Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
C. R. Acad. Sci. Paris, Ser. I 336 (2003) 117–120
COMPTES RENDUS MATHEMATIQUE

Théorie des nombres/Géométrie algébrique

Points algébriques sur certains quotients de courbes de Fermat

Algebraic points on some quotients of Fermat curves

Oumar Sall

U.F.R. de mathématiques, Université Paris 7-Denis Diderot, 175, rue de Chevaleret, 75013 Paris, France

Reçu le 10 octobre 2002 ; accepté le 19 novembre 2002

Présenté par Jean-Pierre Serre

Résumé

Nous déterminons explicitement les points algébriques de degré donné quelconque sur certains quotients de courbes de Fermat de degré 5, 7 ou 11. Cette Note complète les travaux de Gross et Rohrlich (Invent. Math. 44 (1978) 201–224) qui donnent la description de l'ensemble des points algébriques de degré au plus 2 sur les courbes étudiées. ***Pour citer cet article : O. Sall, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

Abstract

We determine explicitly algebraic points of a given degree on some quotients of Fermat curves of degree 5, 7 or 11. This Note completes previous work of Gross and Rohrlich (Invent. Math. 44 (1978) 201–224) who gave a description of points of degree at most two. ***To cite this article: O. Sall, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

1. Introduction

Soit C une courbe algébrique projective lisse définie sur $\mathbf{Q}$; pour toute extension K de $\mathbf{Q}$, on note $C(K)$ l'ensemble des points de C rationnels sur K, et $\bigcup_{[K:\mathbf{Q}]\leqslant d} C(K)$ l'ensemble des points de C définis sur K de degré $\leqslant d$. Le degré d'un point algébrique est le degré de son corps de définition sur $\mathbf{Q}$. Lorsque C est de genre $g \geqslant 2$, on sait depuis Faltings [6] que l'ensemble des points rationnels $C(\mathbf{Q})$ est fini. Une généralisation de ce théorème aux sous-variétés de variétés abéliennes obtenue par Vojta et Faltings [4,14] permet également de décrire qualitativement $\bigcup_{[K:\mathbf{Q}]\leqslant d} C(K)$. Divers travaux étudient cette question [2,7,1]. Tous ces énoncés sont qualitatifs ; un théorème plus précis de Debarre et Klassen [3] montre que, pour une courbe plane lisse C définie sur $\mathbf{Q}$ de degré d, on a

Adresse e-mail : oumarsfr@yahoo.fr (O. Sall).

1631-073X/03/$ – see front matter
doi:10.1016/S1631-073X(02)00028-6

(1) si $d \geqslant 7$ alors $\bigcup_{[K:Q]\leqslant d-2} C(K)$ est fini.
(2) si $d \geqslant 8$ alors, à un nombre fini d'exceptions près, les points de $\bigcup_{[K:Q]\leqslant d-1} C(K)$ se présentent comme intersection de C avec une droite définie sur Q passant par un point rationnel de C.

En général, on ne sait pas déterminer effectivement ces ensembles, même $C(\mathbf{Q})$. La situation est plus favorable lorsque le groupe de Mordell–Weil de la jacobienne $J(\mathbf{Q})$ est fini ; dans ce cas $C(\mathbf{Q})$ peut être effectivement déterminé. Nous montrons dans cette Note que dans quelques cas, les ensembles $\bigcup_{[K:Q]\leqslant d} C(K)$ peuvent être explicitement décrits pour tout d.

Pour $p = 5, 7, 11$, considérons les courbes de Fermat F_p de degré p, c'est-à-dire les courbes planes lisses d'équation projectives $F_p = \{(X, Y, Z) \in \mathbf{P}^2(\overline{\mathbf{Q}})\colon\ X^p + Y^p + Z^p = 0\}$, et les courbes $C_{r,s}(p)$ d'équations affines $C_{r,s}(p) : y^p = x^r(x-1)^s$ avec $1 \leqslant r, s, r+s \leqslant p-1$. Les courbes $C_{r,s}(p)$ sont des quotients des F_p (voir par exemple [8,13]). Le groupe de Mordell–Weil est fini (Faddeev [5], Gross et Rohrlich [8]) dans les cas suivants : $C_{r,s}(p)$ pour $p = 5$ ou 7 et pour $p = 11$ et $r = s$.

