About Jacobians of Fermat cruves

Aleksei Samoilenko

June, 2023

1 Introduction

The decomposition of the Jacobian of the Fermat curve $F(p)$, given by $x^p+y^p = 1$, into simple abelian varieties is known from the works of D. K. Faddeev [1, 2, 3] and is also discussed in the book by S. Lang [4]. The Jacobian $J(F(p))$ is isogenous to

$$\bigoplus_{s=1}^{p-2} J(C_s(p)),$$

where $C_s(p)$ is the *Faddeev curve* defined by the equation $y^p = x^s(1-x)$.

It is known that the varieties $J(C_s(p))$ are absolutely simple, and their algebra of geometric endomorphisms satisfies

$$\mathrm{End}^0_{\mathbb{Q}}\big(J(C_s(p))\big) = \mathbb{Q}(\zeta_p).$$

I have verified that the algebra of endomorphisms defined over $\mathbb{Q}$ is

$$\mathrm{End}^0_{\mathbb{Q}}\big(J(C_s(p))\big) = \mathbb{Q},$$

and I use this to show that these abelian varieties are not modular in the classical sense. This question arose while I was trying to understand the nature of the points constructed by Gross and Rohrlich [5]. Alexander Smirnov suggested that these points could be viewed as Heegner points on the Jacobians of modular curves $J_0(N)$.

Finally, I consider another problem originating from [5], concerning the construction of a conjectural point of infinite order.

2 Over $\mathbb{Q}$

Definition 2.1. An abelian variety A is called *modular over* $\mathbb{Q}$ if there exists a surjective morphism of varieties over $\mathbb{Q}$

$$J_0(N) \longrightarrow A.$$

Definition 2.2. An abelian variety A over $\mathbb{Q}$ is said to be of *GL_2-type* if $\mathrm{End}^0_{\mathbb{Q}}(A)$ is a number field whose degree over $\mathbb{Q}$ equals the dimension of A.

Definition 2.3. Given a newform $f \in S_2^{\mathrm{new}}(N)$, the *modular abelian variety* A_f attached to f is defined as the abelian subvariety

$$A_f = J_0(N)/I_f J_0(N),$$

where I_f is the annihilator of f in the Hecke algebra.

Remark 2.4. The modular abelian variety A_f is defined over $\mathbb{Q}$ - [6].

Theorem 2.5. *Every abelian variety of GL_2-type is isogenous to a modular abelian variety A_f for some modular form f.*

Proof. See Theorem 4.4 in [7]. □

Theorem 2.6.

$$\mathrm{End}_{\mathbb{Q}}\big(J(C_s(p))\big) = \mathbb{Z}.$$

Proof. The Jacobian $J(C_s(p))$ over $\overline{\mathbb{Q}}$ admits complex multiplication induced by the automorphism of the curve

$$(x : y : 1) \longmapsto (x : \zeta_p y : 1).$$

To prove the claim, it suffices to show that any endomorphism not belonging to $\mathbb{Z}$ is not defined over $\mathbb{Q}$. Consider the cotangent bundle of the Jacobian; it possesses a basis consisting of differential forms coming from the curve:

$$\left\{ x^{\langle rm\rangle} y^{\langle sm\rangle} \frac{dy^p}{x^p y^p} \;\middle|\; 1 \le \langle rm\rangle, \langle sm\rangle,\ \langle rm\rangle + \langle sm\rangle \le p-1 \right\},$$

where $\langle x\rangle$ denotes the minimal nonnegative representative of x mod p. The endomorphisms act on these forms as follows:

$$\Big(\sum c_i \zeta_p^i\Big) * x^{\langle rm\rangle} y^{\langle sm\rangle} \frac{dy^p}{x^p y^p} = \sum c_i \zeta_p^i x^{\langle rm\rangle} y^{\langle sm\rangle} \frac{dy^p}{x^p y^p}.$$

If this action were defined over $\mathbb{Q}$, then such forms would have to be invariant under the Galois group. From the formula describing the action of $\mathbb{Z}[\zeta_p]$, it follows that this occurs if and only if the element lies in $\mathbb{Z}$. □

Corollary 2.7. *The Jacobian of the Fermat curve is not modular over $\mathbb{Q}$.*

