Groupe de travail d'analyse ultramétrique

François Gramain

Polynômes d'interpolation sur $\mathbb{Z}[i]$

Groupe de travail d'analyse ultramétrique, tome 6 (1978-1979), exp. n° 16, p. 1-13
<http://www.numdam.org/item?id=GAU_1978-1979__6__A10_0>

© Groupe de travail d'analyse ultramétrique
(Secrétariat mathématique, Paris), 1978-1979, tous droits réservés.

L'accès aux archives de la collection « Groupe de travail d'analyse ultramétrique » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
6e année, 1978/79, n° 16, 13 p.

19 mars 1979

POLYNÔMES D'INTERPOLATION SUR $\mathbb{Z}[i]$

(d'après L. GRUMAN [8])

par François GRAMAIN (*)
[Univ. P. et M. Curie (Paris-VI)]

0. Introduction.

Les problèmes relatifs aux séries d'interpolation sont d'un grand intérêt en théorie des nombres transcendants, et sont liés aux problèmes p-adiques des bases normales (cf. [2]). Par exemple, on sait que les polynômes binômiaux $\binom{x}{n}$ forment une base normale de l'espace des fonctions continues de $\mathbb{Z}_p$ dans $\mathbb{C}_p$. Ces polynômes permettent d'écrire (en complexe et en p-adique) la série d'interpolation de Newton. C'est ainsi que G. PÓLYA [12] montrait, en 1915, que si f est une fonction entière sur $\mathbb{C}$ de type exponentiel $< \log 2$ et telle que $f(\mathbb{N}) \subset \mathbb{Z}$, alors f est un polynôme. Ces polynômes, ou les

$$\Delta(x\ ,\ n) = \frac{x(x+1)\ \dots\ (x+n-1)}{n!}\ ,$$

sont aussi utilisés dans les constructions de fonctions auxiliaires, pour les démonstrations de transcendance ; les principales propriétés que l'on utilise étant qu'ils forment une base de l'espace des polynômes, qu'ils envoient $\mathbb{Z}$ dans $\mathbb{Z}$, et qu'ils croissent moins vite que x^n.

Quand on passe de $\mathbb{Z}$ ou $\mathbb{Z}_p$ à une extension algébrique finie K de $\mathbb{Q}$ ou de $\mathbb{Q}_p$, des difficultés apparaissent. Cependant, Yvette AMICE a montré [1] l'existence d'une base normale de la forme

$$\frac{(x-u_0)(x-u_1)\ \dots\ (x-u_{n-1})}{(u_n-u_0)(u_n-u_1)\ \dots\ (u_n-u_{n-1})}\ .$$

Mais sur l'anneau des entiers de K, les valeurs prises par ces polynômes ne sont entières que p-adiquement, alors que pour la transcendance, on a besoin de polynômes à valeurs entières. En particulier, dans le cas de $\mathbb{Q}(i)$ et de $\mathbb{Z}[i]$, HENSLEY [9] a montré qu'il n'existait pas de polynômes jouant le rôle des $\binom{x}{n}$. Là aussi, la série d'interpolation de Newton, qui fait intervenir les polynômes $\prod_{0\leq i\leq n}(z-\zeta_i)$, où les ζ_i sont les éléments de $\mathbb{Z}[i]$ ordonnés par module puis argument croissants, permet d'obtenir des résultats. Ainsi, en 1929, A. GEL'FOND montrait [5] que si f est une fonction entière sur $\mathbb{C}$ vérifiant

$$f(\mathbb{Z}[i]) \subset \mathbb{Z}[i] \quad \text{et} \quad \limsup_{r\to+\infty} \frac{\log|f|_r}{r^2} < \alpha\ ,$$

(*) Texte reçu le 28 mai 1979.
François GRAMAIN, Mathématiques, Tour 46, Université Pierre et Marie Curie, 4 place Jussieu, 75230 PARIS CEDEX 05.

avec α de l'ordre de 10^{-45}, alors f est un polynôme. Mais, si les polynômes binômiaux permettent de prouver le théorème de Pólya (à la valeur de la constante $\log 2$ près) par la méthode de transcendance de Schneider [14], on ne pouvait pas obtenir le résultat de Gel'fond par cette méthode en utilisant les polynômes z^n.

GRUMAN, lui, utilise les polynômes de Lagrange. Ils ne forment plus une base de l'espace des polynômes, mais sont liés à un ensemble fini, par exemple

$$S = \mathbb{Z}[i] \cap \overline{D}(0\ ,\ r)$$

et s'écrivent

$$\prod_{\zeta_i \in S, i \neq m} (z - \zeta_i)(\zeta_m - \zeta_i)^{-1} .$$

Ils ont tous le même degré $n = \mathrm{card}(S) - 1$, et forment une base de l'espace des polynômes de degré $\leq n$ (Dans le cas de $\mathbb{Z}$, leur analogue est $\binom{z-1}{i-1}\binom{z-i-1}{n-i}$, pour $0 \leq i \leq n$). D'autre part, ils n'envoient pas $\mathbb{Z}[i]$ dans lui-même, mais GRUMAN montre qu'ils ont un dénominateur commun pas trop grand, de l'ordre de $\exp(r^2)$ alors qu'on s'attendrait à $\exp(r^2 \log r)$.

Les majorations de Gruman améliorent celles de Gel'fond, donc son α. Mais GRUMAN utilise une généralisation de la transformation de Fourier-Borel qui lui permet d'obtenir un α encore meilleur, de l'ordre de 1/10. Cette méthode m'a permis de montrer la transcendance de $\exp(\pi)$ (connue depuis 1929 [6]) et, utilisant ses majorations, d'obtenir par une méthode différente une mesure de transcendance de $\exp(\pi)$ [7] du même genre que celle obtenue par J. F. KOSMA et J. POPKEN [11], en 1932.

Les polynômes de Lagrange-Gruman permettent d'utiliser la méthode de Schneider pour prouver le théorème de Gel'fond. Malheureusement, ils ne semblent pas permettre de prouver l'indépendance algébrique (conjecturale) de π et $\exp(\pi)$ ou d'améliorer la mesure d'irrationalité de $\exp \pi$ donnée par la méthode de Baker ([3], chap. 3).

