TORDUES QUADRATIQUES DE COURBES ELLIPTIQUES ET POINTS RATIONNELS SUR LES SURFACES DE CHÂTELET

MASATO KUWATA

Soit E la courbe elliptique sur $\mathbf{Q}$ donnée par l'équation

$$y^2 = x^3 + Ax + B,$$

et soit D un nombre rationnel. La tordue quadratique de E par D est définie par

$$E^D : \quad D\,y^2 = x^3 + Ax + B. \tag{1}$$

La détermination du rang r_D du groupe de Mordell-Weil $E^D(\mathbf{Q})$, pour chaque D, est un problème très difficile. Il n'y a pas de bonne méthode générale actuellement connue pour le déterminer. Dans cette note, on considère plus généralement la tordue quadratique de E par un polynôme $D(t)$ à coefficients rationnels et on s'intéresse à la variation du rang $r_D(t)$ du groupe de Mordell-Weil $E^{D(t)}(\mathbf{Q})$. Plus précisément, on considère la densité de l'ensemble

$$R(E, D(t)) = \{t \in \mathbf{Q} \mid \operatorname{rang} E^{D(t)}(\mathbf{Q}) > 0\}.$$

La conjecture de Mazur [7] suggère que l'ensemble $R(E, D(t))$ est ou bien fini[1] ou bien dense dans $\mathbf{Q}$.

Dans [8], Rohrlich a étudié la variation de $r_D(t)$ en utilisant une méthode conjecturale. La conjecture de Birch et Swinnerton-Dyer, ou plus faiblement, la conjecture de parité, dit que l'ensemble $R(E, D(t))$ contient l'ensemble

$$S^- = \{t \in \mathbf{Q} \mid \text{le signe de l'équation fonctionnelle de } L(E^{D(t)}, s) \text{ est négatif}\}.$$

Rohrlich a alors étudié le signe de l'équation fonctionnelle par 'local root numbers'. Dans le même article il a aussi démontré le théorème suivant qui ne nécessite aucune hypothèse conjecturale.

Théorème 1 (Rohrlich [8])**.** *Soit E une courbe elliptique définie sur $\mathbf{Q}$ et soit $D(t)$ un polynôme* quadratique. *S'il existe $t_0 \in \mathbf{Q}$ tel que $D(t_0) \neq 0$ et le rang de $E^{D(t_0)}(\mathbf{Q})$ est positif, alors l'ensemble de tous les t tels que le rang de $E^{D(t)}(\mathbf{Q})$ est positif est dense dans $\mathbf{R}$.*

Quand $D(t)$ est de degré 3, un théorème similaire a été prouvé sans l'hypothèse de l'existence de t_0 (cf. [5]). Mais dans le cas de degré 2, il n'y a pas de méthode évidente pour trouver un tel t_0.

Date: 17 janvier 1994.

[1]Actuellement, il n'y a pas d'exemple connu de surface elliptique $E_t \to \mathbf{P}^1$ définie sur $\mathbf{Q}$ avec une section rationnelle telle que le groupe de Mordell-Weil $E_t(\mathbf{Q})$ est toujours fini sauf pour un nombre fini de $t \in \mathbf{Q}$. Il y a des gens qui conjecturent la non-existence de telles surfaces elliptiques.

Dans une lettre à Mazur de novembre 1992, Colliot-Thélène a indiqué qu'il pouvait éliminer l'hypothèse d'existence de t_0 dans le théorème de Rohrlich. Dans cette note on s'inspire de remarques de Colliot-Thélène, d'une part pour trouver explicitement un tel t_0 et éliminer ainsi l'hypothèse d'existence du théorème de Rohrlich, et d'autre part pour généraliser le résultat de Rohrlich.

