Math. Res. Lett.
Volume ??, Number ??, 983–990, ??

Twisted Fermat Jacobians with positive Mordell-Weil ranks

Jie Shu and Zikang Wang

In this short note we prove that for any odd prime p there exist infinitely many twisted Fermat Jacobians of exponent p whose Mordell-Weil ranks are positive over $\mathbb{Q}$.

1. Introduction

Let p be an odd prime number. Let δ be a p-th power-free integer and let F_δ be the twisted Fermat curve over $\mathbb{Q}$ of exponent p defined by the affine equation

$$X^p + Y^p = \delta.$$

The curve F_δ has genus $(p-2)(p-1)/2$ and always poses a rational point, i.e., the infinity point $\infty = [1 : -1 : 0]$. Thus F_δ is an elliptic curve with ∞ as the zero element for the group law for $p = 3$, and by Faltings' theorem [9] $F_\delta(\mathbb{Q})$ is finite for $p \geq 5$.

For any integer $1 \leq r \leq p-2$, let $C_{\delta,r}$ be the smooth curve over $\mathbb{Q}$ of genus $(p-1)/2$ defined by the affine equation

$$y^p = x^r(\delta - x). \tag{1.1}$$

There is a quotient map given as

$$\varphi_{\delta,r} : F_\delta \longrightarrow C_{\delta,r}, \quad (X, Y) \mapsto (X^p : X^r Y).$$

Denote by $J_{\delta,r}$ the Jacobian variety of the curve $C_{\delta,r}$. It is known from [7, 8, 12] that the quotient maps $\varphi_{\delta,r}$ induce an isogeny

$$\mathrm{Jac}(F_\delta) \to \prod_{r=1}^{p-2} J_{\delta,r} \tag{1.2}$$

of abelian varieties over $\mathbb{Q}$. Thus these abelian varieties $J_{\delta,r}$ are referred as twisted Fermat Jacobian varieties of exponent p.

For the original Fermat curves, Gross and Rohrlich [11] prove that when $p > 7$ the non-hyperelliptic factors $J_{1,r}$ have positive Mordell-Weil ranks over $\mathbb{Q}$, and they suggest that for $p > 11$ all the abelian factors $J_{1,r}$ should have positive Mordell-Weil ranks. As for the twisted case, Diaconu and Tian [6] prove $J_{\delta,1}$ has Mordell-Weil rank zero over F for infinitely many $\delta \in F^\times/F^{\times p}$, where F denotes the maximal real subfield of the p-th cyclotomic field.

Let $\mathbb{N}^{(p)}$ denote the set of p-th powerfree positive integers, which has positive density among natural numbers.

Theorem 1.1. *Suppose $p \geq 3$ is a prime and $\delta \in \mathbb{N}^{(p)} \setminus \{1, 2, 2^{p-2}\}$. If $F_\delta(\mathbb{Q}) \neq \{\infty\}$, then, for all $1 \leq r \leq p-2$, the twisted Fermat Jacobians $J_{\delta,r}$ have positive Mordell-Weil ranks over $\mathbb{Q}$.*

The proof of Theorem 1.1 relies on the deep results on the cuspidal torsion packets on the original Fermat curves (see [3–5, 10, 16] etc.). We translate these structural results for cuspidal torsion packets to twisted Fermat curves and observe that, generally, for $\delta = a^p + b^p$ with $(a, b) \in \mathbb{Q}^{\times 2}$, the point P, obtained by projecting $(a, b) \in F_\delta(\mathbb{Q})$ to the curve $C_{\delta,r}$, doesn't belong to the cuspidal torsion packet of the curve $C_{\delta,r}$ for any $1 \leq r \leq p-2$. As a result, the class of $P - \infty$ has infinite order in the Jacobian variety $J_{\delta,r}$.