D'après Gross et Rohrlich [8], les courbes $C_{r,s}(p)$ et $C_{1,s'}(p)$ sont birationnellement isomorphes si $rs' \equiv s \pmod{p}$, et il en est de même pour les courbes $C_{r,s}(p)$ et $C_{r',s'}(p)$ si $(r, s) = k(r', s') + p(i, j)$ avec p et k premiers entre eux. Donc toutes les courbes $C_{r,s}(5)$ sont birationnellement isomorphes à $C_{1,1}(5)$ et on peut alors se limiter à l'étude de $C_{1,1}(5)$ pour $p = 5$. De même pour $p = 7$ on peut se limiter à l'étude de $C_{1,1}(7)$ et $C_{1,2}(7)$. Dans cette note nous déterminons *explicitement* les points algébriques de degré donné quelconque sur les courbes hyperelliptiques $C_{1,1}(p)$ avec $p \in \{5, 7, 11\}$; la courbe $C_{1,2}(7)$ est étudiée dans [11]. Voir [9,10,12] pour d'autres exemples explicites.

Notons P_0, P_1, P_∞ les points définis par $P_0 = (0, 0, 1)$, $P_1 = (1, 0, 1)$, $P_\infty = (1, 0, 0)$.

Il résulte des travaux de Gross et Rohrlich dans [8] que $\bigcup_{[K:\mathbf{Q}]\leqslant 2} C_{1,1}(p)(K) = \{(\frac{1}{2} \pm \sqrt{y^p + \frac{1}{4}}, y) \mid y \in \mathbf{Q}\} \cup \{P_\infty\}$, pour $p = 5, 7$ ou 11.

Si on note $\mathcal{M}_0 = \{P_0, P_1, P_\infty\}$ et pour $\delta \geqslant 1$ $\mathcal{M}_\delta = \{(x, y) \mid \big[\mathbf{Q}[y] : \mathbf{Q}\big] = \delta$ et x racine de l'équation $x(x-1) = y^p\}$, on voit immédiatement que $\mathcal{M}_0 \subset C_{1,1}(p)(\mathbf{Q})$ et $\mathcal{M}_\delta \subset \bigcup_{[K:\mathbf{Q}]\leqslant 2\delta} C_{1,1}(p)(K)$. On peut trouver d'autres points de degré $\leqslant l$ de la façon suivante : si $h \in \mathbf{Q}_{(l-m)/2}[Y]$ et $g_1 \in \mathbf{Q}_{(l-p+m)/2}[Y]$ avec $m \in \{0, \ldots, p-1\}$ et $\mathbf{Q}_d[Y]$ désigne l'ensemble des polynômes à coefficients dans $\mathbf{Q}$ de degré $\leqslant d$ en la variable Y ; si $h(y) \neq 0$ et y est racine de l'équation $y^m[h(y)]^2 - g_1(y)[y^{p-m}g_1(y) + h(y)] = 0$, alors le point $(-y^{p-m}g_1(y)/h(y), y)$ est de degré $[\mathbf{Q}[y] : \mathbf{Q}] \leqslant l$. On introduit donc l'ensemble

$$\mathcal{N}_m = \left\{ \left(-\frac{y^{p-m}g_1(y)}{h(y)}, y \right) \;\middle|\; h(y) \neq 0,\ 0 \leqslant \deg(h) \leqslant \frac{l-m}{2},\ 0 \leqslant \deg(g_1) \leqslant \frac{l-p+m}{2}, \right.$$
$$\left. \text{et } y \text{ racine de l'équation } y^m\big[h(y)\big]^2 - g_1(y)\big[y^{p-m}g_1(y) + h(y)\big] = 0 \right\}.$$

Notre résultat principal est que ces deux types de familles $\mathcal{M}_\delta$ et $\mathcal{N}_m$ décrivent tous les points de degré $\leqslant l$ lorsque $p = 5, 7$ ou 11.