1. Les polynômes de Lagrange-Gruman.

LEMME 1. - *Soit* D_j $(j = 1\ ,\ 2)$ *deux disques fermés de rayon* r. *Si*

$$A_j = \mathrm{card}(D_j \cap \mathbb{Z}[i]) ,$$

alors

$$|A_1 - A_2| \leq (2 + \sqrt{2})r + 2 .$$

Remarque. - En fait, on sait que $|A_1 - A_2|$ est un $O(r^{2/3})$ (cf. [4] et [10]) mais, pour la suite, on a besoin d'une majoration explicite.

Démonstration. - Soit $(x_j\ ,\ y_j)$ le centre de D_j. Par translation d'un vecteur de $\mathbb{Z}[i]$ et éventuellement des symétries par rapport à des droites parallèles aux

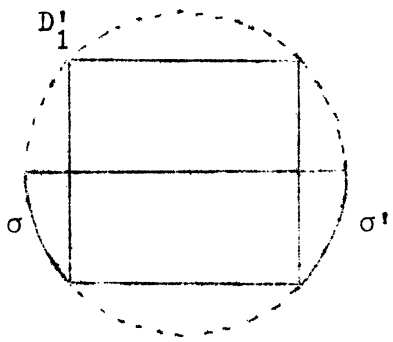
axes et de coordonnées demi-entières, on peut se ramener à

$$0 \leqslant \Delta x = x_2 - x_1 \leqslant \frac{1}{2} \quad \text{et} \quad 0 \leqslant \Delta y = y_2 - y_1 \leqslant \frac{1}{2} .$$

Soit $D_1' = D_1 + \Delta x$ le disque de centre (x_2 , y_1) et de rayon r. Le passage de D_1 à D_1' fait perdre au plus un point de $\mathbb{Z}[i]$ sur chaque droite d'équation $y = n \in \mathbb{Z}$ qui coupe D_1, donc au plus $2r + 1$ points. De même, le passage de D_1' à D_2 fait perdre au plus $2r + 1$ points et on a trivialement $|A_1 - A_2| \leqslant 4r + 2$. Pour raffiner ce résultat, notons S l'ensemble des droites d'équations $y = n$ coupant D_1 et sur lesquelles on ne perd aucun point en passant de D_1 à D_1', et $s = \text{card } S$. Soit G l'ensemble des droites d'équation $y = n$ sur lesquelles on gagne un point en passant de D_1 à D_1', et posons $g = \text{card } G$. Alors, avec des notations évidentes, on a

$$A_1' \geqslant A_1 - (2r + 1) + s + g .$$

Quitte à échanger x et y, on peut supposer $\Delta y \leqslant \Delta x$. Etudions le passage de D_1' à D_2. Soit σ le huitième de $\partial D_1'$ défini par



$$\sigma = \partial D_1' \cap \{x \leqslant x_2 - \frac{r}{\sqrt{2}} \; ; \; y \leqslant y_1\} .$$

Considérons les droites d'équations $x_2 - r \leqslant x = n \leqslant x_2 \frac{r}{\sqrt{2}}$. Si on perd un point (ξ , η) sur une de ces droites, c'est que sa distance "verticale" (distance comptée parallèlement à l'axe imaginaire) à σ est $< \Delta y \leqslant 1/2$. Mais, sa distance "horizontale" à σ est $\leqslant$ à sa distance "verticale", donc, comme $\Delta x \leqslant 1/2$, on n'avait pas perdu de point sur la droite $y = \eta$, en passant de D_1 à D_1', et $\{y=\eta\} \in S$. Par suite, sur ces droites, on perd au plus s points. Considérons maintenant les droites d'équations $x_2 + r/\sqrt{2} \leqslant x = n \leqslant x_2 + r$. Si on perd un point sur une de ces droites, c'est que Δy est supérieur à la distance "verticale" de ce point à $\sigma' = \partial D_1' \cap \{x \geqslant x_2 + r/\sqrt{2} \; ; \; y \leqslant y_1\}$; donc Δx est supérieur à la distance "horizontale" de ce point à σ', et ce point avait été gagné dans le passage de D_1 à D_1'. On perd donc au plus g points sur ces droites. Les autres droites "verticales" à considérer sont en nombre au plus $r\sqrt{2} + 1$. On obtient ainsi

$$A_2 \geqslant A_1' - r\sqrt{2} - 1 - s - g \geqslant A_1 - (2 + \sqrt{2})r - 2 .$$

On montre de manière analogue la même minoration pour $A_1 - A_2$ en utilisant le disque de centre (x_1 , y_2) et de rayon r.

C.Q.F.D.

LEMME 2. - <u>Soit</u>

$$A_0(r) = \text{card}(\overline{D}(0 , r) \cap \mathbb{Z}[i]) \quad \underline{\text{et}} \quad A(r) = \max_{z \in \mathbb{C}} \text{card}(\overline{D}(z , r) \cap \mathbb{Z}[i])$$

où $\overline{D}(z\ ,\ r)$ désigne le disque fermé de centre z et de rayon r. Le tableau suivant donne des majorations de A et A_0 en fonction de r (qui sont les meilleures possibles pour $r < \sqrt{17}/2$)

$r <$	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	1	$\frac{\sqrt{5}}{2}$	$\frac{5}{4}$	$\sqrt{2}$	$\sqrt{\frac{5}{2}}$	$\frac{13}{5\sqrt{2}}$	$\frac{\sqrt{65}}{3\sqrt{2}}$	2	$\frac{\sqrt{17}}{2}$
$A_0(r) \leqslant$	1	1	1	5	5	5	9	9	9	9	13
$A(r) \leqslant$	1	2	4	5	6	7	9	12	13	14	14

Démonstration. - Les majorations de $A_0(r)$ sont faciles à vérifier. Appelons configuration minimale de n points, un ensemble de n points de $\mathbb{Z}[i]$ contenu dans un disque fermé de rayon minimal, rayon que l'on notera $\rho(n)$.

