Étude expérimentale du rang de familles de courbes elliptiques sur $\mathbb{Q}$

Stéfane Fermigier

TABLE DES MATIÈRES

AMS subject classification: 11G40, 11-04

On étudie expérimentalement le rang des courbes elliptiques sur $\mathbb{Q}$ obtenues par spécialisation entière du paramètre t de courbes de rang allant de 0 à 4 sur $\mathbb{Q}(t)$.

This is an experimental study of the rank of elliptic curves over $\mathbb{Q}$ obtained by specializing to integer values the parameter t of curves over $\mathbb{Q}(t)$ having rank 0 to 4.

1. INTRODUCTION

L'étude du rang des courbes elliptiques E sur $\mathbb{Q}$ est un thème où de nombreuses questions restent à ce jour conjecturales. L'une des plus importantes semble être de savoir si ce rang est borné ou non et, plus généralement, de déterminer la distribution des différentes valeurs possibles lorsqu'on fait tendre le conducteur des courbes considérées vers l'infini.

Plus généralement, on peut se poser la question suivante : que peut-on dire du rang des courbes elliptiques obtenues par spécialisation à partir d'une famille de courbes elliptiques paramétrées par une variété contenant une infinité de points rationnels ? Ces rangs sont-ils bornés ? Pour quelles valeurs de r obtient-on une proportion non-nulle de courbes de rang r ?

Cette question est motivée par exemple par une méthode classique de construction de courbes de grand rang sur $\mathbb{Q}$: on part d'un familles de courbes elliptiques, de préférence de grand rang sur son corps de définition, et on considère, parmi de nombreuses spécialisations du ou des paramètres, celles qui conduisent au rang le plus élevé [Mestre 1992 ; Fermigier 1992 ; Nagao 1992 ; 1993a ; 1993b].

1058-6458/96 $0.50 per page

On peut s'interroger de façon théorique sur l'efficacité de ce procédé, c'est-à-dire voir si en partant par exemple d'une courbe de rang r sur $\mathbb{Q}(T)$, on a autant de facilité à obtenir une courbe de rang $r+n$ qu'à obtenir une courbe de rang $r'+n$ en partant d'une famille de rang r'.

Nous montrons ci-dessous qu'une telle hypothèse, due en particulier à Armand Brumer, semble raisonnable. Plus précisément, d'après les exemples que nous avons calculé, il semblerait que pour une famille de rang r sur $\mathbb{Q}(t)$ on trouve des proportions non-nulles de courbes de rang r, $r+1$, $r+2$ et $r+3$, et aussi qu'il y ait des similitudes de comportement entre les différentes courbes, y compris pour des courbes provenant de familles de rangs différents sur $\mathbb{Q}(t)$.

Notons que plusieurs résultats théoriques sur ce type de questions ont été obtenus récemment : voir en particulier [Billard 1995; Fouvry et Pomykala 1993; Michel 1995; Rohrlich 1993].

2. MÉTHODE DE CALCUL DU RANG

La méthode de calcul du rang considérée consiste

- à en fournir une borne inférieure, en exhibant des points rationnels indépendants ;
- à en fournir une borne supérieure, à l'aide des « formules explicites » ;
- éventuellement, à utiliser le signe de l'équation fonctionnelle des fonctions L, pour déterminer la parité du rang.

Les deux derniers points font intervenir les fonctions L, et nécessitent donc de supposer vraies les conjectures de Birch et Swinnerton-Dyer, et de Shimura, Taniyama et Weil.

Recherche des points

On recherche de façon systématique des points rationnels de petite hauteur. Pour cela, on écrit l'équation de la courbe elliptique E sous la forme $Y^2 = f(X)$ avec $f(X) = X^3 + c_4X + c_6$, en utilisant par exemple les formules de [Tate 1975] ou [Silverman 1986]. On considère alors les $x = m/n$, avec m et n entiers dans certains intervalles fixés *a priori* et n un carré, et on cherche les valeurs de x telles que $f(x)$ est un carré dans $\mathbb{Q}$.

Plus précisément, pour chaque valeur de n, on considère l'équation $Y^2 = f(m/n)$. En notant d le ppcm des dénominateurs de $f(X/n)$, on est donc amené à regarder l'équation $Y'^2 = d^2 f(m/n) = g(m)$, avec $y' = dy \in \mathbb{Z}$ et $g \in \mathbb{Z}[m]$, ce qui permet de faire les calculs en entiers et d'utiliser une méthode de crible : dans un premier temps, on tabule les symboles de Legendre $\left(\dfrac{g(m)}{p}\right)$, en utilisant de l'arithmétique multiprécision, pour p premier impair inférieur à 100 et pour $0 \le m < p$, puis on fabrique ensuite des tables qui relèvent ces résultats modulo des produits de tels nombres premiers, calculés de façon à éliminer le plus grand nombre de candidats. Dans un deuxième temps, ces tables sont parcourues simultanément et lorsqu'un m passe le crible, on regarde alors directement si $g(m)$ est un carré.

Le principal avantage de cet algorithme est que, une fois la phase préliminaire passée, l'essentiel des calculs a lieu en entiers courts (32 bits). On n'a à évaluer $g(m)$ (en entiers multiprécision) que lorsque m passe le crible, c'est-à-dire en de très rares occasions. Le reste du temps, les seules opérations nécessaires sont des incrémentations de pointeurs, des lectures de tables et des tests, sans qu'il y ait d'opérations arithmétiques complexes (multiplication, division) à effectuer.

Quelques essais nous ont convaincu que les meilleures performances (pour des intervalles de recherche importants) étaient obtenues avec 5 tables de taille environ 10000, sans que ces chiffres soient sensiblement importants.

Formules explicites

Une façon efficace d'obtenir des majorations du rang, pour les courbes elliptiques de conducteur raisonnablement important (10^8 sur nos exemples, voir beaucoup plus pour les courbes de rang plus élevé) consiste à utiliser les formules explicites, découvertes par Weil dans le cas des corps de nombre et adaptées par Mestre [Mestre 1986] dans le cas des courbes elliptiques.

Néanmoins, pour obtenir les meilleurs résultats possibles, on est obligé de supposer l'hypothèse de Riemann généralisée pour ces courbes.