Théorème. *Soit $p = 5, 7$ ou 11, et $l \geqslant 1$. On a $\bigcup_{[K:\mathbf{Q}]\leqslant l} C_{1,1}(p)(K) = (\bigcup_{0\leqslant m\leqslant p-1} \mathcal{N}_m) \cup (\bigcup_{0\leqslant\delta\leqslant l/2} \mathcal{M}_\delta)$ avec*

$$\mathcal{N}_m = \left\{ \left(-\frac{y^{p-m}g_1(y)}{h(y)}, y \right) \;\middle|\; h(y) \neq 0,\ 0 \leqslant \deg(h) \leqslant \frac{l-m}{2},\ 0 \leqslant \deg(g_1) \leqslant \frac{l-p+m}{2}, \right.$$
$$\left. \textit{et } y \textit{ racine de l'équation } y^m\big[h(y)\big]^2 - g_1(y)\big[y^{p-m}g_1(y) + h(y)\big] = 0 \right\},$$
$$\mathcal{M}_\delta = \big\{(x, y) \mid \big[\mathbf{Q}[y] : \mathbf{Q}\big] = \delta \textit{ et } x \textit{ racine de l'équation} x(x-1) = y^p\big\}.$$

Remarque 1. (1) $\mathcal{N}_m$ est non vide si et seulement si $l - m \geqslant 0$ et $l - p + m \geqslant 0$, en particulier il faut que $l \geqslant p/2$. (2) La preuve permet de retrouver que $C_{1,1}(p)(\mathbf{Q}) = \mathcal{M}_0$ et $\bigcup_{[K:\mathbf{Q}]\leqslant 2} C_{1,1}(p)(K) = \mathcal{M}_0 \cup \mathcal{M}_1$ qui est le résultat

de Gross et Rohrlich dans [8]. (3) On montre aisément que l'équation $\mathcal{E} : y^m[h(y)]^2 - g_1(y)[y^{p-m}g_1(y) + h(y)] = 0$ est de degré $\leqslant l$ en y, et même exactement l si $l - m$ est pair (resp. impair) et $\deg(h) = \frac{l-m}{2}$ (resp. $\deg(g_1) = \frac{l-p+m}{2}$). Les points algébriques de degré exactement l sur $C_{1,1}(p)$ avec $p = 5, 7$ ou 11, sont ceux pour lesquels le degré de $\mathcal{E}$ en y est l (et non seulement $\leqslant l$), et de plus l'équation $\mathcal{E}$ est irréductible sur $\mathbf{Q}$.

Remarque 2. Bien que le théorème permette de décrire $\bigcup_{[K:\mathbf{Q}]\leqslant l} C_{1,1}(p)(K)$, il ne permet pas de décrire $C_{1,1}(p)(K)$ pour un corps de nombres K fixé.

2. Résultats auxiliaires

Pour un diviseur D sur les courbes $C_{r,s}(p)$, nous notons $\pounds(D)$ le $\overline{\mathbf{Q}}$-espace vectoriel des fonctions rationnelles f sur la courbe étudiée telles que $f = 0$ ou $\operatorname{div}(f) \geqslant -D$; $\ell(D)$ désigne la $\overline{\mathbf{Q}}$-dimension de $\pounds(D)$. Comme dans [11], on désigne par $J_{r,s}(p)$ la jacobienne de $C_{r,s}(p)$, et par $j(p)$ la classe notée $[P - P_\infty]$ de $P - P_\infty$, c'est-à-dire que j est le plongement jacobien $C \to J_{r,s}(p)$.