Il est clair que $A(r) < n$ si, et seulement si, $r < \rho(n)$. On a évidemment $\rho(2) = 1/2$, et $\rho(3) = \rho(4) = 1/\sqrt{2}$. De plus, la distance minimale de deux points de $\mathbb{Z}[i]$ est 1, et chaque entier de Gauss a exactement quatre voisins, donc $\rho(5) = 1$.

Il existe une configuration de 9 points contenue dans $\overline{D}(0\ ,\ \sqrt{2})$ donc toute configuration minimale de 8 ou 9 points est contenue dans l'enveloppe convexe des disques fermés de rayon $\sqrt{2}$ et de centres 0, $\frac{i}{2}$, $\frac{1}{2}$ et $\frac{1+i}{2}$ (cf. la preuve du lemme 1). Or cette enveloppe convexe ne contient que les 9 points de $\mathbb{Z}[i]$ considérés au départ (figure 1), qui forment donc une configuration minimale. De plus, le cercle circonscrit à 8 de ces 9 points passe par trois sommets du carré, enveloppe convexe de ces 9 points, donc $\rho(8) = \rho(9) = \sqrt{2}$.

De même, une configuration minimale de 12 points est une partie de la configuration de 13 points de la figure 2, obtenue à partir du disque de centre $(1 + i)/2$ et de rayon $\sqrt{5/2}$. Si une telle configuration de 12 points contient le point 1, elle contient aussi le point 2 ou le point 3, et le rayon du cercle circonscrit est $\geqslant \sqrt{13}/2 > \sqrt{5/2}$, donc elle n'est pas minimale ; par suite la configuration des 12 points contenus dans le disque de départ est minimale, et $\rho(12) = \sqrt{5/2}$. De plus, cette configuration de 13 points contient aussi des configurations minimales de 10 et 11 points. Si ces dernières contiennent le point 1, elles contiennent nécessairement l'un des points 2, 3, 4 ou 5, et le rayon du cercle circonscrit est $\geqslant \sqrt{5/2}$. Si elles ne contiennent pas le point 1, elles contiennent deux points diamétralement opposés sur le cercle de départ (par exemple 2 et 6), et le rayon du cercle circonscrit est encore $\geqslant \sqrt{5/2}$. On a donc $\rho(10) = \rho(11) = \sqrt{5/2}$.

De même, le disque de centre $1/2$ et de rayon $\sqrt{17}/2$ contient 16 entiers de Gauss, donc des configurations minimales de 15 et 16 points sont contenues dans la

configuration de 19 points de la figure 3. Il s'agit de lui enlever 3 points. Mais les distances 1-4, 1-5 et 1-10 sont $\geq \sqrt{17}$. Donc, pour obtenir un rayon $< \sqrt{17}/2$, si l'on conserve le point 1, il faut exclure les points 4, 5 et 10, et alors il reste la distance 3-7 égale à $\sqrt{17}$. Par suite il faut enlever le point 1. De la même façon, si on conserve le point 2, il faut exclure 5 et 6 et alors la distance 4-8 est trop grande. Donc il faut exclure 1 et 2, alors il restera 4 et 8 ou 4 et 9 ou 3 et 7 ; la configuration de départ était donc minimale, et $\rho(16) = \sqrt{17}/2$.. Pour obtenir une configuration minimale de 15 points, il faut enlever 4 points de la configuration de la figure 3. Comme plus haut, si l'on conserve 1, il faut exclure 4, 5 et 10, mais il restera 3 et 7, ou 3 et 8, ou 1 et 10. Donc 1 est exclu. Si l'on conserve 2, il faut exclure 5 et 6. Alors si l'on conserve 3, il faut exclure 7 et 8 donc au total 5 points. Il faut donc exclure 3, mais alors il reste 4 et 8 et le rayon est trop grand. Il faut donc exclure 1 et 2. Alors, si l'on garde 3, il restera 3-7, 3-8 ou 4-9 qui sont de longueur $\sqrt{17}$. Il faut donc exclure 1, 2 et 3. Pour supprimer les segments 4-8 et 4-9, il faut exclure 4 et on obtient une configuration de 15 points dont le cercle circonscrit a pour rayon $3/\sqrt{2} > \sqrt{17}/2$. On a donc $\rho(15) = \rho(16) = \sqrt{17}/2$.

Un disque de rayon $\leq 5/4 < 3/2$ est contenu dans un carré de côtés parallèles aux axes et de côté < 3 . Un tel carré contient au plus 9 points et ils sont alors disposés comme sur la figure 4. Des configurations minimales de 6 et 7 points sont donc des parties de cette configuration de 9 points. Un disque de rayon $< \sqrt{2}$ ne peut contenir deux sommets opposés du carré circonscrit à ces 9 points, il contient donc au plus 7 entiers de Gauss qui forment la configuration minimale de la figure 5 et qui fournit $\rho(7) = 5/4$. D'autre part, $\rho(6) < \sqrt{2}$, et une configuration minimale de 6 points est une partie de la configuration de la figure 5. Par suite elle contient deux points distants de $\sqrt{5}$; or le disque de centre $i/2$ et de rayon $\sqrt{5}/2$ contient 6 entiers de Gauss, donc $\rho(6) = \sqrt{5}/2$ (figure 6).

De même, un disque de rayon < 2 est contenu dans un carré de côtés parallèles aux axes et de côté < 4 . Un tel carré contient au plus 16 entiers de Gauss (figure 7). Un disque de rayon < 2 ne peut pas contenir 2 sommets opposés du carré circonscrit à ces 16 points, donc une configuration minimale de 14 points est donnée par la figure 8, et $\rho(14) = \sqrt{65}/3\sqrt{2}$. Une configuration minimale de 13 points est obtenue pour un rayon < 2 , donc c'est une partie de la configuration minimale de 14 points, à laquelle il faut retirer un point. Si $\rho(13) < \rho(14)$, ce point est nécessairement situé sur le cercle circonscrit à la configuration minimale de 14 points, c'est-à-dire le cercle circonscrit au triangle 123 ou au triangle 124 (figure 8). Si l'on enlève le point 3 (ou 4), ce cercle reste inchangé, donc il faut enlever le point 1 (ou 2), et on obtient ainsi la configuration minimale de la figure 9 qui fournit $\rho(13) = 13/5\sqrt{2}$. Cela achève la justification du tableau.

