UNE REMARQUE SUR CERTAINES FORMES DE WEIERSTRASS

Titem Harrache

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques
175 rue du Chevaleret, 75013 Paris
France
e-mail: titem@math.jussieu.fr, titem_harrache@yahoo.fr

Nouressadat Touafek

Equipe de Théorie des Nombres
Laboratoire de Physique Théorique
Université de Jijel
Algérie
e-mail: nstouafek@yahoo.fr

Abstract. Dans cette note, on s'intéresse à la recherche d'une forme de Weierstrass de courbes de genre 1. On souligne sur des exemples l'intérêt de la méthode pour mettre en évidence les points de torsion ou d'ordre infini et pour obtenir des formes de Weierstrass tempérées.

Keywords: Forme de Weierstrass, Courbes elliptiques.

1991 Mathematics Subject Classification: 11, 14D, 14J

1. Introduction

La transformation classique exposée dans Cassels [4] et les algorithmes de van Hoeij [6] faisant passer de l'équation d'une courbe de genre 1 de bidegré $(2, 2)$ à une équation de Weierstrass utilisent un point rationnel sur un corps K. Lorsque la courbe a plusieurs points définis dans un corps, il est parfois souhaitable d'obtenir une équation de Weierstrass où les autres points apparaissent de façon évidente.

Par exemple, lorsque la courbe C de genre 1 est donnée par une équation $F(x, y) = 0$ du second degré en chaque variable dont les coefficients sont dans un corps K, les pôles ou les zéros des fonctions x et y peuvent être définis dans K. Des exemples seront donnés dans les sections 4 et 5.

Nous nous intéresserons également aux polynômes des faces des polygones de Newton de F et de l'équation de Weierstrass donnée par l'algorithme. Dans certains cas les relations entre ces polynômes sont simples et permettent de construire, si F est *tempéré*, des polynômes de Weierstrass *tempérés*.

2. L'algorithme

Rappelons que si

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

est un modèle de Weierstrass pour une courbe elliptique E, la fonction X sur E possède deux zéros et un pôle double au point à l'infini de la courbe tandis que la fonction Y possède trois zéros et un pôle triple en ce même point à l'infini. En outre $\dfrac{Y^2}{X^3} = 1$ en ce point. Lorsque la courbe de genre 1 est donnée par une équation $F(x, y)$ du second degré en chaque variable, chercher une forme de Weierstrass revient donc à trouver deux fonctions X et Y sur la courbe E, avec X (resp. Y) possédant un pôle double (resp. triple) en l'infini.

Soit $F(x, y)$ un polynôme de degré 2 en chacune des variables qui est une équation pour une courbe de genre 1 (c'est-à -dire le discriminant par rapport à l'une des variables est de degré 4 ou 3).

En ordonnant le polynôme F par rapport à y puis par rapport à x, on obtient l'écriture suivante.

$$\begin{aligned} F(x, y) &= y^2(ax^2 + bx + c) + y(a'x^2 + b'x + c') + a''x^2 + b''x + c'' \\ &= x^2(ay^2 + a'y + a'') + x(by^2 + b'y + b'') + cy^2 + c'y + c''. \end{aligned}$$

On note

$$\begin{array}{lll} M(x) = ax^2 + bx + c, & N(x) = a'x^2 + b'x + c', & R(x) = a''x^2 + b''x + c'', \\ M_1(y) = ay^2 + a'y + a'', & N_1(y) = by^2 + b'y + b'', & R_1(y) = cy^2 + c'y + c''. \end{array}$$

On pose

$$\begin{array}{lll} \tilde{M}(x) = x^2 M\left(\dfrac{1}{x}\right), & \tilde{N}(x) = x^2 N\left(\dfrac{1}{x}\right), & \tilde{R}(x) = x^2 R\left(\dfrac{1}{x}\right), \\ \tilde{M}_1(y) = y^2 M_1\left(\dfrac{1}{y}\right), & \tilde{N}_1(y) = y^2 N_1\left(\dfrac{1}{y}\right), & \tilde{R}_1(y) = y^2 R_1\left(\dfrac{1}{y}\right). \end{array}$$

I. Un des huit polynômes M, R, M_1, R_1, $\tilde{M}$, $\tilde{R}$, $\tilde{M}_1$, $\tilde{R}_1$ a un degré nul

En changeant au besoin x en y ou x en $\dfrac{1}{x}$, y en $\dfrac{1}{y}$, on peut supposer que F s'écrit:

$$F(x, y) = a''x^2 + \left(by^2 + b'y + b''\right)x + cy^2 + c'y + c'' \tag{1}$$

$$= (bx + c)\,y^2 + (b'x + c')\,y + a''x^2 + b''x + c''. \tag{2}$$

Comme la courbe est de genre 1, on a $b \neq 0$.

