COMPUTING L-POLYNOMIALS OF PICARD CURVES FROM CARTIER–MANIN MATRICES

SUALEH ASIF, FRANCESC FITÉ, AND DYLAN PENTLAND,
WITH AN APPENDIX BY A. V. SUTHERLAND

ABSTRACT. We study the sequence of zeta functions $Z(C_p, T)$ of a generic
Picard curve $C : y^3 = f(x)$ defined over $\mathbb{Q}$ at primes p of good reduction
for C. We define a degree 9 polynomial $\psi_f \in \mathbb{Q}[x]$ such that the splitting field
of $\psi_f(x^3/2)$ is the 2-torsion field of the Jacobian of C. We prove that, for
all but a density zero subset of primes, the zeta function $Z(C_p, T)$ is uniquely
determined by the Cartier–Manin matrix A_p of C modulo p and the splitting
behavior modulo p of f and ψ_f; we also show that for primes $\equiv 1 \pmod{3}$ the
matrix A_p suffices and that for primes $\equiv 2 \pmod{3}$ the genericity assumption
on C is unnecessary. An element of the proof, which may be of independent
interest, is the determination of the density of the set of primes of ordinary
reduction for a generic Picard curve. By combining this with recent work
of Sutherland, we obtain a practical deterministic algorithm that computes
$Z(C_p, T)$ for almost all primes $p \le N$ using $N \log(N)^{3+o(1)}$ bit operations.
This is the first practical result of this type for curves of genus greater than 2.

1. INTRODUCTION

Let C be a Picard curve defined over $\mathbb{Q}$, that is, a curve admitting an affine
model given by an equation of the form

$$(1.1) \qquad\qquad y^3 = f(x),$$

where $f \in \mathbb{Q}[x]$ is a degree 4 separable polynomial. Without loss of generality we
will assume from now on that C is given by an integral model in which $f(x) = x^4 + f_2 x^2 + f_1 x + f_0$ and the f_i are integers. Let ζ_3 denote a primitive cubic root
of unity in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. The obvious action of $\langle \zeta_3 \rangle$ on C induces a
ring monomorphism from $\mathbb{Z}[\zeta_3]$ to the geometric endomorphism ring $\operatorname{End}(\operatorname{Jac}(C)_{\overline{\mathbb{Q}}})$
of the Jacobian of C. We will say that C is *generic* if this ring monomorphism is an
isomorphism. This amounts to asking that the geometric endomorphism algebra
$\operatorname{End}(\operatorname{Jac}(C)_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is isomorphic to $\mathbb{Q}(\zeta_3)$.

For a prime p of good reduction for C, let C_p denote the reduction of C modulo p.
The zeta function of C_p is a formal power series

$$Z(C_p, T) := \exp\left(\sum_{n \ge 1} \#C_p(\mathbb{F}_{p^n}) \frac{T^n}{n} \right) \in \mathbb{Q}[[T]],$$

defined in terms of the number of points of C_p over the finite extensions of the finite field of p elements $\mathbb{F}_p$. It can be shown to be a rational function admitting an expression of the form

$$Z(C_p, T) = \frac{L_p(C, T)}{(1 - T)(1 - pT)},$$

where $L_p(C, T)$ is a degree 6 polynomial with coefficients in $\mathbb{Z}$, which we call the L-polynomial of C at p.

The purpose of the present paper is twofold. On the one hand, we contribute several theoretical results related to the L-polynomials of C. On the other hand, we apply these results to develop and implement an efficient and practical deterministic algorithm to compute the $L_p(C, T)$, for almost all p up to some bound N. The sequence of the $L_p(C, T)$ contains deep arithmetic information about C, and it has been the object of celebrated conjectures in number theory, such as generalized forms of the Sato–Tate conjecture (see for example [Ser12, Chap. 8], [KS09]) or of the Lang–Trotter conjecture. Convincing numerical evidence for these conjectures sometimes requires computing $L_p(C, T)$ for p up to a bound N within the range $[2^{30}, 2^{40}]$. In recent years, there have been several breakthroughs to make these computations feasible for curves of genus at most 2; the methods of previous articles, however, do not allow for computations for N within this range for curves of genus 3.

Before we return to this question in more detail let us start by describing the theoretical contributions on which the main algorithm of this paper relies.

Theoretical contributions. Let $\mathcal{C}_p$ denote the Cartier operator acting on the 3-dimensional $\mathbb{F}_p$-vector space $H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})$ of regular differentials of C_p. By the Cartier–Manin matrix A_p of C at p, we will mean the matrix of the operator $\mathcal{C}_p$ acting on this space in a certain basis. By the work of Katz and Serre, the reduction of $L_p(C, T)$ *modulo* p is uniquely determined by A_p (see Section 2.1 for a quick recollection of these facts and their references).

In the first part of this article (corresponding to Sections 2 and 3), we show that in fact A_p carries enough information to uniquely determine $L_p(C, T)$ quite often. In order to state more precisely our main results, let us consider separately the cases $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$. To this aim, let $\mathfrak{S}(C)$ (resp. $\mathfrak{I}(C)$) denote the set of odd primes coprime to the discriminant of f and congruent to 1 (resp. 2) modulo 3. In the first case, we obtain the following.

Theorem 1.1. *Let C be a Picard curve defined over $\mathbb{Q}$. Then:*

(i) *For every $p \geq 53$ in $\mathfrak{S}(C)$ of ordinary reduction for C, the Cartier–Manin matrix of C at p uniquely determines the L-polynomial $L_p(C, T)$.*

(ii) *If C is generic, then every prime in $\mathfrak{S}(C)$ outside a density 0 set is ordinary for C.*

See Corollaries 3.3 and 3.16. Let $g_p(C, T)$ denote the reversed $T^3\chi_p(1/T)$ of the characteristic polynomial $\chi_p(T)$ of $\mathcal{C}_p$ acting on $H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})$. To prove the theorem, we first show that the existence of a functorial map from the crystalline cohomology space $H^1_{\mathrm{crys}}(C_p/\mathbb{Z}_p)$ onto the semisimple subspace $H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})_{\mathrm{ss}}$ implies that the action of $\mathbb{Z}[\zeta_3]$ on these two spaces induces compatible factorizations of the polynomials $L_p(C, T)$ and $g_p(C, T)$, over $\mathbb{Z}[\zeta_3][T]$ and $\mathbb{F}_p[T]$, respectively. This is the content of Section 2.2, which is written for general superelliptic curves

of prime exponent (with no cost of extra conceptual or technical complication with respect to the case of Picard curves).

The first assertion of the theorem is proven in Section 3.1. It relies on the compatible factorizations of $L_p(C, T)$ and $g_p(C, T)$, and uses the Weil bounds and the fact that if p is ordinary, then $g_p(C, T)$ has degree 3.

While the proof of the first assertion is p-adic in nature, the proof of the second statement (accomplished in Section 3.4) relies on ℓ-adic methods. It uses the description of $L_p(C, T)$ in terms of the étale cohomology group $H^1_{\text{ét}}(C_{\overline{\mathbb{Q}}}, \mathbb{Z}_\ell)$ (or alternatively, in terms of the Tate module $T_\ell(\text{Jac}(C))$). It should be regarded as a refinement of [Fit20, Thm. 1] obtained by replacing Ogus' method by that of Sawin (see [Saw16]). We actually need a mild generalization of Sawin's result, which is presented in Section 3.3.

We now turn to primes $p \equiv 2 \pmod 3$. Attached to the Picard curve C, define the polynomial

$$
(1.2) \quad \psi_f(x) := x^9 + 24f_2 x^7 - 168 f_1 x^6 + (1080 f_0 - 78 f_2^2) x^5 + 336 f_1 f_2 x^4
$$
$$
+ (1728 f_0 f_2 - 636 f_1^2 + 80 f_2^3) x^3 + (-864 f_0 f_1 - 168 f_1 f_2^2) x^2
$$
$$
+ (-432 f_0^2 + 216 f_0 f_2^2 - 120 f_1^2 f_2 - 27 f_2^4) x - 8 f_1^3.
$$

The splitting field of $\psi_f(x^3/2)$ is the 2-torsion field of the Jacobian of C. This is explained in the Lemma of the Appendix to this article, which was kindly written for us by Andrew Sutherland. We then have the following result.

Theorem 1.2. *Let C be a Picard curve defined over $\mathbb{Q}$, and let $f, \psi_f \in \mathbb{Z}[x]$ be as in (1.1) and (1.2), respectively. For every prime in $\mathfrak{I}(C)$, the data:*

   (i) *the Cartier–Manin matrix of C at p,*
   (ii) *the knowledge of ψ_f having a root or not modulo p, and*
   (iii) *the knowledge of f being irreducible or not modulo p*

uniquely determine the L-polynomial $L_p(C, T)$.

Its proof is the content of Section 3.2 and the Appendix. It is based on the following simple idea. For all $p \in \mathfrak{I}(C)$, the L-polynomial $L_p(C, T)$ is uniquely determined by the coefficient of T^2. By writing this coefficient as $p - t_p$, one has that $|t_p| \le 2p$. Since condition (i) determines t_p modulo p, the theorem follows from the facts that (ii) determines t_p modulo 2 (see the Theorem in the Appendix), and that (iii) determines it modulo 3 (see Lemma 3.9 and Proposition 3.11). The latter should be no surprise, as it is well known that the splitting field of f is closely related to the 3-torsion field of the Jacobian of C.

We highlight the *constructive* nature of the proofs of Theorems 1.1 and 1.2. By this, we mean that they provide a way to compute $L_p(C, T)$ from the given data. This is exploited in the second part of the paper.

A practical algorithm. In the second part of the paper (corresponding to Section 4), we are concerned with the problem of computing the L-polynomials $L_p(C, T)$, for $p \le N$.

At a *theoretical* level, this problem is well understood: for a fixed smooth and projective curve of genus g and defined over $\mathbb{Q}$, Pila's algorithm [Pil90] (extending [Sch85]) computes the zeta function at a prime p of good reduction using $\log(p)^{g^{O(1)}}$ operations.

As mentioned above, there are situations in which one is interested in computing the zeta functions at all primes $p \leq N$. In these situations, one can do better than applying Pila's algorithm prime by prime. In fact, Harvey has proposed an algorithm that achieves this computation using a total of $N \log(N)^{3+o(1)}$ bit operations (see [Har14] for the case of hyperelliptic curves and [Har15] for the case of a general arithmetic scheme, including, of course, the case of smooth projective curves).

The existence of Pila's and Harvey's theoretical algorithms sets the challenge to develop *practical* versions of them, amenable for implementation and producing effective results when run by real hardware and N is in the range, say, $[2^{30}, 2^{40}]$.

