COMPOSITIO MATHEMATICA

JEAN-FRANÇOIS MESTRE

Formules explicites et minorations de conducteurs de variétés algébriques

Compositio Mathematica, tome 58, n° 2 (1986), p. 209-232

<http://www.numdam.org/item?id=CM_1986__58_2_209_0>

Compositio Mathematica 58 (1986) 209–232

FORMULES EXPLICITES ET MINORATIONS DE CONDUCTEURS DE VARIÉTÉS ALGÉBRIQUES

Jean-François Mestre

I. Introduction

Dans [13] et [14], Weil montre que la plupart des théorèmes portant sur la répartition des nombres premiers (ou plus généralement des idéaux premiers dans un corps de nombres) peuvent se démontrer à l'aide de "formules explicites" reliant cette répartition à celle des zéros de certaines fonctions zêta. Odlyzko, Poitou et Serre ont montré [10] que ces formules permettent également d'obtenir des minorations très fines des discriminants de corps de nombres.

D'autre part, on sait associer à de nombreux objets de nature géométrique (variétés algébriques, motifs, représentations l-adiques, ...) des fonctions $L(s) = \sum_n a_n n^{-s}$, convergeant dans un demi-plan vertical $\mathrm{Re}(s) > \sigma_0$, décomposables en produit eulérien, et dont on conjecture qu'elles sont prolongeables en des fonctions méromorphes d'ordre 1 vérifiant une équation fonctionnelle analogue à celle des fonctions des corps de nombres.

Il était donc tentant à la suite notamment de Moreno [9] d'appliquer les formules explicites de Weil à de telles fonctions L, et d'examiner quelles conséquences auraient sur les objets géométriques cités ci-dessus les vertus supposées de leur fonction L.

Dans un premier paragraphe, on définit d'abord des fonctions L vérifiant les conditions requises pour qu'on puisse écrire des formules explicites raisonnables (I.1 et I.2).

On a ici fait le choix de prendre systématiquement la bande verticale $0 \leqslant \mathrm{Re}(s) \leqslant 1$ comme bande critique de L, ce qui simplifie considérablement les formules obtenues; on peut toujours se ramener à ce cas, par une translation convenable $s \mapsto s + m$. Remarquons cependant l'apparente aberration que représente, pour un arithméticien, le fait de diviser les coefficients a_n de certaines fonctions L, entiers lourds de signification, par d'inesthétiques racines carrées.

Dans le second paragraphe, nous appliquons les formules de I.2 aux formes modulaires; si L désigne la série de Dirichlet associée à une "newform" de poids k pour le groupe $\Gamma_0(N)$, nous obtenons des majorations de l'ordre r de L en $k/2$, le centre de la bande critique de

L, en fonction de N, de k et des coefficients de L.

On trouve en particulier la majoration $r < \log k^2 N$. De plus, si l'on suppose vérifiée l'hypothèse de Riemann pour L, on obtient une majoration du type $r = O(\log k^2 N / \log\log k^2 N)$.

Ces majorations, appliquées aux formes modulaires de poids 2, ont une interprétation géométrique, comme il est expliqué au paragraphe II.2: si E est une courbe elliptique définie sur $\mathbf{Q}$, de conducteur N, sa fonction L est conjecturalement la transformée de Mellin d'une newform de poids 2 et de niveau N, et, toujours conjecturalement, l'ordre en 1 de L est égal au rang de $E(\mathbf{Q})$, le groupe de Mordell-Weil de E.

Pour une courbe E donnée, les majorations dues aux formules explicites donnent d'excellentes approximations de ce rang; ceci semble lié au fait que le premier zéro de L sur la droite critique, distinct de 1, en est assez loin. Nous donnons, à la fin du paragraphe II.2, quelques résultats concernant sa localisation.

L'examen des formules explicites permet également de se convaincre de la validité de l'idée intuitive selon laquelle, pour qu'une courbe elliptique ait un grand rang, il est bon qu'elle ait de nombreux points modulo p pour suffisamment de nombres premiers p (cette intuition était à la base des conjectures de Birch et Swinnerton-Dyer).

On obtient ainsi de nombreuses courbes de rang compris entre 3 et 14, et de conducteur assez petit. Nous en donnons des exemples dans II.3.

Enfin, dans le §III, on applique les formules explicites aux fonctions L provenant de la cohomologie des variétés projectives non singulières définies sur un corps de nombres; si ces fonctions vérifient les conjectures habituelles, on en déduit par exemple le fait qu'une variété abélienne définie sur $\mathbf{Q}$ de dimension $r \geqslant 1$ doit avoir un conducteur strictement supérieur à 10^r; en particulier, elle ne peut pas avoir bonne réduction partout, résultat déjà obtenu par J.-P. Serre, en utilisant les mêmes conjectures, en réponse à une question de L. Szpiro. Notons à ce propos que J.-M. Fontaine vient de démontrer ce dernier résultat, indépendamment de toute conjecture (Invent. Math., 1985, Vol. 81).

Je tiens à exprimer mes plus vifs remerciements à J. Martinet, J. Oesterlé, G. Poitou et J.-P. Serre pour l'aide qu'ils m'ont apportée dans ce travail, ainsi qu'à M. Vallino, directeur du Centre de Calcul de l'E.N.S., rue d'Ulm, pour avoir largement mis à ma disposition de puissants moyens de calcul. Je remercie tout particulièrement J.-M. Frailong, qui a bien voulu m'accorder de nombreuses heures pour établir les logiciels permettant de trouver les courbes de rang élevé du §II.3 et dont les conseils m'ont aidé à mieux cerner l'outil informatique.

I.1. Notations

On se donne deux entiers positifs M et M', deux nombres réels strictement positifs A et B, deux suites de M réels positifs ou nuls a_i et a'_i

$(1 \leqslant i \leqslant M)$ vérifiant $\sum_{i=1}^{M} a_i = \sum_{i=1}^{M} a'_i$, et enfin deux suites de M nombres complexes b_i et b'_i $(1 \leqslant i \leqslant M)$ de partie réelle positive ou nulle.

Soient alors deux fonctions méromorphes $\Lambda_1(s)$ et $\Lambda_2(s)$, vérifiant les conditions suivantes:

(i) il existe $w \in \mathbf{C}^*$, tel que, pour tout s, on a: $\Lambda_1(1-s) = w\Lambda_2(s)$;
(ii) Λ_1 et Λ_2 n'ont qu'un nombre fini de pôles;
(iii) pour $i = 1$ ou 2, la fonction Λ_i diminuée de ses parties singulières est bornée dans toute bande verticale:

$$-\infty < \sigma_0 \leqslant \mathrm{Re}(s) \leqslant \sigma_1 < +\infty;$$

(iv) il existe une constante $c \geqslant 0$ telle que, pour $\mathrm{Re}(s) > 1 + c$, on a:

$$\Lambda_1(s) = A^s \prod_{i=1}^{M} \Gamma(a_i s + b_i) \prod_p \prod_{i=1}^{M'} (1 - \alpha_i(p) p^{-s})^{-1}$$

$$\Lambda_2(s) = B^s \prod_{i=1}^{M} \Gamma(a'_i s + b'_i) \prod_p \prod_{i=1}^{M'} (1 - \beta_i(p) p^{-s})^{-1}$$

où p parcourt l'ensemble des nombres premiers, et où les $\alpha_i(p)$ et les $\beta_i(p)$ sont des nombres complexes de module $\leqslant p^c$.

Dans ce qui suit, on pose

$$L_1(s) = \prod_p \prod_{i=1}^{M'} (1 - \alpha_i(p) p^{-s})^{-1}$$

et $$L_2(s) = \prod_p \prod_{i=1}^{M'} (1 - \beta_i(p) p^{-s})^{-1}.$$

REMARQUE I.1.1.: Il est clair que les fonctions Λ_1, Λ_2, L_1 et L_2 sont d'ordre 1.

REMARQUE I.1.2: La condition $\sum_i a_i = \sum_i a'_i$ assure que, dans toute bande verticale de largeur bornée, il existe m tel que, pour $|s|$ assez grand, $L_i(s) = 0(|\mathrm{Im}(s)|^m)$, $i = 1$ et 2. En effet, on peut toujours inclure une telle bande dans une région R: $-\infty < \sigma_0 < \mathrm{Re(s)} < \sigma_1 < +\infty$ avec $\sigma_0 < 0$ et $\sigma_1 > 1 + c$; si $s = \sigma + it$, on sait ([5], p. 333) que l'on a l'équivalence:

$$|\Gamma(s)| \sim \exp(-\pi|t|/2)\,|t|^{\sigma-1/2}(2\pi)^{1/2}, \qquad (1)$$

quand $|t|$ tend vers l'infini, uniformément dans toute bande verticale de largeur bornée.

Par suite, la condition (iii) implique que, dans R, pour $|t|$ suffisamment grand, on a $L_i(s) = O(\exp(|t|^k))$, k constante, pour $i = 1$ et 2; de plus, les fonctions $L_i(s)$ et $L_i^{-1}(s)$ sont bornées le long de toute droite verticale $\mathrm{Re}(s) = \sigma > 1 + c$.