Denote

$$N^+(p, X) = \{\delta \in \mathbb{N}^{(p)} : \delta \leq X \text{ and } \operatorname{rank}(J_{\delta,r}(\mathbb{Q})) > 0 \text{ for all } 1 \leq r \leq p-2\}.$$

Corollary 1.2. *Suppose $p \geq 3$ is a prime. There exist infinitely many $\delta \in \mathbb{N}^{(p)}$ such that, for all $1 \leq r \leq p-2$, $J_{\delta,r}$ have positive Mordell-Weil ranks over $\mathbb{Q}$. More precisely, as $X \to \infty$,*

$$\#N^+(p, X) \gg X^{2/p}.$$

Proof. Let $F(X, Y) = X^p + Y^p$ and denote $R_p(X)$ to be the number of $\delta \in \mathbb{N}^{(p)}$ with $\delta \leq X$ for which there are integers a, b such that $F(a, b) = \delta$. By [15, Theorem 1], $R_p(X) \gg X^{2/p}$. Now the corollary follows by conjunction with Theorem 1.1. □

Combined with the isogeny decompostion (1.2), the following corollary is immediate.

Corollary 1.3. *Suppose $p \geq 3$ is a prime. For sufficiently large X,*

$$\#\{\delta \in \mathbb{N}^{(p)} : \delta \leq X \text{ and } \operatorname{rank}(\operatorname{Jac}(F_\delta)(\mathbb{Q})) \geq p-2\} \gg X^{2/p}.$$

We remark that the lower bound here is rather weak in contrast with the usual belief that $N^+(p, X)$ should have positive desity within $\mathbb{N}^{(p)}$ for a given p. In fact, Shu [13, Theorem 2] proves that the global root numbers are equi-distributed among the twisted Fermat Jacobians $J_{\delta,r}$ of a given exponent p with $\delta \in \mathbb{N}^{(p)}$. Thus the Birch and Swinnerton-Dyer conjecture predicts that half of the twisted Fermat Jacobians of exponent p have odd (resp. even) Mordell-Weil ranks over $\mathbb{Q}$. A positive density result for Fermat cubics can be found in [1].

2. Cuspidal torsion packets on twisted Fermat curves

In this section, let $p \geq 5$ be a prime. Denote $\mathcal{C}_{\delta,r} = \{(0,0), (\delta, 0), \infty\}$ the set of cusps on $C_{\delta,r}$, and denote by $\mathcal{W}_{\delta,r}$ the set of Weierstrass points on $C_{\delta,r}$. It is known that $C_{\delta,r}$ is hyperelliptic if and only if $r \in \{1, (p-1)/2, p-2\}$, whence $\mathcal{W}_{\delta,r}$ has cardinality $2g + 2 = p + 1$. We embed $C_{\delta,r} \hookrightarrow J_{\delta,r}$ with base point ∞ at infinity, and the cuspidal torsion packet is defined as $\mathcal{T}_{\delta,r} = J_{\delta,r}(\overline{\mathbb{Q}})_{\mathrm{tor}} \cap C_{\delta,r}$.

Define the twist map

$$\phi_{\delta,r} : C_{\delta,r} \longrightarrow C_{1,r}, \quad (x, y) \mapsto \left(\frac{x}{\delta}, \frac{y}{\sqrt[p]{\delta^{r+1}}}\right).$$

We also denote by $\phi_{\delta,r}$ the induced twist isomorphism on the Jacobians

$$\phi_{\delta,r} : J_{\delta,r} \longrightarrow J_{1,r}.$$

If $p = 5$, for $1 \leq r \leq 3$, define the following set $\mathcal{S}_{\delta,r} \subset C_{\delta,r}$:

$$\mathcal{S}_{\delta,1} = \left\{ \left(\frac{(1 \pm \sqrt{5})\delta}{2}, -\omega^i \sqrt[5]{\delta^2} \right) : i = 1, \cdots, 5 \right\},$$

$$\mathcal{S}_{\delta,2} = \left\{ \left(\frac{(3 \pm \sqrt{5})\delta}{2}, -\frac{(1 \pm \sqrt{5})\omega^i \sqrt[5]{\delta^3}}{2} \right) : i = 1, \cdots, 5 \right\},$$

$$\mathcal{S}_{\delta,3} = \left\{ \left(-\frac{(1 \pm \sqrt{5})\delta}{2}, -\frac{(1 \pm \sqrt{5})\omega^i \sqrt[5]{\delta^4}}{2} \right) : i = 1, \cdots, 5 \right\},$$

where ω is a primitive 5-th root of unity.

