Large Galois images for Jacobian varieties of genus 3 curves

Sara Arias-de-Reyna, Cécile Armana, Valentijn Karemaker,
Marusia Rebolledo, Lara Thomas and Núria Vila

Abstract

Given a prime number $\ell \geq 5$, we construct an infinite family of three-dimensional abelian varieties over $\mathbb{Q}$ such that, for any $A/\mathbb{Q}$ in the family, the Galois representation $\overline{\rho}_{A,\ell}\colon G_{\mathbb{Q}} \to \mathrm{GSp}_6(\mathbb{F}_\ell)$ attached to the ℓ-torsion of A is surjective. Any such variety A will be the Jacobian of a genus 3 curve over $\mathbb{Q}$ whose respective reductions at two auxiliary primes we prescribe to provide us with generators of $\mathrm{Sp}_6(\mathbb{F}_\ell)$.

Introduction

Let ℓ be a prime number. This paper is concerned with realisations of the general symplectic group $\mathrm{GSp}_6(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$, arising from the Galois action on the ℓ-torsion points of three-dimensional abelian varieties defined over $\mathbb{Q}$.

More precisely, let $g \geq 1$ be an integer. One can exploit the theory of abelian varieties defined over $\mathbb{Q}$ as follows. If A is an abelian variety of dimension g defined over $\mathbb{Q}$, let $A[\ell] = A(\overline{\mathbb{Q}})[\ell]$ denote the ℓ-torsion subgroup of $\overline{\mathbb{Q}}$-points of A. The natural action of the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $A[\ell]$ gives rise to a continuous Galois representation $\overline{\rho}_{A,\ell}$ taking values in $\mathrm{GL}(A[\ell]) \simeq \mathrm{GL}_{2g}(\mathbb{F}_\ell)$. If the abelian variety A is moreover principally polarised, the image of $\overline{\rho}_{A,\ell}$ lies inside the general symplectic group $\mathrm{GSp}(A[\ell])$ of $A[\ell]$ with respect to the symplectic pairing induced by the Weil pairing and the polarisation of A; thus, we have a representation

$$\overline{\rho}_{A,\ell} \,:\, G_{\mathbb{Q}} \longrightarrow \mathrm{GSp}(A[\ell]) \simeq \mathrm{GSp}_{2g}(\mathbb{F}_\ell),$$

providing a realisation of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$ if $\overline{\rho}_{A,\ell}$ is surjective.

The image of Galois representations attached to the ℓ-torsion points of abelian varieties has been widely studied. For an abelian variety A defined over a number field, the classical result of Serre ensures surjectivity for almost all primes ℓ when $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$ and the dimension of A is 2, 6 or odd (cf. [23]). More recently, Hall [8] proves a result for any dimension, with the additional condition that A has semistable reduction of toric dimension 1 at some prime. This result has been further generalised to the case of abelian varieties over finitely generated fields (cf. [2]).

We can use Galois representations attached to the torsion points of abelian varieties defined over $\mathbb{Q}$ to address the Inverse Galois Problem and its variations involving ramification conditions. For example, the Tame Inverse Galois Problem, proposed by Birch, asks if, given a finite group G, there exists a tamely ramified Galois extension $K/\mathbb{Q}$ with Galois group isomorphic to G. Arias-de-Reyna and Vila solved the Tame Inverse Galois problem for $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ when $g = 1, 2$ and $\ell \geq 5$ is any prime number, by constructing a family of genus g curves C such that the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the Jacobian variety $\mathrm{Jac}(C)$ is surjective and tamely ramified for every curve in the family (cf. [4], [5]). For both $g = 1$ and $g = 2$, the strategy entails determining a set of local conditions at auxiliary primes, (that is to say, prescribing a finite list of congruences that the defining equation of C should satisfy) which ensure the surjectivity of $\overline{\rho}_{\mathrm{Jac}(C),\ell}$, and a careful study of the ramification at ℓ in particularly favourable situations.

In fact, the strategy of ensuring surjectivity of the Galois representation attached to the ℓ-torsion of an abelian variety by prescribing local conditions at auxiliary primes works in great generality. Given a g-dimensional principally polarised abelian variety A over $\mathbb{Q}$, such that the Galois representation $\overline{\rho}_{A,\ell}$ is surjective, it is always possible to find some auxiliary primes p and q

depending on ℓ such that any abelian variety B defined over $\mathbb{Q}$ which is "close enough" to A with respect to the primes p and q (in a sense that can be made precise in terms of p-adic, resp. q-adic, neighbourhoods in moduli spaces of principally polarised g-dimensional abelian varieties with full level structure) also has a surjective ℓ-torsion Galois representation $\overline{\rho}_{B,\ell}$. This is a consequence of Kisin's results on local constancy in p-families of Galois representations; the reader can find a detailed explanation of this aspect in [3, Section 4.2].

In this paper we focus on the case $g = 3$. Our aim is to find auxiliary primes p and q (depending on ℓ), and explicit congruence conditions on polynomials defining genus 3 curves, which ensure that any curve C, defined by an equation over $\mathbb{Z}$ satisfying these congruences, will have the property that the image of $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ coincides with $\mathrm{GSp}_6(\mathbb{F}_\ell)$. In this way we obtain many distinct realisations of $\mathrm{GSp}_6(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$.

To state our main result, we introduce the following notation: we will say that a polynomial $f(x, y)$ in two variables is of *3-hyperelliptic type* if it is of the form $f(x, y) = y^2 - g(x)$, where $g(x)$ is a polynomial of degree 7 or 8 and of *quartic type* if the total degree of $f(x, y)$ is 4.

Theorem 0.1. Let $\ell \geq 13$ be a prime number. For all odd distinct prime numbers $p, q \neq \ell$, with $q > 1.82\ell^2$, there exist $f_p(x, y), f_q(x, y) \in \mathbb{Z}[x, y]$ of the same type (3-hyperelliptic or quartic), such that for any $f(x, y) \in \mathbb{Z}[x, y]$ of the same type as $f_p(x, y)$ and $f_q(x, y)$ and satisfying

$$f(x, y) \equiv f_q(x, y) \pmod q \quad \text{and} \quad f(x, y) \equiv f_p(x, y) \pmod{p^3},$$

the image of the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the ℓ-torsion points of the Jacobian of the projective genus 3 curve C defined over $\mathbb{Q}$ by the equation $f(x, y) = 0$ is $\mathrm{GSp}_6(\mathbb{F}_\ell)$.

Moreover, for $\ell \in \{5, 7, 11\}$ there exists a prime number $q \neq \ell$ for which the same statement holds for each odd prime number $p \neq q, \ell$.

In Section 4 we state and prove a refinement of this Theorem (cf. Theorem 4.1). In fact, we have a very explicit control of the polynomial $f_p(x, y)$. In general we can say little about $f_q(x, y)$, but for any fixed $\ell \geq 13$ and any fixed $q \geq 1.82\ell^2$ we can find suitable polynomials $f_q(x, y)$ by an exhaustive search as follows: there exist only finitely many polynomials $\bar{f}_q(x, y) \in \mathbb{F}_q[x, y]$ of 3-hyperelliptic or quartic type with non-zero discriminant. For each of these, we can compute the characteristic polynomial of the action of the Frobenius endomorphism on the Jacobian of the curve defined by $\bar{f}_q(x, y) = 0$ by counting the $\mathbb{F}_{q^r}$-points of this curve, for $r = 1, 2, 3$, and check whether this polynomial is an ordinary q-Weil polynomial with non-zero middle coefficient, non-zero trace modulo ℓ, and which is irreducible modulo ℓ. Proposition 3.5 ensures that the search will terminate. Then, any lift of $\bar{f}_q(x, y)$, of the same type, gives us a suitable polynomial $f_q(x, y) \in \mathbb{Z}[x, y]$.

Note that the above result constitutes an explicit version of Proposition 4.6 of [3] in the case of principally polarised 3-dimensional abelian varieties. We can explicitly give the size of the neighbourhoods where surjectivity of $\overline{\rho}_{A,\ell}$ is preserved; in other words, we can give the powers of the auxiliary primes p and q such that any other curve defined by congruence conditions modulo these powers gives rise to a Jacobian variety with surjective ℓ-torsion representation.

The proof of Theorem 0.1 is based on two main pillars: the classification of subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ containing a non-trivial transvection, and the fact that one can force the image of $\overline{\rho}_{A,\ell}$ to contain a non-trivial transvection by imposing a specific type of ramification at an auxiliary prime. This strategy goes back to Le Duff [13] in the case of Jacobians of genus 2 hyperelliptic curves, and has been extended to the general case by Hall in [8], where he obtains a surjectivity result for $\overline{\rho}_{A,\ell}$ for almost all primes ℓ.

We already followed this strategy in [1] to formulate an explicit surjectivity result for g-dimensional abelian varieties (see Theorem 3.10 of loc. cit.): let A be a principally polarised g-dimensional abelian variety defined over $\mathbb{Q}$, such that the reduction of the Néron model of A at some prime p is semistable with toric rank 1, and the Frobenius endomorphism at some prime q of good reduction for A acts irreducibly and with trace $a \neq 0$ on the reduction of the Néron model of

A at q. We proved that for each prime number $\ell \nmid 6pqa$, coprime with the order of the component group of the Néron model of A at p, and such that the characteristic polynomial of the Frobenius endomorphism at q is irreducible mod ℓ, then the representation $\overline{\rho}_{A,\ell}$ is surjective.

Section 1 collects some notations and tools that we will use in the rest of the paper. In Section 2 we address the condition of semistable reduction of toric rank 1 at a prime p; we obtain a congruence condition modulo p^3 (cf. Proposition 2.3).

In Section 3 we give conditions ensuring that the reduction of the Néron model of a Jacobian variety $A = \mathrm{Jac}(C)$ at a prime q is an absolutely simple abelian variety over $\mathbb{F}_q$ such that the characteristic polynomial of the Frobenius endomorphism at q is irreducible and has non-zero trace modulo ℓ (cf. Theorem 3.1). We make use of Honda-Tate Theory in the ordinary case, which relates so-called ordinary Weil polynomials to isogeny classes of ordinary abelian varieties defined over finite fields of characteristic q. First, we need to prove the existence of a suitable prime q and a suitable ordinary Weil polynomial; this is the content of Proposition 3.5, whose proof is postponed to Section 5. This polynomial provides us with an abelian variety A_q defined over $\mathbb{F}_q$; any abelian variety A such that the reduction of the Néron model of A at q coincides with A_q will satisfy the desired condition at q. At this point we use the fact that each principally polarised 3-dimensional abelian variety over $\mathbb{F}_q$ is the Jacobian of a genus 3 curve, which can be defined over $\mathbb{F}_q$ up to a quadratic twist.

Once we have established congruence conditions at auxiliary primes p and q, we need to check that any curve C over $\mathbb{Z}$ whose defining equation satisfies these conditions will provide us with a Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ whose image is $\mathrm{GSp}_6(\mathbb{F}_\ell)$. This is carried out in Section 4.

David Zywina communicated to us that he has recently and independently developed a method for studying the image of Galois representations $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the Jacobians of genus 3 plane quartic curves C, for a large class of such curves (cf. [26]). In particular, for each prime ℓ, he obtains a realisation of $\mathrm{GSp}_6(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$.

