Mathematische Annalen (2021) 381:1439–1453
https://doi.org/10.1007/s00208-021-02173-y

Mathematische Annalen

# Tame torsion and the tame inverse Galois problem

Matthew Bisatt[1] · Tim Dokchitser[1]

Received: 3 March 2020 / Revised: 17 March 2021 / Accepted: 30 March 2021 / Published online: 27 April 2021


**Abstract**
Fix a positive integer $g$ and a squarefree integer $m$. We prove the existence of a genus $g$ curve $C/\mathbb{Q}$ such that the mod $m$ representation of its Jacobian is tame. The method is to analyse the period matrices of hyperelliptic Mumford curves, which could be of independent interest. As an application, we study the tame version of the inverse Galois problem for symplectic matrix groups over finite fields.

**Mathematics Subject Classification** 11G30 · 14G22

## 1 Introduction

We say that a number field $F$ is *tame* if $F/\mathbb{Q}$ is tamely ramified at every finite prime of $F$, and *wild* otherwise. The first result of this paper concerns the problem of finding, for fixed $g$ and $m$, a (non-singular projective) curve $C$ of genus $g$ whose Jacobian $J_C$ has tame $m$-torsion field $\mathbb{Q}(J_C[m])$.

**Theorem 1.1** (=5.7) *For every $g \geq 1$ and squarefree $m \geq 1$, there is a curve $C/\mathbb{Q}$ of genus $g$ such that $\mathbb{Q}(J_C[m])$ is tame.*

If $m$ is not squarefree, then $\mathbb{Q}(J_C[m])$ is wild, as it contains $\mathbb{Q}(\zeta_m)$ (by the Weil pairing), which is wild above primes $p$ for which $p^2|m$. In that sense the result is the best possible.

Our strategy will be to reduce to the case where $m = p$ is prime and show that it suffices to construct a curve whose $p$-torsion of the Jacobian is tamely ramified at $p$, which we then do with Mumford curves. To illustrate our Mumford curve approach to this problem, we explain the idea in the elliptic curve setting in the following example.

Communicated by Wei Zhang.

✉ Matthew Bisatt
matthew.bisatt@bristol.ac.uk

Tim Dokchitser
tim.dokchitser@bristol.ac.uk

[1] University of Bristol, Fry Building, Woodland Road, Bristol BS8 1UG, UK

***Example 1.2*** Let $E/\mathbb{Q}_p$ be an elliptic curve with split multiplicative reduction. Then $E$ is isomorphic to a Tate curve and $E(\overline{\mathbb{Q}}_p) \cong \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$ as $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules, for some $q \in p\mathbb{Z}_p$. Moreover any such $q$ gives rise to a Tate curve. In particular, $\mathbb{Q}_p(E[p]) = \mathbb{Q}_p(\zeta_p, q^{1/p})$, and so, whenever $q$ is a $p$-th power (say $q = p^p$), the extension $\mathbb{Q}_p(E[p])/\mathbb{Q}_p$ is tamely ramified.

For our second result, recall that the classical inverse Galois problem asks, given a finite group $G$, if there is a Galois extension $F/\mathbb{Q}$ such that $\mathrm{Gal}(F/\mathbb{Q}) \cong G$? This is open in general, but known for certain classes of groups including soluble groups and $G = S_n, A_n, \mathrm{GSp}_{2g}(\mathbb{F}_p)$. Birch [5, p. 35] further asked whether $F$ can also be taken to be tame? This is known as the tame inverse Galois problem.

We address this problem for $G = \mathrm{GSp}_{2g}(\mathbb{F}_p)$, $p$ odd. It is known when $g = 1$ (all $p$) and $g = 2$ ($p \geq 5$) thanks to the work of Arias-de-Reyna–Vila [3, Theorem 1.2], [4, Theorem 5.3].

**Theorem 1.3** (=6.7) *Fix a positive integer $g$ and an odd prime $p$, such that there is a Goldbach triple for $2g+2$ not containing $p$. There is a curve $C/\mathbb{Q}$ of genus $g$ such that $\mathbb{Q}(J_C[p])$ is tame, and $\mathrm{Gal}(\mathbb{Q}(J_C[p])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_p)$.*

See Conjecture 6.2 for the definition of a Goldbach triple. This is a (slightly) strengthened version of the Goldbach conjecture that predicts that such triples always exist. On the numerical side, we show that, consequently, $\mathrm{GSp}_{2g}(\mathbb{F}_p)$ is tamely realisable as a Galois group over $\mathbb{Q}$ for $g \leq 10^7$ and all $p > 2$; see Lemma 6.10 and the discussion afterwards.

*Layout.* In Sects. 2–5 we address the tame torsion question (Theorem 1.1). Specifically, in Sect. 2 we reduce the tame torsion question to odd primes $p$ and show that it suffices to construct a curve whose $p$-torsion is tamely ramified at $p$. We then focus on Mumford curves, which are the rigid space generalisation of the Tate curve we used in Example 1.2. In Sect. 3, we review hyperelliptic Mumford curves and gather some basic results. We then compute an approximation to the period matrix in Sect. 4 and construct a suitable Mumford curve in Sect. 5. In Sect. 6 we give the application to the inverse Galois problem (Theorem 1.3).

***Remark 1.4*** Ensuring that the mod $p$ representation is tamely ramified at $p$ may also be done via imposing restrictions on the endomorphism algebra instead; for details, see [6]. Moreover the author realises $\mathrm{GSp}_{2g}(\mathbb{F}_p)$ as a Galois group over $\mathbb{Q}$ for all $g$ and odd primes $p$ via a non-constructive density argument [6, Theorem 1.3].

**Notation 1.5** Throughout the paper, we denote

| | |
|---|---|
| $G_F$ | $= \mathrm{Gal}(\overline{F}/F)$, the absolute Galois group of a field F |
| $C$ | (hyperelliptic) non-singular projective curve $C$ of genus $g \geq 1$ |
| $J_C$ | Jacobian of $C$ |
| $\zeta_m$ | primitive $m^{\text{th}}$ root of unity |
| In Sects. 3–5, we write | |
| $K$ | finite extension of $\mathbb{Q}_p$ ($p$ odd) |
| $\mathcal{O}_K, \pi, q_K, e$ | ring of integers of $K$, uniformiser, size of residue field, ramification degree |
| $\lvert\cdot\rvert$ | absolute value on $K$, normalised so that $\lvert\pi\rvert = q_K^{-1}$ |
| $\overline{K}, \mathbb{C}_K$ | an algebraic closure of $K$ and its completion |
| $\Gamma$ | Schottky group, see Definition 3.1 |
| $s_i, a_i, b_i, c_i, r_i$ | see Construction 3.5 |

## 2 Reduction to the prime case and $\ell = p$

First note that for squarefree $m$, the field $\mathbb{Q}(J_C[m])$ is the compositum of $\mathbb{Q}(J_C[p_j])$ for prime divisors $p_j | m$, so it suffices to prove Theorem 1.1 when $m = p$ is prime. In this section, we will reduce the question further to only needing to study the ramification of $\mathbb{Q}(J_C[p])/\mathbb{Q}$ at $p$ via a result of Kisin of local constancy of Galois representations in $\ell$-adic families, and deal with $p = 2$.