Sans perdre de généralité, on peut supposer que $D(t)$ est de la forme $1 - at^2$, $a \neq 0$ et ainsi $E^{D(t)}$ est donnée par

$$E^{D(t)} : \quad (1 - at^2)y^2 = x^3 + Ax + B. \tag{2}$$

En posant $z = ty$, l'équation (2) devient

$$y^2 - az^2 = x^3 + Ax + B. \tag{3}$$

On appelle surface de Châtelet un modèle propre lisse d'une surface affine donnée par ce type d'équation. Maintenant, on considère le modèle projectif S de cette surface définie par l'équation cubique homogène

$$S : \quad (y^2 - az^2)w = x^3 + Axw^2 + Bw^3 \tag{4}$$

dans $\mathbf{P}^3$. D'abord, on observe que c'est une surface cubique géométriquement intègre, non conique, avec exactement deux points singuliers $(x : y : z : w) = (0 : \pm\sqrt{a} : 0 : 1)$. La surface S contient la droite $x = w = 0$ et donc contient des points rationnels.

Colliot-Thélène a indiqué qu'il y a plusieurs techniques pour voir qu'une surface cubique qui n'est pas un cône et qui a un point rationnel lisse a suffisamment de points rationnels. Désormais, on note k le corps de base de caractéristique 0; dans notre cas k sera égal à $\mathbf{Q}$. D'abord, on rappelle la définition suivante.

Définition 1. Une variété V définie sur un corps k est *unirationnelle* s'il existe une application rationnelle dominante $\mathbf{P}^m \to V$ définie sur k.

Si une variété est unirationnelle, alors l'ensemble des points rationnels est Zariski dense. Un point x d'une surface cubique V s'appelle point de *type général* si l'intersection $C(x)$ du plan tangent à V en x avec V est géométriquement irréductible. Manin [6] a donné un critère d'unirationalité.

Théorème 2 (Manin [6, Ch. II, Th. 12.11])**.** *Soit $V \subset \mathbf{P}^3$ une surface cubique qui contient un k-point x de type général. Alors V est une surface unirationnelle sur k et, en particulier, l'ensemble $V(k)$ est Zariski dense.*

Dans notre cas, malheureusement, aucun point de la droite $\ell : x = w = 0$ n'est de type général. En fait, l'intersection du plan tangent à V en un point de ℓ avec V égale 3ℓ. Il est facile de voir, au contraire, que l'hypothèse de Rohrlich nous permet d'avoir un point de type général.

Dans l'introduction de [6] Manin explique deux idées pour construire de nouveaux points à partir des points qui sont déjà connus. Dans notre cas, sa deuxième idée peut être utilisée pour avoir un point de type général. Coray et Tsfasman [4, Lemma 1.2] ont utilisé ces idées de Manin et démontré le théorème suivant.

Théorème 3 (Coray et Tsfasman [4, Lemma 1.2])**.** *Soit $V \subset \mathbf{P}^3$ une surface cubique qui contient deux points doubles et qui ne contient pas d'autres points singuliers. Alors V est une surface unirationnelle sur k.*

Cet énoncé donne l'unirationalité de la surface de Châtelet S et ainsi élimine l'hypothèse d'existence dans le théorème 1.

Il y a en fait plusieurs méthodes pour voir que la surface S est unirationnelle. Coray et Tsfasman ([4, Th. 1.3, Prop. 4.8]) ont démontré que l'on peut considérer la surface S de plusieurs façons différentes. Par exemple, S est birationnellement équivalente à une surface de Del Pezzo de degré 4 avec un point défini sur k. Alors les résultats de Manin ([6, Ch. IV, Th. 29.4 et Th. 30.1] permettent de démontrer l'unirationalité de S.

Pour écrire explicitement une application rationnelle, nous utilisons une autre méthode. On introduit une "transformation magique", ce qui permet de décomposer le torseur universel sur S comme le produit d'une conique ayant un point rationnel et de l'intersection de deux quadriques. Pour plus d'explications au sujet de la transformation magique, on peut consulter [3, II, paragraphe 7] [1, pp. 293–299] [2, pp. 437–441].