Proposition 2.1. *Suppose $p \geq 5$ is a prime and $1 \leq r \leq p-2$.*

(1) *If* $p = 5$, *then all* $C_{\delta,r}$ *are hyperelliptic, and*

$$\mathcal{T}_{\delta,r} = \mathcal{C}_{\delta,r} \cup \mathcal{W}_{\delta,r} \cup \mathcal{S}_{\delta,r}.$$

(2) *If* $p = 7$ *and* $C_{\delta,r}$ *is not hyperelliptic, then*

$$\mathcal{T}_{\delta,r} = \mathcal{W}_{\delta,r}.$$

(3) *If* $p \geq 7$ *and* $C_{\delta,r}$ *is hyperelliptic, then*

$$\mathcal{T}_{\delta,r} = \mathcal{C}_{\delta,r} \cup \mathcal{W}_{\delta,r}.$$

(4) *If* $p \geq 11$ *and* $C_{\delta,r}$ *is not hyperelliptic, then*

$$\mathcal{T}_{\delta,r} = \mathcal{C}_{\delta,r}.$$

Proof. Look at the commutative diagram with vertical twist isomorphisms

$$\begin{tikzcd} C_{\delta,r} \arrow[r, hook] \arrow[d, "\phi_{\delta,r}"'] & J_{\delta,r} \arrow[d, "\phi_{\delta,r}"] \\ C_{\delta,1} \arrow[r, hook] & J_{\delta,1}. \end{tikzcd}$$

A diagram chasing easily shows that $\phi_{\delta,r}(\mathcal{T}_{\delta,r}) = \mathcal{T}_{1,r}$ and $\phi_{\delta,r}(\mathcal{C}_{\delta,r}) = \mathcal{C}_{1,r}$; Moreover, one has $\phi_{\delta,r}(\mathcal{W}_{\delta,r}) = \mathcal{W}_{1,r}$. Thus when $p \geq 7$ the proposition follows from the corresponding results for the case $\delta = 1$ ([4, §8], [5, Theorem 3], [10, Theorem 1.1] and [16, Theorem 1.1]).

Suppose $p = 5$. It follows from [2, 3] that $\mathcal{T}_{1,1} = \mathcal{C}_{1,1} \cup \mathcal{W}_{1,1} \cup \mathcal{S}_{1,1}$. The following maps

$$(x, y) \mapsto \left(1 - \frac{1}{x}, \frac{y^2}{x}\right), \quad (x, y) \mapsto \left(\frac{1}{x}, -\frac{y}{x}\right)$$

define birational equivalences from the affine model (1.1) of $C_{1,1}$ to those of $C_{1,2}$ and $C_{1,3}$ respectively, and thus induce isomorphisms from $J_{1,1}$ to $J_{1,2}$ and $J_{1,3}$ respectively. Thus the result for $\mathcal{T}_{1,1}$ shows that $\mathcal{T}_{1,r} = \mathcal{C}_{1,r} \cup \mathcal{W}_{1,r} \cup \mathcal{S}_{1,r}$ for $r = 2, 3$. Now the first statement follows by applying the twist map $\phi_{\delta,r}$.

