SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

JEAN-FRANÇOIS MESTRE

Courbes elliptiques et formules explicites

Séminaire de théorie des nombres de Grenoble, tome 10 (1981-1982), exp. n° 3, p. 1-10

<http://www.numdam.org/item?id=STNG_1981-1982__10__A3_0>

Séminaire de Théorie des Nombres
28 janvier 1982
Grenoble

COURBES ELLIPTIQUES ET FORMULES EXPLICITES

par Jean-Francois MESTRE

I. – INTRODUCTION

Soit E une courbe elliptique définie sur $\mathbb{Q}$, de conducteur N, et soit r le rang du groupe $E(\mathbb{Q})$ de ses points rationnels. On ignore si r est ou non borné quand E parcourt l'ensemble des courbes elliptiques sur $\mathbb{Q}$. Néron a cependant trouvé une famille infinie de courbes elliptiques pour lesquelles r est supérieur ou égal à 11. Sa méthode, de nature purement algébrique, semble malheureusement difficile à appliquer pour des rangs supérieurs.

D'autre part, on ne connaît pas de majoration raisonnable de r en fonction des invariants de la courbe : la démonstration du théorème de Mordell-Weil fournit en effet la seule majoration connue, de la forme $r = 0(\text{Log}\, N)$, qui se révèle très mauvaise dans la pratique. Mazur [2] a cependant montré que dans le cas où E a de la torsion sur $\mathbb{Q}$ on a une majoration du type $r = 0(\text{Log}\, N / \text{Log Log}\, N)$. Ces majorations s'obtiennent en étudiant certains groupes de cohomologie (galoisienne ou fppf) et sont donc d'origine algébrique.

On montre ici qu'un détour par des méthodes analytiques n'est pas sans intérêt : on peut ainsi construire des courbes de rang élevé, par exemple la courbe :

$$y^2 - 246xy + 36599029y = x^3 - 89199x^2 - 19339780x - 36239244$$

de conducteur $N = 60259.550469.11241887.722983930261$ et qui est de rang supérieur ou égal à 12 (vraisemblablement égal à 12).

D'autre part, il ne semble pas absolument déraisonnable de penser qu'en continuant les calculs on puisse trouver des courbes de rang arbitrairement grand : rien dans la méthode ne semble s'y opposer, hormis toutefois, et ce n'est pas négligeable, notamment financièrement, le temps de calcul nécessaire sur ordinateur.

Par ailleurs, les mêmes méthodes analytiques permettent de trouver des majorations conjecturales, mais fines, du rang d'une courbe en fonction de son conducteur ; en particulier, si E est une courbe vérifiant les conjectures du paragraphe II, on a une majoration de la forme $r = 0(\mathrm{Log}\, N / \mathrm{Log}\, \mathrm{Log}\, N)$, que E ait ou non de la torsion sur Q .

II. – LES CONJECTURES

Si E est une courbe elliptique définie sur Q , de conducteur N , on définit sa fonction L par

$$L(s) = \sum_n a_n n^{-s} = \prod_{p/N} \left(1-a_p p^{-s}\right)^{-1} \prod_{p\nmid N} \left(1-a_p p^{-s}+p^{1-2s}\right)^{-1}$$

les coefficients a_p étant définis comme suit :

i) si p divise N , $a_p = 0$ (resp. 1, resp. -1) si la réduction de E modulo p est additive (resp. multiplicative déployée, resp. multiplicative non déployée) ;

ii) si p ne divise pas N , $a_p = p+1-N_p$, N_p étant le nombre de points de E modulo p . Dans ce cas, $a_p = \alpha_p + \bar{\alpha}_p$, α_p et $\bar{\alpha}_p$ étant des nombres complexes conjugués de module égal à $\sqrt{p}$.

Dans le cas où E est à multiplications complexes, cette fonction L n'est autre qu'une fonction L de Hecke associée à un Grossencharacter. Dans le cas général, le seul résultat démontré - et trivial - est sa convergence pour $Re(s) > 3/2$. L'attrait exercé par ces fonctions réside en fait dans les deux conjectures suivantes :

II. 1 - CONJECTURE DE BIRCH ET SWINNERTON-DYER.

La fonction L d'une courbe elliptique est prolongeable en une fonction holomorphe au voisinage de 1 , et son ordre en 1 est égal au rang du groupe de Mordell-Weil de E sur Q .

