

FAMILLES DE COURBES ELLIPTIQUES DE RANG ≥ 1 ET REMARQUES SUR UNE FONCTION ARITHMÉTIQUE ASSOCIÉE À UN ALGORITHME DE 2-DESCENTE DE TATE

CLAUDE LÉVESQUE

RÉSUMÉ. Nous exhibons quelques familles infinies de courbes elliptiques sur $\mathbf{Q}$ dont le rang est ≥ 1 . Pour chaque courbe elliptique E considérée, nous exhibons un point rationnel P de la courbe elliptique E et le théorème de Lutz-Nagell nous garantira que le double $2P = (x_2, y_2)$ n'est pas de torsion, x_2 s'avérant ne pas être un entier. Nous considérons ensuite la fonction arithmétique $\tilde{f}_m(n) := \#\{i \in \mathbf{N} : i|n \text{ et } i + m + \frac{n}{i} \text{ est un carré parfait}\}$ et nous montrons que $\limsup_{m,n \rightarrow \infty} \tilde{f}_m(n) = +\infty$. Nous déterminons enfin l'ordre moyen de $\tilde{f}_m(n)$.

ABSTRACT. A few infinite families of elliptic curves over $\mathbf{Q}$ of rank ≥ 1 are exhibited. For each elliptic curve E under consideration, we exhibit a rational point P on E to conclude from the Lutz-Nagell theorem that $2P = (x_2, y_2)$ is not a torsion point, since x_2 turns out not to be an integer. Then we study the arithmetical function $\tilde{f}_m(n) := \#\{i \in \mathbf{N} : i|n \text{ and } i + m + \frac{n}{i} \text{ is a perfect square}\}$; we show that $\limsup_{m,n \rightarrow \infty} \tilde{f}_m(n) = +\infty$ and we estimate the average order of $\tilde{f}_m(n)$.

1. Introduction. L.J. Mordell [Mor] a démontré que l'ensemble $E(\mathbf{Q})$ des points rationnels de la courbe elliptique sur $\mathbf{Q}$

$$E : Y^2 = X^3 + sX^2 + tX + u, \quad \text{avec } s, t, u \in \mathbf{Z},$$

est un groupe de type fini isomorphe (modulo la torsion) à un produit direct de r copies de $\mathbf{Z}$; l'entier r est alors dit le rang de E sur $\mathbf{Q}$; de plus, le discriminant de E est (voir page 68 de [H])

$$\Delta = -16(4t^3 + 27u^2) + 16(s^2t^2 - 4s^3u + 18stu) \neq 0,$$

et l'abscisse $x(2P)$ du point $P = (x_1, y_1)$ de E , où $y_1 \neq 0$, est (voir page 25 de [H])

$$x(2P) = \left(\frac{3x_1^2 + 2sx_1 + t}{2y_1} \right)^2 - s - 2x_1 = \left(\frac{x_1^2 - t}{2y_1} \right)^2 - \frac{u(2x_1 + s)}{y_1^2}.$$

Reçu le 20 octobre 1994 et, sous forme définitive, le 8 mars 1996.

Nous nous intéresserons surtout aux courbes elliptiques E de la forme

$$E : Y^2 = X^3 + mX^2 + nX, \quad \text{avec } m, n \in \mathbf{Z},$$

le discriminant de E étant $\Delta = 16n^2(m^2 - 4n) \neq 0$. J. Tate a donné un algorithme permettant de trouver la valeur r du rang d'une telle courbe E (dont la 2-torsion n'est pas triviale). Voici la description de cet algorithme de 2-descente dont l'intérêt ne fait aucun doute, mais qu'on ne peut malheureusement pas pour le moment qualifier d'effectif :

- (i) appelez $g(n)$ le nombre d'entiers c de $\mathbf{Z}$ tels que $c|n$, c est sans facteur carré et l'équation diophantienne

$$cS^4 + mS^2T^2 + \frac{n}{c}T^4 = U^2 \quad (1.1)$$

possède une solution entière (S, T, U) non triviale, (i.e. $(S, T, U) \neq (0, 0, 0)$);

- (ii) considérez la courbe E' qui est 2-isogène à E ,

$$E' : Y^2 = X^3 + m'X^2 + n'X, \quad \text{où } m' = -2m, \quad \text{et } n' = m^2 - 4n;$$

- (iii) définissez $g'(n')$ de façon semblable à $g(n)$;

- (iv) le rang r de E vérifie alors l'égalité

$$2^r = \frac{g(n)g'(n')}{4}.$$

Pour plus de détails, on peut consulter les notes célèbres de J. Tate [Ta], où les jolies notes des frères Murty [M-M]. Si on n'a pas accès à la littérature underground, voir [Co, H, S, Cas] ou [Mur].

Considérant la courbe elliptique $E : Y^2 = X^3 + nX$, D. Clark [Cl] a associé au rang de E la fonction arithmétique

$$f(n) := \#\{(a, b) \in \mathbf{Z} \times \mathbf{Z} : ab = n \text{ et } a + b \text{ est un carré parfait}\}.$$

Il a prouvé que $\limsup_{n \rightarrow \infty} f(n) = +\infty$ et a aussi déterminé (avec une preuve erronée) l'ordre moyen de $f(n)$, i.e. le comportement asymptotique de $\sum_{1 \leq n \leq x} f(n)$.

Fixons $m \in \mathbf{Z}$; pour $n \neq 0$, définissons la fonction arithmétique

$$f_m(n) := \#\{(a, b) \in \mathbf{Z} \times \mathbf{Z} : ab = n \text{ et } a + m + b \text{ est un carré parfait}\}. \quad (1.2)$$

Cette définition découle naturellement de l'algorithme de Tate et correspond à la situation où l'équation diophantienne (1.1) possède la solution $(S, T) = (1, 1)$. Il devient alors clair que le rang r de la courbe elliptique

$$E : Y^2 = X^3 + mX^2 + nX, \quad \text{où } m, n \in \mathbf{Z} \text{ avec } \Delta = 16n^2(m^2 - 4n) \neq 0,$$

vérifie l'inégalité $f_m(n) \leq 2^{r+2}$ lorsque n est sans facteur carré.