C.Q.F.D.

On ordonne les entiers de Gauss par module puis argument croissants :

$$\zeta_0 = 0 \ , \quad \zeta_1 = 1 \ , \quad \zeta_2 = i \ , \quad \zeta_3 = -1 \ , \quad \zeta_4 = -i \ , \quad \zeta_5 = 1 + i \ , \ldots ,$$
$$|\zeta_{n_{k-1}+1}| = \ldots = |\zeta_{n_k}| = r_k \ ; \quad \ldots$$

On sait que $n_k = \pi r_k^2 + O(r_k)$ (voir la remarque à la suite du lemme 1. Dans ce cas particulier, on sait que $n_k - \pi r_k^2 \in O(r_k^{\alpha})$ avec $\alpha = \frac{24}{37} + \varepsilon$ (CHEN, 1963, et on conjecture $\alpha = \frac{1}{2} + \varepsilon$).

Les polynômes de Lagrange associés au disque de centre 0 et de rayon r_k sont les

$$\prod_{0 \leqslant n \leqslant n_k, n \neq m} (z - \zeta_n)(\zeta_m - \zeta_n)^{-1} \ .$$

Le lemme suivant majore leur dénominateur.

LEMME 3. - <u>Soit</u> β_k <u>le</u> p.p.c.m. (<u>dans</u> $\mathbb{Z}[i]$) <u>des</u> $\alpha_{m,k} = \prod_{0 \leqslant n \leqslant n_k, n \neq m} (\zeta_m - \zeta_n)$ <u>pour</u> $0 \leqslant m \leqslant n_k$. <u>Alors, il existe</u> $\gamma_k \in \mathbb{Z}[i]$ <u>tel que</u> β_k <u>divise</u> $\alpha_{0,k}\, \gamma_k$, <u>et vérifiant</u> $|\gamma_k| < \exp(4{,}88018 r_k^2)$ <u>pour</u> k <u>assez grand.</u>

<u>Remarque.</u> - Le k assez grand est effectif, et fourni par le théorème des nombres premiers.

<u>Démonstration.</u> - On a $|\zeta_n| \leqslant r_k$, donc $\zeta_m - \zeta_n \in \overline{D}(\zeta_m \ , \ r_k) \subset \overline{D}(0 \ , \ 2r_k)$. On peut donc écrire $\beta_k = \prod q^{v_q(\beta_k)}$, où q décrit l'ensemble des nombres premiers de $\mathbb{Z}[i]$ tels que $|q| \leqslant 2r_k$.

Posons

$$A(m \ , \ \ell \ , \ q) = \mathrm{card}\{\zeta \in \mathbb{Z}[i] \ ; \ \ \zeta \neq 0 \ , \ \ |q^{\ell}\zeta - \zeta_m| \leqslant r_k\} \ .$$

C'est le nombre des multiples non nuls de q^{ℓ} situés dans $\overline{D}(\zeta_m \ , \ r_k)$, et si $r = r_k/|q|$, on a

$$A(m \ , \ 1 \ , \ q) \leqslant A(r) - 1 \quad \text{et} \quad A(0 \ , \ 1 \ , \ q) = A_0(r) - 1 \ .$$

Si $|q| > 2r_k/\sqrt{17}$, et si de plus $|q|^2 > 2r_k$ (ce qui est vérifié dès que $4r_k^2 > 2.17 r_k$, donc pour k assez grand), on a

$$v_q(\alpha_{m,k}) \leqslant A(m \ , \ 1 \ , \ q) \ .$$

Pour $|q| \leqslant 2r_k/\sqrt{17}$, le lemme 1 montre que

$$A(m \ , \ \ell \ , \ q) \leqslant A(0 \ , \ \ell \ , \ q) + (2 + \sqrt{2}) r_k |q|^{-\ell} + 2 \ ;$$

et on a

$$A(0 \ , \ \ell \ , \ q) = A_0(r|q|^{-\ell}) - 1 \ .$$

De plus, si $\delta_q = [\log 2r_k/\log|q|]$, où $[x]$ désigne la partie entière de x , on a

$$v_q(\alpha_{m,k}) \leqslant \delta_q \, A(m,\delta_q,q) + (\delta_q - 1)[A(m,\delta_q - 1,q) - A(m,\delta_q,q)] + \ldots + 1[A(m,1,q) - A(m,2,q)]$$

c'est-à-dire

$$v_q(\alpha_{m,k}) \leqslant \Sigma_{1\leqslant \ell\leqslant \delta_q} A(m\ ,\ \ell\ ,\ q)\ .$$

D'après le lemme 2, il en résulte que β_k divise $\Pi_{1\leqslant j\leqslant 10} I_j$, où

$I_1 = \Pi_{|q|\leqslant r_k} q^{\Sigma_\ell A(0,\ell,q)}$, $I_2 = \Pi_{1/2\leqslant r<1/\sqrt{2}}\, q$, $I_3 = \Pi_{1/\sqrt{2}\leqslant r<1}\, q^3$,

$I_4 = \Pi_{\sqrt{5}/2\leqslant r<5/4}\, q$, $I_5 = \Pi_{5/4\leqslant r<\sqrt{2}}\, q^2$, $I_6 = \Pi_{\sqrt{5/2}\leqslant r<13/5\sqrt{2}}\, q^3$,

$I_7 = \Pi_{13/5\sqrt{2}\leqslant r<\sqrt{65}/3\sqrt{2}}\, q^4$, $I_8 = \Pi_{\sqrt{65}/3\sqrt{2}\leqslant r<2}\, q^5$, $I_9 = \Pi_{2\leqslant r<\sqrt{17}/2}\, q$,

$I_{10} = \Pi_{r\geqslant\sqrt{17}/2}\, q^{2\delta_q+(2+\sqrt{2})r_k\Sigma_\ell|q|^{-\ell}}$.

Mais $I_1 = \alpha_{0,k}$, donc $\gamma_k = \Pi_{j=2}^{10} I_j$ convient.