Soit E une courbe elliptique qui vérifie les conjecture de Birch et Swinnerton-Dyer et de Shimura, Taniyama et Weil, de conducteur N_E et dont la fonction L s'écrit $L_E(s) = \sum_n a_n n^{-s}$. Soit F une fonction réelle à support compact telle que $F(0) = 1$ et telle que $(F(x) - F(0))/x$ est à variation bornée. Alors on a

$$\sum_\rho \Phi(\rho) + 2\sum_{p,m} b_{p^m} F(m \log p)\frac{\log p}{p^m} = \log N_E - 2\log 2\pi - 2\int_0^\infty \left(\frac{F(x)}{e^x - 1} - \frac{e^{-x}}{x}\right) dx,$$

où $b_{p^m} = \alpha_p^m + \bar{\alpha}_p^m$ si $a_p = \alpha_p + \bar{\alpha}_p$, avec α_p valeur propre du Frobenius en p, lorsque $p \not| N$, et $b_{p^m} = \alpha_p^m$ pour $p|N$; $\sum_\rho$ signifie la somme sur les zéros de L situé dans la « bande critique » $0 < \operatorname{Re} s < 2$; $\sum_{p,m}$ désigne la somme sur tous les nombres premiers p et tous les entiers strictement positifs m ; enfin Φ est définie par

$$\Phi(s) = \int_{-\infty}^{+\infty} F(x)e^{(s-1)x} dx.$$

Supposons maintenant que tous les zéros de L_E de la bande critique sont situés sur la droite critique $\operatorname{Re} s = 1$ (hypothèse de Riemann généralisée). Soit F est une fonction à transformée de Fourier positive, c'est-à-dire telle que $\Phi(s) \geq 0$ sur la droite critique. On peut prendre par exemple la fonction $F_\lambda(x) = f(x/\lambda)$ avec

$$f(x) = \begin{cases} (1-|x|)\cos \pi x + \dfrac{\sin \pi |x|}{\pi} & \text{pour } |x| < 1, \\ 0 & \text{pour } |x| \geq 1. \end{cases}$$

Ainsi, F_λ est à support compact et de classe C^2 par morceaux. Si r est la multiplicité de 0 en tant que zéro de L_E, conjecturalement égale au rang de E par la conjecture de Birch et Swinnerton-Dyer, on obtient la majoration du rang $\operatorname{rg} E \leq \lfloor r_\lambda^+(E) \rfloor$, où

$$r_\lambda^+(E) = \Phi_\lambda(1)^{-1} \times \left(\log \frac{N_E}{(2\pi)^2} - 2\sum_{p^m < e^\lambda} b_{p^m} F_\lambda(m \log p)\frac{\log p}{p^m} - 2\int_0^\infty \left(\frac{F_\lambda(x)}{e^x - 1} - \frac{e^{-x}}{x}\right) dx\right),$$

avec $\Phi_\lambda(1) = 2\int_0^\lambda F_\lambda(x)\, dx = \lambda\Phi_1(1)$. Notons que $r_\lambda^+(E)$ converge vers $\operatorname{rg} E$ quand λ tend vers l'infini.

Le calcul des coefficients a_p, à l'aide de l'algorithme *baby step / giant step* de Shanks-Mestre, reste raisonnablement rapide pour $p < 10^5$ voire plus.

Il existe d'autres méthodes de majoration du rang, exposées dans [Buhler et al. 1985] ou [Gebel et Zimmer 1994]. Ces méthodes reposent sur le calcul de $L_E^{(r)}(1)$ dont on souhaite montrer la non-annulation pour $r = \operatorname{rg} E$. Mais ce calcul nécessite de l'ordre de $O(\sqrt{N})$ coefficients a_n, si on connait le signe de l'équation fonctionnelle, et plus encore si on ne le connait pas.

Bien que ce soit difficile à justifier théoriquement, on obtient avec les formules explicites de bonnes majorations plus rapidement, dans le cas des courbes de rang élevé. En effet, comme la qualité de la majoration obtenue dépend des zéros de la fonction L_E dans la bande critique, qui restent à ce jour très mal connus, il n'est pas possible de déterminer *a priori* une valeur du paramètre de coupure λ qu'il convient de choisir pour obtenir la valeur exacte du rang.

Il apparaît cependant comme évident que les calculs, comme avec toute méthode qui utilise les fonctions L, sont d'autant plus rapides que les conducteurs des courbes considérées sont petits. Une évaluation expérimentale de ce phénomène a fait l'objet d'une étude plus poussée, présentée à la section 5.

Notons aussi que l'hypothèse de Riemann généralisée n'est pas indispensable pour faire marcher les formules explicites : il suffit de remplacer F_λ par

G_λ avec $G_\lambda(x) = F_\lambda(x)/\mathrm{ch}(x)$. La fonction G_λ est alors à transformée de Fourier positive dans toute la bande critique, ce qui nous affranchit de GRH. Le problème est que maintenant $r_\lambda^+(E)$ ne tend plus vers $\mathrm{rg}\, E$ quand λ tend vers l'infini. Alors $r_\lambda^+(E)$ admet un minimum puis tens vers l'infini avec λ. Ce minimum peut suffire à calculer le rang pour les courbes de petit conducteur, mais ce n'est pas le cas pour les courbes de gros conducteur.

Parité du rang

Soit E une courbe elliptique qui vérifie les conjectures de Birch et Swinnerton-Dyer et de Shimura, Taniyama et Weil. Alors la parité de son rang est donnée par le signe de l'équation fonctionnelle de sa fonction L. Plus précisément, si on pose $\Lambda_E(s) = (2\pi)^{-s} N_E^{s/2} \Gamma(s) L_E(s)$, alors on a

$$\Lambda_E(2-x) = \varepsilon \Lambda_E(x), \qquad \text{avec } \varepsilon = (-1)^{\mathrm{rg}\, E(\mathbb{Q})}.$$

D'après Deligne [1973], ε s'écrit comme un produit de facteurs locaux :

$$\varepsilon = -\prod_{p \mid \Delta_E} \varepsilon_p.$$

Ces facteurs locaux ont été calculés explicitement dans de nombreux cas. Ainsi d'après Atkin-Lehner [Atkin et Lehner 1970], on sait que si E a réduction multiplicative, on a pour tout p :

$$\varepsilon_p = -a_p = -\left(\frac{-c_6}{p}\right);$$

si E a réduction additive, on sait déterminer ε_p pour tout $p > 3$ en fonction de p et du type de Kodaira de E_p. Ces résultats, que l'on peut retrouver à l'aide par exemple de [Rohrlich 1993] et [Tate 1975], sont résumés par le tableau 1.

En résumé, pour toute courbe qui a réduction soit lisse, soit multiplicative en 2 et 3, on peut déterminer son rang r en ne connaissant que $r-1$ générateurs du groupe de Mordell-Weil, et en sachant que $\lfloor r_\lambda^+(E) \rfloor \le r+1$. Ceci permet donc de calculer le rang beaucoup plus rapidement.

Afin d'obtenir de grands nombres de courbes de chaque famille pour nos calculs, on n'a considéré que des familles qui ont réduction lisse ou multiplicative en 2 et 3, lorsqu'on spécialise le paramètre en des valeurs entière. C'est cet argument qui nous a incité à ne considérer que des spécialisations entières, et non pas rationnelles, car il n'aurait pas été possible d'éviter d'avoir des réductions additives en 2 et 3.

type	ε_p	validité
I_n	$-\left(\frac{-c_6}{p}\right)$	p quelconque
II	$\left(\frac{-1}{p}\right)$	$p > 3$
III	$\left(\frac{-2}{p}\right)$	$p > 3$
IV	$\left(\frac{-3}{p}\right)$	$p > 3$
I_0^*	$\left(\frac{-1}{p}\right)$	$p > 3$
II^*	$\left(\frac{-1}{p}\right)$	$p > 3$
III^*	$\left(\frac{-2}{p}\right)$	$p > 3$
IV^*	$\left(\frac{-3}{p}\right)$	$p > 3$
I_n^*	$\left(\frac{-1}{p}\right)$	$p > 3$

TABLEAU 1. Valeurs de ε_p.