□

3. Points of infinite order

Proposition 3.1. *Suppose $p \geq 5$ is a prime and $\delta \in \mathbb{N}^{(p)} \backslash \{2, 2^{p-2}\}$. Then any point in $\mathcal{T}_{\delta,r} \backslash \mathcal{C}_{\delta,r}$ (if non-empty) is not rational over $\mathbb{Q}$.*

Proof. By Proposition 2.1, if $p \geq 11$ and $C_{\delta,r}$ is not hyperelliptic, then $\mathcal{T}_{\delta,r} \backslash \mathcal{C}_{\delta,r}$ is empty. In the following we distinguish two cases.
(1) $p \geq 5$ and $C_{\delta,r}$ is hyperelliptic. First we prove the Weierstrass points $\mathcal{W}_{\delta,r} \backslash \{\infty\}$ are not rational. Suppose $C_{\delta,r}$ is hyperelliptic, i.e., $r \in \{1, (p-1)/2, p-2\}$. The substitutions

$$u = -y, v = x - \delta/2 \text{ and } u = y/\delta x, v = \left(\delta^{\frac{p-1}{2}} x\right)^{-1} - \left(2\delta^{\frac{p+1}{2}}\right)^{-1}$$

transform the affine models (1.1) of $C_{\delta,1}$ and $C_{\delta,p-2}$ respectively into

$$v^2 = u^p + (\delta/2)^2 \text{ and } v^2 = u^p + \left(4\delta^{p+1}\right)^{-1}. \tag{3.1}$$

In terms of the equations (3.1), the Weierstrass points away from infinity on $C_{\delta,1}$ and $C_{\delta,p-2}$ are given respectively as

$$\left\{\left(-\omega^i \sqrt[p]{(\delta/2)^2}, 0\right) : i = 1, \cdots, p\right\} \text{ and } \left\{\left(-\omega^i \sqrt[p]{\left(4\delta^{p+1}\right)^{-1}}, 0\right) : i = 1, \cdots, p\right\},$$

where ω is a primitive p-th root of unity. It follows from the assumption $\delta \notin \{2, 2^{p-2}\}$ that none of these points are rational over $\mathbb{Q}$. Thus the results for $C_{\delta,1}$ and $C_{\delta,p-2}$ follow.

On the other hand, the substitutions

$$u = \delta - x, v = y^{p-2} x^{-\frac{p-3}{2}} \text{ and } x = \delta - u, y = v^{\frac{p-1}{2}} u^{-\frac{p-3}{2}}$$

define a birational equivalence over $\mathbb{Q}$ of the affine models (1.1) from $C_{\delta,(p-1)/2}$ to $C_{\delta,p-2}$, which is defined at all Weierstrass points away from infinity. Thus the result for $C_{\delta,(p-1)/2}$ follows from that of $C_{\delta,p-2}$.

By Proposition 2.1, if $p \geq 7$ and $C_{\delta,r}$ is hyperelliptic, then $\mathcal{T}_{\delta,r} \backslash \mathcal{C}_{\delta,r} = \mathcal{W}_{\delta,r} \backslash \{\infty\}$; If $p = 5$, then all $C_{\delta,r}$ are hyperelliptic and $\mathcal{T}_{\delta,r} \backslash \mathcal{C}_{\delta,r} = (\mathcal{W}_{\delta,r} \cup \mathcal{S}_{\delta,r}) \backslash \{\infty\}$. Thus the proposition holds when $p \geq 5$ and $C_{\delta,r}$ is hyperelliptic.
(2) $p = 7$ and $C_{\delta,r}$ is not hyperelliptic. In this case, we have $r = 2$ or 4, and by Proposition 2.1, $\mathcal{T}_{\delta,r} \backslash \mathcal{C}_{\delta,r} = \mathcal{W}_{\delta,r} \backslash \mathcal{C}_{\delta,r}$. Since the twist map $\phi_{\delta,r}$:

