Advanced Studies in Pure Mathematics 63, 2012
Galois–Teichmüller Theory and Arithmetic Geometry
pp. 449–456

An abelian surface with constrained 3-power torsion

Christopher Rasmussen

Abstract.

In my talk at the Galois Theoretic Arithmetic Geometry meeting, I described recent joint work with Akio Tamagawa on a finiteness conjecture regarding abelian varieties whose ℓ-power torsion is constrained in a particular fashion. In the current article, we introduce the conjecture and provide some geometric motivation for the problem. We give some examples of the exceptional abelian varieties considered in the conjecture. Finally, we prove a new result—that the set $\mathscr{A}(\mathbb{Q}, 2, 3)$ of $\mathbb{Q}$-isomorphism classes of dimension 2 abelian varieties with constrained 3-power torsion is non-empty, by demonstrating an explicit element of the set.

§1. Introduction

Let ℓ be a prime number, and let

$$\rho_\ell \colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Out}\big(\pi_1(\mathbb{P}^1_{01\infty})\big) \tag{1}$$

be the canonical outer pro-ℓ Galois representation on the fundamental group of $\mathbb{P}^1_{01\infty}$, the projective line with three points deleted. The kernel of ρ_ℓ corresponds to a subfield $\text{山}(\ell) \subseteq \bar{\mathbb{Q}}$, which is known to be a pro-ℓ extension of $\mathbb{Q}(\mu_{\ell^\infty})$, unramified outside ℓ [AI88].

For any number field k, let $\text{天}(k, \ell)$ denote the *maximal* pro-ℓ extension of $k(\mu_{\ell^\infty})$ which is unramified away from ℓ. We write simply 山 for $\text{山}(\ell)$ and 天 for $\text{天}(k, \ell)$ if there is no confusion.[1] If $k \subset \text{山}$, then we have $\text{天}(k, \ell) = \text{天}(\mathbb{Q}, \ell)$. Of course, we have the containment $\text{山} \subseteq \text{天}$.

In [Iha86], Ihara asked whether the fields 山 and 天 coincide; this question is still open. The kanji character 山, *san*, has the meaning

Received March 31, 2011.
Revised September 28, 2011.
2010 *Mathematics Subject Classification.* Primary 14H30; Secondary 11G10, 11G32.

[1] In earlier papers by the author, the field $\text{山}(\ell)$ was denoted Ω_ℓ and the field $\text{天}(\mathbb{Q}, \ell)$ was denoted Λ_ℓ.

'mountain.' The character 天, *ten*, has the meaning 'heaven.' Ihara's question asks whether two large and natural extensions, one known to be contained in the other, happen to coincide. The notation used here tries to capture the spirit of Ihara's question in the following form: *Does the mountain reach the heavens?* If Ihara's question may be affirmed, then any subfield of 天 should also appear in 山. Here, we consider one natural source of subfields of 天—namely, the fields of ℓ-power torsion of cetain Jacobian varieties which we now describe.

Suppose that $k \subseteq$ 山 is a number field and C/k is a complete nonsingular curve. We say that C admits the structure of a *geometric ℓ-cover* of $\mathbb{P}^1_{01\infty}$ if there exists a morphism $f\colon C \to \mathbb{P}^1$, defined over $\bar{\mathbb{Q}}$, with the following property: The Galois closure of $f \otimes \bar{\mathbb{Q}}$ has degree a power of ℓ, and branches only over the set $\{0, 1, \infty\}$.

Suppose C/k admits the structure of a geometric ℓ-cover of $\mathbb{P}^1_{01\infty}$. Then C must obtain good reduction away from ℓ over some finite extension of the field of definition of the covering $f\colon C \to \mathbb{P}^1$ (see, for example, [Liu03, Theorem. 2.12] or [Wew05, Theorem. 1.2]). For simplicity, let us assume C/k already possesses good reduction away from ℓ. Let J denote the Jacobian variety of C. By [Mil86, Corollary 12.3]), J has good reduction away from ℓ also, and so the extension $k(J[\ell^\infty])/k(J[\ell])$ is pro-ℓ and unramified outside ℓ. Hence, if $J[\ell]$ is rational over 天, then $k(J[\ell^\infty]) \subseteq$ 天.

