4]. Le théorème 1 s'acquiert à partir des deux lemmes en analysant, pour chaque situation, les valeurs de υ rencontrées - la constante $4/7$ provient, en quelque sorte, de $\vartheta(2/7)=\vartheta_1(2/7)=4/7$ (voir figure).

2.- Quelques applications

Le lemme 1 peut être employé dans un grand nombre de situations. Ainsi, en partant de l'inégalité

$$\pi_2(x) \leqslant S(\mathcal{A};\mathcal{P},z_1) - \frac{1}{2}\sum_{z_1\leqslant p_1<z} S(\mathcal{A}_{p_1};\mathcal{P},z_1) + \frac{1}{2}\sum_{z_1\leqslant p_3\leqslant p_2\leqslant p_1<z} S(\mathcal{A}_{p_1p_2p_3};\mathcal{P},p_3) + O(x^{1/2})$$

(où $\mathcal{P}=\{p\neq 2\}$ et $z_1\leqslant z\leqslant x^{1/2}$)

déjà utilisée par Pan ([21]), Fouvry et Grupp sont parvenus au

COROLLAIRE 2 ([8]).- *Pour* x *suffisamment grand, on a l'inégalité*

$$\pi_2(x) \leqslant 3{,}454\ B\ x\ \log^{-2} x .$$

Ce résultat se généralise aux nombres premiers $\leqslant x$, de la forme $p-a$, avec uniformité sur $|a| \leqslant (\log x)^A$ (A quelconque) et s'incorpore aux travaux de Huxley ([16], [17]) sur la différence $p_{n+1}-p_n$ (p_n désigne le nombre premier de rang n). On a

COROLLAIRE 3 ([8]).- *Il existe* $c_1>0$, *tel que, pour* x *suffisamment grand, on ait la minoration*

$$|\{p_n \leqslant x \ : \ p_{n+1}-p_n \leqslant 0{,}4342 \log p_n\}| \geqslant c_1 \, x \log^{-1} x \ .$$

Ce résultat doit être comparé à la récente majoration de Maier ([20]) : $\underline{\lim}\ (p_{n+1}-p_n)/(\log p_n) \leqslant 0{,}248$; malheureusement, sa technique très ingénieuse ne permet apparemment pas d'exprimer cette borne sous la forme du corollaire 3.

3.- Vers la conjecture d'Artin

Artin, en 1927, proposa la conjecture suivante :

Tout entier relatif a , *différent de* -1 *et d'un carré parfait est une racine primitive pour une infinité de nombres premiers.*

Hooley, en admettant une certaine généralisation de l'hypothèse de Riemann, prouva l'exactitude de cette hypothèse, et même, qu'il y a une densité positive - dépendant de a - de nombres premiers pour lesquels a est une racine primitive ([15]). Il y a quelque temps encore, on ne savait même pas si la conjecture d'Artin est vraie pour au moins un a . En 1984, Gupta et Ram Murty ([11]) ont montré que si p_1, p_2, p_3 sont trois nombres premiers distincts, la conjecture d'Artin est vraie pour au moins un a appartenant à S , où

$$S = \{p_1 p_3^2,\ p_1^3 p_2^2, p_1^2 p_2^2, p_2^3 p_3^2, p_2^2 p_3, p_1^2 p_3^3, p_1 p_2^3, p_1^3 p_2^2 p_3^2, p_2 p_3^3,$$
$$p_1^2 p_2^3 p_3, p_1^3 p_3, p_1 p_2^2 p_3^3, p_1 p_2 p_3\}$$

et par conséquent, que la conjecture d'Artin est vraie pour une infinité de a . Leur idée principale, est de chercher dans un ensemble très particulier :

$$E(x) = \{p \leqslant x \ ; \ p' | p-1 \Rightarrow p' = 2 \quad \text{ou} \quad p' > x^{\xi}\} \qquad (\xi \text{ constante } > 1/4)$$

des nombres p pour lesquels a soit racine primitive. En effet, pour $p \in E(x)$, on a $v(p-1) \leqslant 4$, ce qui permet de contrôler la nature, le nombre et les indices des sous-groupes de $(\mathbb{Z}/p\mathbb{Z})^*$ multiplicatif. La minoration

$$|E(x)| \gg x \log^{-2} x$$

est une conséquence de [9] (avec l'exposant 9/17). Mais Heath-Brown a remarqué que le théorème 1 combiné avec la technique d'inversion du rôle des variables entraînait pour l'ensemble