**Lemma 2.1** *Let $m = p_1 p_2 \cdots p_n$, with $p_j$ distinct primes. Let $C/\mathbb{Q}$ be a curve of genus $g$ such that*

(i) *$C$ has semistable reduction at all primes $\ell \leq 2g + 1$;*
(ii) *$\mathbb{Q}_{p_j}(J_C[p_j]) \cong \mathbb{Q}_{p_j}(\zeta_{p_j})$ for $1 \leq j \leq n$.*

*Then $\mathbb{Q}(J_C[m])$ is tame.*

***Proof*** Note $\mathbb{Q}(J_C[m])$ is the compositum of the fields $\mathbb{Q}(J_C[p_j])$ so it suffices to prove that these are all tame. Fix a prime $p = p_j$; we have to show that $\mathbb{Q}(J_C[p])/\mathbb{Q}$ is tamely ramified at $\ell$ for all primes $\ell$; note that by condition (ii), we may assume that $\ell \neq p$.

If $\ell > 2g + 1$, then a result of Serre–Tate [15, p. 497] tells us that the extension is tamely ramified at $\ell$. On the other hand, if $\ell \leq 2g + 1$, then this follows from Grothendieck's characterisation of inertia on semistable abelian varieties [8, Proposition 3.5]; see also [4, Theorem 2.1] for a direct proof of this.

**Theorem 2.2** *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 $\tilde{f} \equiv f \bmod \ell^N$ and $\deg(f) = \deg(\tilde{f})$, then $C_{\tilde{f}} : y^2 = \tilde{f}(x)$ is a hyperelliptic curve with*

$$J_{C_{\tilde{f}}}[m] \cong J_{C_f}[m]$$

*as $G_{\mathbb{Q}_\ell}$-modules.*

***Proof*** This is a special case of [12, Theorem 5.1(1)]. Note that for $N$ large enough, all $\tilde{f} \equiv f \mod \ell^N$ are squarefree, and so define an $\ell$-adic family of hyperelliptic curves of the same genus.

With this theorem, we only need to construct genus $g$ hyperelliptic curves $C_\ell/\mathbb{Q}_\ell$ at each prime $\ell \le 2g+1$ and then glue them together with sufficient congruence conditions in order to realise the $m$-torsion as a tame extension.

To construct a curve $C/\mathbb{Q}_p$ such that $J_C$ is semistable with $\mathbb{Q}_p(J_C[p]) \cong \mathbb{Q}_p(\zeta_p)$ we will use the theory of Mumford curves. For simplicity in this approach however, we will assume that $p$ is odd, so we briefly record below a curve that covers the case $p = 2$.

**Proposition 2.3** *Let $a_1, \dots, a_{g+1} \in \mathbb{Z}_2\backslash\{0\}$ have pairwise distinct 2-adic valuations, and $0 \ne N \in \mathbb{Z}_2$ satisfies $v_2(N) \ge \sum_i v_2(a_i)$. Let $C/\mathbb{Q}_2$ be the genus $g$ hyperelliptic curve*

$$y^2 + h(x)y = -N^2, \quad h(x) = \prod_{i=1}^{g+1}(x - a_i).$$

*Then the $J_C/\mathbb{Q}_2$ is semistable, and $J_C[2] \subset J_C(\mathbb{Q}_2)$.*

***Proof*** By assumption on the $a_i$, the Newton polygon of $h$ breaks completely, and [7, Thm 1.2(6,7)] shows that $J_C$ is semistable and has totally toric reduction. Next, completing the square and replacing $y$ by $y/2$ we see that $C$ is isomorphic to

$$y^2 = (h(x) - 2N)(h(x) + 2N).$$

As $v_2(2N) > v_2(h(0))$, the polynomials $h(x) - 2N$ and $h(x) + 2N$ have the same Newton polygon as $h$, and so factor completely over $\mathbb{Z}_2$ as well. It follows that $J_C[2] \subset J_C(\mathbb{Q}_2)$.

## 3 Mumford curves and Whittaker groups

In this paper, we will only need to concern ourselves with hyperelliptic Mumford curves in which case the Schottky group will be of a particular type called a Whittaker group. For more details on the background of Mumford curves in general, see [9].

From now on, we suppose that $p \ge 3$ and let $K/\mathbb{Q}_p$ be a finite extension. Let $v$ be the normalised valuation on $K$, and $\mathcal{O}_K, \pi, q_K, e, |\cdot|, \mathbb{C}_K$ as in Notation 1.5.

**Definition 3.1** Let $\Gamma \subset \mathrm{PGL}_2(K)$ be a subgroup, acting on $\mathbb{P}^1(\mathbb{C}_K)$ by Möbius transformations.

(i) A point $x \in \mathbb{P}^1(\mathbb{C}_K)$ is a *limit point* of $\Gamma$ if there exists $y \in \mathbb{P}^1(\mathbb{C}_K)$ and an infinite sequence $(\gamma_n) \subset \Gamma$ with $\gamma_n$ distinct and $\lim \gamma_n(y) = x$.
(ii) $\Gamma$ is a *Schottky group* if it is discrete, free, and finitely generated.
(iii) Suppose $\Gamma$ is Schottky. Let $\Omega_\Gamma = \mathbb{P}^1(\mathbb{C}_K) - \{\text{limit points of } \Gamma\}$. Then $\Omega_\Gamma/\Gamma$ is a *Mumford curve* of genus equal to the rank of $\Gamma$.
(iv) Let $\Gamma$ be a Schottky group. If the associated Mumford curve is hyperelliptic, then $\Gamma$ is called a *Whittaker group*.

***Example 3.2*** Let $q \in K$ be such that $|q| < 1$ and let $\gamma = \left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $\Gamma = \langle \gamma \rangle$ is Schottky of rank 1. Moreover, $\Omega_\Gamma = \mathbb{P}^1(\mathbb{C}_K) - \{0, \infty\}$, and the corresponding Mumford curve is isomorphic to the Tate curve associated to $q$.

