Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Marc Deshouillers

Théorème de Miech sur les nombres presque-premiers dans les fonctions polynômes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, n° 2 (1966-1967), exp. n° 19, p. 1-13

<http://www.numdam.org/item?id=SDPP_1966-1967__8_2_A9_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
8e année, 1966/67, n° 19

24 avril 1967

THÉORÈME DE MIECH SUR LES NOMBRES PRESQUE-PREMIERS DANS LES FONCTIONS POLYNÔMES

par Jean-Marc DESHOUILLERS

1. Introduction du problème.

Le problème que nous nous proposons d'étudier est né d'une généralisation de l'hypothèse sur l'infinité des nombres premiers jumeaux ; cette hypothèse peut se formuler de la manière suivante : Soit P le polynôme de $\underset{\sim}{N}$ dans $\underset{\sim}{N}$, défini par $P(x) = x(x+2)$. Il existe une infinité d'entiers n tels que $P(n)$ ait au plus deux facteurs premiers.

Nous allons généraliser le problème de la manière suivante : Soit P une fonction polynôme de $\underset{\sim}{N}$ dans $\underset{\sim}{N}$; on cherche un nombre $\ell(P)$, le plus petit possible, tel qu'il existe une infinité d'entiers m tels que $\overline{v}(P(m)) \leqslant \ell(P)$, avec la notation suivante : soit $d = \prod_i P_i^{\alpha_i}$, alors

$$v(d) = \sum_i 1 , \qquad \overline{v}(d) = \sum_i \alpha_i .$$

Nous dirons alors que P engendre une famille infinie de nombres presque-premiers d'ordre $\ell(P)$.

Dans cette étude, nous allons considérer des polynômes "quadratfrei", c'est-à-dire admettant la décomposition en facteurs irréductibles suivante :

$$P = \prod_{i=1}^{k} P_i ,$$

avec :

$$i \neq j \implies (P_i , P_j) = 1 ,$$

$$\forall\, n \in \underset{\sim}{N} - \{1\} , \quad \exists\, x : \ P(x) \not\equiv 0[n] .$$

On notera h_i le degré de P_i, et h le degré de P.

Nous nous proposons de montrer le résultat suivant (MIECH [4]) ;

Tout polynôme P "quadratfrei" engendre une famille infinie de nombres presque-premiers d'ordre

$$\sum_{i=1}^{k} [9h_i/5] + \left[k \sum_{j=1}^{k} \frac{1}{j} + k \log \frac{5}{2}\right] .$$

Nous montrerons en fait un résultat plus précis, puisque nous aurons une minoration du nombre des entiers m inférieurs à N tels que $P(m)$ soit presque-premier de cet ordre.

2. Fil conducteur de la démonstration.

Notations :

$\omega(p)$ est le nombre d'entiers x compris entre 0 et $p-1$, tels que $P(x) \equiv 0[p]$

$$D = \prod_{\substack{p \leq z \\ \omega(p)>0}} p .$$

La méthode utilisée dans la démonstration sera la méthode du crible dûe à BRUN [1] et SELBERG [5]. Soient M_1 et T deux constantes ne dépendant que de P, nous allons définir une suite de nombres ρ_d tels que :

$$v((G(n) , D)) \leq T \implies \sum_{d|(G(n),D)} \rho_d \leq M_1 ,$$

$$v((G(n) , D)) > T \implies \sum_{d|(G(n),D)} \rho_d \leq 0 .$$

Soit alors $\Phi_0(N)$ le nombre des entiers n ne dépassant pas N tels que $G(n)$ n'ait pas plus de T facteurs premiers inférieurs ou égaux à z, nous aurons :

$$M_1 \, \Phi_0(N) \geq N \sum_{d|D} \frac{\rho_d \, \omega(d)}{d} + O\Big(\sum_{d|D} |\rho_d \, R_d| \Big) .$$

Au § 3, nous nous occuperons de définir les ρ_d en fonction d'autres suites, selon l'idée de SELBERG (cf. [5], [6]).

