Canad. Math. Bull. Vol. **53** (1), 2010 pp. 58–63
doi:10.4153/CMB-2010-010-2

Ranks in Families of Jacobian Varieties of Twisted Fermat Curves

Andrzej Dąbrowski and Tomasz Jędrzejak

Abstract. In this paper, we prove that the unboundedness of ranks in families of Jacobian varieties of twisted Fermat curves is equivalent to the divergence of certain infinite series.

1 Introduction

K. Rubin and A. Silverberg showed that the unboundedness of ranks of the quadratic twists of an elliptic curve is equivalent to the divergence of certain infinite series [6]. In this paper we prove an analogous result for the family of Jacobian varieties of (twisted) Fermat curves $C_m^p : x^p + y^p = m$ (p fixed odd prime), where m runs through p-th power free integers (Theorems 1 and 6).

Fix non-zero integer m' so that $C_{m'}^p(\mathbf{Q}) \neq \varnothing$, and choose $\alpha \in \overline{\mathbf{Q}}$ satisfying $\alpha^p = \frac{m}{m'}$. Then we have an isomorphism (defined over $\mathbf{Q}(\alpha)$) $\phi\colon C_m^p \to C_{m'}^p$, $\phi([x, y, z]) = [x, y, \alpha z]$. This induces an isomorphism of Jacobian varieties $\phi\colon J_m^p \to J_{m'}^p$.

Let $D_{m'}^p \in \operatorname{Div}(J_{m'}^p)$ be a fixed symmetric, positive divisor, defined over $\mathbf{Q}$. Let $\hat{h}_m^p\colon J_m^p(\overline{\mathbf{Q}}) \to \mathbf{R}$ be the canonical height with respect to the divisor $3\phi^\star D_{m'}^p$. In particular, $\hat{h}_m^p$ is a positive definite quadratic form on $J_m^p(\mathbf{Q})/\text{torsion}$. For non-negative real numbers i and j define the infinite series

$$T_p(i, j) = \sum_{m \in \mathbf{N}^{(p)}} |m|^{-i} \sum_{P \in J_m^p(\mathbf{Q}) \setminus J_m^p(\mathbf{Q})_{tors}} \hat{h}_m^p(P)^{-j},$$

where $\mathbf{N}^{(p)}$ denotes the set of all p-th power free integers.

Our main result is the following.

Theorem 1 *Fix a positive real number j. The following conditions are equivalent:*

(i) $\operatorname{rank}(J_m^p(\mathbf{Q})) < 2j$ *for every p-th power free integer m,*
(ii) $T_p(i, j)$ *converges for some* $i \geq 1$,
(iii) $T_p(i, j)$ *converges for every* $i \geq 1$,
(iv) $T_p(i, j)$ *converges for* $i = 1$.

Received by the editors October 30, 2006; revised September 12, 2008.
Published electronically December 4, 2009.
AMS subject classification: **11G10**, 11G05, 11G50, 14G05, 11G30, 14H45, 14K15.
Keywords: Fermat curve, Jacobian variety, elliptic curve, canonical height.

2 Proof of Theorem 1

We start with the following general observation. If A is an abelian variety over $\mathbf{Q}$ and $c \in \operatorname{Pic}(A)$, let

$$h_{A,c}^{\min} = \min_{P \in A(\mathbf{Q}) \setminus A(\mathbf{Q})_{\text{tors}}} \hat{h}_{A,c}(P).$$

Lemma 2 *Suppose A is an abelian variety over $\mathbf{Q}$ and j is a positive real number. Let* $r = \operatorname{rank} A(\mathbf{Q})$.

(i) *If $r \geq 2j$ and U is a nonempty open subset of the identity component $A(\mathbf{R})^0$ of $A(\mathbf{R})$, then*

$$\sum_{P \in (A(\mathbf{Q}) \setminus A(\mathbf{Q})_{\text{tors}}) \cap U} \hat{h}_{A,c}(P)^{-j}$$

diverges.

(ii) *If $r < 2j$, then there exists a constant C_j depending only on j (and independent of A) such that*

$$\sum_{P \in A(\mathbf{Q}) \setminus A(\mathbf{Q})_{\text{tors}}} \hat{h}_{A,c}(P)^{-j} \leq \# A(\mathbf{Q})_{\text{tors}} (h_{A,c}^{\min})^{-j} C_j.$$

Proof The proof is analogous to the proof of [6, Proposition 2.4]. ■

Now we prove that for fixed p the order of $J_m^p(\mathbf{Q})_{\text{tors}}$ is bounded.