$$E^*(x)=\{p\leqslant x \ ; \ p'\mid p-1 \Rightarrow p'=2 \quad \text{ou} \quad p'>x^{\xi}, \upsilon(p-1)\leqslant 3\}$$

la minoration

$$|E^*(x)|>>x \log^{-2} x$$

et qu'il est plus économique de travailler avec $E^*(x)$, car, pour $p\in E^*(x)$, $(\mathbb{Z}/p\mathbb{Z})^*$ a moins de possibilités de sous-groupes. Suivant les arguments de Gupta et Ram Murty, Heath-Brown restreint $|S|$ et prouve entre autres, les majorations significatives suivantes :

THÉORÈME 2 ([14]).- *On a les relations*

$$|\{ p \ ; \ p \text{ ne vérifie pas la conjecture d'Artin}\}|\leqslant 2$$

et

$$|\{ a \ ; \ |a|\leqslant x \ , \ a \text{ ne vérifie pas la conjecture d'Artin}\}|<<x^{1/2} \ .$$

Apparemment, on ne sait toujours pas, s'il existe $a\in\mathbb{Z}$, qui soit racine primitive pour un ensemble de nombres premiers de densité (relative) inférieure positive.

III.- Théorème de Brun-Titchmarsh

Pour étudier $\pi(x;q,a)$, avec $(a,q)=1$, on peut aussi travailler avec les formules de crible. Ainsi, pour

$$\mathcal{A}=\mathcal{A}^{(q)} \ , \ \mathcal{P}=\mathcal{P}^{(q)}=\{p \ ; \ p\nmid q\} \ , \ X = xq^{-1} \ , \ \omega(p)= 1$$

et la majoration triviale

$$|r(\mathcal{A}^{(q)},d)|\leqslant 1$$

on parvient à la formule ([12]) :

$$\pi(x;q,a) \leqslant \frac{(2+\varepsilon)x}{\varphi(q)\ \log(x/q)} \qquad \text{pour} \quad x>x_0(\varepsilon) \quad \text{et} \quad q\leqslant x/2 \ .$$

Cette majoration, plutôt grossière a été notablement améliorée en particulier par l'emploi de (1.3) au lieu de (1.2) (se reporter à l'introduction de [19] pour une présentation de ces résultats) et entre dans le cadre du théorème de Brun-Titchmarsh.

On peut aussi regarder le théorème de Brun-Titchmarsh en moyenne, plus précisément considérer le problème suivant :

Chercher les fonctions $C(t)$ *définies et continues par morceaux sur* $[0,1[$ *ayant la propriété suivante :*

$$\forall \varepsilon>0\ ,\ \forall A\ ,\ \exists x_0(\varepsilon,A),\ \forall t\in[0,1-\varepsilon],\ \forall x>x_0(\varepsilon,A)$$

on a l'inégalité

$$\pi(x;q,1) \leqslant (C(t)+\varepsilon)\ \frac{x}{\varphi(q)\ \log x} \tag{3.1}$$

pour tout q *de l'intervalle* $[x^t,2x^t]$ *avec au plus* $x^t(\log x)^{-A}$ *exceptions.*

(Pour simplifier on s'est restreint à $a=1$.) Pour ce problème, on cherche donc D , le plus grand possible, tel que le terme d'erreur de (1.3) soit "presque toujours petit", ce qui se traduit par l'estimation

$$\sum_{Q\leqslant q\leqslant 2Q}\ \gamma_q \sum_{\substack{d<D\\(d,q)=1}} \lambda_d^+\ r(\mathcal{A}^{(q)},d) = O_B(x(\log x)^{-B}) \tag{3.2}$$

avec B quelconque, $Q=x^t$ et γ_q une suite quelconque vérifiant $|\gamma_q|\leqslant 1$. La relation (3.2) se ramène à des relations de la forme

$$\forall B \sum_{d<D} \lambda_d^+\ \Delta((\gamma_q),(1)\ ;\ x,xQ^{-1},d,-1) = O_B(x(\log x)^{-B})$$

et le lemme 2 affirme que cette relation est vraie pour

$$D=x^{\theta_1(1-t)-\varepsilon}\ .$$

Finalement, en remarquant que le théorème de Bombieri-Vinogradov donne, pour $t<1/2$, la valeur conjecturée $C(t)=1$, on a

