Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Ju. V. Linnik

Sur une application du théorème d'André Weil à la théorie des caractères de Dirichlet

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, nº 1 (1966-1967), exp. nº 6, p. 1-7

<http://www.numdam.org/item?id=SDPP_1966-1967__8_1_A6_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
8e année, 1966/67, n° 6

19 décembre 1966

SUR UNE APPLICATION DU THÉORÈME D'ANDRÉ WEIL À LA THÉORIE DES CARACTÈRES DE DIRICHLET

par Ju. V. LINNIK

1. - Le célèbre théorème d'André WEIL sur le nombre des diviseurs du premier degré d'un corps de fonctions d'une variable sur un corps fini (le problème de Riemann pour les courbes) a conduit à des succès considérables dans la théorie analytique des nombres. Rappelons ce théorème pour le corps des constantes, premier et fini (corps des restes mod p).

$p \geqslant 0$ étant un nombre premier, on considère une courbe irréductible $Q(x, y) = 0$ au-dessus du corps P sus-mentionné. Les diviseurs de degré 1 correspondent aux points de cette courbe appartenant au corps P . Pour le nombre N de ces diviseurs, nous avons l'estimation :

$$|N - (p + 1)| \leqslant g\sqrt{p} \quad , \tag{1}$$

g étant le genre de notre courbe.

Le rôle fondamental du théorème d'André Weil, et de ses généralisations pour la théorie des nombres algébriques et la géométrie algébrique, est bien connu. L'influence de ce théorème sur la théorie analytique des nombres apparaît d'abord dans le travail fondamental de M. EICHLER [5] (1954), où les estimations optimales pour l'erreur dans la formule bien connue de la représentation des nombres entiers par une forme quadratique quaternaire définie ont été obtenues à l'aide de ce théorème. La solution du problème de Hardy-Littlewood sur l'équation

$$n = p + x^2 + y^2 \quad ,$$

p étant un nombre premier, et d'autres problèmes de ce genre [7] dépendent aussi du théorème d'André Weil (récemment, les travaux de E. BOMBIERI [1] ont montré que l'on peut maintenant s'en passer).

Enfin, les remarquables travaux de D. BURGESS (1957-1963) [2], [3], [4] ont montré comment, à l'aide de ce théorème, on peut avancer dans l'étude des hypothèses de I. M. VINOGRADOV.

2. - Rappelons l'énoncé des hypothèses de I. M. VINOGRADOV (voir par exemple [6]). Considérons un nombre entier D et l'ensemble des caractères de Dirichlet

$(\chi(n))$ pour le module D , dont le caractère principal sera exclu ; on aura donc $\varphi(D) - 1$ caractères non-principaux.

Soit χ l'un de ces caractères ; les nombres $n \in [1 , D]$, tels que

$$\chi(n) \neq 0 , 1 ,$$

seront appelés non-résidus pour le caractère χ ; $N_{min}(D , \chi)$ désignera le moindre non-résidu pour χ . Nous désignerons par $P_{min}(D , \chi)$ le plus petit résidu premier pour χ , c'est-à-dire le plus petit nombre premier n pour lequel

$$\chi(n) = 1$$

(les nombres premiers q , pour lesquels $\chi(q) = 0$, sont les diviseurs de D , et ne nous intéressent pas).

$d_{max}(D , \chi)$ sera la distance maximale entre deux non-résidus consécutifs du segment $[1 , D - 1]$.

Les trois hypothèses de I. M. VINOGRADOV sont :

(2) $$(V_I) \quad N_{min}(D , \chi) = O(D^{\varepsilon})$$

pour tout $\varepsilon > 0$, uniformément par rapport à χ ;

(3) $$(V_{II}) \quad P_{min}(D , \chi) = O(D^{\varepsilon})$$

pour tout $\varepsilon > 0$, uniformément par rapport à χ ;

(4) $$(V_{III}) \quad d_{max}(D , \chi) = O(D^{\varepsilon})$$

pour tout $\varepsilon > 0$, uniformément par rapport à χ .