The construction of Mumford curves is analytic, so computing an algebraic model for them is in general difficult. The main approach is to construct a good fundamental domain, which we do via $p$-adic discs; we briefly set up some notation for them.

**Notation** Let $c, r \in \mathbb{C}_K$. We define the *open disc* $B(c, r)$ and *closed disc* $\overline{B(c, r)}$ with centre $c$ and radius $r$ as

$$B(c, r) = \{z \in \mathbb{C}_K : |z - c| < |r|\}, \quad \overline{B(c, r)} = \{z \in \mathbb{C}_K : |z - c| \leq |r|\}.$$

**Definition 3.3** Let $\Gamma$ be a Schottky group of rank $g$. Then a set $F$ is called a *good fundamental domain* for $\Gamma$ if:

(i) $F = \mathbb{P}^1(\mathbb{C}_K) - \left(\bigcup_{i=1}^{g} (B_i \cup B_i')\right)$ where $B_1, B_1', \ldots, B_g, B_g'$ are $2g$ open discs with centres in $K$;
(ii) The closed discs $\overline{B_1}, \overline{B_1'}, \ldots, \overline{B_g}, \overline{B_g'}$ are disjoint;
(iii) $\Gamma$ is generated by elements $\gamma_1, \ldots, \gamma_g$ such that $\gamma_i(\mathbb{P}^1(\mathbb{C}_K) - B_i) = \overline{B_i'}$ and $\gamma_i(\mathbb{P}^1(\mathbb{C}_K) - \overline{B_i}) = B_i'$ for $1 \leq i \leq g$.

In this case, we say that the generators $\gamma_1, \ldots, \gamma_g$ are *in good position*.

**Proposition 3.4** *Every Schottky group has a good fundamental domain. Conversely, given a set $F$ satisfying conditions (i) and (ii), there exists a Schottky group with good fundamental domain $F$.*

***Proof*** See [9, I.4.1.3 and I.4.1.4].

For hyperelliptic Mumford curves, one constructs a Whittaker group via a suitable choice of $2g + 2$ points as follows:

**Construction 3.5** (i) Let $Z = \{a_1, b_1, \ldots, a_g, b_g, a_\infty = 1, b_\infty = \infty\}$ be a set of $2g + 2$ distinct points of $\mathbb{P}^1(K)$.
(ii) For each pair $a_i, b_i$, let $c_i = \frac{a_i + b_i}{2}$, $r_i = \frac{b_i - a_i}{2}$ if $i \leq g$.
(iii) Let $s_i = \begin{pmatrix} c_i & r_i^2 - c_i^2 \\ 1 & -c_i \end{pmatrix}$ if $i \leq g$ and $s_\infty = \begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix}$ be involutions in $\mathrm{PGL}_2(K)$ fixing $a_i, b_i$.
(iv) Let $\Gamma_Z = \langle s_1 s_\infty, \ldots, s_g s_\infty \rangle$.

**Definition 3.6** Let $Z$ be a set of $2g + 2$ distinct points. If the corresponding group $\Gamma_Z$ is a Whittaker group of rank $g$, then we say that $Z$ is in good position.

***Remark 3.7*** (i) To check if $\Gamma_Z$ is Schottky, let $B_i = B(c_i, r_i)$ and $B_i' = s_\infty(B_i)$ for $i \leq g$. Then it suffices to check the conditions (i) and (ii) of Definition 3.3 for these $2g$ discs to see if they define a good fundamental domain.
(ii) We can always suppose that $0, 1, \infty \in Z$ by applying a Möbius transformation. This changes $\Gamma_Z$ to a conjugate subgroup and gives an isomorphic Mumford curve.

(iii) Note that the construction requires a choice of pairing on $Z$. One can show that there is at most one pairing on $Z$ such that it is in good position.
(iv) The equation of the hyperelliptic curve $C = \Omega_{\Gamma_Z}/\Gamma_Z$ is (see [9, p. 279])

$$C\colon y^2 = \prod_{z\in Z}(x-\theta(0,1;z)),$$

where $\theta(0,1;z) = \prod_{w\in W_Z}\frac{z-w(0)}{z-w(1)}$ and $W_Z = \langle s_1,\dots,s_g,s_\infty\rangle$ is the group generated by the associated involutions; the 2:1 map $C\to\mathbb{P}^1$ is $\Omega_{\Gamma_Z}/\Gamma_Z \to \Omega_{\Gamma_Z}/W_Z$.

**Lemma 3.8** [[11, Lemma 5.5, Theorem 5.7]] *Let $Z = \{a_1 = 0, b_1, a_2, \dots, a_g, b_g, a_\infty = 1, b_\infty = \infty\}$ be a set of $2g+2$ distinct points. Suppose*

- $0 < |b_1| < |a_2| \le |b_2| \le |a_3| \cdots \le |b_g| < 1$;
- $\frac{|r_i|}{|c_i - c_j|} < 1$ *for all distinct* $1 \le i, j \le g$.

*Then:*

(i) *The points of $Z$ are in good position;*
(ii) *$\Gamma = \langle s_1 s_\infty, \dots, s_g s_\infty\rangle$ is a Whittaker group of rank $g$;*
(iii) *A good fundamental domain for $\Gamma$ is given by the complement of the discs $B_i = B(c_i, r_i)$ and $B_i' = B(2-c_i, r_i)$, $1 \le i \le g$.*

We will now implicitly assume these assumptions in the lemma whenever we deal with a Whittaker group. For two discs $B$, $B'$, we denote by $d(B, B')$ the corresponding metric coming from the standard one on the Berkovich line $\mathbb{P}^{1,an}$ (see for example [13, p. 7]).

**Lemma 3.9** (i) *Let $i \ne j$. Then $d(B_i, B_j) = d(B_i', B_j') = \log_p \frac{|c_i - c_j|^2}{|r_i r_j|}$.*
(ii) *For all $i, j$, $d(B_i, B_j') = \log_p \frac{1}{|r_i r_j|}$.*

*In particular, the minimum distance, $m_\Gamma$,*[1] *between two distinct discs is* $\min_{i\ne j\le g} \log_p \frac{|c_i - c_j|^2}{|r_i r_j|}$.

***Proof*** For the first part, note that the smallest disc containing $B_i$ and $B_j$ is $B(c_i, c_i - c_j)$ and the statement follows from the definition. For the second part, we get $d(B_i, B_j') = \frac{|2 - c_i - c_j|^2}{|r_i r_j|}$ and note that the numerator is a unit as $p \ne 2$ and the centres $c_i$ are integral non-units. The minimum now follows.