Let us summarize part of the progress which has been made toward the obtaining of practical versions of Harvey's algorithm. In the hyperelliptic curve case, practical algorithms to compute the Cartier–Manin matrix A_p have been developed and implemented by Harvey and Sutherland (see [HS14] and [HS16]). In [HMS16], such practical algorithms were developed for genus $g = 3$ geometrically hyperelliptic curves, that is, curves admitting an affine model given by the equations

$$h(x, y) = 0, \qquad w^2 = f(x, y),$$

where $f, h \in \mathbb{Z}[x, y]$ are polynomials of respective degrees 4 and 2. In genus $g \leq 2$, computing A_p suffices to compute the L-polynomial, but this is no longer true for $g \geq 3$. This makes adapting Harvey's algorithm more difficult.

In another direction, the case of cyclic covers of the projective line has been examined in [ABCMT19]. The authors provide an algorithm to compute the L-polynomial at p using $p^{1/2+o(1)}$ bit operations in the case of a superelliptic curve, and this yields the fastest practical algorithm in the literature for computing the L-polynomials at all primes $p \leq N$. In [Abe18], a Las Vegas type algorithm with expected complexity $\log(p)^{14+o(1)}$ is provided to compute the L-polynomial at p of a genus three hyperelliptic curve. However, for computing the L-polynomials at all $p \leq N$, when N is in the range we consider, [ABCMT19] still exhibits better performance.

For a Picard curve C defined over $\mathbb{Q}$, our case of interest, [BTW05] provides an algorithm of complexity $O(p^{1/2})$ to compute $L_p(C, T)$. The main computational contribution of this article is a practical deterministic algorithm for the computation of the L-polynomials of a generic Picard curve at *almost* all primes $p \leq N$, performing $N \log(N)^{3+o(1)}$ bit operations. This is obtained by combining the recent work of Sutherland [Sut20] with the constructive proofs of Theorems 1.1 and 1.2.

Before stating the result more precisely, let us establish some conventions and notation. From now on, the term *algorithm*, without further qualification, is used to refer to a deterministic algorithm. For a generic Picard curve C defined over $\mathbb{Q}$, let $\mathfrak{S}^*(C)$ denote the subset of ordinary primes of $\mathfrak{S}(C)$. For $N \geq 1$, set

$$\mathfrak{S}_N^*(C) := \mathfrak{S}^*(C) \cap [1, N], \qquad \mathfrak{I}_N(C) := \mathfrak{I}(C) \cap [1, N].$$

Theorem 1.3. *Let C be a generic Picard curve. Algorithm 4.2 determines $\mathfrak{S}_N^*(C)$ and returns $L_p(C, T)$ for every prime $p \in \mathfrak{S}_N^*(C) \cup \mathfrak{I}_N(C)$ using $N \log(N)^{3+o(1)}$ bit operations.*

One might speculate that the time spent with the computation of the $L_p(C, T)$ for primes $p \leq N$ in the complement of the set $\mathfrak{S}_N^*(C) \cup \mathfrak{I}_N(C)$ using existing algorithms (such as [ABCMT19] or lifting methods; see Remark 4.5) would be

subsumed by the bound $N \log(N)^{3+o(1)}$. Despite showing that this complement is of 0 density, we were not able to prove that it is thin enough to retrieve such a conclusion. Algorithm 4.2 is described in Section 4.1, where we also analyze its correctness and running time. In Section 4.2, we discuss our implementation of the algorithm and its speed compared to the implementation in [Sut20]. In Section 4.2, we also explain how the methods of this article can be combined with the algorithm of [ABCMT19] to provide a constant factor improvement in the performance of the latter.

2. Preliminaries

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let $\overline{\mathbb{Z}}$ denote its ring of algebraic integers. For a rational prime p, let $\mathbb{F}_p$ denote the finite field with p elements, and let v_p denote a prime ideal of $\overline{\mathbb{Z}}$ lying above p (by abuse of notation, we will also denote by v_p the corresponding extension of the p-adic valuation). The residue field of v_p is an algebraic closure of $\mathbb{F}_p$, which we will denote by $\overline{\mathbb{F}}_p$.

Let D_{v_p} denote the decomposition group of v_p. We will denote by φ_p the (arithmetic) Frobenius element of $G_{\mathbb{F}_p} := \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ and by Frob_p a preimage in D_{v_p} of φ_p by the canonical projection from D_{v_p} to $G_{\mathbb{F}_p}$.

2.1. L-polynomials modulo p.
Throughout this section, C denotes a smooth and projective curve of genus g defined over $\mathbb{Q}$. Let S denote a finite set of primes such that C has good reduction outside S. By this, we mean that there exists a smooth and projective scheme $\mathcal{C} \to \mathrm{Spec}(\mathbb{Z}) - S$ whose generic fiber is C. We will denote by C_p the special fiber of $\mathcal{C}$ at p, and will refer to it as the reduction of C modulo p. We will denote by $\mathrm{Jac}(C)$ the Jacobian of C.

Reduction from étale cohomology. Let ℓ denote a rational prime. Suppose from now on that $p \neq \ell$ is a prime of good reduction for C. Let $V_\ell(\mathrm{Jac}(C))$ denote the rational ℓ-adic Tate module of $\mathrm{Jac}(C)$. We define the L-polynomial of C at p as

$$(2.1) \quad L_p(C,T) := \det(1 - \mathrm{Frob}_p\, T \mid V_\ell(\mathrm{Jac}(C))) = \det(1 - \mathrm{Frob}_p^{-1}\, T \mid H^1_{\mathrm{\acute{e}t}}(\overline{C}, \mathbb{Z}_\ell)).$$

Here $\overline{C}$ stands for the base change of C from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$. It is a degree $2g$ polynomial with integer coefficients, and it does not depend on the choice of ℓ. Let us write

$$g_p(C,T) := \det(1 - \varphi_p^{-1}T \mid H^1_{\mathrm{\acute{e}t}}(\overline{C}_p, \mathbb{Z}/p\mathbb{Z})),$$

where $\overline{C}_p$ is the base change of C_p from $\mathbb{F}_p$ to $\overline{\mathbb{F}}_p$. By [Kat73, Thm. 3.1], we have the congruence

$$(2.2) \qquad\qquad L_p(C,T) \equiv g_p(C,T) \qquad (\mathrm{mod}\ p).$$

We will give an alternative description of $g_p(C,T)$ in terms of the Cartier operator. Let $F_p : C_p \to C_p$ be the absolute Frobenius, the map which is the identity on the underlying topological space of C_p and which acts by $F_p(\nu) = \nu^p$ on sections ν of $\mathcal{O}_{C_p}$. By abuse of notation, let us also denote by F_p the map

$$H^1(C_p, \mathcal{O}_{C_p}) \to H^1(C_p, \mathcal{O}_{C_p})$$

induced in cohomology. Let $\mathcal{C}_p \colon H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p}) \to H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})$ denote the Cartier operator as defined in [Ser58, §10] (see also [Sut20, §2] or [AH19, §2] for

a concise treatment). The $\mathbb{F}_p$-linear operators F_p and $\mathcal{C}_p$ give rise to $\overline{\mathbb{F}}_p$-linear operators

$$F_p \otimes \overline{\mathbb{F}}_p \colon H^1(\overline{C}_p, \mathcal{O}_{\overline{C}_p}) \to H^1(\overline{C}_p, \mathcal{O}_{\overline{C}_p}),$$

$$\mathcal{C}_p \otimes \overline{\mathbb{F}}_p \colon H^0(\overline{C}_p, \Omega^1_{\overline{C}_p/\overline{\mathbb{F}}_p}) \to H^0(\overline{C}_p, \Omega^1_{\overline{C}_p/\overline{\mathbb{F}}_p}).$$

We denote with a subscript $_{\mathrm{ss}}$ the semisimple part of the above spaces with respect to the respective operators. Fundamental to our discussion will be the existence of isomorphisms

$$(2.3) \qquad H^1_{\text{ét}}(\overline{C}_p, \mathbb{Z}/p\mathbb{Z}) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \simeq H^1(\overline{C}_p, \mathcal{O}_{\overline{C}_p})_{\mathrm{ss}} \simeq H^0(\overline{C}_p, \Omega^1_{\overline{C}_p/\overline{\mathbb{F}}_p})_{\mathrm{ss}}.$$

For the first isomorphism we refer to [Kat73, Prop. 2.2.5], where it is moreover shown that it transforms the automorphism $\varphi_p^{-1} \otimes \overline{\mathbb{F}}_p$ into the automorphism $F_p \otimes \overline{\mathbb{F}}_p$. The second isomorphism is Serre duality, and by [Ser58, Prop. 9] it sends $F_p \otimes \overline{\mathbb{F}}_p$ to $\mathcal{C}_p \otimes \overline{\mathbb{F}}_p$. We deduce that

$$g_p(C,T) = \det(1 - \mathcal{C}_p T \,|\, H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})_{\mathrm{ss}}) = \det(1 - \mathcal{C}_p T \,|\, H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})).$$

Reduction from crystalline cohomology. Crystalline cohomology provides a functorial version of (2.2), which we now recall. Let W denote the ring of Witt vectors of $\mathbb{F}_p$, and let $H^1_{\mathrm{crys}}(C_p/W)$ denote the crystalline cohomology of C_p. The latter is a free module over $W \simeq \mathbb{Z}_p$ of rank $2g$. By abuse of notation, we also denote by

$$F_p \colon H^1_{\mathrm{crys}}(C_p/W) \to H^1_{\mathrm{crys}}(C_p/W)$$

the map induced by the absolute Frobenius. By [KM74], we have the equality

$$(2.4) \qquad L_p(C,T) = \det(1 - F_p T \,|\, H^1_{\mathrm{crys}}(C_p/W)).$$

The cohomology group $H^1_{\mathrm{crys}}(C_p/W)$ comes equipped with a functorial map to de Rham cohomology

$$(2.5) \qquad H^1_{\mathrm{crys}}(C_p/W) \to H^1_{\mathrm{dR}}(C_p/\mathbb{F}_p) \to H^1_{\mathrm{dR}}(C_p/\mathbb{F}_p)_{\mathrm{ss}}$$

preserving the action of the absolute Frobenius on the respective spaces. By [Kat73, (3.3.4)] and Serre duality, respectively, there are functorial isomorphisms

$$H^1_{\mathrm{dR}}(C_p/\mathbb{F}_p)_{\mathrm{ss}} \simeq H^1(C_p, \mathcal{O}_{C_p})_{\mathrm{ss}} \simeq H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})_{\mathrm{ss}}$$

mapping F_p to $\mathcal{C}_p$. Together with (2.5), this provides a functorial map

$$(2.6) \qquad H^1_{\mathrm{crys}}(C_p/W) \to H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})_{\mathrm{ss}}$$

mapping the absolute Frobenius F_p to the Cartier operator $\mathcal{C}_p$, which refines (2.2) and which will be exploited in Section 2.2.

Note that further subtleties arise when working over a nonprime field, but we will not encounter them in our discussion.