D'autre part, d'après (1) et la relation $\Sigma_i a_i = \Sigma_i a_i'$, on a sur toute droite verticale:

$$\prod_i \Gamma(a_i s + b_i)/\Gamma(a_i'(1-s) + b_i') = O(|t|^m),$$

pour $|t|$ assez grand et m convenable (en effet, les termes en $\exp(-a_i \pi |t|/2)$ s'éliminent). On peut donc appliquer le théorème de Phragmen-Lindelöf ([5], p. 262), d'où la majoration $L_i(s) = O(|t|^m)$.

REMARQUE I.1.3: Des techniques classiques permettent alors de montrer, à partir de I.1.1 et I.1.2, le résultat suivant:

Il existe α tel que, pour tout entier m tel que $|m| \geqslant 2$, il existe T_m compris entre m et $m+1$ tel que, pour $i = 1$ ou 2, $\Lambda_i(s)$ n'a pas de zéro dans la bande $|t - T_m| < \alpha/\log|m|$. De plus, il existe B tel que, pour $i = 1$ ou 2, $|\Lambda_i'/\Lambda_i(\sigma + iT_m)| \leqslant B(\log|m|)^2$, pour $-1 < \sigma < 2$.

I.2. Formules explicites

Soit F une fonction réelle, définie sur $\mathbf{R}$, vérifiant les conditions suivantes:

(i) il existe $\epsilon > 0$ tel que $F(x)\exp((1/2 + c + \epsilon)x)$ soit sommable;

(ii) il existe $\epsilon > 0$ tel que $F(x)\exp((1/2 + c + \epsilon)x)$ soit à variation bornée, la valeur en chaque point étant la moyenne des limites à gauche et à droite;

(iii) la fonction $(F(x) - F(0))/x$ est à variation bornée.

On a alors la formule:

$$\sum_\rho \Phi(\rho) - \sum_\mu \Phi(\mu) + \sum_{i=1}^M I(a_i, b_i)$$

$$+ \sum_{i=1}^M J(a_i', b_i') = F(0)\log(AB)$$

$$- \sum_{p,i,k\geqslant 1} \left(\alpha_i^k(p) F(k\log p) + \beta_i^k(p)\, F(-k\log p)\right)\frac{\log p}{p^{k/2}}$$

où

$$I(a, b) = a\int_0^{+\infty} \left(f(ax)\, e^{-(a/2+b)x}/(1 - e^{-x}) - F(0)\, e^{-x}/x\right) dx$$

et

$$J(a, b) = a\int_0^{+\infty} \left(F(-ax)\,e^{-(a/2+b)x}/(1-e^{-x}) - F(0)\,e^{-x}/x\right) dx$$

et où ρ (resp. μ) parcourt les zéros (resp. les pôles) de Λ_1 de partie réelle comprise entre $-c$ et $1+c$, comptés avec leur multiplicité; la fonction Φ est définie par

$$\Phi(s) = \int_{-\infty}^{+\infty} F(x)\, e^{(s-1/2)x}\, dx;$$

d'autre part, on doit comprendre $\Sigma_\rho \Phi(\rho)$ comme $\lim_{T\to+\infty} \Sigma_{|\mathrm{Im}\rho|<T}\, \Phi(\rho)$.

La démonstration est calquée sur celle de [10]; on a l'égalité

$$\sum_{|\mathrm{Im}\rho|<T_m} \Phi(\rho) - \sum_{|\mathrm{Im}\mu|<T_m} = \left(\tfrac{1}{2}\pi i\right)\int \Phi(s)\Lambda_1'(s)/\Lambda_1(s)\, ds,$$

l'intégrale étant prise sur le bord d'une réctangle $[-a, 1+a]\times[-T_m, T_m]$ avec T_m tel que dans la Remarque I.1.3 et $a = c+\epsilon$, où ϵ est tel que $F(x)\, e^{1/2+c+\epsilon}$ est sommable et à variation bornée. La fonction Φ est alors $o(1/|t|)$ dans la bande verticale $-a \leqslant \mathrm{Re}(s) \leqslant 1+a$, et d'après I.1.3 les parties horizontales de l'intégrale tendent vers 0 quand T_m tend vers l'infini. D'autre part, l'équation fonctionnelle reliant Λ_1 et Λ_2 permet d'écrire l'intégrale sur les bords verticaux sous la forme

$$\frac{1}{2\pi i}\int_{1+a-iT}^{1+a+iT} \left(\Phi(s)\Lambda_1'(s)/\Lambda_1(s) + \Phi(1-s)\Lambda_2'(s)/\Lambda_2(s)\right) ds.$$

Montrons que $\int_{1+a-iT}^{1+a+iT} \Phi(s)\ \Lambda_1'(s)/\Lambda_1(s)$ tend vers

$$-\sum_{i,p,k} \alpha_i^k(p) F(k\log p) p^{-k/2} \log p - \sum_{i=1}^{M} I(a_i, b_i)$$

lorsque $T \to +\infty$;

cela suffit à démontrer la formule, si l'on remarque qu'on passe de $\Phi(s)$ à $\Phi(1-s)$ en remplaçant $F(x)$ par $F(-x)$.

Partie ultramétrique. On écrit $L_1'/L_1(s) = -\Sigma_{p,i,k\geqslant 1}\alpha_i^k(p)\ p^{-ks}\log p$, d'où:

$$\frac{1}{2\pi i}\int_{1+a-iT}^{1+a+iT} \Phi(s) L_1'/L_1(s)\, ds$$

$$= -\frac{1}{2\pi}\int_{-T}^{T}\left(\int_{-\infty}^{+\infty} F(x)\, e^{(1/2+a+it)x}\, dx\right)$$

$$\times\left(\sum \alpha_i^k(p) p^{-k(1+a+it)} \log p\right) dt$$

terme qui tend vers $-\sum \alpha_i^k\ (p)\ p^{-k/2} \log p\ F(k \log p)$, comme on le voit en recopiant la démonstration de Poitou ([10], p. 2).
Partie archimédienne. Posons

$$\varphi(t) = \Phi\left(\tfrac{1}{2} + it\right), \quad \text{et } G(s) = A^s \prod_{i=1}^{M} \Gamma(a_i s + b_i).$$

Le fait que $G'/G(s)$ soit $O(\log(|t|)$ dans toute bande verticale de largeur bornée permet de remplacer

$$\int_{1+a-iT}^{1+a+iT} \Phi(s) G'(s)/G(s)\ \mathrm{d}s \quad \text{par} \int_{\frac{1}{2}-iT}^{\frac{1}{2}+iT} \Phi(s) G'/G(s)\ \mathrm{d}s,$$

la différence de ces deux intégrales tendant vers 0 quand $T \to +\infty$. Il est clair que le terme correspondant à A^s tend vers $F(0)\log(A)$, les hypothèses faites sur F permettant d'appliquer la loi de réciprocité de Fourier. Il nous reste à examiner les intégrales de la forme

$$\int_{\frac{1}{2}-\mathrm{i}T}^{\frac{1}{2}+\mathrm{i}T} \Phi(s) \Gamma'/\Gamma(a_i s + b_i)\ \mathrm{d}s,$$

ou, si l'on préfère, en utilisant la fonction digamma $\psi(z) = \Gamma'(z)/\Gamma(z)$, les intégrales $\int_{-T}^{T} \varphi(t)\ \psi(\sigma + iat)\ \mathrm{d}t$ où $\sigma = a/2 + b$.

LEMME I.2.1. *On a l'égalité*

$$\frac{1}{2\pi} \int \varphi(t) \psi(\sigma + \mathrm{i}at)\ \mathrm{d}t = -\int_0^{+\infty} \left(\frac{F(ax)\ \mathrm{e}^{-\sigma x}}{1 - \mathrm{e}^{-x}} - F(0) \frac{\mathrm{e}^{-x}}{x} \right) \mathrm{d}x.$$

Pour démontrer ce lemme, on utilise le lemme suivant, démontré dans [10]:

LEMME I.2.2. *Soit $k(x)$ une fonction sommable et de carré sommable, et soit $\rho(t) = \int_{-\infty}^{+\infty} k(x)\ (1 - \mathrm{e}^{itx})/x\ \mathrm{d}x$; on suppose que $\rho(t)$ $\gamma(t)$ tend vers 0 quand $t \to +\infty$, avec $\gamma(t)$ transformée de Fourier de $(F(x) - F(0))/x$. Alors $(1/2\pi) \int_{-\infty}^{+\infty} \rho(t)\ \varphi(t)\ \mathrm{d}t$ converge et est égale à $\int_{-\infty}^{+\infty} k(x)\ (F(0) - F(x))/x\ \mathrm{d}x$.*

Rappelons que $\psi(s) = -\int_0^{+\infty} (\mathrm{e}^{-sx}/(1 - \mathrm{e}^{-x}) - \mathrm{e}^{-x}/x)\ \mathrm{d}x$, d'où

$$\psi(\sigma + iat) - \psi(\sigma) = -\int_0^{+\infty} \mathrm{e}^{-x} (\mathrm{e}^{-\mathrm{i}atx} - 1)/(1 - \mathrm{e}^{-x})\ \mathrm{d}x$$

$$= \int_{-\infty}^{+\infty} k(x)(1 - \mathrm{e}^{\mathrm{i}tx})/x\ \mathrm{d}x,$$

en posant $k(x) = e^{-\sigma x/a}(x/a)/(1 - e^{-x/a})$ si x est positif, et $k(x) = 0$ sinon. Le Lemme I.2.2 permet alors d'écrire

$$\frac{1}{2\pi}\int \varphi(t)(\psi(\sigma + iat) - \psi(\sigma))\, dt$$

$$= \int_0^{+\infty} (F(0) - F(ax))\, e^{-\sigma x}/(1 - e^{-x})\, dx,$$

d'où le Lemma I.2.1, et la démonstration des formules explicites.