En considérant la forme (2) de F on voit que y a deux pôles simples, l'un pour $x = -c/b$ et l'autre noté A qui est un pôle de x; en considérant la forme (1) de F on voit que x a un pôle double en A.

Donc y a un unique pôle simple qui est un pôle double de x. Par suite, la fonction $U = y(bx + c)$ possède un pôle triple en A. Donc, en multipliant (2) par $(bx + c)$, en posant $X = -ba''x$ et $Y = ba''U$, l'équation liant X et Y

$$Y^2 + (-b'X + bc'a'')Y - X^3 + (ca'' + bb'')X^2 - ba''(cb'' + bc'')X + (ba'')^2cc'' = 0$$

est une équation de Weierstrass de la courbe.

II. Aucun des huit polynômes n'est constant mais l'un d'eux est de degré 1

On peut alors écrire

$$\begin{aligned} F(x, y) &= y^2(bx + c) + y(a'x^2 + b'x + c') + a''x^2 + b''x + c'' \\ &= x^2(a'y + a'') + x(by^2 + b'y + b'') + cy^2 + c'y + c'', \end{aligned}$$

avec $ba' \neq 0$. Dans ce cas, x et y ont chacun 2 pôles distincts; de plus x et y ont un pôle simple commun A.

La fonction $X = (bx + c)(a'y + a'')$ aura donc un pôle double en A qui est un pôle simple de y. L'équation en X et y sera par suite du type **I**.

$$\begin{aligned} G(X, y) &= (b^2X + c^2a'^2 - bb'ca' + c'b^2a')y^2 + ... \\ &= X^2 + ... \end{aligned}$$

III. Cas général: les huit polynômes sont de degré 2

a) La courbe affine définie par $F(x, y)$ a un point $(x_0, y_0) \in K^2$.
Après une translation, on peut supposer $x_0 = y_0 = 0$ et on obtient $c'' = 0$. En posant $U = \dfrac{1}{x}$ et $V = \dfrac{1}{y}$, on obtient

$$\begin{aligned} &(c + c'U)V^2 + (b + b'U + b''U^2)V + a + a'U + a''U^2 = 0 \\ &(a'' + b''V)U^2 + (a' + b'V + c'V^2)U + a + bV + cV^2 = 0 \end{aligned}$$

et on est dans le cas **I** ou **II**.

b) Si la courbe projective d'équation affine $F(x, y) = 0$ a un point K-rationnel à l'infini, alors c'est le point double $(1, 0, 0)$ (ou $(0, 1, 0)$) et les tangentes au point $(1, 0, 0)$ (ou $(0, 1, 0)$) sont rationnelles. Il en résulte que le polynôme M a une racine $x_1 \in K$ (ou le polynôme M_1 a une racine $y_1 \in K$). Soit

$$U = \frac{1}{x - x_1} \qquad \left(\text{ou } V = \frac{1}{y - y_1}\right).$$

L'équation devient alors:

$$\begin{aligned} &y^2(a + U(2ax_1 + b)) + y(a' + U(2a'x_1 + b') + U^2(a'x_1^2 + b'x_1 + c')) \\ &+ a'' + U(2a''x_1 + b'') + U^2(a''x_1^2 + b''x_1 + c'') \\ &= U^2(a''x_1^2 + b''x_1 + c'' + y(a'x_1^2 + b'x_1 + c')) \\ &+ U((2ax_1 + b)y^2 + (2a'x_1 + b')y + 2a''x_1 + b'') + ay^2 + a'y + a'' \end{aligned}$$

et on est dans le cas **I** ou **II** de l'algorithme.

3. Le cas d'une cubique

Le cas d'une courbe de genre 1 définie par un polynôme de degré 3 en x et y avec un point rationnel $(x_0, y_0) \in K^2$ se ramène au calculs précédent.

Supposons que F s'écrive

$$F(x,y) = x^3 + ax^2y + bxy^2 + cy^3 + dx^2 + exy + fy^2 + gx + hy + i.$$

Après une translation, on peut supposer que $i = 0$. Comme la courbe est lisse g et h ne sont pas tous deux nuls, on peut se ramener par un changement de variables à ce que la tangente en $(0,0)$ soit la droite $y = 0$ i.e. $g = 0$.

En posant

$$x = \frac{u}{w},\ y = \frac{1}{w}$$

on obtient l'équation

$$u^3 + (a + dw)u^2 + (b + ew)u + fw + c + hw^2 = 0.$$

Si $d = 0$, on a la forme de Weierstrass, sinon en posant $w_1 = w + \dfrac{u}{d}$ on se ramème au cas **I** de l'algorithme.

4. Exemples et applications

4.1. Constructions de courbes elliptiques sur $\mathbb{Q}(t)$ avec point de 7-torsion rationnel et rang ≥ 1 sur $\mathbb{Q}(t)$. La recherche de familles de courbes elliptiques sur $\mathbb{Q}$ avec N-torsion et de rang ≥ 1 sur $\mathbb{Q}$ conduit à l'étude de la surface elliptique modulaire S_N.