Lemma 3 *We have $\# J_m^p(\mathbf{Q})_{\text{tors}} \leq c_p$, for certain positive constants c_p.*

Proof Let $C_{m,s}(p) : y^p = x(m-x)^s$; note it has genus $(p-1)/2$ for each m. Consider the rational maps $\phi_s \colon C_m^p \to C_{m,s}(p)$ defined by $\phi_s(X, Y, 1) = (X^p, XY^s, 1)$ for $s = 1, \dots, p-2$. We also denote by ϕ_s the induced map between the corresponding Jacobi varieties: $\phi_s \colon J_m^p \to J_{m,s}(p)$. We obtain an isogeny over $\mathbf{Q}$

$$\phi = \prod_{s=1}^{p-2} \phi_s \colon J_m^p \to \prod_{s=1}^{p-2} J_{m,s}(p),$$

with $\operatorname{Ker}(\phi)$ consisting of points of order p.

We show, using the Weil-style method, that $J_{m,s}(p)(\mathbf{Q})_{\text{tors}} \subset \mathbf{Z}/2p\mathbf{Z}$. First, it is clear that $\# C_{m,s}(p)(\mathbf{F}_{l^n}) = l^n + 1$, if $p \not| l^n - 1$. Now

$$\# C_{m,s}(p)(\mathbf{F}_{l^n}) = l^n + 1 - (\alpha_1^n + \cdots + \alpha_{p-1}^n)$$

(with α_i algebraic integers), where the polynomial $P(T) = \prod_{i=1}^{p-1}(1 - \alpha_i T)$ has rational integer coefficients (and leading coefficient $l^{(p-1)/2}$), and satisfies $P(T) = l^{(p-1)/2} T^{p-1} P(\frac{1}{lT})$. Assuming l is a primitive root modulo p, we easily obtain

$$\# J_{m,s}(p)(\mathbf{F}_l) = P(1) = l^{(p-1)/2} + 1.$$

Now follow the proof of [3, Lemma 1.2]. ■

https://doi.org/10.4153/CMB-2010-010-2 Published online by Cambridge University Press

Now we recall the lower bound for the canonical height of non-torsion points on $J_m^p(\mathbf{Q})$.

Lemma 4 *Every non-torsion point $P \in J_m^p(\mathbf{Q})$ satisfies $\hat{h}_m^p(P) > C_p \log|m|$, with a positive constant C_p.*

Proof Silverman [7, Theorem 5] stated that, in our situation, every point $P \in J_m^p(\mathbf{Q})$ satisfies either (i) $P = [\zeta]P$ for some $\zeta \in \mu_p \setminus \{1\}$ or (ii) $\hat{h}_m^p(P) > C_p \log|m|$ with a positive constant C_p. Since $\prod(1-\zeta) = p$, we see that every point satisfying (i) is in $J_m^p[p]$, the group of p-division points of J_m^p. Hence the first case does not occur. ■

The last preliminary result which we prove says that for any odd prime p there exists a positive integer $m(p)$ such that $\operatorname{rank}(J_{m(p)}^p(\mathbf{Q})) \geq 2$.

Lemma 5 *We have* $\operatorname{rank}(J_{19}^3(\mathbf{Q})) = 2$, $\operatorname{rank}(J_{33}^5(\mathbf{Q})) \geq 2$, $\operatorname{rank}(J_{129}^7(\mathbf{Q})) \geq 2$, *and* $\operatorname{rank}(J_1^p(\mathbf{Q})) \geq 2$ *for $p > 7$.*

Proof The fact that $\operatorname{rank}(J_{19}^3(\mathbf{Q})) = 2$ can be checked using Cremona's program, mwrank, or can be found in his tables [2] (J_{19}^3 is the curve $9747f2$ with the minimal Weierstrass equation $y^2 + y = x^3 - 2437$).