In [AI88], Anderson and Ihara give conditions on C which imply the containment $k(J[\ell^\infty]) \subseteq$ 山. Given a geometric ℓ-cover satisfying $k(J[\ell]) \subseteq$ 天, one may then test Ihara's question with these conditions. This has been carried out in several cases; more details are given below. However, outside of a few well-known families of geometric ℓ-covers, it is not so easy to produce curves with the requisite properties. Of course, the Jacobian of such a curve is simply an abelian variety satisfying a certain arithmetic constraint. It appears this arithmetic constraint is rather strong, which motivates the following conjecture.

If A/k is an abelian variety, let $[A]$ denote its k-isomorphism class. We define the following sets: For any prime ℓ, any number field k, and any $g \geq 0$, let

$$\mathscr{A}(k, g, \ell) := \{[A] : A/k \text{ has dimension } g \text{ and } k(A[\ell^\infty]) \subseteq \text{天}\}. \tag{2}$$

Next, set

$$\mathscr{A}(k, g) := \{([A], \ell) : [A] \in \mathscr{A}(k, g, \ell)\}. \tag{3}$$

At least in theory, a class $[A]$ might belong to $\mathscr{A}(k, g, \ell)$ for more than one value of ℓ, if A/k has everywhere good reduction. The reader is

cautioned *not* to assume the map

$$\mathscr{A}(k,g) \to \bigcup_{\ell} \mathscr{A}(k,g,\ell), \qquad ([A],\ell) \mapsto [A] \tag{4}$$

is a bijection!

For any choice of k, g, and ℓ, the set $\mathscr{A}(k,g,\ell)$ is finite. If $[A] \in \mathscr{A}(k,g,\ell)$, then the dimension and field of definition of A are fixed, and the primes of bad reduction are restricted to the finite set of primes $\mathfrak{l}$ of k over ℓ. Hence, by the Shafarevich Conjecture, only finitely many such classes exist. However, one expects more. In [RT08], the following conjecture is presented:

Conjecture 1. *For any fixed k and $g \geq 0$, the set $\mathscr{A}(k,g)$ is finite.*

In my talk at the conference, I discussed the following results, which will appear in a joint paper with Tamagawa:

Theorem 1 (R.–Tamagawa). *Let k be a number field and $g \geq 0$. Under assumption of the Generalized Riemann Hypothesis, the set $\mathscr{A}(k,g)$ is finite.*

Theorem 2 (R.–Tamagawa). *Without assuming the Generalized Riemann Hypothesis, the set $\mathscr{A}(k,g)$ is finite in the following cases:*

- *$k = \mathbb{Q}$, $g \leq 3$;*
- *$[k:\mathbb{Q}] \leq 3$, $g = 1$;*
- *$k/\mathbb{Q}$ a Galois extension of exponent 3 and $g = 1$.*

The finiteness of $\mathscr{A}(\mathbb{Q},1)$ is given in [RT08], along with an explicit computation of the set $\mathscr{A}(\mathbb{Q},1)$. In the spirit of Ihara's question, one may also consider whether $\mathbb{Q}(E[\ell^\infty]) \subseteq$ 山 for $[E] \in \mathscr{A}(\mathbb{Q},1)$, and with at most two exceptions, this is known to be true. In general, proving $\mathbb{Q}(A[\ell^\infty]) \subseteq$ 山 is quite a delicate question. The case of elliptic curves over $\mathbb{Q}$ was handled by using the special fact that almost all such curves either admit the structure of a geometric ℓ-cover, or possess complex multiplication—see [RT08] for details.

§2. The criterion of Anderson and Ihara

Again, we assume $k \subset$ 山 is a number field. Let C/k be a curve which admits the structure of a geometric ℓ-cover, and let J denote its Jacobian variety. Anderson and Ihara have demonstrated a sufficient criterion under which J satisfies the condition $k(J[\ell^\infty]) \subseteq$ 山. (Of course, this is only a stronger condition than containment in 天 if the answer to Ihara's question is negative.)