2.2. **Superelliptic curves and Cartier–Manin matrices.** From now on, let C be a superelliptic curve defined over $\mathbb{Q}$, that is, a curve admitting an affine model given by the equation

$$y^m = f(x),$$

where $m \geq 2$ is an integer and $f \in \mathbb{Z}[x]$ is a separable polynomial of degree $d \geq 3$. Let $\mathcal{O}$ denote $\mathbb{Z}[\zeta_m]$, where ζ_m denotes a fixed primitive mth root of unity in $\overline{\mathbb{Z}}$.

We will further assume that m is prime. Then (see [Sch98, p. 149]) the action of $\langle \zeta_m \rangle$ on C induces a ring monomorphism

$$(2.7) \qquad \mathcal{O} \hookrightarrow \mathrm{End}(\mathrm{Jac}(C)_{\mathbb{Q}(\zeta_m)}).$$

The genus of C is then expressed by the formula

$$g = \frac{(d-1)(m-1) - \gcd(m,d) + 1}{2}.$$

Let $\mathfrak{S}(C)$ denote the set[1] of rational primes coprime to the discriminant of f and to its leading coefficient, and congruent to 1 modulo m. Assume until the end of this section that p belongs to $\mathfrak{S}(C)$. In particular, p is a prime of good reduction for C which splits completely in $\mathbb{Q}(\zeta_m)$. The choice of a prime v_p of $\overline{\mathbb{Z}}$ lying over p singles out one of the $\varphi(m)$ primes of $\mathcal{O}$ lying over p, where φ denotes Euler's totient function. Call it $\mathfrak{p}_0$. For a prime $\mathfrak{p}$ of $\mathcal{O}$ lying over p, define the $\mathbb{F}_p$-algebra map

$$(2.8) \qquad \sigma_{\mathfrak{p}} \colon \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p \simeq \bigoplus_{\mathfrak{p}' \mid \mathfrak{p}} \mathbb{F}_{\mathfrak{p}'} \xrightarrow{\mathrm{pr}_{\mathfrak{p}}} \mathbb{F}_p,$$

where $\mathrm{pr}_{\mathfrak{p}}$ denotes the projection from the $\mathbb{F}_{\mathfrak{p}}$-component. To shorten the notation, we will often simply write σ to denote $\sigma_{\mathfrak{p}}$, and σ_0 to denote $\sigma_{\mathfrak{p}_0}$. Note that there exists an integer $1 \leq j(\sigma) \leq m$ such that the equality

$$(2.9) \qquad \sigma(\zeta_m) = \sigma_0(\zeta_m)^{j(\sigma)}$$

holds in $\mathbb{F}_p$. Fix a W-algebra map $\mathcal{O} \otimes_{\mathbb{Z}} W \to W$ rendering the diagram

$$(2.10)$$

$$\begin{array}{ccc} \mathcal{O} \otimes_{\mathbb{Z}} W & \longrightarrow & W \\ \downarrow{\scriptstyle \otimes_W \mathbb{F}_p} & & \downarrow{\scriptstyle \otimes_W \mathbb{F}_p} \\ \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p & \xrightarrow{\sigma} & \mathbb{F}_p \end{array}$$

commutative. Let us still denote by σ the map $\mathcal{O} \otimes_{\mathbb{Z}} W \to W$.

We will use σ_0 to define an action of the cyclic group $\langle \zeta_m \rangle$ on C_p. It is given by

$$[\zeta_m]_{\sigma_0} \cdot (x, y) = (x, \sigma_0(\zeta_m) y).$$

Define the σ-eigenspaces

$$H_\sigma^1(C_p/W) := H_{\mathrm{crys}}^1(C_p/W) \otimes_{\mathcal{O} \otimes_{\mathbb{Z}} W, \sigma} W,$$

$$H_\sigma^0(C_p, \Omega^1_{C_p/\mathbb{F}_p}) := H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p}) \otimes_{\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p, \sigma} \mathbb{F}_p.$$

The commutativity of (2.10) yields a commutative diagram

$$\begin{array}{ccc} H_{\mathrm{crys}}^1(C_p/W) & \xrightarrow{\hspace{3cm} \otimes_W \mathbb{F}_p \hspace{3cm}} & H_{\mathrm{crys}}^1(C_p/W) \otimes_W \mathbb{F}_p \\ \downarrow & & \downarrow \\ H_\sigma^1(C_p/W) & \xrightarrow{\otimes_W \mathbb{F}_p} H_\sigma^1(C_p/W) \otimes_W \mathbb{F}_p \xrightarrow{\simeq} & (H_{\mathrm{crys}}^1(C_p/W) \otimes_W \mathbb{F}_p) \otimes_{\mathcal{O} \otimes \mathbb{F}_p, \sigma} \mathbb{F}_p, \end{array}$$

where the vertical arrows are projections to the respective σ-eigenspaces. By combining the bottom row of the above diagram with the functorial map (2.6), we obtain a map

$$(2.11) \qquad H_\sigma^1(C_p/W) \to H_\sigma^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})_{\mathrm{ss}}$$

[1]Note that the set $\mathfrak{S}(C)$ in fact depends on the model chosen for C.

that sends the absolute Frobenius F_p to the Cartier operator $\mathcal{C}_p$. Set the polynomials

(2.12)
$$L_p^\sigma(C, T) := \det(1 - F_p T \mid H_\sigma^1(C_p/W)),$$
$$g_p^\sigma(C, T) := \det(1 - \mathcal{C}_p T \mid H_\sigma^0(C_p, \Omega_{C_p/\mathbb{F}_p}^1)_{\mathrm{ss}}) = \det(1 - \mathcal{C}_p T \mid H_\sigma^0(C_p, \Omega_{C_p/\mathbb{F}_p}^1)).$$

We now describe the basis of $H^0(C_p, \Omega_{C_p/\mathbb{F}_p}^1)$ given by [Sut20, Lem. 6]. Namely, set

$$\mu := m - \left\lfloor \frac{m}{d} \right\rfloor - 1, \quad \text{and} \quad d_j := d - \left\lfloor \frac{dj}{m} \right\rfloor - 1 \text{ for } 1 \le j \le \mu,$$

and then define

(2.13)
$$\omega_{i,j} = x^{i-1} y^{j-m} dx \qquad \text{for } 1 \le j \le \mu,\ 1 \le i \le d_j.$$

We then denote by $\boldsymbol{\omega}$ the basis $(\omega_{11}, \omega_{12}, \ldots, \omega_{21}, \ldots)$, where the ω_{ij} are lexicographically ordered by subindex. Let A_p be the matrix of the Cartier operator $\mathcal{C}_p$ acting on $H^0(C_p, \Omega_{C_p/\mathbb{F}_p}^1)$ with respect to $\boldsymbol{\omega}$. We refer to A_p as the *Cartier–Manin matrix* of C_p with respect to $\boldsymbol{\omega}$.

Let $\boldsymbol{\omega}^\sigma$ denote the tuple $(\omega_{i,j(\sigma)})_i$, where i runs over the interval $[1, d_{j(\sigma)}]$ and $j(\sigma)$ is as defined in (2.9). From the relation

$$[\zeta_m]_{\sigma_0}^*(\omega_{i,j(\sigma)}) = \sigma_0(\zeta_m)^{j(\sigma)} \omega_{i,j(\sigma)} = \sigma(\zeta_m) \omega_{i,j(\sigma)},$$

we obtain that $\boldsymbol{\omega}^\sigma$ is a basis of the σ-eigenspace $H_\sigma^0(C_p, \Omega_{C_p/\mathbb{F}_p}^1)$. Let us denote by A_p^σ the matrix of the restriction of $\mathcal{C}_p$ on this subspace with respect to $\boldsymbol{\omega}^\sigma$.

Lemma 2.1. *The following holds:*

  (i) $L_p^\sigma(C, T)$ *is a polynomial with coefficients in* $\mathcal{O}$ *and degree* $2g/\varphi(m)$.

  (ii) *We have factorizations*

$$L_p(C, T) = \prod_\sigma L_p^\sigma(C, T), \qquad g_p(C, T) = \prod_\sigma g_p^\sigma(C, T)$$

  where $\sigma = \sigma_{\mathfrak{p}} : \mathcal{O} \otimes_{\mathbb{Z}} W \to W$ *runs through the W-algebra maps defined in (2.10). Moreover, for every such σ we have*

$$L_p^\sigma(C, T) \equiv g_p^\sigma(C, T) \equiv T^{d_{j(\sigma)}} \cdot \chi_p^\sigma(1/T) \qquad (\mathrm{mod}\ \mathfrak{p}_0),$$

  where χ_p^σ *is the characteristic polynomial of* A_p^σ.

Proof. Given the ring homomorphism (2.7), in the "ℓ-adic setting", part (i) is a special case of [Rib76, Thm. 2.11, Thm. 2.12]. The same arguments apply in the present "p-adic setting". The first part of (ii) follows from the eigenspace decompositions

$$H^1(C_p/W) \simeq \bigoplus_\sigma H_\sigma^1(C_p/W), \qquad H_\sigma^0(C_p, \Omega_{C_p/\mathbb{F}_p}^1) \simeq \bigoplus_\sigma H_\sigma^0(C_p, \Omega_{C_p/\mathbb{F}_p}^1).$$

As for the second part, by (2.11), we have a congruence

$$L_p^\sigma(C, T) \equiv g_p^\sigma(C, T) \qquad (\mathrm{mod}\ \mathfrak{p}_0),$$

and the discussion in the paragraph preceeding this lemma implies that $g_p^\sigma(C, T)$ is the reversed characteristic polynomial of A_p^σ. $\qquad\square$

3. L-POLYNOMIALS OF PICARD CURVES: SOME THEORETICAL RESULTS

From now on, let C be a Picard curve defined over $\mathbb{Q}$, that is, a curve admitting an affine model given by the equation

$$y^3 = f(x),$$

where $f(x) = x^4 + f_2 x^2 + f_1 x + f_0$ is a separable polynomial in which the f_i are integers. Thus C is a superelliptic curve for which $m = 3$ and $d = 4$, and accordingly we will denote $\mathbb{Z}[\zeta_3]$ by $\mathcal{O}$ from now on.

3.1. **The split case.** Recall from the introduction that $\mathfrak{S}(C)$ denotes the set of primes coprime to the discriminant of f and congruent to 1 modulo 3. Resume also the notations from Section 2.2, with the following slight modifications: for a prime p in $\mathfrak{S}(C)$ we simply denote by $\mathfrak{p}$ the prime of $\mathcal{O}$ singled out by v_p and by $\overline{\mathfrak{p}}$ the prime of $\mathcal{O}$ such that $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$; we write σ and $\overline{\sigma}$ for the maps $\sigma_{\mathfrak{p}}$ and $\sigma_{\overline{\mathfrak{p}}}$. We also fix once and for all generators $\pi, \overline{\pi}$ in $\mathcal{O}$ of the ideals $\mathfrak{p}, \overline{\mathfrak{p}}$.