Now consider J_{33}^5. All the curves $C_{33,r}(5)$ $(r = 1,2,3)$ are hyperelliptic of genus 2. Indeed, by substitution $(x,y) \mapsto (\frac{y}{32} + \frac{33}{2}, -\frac{x}{4})$ in the equation of $C_{33,1}(5)$ and

$$(x,y) \mapsto \Big(33 - \Big(\frac{132}{x}\Big)^5\Big(\frac{y}{2^5 33^2} - \frac{1}{2}\Big), \Big(\frac{132}{x}\Big)^4\Big(\frac{y}{2^5 33^2} - \frac{1}{2}\Big)\Big)$$

in the equation of $C_{33,3}(5)$ we obtain the equations $y^2 = x^5 + 528^2$ and $y^2 = x^5 + 132^4$. Using the Riemann–Hurwitz formula we immediately obtain $2g(C_{33,r}(5)) - 2 = 2$. Moreover, there exists a birational equivalence $C_{33,2}(5) \to C_{33,3}(5)$ given by

$$(x,y) \mapsto \Big(33 - \frac{y^5}{(33-x)^2}, \frac{y^3}{33-x}\Big).$$

Consider the divisor $D = (-8, 496) - \infty$ on the above model of $C_{33,1}(5)$. Using [5, Appendix] or [1], one immediately checks that $10D$ is not principal. Using the proof of Lemma 3 we conclude that $J_{33,1}(5)(\mathbf{Q})$ is infinite. Similarly, $J_{33,3}(5)(\mathbf{Q})$ is infinite: consider the divisor $D = (33, 18513) - \infty$.

Similarly, one checks that $J_{129,s}(7)(\mathbf{Q})$ are infinite for $s = 1, 5$: consider the divisor $(-8, 8128) - \infty$ on the model $y^2 = x^7 + 8256^2$ of $C_{129,1}(7)$ and the divisor $(129, 139534785) - \infty$ on the model $y^2 = x^7 + 516^6$ of $C_{129,5}(7)$.

The last estimate $\operatorname{rank}(J_1^p(\mathbf{Q})) \geq 2$ for $p > 7$ follows from [3, Theorem 2.1]. ■

Proof of Theorem 1 Fix a positive number j. Clearly, (iii) $\Rightarrow$ (ii).

Now assume that $T_p(i,j)$ converges for some $i \geq 1$. In particular, for every $m \in \mathbf{N}^{(p)}$ the inner sum

$$\sum_{P \in J_m^p(\mathbf{Q}) \setminus J_m^p(\mathbf{Q})_{\mathrm{tors}}} \hat{h}_m^p(P)^{-j}$$

converges. From Lemma 2(i) we obtain $\operatorname{rank}(J_m^p(\mathbf{Q})) < 2j$, which shows (ii) $\Rightarrow$ (i).

https://doi.org/10.4153/CMB-2010-010-2 Published online by Cambridge University Press

Now assume that $\operatorname{rank}(J_m^p(\mathbf{Q})) < 2j$ for every $m \in \mathbf{N}^{(p)}$. Put $h_{m,p}^{\min} = h_{J_m^p, 3\phi^\star D_m^p}^{\min}$. By Lemma 2(ii) and Lemma 3 we have

$$\sum_{P \in J_m^p(\mathbf{Q}) \setminus J_m^p(\mathbf{Q})_{\text{tors}}} \hat{h}_m(P)^{-j} \leq c_p (h_{m,p}^{\min})^{-j} C_j.$$

Therefore,

$$T_p(i,j) \leq c_p C_j \sum_{m \in \mathbf{N}^{(p)}} |m|^{-i} (h_{m,p}^{\min})^{-j}.$$

It follows from Lemma 4 that $\hat{h}_m^p(P) \gg \log|m|$. Therefore, there exists a positive constant C (independent of m) such that $h_{m,p}^{\min} \geq C \log|m|$. Thus, there exists a positive constant C_j' such that

$$T_p(i,j) \leq C_j' \sum_{m \in \mathbf{N}^{(p)}} |m|^{-i} (\log|m|)^{-j} \leq 2C_j' \sum_{m=1}^{\infty} m^{-i} (\log(m))^{-j}.$$

It follows that $T_p(i,j)$ converges if $i > 1$, or if $i = 1$ and $j > 1$. But $j > 1$ by Lemma 5, so $T_p(i,j)$ converges. Hence (i) $\Rightarrow$ (iii). Since $T_p(i,j)$ is decreasing as a function of i, conditions (iii) and (iv) are equivalent. ∎

3 The Case of Cubic Twists of the Fermat Elliptic Curve

In this section we prove a "more explicit" result for the family $E_m : x^3 + y^3 = m$ of cubic twists of the Fermat curve $E_1 : x^3 + y^3 = 1$ ($m \in \mathbf{Z} \setminus \{0\}$). Note that E_m has the Weierstrass equation $y^2 = x^3 - 432m^2$ (see [4, p. 52]).