A noter que pour plus de 20000 courbes, on a pu déterminer exactement le rang à l'aide de la recherche des points rationnels et des formules explicites, et vérifier que les résultats coïncidaient toujours avec ce que prédit la parité, ce qui constitue une vérification partielle de l'algorithme.

Considérations pratiques

Les méthodes de minoration et de majoration du rang considérées dépendent chacune de constantes : d'une part les hauteurs maximales des points que l'on recherche, et d'autre part le nombre de coefficients a_p considérés dans les formules explicites.

On est donc amené à procéder de manière itérative : on augmente les valeurs de ces constantes, jusqu'à ce qu'on obtienne une fourchette d'estimation qui permette de déterminer le rang de façon sûre, avec l'aide éventuelle de l'équation fonctionnelle.

Il semble que l'étape la plus importante soit la recherche des points de petite hauteur, qui peut prendre plusieurs dizaines d'heures avant de produire un nouveau point.

Pour les calculs que nous avons réalisés, on a déclaré le rang d'une courbe inconnu après avoir cherché les points d'abscisse $x = m/n$ avec $|m| < 320000$, n carré, $0 < n < 640$, et calculé r_λ^+ avec $\exp\lambda = 70000$.

Considérations informatiques

Pour réaliser les calculs, on a utilisé des programmes C construits à l'aide de la bibliothèque de calculs arithmétiques PARI, ainsi qu'une librairie de distribution de calculs développée elle-même au-dessus du système PVM3 [Geist et al. 1994].

Le principe de cette librairie est de pouvoir profiter des stations de travail d'un (ou plusieurs) site(s) de recherche pendant les heures où elles ne sont pas utilisées par leurs utilisateurs légitimes. De gros efforts ont été fournis afin de rendre le système le plus transparent possible pour les utilisateurs des stations.

En ce qui concerne la distribution des calculs, elle se fait suivant le schéma maître / esclave, avec un programme maître qui envoie, à l'aide de PVM, l'ordre de calculer le rang d'une courbe donnée à des processus esclaves qui s'exécutent sur les stations où personne ne travaille. Lorsqu'un utilisateur se loge sur une station, les calculs sont abandonnés et le programme esclave termine, afin de ne pas encombrer la mémoire de la station. La même courbe est envoyée ultérieurement à une autre station lorsqu'elle est libérée, ou lorsqu'elle finit son calcul en court.

Les calculs ont été réalisés sur les machines du département de mathématique et d'informatique de l'École Normale Supérieure, soit environ 60 stations SPARC. Ils ont duré environ quatre mois, ce qui représente de façon très approximative 30000 jours·Mips de travail CPU.

Une partie des calculs a été également effectuée sur la Connection Machine CM5 de l'institut de physique du globe, à Jussieu (la CM5 est une machine multiprocesseur à processeurs SPARC, sur laquelle le programme peut s'exécuter suivant le même principe, avec très peu de modifications).

3. LES COURBES CONSIDÉRÉES

Il s'agit de construire des courbes sur $\mathbb{Q}(t)$ de rang allant de 0 à 4. Pour cela, on assigne un certain nombre de points et on regarde quelles contraintes cela entraîne sur les coefficients de la courbe.

Il n'est pas difficile de montrer que les points rationnels $P_1, \dots, P_r$ qu'on leur a assigné sont indépendants, en spécialisant t en quelques valeurs rationnelles et en calculant le rang de la matrice des hauteurs canoniques $h_{i,j} = \langle P_i, P_j \rangle$: d'après le théorème de spécialisation de Silverman, les points obtenus par spécialisation finissent par devenir indépendants au bout d'un nombre fini d'essais (qui n'est pas connu *a priori*).

Il est plus délicat de montrer que les courbes considérées n'ont pas de points indépendants *supplémentaires.* Pour cela, on peut calculer le rang de la réduction de E sur $\mathbb{F}_p(t)$, qui est égal au rang de E sur $\mathbb{Q}$ pour p assez grand. Ceci peut se faire à l'aide du théorème de Shioda [Shioda 1990], qui affirme que le groupe de Mordell-Weil d'une courbe sur un corps de fonctions est engendré par des points de la forme $P = (x, y)$ (dans le modèle de Weierstraß) avec $x = \alpha t^2 + \beta t + \gamma$ (il n'y a qu'un nombre fini de tels points, donc l'algorithme termine).

On n'a pas réalisé ces calculs, mais plutôt admis que le rang d'une famille est le plus petit r tel qu'un pourcentage non-négligeable (c'est-à-dire supérieur à 10%) de courbes spécialisées est de rang r.

Comme l'utilisation de la parité du rang nécessite que les courbes aient réduction lisse ou multiplicative en 2 et 3, on a par ailleur éliminé toutes les courbes qui ne répondaient pas à ce critère (il suffit pour le vérifier de tester un nombre fini de valeur de t). On a pour cela réalisé un programme qui filtre les “mauvaises” courbes.

Enfin, pour l'intérêt de notre expérience, aucune courbe considérée ne doit bien évidemment être constante, ni être isotriviale (en effet, les “tordues” se comportent conjecturalement de façon très particulière). Ceci nous conduit donc à ne considérer que des courbes d'invariant j non-constant.

Dans ce qui suit, on écrit les courbes elliptiques sous la forme de Weierstraß

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

Courbes de rang 0

On a choisi des courbes avec des petits coefficients (linéaires en t), de façon à ce que le conducteur n'augmente pas trop vite avec t, sans autres contraintes particulières.

Courbes de rang 1

On a considéré des courbes avec $(0, 0)$ comme point rationnel, ce qui conduit à la contrainte $a_6 = 0$. Il faut néanmoins faire en sorte que a_1 ou a_3 soient non-nuls, de façon à ce que $(0, 0)$ ne soit pas un point de torsion (d'ordre 2).

Courbes de rang 2

On a utilisé des courbes construites de sorte que $(0, 0)$ et $(1, 0)$ soient des points rationnels. On aboutit aux contraintes $a_6 = 0$ et $a_2 + a_4 + 1 = 0$, ce qui nous a conduit à poser $a_2 = t$, $a_4 = -t - 1$ et à faire varier a_1 et a_3 de façon à obtenir plusieurs familles.

Courbes de rang 3 **et** 4

Soit $P = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$, et $Q = P(x - t)P(x + t)$. Alors Q peut s'écrire $Q = S^2 - R$, avec S de degré 4 et R de degré 3 sur $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, t]$. Lorsqu'on spécialise $\alpha_1, \ldots, \alpha_4$ en des valeurs entières, on obtient pour une infinité de valeurs un polynôme R tel que la courbe $y^2 = R$ est une courbe elliptique. Par ailleurs, elle possède 16 points rationnels de la forme $(\alpha_i + t,\ \pm R(\alpha_i + t))$ et $(\alpha_i + t,\ \pm R(\alpha_i + t))$, dont 4 au plus peuvent être indépendants : en effet, il n'est pas difficile de trouver des relations de la forme $P_i + P_j = P'_i + P'_j$.