Lemme 1 (voir [11], Lemme 1). $\operatorname{div}(x) = p(P_0) - p(P_\infty)$, $\operatorname{div}(x-1) = p(P_1) - p(P_\infty)$, $\operatorname{div}(y) = r(P_0) + s(P_1) - (r+s)(P_\infty)$.

Remarque. Les résultats suivants sont des conséquences du Lemme 1. (1) $pj(P_0) = pj(P_1) = 0$. (2) $rj(P_0) + sj(P_1) = 0$, donc $j(P_0)$ et $j(P_1)$ engendrent le même sous-groupe isomorphe à $\mathbf{Z}/p\mathbf{Z}$ dans $J_{r,s}(p)(\mathbf{Q})$.

Pour $1 \leqslant s \leqslant p-2$, nous notons $J_{1,s}(p)$ la jacobienne de $C_{1,s}(p)$, ou tout simplement $C_{1,s}$, $J_{1,s}$ s'il n'y a pas d'ambiguité. On se restreint dans la suite aux courbes $C_{1,1}$.

La courbe $\mathbf{C}_{1,1}(p)$ a pour équation $y^p = x(x-1)$; d'après Gross et Rohrlich ([8], Théorème 1.1), pour $p \geqslant 5$ on a $J_{1,1}(p)(\mathbf{Q})_{\text{torsion}} \cong \mathbf{Z}/p\mathbf{Z}$, et d'après Faddeev [5] pour $p \in \{5, 7, 11\}$ on a $J_{1,1}(p)(\mathbf{Q})_{\text{torsion}} = J_{1,1}(p)(\mathbf{Q})$ (voir aussi [8], p. 219).

Lemme 2. *Une* $\mathbf{Q}$*-base de* $\pounds(lP_\infty)$*, est donnée par* $\mathfrak{B} = \{y^i,\ i \leqslant l/2\} \cup \{xy^j,\ j \leqslant (l-p)/2\}$.

Démonstration. La courbe $C_{1,1}(p)$ est hyperelliptique et son genre est égal à $g = (p-1)/2$. Le point P_∞ est un point de Weierstrass. Il est clair que $\mathfrak{B}$ est une partie libre de $\pounds(lP_\infty)$; il reste à montrer que $\dim(\mathfrak{B}) = \dim(\pounds(lP_\infty))$. Pour $l \leqslant 2g-2$, le lemme résulte du Lemme 1. Supposons que $l \geqslant 2g-1$, donc d'après le théorème de Riemann–Roch on a $\dim(\pounds(lP_\infty)) = l - g + 1$.

Considérons les cas suivants :

1^{er} cas : supposons que l est pair, et posons $l = 2h$. On a alors $i \leqslant l/2 \Leftrightarrow i \leqslant 2h/2 = h$; $j \leqslant (l-p)/2 \Leftrightarrow j \leqslant (2h-p)/2 \Leftrightarrow j \leqslant (2h-p-1)/2 = h-g-1$. Donc on a $\mathfrak{B} = \{1, y, \ldots, y^h\} \cup \{x, xy, \ldots, xy^{h-g-1}\}$, et par suite $\dim(\mathfrak{B}) = (h+1) + (h-g) = 2h - g + 1 = l - g + 1 = \dim(\pounds(lP_\infty))$.

$2^{\text{ième}}$ cas : supposons que l est impair, et posons $l = 2h+1$. On a alors $i \leqslant l/2 \Leftrightarrow i \leqslant (2h+1)/2 \Leftrightarrow i \leqslant 2h/2 = h$; $j \leqslant (l-p)/2 \Leftrightarrow j \leqslant (2h+1-p)/2 = h-g$. Donc on a $\mathfrak{B} = \{1, y, \ldots, y^h\} \cup \{x, xy, \ldots, xy^{h-g}\}$, et par suite $\dim(\mathfrak{B}) = (h+1) + (h-g+1) = 2h - g + 2 = l - g + 1 = \dim(\pounds(lP_\infty))$.