$C_{\delta,r} \to C_{1,r}$ preserves cuspidal torsion packets, cusps and Weierstrass points,

$$\mathcal{T}_{\delta,r}\backslash\mathcal{C}_{\delta,r} = \phi_{\delta,r}^{-1}(\mathcal{T}_{1,r}\backslash\mathcal{C}_{1,r}) = \phi_{\delta,r}^{-1}(\mathcal{W}_{1,r}\backslash\mathcal{C}_{1,r}).$$

Now assume $r = 2$ and then $C_{1,2}$ is the Klein curve treated in [4, §8]. Let $G \subset \mathrm{Aut}_{\mathbb{C}}(C_{1,2})$ and $P \in C_{1,2}$ be as defined in [4, p. 203], and denote

$$G_\delta = \phi_{\delta,2}^{-1} G \phi_{\delta,2} \subset \mathrm{Aut}_{\mathbb{C}}(C_{\delta,2}), \quad P_\delta = \phi_{\delta,2}^{-1}(P) \in C_{\delta,2}.$$

It follows from the discussion in [4, §8] that $\mathcal{W}_{1,2}\backslash\mathcal{C}_{1,2} = GP$. Thus

$$\mathcal{T}_{\delta,2}\backslash\mathcal{C}_{\delta,2} = \phi_{\delta,2}^{-1}(\mathcal{W}_{1,2}\backslash\mathcal{C}_{1,2}) = G_\delta P_\delta.$$

On the other hand, in terms of the model (1.1), one has

$$P_\delta = \Big(-\delta(\omega+\omega^{-1})^2(\omega^2+\omega^{-2})^3, -\sqrt[7]{\delta^3}(\omega+\omega^{-1})(\omega^2+\omega^{-2})\Big) \in C_{\delta,2},$$

and $G_\delta = \langle\tau\rangle \ltimes \langle\sigma\rangle \subset \mathrm{Aut}_{\mathbb{C}}(C_{\delta,2})$ is a group of order 21, where σ and τ are explicitly given as

$$\sigma(x,y) = (x, \omega y) \text{ and } \tau(x,y) = (\delta^2 x^2 y^{-7}, -\sqrt[7]{\delta^5} x y^{-3}).$$

Here ω denotes a primitive 7-th root of unity. Then a straightforward calculation shows that $\mathcal{T}_{\delta,2}\backslash\mathcal{C}_{\delta,2} = G_\delta P_\delta$ consists of the 21 points of the form

$$\Big(-\delta(\omega^j+\omega^{-j})^2(\omega^{2j}+\omega^{-2j})^3, -\sqrt[7]{\delta^3}\omega^i(\omega^j+\omega^{-j})(\omega^{2j}+\omega^{-2j})\Big)$$

where $i = 1, 2, \cdots, 7$ and $j = 1, 2, 4$.

As for the case $r = 4$, the substitution

$$u = \frac{\delta^2}{x}, v = -\frac{y\sqrt[7]{\delta^9}}{x}$$

defines a birational equivalence between the affine models (1.1) of $C_{\delta,2}$ and $C_{\delta,4}$, from which we can compute that $\mathcal{T}_{\delta,4}\backslash\mathcal{C}_{\delta,4}$ consists of the 21 points of the form

$$\left(-\frac{\delta}{(\omega^j+\omega^{-j})^2(\omega^{2j}+\omega^{-2j})^3}, -\frac{\omega^i\sqrt[7]{\delta^5}}{(\omega^j+\omega^{-j})(\omega^{2j}+\omega^{-2j})^2}\right)$$

where $i = 1, 2, \cdots, 7$ and $j = 1, 2, 4$.

From these explicit coordinates, we conclude the proposition as desired.

□

Prooof of Theorem 1.1. Suppose $\delta \in \mathbb{N}^{(p)} \backslash \{1, 2, 2^{p-2}\}$ and $F_\delta(\mathbb{Q}) \neq \{\infty\}$. Then $\delta = a^p + b^p$ for some $(a, b) \in \mathbb{Q}^{\times 2}$, and let $P = \varphi_{\delta,r}(a, b) \in C_{\delta,r}(\mathbb{Q})$.