Acknowledgements.– We are very grateful to Christophe Ritzenthaler for many insightful suggestions. We want to thank Jean-Pierre Serre for pointing us to the references [25, 22] and for a useful discussion on the literature for the descent of curves over finite fields (see Remark 3.7). We want to thank Irene Bouw and Matthieu Romagny for providing us with clarifications regarding the geometry of curves. Finally, we thank David Zywina for sending us his preprint [26].

This collaboration was initiated during the WIN-Europe conference in Luminy, 2013. We are grateful for the hospitality of the Institut Henri Poincaré during a short visit. S. Arias-de-Reyna and N. Vila are partially supported by the project MTM2012-33830 of the Ministerio de Economía y Competitividad of Spain, C. Armana by a BQR 2013 Grant from Université de Franche-Comté and M. Rebolledo by the ANR Project Régulateurs ANR-12-BS01- 0002. L. Thomas would like to thank the Laboratoire de Mathématiques de Besançon for its support.

1 Geometric preliminaries

In this section we recall some background from algebraic geometry and fix some notations.

1.1 Hyperelliptic curves and curves of genus 3

A smooth geometrically connected projective curve[1] C of genus $g \geq 1$ over a field K is *hyperelliptic* if there exists a degree 2 finite separable morphism from $C_{\overline{K}} = C \times_K \overline{K}$ to $\mathbb{P}^1_{\overline{K}}$. If K is algebraically closed or a finite field, then such a curve C has a *hyperelliptic equation* defined over K[2]. That is to say, the function field of C is $K(x)[y]$ under the relation $y^2 + h(x)y = g(x)$ with $g(x), h(x) \in K[x]$, $\deg(g(x)) \in \{2g+1, 2g+2\}$, and $\deg(h(x)) \leq g$. Moreover, if $\mathrm{char}(K) \neq 2$, we can take

[1] In this article, we will say that a *curve over a field* K is an algebraic variety over K whose irreducible components are of dimension 1. (In particular, a curve can be singular.)

[2] When K is not algebraically closed nor a finite field, the situation can be more complicated (cf. [14, Section 4.1]).

$h(x) = 0$. Indeed, in that case, the conic defined as the quotient of C by the group generated by the hyperelliptic involution has a K-rational point, hence is isomorphic to $\mathbb{P}^1_K$ (see e.g. [14, Section 1.3] for more details). The curve C is the union of the two affine open schemes

$$U = \mathrm{Spec}\left(K[x,y]/(y^2 + h(x)y - g(x))\right) \quad \text{and}$$
$$V = \mathrm{Spec}\left(K[t,w]/(w^2 + t^{g+1}h(1/t)y - t^{2g+2}g(1/t))\right)$$

glued along $\mathrm{Spec}(K[x,y,1/x]/(y^2 + h(x)y - g(x)))$ via the identifications $x = 1/t, y = t^{-g-1}w$.

If $\mathrm{char}(K) \neq 2$, then any separable polynomial $g(x) \in K[x]$ of degree $2g+1$ or $2g+2$ gives rise to a hyperelliptic curve C of genus g defined over K by glueing the open affine schemes U and V (with $h(x) = 0$) as above. We will say that C is *given by the hyperelliptic equation* $y^2 = g(x)$. We will also say, as in the introduction, that a polynomial in two variables is of *g-hyperelliptic type* if it is of the form $y^2 - g(x)$ with $g(x)$ a polynomial of degree $2g+1$ or $2g+2$.

In this article, we are especially interested in curves of genus 3. If C is a smooth geometrically connected projective non-hyperelliptic curve of genus 3 defined over a field K, then its canonical embedding $C \hookrightarrow \mathbb{P}^2_K$ identifies C with a smooth plane quartic curve defined over K. This means that the curve C has a model over K given by $\mathrm{Proj}(K[X,Y,Z]/F(X,Y,Z))$ where $F(X,Y,Z)$ is a degree 4 homogeneous polynomial with coefficients in K. Conversely, any smooth plane quartic curve is the image by a canonical embedding of a non-hyperelliptic curve of genus 3. If this curve is $\mathrm{Proj}(K[X,Y,Z]/F(X,Y,Z))$ where $F(X,Y,Z)$ is the homogenisation of a degree 4 polynomial $f(x,y) \in K[x,y]$, we will say that C is the *quartic plane curve defined by the affine equation* $f(x,y) = 0$. We will say, as in the introduction, that a polynomial in two variables is of *quartic type* if its total degree is 4.

1.2 Semistable curves and their generalised Jacobians

We briefly recall the basic notions we need about semistable and stable curves, give the definition of the intersection graph of a curve and explain the link between this graph and the structure of their generalised Jacobian. The classical references we use are essentially [15] and [6]. For a nice overview which contains other references, the reader could also consult [18].

A curve C over a field k is said to be *semistable* if the curve $C_{\overline{k}} = C \times_k \overline{k}$ is reduced and has at most ordinary double points as singularities. It is said to be *stable* if moreover $C_{\overline{k}}$ is connected, projective of arithmetic genus ≥ 2, and if any irreducible component of $C_{\overline{k}}$ isomorphic to $\mathbb{P}^1_{\overline{k}}$ intersects the other irreducible components in at least three points. A proper flat morphism of schemes $\mathcal{C} \to S$ is said to be *semistable* (resp. *stable*) if it has semistable (resp. stable) geometric fibres.

Let R be a discrete valuation ring with fraction field K and residue field k. Let C be a smooth projective geometrically connected curve over K. A *model* of C over R is a normal scheme $\mathcal{C}/R$ such that $\mathcal{C} \times_R K \cong C$. We say that C has *semistable reduction* (resp. *stable reduction*) if C has a model $\mathcal{C}$ over R which is a semistable (resp. stable) scheme over R. If such a stable model exists, it is unique up to isomorphism and we call it *the stable model of C over R* (cf. [15, Chap.10, Definition 3.27 and Theorem 3.34]). If the curve C has genus $g \geq 1$, then it admits a minimal regular model $\mathcal{C}_{min}$ over R, unique up to unique isomorphism. Moreover, $\mathcal{C}_{min}$ is semistable if and only if C has semistable reduction, and if $g \geq 2$, this is equivalent to C having stable reduction (cf. [15, Chap. 10, Theorem 3.34], or [18, Theorem 3.1.1] when R is strictly henselian).

Assume that C is a smooth projective geometrically connected curve of genus $g \geq 2$ over K with semistable reduction. Denote by $\mathcal{C}$ its stable model over R and by $\mathcal{C}_{min}$ its minimal regular model over R. We know that the Jacobian variety $J = \mathrm{Jac}(C)$ of C admits a Néron model $\mathcal{J}$ over R and the canonical morphism $\mathrm{Pic}^0_{\mathcal{C}/R} \to \mathcal{J}^0$ is an isomorphism (cf. [6, §9.7, Corollary 2]). Note that since $\mathcal{C}_{min}$ is also semistable, we have $\mathrm{Pic}^0_{\mathcal{C}_{min}/R} \cong \mathcal{J}^0$. Moreover, the abelian variety J has semistable reduction, that is to say $\mathcal{J}^0_k \cong \mathrm{Pic}^0_{\mathcal{C}_k/k}$ is canonically an extension of an abelian variety by a torus T. As we will see, the structure of the algebraic group $\mathcal{J}^0_k$ (by which we mean the toric rank and the order of the component group of its geometric special fibre) is related to the intersection graphs of $\mathcal{C}_{\overline{k}}$ and $\mathcal{C}_{min,\overline{k}}$.

Let X be a curve over $\overline{k}$. Consider the *intersection graph* (or *dual graph*) $\Gamma(X)$, defined as the graph whose vertices are the irreducible components of X, where two irreducible components X_i and X_j are connected by as many edges as there are irreducible components in the intersection $X_i \cap X_j$. In particular, if the curve X is semistable, two components X_i and X_j are connected by one edge if there is a singular point lying on both X_i and X_j. Here $X_i = X_j$ is allowed. The *(intersection) graph without loops*, denoted by $\Gamma'(X)$, is the graph obtained by removing from $\Gamma(X)$ the edges corresponding to $X_i = X_j$.

Next, we paraphrase [6, §9.2, Example 8], which gives the toric rank in terms of the cohomology of the graph $\Gamma(\mathcal{C}_{\overline{k}})$.

Proposition 1.1 ([6], §9.2, Ex. 8)**.** The Néron model $\mathcal{J}$ of the Jacobian of the curve $\mathcal{C}_k$ has semistable reduction. More precisely, let $X_1, \ldots, X_r$ be the irreducible components of $\mathcal{C}_k$, and let $\widetilde{X}_1, \ldots, \widetilde{X}_r$ be their respective normalisations. Then the canonical extension associated to $\mathrm{Pic}^0_{\mathcal{C}_k/k}$ is given by the exact sequence

$$1 \longrightarrow T \hookrightarrow \mathrm{Pic}^0_{\mathcal{C}_k/k} \xrightarrow{\pi^*} \prod_{i=1}^{r} \mathrm{Pic}^0_{\widetilde{X}_i/k} \longrightarrow 1$$

where the morphism π^* is induced by the morphisms $\pi_i : \widetilde{X}_i \longrightarrow X_i$. The rank of the torus T is equal to the rank of the cohomology group $H^1(\Gamma(\mathcal{C}_{\overline{k}}), \mathbb{Z})$.

We will use the preceding result in Sections 2 and 3. Note that the toric rank does not change if we replace $\mathcal{C}$ by $\mathcal{C}_{min}$.

The intersection graph of $\mathcal{C}_{min,\overline{k}}$ also determines the order of the component group of the geometric special fibre $\mathcal{J}_{\overline{k}}$. Indeed, the scheme $\mathcal{C}_{min} \times R^{sh}$, where R^{sh} is the strict henselisation of R, fits the hypotheses of [6, §9.6, Proposition 10] which gives the order of the component group in terms of the graph of $\mathcal{C}_{min,\overline{k}}$; we reproduce it here for the reader's convenience.

Proposition 1.2 ([6], §9.6, Prop. 10)**.** Let X be a proper and flat curve over a strictly henselian discrete valuation ring R with algebraically closed residue field $\overline{k}$. Suppose that X is regular and has geometrically irreducible generic fibre as well as a geometrically reduced special fibre $X_{\overline{k}}$. Assume that $X_{\overline{k}}$ consists of the irreducible components $X_1, \ldots, X_r$ and that the local intersection numbers of the X_i are 0 or 1 (the latter is the case if different components intersect at ordinary double points). Furthermore, assume that the intersection graph without loops $\Gamma'(X_{\overline{k}})$ consists of l arcs of edges $\lambda_1, \ldots, \lambda_l$, starting at X_1 and ending at X_r, each arc λ_i consisting of m_i edges. Then the component group $\mathcal{J}(R^{sh})/\mathcal{J}^0(R^{sh})$ has order $\sum_{i=1}^{l} \prod_{j \neq i} m_j$.

We will use this result in the proof of Proposition 2.3.

2 Local conditions at p

Let $p > 2$ be a prime number. Denote by $\mathbb{Z}_p$ the ring of p-adic integers and by $\mathbb{Q}_p$ the field of p-adic numbers.