With the notation of Section 2.2, we have that $d_1 = 2$ and $d_2 = 1$. Set $n_1 := (2p-2)/3$ and $n_2 := (p-1)/3$. Let $\tilde{f} \in \mathbb{F}_p[x]$ denote the reduction of $f \in \mathbb{Z}[x]$ modulo p and let f_a^n denote the coefficient of x^a in $\tilde{f}(x)^n$. From [Sut20, (8)] we see that

$$(3.1) \qquad A_p^\sigma = \begin{pmatrix} f_{p-1}^{n_1} & f_{p-2}^{n_1} \\ f_{2p-1}^{n_1} & f_{2p-2}^{n_1} \end{pmatrix}, \qquad A_p^{\overline{\sigma}} = \left(f_{p-1}^{n_2} \right).$$

Recall the polynomials defined in (2.12). Note that $L_p^\sigma(C,T)$ and $L_p^{\overline{\sigma}}(C,T)$ are complex conjugate to each other. Let us define their coefficients as:

$$L_p^\sigma(C,T) =: 1 - a_{\mathfrak{p}}T + b_{\mathfrak{p}}T^2 - c_{\mathfrak{p}}T^3,$$
$$L_p^{\overline{\sigma}}(C,T) =: 1 - a_{\overline{\mathfrak{p}}}T + b_{\overline{\mathfrak{p}}}T^2 - c_{\overline{\mathfrak{p}}}T^3,$$
$$g_p^\sigma(C,T) =: 1 - r_{\mathfrak{p}}T + s_{\mathfrak{p}}T^2,$$
$$g_p^{\overline{\sigma}}(C,T) =: 1 - r_{\overline{\mathfrak{p}}}T.$$

Recall that a prime p is said to be ordinary for C if the central coefficient of $L_p(C,T)$ is not divisible by p, or equivalently if the polynomial $g_p(C,T) \in \mathbb{F}_p[T]$ has degree 3. Our goal is to show that, for an ordinary prime p, the L-polynomial $L_p(C,T)$ can be recovered from the Cartier–Manin matrix.

Lemma 3.1. *Let p in $\mathfrak{S}(C)$ be of ordinary reduction for C. Then there exists a sixth root of unity ζ such that*

$$(3.2) \qquad\qquad\qquad c_{\mathfrak{p}} = \zeta\overline{\pi}p.$$

Proof. Since $c_{\mathfrak{p}}$ divides p^3 and it is the product of three p-Weil numbers, there exists an integer $0 \le i \le 3$ such that $c_{\mathfrak{p}} = \zeta\pi^i\overline{\pi}^{3-i}$, where ζ is a unit of $\mathcal{O}$ and thus a sixth root of unity. Since $g_p^\sigma(C,T)$ has degree < 3, we know that $i \ge 1$. Proving the lemma amounts to showing that $i = 1$. Let $\alpha_{\mathfrak{p}}$ denote a reciprocal root of $L_p^\sigma(C,T)$. Since α_p is an algebraic integer and $\alpha_p\overline{\alpha}_p = p$, we have $0 \le v_p(\alpha_p) \le 1$. Since p is ordinary, the polynomial $g_p^\sigma(C,T)$ has degree 2. The usual Newton polygon argument then shows that two of the reciprocal roots of $L_p^\sigma(C,T)$ have v_p-adic valuation 0. Hence the v_p-adic valuation of $c_{\mathfrak{p}}$ is that of the third reciprocal root of $L_p^\sigma(C,T)$, which as argued before is at most 1. The lemma follows. $\square$

Lemma 3.2. *For p in $\mathfrak{S}(C)$ the following hold:*

(i) $pb_{\mathfrak{p}} = c_{\mathfrak{p}} \cdot a_{\overline{\mathfrak{p}}}$.

(ii) *If $b_{\mathfrak{p}}$ is not divisible by π, then $a_{\overline{\mathfrak{p}}}$ is not divisible by π.*

(iii) *p is ordinary for C if and only if $b_{\mathfrak{p}}$ is not divisible by π.*

(iv) *p is ordinary for C if and only if $b_{\mathfrak{p}}$ (or, equivalently, $b_{\overline{\mathfrak{p}}}$) is not divisible by p.*

Proof. Complex conjugation interchanges the roots of $L_p^{\sigma}(C, T)$ and those of $L_p^{\overline{\sigma}}(C, T)$. Therefore we can pair each reciprocal root $\alpha_{\mathfrak{p}}$ of $L_p^{\sigma}(C, T)$ with a reciprocal root $\alpha_{\overline{\mathfrak{p}}}$ of $L_p^{\overline{\sigma}}(C, T)$ in such a way that $\alpha_{\mathfrak{p}} \cdot \alpha_{\overline{\mathfrak{p}}} = p$, and this implies (i) (c.f. [BTW05, (3.3)]). The coprimality of π and $\overline{\pi}$ and part (i), imply that $v_p(a_{\overline{\mathfrak{p}}}) = 1 + v_p(b_{\mathfrak{p}}) - v_p(c_{\mathfrak{p}})$. Since $g_p^{\sigma}(C, T)$ has degree ≤ 2, we have $v_p(c_{\mathfrak{p}}) \geq 1$. Thus $v_p(a_{\overline{\mathfrak{p}}}) \leq v_p(b_{\mathfrak{p}})$, and (ii) follows. By Lemma 2.1, the prime p is ordinary for C if and only if

$$g_p^{\sigma}(C, T) \cdot g_p^{\overline{\sigma}}(C, T) = g_p(C, T) \in \mathbb{F}_p[T]$$

has degree 3. This happens if and only if $s_{\mathfrak{p}}, r_{\overline{\mathfrak{p}}}$ are nonzero, which by (ii) amounts to saying that $b_{\mathfrak{p}}$ is not divisible by π. This shows (iii). Finally, note that since $b_{\mathfrak{p}}$ is always divisible by $\overline{\pi}$, divisibility by p amounts to divisibility by π. $\square$

Corollary 3.3. *Let $p \geq 53$ be a prime in $\mathfrak{S}(C)$ ordinary for C. Then the Cartier–Manin matrix A_p of C at p uniquely determines the L-polynomial $L_p(C, T)$.*

Proof. We will in fact show that $g_p^{\sigma}(C, T)$ and $g_p^{\overline{\sigma}}(C, T)$ already uniquely determine $L_p(C, T)$. By Lemma 2.1 and part (i) of Lemma 3.2, in order to determine $L_p(C, T)$ it suffices to determine $a_{\mathfrak{p}}$ and $c_{\mathfrak{p}}$. Write $a_{\mathfrak{p}} = x + \zeta_3 y$ for some integers x and y. Recall the map $\sigma: \mathcal{O} \otimes \mathbb{F}_p \to \mathbb{F}_p$, originating from the prime of $\mathcal{O}$ singled out by v_p. Recall that the generator of this prime has been denoted π. Given $\alpha \in \mathcal{O}$, by abuse of notation, let us write $\sigma(\alpha)$ to denote $\sigma(\alpha \otimes 1)$. Then the reductions of x and y modulo p are uniquely determined by the invertible linear system

$$(3.3) \qquad \begin{pmatrix} 1 & \sigma(\zeta_3) \\ 1 & \overline{\sigma}(\zeta_3) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r_{\mathfrak{p}} \\ r_{\overline{\mathfrak{p}}} \end{pmatrix}.$$

From the trivial inequalities $(2y - x)^2 \geq 0$ and $(2x - y)^2 \geq 0$ and the Weil bound $|a_{\mathfrak{p}}| \leq 3\sqrt{p}$, one finds that

$$\max\{x^2, y^2\} \leq \frac{4}{3}(x^2 + y^2 - xy) = \frac{4}{3}|a_{\mathfrak{p}}|^2 \leq 12p.$$

Therefore the reductions of x and y modulo p determine x and y uniquely as soon as $p \geq 53$. The coefficient $c_{\mathfrak{p}}$ is uniquely determined by the sixth root of unity $\zeta \in \mathcal{O}$ appearing in (3.2). Note that ζ is determined by its image $\sigma(\zeta) \in \mathbb{F}_p$. Using that p is ordinary, by Lemma 3.2 the equation

$$(3.4) \qquad \qquad \sigma(\zeta) = \frac{\sigma(b_{\mathfrak{p}})}{\sigma(a_{\overline{\mathfrak{p}}})\sigma(\overline{\pi})} = \frac{s_{\mathfrak{p}}}{r_{\overline{\mathfrak{p}}}\sigma(\overline{\pi})}$$

makes sense in $\mathbb{F}_p$, and it determines $\sigma(\zeta)$. $\square$

In Section 4 Corollary 3.3 will be used to describe an algorithm to compute the $L_p(C, T)$ for ordinary primes p in $\mathfrak{S}(C)$.

In Section 3.4 we will study the density of ordinary primes. In order to do so, we will need to apply an analogue of Lemma 3.2 to certain "λ-adic counterparts" of the polynomials $L_p^{\sigma}(C, T)$. We conclude this section by defining these polynomials

and discussing analogues of Lemma 3.1 and Lemma 3.2 in the λ-adic setting. Let $\ell \neq p$ be a prime totally split in $\mathcal{O}$, and let λ and $\overline{\lambda}$ denote the primes of $\mathcal{O}$ lying above ℓ. Denote by $\mathcal{O}_\lambda$ the completion of $\mathcal{O}$ at λ and consider the module

$$(3.5) \qquad H^1_\lambda(\overline{C}) := H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell) \otimes_{\mathcal{O} \otimes \mathbb{Z}_\ell, \sigma_\lambda} \mathbb{Z}_\ell.$$

The above tensor product is taken with respect to the $\mathbb{Z}_\ell$-algebra map

$$\sigma_\lambda \colon \mathcal{O} \otimes \mathbb{Z}_\ell \simeq \mathcal{O}_\lambda \oplus \mathcal{O}_{\overline{\lambda}} \xrightarrow{\text{pr}_\lambda} \mathbb{Z}_\ell,$$

where pr_λ denotes projection from the $\mathcal{O}_\lambda$-component. We define an action of the absolute Galois group $G_{\mathbb{Q}(\zeta_3)}$ on $H^1_\lambda(\overline{C})$ by letting it act naturally on $H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell)$ and trivially on $\mathbb{Z}_\ell$. Since p splits in $\mathcal{O}$, we have $\text{Frob}_p \in D_{v_p} \subseteq G_{\mathbb{Q}(\zeta_3)}$, and the polynomial

$$L^\lambda_p(C, T) := \det(1 - \text{Frob}_p^{-1} T \mid H^1_\lambda(\overline{C}))$$

is well defined. By [Rib76, Thm. 2.11, Thm. 2.12], it has coefficients in $\mathcal{O}$ and degree 3. Define similarly $H^1_{\overline{\lambda}}(\overline{C})$ and $L^{\overline{\lambda}}_p(C, T)$. The decomposition $H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell) \simeq H^1_\lambda(\overline{C}) \oplus H^1_{\overline{\lambda}}(\overline{C})$ implies that

$$L_p(C, T) = L^\lambda_p(C, T) \cdot L^{\overline{\lambda}}_p(C, T).$$

Note that the polynomials $L^\lambda_p(C, T)$ and $L^{\overline{\lambda}}_p(C, T)$ are complex conjugate to each other. Set the following notation for their coefficients

$$L^\lambda_p(C, T) =: 1 - a_{\mathfrak{p}, \lambda} T + b_{\mathfrak{p}, \lambda} T^2 - c_{\mathfrak{p}, \lambda} T^3, \quad L^{\overline{\lambda}}_p(C, T) =: 1 - a_{\mathfrak{p}, \overline{\lambda}} T + b_{\mathfrak{p}, \overline{\lambda}} T^2 - c_{\mathfrak{p}, \overline{\lambda}} T^3.$$

Remark 3.4. Let δ_λ denote $\det(H^1_\lambda(\overline{C}))$. By [Fit20, Thm. 14], the 1-dimensional representation δ_λ is a Hecke character of infinity type equivalent to $(1, 2)$. After interchanging λ and $\overline{\lambda}$ if necessary, this implies that

$$\delta_\lambda(\text{Frob}_p) = \zeta \overline{\pi} p,$$

where ζ is a root of unity in $\mathcal{O}$, and hence a sixth root of unity. It follows that $c_{\mathfrak{p}, \lambda} = \delta_\lambda(\text{Frob}_p) = \zeta \overline{\pi} p$, in analogy with Lemma 3.1.