Au § 4, nous modifierons l'expression $\sum_{d|D} \rho_d / f(d)$ par des voies arithmétiques pour la minorer par une expression ne contenant que des termes du type $\sum_{r \leq u} \frac{\mu^2(r)}{f'(r)}$ ou $\sum_{d \leq v} \frac{1}{f(d)}$, f' étant liée à f par la relation $f(n) = \sum_{\sigma|n} f'(\sigma)$. Dans cette partie, comme dans la suite, nous nous bornerons aux d tels que $v(d) = \overline{v}(d)$.

Au § 5, nous procéderons à l'évaluation asymptotique des deux sommes définies ci-dessus. Le lemme fondamental sera le résultat suivant (MANN [3]) :

Soit $\mathbb{Q}(\theta)$ le corps engendré par la relation $P(\theta) = 0$. Alors, pour tous les nombres premiers, sauf un nombre fini, $\omega(p)$ est le nombre d'idéaux premiers du premier degré (sur $\mathbb{Q}(\theta)$) contenant p.

Mais ces nombres d'idéaux premiers représentent les coefficients de la fonction zêta du corps $\mathbb{Q}(\theta)$. L'utilisation d'un théorème, dû à WEBER (cité en [2]), sur la somme des coefficients de la fonction zêta nous conduira à l'approximation recherchée :

$$\sum_{d|D} \rho_d/f(d) \geq C/(\log z)^k ,$$

où C est une constante ne dépendant que de P .

Dans le § 6, nous nous occuperons du terme erreur $O(\sum_{d|D} |\rho_d R_d|)$, en montrant que c'est un $O(z^t)$ avec $0 < t < 1$, tandis que dans le § 7, nous exploiterons l'inégalité obtenue :

$$M_1 \Phi_0(N) \geq CN/(\log N)^k + O(N^{1-w}) , \quad (0 < w < 1) ,$$

en montrant qu'elle subsiste si l'on abandonne l'hypothèse $v(d) = \overline{v}(d)$ (i. e. d. d est quadratfrei) que nous avions envisagée dans les § 4 à § 6.

3. Détermination des ρ_d .

La suite des ρ_d sera définie en fonction des trois suites γ_a , λ_b , y_r astreintes à satisfaire les conditions suivantes :

(i) $\gamma_a = 0$, si $\mu(a) = 0$ ou si $a > z$;

(ii) $\lambda_b = 0$, si $\mu(b) = 0$ ou si $b > z^\alpha$ ($0 < \alpha < 1$ sera déterminé par la suite) ;

(iii) $A = \sum_{r \leq z^\alpha} \mu(r)\, y_r \neq 0$, si $z > 1$;

(iv) $|\frac{\lambda_1}{A}| = 1$ et $v(d)$ borné $\Longrightarrow$ $|\frac{\lambda_\alpha}{A}| \leq M_2$.

On définit alors

$$\rho_d = \sum_{[a,b,c]=d} \gamma_a \frac{\lambda_b}{A} \frac{\lambda_c}{A} ,$$

ce qui implique

$$\sum_{d|m} \rho_d = (\sum_{d|m} \gamma_a)(\sum_{b|m} \frac{\lambda_b}{A})^2 .$$

Soient T un réel positif, et ε un réel positif inférieur à 1 , qui seront déterminés plus tard. On pose :

$\gamma_a = 0$, si a n'est pas premier, ou si $a > z$,

$\gamma_1 = T$,

$\gamma_p = -T$, si $p \leqslant z^\varepsilon$,

$\gamma_p = -1$, si $z^\varepsilon < p \leqslant z$.

Alors

$$\sum_{d|m} \rho_d = (T - \sum_{\substack{p|m \\ p\leqslant z^\varepsilon}} T - \sum_{\substack{p|m \\ z^\varepsilon<p\leqslant z}} 1)(\sum_{\substack{b|m \\ b\leqslant z^\alpha}} \frac{\lambda_b}{A})^2 .$$

D'après l'axiome (iv), on voit qu'il existe M_3 tel que :

$0 \leqslant \sum_{d|m} \rho_d \leqslant M_3$, si m n'a pas plus de $[T]$ facteurs premiers entre z^ε et z et aucun inférieur à z^ε ; nous dirons alors que m possède la propriété $(\mathcal{P})$;

$\sum_{d|m} \rho_d \leqslant 0$, dans tous les autres cas.