Ces hypothèses ne sont ni démontrées ni réfutées jusqu'à présent. Des résultats plus faibles, connus jusqu'à l'année 1958, étaient :

$$N_{min}(D , \chi) = O(D^{1/2})$$

(conséquence d'un théorème de Gauss démontré en 1796) ;

$$N_{min}(D , \chi) = O(D^{(1/2 \sqrt{e})+\varepsilon}) ,$$

e étant le nombre de Neper et $\varepsilon > 0$ aussi petit que l'on veut (I. M. VINOGRADOV, 1926, voir [7]) ;

$$d_{max}(\chi , D) = O(D^{1/2})$$

(I. M. VINOGRADOV, 1925, voir [7]) ;

$$P_{min}(\chi\ ,\ D) = O(D^{1/2})$$

pour D n'ayant pas de facteurs carrés autres que 4 (conséquence du théorème de C. L. Siegel démontré en 1935 [10]).

3. - Le premier travail remarquable de D. BURGESS parut en 1958 [3]. En appliquant le théorème d'André Weil d'une façon extrêmement ingénieuse, D. BURGESS obtient :

$$N_{min}(D\ ,\ \chi) = O(D^{(1/4\sqrt{e})+\varepsilon})\ , \tag{5}$$

$$d_{max}(D\ ,\ \chi) = O(D^{(1/4)+\varepsilon})\ , \tag{6}$$

pour tout $\varepsilon > 0$.

Il faut remarquer que (2) et (3) sont des conséquences immédiates de l'hypothèse de Riemann généralisée, affirmant que tous les zéros des fonctions de Dirichlet $L(s\ ,\ \chi)$ dans la bande critique $0 < \mathrm{Re}\ s < 1$ sont situés sur la ligne droite $\mathrm{Re}\ s = \frac{1}{2}$, mais que (4) n'en est pas une, et même le résultat remarquable de D. BURGESS [4] n'est pas une conséquence immédiate de l'hypothèse de Riemann généralisée. Comme ce résultat est une conséquence de l'inégalité (1), on voit bien que cette inégalité, c'est-à-dire le théorème d'André Weil, peut donner, dans la théorie analytique des caractères de Dirichlet, des résultats plus profonds que l'hypothèse de Riemann.

4. - Nous montrerons ici que les raisonnements de D. BURGESS [1] peuvent être appliqués à étudier l'hypothèse (V_{II}), à savoir que ces raisonnements, conjugués avec le théorème classique de C. L. Siegel [10], pour le cas des caractères réels $\chi(n)$, conduisent à l'inégalité

$$P_{min}(D\ ,\ \chi) = O(D^{(1/4)+\varepsilon}) \tag{7}$$

pour D n'ayant pas de facteurs carrés autres que 4 . La démonstration correspondante suivra la note [11] de A. I. VINOGRADOV et de l'auteur ; nous y ajouterons encore quelques résultats.

Nous **n'exposerons** ici en détail que le cas des caractères quadratiques (caractères réels), les autres cas ne seront qu'esquissés.

Soit $\chi(n)$ un caractère réel pour le module D du type sus-mentionné ; formons la série de Dirichlet

$$L(s\ ,\ \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}\ .$$

Posons $s = \sigma + it$; la série est convergente pour $\sigma > 0$. Considérons la série de Dirichlet :

(8) $$Z(s) = \zeta(s)\ L(s\ ,\ \chi)\ ,$$

où $\zeta(s)$ est la fonction de Riemann. Nous avons :

(9) $$Z(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad (\mathrm{Re}\ s > 1)\ ,$$

a_n étant le nombre des représentations du nombre n comme la norme d'un idéal dans le corps quadratique $h(\sqrt{D})$ ou $h(\sqrt{-D})$, suivant le type du caractère réel χ . Il est bien connu que si l'on forme la fonction sommatoire pour (9) :

(10) $$S(x) = \sum_{a\leqslant x} a_n\ ,$$

ce sont les nombres n qui se décomposent entièrement dans le corps quadratique correspondant qui forment une partie importante de la somme (10) pour x grand ; les autres nombres ne donnent que les facteurs carrés dont le rôle est négligeable.