It is well known (see [4, Theorem 5.3] or [8, Exercise 10.19]) that

$$E_1(\mathbf{Q}) = \{O, (1,0), (0,1)\}, \quad E_2(\mathbf{Q}) = \{O, (1,1)\}, \quad E_m(\mathbf{Q})_{tors} = \{O\}$$

for cube-free integers $m \geq 3$. Also $\operatorname{rank}(E_m(\mathbf{Q})) \geq 1$ if and only if there exist $k, l, n \in \mathbf{Z} \setminus \{0\}$, $k \neq \pm n$, satisfying $n^3 + k^3 = ml^3$.

For $q \in \mathbf{Q} \setminus \{0\}$, let $c(q)$ denote the cubefree part: $q = c(q)r^3$. Put

$$\Psi = \{(n,k) \in \mathbf{N} \times \mathbf{Z} : (n,k) = 1, nk \neq 0, |n| \neq |k|\},$$

and, for cubefree m, $\Psi_m = \{(n,k) \in \Psi : c(n^3 + k^3) = m\}$. Then, of course, $\operatorname{rank}(E_m(\mathbf{Q})) \geq 1$ if and only if $\Psi_m \neq \varnothing$.

For non-negative real numbers i and j define the infinite sum

$$S(i,j) = \sum_{(n,k) \in \Psi} c(n^3 + k^3)^{-i} \max\Big\{\log(|nk|), \frac{2}{3} \log\Big|\frac{n^3 + k^3}{c(n^3 + k^3)}\Big|\Big\}^{-j}.$$

https://doi.org/10.4153/CMB-2010-010-2 Published online by Cambridge University Press

The main result of this section is the following.

Theorem 6 *Fix a positive real number j. The following conditions are equivalent:*

(i) $\operatorname{rank}(E_m(\mathbf{Q})) < 2j$ *for every cubefree $m \in \mathbf{N}$,*
(ii) *$S(i, j)$ converges for some $i \geq 1$,*
(iii) *$S(i, j)$ converges for every $i \geq 1$,*
(iv) *$S(i, j)$ converges for $i = 1$.*

We start with a series of preliminary results.

Lemma 7 *The map*

$$\phi_m(n, k) = \left(\frac{n}{l}, \frac{k}{l}\right),$$

where $l^3 m = n^3 + k^3$, defines a bijection $\phi_m \colon \Psi_m \to E_m(\mathbf{Q}) \setminus E_m(\mathbf{Q})_{\mathrm{tors}}$.

Proof The proof is an easy calculation, and left to the reader. ■

Consider the rational function $f \in \overline{\mathbf{Q}}(E_m)$ defined by $f((x, y)) = xy$. Let $h_{xy}(P) = h(f(P))$ denote the corresponding (naive) height on $E_m(\overline{\mathbf{Q}})$. For $P = (\frac{n}{l}, \frac{k}{l}) \in E_m(\mathbf{Q})$, we have

$$h_{xy}(P) = \max\left\{ \log(|nk|), \frac{2}{3} \log\left| \frac{n^3 + k^3}{m} \right| \right\}.$$

Let $\hat{h}_m$ denote the canonical height on $E_m(\overline{\mathbf{Q}})$. Since $\deg(f) = (\overline{\mathbf{Q}}(E_m) : \overline{\mathbf{Q}}(f)) = 6$, we obtain

$$\hat{h}_m(P) = \frac{1}{6} \lim_{N\to\infty} \frac{h_{xy}(2^N P)}{4^N}.$$

Lemma 8 *Let E and E' be elliptic curves defined over a number field K. Assume there is an isomorphism over K: $f \colon E \to E'$. Then for any $P \in E(K)$, we have $\hat{h}_E(P) = \hat{h}_{E'}(f(P))$.*

Proof This is well known [8]. ■

For non-negative real numbers i and j we define an additional series (*cf.* §1)

$$T(i, j) = \sum_{m\in\mathbf{N}^{(3)}} m^{-i} \sum_{P\in E_m(\mathbf{Q})\setminus E_m(\mathbf{Q})_{\mathrm{tors}}} \hat{h}_m(P)^{-j},$$

where $\mathbf{N}^{(3)}$ denotes the set of all cube-free positive integers.