Par exemple pour $N = 7$, toute courbe elliptique sur $\mathbb{Q}$ ayant un point d'ordre 7 rationnel peut être définie par l'équation suivante

$$Y^2 - (d^2 - d - 1)XY - d^2(d-1)Y = X^3 - d^2(d-1)X^2,$$

avec $d \in \mathbb{Q}$, le point $(0,0)$ est d'ordre 7.

Si on considére d comme variable alors on note S_7 la surface d'équation l'équation précédente.

Dans le cas de torsion $N = 7, 8$ et 2×6, la surface elliptique S_N est une surface $K3$ de nombre de Picard $\rho = 20$. Une possibilité pour cette recherche est de construire d'autres fibrations elliptiques de la surface S_N (voir [7], [5] et [9]).

Pour $N = 7$, on montre que la surface S_7 est birationnellement équivalente à la surface

$$-d(d-1)xy + (xy - x - y)(1 + d(xy - x - y)) = 0.$$

On sait construire des fibrations de S_7

$$S_7 \longrightarrow B \simeq \mathbb{P}^1_t$$

où B est la base de la fibration et t un générateur du corps des fonctions de B, si t est dans l'ensemble

$$\left\{\frac{d-1}{x-1}, \frac{d}{1-y}, \frac{dy-1}{x-1}, \frac{dy-1}{x}, \frac{d-1}{(x-1)(y-1)}\right\};$$

dans ce cas les fibrations construites ont des mauvaises fibres de type I_n, I_n^* et il est facile d'obtenir une équation bidegré $(2,2)$.

Nous détaillons le calcul pour $t = \dfrac{dy-1}{x}$.

On pose donc $t = \dfrac{dy-1}{x}$ et on élimine d entre les deux équations on obtient l'équation $F(x,y) = 0$ avec

$$\begin{aligned} F(x,y) &= (x-1)(tx-t+1)y^2 + (-2tx^2 + (3t-2)x + 2)y \\ &\quad - (tx+1)((t-1)x+1) \\ &= t(y^2 - 2y - t + 1)x^2 + ((-2t+1)y^2 + (3t-2)y \\ &\quad - 2t + 1)x + (t-1)y^2 + 2y - 1. \end{aligned}$$

On est dans le cas **III** de l'algorithme.

En posant $U = \dfrac{1}{x-1}$, l'équation $F(x,y) = 0$ devient $G(U,y) = 0$ avec

$$\begin{aligned} G(U,y) &= -(U+t)y^2 - (tU^2 - (t+2)U - 2t)y + ((t+1)U + t)(tU + t - 1)) \\ &= (-ty + t^2 + t)U^2 + (-y^2 + (t+2)y + 2t^2 - 1)U - t(y^2 - 2y - t + 1). \end{aligned}$$

On est alors dans le cas **II**.

Le changement de variables $X = -(U+t)(-ty + t^2 + t)$ donne l'équation $G_1(X,y) = 0$ avec

$$\begin{aligned} G_1(X,y) &= (X + t^3(t+1))y^2 - (2t^2 + t + 2)(X + t^3)y \\ &\quad + (X + t^3)(X + t^3 + 1) \\ &= X^2 + X(y^2 - (2t^2 + t + 2)y + 2t^3 + 1) \\ &\quad + t^3(-y + t + 1)(-(t+1)y + t^2 - t + 1). \end{aligned}$$

et on est dans le cas le cas **I** de l'algorithme.

On pose $Y = (X + t^3(t+1))y$ et on a l'équation $G_2(X,Y) = 0$ avec

$$\begin{aligned} G_2(X,Y) = &Y^2 - (2t^2 + t + 2)(X + t^3)Y + X^3 + (t^4 + 3t^3 + 1)X^2 \\ &+ (t+1)(2t^3 + t^2 - t + 2)t^3X + (t+1)^2(t^2 - t + 1)t^6. \end{aligned}$$

En changeant enfin X par $-X$, on aura l'équation de Weierstrass W_t

$$Y^2 + (2t^2 + t + 2)(X - t^3)Y = (X - t^3)(X - t^3 - 1)(X - t^3(t+1)).$$

Cette forme de Weierstrass permet d'obtenir le rang du groupe de Mordell-Weil de la courbe ([5]).