## 4 Approximation of the period matrix

Let $\Gamma$ be a Schottky group with generators $\gamma_1, \dots, \gamma_g$ in good position. Let $B_1, \dots, B_g$, $B_1', \dots, B_g'$ be the associated disjoint discs defining the fundamental domain such that $\gamma_k(\mathbb{P}^1(\mathbb{C}_K) - B_k') = \overline{B_k}$ for all $k$. We define the closure of an open disc $B$ as $\overline{B}$, the boundary of $B$ to be $\partial B := \overline{B}\setminus B$ and the diameter of $B$ as $\operatorname{diam}(B) = \sup_{x,y\in\overline{B}} |x-y|$.

[1] This depends on the choice of a good fundamental domain and not just $\Gamma$.

**Notation 4.1** For a free group $\Gamma = \langle \gamma_1, \gamma_2, \ldots, \gamma_g \rangle$, we let $\Gamma_n$ be the subset consisting of all elements of $\Gamma$ of reduced word length at most $n$.

$$\text{For id} \neq \gamma \in \Gamma_1, \text{ we define } B_\gamma = \begin{cases} B_k & \text{if } \gamma = \gamma_k, \quad k = 1, \ldots, g; \\ B'_k & \text{if } \gamma = \gamma_k^{-1}, \quad k = 1, \ldots, g. \end{cases}$$

**Lemma 4.2** *Let $a \in \partial B'_i, z \in \partial B'_j$. Let* id $\neq \gamma \in \Gamma_1$. *Let $z_j, z'_j, z_\gamma$ be centres of $B_j, B'_j, B_\gamma$ respectively.*

(i) *If $\gamma \neq \gamma_j^{-1}$, then* $\left| \dfrac{z - \gamma a}{z - \gamma\gamma_i a} - 1 \right| \leq \dfrac{\operatorname{diam}(\overline{B_\gamma})}{|z'_j - z_\gamma|}$;

(ii) *If $\gamma \neq \gamma_j$, then* $\left| \dfrac{\gamma_j z - \gamma a}{\gamma_j z - \gamma\gamma_i a} - 1 \right| \leq \dfrac{\operatorname{diam}(\overline{B_\gamma})}{|z_j - z_\gamma|}$.

***Proof*** We prove the first part; the second part is analogous. First note that $\frac{z-\gamma a}{z-\gamma\gamma_i a} - 1 = \frac{\gamma\gamma_i a - \gamma a}{z-\gamma\gamma_i a}$. Since $a \in \partial B'_i$, we have that $\gamma a, \gamma\gamma_i a \in \overline{B_\gamma}$ and hence $|\gamma\gamma_i a - \gamma a| \leq \operatorname{diam}(\overline{B_\gamma})$.

Since $\gamma \neq \gamma_j^{-1}$, the discs $B'_j$ and $B_\gamma$ are disjoint, so let $z'_j, z_\gamma$ be centres of $B'_j, B_\gamma$ respectively. Now $z, z'_j \in \overline{B'_j}$ and $z_\gamma \notin \overline{B'_j}$, so $|z'_j - z_\gamma| > |z - z'_j|$. Similarly $|z'_j - z_\gamma| > |z_\gamma - \gamma\gamma_i a|$ using $B_\gamma$. Hence

$$|z - \gamma\gamma_i a| = |z - z'_j + z'_j - z_\gamma + z_\gamma - \gamma\gamma_i a| = |z'_j - z_\gamma|,$$

by the ultrametric triangle inequality.

We now return to the case where $\Gamma$ is a Whittaker group and continue our notation from §3. The Jacobian $J_{\Omega_\Gamma/\Gamma}$ has a $g \times g$ *period matrix* $Q = (Q_{ij})$ whose entries can be computed in terms of $\Gamma$ (see [9] VI.2)

$$Q_{ij} = \prod_{\gamma \in \Gamma} \frac{(z - \gamma a)(\gamma_j z - \gamma\gamma_i a)}{(z - \gamma\gamma_i a)(\gamma_j z - \gamma a)},$$

for any choice of non-conjugate $a, z \in \Omega_\Gamma$.

**Notation 4.3** For a subset $S \subset \Gamma$, let

$$Q_{ij}^S = \prod_{\gamma \in S} \frac{(z - \gamma a)(\gamma_j z - \gamma\gamma_i a)}{(z - \gamma\gamma_i a)(\gamma_j z - \gamma a)}.$$

If $S = \Gamma_n$, we write $Q_{ij}^n$ for $Q_{ij}^{\Gamma_n}$; clearly $\lim_{n\to\infty} Q_{ij}^n = Q_{ij}$.

**Lemma 4.4** *Let $q \in K$ be such that* $\max_{i \neq j} \dfrac{|r_i|}{|c_i - c_j|} \leq |q| < 1$. *Then* $\left| \dfrac{Q_{ij}^1}{Q_{ij}} - 1 \right| < |q|$.

***Proof*** We have $\left|\frac{Q^1_{ij}}{Q_{ij}} - 1\right| \le q_K^{-em_\Gamma}$ by [13, Theorem 3.6],[2] and $\max_{i\ne j} \frac{|r_i|}{|c_i - c_j|} > \max_{i\ne j} \frac{|r_i r_j|}{|c_i - c_j|^2} = q_K^{-em_\Gamma}$ since the discs are disjoint.

**Theorem 4.5** *Let $q \in K$ be such that $\max_{i\ne j} \frac{|r_i|}{|c_i-c_j|} \le |q| < 1$. Let $a \in \partial B'_i$, $z \in \partial B'_j$ be distinct mod $\Gamma$. Define*

$$Q^\alpha_{ij} = Q^0_{ij} \frac{(z - \gamma_j^{-1}a)(\gamma_j z - \gamma_j a)}{(z - \gamma_j^{-1}\gamma_i a)(\gamma_j z - \gamma_j\gamma_i a)}.$$

*Then*

$$\left|\frac{Q^\alpha_{ij}}{Q_{ij}} - 1\right| \le |q|.$$

***Proof*** Note first that such a $q$ exists by Lemma 3.8. Using Lemma 4.4, we only need to consider the contributions from non-identity elements in $\Gamma_1$. The result is then immediate from Lemma 4.2.

We will now compute $Q^\alpha_{ij}$ to get an explicit formula. By choosing the auxiliary parameters $a, z$ carefully, we will not need to distinguish between the cases $i = j$ and $i \ne j$, and we find that $Q^\alpha_{ij} = Q^0_{ij}$ with this choice.