3. Démonstration du théorème

Soit $R \in C_{1,1}(p)(\overline{\mathbf{Q}})$ avec $[\mathbf{Q}(R) : \mathbf{Q}] = l$, et $R \notin \{P_0, P_1, P_\infty\}$. Notons $R_1, \ldots, R_l$ les conjugués de R, et travaillons avec $t = [R_1 + \cdots + R_l - lP_\infty]$ qui est un point de $J_{1,1}(p)(\mathbf{Q}) = \{mj(P_0) \mid 0 \leqslant m \leqslant p-1\}$; donc $t = mj(P_0)$ avec $0 \leqslant m \leqslant p-1$. On a alors $[R_1 + \cdots + R_l - lP_\infty] = mj(P_0) = (m-p)j(P_0) = (m-p)[P_0 - P_\infty]$.

Il existe alors une fonction f à coefficients dans $\mathbf{Q}$ telle que $\operatorname{div}(f) = R_1 + \cdots + R_l + (p-m)P_0 - (l+p-m)P_\infty$, donc $f \in \mathcal{L}((l+p-m)P_\infty)$. D'après le Lemme 2 on a $f = g(y) + xh(y)$ avec $g \in \mathbf{Q}_{(l+p-m)/2}[Y]$ et $h \in \mathbf{Q}_{(l-m)/2}[Y]$. Ecrivons $g(y) = y^a g_0(y)$ avec $g_0(0) \neq 0$ et $a \geqslant 0$; on a donc $\operatorname{ord}_{P_0}(g(y)) = a$. Comme $\operatorname{ord}_{P_0}(f) = \operatorname{ord}_{P_0}(g(y) + xh(y)) = p - m$ et $\operatorname{ord}_{P_0}(x) = p$, on en déduit que $a \geqslant p - m$. On peut donc écrire $g(y) = y^{p-m} g_1(y)$, et par suite $f = y^{p-m} g_1(y) + xh(y)$. Aux points R_i on doit avoir $y^{p-m} g_1(y) + xh(y) = 0$. Comme $R \notin \{P_0, P_1, P_\infty\}$, on a $y(R) \neq 0$ et $y(R) \neq \infty$; l'étude peut se ramener aux deux cas suivants :

1er cas : aux points R_i on suppose $h(y) \neq 0$; donc $x = -y^{p-m} g_1(y)/h(y)$ et par suite $y^p = x(x-1) \Leftrightarrow y^p [h(y)]^2 = y^{p-m} g_1(y)[y^{p-m} g_1(y) + h(y)]$, et en simplifiant par y^{p-m} on obtient $y^m [h(y)]^2 = g_1(y)[y^{p-m} g_1(y) + h(y)]$. On trouve ainsi une famille de points

$$\mathcal{N}_m = \left\{ \left(-\frac{y^{p-m} g_1(y)}{h(y)}, y \right) \;\middle|\; h(y) \neq 0,\ 0 \leqslant \deg(h) \leqslant \frac{l-m}{2},\ 0 \leqslant \deg(g_1) \leqslant \frac{l-p+m}{2}, \right.$$
$$\left. \text{et } y \text{ racine de l'équation } y^m \big[h(y)\big]^2 - g_1(y)\big[y^{p-m} g_1(y) + h(y)\big] = 0 \right\}.$$

2ème cas : aux points R_i on suppose $h(y) = 0$; on a alors $y^{p-m} g_1(y) = 0$, donc $g_1(y) = 0$ puisque on a supposé $R \notin \{P_0, P_1, P_\infty\}$; et par suite h et g_1 ont comme facteur commun le polynôme minimal de $y(R)$ sur $\mathbf{Q}$ que nous noterons Δ.