Notre fonction $f_m(n)$ est une généralisation de la fonction $f(n)$ de D. Clark, vu que les deux coïncident lorsque $m = 0$. Nous tenons cependant à dire que cette fonction $f_m(n)$ n'est pas vraiment nouvelle, car elle fut implicitement considérée en 1974 par

D.E. Penny et C. Pomerance : voir l'équation (4) de [Pe-Po 1]; voir aussi [Pe-Po 2] et [Kr]. Déjà là, et même auparavant, il est vraiment clair que si pour un $m \in \mathbf{Z}$ on avait

$$\limsup_{\substack{n \rightarrow \infty \\ n \text{ sans facteur carré}}} f_m(n) = +\infty,$$

eh bien!, il existerait des courbes elliptiques de rang plus grand que n'importe quel entier fixé à l'avance.

Dans cet article, nous commençons par exhiber quelques familles infinies de courbes elliptiques de rang ≥ 1 . Pour chaque courbe elliptique considérée, nous exhiberons en fait un point rationnel (x_0, y_0) dont l'abscisse x_0 n'est pas un nombre entier. Le théorème de Lutz-Nagell [H] nous garantira que (x_0, y_0) n'est pas de torsion. En effet, ce dernier théorème affirme que si (x_0, y_0) est un point de torsion de la courbe elliptique à coefficients entiers $E : Y^2 = X^3 + sX^2 + tX + u$, alors x_0 et y_0 sont tous deux des entiers rationnels. Puis nous nous proposons d'étudier la fonction $f_m(n)$ et de montrer que

$$\limsup_{m, n \rightarrow \infty} f_m(n) = +\infty.$$

Il n'y a, hélas!, aucune originalité dans les preuves que nous donnerons, mais nous croyons en l'importance d'énoncer des résultats qui d'une part sont amusants et qui d'autre part sont plus généraux que ceux de [Cl].

2. Des courbes elliptiques de rang ≥ 1 . Les courbes elliptiques E que nous considérons dans ce chapitre sont toutes définies sur $\mathbf{Q}$ et sont (sous certaines conditions) de rang ≥ 1 , parce qu'en chaque cas nous pouvons explicitement exhiber un point P sur la courbe E tel que le double $2P$ de ce point P n'est pas de torsion.

Proposition 2.1.

- (i) Soit $m \in \mathbf{Z}$. Alors la courbe elliptique $E : Y^2 = X^3 + mX^2 + NX$ est de rang ≥ 1 , lorsque

$$N = cB^2 - cm - c^2$$

avec $c, B \in \mathbf{Z}$, non nuls et assujettis aux restrictions

$$B^2 \neq m + c, \quad B \nmid (m + 2c).$$

- (ii) Soit $n \in \mathbf{Z}$ avec $n \neq 0$. Alors la courbe elliptique $E : Y^2 = X^3 + MX^2 + nX$ est de rang ≥ 1 , lorsque

$$M = A^2 - \frac{n}{c} - c$$

avec $c, A \in \mathbf{Z}$, non nuls et assujettis aux restrictions

$$c \mid n, \quad A \nmid \frac{n - c^2}{c}.$$

Démonstration. (i) Le discriminant Δ de E est $16N^2(m^2 - 4N)$ et est non nul si $N \neq 0$ et si $m^2 \neq 4N$. Or $N = 0$ entraîne $B^2 = m + c$, une contradiction. Et $m^2 = 4N$ entraîne $4cB^2 = (m + 2c)^2$, i.e. entraîne $B|(m + 2c)$, une autre contradiction. Considérant le point $P = (c, cB)$ de E , nous voyons que l'abscisse $x(2P)$ du point $2P$ est le nombre

$$x(2P) = \left(\frac{B^2 - (m + 2c)}{2B} \right)^2$$

qui n'est jamais entier vu que $B \nmid (m + 2c)$. Donc $2P$ n'est pas un point de torsion, de sorte que E est de rang ≥ 1 .

(ii) Ici $\Delta = 16n^2(M^2 - 4n) \neq 0$ car $n \neq 0$ et car $M^2 \neq 4n$. En effet, si $M^2 = (A^2 - (\frac{n}{c} + c))^2 = 4n$, alors

$$A^2 \mid \left(\frac{n}{c} + c \right)^2 - 4n = \left(\frac{n - c^2}{c} \right)^2, \text{ i.e. } A \mid \frac{n - c^2}{c},$$

une contradiction. Enfin l'abscisse du point $2P$, où $P = (c, cA)$ est un point de E , prend la valeur

$$x(2P) = \left(\frac{n - c^2}{2cA} \right)^2$$

et n'est jamais un entier, de sorte que E est de rang ≥ 1 . $\square$

Considérons maintenant des courbes elliptiques dites *pythagoriciennes*.