**Lemma 4.6** *Let $a \in \partial B'_i$, $z \in \partial B'_j$ and assume $a \ne z$ if $i = j$. Then $a \not\equiv z \mod \Gamma$.*

***Proof*** We shall adapt the proof of [13, Lemma 2.4]. In fact, we shall prove that $\gamma a$ is contained in the interior of the open disc $B_{h_1}$ (continuing notation from above), where $\gamma = h_1 \cdots h_m$ as a reduced word, unless $\gamma \in \{\mathrm{id}, \gamma_i\}$. Note that $\gamma_k(\mathbb{P}^1 \setminus \overline{B'_k}) = B_k$ and moreover $\gamma_k(\partial B'_k) = \partial B_k$ for all $k$.

If $h_m \ne \gamma_i$ then $h_m a \in B_{h_m}$ and hence iteratively we have $\gamma a \in B_{h_1}$. If $h_m = \gamma_i$, then $h_m a \in \partial B_i$ so if $m \ge 2$, then $h_{m-1} \ne \gamma_i^{-1}$ so proceeding similarly we have $\gamma a \in B_{h_1}$. Moreover, note $\gamma_i a \ne z$ since $B'_j \ne B_i$. Lastly, if $\gamma = \mathrm{id}$, then $a \ne z$ by assumption.

**Lemma 4.7** *Let $a = 2 - c_i + r_i$ and $z = 2 - c_j - r_j$. Then*

(i) *$a \in \partial B'_i$, $z \in \partial B'_j$, and $a$ and $z$ are distinct mod $\Gamma$.*
(ii) *$Q^0_{ij} = \left(\frac{c_i - c_j - r_i - r_j}{2 - c_i - c_j + r_i - r_j}\right)^2$ for all $1 \le i, j \le g$.*
(iii) *$Q^0_{ii} = \left(\frac{r_i}{c_i - 1}\right)^2$ for all $1 \le i \le g$.*
(iv) *$Q^\alpha_{ij} = Q^0_{ij}$.*

***Proof*** (i) Follows from Lemma 4.6.

[2] Note that under our normalisation $|p| = q_K^{-e}$ in contrast to [13] who use $|p| = p^{-1}$.

(ii) We have $\gamma_k = \begin{matrix} c_k & c_k^2 - r_k^2 - 2c_k \\ 1 & c_k - 2 \end{matrix}$ for all $k$. From this we compute explicitly that $\gamma_i a = c_i - r_i$ and similarly $\gamma_j z = c_j + r_j$. Now the claim follows from

$$z - a = (c_i - c_j) - (r_i + r_j), \quad z - \gamma_i a = 2 - c_i - c_j + r_i - r_j,$$
$$\gamma_j z - \gamma_i a = -(z - a), \quad \gamma_j z - a = -(z - \gamma_i a).$$

(iii) This follows from (2), by setting $i = j$.

(iv) We compute $(z - \gamma_j^{-1} a)(\gamma_j z - \gamma_j a)/(z - \gamma_j^{-1}\gamma_i a)(\gamma_j z - \gamma_j \gamma_i a)$. The claim now follows from

$$z - \gamma_j^{-1} a = -r_j - \frac{r_j^2}{-2 + c_i + c_j - r_i}, \quad z - \gamma_j^{-1}\gamma_i a = -r_j + \frac{r_j^2}{c_i - c_j - r_i},$$
$$\gamma_j z - \gamma_j \gamma_i a = -(z - \gamma_j^{-1} a), \quad \gamma_j z - \gamma_j a = -(z - \gamma_j^{-1}\gamma_i a).$$

## 5 Tame torsion

**Lemma 5.1** *Let $a \in 1 + \pi^N \mathcal{O}_K$ for some positive integer $N$. If $em \leq N$, then $x^m - a$ has a root in $\mathcal{O}_K$. In particular, every element of $1 + \pi^{em}\mathcal{O}_K$ is an $m^{th}$ power for all $m \geq 1$.*

***Proof*** This is a simple application of Hensel's lemma, where we use the version that states there is a lift of a root $a_0$ (in the residue field) of a polynomial $f$ if $v(f(a_0)) > 2v(f'(a_0))$, where we use $f = x^m - a$ and $a_0 = 1$.

Note that $v(f(a_0)) \geq N$ by construction and $f'(a_0) = m$, so $v(f'(a_0)) = ev_p(m)$ where $v_p$ is the standard $p$-adic valuation on $\mathbb{Z}$. Now

$$\begin{aligned} v_p(m) &\leq \log_p(m), \\ &< \ln(m) \quad \text{as } p \geq 3, \\ &\leq \frac{m}{2} \quad \text{by bounds on ln,} \end{aligned}$$

so $v(f'(a_0)) < \frac{em}{2}$ and the result follows.

**Lemma 5.2** *Let $r_i = \pi^{em\alpha}$, $c_i = 2\pi^{em\beta}$ for some $\alpha, \beta > 0$. Then $(\frac{r_i}{1-c_i})^2$ is an $m^{th}$ power in $\mathcal{O}_K$.*

***Proof*** We have $(1 - c_i)^2 \in 1 + \pi^{em}\mathcal{O}_K$, so it is an $m^{\text{th}}$ power by Lemma 5.1.

**Lemma 5.3** *Let $r_i = \pi^{em\alpha_i}, r_j = \pi^{em\alpha_j}, c_i = 2\pi^{em\beta_i}, c_j = 2\pi^{em\beta_j}$ with $\alpha_i, \alpha_j, \beta_i, \beta_j$ distinct positive integers with $\beta_i, \beta_j < \alpha_i, \alpha_j$. Then $\left(\frac{c_i - c_j - r_i - r_j}{2 - c_i - c_j + r_i - r_j}\right)^2$ is an $m^{th}$ power in $\mathcal{O}_K$.*

***Proof*** Without loss of generality, suppose $\beta_i < \beta_j$. Then

$$\begin{aligned} c_i - c_j - r_i - r_j &= 2\pi^{em\beta_i}\big(1 - \pi^{em(\beta_j-\beta_i)} - \frac{1}{2}\pi^{em(\alpha_i-\beta_i)} - \frac{1}{2}\pi^{em(\alpha_j-\beta_i)}\big) \\ &\in 2\pi^{em\beta_i}(1+\pi^{em}\mathcal{O}_K), \end{aligned}$$

which is twice an $m^{\text{th}}$ power by Lemma 5.1. On the other hand, the denominator is

$$\begin{aligned} 2 - c_i - c_j + r_i - r_j &= 2\big(1 - \pi^{em\beta_i}\big(1 + \pi^{em(\beta_j-\beta_i)} + \frac{1}{2}\pi^{em(\alpha_i-\beta_i)} - \frac{1}{2}\pi^{em(\alpha_j-\beta_i)}\big)\big) \\ &\in 2(1+\pi^{em}\mathcal{O}_K), \end{aligned}$$

which is also twice an $m$th power.

