ACTA ARITHMETICA
LXXXII.4 (1997)

Une courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 22

par

Stéfane Fermigier (Paris)

Nous présentons un exemple de courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 22, en détaillant les méthodes qui ont permis cette découverte.

1. Introduction. Dans [5], et dans [7] avec Kouya, Nagao donne deux exemples de courbes elliptiques définies sur $\mathbb{Q}$ avec respectivement 20 et 21 points rationnels indépendants. Nous n'avions jusqu'à une date récente pas réussi à obtenir de nouveaux exemples comparables (i.e. de courbes de rang ≥ 20).

Nous avons pourtant récemment (mai 1996) réussi à améliorer ce résultat, en employant essentiellement des méthodes désormais classiques, avec juste un ingrédient supplémentaire.

2. Construction

2.1. *Courbes de rang ≥ 12 sur $\mathbb{Q}(t)$.* Le point de départ de notre construction est une famille à deux paramètres de courbes elliptiques sur $\mathbb{Q}(t)$ de rang ≥ 12 dont Jean-François Mestre nous a communiqué la construction [4].

Soient, dans $\mathbb{Q}(u, v)$,

$$\begin{aligned}
a_1 = {} & -v+v^2-v^3+v^4+2uv+v^2u-2v^3u+v^4u+u^2+u^2v-2v^2u^2 \\
& -2v^3u^2+u^3v^2-u^4, \\
a_2 = {} & v^3u^2-2v^2u^2+v^2u-2u^3v^2-2u^3v+u^2v+u^4v+2uv \\
& -v^4-u+v^2-u^3+u^2+u^4, \\
a_3 = {} & -v^4u+2v^3u+v^3u^2+v^2u^2+v^2u-u^3v^2-2u^3v-2u^2v \\
& +u^4v-v+v^3-2u^3+u^2+u^4, \\
a_4 = {} & v-v^2+v^3-v^4+u-2uv+v^2u+2v^3u-2u^2-2u^2v+v^2u^2 \\
& +v^3u^2+u^3-u^4v,
\end{aligned}$$

1991 *Mathematics Subject Classification*: 11G05, 14H52, 11Y50.

$$a_5 = v^4u - 2v^3u - v^3u^2 + v^2u^2 - 2v^2u + u^3v^2 + 2u^3v + u^2v + v^4 - u - 2v^3 + v^2 + u^3 - u^4v,$$
$$a_6 = v - 2v^2 + v^3 + u - 2uv - 2v^2u - v^4u - u^2 + u^2v + v^2u^2 + u^3 + 2u^3v + u^3v^2 - u^4.$$

Posons ensuite, comme dans [2],

$$p_6 = (x - a_1)\dots(x - a_6), \quad \text{puis} \quad q = p_6(x - t)p_6(x + t).$$

On peut ensuite trouver deux polynômes g et r tels que $\deg_x g = 6$, $\deg_x r \le 5$ et $q = g^2 - r$. Avec notre choix de $a_1, \dots, a_6$, le polynôme r est en fait de degré 4 (en x, sur $\mathbb{Q}(u, v, t)$). La courbe quartique $Q : y^2 = r(x)$ a 12 points rationnels sur $\mathbb{Q}(t)$, d'abscisses $x_1 \pm t, \dots, x_6 \pm t$, plus un treizième, d'abscisse $A + Bt$, avec

$$A = (3u^2v + 3u^3v^2 + 2u^4v + uv - 4v^3u - 3v^2u^2 + 3v^3u^2 - 4u^3v + v^3 + 2v^4u - 3u^4 + u^3 - 3v^4 + u + 3v^2u + v - u^4v^3 - 2u^4v^2 - u^3v^4 - 4u^3v^3 + u^2v^5 - 2u^2v^4 + uv^5 + u^5v^2 + u^5v - v^6 - u^6 + 2v^5 + 2u^5)/(u^2 + v^2 + 1),$$
$$B = (-u^2 - v^2 + 2u + 2v + 1)/(u^2 + v^2 + 1).$$

A noter qu'on peut fréquemment, pour certaines valeurs de u et v, appliquer la paramétrisation de [3] pour en déduire des courbes de rang ≥ 13 sur $\mathbb{Q}(t)$. On retrouve en particulier la courbe de Nagao [6] en partant de $u = 2$ et $v = 5$.