Pour avoir une courbe avec 3 points, il suffit de prendre $\alpha_3 = \alpha_4 = 0$, ce qui donne les courbes :

$$\begin{aligned} y^2 = 4(\alpha_1 + \alpha_2)x^3 \\ - 4\alpha_1\alpha_2x^2 + 4t^2(\alpha_1 + \alpha_2)x + t^2(\alpha_1 + \alpha_2). \end{aligned}$$

En choisissant α_1 et α_2 tels que $0 < |\alpha_2| < \alpha_1$, on obtient ainsi des courbes non-isomorphes qui ont en général 3 points indépendants.

Pour les courbes de rang 4, on peut s'imposer $\sum \alpha_i = 0$, à cause de l'invariance par translation. Si on écrit P sous la forme $P = x^4 + b_2x^2 + b_1x + b_0$, on obtient des courbes de la forme :

$$y^2 = -8b_1x^3 + (4b_2^2 - 16b_0)x^2 + (4b_1b_2 + 8t^2b_1)x + b_1^2.$$

Notons enfin que comme les familles obtenues par cette dernière méthode sont définies sur $\mathbb{Q}(t^2)$. On n'a donc spécialisé t qu'en des valeurs positives.

4. COMMENTAIRES DES RÉSULTATS

Nous présentons, dans les tableaux 2, une synthèse des résultats obtenus.

Chaque tableau donne :

- les coefficients a_1, a_2, a_3, a_4, a_6 de la courbe ;
- le “type” du discriminant, c'est-à-dire le nombre de racines simples, doubles, etc., l'infini étant compté avec la multiplicité qui convient (avec la notation suivante : a^b signifie b racines a-uples) ;
- la plus petite ($t_{\min}$) et la plus grande ($t_{\max}$) valeur du paramètre t des courbes dont on a pu calculer le rang, ainsi que le nombre total de courbes calculées dans la famille (c'est-à-dire pour $t_{\min} \le t \le t_{\max}$, en enlevant les courbes singulières) ;
- la valeur maximale du logarithme en base 10 du conducteur des courbes où le calcul a échoué (c'est-à-dire pour $t = t_{\max} + 1$ ou $t = t_{\min} - 1$).
- le pourcentage de courbes de rang 0, 1, 2, etc. parmi les courbes considérées.
- le pourcentage de courbes de rang pair ;

coefficients sur $\mathbb{Q}(t)$					type			#	$\log_{10}$	% de spécialisations de rang égal à						%	rang
a_1	a_2	a_3	a_4	a_6	de Δ	$t_{\min}$	$t_{\max}$	tot	$N_{\max}$	0	1	2	3	4	5	pair	moy
familles de rang 0 sur $\mathbb{Q}(t)$																	
1	0	0	t	0	$1^1 2^1 9^1$	−999	865	1864	7.68	39.38	47.69	12.34	0.59	0.00		51.72	0.74
1	−2	0	t	0	$1^1 2^1 9^1$	−876	801	1677	7.69	35.48	51.22	12.88	0.42	0.00		48.36	0.78
1	1	0	t	0	$1^1 2^1 9^1$	−600	700	1300	7.50	37.92	49.92	11.38	0.77	0.00		49.31	0.75
1	0	0	2	t	$1^2 10^1$	−457	757	1215	8.39	33.25	46.17	17.94	2.55	0.08		51.28	0.90
1	0	0	−1	t	$1^2 10^1$	−464	678	1143	8.30	36.57	47.16	13.82	2.27	0.17		50.57	0.82
1	0	−2	1	t	$1^2 10^1$	−470	636	1106	8.25	31.65	50.36	16.55	1.45	0.00		48.19	0.88
1	0	1	−1	t	$1^2 10^1$	−480	612	1093	8.21	31.66	47.94	18.30	2.10	0.00		49.95	0.91
1	1	−1	1	t	$1^2 10^1$	−476	606	1083	8.20	32.23	50.14	15.60	2.03	0.00		47.83	0.87
1	1	1	1	t	$1^2 10^1$	−427	594	1022	8.18	31.02	49.51	17.51	1.86	0.10		48.63	0.91
−1	1	−2	1	t	$1^2 10^1$	−399	595	995	8.19	30.35	48.14	19.60	1.91	0.00		49.95	0.93
1	1	−3	1	t	$1^2 10^1$	−364	614	978	8.22	35.48	47.65	15.54	1.33	0.00		51.02	0.83
1	0	−1	1	t	$1^2 10^1$	−284	698	983	8.32	28.99	48.93	19.94	2.03	0.10		49.03	0.95
−1	1	−3	1	t	$1^2 10^1$	−489	486	976	8.01	30.43	50.31	17.01	2.25	0.00		47.44	0.91
0	1	1	1	t	$1^2 10^1$	−363	612	976	8.21	28.07	49.08	20.39	2.36	0.10		48.57	0.97
1	0	0	1	t	$1^2 10^1$	−276	694	971	8.32	31.31	48.71	16.99	2.99	0.00		48.30	0.92
0	1	3	1	t	$1^2 10^1$	−321	610	932	8.21	27.58	49.03	20.82	2.47	0.11		48.50	0.98
1	0	1	−2	t	$1^2 10^1$	−378	542	921	8.11	34.42	42.89	19.76	2.93	0.00		54.18	0.91
1	0	1	1	t	$1^2 10^1$	−382	502	885	8.04	31.64	48.47	17.97	1.92	0.00		49.60	0.90
−1	1	0	1	t	$1^2 10^1$	−363	481	845	8.00	31.24	47.22	18.46	3.08	0.00		49.70	0.93
1	0	1	2	t	$1^2 10^1$	−244	576	821	8.16	30.57	50.06	16.69	2.56	0.12		47.38	0.92
1	0	2	1	t	$1^2 10^1$	−354	452	807	7.95	34.08	46.84	16.98	2.11	0.00		51.05	0.87
1	0	0	−2	t	$1^2 10^1$	−325	437	763	7.92	33.68	46.79	16.78	2.75	0.00		50.46	0.89
1	0	−3	1	t	$1^2 10^1$	−252	454	707	7.96	31.54	48.23	17.68	2.55	0.00		49.22	0.91
1	1	−2	1	t	$1^2 10^1$	−205	339	544	7.70	28.31	52.39	18.75	0.55	0.00		47.06	0.92
1	1	1	t	1	$1^3 9^1$	−189	134	324	8.64	41.98	51.23	6.48	0.31	0.00		48.46	0.65
1	0	2	t	1	$1^3 9^1$	−126	181	308	8.59	43.18	47.40	9.09	0.32	0.00		52.27	0.67
1	1	3	t	1	$1^3 9^1$	−191	115	306	8.65	39.87	54.25	5.56	0.33	0.00		45.42	0.66
0	1	3	t	1	$1^3 9^1$	−159	135	295	8.42	36.27	49.15	12.54	2.03	0.00		48.81	0.80
1	1	2	t	1	$1^3 9^1$	−150	141	292	8.34	37.33	52.05	10.62	0.00	0.00		47.95	0.73
1	0	−2	t	1	$1^3 9^1$	−94	183	278	8.59	43.88	47.48	8.27	0.36	0.00		52.16	0.65
1	0	3	t	1	$1^3 9^1$	−150	105	256	8.33	39.06	46.09	13.28	1.56	0.00		52.34	0.77
familles de rang 1 sur $\mathbb{Q}(t)$																	
1	−2	0	t	1	$1^3 9^1$	−767	543	1311	10.46	0.15	31.96	45.39	20.14	2.21	0.15	47.75	1.93
1	1	−1	t	0	$1^3 9^1$	−711	477	1189	10.36	0.08	26.24	46.26	24.64	2.61	0.17	48.95	2.04
1	1	1	t	0	$1^3 9^1$	−716	476	1193	10.37	0.08	26.40	46.10	24.64	2.60	0.17	48.78	2.04
1	0	1	t	0	$1^3 9^1$	−542	455	998	10.01	0.20	29.96	46.29	20.94	2.51	0.10	49.00	1.96
1	0	0	t	1	$1^3 9^1$	−543	415	959	10.01	0.31	33.16	46.09	18.25	2.09	0.10	48.49	1.89
1	0	3	t	0	$1^3 9^1$	−514	388	902	9.94	0.22	36.47	47.78	14.08	1.44	0.00	49.45	1.80
0	1	1	t	0	$1^3 9^1$	−573	316	890	10.08	0.22	32.81	41.91	20.56	4.27	0.22	46.40	1.97
1	1	−2	t	0	$1^3 9^1$	−436	252	689	9.73	0.00	30.33	48.48	19.30	1.74	0.15	50.22	1.93
0	1	3	t	0	$1^3 9^1$	−382	378	761	9.56	0.13	32.98	46.78	18.66	1.45	0.00	48.36	1.88
1	1	0	t	1	$1^3 9^1$	−437	251	689	9.73	0.00	30.33	48.48	19.30	1.74	0.15	50.22	1.93
1	t	−1	$-t-1$	0	$1^2 2^1 8^1$	1	454	454	9.18	0.00	30.18	51.76	16.96	1.10	0.00	52.86	1.89
1	1	3	t	0	$1^3 9^1$	−131	295	427	9.23	0.23	35.60	47.78	14.75	1.64	0.00	49.65	1.82