The case $p = 3$ is direct. The elliptic curve $C_{\delta,1}$ has Weierstrass equation $v^2 = u^3 + 16\delta^2$. Since $\delta \in \mathbb{N}^{(3)} \backslash \{2\}$, $16\delta^2$ is a square but not a sixth power. Then $C_{\delta,1}(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$ is given by the cusps (for example see [14, Exercise 10.19]). The point $P = \varphi_{\delta,1}(a, b) = (a^3, ab)$ is not a cusp and thus a point of infinite order.

Suppose $p \geq 5$. It suffices to prove that the point P doesn't lie in the cuspidal torsion packet $\mathcal{T}_{\delta,r}$ of $C_{\delta,r}$. First, $P = \varphi_{\delta,r}(a, b) = (a^p, a^r b) \in C_{\delta,r}(\mathbb{Q})$ is always not a cusp for $ab \neq 0$. Since P is a rational point, it follows from Proposition 3.1 that $P \notin \mathcal{T}_{\delta,r}$. Therefore the divisor class $[P - \infty]$ in $J_{\delta,r}(\mathbb{Q})$ has infinite order as desired.

□

References

[1] L. Alpöge and M. Bhargava and A. Shnidman. Integers expressible as the sum of two rational cubes. *arXiv:2210.10730.*

[2] J. Boxall and D. Grant. Examples of torsion points on genus two curves. *Trans. Amer. Math. Soc.*, 352(10):4533–4555, 2000.

[3] R. F. Coleman. Torsion points on Fermat curves. *Compositio Math.*, 58(2):191–208, 1986.

[4] R. F. Coleman. Torsion points on abelian etale coverings of $\mathbb{P}^1 - \{0, 1, \infty\}$. *Trans. Amer. Math. Soc.*, 311(1):185–208, 1989.

[5] R. F. Coleman, A. Tamagawa, and P. Tzermias. The cuspidal torsion packet on the Fermat curve. *J. Reine Angew. Math.*, 496:73–81, 1998.

[6] A. Diaconu and Y. Tian. Twisted Fermat curves over totally real fields. *Annals of Math.*, 162:1353–1376, 2005.

[7] D. K. Faddeev. Invariants of divisor classes for the curves $x^k(1 - x) = y^\ell$. *Trudy Mat. Inst. Steklov.*, 64:284–293, 1961.

[8] D. K. Faddeev. On the divisor class groups of some algebraic curves. *Sov. Math.*, 2(1):67–69, 1961.

[9] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73:349–366, 1983.

[10] D. Grant and D. Shaulis. The cuspidal torsion packet on hyperelliptic Fermat quotients. *Journal de Théorie des Nombres de Bordeaux*,

16:577–585, 2004.

[11] B. H. Gross and D. E. Rohrlich. Some results on the Mordell-Weil group of the Jacobian of the Fermat curve. *Invent. Math.*, (201–224), 1978.

[12] D. E. Rohrlich. The periods of the Fermat curve, appendix to “On the periods of abelian integrals and a formula of Chowla and Selberg”. *Invent. Math.*, 45:193–211, 1978.

[13] J. Shu. Root numbers for the Jacobian varieties of Fermat curves. *J. Number Theory*, 226:243–270, 2021.

[14] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[15] C. L. Stewart and J. Top. On ranks of twists of elliptic curves and power-free values of binary forms. *J. Amer. Math. Soc.*, 8(4):943–973, 1995.

[16] P. Tzermias. Almost rational torsion points and the cuspidal torsion packet on Fermat quotient curves. *Math. Res. Lett.*, (1):99–105, 2007.

Department of Mathematics, Tongji University
Tongji University, Shanghai 200092, China
E-mail address: shujie@tongji.edu.cn

Department of Mathematics, Tongji University
Tongji University, Shanghai 200092, China
E-mail address: wangzikang@tongji.edu.cn