Pour majorer γ_k on utilise le théorème des nombres premiers. Si q est premier dans $\underset{\sim}{Z}[i]$, alors ou bien $q = 1 + i$ (à une unité près), ou bien $q \in \underset{\sim}{Z}$ et c'est un nombre premier de $\underset{\sim}{Z}$ congru à 3 modulo 4 , ou bien $q\bar{q} \in \underset{\sim}{Z}$ est premier dans $\underset{\sim}{Z}$, congru à 1 modulo 4 et q et $\bar{q}$ sont des premiers non associés dans $\underset{\sim}{Z}[i]$. Soit $\pi_1(x)$ (resp. $\pi_3(x)$) le nombre des nombres premiers de $\underset{\sim}{Z}$ congrus à 1 (resp. 3) modulo 4 et $\leqslant x$. Alors, au voisinage de l'infini on a $\pi_1(x) \sim \pi_3(x) \sim \frac{x}{2\log x}$. Alors on a

$$\log|I_2| \leqslant (\pi_3(2r_k) + 2\pi_1(4r_k^2) - 2\pi_1(2r_k^2))\log(2r_k) \leqslant (1+\varepsilon)r_k^2\ .$$

De la même façon, on a

$$\log|I_3| \leqslant (\tfrac{3}{2}+\varepsilon)r_k^2\ ,\quad \log|I_4| \leqslant (2/25+\varepsilon)r_k^2\ ,$$

$\log|I_5| \leqslant (7/50+\varepsilon)r_k^2$, $\log|I_6| \leqslant 3(1+\varepsilon)(1/5 - 25/13^2)r_k^2$,

$\log|I_7| \leqslant 2(1+\varepsilon)(50/13^2 - 18/65)r_k^2$, $\log|I_8| \leqslant 5/2\ (1+\varepsilon)(18/65 - 1/4)r_k^2$,

$\log|I_9| \leqslant 1/2\ (1+\varepsilon)(1/4 - 4/17)r_k^2$, pour k assez grand.

Pour majorer $|I_{10}|$, on néglige la contribution de $1 + i$ qui est un $e^{O(r_k)}$, et on étudie séparément

$$I_{11} = \Pi\, q^{2\delta_q}\ ,\quad I_{12} = I_{10}/I_{11}\ .$$

On a

$$\log|I_{11}| \leqslant \Sigma\, 2\delta_q \log|q| \leqslant \Sigma\, 2\log 2r_k$$
$$\leqslant 2(\pi_3(r_k\sqrt{17}/2) + 2\pi_1(17r_k^2/4))\log(2r_k) < (4/17+\varepsilon)r_k^2\ .$$

D'autre part,

$$\log|I_{12}| \leqslant (2+\sqrt{2})r_k\,\Sigma_q(\Sigma_\ell\,|q|^{-\ell})\log|q| \leqslant (2+\sqrt{2})r_k\,\Sigma_q\,\frac{\log|q|}{|q|-1}\ .$$

Si p désigne un nombre premier dans $\underset{\sim}{Z}$, on a

$$\sum_{|q|\leqslant x} \frac{\log|q|}{|q|-1} = \sum_{\substack{p\leqslant x\\ p\equiv 3[4]}} \frac{\log p}{p-1} + \sum_{\substack{p\leqslant x^2\\ p\equiv 1[4]}} \frac{\log p}{\sqrt{p}-1} \quad \text{(en négligeant } q=1+i \text{ , id est } p=2 \text{).}$$

Mais

$$\sum_{\substack{p\leqslant x^2\\ p\equiv 1[4]}} \frac{\log p}{\sqrt{p}-1} = \int_2^{x^2} \frac{\log t}{\sqrt{t}-1}\, d\pi_1(t) = \frac{\log t}{\sqrt{t}-1}\,\pi_1(t)\Big]_2^{x^2}$$
$$- \int_2^{x^2} \frac{\pi_1(t)}{t(\sqrt{t}-1)}\, dt + \frac{1}{2}\int_2^{x^2} \frac{\pi_1(t)\log t}{\sqrt{t}(\sqrt{t}-1)^2}\, dt .$$

Or

$$\frac{1}{2}\int_2^{x^2} \frac{\pi_1(t)\log t}{\sqrt{t}(\sqrt{t}-1)^2}\, dt \leqslant c(\varepsilon) + \frac{1+\varepsilon}{4}\int_2^{x^2} \frac{\sqrt{t}}{(\sqrt{t}-1)^2}\, dt \leqslant c'(\varepsilon) + (1+\varepsilon)\left(\frac{x}{2} + \log x\right) ,$$

où c et c' sont deux constantes et x est assez grand. De même

$$\int_2^{x^2} \frac{\pi_1(t)}{t(\sqrt{t}-1)}\, dt \geqslant c''(\varepsilon) + 2(1-\varepsilon)\log x ,$$

donc, pour x assez grand,

$$\sum_{\substack{p\leqslant x^2\\ p\equiv 1[4]}} \frac{\log p}{\sqrt{p}-1} < (1+\varepsilon)x ,$$

et de manière analogue $\displaystyle\sum_{\substack{p\leqslant x\\ p\equiv 3[4]}} \frac{\log p}{p-1} = O(\log x)$ alors

$$\log|I_{12}| \leqslant (1+\varepsilon)(2+\sqrt{2})\frac{2}{\sqrt{17}}\, r_k^2 ,$$

et le lemme est démontré.

C.Q.F.D.

LEMME 4. - <u>Il existe</u> $\tilde{\gamma}_k \in \underset{\sim}{Z}[i]$ <u>tel que</u> $\alpha_{0,k} = \prod_{1\leqslant n\leqslant n_k} \zeta_n$ <u>divise</u> $\tilde{\gamma}_k \prod_{\substack{0\leqslant n\leqslant n_k\\ n\neq m}} (z-\zeta_n)$ <u>pour tout</u> $m \leqslant n_k$ <u>et pour tout</u> $z \in \underset{\sim}{Z}[i]$,

<u>et vérifiant</u> $\log|\tilde{\gamma}_k| \leqslant 4{,}91422 r_k^2$ <u>pour</u> k <u>assez grand.</u>