Remark 3.5. By unique factorization in $\mathcal{O}[T]$, if $L^\sigma_p(C, T)$ is irreducible, then after interchanging λ and $\overline{\lambda}$ we have that

$$(3.6) \qquad L^\sigma_p(C, T) = L^\lambda_p(C, T).$$

Hence when $L^\sigma_p(C, T)$ is irreducible, (3.6) together with Remark 3.4 provides an alternative proof of Lemma 3.1. It may be interesting to investigate to which further generality equality (3.6) holds, which may be possible via comparison isomorphisms in cohomology. Instead of taking this approach in this paper, we will show that the polynomials $L^\lambda_p(C, T)$ and $L^{\overline{\lambda}}_p(C, T)$ satisfy the same desired properties that $L^\sigma_p(C, T)$ and $L^{\overline{\sigma}}_p(C, T)$ satisfy. This is explained in Remark 3.6.

Remark 3.6. A glimpse at the proof of Lemma 3.2 shows that the only properties of $L^\sigma_p(C, T)$ and $L^{\overline{\sigma}}_p(C, T)$ that it uses are that they belong to $\mathcal{O}[T]$, that they are complex conjugates to each other, that their product is $L_p(C, T)$, and that the reductions of $L^\sigma_p(C, T)$ and $L^{\overline{\sigma}}_p(C, T)$ modulo p have degree ≤ 2. That $L^\lambda_p(C, T)$ and $L^{\overline{\lambda}}_p(C, T)$ satisfy the first three properties follows from their definition. In virtue of Remark 3.4, the fourth property also holds. Therefore Lemma 3.2 also holds after replacing $a_{\overline{\mathfrak{p}}}, b_{\mathfrak{p}}, c_{\mathfrak{p}}$ with $a_{\mathfrak{p}, \overline{\lambda}}, b_{\mathfrak{p}, \lambda}, c_{\mathfrak{p}, \lambda}$.

Remark 3.7. It would be interesting to investigate to which extent the results of this section admit generalizations to superelliptic curves of the form $y^4 = f(x)$, where f is a degree 3 polynomial.

3.2. **The inert case.** Let $\mathfrak{I}(C)$ denote the set of rational primes coprime to the discriminant of f and congruent to 2 modulo 3. In particular, any prime of $\mathfrak{I}(C)$ is of good reduction for C.

Lemma 3.8. *For every p in $\mathfrak{I}(C)$ there exist algebraic integers $\alpha, \overline{\alpha}$ satisfying $\alpha \cdot \overline{\alpha} = p$ such that*

$$L_p(C, T) = (1 + pT^2)(1 - \alpha^2 T^2)(1 - \overline{\alpha}^2 T^2).$$

In particular, $L_p(C, T) = (1 + pT^2)(1 - t_p T^2 + p^2 T^4)$, where t_p is an integer such that $|t_p| \leq 2p$.

Proof. The statement follows from the fact that $\#C_p(\mathbb{F}_p) = 1 + p$ and $\#C_p(\mathbb{F}_{p^3}) = 1 + p^3$ (see [BTW05, Lemma 2.1]). $\qquad\square$

Let $\tilde{f} \in \mathbb{F}_p[x]$ denote the reduction of f modulo p.

Lemma 3.9. *For every p in $\mathfrak{I}(C)$, we have:*

$$t_p \equiv \begin{cases} 2 \pmod{3} & \text{if } \tilde{f} \in \mathbb{F}_p[x] \text{ is reducible,} \\ 1 \pmod{3} & \text{if } \tilde{f} \in \mathbb{F}_p[x] \text{ is irreducible.} \end{cases}$$

Proof. On the one hand, from Lemma 3.8 one easily finds that

$$\#C_p(\mathbb{F}_{p^2}) = (1 + p)^2 - 2(\alpha^2 + \overline{\alpha}^2) \equiv t_p \pmod{3}.$$

On the other hand, since every nonzero element of $\mathbb{F}_{p^2}$ has three distinct cubic roots and $\overline{C}_p$ has a single ($\mathbb{F}_p$-rational) point at infinity P_∞, its number of points over $\mathbb{F}_{p^2}$ satisfies

$$\#C_p(\mathbb{F}_{p^2}) \equiv 1 + n(\tilde{f}) \pmod{3},$$

where $n(\tilde{f})$ is the number of roots of $\tilde{f}$ over $\mathbb{F}_{p^2}$. The lemma follows from the fact that $n(\tilde{f}) = 0$, 1, or 4 depending on whether $\tilde{f} \in \mathbb{F}_p[x]$ is irreducible, decomposes and has an irreducible factor of degree 3, or decomposes in factors of degree at most 2, respectively. $\qquad\square$

Lemma 3.9 tells that for every p in $\mathfrak{I}(C)$ the reduction of $L_p(C, T)$ modulo 3 is uniquely determined by the factorization of $\tilde{f} \in \mathbb{F}_p[x]$. Let us give an alternative proof of this fact, which will also extend to the case that p belongs to $\mathfrak{S}(C)$. The method is an adaptation of the technique used in [CDF20], where the hyperelliptic case (of arbitrary genus) was considered.

We will first need to introduce some notations. Let $\mathrm{Jac}(C)$ denote the Jacobian variety of C. Let $\alpha_i \in \overline{\mathbb{Q}}$, for $1 \leq i \leq 4$, denote the roots of $f \in \mathbb{Z}[x]$, and denote by E_i the degree 0 divisor $(\alpha_i, 0) - P_\infty$. By [Aru21, Prop. 2.1], there is a degree 3 effective divisor $\tilde{D}_i$ such that

$$(1 - \zeta_3)\tilde{D}_i \sim E_i.$$

Let D_i denote the degree 0 divisor $\tilde{D}_i - 3P_\infty$, and thus also $(1 - \zeta_3)D_i \sim E_i$.

Note that $3E_i, 3D_i \sim 0$, and let V_1 denote the subspace of $\mathrm{Jac}(C)[3](\overline{\mathbb{Q}})$ generated by the classes $[E_i]$. Note that V_1 is stable under the Galois action. Let $[\overline{D}_i]$ denote the image of $[D_i]$ in the quotient $V_2 := \mathrm{Jac}(C)[3](\overline{\mathbb{Q}})/V_1$.

Lemma 3.10. $[\overline{D}_1], [\overline{D}_2], [\overline{D}_3]$ *is a basis for V_2.*

Proof. Note that V_1 is generated by $[E_1], [E_2], [E_3]$ since $-E_1 - E_2 - E_3 \sim E_4$. In fact, by [Sch98, Prop. 3.2], there is a $G_{\mathbb{Q}}$-equivariant isomorphism

$$(3.7) \qquad \qquad \mathrm{Jac}(C)[1 - \zeta_3](\overline{\mathbb{Q}}) \simeq V_1$$

of 3-dimensional $\mathbb{F}_3$-vector spaces. Hence it suffices to show that $[\overline{D}_1], [\overline{D}_2], [\overline{D}_3]$ are linearly independent. Suppose there were a nontrivial linear relation among $[\overline{D}_1], [\overline{D}_2], [\overline{D}_3]$. This would yield, by multiplication by $(1 - \zeta_3)$, a nontrivial linear relation among $[E_1], [E_2], [E_3]$, but this is absurd. $\qquad \square$

Proposition 3.11. *Let $\{d_i\}_i$ denote the set of degrees of the irreducible factors of $\tilde{f}$. Then:*

(i) *For every p in $\mathfrak{S}(C)$, we have*

$$L_p(C, T) \equiv (1 - T)^{-2} \prod_i (1 - T^{d_i})^2 \pmod 3.$$

(ii) *For every p in $\mathfrak{I}(C)$, we have*

$$L_p(C, T) \equiv (1 - T^2)^{-1} \prod_i (1 - T^{d_i})(1 - (2T)^{d_i}) \pmod 3.$$

Proof. For any prime p of good reduction, by taking $\ell = 3$ in (2.1), we obtain

$$L_p(C, T) \equiv \det(1 - \mathrm{Frob}_p T \mid \mathrm{Jac}(C)[3](\overline{\mathbb{Q}})) \pmod 3.$$

By Lemma 3.10, we need only determine how Frob_p acts on the basis $[E_i]$ for V_1 and $[\overline{D}_i]$ for V_2. Associated to Frob_p, there is an element τ in the symmetric group on 4 letters such that $\mathrm{Frob}_p(\alpha_i) = \alpha_{\tau(i)}$. Then $\mathrm{Frob}_p([E_i]) = [E_{\tau(i)}]$. Note that the set of lengths of the cycles in the cycle decomposition of τ coincides with the set of degrees $\{d_i\}_i$.