THÉORÈME 3 ([5],[7]).- *Soit* $\delta_0<1/2$, *alors la fonction* $C(t)$ *définie par*

$$C(t) = \begin{cases} 1 & \text{si } t\leqslant\delta_0 \\ 2/\theta_1(1-t) & \text{si } \delta_0<t<1 \end{cases} \qquad \text{vérifie (3.1) .}$$

Une application du théorème de Brun-Titchmarsch en moyenne est la recherche des $p-1$ avec un très grand facteur premier. Par la technique de Tchebyshev-Hooley, on montre, en posant $P^+(n)=\max\{p\ ;\ p|n\}$, que si $C(t)$ est une fonction vérifiant (3.1), on a :

$$\forall\varepsilon>0 \quad \exists x_0(\varepsilon) \quad \exists c_2(\varepsilon)>0$$
$$x>x_0(\varepsilon) \Rightarrow |\{p\ :\ p\leqslant x\ P^+(p-1)\geqslant x^{\delta-\varepsilon}\}| \geqslant c_2 x\log^{-1}x \tag{3.3}$$

où δ est défini par l'égalité : $\int_0^{\delta} C(t)dt=1$. Ainsi le théorème conduit à $\delta=0,65998$.

1) Amélioration du théorème 2

Une étude soigneuse de la formule (1.3) montre que le crible ignore un cetain nombre de termes, dont on peut tenir compte dans le cas particulier du criblage de $\mathcal{A}^{(q)}$. Il apparaît alors plus économique tout en s'inspirant de la démonstration de (1.3), de travailler avec l'identité de Buchstab itérée. On utilise, entre autres, le lemme suivant :

LEMME 3 ([3],[6]).- *Sous les conditions* (2.3) *et* (2.4), *on a, pour tout* $\varepsilon>0$, tout A , tout υ $(\varepsilon\leqslant\upsilon\leqslant 1-\varepsilon)$, *tout* $x\geqslant 2$ *et tout entier* a , *la relation*

$$\sum_{\substack{(q,a)=1\\ q\leqslant x^{\vartheta_2(\upsilon)-\varepsilon}}} |\Delta(\ldots)| = O_A(x(\log x)^{-A})$$

avec

$$\vartheta_2(t) = \begin{cases} \frac{1}{2}+\frac{t}{2} & \text{pour } 0\leqslant t\leqslant \frac{1}{10} \\ \frac{5}{8}-\frac{3}{4}t & \text{pour } \frac{1}{10}\leqslant t\leqslant \frac{1}{6} \\ \frac{1}{2} & \text{pour } \frac{1}{6}\leqslant t\leqslant 1 \ . \end{cases}$$

Ce lemme a une démonstration proche de celle du lemme 1 ; en comparant les valeurs de $\vartheta(t)$ et $\vartheta_2(t)$, on se convainc de la difficulté d'améliorer le théorème de Bombieri-Vinogradov avec des valeurs absolues.

Des arguments combinatoires assez compliqués permettent d'améliorer la fonction $C(t)$ du théorème 2 pour $1/2\leqslant t\leqslant 3/5$ ([7]), en particulier $C(1/2)$ voit sa valeur passer de 2,67 à 1,73 , et on montre que (3.3) est vraie pour $\delta=\delta_1=0,6687$. Cette dernière relation a eu un regain d'importance, lorsque Adleman et Heath-Brown ont établi un lien entre une relation de la forme (3.3) avec $\delta>2/3$ et le premier cas du théorème de Fermat (FLT 1). On a :

THÉORÈME 4 ([1],[7]).- *Il existe* $c_3>0$, *tel que pour* x *suffisamment grand, on ait*

$$\sum_{x^{\delta_1} \leqslant p \leqslant x} \frac{1}{p} \geqslant c_3 .$$

FLT 1 vrai pour l'exposant p.

Ainsi le premier cas du théorème de Fermat est vrai pour une infinité d'exposants premiers (voir [23] pour une présentation des différents critères sur FLT 1).