**Theorem 5.4** *Let $m \geq 1$, and*

- *$\alpha_1 > \alpha_2 > \cdots > \alpha_g > \beta_2 > \beta_3 > \cdots > \beta_g$ positive integers;*
- *$r_1 = c_1 = \pi^{em\alpha_1}$, and $r_i = \pi^{em\alpha_i}$, $c_i = 2\pi^{em\beta_i}$ for $2 \leq i \leq g$;*
- *$a_i = c_i - r_i$, $b_i = c_i + r_i$ for $1 \leq i \leq g$.*

*Then:*

(i) $a_1 = 0$;

(ii) $0 < |b_1| < |a_2| \leq |b_2| \leq |a_3| \cdots \leq |b_g| < 1$;

(iii) $\dfrac{|r_i|}{|c_i - c_j|} \leq q_K^{-em} < 1$ *for all distinct* $1 \leq i, j \leq g$;

(iv) $\big(\frac{c_i - c_j - r_i - r_j}{2 - c_i - c_j + r_i - r_j}\big)^2$ *is an $m$th power in $\mathcal{O}_K$ for all* $1 \leq i, j \leq g$.

(v) *Let $Q = (Q_{ij})$ denote the period matrix of the abelian variety $J_{\Omega_\Gamma/\Gamma}$ Then $Q_{ij}$ is an $m$th power for all* $1 \leq i, j, \leq g$.

***Proof*** (i) Note $a_1 = c_1 - r_1 = 0$ by definition.

(ii) Observe that for $i \geq 2$, $|a_i| = |b_i| = |c_i| = q_K^{-em\beta_i}$. Since the $\beta_i$ are decreasing and $a_i, b_i \in \pi\mathcal{O}_K$, we have $|a_2| \leq |b_2| \leq |a_3| \cdots \leq |b_g| < 1$. Lastly note $|b_1| = |2\pi^{em\alpha_1}| < |a_2|$.

(iii) We compute that for $i \neq j$, $\dfrac{|r_i|}{|c_i - c_j|} = \dfrac{|\pi^{em\alpha_i}|}{|\pi^{em\beta_j}|} = q_K^{-em(\alpha_i-\beta_j)}$ where we suppose $i < j$ without loss of generality. Since $\alpha_i > \beta_j$, we are done.

(iv) First suppose $i = j$. If $i \neq 1$, then this follows directly from Lemma 5.2; the same proof also works for $i = 1$. Now suppose $i \neq j$. If $i, j \geq 2$, then this is Lemma 5.3. If $i = 1$ or $j = 1$, then one can apply the same proof using the simplification $c_1 = r_1$.

(v) By (iv), we have that $Q_{ij}^0$ is an $m^{\text{th}}$ power. Now by Theorem 4.5, Lemma 4.7(4) and (iii), $\big|\frac{Q_{ij}^0}{Q_{ij}} - 1\big| \leq q_K^{-em}$ hence $Q_{ij}^0 = Q_{ij}(1 + \pi^{em}b)$ for some $b \in \mathcal{O}_K$. Since $Q_{ij}^0$ and $1 + \pi^{em}b$ are $m^{\text{th}}$ powers (by Lemma 5.1), so is $Q_{ij}$.

**Lemma 5.5** *Let $J/K$ be an abelian variety with a Raynaud parameterisation $J \cong (\overline{K}^\times)^g/Q$. Let $m > 1$ and suppose every entry in the period matrix $Q$ is an $m$th power in $K$. Then*

$$J[m] \cong \mu_m^g \times (\mathbb{Z}/m\mathbb{Z})^g$$

*as $G_K$-modules. Here $\mathbb{Z}/m\mathbb{Z}$ has a trivial action, and $\mu_m = \langle \zeta_m \rangle \subset \overline{K}$ is the set of $m$th roots of unity, with natural action. In particular, $K(J[m]) = K(\zeta_m)$.*

***Proof*** Recall that $J(\overline{K}) \cong (\overline{K}^\times)^g/Q$ as $G_K$-modules. Let $Q = (Q_{ij})$. Then

$$J[m] = \mu_m^g \times \langle (Q_{i1}^{1/m}, Q_{i2}^{1/m}, \ldots, Q_{ig}^{1/m}),\ i = 1, \ldots, g \rangle.$$

As every $Q_{ij} \in K^\times$ is an $m^{\text{th}}$ power, the result follows.

**Theorem 5.6** *Fix an integer $g \geq 1$. Let*

- *$\alpha_i = 2g - i$ for $1 \leq i \leq g$, and $\beta_i = g - i + 1$ for $2 \leq i \leq g$;*
- *$r_1 = c_1 = \pi^{p\alpha_1}$, and $r_i = \pi^{p\alpha_i}$, $c_i = 2\pi^{p\beta_i}$ for $2 \leq i \leq g$.*

*Let $C/K$ be the corresponding genus $g$ hyperelliptic Mumford curve given by Construction 3.5. Then $J_C$ is semistable and $K(J_C[p]) = K(\zeta_p)$.*

***Proof*** Recall that all Mumford curves are semistable (see for example [9, Theorem 2.12.2]). By Theorem 5.4 with $m = p$, every entry of the period matrix of $J_C$ is a $p^{th}$ power; the statement now follows from Lemma 5.5 with $m = p$.

**Theorem 5.7** *Fix a positive integer $g$ and squarefree integer $m$. Then there exists a non-singular projective curve $C/\mathbb{Q}$ of genus $g$ such that $\mathbb{Q}(J_C[m])$ is tame.*

***Proof*** By Kisin's result (Theorem 2.2) we need only choose a suitable genus $g$ hyperelliptic curve $C_\ell$ for the finite set of primes $\ell \leq 2g + 1$ and $\ell \mid m$; if $\ell \nmid m$ we take $C_\ell$ to be semistable at $\ell$ (e.g. good reduction at $\ell$). For $\ell \mid m$, $\ell \neq 2$, Theorem 5.6 with $K = \mathbb{Q}_\ell$, $p = \ell$ provides a construction of a genus $g$ hyperelliptic curve $C_\ell$ such that $\mathbb{Q}_\ell(J_{C_\ell}[\ell]) \cong \mathbb{Q}_\ell(\zeta_\ell)$; similarly we can use Proposition 2.3 if $\ell = 2$. We are now done by Lemma 2.1.