Let Δ denote the field of Puiseux series over $\mathbb{Q}$ in the parameter $\frac{1}{\tau}$:

$$\Delta := \mathbb{Q}((\tfrac{1}{\tau}))[\tau^r : r \in \mathbb{Q}]. \tag{5}$$

Here is Anderson and Ihara's result [AI88]:

Proposition 1. *Suppose C/k admits the structure of a geometric ℓ-cover via the morphism $f\colon C \to \mathbb{P}^1$, which is defined over* 凵. *Moreover, suppose there exists a point $y \in C(\text{凵}\cdot\Delta)$ such that $f(y) = \tau \in \mathbb{P}^1(\bar{\mathbb{Q}}\cdot\Delta)$. Then $J[\ell^\infty]$ is rational over* 凵, *and so also* 天.

Consequently, these Jacobians give explicit elements of $\mathscr{A}(k, g, \ell)$ when the criterion can be verified. We give a few examples. The Jacobian J_F of the Fermat curve

$$F\colon X^{\ell^n} + Y^{\ell^n} = Z^{\ell^n} \tag{6}$$

necessarily satisfies $[J_F] \in \mathscr{A}(\mathbb{Q}, \frac{1}{2}(\ell^n - 1)(\ell^n - 2), \ell)$. Of course, the decomposition of this Jacobian into simple abelian varieties gives abelian varieties of smaller dimensions g' which necessarily fall into classes of $\mathscr{A}(\mathbb{Q}, g', \ell)$. Anderson and Ihara give two other families of examples: the Heisenberg curves of level ℓ^n for any prime ℓ, and the principal modular curves of level 2^n (for $\ell = 2$).

In [Ras04], it is shown that every elliptic curve $E/\mathbb{Q}$ with good reduction away from 2 admits the structure of a geometric 2-cover, and satisfies $\mathbb{Q}(E[2^\infty]) \subset$ 凵. On the other hand, if ζ_n is a primitive 2^n-th root of unity, then the curve

$$E_n\colon y^2 = x(x + \zeta_n)(x - (1 - \zeta_n)) \tag{7}$$

satisfies $[E_n] \in \mathscr{A}(\mathbb{Q}(\zeta_n), 1, 2)$, but is not defined over $\mathbb{Q}(\zeta_{n-1})$ [Ras04]. Thus, we have an infinite ascending chain of sets, with each containment proper:

$$\mathscr{A}(\mathbb{Q}, 1, 2) \subset \mathscr{A}(\mathbb{Q}(\mu_4), 1, 2) \subset \mathscr{A}(\mathbb{Q}(\mu_8), 1, 2) \subset \cdots. \tag{8}$$

Thus, even though the sets $\mathscr{A}(k, g, \ell)$ are finite, they may be arbitrarily large.

In general, our knowledge of the sets $\mathscr{A}(k, g)$ is decidedly murky beyond these finiteness results. In [RT08], it is shown that $\mathscr{A}(\mathbb{Q}, 1, \ell) = \varnothing$ for every $\ell > 163$. This is done by identifying elements of $\mathscr{A}(\mathbb{Q}, 1, \ell)$ with noncuspidal points of $X_0(\ell)(\mathbb{Q})$, and appealing to Mazur's classification [Maz78]. Similar bounds for ℓ such that the sets $\mathscr{A}(k, 1, \ell)$ are empty, where $[k : \mathbb{Q}] = 2$ and k is not an imaginary quadratic extension of class number one, are *almost* available—there are effective estimates, with the exception of at most one prime. See [Mom95] for details.

§3. A New Example

Even for a particular choice of k, g, and ℓ, it can be nontrivial to determine whether $\mathscr{A}(k, g, \ell)$ is nonempty. There is one trivial construction for elements in this set; suppose that $\mathscr{A}(k, 1, \ell)$ is non-empty. Selecting g classes $[E_i] \in \mathscr{A}(k, 1, \ell)$ (possibly with repetition), we certainly find $[E_1 \times \cdots \times E_g] \in \mathscr{A}(k, g, \ell)$.

In this fashion, we see immediately that $\mathscr{A}(\mathbb{Q}, 2, 3)$ is non-empty, as it contains the classes of all products $[E \times E']$ for $[E], [E'] \in \mathscr{A}(\mathbb{Q}, 1, 3)$. Here we demonstrate a more interesting class in $\mathscr{A}(\mathbb{Q}, 2, 3)$, by constructing an explicit example of a curve of genus 2 which admits the structure of a geometric 3-cover.