Tout d'abord, on a 8 points évidents sur la courbe d'équation $F(x,y)=0$:

$$A_1=(x=1,\infty) \qquad A_2=\left(\frac{t-1}{t},\infty\right)$$
$$A_1'=(1,t+1) \qquad A_2'=\left(\frac{t-1}{t},\frac{t^2-t+1}{t+1}\right)$$
$$A_3=\left(-\frac{1}{t},0\right) \qquad A_4=\left(-\frac{1}{t},\frac{1}{t+1}\right)$$
$$A_5=\left(-\frac{1}{t-1},0\right) \quad A_6=\left(-\frac{1}{t-1},\frac{t+1}{t^2-t+1}\right)$$

Le point A_1 donne le point $(X=\infty,Y=\infty)$ de W_t.

En résumé, le passage de l'équation de F à W_t est donné par les transformations

$$U=\frac{1}{x-1},X=(U+t)(-ty+t+t^2),Y=(-X+t^3(t+1))y$$

ce qui permet de calculer les coordonnées des points suivants dans le modèle W_t

$$A_1'=(X=-t(2t+1),Y=t(t+1)(t^3+t^2+2t+1)) \quad A_2'=(0,t^3(t^2-t+1))$$
$$A_3=(t^3,0) \qquad A_5=(t^3+1,0)$$
$$A_4=\left(-\frac{t^4(t+2)}{(t+1)^2},\frac{t^3(t^3+2t^2+t+1)}{(t+1)^3}\right) \qquad A_6=(-t(t^2-1),t(t+1)^2)$$

Enfin le diviseur de la fonction y étant égal à $-A_1-A_2+A_3+A_5$ il en résulte que sur W_t les points $-A_2,A_3,A_5$ sont alignés. On obtient alors

$A_2=(X=t^3+t^4,Y=-t^4(2t^2+t+2))$.

On vérifie que, sur la courbe elliptique W_t le point $A_3=(t^3,0)$ est d'ordre 2 et que c'est le seul point d'ordre 2 sur $\mathbb{C}(t)$. On vérifie à l'aide d'un logiciel que pour $t=1$ les deux points A_2' et A_5 sont d'ordre infini et indépendants.

Nous allons montrer qu'en fait le rang du groupe de Mordell-Weil de la courbe elliptique W_t sur $\mathbb{Q}(t)$ est 2.

Les fibres singulières de la fibration

$$\begin{aligned} S_7 &\longrightarrow \mathbb{P}^1 \\ (x,y,d) &\longmapsto t \end{aligned}$$

sont de type I_4^*, I_4^*, I_1,I_1,I_1,I_1. Par suite, d'après la formule [12],

$$\rho=r+2+\sum_t(m_t-1)$$

où r désigne le rang du groupe de Mordell-Weil de W_t sur $\mathbb{C}(t)$, m_t le nombre de composantes irréductibles des fibres singulières de S_7 on trouve $r=2$.

Pour déterminer le groupe de torsion on utilise le résultat suivant:

On sait que l'application de spécialisation, pour $t_0\in\mathbb{C}$

$$W_t^0(\mathbb{C}(t))_{tor}\to W_{t_0}^{ns}(\mathbb{C})$$

est injective, où $W_t^0(\mathbb{C}(t))$ est le sous-groupe de $W_t(\mathbb{C}(t))$ formé des points qui se spécialisent en des points lisses de $W_{t_0}(\mathbb{C})$ [8]. Ceci est vrai même pour les mauvaises fibres et dans ce cas $W_{t_0}^{ns}(\mathbb{C})$ est la composante connexe de zéro de la fibre du modéle de Néron de W_t.

Considérant les mauvaises fibres I_4^* et I_1 on voit que $W_t(\mathbb{C}(t))_{tor}$ est un sous groupe de $\mathbb{C} \times (\mathbb{Z})^2$ et de $\mathbb{C}^*$, ce qui implique que $W_t(\mathbb{C}(t))_{tor}$ est d'ordre 2. Il en résulte que $W_t(\mathbb{Q}(t))_{tor} = \langle A_3 \rangle$.

La forme de Weierstrass ainsi obtenue met en évidence deux points sur $\mathbb{Q}(t)$ d'ordre infini et indépendants, ce qui montre l'existence d'une infinité de courbes rationnelles sur S_7. D'autre part ajouter un point d'ordre infini sur la fibration en t définit un automorphisme d'ordre infini sur la surface S_7. On obtient ainsi le théoòreme.

Théorème 4.1. *L'ensemble des points rationnels de la surface S_7 est Zariski dense et le groupe des automorphismes de cette surface est infini, ce groupe contenant un sous groupe isomorphe à $\mathbb{Z}^2$.*

Remarque 1.

1. On peut donner explicitement ces automorphismes en utilisant les formules habituelles d'addition sur la forme de Weierstrass W_t.
2. En utilisant en plus le paragraphe 3 on peut aussi considérer le cas $t = \dfrac{d}{1-y}$.