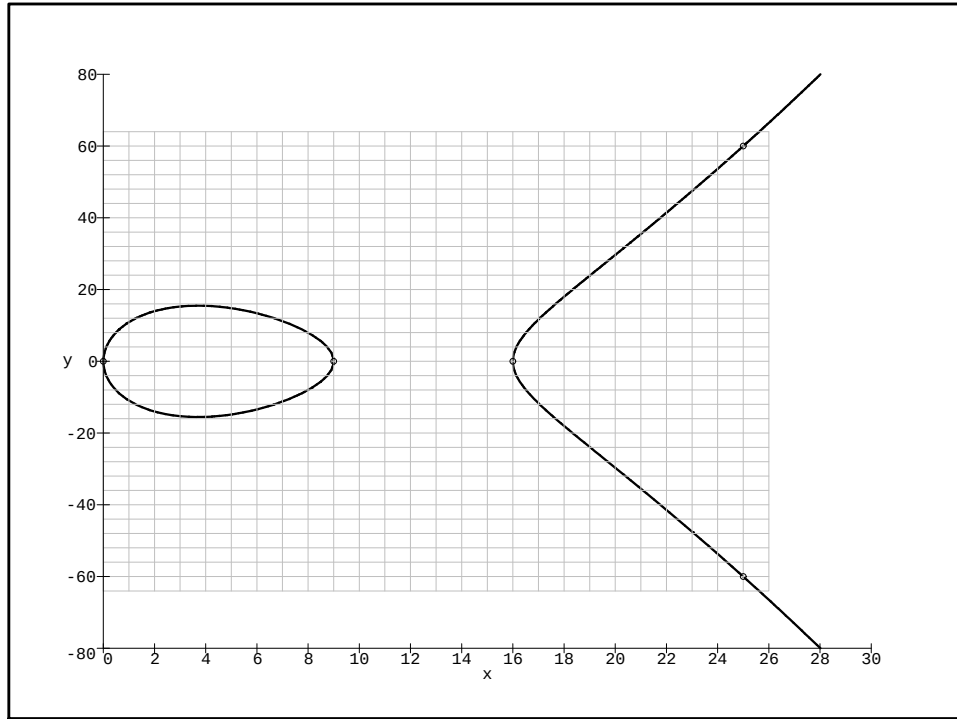


Figure. Courbe elliptique $E : Y^2 = X(X - 3^2)(X - 4^2)$

Proposition 2.2. Soit (a, b, c) un triplet pythagoricien, i.e. a, b, c sont des entiers non nuls, copremiers deux à deux, qui vérifient $a^2 + b^2 = c^2$. Alors la courbe elliptique pythagoricienne

$$E : Y^2 = X(X - a^2)(X - b^2) = X^3 - c^2X^2 + a^2b^2X$$

est de rang ≥ 1 .

Démonstration. Le point $P = (c^2, abc)$ est un point de la courbe elliptique E dont le discriminant $\Delta = 16a^4b^4(a^2 - b^2)^2$ est non nul car $(a^2 - b^2)^2 \neq 0$. L'abscisse de $2P$ est

$$x(2P) = \left(\frac{c^4 - a^2b^2}{2abc} \right)^2$$

et n'est jamais un entier car $c \neq \mp 1$ et $c \nmid a^2b^2$ (ou plus simplement car le numérateur de $x(2P)$ est impair). Donc $2P$ n'est pas de torsion et le rang de E est ≥ 1 . $\square$

Proposition 2.3.

- (i) Supposons que a, b, c sont des entiers non nuls tels que a et b ne sont pas tous les deux pairs, et vérifient l'égalité $a + b = c$ avec $a \neq b$. Alors la courbe elliptique

$$E' : abcY^2 = X(X - a)(X - b) = X^3 - cX^2 + abX$$

est de rang ≥ 1 .

- (ii) La courbe elliptique (isomorphe à E')

$$E : Y^2 = X(X - (abc)a)(X - (abc)b) = X^3 - (abc)cX^2 + (abc)^2abX$$

est aussi de rang ≥ 1 .

Démonstration. (i) Le premier résultat découle de (ii). Remarquons en passant que $(c, 1)$ est un point de E' .

(ii) Le discriminant de E est $\Delta = 16(abc)^6a^2b^2(a - b)^2 \neq 0$. La courbe E contient $P = ((abc)c, (abc)^2)$ et l'abscisse

$$x(2P) = \left(\frac{a^2 + ab + b^2}{2} \right)^2$$

de $2P$ n'est pas un entier. $\square$

Corollaire 2.4. Soit p un premier impair. Supposons que le dernier théorème de Fermat est faux, i.e. supposons qu'il existe des entiers a, b, c non nuls tels que $a^p + b^p = c^p$ avec $(a, b) = 1$.

- (i) Alors la courbe elliptique

$$E' : abcY^2 = X(X - a^p)(X - b^p) = X^3 - c^pX^2 + (ab)^pX$$

est de rang ≥ 1 .

- (ii) De plus, la courbe elliptique (isomorphe à E')

$$E : Y^2 = X(X - (abc)a^p)(X - (abc)b^p) = X^3 - (abc)c^pX^2 + (abc)^2(ab)^pX$$

est aussi de rang ≥ 1 .

Il est aisé d'exhiber d'autres familles de courbes elliptiques de rang ≥ 1 .

Proposition 2.5. Soient f, g, h des entiers non nuls de $\mathbf{Z}$ tels que ou bien $f \nmid g^2h^2$, ou bien $g \nmid f^2h^2$, ou bien $h \nmid f^2g^2$. Alors les courbes elliptiques suivantes sont toutes de rang ≥ 1 :

- (i) $E : Y^2 = X(X - f^2 + g^2)(X - f^2 + h^2)$ où $f \notin \{g, -g, h, -h\}$ et $g \notin \{h, -h\}$;
- (ii) $E : Y^2 = X(X - f^2 - g^2)(X - f^2 - h^2)$ où $g \notin \{h, -h\}$;
- (iii) $E : Y^2 = X(X + f^2 + g^2)(X + f^2 - h^2)$ où $f \notin \{h, -h\}$.

Démonstration. (i) Ici $\Delta = 16(f^2 - g^2)^2(f^2 - h^2)^2(g^2 - h^2)^2 \neq 0$. Le point $P = (f^2, fgh) \in E$ et

$$x(2P) = \left(\frac{f^2g^2 + f^2h^2 - g^2h^2}{2fgh} \right)^2 \notin \mathbf{Z}.$$

- (ii) Cette fois, $\Delta = 16(f^2 + g^2)^2(f^2 + h^2)^2(g^2 - h^2)^2 \neq 0$, $P = (f^2, fgh) \in E$ et

$$x(2P) = \left(\frac{f^2g^2 + f^2h^2 + g^2h^2}{2fgh} \right)^2 \notin \mathbf{Z}.$$

- (iii) Enfin $\Delta = 16(f^2 + g^2)^2(f^2 - h^2)^2(g^2 + h^2)^2 \neq 0$, $P = (-f^2, fgh) \in E$ et

$$x(2P) = \left(\frac{f^2g^2 - f^2h^2 - g^2h^2}{2fgh} \right)^2 \notin \mathbf{Z}. \quad \square$$

Proposition 2.6. Soient f, g, h des entiers non nuls de $\mathbf{Z}$ tels que ou bien $g \nmid h^2$, ou bien $h \nmid fg^2$. Alors les courbes elliptiques suivantes sont de rang ≥ 1 :

- (i) $E : Y^2 = X(X - f + fg^2)(X - f + h^2)$ où $g \neq \mp 1$, $f \neq h^2$ et $h^2 \neq fg^2$;
- (ii) $E : Y^2 = X(X + f + fg^2)(X + f - h^2)$ où $f \neq h^2$.