Soit alors $\Phi(N)$ le nombre des entiers n inférieurs ou égaux à N tels que $(G(n) , D)$ possède la propriété $(\mathcal{P})$:

$$M_3\, \Phi(N) \geqslant M_3 \sum_{\substack{n\leqslant N \\ (G(n),D)\in \mathfrak{p}}} 1 \geqslant \sum_{n\leqslant N} \sum_{d|(G(n),D)} \rho_d .$$

Si l'on pose $f(d) = \frac{d}{\omega(d)}$, on obtient une fonction faiblement multiplicative telle que

$$M_3\, \Phi(N) \geqslant N \sum_{d|D} \rho_d/f(d) + O(\sum_{d|D} |\rho_d\, R_d|) , \qquad \text{avec } |R_d| < \omega(d) .$$

4. Minoration de l'expression $\sum_{d|D} \rho_d/f(d)$.

Dans ce paragraphe, de même que dans les paragraphes 5 et 6, nous nous bornerons à considérer des entiers sans carré. Lorsqu'une sommation sera étendue à de tels entiers, nous remplacerons le signe de sommation Σ par le signe Σ' .

LEMME 4.1. - Soit $f_a(d) = f(d/(a , d))$,

$$1/f([a , b , c]) = (f_a((b , c)))/(f(a)\, f_a(b)\, f_a(c)) .$$

Il suffit d'écrire la relation sous la forme

$$f(a)\, f(b/(a , b))\, f(c/(a , c)) = f([a , b , c])\, f((b , c)/(a , b , c)) ,$$

et d'utiliser le fait que a , b , c sont quadratfrei, et que f est faiblement multiplicative.

LEMME 4.2. - On définit les fonctions $f'(n)$ et $f'_a(n)$ par les relations

$$f(n) = \sum_{\sigma|n} f'(\sigma) \qquad \text{et} \qquad f_a(n) = \sum_{\sigma|n} f'_a(\sigma) \ .$$

En appliquant la formule d'inversion de Möbius qui donne f' en fonction de f, on trouve

$$f'_a(n) = \begin{cases} f'(n) & \text{si } (n\ ,\ a) = 1\ , \\ 0 & \text{si } (n\ ,\ a) > 1\ . \end{cases}$$

LEMME 4.3. - Soit

$$y_r = \sum_{d \leqslant z^\alpha}{}' \frac{\lambda_d}{f(d)} \ .$$

Alors

$$\sum_{d|D} \rho_d/f(d) = \frac{1}{A^2}\Big(\gamma_1 \sum_{r \leqslant z^\alpha}{}' f'(r)\ y_r^2 + \sum_{p \leqslant z}{}' \frac{\gamma_p}{f(p)} \sum_{\substack{r \leqslant z^\alpha \\ (r,p)=1}}{}' f'(r)\ (y_r + f'(p)\ y_{pr})^2\Big) \ .$$

En effet, si on applique le lemme 4.1 à la définition des ρ_d, on trouve

$$\sum_{d|D} \rho_d/f(d) = \frac{1}{A^2} \sum_{\substack{a \leqslant z \\ b,c \leqslant z^\alpha}}{}' \frac{\lambda_a}{f(a)} \frac{\lambda_b}{f_a(b)} \frac{\lambda_c}{f_a(c)} f_a((b\ ,\ c)) \ .$$

Alors on remplace $f_a((b\ ,\ c))$ par $\sum_{r|(b,c)}{}' f'_a(r)$, puis on utilise le lemme 4.2 pour exprimer $f'_a(r)$.

LEMME 4.4. - $y_r = \sum_{d \leqslant z^\alpha}{}' \lambda_d/f(d) \iff \lambda_d/f(d) = \sum_{rd \leqslant z^\alpha} \mu(r)\ y_{rd}$.

Il suffit de remplacer dans le premier terme les $\lambda_d/f(d)$ par la valeur qu'ils ont dans le second terme, et réciproquement pour les y_r.