<u>Démonstration.</u> - Posons $A(z, \ell, q) = \mathrm{card}\{\zeta \in \underset{\sim}{Z}[i] ;\ \zeta \neq 0 ,\ |q^\ell \zeta - z| \leqslant r_k\}$, alors, comme au lemme 3, il est clair que

$$\prod_q q^{\sum_\ell A(z,\ell,q)}$$

divise $\prod_{0\leqslant n\leqslant n_k}(z-\zeta_n)$, où le produit est étendu aux q premiers dans $\underset{\sim}{Z}[i]$ tels que $|q| \leqslant r_k$, et la somme aux entiers naturels ℓ tels que $A(z,\ell,q) \geqslant 1$. Pour tous les q considérés, on a $v_q(z-\zeta_m) \leqslant \sum_\ell 1$, donc $\prod_{\substack{0\leqslant n\leqslant n_k\\ n\neq m}}(z-\zeta_n)$ est divisible par

$$\prod_q q^{\sum_\ell (A(z,\ell,q)-1)} .$$

Mais

$$\alpha_{0,k} = \prod_q q^{\sum_\ell A(0,\ell,q)}$$

et le lemme 1 montre que

$$A(z\ ,\ \ell\ ,\ q) - A(0\ ,\ \ell\ ,\ q) \geqslant -2 - (2+\sqrt{2})r_k|q|^{-\ell}\ ,$$

on peut donc poser

$$\tilde{\gamma}_k = \prod_q q^{(2+\sqrt{2})r_k\sum_\ell|q|^{-\ell}+3\delta_q} \quad \text{où} \quad \delta_q = [\frac{\log r_k}{\log|q|}]$$

et un calcul analogue à celui de la fin de la preuve du lemme 3 donne le résultat.

C.Q.F.D.

On peut alors donner les propriétés des polynômes de Lagrange-Gruman :

THÉORÈME 1. - <u>Avec les notations précédentes, les polynômes</u>

$$h_{m,k}(z) = \gamma_k\ \tilde{\gamma}_k \prod_{\substack{0\leqslant j\leqslant n_k \\ j\neq m}} \frac{z-\zeta_j}{\zeta_m-\zeta_j} \qquad (0 \leqslant m \leqslant n_k)$$

<u>forment une base de l'espace des polynômes de degré</u> $\leqslant n_k$. <u>Ils vérifient</u> $h_{m,k}(\mathbb{Z}[i]) \subset \mathbb{Z}[i]$, <u>et</u>

$$\log|h_{m,k}(z)| \leqslant \pi r_k^2 \log(1+\frac{|z|}{r_k}) + 11{,}36519 r_k^2 + O(r_k \log(|z| + r_k))$$

<u>pour</u> k <u>assez grand.</u>

<u>Démonstration.</u> - La première partie du théorème est claire, car les $h_{m,k}$ sont, à un coefficient non nul près, les polynômes d'interpolation de Lagrange relatifs à $\mathbb{Z}[i] \cap \overline{D}(0\ ,\ r_k)$; et on a construit γ_k et $\tilde{\gamma}_k$ pour que les $h_{m,k}$ envoient $\mathbb{Z}[i]$ dans $\mathbb{Z}[i]$.

Pour étudier la croissance des $h_{m,k}$ il s'agit d'évaluer le module de

$$\prod_j(z-\zeta_s) = \prod_s a_s$$

où $a_s = z - \zeta_j$ décrit $S = \{\zeta \in \mathbb{Z}[i]\ ;\ |\zeta - z| \leqslant r_k\ ,\ \zeta \neq 0\}$.

Le fait d'ajouter le facteur $z - \zeta_m$ est sans importance, compte tenu du terme d'erreur dans la majoration.

Soit A_s le carré de centre a_s , de côtés de longueur 1 parallèles aux axes. Le théorème des accroissements finis montre que

$$|\log|a_s| - \iint_{A_s} \log|\zeta|\ dxdy| \leqslant (\sqrt{2}\ |a_s| - 1)^{-1} \quad \text{si} \quad |a_s| \geqslant 2\ ,$$

d'où

$$\sum_s \log|a_s| - \sum_s \iint_{A_s} \log|\zeta|\ dxdy = O(r_k)\ .$$

En effet cette différence est majorée par une constante due aux carrés A_s éven-

tuels, proches de 0 , plus un $O(\sum_s(\sqrt{2}\,|a_s| - 1)^{-1})$ qui est de l'ordre de $\iint_{\overline{D}(z,r_k)} d\rho d\theta$ donc un $O(r_k)$ comme on le voit, par exemple, en distinguant les cas $|z| < 3r_k$ et $|z| \geqslant 3r_k$. D'autre part, si $D = \{\zeta \in \mathbb{C} \; ; \; |\zeta - z| \leqslant r_k\}$, on a

$$\sum_s \iint_{A_s} \log|\zeta| \, dxdy - \iint_D \log|\zeta| \, dxdy = O(r_k \log(|z| + r_k)) ,$$

car cette différence provient d'environ $2\pi r_k$ carrés A_s proches du bord de D , où l'on a $\log|\zeta| \leqslant 2 \log(|z| + r_k)$. Finalement, on obtient

$$\log|\prod(z - \zeta_j)| \leqslant \iint_D \log|\zeta| \, dxdy + O(r_k \log(|z| + r_k)) .$$

Il reste à calculer

$$\iint_D \log|\zeta| \, dxdy = r_k^2 \iint_{D'} \log(r_k|\zeta|) \, dxdy , \text{ où } D' = \{\zeta \in \mathbb{C} \; ; \; |\zeta - \frac{z}{r_k}| \leqslant 1\} .$$

Mais cette intégrale est stable par rotation de centre 0 , et on peut supposer $z = -i\delta r_k$ avec $\delta > 0$. Alors

$$\iint_{D'} \log(r_k|\zeta|) \, dxdy = \pi \log r_k + \iint_{\overline{D}(0,1)} \log\sqrt{x^2 + (y + \delta)^2} \, dxdy$$

et cette dernière intégrale est majorée par $\pi \log(1 + |z|/r_k)$. On obtient donc

$$\log|\prod(z - \zeta_j)| \leqslant \pi r_k^2 \log r_k + \pi r_k^2 \log(1 + \frac{|z|}{r_k}) + O(r_k \log(r_k + |z|)) .$$

Un calcul analogue fournit

$$\log|\prod_{j \neq m}(\zeta_m - \zeta_j)| = \pi r_k^2 \log r_k + r_k^2 \iint_{\overline{D}(0,1)} \log\sqrt{x^2 + (y+\delta)^2} \, dxdy + O(r_k \log r_k)$$

où $r_k \, \delta = |\zeta_m|$, donc $0 \leqslant \delta \leqslant 1$, et un facile calcul de dérivée montre que l'intégrale est minimum pour $\delta = 0$ et vaut $\frac{-\pi}{2}$, d'où le résultat.