Démonstration. (i) Ici $\Delta = 16f^2(1 - g^2)^2(f - h^2)^2(fg^2 - h^2)^2 \neq 0$, $P = (f, fgh) \in E$ et

$$x(2P) = \left(\frac{h^2 + fg^2 - g^2h^2}{2gh} \right)^2 \notin \mathbf{Z}.$$

- (ii) Cette fois, $\Delta = 16f^2(1 + g^2)^2(f - h^2)^2(fg^2 + h^2)^2 \neq 0$, $P = (-f, fgh) \in E$ et

$$x(2P) = \left(\frac{h^2 - fg^2 + g^2h^2}{2gh} \right)^2 \notin \mathbf{Z}. \quad \square$$

Proposition 2.7. Soient t, c, A des entiers de $\mathbf{Z}$ tels que $A \neq 0$, $2A \nmid (t + 3c^2)$ (de sorte que $(t, c) \neq (0, 0)$) et $\Delta = -16(4t^3 + 27(-c^3 - tc + A^2)^2) \neq 0$. Alors la courbe elliptique $E : Y^2 = X^3 + tX + (A^2 - c^3 - ct)$ de discriminant Δ est de rang ≥ 1 .

Démonstration. Ici $P = (c, A) \in E$ et

$$x(2P) = \left(\frac{t + 3c^2}{2A} \right)^2 - 2c \notin \mathbf{Z}. \quad \square$$

Proposition 2.8. Soit $c \in \{1, -1\}$ et soit f un entier > 1 . Alors la courbe elliptique $E : Y^2 = X^3 + c(f^2 - c)X$ est de rang ≥ 1 .

Démonstration. Ici $\Delta = -64c^3(f^2 - c)^3 \neq 0$, $P = (c, f) \in E$ et

$$x(2P) = \left(\frac{cf^2 - 2}{2f} \right)^2 \notin \mathbf{Z} . \quad \square$$

Proposition 2.9. Soient c, s, t des entiers positifs tels que $s > t$ et $s \equiv t \pmod{2}$. Alors la courbe elliptique $E : Y^2 = X^3 - c^s X^2 + c^t X$ est de rang ≥ 1 .

Démonstration. Ici $\Delta = 16c^{2t}(c^{2s} - 4c^t) \neq 0$ car $s > t$. De plus $P = (c^s, c^{(s+t)/2}) \in E$ et

$$x(2P) = \left(\frac{c^{2s} - c^t}{2c^{(s+t)/2}} \right)^2 \notin \mathbf{Z} . \quad \square$$

Proposition 2.10. Soient a, b des entiers non nuls de $\mathbf{Z}$ tels que $b \nmid 3a^4$. Alors la courbe elliptique $E : Y^2 = X^3 \pm (a^3 \pm 3ab^2)^2$ est de rang ≥ 1 .

Démonstration. Ici $\Delta = -16 \cdot 27a^4(a^2 \pm 3b^2)^2 \neq 0$. Prenons $P = (b^2 \mp a^2, b^3 \pm 3a^2b)$; alors

$$x(2P) = \left(\frac{(3b^4 \mp 6b^2a^2 + 3a^4)}{2b(b^2 \pm 3a^2)} \right)^2 - 2(b^2 \mp a^2) \notin \mathbf{Z}$$

car $b \nmid 3a^4$. $\square$

En considérant $2P$ où $P = (c, G)$, nous pourrions donner des conditions sur c et G pour que les courbes elliptiques

- (i) $E_U : Y^2 = X^3 + sX^2 + tX + U$ avec $U = G^2 - c^3 - sc^2 - tc$,
- (ii) $E_T : Y^2 = X^3 + sX^2 + tX + u$ avec $T = \frac{G^2 - u}{c} - sc - c^2$,
- (iii) $E_S : Y^2 = X^3 + SX^2 + tX + u$ avec $S = \frac{G^2 - u - tc}{c^2} - c$,
- (iv) $E : Y^2 = X^3 + sX^2 + tX + (G^2 - c^3 - sc^2 - tc)$,

soient respectivement de rang ≥ 1 , mais nous préférons laisser cet exercice au lecteur. De même aura-t-il le loisir de considérer $2P$ où $P = (c, cA)$ et de donner des conditions sur c et A pour que les courbes elliptiques

- (v) $E : Y^2 = X^3 + A^2X^2 - c^3$,
- (vi) $E : Y^2 = X^3 + cA^2X - c^3$,
- (vii) $E : Y^2 = X^3 + (A^2 - c - t - u)X^2 + tcX + c^2u$,
- (viii) $E : Y^2 = X^3 + sX^2 + (cA^2 - c^2sc - u)X + tcX + cu$,

soient respectivement de rang ≥ 1 .

3. Sur la grandeur de $f_m(n)$. Avec carrément la même méthode que celle de D. Clark [Cl], nous allons démontrer le résultat suivant à propos de la fonction $f_m(N)$ définie en (1.2). En fait, cette méthode n'est pas nouvelle et est un artifice classique connu depuis longtemps des spécialistes des courbes elliptiques.

Proposition 3.1. Soient $m \geq 0$ et $N > 0$ des entiers tels que la courbe elliptique $E : Y^2 = X^3 + mX^2 + NX$ de discriminant non nul soit de rang ≥ 1 . Alors pour tout entier positif ℓ , il existe des entiers R et S non nuls tels que

$$f_{mR^2S^2}(NR^4S^4) \geq 2\ell f_m(N).$$

D'où

$$\limsup_{m,n \rightarrow \infty} f_m(n) = +\infty.$$

Démonstration. Un point entier (x, y) , qui est sur la courbe E et qui a la propriété que $x|y$ avec $x \neq 0$, donnera naissance à une factorisation de N :

$$\frac{y^2}{x^2} = x + m + \frac{N}{x}.$$

Choisissons (sur E) ℓ points rationnels que nous pouvons supposer sans perte de généralité de la forme

$$\left(\frac{t_1}{s_1^2}, \frac{r_1}{s_1^3}\right), \left(\frac{t_2}{s_2^2}, \frac{r_2}{s_2^3}\right), \dots, \left(\frac{t_\ell}{s_\ell^2}, \frac{r_\ell}{s_\ell^3}\right)$$

et qui possèdent les propriétés suivantes : ils sont tous différents deux à deux, d'abscisses non nulles, d'ordonnées non nulles et vérifient en dernier essor

$$\frac{t_i t_j}{s_i^2 s_j^2} \neq N \quad \forall i, j \in \{1, 2, \dots, \ell\}. \quad (3.1)$$

Tout cela est possible car la courbe elliptique E (dont l'existence postulée est garantie par la proposition 2.1) est de rang ≥ 1 . Posons

$$R = \prod_{i=1}^{\ell} r_i, \quad S = \prod_{i=1}^{\ell} s_i,$$

et considérons la courbe elliptique $\tilde{E} : Y^2 = X^3 + mR^2S^2X^2 + NR^4S^4X$, dont le discriminant est non nul.