Definition 2.1. Let $f(x,y) \in \mathbb{Z}_p[x,y]$ be a polynomial with $f(0,0) = 0$ or $v_p(f(0,0)) > 2$. We say that $f(x,y)$ is of type:

(H) if $f(x,y) = y^2 - g(x)$, where $g(x) \in \mathbb{Z}_p[x]$ is of degree 7 or 8 and such that

$$g(x) \equiv x(x-p)m(x) \bmod p^2\mathbb{Z}_p[x],$$

with $m(x) \in \mathbb{Z}_p[x]$ such that its mod p reduction has simple non-zero roots in $\mathbb{F}_p$;

(Q) if $f(x,y)$ is of total degree 4 and such that

$$f(x,y) \equiv px + x^2 - y^2 + x^4 + y^4 \bmod p^2\mathbb{Z}_p[x,y].$$

For $f(x,y) \in \mathbb{Z}_p[x,y]$ a polynomial of type (H) or (Q), we will consider the projective curve C defined by $f(x,y) = 0$ as explained in Subsection 1.1 and the scheme $\mathcal{C}$ over $\mathbb{Z}_p$ defined, for each case of Definition 2.1 respectively, as follows:

(H) the union of the two affine subschemes

$$U = \mathrm{Spec}(\mathbb{Z}_p[x,y]/(y^2 - g(x))) \text{ and } V = \mathrm{Spec}(\mathbb{Z}_p[t,w]/(w^2 - g(1/t)t^8))$$

glued along $\mathrm{Spec}(\mathbb{Z}_p[x,y,1/x]/(y^2 - g(x))$ via $x = 1/t, y = t^{-4}w$;

(Q) the scheme $\mathrm{Proj}(\mathbb{Z}_p[X,Y,Z]/(F(X,Y,Z)))$, where $F(X,Y,Z)$ is the homogenisation of $f(x,y)$.

This scheme has generic fibre C.

Proposition 2.2. Let $f(x,y) \in \mathbb{Z}_p[x,y]$ be a polynomial of type (H) or (Q) and C be the projective curve defined by $f(x,y) = 0$. The curve C is a smooth projective and geometrically connected curve of genus 3 over $\mathbb{Q}_p$ with stable reduction. Moreover, the scheme $\mathcal{C}$ is the stable model of C over $\mathbb{Z}_p$ and the stable reduction is geometrically integral with exactly one singularity, which is an ordinary double point.

Proof. With the description we gave in Subsection 1.1 of what we called the *projective curve defined by* f, smoothness over $\mathbb{Q}_p$ follows from the Jacobian criterion. This implies that C is a projective curve of genus 3.

The polynomials defining the affine schemes U and V and the quartic polynomial $F(X,Y,Z)$ are all irreducible over $\overline{\mathbb{Q}}_p$, hence over $\mathbb{Z}_p$. So the curve C is geometrically integral (hence geometrically irreducible and geometrically connected) and $\mathcal{C}$ is integral as a scheme over $\mathbb{Z}_p$. It follows in particular that $\mathcal{C}$ is flat over $\mathbb{Z}_p$ (cf. [15, Chap. 4, Corollary 3.10]). Hence, $\mathcal{C}$ is a model of C over $\mathbb{Z}_p$.

We will show that $\mathcal{C}_{\mathbb{F}_p}$ is semistable (i.e. reduced with only ordinary double points as singularities) with exactly one singularity.

Combined with flatness, semistability will imply that the scheme $\mathcal{C}$ is semistable over $\mathbb{Z}_p$. Since C has genus greater than 2, and $C = \mathcal{C}_{\mathbb{Q}_p}$ is smooth and geometrically connected, this is then equivalent to saying that C has stable reduction at p with stable model $\mathcal{C}$, as required (cf. [18, Theorem 3.1.1]).

In what follows, we denote by $\bar{\cdot}$ the reduction modulo p of any polynomial with coefficient in $\mathbb{Z}_p$. In Case (H), $\mathcal{C}_{\overline{\mathbb{F}}_p}$ is the union of the two affine subschemes $U' = \mathrm{Spec}(\overline{\mathbb{F}}_p[x,y]/(y^2 - x^2\bar{m}(x)))$ and $V' = \mathrm{Spec}(\overline{\mathbb{F}}_p[t,w]/(w^2 - \bar{m}(1/t)t^6))$, glued along $\mathrm{Spec}(\overline{\mathbb{F}}_p[x,y,1/x]/(y^2 - \bar{g}(x))$ via $x = 1/t$ and $y = t^{-4}w$ (cf. [15, Chap. 10, Example 3.5]). In Case (Q), the geometric special fibre is $\mathrm{Proj}(\overline{\mathbb{F}}_p[X,Y,Z]/(\bar{F}(X,Y,Z)))$. In both cases, the defining polynomials are irreducible over $\overline{\mathbb{F}}_p$. Hence, $\mathcal{C}_{\overline{\mathbb{F}}_p}$ is integral, i.e. reduced and irreducible.

Next, we prove that $\mathcal{C}_{\overline{\mathbb{F}}_p}$ has only one ordinary double point as singularity. For Case (H), see e.g. [15, Chap. 10, Examples 3.4, 3.5 and 3.29]. For Case (Q), we proceed analogously: first consider the open affine subscheme of $\mathcal{C}_{\overline{\mathbb{F}}_p}$ defined by $U = \mathrm{Spec}(\overline{\mathbb{F}}_p[x,y]/\bar{f}(x,y))$, where $\bar{f}(x,y) = x^2 - y^2 + x^4 + y^4 \in \mathbb{F}_p[x,y]$. Since $\mathcal{C}_{\overline{\mathbb{F}}_p} \backslash U$ is smooth, it suffices to prove that U has only ordinary double singularities. Let $u \in U$. The Jacobian criterion shows that U is smooth at $u \neq (0,0)$. So suppose that $u = (0,0)$, and note that $\bar{f}(x,y) = x^2(1+x^2) - y^2(1-y^2)$. Since $2 \in \overline{\mathbb{F}}_p^\times$, there exist $a(x) = 1 + xc(x) \in \overline{\mathbb{F}}_p[[x]]$ and $b(y) = 1 + yd(y) \in \overline{\mathbb{F}}_p[[y]]$ such that $1 + x^2 = a(x)^2$ and $1 - y^2 = b(y)^2$, by ([15, Chap. 1, Exercise 3.9]). Then we have

$$\widehat{\mathcal{O}}_{U,u} \cong \overline{\mathbb{F}}_p[[x,y]]/(xa(x) + yb(y))(xa(x) - yb(y)) \cong \overline{\mathbb{F}}_p[[t,w]]/(tw).$$

It follows that $\mathcal{C}_{\overline{\mathbb{F}}_p}$ has only one singularity (at $[0:0:1]$) which is an ordinary double singularity. We have thus showed that $\mathcal{C}$ is the stable model of C over $\mathbb{Z}_p$ and that its special fibre is geometrically integral and has only one ordinary double singularity.

$\square$

Proposition 2.3. Let $f(x,y) \in \mathbb{Z}_p[x,y]$ be a polynomial of type (H) or (Q) and C be the projective curve defined by $f(x,y)=0$. The Jacobian variety $\mathrm{Jac}(C)$ of the curve C has a Néron model $\mathcal{J}$ over $\mathbb{Z}_p$ which has semi-abelian reduction of toric rank 1. The component group of the geometric special fibre of $\mathcal{J}$ over $\overline{\mathbb{F}}_p$ has order 2.

Proof. By Proposition 2.2, the curve C is a smooth projective geometrically connected curve of genus 3 over $\mathbb{Q}_p$ with stable reduction and stable model $\mathcal{C}$ over $\mathbb{Z}_p$. Let $\mathcal{C}_{min}$ be the minimal regular model of C. As recalled in Subsection 1.2, $\mathrm{Jac}(C)$ admits a Néron model $\mathcal{J}$ over $\mathbb{Z}_p$ and the canonical morphism $\mathrm{Pic}^0_{\mathcal{C}/\mathbb{Z}_p} \to \mathcal{J}^0$ is an isomorphism. In particular, $\mathcal{J}$ has semi-abelian reduction and $\mathcal{J}^0_{\overline{\mathbb{F}}_p} \cong \mathrm{Pic}^0_{\mathcal{C}_{\overline{\mathbb{F}}_p}/\overline{\mathbb{F}}_p}$. Since $\mathcal{C}_{min}$ is also semistable, we have $\mathrm{Pic}^0_{\mathcal{C}_{min}/S} \cong \mathcal{J}^0$.

By Proposition 1.1, the toric rank of $\mathcal{J}^0_{\overline{\mathbb{F}}_p}$ is equal to the rank of the cohomology group of the dual graph of $\mathcal{C}_{\overline{\mathbb{F}}_p}$. Since $\mathcal{C}_{\overline{\mathbb{F}}_p}$ is irreducible and has only one ordinary double point, the dual graph consists of one vertex and one loop, so the rank of $\mathcal{J}^0_{\overline{\mathbb{F}}_p}$ is 1.

To determine the order of the component group of the geometric special fibre $\mathcal{J}_{\overline{\mathbb{F}}_p}$, we apply Proposition 1.2 to the minimal regular model $\mathcal{C}_{min} \times \mathbb{Z}_p^{sh}$, where $\mathbb{Z}_p^{sh}$ is the strict henselisation of $\mathbb{Z}_p$. This is still regular and semistable over $\mathbb{Z}_p^{sh}$ (cf. [15, Chap. 10, Proposition 3.15-(a)]). Let e denote the thickness of the ordinary double point of $\mathcal{C}_{\overline{\mathbb{F}}_p}$ (as defined in [15, Chap. 10, Definition3.23]). Then by [15, Chap. 10, Corollary 3.25], the geometric special fibre $\mathcal{C}_{min,\overline{\mathbb{F}}_p}$ of $\mathcal{C}_{min} \times \mathbb{Z}_p^{sh}$ consists of a chain of $e-1$ projective lines over $\mathbb{F}_p$ and one component of genus 2 (where the latter corresponds to the irreducible component $\mathcal{C}_{\overline{\mathbb{F}}_p}$), which meet transversally at rational points. It follows from Proposition 1.1 that the order of the component group $\mathcal{J}(\mathbb{Z}_p^{sh})/\mathcal{J}^0(\mathbb{Z}_p^{sh})$ of the geometric special fibre is equal to the thickness e.

We will now show that in both cases (H) and (Q), the thickness e is equal to 2, which will conclude the proof of Proposition 2.3. For this, in several places, we will use the well-known fact that every formal power series in $\mathbb{Z}_p[[x]]$ (resp. $\mathbb{Z}_p[[y]]$, $\mathbb{Z}_p[[x,y]]$) with constant term 1 (or more generally a unit square in $\mathbb{Z}_p$) is a square in $\mathbb{Z}_p[[x]]$ (resp. $\mathbb{Z}_p[[y]]$, $\mathbb{Z}_p[[x,y]]$) of some invertible formal power series.

Let U denote the affine subscheme $\mathrm{Spec}(\mathbb{Z}_p[x,y]/(f(x,y)))$ which contains the ordinary double point $P=[0:0:1]$. Firstly, we claim that, possibly after a finite extension of scalars $R/\mathbb{Z}_p$ which splits the singularity, in both cases we may write in $R[[x,y]]$:

$$\pm f(x,y) = x^2a(x)^2 - y^2b(y)^2 + p\alpha x + p^2yg(x,y) + p^r\beta \tag{1}$$

where $a(x) \in R[[x]]^\times, b(y) \in R[[y]]^\times, g(x,y) \in \mathbb{Z}_p[x,y], \alpha \in \mathbb{Z}_p^\times,\ \beta \in \mathbb{Z}_p$. Moreover, from the assumptions on f, it follows that either $\beta=0$, or $\beta \in \mathbb{Z}_p^\times$ and $r = v_p(f(0,0)) > 2$.