***Remark 5.8*** The same approach works to construct a curve $C/\mathbb{Q}_p$ such that $\mathbb{Q}_p(J_C[p^n]) = \mathbb{Q}_p(\zeta_{p^n})$ for any $n \geq 1$ but note that this is wildly ramified if $n \neq 1$. However we can give global curves $C/\mathbb{Q}$ such that $\mathbb{Q}(J_C[m])/\mathbb{Q}(\zeta_m)$ is a tame extension any odd integer $m$.

## 6 The tame inverse Galois problem

In this section, we investigate the tame version of the inverse Galois problem when $G$ is of the form $\mathrm{GSp}_{2g}(\mathbb{F}_p)$ via the mod $p$ representation of abelian varieties.

***Remark 6.1*** An alternative approach to force surjectivity is to ensure $\mathrm{End}\, A = \mathbb{Z}$ (to guarantee this, take $\mathrm{Gal}(f) \cong S_{\deg(f)}$ and apply [16, Theorem 2.1]) and then apply Serre's open image theorem to obtain surjectivity for $p$ sufficiently large.[3] There are two problems with this however: we do not know precisely what sufficiently large means and more importantly this says nothing for small $p$.

**Conjecture 6.2** (Goldbach + $\varepsilon$) *Let $n \geq 4$ be an even integer. Then there exist primes $q_1, q_2, q_3$ such that $q_1 \leq q_2 < q_3 < n$ and $q_1 + q_2 = n$. We refer to $(q_1, q_2, q_3)$ as a* Goldbach triple for $n$.

**Conjecture 6.3** (Double Goldbach + $\varepsilon$) *Let $n$ be a positive even integer. Then there exist primes $q_1, q_2, q_3, q_4, q_5$ such that $q_4 < q_1 \leq q_2 < q_5 < q_3 < n$ and $q_1 + q_2 = q_4 + q_5 = n$.*

**Theorem 6.4** *Let $p \geq 5$ be prime and let $A/\mathbb{Q}$ be a principally polarised abelian variety of dimension $g$. Suppose:*

(i) *The $G_{\mathbb{Q}}$-action on $A[p]$ is irreducible, primitive and contains a transvection;*
(ii) $\mathbb{Q}_p(A[p]) \cong \mathbb{Q}_p(\zeta_p)$;
(iii) *$A$ is semistable at $\ell$ for all primes $\ell \leq 2g + 1$.*

*Then* $\mathrm{Gal}(\mathbb{Q}(A[p])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_p)$ *and $\mathbb{Q}(A[p])$ is tame. The same holds for $p = 3$ if $A[3] \otimes_{\mathbb{F}_3} \overline{\mathbb{F}}_3$ is irreducible and primitive.*

***Proof*** By [1, Theorem 5.3], condition (i) implies that $\mathrm{Gal}(\mathbb{Q}(A[p])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_p)$ (including $p = 3$). The claim that $\mathbb{Q}(A[p])$ is tame follows from Lemma 2.1.

Before we state an explicit version of the above theorem, we need some quick definitions.

**Definition 6.5** Let $p$ be a prime and let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$ be a squarefree monic polynomial. Fix an integer $t \geq 1$.

(i) We say that $f$ is $t$-Eisenstein at $p$ if $v_p(a_i) \geq t$ for all $i$ and $v_p(a_0) = t$.
(ii) Let $q_1, \ldots, q_k$ be rational primes. We say that $f$ is of type $t - \{q_1, \ldots, q_k\}$ if it can be factored over $\mathbb{Z}_p[x]$ as

$$f(x) = h(x) \prod_{i=1}^{k} g_i(x - \alpha_i),$$

for some $\alpha_i \in \mathbb{Z}_p$ such that $\alpha_i \not\equiv \alpha_j \mod p$ for $i \neq j$, $g_i(x)$ is $t$-Eisenstein of degree $q_i$ and the reduction mod $p$, $\overline{h}(x)$, of $h(x)$ is separable with $\overline{h(\alpha_i)} \neq 0$ for all $i$.

**Theorem 6.6** *Let $C/\mathbb{Q} : y^2 = f(x)$ be a hyperelliptic curve of genus $g$ and Jacobian $J_C$. Assume $2g + 2$ satisfies Conjecture 6.2 and let $(q_1, q_2, q_3)$ be a Goldbach triple. Fix an odd prime $p \neq q_1, q_2, q_3$.*

*Choose primes $p_1, p_2, p_3 > \max(2g + 1, p)$ such that:*

[3] This is sufficient if $\dim A$ is odd [14, Corollaire p. 51]; otherwise we need an extra local condition due to the Mumford–Tate group [10, Theorem 1].

- *$p_2$ is a primitive root modulo $q_1$ and modulo $q_2$;*
- *$p_3$ is a primitive root modulo $q_3$;*
- *If $p = 3$, then moreover suppose that $p_2 \equiv p_3 \equiv 1 \mod 3$.*

*Suppose:*

(i) *$f(x)$ has type $1 - \{2\}$ at $p_1$;*
(ii) *$f(x)$ has type $1 - \{q_1, q_2\}$ at $p_2$;*
(iii) *$f(x)$ has type $2 - \{q_3\}$ at $p_3$;*
(iv) *$J_C$ is semistable at all $\ell \notin \{p_2, p_3\}$;*
(v) *$J_C$ is totally toric at $p$;*
(vi) *$\mathbb{Q}_p(J_C[p]) \cong \mathbb{Q}_p(\zeta_p)$.*

*Then $\mathrm{Gal}(\mathbb{Q}(J_C[p])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_p)$ and $\mathbb{Q}(J_C[p])/\mathbb{Q}$ is tame.*

***Proof*** This is a slight reformulation of [1, Theorem 6.2] where we can weaken some of the hypotheses since $p$ is fixed.

Suppose first that $p \geq 5$. Then condition (i) implies the existence of a transvection [1, Lemma 2.9], whereas (ii) and (iii) imply that $J_C[p]$ is irreducible [1, Lemma 3.2]. Primitivity follows from (iv) and (v) (cf. [1, Remark 6.1]); the result now follows from Theorem 6.4. For the case $p = 3$, the same argument as [1, Theorem 6.5] holds.

