TAME TORSION AND ENDMORPHISMS

MATTHEW BISATT

Abstract. Fix a positive integer $g$ and rational prime $p$. We prove the existence of a genus $g$ curve $C/\mathbb{Q}$ such that the mod $p$ representation of its Jacobian is tame by imposing conditions on the endomorphism algebra.

1. Introduction

Let $C/\mathbb{Q}$ be a nice curve of genus $g$ with Jacobian $J_C$. Fix a prime $p$. Then it is well known that the subgroup of points of $J_C$ of order dividing $p$, $J_C[p]$, defines a finite Galois extension $\mathbb{Q}(J_C[p])/\mathbb{Q}$. We would like to control the ramification of this extension as much as possible.

We say that a number field $F$ is tame (resp. unramified) if $F/\mathbb{Q}$ is tamely ramified (resp. unramified) at every finite prime of $F$. Throughout, we will always write $\zeta_m$ for a primitive $m$-th root of unity.

Remark 1.1. Let $\zeta_p$ be a primitive $p$-th root of unity. Recall that by the Weil pairing, we have $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(J_C[p])$. If $p$ is odd, then $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is (tamely) ramified at $p$ and hence $\mathbb{Q}(J_C[p])$ cannot be unramified over $\mathbb{Q}$.  

If $p = 2$, then we can ensure that $\mathbb{Q}(J_C[2]) = \mathbb{Q}$ (which is unramified), for example by using the genus $g$ hyperelliptic curve $C : y^2 = \prod_{j=0}^{2g} (x - j)$.

In this short note, we shall discuss the question of whether we can make the extension $\mathbb{Q}(J_C[p])$ tame. In particular, we prove the following result:

Theorem 1.2. Fix a positive integer $g$ and rational prime $p$. Then there exists a nice curve $C/\mathbb{Q}$ of genus $g$ such that $\mathbb{Q}(\text{Jac}(C)[p])/\mathbb{Q}$ is tame.

Remark 1.3. Before we start proving Theorem 1.2, we note that there is an alternative proof in [BD] with an identical approach for $\ell \neq p$. However the approach for $\ell = p$ is substantially different; they use the theory of Mumford curves whereas here we will impose restrictions on the endomorphism algebra. Moreover, they treat the case $p = 2$ separately which is not necessary here.

Layout of the paper. In [B], we give Kisin’s result on local constancy in $p$-adic families which enables us to reduce our global problem to a local

\begin{itemize}
\item[\textit{Date:}] December 18, 2019.
\item[\textit{Remark 1.1.}] In fact, the only unramified number field is $\mathbb{Q}$ by the theorem of Hermite–Minkowski.
\end{itemize}
problem, and provide a proof assuming the endomorphism ring of a particular family of curves. In §3, we recap the theory of abelian varieties with complex multiplication and explain how this enables us to ensure tame ramification at $p$. We then give an explicit family of curves whose Jacobians have suitable endomorphism rings in §4 which completes the proof of Theorem 1.2.

Acknowledgements. We would like to thank Vladimir Dokchitser for suggesting this approach and helpful conversations.

2. Local strategy

We now discuss conditions to ensure that $\mathbb{Q}(J_{C}[p])/\mathbb{Q}$ is tame. Our approach will be to impose some local conditions on $C$ in order to guarantee tameness at each prime and then apply the following result of Kisin which allows us to amalgamate these local conditions using the Chinese remainder theorem.

**Theorem 2.1.** Let $\ell$ be a prime. Let $C_f : y^2 = f(x)$ be a hyperelliptic curve, with $f \in \mathbb{Z}_\ell[x]$ squarefree. For every $m \geq 1$, there exists $N \geq 1$ such that if $\tilde{f} \equiv f \mod \ell^N$ then $C_{\tilde{f}} : y^2 = \tilde{f}(x)$ is a hyperelliptic curve with

$$\text{Jac}(C_f)[m] \cong \text{Jac}(C_{\tilde{f}})[m]$$

as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\ell)$-modules.

**Proof.** This is a special case of [Kis99, Theorem 5.1(1)]. Note that for $N$ large enough, all $\tilde{f} \equiv f \mod p^N$ have the same degree as $f$ and are squarefree, and so define a $p$-adic family of hyperelliptic curves of the same genus. □

We begin with giving the local conditions away from $p$.

**Lemma 2.2.** Fix a rational prime $p$. Let $C/\mathbb{Q}$ be a genus $g$ curve with Jacobian $J_C$ such that:

(i) $C$ has good reduction at all $\ell \leq 2g + 1, \ell \neq p$;

(ii) $\mathbb{Q}_p(J_C[p])/\mathbb{Q}_p$ is tamely ramified.