II. 2 - CONJECTURE DE WEIL.

Si $L(s) = \sum_n a_n n^{-s}$ est la fonction L d'une courbe elliptique définie sur Q , la fonction $f(z) = \sum_n a_n \exp(2\pi i n z)$ est une "new form" de poids 2 , au sens d'Atkin-Lehner [1], pour le groupe $\Gamma_0(N)$. En particulier, la fonction $\Lambda(s) = (\sqrt{N}/2\pi)^s \Gamma(s) L(s)$ est entière, et vérifie l'équation fonctionnelle $\Lambda(s) = C\Lambda(2-s)$, C étant une constante égale à ± 1 .

Outre ces deux conjectures célèbres, il semble loisible d'en énoncer une troisième :

II. 3 - CONJECTURE DE RIEMANN GENERALISEE.

La fonction L d'une courbe elliptique est prolongeable en une fonction entière dont les seuls zéros dans la bande verticale $\frac{1}{2} < Re(s) < \frac{3}{2}$ sont situés sur la droite $Re(s) = 1$.

III. –

III.1 - FORMULES EXPLICITES.

Les formules explicites de Weil [5] sont faciles à généraliser au cas des formes modulaires : soit donc $f(z) = \sum a_n e^{2\pi inz}$ une forme nouvelle de poids k pour le groupe $\Gamma_0(N)$, et $L(s) = \sum a_n n^{-s} = \prod_{p|N} (1 - a_p p^{-s})^{-1} \prod_{p\nmid N} (1-a_p p^{-s}+p^{1-2s})^{-1}$ sa transformée de Mellin. Si p divise N, on définit $b(p^m) = (a_p)^m$; sinon, on pose $b(p^m) = \alpha_p^m + \alpha'^m_p$, où α_p et α'_p sont les racines du polynôme $T^2 - a_p T + p$.

Soit d'autre part, une fonction F réelle, paire, telle que $F(0) = 1$, et vérifiant les conditions suivantes :

i) il existe $\epsilon > 0$ tel que $F(x)e^{(\frac{1}{2}+\epsilon)x}$ soit sommable ;

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

iii) la fonction $(F(x)-1)/x$ est à variation bornée.

Soit $\Phi(s) = \int_{-\infty}^{+\infty} F(x)e^{(s-k/2)x}dx$, et soit $\varphi(t) = \int_{-\infty}^{+\infty} F(x)e^{itx}dx$. On a alors la formule :

$$(1) \qquad \sum_\rho \Phi(\rho) + 2 \sum_{p,m\geq 1} b(p^m)\operatorname{Log} p \,/\, p^{mk/2} F(m \operatorname{Log} p)$$
$$= \operatorname{Log} N - 2\operatorname{Log}(2\pi) - 2 I_F ,$$

où ρ parcourt les zéros de L situés dans la bande $k/2 \leq \operatorname{Re}(s) \leq k/2 + 1$; I_F est donnée par la formule : $\int_{-\infty}^{+\infty} \left(F(x)e^{-kx/2}/(1-e^{-x}) - e^{-x}/x\right)dx$.

III.2 - APPLICATIONS AUX COURBES ELLIPTIQUES.

Soit E une courbe elliptique définie sur $\mathbb{Q}$, de conducteur N ; dans tout ce paragraphe, on suppose qu'elle vérifie les conjectures II.1,

II.2 et II.3 ; soit alors F une fonction vérifiant les conditions de III.1, et telle que $\varphi(t)$ soit positive ou nulle pour tout t ; si r désigne le rang de $E(Q)$, on déduit alors de (1) une majoration de r :

$$(2) \qquad r\varphi(0) \leq \operatorname{Log} N - 2\operatorname{Log}(2\pi) - 2I_F - 2 \sum_{p,m\geq 1} b(p^m)\operatorname{Log} p\, F(\operatorname{Log}(p^m))/p^m$$

On peut ici écrire :

$$I_F = \int_{-\infty}^{+\infty} \left(F(x)/(e^x-1) - e^{-x}/x\right)dx \ .$$

La méthode employée usuellement pour optimiser de telles majorations est la suivante : on part d'une fonction F à support compact (nous prenons dans ce paragraphe la fonction d'Odlysko nulle en dehors de $[-1,1]$, paire, et telle que $F(x) = (1-x)\cos(\pi x) - \sin(\pi x)/\pi$ pour x positif inférieur à 1). Pour λ réel positif, on pose $F_\lambda(x) = F(x/\lambda)$; alors $\varphi_\lambda(t) = \lambda\varphi(\lambda t)$. On cherche alors λ minimisant les majorations (2). En majorant brutalement $|b(p^m)|$ par $2p^{m/2}$, et en prenant λ de l'ordre de $2\operatorname{Log}\operatorname{Log} N$, on trouve alors :

$$r \leq (\pi^2/16)\operatorname{Log} N/\operatorname{Log}\operatorname{Log} N + 0(\operatorname{Log} N/(\operatorname{Log}\operatorname{Log} N)^3) \ .$$

Ces formules n'ont, à vrai dire, que peu d'intérêt tant que l'on ignore si le rang d'une courbe elliptique peut être ou non arbitrairement grand. Par contre, à partir d'une courbe elliptique E donnée explicitement, on peut trouver des majorations très fines du rang de $E(Q)$ en calculant un nombre de coefficients a_p relativement restreint et en appliquant la formule (2).