Michael Stoll has computed a list of curves of genus two with odd discriminant.[2] We consider the following curve from Stoll's list, which has discriminant $6561 = 3^8$. Let C be the normalization of the projective curve given by the equation:

$$Y^2Z^4 + (YZ^2 + X^3)(X^3 + Z^3) = 0. \tag{9}$$

The curve given by this equation is nonsingular everywhere except at the point $\infty^* = [0 : 1 : 0]$. With respect to the affine coordinates $x = X/Z, y = Y/Z$, the curve has a smooth affine equation given by

$$C_0 \colon y^2 + y(x^3 + 1) + x^3(x^3 + 1) = 0.$$

On the other hand, with respect to $w = X/Y$, $z = Z/Y$, the affine equation

$$C_1 \colon z^4 + z^2w^3 + w^6 + z^5 + w^3z^3 = 0$$

contains the singular point ∞^*, given by $(0, 0)$ on C_1. After blowing up, we find an affine chart for the normalization:

$$C_2 \colon s^4u^3 + s^3u^3 + s^2 + s + 1 = 0.$$

The point ∞^* of C_1 corresponds to the two nonsingular points $\infty_1 = (\omega, 0)$ and $\infty_2 = (\omega^2, 0)$ of C_2, where ω is a primitive cube root of unity. A birational mapping between C_2 and C_0 is given by

$$x = \frac{1}{us}, y = \frac{1}{u^3s^2}.$$

[2] At the time of this article, the data was available at Stoll's web site; see `http://www.faculty.jacobs-university.de/mstoll/data`.

Proposition 2. *Let J denote the Jacobian variety of C. Then $[J] \in \mathscr{A}(\mathbb{Q}, 2, 3)$. In fact, J satisfies the (possibly) stronger condition*

$$\mathbb{Q}(J[3^\infty]) \subseteq \text{山} = \text{山}\,(3). \tag{10}$$

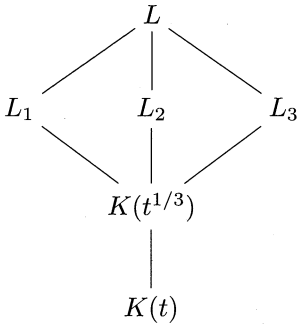
Proof. We must demonstrate a geometric 3-covering $f\colon C \to \mathbb{P}^1$ which satisfies the criterion of Anderson and Ihara. We let $f = g^3$, where

$$g = -\frac{y + x^3}{x^3} = -(s + 1).$$

It is not hard to check that $(g) = 3(P_1) - 3(P_2)$, where on C_0, these points are given by $P_1 = (0, 0)$, $P_2 = (0, -1)$. Moreover, the function g is totally ramified at the four points P_1, P_2, ∞_1, ∞_2 and unramified elsewhere. Consequently, f is a degree 9 map branched only over the three point set $\{0, 1, \infty\}$.

We need to be sure that the Galois closure of $f \otimes \bar{\mathbb{Q}}$ has 3-power degree. Let $K = \mathbb{Q}(\omega)$, and let t be a generator for the function field $f^*K(\mathbb{P}^1)$; that is, $t = f(x, y)$. We have the following field diagram:

(11)



Here, $L_1 = K(C) = K(x, y) = K(x, t)$. The minimal polynomial for x over $K(t)$ is

$$m_{x,K(t)}(X) = X^9 + \frac{3t}{(t-1)^2}X^3 - \frac{t}{(t-1)^2}. \tag{12}$$

Moreover, over the field $K(t^{1/3})$, $m_{x,K(t)}(X)$ splits into three cubic factors, as:

$$\begin{aligned} m_{x,K(t)}(X) = &\left(X^3 - \frac{t^{2/3} - t^{1/3}}{t-1}\right)\left(X^3 - \frac{\omega^2 t^{2/3} - \omega t^{1/3}}{t-1}\right) \\ &\cdot \left(X^3 - \frac{\omega t^{2/3} - \omega^2 t^{1/3}}{t-1}\right). \end{aligned} \tag{13}$$

Denote these cubic factors by m_1, m_2, and m_3, labeled so that x is a root of m_1. Each of the m_i is an irreducible polynomial in $K(t^{1/3})[X]$, and L_1 coincides with the splitting field of m_1 over $K(t^{1/3})$. Similarly, for $i = 2, 3$, we let L_i denote the splitting field of m_i over $K(t^{1/3})$. The Galois closure of $L_1/K(t)$ is the compositum $L := L_1L_2L_3$. The extension $L_1/K(t)$ is a tower of 3-extensions, and (as $\omega \in K$), we are guaranteed the Galois closure L has 3-power degree over $K(t)$. Hence, the covering f is a geometric 3-cover.