Posons $h = \Delta \cdot h_2$, $g_1 = \Delta \cdot g_2$ et $\deg(\Delta) = [\mathbf{Q}(y(R)) : \mathbf{Q}] = \delta$. On a alors $0 \leqslant \deg(h_2) \leqslant (l-m)/2 - \delta = (l - 2\delta) - m/2$ et $0 \leqslant \deg(g_2) \leqslant (l-p+m)/2 - \delta = (l-2\delta) - (p-m)/2$, d'où $l - 2\delta \geqslant 0$ ou encore $\boxed{l \geqslant 2\delta}$ (i). Si nous désignons par Z le diviseur des zéros de $\Delta(y)$, on peut écrire $\operatorname{div}(\Delta(y)) = Z - 2\delta P_\infty$; comme $R_1, \ldots, R_l$ sont des zéros de $\Delta(y)$ on a $\operatorname{div}(\Delta(y)) = R_1 + \cdots + R_l + (Q_1 + \cdots + Q_{2\delta - l}) - 2\delta P_\infty$, et on doit donc avoir $\boxed{l \leqslant 2\delta}$ (ii). Les relations (i) et (ii) montrent que $l = 2\delta$, et par suite $\operatorname{div}(\Delta(y)) = R_1 + \cdots + R_l - lP_\infty$. On trouve ainsi une famille de points de degré $\leqslant 2\delta = l$: $\mathcal{M}_\delta = \{(x, y) \mid [\mathbf{Q}[y] : \mathbf{Q}] = \delta$ et x racine de l'équation $x(x-1) = y^p\}$. □

Remerciements

Je tiens à remercier très chaleureusement le professeur Marc Hindry de l'université Denis Diderot (Paris 7, France) pour m'avoir aidé à rédiger cette Note.

Références

[1] D. Abramovic, J. Harris, Abelian varieties and curves in $W_d(C)$, Compositio Math. 78 (1991) 227–238.
[2] O. Debarre, R. Fahlaoui, Abelian varieties and curves in $W_d^r(C)$ and points of bounded degree on algebraic curves, Compositio Math. 88 (1993) 235–249.
[3] O. Debarre, M. Klassen, Points of low degree on smooth plane curves, J. Reine Angew. Math. 446 (1994) 81–87.
[4] Diophantine approximation on Abelian varieties, Ann. Math. 133 (1991) 549–576.
[5] D. Faddeev, On the divisor class groups of some algebraic curves, Dokl. Akad. Nauk SSSR 136 (1961) 296–298. English translation: Soviet Math. Dokl. 2 (1) (1961) 67–69.
[6] G. Faltings, Endlichkeitsätze für abelsch Varietäten über Zahlkörpen, Invent. Math. 73 (1983) 349–366.
[7] G. Frey, Curves with infinitely many points of fixed degree, Israel J. Math. 85 (1994) 79–83.
[8] B. Gross, D. Rohrlich, Some results on the Mordell–Weil group of the Jacobian of the Fermat curve, Invent. Math. 44 (1978) 201–224.
[9] M. Klassen, P. Tzermias, Algebraic points of low degree on the Fermat quintic, Acta Arith. 82 (4) (1997) 393–401.
[10] O. Sall, Points algébriques de petit degré sur les courbes de Fermat, C. R. Acad. Sci. Paris Sér. I 330 (2000) 67–70.
[11] O. Sall, Points cubiques sur la quartique de Klein, C. R. Acad. Sci. Paris Sér. I 333 (2001) 931–934.
[12] P. Tzermias, Algebraic points of low degree on the Fermat curve of degree seven, Manuscriptc Math. 97 (4) (1998) 483–488.
[13] P. Tzermias, Torsion parts of Mordell–Weil groups of Fermat Jacobians, Internat. Math. Res. Notices 7 (1998) 359–369.
[14] Siegel's theorem in the compact case, Ann. Math. 133 (1991) 509–548.