Choix des y_r :

$$r > z^\alpha \implies y_r = 0\ ,$$

$$r \leqslant z^\alpha \implies \begin{cases} y_r = 0 & \text{si } \omega(r) = 0\ , \\ y_r = \mu(r)/f'(r) & \text{si } \omega(r) \neq 0\ . \end{cases}$$

Ce choix détermine la connaissance, non seulement des y_r, mais également de A et de la suite λ. Il faut donc vérifier que les conditions (ii), (iii) et (iv) sont satisfaites.

(ii) Si $b > z^\alpha$, $\lambda_b/f(b) = 0$ donc $\lambda_b = 0$;

Si $b \leqslant z^\alpha$, et $\mu(b) = 0$,

$$\lambda_b = f(b) \sum_{rb \leqslant z^\alpha} (\mu(r)\ \mu(rb))/f'(r) .$$

Mais $\mu(b) = 0 \implies \mu(rb) = 0$. Donc $\lambda_b = 0$.

(iii) $A = \sum_{r \leqslant z^\alpha} \mu(r)\ y_r = \sum_{r \leqslant z^\alpha} \mu(r)^2/f'(r) > 0$ (La formule d'inversion de Möbius entraîne que $\forall\ n :\ f(n) \geqslant 0 \implies \forall\ \sigma :\ f'(\sigma) \geqslant 0$.)

(iv) $\lambda_1 = \sum_{rd \leqslant z^\alpha} \mu(r)\ y_r = A$.

$$\frac{\lambda_d}{A} = f(d)\ \Big(\sum_{rd \leqslant z^\alpha} \mu(r)\ y_{rd}\Big)/\Big(\sum_{rd \leqslant z^\alpha} \mu(r)\ y_r\Big) .$$

Au numérateur, on se borne à $(r\ ,\ d) = 1$, car

$$(r\ ,\ d) > 1 \implies \mu(rd) = 0 \implies y_{rd} = 0 .$$

Alors on utilisera le fait que f' est faiblement multiplicative,

$$\Big|\frac{\lambda_d}{A}\Big| = f(d)\ \Big|\frac{\mu(d)}{f'(d)}\Big|\ \Big|\Big(\sum_{\substack{rd \leqslant z^\alpha \\ (r,d)=1}} (\mu(r))^2/f'(r)\Big)/\Big(\sum_{rd \leqslant z^\alpha} (\mu(r))^2/f'(r)\Big)\Big| ,$$

$$\Big|\frac{\lambda_d}{A}\Big| \leqslant \frac{f(d)}{f'(d)} .$$

Mais la formule d'inversion de Möbius s'écrit $f'(d) = f(d) \prod_{p|n} \Big(1 - \frac{1}{f(p)}\Big)$. Soit

$$\frac{f(d)}{f'(d)} = \prod_{p|n} \Big(\frac{p}{p - \omega(p)}\Big) = \prod_{\substack{p|n \\ p \leqslant h}} \Big(\frac{p}{p - \omega(p)}\Big) \prod_{\substack{p|n \\ p > h}} \Big(\frac{p}{p - \omega(p)}\Big) ,$$

$$\frac{f(d)}{f'(d)} \leqslant h!\ (h + 1)^{\nu(n)} ,$$

expression bornée si $\nu(n)$ est bornée.

<u>Expression de</u> $\sum_{d|D} \frac{\rho_d}{f(d)}$: On part de l'expression fournie par le lemme 4.3, et on remplace $y_r + f'(p)\ y_{pr}$ par sa valeur, c'est-à-dire

$$y_r + f'(p)\ y_{pr} = \begin{cases} 0 & \text{si } rp > z^\alpha , \\ \dfrac{\mu(r)}{f'(r)} & \text{si } rp \leqslant z^\alpha . \end{cases}$$

Ce qui nous conduit à

$$\sum_{d|D} \frac{\rho_d}{f(d)} = \frac{1}{A^2}\Big(\gamma_1 \sum_{r\leqslant z^\alpha}{}' \frac{\mu^2(r)}{f'(r)} + \sum_{p\leqslant z}{}' \frac{\gamma_p}{f(p)} \sum_{\substack{z^\alpha/p\leqslant r\leqslant z^\alpha \\ (r,p)=1}} \frac{\mu^2(r)}{f'(r)}\Big) .$$