2.2. *Recherche de courbes intéressantes sur* $\mathbb{Q}(t)$. On utilise la construction précédente pour fournir, en faisant varier u et v, une liste de courbes de rang ≥ 12 sur $\mathbb{Q}(t)$ (on élimine bien sûr toutes les courbes dégénérées ou dont les 12 points ne sont pas indépendants). On trie ensuite cette liste à l'aide d'une "fonction heuristique", comme Nagao et Kouya dans [7] : si $E(t)$ est une famille de courbes à un paramètre, on considère

$$\mathcal{S}(E(t), M) = \sum_{u=0}^{M-1} \sum_{p \text{ premier} < M} \frac{2 - a_p(\widetilde{E}(u))}{p + 1 - a_p(\widetilde{E}(u))} \cdot \frac{\log p}{p},$$

où $\widetilde{E}(u)$ est le modèle minimal (sur $\mathbb{Z}$) de la courbe obtenue en spécialisant t en u dans $E(t)$, et a_p le nombre de points d'une courbe sur $\mathbb{F}_p$. Cette formule est une sorte de moyenne des fonctions heuristiques considérées par exemple dans [1]. On s'accorde à penser que la famille donnera plus de courbes de grand rang si $\mathcal{S}(E, M)$ est élévé. On a pris en pratique la valeur $M = 500$.

Parmi les courbes que nous avons étudiées (une centaine), la "meilleure" (du point de vue de la fonction heuristique) est celle qui correspond aux paramètres $(a_1, \dots, a_6) = (0, 55, 314, 378, 1007, 1036)$. Comme ces para-

mètres sont de taille raisonnable, c'est sur cette courbe que nous avons concentré la suite de nos investigations.

2.3. *Recherche de courbes sur* $\mathbb{Q}$. On utilise ensuite encore la méthode des fonctions heuristiques, cette fois sur la famille déterminée ci-dessus. La fonction considérée cette fois est

$$S(E,M) = \sum_{p \leq M} \frac{2 - a_p}{p + 1 - a_p} \log p.$$

On calcule $S(E,M)$ pour E dans la famille considérée et pour différentes valeurs de M : 50, 100, 200, 400, 1000 et 2000. A chaque étape, on élimine les courbes qui sont en dessous de certains seuils, déterminés empiriquement pour laisser passer les courbes de grand rang déjà connues (avec une marge d'autant plus grande que M est faible).

On utilise par ailleurs une astuce de Nagao qui permet d'accélérer considérablement les calculs.

A l'aide de nos bibliothèques de calcul sur les courbes elliptiques (basée sur PARI) et de calculs distribués (basée sur PVM3), on a ainsi obtenu en environ une semaine de calculs sur une centaine de stations SUN la courbe de paramètre $t = 19754/39$, sur laquelle on a ensuite trouvé 22 points rationnels indépendants.

Les valeurs de la fonction heuristique $S(E,M)$ pour notre courbe, notée E_{22}, les courbes de Nagao et Kouya [7] (resp. Nagao [5]), de rang resp. ≥ 21 et ≥ 20, notées E_{21} et E_{20}, et notre courbe de rang ≥ 19 (cf. [1]), notée E_{19}, sont données par le tableau suivant :

M	50	100	200	400	1000	2000	4000	10000
E_{22}	29.49	44.12	57.54	81.51	105.17	122.76	143.84	166.47
E_{21}	28.01	43.74	60.95	74.75	99.98	113.77	126.56	154.71
E_{20}	26.26	42.78	57.03	76.47	100.06	111.81	128.12	148.81
E_{19}	27.85	42.84	61.69	76.47	99.73	113.65	131.22	155.42

Comme on le voit, la courbe E_{22} arrive très nettement en tête pour $M \geq 400$, alors que les trois autres sont plus serrées. En particulier, la courbe E_{19} arrive devant E_{20} et E_{21} pour les grandes valeurs de M. Bien sûr, on ne peut rien en conclure puisqu'on ne connaît le rang exact d'aucune de ces courbes !