II. Applications aux formes modulaires et aux courbes elliptiques

Soit $f(z) = \Sigma_{n \geq 0}\ a_n\, e^{2\pi i n z}$ une forme modulaire de poids k pour le groupe $\Gamma_0(N)$, et soit $L(s) = \Sigma_{n \geq 1}\ a_n n^{-s}$ la série de Dirichlet associée. Si f est une "newform" au sens d'Atkin-Lehner [2], on a un développement de L en produit d'Euler

$$L(s) = \prod_{p \mid N} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p \nmid N} \left(1 - a_p p^{-s} + p^{k-1-s}\right)^{-1}.$$

Deligne a montré [4] que, si p est un nombre premier ne divisant pas N, $|a_p| \leq 2p^{(k-1)/2}$, ce qui équivaut à dire que les racines α_p et α'_p du polynôme $T^2 - a_p T + p^{k-1}$ sont conjuguées de module $p^{(k-1)/2}$.

D'autre part, Atkin et Lehner ont montré [2] que, si p^2 divise N, $a_p = 0$, et que, si p divise exactement N, $a_p = \pm p^{(k/2)-1}$.

Le fait que f est une newform implique de plus que la fonction $\Lambda(s) = (\sqrt{N}/2\pi)^s \Gamma(s)\, L(s)$ est entière et vérifie l'équation fonctionnelle $\Lambda(s) = C\Lambda(k - s)$, C constante égale à ± 1. On se ramène immédiatement à une fonction satisfaisant aux conditions de I.1 en posant $L_1(s) = L_2(s) = L(s + (k-1)/2)$, et en prenant
$\Lambda_1(s) = \Lambda_2(s) = (\sqrt{N}/2\pi)^s\ \Gamma(s + (k-1)/2)\ L_1(s)$.

On peut à présent appliquer les formules I.2; on ne perd rien en généralité en supposant la fonction auxiliaire F paire, puisque $\Lambda_1 = \Lambda_2$. Posons d'autre part $b(p^m) = (a_p)^m$ si p divise N, et $b(p^m) = \alpha_p^m + \alpha'^m_p$ sinon. Alors, pour F paire vérifiant les conditions (i), (ii), (iii) de I.2, on obtient la formule:

$$\sum_{\rho} \Phi(\rho) + 2 \sum_{p,m} b(p^m) F(m \log p) \frac{\log p}{p^{mk/2}}$$

$$= F(0)(\log N - 2 \log 2\pi) - 2I_F$$

où

$$I_F = \int_0^{+\infty} \left(\frac{F(x)\, e^{-kx/2}}{1 - e^{-x}} - F(0) \frac{e^{-x}}{x} \right) dx.$$

Ici, ρ parcourt les zéros de L situés dans la bande critique $k/2 < \mathrm{Re}(s) < (k+1)/2$,
et on a posé

$$\Phi(s) = \int_{-\infty}^{+\infty} F(x)\, \mathrm{e}^{(s-k/2)x}\, \mathrm{d}x.$$

II.1. Majoration de l'ordre de L au centre de sa bande critique

Si r désigne l'ordre en $k/2$ de L, la formule précédente permet d'en obtenir de bonnes majorations, à l'aide de fonctions auxiliaires F convenables.

II.1.1. Majorations sans GRH

Soit F une fonction paire vérifiant les conditions (i), (ii), (iii) de I.1 et telle que $\mathrm{Re}\ \Phi(s)$ soit positive pour $(k-1)/2 < \mathrm{Re}(s) < (k+1)/2$.

Cela implique que $F(0) = \int_{-\infty}^{+\infty} \Phi(k/2 + \mathrm{i}t)\, \mathrm{d}t$ est strictement positive.

On peut donc choisir F telle que $F(0) = 1$, sans perdre de généralité. D'autre part, on a

$$I_F = \int_0^{+\infty} \left(F(x)\, \mathrm{e}^{-kx/2}/(1-\mathrm{e}^{-x}) - \mathrm{e}^{-x}/x \right) \mathrm{d}x$$

$$= -\psi\left(\frac{k}{2}\right) - \int_0^{+\infty} \mathrm{e}^{-kx/2}(1-F(x))/(1-\mathrm{e}^{-x})\, \mathrm{d}x.$$

On en déduit la majoration:

$$r\Phi\left(\frac{k}{2}\right) < \log N - 2\log 2\pi + 2\psi\left(\frac{k}{2}\right)$$

$$+2\int_0^{+\infty} (1-F(x))/(\mathrm{e}^x - 1)\, \mathrm{d}x$$

$$-2\sum_{p,m} b(p^m) F(m \log p)\, p^{-mk/2} \log p.$$

Le fait que $\psi(k/2) < \log(k/2)$ et que $|b(p^m)| < 2p^{(k-1)m/2}$ permet d'obtenir la majoration plus simple suivante:

$$r\Phi\left(\frac{k}{2}\right) < \log(k^2 N) - 2\log 4\pi + 2\int_0^{+\infty} (1-F(x))/(\mathrm{e}^x - 1)\, \mathrm{d}x$$

$$+4\sum_{p,m} \frac{F(m \log p)}{p^{m/2}} \log p$$

EXEMPLE: Soit g une fonction à support compact, de transformée de Fourier positive; posons $g_\lambda(x) = g(x/\lambda)$, et $F_\lambda(x) = g_\lambda(x)/\mathrm{ch}(x/2)$.

Il est connu (voir par ex. [10]) que la fonction Φ_λ attachée à F_λ a une partie réelle positive dans la bande critique. En faisant varier λ, on obtient ainsi une série de majorations, d'autant plus fines que λ est grand.

Prenons par example $g(x)$ paire, nulle en-dehors de $[-1, 1]$, et telle que $g(x) = 1 - |x|$ pour $x \in [-1, 1]$; choisissons $\lambda = \log 3$. La majoration ci-dessus s'écrit alors:

$$1{,}072r < \log(k^2N) - 2\log 4\pi + 2{,}4 + 0{,}683$$

soit:

$$1{,}072r < \log(k^2N) - 1{,}97.$$

En particulier, on a la majoration très simple: $r < \log k^2N$.

Il est clair que, pour une fonction L donnée, dont on connaît les premiers coefficients, on a intérêt à ne pas utiliser la majoration brutale $|a_p| \leqslant 2p^{(k-1)/2}$, mais la véritable valeur de a_p. Pour de petits niveaux N, les majorations obtenues sont généralement assez précises.

II.1.2. Majorations sous GRH

Nous supposons dans ce paragraphe que les seuls zéros de L situés dans la bande critique ont une partie réelle égale à $k/2$. Il suffit donc, pour obtenir des majorations de r, d'utiliser des fonctions F de transformée de Fourier $\varphi(t) = \int_{-\infty}^{+\infty} F(x)\, \mathrm{e}^{itx}\, \mathrm{d}x$ positive.

Soit donc F une fonction paire, à support compact, nulle en dehors de $[-1, 1]$, telle que pour tout x, $F(x) \leqslant 1$ et $F(0) = 1$. Pour λ réel positif, on pose $F_\lambda(x) = F(x/\lambda)$; si $\varphi_\lambda(t)$ est la transformée de Fourier de F_λ, on a la relation $\varphi_\lambda(t) = \lambda\varphi(\lambda t)$.

La fonction F étant toujours inférieure à 1, on peut majorer le terme non archimédien $|\Sigma_{p,m}\, b(p^m)\, F(m \log p) \log p/p^{mk/2}|$ par

$$\sum_{p^m \leqslant \mathrm{e}^\lambda} p^{-m/2} \log p$$

une utilisation facile du théorème des nombres premiers montre alors que ce terme est inférieur à $2\, \mathrm{e}^{\lambda/2} \log 3$ (en effet, $\Sigma_{p^m \leqslant x} \log p < x \log 3$ pour tout $x > 1$). On obtient donc une majoration de la forme:

$$\lambda r\varphi(0) < \log(k^2N) + 8\, \mathrm{e}^{\lambda/2} \log 3 - 2\log 4\pi + 2\int_0^{+\infty} (1 - F(x))/(\mathrm{e}^x - 1)\, \mathrm{d}x$$

à condition que F ait une transformée de Fourier positive sur $\mathbf{R}$.