2) La fonction $\pi(x;q,1)$ pour q autour de $\sqrt{x}$

On a, dans [7], contourné le phénomène de parité pour presque tout q, puisque $C(t)<2$ pour $t=1/2$. Il est naturel de se demander : jusqu'à quelle valeur peut-on descendre ? Qu'en est-il de la minoration de $\pi(x;q,1)$?
Rousselet a donc poursuivi les arguments de [7] en y incorporant un nouvel ingrédient :

LEMME 4 ([10]).- *Pour tout* $\varepsilon>0$, *tout* Δ $(0<\Delta\leqslant 1)$, *tout* $q\geqslant 1$, *tout entier* a *premier avec* q *et tous les* $M_i\geqslant 1$ $(1\leqslant i\leqslant 3)$, *on a*

$$\sum_{\substack{m_1m_2m_3\equiv a[q] \\ M_i\leqslant m_i<M_i(1+\Delta)}} 1 = \frac{1}{\varphi(q)} \sum_{\substack{(m_1m_2m_3,q)=1 \\ M_i\leqslant m_i<M_i(1+\Delta)}} 1 + O_\varepsilon\left((M_1M_2M_3)^{46/75+\varepsilon}\, q^{-7/30}\right) .$$

La démonstration de Friedlander et Iwaniec combine la méthode de Burgess et la majoration des sommes de Kloosterman de dimension 2, conséquence de la résolution par Deligne de la conjecture de Weil. Le lemme 4 conduit à une formule asymptotique de la somme

$$\sum_{\substack{n\leqslant x \\ n\equiv a[q]}} \tau_3(n)$$

pour $q\leqslant x^{1/2+1/230-\varepsilon}$, récemment Heath-Brown a élargi cette zone, par une méthode un peu différente ([13]).
Rousselet a démontré :

THÉORÈME 5 ([24]).- *Pour tout* $A>0$ *, pour tout* t *inférieur à* $1/2 + 10^{-100}$, *il existe* $x_0(A)$, *tel que pour* x *supérieur à* $x_0(A)$, *on ait les inégalités :*

$$0,85 \frac{x}{\varphi(q) \log x} \leqslant \pi(x ; q,1) \leqslant 1,48 \frac{x}{\varphi(q) \log x}$$

pour tout q *de* $[x^t, 2x^t]$ *avec au plus* $x^t(\log x)^{-A}$ *exceptions.*

La minoration est assez proche de la valeur conjecturée, et sa démonstration profite au maximum des propriétés de décomposition des variables rencontrées, pour appliquer les lemmes 1,2,3 ou 4. Une application de cette minoration est :

COROLLAIRE 4 ([24]).- *Une infinité de nombres premiers* p *vérifie* $P^+(p-1) < p^{0,316}$.

Le problème de trouver $p-1$ avec uniquement des petits facteurs premiers, fut abordé par Pomerance ([22]) et Balog ([2]), ce dernier obtint pour exposant $0,35$, dans l'inégalité précédente.

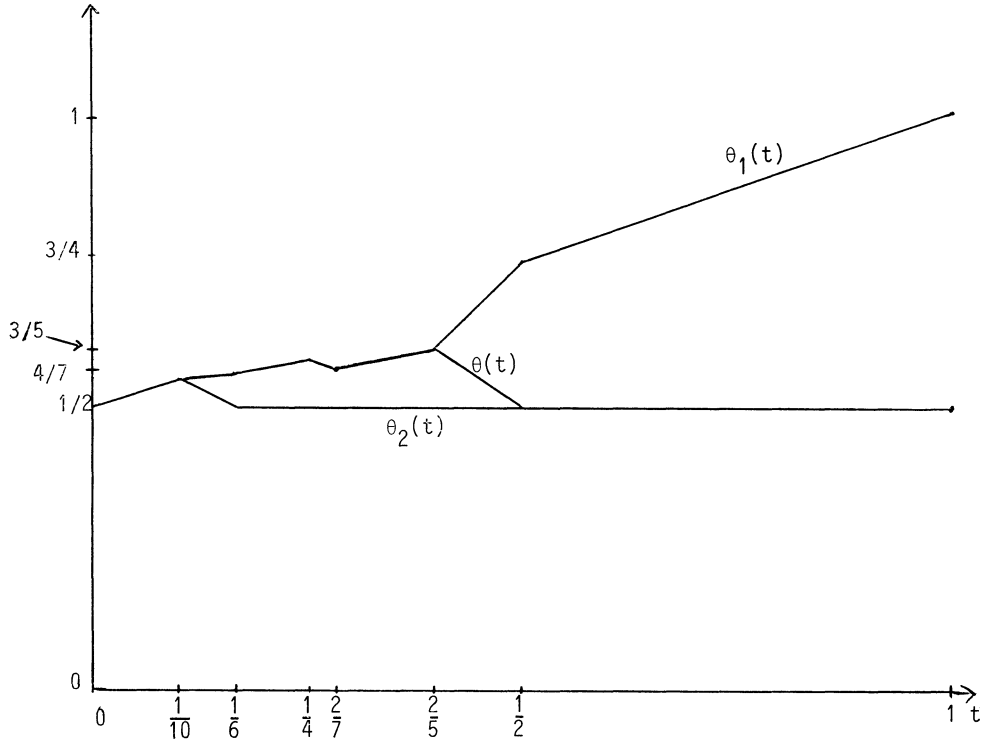
1
3/4
3/5
4/7
1/2
0
$\theta_1(t)$
$\theta(t)$
$\theta_2(t)$
0
$\frac{1}{10}$
$\frac{1}{6}$
$\frac{1}{4}$
$\frac{2}{7}$
$\frac{2}{5}$
$\frac{1}{2}$
1
t