On suppose que θ est une racine du polynôme $x^3 + Ax + B$. On peut écrire $x^3 + Ax + B = N_{K/k}(x - \theta)$, où $K = k[X]/(X^3 + AX + B)$. On introduit les variables R et S et on considère le système d'équations

$$y^2 - az^2 = x^3 + Ax + B,$$
$$x - \theta = R^2 - aS^2.$$

Maintenant, on introduit les variables U_i, V_i, $i = 1, 2, 3$, et on pose

$$R = U_1 + U_2\theta + U_3\theta^2,$$
$$S = V_1 + V_2\theta + V_3\theta^2.$$

Le système d'équations ci-dessus s'écrit donc

$$y^2 - az^2 = x^3 + Ax + B, \tag{4.1}$$

$$x - \theta = (U_1 + U_2\theta + U_3\theta^2)^2 - a(V_1 + V_2\theta + V_3\theta^2)^2. \tag{4.2}$$

La seconde équation est équivalente au système

$$x = q_0(U_i, V_i),$$
$$-1 = q_1(U_i, V_i),$$
$$0 = q_2(U_i, V_i),$$

où q_0, q_1 et q_2 sont des formes quadratiques à coefficients rationnels en les variables U_i, V_i. Donc on a une variété affine W de dimension 6 définie sur k. Évidemment, il y a un morphisme dominant de W vers S donné en ignorant les variables U_i, V_i.

Maintenant, on applique au système ci-dessus une "transformation magique"; on introduit le changement de variable – qu'il faut voir comme defini sur k – donné par

$$Y + \sqrt{a}Z = (y + \sqrt{a}z)/N_{K(\sqrt{a})/k(\sqrt{a})}(R + \sqrt{a}S). \tag{6}$$

Par substitution de (4.1.2) dans (4.1.1) et en utilisant (6), on trouve que la variété W est k-birationnelle à la variété de l'espace affine, en les coordonnées (x, Y, Z, U_i, V_i), donnée par le système

$$Y^2 - aZ^2 = 1, \tag{6.1}$$

$$x - \theta = (U_1 + U_2\theta + U_3\theta^2)^2 - a(V_1 + V_2\theta + V_3\theta^2)^2. \tag{6.2}$$

En d'autres termes, la variété W s'est décomposée en le produit d'une conique possédant un point rationnel et d'une variété de l'espace affine, en les coordonnées (x, U_i, V_i), donnée par l'équation (7.2).

En développant (7.2), on obtient par identification

$$x = U_1^2 - aV_1^2 + 2B\,(aV_2V_3 - U_2U_3), \tag{7.1}$$

$$-1 = 2\,(U_1U_2 - aV_1V_2) + 2A\,(aV_2V_3 - U_2U_3) + B\,(aV_3^2 - U_3^2), \tag{7.2}$$

$$0 = 2\,(U_1U_3 - aV_1V_3) + U_2^2 - aV_2^2 + A\,(aV_3^2 - U_3^2). \tag{7.3}$$

On voit que les équations (8.2) et (8.3) ne contiennent ni de terme en U_1^2, ni de terme en V_1^2. C'est le reflet du fait que la variété projective dans $\mathbf{P}^6$ donnée par

$$\begin{aligned} -T^2 &= 2\,(U_1U_2 - aV_1V_2) + 2A\,(aV_2V_3 - U_2U_3) + B\,(aV_3^2 - U_3^2), \\ 0 &= 2\,(U_1U_3 - aV_1V_3) + U_2^2 - aV_2^2 + A\,(aV_3^2 - U_3^2) \end{aligned}$$

contient la droite $T = U_2 = V_2 = U_3 = V_3 = 0$. L'existence de cette droite permet de paramétrer l'intersection des deux quadriques (8.2) et (8.3) (cf. [3, I, Prop. 2.2]). En effet, il est facile de voir que l'on peut résoudre le système d'équations (8.2) et (8.3) d'inconnues U_1 et V_1 si et seulement si $U_2V_3 - V_2U_3$ est non nul. Dans ce cas, en remplaçant dans (8.1) U_1 et V_1 par les solutions du système (8.2) et (8.3), on obtient pour x un quotient de polynômes en U_2, U_3, V_2 et V_3. Ce quotient de polynômes est trop compliqué pour être écrit ici; nous donnerons à la fin de cette note les codes de Maple qui permettent de le calculer.