Then $\mathbb{Q}(J_C[p])/\mathbb{Q}$ is tame.

**Proof.** We have to show that $\mathbb{Q}(J_C[p])/\mathbb{Q}$ is tamely ramified at $\ell$ for all primes $\ell \neq p$. If $\ell \leq 2g + 1$ then $C$, and hence $J_C$, has good reduction at $\ell$ by assumption. The criterion of Néron–Ogg–Shafarevich then implies that $\mathbb{Q}(J_C[p])/\mathbb{Q}$ is unramified at $\ell$. On the other hand, if $\ell > 2g + 1$, then the extension is always tamely ramified at $\ell$ by a result of Serre–Tate [ST68, p.497]. □

It remains to provide a condition at $p$ to ensure tameness. We do this using endomorphism algebras through the following result.
Theorem 2.3 (=Theorem 4.3). Fix a positive integer $g$ and rational prime $p$. Choose $n \in \{2g+1, 2g+2\}$ such that $p \nmid n$. Let $C_n/\mathbb{Q}$ be the hyperelliptic curve $y^2 = x^n - 1$ with Jacobian $J_n$. Then $\mathbb{Q}_p(J_n[p])/\mathbb{Q}_p$ is tamely ramified.

We are now in a position to prove Theorem 1.2, assuming the above theorem. The remainder of the paper will then be dedicated to providing a proof of Theorem 2.3.

Proof of Theorem 1.2. We will construct a family of hyperelliptic curves $C_f : y^2 = f(x)$ of genus $g$ which satisfy this condition, where $\deg(f) = 2g+2$.

For primes $\ell \leq 2g+1$, $\ell \neq p$ choose a polynomial $f_\ell(x)$ of degree $2g+2$ such that $C_{f_\ell}$ has good reduction at $\ell$ (in the case of $\ell = 2$, explicit conditions are given in [AD19, Lemma 7.7]). Note that if $f \equiv f_\ell \mod \ell$, then the discriminants of $C_f$ and $C_{f_\ell}$ are equal mod $\ell$ and hence $C_f$ will also have good reduction at $\ell$.

For $\ell = p$, choose $n \in \{2g+1, 2g+2\}$ such that $p \nmid n$ and suppose $f \equiv x^n - 1 \mod p^N$ where $N$ is as in Theorem 2.1 (if necessary, change $C_n : y^2 = x^n - 1$ to an even degree model). Now let $f(x)$ be a squarefree polynomial of degree $2g+2$ satisfying the above congruence conditions and let $C_f : y^2 = f(x)$. Then by Theorem 2.1 and Theorem 2.3, $\mathbb{Q}_p(J_{C_f}[p])/\mathbb{Q}_p$ is tamely ramified. The result now follows from Lemma 2.2. □

Remark 2.4. Observe that for $p \neq 2$, the hyperelliptic curve $C_n$ has good reduction at $p$ for $p \nmid n$. Hence it is possible to extend this approach to constructing curves $C/F$ such that $\mathbb{Q}(C[m])/\mathbb{Q}$ is tame whenever $m$ is odd and squarefree. We do not prove this more general statement here however but instead refer the reader to [BD].

3. Abelian varieties with complex multiplication

In order to obtain a sufficiently large endomorphism ring, we consider abelian varieties with complex multiplication. In this section, we will provide the relevant background and show how this can give us the tame torsion result we want; in the next section will realise this as the Jacobian of a curve.

Definition 3.1. Let $A/\mathbb{Q}_p$ be an abelian variety of dimension $g$. Let $F$ be an étale $\mathbb{Q}$-algebra of dimension $2g$. We say that $A$ has complex multiplication by an order $R \subset F$ if

$$\text{End}_{\mathbb{Q}_p}(A) \cong R.$$ 

Note that if $A/\mathbb{Q}_p$ is absolutely simple, then $F$ is a number field and $R$ has finite index inside the ring of integers $\mathcal{O}_F$. The benefit of having lots of endomorphisms is that it heavily restricts the possible choices of $\mathbb{Q}_p(A[p])$; in fact, the Galois group of the $p$-torsion field is abelian once all the endomorphisms are defined over the base field of $A$.