Mais les γ_p étant non-positifs, on peut laisser la condition $(r , p) = 1$ en remplaçant l'égalité par une inégalité

$$\sum_{d|D} \frac{\rho_d}{f(d)} \geqslant \frac{R}{A^2} = \frac{1}{A^2}\Big(T \sum_{r\leqslant z^\alpha}{}' \frac{\mu^2(r)}{f'(r)} + \sum_{p\leqslant z}{}' \frac{\gamma_p}{f(p)} \sum_{z^\alpha/p\leqslant r\leqslant z^\alpha}{}' \frac{\mu^2(r)}{f'(r)}\Big) .$$

5. Calcul de R .

Pour calculer R , il nous faut calculer les sommes du type

$$\sum_{r\leqslant z}{}' \frac{\mu^2(r)}{f'(r)} \qquad \text{et} \qquad \sum_{p\leqslant z}{}' \frac{1}{f(p)} .$$

On pose alors

$$a_n = \frac{\mu^2(n)}{f'(n)}\, n ,$$

et on considère la série de Dirichlet $\sum' \frac{a_n}{n^s}$. Des propriétés de cette série, on va déduire une expression asymptotique de la somme

$$\sum_{n\leqslant x}{}' a_n = \sum_{n\leqslant x}{}' \frac{\mu^2(n)}{f'(n)}\, n .$$

On en déduira alors $\sum_{n\leqslant x}{}' \frac{\mu^2(n)}{f'(n)}$ par la relation

$$\sum_{n\leqslant x}{}' \frac{a_n}{n} = \int_1^x \Big(\sum_{n\leqslant x}{}' a_n\Big) \frac{1}{u^2}\, du + \Big(\sum_{n\leqslant x} a_n\Big) \frac{1}{x} .$$

N.-B. - Dans le calcul de R , nous nous bornerons à considérer le cas où P est irréductible $(k = 1)$, le cas général se déduisant de celui-là par des intermèdes techniques sur les séries de Dirichlet, et l'algèbre combinatoire.

LEMME 5.1. - Soit

$$\sum_1^\infty \frac{a_n}{n^s} \equiv \Big(\sum_1^\infty \frac{b_n}{n^s}\Big)\Big(\sum_1^\infty \frac{c_n}{n^s}\Big) \qquad (s > 1) .$$

On suppose que $\sum_1^\infty \frac{b_n}{n^s}$ converge absolument pour $s > s_0$ $(0 < s_0 < 1)$, et que

$$\sum_{n\leq x} c_n = Cx + O(x^v) \qquad (s_0 < v < 1) ;$$

alors

$$\sum_{n\leq x} a_n = (\sum_1^\infty{}' \frac{b_n}{n^s})Cx + O(x^v) .$$

Pour calculer

$$B = \sum_1^\infty{}' \frac{\mu^2(n)}{n^{s-1} f'(n)} ,$$

on le met sous la forme

$$B = \prod_p{}' (1 + \frac{1}{p^{s-1} f'(p)}) = \prod_p (1 + \frac{\omega(p)}{p^{s-1}(p - \omega(p))}) (1 - \frac{1}{p^s})^{\omega(p)} \prod_p (1 - \frac{1}{p^s})^{-\omega(p)} ,$$

où le premier produit infini peut être considéré comme série de Dirichlet convergeant absolument pour $s > \frac{1}{2}$.

LEMME 5.2 ([3], p. 63, théorème 8.1). - Soit $\mathbb{Q}(\theta)$ le corps engendré par θ tel que $P(\theta) = 0$. Alors, pour tout nombre premier, $\omega(p)$ est le nombre d'idéaux premiers de $\mathfrak{a}(\theta)$ du premier degré contenant p .

LEMME 5.3. - Soit $\zeta(s)$ la fonction zêta du corps $\mathbb{Q}(\theta)$:

$$\prod_p (1 - \frac{1}{p^s})^{-\omega(p)} = H_1(s)\, \zeta(s) ,$$

où $H_1(s)$ est une série de Dirichlet convergeant absolument pour $s > \frac{1}{2}$.