Pour l'équation (6.1.1), on a une solution $(Y, Z) = (1, 0)$ et donc on peut paramétrer les solutions par

$$\begin{aligned} Y(s) &= \frac{1 + as^2}{1 - as^2}, \\ Z(s) &= \frac{2s}{1 - as^2}. \end{aligned}$$

En utilisant (6), on obtient pour y et z des quotients de polynômes en U_i, V_i et s. On remplace à nouveau U_1 et V_1 par les solutions du système (8.2) et (8.3) et on obtient des quotients de polynômes en U_2, U_3, V_2 et V_3, qui sont aussi très compliqués.

Pour avoir une application rationnelle dominante $\mathbf{P}^2 \to S$, il suffit de spécialiser les valeurs de U_2, U_3, V_2 et V_3. En posant $U_2 = 0$, $U_3 = 1$, $V_2 = v$ et $V_3 = 0$, où v est un paramètre, on obtient

$$\begin{aligned} U_1 &= \frac{1}{2}(A + av^2), \\ V_1 &= -\frac{1}{2av}(B - 1). \end{aligned}$$

On a donc

$$x(v) = \frac{1}{4\,av^2}\Big(av^2\,(A+av^2)^2 - (B-1)^2\Big)$$

et la norme $N_{K(\sqrt{a})/k(\sqrt{q})}(R+\sqrt{a}S)$ s'écrit sous la forme $R_0(v)+\sqrt{a}S_0(v)$ où

$$R_0(v) = \frac{1}{8\,av^2}\Big(av^2\,(A+av^2)^3 - (A+av^2)(B-1)^2 + 4av^2\,(B+1)\Big),$$
$$S_0(v) = \frac{1}{8\,a^2v^3}\Big(4a^2v^4\,(A+av^2) + av^2\,(A+av^2)^2(B-1) - (B-1)^3\Big).$$

Donc on peut définir une application $(v,s)\mapsto(x(v,s),y(v,s),z(v,s))\in S$ par

$$\begin{aligned} x(v,s) &= x(v),\\ y(v,s) &= R_0(v)Y(s) + aS_0(v)Z(s),\\ z(v,s) &= R_0(v)Z(s) + S_0(v)Y(s). \end{aligned}$$

Il est facile de voir que cette application est dominante et on a ainsi démontré l'unirationalité de S explicitement.

En utilisant l'application ci-dessus, on peut simplifier la démonstration du théorème 1.

Démonstration. Démonstration du théorème 1 En posant $t(v) = z(v,0)/y(v,0)$, on obtient pour chaque v un point $P(v) = (x(v), y(v,0))$ dans le groupe $E^{D(t(v))}(\mathbf{Q})$. En utilisant un lemme de Rohrlich [8, §8, p. 147], on voit que les points $P(v)$ sont tous d'ordre infini sauf un nombre fini d'entre eux. Puisque $t(v)$ est le quotient d'un polynôme de degré 6 par un polynôme de degré 9, l'application de $\mathbf{R}$ vers $\mathbf{R}$ définie par $v\mapsto t(v)$ est surjective sur $\mathbf{R}$ et ainsi l'ensemble $\{t(v)\mid v\in\mathbf{Q}\}$ est dense dans $\mathbf{R}$. Cela termine la démonstration. □

Après avoir construit une application rationnelle $\mathbf{P}^2\to S$, on peut démontrer de manière élémentaire la conjecture de Mazur [7, Conjecture 1] pour la surface de Châtelet définie par (4).