Suppose that p is in $\mathfrak{S}(C)$. In this case $\mathrm{Frob}_p(1 - \zeta_3) = (1 - \zeta_3)$, and hence, from the definition of the $[E_i]$ and $[D_i]$, we find

$$\mathrm{Frob}_p([E_i]) = [E_{\tau(i)}], \qquad (1 - \zeta_3) \mathrm{Frob}_p([D_i]) = (1 - \zeta_3)[D_{\tau(i)}].$$

By (3.7), the second equality means that $\mathrm{Frob}_p([D_i])$ and $[D_{\tau(i)}]$ differ by an element of V_1. Hence $\mathrm{Frob}_p([\overline{D}_i]) = [\overline{D}_{\tau(i)}]$. By Lemma 3.12 below applied to V_1 and V_2, we deduce that

$$L_p(C, T) \equiv (1 - T)^{-2} \prod_i (1 - T^{d_i})^2 \pmod 3.$$

Suppose that p is in $\mathfrak{I}(C)$. In this case, we have that $\mathrm{Frob}_p(1 - \zeta_3) = 1 - \zeta_3^2$, and thus we get

$$(1 - \zeta_3^2) \mathrm{Frob}_p([D_i]) = \mathrm{Frob}_p((1 - \zeta_3)[D_i]) = \mathrm{Frob}_p([E_i]) = [E_{\tau(i)}] = (1 - \zeta_3)[D_{\tau(i)}].$$

By (3.7), the above equality means that $(1 + \zeta_3) \mathrm{Frob}_p([D_i])$ and $[D_{\tau(i)}]$ differ by an element of V_1. Since $(1 - \zeta_3) \mathrm{Frob}_p([D_i])$ is an element of V_1, we get that $2 \mathrm{Frob}_p([\overline{D}_i]) = [\overline{D}_{\tau(i)}]$, or equivalently that $\mathrm{Frob}_p([\overline{D}_i]) = 2[\overline{D}_{\tau(i)}]$. By Lemma 3.12 applied to V_1 and V_2, we deduce that

$$L_p(C, T) \equiv (1 - T)^{-1}(1 - 2T)^{-1} \prod_i (1 - T^{d_i})(1 - (2T)^{d_i}) \pmod 3,$$

which completes the proof of the proposition. $\qquad \square$

Lemma 3.12 is used in the proof of Proposition 3.11.

Lemma 3.12. *Let k be a field, V a k-vector space of dimension n, and $v_1, \ldots, v_n$ a basis of V. Define $v_{n+1} := -v_1 + \cdots - v_n$. Let $f \colon V \to V$ be the k-linear automorphism defined by*

$$f(v_i) = a v_{\tau(i)}, \qquad \text{for } i = 1, \ldots, n,$$

where $a \in k$ and τ is an element of the symmetric group in $n+1$ letters. Let $\{d_i\}_i$ be the set of lengths of the cycles in the cycle decomposition of τ. Then the reversed characteristic polynomial of f is

$$\chi_{f,V}(T) = \frac{1}{1 - aT} \prod_i (1 - (aT)^{d_i}).$$

Proof. Let W be a k-vector space of dimension $n+1$ with basis $w_1, \ldots, w_{n+1}$. Define the k-linear maps

$$\Phi \colon W \to V, \qquad g \colon W \to W,$$

by $\Phi(w_i) = v_i$ and $g(w_i) = a w_{\tau(i)}$. It is clear that Φ is equivariant with respect to the actions of g and f on W and V, respectively, and that the kernel N of Φ is generated by $\sum_i w_i$. Therefore $\chi_{f,V}(T) = \chi_{g,W}(T)/(1 - aT)$, and the lemma follows. $\square$

Recall the polynomial ψ_f defined in (1.2). Let $\tilde{\psi}_f$ denote its reduction modulo p.

Theorem 3.13. *Let C be a Picard curve defined over $\mathbb{Q}$, and let $f, \psi_f \in \mathbb{Z}[x]$ be as in (1.1) and (1.2), respectively. For every prime in $\mathfrak{I}(C)$, the data:*

   (i) *the Cartier–Manin matrix of C at p,*
   (ii) *the knowledge of $\tilde{\psi}_f$ having an $\mathbb{F}_p$-rational root or not, and*
   (iii) *the knowledge of $\tilde{f} \in \mathbb{F}_p[x]$ being irreducible or not*

uniquely determine the L-polynomial $L_p(C, T)$.

Proof. By Lemma 3.8, it suffices to determine t_p. Since $|t_p| \le 2p$, it suffices to detemine t_p modulo $6p$. But (i) determines t_p modulo p; by the Theorem in the Appendix, (ii) determines t_p modulo 2; and both by Lemma 3.9 or Proposition 3.11, (iii) determines t_p modulo 3. $\square$

In Section 4 Theorem 3.13 will be used to describe a (deterministic) algorithm to compute the $L_p(C, T)$ for primes p in $\mathfrak{I}(C)$. Let $\mathrm{Jac}(C_p)$ denote the Jacobian variety of C_p, and let n (resp. λ) denote the order (resp. exponent) of the group of $\mathbb{F}_p$-rational points of $\mathrm{Jac}(C_p)$. Below we present a variant of Theorem 3.13 in which we replace condition (ii) by the knowledge of λ.

Theorem 3.14. *Let $p \ge 877$ be a prime in $\mathfrak{I}(C)$. The data:*

   (i) *t_p modulo p,*
   (ii) *the knowledge of $\tilde{f} \in \mathbb{F}_p[x]$ being irreducible or not, and*
   (iii) *the exponent λ of $\mathrm{Jac}(C_p)(\mathbb{F}_p)$*

uniquely determine the L-polynomial $L_p(C, T)$.

Proof. Since $n = (1+p)(1+p^2 - t_p)$, in order to determine t_p, it suffices to determine n. By Lemmas 3.8 and 3.9, from (i) and (ii) we may assume given an integer $0 \le s_p \le 3p$ such that $t_p \equiv s_p \pmod{3p}$. In fact, s_p uniquely determines t_p

unless $p \leq s_p \leq 2p$, and hence we will assume that the latter restriction holds from now on. In this case, the order n is either

$$(3.8) \qquad n_1 = (1+p)(1+p^2 - s_p) \qquad \text{or} \qquad n_2 = (1+p)(1+p^2 - s_p + 3p).$$

If λ fails to divide one among n_1 and n_2, then the order n is uniquely determined. Thus, we suppose from now on that λ divides both n_1 and n_2, and hence that it divides their difference $3p(p+1)$. By [CFADLNV05, Prop. 5.78], we have that

$$(3.9) \qquad \mathrm{Jac}(C_p)(\mathbb{F}_p) \simeq \bigoplus_{j=1}^{6} \mathbb{Z}/m_j\mathbb{Z},$$

where the integers m_j satisfy $m_j \mid m_{j+1}$ for $1 \leq j \leq 5$, $m_j \mid p-1$ for $1 \leq j \leq 3$, and $m_6 = \lambda$.

Suppose first that p does not divide m_6. Then m_6 must divide $3(1+p)$. Since $p \equiv 2 \pmod{3}$ and for $1 \leq j \leq 3$ we have that m_j divides $p-1$ and m_6, this implies that $m_j \mid 2$ for $1 \leq j \leq 3$. For $4 \leq j \leq 6$, let us write $m_j = 3(1+p)/c_j$ for some integer c_j. From (3.8) and the bounds on s_p, we obtain

$$(p+1)(p-1)^2 \leq \# \mathrm{Jac}(C_p)(\mathbb{F}_p) \leq (p+1)^3.$$

This implies

$$1 \leq \frac{c_4 c_5 c_6}{27 m_1 m_2 m_3} \leq \left(\frac{p+1}{p-1}\right)^2 =: B(p).$$

A straightforward computation shows that $B(p) < 1 + 2^{-3} \cdot 3^{-3}$ under the assumption of the statement that $p \geq 877$. Since the denominator of the central term of the above inequality is bounded by $2^3 \cdot 3^3$, we deduce that $c_4 c_5 c_6 = 27 m_1 m_2 m_3$, or equivalently that $n = (1+p)^3$, $s_p = p$, and $t_p = -2p$.

Suppose next that p divides m_6. Then (3.8) implies that $s_p = p + 1$. Therefore

$$(3.10) \qquad n_1 = (1+p)p(p-1) \qquad \text{and} \qquad n_2 = (1+p)p(p+2).$$

We claim that this can only occur if p is a Fermat prime. Indeed, suppose the contrary for the sake of contradiction. Then there is an odd prime ℓ dividing $p-1$. Note that such an ℓ does not divide $(1+p)p$. As $p \equiv 2 \pmod{3}$, in particular we have that $\ell \neq 3$ and thus ℓ does not divide n_2. Let ℓ' be a prime dividing $p+2$. Since $p \equiv 2 \pmod{3}$, necessarily $\ell' \geq 5$. Note that such an ℓ' does not divide n_1. By Lagrange's theorem, exactly one among ℓ and ℓ' divides λ. But this is a contradiction with the fact that λ divides both n_1 and n_2. Thus there exists an integer r such that $p = 2^r + 1$. If $r \geq 6$ (which is clearly satisfied by assumption), we have $v_2(n_1) \geq 7$, where v_2 denotes the 2-adic valuation. Hence $n = n_1$ implies that $v_2(m_6) \geq 2$. On the other hand, we have that $v_2(m_6) = 1$ if $n = n_2$. $\square$

In Section 4.1, Theorem 3.14 will be used to sketch a randomized algorithm of Las Vegas type with the same complexity as the deterministic one to compute the $L_p(C, T)$ for p in $\mathfrak{I}(C)$.

3.3. Interlude on a theorem of Sawin.
Throughout this section, let A be an abelian variety defined over a number field k and of dimension g, let E be a number field of degree e, and suppose that there exists a $\mathbb{Q}$-algebra homomorphism

$$E \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q},$$

where $\mathrm{End}(A)$ denotes the ring of endomorphisms of A defined over k.

By [Fit20, Thm. 1], if $g = 3$ and E is imaginary quadratic, there exists a positive density set of primes of k of ordinary good reduction for A. In Section 3.4, we will refine this result in the particular case that A is the Jacobian of a *generic* Picard curve C. More precisely, we will show that every prime in $\mathfrak{S}(C)$ outside a density 0 set is ordinary for C.

The main input in the proof of [Fit20, Thm. 1] is a result due to Ogus (see for example [Fit20, Prop. 8, Prop. 10]), which allows to prove the existence of a positive density of ordinary primes by studying the p-divisibility of the trace of a certain Galois representation. In order to obtain the sought refinement of [Fit20, Thm. 1], we will take the powerful approach of [Saw16], which by a finer argument permits to in fact compute the exact value of this density. In this section, we present a mild generalization of [Saw16, Thm. 1]. It is this generalization that will be employed in Section 3.4.