LEMME 5.4 (WEBER) ([2], p. 81). - Soient a_n les coefficients de la série de ζ :

$$\zeta(s) = \sum_1^\infty \frac{a_n}{n^s} \qquad (s > 1) ;$$

alors

$$\sum_{n\leq x} a_n = Ax + O(x^v) , \qquad \text{avec} \quad v = 1 - \frac{1}{h} .$$

Des lemmes 1, 3, 4, on déduit :

$$\sum_{n\leq x}{}' \frac{\mu^2(n)\, n}{f'(n)} = Ex + O(x^v) , \qquad v = \sup(\tfrac{2}{3} , 1 - \tfrac{1}{h}) .$$

D'après la formule d'intégration citée ci-dessus, on a le lemme suivant :

LEMME 5.5.

$$\sum_{y<n\leq x}{}' \frac{\mu^2(n)}{f'(n)} = C(\log x - \log y) + O(x^{(v-1)} \log x) .$$

Occupons-nous maintenant de la somme $\sum_{p\leq x}{}' \frac{1}{f(p)}$. Nous utiliserons le résultat suivant dû à LANDAU ([2], p. 114-115 et p. 149-150) :

$$\sum_{N(\mathfrak{p})\leq x} 1/N(\mathfrak{p}) = \log\log x + B + O(1/\log x) ,$$

quand $\mathfrak{p}$ est un idéal premier dans l'anneau des entiers engendré par un zéro de P , et $N(\mathfrak{p})$ sa norme. Alors

$$\sum_{p\leq x}{}' \frac{1}{f(p)} = \sum_{p\leq x} \frac{\omega(p)}{p} = \log\log x + B + O(1/\log x) .$$

Nous pouvons maintenant calculer R .

LEMME 5.6. - Soit $\varepsilon = \beta\alpha$, avec $0 < \beta < 1$:

$$R = E\alpha \log z(T - (T-1)\beta - 1 - \log\tfrac{1}{\alpha}) + O(\log\log z) .$$

C'est maintenant que nous allons déterminer T . Nous imposons à α d'être rationnel, donc nous pouvons trouver η tel que $[1 + \log\frac{1}{\alpha} + \eta] = [1 + \log\frac{1}{\alpha}]$. Alors, on prend $T = 1 + \log\frac{1}{\alpha} + \eta$, puis on choisit β assez petit pour que $(T-1)\beta > \frac{\eta}{2}$. Alors

$$\sum_{d|D} \rho_d/f(d) \geq \frac{E\alpha \log z}{A^2} (\tfrac{\eta}{2} + O(\log\log z/\log z)) .$$

Mais

$$A = \sum_{r\leq z^{\alpha}}{}' \frac{\mu^2(r)}{f'(r)} = E\alpha \log z + O(z^{\alpha(v-1)} \log z) .$$

Donc

$$\sum_{d|D} \rho_d/f(d) \geq \frac{1}{E\alpha \log z} \frac{(\frac{\eta}{2} + O(\log\log z/\log z))}{(1 + O(z^{\alpha(v-1)}))} .$$

Donc il existe une constante C telle que, à partir d'un certain rang, on ait

$$\sum_{d|D} \rho_d/f(d) \geq C/\log z .$$

Cas général : Pour $k \neq 1$, le résultat est le suivant : on prend

$$T = k \sum_{1}^{k} \frac{1}{j} + k \log \frac{1}{\alpha} + \eta , \qquad \text{avec } [T] = [T - \eta] ,$$

et on trouve qu'il existe une constante C pour que l'on ait, à partir d'un certain rang,

$$\sum_{d|D} \rho_d / f(d) \geq C/(\log z)^k .$$

6. Le terme erreur.

Nous nous proposons de montrer dans ce paragraphe que,

$$\forall\ \varepsilon_1 > 0 , \qquad \sum_{d|D} |\rho_d R_d| = O(z^{(1+2\alpha)(1+\varepsilon_1)}) .$$