4.2. Constructions de courbes elliptiques sur $\mathbb{Q}$ avec point de 7-torsion rationnel et rang≥ 2 sur $\mathbb{Q}$. Pour la recherche des courbes elliptiques sur $\mathbb{Q}$ avec point de 7-torsion rationnel et rang≥ 2 sur $\mathbb{Q}$, on amené à résoudre des équations diophantiennes qui se présentant sous la forme $\dfrac{A(X)}{B(X)} = \dfrac{C(Y)}{D(Y)}\ (= d)$ avec A, B, C, D des polynômes de degré ≤ 2 de $\mathbb{Q}(t)$ ou bien $A = C$ et $B = D$ deux polynômes de degré ≤ 3 sans facteurs communs. Le cas de polynômes de degré ≤ 2 a été traité dans [7]. Nous nous intéressons ici au cas $A = C$, $B = D$ polynômes de degré ≤ 3 avec $A = X^3 + pX^2 + qX + r$ et $B(X) = X\,(X-d)\,(X-e)$ (voir [5]). Nous supposerons aussi que A et B sont premiers entre eux, ce qui entraîne que leur résultant n'est pas nul.

Théorème 4.2. *Soit $A = X^3 + pX^2 + qX + r$ et $B = X\,(X-e)\,(X-d)$, avec $d\,e \neq 0$, deux polynômes premiers entre eux de $K[X]$. La courbe elliptique sur K définie par*

$$F(X,Y) = \frac{A(X)B(Y) - A(Y)B(X)}{X-Y}$$

a une équation de Weierstrass en Z et T

$$Z^2 + (edp + (e+d)\,q + 3r)\,ZT + SZ = T^3$$

où $S = rA(d)A(e)$ *est le résultant des polynômes* A *et* B. *De plus, le point* $(T = 0, Z = 0)$ *est d'ordre* 3 *et le point* $\left(T = \dfrac{d(d-e)rA(e)}{e^2}, Z = \dfrac{r^2(d-e)^3A(e)}{e^3}\right)$ *est en général d'ordre infini.*

Proof. Le changement de variables $x = 1/X$, $y = 1/Y$ nous donne

$$\begin{aligned} &r(ey-1)(dy-1)x^2-(r(d+e)y^2+(ped+q(e+d)-r)y+de-q)x+ry^2\\ &\quad-(ed-q)y+e+d+p\\ &\quad= r(ex-1)(dx-1)y^2-(r(d+e)x^2+(ped+q(e+d)-r)x+de-q)y+rx^2\\ &\quad-(ed-q)x+e+d+p. \end{aligned}$$

Puis le changement de variable $U = \dfrac{1}{ex-1}$ nous ramène au cas **II**,

$$\begin{aligned} &A(e)(dy-1)U^2+(re(e-d)y^2+(e^2(dp+q)+e(dq+r)+2rd)y-2r-qe+de^2)U\\ &\quad-r(ey-1)(dy-1)\\ &\quad= re((e-d)U-d)y^2+(dA(e)U^2+((pd+q)e^2+(qd+r)e+2rd)U+r(e+d))y\\ &\quad-A(e)U^2+(de^2-qe-2r)U-r. \end{aligned}$$

Cas $d \neq e$: Enfin le changement de variable

$$T_1 = (dy-1)(U(e-d)-d)$$

nous conduit au cas **I**. On obtient donc

$$\begin{aligned} &reT_1^2+(d^2A(e)U^2+(2re^2+pe^2d^2+dqe(e+d)-red+2rd^2)U+rd(d-e))T_1\\ &\quad+e^2A(d)U((e-d)U-d)\\ &\quad= (d^2A(e)T_1+e^2(e-d)A(d))U^2\\ &\quad+(((pd^2+qd+2r)e^2+(qd^2-rd)e+2rd^2)T_1-de^2A(d))U-rT_1(-eT_1-d(d-e)). \end{aligned}$$

On pose alors

$$Z_1 = (d^2A(e)T_1 + e^2(e-d)A(d))U.$$

Par suite, il vient

$$\begin{aligned} &-Z_1^2-(pe^2d^2+qed(d+e)+r(2d^2+2e^2-de))Z_1T_1+de^2A(d)Z_1\\ &\quad+rT_1(eT_1+d(d-e))(-d^2A(e)T_1+e^2(d-e)A(d))=0 \end{aligned}$$

Quelques changements de variables nous donnent enfin la forme de Weierstrass proposée:

$$Z_1 = -\frac{Z_2}{red^2A(e)} \qquad T_1 = -\frac{T_2}{red^2A(e)}$$

$$Z_2 = Z_3 - r(d-e)^2T_2$$

$$Z = \frac{Z_3}{(de)^3} \qquad T = \frac{T_2}{(de)^2}$$

Le modèle de Weierstrass

$$Z^2 + (edp + (e+d)\,q + 3r)\,ZT + rA(d)A(e)Z = T^3$$

est bien défini sur K. On voit également sur ce modèle que le point $(T = 0, Z = 0)$ est de 3-torsion et le point $\left(T_1 = -\dfrac{d(d-e)}{e}, Z_1 = 0\right)$ soit $\left(T = \dfrac{d(d-e)rA(e)}{e^2}, Z = \dfrac{r^2(d-e)^3A(e)}{e^3}\right)$ est K-rationnel en général d'ordre infini.