Let ℓ be a rational prime, $V_\ell(A)$ denote the rational ℓ-adic Tate module of A, and

$$\varrho_{A,\ell} \colon G_k \to \mathrm{Aut}(V_\ell(A))$$

be the associated ℓ-adic representation. Our first task will be to define some spaces $V_\lambda(A)$, which are analogues of the spaces $H^1_\lambda(\overline{C})$ introduced in (3.5) in our current more general setting. From now on, suppose that ℓ is totally split in E so that $E_\lambda \simeq \mathbb{Q}_\ell$. For every prime λ of E lying above ℓ, let E_λ be the completion of E at λ, and let $V_\lambda(A)$ denote the tensor product $V_\ell(A) \otimes_{E \otimes \mathbb{Q}_\ell, \sigma_\lambda} E_\lambda$ taken with respect to the $\mathbb{Q}_\ell$-algebra map

$$\sigma := \sigma_\lambda \colon E \otimes \mathbb{Q}_\ell \simeq \bigoplus_{\lambda' | \ell} E_{\lambda'} \xrightarrow{\mathrm{pr}_\lambda} \mathbb{Q}_\ell,$$

where pr_λ denotes the projection from the E_λ-component. Denote by G_k the absolute Galois group of k. By letting G_k act naturally on $V_\ell(A)$ and trivially on E_λ, one obtains a continuous representation

$$\varrho_{A,\lambda} \colon G_k \to \mathrm{Aut}(V_\lambda(A)) \simeq \mathrm{GL}_{2g/e}(\mathbb{Q}_\ell)$$

unramified outside a finite set S of primes of k and which is integral and of weight 1 (by [Rib76, Thm. 2.11]). By integral, we mean that the characteristic polynomial of $\varrho_{A,\lambda}(\mathrm{Frob}_\mathfrak{p})$ has coefficients in the ring of integers $\mathcal{O}_E$ of E for every prime $\mathfrak{p}$ of k outside S. After fixing a polarization on A, the image Γ of $\varrho_{A,\ell}$ sits inside $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$. Let G denote the Zariski closure of Γ inside GSp_{2g} (seen as an algebraic group over $\mathbb{Q}_\ell$). Let Γ_λ denote the image of $\varrho_{A,\lambda}$ inside $\mathrm{GL}_{2g/e}(\mathbb{Q}_\ell)$ and let G_λ denote the Zariski closure of Γ_λ inside $\mathrm{GL}_{2g/e}$. The isomorphism

$$V_\ell(A) \simeq \bigoplus_\lambda V_\lambda(A)$$

of $\mathbb{Q}_\ell[G_k]$-modules induces a monomorphism $G \hookrightarrow \prod_\lambda G_\lambda$. Composing this injection with the projection to the λ-component yields a representation of G inside $\mathrm{GL}_{2g/e}(\mathbb{Q}_\ell)$ that we will denote by W_λ. Let χ denote the restriction to G of the similitude character of GSp_{2g}. Let w_λ denote the number of connected components of G on which the trace of the representation $\wedge^2 W_\lambda \otimes \chi^{-1}$ is identically equal to a constant function. By $\mathrm{Nm}(\cdot)$ we denote both the absolute norm function on ideals of a given number field, and the absolute norm function on algebraic numbers. For

a prime $\mathfrak{p}$ outside S, let us denote by $b_{\mathfrak{p},\lambda}$ the trace[2] $\mathrm{Tr}(\wedge^2 \varrho_{A,\lambda}(\mathrm{Frob}_{\mathfrak{p}}))$. Note that if $\wedge^2 W_\lambda \otimes \chi^{-1}$ is identically equal to the constant function $t \in \mathbb{Q}_\ell$ on a connected component of G, then there exist at least two primes $\mathfrak{p}$ and $\mathfrak{q}$ of k such that

$$t = \frac{b_{\mathfrak{p},\lambda}}{\mathrm{Nm}(\mathfrak{p})} = \frac{b_{\mathfrak{q},\lambda}}{\mathrm{Nm}(\mathfrak{q})}.$$

This implies that t in fact belongs to $\mathcal{O}_E \subseteq \mathbb{Q}_\ell$. We will denote by p the residue characteristic of the prime $\mathfrak{p}$.

Theorem 3.15 (After Sawin). *Suppose that E is either $\mathbb{Q}$ or an imaginary quadratic field. The density of the set of primes $\mathfrak{p}$ of k outside S such that $b_{\mathfrak{p},\lambda}$ is divisible by p equals w_λ divided by the number of connected components of G.*

Proof. Let T denote the set of elements t in $\mathcal{O}_E$ such that $|\mathrm{Nm}(t)| \leq \binom{2g/e}{2}^2$. For any real number $C \geq 0$ the set of elements a of $\mathcal{O}_E$ whose norm satisfies $|\mathrm{Nm}(a)| \leq C$ is finite. Indeed, if $E = \mathbb{Q}$ this is obvious, and if E is an imaginary quadratic field, then this follows from the fact that both the number of units in $\mathcal{O}_E$ and the number of ideals of absolute norm $\leq C$ are finite. Therefore the set T is finite. Since $\wedge^2 \varrho_{A,\lambda}$ is of weight 2, for every prime $\mathfrak{p}$ outside S we have

$$\left| \mathrm{Nm}\left(\frac{b_{\mathfrak{p},\lambda}}{p} \right) \right| \leq \dim(\wedge^2 W_\lambda)^2 = \binom{2g/e}{2}^2,$$

and thus if $b_{\mathfrak{p},\lambda} = pt$, for some $t \in \mathcal{O}_E$ and some $\mathfrak{p}$ outside S, then $t \in T$. Let Z_λ^t denote the closed subset of G on which $\wedge^2 W_\lambda \otimes \chi^{-1}$ is identically equal to the constant function t. Let Z_λ denote the finite union

$$Z_\lambda := \bigcup_{t \in T} Z_\lambda^t.$$

Let μ denote the Haar measure of Γ, normalized so that it has total mass 1. Then exactly as in the proof of [Saw16, Thm. 1] one shows that $\mu(Z_\lambda \cap \Gamma)$ is the sought for density and that $\mu(Z_\lambda \cap \Gamma)$ equals w_λ divided by the number of connected components of G. $\qquad\square$

3.4. **Ordinary primes for generic Picard curves.** Resume the notations from Sections 3.1 and 3.2. In particular, let C be a Picard curve defined over $\mathbb{Q}$.

Corollary 3.16. *Suppose that C is a generic Picard curve. Then, every prime p in $\mathfrak{S}(C)$ outside a density 0 set is ordinary for C.*

Proof. Let $k = E = \mathbb{Q}(\zeta_3)$ and $A = \mathrm{Jac}(C)_k$. Denote by G the Zariski closure of the image of the ℓ-adic representation attached to A. By [FKRS12, Prop. 2.17], when C is generic, G is connected (in fact, Upton [Upt09] has shown that if C is generic, then for all but finitely many $\ell \equiv 1 \pmod 3$ one has $\varrho_{A,\ell}(G_k) \simeq \mathrm{GL}_3(\mathbb{Z}_\ell)$). Since the trace of $\wedge^2 W_\lambda \otimes \chi^{-1}$ is not constant on G, the set of primes p in $\mathfrak{S}(C)$ for which $b_{\mathfrak{p},\lambda}$ is divisible by p has density 0. But, by Lemma 3.2 and Remark 3.6, a prime p in $\mathfrak{S}(C)$ is ordinary for C if and only if $b_{\mathfrak{p},\lambda}$ is not divisible by p. $\qquad\square$

Combining Corollary 3.16 with Corollary 3.3, we obtain the following result.

---

[2]In the particular case that A is the Jacobian of a Picard curve and $E = \mathbb{Q}(\zeta_3)$, this coincides with the definition of $b_{\mathfrak{p},\lambda}$ given in Section 3.1.

Corollary 3.17. *Suppose that C is a generic Picard curve. Then, for every prime p in $\mathfrak{S}(C)$ outside a density 0 set, the Cartier–Manin matrix of C at p uniquely determines the L-polynomial $L_p(C,T)$.*

By Lemma 3.8, no prime in $\mathfrak{I}(C)$ is ordinary. Let b_p denote the coefficient of T^2 in $L_p(C,T)$. For the sake of completeness, we study the density of the set of primes in $\mathfrak{I}(C)$ for which $b_p \equiv 0 \pmod{p}$.

Corollary 3.18. *Suppose that C is a generic Picard curve. Then, the set of primes p in $\mathfrak{I}(C)$ such that $b_p \equiv 0 \pmod{p}$ has density 0.*

Proof. Since C is generic, the Zariski closure G of the image of $\varrho_{A,\ell}$ consists of two connected components G^0 and G^1, which are the respective Zariski closures of the images of $G_{\mathbb{Q}(\zeta_3)}$ and $G_{\mathbb{Q}} - G_{\mathbb{Q}(\zeta_3)}$. By Theorem 3.15 applied to $k = E = \mathbb{Q}$, $A = \mathrm{Jac}(C)$, and $\lambda = \ell$, it suffices to show that the trace of $\wedge^2 W_\ell \otimes \chi$ on G^1 is not a constant function.

Let $\mathrm{ST}(A)$ denote the Sato–Tate group of A. It is a compact real Lie subgroup of the unitary symplectic group $\mathrm{USp}(6)$ of degree 6. Let $\mathrm{U}(3)$ denote the unitary group of degree 3 in its standard representation, and let $I_3 \in \mathrm{U}(3)$ denote the identity matrix. Let W denote the standard representation of $\mathrm{USp}(6)$. By [FKS21, §3.3.1], we have that $\mathrm{ST}(A) = \langle \mathrm{ST}(A)^0, J \rangle$, where

$$\mathrm{ST}(A)^0 = \left\{ \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix} : u \in \mathrm{U}(3) \right\} \quad \text{and} \quad J = \begin{pmatrix} 0 & I_3 \\ -I_3 & 0 \end{pmatrix}.$$

As argued in the proof of [Saw16, Thm. 3], the trace of $\wedge^2 W_\ell \otimes \chi$ on G^1 is a constant function if and only if the trace of $\wedge^2 W$ on $J\mathrm{ST}(A)^0$ is a constant function. But the latter is not true, since if we set

$$A = J \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix}, \quad \text{with } u = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

then $\mathrm{Tr} \wedge^2 W(A) = 0$, while $\mathrm{Tr} \wedge^2 W(J) = 3$. $\qquad \square$

4. L-polynomials of Picard curves: A practical algorithm

Let C be a generic Picard curve defined over $\mathbb{Q}$. In this section we use the results obtained in Section 3 to develop and implement an algorithm for the computation of the L-polynomials $L_p(C,T)$ for almost all primes up to some bound N. We first describe the algorithm, then analyze its running time and correctness, and finally discuss its implementation.

4.1. **Description.** Denote by $\mathfrak{S}^*(C)$ the subset of ordinary primes in $\mathfrak{S}(C)$. For $N \geq 1$, set

$$\mathfrak{S}_N^*(C) := \mathfrak{S}^*(C) \cap [1, N], \qquad \mathfrak{I}_N(C) := \mathfrak{I}(C) \cap [1, N].$$

We will rely on the following algorithms documented in the literature:

- COMPUTECARTIERMANINMATRICES ([Sut20, p. 10]). Algorithm that, given an integer $N \geq 1$ and a Picard curve C, computes the Cartier–Manin matrix A_p of C at p for every prime $5 \leq p \leq N$ not dividing the discriminant of f.
  Running time: $N \log(N)^{3+o(1)}$.

- FINDCUBICROOTS (See Remark 4.1). Algorithm that, given an integer $N \geq 1$, returns a primitive cubic root of unity in $\mathbb{F}_p^\times$ for every prime $p \equiv 1$ (mod 3) and $\leq N$.
  Running time: $N \log(N)^{3+o(1)}$.

- ISIRREDUCIBLE ([GG13, Thm. 14.4]). Algorithm that, given the polynomial $\tilde{f} \in \mathbb{F}_p[x]$ of degree 4, determines whether it is irreducible or not.
  Running time: $\log(p)^{2+o(1)}$.