Theorem 3.2 ([ST68, p.502]). Let $\mathcal{K}/\mathbb{Q}_p$ be a finite extension and let $A/\mathcal{K}$ be an abelian variety with complex multiplication by $R \subset F$. Suppose that
all endomorphisms of $A$ are defined over $\mathcal{K}$, i.e. $\text{End}_\mathcal{K}(A) = \text{End}_{\mathbb{Q}_p}(A)$. Let $p$ be a prime and let $\rho$ be the mod $p$ Galois representation of $A/\mathcal{K}$. Then $\text{Im}(\rho) \subset (R \otimes \mathbb{Z}_p)^\times$.

We will restrict to the setting where $R = \mathcal{O}_F$ is integrally closed in $F$ which guarantees that $A[p]$ is a free module of rank 1 over $\mathcal{O}_F \otimes \mathbb{Z}_p$. This also enables us to compute $\mathcal{O}_F \otimes \mathbb{Z}_p$ explicitly.

**Lemma 3.3.** Let $F$ be a number field and let $p$ be a prime. Then

$$\mathcal{O}_F \otimes \mathbb{Z}_p \cong \prod_{v|p} \mathbb{F}_v[e],$$

where $\mathbb{F}_v$ is the residue field of $\mathcal{O}_F$ at $v$, $e(v|p)$ is the ramification degree and the product is over places $v$ of $F$ dividing $p$.

**Proof.** This follows from the fact that $\mathcal{O}_F \otimes \mathbb{Z}_p \cong \mathcal{O}_F/p\mathcal{O}_F$. □

In general $F = \prod F_i$ will be a finite product of number fields, so we will write $\mathcal{O}_F = \prod \mathcal{O}_{F_i}$ for the maximal order of $F$.

**Lemma 3.4.** Let $A/\mathbb{Q}_p$ be an abelian variety with complex multiplication by the ring of integers $\mathcal{O}_F$ of an étale $\mathbb{Q}$-algebra $F = \prod F_i$ with $F_i$ number fields. Let $\mathcal{K}/\mathbb{Q}_p$ be a finite extension such that $\text{End}_\mathcal{K}(A) = \text{End}_{\mathbb{Q}_p}(A)$.

Suppose that:

(i) $p$ is unramified in $F_i/\mathbb{Q}$ for all $i$;

(ii) $\mathcal{K}/\mathbb{Q}_p$ is tamely ramified.

Then $\mathbb{Q}_p(A[p])/\mathbb{Q}_p$ is tamely ramified.

**Proof.** We prove the stronger statement that $\mathcal{K}(A[p])/\mathbb{Q}_p$ is tamely ramified. By our assumption, it suffices to show that $\mathcal{K}(A[p])/\mathcal{K}$ is tamely ramified. Since $A$ has complex multiplication by $\mathcal{O}_F$, $\text{Gal}(\mathcal{K}(A[p])/\mathcal{K})$ is contained in a subgroup of $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$ by Theorem 3.2. However, $\mathcal{O}_F \otimes \mathbb{Z}_p$ is a product of finite fields of characteristic $p$ by Lemma 3.3 since $p$ is unramified in $F_i$ for all $i$. Hence $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$ has order coprime to $p$.

Therefore the order of $\text{Gal}(\mathcal{K}(A[p])/\mathcal{K})$ is also coprime to $p$ and hence the extension is tamely ramified at $p$ as the image of wild inertia is a $p$-group. □

### 4. Constructing the endomorphism algebra

We now construct a suitable curve whose Jacobian has complex multiplication in order to be able to apply the above results. We do this by explicitly computing the endomorphism ring for a particular class of curves; we closely follow the ideas in [Zar05, §4] but adapt them for a more general cyclic cover.

Throughout this section, we let $C_n/\mathbb{Q}_p : y^2 = x^n - a$ be a hyperelliptic curve, $a \in \mathbb{Q}_p^\times$, and we will write $J_n$ for its Jacobian.
Lemma 4.1. Let \( C_n : y^2 = x^n - a \) be a hyperelliptic curve, \( a \in \mathbb{Q}_p^\times \), with Jacobian \( J_n \). Let \( \delta_n \) denote both the \( \mathbb{Q}_p \)-automorphism of \( C_n \) given by \( (x, y) \mapsto (\zeta_n x, y) \) and the corresponding automorphism of \( J_n \) given by Albanese functoriality. Then the subring \( \mathbb{Z}[\delta_n] \subset \text{End}_{\mathbb{Q}_p} J_n \) is isomorphic to \( \mathbb{Z}[t]/P_n(t) \), where \( P_n(t) \in \mathbb{Z}[t] \) be the polynomial defined by

\[
P_n(t) = \begin{cases} 
\frac{t^n - 1}{t - 1} = t^{n-1} + \cdots + t + 1 & \text{if } n \text{ is odd;} \\
\frac{t^n - 1}{t^2 - 1} = t^{\frac{n}{2} - 1} + \cdots + t + 1 & \text{if } n \text{ is even.}
\end{cases}
\]