We prove the claim case by case:

(H) We have $f(x,y) = y^2 - g(x) = y^2 - x(x-p)m(x) + p^2h(x)$ for some $h(x) \in \mathbb{Z}_p[x]$. Since $h(x) = h(0) + xs(x)$ for some $s(x) \in \mathbb{Z}_p[x]$ and $m(x) + ps(x) = m(0) + ps(0) + xt(x)$ for some $t(x) \in \mathbb{Z}_p[x]$, we obtain

$$\begin{aligned} f(x,y) &= y^2 - x^2m(x) + px(m(x)+ps(x)) + p^2h(0) \\ &= y^2 - x^2(m(x)-pt(x)) + px(m(0)+ps(0)) + p^2h(0). \end{aligned}$$

Since $m(0) \not\equiv 0 \pmod p$, we have $m(0) - pt(0) \in \mathbb{Z}_p^\times$, hence if we extend the scalars to some finite extension R over $\mathbb{Z}_p$, in which $m(0)-pt(0)$ is a square, we get that $(m(x)-pt(x))$ is a square of some $a(x)$ in $R[[x]]^\times$. Then $-f(x,y)$ has the expected form. Note that $R/\mathbb{Z}_p$ is unramified because $p \neq 2$ and $m(0) \not\equiv 0 \pmod p$, so we still denote the ideal of R above $p \in \mathbb{Z}_p$ by p.

(Q) We have $f(x,y) = x^4 + y^4 + x^2 - y^2 + px + p^2 h(x,y)$ for some $h(x,y) \in \mathbb{Z}_p[x,y]$. We may write $h(x,y) = \delta + x\gamma + x^2 s(x) + yt(x,y)$ for some $\gamma, \delta \in \mathbb{Z}_p$, $s(x) \in \mathbb{Z}_p[x]$ and $t(x,y) \in \mathbb{Z}_p[x,y]$. We obtain

$$\begin{aligned} f(x,y) &= x^2(1+x^2) - y^2(1-y^2) + px + p^2(\delta + x\gamma + x^2 s(x) + yt(x,y)) \\ &= x^2(1+x^2+p^2 s(x)) - y^2(1-y^2) + px(1+p\gamma) + p^2 yt(x,y) + p^2\delta. \end{aligned}$$

Since $1+x^2+p^2s(x)$ and $1-y^2$ have constant terms which are squares in $\mathbb{Z}_p^\times$, the formal power series are squares in $\mathbb{Z}_p[[x]]$, resp. $\mathbb{Z}_p[[y]]$. So $f(x,y)$ again has the desired form.

Next, we show that $e = 2$ for $\pm f(x,y)$ of the form (1). In $R[[x,y]]$, we have

$$\pm f(x,y) = \left(xa(x) + p\frac{\alpha}{2a(x)}\right)^2 - \left(yb(y) - p^2\frac{g(x,y)}{2b(y)}\right)^2 + p^2 c(x,y),$$

where $c(x,y) = p^{r-2}\beta - \frac{\alpha^2}{4a(x)^2} + p^2\frac{g(x,y)^2}{4b(y)^2}$. Since either $\beta = 0$ or $r > 2$ and $\frac{\alpha^2}{4a(0)^2} \not\equiv 0 \pmod p$, the constant term γ of the formal power series $c(x,y)$ belongs to $R^\times$. It follows that $\gamma^{-1}c(x,y)$ is the square of some formal power series $d(x,y) \in R[[x,y]]^\times$. Defining the variables

$$u = \frac{xa(x)}{d(x,y)} + p\frac{\alpha}{2a(x)d(x,y)} - \frac{yb(y)}{d(x,y)} + p^2\frac{g(x,y)}{2b(y)d(x,y)}$$

and

$$v = \frac{xa(x)}{d(x,y)} + p\frac{\alpha}{2a(x)d(x,y)} + \frac{yb(y)}{d(x,y)} - p^2\frac{g(x,y)}{2b(y)d(x,y)},$$

we get $\widehat{O}_{U\times R,P} \cong R[[u,v]]/(uv \pm p^2\gamma)$. Since $\gamma \in R^\times$, it follows that $e = 2$.

□

3 Local conditions at q

This section is devoted to the proof of the following key result. In the statement, the two conditions on the characteristic polynomial, namely non-zero trace and irreducibility modulo ℓ, are the ones appearing in Theorem 2.10 of [1] which is used to prove the main Theorem 0.1.

Theorem 3.1. Let $\ell \geq 13$ be a prime number. For every prime number $q > 1.82\ell^2$, there exists a smooth geometrically connected curve C_q of genus 3 over $\mathbb{F}_q$ whose Jacobian variety $\mathrm{Jac}(C_q)$ is a 3-dimensional ordinary absolutely simple abelian variety such that the characteristic polynomial of its Frobenius endomorphism is irreducible modulo ℓ and has non-zero trace modulo ℓ.

Moreover, for $\ell \in \{3,5,7,11\}$, there exists a prime number $q > 1.82\ell^2$ such that the same statement holds.

For any integer $g \geq 1$, a g-dimensional abelian variety over a finite field k with q elements is said to be *ordinary* if its group of $\mathrm{char}(k)$-torsion points has rank g.

The proof of Theorem 3.1 relies on Honda-Tate theory, which relates abelian varieties to Weil polynomials:

Definition 3.2. A *Weil q-polynomial*, or simply a *Weil polynomial*, is a monic polynomial $P_q(X) \in \mathbb{Z}[X]$ of even degree $2g$ whose complex roots are all *Weil q-numbers*, i.e., algebraic integers with absolute value $\sqrt{q}$ under all of their complex embeddings. Moreover, a Weil q-polynomial is said to be *ordinary* if its middle coefficient is coprime to q.

In particular, for $g = 3$, every Weil q-polynomial of degree 6 is of the form

$$P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3$$

for some integers a, b and c (cf. [10, Proposition 3.4]). Such a Weil polynomial is ordinary if, moreover, c is coprime to q.

Conversely, not every polynomial of this form is a Weil polynomial. However, we will prove in Proposition 5.1 that for $q > 1.82\ell^2$, every polynomial as above with $|a|, |b|, |c| < \ell$ is a Weil q-polynomial.

As an important example, the characteristic polynomial of the Frobenius endomorphism of an abelian variety over $\mathbb{F}_q$ is a Weil q-polynomial, by the Riemann hypothesis as proven by Deligne.

A variant of the Honda-Tate Theorem (cf. [10, Theorem 3.3]) states that the map which sends an ordinary abelian variety over $\mathbb{F}_q$ to the characteristic polynomial of its Frobenius endomorphism induces a bijection between the set of isogeny classes of ordinary abelian varieties of dimension $g \geq 1$ over $\mathbb{F}_q$ and the set of ordinary Weil q-polynomials of degree $2g$. Moreover, under this bijection, isogeny classes of simple ordinary abelian varieties correspond to irreducible ordinary Weil q-polynomials.

Hence, the proof of Theorem 3.1 consists in proving the existence of an irreducible ordinary Weil q-polynomial of degree 6 which gives rise to an isogeny class of simple ordinary abelian varieties of dimension 3. By Howe (cf. [10, Theorem 1.2]), such an isogeny class contains a principally polarised abelian variety A over $\mathbb{F}_q$, which is the Jacobian variety of some curve C_q defined over $\overline{\mathbb{F}}_q$ by results due to Oort and Ueno. If this abelian variety A is moreover absolutely simple, the curve is geometrically irreducible and we can conclude by a Galois descent argument. Thus, it is a natural question whether the Weil q-polynomial determines if the abelian varieties in the isogeny class are absolutely simple.

In [11], Howe and Zhu give a sufficient condition for an abelian variety over a finite field to be absolutely simple; for ordinary varieties, this condition is also necessary. Let A be a simple abelian variety over a finite field, π its Frobenius endomorphism and $m_A(X) \in \mathbb{Z}[X]$ the minimal polynomial of π. Since A is simple, the subalgebra $\mathbb{Q}(\pi)$ of $\operatorname{End}(A) \otimes \mathbb{Q}$ is a field; it contains a filtration of subfields $\mathbb{Q}(\pi^d)$ for $d > 1$. If moreover A is ordinary, then the fields $\operatorname{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$ and $\mathbb{Q}(\pi^d)$ $(d > 1)$ are all CM-fields, i.e., totally imaginary quadratic extensions of a totally real field. A slight reformulation of Howe and Zhu's criterion is the following (see Proposition 3 and Lemma 5 of [11]):

Proposition 3.3 (Howe-Zhu criterion for absolute simplicity)**.** *Let A be a simple abelian variety over a finite field k. If $\mathbb{Q}(\pi^d) = \mathbb{Q}(\pi)$ for all integers $d > 0$, then A is absolutely simple. If A is ordinary, then the converse is also true, and if $\mathbb{Q}(\pi^d) \neq \mathbb{Q}(\pi)$ for some $d > 0$, then A splits over the degree d extension of k. Moreover, if $\mathbb{Q}(\pi^d)$ is a proper subfield of $\mathbb{Q}(\pi)$ such that $\mathbb{Q}(\pi^r) = \mathbb{Q}(\pi)$ for all $r < d$, then either $m_A(X) \in \mathbb{Z}[X^d]$, or $\mathbb{Q}(\pi) = \mathbb{Q}(\pi^d, \zeta_d)$ for a primitive d-th root of unity ζ_d.*

From this criterion, Howe and Zhu give elementary conditions for a simple 2-dimensional abelian variety to be absolutely simple, see [11, Theorem 6]. Elaborating on their criterion and inspired by [11, Theorem 6], we prove the following for dimension 3:

Proposition 3.4. *Let A be an ordinary simple abelian variety of dimension 3 over a finite field k of odd cardinality q. Then either A is absolutely simple or the characteristic polynomial of the Frobenius endomorphism of A is of the form $X^6 + cX^3 + q^3$ with c coprime to q and A splits over the degree 3 extension of k.*

Proof. Let A be an ordinary simple but not absolutely simple abelian variety of dimension 3 over k. Since A is simple, the characteristic polynomial of π is $m_A(X)$. We apply Proposition 3.3 to A:

Let d be the smallest integer such that $\mathbb{Q}(\pi^d) \neq \mathbb{Q}(\pi)$. Either $m_A(X) \in \mathbb{Z}[X^d]$ or there exists a d-th root of unity ζ_d such that $\mathbb{Q}(\pi) = \mathbb{Q}(\pi^d, \zeta_d)$.

We will prove by contradiction that $m_A(X) \in \mathbb{Z}[X^d]$. Since $m_A(X)$ is ordinary, the coefficient of degree 3 is non-zero, and it will follow that $d = 3$ and that $m_A(X)$ has the form $X^6 + cX^3 + q^3$, proving the proposition.