Cas $d = e$: On se trouve déjà au cas **I**. L'algorithme nous donne alors la même forme de Weierstrass que précédemment avec $e = d$. ∎

Remarque 2.

- Si $e = 0$, $d \neq 0$ (ou si $e \neq 0$, $d = 0$) le changement de variables $x = 1/X$, $y = 1/Y$ nous donne

$$\begin{aligned} &r(dy-1)x^2 + (rdy^2 + (dq-r)y - q)x - ry^2 - qy - (d+p) \\ &\quad = r(dx-1)y^2 + (rdx^2 + (dq-r)x - q)y - rx^2 - qx - (d+p) \end{aligned}$$

  c'est-à-dire le cas **II** de l'algorithme. Le changement de variables

$$\begin{aligned} T &= -r^2(dx-1)(dy-1), \\ Z &= r(dy-1)T \end{aligned}$$

  nous donne la forme de Weierstrass

$$Z^2 + (dq+3r)TZ + r^2A(d)Z = T^3.$$

- Si le polynôme A se factorise sur K, on a des points supplmentaires sur la courbe pouvant donner au plus deux points indpendants.
- Si l'on prend pour polynômes $A = X^3 + aX + b$ et $B = X(X-e)$, par un calcul analogue on peut pour certaines valeurs de b et e obtenir des points de 2-torsion sur le corps contenant les coefficients des polynômes.

5. Forme de Weierstrass tempérée

Soit $P \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$. On note

$$P(x,y) = \sum_{(n,m)\in\mathbb{Z}^2} a_{(n,m)}x^n y^m.$$

On appelle polygone de Newton Δ_P associé au polynôme P, l'enveloppe convexe de l'ensemble des points $\{(n,m) \in \mathbb{Z}^2 / a_{(n,m)} \neq 0\}$.

A une face τ du polygone de Newton on associe un polynôme P_τ d'une seule variable dont le degré est égal au nombre de points du réseau des entiers situés sur la face moins 1. On définit alors P_τ par

$$P_\tau = \sum_{k=0}^{\infty} a_{\tau(k)} t^k, \qquad \tau \in \Delta$$

où la paramétrisation de la face est définie dans le sens indirect sur Δ de façon à noter $\tau(0), \tau(1), ...,$ les points consécutifs du réseau des entiers sur Δ.

Un polynôme de deux variables est dit tempéré si les polynômes associés aux faces de son polygone de Newton n'ont pour racines que des racines de l'unité. Si P est à coefficients rationnels et définit une courbe elliptique E, le fait d'être tempéré garantit l'appartenance du symbole de Steinberg $\{x, y\}$ au second groupe de K-théorie $K_2(E)$ [10] .

Si E possède en outre un modèle de Weierstrass tempéré, cela permet de calculer le régulateur elliptique de E donc de donner une expression de $L(E, 2)$ en terme d'une combinaison linéaire de dilogarithmes elliptiques de points de la courbe elliptique.

Le régulateur elliptique permet en outre de comparer les mesures de Mahler de polynômes définissant les mêmes courbes elliptiques [11] et dans certains cas de démontrer des relations *exotiques* sur le dilogarithme elliptique [1], [13].

Nous pouvons montrer le résultat suivant.

Proposition 1. *Soit $P \in \mathbb{Z}[x, y]$ de bidegré $(2, 2)$ définissant une courbe elliptique. On suppose P tempéré et vérifiant la condition I) de l'algorithme. Alors la forme de Weierstrass donnée par l'algorithme est tempérée.*

Proof. Soit P tempéré; il s'écrit donc

$$P(x, y) = (x + \epsilon)y^2 + (b'x + c')y + \epsilon' x^2 + b''x + \epsilon''$$

avec $\epsilon = \pm 1$, $\epsilon' = \pm 1$, $\epsilon'' = \pm 1$, $c' = 0$ ou $c' = \pm 2, \pm 1$ si $\epsilon\epsilon'' = 1$, $b'' = 0$ ou $b'' = \pm 2, \pm 1$ si $\epsilon'\epsilon'' = 1$, de sorte que les polynômes des faces $t + \epsilon$, $\epsilon t^2 + c't + \epsilon''$, $\epsilon'' t^2 + b''t + \epsilon'$, $\epsilon' t + 1$ ne possèdent que des racines de l'unité.