We now must verify the condition on Puiseux series for the covering f. That is, we must demonstrate a point $(\tilde{x}, \tilde{y}) \in C(\text{凵} \cdot \Delta)$ which satisfies $f(\tilde{x}, \tilde{y}) = \tau \in \mathbb{P}^1(\Delta)$. This is an easy calculation. For example, the following point satisfies the condition:

$$
\begin{aligned}
\tilde{x} &= \tau^{1/9}\frac{(1-\tau^{1/3})^{1/3}}{(1-\tau)^{1/3}} \\
&= \tau^{1/9}\cdot\left(1-\frac{1}{3}\tau^{1/3}-\frac{1}{9}\tau^{2/3}+\frac{22}{81}\tau+\cdots\right), \\
\tilde{y} &= -\tau^{1/3}\frac{(1-\tau^{2/3})}{1-\tau} \\
&= \tau^{1/3}\left(-1+\tau^{2/3}-\tau+\tau^{5/3}+\cdots\right).
\end{aligned}
\tag{14}
$$

Q.E.D.

Remark. In fact, the geometric automorphism group G of the curve C is the dihedral group of 12 elements. The group G possesses several elements of order two besides the hyperelliptic involution. However, none of these additional order two automorphisms are $\mathbb{Q}$-rational. Let φ_1, φ_2 be two such automorphisms, which generate a Klein four group inside of G. Then the quotients $E_i := C/\varphi_i$ are elliptic curves, and necessarily J is isogenous to $E_1 \times E_2$ [Igu60, p. 648]. However, these curves are not defined over $\mathbb{Q}$. Hence, the class $[J]$ still provides an "interesting example" in the sense described at the start of this section.

Acknowledgments. I would like to thank the referee for his or her very helpful comments on this paper. In addition, I am grateful to Cam McLeman for many helpful discussions, and to the conference organizers for their generous invitation to participate. My participation was supported in part by a grant from the National Science Foundation (DMS 1044746).

References

[AI88] G. Anderson and Y. Ihara, Pro-ℓ branched coverings of $\mathbf{P}^1$ and higher circular ℓ-units, Ann. of Math. (2), **128** (1988), 271–293.

[Igu60] J. Igusa, Arithmetic variety of moduli for genus two, Ann. of Math. (2), **72** (1960), 612–649.

[Iha86] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math. (2), **123** (1986), 43–106.

[Liu03] Q. Liu, Reduction and lifting of finite covers of curves, In: Proceedings of the 2003 Workshop on Cryptography and Related Mathematics, Chuo Univ., 2003, pp. 161–180, available at `http://www.math.u-bordeaux.fr/~liu`.

[Maz78] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math., **44** (1978), 129–162.

[Mil86] J. S. Milne, Jacobian varieties, In: Arithmetic Geometry, Storrs, Conn., 1984, Springer-Verlag, 1986, pp. 167–212.

[Mom95] F. Momose, Isogenies of prime degree over number fields, Compositio Math., **97** (1995), 329–348.

[Ras04] C. Rasmussen, On the fields of 2-power torsion of certain elliptic curves, Math. Res. Lett., **11** (2004), 529–538.

[RT08] C. Rasmussen and A. Tamagawa, A finiteness conjecture on abelian varieties with constrained prime power torsion, Math. Res. Lett., **15** (2008), 1223–1232.

[Wew05] S. Wewers, Stable reduction of three point covers, J. Théor. Nombres Bordeaux, **17** (2005), 405–421.

Department of Mathematics & Computer Science
Wesleyan University
Middletown, Connecticut 06459
U.S.A.
E-mail address: `crasmussen@wesleyan.edu`