Le choix des points rationnels sur la courbe E nous donne l'égalité

$$\left(\frac{r_i}{s_i^3}\right)^2 = \left(\frac{t_i}{s_i^2}\right)^3 + m \left(\frac{t_i}{s_i^2}\right)^2 + N \left(\frac{t_i}{s_i^2}\right),$$

i.e. $r_i^2 = t_i^3 + ms_i^2t_i^2 + Ns_i^4t_i$. D'où $t_i|r_i^2$ pour tout i . Il est maintenant aisé de vérifier que les ℓ points

$$(x_i, y_i) = \left(R^2 \left(\frac{S}{s_i}\right)^2 t_i, R^3 \left(\frac{S}{s_i}\right)^3 r_i\right)$$

sont des points entiers distincts de la courbe $\tilde{E}$ vérifiant la propriété de divisibilité

$$R^2 \left(\frac{S}{s_i}\right)^2 t_i \mid R^3 \left(\frac{S}{s_i}\right)^3 r_i;$$

en effet, la propriété $t_i | r_i^2$ entraîne $t_i | Rr_i$. Nous avons donc $f_{mR^2S^2}(NR^4S^4) \geq 2\ell$ aussitôt que nous voyons que $(NR^4S^4/x_i, Ns_i^4y_i/t_i^2)$ est un point de la courbe $\tilde{E}$. L'idée derrière ceci est que si le diviseur x_i de NR^4S^4 fait notre affaire (en générant l'abscisse d'un point de $\tilde{E}$), alors NR^4S^4/x_i fait aussi notre bonheur (en générant l'abscisse d'un autre point de $\tilde{E}$). Il faut donc nous assurer que pour tout $i, j \in \{1, \dots, \ell\}$ nous avons $NR^4S^4/x_j \neq x_i$. C'est heureusement le cas à cause de l'hypothèse (3.1). $\square$

En posant $m = 0$, nous déduisons le résultat de D. Clark [Cl] :

$$f_0(NR^4S^4) > 2\ell f_0(N) \quad \text{et} \quad \limsup_{n \rightarrow \infty} f_0(n) = +\infty.$$

4. Sur l'ordre moyen de $\tilde{f}_m(n)$. Au cours de cette section, supposons que $M \geq 0$. Pour $n > 0$, définissons maintenant la fonction arithmétique

$$\tilde{f}_M(n) := \# \left\{ i \in \mathbf{N} : i | n \text{ et } i + M + \frac{n}{i} = c_{ni}^2 \text{ pour un } c_{ni} \in \mathbf{N} \right\}.$$

Elle est apparentée à $f_M(n)$: au lieu de $i \in \mathbf{Z}$, on prend $i \in \mathbf{N}$. Nous nous proposons de déterminer l'ordre moyen de $\tilde{f}_M(n)$, i.e. le comportement asymptotique de $\sum_{1 \leq n \leq T} \tilde{f}_M(n)$. Ici T est un entier suffisamment grand et, retenons-le bien, $1 \leq n \leq T$.

Après avoir multiplié par i chaque membre de l'égalité $i + M + \frac{n}{i} = c_{ni}^2$, nous trouvons que

$$1 \leq n = -i^2 - Mi + c_{ni}^2 i \leq T.$$

D'où

$$i^2 + (c_{ni}^2 - M)i + T \geq 0 \quad \text{avec} \quad c_{ni}^2 - M > 0.$$

Remarquons que le polynôme quadratique $Z^2 - (c_{ni}^2 - M)Z + T$ est égal au produit de polynômes linéaires

$$\left(Z - \frac{1}{2} \left(c_{ni}^2 - M - \sqrt{(c_{ni}^2 - M)^2 - 4T} \right) \right) \left(Z - \frac{1}{2} \left(c_{ni}^2 - M + \sqrt{(c_{ni}^2 - M)^2 - 4T} \right) \right).$$

Nous utiliserons dans les lignes qui suivent la fonction $[x]$ définie, rappelons-le, comme le plus grand entier contenu dans x : $[x] \leq x < [x] + 1$.

Lemme 4.1. *Soit $M \geq 0$ et soit T suffisamment grand. Alors*

$$\begin{aligned} \sum_{1 \leq n \leq T} \tilde{f}_m(n) &= \sum_{\sqrt{M+2} \leq c \leq \sqrt{M+2\sqrt{T}}} (c^2 - 1 - M) \\ &\quad + 2 \left(\sum_{\sqrt{M+2\sqrt{T}} < c \leq \sqrt{M+1+T}} \left\lceil \frac{c^2 - M - \sqrt{(c^2 - M)^2 - 4T}}{2} \right\rceil \right). \end{aligned}$$

Démonstration. Nous voulons transformer la somme de gauche ordonnée selon l'ordre croissant de n en une somme ordonnée selon l'ordre croissant de c , où c sera tel que $i + M + \frac{n}{i} = c^2_{ni} = c^2$. Nous savons donc que $\sqrt{M+2} \leq c \leq \sqrt{M+1+T}$. La question maintenant est de savoir combien pour un c fixe donné il y a de couples (i, n) tels que $1 \leq n \leq T$, $i|n$ et $i + M + \frac{n}{i} = c^2$.