En choisissant λ de l'ordre de 2 log log k^2N, on voit que

$$r = O\big(\log(k^2N)/\log\log(k^2N)\big).$$

Soit à présent une fonction F, paire, à support compact, vérifiant toujours les conditions (i), (ii) et (iii) de I.2, et dont la transformée de Fourier φ est positive sur $[-1, 1]$ et négative ailleurs (il n'est pas difficile de construire de telles fonctions: soit G de classe C^4, paire, à support compact, vérifiant les conditions (i), (ii) et (iii) de I.2 et de transformée de Fourier positive; alors la fonction $G + G''$, de transformée de Fourier $(1 - t^2)G$, vérifie les conditions requises). Soit à nouveau $F_\lambda(x) = F(x/\lambda)$; si t_0 est le premier zéro de L distinct de $k/2$ situé sur la droite critique $\mathrm{Re}(s) = k/2$, posons $\lambda = 1/t_0$. On a alors une minoration de r:

$$\lambda r\varphi(0) > \log Nk^2 - O(e^{\lambda/2})$$

obtenue par une méthode analogue à la précédente. Puisque $r = O(\log k^2N/\log\log k^2N)$, on en déduit l'existence d'une constante a telle que $\lambda > a \log\log k^2N$, c'est-à-dire $t_0 < K/\log\log k^2N$. D'où la proposition:

PROPOSITION II.1. *Soit f une newform de poids k pour le groupe $\Gamma_0(N)$, et soit L la série de Dirichlet associée. Supposons que les zéros de L situés dans la bande critique $k/2 - 1 < \mathrm{Re}(s) < k/2 + 1$ soient tous situés sur la droite $\mathrm{Re}(s) = k/2$ (hypothèse de Riemann généralisée). Alors:*

(*i*) *il existe une constante absolue A telle que l'ordre en $k/2$ de L soit majoré par $A \log k^2N/\log\log k^2N$.*

(*ii*) *Soit t_0 l'ordonnée du premier zéro de L distinct de $k/2$ et situé sur la droite $\mathrm{Re}(s) = k/2$. Il existe une constante absolue B telle que $|t_0| < B/\log\log k^2N$.*

II.2. Application aux courbes elliptiques

Soit E une courbe elliptique définie sur $\mathbf{Q}$, de conducteur N. Weil a conjecturé [15] que sa fonction L est la transformée de Mellin d'une newform de poids 2 pour la groupe $\Gamma_0(N)$. D'autre part, Birch de Swinnerton-Dyer ont conjecturé [3] que l'ordre en 1 de L est égal au rang de $E(\mathbf{Q})$, le groupe de Mordell-Weil de E. Si ces deux conjectures sont vérifiées, on peut donc déduire des formules explicites décrites précédemment une majoration du rang de $E(\mathbf{Q})$.

Nous supposons désormais que E vérifie les deux conjectures ci-dessus, et de plus que sa fonction L vérifie la conjecture de Riemann

généralisée. Si F est une fonction paire, telle que $F(0) = 1$ et vérifiant les conditions (i), (ii) et (iii) de I.2, la formule de I.2 s'écrit:

$$\sum_{\rho} \Phi(\rho) + 2 \sum_{p,m} b(p^m) F(m \log p) \frac{\log p}{p^m}$$

$$= \log N - 2 \log 2\pi - 2 \int_0^{+\infty} (F(x)/(e^x - 1) - e^{-x}/x)\, dx.$$

Dans ce qui suit, nous choisissons pour F la fonction utilisée par Odlysko pour obtenir ses minorations de discriminants de corps de nombres, égale à $(1 - |x|) \cos \pi x + \sin \pi |x|/\pi$ pour $x \in [-1, 1]$ et nulle ailleurs. Comme précédemment, pour réel positif, nous posons $F_\lambda(x) = F(x/\lambda)$; la fonction F est à transformée de Fourier positive, d'où pour λ une majoration de r, l'ordre en 1 de L, conjecturalement égal au rang de $E(\mathbf{Q})$, de la forme:

$$\lambda r \varphi(0) \leqslant \log N - 2 \sum_{p^m \leqslant e^\lambda} b(p^m) F(m \log p) \frac{\log p}{p^m} - M_\lambda$$

où

$$M_\lambda = 2\left(\log 2\pi + \int_0^{+\infty} (F_\lambda(x)/(e^x - 1) - e^{-x}/x)\, dx\right).$$

Ici, $\varphi(0) = 8/\pi^2$ et l'intégrale $I_\lambda = \int_0^{+\infty} (F_\lambda(x)/(e^x - 1) - e^{-x}/x)\, dx$ tend vers $y = 0{,}577\ldots$ lorsque $\lambda \to +\infty$. Le tableau ci-dessous donne quelques valeurs de M_λ:

λ	log 17	log 19	log 23	log 50	log 100
M_λ	3,727...	3,777...	3,888...	4,102...	4,239...

Il suffit donc, pour obtenir la majoration (1), de calculer a_p pour $p < e^\lambda$, ce qui revient à calculer N_p, le nombre de points de E modulo p, qui est lié à a_p par la formule $a_p = p + 1 - N_p$.

Le résultat remarquable est qu'il suffit généralement de calculer un petit nombre de N_p pour avoir une bonne approximation de r. Prenons par exemple $\lambda = \log 23$; la majoration devient:

$$r \leqslant 0{,}3935 \log N - 1{,}530 - 0{,}786 \sum_{p^m \leqslant 19} b(p^m) F(m \log p) \frac{\log p}{p^m}$$

qui nécessite seulement le calcul de a_p pour $p \leqslant 19$. Dans le tableau

ci-dessous, nous indiquons les majorations obtenues pour quelques unes des courbes des tables de [8]:

N	11 B	14 C	15 C	17 C	19 B	20 B	21 B	24 B	26 B	26 D
$r \leqslant$	0,0014	0,051	0,0088	0,0015	0,0012	0,0013	0,0157	0,0154	0,0592	0,0684
r	0	0	0	0	0	0	0	0	0	0
N	189 F	189 C	196 A	196 C	197 A	200 G	200 B	200 A	200 E	200 C
$r \leqslant$	0,430	1,003	1,006	0,206	1,087	0,432	0,942	0,106	0,185	1,011
r	0	1	1	0	1	0	0	0	0	1

On peut d'autre part majorer brutalement a_p par $-E(2p^{1/2})$, où $E(x)$ est la partie entière de x, et calculer les majorations obtenues. Prenons par exemple $\lambda = \log 100$. On obtient la majoration

$$r < 0{,}268 \log N + 1{,}03,$$

qui se révèle assez précise pour de petits conducteurs. Dans le tableau ci-dessous, je donne la majoration obtenue pour les courbes qui, parmi celles que je connais, ont le plus petit conducteur pour un rang donné inférieur à 8:

Soit E: $y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$.

α_1	α_2	α_3	α_4	α_6	N	r	$r \leqslant$
0	−1	1	0	0	11	0	1,702
0	0	1	−1	0	37	1	2,0411
0	1	1	−2	0	389	2	2,699
0	0	1	−7	6	5077	$\geqslant 3$	3,317
0	0	1	−7	36	545723	$\geqslant 4$	4,571
0	−21	67	−10	30	179843077	$\geqslant 5$	6,125
0	−63	351	56	22	$5{,}17\ldots 10^{10}$	$\geqslant 6$	7,64
0	−168	1641	161	−8	$3{,}27\ldots 10^{12}$	$\geqslant 7$	9,08
−2	737	531	1262	−110	$1{,}79\ldots 10^{15}$	$\geqslant 8$	10,42

Notons que pour une courbe E ayant partout réduction semi-stable et vérifiant les conjectures de Weil et de Birch et Swinnerton-Dyer, le rang est pair si et seulement si le nombre de nombres premiers où E a une réduction multiplicative déployée est impair. Cela permet parfois d'améliorer la majoration obtenue par les formules ci-dessus, par exemple pour la sixième (resp. 7e) courbe du tableau précédent, dont l'examen des places divisant N montre que le rang est impair (resp. pair).

REMARQUE: Dans ce tableau, les six dernières courbes ont été obtenues par la méthode explicitée dans le paragraphe suivant. On obtient une minoration de leur rang en exhibant un nombre convenable de points indépendants, mais il est a priori possible que le rang soit supérieur à ce nombre. Si les conjectures citées précédemment sont exactes, le rang de ces courbes est exactement celui indiqué dans l'avant-dernière colonne:

seules les deux dernières courbes posent problème d'après le tableau; néanmoins, en prenant $\lambda = \log 500$ dans les formules précédentes, on trouve la majoration

$$r < 0{,}1986 \log N + 2{,}46,$$

qui donne une majoration de 8,17 (resp. 9,44) pour l'avant-dernière (resp. la dernière) courbe. La remarque précédente sur la parité du rang permet, après examen des diverses places à mauvaise réduction, de conclure.