On a donc

$$\begin{aligned} P(x, y) &= (x + \epsilon)y^2 + (b'x + c')y + \epsilon' x^2 + b''x + \epsilon'' \\ &= \epsilon' x^2 + (y^2 + b'y + b")x + \epsilon y^2 + c'y + \epsilon''. \end{aligned}$$

On pose alors $Y = (x + \epsilon)y$ et l'on obtient, au besoin en posant $x = -X$, la forme de Weierstrass à partir de l'équation

$$Y^2 + Y(b'x + c') + (\epsilon' x^2 + b''x + \epsilon'')(x + \epsilon) = 0.$$

On vérifie aisément que ce dernier polynôme est tempéré. ∎

Corollaire 5.1. *Soit P un polynôme tempéré. On suppose qu'après une transformation convenable, le polynôme obtenu soit tempéré et satisfasse le cas I) de l'algorithme. Alors P possède une forme de Weierstrass tempérée.*

On peut donner de nombreux exemples de polynômes satisfaisant la proposition ou son corollaire.

5.1. Familles de polynômes tempérés définissant des courbes elliptiques ayant une forme de Weierstrass tempérée

1) La famille

$$y^2x + y(kx + 1) + x^2$$

a la forme de Weierstrass tempérée

$$Y^2 + Y(-kX + 1) = X^3.$$

L'isomorphisme est donné par

$$x = -X, \qquad y = -Y/X.$$

Le point $P = (X = 0, Y = 0)$ image du point $(x = 0, y = 0)$ est un point de 3-torsion tel que $2P = (X = 0, Y = -1)$ soit l'image du point $(x = 0, y = \infty)$.

2) La famille

$$y^2x + y(kx + 1) + x^2 + x$$

a la forme de Weierstrass tempérée

$$Y^2 + kXY + Y = X^3 - X^2.$$

L'isomorphisme est donné par

$$x = -X, \qquad y = -Y/X.$$

Les zéros de x sont ceux de X, i.e. les points $P = (X = 0, Y = 0)$ et $P_1 = (X = 0, Y = -1)$. Les zéros de y à savoir $(x = 0, y = 0)$ et $(x = -1, y = 0)$ donnent les points $P = (X = 0, Y = 0)$ et $P_2 = (X = 1, Y = 0)$. Le pôle de y donne le point P_1. On vérifie facilement, avec PARI par exemple, que pour $k \neq 0, 1$, la courbe elliptique correspondante a un groupe de torsion trivial et un rang 1 avec P d'ordre infini.

Pour $k = 0$, le point P est d'ordre 5 (la courbe correspondante est la courbe modulaire $X_1(11)$).

Pour $k = 1$, les points P et P_1 sont d'ordre 4, le point P_2 est d'ordre 2.

3) La famille E_k, $k \neq 1$ ([13])

$$y^2x + y(x^2 + kx + 1) + x^2 + x$$

a la forme de Weierstrass tempérée

$$Y^2 - kXY + Y = X(X - 1)^2.$$

L'isomorphisme est donné par

$$x = \frac{X(X-1)}{Y-X+1}, \qquad y = \frac{-Y}{X-1}$$

et l'isomorphisme inverse par

$$X = -x(y+1) \qquad Y = y(xy+x+1).$$

En effet, les équations

$$y^2x + (x^2+kx+1)y + x(x+1) = 0$$
$$x^2(y+1) + x(y^2+ky+1) + y = 0$$

montrent que l'on est dans le cas II). La transformation $x = \dfrac{-X}{y+1}$ nous ramène au cas I) avec le modèle tempéré

$$X^2 - (y^2+ky+1)X + y^2 + y = 0$$
$$(-X+1)y^2 + (-kX+1)y + X^2 - X = 0.$$

La transformation $Y = -(X+1)y$ va alors donner le modèle de Weierstrass tempéré W_k

$$Y^2 - kXY + Y = X(X-1)^2.$$

Il résulte de l'isomorphisme précédent que les zéros (resp. pôles) de x dans E_k, à savoir $(x=0, y=0)$, $(x=0, y=\infty)$ (resp. $(x=\infty, y=-1)$, $(x=\infty, y=\infty)$) donnent les points $(X=0, Y=0)$, $(X=1, Y=k-1)$ (resp. $(2-k, 1-k)$,(0)) dans le modèle de Weierstrass W_k.

De même, les zéros (resp. pôles) de y dans E_k, à savoir $(x=0, y=0)$, $(x=-1, y=0)$ (resp. $(x=0, y=\infty)$, $(x=\infty, y=\infty)$) donnent les points $(X=0, Y=0)$, $(X=1, Y=0)$ (resp. $(1, k-1)$,(0)) dans le modèle de Weierstrass W_k.

Supposons $k \neq 2, 3$ et posons $P = (X=1, Y=0)$.