Par exemple, supposons que $M+2$ n'est pas un carré parfait. Les premières valeurs admissibles de l'entier c qui apparaît dans l'identité $i + M + \frac{n}{i} = c^2$, et des entiers i et n correspondants, sont les suivantes:

$$(i) \ c = \left[\sqrt{M} \right] + 1, \quad (i, n) = \left(j, j \left(\left[\sqrt{M} + 1 \right]^2 - M - j \right) \right) \\ \text{pour } j = 1, 2, \dots, \left[\sqrt{M} + 1 \right]^2 - M - 1;$$

$$(ii) \ c = \left[\sqrt{M} \right] + 2, \quad (i, n) = \left(j, j \left(\left[\sqrt{M} + 2 \right]^2 - M - j \right) \right) \\ \text{pour } j = 1, 2, \dots, \left[\sqrt{M} + 2 \right]^2 - M - 1;$$

$$(iii) \ c = \left[\sqrt{M} \right] + 3, \quad (i, n) = \left(j, j \left(\left[\sqrt{M} + 3 \right]^2 - M - j \right) \right) \\ \text{pour } j = 1, 2, \dots, \left[\sqrt{M} + 3 \right]^2 - M - 1 \dots$$

Et la liste des c se poursuit tant et aussi longtemps que $n \leq T$, i.e. tant que

$$i^2 - (c^2 - M)i + T \geq 0.$$

Nous sommes donc amenés à considérer les deux possibilités suivantes :

(A) $(c^2 - M)^2 - 4T \leq 0$, i.e. $c \leq \sqrt{M+2\sqrt{T}}$, de sorte que

$$\sqrt{M+2} \leq c \leq \sqrt{M+2\sqrt{T}}.$$

(B) $(c^2 - M)^2 - 4T > 0$, $i \leq c^2 - M - \sqrt{(c^2 - M)^2 - 4T}$ et $i \geq c^2 - M + \sqrt{(c^2 - M)^2 - 4T}$; nous pouvons ignorer les derniers i , car $i \geq c^2 - M + \sqrt{(c^2 - M)^2 - 4T}$ entraîne $i > c^2 - M = i + \frac{n}{i}$, une contradiction; de plus, $(c^2 - M)^2 - 4T > 0$ est équivalent à $c > \sqrt{M+2\sqrt{T}}$, de sorte que

$$\sqrt{M+2\sqrt{T}} < c \leq \sqrt{M+1+T}.$$

Nous pouvons alors déduire que

$$\begin{aligned}
& \sum_{1 \leq n \leq T} \tilde{f}_m(n) \\
&= \sum_{\sqrt{M+2} \leq c \leq \sqrt{M+2\sqrt{T}}} \# \left\{ i \in \mathbf{N} : \exists n \text{ vérifiant } 1 \leq i \leq n \leq T, i|n \text{ et } i + M + \frac{n}{i} = c^2 \right\} \\
&\quad + \sum_{\sqrt{M+2\sqrt{T}} < c \leq \sqrt{M+1+T}} \# \left\{ i \in \mathbf{N} : \exists n \text{ vérifiant } 1 \leq i \leq n \leq T, i|n \text{ et } i + M + \frac{n}{i} = c^2 \right\} \\
&= \sum_{\sqrt{M+2} \leq c \leq \sqrt{M+2\sqrt{T}}} (c^2 - 1 - M) \\
&\quad + \sum_{\sqrt{M+2\sqrt{T}} < c \leq \sqrt{M+1+T}} \left(2 \left(\sum_{1 \leq i \leq \left[\frac{1}{2}(c^2 - M - \sqrt{(c^2 - M)^2 - 4T}) \right]} 1 \right) \right). \quad \square
\end{aligned}$$

Nous utiliserons le lemme technique suivant, dans l'énoncé duquel, par souci de généralité, nous supposons $M \in \mathbf{Z}$.

Lemme 4.2. Soit $M \in \mathbf{Z}$. Soit $x \geq 0$ tel que $M + 2\sqrt{x} \geq 0$ et soit

$$\sqrt{M + 2\sqrt{x}} \leq z \leq \sqrt{M + 1 + x}. \quad (4.1)$$

Alors

$$\frac{2x}{z^2 - M} + \frac{2x^2}{(z^2 - M)^3} \leq z^2 - M - \sqrt{(z^2 - M)^2 - 4x} \leq \frac{2x}{z^2 - M} + \frac{8x^2}{(z^2 - M)^3}.$$

Démonstration. Remarquons d'abord que l'hypothèse (4.1) est équivalente à

$$2\sqrt{x} \leq z^2 - M \leq x + 1. \quad (4.2)$$

De plus, les deux inégalités convoitées sont équivalentes à

$$\begin{aligned}
z^2 - M - \frac{2x}{z^2 - M} - \frac{2x^2}{(z^2 - M)^3} &\geq \sqrt{(z^2 - M)^2 - 4x} \\
&\geq z^2 - M - \frac{2x}{z^2 - M} - \frac{8x^2}{(z^2 - M)^3}.
\end{aligned} \quad (4.3)$$

Le membre de droite de (4.3) est positif ou nul, car d'après (4.2),

$$\frac{2x}{z^2 - M} + \frac{8x^2}{(z^2 - M)^3} \leq \frac{2x}{2\sqrt{x}} + \frac{8x^2}{8x^{3/2}} = 2\sqrt{x} \leq z^2 - M.$$

Le membre de gauche de (4.3) est donc *a fortiori* positif ou nul.

(i) Après avoir élevé au carré chaque membre de la première inégalité de (4.3), il nous faut vérifier l'inégalité suivante

$$(z^2 - M)^2 + \frac{4x^2}{(z^2 - M)^2} + \frac{4x^4}{(z^2 - M)^6} - 4x - \frac{4x^2}{(z^2 - M)^2} + \frac{8x^3}{(z^2 - M)^4} \geq (z^2 - M)^2 - 4x,$$

que personne n'osera contester.