Le fait que les majorations précédentes sont bonnes provient de ce que les zéros de L autres que 1 sont "assez" éloignés de 1, comme on peut le remàrquer expérimentalement pour les courbes ci-dessus. Plus précisément, il semble que l'ordonnée minimale d'un tel zéro soit de l'ordre de $1/\log N$. Un tel résultat paraît difficile à prouver dans le cas général. On peut néanmoins le montrer pour une classe de fonctions L assez large:

Soit f une "newform" pour le groupe $\Gamma_0(N)$, et soit $L(s)$ la série de Dirichlet associée. La fonction f est réelle sur la demi-droite des imaginaires purs d'ordonnée strictement positive; en suivant Mazur et Swinnerton-Dyer [6], appelons point critique fondamental d'ordre impair de f (ou de L) un point de cette demi-droite où f change de signe. Si r désigne l'ordre en 1 de L, Mazur et Swinnerton-Dyer montrent dans [6] que r est inférieur ou égal au nombre de points critiques fondamentaux de f, et de même parité. D'autre part, parmi toutes les courbes de conducteur $\leqslant 430$, il n'en existe que 17 pour lesquelles r est strictement inférieur à ce nombre de points. Nous démontrons ici le résultat suivant:

THÉORÈME: *Soit f une "newform" de poids k pour le groupe $\Gamma_0(N)$, et soit L la série de Dirichlet associée. Supposons que le nombre de points critiques fondamentaux d'ordre impair de f soit égal à l'ordre en $k/2$ de L. Alors, si s est un zéro de L distinct de $k/2$, on a l'inégalité*:

$$|s - (k/2)| > C_0/\log(kN),$$

où C_0 est une constante absolue (on peut par exemple prendre $C_0 = 1/10$).

Posons $g(t) = f(it/\sqrt{N}) = \sum_n a_n \exp(-2\pi nt/\sqrt{N})$ pour $t > 0$. Deligne a montré que, si p ne divise pas N, $|a_p| \leqslant 2p^{(k-1)/2}$. D'autre part, les résultats d'Atkin-Lehner [2] montrent que ceci est vrai si p divise N. Donc, pour tout n, $|a_n| \leqslant \sigma_0(n) n^{(k-1)/2} \leqslant n^{(k+1)/2}$. Si $q = \exp(-2\pi t/\sqrt{N})$, une majoration immédiate de $a_2 q + a_3 q^2 + a_4 q^3 + \ldots$ donne le lemme:

LEMME 1: $t \geqslant k\sqrt{N} \Rightarrow 0{,}9\ q < g(t) < 1{,}1\ q$.

Désignons par $t_1, \ldots, t_r$ les points critiques fondamentaux d'ordre impair de f, et posons

$$P(X) = \prod_{i=1}^{r} (X - \log t_i) = \prod_{i=1}^{r} (X - x_i),$$

où $x_i = \log t_i$.

LEMME 2. *Soit j un entier supérieur ou égal à r; le polynôme Q_j, quotient de X^j par P est donné par*:

$$Q_j(X) = \sum_{i=0}^{j-r} c_i X^{j-r-i}, \quad \text{avec } c_i = \sum_{\Sigma r_l = i} \prod_{l=1}^{r} x_l^{n_l}.$$

D'autre part, les c_i sont tout positifs ou nuls.

En effet, le développement en puissances croissantes de $1/P(X)$ s'écrit

$$1/\prod_{i=1}^{r} (X - x_i) = X^{-r} \prod_{i=1}^{r} \left(1 + (x_i/X) + (x_i/X)^2 + \ldots\right),$$

d'où Q_j et les c_i. Le fait qu'ils sont positifs provient de ce que, si x_i est une racine de P, $-x_i$ en est également une, d'après l'équation fonctionnelle de f.

Let zéros de L dans la bande critique sont les mêmes que ceux de la fonction

$$\Lambda(s) = \left(\sqrt{N}/2\pi\right)^s \Gamma(s) L(s) = \int_0^{+\infty} g(t) t^{s-1}\, \mathrm{d}t.$$

Or l'équation fonctionnelle de f implique que, pour $t > 0$, $g(1/t) = Ct^k g(t)$, avec $C = \pm 1$. Par suite:

$$\lambda(s) = \int_0^{+\infty} t^{s-1} g(t)\, \mathrm{d}t = \int_1^{+\infty} g(t) t^{(k/2)-1} \left(t^{(s-k)/2} + Ct^{(k/2)-s}\right) \mathrm{d}t$$

$$= \sum_{j=0}^{+\infty} I_j (s - k/2)^j \left(1 + C(-1)^j\right)/j!$$

où $I_j = \int_1^{+\infty} g(t) t^{(k/2)-1} \log^j t\, \mathrm{d}t$.

L'hypothèse de la proposition implique que les dérivées de Λ en 1 d'ordre strictement inférieur à r sont nulles, donc:

$$\lambda(s) = \sum_{j \geqslant r} I_j (s - k/2)^j \left(1 + C(-1)^j\right)/j!. \qquad (1)$$

LEMME 3: *Soit* $\alpha_j = (j-r)kN$; *on a l'inégalité, pour* $j > r$, *et* $j-r$ *pair*:

$$|I_j| \leqslant C_1 I_r Q_j(\log \alpha_j)$$

où C_1 *est une constante absolue.*

Admettons provisoirement ce lemme, et montrons qu'il entraîne la proposition.

En effet, d'après le lemme 1, les t_i sont inférieurs à $k\sqrt{N}$, donc à α_j pour $j > r$. Il est alors clair, d'après le Lemme 2, que

$$Q_j(\operatorname{Log} \alpha_j) \leqslant \binom{j}{r} (\log \alpha_j)^{j-r}.$$

Soit alors C_2 une constante telle que, pour tout couple a, b de réels $\geqslant \log 2$, on a: $a+b \leqslant C_2 ab$, et soit C_3 une constante majorant, pour tout $x \geqslant 2$, $\log^x x/x!$; on obtient alors comme majoration de I_j:

$$|I_j| \leqslant C_1 C_3 (C_2 \log(Nk))^{j-r} j!/r!.$$

Soit à présent s zéro de Λ; d'après (1), on doit avoir:

$$I_r/r! = -\sum_{j=r+2}^{+\infty} I_j (s-k/2)^{j-r}/j!,$$

la sommation du membre de droite étant effectuée sur les j de même parité que r. D'après ce qui précède, on en déduit que

$$1 < C_1 C_3 \sum_{j=1}^{\infty} (C_2 \log(Nk)\,|s-k/2|)^{2j},$$

ce qui implique que

$$|s-k/2| \geqslant 1/C_2\sqrt{1+C_1C_3}\log(kN).$$

D'où la proposition.

Il nous reste à démontrer le Lemme 3. Soit donc $\alpha_j = (j-r)kN$; on a:

$$I_j = \int_1^{+\infty} g(t) t^{(k/2)-1} \log^j t \, dt$$

$$= \int_1^{+\infty} g(t) t^{(k/2)-1} P(\log t) Q_j(\log t) \, dt,$$

grâce au Lemme 2 et au fait que le reste R_j de la division de X^j par P est formé de monômes de même parité que r.

Le point important est qu'à présent la fonction $g(t)P(\log t)$ est positive pour $t \geqslant 1$; on en déduit immédiatement la majoration:

$$\int_1^{\alpha_1} g(t)P(\log t)Q_j(\log t)t^{(k/2)-1}\,dt \leqslant I_r Q_j(\log \alpha_j).$$

Il reste à majorer $\int_{\alpha_j}^{+\infty} g(t)\ P(\log t)\ Q_j(\log t)t^{(k/2)-1}\,dt$. Le Lemme 1 nous en donne une première majoration par 1.1:

$$\int_{\alpha_j}^{+\infty} e^{-2\pi t/\sqrt{N}} t^{(k/2)-1} P(\log t)Q_j(\log t)\,dt.$$

Soit J cette dernière intégrale; remarquons que, pour $x > \sup x_t$, on a $P'(x)/P(x) \leqslant r/(x - \sup(x_t)$, et $Q'(x)/Q(x) \leqslant (j-r)/x$. Une intégration par parties de J nous permet alors d'obtenir la majoration:

$$\begin{aligned} J &\leqslant \sqrt{N}/2\pi\, e^{-2\pi\alpha_j/\sqrt{N}} \alpha_j(k/2) - 1S(\log \alpha_j) \\ &\quad + \sqrt{N}/2\pi \int_{\alpha_j}^{+\infty} t^{(k/2)-2}\, e^{-2\pi t/\sqrt{N}} S(\log t) \\ &\quad \times \left((k/2) - 1 + r/\log\left(t/k\sqrt{N}\right) + (j-r)/\log t\right) dt \end{aligned}$$

où on a posé $S(X) = P(X)Q_j(X)$; on sait d'autre part (II.1.1) qu'on a la majoration $r \leqslant \log(k^2 N)$; la seconde intégrale de la majoration ci-dessus est alors majorée par $3J/2\pi$, d'où l'inégalité:

$$J \leqslant 2\sqrt{N}/2\pi\, e^{-2\pi\alpha_j/\sqrt{N}} \alpha_j^{(k/2)-1} S(\log \alpha_j).$$

D'autre part, d'après le Lemme 1, il est clair que

$$\begin{aligned} I_r &\geqslant 0{,}9 \int_{\alpha_j}^{+\infty} e^{-2\pi t/\sqrt{N}} t^{(k/2)-1} P(\log t)\,dt \\ &> 0{,}9\sqrt{N}/2\pi\, e^{-2\pi\alpha_j/\sqrt{N}} P(\log \alpha_j)\alpha_j^{(k/2)-1} \end{aligned}$$

d'où $J \leqslant 2{,}3\ I_r\ Q_j(\log \alpha_j)$ et enfin que $I_j \leqslant C_1\ I_r\ Q_j(\log \alpha_j)$ où l'on peut prendre pour C_1 la valeur 3,6 (à vrai dire, un calcul plus fin de J permet de montrer que l'on peut pendre pour C_1 la valeur 1,1). D'où le Lemme 3, et la proposition.