Proof. Assume that $J(F(p))$ is modular. Then there exists a nontrivial morphism $J_0(N) \to J(F(p))$. By decomposing these Jacobians into simple components and applying Schur's lemma, we obtain that there must exist an isogeny

$$A_f \longrightarrow J(C_s)$$

for some modular abelian variety A_f. However, in this case the corresponding endomorphism algebras would have to be isomorphic, which is impossible since

$$\deg_{\mathbb{Q}}\big(\mathrm{End}^0_{\mathbb{Q}}(A_f)\big) = \dim A_f > 1, \qquad \mathrm{End}^0_{\mathbb{Q}}(J(C_s(p))) = \mathbb{Q}.$$

□

3 Over $\overline{\mathbb{Q}}$

Definition 3.1. An abelian variety A is said to be *modular* over $\overline{\mathbb{Q}}$ if there exists a surjective morphism of varieties over $\overline{\mathbb{Q}}$

$$J_0(N) \longrightarrow A.$$

If the Jacobian of the Fermat curve is modular, then there also exists a nonzero morphism from a modular abelian variety A_f, which is likewise a direct summand, though not necessarily simple.

Theorem 3.2. *If A_f is an abelian variety of CM type, then over $\overline{\mathbb{Q}}$ it is isogenous to a power of an elliptic curve with complex multiplication.*

Proof. Proposition 1.5 in [8]. □

Corollary 3.3. *If the abelian variety A_f in the previous theorem had complex multiplication, then the assumption of modularity would be false.*

Proof. In that case, there would exist an isogeny between an elliptic curve E and $J(C_s)$. Since

$$\dim J(C_s) = g(C_s) = \frac{p-1}{2} \neq 1,\ p > 3$$

we obtain a contradiction. □

Theorem 3.4. *If A_f has no complex multiplication, then the algebra of geometric endomorphisms*

$$\mathrm{End}^0_{\overline{\mathbb{Q}}}(A_f)$$

is a central simple algebra over the totally real subfield

$$\mathrm{End}^0_{\mathbb{Q}}(A_f).$$

Proof. Proposition 1.3 in [9]. The variety A_f is isogenous to a power of a simple abelian variety B. The endomorphism algebra of B is a central division algebra over the totally real subfield $\mathrm{End}^0_{\mathbb{Q}}(A_f)$. □

Corollary 3.5. *If the abelian variety A_f in the previous theorem had no complex multiplication, then the assumption of modularity would again be false.*

Proof. In that case, there would exist an isogeny $B \to J(C_s)$, hence their endomorphism algebras would be isomorphic. However, $\mathbb{Q}(\zeta_p)$ is not central over a totally real field, a contradiction. □

4 Missing Point

The rank computed by Gross and Rohrlich is not the full rank of the Fermat Jacobians; moreover, it equals the full rank only for $p = 11$. For $p = 13$, under the Birch–Swinnerton-Dyer conjecture, there exists exactly one additional point on the Jacobian $J(C_1)$ of the hyperelliptic curve

$$v^{13} = u(1-u) \;\sim\; y^2 = 4x^{13} - 1.$$

For Jacobians of hyperelliptic curves, there exists a useful computational tool called *Mumford coordinates*. My idea was that this formalism might help to find the missing point by brute-force search.

Definition 4.1. *Mumford coordinates* of a divisor on $y^2 = f(x)$ are a pair of polynomials with rational coefficients $a(x), b(x) \in \mathbb{Q}[x]$ such that $\deg b < \deg a$ and $a \mid (f - b^2)$.

Theorem 4.2. *The correspondence between reduced divisors and Mumford coordinates is given as follows:*

$$D \longrightarrow \begin{cases} a(x) = \prod (x - x_i)^{m_i}, \\ b(x) \text{ of degree } < \deg a \text{ interpolating } b(x_i) = y_i, \\ a(x) \mid (f - b^2), \end{cases}$$

where $D = \sum (m_i P_i - m_i \infty)$ *with* $P_i = (x_i, y_i)$.

Conversely,

$$a(x), b(x) \longrightarrow \gcd\big(\operatorname{div}(a(x)), \operatorname{div}(b(x) - y)\big),$$

where

$$\gcd(D_1, D_2) = \sum_P \min(m_P, n_P) P - \sum_P \min(m_P, n_P) \infty.$$

Proof. See, for example, an elementary introduction to hyperelliptic curves [10]. □

Theorem 4.3. *To add two reduced divisors* $D_1 = (a_1(x), b_1(x))$ *and* $D_2 = (a_2(x), b_2(x))$ *in Mumford coordinates, compute*

$$d = \gcd(a_1, a_2, b_1 + b_2), \qquad d = h_1 a_1 + h_2 a_2 + h_3 (b_1 + b_2),$$

and then set

$$a = \frac{a_1 a_2}{d}, \qquad b = \frac{h_1 a_1 b_2 + h_2 a_2 b_1 + h_3 (b_1 b_2 + f)}{d} \pmod{a}.$$