So, suppose that $m_A(X) \notin \mathbb{Z}[X^d]$. The field $K = \mathbb{Q}(\pi) = \mathbb{Q}(\pi^d, \zeta_d)$ is a CM-field of degree 6 over $\mathbb{Q}$, hence its proper CM-subfield $L = \mathbb{Q}(\pi^d)$ has to be a quadratic imaginary field. It follows that $\phi(d) = 3$ or 6, where ϕ denotes the Euler totient function. However, $\phi(d) = 3$ has no solution, so we must have $\phi(d) = 6$, i.e. $d \in \{7, 9, 14, 18\}$, and $K = \mathbb{Q}(\zeta_d)$. Note that $\mathbb{Q}(\zeta_7) = \mathbb{Q}(\zeta_{14})$ and $\mathbb{Q}(\zeta_9) = \mathbb{Q}(\zeta_{18})$, and they contain only one quadratic imaginary field; namely, $\mathbb{Q}(\sqrt{-7})$ for $d = 7$ (resp. 14), and $\mathbb{Q}(\sqrt{-3})$ for $d = 9$ (resp. $d = 18$) (cf. [24]). Let σ be a generator of the (cyclic) group $\mathrm{Gal}(K/L)$ of order 3. In their proof of [11, Lemma 5], Howe and Zhu show that we can choose ζ_d such that $\pi^\sigma = \zeta_d \pi$. Moreover, $\zeta_d^\sigma = \zeta_d^k$ for some integer k (which can be chosen to lie in $[0, d-1]$). Since σ is of order 3, we have $\pi = \pi^{\sigma^3} = \zeta_d^{(k^2+k+1)}\pi$, which gives $k^2 + k + 1 \equiv 0 \pmod{d}$. This rules out the case $d = 9$ and 18, because -3 is neither a square modulo 9 nor a square modulo 18. So $d = 7$ or 14, $K = \mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\pi^d) = \mathbb{Q}(\sqrt{-7})$. It follows that the characteristic polynomial of π^d, which is of the form

$$X^6 + \alpha X^5 + \beta X^4 + \gamma X^3 + \beta q^d X^2 + \alpha q^{2d} X + q^{3d} \in \mathbb{Z}[X],$$

is the cube of a quadratic polynomial of discriminant -7. This is true if and only if

$$\alpha^2 - 36q^d + 63 = 0, \quad \alpha^2 - 3\beta + 9q^d = 0 \quad \text{and} \quad \alpha^3 - 27\gamma + 54\alpha q^d = 0,$$

that is,

$$\alpha^2 = 9(4q^d - 7), \quad \beta = 3(5q^d - 7) \quad \text{and} \quad 3\gamma = \alpha(10q^d - 7).$$

However, the first equation has no solution in q. Indeed, suppose that $4q^d - 7$ is a square, say u^2 for some integer u. Then u is odd, say $u = 1 + 2t$ for some integer t, hence $4q^d = 8 + 4t(t+1)$, so 2 divides q, which contradicts the hypothesis.

Hence, we obtain that $m_A(X) \in \mathbb{Z}[X^d]$ and Proposition 3.4 follows. □

Finally, the proof of Theorem 3.1 relies on Proposition 3.4 and the following proposition, whose proof consists on counting arguments and is postponed to Section 5:

Proposition 3.5. For any prime number $\ell \geq 13$ and any prime number $q > 1.82\ell^2$, there exists an ordinary Weil q-polynomial $P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3$, with $a \not\equiv 0 \pmod{\ell}$, which is irreducible modulo ℓ. For $\ell \in \{3, 5, 7, 11\}$, there exists some prime number $q > 1.82\ell^2$ and an ordinary Weil q-polynomial as above. Moreover, for all $\ell \geq 3$, the coefficients a, b, c can be chosen to lie in $\mathbb{Z} \cap [-(\ell-1)/2, (\ell-1)/2]$.

Remark 3.6. Computations suggest that for $\ell \in \{5, 7, 11\}$ and *any* prime number $q > 1.82\ell^2$, there still exist integers a, b, c such that Proposition 3.5 holds. For $\ell = 3$, this is no longer true: our computations indicate that if q is such that $\left(\frac{q}{\ell}\right) = -1$, then there are no suitable a, b, c, while if q is such that $\left(\frac{q}{\ell}\right) = 1$, they indicate that there are 4 suitable triples (a, b, c).

We now have all the ingredients to prove Theorem 3.1.

Proof of Theorem 3.1. Let ℓ and q be two distinct prime numbers as in Proposition 3.5 and let $P_q(X)$ be an ordinary Weil q-polynomial provided by this proposition. Since the polynomial $P_q(X)$ is irreducible modulo ℓ, it is a fortiori irreducible over $\mathbb{Z}$. It is also ordinary and of degree 6. Hence, by Honda-Tate theory, it defines an isogeny class $\mathcal{A}$ of ordinary simple abelian varieties of dimension 3 over $\mathbb{F}_q$. By Proposition 3.4, since $a \neq 0$, the abelian varieties in $\mathcal{A}$ are actually absolutely simple. Moreover, according to Howe (cf. [10, Theorem 1.2]), $\mathcal{A}$ contains a principally polarised abelian variety (A, λ).

Now, by the results of Oort-Ueno (cf. [16, Theorem 4]), there exists a so-called good curve C defined over $\overline{\mathbb{F}}_q$ such that (A, λ) is $\overline{\mathbb{F}}_q$-isomorphic to $(\mathrm{Jac}(C), \mu_0)$, where μ_0 denotes the canonical polarisation on $\mathrm{Jac}(C)$. A curve over $\overline{\mathbb{F}}_q$ is a *good curve* if it is either irreducible and non-singular or a non-irreducible stable curve whose generalised Jacobian variety is an abelian variety (cf. [10, Definition (13.1)]). In particular, the curve C is stable, and so semi-stable. Since the generalised Jacobian variety $\mathrm{Jac}(C) \cong \mathrm{Pic}^0_C$ is an abelian variety, the torus appearing in the short exact sequence of Proposition 1.1 is trivial. Hence, there is an isomorphism $\mathrm{Jac}(C) \cong \prod_{i=1}^r \mathrm{Pic}^0_{\widetilde{X_i}}$, where $\widetilde{X_1}, \ldots, \widetilde{X_r}$ denote the normalisations of the irreducible component of C over $\overline{\mathbb{F}}_q$. Since $\mathrm{Jac}(C)$ is absolutely simple, we conclude that $r = 1$, i.e., the curve C is irreducible, hence smooth.

We can therefore apply Theorem 9 of the appendix by Serre in [12] (see also the reformulation in [17, Theorem 1.1]) and conclude that the curve C descends to $\mathbb{F}_q$. Indeed, there exists a smooth and geometrically irreducible curve C_q defined over $\mathbb{F}_q$ which is isomorphic to C over $\overline{\mathbb{F}}_q$. Moreover, either (A, λ) or a quadratic twist of (A, λ) is isomorphic to $(\mathrm{Jac}(C_q), \mu)$ over $\mathbb{F}_q$, where μ denotes the canonical polarisation of $\mathrm{Jac}(C_q)$. The characteristic polynomial of $\mathrm{Jac}(C_q)$ is $P_q(X)$ or $P_q(-X)$, since the twist may replace the Frobenius endomorphism with its negative.

Note that the polynomial $P_q(-X)$ is still an ordinary Weil polynomial which is irreducible modulo ℓ with non-zero trace, and $\mathrm{Jac}(C_q)$ is still ordinary and absolutely simple. This proves Theorem 3.1. □

Remark 3.7. In the descent argument above, the existence of a non-trivial quadratic twist may occur in the non-hyperelliptic case only. This obstruction for an abelian variety over $\overline{\mathbb{F}}_q$ to be a jacobian over $\mathbb{F}_q$ was first stated by Serre in a Harvard course [22]; it was derived from a precise reformulation of Torelli's theorem that Serre attributes to Weil [25]. Note that Sekiguchi investigated the descent of the curve in [19] and [20], but, as Serre pointed out to us, the non-hyperelliptic case was incorrect. According to MathSciNet review MR1002618 (90d:14032), together with Sekino, Sekiguchi corrected this error in [21].

4 Proof of the main theorem

The goal of this section is to prove Theorem 0.1, by collecting together the results from Sections 2 and 3. We keep the notation introduced in Subsection 1.1; in particular, we will consider genus 3 curves defined by polynomials which are of 3-hyperelliptic or quartic type. We will prove the following refinement of Theorem 0.1:

Theorem 4.1. Let $\ell \geq 13$ be a prime number. For each prime number $q > 1.82\ell^2$, there exists $\bar{f}_q(x,y) \in \mathbb{F}_q[x,y]$ of 3-hyperelliptic or quartic type, such that if $f(x,y) \in \mathbb{Z}[x,y]$ is a lift of $\bar{f}_q(x,y)$, of the same type, satisfying the following two conditions for some prime number $p \notin \{2, q, \ell\}$:

1. $f(0,0) = 0$ or $v_p(f(0,0)) > 2$;
2. $f(x,y)$ is congruent modulo p^2 to:

$$\begin{cases} y^2 - x(x-p)m(x) & \text{if } \bar{f}_q(x,y) \text{ is of hyperelliptic type} \\ x^4 + y^4 + x^2 - y^2 + px & \text{if } \bar{f}_q(x,y) \text{ is of quartic type} \end{cases}$$

for some $m(x) \in \mathbb{Z}_p[x]$ of degree 5 or 6 with simple non-zero roots modulo p;

then the projective curve C defined over $\mathbb{Q}$ by the equation $f(x,y) = 0$ is a smooth projective geometrically irreducible genus 3 curve, such that the image of the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the ℓ-torsion of $\mathrm{Jac}(C)$ coincides with $\mathrm{GSp}_6(\mathbb{F}_\ell)$.

Moreover, if $\ell \in \{5, 7, 11\}$, the statement is true, replacing "For each prime number q" by "There exists an odd prime number q".

Remark 4.2. Let $\ell \geq 5$ be a prime number. Note that it is easy to construct infinitely many polynomials $f(x,y)$ satisfying the conclusion of Theorem 4.1: choose a polynomial $f_p(x,y)$ satisfying the conditions in Definition 2.1. Then it suffices to choose each coefficient of $f(x,y)$ as a lift of the corresponding coefficient of $\bar{f}_q(x,y)$ to an element of $\mathbb{Z}$, which is congruent mod p^3 to the corresponding coefficient of $f_p(x,y)$. This also proves that Theorem 0.1 follows from Theorem 4.1.

For the convenience of the reader, we recall the contents of Theorem 3.10 from [1]: Let A be a principally polarised n-dimensional abelian variety defined over $\mathbb{Q}$. Assume that A has semistable reduction of toric rank 1 at some prime number p. Denote by Φ_p the group of connected components of the Néron model of A at p. Let q be a prime of good reduction of A and $P_q(X) = X^{2n} + aX^{2n-1} + \cdots + q^n \in \mathbb{Z}[X]$ the characteristic polynomial of the Frobenius endomorphism acting on the reduction of A at q. Then for all primes ℓ which do not divide $6pqa|\Phi_p|$ and such that the reduction of $P_q(X)$ mod ℓ is irreducible in $\mathbb{F}_\ell$, the image of $\overline{\rho}_{A,\ell}$ coincides with $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$.

Proof of Theorem 4.1. Fix a prime $\ell \geq 5$. Let q and C_q be a prime, respectively a genus 3 curve over $\mathbb{F}_q$, provided by Theorem 3.1. The curve C_q is either a plane quartic or a hyperelliptic curve. More precisely, it is defined by an equation $\bar{f}_q(x,y) = 0$, where $\bar{f}_q(x,y) \in \mathbb{F}_q[x,y]$ is a quartic type polynomial in the first case and a 3-hyperelliptic type polynomial otherwise (cf. Subsection 1.1). Note that if $f(x,y) \in \mathbb{Z}[x,y]$ is a quartic (resp. 3-hyperelliptic type) polynomial which reduces to $\bar{f}_q(x,y)$ modulo q, then it defines a smooth projective genus 3 curve over $\mathbb{Q}$ which is geometrically irreducible.