TABLEAU 2. Résultats obtenus par famille. Dans la colonne "type de Δ", a^b signifie que le discriminant a b racines a-uples. Les colonnes suivantes donnent la plus petite et la plus grande valeur du paramêtre t des courbes dont on a pu calculer le rang, puis le nombre total de courbes considérées dans cet intervalle (c'est-à-dire le nombre de courbes non-singulières obtenues par spécialization avec $t_{\min} \leq t \leq t_{\max}$), et la valeur maximale du logarithme du conducteur des courbes en dehors de l'intervalle $[t_{\min}, t_{\max}]$. Les deux dernières colonnes donnent le pourcentage de courbes de rang pair, et le rang moyen sur les courbes considérées. La suite du tableau est au verso.

coefficients de la courbe sur $\mathbb{Q}(t)$					type			#	$\log_{10}$	% de spécialisations de rang égal à									%	rang
a_1	a_2	a_3	a_4	a_6	de Δ	$t_{\min}$	$t_{\max}$	tot	$N_{\max}$	0	1	2	3	4	5	6	7	8	pair	moy
familles de rang 2 sur $\mathbb{Q}(t)$																				
1	t	0	$-3-2t$	1	$1^4 8^1$	-250	670	921	12.82	0.22	0.54	33.44	43.00	19.87	2.93	0.00			53.53	2.91
1	t	-19	$-t-1$	0	$1^4 8^1$	-252	628	881	12.06	0.00	0.34	35.07	49.15	14.19	1.25	0.00			49.26	2.81
1	t	2	$-t-1$	0	$1^4 8^1$	-233	595	829	12.31	0.00	0.72	34.02	45.72	17.73	1.81	0.00			51.75	2.86
1	t	-16	$-t-1$	0	$1^4 8^1$	-165	445	611	11.47	0.00	0.65	40.75	46.64	11.46	0.49	0.00			52.21	2.70
1	t	13	$-t-1$	0	$1^4 8^1$	-310	516	827	11.88	0.00	0.12	37.73	46.55	14.75	0.85	0.00			52.48	2.78
1	t	-14	$-t-1$	0	$1^4 8^1$	-255	483	739	11.75	0.00	0.27	36.94	48.17	14.34	0.27	0.00			51.29	2.77
1	t	10	$-t-1$	0	$1^4 8^1$	-237	501	739	11.91	0.00	0.27	39.24	48.44	11.10	0.95	0.00			50.34	2.73
0	t	11	$-t-1$	0	$1^4 8^1$	-238	500	739	11.89	0.00	0.41	33.69	48.17	15.97	1.76	0.00			49.66	2.85
1	t	-11	$-t-1$	0	$1^4 8^1$	-184	550	735	12.08	0.00	0.27	35.65	46.39	17.01	0.68	0.00			52.65	2.82
0	t	7	$-t-1$	0	$1^4 8^1$	-233	496	730	11.95	0.00	0.14	34.66	48.22	15.07	1.92	0.00			49.73	2.84
1	t	-8	$-t-1$	0	$1^4 8^1$	-299	519	819	12.02	0.00	0.49	37.85	46.40	13.92	1.34	0.00			51.77	2.78
1	t	19	$-t-1$	0	$1^4 8^1$	-200	524	725	11.53	0.00	0.41	34.76	50.90	13.10	0.83	0.00			47.86	2.79
0	t	3	$-t-1$	0	$1^4 8^1$	-203	452	656	11.83	0.00	1.07	35.67	48.48	14.33	0.46	0.00			50.00	2.77
0	t	19	$-t-1$	0	$1^4 8^1$	-217	500	718	11.46	0.00	0.56	30.36	50.70	16.30	2.09	0.00			46.66	2.89
1	t	17	$-t-1$	0	$1^4 8^1$	-254	458	713	11.38	0.00	0.56	34.36	50.77	13.32	0.98	0.00			47.69	2.80
0	t	9	$-t-1$	0	$1^4 8^1$	-209	500	710	11.93	0.00	0.42	39.44	47.61	11.69	0.85	0.00			51.13	2.73
0	t	1	$-t-1$	0	$1^4 8^1$	-200	500	701	12.01	0.14	0.43	29.67	47.36	19.40	2.85	0.14			49.36	2.95
1	t	-7	$-t-1$	0	$1^4 8^1$	-192	500	693	11.97	0.00	0.43	38.67	45.60	14.29	1.01	0.00			52.96	2.77
1	t	8	$-t-1$	0	$1^4 8^1$	-189	499	689	11.94	0.00	0.58	34.69	49.64	14.22	0.87	0.00			48.91	2.80
1	t	-2	$-t-1$	0	$1^4 8^1$	-213	507	721	12.03	0.00	0.69	30.79	47.57	19.56	1.39	0.00			50.35	2.90
0	t	13	$-t-1$	0	$1^4 8^1$	-184	500	685	11.83	0.00	0.44	32.26	47.01	19.12	1.17	0.00			51.39	2.88
1	t	16	$-t-1$	0	$1^4 8^1$	-193	489	683	11.62	0.00	0.15	32.80	50.66	15.08	1.32	0.00			47.88	2.85
0	t	17	$-t-1$	0	$1^4 8^1$	-181	500	682	11.64	0.00	0.44	32.40	48.39	17.16	1.61	0.00			49.56	2.87
1	t	-10	$-t-1$	0	$1^4 8^1$	-197	481	679	11.85	0.00	0.44	40.35	46.69	11.63	0.88	0.00			51.99	2.72
1	t	-13	$-t-1$	0	$1^4 8^1$	-236	412	649	11.47	0.00	0.31	40.52	47.00	11.71	0.46	0.00			52.23	2.71
1	t	-5	$-t-1$	0	$1^4 8^1$	-172	504	677	12.01	0.00	0.59	38.55	44.90	14.48	1.48	0.00			53.03	2.78
1	t	11	$-t-1$	0	$1^4 8^1$	-168	500	669	11.88	0.00	0.15	37.97	46.64	14.50	0.75	0.00			52.47	2.78
1	t	-17	$-t-1$	0	$1^4 8^1$	-172	492	665	11.63	0.00	0.30	33.08	50.23	15.04	1.35	0.00			48.12	2.84
1	t	4	$-t-1$	0	$1^4 8^1$	-199	465	665	11.86	0.00	0.45	38.20	45.86	14.44	0.90	0.15			52.78	2.78
0	t	5	$-t-1$	0	$1^4 8^1$	-173	415	589	11.66	0.00	0.68	39.73	44.99	13.75	0.85	0.00			53.48	2.74
1	t	1	$-t-1$	0	$1^4 8^1$	-188	438	627	11.78	0.16	0.64	32.54	48.64	15.47	2.55	0.00			48.17	2.86
1	t	-4	$-t-1$	0	$1^4 8^1$	-179	445	625	11.80	0.00	0.48	38.08	45.76	13.92	1.76	0.00			52.00	2.78