Proof. Let \( g \) be the genus of \( C_n \) and let \( \Omega^1(C_n) \) be the vector space of differentials of the first kind of \( C_n \). Recall that a basis of \( \Omega^1(C_n) \) is given by \( \omega_i = x^i \frac{dx}{y} \), \( 0 \leq i \leq g - 1 \). Moreover, these are eigenvectors for the corresponding automorphism \( \delta_n^* \) on \( \Omega^1(C_n) \) (given by functoriality) with eigenvalues \( c_{n,i}^* i+1 \); note that these are never 1 nor -1 as \( 2g < n \).

One can now check that \( P_n(\delta_n^*) = 0 \) in \( \text{End}(\Omega^1(C_n)) \) and moreover that \( P_n \) is the minimal polynomial for \( \delta_n^* \) in \( \mathbb{Q}[t] \).

Fix \( P_0 = (0, \sqrt{a}) \in C_n(\mathbb{Q}_p) \) which is \( \delta_n \)-invariant and define the Abel–Jacobi map \( \text{AJ} : C_n \to J_n \) using \( P_0 \). The induced map \( \text{AJ}^* : \Omega^1(J_n) \to \Omega^1(C_n) \) is then an isomorphism which commutes with \( \delta_n \). Hence \( \delta_n \) and \( \delta_n^* \) have the same minimal polynomial \( P_n(t) \) in their respective endomorphism rings.

Theorem 4.2. Let \( C_n/\mathbb{Q}_p : y^2 = x^n - a \) be a hyperelliptic curve, \( a \in \mathbb{Q}_p^\times, n \geq 3 \), with Jacobian \( J_n \). Then

\[
\text{End}_{\mathbb{Q}_p}(J_n) \cong \prod_{d|n, d > 2} \mathbb{Z}[\zeta_d].
\]

Proof. By the above lemma, \( \mathbb{Z}[\delta_n] \cong \prod_{d|n, d > 2} \mathbb{Z}[\zeta_d] \) so it just remains to prove the equality. Note that \( J_n \) is an abelian variety with complex multiplication by \( F = \mathbb{Q}[\delta_n] \cong \prod_{d|n, d > 2} \mathbb{Q}(\zeta_d) \) (this has dimension \( 2g \) over \( \mathbb{Q} \)). Since \( \mathbb{Z}[\delta_n] \) is the maximal order of \( F \), we have equality.

We are now finally in a position to prove Theorem 2.3

Theorem 4.3 (=Theorem 2.3). Fix a positive integer \( g \) and rational prime \( p \). Choose \( n \in \{2g + 1, 2g + 2\} \) such that \( p \nmid n \). Let \( C_n/\mathbb{Q} \) be the hyperelliptic curve \( y^2 = x^n - 1 \) with Jacobian \( J_n \). Then \( \mathbb{Q}_p(J_n[p])/\mathbb{Q}_p \) is tamely ramified.

Proof. First note that such a choice of \( n \) is always possible. Now the endomorphism algebra is \( F = \prod_{d|n, d > 2} \mathbb{Q}(\zeta_d) \) and note that each subfield of \( F \) is contained in \( \mathbb{Q}(\zeta_n) \). As \( p \nmid n, p \) is unramified in \( \mathbb{Q}(\zeta_n) \).
Moreover, we can see by construction that all endomorphisms are defined over $K = \mathbb{Q}_p(\zeta_n)$ which is tamely ramified. The theorem now follows from Lemma 3.4.

\begin{flushright}
$\square$
\end{flushright}

REFERENCES

[AD19] S. Anni and V. Dokchitser. Constructing hyperelliptic curves with surjective Galois representations. Trans. Amer. Math. Soc. (to appear), 2019.

[BD] M. Bisatt and T. Dokchitser. Tame torsion and the tame inverse Galois problem.

[Kis99] M. Kisin. Local constancy in p-adic families of Galois representations. Math. Z., (230):569–593, 1999.

[ST68] J. Serre and J. Tate. Good reduction of abelian varieties. The Annals of Mathematics, 88(3):492–517, 1968.

[Zar05] Y. Zarhin. Endomorphism algebras of superelliptic Jacobians. In Geometric methods in algebra and number theory, pages 339–362. Birkhäuser, 2005.