Nous avons maintenant, pour $x \geqslant 1$,

(11) $$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{s^3}\, Z(s)\ ds = \frac{1}{2} \sum_{n\leqslant x} a_n\ \ell_n^2\ \frac{x}{n} = S_1(x)\ .$$

Les raisonnements de BURGESS [2], s'appuyant sur l'inégalité de A. Weil (1), conduisent à l'estimation suivante :

(12) $$\sum_{n\leqslant y} \chi(n) = O(y^{1-z_0}) \qquad \text{pour}\quad y \geqslant D^{(1/4)+\varepsilon_0}$$

(z_0 , z_1 , ... sont de petites constantes positives choisies les unes après les autres, et $\varepsilon_0 > 0$ une constante aussi petite que l'on veut). Posons $s = \sigma + it$. La fonction $Z(s) = \zeta(s)\ L(s\ ,\ \chi)$ peut être estimée sur les droites verticales assez proches de la droite $\sigma = 1$ à l'aide de (12). Considérons la droite

$$s = \sigma_0 + it\ ,$$

où

(13) $$\sigma_0 = 1 - z_1\ ; \qquad z_1 = \frac{z_0}{2}\ .$$

En vertu de (12), nous avons, sur cette droite, en utilisant le théorème de sommation d'Abel et les raisonnements habituels de la théorie des séries L de Dirichlet (voir par exemple [9]) :

$$(14) \qquad |L(s\ ,\ \chi)| \leqslant \Big|\sum_{n=1}^{D^{(1/4)+\varepsilon_0}} \frac{\chi(n)}{n^s}\Big| + \Big|\sum_{n>D^{(1/4)+\varepsilon_0}} \frac{\chi(n)}{n^s}\Big| \leqslant D^{z_1((1/4)+\varepsilon_0)} + O(|t|+1).$$

D'autre part, nous avons sur la même droite :

$$(15) \qquad |\zeta(s)| = O[(|t|+1)^{z_1}]$$

(voir [9]). En déplaçant le contour $(2 - i\infty\ ,\ 2 + i\infty)$ sur la ligne (13), nous dépassons le pôle de résidu $xL(1\ ,\ \chi)$, et nous avons, pour tout $x \geqslant D^{(1/4)+2\varepsilon_0}$,

$$(16) \qquad S_1(x) = \frac{1}{2}\sum_{n\leqslant x} a_n\, \ell_n^2\, \frac{x}{n} = xL(1\ ,\ \chi) + \frac{1}{2\pi i}\int_{\sigma_0-i\infty}^{\sigma_0+i\infty} \frac{x^s}{s^3}\, Z(s)\, ds \quad .$$

En utilisant (15) et (16), nous obtenons :

$$(17) \qquad \Big|\frac{1}{2\pi i}\int_{\sigma_0-i\infty}^{\sigma_0+i\infty} \frac{x^s}{s^3}\, Z(s)\, ds\Big| = O(x^{\sigma_0} D^{z_1(\frac{1}{4}+\varepsilon_0)}) \quad .$$

La partie droite de (17) peut s'écrire :

$$(18) \qquad O\Big(x.\Big(\frac{D^{(1/4)+\varepsilon_0}}{x}\Big)^{-z_1}\Big) \quad .$$

Comme $x \geqslant D^{(1/4)+2\varepsilon_0}$, nous avons :

$$(19) \qquad \eta_x = \Big(\frac{D^{(1/4)+\varepsilon_0}}{x}\Big)^{-z_1} \leqslant D^{-\varepsilon_0 . z_1} \quad .$$

5. - Ainsi, (16) nous donne :

$$(20) \qquad S_1(x) = \frac{1}{2}\sum_{n\leqslant x} a_n\, \ell_n^2\, \frac{x}{n} = xL(1\ ,\ \chi) + x\eta_x \quad ,$$

où η_x est donné par la relation (19).

Le théorème de C. L. Siegel [10] nous apprend maintenant que

$$(21) \qquad L(1\ ,\ \chi) > c_\varepsilon\, D^{-\varepsilon} \quad ,$$

$\varepsilon > 0$ étant aussi petit que l'on veut. En prenant $\varepsilon \leqslant \frac{\varepsilon_0\, z_1}{2}$, nous avons alors, en vertu de (19) et (20),

$$S_1(x) = xL(1\ ,\ \chi)(1 + \eta'_x) \qquad \text{pour} \quad x \geqslant D^{(1/4)+2\varepsilon_0} \ , \tag{22}$$

où

$$\eta^1_x \leqslant (\eta_x)^{1/2} \ . \tag{23}$$

Comme les valeurs a_n sont non-négatives, on peut tirer de (22), en employant des méthodes taubériennes élémentaires [9], la relation asymptotique :

$$S(x) = \sum_{n \leqslant x} a_n \sim xL(1\ ,\ \chi) \qquad \text{pour} \quad x \geqslant D^{(1/4)+2\varepsilon_0} \ , \quad D \to \infty \ . \tag{24}$$

Cette relation éclaire la distribution asymptotique des idéaux de petites normes. Nous voyons qu'il existe des idéaux non-unités dont la norme n'excède pas

$$c_\varepsilon \ D^{(1/4)+\varepsilon} \ ,$$

$2\varepsilon_0$ étant un nombre arbitrairement petit.