C.Q.F.D.

2. Une application : Le théorème de Gel'fond [5] par la méthode de Schneider.

Dans un article récent, M. WALDSCHMIDT [14] montre le théorème de Polya [12] par la méthode de Schneider, mais, faute de polynômes d'interpolation convenables sur $\mathbb{Z}[i]$, il obtient un résultat plus faible que celui de GEL'FOND. Les polynômes de Lagrange-Gruman permettent d'obtenir la généralisation suivante du résultat de GEL'FOND, par la même méthode [8].

THÉORÈME 2. - *Soit* $K \supset \mathbb{Z}[i]$ *un corps de nombres de degré* $\delta = [K : \mathbb{Q}]$, γ_0 *et* γ_1 *deux réels positifs, et* $S \subset \mathbb{Z}[i]$ *vérifiant, pour* r *assez grand,* $\mathrm{card}\{S \cap \overline{D}(0 , r)\} \geqslant \gamma_0 r^2$. *Alors il existe un réel* $\alpha > 0$, *ne dépendant que de* δ , γ_0 *et* γ_1 , *tel que, si* f *et* g *sont des fonctions entières vérifiant, pour* r *assez grand,*

(i) $\max\{\log|f|_r \; ; \; \log|g|_r\} \leqslant \alpha r^2$,

(ii) *Pour tout* $\zeta \in S$, $g(\zeta) \neq 0$ *et* $\frac{f(\zeta)}{g(\zeta)} \in K$,

(iii) $\max_{\zeta \in S \cap \overline{D}(0,r)} \{-\log|g(\zeta)| \; , \; s(f(\zeta)/g(\zeta))\} \leqslant \gamma_1 r^2$,

alors f/g est une fonction rationnelle.

Les notations étant $|f|_r = \max_{z\in\overline{D}(0,r)}|f(z)|$ et, si $x \in K$, la taille de x est $s(x) = \max\{\log|\overline{x}|, \log \text{dén}(x)\}$ où $|\overline{x}|$ est le maximum des modules des conjugués de x, et $\text{dén}(x)$, le dénominateur de x, est le générateur positif de l'idéal de $\mathbb{Z}$ formé des d tels que dx est entier algébrique.

Démonstration. - Pour simplifier les calculs, nous ne prouverons que le résultat de GEL'FOND : Il existe $\alpha > 0$, tel que si f est une fonction entière vérifiant $f(\mathbb{Z}[i]) \subset \mathbb{Z}[i]$ et $\log|f|_r \leq \alpha r^2$ pour r assez grand, alors f est un polynôme.

On construit une fonction auxiliaire

$$F(z) = \sum_{|\zeta_m|\leq r_k} \sum_{0\leq \ell < L} a_{m,\ell}\, h_{m,k}(z)(f(z))^{\ell} .$$

Les paramètres à choisir sont k et L. On définit k par $r_k \leq \beta N < r_{k+1}$, où N est un entier assez grand et β un réel positif (on peut choisir $\beta = 1/2$) et L est un réel positif (on peut choisir $L = 9$). La preuve se décompose en deux pas.

Premier pas : On construit $a_{m,\ell} \in \mathbb{Z}$ non tous nuls, tels que $F(\zeta) = 0$ pour tout $\zeta \in \mathbb{Z}[i] \cap \overline{D}(0, N)$ et $|a_{m,\ell}| \leq \exp(c_1 N^2)$ où c_1 est une constante.

En effet, $F(\zeta) = \sum_m \sum_\ell a_{m,\ell}\, h_{m,k}(\zeta)\, f(\zeta)^{\ell} = 0$ peut être considéré comme un système d'équations linéaires homogènes à coefficients dans $\mathbb{Z}[i]$ en les $a_{m,\ell}$. Il y a environ πN^2 équations à $\pi N^2 \beta^2 L$ inconnues, et les coefficients ont une taille majorée par $\alpha N^2 L + c_2 N^2$ (où c_2 est une constante fournie par le théorème 1). Le résultat est donc une conséquence du lemme de Siegel ([13], lemme 1.3.1).

C'est dans ce premier pas que les polynômes de Lagrange-Gruman jouent leur rôle essentiel. Leur croissance "faible" permet de choisir L constant, alors que si on construit F avec les polynômes z^m il faut que L croisse avec N ce qui fournit une fonction F qui croît plus vite et on a une majoration moins bonne dans le deuxième pas de la démonstration, quand on applique le lemme de Schwarz.

Deuxième pas : Pour tout entier $M \geq 0$, on a la propriété

(P_M) $$F(\zeta) = 0 \text{ pour tout } \zeta \in \mathbb{Z}[i] \cap \overline{D}(0, M) .$$

Le théorème en résulte, car F est une fonction entière de type $\leq \alpha L$ d'ordre 2 et pour α assez petit, on a $\alpha L < \pi/2$; de plus F s'annule sur $\mathbb{Z}[i]$ et la formule de Jensen montre donc que F est identiquement nulle. Par suite f est algébrique, et comme elle est entière, c'est un polynôme.

Nous allons donc prouver la propriété (P_M), par récurrence sur M. Le premier pas montre qu'elle est vraie pour $M \leq N$. Supposons (P_M) vraie. Le lemme de Schwarz [14] appliqué à F montre que si $R \geq M + 1$, on a

$$\log|F|_{M+1} \leq \log|F|_R - \pi M^2 \log \frac{R^2 + (M+1)^2}{2R(M+1)} .$$

On choisit $R = \rho(M+1)$ avec $\rho > 1$, et en ne conservant que les parties principales des estimations (N est grand), on obtient

$$\log|F|_{M+1} \leqslant c_1 N^2 + \pi\beta^2 N^2(c_2 + \log(1 + \frac{\rho(M+1)}{\beta N})) + \alpha\rho^2 L(M+1)^2 - \pi M^2 \log\frac{\rho}{2} = \varphi(M) .$$

Pour conclure à (P_{M+1}), il suffit que $\varphi(M) < 0$, car $F(\zeta) \in Z[i]$ si $\zeta \in Z[i]$, donc $F(\zeta) = 0$ ou $|F(\zeta)| \geqslant 1$.