Si E est une courbe elliptique définie sur $\mathbf{Q}$, une conjecture assez crédible affirme que, pour tout entier M, il existe un corps quadratique K (ou, si l'on préfère, une courbe E_χ définie sur $\mathbf{Q}$, obtenue à partir de E par torsion par un caractère quadratique) tel que $E(K)$, groupe des points de E rationnels sur K (resp. $E_\chi(\mathbf{Q})$) ait un rang supérieur à M. Le versant modulaire de cette conjecture, via la conjecture de Birch et Swinnerton-Dyer, est que, pour toute forme modulaire f de poids k, et pour tout entier M, il existe un caractère quadratique χ tel que M soit

inférieur à l'ordre en $k/2$ de la série L_χ, transformée de Mellin de f_χ, "tordue" de f par χ. Au vu des considérations précédentes, on peut se demander si, f étant une "newform" de poids k pour le groupe $\Gamma_0(N)$, pour tout entier M, il existe un caractère quadratique χ tel que le nombre de points critiques fondamentaux d'ordre impair de f_χ soit supérieur à M. La réponse est affirmative:

PROPOSITION: *Soit f une newform de poids k pour le groupe $\Gamma_0(N)$. Alors, pour tout entier M, il existe un caractère quadratique χ tel que M soit inférieur au nombre de points critiques fondamentaux d'ordre impair de f_χ, "tordue" de f par χ.*

En effet, soit f une telle forme, et soit Q le nombre de ses points critiques fondamentaux d'ordre impair; on peut toujours supposer $Q \geqslant 1$ (si $Q = 0$, on tord f par un caractère χ de conducteur m tel que $\chi(-N) = -1$, ce qui assure que $i\sqrt{Nm}$ est un point critique fondamental d'ordre impair de f_χ, la constante de l'équation fonctionnelle de f_χ étant égale à -1). Soient $t_1 < t_2 < \ldots < t_Q$ les ordonnées des points critiques, et posons $\rho = \inf_i \sup_{t_i < t < t_{i+1}} |f(it)|$.

D'après le Lemme 1, on sait que, pour tout i, $1/Nk \leqslant t_i$. Posons $q = e^{-2\pi/kN}$, et soit n_0 un entier tel que $\sum_{n \geqslant n_0} n^{(k+1)/2} q^n < \rho$.

Considérons alors un caractère quadratique χ de conducteur m premier à N et supérieur à $k\sqrt{N}$, et tel que, pour tout n inférieur à n_0, $\chi(n) = 1$.

Par construction, f_χ change au moins Q fois de signe sur l'intervalle $[i/m\sqrt{N}, i\infty[$, et son nombre de points critiques fondamentaux est donc supérieur à $2Q$. Un raisonnement par récurrence permet de conclure.

II.3. Obtention de courbes elliptiques de rang élevé

L'examen des formules explicites de II.1 semble indiquer que, pour qu'une courbe elliptique ait un rang élevé, il est bon que les coefficients a_p de sa fonction L soient négatifs et de valeur absolue la plus grande possible, c'est-à-dire que N_p, le nombre de points de E modulo p, soit le plus grand possible pour de nombreux nombres premiers.

L'expérience montre qu'effectivement, si l'on construit de telles courbes, leur rang est souvent non nul, et semble même croître à condition de fixer un nombre suffisant de congruences. L'algorithme exact utilisé pour les calculs est décrit dans [7].

Nous donnons ici les courbes qui, parmi toutes celles trouvées par cette méthode, ont le plus petit conducteur, et pour lesquelles on a trouvé un système de r points indépendants, pour r compris entre 3 et 14. Chaque courbe est donnée par les coefficients a_1, a_2, a_3, a_4, a_6 d'une équation minimale de Weierstrass:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Nous indiquons également le discriminant D, le conducteur N, les abscisses de r points indépendants, ainsi que le nombre de points entiers d'abscisse $< M$. Pour $r = 3$, 4 ou 5, on donne la liste des abscisses de ces points. Il n'est évidemment pas exclu qu'il existe d'autres points entiers d'abscisse supérieure.

D'autre part, le rang de ces courbes peut a priori être strictement supérieur à r; néanmoins, les formules explicites de I.1.2 permettent de montrer qu'il y a égalité pour les courbes dont la fonction L vérifie l'hypothèse de Riemann généralisée et les conjectures de Weil et de Birch et Swinnerton-Dyer.

- $r = 3$
  $a_1 = 0,\ a_2 = 0,\ a_3 = 1,\ a_4 = -7,\ a_6 = 6$
  $D = N = 5077$
  Abscisses de 3 points indépendants: $x = -3, -2, -1$.
  Il y a 18×2 points entiers d'abscisse inférieure à $M = 1000000$: $x = -3, -2, -1, 0, 1, 2, 3, 4, 8, 11, 14, 21, 37, 52, 93, 342, 406, 816$.
- $r = 4$
  $a_1 = 0,\ a_2 = 0,\ a_3 = 1,\ a_4 = -7,\ a_6 = 36$
  $D = -N = -545723$
  Abscisses de 4 points indépendants: $x = -4, -3, -2, -1$.
  Il y a 28×2 points entiers d'abscisse inférieure à $M = 1000000$: $x = -4, -3, -2, -1, 1, 2, 3, 4, 6, 9, 15, 17, 32, 36, 40, 43, 118, 139, 149, 172, 218, 1689, 4962, 9733, 13613, 13771, 31601, 383540$.
- $r = 5$
  $a_1 = 0,\ a_2 = -21,\ a_3 = 67,\ a_4 = -10,\ a_6 = 30$
  $D = N = 179843077$
  Abscisses de 5 points indépendants: $x = -6, -5, 1, 2, 5$.
  Il y a 31×2 points entiers d'abscisse inférieure à $M = 1000000$: $x = -6, -5, 1, 2, 5, 6, 8, 9, 18, 19, 20, 23, 27, 40, 46, 61, 75, 88, 96, 127, 204, 209, 240, 629, 1503, 1553, 2510, 4374, 4559, 37473, 42421$.
- $r = 6$
  $a_1 = 0,\ a_2 = -63,\ a_3 = 351,\ a_4 = 56,\ a_6 = 22$
  $D = N = 51714450757$
  Abscisses de 6 points indépendants: $x = -19, -16, -15, -2, 3, 4$.
  Il y a 45×2 points entiers d'abscisse inférieure à $M = 2000000$.
- $r = 7$
  $a_1 = 0,\ a_2 = -168,\ a_3 = 1641,\ a_4 = 161,\ a_6 = -8$
  $D = N = 3274452416197$
  Abscisses de 7 points indépendants: $x = -53, -52, -46, -43, -41, -24, -17$.
  Il y a 69×2 points entiers d'abscisse inférieure à $M = 3000000$.
- $r = 8$
  $a_1 = -2,\ a_2 = 737,\ a_3 = 531,\ a_4 = 1262,\ a_6 = -110$
  $D = -N = 1797078886904843$
  Abscisses de 8 points indépendants: $x = -737, -682, -679, -664,$

$-642, -636, -605, -595.$

Il y a 90×2 points entiers d'abscisse inférieure à $M = 3000000$.

- $r = 9$

$a_1 = 0,\ a_2 = 3576,\ a_3 = 9767,\ a_4 = 425,\ a_6 = -2412$

$D = -N = 70024818441029590043$

Abscisses de 9 points indépendants: $x = -3527, -3477, -3304, -3276, -3205, -3183, -3090, -2981, -2702.$

Il y a 91×2 points entiers d'abscisse inférieure à $M = 4000000$.

- $r = 10$

$a_1 = 0,\ a_2 = -15336,\ a_3 = 1461695,\ a_4 = -415,\ a_6 = -80334$

$D = N = 51806242738325750394997$

Abscisses de 10 points indépendants: $x = -5109, -4994, -4549, -4475, -4123, -3882, -3817, -2981, -2671, -2600.$

Il y a 120×2 points entiers d'abscisse inférieure à $M = 4000000$.