Soient h le degré de P , et d un nombre sans carré. On considère

$$A_d = \{p : p/d , p^{\varepsilon_1/2} \leq Q\} ,$$

$$B_d = \{p : p/d , p^{\varepsilon_1/2} > Q\} .$$

Alors

$$|R_d| \leq \omega(d) = \prod_{p \in A_d} \frac{\omega(p)}{p^{\varepsilon_1/2}} \prod_{p \in B_d} \frac{\omega(p)}{p^{\varepsilon_1/2}} d^{\varepsilon_1/2} = O(d^{\varepsilon_1/2}) ,$$

car $\omega(p) \leq h$. Donc

$$\sum_{d|D} |\rho_d R_d| = O\Big(\sum_{d|D} |\rho_d| z^{(1+2\alpha)\varepsilon_1/2} \Big) .$$

Mais

$$\sum_{d|D} |\rho_d| \leq \Big(\sum_{d \leq z} |\gamma_a| \Big) \Big(\sum_{b \leq z^\alpha} \frac{|\lambda_b|}{A} \Big)^2 .$$

Or

$$\sum_{d \leq z} |\gamma_a| = O(z(\log z)^{-1}) ,$$

par définition des γ_a .

$$\Big|\frac{\lambda_b}{A}\Big| \leq \prod_{p|d} (1 - \frac{\omega(p)}{p})^{-1} \leq \exp\Big(- \sum_{p \leq z^\alpha} \log(1 - \frac{\omega(p)}{p})\Big) = O(\log^k z) .$$

La première inégalité a été vue dans la vérification de (iv) (§ 4). D'où l'on déduit

$$\sum_{d|D} |\rho_d R_d| = O(z^{(1+2\alpha)(1+\varepsilon_1)}) .$$

7. Interprétation.

Nous venons de montrer qu'il existe C_1 :

$$\Phi(N) \geq C_1 N/\log^k z + O(z^{(1+2\alpha)(1+\varepsilon_1)}) .$$

On pose

$$B = \frac{1}{1+2\alpha} \frac{1-\varepsilon_1}{1+\varepsilon_1} \qquad \text{et} \qquad z = N^B .$$

Alors

$$\Phi(N) \geq C_1 N/(\log N)^k + O(N^{(1-\varepsilon_1)}) ,$$

donc il existe C_2 tel que, à partir d'un certain rang,

$$\Phi(N) > \frac{C_2 N}{(\log N)^k} .$$

Cela signifie qu'il y a plus de $C_2 N/(\log N)^k$ entiers n inférieurs à N tels que $P(n)$ n'ait pas de facteur premier plus petit que $N^{\beta\varepsilon}$ (on posera $\beta\varepsilon = \delta$), et au plus $[T]$ supérieurs à N^B .

Posons $\alpha = \frac{2}{5}$ ($\alpha \in \mathbb{Q}$ et $0 < \alpha < \frac{1}{2}$, ce qui était demandé), et déterminons ε_2 par $(1-\varepsilon_2) = (1-\varepsilon_1)(1+\varepsilon_1)^{-1}$. Dans ces conditions,

$$B = 5(1-\varepsilon_2)/9 .$$

Nous appellerons "petit premier", un premier p : $N^\delta < p < N^B$.
Nous appellerons "grand premier", un premier p : $p \geq N^B$.

LEMME 7.1. - Pour chaque P_i , $P_i(n)$ a au plus $[9h_i/5]$ grands premiers (chacun compté avec son ordre de multiplicité), si n est compté par Φ .

Puisque P_i est de degré h_i , $\exists\, B_i$ tel que

$$x \geq 1 \implies |P_i(x)| \leq B_i x^{h_i} .$$

Raisonnons par l'absurde en supposant que $P_i(n)$ ait $[9h_i/5] + 1$ ou plus de "grands" facteurs premiers. On aurait

$$B_i N^{h_i} > |P_i(m)| > (N^B)^{([9h_i/5]+1)} .$$

Soit

$$B_i N^{h_i} > N^{5(1-\varepsilon_2)([9h_i/5]+1)/9} .$$

ce qui est faux si $\varepsilon_2 < \dfrac{1 - \{9h_i/5\}}{1 + [9h_i/5]}$, par exemple $\varepsilon_2 = \frac{1}{5}\dfrac{1}{2h+1}$; on s'est donc fixé

$$B = 2(5h + 2)/9(2h + 1) .$$

En ce qui concerne les "petits" premiers, nous avons supposé, au début du paragraphe 4, qu'ils n'intervenaient jamais au carré. Nous allons montrer que cette hypothèse n'est pas gênante, plus précisément :

LEMME 7.2. - Le nombre des entiers m tels que $P(m)$ soit divisible par le carré d'un nombre premier compris entre N^δ et N^B est un $O(N^{1-\delta})$.