Pour $M = N$, il s'agit de vérifier

$$c_1 + \pi\beta^2(c_2 + \log(1 + \frac{\rho}{\beta})) + \alpha\rho^2 L - \pi \log\frac{\rho}{2} < 0 . \tag{1}$$

Si cela est vérifié, il est clair que $\varphi(M)$ est une fonction décroissante de M, donc le théorème est démontré.

Choisissons ρ assez grand pour que

$$\frac{\pi}{2}(1 - \beta^2) \log \rho > c_1 + c_2 \pi\beta^2 + \pi\beta^2 \log(1 + \frac{1}{\beta}) + \pi \log 2 .$$

Alors il suffit de prendre α assez petit pour que (1) soit réalisée.

C.Q.F.D.

Remarque. - Même sans optimiser le choix des paramètres, on obtient un α bien meilleur que celui de GEL'FOND [5]. Par exemple, pour $\beta = 1/4$, $\rho = 8$ et $\beta^2 L = 11$, on obtient un $\alpha > 1{,}3.10^{-4}$.

Figures

Echelle : 0 1

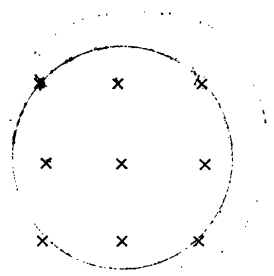


figure 1

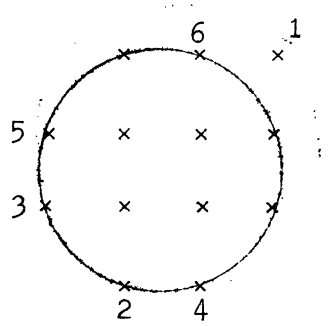


figure 2

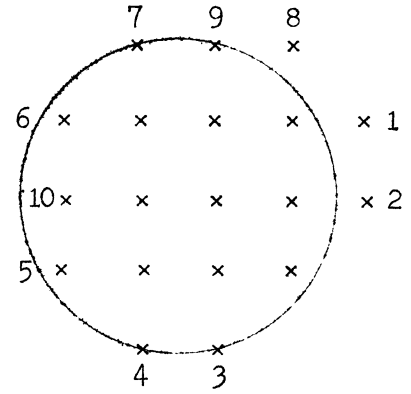


figure 3

figure 4

figure 5

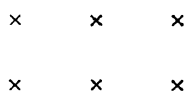


figure 6

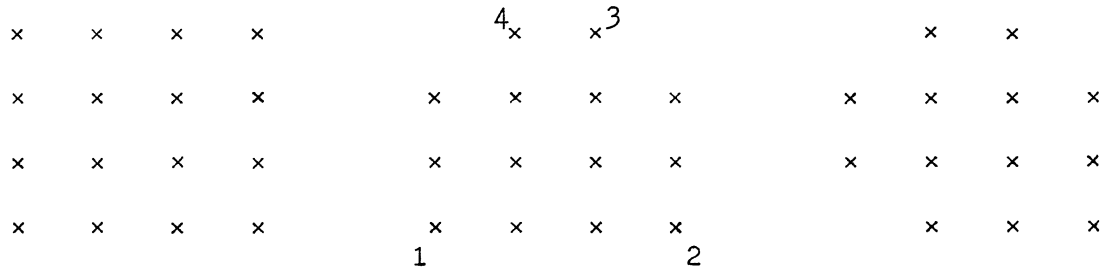


figure 7 figure 8 figure 9

BIBLIOGRAPHIE

[1] AMICE (Y.). - Interpolation p-adique, Bull. Soc. math. France, t. 92, 1964, p. 117-180 (Thèse Sc. math., Paris, 1963).

[2] AMICE (Y.). - Les nombres p-adiques, Paris, Presses Universitaires de France, 1975 (Collection SUP, "Le Mathématicien", 14).

[3] BAKER (A.). - Transcendental number theory. - Cambridge University Press, 1975.

[4] CHAIX (H.). - Points frontières de certains compacts convexes appartenant à un réseau dans $\underset{\sim}{R}^2$ et $\underset{\sim}{R}^3$, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 19e année, 1977/78, n° 16, 12 p.

[5] GEL'FOND (A.). - Sur les propriétés arithmétiques des fonctions entières, Tôhoku math. J., t. 30, 1929, p. 280-285.

[6] GEL'FOND (A.). - Sur les nombres transcendants, C. R. Acad. Sc. Paris, t. 189, 1929, Série A, p. 1224-1226.

[7] GRAMAIN (F.). - Sur la transcendance de e^{π} (à paraître).

[8] GRUMAN (L.). - Propriétés arithmétiques des fonctions entières (à paraître).

[9] HENSLEY (D.). - Polynomials which take gaussian integer values at gaussian integers, J. Number Theory, t. 9, 1977, p. 510-524.

[10] HERZ (C. S.). - On the number of lattice points in a convex set, Amer. J. of Math., t. 84, 1962, p. 126-133.

[11] KOKSMA (J. F.) und POPKEN (J.). - Zur Transzendenz von e^{π}, J. für reine und angew. Math., t. 168, 1932, p. 211-230.

[12] PÓLYA (G.). - Über ganzwertige ganze Funktionen, Rend. Circ. math. Palermo, t. 40, 1915, p. 1-16.

[13] WALDSCHMIDT (M.). - Nombres transcendants. - Berlin, Springer-Verlag, 1974 (Lecture Notes in Mathematics, 402).

[14] WALDSCHMIDT (M.). - Pólya's theorem by Schneider's method, Acta Math. Acad. Sc. Hungaricae, t. 31, 1978, p. 21-25.