(ii) Après avoir élevé au carré chaque membre de la seconde inégalité de (4.3), demandons-nous s'il est vrai que

$$(z^2 - M)^2 + \frac{4x^2}{(z^2 - M)^2} + \frac{64x^4}{(z^2 - M)^6} - 4x - \frac{16x^2}{(z^2 - M)^2} + \frac{32x^3}{(z^2 - M)^4} \leq (z^2 - M)^2 - 4x,$$

i.e. s'il est vrai que

$$\frac{8x}{(z^2 - M)^2} + \frac{16x^2}{(z^2 - M)^4} \leq 3.$$

Eh oui! c'est vraiment le cas, car d'après (4.2), $(z^2 - M)^2 \geq 4x$, de sorte que

$$\frac{8x}{(z^2 - M)^2} + \frac{16x^2}{(z^2 - M)^4} \leq \frac{8x}{4x} + \frac{16x^2}{16x^2} = 3. \quad \square$$

Avant de passer à la proposition suivante, rappelons que $F(t) \ll G(t)$ veut dire qu'il existe une constante positive c et un nombre réel positif t_0 tels que $F(t) \leq cG(t)$, pour $t \geq t_0$. Rappelons aussi la formule

$$\sum_{1 \leq j \leq J} j^2 = \frac{1}{3}J^3 + \frac{1}{2}J^2 + \frac{1}{6}J.$$

De plus, posons

$$H(c) := \left[\frac{1}{2} \left(c^2 - M - \sqrt{(c^2 - M)^2 - 4T} \right) \right].$$

Proposition 4.3. Soit M un entier ≥ 0 et soit T suffisamment grand. Alors

$$T^{3/4} \ll \sum_{1 \leq n \leq T} \tilde{f}_m(n) \ll T^{3/4}.$$

Démonstration. Soit $e = 1$ (resp. $e = 0$) si $M + 2$ est (resp. n'est pas) un carré parfait. Utilisons le lemme 4.1, en nous rappelant préalablement comment approximer une somme par une intégrale. Il existe donc θ avec $0 \leq \theta \leq 1$ tel que

$$\begin{aligned} \sum_{1 \leq n \leq T} \tilde{f}_m(n) &= \frac{1}{3} \left[\sqrt{M + 2\sqrt{T}} \right]^3 + \frac{1}{2} \left[\sqrt{M + 2\sqrt{T}} \right]^2 + \frac{1}{6} \left[\sqrt{M + 2\sqrt{T}} \right] \\ &\quad - \frac{1}{3} \left(\left[\sqrt{M + 2} \right] - e \right)^3 - \frac{1}{2} \left(\left[\sqrt{M + 2} \right] - e \right)^2 - \frac{1}{6} \left(\left[\sqrt{M + 2} \right] - e \right) \\ &\quad - (M + 1) \left(\left[\sqrt{M + 2\sqrt{T}} \right] - \left[\sqrt{M + 2 - e} \right] \right) \\ &\quad + \theta \left(H \left(\left[\sqrt{M + 1 + T} \right] \right) - H \left(\left[\sqrt{M + 2\sqrt{T}} \right] \right) \right) + 2 \int_{\left[\sqrt{M + 2\sqrt{T}} \right]}^{\left[\sqrt{M + 1 + T} \right]} H(c) dc. \end{aligned}$$

Donc nous obtenons, grâce au lemme 4.2,

$$\begin{aligned} \sum_{1 \leq n \leq T} \tilde{f}_m(n) &\ll T^{3/4} + \int_{\left[\sqrt{M+2\sqrt{T}}\right]}^{\left[\sqrt{M+1+T}\right]} \left(c^2 - M - \sqrt{(c^2 - M)^2 - 4T} \right) dc \\ &\ll T^{3/4} + \int_{\left[\sqrt{M+2\sqrt{T}}\right]}^{\left[\sqrt{M+1+T}\right]} \left(\frac{2T}{c^2 - M} + \frac{8T^2}{(c^2 - M)^3} \right) dc. \end{aligned}$$

Or pour T suffisamment grand, $c^2 > M + 2\sqrt{T} > 2M$, de sorte que $M < c^2/2$; donc $c^2 - M > c^2/2$; d'où $2T/(c^2 - M) < 4T/c^2$ et $8T^2/(c^2 - M)^3 < 64T^2/c^6$. Donc

$$\sum_{1 \leq n \leq T} \tilde{f}_m(n) \ll T^{3/4} + \int_{\left[\sqrt{M+2\sqrt{T}}\right]}^{\left[\sqrt{M+1+T}\right]} \left(\frac{4T}{c^2} + \frac{64T^2}{c^6} \right) dc \ll T^{3/4}.$$

Enfin

$$\sum_{1 \leq n \leq T} \tilde{f}_m(n) > \sum_{\sqrt{M+2} \leq c \leq \sqrt{M+2\sqrt{T}}} (c^2 - 1 - M) \gg T^{3/4}. \quad \square$$

En prenant $m = 0$ dans la proposition précédente, nous obtenons le résultat de D. Clark [Cl] :

$$x^{3/4} \ll \sum_{1 \leq n \leq x} \tilde{f}_0(n) = \sum_{1 \leq n \leq x} f(n) \ll x^{3/4}.$$

Cependant sa preuve (cf. page 183 de [Cl]) est malheureusement fausse, comme on peut d'ailleurs s'en convaincre facilement au moyen d'exemples numériques.

Remerciements. Une partie de cet article fut écrite pendant un congé sabbatique au CRM de l'Université de Montréal; je remercie Francis Clark, alors directeur du CRM, pour le soutien obtenu. C'est Pierre Lacombe (étudiant) qui a programmé la courbe elliptique qui apparaît dans cet article. Enfin, il me faut bien l'avouer, j'ai bénéficié de subventions FCAR (Québec) et CRSNG (Canada).

English extended abstract. A few infinite families of elliptic curves over $\mathbf{Q}$ of rank ≥ 1 are exhibited. For each elliptic curve E under consideration, we exhibit a rational point P on E to conclude from the Lutz-Nagell theorem that $2P = (x_2, y_2)$ is not a torsion point: in each case, it turns out that x_2 is not an integer. The elliptic curves exhibited are the following ones:

- (i) $E : Y^2 = X^3 + mX^2 + NX$ where $N = cB^2 - cm - c^2$, with $m, c, B \in \mathbf{Z}; cB \neq 0, B^2 \neq m + c$ and $B \nmid (m + 2c)$.
- (ii) $E : Y^2 = X^3 + MX^2 + nX$ where $M = A^2 - \frac{n}{c} - c$, with $n, c, A \in \mathbf{Z} \setminus \{0\}; c|n$ and $A \nmid \frac{n-c^2}{c}$.
- (iii) $E : Y^2 = X(X - a^2)(X - b^2)$ where $a^2 + b^2 = c^2$, with $a, b, c \in \mathbf{Z} \setminus \{0\}$ and $(a, b) = 1$.