1	t	14	$-t-1$	0	$1^4 8^1$	-135	475	611	11.67	0.00	0.65	42.55	45.34	10.80	0.65	0.00			53.36	2.68
1	t	5	$-t-1$	0	$1^4 8^1$	-282	316	599	11.17	0.00	0.67	43.07	46.74	9.18	0.33	0.00			52.25	2.65
1	t	7	$-t-1$	0	$1^4 8^1$	-220	368	589	11.41	0.00	0.85	38.54	47.20	12.90	0.51	0.00			51.44	2.74
familles de rang 3 sur $\mathbb{Q}(t)$																				
0	5	0	$-16t^2$	$64t^2$	$1^4 2^1 6^1$	0	488	488	14.95		0.20	0.82	28.89	47.75	20.49	1.84			50.41	3.93
0	41	0	$-64t^2+544$	2304	$1^4 2^1 6^1$	0	486	486	14.77		0.41	0.82	31.69	51.44	13.99	1.65			53.91	3.83
0	73	0	$-144t^2+1368$	1296	$1^4 2^1 6^1$	0	316	316	14.96		0.00	1.90	35.44	47.15	14.24	1.27			50.32	3.78
0	-7	0	$-16t^2$	$256t^2$	$1^4 2^1 6^1$	0	306	306	13.76		0.65	1.96	37.58	50.00	9.48	0.33			52.29	3.67
familles de rang 4 sur $\mathbb{Q}(t)$																				
0	41	0	$-16t^2+184$	144	$1^6 6^1$	0	505	506	16.65			0.59	1.19	28.06	47.43	19.76	2.77	0.00	48.42	4.92
0	161	0	$-400t^2+7000$	90000	$1^6 6^1$	0	394	395	18.70			0.51	1.77	27.85	46.58	20.25	2.53	0.25	48.86	4.92
0	49	0	$-144t^2+504$	1296	$1^6 6^1$	0	387	388	17.99			0.77	0.77	28.87	44.33	22.94	1.80	0.26	53.09	4.93
0	169	0	$-576t^2+3744$	20736	$1^6 6^1$	0	355	356	18.37			1.12	1.97	35.39	46.07	14.61	0.56	0.00	51.40	4.72
0	505	0	$-1296t^2+66744$	2624400	$1^6 6^1$	0	310	311	18.37			0.64	1.61	35.05	45.34	14.79	2.25	0.00	50.48	4.78
0	361	0	$-3600t^2+34200$	810000	$1^6 6^1$	0	298	299	19.41			0.33	2.01	32.11	45.82	17.39	2.01	0.00	50.17	4.83
0	281	0	$-784t^2+18424$	345744	$1^6 6^1$	0	296	297	18.40			0.67	2.02	30.98	44.11	21.21	0.67	0.00	52.86	4.84
0	649	0	$-2304t^2+42624$	331776	$1^6 6^1$	0	267	268	18.23			0.75	2.24	35.07	48.13	13.06	0.37	0.00	48.88	4.71
0	601	0	$-1296t^2+105624$	5143824	$1^6 6^1$	0	265	266	17.96			0.38	2.26	36.84	42.86	15.79	1.50	0.00	53.01	4.75
0	217	0	$-144t^2+14616$	291600	$1^6 6^1$	0	260	261	17.43			0.77	3.83	44.44	37.55	12.26	0.77	0.00	57.47	4.58
0	409	0	$-1296t^2+27864$	104976	$1^6 6^1$	0	256	257	16.92			0.78	0.78	34.24	43.19	19.07	1.56	0.00	54.09	4.82

TABLEAU 2 (suite)

– le rang moyen sur les courbes considérées.

Nous n'avons retenu que les familles où on avait réussi à calculer les rangs de plus de 250 courbes spécialisées. Les tableaux sont ordonnés par ordre décroissant du nombre de courbes calculées, ce qui rend les résultats du haut de chaque tableau probablement plus significatifs que ceux du bas.

Données générales. On a retenu les résultats concernant 66918 courbes appartenant à 93 familles. En fonction du rang des familles, ces courbes se répartissent comme suit :

rg $E(t)$	#familles	#courbes
0	31	26666
1	12	10462
2	35	24590
3	4	1596
4	11	3604

Parité. On conjecture que pour une famille donnée, la moitié des courbes seront de rang pair et l'autre de rang impair. Les résultats obtenus sont assez proches de cette conjecture.

Le tableau suivant donne les valeurs extrêmes et moyennes du pourcentage de courbes de rang pair, notés $P_{\min}$, $P_{\max}$ et P_{moy}, en fonction du rang des familles.

rg $E(t)$	$P_{\min}$	$P_{\max}$	P_{moy}
0	45.42	54.18	49.56
1	46.40	52.86	48.89
2	46.66	53.53	50.84
3	50.32	53.91	51.82
4	48.42	57.47	51.39

Distribution du rang. Le tableau 3 est une synthèse des résultats sur le rang. Partant d'une famille de rang r, on constate qu'on obtient toujours des courbes de rang r, $r+1$, $r+2$ et $r+3$ (à une exception près pour le rang $r+3$). On ne trouve que rarement du $r+4$ et jamais de $r+5$, mais bien sûr le faible nombre de courbes considérées ne permet pas de conclure.

r		rang $= r$	$r+1$	$r+2$	$r+3$	$r+4$
	min	27.58	42.89	5.56	0.00	0.00
0	max	43.88	54.25	20.82	3.08	0.17
	moy	33.46	48.65	16.07	1.79	0.03
	min	26.24	41.91	14.08	1.10	0.00
1	max	36.47	51.76	24.64	4.27	0.22
	moy	30.99	46.51	20.01	2.24	0.11
	min	29.67	43.00	9.18	0.27	0.00
2	max	43.07	50.90	19.87	2.93	0.15
	moy	36.10	47.46	14.72	1.23	0.01
	min	28.89	47.15	9.48	0.33	0.00
3	max	37.58	51.44	20.49	1.84	0.00
	moy	32.71	49.19	15.16	1.38	0.00
	min	27.85	37.55	12.26	0.37	0.00
4	max	44.44	48.13	22.94	2.77	0.26
	moy	32.82	44.98	17.76	1.64	0.06

TABLEAU 3. Résultats sur le rang.