Prenons par exemple $\lambda = \operatorname{Log} 23$; la fonction F étant la fonction d'Odlysko décrite ci-dessus, on a alors $I_F \simeq 0,1067$, d'où la majoration :

$$(3) \qquad r \leq 0,3935\operatorname{Log} N - 1,5302 - 0,786 \sum_{p^m\leq 23} b(p^m)\operatorname{Log} p\, F(\operatorname{Log}(p^m))/p^m \ .$$

Il suffit donc de calculer les coefficients a_p pour $p = 2,3,5,7,11,13,17,19$, puis les termes $b(4)$, $b(8)$, $b(16)$ et $b(9)$. Cela donne expérimentalement

de bonnes majorations pour des courbes de conducteur inférieur à 1000 ; en particulier, si l'on applique la formule (3) à toutes les courbes de conducteur ≤ 200 issues des tables de [4], on trouve la valeur exacte du rang de ces courbes en prenant la partie entière de la majoration obtenue. Voici quelques majorations obtenues pour des courbes mises sous forme de Weierstrass $y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$

α_1	α_2	α_3	α_4	α_6	N	rang	majoration
0	-1	1	0	0	11	0	0,00142
0	-1	1	-40	-221	121	0	0,024
0	0	1	-1	0	37	1	1,00097
0	0	1	-3	0	189	1	1,083
0	1	1	-2	0	389	2	2,008
0	0	1	-1	6	16811	3	3,37

Le fait que ces majorations sont bonnes provient de ce que les zéros non réels de L sur la droite $\mathrm{Re}(s) = 1$ sont assez éloignés de l'axe réel : expérimentalement, l'ordonnée minimale de ces zéros est de l'ordre de $1/\mathrm{Log}\,N$; ce fait peut être démontré pour certaines classes de courbes elliptiques (par exemple pour les courbes dont le rang est égal au nombre de points critiques fondamentaux d'ordre impair [3] de leur fonction L et est inférieur ou égal à 2).

D'autre part, si E est une courbe elliptique de conducteur N , les majorations (2) appliquées aux fonctions F_λ donnent (toujours expérimentalement...) de bons résultats pour λ de l'ordre de $2\,\mathrm{Log}\,\mathrm{Log}\,N$; cela signifie que les nombres premiers p importants pour caractériser le rang de E semblent inférieurs à $C(\mathrm{Log}\,N)^2$, C constante indépendante de N .

III. 3 - CONSTRUCTION DE COURBES ELLIPTIQUES DE RANG ASSEZ ELEVE.

Les considérations précédentes permettent d'espérer que, pour obtenir des courbes de rang élevé, il suffit d'en construire dont les coefficients a_p sont minimaux pour suffisamment de nombres premiers p . L'algorithme est alors le suivant :

• soit M un entier, P_M l'ensemble des nombres premiers inférieurs ou égaux à M , et R le produit de ces nombres premiers. On calcule les congruences que doivent vérifier les coefficients c_4 et c_6 d'une courbe elliptique pour que, quelque soit $p \leq P_M$, $a_p = -E(2\sqrt{p})$.

• On fixe ensuite deux entiers K et K' dépendant des capacités de calcul dont on dispose. Pour k de valeur absolue inférieure à K , on calcule k'_o tel que $(c_4+kR)^3 - (c_6+k'_oR)^2$ soit de valeur absolue minimale ; pour chacune des courbes de coefficients c_4+kR , $c_6+(k'_o+k')R$, avec $|k'| \leq K'$, on calcule les coefficients a_p pour p inférieur à M^2 . Si la majoration (2) est convenable (avec $\lambda = 2\,\mathrm{Log}\,M$) , on cherche des points entiers de la courbe, et, si on en trouve suffisamment, on calcule la matrice des hauteurs de ces points, qu'on diagonalise. On obtient ainsi une minoration du rang de la courbe.