Let now $p \notin \{2,q,\ell\}$ be a prime. Assume that $f(x,y) \in \mathbb{Z}[x,y]$ is a polynomial of the same type as $\bar{f}_q(x,y)$ which is congruent to $\bar{f}_q(x,y)$ modulo q and also satisfies the two conditions of the statement of Theorem 4.1 for this p. We claim that the curve C defined over $\mathbb{Q}$ by the equation $f(x,y) = 0$ satisfies all the conditions of the explicit surjectivity result of ([1, Theorem 3.10]). Namely, Proposition 2.2 implies that C is a smooth projective geometrically connected curve of genus 3 with stable reduction. Moreover, according to Proposition 2.3, the Jacobian $\mathrm{Jac}(C)$ is a principally polarised 3-dimensional abelian variety over $\mathbb{Q}$, and its Néron model has semistable reduction at p with toric rank equal to 1. Furthermore, the component group Φ_p of the Néron model of $\mathrm{Jac}(C)$ at p has order 2. Finally, by the choice of q and C_q provided by Theorem 3.1, q is a prime of good reduction of $\mathrm{Jac}(C)$ such that the Frobenius endomorphism of the special fibre at q has Weil polynomial $P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3$, which is irreducible modulo ℓ. Since the prime ℓ does not divide $6pqa|\Phi_p|$, we conclude that the image of the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the ℓ-torsion of $\mathrm{Jac}(C)$ coincides with $\mathrm{GSp}_6(\mathbb{F}_\ell)$. □

5 Counting irreducible Weil polynomials of degree 6

In this section, we will prove Proposition 3.5 stated in Section 3.

This proof is based on Proposition 5.1 as well as Lemmas 5.3 and 5.4 below.

Let ℓ and q be distinct prime numbers. Consider a polynomial of the form

$$P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3 \in \mathbb{Z}[X]. \qquad (*)$$

Proposition 5.1 ensures that for $q \gg \ell^2$, every polynomial $(*)$ with coefficients in $]-\ell,\ell[$ is a Weil polynomial. Then Lemmas 5.3 and 5.4 allow us to show that the number of such polynomials which are irreducible modulo ℓ is strictly positive.

Proposition 5.1. Let ℓ and q be two prime numbers.

1. Suppose that $q > 1.67\ell^2$. Then every polynomial

$$X^4 + uX^3 + vX^2 + uqX + q^2 \in \mathbb{Z}[X]$$

with integers u, v of absolute value $< \ell$ is a Weil q-polynomial.

2. Suppose that $q > 1.82\ell^2$. Then every polynomial

$$P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3 \in \mathbb{Z}[X],$$

with integers a, b, c of absolute value $< \ell$, is a Weil q-polynomial.

Remark 5.2. The power in ℓ is optimal, but the constants 1.67 and 1.82 are not.

Let D_6^{*-} be the number of polynomials of the form $P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3 \in \mathbb{Z}[X]$ with a, b, c in $[-(\ell-1)/2, (\ell-1)/2]$, $a, c \neq 0$ and whose discriminant Δ_{P_q} is not a square modulo ℓ, and R_6 the number of such polynomials which are reducible modulo ℓ. Denoting by $\left(\frac{\cdot}{\ell}\right)$ the Legendre symbol, we have:

Lemma 5.3. Let $\ell > 3$, then $D_6^{*-} \geq \frac{1}{2}(\ell-1)^2\left(\ell - 1 - \left(\frac{q}{\ell}\right)\right) + \frac{1}{2}(\ell-1)\left(\frac{q}{\ell}\right)\left(1 - \left(\frac{-1}{\ell}\right)\right) - \ell(\ell-1)$.

Lemma 5.4. Let $\ell > 3$, then $R_6 \leq \frac{3}{8}\ell^3 - \frac{5}{8}\ell^2\left(\frac{q}{\ell}\right) - \ell^2 + \frac{3}{2}\ell\left(\frac{q}{\ell}\right) + \frac{5}{8}\ell - \frac{3}{8}\left(\frac{q}{\ell}\right) - \frac{1}{2}$.

We postpone the proofs of Proposition 5.1 as well as Lemmas 5.3 and 5.4 to the following subsections but now use those statements to prove Proposition 3.5. Before that, let us recall a result of Stickelberger, as proven by Carlitz in [7], which will also be useful for proving Lemmas 5.3 and 5.4: For any monic polynomial $P(X)$ of degree n with coefficients in $\mathbb{Z}$, and any odd prime number ℓ not dividing its discriminant Δ_P, the number s of irreducible factors of $P(X)$ modulo ℓ satisfies

$$\left(\frac{\Delta_P}{\ell}\right) = (-1)^{n-s}.$$

Proof of Proposition 3.5. Let $\ell > 3$ be a prime number. It follows from Stickelberger's result that if $P_q(X)$ as in $(*)$ is irreducible modulo ℓ, then $\left(\frac{\Delta_{P_q}}{\ell}\right) = -1$. Hence by Proposition 5.1, when $q > 1.82\ell^2$, we find that $(D_6^{*-} - R_6)$ is exactly the number of degree 6 ordinary Weil polynomials which have non-zero trace modulo ℓ and are irreducible modulo ℓ.

By Lemmas 5.3 and 5.4, we have

$$D_6^{*-} - R_6 \geq \frac{1}{8}\ell^3 + \frac{1}{8}\ell^2\left(\frac{q}{\ell}\right) - \frac{1}{2}\ell\left(\frac{-q}{\ell}\right) - \frac{3}{2}\ell^2 + \frac{1}{2}\left(\frac{-q}{\ell}\right) + \frac{15}{8}\ell - \frac{5}{8}\left(\frac{q}{\ell}\right),$$

which is strictly positive for all q, provided that $\ell \geq 13$.

For $\ell = 3, 5, 7$ or 11, direct computations of $(D_6^{*-} - R_6)$ using Sage show that $q = 19$ for $\ell = 3$, $q = 47$ for $\ell = 5$, $q = 97$ for $\ell = 7$, $q = 223$ for $\ell = 11$ will answer to the conditions of Proposition 3.5. Actually, computations indicate that for $\ell = 5, 7, 11$, $(D_6^{*-} - R_6)$ should be strictly positive for any prime number q and for $\ell = 3$, it should be strictly positive for all prime numbers q which are not squares modulo ℓ (see Remark 3.6). ☐

5.1 Proof of Proposition 5.1

Recall that ℓ and q are two prime numbers.

We first consider degree 4 polynomials. One can prove that a polynomial $X^4 + uX^3 + vX^2 + uqX + q^2 \in \mathbb{Z}[X]$ is a q-Weil polynomial if and only if the integers u, v satisfy the following inequalities:

(1) $|u| \leq 4\sqrt{q}$,

(2) $2|u|\sqrt{q} - 2q \leq v \leq \frac{u^2}{4} + 2q$.

Let $q > 1.67\ell^2$ and $Q(X) = X^4 + uX^3 + vX^2 + uqX + q^2 \in \mathbb{Z}[X]$ with $|u| < \ell, |v| < \ell$. Then $q \geq \frac{1}{16}\ell^2$ and, since $\ell \geq 2$, we have $q \geq \frac{1}{4}\ell^2 \geq \frac{1}{2}\ell$ so (1) and the right hand side inequality in (2) are satisfied. Finally, $q \geq \left(1 + \frac{1}{2\sqrt{3}}\right)^2 \ell^2$ so $\sqrt{q} \geq \left(1 + \frac{1}{2\sqrt{q}}\right)\ell$ and the left hand side inequality in (2) is satisfied. This proves that $Q(X)$ is a Weil polynomial and the first part of the proposition.

Now we turn to degree 6 polynomials. The proof is similar to the degree 4 case. According to Haloui [9, Theorem 1.1], a degree 6 polynomial of the form $(*)$ is a Weil polynomial if its coefficients satisfy the following inequalities:

(1) $|a| < 6\sqrt{q}$,

(2) $4\sqrt{q}|a| - 9q < b \le \frac{a^2}{3} + 3q$,

(3) $-\frac{2a^3}{27} + \frac{ab}{3} + qa - \frac{2}{27}(a^2 - 3b^2 + 9q)^{\frac{3}{2}} \le c \le -\frac{2a^3}{27} + \frac{ab}{3} + qa + \frac{2}{27}(a^2 - 3b^2 + 9q)^{\frac{3}{2}}$,

(4) $-2qa - 2\sqrt{q}b - 2q\sqrt{q} < c < -2qa + 2\sqrt{q}b + 2q\sqrt{q}$.

Let $q > 1.82\ell^2$ and $P_q(X)$ a polynomial of the form $(*)$ with $|a|, |b|, |c| < \ell$. Then we note:

- We have $q > \frac{1}{36}\ell^2$, so $\ell < 6\sqrt{q}$ and (1) is satisfied.
- The right hand side inequality of (2) is satisfied since $\ell \le 3q$. Moreover we have $q > (1 + \sqrt{17/8})\ell^2 \ge 4\ell^2(1 + \sqrt{1 + 9/4\ell})^2/81$. Hence $9q - 4\ell\sqrt{q} - \ell > 0$ and the left hand inequality of (2) is satisfied.
- A sufficient condition to have both inequalities in (3) is
$$2\ell^3 + 9\ell^2 + 27q\ell - 2(-3\ell^2 + 9q)^{3/2} + 27\ell \le 0.$$
A computation shows that this inequality is equivalent to $A \le B$, with
$$A = \ell^6\left(\frac{28}{729} + \frac{1}{81\ell} + \frac{7}{108\ell^2} + \frac{1}{6\ell^3} + \frac{1}{4\ell^4}\right) \text{ and } B = q^3\left(1 - \frac{5}{4}\frac{\ell^2}{q} + \frac{\ell^4}{q^2}\left(\frac{8}{27} - \frac{1}{6\ell} - \frac{1}{2\ell^2}\right)\right).$$
Since $\ell \ge 2$, we have $A \le \frac{4537}{46656}\ell^6$ and $B \ge q^3\left(1 - \frac{5}{4}\frac{\ell^2}{q} + \frac{19}{216}\frac{\ell^4}{q^2}\right)$. Furthermore, since the polynomial
$$\frac{4537}{46656}X^3 - \frac{19}{216}X^2 + \frac{5}{4}X - 1$$
has only one real root with approximate value 0.805, we find that $A \le B$, because $q \ge 1.243\ell^2$.
- Since $q > 1.82\ell^2$ and $\ell \ge 2$, we have $\ell\left(\frac{1}{2q} + \frac{1}{\sqrt{q}} + 1\right) \le \ell\left(\frac{1}{22} + \frac{1}{\sqrt{11}} + 1\right) < \sqrt{q}$. Hence, $-2q\ell - 2\sqrt{q}\ell + 2q\sqrt{q} - \ell > 0$ and (4) is satisfied.

This proves that $P_q(X)$ is a Weil polynomial and the second part of the proposition. □

5.2 Proofs of Lemmas 5.3 and 5.4

In this section, $\ell > 2$, $q \neq \ell$ are prime numbers and we, somewhat abusively, denote with the same letter an integer in $[-(\ell-1)/2, (\ell-1)/2]$ and its image in $\mathbb{F}_\ell$.

We will use the following elementary lemma.