On peut observer d'importantes variations entre les courbes, mais néanmoins certaines tendances semblent se dessiner. Les courbes de rang $r+1$ sont toujours majoritaires (à une exception près), suivies en géneral par les courbes de rang r puis de rang $r+2$. Les courbes de rang $\geq r+4$ sont toujours en quantité très faible, jamais plus de quelques pourcents. Enfin, lorsqu'on considère les moyennes sur toutes les courbes issues de familles de même rang, on trouves des valeurs très proches, de l'ordre de 32% pour le rang r, 48% pour le rang $r+1$, 18% pour le rang $r+2$ et 2% pour le rang $r+3$.

Les graphiques de la figure 1 montrent les pourcentages de courbes de différents rangs pour les courbes $y^2+xy=x^3+tx$ (rang 0) et $y^2+xy=x^3-2x^2+tx+1$ (rang 1), avec t prenant des valeurs inférieures en valeur absolue au paramètre $t_{\max}$ représenté en abscisse.

Enfin, il peut être instructif d'examiner le rang moyen, noté ici $\bar{r}$, des courbes de chaque famille. Le tableau 4 présente les valeurs extrêmes $\bar{r}_{\min}$ et $\bar{r}_{\max}$, ainsi que la moyenne notés $\bar{r}_{\text{moy}}$, en fonction du rang des familles. On constate que les valeurs moyennes sont stables autour de $r+0.85$, où r est le rang de la familles sur $\mathbb{Q}(t)$.

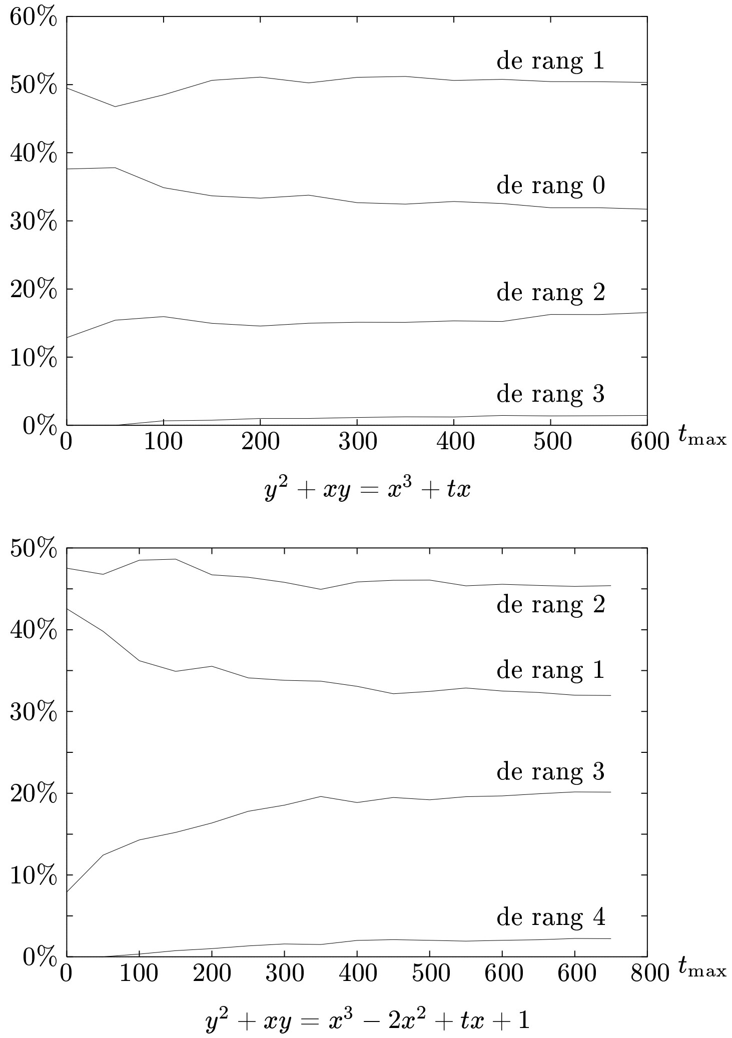

FIGURE 1. Pourcentages de courbes de différents rangs pour la famille $y^2+xy=x^3+tx$ (rang 0) et pour la famille $y^2+xy=x^3-2x^2+tx+1$ (rang 1), sur l'intervalle $-t_{\max} \le t \le t_{\max}$.

$\operatorname{rg} E(t)$	$\bar r_{\min}$	$\bar r_{\max}$	$\bar r_{\text{moy}}$
0	0.65	0.98	0.86
1	1.80	2.04	1.94
2	2.65	2.95	2.80
3	3.67	3.93	3.82
4	4.58	4.93	4.82

TABLEAU 4. Valeurs extrêmes et moyenne de r en fonction du rang des familles.

5. ÉTUDE COMPLÉMENTAIRE SUR LES FORMULES EXPLICITES

On a tenté de mettre en évidence, à l'aide des données que l'on avait collectées, la dépendance entre le conducteur d'une courbe et le paramètre de coupure λ qu'il convient de choisir pour optenir une majoration qui donne la valeur exacte du rang, c'est-à-dire telle que $\operatorname{rg} E = \lfloor r_\lambda^+(E) \rfloor$.

Pour cela, on a choisit de regarder les courbes de rang 0, 1 et 2 issues de la famille $y^2+xy=x^3+tx$, baptisée E_0 dans ce qui suit car elle est de rang 0, les courbes de rang 2, 3 et 4 issues de la famille E_2 : $y^2+xy=x^3+x^2-(3+2t)x+1$ (de rang 2 sur $\mathbb{Q}(t)$), et enfin les courbes de rang 4, 5 et 6 issues de la famille E_4 :

$$y^2=x^3+113x^2+(-16t^2+3880)x+(-384t^2+42000),$$

de rang 4. On a choisit ces familles car c'étaient celles où on avait pu calculer le plus grand nombre de rangs.

On a ordonné ces courbes par conducteur croissant, et on a calculé r_λ^+ en faisant croître $\exp\lambda$ géométriquement de 2 à 300000, en s'arrêtant dès que $\lfloor r_\lambda^+(E) \rfloor = \operatorname{rg} E$. On a arrêté les calculs à chaque fois qu'on a trouvé une courbe telle que $r^+_{\log 300000}(E) \ge \operatorname{rg} E + 1$.

On a tracé les graphiques donnant λ en fonction de $\log N$ dans chacun des cas considérés. Le tableau 5 donne pour chaque cas :

– le nombre de courbes où le calcul a réussi,
– la plus grande valeur du logarithme du conducteur atteinte,
– les valeurs extrêmes du rapport $\alpha = \lambda/\log N$, ainsi que la valeur moyenne, notées respectivement $\alpha_{\min}$, $\alpha_{\max}$ et α_{moy}.