**Corollary 6.7** *Fix a positive integer $g$ and assume $2g + 2$ satisfies Conjecture 6.2. Fix an odd prime $p$. If there exists a Goldbach triple for $2g + 2$ not containing $p$, then there exists a curve $C/\mathbb{Q}$ of genus $g$ such that $\mathrm{Gal}(\mathbb{Q}(J_C[p])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_p)$ and $\mathbb{Q}(J_C[p])$ is tame.*

***Remark 6.8*** If $2g + 2$ satisfies Double Goldbach as well (Conjecture 6.3), then the conclusion holds for all odd primes $p$ by applying the statement with the Goldbach triples $(q_4, q_5, q_3)$ and $(q_1, q_2, q_5)$. Double Goldbach has been numerically verified by Anni–Dokchitser (cf. [1, Remark 6.6]) to hold for all $g \leq 10^7$, excepting $g = 1, 2, 3, 4, 5, 7, 13$.

***Remark 6.9*** Observe that if $q = 2g+1$ is prime, then we do not need to use a Goldbach triple; imposing that $f(x)$ has type $1 - \{q\}$ at some large prime ensures that $J_C[p]$ is an irreducible $G_{\mathbb{Q}}$-representation and we only then need to avoid $p = q$ for the same result.

Combining the above results with those of Arias-de-Reyna–Vila for $g \leq 2$ [3, Theorem 1.2], [4, Theorem 5.3] and Remark 6.9, we find that the remaining cases for odd $p$ and small genus are hence as follows:

The reason for these exceptions is that the method of Anni–Dokchitser uses a Goldbach triple to ensure that $J_C[p]$ is an irreducible $G_{\mathbb{Q}}$-module when $p$ is not in the Goldbach triple. Instead, we take a different approach to ensure that the mod $p$ representation is surjective.

**Lemma 6.10** *Let $C/\mathbb{Q} : y^2 = f(x)$ be a hyperelliptic curve of genus $g$. Let*

$$\rho\colon \mathrm{Gal}(\mathbb{Q}(J_C[p])/\mathbb{Q}) \to \mathrm{GSp}_{2g}(\mathbb{F}_p)$$

*be the mod $p$ representation of $J_C$. Suppose that*

| Genus | Primes excluded |
|---|---|
| 3 | 7 |
| 4 | 5, 7 |
| 5 | 11 |
| 7 | 5, 11, 13 |
| 13 | 11, 17. |

(i) *$f$ has type $1-\{2\}$ at some prime $p_1$;*
(ii) *For some prime $\ell \neq p$ of good reduction for $C$, the reduction mod $p$ of the characteristic polynomial of a Frobenius element at $\ell$ is irreducible with nonzero trace.*

*Then $\rho$ is surjective.*

***Proof*** This is just a reformulation of [2, Corollary 2.2], where condition (i) forces the existence of a transvection (cf. proof of Theorem 6.6).

Condition (i) is easy to force at some large prime $p_1 > \max(2g+1, p)$ so it just remains to exhibit curves which satisfy the second condition for each of our exceptional cases in order to give an affirmative answer to the tame inverse Galois problem in these cases as well. In the table below, we give polynomials $f$ defining hyperelliptic curves, and a prime $\ell$ such that the image of $\mathrm{Frob}_\ell$ has the properties required for condition (ii).

| $(g, p)$ | $f(x)$ | $\ell$ |
|---|---|---|
| (3,7) | $x^7+x^3+3x^2+x+1$ | 3 |
| (4,5) | $x^9+x^3+x^2+x+1$ | 3 |
| (4,7) | $x^9+2x^3+2x^2+x+1$ | 3 |
| (5,11) | $x^{11}+x^3+3x^2+x+1$ | 3 |
| (7,5) | $x^{15}+3x^3+x^2+3x+1$ | 3 |
| (7,11) | $x^{15}+4x^3+x^2+5x+1$ | 5 |
| (7,13) | $x^{15}+2x^3+2x^2+2x+1$ | 3 |
| (13,11) | $x^{27}+x^3+2x^2+2x+1$ | 5 |
| (13,17) | $x^{27}+x^3+2x^2+x+1$ | 5 |

Lastly we note that we are unable to do anything in the case $p=2$ since for a hyperelliptic curve, the image of the mod 2 representation is always contained in a subgroup isomorphic to the symmetric group $S_{2g+2}$ and hence will never be surjective for $g \geq 3$.

## Declarations

**Conflict of interest** On behalf of all authors, the corresponding author states that there is no conflict of interest. Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

## References

1. Anni, S., Dokchitser, V.: Constructing hyperelliptic curves with surjective Galois representations. Trans. Am. Math. Soc. **373**, 1477–1500 (2020)
2. Arias-de Reyna, S., Kappen, C.: Abelian varieties over number fields, tame ramification and big Galois image. Math. Res. Lett. **20**(1), 1–17 (2013)
3. Arias-de Reyna, S., Vila, N.: Tame Galois realizations of GL2(Fl) over Q. J. Number Theory **129**(5), 1056–1065 (2009)
4. Arias-de Reyna, S., Vila, N.: Tame Galois realizations of GSp4(Fl) over Q. Int. Math. Res. Not. **9**, 2028–2046 (2011)
5. Birch, B.: Noncongruence subgroups, covers and drawings. In: The Grothendieck Theory of Dessins d'Enfants, pp. 25–46 (1994)
6. Bisatt, M.: Tame torsion, the tame inverse Galois problem, and endomorphisms. Manuscr. Math. **165**, 283–290 (2021)
7. Dokchitser, T.: Models of curves over DVRs. Duke Math. J. (2020). arXiv:1807.00025
8. Grothendieck, A.: Modèles de Néron et monodromie. In: Groupes de Monodromie en Géométrie Algébrique, SGA7 I, Lecture Notes in Mathematics, vol. 288, pp. 313–523. Springer (1972)
9. Gerritzen, L., van der Put, M.: Schottky Groups and Mumford Curves. Springer, Berlin (1980)
10. Hall, C.: An open-image theorem for a general class of abelian varieties. Bull. Lond. Math. Soc. **43**(4), 703–711 (2011)
11. Kadziela, S.: Rigid analytic uniformization of hyperelliptic curves. PhD thesis, University of Illinois at Urbana-Champaign (2007)
12. Kisin, M.: Local constancy in p-adic families of Galois representations. Math. Z. **230**, 569–593 (1999)
13. Morrison, R., Ren, Q.: Algorithms for Mumford curves. J. Symb. Comput. **68**, 259–284 (2015)
14. Serre, J.-P.: Lettre a Marie-France Vignéras. In: Œuvres/Collected papers IV, pp. 38–55. Springer (2000)
15. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. **88**(3), 492–517 (1968)
16. Zarhin, Y.: Hyperelliptic Jacobians without complex multiplication. Math. Res. Lett. **7**(1), 123–132 (2000)