Le théorème classique de Minkowski nous apprend l'existence des idéaux d'une classe donnée dont la norme n'excède pas $|d|^{1/2}$, d étant le discriminant du corps. Notre estimation $c_\varepsilon\ D^{(1/4)+\varepsilon}$ est plus précise pour les corps quadratiques, mais elle ne précise pas la classe de l'idéal. Il est aisé de voir, d'ailleurs, qu'il est impossible d'améliorer l'estimation de Minkowski pour les idéaux appartenant à une classe donnée, l'amélioration étant possible seulement si l'on ne précise pas la classe.

La relation (7) est maintenant facile à prouver. Si D est un nombre quelconque, n'ayant pas de diviseurs carrés autres que 4 , considérons le caractère réel $\chi(n)$ pour le module D . La relation (24) nous apprend l'existence des nombres premiers q , tels que $\chi(q) = +1$. Comme $2\varepsilon_0$ est arbitrairement petit, nous avons donc (7).

6. - On peut généraliser la relation (24) pour les corps de Kummer, en prenant

$$Z(s) = \zeta(s) \prod_{\chi \bmod D} L(s\ ,\ \chi) \ ,$$

où χ sont des caractères non-principaux pour le module D . On obtient de la sorte que, dans tout corps de Kummer $h(\sqrt[n]{D})$, il existe des idéaux $\mathfrak{a}$ dont la norme

$$|N(\mathfrak{a})| \leqslant c_\varepsilon |d|^{(1/4)+\varepsilon} \ ,$$

$\varepsilon > 0$ étant arbitrairement petit.

La relation (24) est utile dans l'application des méthodes ergodiques à la théorie des corps algébriques [8]. Elle permet d'étudier, de façon beaucoup plus simple que jusqu'à présent, la distribution des points entiers sur la sphère

$$x^2 + y^2 + z^2 = m \quad ,$$

et, en général, sur les ellipsoïdes et hyperboloïdes dans l'espace à trois dimensions.

BIBLIOGRAPHIE

[1] BOMBIERI (Enrico). - The large sieve. - Milano, 1965.

[2] BURGESS (D. A.). - The distribution of quadratic residues and non-residues, Mathematika, London, t. 4, 1957, p. 106-112.

[3] BURGESS (D. A.). - A note on the distribution of residues and non-residues, J. London math. Soc., t. 38, 1963, p. 253-256.

[4] BURGESS (D. A.). - A note on L-functions, J. London math. Soc., t. 39, 1964, p. 103-108.

[5] EICHLER (Martin). - Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. der Math., t. 5, 1954, p. 355-366.

[6] GEL'FOND (A. O.) et LINNIK (Ju. V.). - Méthodes élémentaires dans la théorie analytique des nombres. - Paris, Gauthier-Villars, 1965 (Monographies internationales modernes, 6).

[7] LINNIK (Ju. V.). - The dispersion method in binary additive problems, Translated by S. Schuur. - Providence, American mathematical Society, 1963.

[8] LINNIK (Ju. V.). - Propriétés ergodiques des corps algébriques [en russe]. - Leningrad, 1967 (à paraître).

[9] PRACHAR (Karl). - Primzahlverteilung. - Berlin, Springer-Verlag, 1957 (Die Grundlehren der mathematischen Wissenschaften, 91).

[10] SIEGEL (Carl Ludwig). - Über die Klassenzahl quadratischer Zahlkörper, Acta Arithm., Warszawa, t. 1, 1935, p. 83-86.

[11] VINOGRADOV (A. I.) et LINNIK (Ju. V.). - Les courbes hyperelliptiques et le plus petit résidu premier [en russe], Doklady Akad. Nauk SSSR, t. 168, 1966, n° 5.