3. Résultats

THÉORÈME 1. *Soit* E_{22} *la courbe elliptique*

$$\begin{aligned} E_{22} : y^2 + xy + y &= x^3 - 940299517776391362903023121165864x \\ &\quad + 10707363070719743033425295515449274534651125011362 \end{aligned}$$

et soient $P_1, \ldots, P_{22}$ *comme ci-dessous. Alors* $E_{22}(\mathbb{Q})$ *est de rang* ≥ 22 *sur* $\mathbb{Q}$ *et* $P_1, \ldots, P_{22}$ *sont des points indépendants dans* $E(\mathbb{Q})$.

$$P_1 = [32741153161482344264/3025, \\ -22308967458711097957853216 9697/166375],$$

$$P_2 = [215521674613198983365/24649, \\ -68729491550613535542357043789 47/3869893],$$

$$P_3 = [637312541911044643/81, -1420356190129296832193564087/729],$$

$$P_4 = [-11906250919327880080/361, \\ -16580788535875788634285886853/6859],$$

$$P_5 = [-136152345735493381/4, -144822705450457359132816 93/8],$$

$$P_6 = [-27830298157016213012252/7134241, \\ 72099692861364392796183359497454267/19055557711],$$

$$P_7 = [4127671322151440, 26261076920456131162916 46],$$

$$P_8 = [6175679781777296, 22662543359970331246784 49],$$

$$P_9 = [12047255022287093, 10619932365259439209804 77],$$

$$P_{10} = [416685837455186583191/32761, \\ 532126822278670966916031158736 9/5929741],$$

$$P_{11} = [149915813139075767108024/10220809, \\ 87043268381086469491776631579171 17/32675926373],$$

$$P_{12} = [58759417448623559/4, 20309685531507133986546 57/8],$$

$$P_{13} = [237195157887349854919517/16024009, \\ -11477798111611307979707215505421441/64144108027],$$

$$P_{14} = [9568474434078537574436/687241, \\ 319520556343135681977874272805086/569722789],$$

$$P_{15} = [1725892668710258675291/177241, \\ 11737805066346484577096645302 5039/74618461],$$

$$P_{16} = [-35277008506980340471/1024, \\ 48766027143946934186731674507/32768],$$

$$P_{17} = [-2752742763529705669/121, 60005322521859823812335856 99/1331],$$

$$P_{18} = [-18552633109178014, -46654662158243394367179 66],$$

$$P_{19} = [-11325170733869118773764 9969/3304065361, \\ 3101525278948314708200098723732293417 39/189920981015641],$$

$$P_{20} = [-7572001778163591251/729, \\ -86590661426506799357663502953/19683],$$

$$P_{21} = [-3805260485540322851522 11/11242609,$$
$$730812357449313076847906230684902 33/37696467977],$$
$$P_{22} = [-1503889497722021588110681/42784681,$$
$$-160705885170116750151534640924719585/279854598421].$$

P r e u v e. La matrice des hauteurs de Néron–Tate de ces points, calculée avec PARI, est inversible, de déterminant $\simeq 1.299202 \cdot 10^{22}$. ∎

Références

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

[2] J.-F. Mestre, *Courbes elliptiques de rang* ≥ 11 *sur* $\mathbb{Q}(t)$, ibid. 313 (1991), 139–142.

[3] —, *Courbes elliptiques de rang* ≥ 12 *sur* $\mathbb{Q}(t)$, ibid. 313 (1991), 171–174.

[4] —, communication privée, 1993.

[5] K.-I. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20, Proc. Japan Acad. Ser. A 69 (8) (1993), 291–293.

[6] —, *An example of elliptic curve over* $\mathbb{Q}(T)$ *with rank* ≥ 13, ibid. 70 (5) (1994), 152–153.

[7] K.-I. Nagao and T. Kouya, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 21, ibid. 70 (4) (1994), 104–105.

UFR de mathématiques
Université Paris VII
2, place Jussieu
75005 Paris, France
E-mail: fermigie@math.jussieu.fr

Reçu le 21.1.1997 (3120)