Lemma 5.5. Let $D \in \mathbb{F}_\ell^*$ and $\varepsilon \in \{-1, 1\}$. We have
$$\sharp\left\{x \in \mathbb{F}_\ell; \left(\frac{x^2 - D}{\ell}\right) = \varepsilon\right\} = \frac{1}{2}\left(\ell - 1 - \varepsilon - \left(\frac{D}{\ell}\right)\right);$$
and
$$\sharp\left\{(x, y) \in \mathbb{F}_\ell^2; \left(\frac{x^2 - Dy^2}{\ell}\right) = \varepsilon\right\} = \frac{1}{2}(\ell - 1)\left(\ell - \left(\frac{D}{\ell}\right)\right).$$

5.2.1 Estimates on the number of degree 4 Weil polynomials modulo ℓ

Proposition 5.6. 1. For $\varepsilon \in \{-1,1\}$, we denote by D_4^{ε} the number of degree 4 polynomials of the form $X^4+uX^3+vX^2+uqX+q^2 \in \mathbb{F}_\ell[X]$ with discriminant Δ such that $\left(\frac{\Delta}{\ell}\right)=\varepsilon$. Then

$$D_4^- = \frac{1}{2}(\ell-1)\left(\ell-\left(\frac{q}{\ell}\right)\right) \quad \text{and} \quad D_4^+ = \frac{1}{2}(\ell-3)\left(\ell-\left(\frac{q}{\ell}\right)\right)+1.$$

2. The number N_4 of degree 4 Weil polynomials with coefficients in $[-(\ell-1)/2,(\ell-1)/2]$ which are irreducible modulo ℓ satisfies

$$N_4 \leq \frac{1}{4}(\ell+1)(\ell-1). \tag{2}$$

3. The number T_4 of degree 4 Weil polynomials with coefficients in $[-(\ell-1)/2,(\ell-1)/2]$ with exactly two irreducible factors modulo ℓ satisfies

$$T_4 \leq \frac{1}{4}(\ell-3)\left(\ell-\left(\frac{q}{\ell}\right)\right)+\frac{1}{8}(\ell-1)(\ell+1). \tag{3}$$

Moreover, if $q>1.67\ell^2$, Inequalities (2) and (3) are equalities.

Proof. First, we compute D_4^{ε}. The polynomial $Q(X)=X^4+uX^3+vX^2+uqX+q^2$ has discriminant

$$\Delta = q^2\kappa^2\delta \quad \text{where} \quad \kappa=-u^2-8q+4v \quad \text{and} \quad \delta=(v+2q)^2-4qu^2.$$

So, since $q\in\mathbb{F}_\ell^*$, we have $\left(\frac{\Delta}{\ell}\right)=\left(\frac{\kappa}{\ell}\right)^2\left(\frac{\delta}{\ell}\right)$. Moreover, notice that if $\kappa=0$ then $\delta=(v-6q)^2$. Hence the set $\mathcal{D}_4^{\varepsilon}$ of $(u,v)\in\mathbb{F}_\ell^2$ such that $\left(\frac{\Delta}{\ell}\right)=\varepsilon$ is equal to

$$\begin{aligned}\mathcal{D}_4^{\varepsilon} &= \left\{(u,v)\in\mathbb{F}_\ell^2;\left(\frac{\delta}{\ell}\right)=\varepsilon\right\}\setminus\left\{(u,v)\in\mathbb{F}_\ell^2;\left(\frac{\delta}{\ell}\right)=\varepsilon \text{ and } \kappa=0\right\}\\ &= \left\{(u,v)\in\mathbb{F}_\ell^2;\left(\frac{\delta}{\ell}\right)=\varepsilon\right\}\setminus\left\{(u,v)\in\mathbb{F}_\ell^2;\left(\frac{v-6q}{\ell}\right)^2=\varepsilon \text{ and } u^2=4(v-2q)\right\}.\end{aligned}$$

It follows that

$$D_4^- = \sharp\mathcal{D}_4^- = \sharp\left\{(u,v)\in\mathbb{F}_\ell^2;\left(\frac{\delta}{\ell}\right)=-1\right\}$$

and

$$D_4^+ = \sharp\mathcal{D}_4^+ = \sharp\left\{(u,v)\in\mathbb{F}_\ell^2;\left(\frac{\delta}{\ell}\right)=1\right\}-\sharp\left\{(u,v)\in\mathbb{F}_\ell^2; v\neq 6q \text{ and } u^2=4(v-2q)\right\}.$$

Since the map $(u,v)\mapsto(v+2q,2u)$ is a bijection on $\mathbb{F}_\ell^2$ (because $\ell\neq 2$), by Lemma 5.5 we have

$$\sharp\left\{(u,v)\in\mathbb{F}_\ell^2;\left(\frac{\delta}{\ell}\right)=\varepsilon\right\}=\sharp\left\{(x,y)\in\mathbb{F}_\ell^2;\left(\frac{x^2-qy^2}{\ell}\right)=\varepsilon\right\}=\frac{(\ell-1)}{2}\left(\ell-\left(\frac{q}{\ell}\right)\right)$$

for any $\varepsilon\in\{\pm1\}$. This gives the result for D_4^-. Moreover

$$\begin{aligned}\sharp\left\{(u,v);\ v\neq 6q \text{ and } u^2=4(v-2q)\right\} &= \sharp\left\{(u,v);\ u^2=4(v-2q)\right\}-\sharp\{u\in\mathbb{F}_\ell; u^2=16q\}\\ &= \ell-1-\left(\frac{q}{\ell}\right).\end{aligned}$$

This gives the result for D_4^+.

Next, we bound the quantity N_4. By Stickelberger's result recalled at the beginning of the section, if a monic polynomial of degree 4 in $\mathbb{Z}[X]$ is irreducible modulo ℓ then it has non-square discriminant modulo ℓ. Conversely, if a monic degree 4 polynomial in $\mathbb{Z}[X]$ has non-square discriminant modulo ℓ, then it has one or three distinct irreducible factors in $\mathbb{F}_\ell[X]$. If the reduction of a degree 4 Weil polynomial with non-square discriminant modulo ℓ has three distinct irreducible factors in $\mathbb{F}_\ell[X]$, then it has the form

$$(X-\alpha')(X-q/\alpha')(X^2-B'X+q)$$

with $X^2-B'X+q$ irreducible in $\mathbb{F}_\ell[X]$ and $\alpha' \neq q/\alpha'$ in $\mathbb{F}_\ell^*$. By Lemma 5.5, there are

$$\frac{1}{4}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)\left(\ell-\left(\frac{q}{\ell}\right)\right)$$

such polynomials with three irreducible factors. It follows that

$$N_4 \leq D_4^- - \frac{1}{4}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)\left(\ell-\left(\frac{q}{\ell}\right)\right) \leq \frac{1}{4}(\ell-1)(\ell+1).$$

Finally, we bound the quantity T_4. As in the paragraph above, Stickelberger's result implies that a degree 4 Weil polynomial $Q(X)$ in $\mathbb{Z}[X]$ has exactly two distinct irreducible factors modulo ℓ if and only if $\left(\frac{\Delta_Q}{\ell}\right) = 1$ and $Q(X) \pmod{\ell}$ does not have four distinct roots in $\mathbb{F}_\ell$. By Lemma 5.5, there are

$$\frac{1}{8}\left(\ell-\left(\frac{q}{\ell}\right)-2\right)\left(\ell-\left(\frac{q}{\ell}\right)-4\right)$$

Weil polynomials with coefficients in $[-(\ell-1)/2, (\ell-1)/2]$ whose reduction modulo ℓ has four distinct roots in $\mathbb{F}_\ell$. It follows that

$$\begin{aligned} T_4 &\leq D_4^+ - \frac{1}{8}\left(\ell-\left(\frac{q}{\ell}\right)-2\right)\left(\ell-\left(\frac{q}{\ell}\right)-4\right) \\ &\leq \frac{1}{4}(\ell-3)\left(\ell-\left(\frac{q}{\ell}\right)\right)+\frac{1}{8}(\ell-1)(\ell+1). \end{aligned}$$

When $q > 1.67\ell^2$, these upper bounds for N_4 and T_4 are equalities, since in this case, by Proposition 5.1, every polynomial of the form $X^4+uX^3+vX^2+uqX+q^2$ with $|u|,|v|<\ell$ is a Weil polynomial. □

5.2.2 Proof of Lemma 5.4

Let $P_q(X)$ be a degree 6 Weil polynomial with coefficients in $[-(\ell-1)/2, (\ell-1)/2]$ and non-square discriminant modulo ℓ. We may drop the conditions $a \neq 0, c \neq 0$ to simplify computations for finding an upper bound for R_6. By Stickelberger's result, $P_q(X)$ has 1, 3 or 5 distinct irreducible factors in $\mathbb{F}_\ell[X]$. Note that a root α of $P_q(X)$ in $\overline{\mathbb{F}}_\ell$ is in $\mathbb{F}_\ell$ if and only q/α is also in $\mathbb{F}_\ell$. So a degree 6 Weil polynomial $P_q(X)$ with non-square discriminant modulo ℓ is reducible modulo ℓ if and only if its factorisation in $\mathbb{F}_\ell[X]$ is of one of the following types:

1. $P_q(X) \equiv (X-\alpha)(X-\frac{q}{\alpha})(X-\beta)(X-\frac{q}{\beta})(X^2-CX+q)$, with C^2-4q non-square modulo ℓ and $\alpha \neq q/\alpha$, $\beta \neq q/\beta$ and $\{\alpha, q/\alpha\} \neq \{\beta, q/\beta\}$; equivalently $P_q(X) \equiv (X^2-AX+q)(X^2-BX+q)(X^2-CX+q)$ where the first two quadratic polynomials are distinct and both reducible and the third one is irreducible;

2. $P_q(X) \equiv (X-\alpha)(X-\frac{q}{\alpha})Q(X)$, where $\alpha \neq q/\alpha$ and the irreducible factor $Q(X)$ is the reduction of a degree 4 Weil polynomial;

3. $P_q(X)$ is the product of three distinct irreducible quadratic polynomials, i.e., $P_q(X) \equiv (X^2-CX+q)Q(X)$ where X^2-CX+q is irreducible and $Q(X)$ is the reduction of a degree 4 Weil polynomial which has two distinct irreducible factors, both of which are distinct from X^2-CX+q.

We will count the number of polynomials of each type.

Type 1. By Lemma 5.5, there are $\frac{1}{2}\left(\ell-\left(\frac{q}{\ell}\right)\right)$ irreducible quadratic polynomials X^2-CX+q. Also by Lemma 5.5, there are $\frac{1}{2}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)$ choices for reducible X^2-AX+q without a double root and then there are $\frac{1}{2}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)-1$ choices for reducible X^2-BX+q without a double root and distinct from X^2-AX+q. It follows that there are $\frac{1}{16}\left(\ell-\left(\frac{q}{\ell}\right)\right)\left(\ell-\left(\frac{q}{\ell}\right)-2\right)\left(\ell-\left(\frac{q}{\ell}\right)-4\right)$ such polynomials.