Figure.

BIBLIOGRAPHIE

[1] L. M. ADLEMAN and D.R. HEATH-BROWN, *The first case of Fermat's Last Theorem*, Invent. Math. 79 (1985), 408-413.

[2] A. BALOG, p+a *without large prime factors*, Séminaire de Théorie des Nombres de Bordeaux (1983-1984), exposé n°31.

[3] E. BOMBIERI, J. FRIEDLANDER and H. IWANIEC, *Primes in arithmetic progressions to large moduli*, Acta Math. (à paraître).

[4] J.-M. DESHOUILLERS and H. IWANIEC, *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. Math. 70 (1982), 219-288.

[5] J.-M. DESHOUILLERS and H. IWANIEC, *On the Brun-Titchmarsh Theorem on average*, Topics in classical number theory-János Bolyai Mathematical Society (1984), vol. 1, 319-333.

[6] E. FOUVRY, *Autour du théorème de Bombieri-Vinogradov*, Acta Math. (1984), 219-244.

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

[8] E. FOUVRY and F. GRUPP, *On the switching principle in sieve theory*, J. reine angew. Math. (à paraître).

[9] E. FOUVRY and H. IWANIEC, *Primes in arithmetic progressions*, Acta Arith. 42 (1983), 197-218.

[10] J. FRIEDLANDER and H. IWANIEC, *Incomplete Kloosterman sums and a divisor problem*, Annals of Math. 121 (1985), 319-350.

[11] R. GUPTA and M. RAM MURTY, *A remark on Artin's conjecture*, Inv. Math. 78 (1984), 127-130.

[12] H. HALBERSTAM and H.-E. RICHERT, *Sieve Methods*, Academic Press, London 1974.

[13] D. R. HEATH-BROWN, *The divisor function* $d_3(n)$ *in arithmetic progressions*, Acta Arith. (à paraître).

[14] D. R. HEATH-BROWN, *Artin's conjecture for primitive roots* (à paraître).

[15] C. HOOLEY, *On Artin's conjecture*, J. reine angew. Math. 226 (1967), 209-220.

[16] M. N. HUXLEY, *Small differences between consecutive primes* II, Mathematika 24 (1977), 142-152.

[17] M. N. HUXLEY, *An application of the Fouvry-Iwaniec theorem*, Acta Arith. 43 (1984), 441-443.

[18] H. IWANIEC, *A new form of the error term in the linear sieve*, Acta Arith. 37 (1980), 307-321.

[19] H. IWANIEC, *On the Brun-Titchmarsh Theorem*, J. Math. Soc. of Japan 34 (1982), 95-123.

[20] H. MAIER, *Small differences between primes numbers* (à paraître).

[21] C. D. PAN, *A new mean value theorem and its applications*, Recent progress in analytic number theory, vol.1, 257-287, Academic Press, London 1981.

[22] C. POMERANCE, *Popular values of Euler's function*, Mathematika 27 (1980), 84-89.

[23] P. RIBENBOIM, *13 lectures on Fermat's Last Theorem*, Berlin-Heidelberg-New York : Springer 1979.

[24] B. ROUSSELET, *Inégalités de type Brun-Titchmarsh en moyenne* (à paraître).

E. FOUVRY
U.A. 040226
U.E.R. de Mathématiques
Université de Bordeaux I
351, cours de la Libération
F - 33405 TALENCE CEDEX