The resulting divisor may not be reduced, so we apply the reduction step:

$$a' = \frac{f - b^2}{a}, \qquad b' = -b \pmod{a'}.$$

Example 4.1. *Let us show that the obvious point $P = (0, 1)$ on the curve $y^2 = 4x^{13} + 1$ provides a torsion generator on the Jacobian. First, this divisor is not principal, since any rational function having poles only at ∞ must be a polynomial in x and therefore has a zero at the conjugate point $\mathfrak{c}P = (0, -1)$. The coordinates of $D = P - \infty$ are $(x, 1)$. We can multiply it repeatedly until the genus $g = 6$, so*

$$7D \leftrightarrow (x^7, 1).$$

Reducing gives $(x^6, -1)$; continuing up to $13D$, we obtain

$$13D \leftrightarrow (x, -1) + (x, +1) = (1, -1) \leftrightarrow 0.$$

Remark 4.4. I attempted to find the missing point in Mumford coordinates and to verify that it corresponds to a point of infinite rank, using the known addition law and the fact that $J(C_1)_{\text{tors}} = \mathbb{Z}/13\mathbb{Z}$. However, my computations on a laptop were limited to a small search range.

5 Further research

By Belyi's theorem, every algebraic curve of genus $g > 1$ defined over a number field can be uniformized as a quotient of the upper half-plane $\mathcal{H}$ by some subgroup $\Gamma \subset SL_2(\mathbb{Z})$. However, this subgroup need not be congruence.

In the case of the Fermat curve, one can consider the subgroup

$$\Phi(N) = \langle A^N, B^N, [\Phi, \Phi] \rangle,$$

where A and B are free generators of the rank-two free group Φ. Thus $\Phi(N)$ is the unique normal subgroup of Φ such that

$$\Phi/\Phi(N) \simeq (\mathbb{Z}/N\mathbb{Z})^2.$$

It is known that, in the natural realization of $\Phi(N)$ as a subgroup of the Sanov subgroup $\Gamma(2) \subset SL_2(\mathbb{Z})$, which is free on

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix},$$

$\Phi(N)$ is *noncongruence* except for $N = 2, 4, 8$.

This raises the following question: can one define a meaningful notion of *noncongruence Heegner points*, and do such points enjoy arithmetic properties analogous to the classical Heegner points on modular curves? In particular, could the point constructed by Gross and Rohrlich be interpreted as a Heegner-type point in this noncongruence setting?

References

[1] D. K. Faddeev, "On the divisor class group on the curve $x^4 + y^4 = 1$," *Doklady Akademii Nauk SSSR*, **134**:4 (1960), 776–777. (in Russian)

[2] D. K. Faddeev, "On the divisor class group on certain algebraic curves," *Doklady Akademii Nauk SSSR*, **136**:2 (1961), 296–298. (in Russian)

[3] D. K. Faddeev, "On the invariants of divisor classes for the curves $x^k(1-x) = y^l$ in the l-adic cyclotomic field," *Trudy Matematicheskogo Instituta imeni V. A. Steklova*, **64**, Academy of Sciences of the USSR, Moscow, 1961, 284–293. (in Russian)

[4] S. Lang, *Introduction to Algebraic and Abelian Functions*, 2nd ed., Springer, 1982.

[5] B. Gross and D. Rohrlich, "Some results on the Mordell–Weil group of the Jacobian of the Fermat curve," *Inventiones Mathematicae*, **44** (1978), 201–224.

[6] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.

[7] K. A. Ribet, "Abelian varieties over $\mathbb{Q}$ and modular forms," in *Proceedings of the KAIST Mathematics Workshop*, Korea Advanced Institute of Science and Technology, Taejon, 1992, pp. 53–79.

[8] G. Shimura, "Class fields over real quadratic fields and Hecke operators," *Annals of Mathematics*, **95**:1 (1972), 130–190.

[9] E. E. Pyle, "Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components," in *Modular Curves and Abelian Varieties*, eds. J. E. Cremona, J. C. Lario, J. Quer, and K. A. Ribet, Progress in Mathematics, vol. 224, Birkhäuser, Basel, 2004.

[10] A. J. Menezes, Y.-H. Wu, and R. J. Zuccherato, "An Elementary Introduction to Hyperelliptic Curves," November 7 1996.