Lemma 9 *$S(i, j)$ is convergent if and only if $T(i, j)$ is convergent.*

Proof We have

$$\begin{aligned} S(i, j) &= \sum_{(n,k)\in\Psi} c(n^3 + k^3)^{-i} \max\left\{ \log(|nk|), \frac{2}{3} \log\left| \frac{n^3 + k^3}{c(n^3 + k^3)} \right| \right\}^{-j} \\ &= \sum_{m\in\mathbf{N}^{(3)}} m^{-i} \sum_{(n,k)\in\Psi_m} \max\left\{ \log(|nk|), \frac{2}{3} \log\left| \frac{n^3 + k^3}{m} \right| \right\}^{-j} \\ &= \frac{1}{2} \sum_{m\in\mathbf{N}^{(3)}} m^{-i} \sum_{P\in E_m(\mathbf{Q})\setminus E_m(\mathbf{Q})_{tors}} h_{xy}(P)^{-j}, \end{aligned}$$

https://doi.org/10.4153/CMB-2010-010-2 Published online by Cambridge University Press

where in the last step we use Lemma 7.

Let $P = (a, b) \in E_m(\overline{\mathbf{Q}})$. Then $P' = (\frac{a}{m^{1/3}}, \frac{b}{m^{1/3}}) \in E_1(\overline{\mathbf{Q}})$, and using Lemma 8, we obtain $\hat{h}_m(P) = \hat{h}_1(P')$. It follows from the known properties of heights that $|\hat{h}_1(P) - \frac{1}{6}h_{xy}(P)|$ is bounded independent of $P \in E_1(\overline{\mathbf{Q}})$. Therefore there exists a constant $C > 0$ (independent of P and m) such that for any $P \in E_m(\mathbf{Q})$ we have $|\hat{h}_m(P) - \frac{1}{6}h_{xy}(P)| \leq C$.

There are only finitely many $P \in E_m(\mathbf{Q})$ satisfying $\frac{1}{12}h_{xy}(P) \leq C$. Hence for almost all P we have $\frac{1}{12}h_{xy}(P) \leq \hat{h}_m(P) \leq \frac{1}{4}h_{xy}(P)$, and the assertion follows. ∎

Proof of Theorem 6 Combine Theorem 1 with Lemma 9. ∎

Acknowledgement We would like to thank the anonymous referee for suggestions which improved the final version.

References

[1] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2. London Mathematical Society Lecture Note Series 230. Cambridge University Press, Cambridge, 1996

[2] J. E. Cremona, *Elliptic Curve Data.* http://www.warwick.ac.uk/~masgaj/ftp/data/.

[3] B. H. Gross and D. E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve.* Invent. Math. **44**(1978), no. 3, 201–224 doi:10.1007/BF01403161

[4] A. N. Knapp, *Elliptic Curves*. Mathematical Notes 40. Princeton University Press, Princeton, NJ, 1992

[5] N. Koblitz, *Algebraic Aspects of Cryptography*. With an appendix by A. J. Menezes, Y.-H. Wu, and R. J. Zuccherato. Algorithms and Computation in Mathematics 3. Springer-Verlag, Berlin, 1998.

[6] K. Rubin and A. Silverberg, *Ranks of elliptic curves in families of quadratic twists.* Experiment. Math. **9**(2000), no. 4, 583–590

[7] J. H. Silverman, *Representations of integers by binary forms and the rank of the Mordell–Weil group*. Invent. Math. **74**(1983), no. 2, 281–292. doi:10.1007/BF01394317

[8] ———, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

University of Szczecin, Institute of Mathematics, ul. Wielkopolska 15, 70-451 Szczecin, Poland
e-mail: dabrowsk@wmf.univ.szczecin.pl
tjedrzejak@gmail.com