Notons que la donnée $\log N_{\max}$ n'est pas significative pour les courbes de rang $r+2$ issues des courbes E_r, $r=0,2,4$, car dans ce cas on s'est arrêté après avoir calculé avec succès toutes les courbes.

Il ne faut pas non plus comparer les nombres de courbes issues des trois familles, car pour E_2 et E_4, on n'a considéré que les paramètres $t \ge 0$.

	rg	#	$\log N_{\max}$	$\alpha_{\min}$	$\alpha_{\max}$	α_{moy}
E_0	0	164	13.0547	0.3408	0.9503	0.5603
	1	433	15.2336	0.2764	0.8489	0.4237
	2	230	(17.9197)	0.2522	0.5809	0.3520
E_2	2	57	21.5492	0.2530	0.5277	0.3851
	3	172	25.6669	0.2246	0.4778	0.3384
	4	165	(29.5045)	0.2015	0.3905	0.2879
E_4	4	95	34.1659	0.2207	0.3752	0.3005
	5	179	37.2875	0.2017	0.3349	0.2707
	6	100	(39.6906)	0.1806	0.2924	0.2240

TABLEAU 5. Valeurs extrêmes et moyenne du quotient $\alpha = \lambda/\log N$ pour trois familles (page 127).

La première constatation est que les formules explicites sont d'autant plus efficaces que le rang des courbes considérées est grand.

En ce qui concerne les courbes de rang ≤ 2, sur nos exemples, on peut douter de la supériorité des formules explicites sur les méthodes de calcul des fonctions L (qui sont en $O(\sqrt{N})$, ce qui correspond asymptotiquement à $\alpha = 1/2$). En moyenne, on semble cependant obtenir des $\alpha < 1/2$ à partir du rang 1.

Il faut noter aussi que les rapports α obtenus avec les courbes de rang 2 obtenues à partir de E_0 et E_2 ou avec les courbes de rang 4 obtenues à partir de E_2 et E_4 sont très similaires.

REMERCIEMENTS

Je remercie Jean-François Mestre qui m'a suggéré ces recherches et Antoine Chambert-Loir qui les a encouragées.

POUR OBTENIR LES FICHIERS

L'intégralité des résultats des calculs est disponible par ftp anonyme sur le serveur `ftp.ens.fr`, dans le répertoire `/pub/maths`, qui contient par ailleurs les renseignements nécessaires à l'interprétation des fichiers.

BIBLIOGRAPHIE

[Atkin et Lehner 1970] A. O. L. Atkin et J. Lehner, "Hecke operators on $\Gamma_0(N)$", *Math. Ann.* **185** (1970), 134–160.

[Billard 1995] Hervé Billard, "Sur la répartition des points rationnels de surfaces algébriques", thèse de doctorat de l'université Paris 7, 1995.

[Brumer 1991] Armand Brumer et Oisin McGuinness, "The behavior of the Mordell–Weil group of elliptic curves", *Bull. Amer. Math. Soc.* **23** (1990), 375–382.

[Buhler et al. 1985] J. P. Buhler, B. H. Gross et D. B. Zagier, "On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3", *Math. Comp.* **44**, 473–481, 1985.

[Deligne 1973] Pierre Deligne, "Les constantes des équations fonctionnelles des fonctions L", pp. 501–595 dans *Modular Functions of One Variable* (Antwerp, 1972), volume 2, Lect. Notes in Math. **349**, Springer, Berlin, 1973.

[Fermigier 1992] Stéfane Fermigier, "Un exemple de courbe elliptique sur $\mathbb{Q}$ de rang ≥ 19", *C. R. Acad. Sci. Paris* (série 1) **315** (1992), 719–722.

[Fouvry et Pomykala 1993] Etienne Fouvry et Jacek Pomykala, "Rang des courbes elliptiques et sommes d'exponentielles", *Monatshefte für Mathematik* **116** (1993), 111–125.

[Gebel et Zimmer 1994] Josef Gebel et Horst G. Zimmer, "Computing the Mordell–Weil group of an elliptic curve over $\mathbb{Q}$", pp. 61–83 dans *Elliptic curves and related topics* (édité par H. Kisilevsky et M. R. Murty), CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, 1994.

[Geist et al. 1994] Al Geist et al., *PVM: Parallel Virtual Machine: A Users' Guide and Tutorial for Networked Parallel Computing*, MIT Press, Cambridge, MA, 1994. On pourra trouver des informations sur le système PVM3 et en télécharger les sources sur le site officiel du groupe PVM, à l'adresse http://www.epm.ornl.gov/pvm/.

[Mestre 1986] Jean-François Mestre, "Formules explicites et minorations de conducteurs de variétés algébriques", *Compositio Mathematica* **58** (1986), 209–232.

[Mestre 1991a] Jean-François Mestre, "Courbes elliptiques de rang ≥ 11 sur $\mathbb{Q}(t)$", *C. R. Acad. Sci. Paris* (série 1) **313** (1991), 139–142.

[Mestre 1991b] Jean-François Mestre, "Courbes elliptiques de rang ≥ 12 sur $\mathbb{Q}(t)$", *C. R. Acad. Sci. Paris* (série 1) **313** (1991), 171–174.

[Mestre 1992] Jean-François Mestre, "Un exemple de courbe elliptique sur $\mathbb{Q}$ de rang ≥ 15", *C. R. Acad. Sci. Paris* (série 1) **314** (1992), 453–455.

[Michel 1995] Philippe Michel, "Rang moyen de familles de courbes elliptiques et lois de Sato–Tate", *Monatshefte für Mathematik* **120** (1995), 127–136.

[Nagao 1992] Koh-ichi Nagao, "Examples of elliptic curves over $\mathbb{Q}$ with rank ≥ 17", *Proc. Japan Acad.* A**68**(9) (1992), 287–289.

[Nagao 1993a] Koh-ichi Nagao, "An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20", *Proc. Japan Acad.* A**69**(9) (1992), 291–293.

[Nagao 1993b] Koh-ichi Nagao et Tomonori Kouya, "An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 21", prépublication, Shiga Polytechnic College, 1993.

[Nagao 1993c] Koh-ichi Nagao, "An example of elliptic curve over $\mathbb{Q}(T)$ with rank ≥ 13", prépublication, Shiga Polytechnic College, 1993.

[Rohrlich 1993] David E. Rohrlich, "Variation of the root number in families of elliptic curves", *Comm. Math.* **87** (1993), 119–151.

[Shioda 1990] Tetsuji Shioda, "On the Mordell–Weil Lattices", *Comm. Math. Univ. Sancti Pauli* **39**(2), 1990.

[Silverman 1986] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[Tate 1975] John Tate, "Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil", pp. 33–53 dans Modular Functions of one Variable (Antwerp 1972), volume 4, Lect. Notes in Math **476**, Springer, Berlin 1975.

Stéfane Fermigier, Mathématiques, Université Paris 7 Denis Diderot, France (fermigie@frmap711.mathp7.jussieu.fr)

Received September 25, 1995 ; accepted March 15, 1996