On a alors

$P = (1,0)$ $\qquad -P = (1, k-1)$

$2P = (0,-1)$ $\qquad -2P = (0,0)$

$3P = (2-k, -(k-1)(k-2))$ $\qquad -3P = (-k+2, -k+1)$

$4P = (3-k, 3-k)$ $\qquad -4P = (-k+3, -k^2+4k-4)$

$$5P = \left(\frac{1}{(k-2)^2}, \frac{k-1}{(k-2)^3}\right)$$

$$-5P = \left(\frac{1}{(k-2)^2}, -\frac{(k-1)(k-3)^2}{(k-2)^3}\right)$$

$$6P = \left(\frac{k^2-5k+7}{(k-3)^2}, \frac{(k-2)^2(k^2-5k+7)}{(k-3)^3}\right)$$

$$-6P = \left(\frac{k^2-5k+7}{(k-3)^2}, -\frac{1}{(k-3)^3}\right).$$

Donc si $k = 2$, $3P = -2P$ et le point P est un point de 5-torsion.

Et si $k = 3$, $4P = -2P$ et le point P est un point de 6-torsion.

Si $k \neq 2, 3, 1$ (cas non elliptique), le point P est d'ordre infini.

Par ailleurs, les zéros de x s'envoient par l'isomorphisme sur les points $-2P$ et $-P$; les pôles de x s'envoient sur $-3P$ et (0). Les zéros de y s'envoient par l'isomorphisme sur les points $-2P$ et P; les pôles de y s'envoient sur $-P$ et (0).

5.2. Les modèles tempérés de la courbe $21A$**.** La courbe $21A$ des tables de Cremona ayant pour modèle de Weierstrass tempéré

$$Y^2 + XY = X^3 + X$$

possède un autre modèle de Weierstrass tempéré

$$Y_1^2 + 3X_1Y_1 = X_1(X_1 - 1)^2.$$

Ce dernier modèle est obtenu avec l'algorithme précédent à partir du modèle [3] réciproque

$$y^2 + y(x^2 + 3x + 1) + x^2 = 0$$

Il existe en outre deux autres modèles réciproques de la courbe $21A$ [3], le modèle

$$(x + 1)^2y^2 + xy + (x + 1)^2 = 0$$

et le modèle

$$y^2(x + 1)^2 + y(2(x + 1)^2 - 9x) + (x + 1)^2 = 0$$

auquels s'appliquent la proposition ou le corollaire; mais on obtient dans les deux cas le modèle tempéré de Cremona.

Remerciements. Nous tenons à remercier le rapporteur pour ses remarques et commentaires constructifs qui ont permis d'améliorer la présentation de l'article. Ce travail a été réalisé pendant le(s) visite(s) du deuxième auteur à l'équipe de Théorie des Nombres de l'Institut de Mathématiques de Jussieu; il exprime sa gratitude à Mme M.J. Bertin pour son accueil chaleureux et aussi pour les fructueuses discussions sur le sujet avec d'autres membres de l'équipe.

Références

[1] Bertin, M.J., *Mesure de Mahler et régulateur elliptique: Preuve de deux relations exotiques*, CRM Proc. Lectures Notes, 36 (2004), 1-12.

[2] Bloch, S. and Grayson, D., *K_2 and L-functions of elliptic curves computer calculations*. I, Contemp. Math. 55 (1986), 79-88.

[3] Boyd, D.W., *Mahler's measure and special values of L-functions*, Experiment. Math. 7 (1998), no. 1, 37-82.

[4] Cassels, J.W.S., *Lectures on elliptic curves*, London Math. Soc. Student texts 24, Cambridge University Press, Cambridge, 1991.

[5] Harrache, T., Thèse de Doctorat, Université Paris 6 (2009).

[6] Hoeij, M. van, *An algorithm for computing the Weierstrass normal form*, International symposium on symobolic and algebraic computation 1995, 90-95.

[7] Lecacheux, O., *Rang de familles de courbes elliptiques*, Acta Arith. 109 (2003), no. 2, 131-142.

[8] Miranda, R., Persson, U., *Torsion subgroup of elliptic surfaces*, Compositio Math. 72 (1989), 249-267.

[9] Rabarison, P., Thèse de Doctorat, Université de Caen (2008).

[10] Rodriguez-Villegas, F., *Modular Mahler measures* I, Topics in Number Theory (S. D. Ahlgren, G. E. Andrews, and K. Ono, eds), Kluwer, Dordrecht, 1999, 17-48.

[11] Rodriguez-Villegas, F., *Identities between Mahler measures, Number theory for the millenium*, III (Urbana, IL, 2000), 223-229, A K Peters, Natick, MA, 2002.

[12] Shioda, T., *On the Mordell-Weil Lattices*, Commentarii Mathematici Universitatis Sancti Pauli, Vol. 39 n ° 2 (1990), 211-240.

[13] Touafek, N., Thèse de Doctorat, Université de Constantine (2008).

Accepted: 23.04.2011