Théorème 4. *L'ensemble des points rationnels $S(\mathbf{Q})$ de la surface de Châtelet* (4) *est toujours non vide et sa clôture est ouverte dans l'ensemble des points réels $S(\mathbf{R})$.*

En utilisant l'application rationnelle obtenue ci-dessus, on voit que la surface S a suffisamment de points rationnels. Pour la démonstration du théorème, il faut 'propager' les points rationnels partout sur la surface S. Il y a en fait plusieurs méthodes pour le faire.

Méthode 1. Soit C_{x_0} la conique obtenue par la spécialisation $x = x_0$ dans (4). S'il y a un point défini sur k dans C_{x_0}, on peut paramétrer C_{x_0} sur k et donc l'ensemble des points rationnels est dense dans l'ensemble des points réels.

Méthode 2. Soit E_{z_0} la courbe elliptique obtenue par la spécialisation $z = z_0$. S'il y a un point d'ordre infini défini sur k dans E_{z_0}, on peut multiplier ce point et donc l'ensemble des points rationnels est dense au moins dans la composante connexe de l'ensemble des points réels qui contient O.

Méthode 3. Soit V un ensemble ouvert dans $S(\mathbf{R})$ et soit P un point dans $S(\mathbf{R})$. Un point $Q\in S(\mathbf{R})$ est dans l'ensemble *V-opposé de P* si

(1) $P \neq Q$ et la droite $PQ \subset \mathbf{P}^3$ n'est ni contenue dans $S(\mathbf{P})$, ni tangente à $S(\mathbf{R})$.
(2) Le troisième point d'intersection de la droite PQ avec $S(\mathbf{R})$ est dans V.

Si P et Q sont deux points rationnels distincts dans S, le troisième point d'intersection avec S est aussi rationnel. Donc, si P est un point rationnel, un point rationnel de V donne un point rationnel de $V(P)$.

Swinnerton-Dyer a utilisé la méthode 3 pour démontrer le théorème ci-dessus pour les surfaces cubiques *lisses* (cf. [7, §4, Therorm]). Cette preuve est directement généralisable pour la surface S. La démonstration suivante utilise les trois méthodes ci-dessus.

Démonstration. Démonstration du théorème 4 *Cas 1.* $A \geq 0$. Dans ce cas, la courbe elliptique E_z a toujours une seule composante connexe. La surjectivité de l'application $v \mapsto z(v, 0)$ et l'utilisation de la méthode 2 permettent de démontrer le théorème.

Cas 2. $A < 0$, $a > 0$. Dans ce cas, l'application $v \mapsto x(v)$ est surjective. On peut donc utiliser la méthode 1 et démontrer que $S(\mathbf{Q})$ est dense dans $S(\mathbf{R})$.

Cas 3. $A < 0$, $a < 0$. Dans ce cas, $S(\mathbf{R})$ a deux composantes connexes. Celle qui contient la droite $x = w = 0$ est notée Ω_0, et l'autre est notée Ω_1. L'ensemble des points rationnels est dense dans Ω_0 pour la même raison que dans le cas 1. Soit $P = (x_0 : y_0 : z_0 : w_0)$ un point rationnel dans Ω_1 et soit π le plan tangent à S en P. Alors l'ensemble $\Omega_0(P)$ est égal à $\Omega_1 \setminus \{P\}$. Donc l'ensemble des points rationnels est aussi dense dans Ω_1. □

Remarque 1. Colliot-Thélène m'a indiqué que la théorie des torseurs universels donne cet énoncé pour les modèles projectifs lisses de S ([3, II, Theorem 8.7]). La preuve consiste en une combinaison des principes généraux de [2, Prop. 3.8.10] et de [3, II, Theorem 8.1].