En effet, soit P' la dérivée de P ; alors

ou bien $\omega(p^2) = \omega(p)$,

ou bien $\begin{cases} P(x) \equiv 0[p] \\ P'(x) \equiv 0[p] \end{cases}$ admet une racine.

Mais P est "quadratfrei", donc, d'après BEZOUT, il existe trois entiers relatifs a , b , c tels que $aP + bP' = c$, ce qui implique que le nombre de facteurs communs à P et P' est borné, donc $\omega(p^2)$ est borné.

Le nombre des entiers $n \leqslant N$ satisfaisant $P(n) = 0[p^2]$ est inférieur à

$$\sum_{N^\delta \leqslant p \leqslant N^B} \left(\frac{N}{p^2}\omega(p^2) + R_{p^2}\right) , \qquad \text{avec } R_{p^2} \leqslant \omega(p^2) ,$$

donc inférieur à

$$2 \sum_{N^\delta \leqslant p \leqslant N^{\frac{1}{2}}} \left(\frac{N}{p^2}\omega(p^2)\right) + O\Big(\sum_{N^{\frac{1}{2}} \leqslant p \leqslant N^B} 1\Big) , \qquad \text{car } \omega(p^2) \text{ est borné ,}$$

c'est-à-dire un

$$O\left(N \int_{N^\delta}^{N^{\frac{1}{2}}} \frac{1}{x^2}\,dx\right) + O(N^{5/9}) , \qquad \text{car } B < \frac{5}{9} ,$$

donc un $O(N^{1-\delta})$.

La conclusion des paragraphes 5 et 6, les lemmes 7.1 et 7.2 nous conduisent au théorème suivant :

THÉORÈME de MIECH ([4]). - Soit P un polynôme "quadratfrei". Il existe deux réels δ et B avec $0 < \delta < B < 1$, et une constante C, tels que :

Il existe plus de $CN/(\log N)^k$ entiers $n \leq N$ tels que :

$P(n)$ n'ait aucun facteur premier inférieur à N^δ ;

$P(n)$ ait au plus $[k + \sum_1^k \frac{1}{j} + k \log \frac{5}{2}]$ facteurs premiers (chacun compté avec son ordre de multiplicité) compris entre N^δ et N^B ;

Chaque $P_i(n)$ ait au plus $[9h_i/5]$ diviseurs premiers (chacun compté avec son ordre de multiplicité) supérieur à N^B .

BIBLIOGRAPHIE

[1] BRUN (Viggo). - Le crible d'Eratosthène et le théorème de Goldbach, Norske Vidensk. Selsk., Kristiania, Skr., 1920, n° 3, 36 p.

[2] LANDAU (Edmund). - Über die zu einem algebraischen Zahlkörper gehörige Zetafunction und die Ausdehnung der Tschebyschefschen Primzahlentheorie auf das Problem der Vertheilung der Primideale, J. für reine und angew. Math., t. 125, 1903, p. 64-188.

[3] MANN (Henry B.). - Introduction to algebraic number theory. - Columbus, The Ohio State University Press, 1955 (Graduate School Studies. Mathematics Series, 1).

[4] MIECH (R. J.). - Almost primes generated by a polynomial, Acta Arithm. Warszawa, t. 10, 1964, p. 9-30.

[5] SELBERG (Atle). - On an elementary method in the theory of primes, Norske Vidensk. Selsk. Forhandl., Trondhjem, 19, 1947, n° 18, p. 64-67.

[6] TEISSIER (Bernard). - Crible de Brun, Séminaire Delange-Pisot-Poitou : Théorie des nombres, t. 7, 1965/66, n° 11, 13 p.