Type 2. By Proposition 5.6 and Lemma 5.5, the number of polynomials with decomposition of this type is

$$\frac{1}{2}\left(\ell-\left(\frac{q}{\ell}\right)-2\right)N_4\leq\frac{1}{8}(\ell+1)(\ell-1)\left(\ell-\left(\frac{q}{\ell}\right)-2\right).$$

Type 3. Proposition 5.6 and Lemma 5.5 imply that there are

$$\leq\frac{1}{2}\left(\ell-\left(\frac{q}{\ell}\right)\right)T_4\leq\frac{1}{8}\left(\ell-\left(\frac{q}{\ell}\right)\right)^2(\ell-3)+\frac{1}{16}(\ell-1)(\ell+1)\left(\ell-\left(\frac{q}{\ell}\right)\right)$$

polynomials of this type. [3]

Summing these three upper bounds yields the lemma. □

5.2.3 Proof of Lemma 5.3

The discriminant of $P_q(X)$ is $\Delta_{P_q}=q^6\Gamma^2\delta$, where

$$\Gamma=8qa^4+9q^2a^2-42qa^2b+a^2b^2-4a^3c+108q^3-108q^2b+36qb^2-4b^3+54qac+18abc-27c^2$$

and

$\delta=(c+2aq)^2-4q(b+q)^2$. Hence, we have

$$\begin{aligned}
D_6^{*-} &= \sharp\left\{(a,b,c);a,c\neq 0,\Gamma\not\equiv 0 \bmod \ell \text{ and } \left(\frac{\delta}{\ell}\right)=-1\right\}\\
&= \sharp\left\{(a,b,c);a,c\neq 0,\left(\frac{\delta}{\ell}\right)=-1\right\}-\sharp\left\{(a,b,c);a,c\neq 0,\Gamma\equiv 0 \bmod \ell \text{ and } \left(\frac{\delta}{\ell}\right)=-1\right\}\\
&\geq M-W,
\end{aligned}$$

where $M=\sharp\left\{(a,b,c);a,c\neq 0,\left(\frac{\delta}{\ell}\right)=-1\right\}$ and $W=\sharp\{(a,b,c);a\neq 0,\Gamma\equiv 0 \bmod \ell\}$.

Computation of M. Since $\ell>2$ and $q\in\mathbb{F}_\ell^*$, for any fixed $c\in\mathbb{F}_\ell^\times$, the map $(a,b)\mapsto(c+2aq,b+q)$ is a bijection from $\mathbb{F}_\ell^*\times\mathbb{F}_\ell$ to $\mathbb{F}_\ell\backslash\{c\}\times\mathbb{F}_\ell$. From this and Lemma 5.5 we deduce that

$$\begin{aligned}
M &= \sum_{c\in\mathbb{F}_\ell^*}\sharp\left\{(x,y)\in\mathbb{F}_\ell^2;x\neq c,\left(\frac{x^2-4qy^2}{\ell}\right)=-1\right\}\\
&= \sum_{c\in\mathbb{F}_\ell^*}\sharp\left\{(x,y)\in\mathbb{F}_\ell^2;\left(\frac{x^2-4qy^2}{\ell}\right)=-1\right\}-\sum_{c\in\mathbb{F}_\ell^*}\sharp\left\{y\in\mathbb{F}_\ell;\left(\frac{c^2-4qy^2}{\ell}\right)=-1\right\}\\
&= \frac{1}{2}(\ell-1)^2\left(\ell-\left(\frac{q}{\ell}\right)\right)-\sum_{c\in\mathbb{F}_\ell^*}M_c',
\end{aligned}$$

where

$$M_c'=\sharp\left\{y\in\mathbb{F}_\ell;\left(\frac{c^2-4qy^2}{\ell}\right)=-1\right\}=\sharp\left\{y\in\mathbb{F}_\ell;\left(\frac{y^2-(c^2/4q)}{\ell}\right)=-\left(\frac{-q}{\ell}\right)\right\}.$$

[3] The first inequality is due to the fact that we do not take into account that X^2-CX+q has to be distinct from the factors of $Q(X)$.

By Lemma 5.5, if $\left(\frac{-q}{\ell}\right) = -1$, then

$$M'_c = \sharp\left\{y \in \mathbb{F}_\ell; \left(\frac{y^2 - (c^2/4q)}{\ell}\right) = 1\right\} = \frac{1}{2}\left(\ell - 2 - \left(\frac{q}{\ell}\right)\right)$$

and if $\left(\frac{-q}{\ell}\right) = 1$, then

$$M'_c = \sharp\left\{y \in \mathbb{F}_\ell; \left(\frac{y^2 - (c^2/4q)}{\ell}\right) = -1\right\} = \frac{1}{2}\left(\ell - \left(\frac{q}{\ell}\right)\right).$$

This can be rewritten, for all q and ℓ, as $M'_c = \frac{1}{2}\left(\ell - 1 - \left(\frac{q}{\ell}\right) + \left(\frac{-q}{\ell}\right)\right)$. We obtain

$$M = \frac{1}{2}(\ell-1)^2\left(\ell - 1 - \left(\frac{q}{\ell}\right)\right) + \frac{1}{2}(\ell-1)\left(\frac{q}{\ell}\right)\left(1 - \left(\frac{-1}{\ell}\right)\right).$$

Computation of $W = \sharp\left\{(a,b,c) \in \mathbb{F}_\ell^3; a \neq 0, \Gamma = 0\right\}$. Note that Γ can be viewed as a degree 2 polynomial in c over $\mathbb{F}_\ell[a,b]$:

$$\Gamma = -27c^2 + G_1 c + G_0, \quad \text{where} \quad G_1(a,b) = -2a(2a^2 - 27q - 9b)$$

and $G_0(a,b) = 8qa^4 + 9q^2a^2 - 42qa^2b + a^2b^2 + 108q^3 - 108q^2b + 36qb^2 - 4b^3$. The discriminant of Γ as a polynomial in c is $\gamma = 16(a^2 + 9q - 3b)^3$. So $\Gamma \equiv 0 \bmod \ell$ if and only if

$$\left(\left(\frac{\gamma}{\ell}\right) = 1 \text{ and } c = \frac{-1}{54}(-G_1 \pm \sqrt{\gamma})\right) \text{ or } \left(\gamma = 0 \text{ and } c = \frac{1}{54}G_1\right),$$

where $\sqrt{\gamma}$ denotes a square root of γ in $\mathbb{F}_\ell$. It follows that

$$\begin{aligned} W &= 2 \cdot \sharp\left\{(a,b) \in \mathbb{F}_\ell^2; a \neq 0, \left(\frac{\gamma}{\ell}\right) = 1\right\} + \sharp\left\{(a,b) \in \mathbb{F}_\ell^2; a \neq 0, \gamma = 0\right\} \\ &= 2 \cdot \sharp\left\{(a,b) \in \mathbb{F}_\ell^2; a \neq 0, \left(\frac{a^2 - 3(b-3q)}{\ell}\right) = 1\right\} + \sharp\left\{(a,b) \in \mathbb{F}_\ell^2; a \neq 0, a^2 = 3(b-3q)\right\}. \end{aligned}$$

Since $\ell > 3$, the map $b \mapsto 3(b - 3q)$ is a bijection on $\mathbb{F}_\ell$. So we have

$$\begin{aligned} W &= 2 \cdot \sharp\left\{(x,y) \in \mathbb{F}_\ell^2; x \neq 0, \left(\frac{x^2 - y}{\ell}\right) = 1\right\} + \sharp\left\{(x,y) \in \mathbb{F}_\ell^2; x \neq 0, x^2 = y\right\} \\ &= 2 \cdot \sum_{y \in \mathbb{F}_\ell} \sharp\left\{x \in \mathbb{F}_\ell; \left(\frac{x^2 - y}{\ell}\right) = 1\right\} - 2 \cdot \sharp\left\{y \in \mathbb{F}_\ell; \left(\frac{-y}{\ell}\right) = 1\right\} + \sum_{y \in \mathbb{F}_\ell^*} \sharp\{x \in \mathbb{F}_\ell^*; x^2 = y\} \\ &= \sum_{y \in \mathbb{F}_\ell^*}\left(\ell - 2 - \left(\frac{y}{\ell}\right)\right) + 2(\ell - 1) - (\ell - 1) + (\ell - 1), \end{aligned}$$

using Lemma 5.5 (the second term is the contribution of $y = 0$). This yields $W = \ell(\ell - 1)$ and computing $M - W$ concludes the proof. □

References

[1] Sara Arias-de-Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila. Galois representations and Galois groups over $\mathbb{Q}$. *Preprint, arXiv:1407.5802*, 2014.

[2] Sara Arias-de Reyna, Wojciech Gajda, and Sebastian Petersen. Big monodromy theorem for abelian varieties over finitely generated fields. *J. Pure Appl. Algebra*, 217(2):218–229, 2013.

[3] Sara Arias-de-Reyna and Christian Kappen. Abelian varieties over number fields, tame ramification and big Galois image. *Math. Res. Lett.*, 20(1):1–17, 2013.

[4] Sara Arias-de-Reyna and Núria Vila. Tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_l)$ over $\mathbb{Q}$. *J. Number Theory*, 129(5):1056–1065, 2009.

[5] Sara Arias-de-Reyna and Núria Vila. Tame Galois realizations of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ over $\mathbb{Q}$. *Int. Math. Res. Not. IMRN*, (9):2028–2046, 2011.

[6] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[7] Leonard Carlitz. A theorem of Stickelberger. *Math. Scand.*, 1:82–84, 1953.

[8] Chris Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.

[9] Safia Haloui. The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. *J. Number Theory*, 130(12):2745–2752, 2010.

[10] Everett W. Howe. Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.*, 347(7):2361–2401, 1995.

[11] Everett W. Howe and Hui June Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *J. Number Theory*, 92(1):139–163, 2002.

[12] Kristin Lauter. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *J. Algebraic Geom.*, 10(1):19–36, 2001. With an appendix in French by J.-P. Serre.

[13] Pierre Le Duff. Représentations galoisiennes associées aux points d'ordre l des jacobiennes de certaines courbes de genre 2. *Bull. Soc. Math. France*, 126(4):507–524, 1998.

[14] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.

[15] Qing Liu. *Algebraic geometry and arithmetic curves (second edition, 2006)*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[16] Frans Oort and Kenji Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20:377–381, 1973.

[17] Christophe Ritzenthaler. Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves. *LMS J. Comput. Math.*, 13:192–207, 2010.

[18] Matthieu Romagny. Models of curves. In *Arithmetic and geometry around Galois theory. Based on two summer schools, Istanbul, Turkey, 2008 and 2009*, pages 149–170. Basel: Birkhäuser, 2013.

[19] Tsutomu Sekiguchi. The coincidence of fields of moduli for nonhyperelliptic curves and for their Jacobian varieties. *Nagoya Math. J.*, 82:57–82, 1981.

[20] Tsutomu Sekiguchi. Erratum: "The coincidence of fields of moduli for nonhyperelliptic curves and for their Jacobian varieties" [Nagoya Math. J. **82** (1981), 57–82]. *Nagoya Math. J.*, 103:161, 1986.

[21] Kaoru Sekino and Tsutomu Sekiguchi. On the fields of definition for a curve and its Jacobian variety. *Bull. Fac. Sci. Engrg. Chuo Univ. Ser. I Math.*, 31:29–31 (1989), 1988.

[22] Jean-Pierre Serre. Rational points on curves over finite fields. *Lectures given at Harvard University. Notes by F. Q. Gouvêa*, 1985.

[23] Jean-Pierre Serre. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.

[24] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[25] André Weil. Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:33–53, 1957.

[26] David Zywina. An explicit jacobian of dimension 3 with maximal Galois action. *Preprint, http://www.math.cornell.edu/~zywina/papers/GSp6example.pdf*, 2015.