- $r = 11$

$a_1 = -64,\ a_2 = -9007,\ a_3 = 1066633,\ a_4 = -1499708,\ a_6 = -1006950$

$D = N = 18034061681836267671024 37$

Abscisses de 11 points indépendants: $x = -5965, -5880, -5852, -5639, -5548, -5500, -5325, -5247, -5003, -4950, -4833.$

Il y a 170×2 points entiers d'abscisse inférieure à $M = 3500000$.

- $r = 12$

$a_1 = -246,\ a_2 = -89199,\ a_3 = 36599029,\ a_4 = -19339780,\ a_6 = -36239244$

$D = N = 26960171259013040954494249 7797$

Abscisses de 12 points indépendants: $x = 74111, 74183, 74203, 74322, 74357, 74487, 74589, 74702, 74855, 74905, 75513, 75798.$

Il y a 165×2 points entiers d'abscisse inférieure à $M = 3500000$.

- $r = 13$

$a_1 = 0,\ a_2 = 0,\ a_3 = 1,\ a_4 = -6084700339627,\ a_6 = 5849846670724704096$

$D = -N = -213704722035407048330451124880441901323$

Abscisses de 13 points indépendants: $x = -1302989, -1302202, -1301486, -1297698, -1274967, -1262185, -1247135, -1218648, -1194464, -1165483, -1160169, -1134412, -1037679.$

Il y a 117×2 points entiers d'abscisse inférieure à $M = 4000000$.

- $r = 14$

$a_1 = 0,\ a_2 = 2597055,\ a_3 = 357573631,\ a_4 = -549082,\ a_6 = -19608054$

$D = -N = -362753324321317159846799 43280544970923$

Abscisses de 14 points indépendants: $x = -2581568, -2561042, -2549928, -2530674, -2513636, -2487058, -2477635, -2445531, -2423028, -2389860, -2359927, -2324873, -2239499, -2231702.$

Il y a 184×2 points entiers d'abscisse inférieure à $M = 4200000$, Si l'on pousse la recherche plus loin, on trouve 256×2 points entiers d'abscisse inférieure à 700000000.

III. Application aux groupes de cohomologie des variétés algébriques

Soit K un corps de nombres, de degré n et de discriminant D, et soit X une variété algébrique projective non singulière définie sur K; l'ensemble $X(\mathbf{C})$ des points de X à valeurs dans $\mathbf{C}$ est alors muni d'une structure de variété analytique complexe, et $H^m(X(\mathbf{C}), \mathbf{C})$ se décompose en une somme de sous-espaces de Hodge $V^{p,q}$ $(p+q=m)$ de dimension $h(p, q)$, avec $\Sigma_{p,q} h(p, q) = B_m$, le m$^{\text{ième}}$ nombre de Betti de $X(\mathbf{C})$.

D'autre part, si v est une place non-archimédienne de K, de norme Nv, on sait associer à X un entier f_v et un polynôme $P_{m,v}(T) = \prod_{\alpha=1}^{B_{m,v}}(1 - \lambda_{\alpha,v} T)$,
tels que $B_{m,v} \leqslant B_m$, $|\lambda_{\alpha,v}| \leqslant Nv^{m/2}$ et $f_v \geqslant 0$ (ces trois inégalités devenant des égalités si X a bonne réduction en v), et tels qu'il semble raisonnable de faire la conjecture suivante:

$$\text{Soit } N = \prod_v Nv^{f_v}, \quad \text{et } A = \left(N \mid D \mid^{B_m} (2\pi)^{-nB_m} \right)^{1/2};$$

la fonction

$$\Lambda(s) = A^s \left(\prod_{p<q} \Gamma(s-p)^{h(p,q)} \right)^n \prod_v \frac{1}{P_m(Nv^{-s})}$$

qui converge a priori pour $\mathrm{Re}(s) > (m/2) + 1$, se prolonge en une fonction entière, d'ordre 1, et vérifie l'équation fonctionnelle
$\Lambda(s) = w\Lambda(m + 1 - s)$,
où w vaut ± 1.

Les définitions de f_v et $P_{m,v}$ sont données dans [11].

Par la translation $s \mapsto s + (m/2)$, on se ramène au cas des fonctions définies dans I.1, et on peut donc appliquer les formules explicites de I.2: si F est une fonction réelle, paire, vérifiant $F(0) = 1$ et les conditions (i), (ii) et (III) de I.2, et si $\Phi(s) = \int_{-\infty}^{+\infty} F(x)\, \mathrm{e}^{(s-(m+1)/2)x}\, \mathrm{d}x$ on a la formule:

$$\sum_\rho \Phi(\rho) = 2 \sum_{v,\alpha,k} (\lambda_{\alpha,v})^k F(k \log(Nv)) \frac{\log(Nv)}{(Nv)^{k(m+1)/2}}$$

$$= 2 \log A - n \sum_{p,q} h(p, q) I_{p,q}$$

où

$$I_{p,q} = \int_0^{+\infty} \left(F(x)\, \mathrm{e}^{-(m/2 - \inf(p,q))x}/2\ sh(x/2) - \mathrm{e}^{-x}/x \right) \mathrm{d}x$$

et où ρ parcourt les zéros de Λ tels que $m/2 < \mathrm{Re}(\rho) < 1 + m/2$.

Soit $f(x)$ la fonction d'Odlyzko déjà définie dans II, paire, nulle en dehors de $[-1, 1]$, telle que, pour $0 \leqslant x \leqslant 1$, on ait:

$$f(x) = (1 - x)\cos(\pi x) + \sin(\pi x)/\pi.$$

On pose également, pour λ positif, $F_\lambda(x) = F(x/\lambda)/\mathrm{ch}(x/2)$. La fonction Φ_λ associée à F_λ a alors une partie réelle positive dans la bande critique $m/2 \leqslant \mathrm{Re}(s) \leqslant 1 + m/2$; de plus, il est clair que pour tout couple (p, q), on a $I_{p,q} \geqslant I_{0,m}$, d'où la minoration de A:

$$2 \log A \geqslant nB_m I_{0,m} + 2 \sum_{Nv \leqslant e^\lambda, k} (\lambda_{\alpha,v})^k F_\lambda(k \log(Nv)) \frac{\log(Nv)}{(Nv)^{k(m+1)/2}}.$$

Prenons par example $\lambda = \log 2$; les intégrales $I_{0,m}$ correspondantes décroissent quand m croît, et le terme non archimédien est évidemment nul. Pour $m = 11$, on trouve alors une minoration de $\log(N \mid D \mid^{B_m})$ de $-0{,}064n\ B_m$, ce qui ne fournit aucun renseignement; par contre, pour $m = 10$, on trouve $\log(N \mid D \mid^{B_m}) > 0{,}0033n\ B_m$; comme nous nous sommes restreints à des valeurs de m impaires, nous en déduisons que, pour m impair $\leqslant 9$, $N \mid D \mid^{B_m}$ est strictement supérieur à 1, pourvu que B_m soit non nul. En particulier, si X est une variété abélienne de dimension r définie sur $\mathbf{Q}$, on a $B_1 = 2r$; par suite, si les conjecture standard sur sa fonction L sont vérifiées, elle ne peut pas avoir bonne réduction partout.

A vrai dire, dans le cas des variétés abéliennes, on peut améliorer ce résultat: comme me l'a fait remarquer Oesterlé, Serre a en effet démontré [12], que, si A est une variété abélienne de dimension g définie sur le corps fini $\mathbf{F}_q$ à q éléments, la somme $\Sigma\lambda_i$ des valeurs propres du Frobenius agissant sur le premier groupe de cohomologie de A est majorée par $gE(2q^{1/2})$; par suite, si A est une variété abélienne définie sur $\mathbf{Z}$, pour tout p, les racines du polynôme $P_{1,p}(T) = \pi(1 - \lambda_{i,p}T)$ vérifient $|\Sigma\, \lambda_{i,p}| \leqslant g\ E(2\sqrt{p})$ (en cas de mauvaise réduction de A en p, il suffit de décomposer $P_{1,p}$ en trois polynômes à coefficients entiers correspondant respectivement à la partie abélienne de A mod p, où on peut appliquer le résultat de Serre, à la partie multiplicative, où les λ_i sont de module 1, et à la partie unipotente, où ils sont nuls).

Alors, en prenant $\lambda = 1{,}33$ dans les formules ci-dessus, on trouve la minoration $N > 10{,}32^g$, où N est le conducteur de A.

On en déduit:

PROPOSITION: *Soit A une variété abélienne définie sur $\mathbf{Q}$, de dimension $r \geqslant 1$ et de conducteur N. Supposons que sa fonction L soit prolongeable en une fonction entière, et que la fonction $\lambda(s) = N^{s/2}((2\pi)^{-s}\ \Gamma(s))^r\ L(s)$ soit entière, d'ordre 1, et vérifie l'équation fonctionnelle $\Lambda(s) = w\Lambda(2 - s)$, avec $w = \pm 1$.*

Alors on a l'inégalité $N > 10^r$. En particulier, A ne peut pas avoir partout bonne réduction.