- (iv) $E : abcY^2 = X(X - a)(X - b)$ where $a + b = c$, with $a, b, c \in \mathbf{Z} \setminus \{0\}$, $a \neq b$ and $2 \nmid (a + b + ab)$.
- (v) $E : Y^2 = X(X - f^2 + g^2)(X - f^2 + h^2)$ where $f, g, h \in \mathbf{Z} \setminus \{0\}$, with either $f \nmid g^2h^2$, or $g \nmid f^2h^2$, or $h \nmid f^2g^2$, and with $f \notin \{g, -g, h, -h\}$ and $g \notin \{h, -h\}$.
- (vi) $E : Y^2 = X(X - f^2 - g^2)(X - f^2 - h^2)$ where $f, g, h \in \mathbf{Z} \setminus \{0\}$, with either $f \nmid g^2h^2$, or $g \nmid f^2h^2$, or $h \nmid f^2g^2$, and with $g \notin \{h, -h\}$.
- (vii) $E : Y^2 = X(X + f^2 + g^2)(X + f^2 - h^2)$ where $f, g, h \in \mathbf{Z} \setminus \{0\}$, with either $f \nmid g^2h^2$, or $g \nmid f^2h^2$, or $h \nmid f^2g^2$, and with $f \notin \{h, -h\}$.
- (viii) $E : Y^2 = X(X - f + fg^2)(X - f + h^2)$ where $f, g, h \in \mathbf{Z} \setminus \{0\}$, with either $g \nmid h^2$, or $h \nmid fg^2$ and with $g \neq \pm 1$, $f \neq h^2$ and $h^2 \neq fg^2$.
- (ix) $E : Y^2 = X(X + f + fg^2)(X + f - h^2)$ where $f, g, h \in \mathbf{Z} \setminus \{0\}$, with either $g \nmid h^2$, or $h \nmid fg^2$ and with $f \neq h^2$.
- (x) $E : Y^2 = X^3 + tX + (A^2 - c^3 - ct)$ where $t, c, A \in \mathbf{Z}$, with $A \neq 0$, $\Delta = -16(4t^3 + 27(-c^3 - tc + A^2)^2) \neq 0$ and $2A \nmid (t + 3c^2)$.
- (xi) $E : Y^2 = X^3 + c(f^2 - c)X$ where $c \in \{1, -1\}$, $f \in \mathbf{N}$ with $f > 1$.
- (xii) $E : Y^2 = X^3 - c^s X^2 + c^t$ where $c, s, t \in \mathbf{N} \setminus \{0\}$, with $s > t$ and $s \equiv t \pmod{2}$.
- (xiii) $E : Y^2 = X^3 \pm (a^3 \pm 3ab^2)^2$ where $a, b \in \mathbf{Z} \setminus \{0\}$, with $b \nmid 3a^4$.

Let us now fix $m \in \mathbf{Z}$; for $n \neq 0$ define the arithmetical function

$$f_m(n) := \#\{(a, b) \in \mathbf{Z} \times \mathbf{Z} : ab = n \text{ and } a + m + b \text{ is a perfect square}\}.$$

This function is related to the elliptic curve $E : Y^2 = X^3 + mX^2 + nX$, with $m, n \in \mathbf{Z}$, where the discriminant of E is $\Delta = 16n^2(m^2 - 4n) \neq 0$; the 2-descent algorithm of Tate asks for the number of integers c such that $c|n$, c is square-free and the Diophantine equation $cS^4 + mS^2T^2 + \frac{n}{c}T^4 = U^2$ is solvable. Using an idea of D. Clark (this is in fact a classical idea), we prove the following result.

Proposition 3.1. *Let $m \geq 0$ and $N > 0$ be integers such that the elliptic curve $E : Y^2 = X^3 + mX^2 + NX$ of discriminant $\neq 0$ be of rank ≥ 1 . Then for every $\ell \geq 1$, there exist R and S different from 0 such that*

$$f_{mR^2S^2}(NR^4S^4) \geq 2\ell f_m(N).$$

Finally, for $M \geq 0$ and $n \geq 0$ we define the arithmetical function

$$\tilde{f}_M(n) := \#\left\{i \in \mathbf{N} : i|n \text{ and } i + M + \frac{n}{i} = c_{ni}^2 \text{ for some } c_{ni} \in \mathbf{N}\right\}.$$

Then we prove the following proposition.

Proposition 4.3. *Let $M \geq 0$ and let T be a sufficiently large integer. Then*

$$T^{3/4} \ll \sum_{1 \leq n \leq N} \tilde{f}_M(n) \ll T^{3/4}.$$

BIBLIOGRAPHIE

- [Cas] J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, Cambridge, 1991.
- [Cl] D. Clark, *An Arithmetical Function Associated with the Rank of Elliptic Curves*, *Canad. Math. Bull.* **34** (1991), 181–185.
- [Co] J. Coates, *Elliptic Curves and Iwasawa Theory*, *Modular Forms* (R. Rankin, ed.), Halsted Press, New York, 1984, pp. 51–73.
- [H] D. Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 1987.
- [Kn] A. W. Knap, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.
- [Ko] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.
- [Kr] T. J. Kretschmer, *Construction of Elliptic Curves with Large Rank*, *Math. of Comp.* **46** (1986), 627–635.
- [Mor] L. J. Mordell, *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees*, *Proc. Camb. Phil. Soc.* **21** (1922), 179–192.
- [Mur] M. R. Murty, *Elliptic Curves and Modular Forms*, *Canad. Math. Bull.* **34** (1991), 375–384.
- [M-M] M. R. Murty et V. K. Murty, *Lectures on Elliptic Curves* (Notes non publiées).
- [Pe-Po1] D. E. Penney et C. Pomerance, *A Search for Elliptic Curves with Large Rank*, *Math. of Comp.* **28** (1974), 851–853.
- [Pe-Po2] D. E. Penney et C. Pomerance, *Three Elliptic Curves with Rank at Least Seven*, *Math. of Comp.* **29** (1975), 965–967.
- [S] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
- [Ta] J. Tate, *Rational Points on Elliptic Curves*, *Philips Lectures*, Haverford College, 1961 (Notes non publiées).

C. LÉVESQUE

CICMA

DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUE

UNIVERSITÉ LAVAL

QUÉBEC QC G1K 7P4

CANADA