Remarque 2. Dans le cas 3, il est possible qu'il n'y ait pas de points rationnels dans Ω_2. Un exemple de telle surface est donnée par

$$y^2 + z^2 = (4x - 7)(x^2 - 2).$$

Voir [9].

Voici les codes de Maple:

```
R:=proc(r) U1+U2*r+U3*r^2 end;
S:=proc(r) V1+V2*r+V3*r^2 end;

# calcul de la norme $N_{K({\sqrt a})/k({\sqrt a})}$.

N0:=(R(r1)+sqa*S(r1))*(R(r2)+sqa*S(r2))*(R(-r1-r2)+sqa*S(-r1-r2)):
N:=collect(simplify(expand(N0),{sqa^2=a}),sqa):
ReN:=collect(coeff(N,sqa,0),{U1,V1},'distributed'):
ImN:=collect(coeff(N,sqa),{U1,V1},'distributed'):
relations:={r1^2+r1*r2+r2^2=-A,r1*r2*(r1+r2)=B}:
ReN:=map(factor,
        collect(simplify(ReN,relations),{U1,V1},'distributed')):
```

```
ImN:=map(factor,
         collect(simplify(ImN,relations),{U1,V1},'distributed')):

# calcul des \'{e}quations pour x.

eq:=collect(simplify(expand(R(r)^2-a*S(r)^2),{r^3=-A*r-B}),r):
q0:=coeff(eq,r,0):
q1:=coeff(eq,r):
q2:=coeff(eq,r,2):
solution:=solve({q1+1,q2},{U1,V1}):
x:=simplify(subs(solution,q0)):

# param\'{e}trisation de  Y  et  Z.

Y_s:=(1+a*s^2)/(1-a*s^2):
Z_s:=2*s/(1-a*s^2):

# specialise U2=0, U3=1, V2=v, V3=0.

x_v:=subs({U2=0,U3=1,V2=v,V3=0},x);
R0_v:=simplify(subs({U2=0,U3=1,V2=v,V3=0}, subs(solution, ReN)));
S0_v:=simplify(subs({U2=0,U3=1,V2=v,V3=0},
subs(solution, ImN)));
y_vs:=R0_v*Y_s+a*Z_s*S0_v;
z_vs:=R0_v*Z_s+S0_v*Y_s;
t_v:=simplify(S0v/R0v);

# v\'{e}rification.

simplify(y_vs^2-a*z_vs^2-x_v^3-A*x_v-B);
```

Références

1. A. Beauville, J.-L. Colliot-Thélène, J.-J. Sansuc, et H. P. F. Swinnerton-Dyer, *Variétés stablement rationnelles non rationnelles*, Ann. of Math. **121** (1985), 283–318.
2. J.-L. Colliot-Thélène et J.-J. Sansuc, *La descente sur les variétés rationnelles II*, Duke Math. J. **54** (1987), 375–492.
3. J.-L. Colliot-Thélène, J.-J. Sansuc, and H. P. F. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces I*, J. Reine Angew. Math. **373** (1987), 37–107; *II* ibid, **374** (1987), 72–168.
4. D. F. Coray and M. A. Tsfasman, *Arithmetic on singular Del Pezzo surfaces*, Proc. London Math. Soc. **57** (1988), 25–87.
5. M. Kuwata and L. Wang, *Topology of rational points on isotrivial elliptic surfaces*, Duke Intl. Math. Res. Notices (1993), 113–123.
6. Y. I. Manin, *Cubic forms*, second ed., North Holland, 1986.
7. B. Mazur, *The topology of rational points*, Journal of Exprimental Mathematics **1** (1992), 35–45.
8. D. E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. **87** (1993), 119–151.
9. H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika (1962), 54–56.

Département de Mathématiques, Université de Caen, Esplanade de la Paix, 14032 Caen Cedex, France

E-mail address: kuwata@univ-caen.fr