Ce procédé, qui repose sur de nombreuses conjectures, permet néanmoins de trouver explicitement des courbes qui ont effectivement un rang élevé. On trouve ainsi de nombreuses courbes de rang 8 (en faisant $M=17$ dans l'algorithme ci-dessus), de rang 9 (avec $M=19$), de rang 10 ($M=23$) , de rang 11 ($M=29$) , de rang 12 ($M=31$) . Outre la courbe de rang 12 citée dans l'introduction, voici en exemple deux courbes de rang 11 :

$$y^2 - 64xy + 1066633y = x^3 - 9007x^2 - 1499708x - 1006950$$

$$N = 18034061681836267671024 37$$

$$y^2 + 11544xy + 15151y = x - 33273156x - 3121x - 660$$

$$N = 1814035408414888831495208037 .$$

Un autre intérêt de cette méthode est de fournir des courbes elliptiques qui, sous forme minimale, ont de nombreux points entiers : par exemple, la première courbe de rang 11 citée ci-dessus a au moins 167 points entiers !

Pour finir, il peut être utile de donner quelques exemples de courbes elliptiques de la forme

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

de rang 7, 8, 9 ou 10 et ayant des coefficients assez "petits" :

a_1	a_2	a_3	a_4	a_6	Δ	rang $\geq$
0	-2265	82483	458	27744	$1,46\ 10^{19}$	7
0	-789	15023	-610	-7392	$4,06\ 10^{17}$	7
0	-3132	134741	-1369	-47340	$3,08\ 10^{19}$	7
0	-1389	39631	920	-11580	$5,96\ 10^{17}$	7
0	-1860	61549	503	22926	$2,29\ 10^{19}$	7
0	-3096	132377	335	-54540	$2,81\ 10^{19}$	7
0	-2007	69045	1616	12514	$1,90\ 10^{18}$	7
0	-2007	68935	1616	-2226	$3,84\ 10^{18}$	7
0	-1983	67881	-274	-16748	$1,81\ 10^{18}$	7
0	-2712	108429	-529	-26390	$2,13\ 10^{19}$	8
2	1529	799	-1916	-714	$-3,65\ 10^{16}$	8
0	507	6931	416	-3918	$-1,62\ 10^{17}$	8
2	2324	475	-1037	0	$-4,54\ 10^{16}$	8
0	789	51063	-810	-35690	$-2,04\ 10^{20}$	8
0	3087	6161	-1834	-258	$-1,79\ 10^{19}$	8
0	3537	3385	776	-2424	$-8,11\ 10^{18}$	8
0	1821	7695	-940	-1196	$-5,82\ 10^{18}$	8

0	3396	5009	-205	-3600	-1,57	10^{19}	8
0	1800	7875	1013	-2210	-5,88	10^{18}	8
0	1305	4691	-802	-3624	-7,97	10^{17}	8
0	2286	7421	2285	0	-1,06	10^{19}	8
0	630	8221	623	-3774	-3,92	10^{17}	8
0	3729	3435	-1030	-2174	-9,79	10^{18}	8
0	2253	7817	-1234	-1782	-1,13	10^{19}	8
0	3228	9479	131	-3360	-4,86	10^{19}	8
-2	737	531	1262	-110	-1,80	10^{15}	8
0	3576	9767	425	-2412	-7,00	10^{19}	9
0	-3537	121333	-1954	33708	4,57	10^{21}	9
0	-7665	504791	6608	-130344	8,20	10^{22}	9
0	-11565	957527	-9382	174384	1,45	10^{21}	9
0	-8148	562205	-49	50046	3,82	10^{22}	9
0	-6408	394059	4091	-159278	2,41	10^{21}	9
0	-4806	253669	-25	37422	2,49	10^{21}	9
-2	7664	6401	10279	2736	-2,95	10^{20}	9
0	-12117	1026611	1946	101250	7,15	10^{21}	9
0	-12288	1048249	731	-464478	1,97	10^{22}	9
0	24222	121877	-14869	-41760	-3,38	10^{24}	10
0	-16104	1572517	8375	161178	1,15	10^{23}	10
0	-15336	1461695	-415	-80334	5,18	10^{22}	10
0	88776	1	-36625	-11425292340	5,11	10^{26}	10

BIBLIOGRAPHIE

[1] ATKIN A.O.L., LEHNER J., Hecke operators on $\Gamma_0(m)$. Maths. Ann. 185 (1970), 134-160.

[2] MAZUR B., Rational points of abelian varieties with values in towers of number fields. Inv. Math. 18 (1972), 183-266.

[3] MAZUR B., SWINNERTON-DYER P., Arithmetic of Weil curves. Inv. Math. 25 (1974), 1-61.

[4] Modular functions of one variable IV. (Springer Lecture Notes, vol. 476), 82-113.

[5] WEIL A., Sur les formules explicites de la théorie des nombres premiers. Comm. Sem. Math. Lund (volume dédié à M. Riesz), Lund (1952), 252-265.