REMARQUE 1: Plus généralement, les minorations précédentes montrent qu'il n'existe pas de motif non nul défini sur $\mathbf{Z}$ de poids impair $\leqslant 9$,

ayant bonne réduction partout et dont la fonction L vérifie les conjectures standard. Le fait que la série $\sum_n \tau(n)n^{-s}$, τ étant la fonction de Ramanujan, se comporte comme la série L d'un motif sur $\mathbf{Z}$ de poids 11 ayant bonne réduction partout montre que 9 est la meilleure borne possible.

REMARQUE 2: On pourrait faire des calculs analogues pour m pair. Néanmoins, dans ce cas, la facteur archimédien est plus complexe, et d'autre part la fonction L attachée au $m^{\text{ième}}$ groupe de cohomologie peut avoir des pôles.

REMARQUE 3: Soit E une courbe elliptique définie sur un corps quadratique de discriminant D, et dont la fonction L est prolongeable en une fonction entière et vérifie l'équation fonctionnelle habituelle.

Les minorations ci-dessus montrent qu'elle ne peut pas avoir bonne réduction partout si $|D| \leqslant 10$. A vrai dire, on peut affiner les calculs, notamment en tenant compte de facteurs locaux dans le terme non archimédien. Examinons par exemple le cas des corps quadratiques réels: Stroeker (resp. Tate, resp. Oort) ont trouvé des exemples de courbes ayant bonne réduction partout sur $\mathbf{Q}(\sqrt{D})$, avec $D = 28$ (resp. 29, resp. 41).

Les formules explicites décrites plus haut permettent d'éliminer les discriminants inférieurs à 28, sauf 17, 21 et 24 (toujours sous l'hypothèse d'une équation fonctionnelle pour la fonction L de E). Les cas $D = 17$, et $D = 21$ restent en suspens; par contre, on peut exhiber la courbe suivante, définie sur $\mathbf{Q}(\sqrt{24})$, et ayant bonne réduction partout:

$$y^2 + (2 - \sqrt{6})xy + (1 - \sqrt{6})y$$
$$= x^3 - (162 + 66\sqrt{6})x - (1122 + 498\sqrt{6})$$

de discriminant $5 + 2\sqrt{6}$, qui est une unité fondamentale de $\mathbf{Q}(\sqrt{6})$.

Appendice

La plupart des calculs indiqués dans cet article ont été effectués à l'aide d'une simple calculatrice de poche; certains ont nécessité l'emploi d'un micro-ordinateur, en l'occurrence le ZX 81 de Sinclair.

Enfin, notamment pour l'obtention des courbes de rang 12 (resp. 13, 14) du §II.3, on a utilisé l'Univac de l'Université d'Orsay (resp. l'IBM 4341 de l'ENS, rue d'Ulm).

Il est bon de donner quelques précisions concernant la validité de ces calculs; les plus délicats à justifier sont sans doute les calculs d'intégrale: c'est pourquoi nous développons ici endétail, à titre d'exemple, la manière dont a été obtenue dans le §III, la minoration $N > 10^g$, où N est la

conducteur d'une variété abélienne définie sur $\mathbf{Q}$ de dimension g; une valeur précise de l'intégrale figurant dans les formules explicites y est en effet nécessaire.

Il s'agit donc de calculer

$$I(\lambda) = \int_0^\lambda \left(\frac{2f(x/\lambda)\, e^{x/2}}{e^{2x}-1} - \frac{e^{-x}}{x} \right) dx - \int_\lambda^{+\infty} \frac{e^{-x}}{x} dx$$

où $f(x) = (1\text{-}x)\cos(\pi x) + \sin(\pi x)/\pi$.

Pour $\lambda < \pi/2$, le développement en série de t
$e^{ut}/e^t - 1 = \Sigma_{n \geqslant 0}\ B_n(u)\ t^n/n!$,
où les $B_n(u)$ sont les polynômes de Bernoulli, nous permet d'écrire

$$I(\lambda) = J(\lambda) + K(\lambda)$$

où

$$J(\lambda) = \int_0^\lambda \frac{f(x/\lambda) - e^{-x}}{x} dx - \int_<^{+\infty} \frac{e^{-x}}{x} dx$$

et

$$K(\lambda) = \sum_{n \geqslant 1} B_n\left(\frac{1}{4}\right) \frac{2^n \lambda^n}{n!} \int_0^1 f(x) n^{n-1}\, dx.$$

Après quelques transformations, il est facile de voir que

$$J(\lambda) = \mathrm{Si}(\pi)/\pi - \mathrm{Cin}(\pi) + \log(\lambda) + \gamma$$

où $\mathrm{Si}(t) = \int_0^t [\sin(x)/x]\, dx$ et $\mathrm{Cin}(t) = \int_0^t [1 - \cos(x)/x]\, dx$, et où γ est la constante d'Euler

En utilisant les tables [1], on trouve alors $J(\lambda) = \log(\lambda) - 0{,}481572\ldots$ D'autre part, on sait que $B_n\left(\frac{1}{4}\right) = -2^{-n}(1 - 2^{1-n})B_n - n4^{-n}E_{n-1}$, où les B_n (resp. E_n) sont les nombres de Bernoulli (resp. d'Euler).

Enfin, une intégration par parties permet de montrer que

$$\int_0^1 f(x) x^{n-1}\, dx = \frac{\pi}{n} \int_0^1 (1-x) x^n \sin(\pi x)\, dx,$$

intégrale qui se calcule par récurrence sur n.

Par suite, on a le développement $I(\lambda) = -0{,}481572 + \log(\lambda) + \Sigma_{n \geqslant 1}$ $c_n \lambda^n$, valable pour $\lambda < \pi/2$; les c_n sont négatifs pour $n \equiv 1$ et 2 modulo 4, et positifs sinon:

n	1	2	3	4	5	6
c	$-0{,}202642\ldots$	$-0{,}004221\ldots$	$0{,}002399\ldots$	$0{,}000021\ldots$	$-0{,}000061\ldots$	$-1{,}7\ldots 10^{-7}$

Le terme d'erreur se majore à partier des majorations classiques sur les nombres de Bernoulli et d'Euler.

Pour $\lambda = 1{,}33$, on trouve $I(1{,}33) = -0{,}467411\ldots$ avec une erreur inférieure à $5{,}10^{-6}$. Il suffit ensuite de calculer le terme correspondant à la partie non archimédienne des formules explicites (seuls sont pris en compte les nombres premiers inférieurs à $e^{1{,}33}$, i.e. 2 et 3) pour obtenir la minoration $N > 10{,}323^g$.

Bibliographie

[1] M. ABRAMOWITZ, I. STEGUN: *Handbook of Mathematical Functions*, Dover publications (1970).

[2] A.O.L. ATKIN et J. LEHNER: Hecke operators on $\Gamma_0(m)$. *Math. Ann.* 185 (1970) 134–160.

[3] B.J. BIRCH et H.P.F. SWINNERTON-DYER: Notes on elliptic curves (II). *J. reine angew. Math.* 218 (1965) 79–108.

[4] P. DELIGNE: *Formes modulaires et représentations l-adiques*. Séminaire Bourbaki, 1968–1969, no. 355.

[5] S. LANG: *Algebraic Number Theory*. Addison-Wesley (1970).

[6] B. MAZUR et H.P.F. SWINNERTON-DYER: Arithmetic of Weil curves. *Invent. Math.* 25 (1974) 1–61.

[7] J.-F. MESTRE: Construction d'une courbe elliptique de rang $\geqslant 12$. *C.R. Acad. Sci. Paris* 295 (1982) 643–644.

[8] Modular functions o one variable IV, *Lecture Notes in Math.* no. 476, Springer-Verlag (1975).

[9] C.J. MORENO: Explicit formulas in the theory of automorphic forms. *Lecture Notes in Math.* no. 626, Springer-Verlag (1976).

[10] G. POITOU: *Sur les petits discriminats*, Séminaire Delange-Pisot-Poitou, 1976–1977, no. 6.

[11] J.-P. SERRE: *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou, 1969–1970, no. 19.

[12] J.-P. SERRE: Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini. *C.R. Acad. Sci. Paris*, t. 296 (1983) 397–402.

[13] A. WEIL: Sur les "formules explicites de la théorie des nombres premiers", *Comm. Sem. Math. Lund*, Lund (1952) 252–265 (= *Oeuvres Sci.*, II, 48–61).

[14] A. WEIL: Sur les formules explicites de la théorie des nombres, *Izvestia Akad. Nauk S.S.S.R., Ser. Math.* 36 (1972) 3–18 (= *Oeuvres Sci.*, III, 249–264).

[15] A. WEIL: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.* 168 (1967) 149–156 (= *Oeuvres Sci.*, III, 165–172).

(Oblatum 20-IX-1984)

Ecole Normal Supérieure
45 Rue d'Ulm
F-75005, Paris
France