- HASRATIONALROOT (See the Corollary in the Appendix). Algorithm that, given the polynomial $\tilde{\psi}_f \in \mathbb{F}_p[x]$ of degree 9, determines whether it has an $\mathbb{F}_p$-rational root or not.
  Running time: $\log(p)^{2+o(1)}$.

Remark 4.1. We describe algorithm FINDCUBICROOTS. Pick an elliptic curve with CM discriminant $D = -12$, for example $E\colon y^2 = x^3 - 15x + 22$. The algorithms given in [HS14], [HS16], and [Sut20] compute the trace of Frobenius t_p of E at p for all primes $p \leq N$ in time $N \log(N)^{3+o(1)}$, excluding a finite subset of all primes. For every prime $p \equiv 1$ (mod 3), which is necessarily of good ordinary reduction, there exists an integer u_p satisfying the norm equation

$$4p = t_p^2 + 12u_p^2.$$

Since p is ordinary for E, u_p is invertible modulo p, and the above equation provides a way to compute a square root of -3 in $\mathbb{F}_p$ as $t_p/(2u_p)$, and hence $\zeta_3 \in \mathbb{F}_p$. We note that this is a one-time computation if one wishes to run the algorithm for multiple curves.

At this point we have described all the theoretical and computational tools necessary in order to state the main algorithm of this article.

Algorithm 4.2 (COMPUTELPOLYNOMIALS). Given an integer $N \geq 1$ and a Picard curve C over $\mathbb{Q}$, compute $L_p(C, T)$ for every prime $p \in \mathfrak{S}_N^*(C) \cup \mathfrak{I}_N(C)$, by following the steps:

  (a) Apply COMPUTECARTIERMANINMATRICES to obtain A_p for every prime $5 \leq p \leq N$ not dividing the discriminant of f.
  (b) By means of FINDCUBICROOTS, find primitive cubic roots of unity for every $p \equiv 1$ (mod 3) up to N.
  (c) For every $p \equiv 1$ (mod 3) as in (a), determine whether $p \in \mathfrak{S}^*(C)$, by computing $\mathrm{rk}(A_p)$, and if so then:
    (1) If $p < 53$, then use naive point counting to compute $L_p(C, T)$. Otherwise continue to (2).
    (2) Let $\sigma(\zeta_3), \overline{\sigma}(\zeta_3) \in \mathbb{F}_p^\times$ be the primitive cubic roots of unity found in (b). Solve the linear system (3.3) to determine $a_{\mathfrak{p}}$ (and hence $a_{\overline{\mathfrak{p}}}$).
    (3) Choose an integer $1 \leq \gamma \leq p$ such that $\gamma \equiv \sigma(\zeta_3)$ (mod p). Determine $\pi \in \mathbb{Z}[\zeta_3]$ as the $\gcd(\gamma - \zeta_3, p)$, by applying the extended Euclidean division algorithm in $\mathbb{Z}[\zeta_3]$.
    (4) Solve the linear equation (3.4) to determine ζ and thereby $c_{\mathfrak{p}}$.
    (5) Apply part (i) of Lemma 3.2 to determine $b_{\mathfrak{p}}$ and thereby $L_p(C, T)$.
  (d) For every $p \equiv 2$ (mod 3) as in (a), let t_p be as in Lemma 3.8. Then:
    (1) Determine t_p modulo p by means of A_p.

(2) Apply the Corollary in the Appendix to determine t_p modulo 2 by applying HasRationalRoot to $\tilde{\psi}_f$.
(3) Apply Lemma 3.9 or Proposition 3.11 to determine t_p modulo 3 by applying IsIrreducible to $\tilde{f}$.
(4) Determine $L_p(C, T)$ from the above information by using Lemma 3.8.

Theorem 4.3. *Let C be a Picard curve. Algorithm 4.2 computes $L_p(C, T)$ for every prime $p \in \mathfrak{S}_N^*(C) \cup \mathfrak{I}_N(C)$ in time $N \log(N)^{3+o(1)}$. When C is generic, the complement of $\mathfrak{S}^*(C) \cup \mathfrak{I}(C)$ in the set of primes has density 0.*

Proof. Once we have computed the Cartier–Manin matrix by using ComputeCartierManinMatrices, correctness of the algorithm follows from the proofs of Corollary 3.3 and Theorem 3.13. Note that in step (c) (3), we may set $\pi = \gcd(\gamma - \zeta_3, p)$ in virtue of the Dedekind–Kummer theorem. As for complexity, note that both steps (a) and (b) already have the claimed complexity (although we note that (b) is a one-time computation). We only need to show that the remaining steps do not exceed this complexity. As we have seen, none of the algorithms IsIrreducible and HasRationalRoot does, and the remaining steps are clearly faster as they solve a small linear system or compute a small gcd in $\mathbb{Z}[\zeta_3]$. In the generic case, the claim about density is ensured by Corollary 3.16. $\square$

Remark 4.4. There exist several methods of verifying that a given Picard curve C defined over $k = \mathbb{Q}(\zeta_3)$ is generic. On the one hand, one may apply the criterions provided by Zarhin (specifically see [Zar18, Thm 1.3]). On the other hand, one can use results due to Upton. More precisely, we claim that if $\ell \geq 5$ is a prime $\equiv 1 \pmod 3$ such that the mod-ℓ image of the Galois representation associated to $A := \mathrm{Jac}(C)$ is $\mathrm{GL}_3(\mathbb{F}_\ell)$, then C is generic. Indeed, by [Upt09, Prop. 6], the hypotheses imply that the image of the ℓ-adic representation $\varrho_{A,\ell}$ is $\mathrm{GL}_3(\mathbb{Z}_\ell)$. Then, for any finite extension L/k, the commutant of $\varrho_{A,\ell}(G_L)$ in $\mathrm{End}(V_\ell(A))$ is 2-dimensional. By Faltings' isogeny theorem, this commutant is $\mathrm{End}(A_L) \otimes \mathbb{Q}_\ell$, and hence $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathbb{Z}[\zeta_3]$, which completes the proof of the claim. Verifying that the mod-ℓ image of the Galois representation associated to A is $\mathrm{GL}_3(\mathbb{F}_\ell)$ can be done by using [Upt09, Lemma 3] and computing a few $L_p(C, T)$ (this is done in [Upt09, §6] for two specific curves, to which we will return in Section 4.2).

Remark 4.5. Note that by Dirichlet's density theorem and by Corollary 3.16, the set of primes $p \leq N$ in $\mathfrak{S}(C) - \mathfrak{S}^*(C)$ has size $o(N/\log(N))$. Despite being unable to prove it, it is conceivable that this set is actually small enough so that the combination of Algorithm 4.2 with the algorithm of [ABCMT19] (to separately treat the primes in $\mathfrak{S}(C) - \mathfrak{S}^*(C)$) would yield an algorithm to compute $L_p(C, T)$ for every prime $p \leq N$ in time $N \log(N)^{3+o(1)}$.

We will now sketch how one can use the proof of Theorem 3.14 to give a randomized algorithm of Las Vegas time accomplishing the same task as ComputeLPolynomials and having the same expected complexity (for details and an actual implementation we refer to [AP20]).

While from a computational perspective the determination of the exponent λ of $\mathrm{Jac}(C_p)(\mathbb{F}_p)$ presents difficulties, a detailed examination of the proof of Theorem 3.14 shows that only partial (and effectively computable) information on λ is required in order to uniquely determine $L_p(C, T)$.

The variant that we want to discuss only differs from Algorithm 4.2 in case p is in $\mathfrak{J}(C)$. Let $p \geq 877$ be one such prime. Assume given the data (i) and (ii) of Theorem 3.14. Suppose also that we are in the case that there exists $p \leq s_p \leq 2p$ such that $t_p \equiv s_p \pmod{3p}$, and let n_1 and n_2 be as defined by (3.8). We claim that exactly one of the following options occurs:

   (i) $s_p \neq p, p+1$ or $s_p = p+1$ and p is not a Fermat prime. In this case, $\lambda \nmid 3p(p+1) = n_2 - n_1$ so it cannot divide both n_1 and n_2. Thus, there is a point P in $\mathrm{Jac}(C_p)(\mathbb{F}_p)$ such that $n_i \cdot P \neq 0$ for $i = 1$ or 2, and then $n = n_{3-i}$.
   (ii) $s_p = p$ and there is a prime $\ell \geq 5$ dividing λ but not $p+1$. In this case $n = (p+1)(p^2 - p + 1)$.
   (iii) $s_p = p$ and there are three points P, Q, R in $\mathrm{Jac}(C_p)(\mathbb{F}_p)$ generating a subgroup of order divisible by $3^{v_3(p+1)+2}$. In this case $n = (p+1)^3$.
   (iv) $s_p = p+1$, p is a Fermat prime, and there is an odd prime ℓ dividing λ but not $p(p+1)(p-1)$. In this case $n = (1+p)p(p+2)$.
   (v) $s_p = p+1$, p is a Fermat prime, and there is a point P in $\mathrm{Jac}(C_p)(\mathbb{F}_p)$ of order divisible by 4. In this case $n = (1+p)p(p-1)$.

Indeed, it has been shown in the course of the proof of Theorem 3.14 that we have the conclusion of (i) if $s_p \neq p, p+1$ or if $s_p = p+1$ and p is not a Fermat prime. From (3.8), $s_p = p$ implies that n is either $n_1 = (p+1)(p^2 - p + 1)$ or $n_2 = (p+1)^3$. To show that (ii) and (iii) are mutually exclusive, it suffices to note that $v_3(p^2 - p + 1) = 1$. Thus, $v_3(n_1) = v_3(p+1)+1$ and $p^2 - p + 1$ has a divisor $\ell \geq 5$. Such an ℓ necessarily fails to divide $p+1$. Recall the values m_j introduced in (3.9). It remains to show that if $n = n_2$, then $v_3(m_4 m_5 m_6) \geq v_3(p+1) + 2$. But we have seen that $v_3(m_j) = 0$ for $1 \leq j \leq 3$ and therefore we have $v_3(m_4 \cdot m_5 \cdot m_6) = 3v_3(p+1) \geq v_3(p+1)+2$. From (3.8), $s_p = p+1$ implies that n is either $n_1 = (1+p)p(p-1)$ or $n_2 = (1+p)p(p+2)$. Under the assumption that p is a Fermat prime, the conclusions of (iv) and (v) have been seen at the end of the proof of Theorem 3.14.

Given these five cases, we may produce a Las Vegas algorithm by generating random points of the Jacobian (using [MJS20, §12.2], for example) and checking these conditions efficiently (using the methods of [Sut11], for example). We note that to check each such condition only requires expected $O(1)$ random elements of $\mathrm{Jac}(C_p)(\mathbb{F}_p)$. On a generic Picard curve, Section 3.4 ensures a dense subset of primes fall into case (i), the simplest case to check. The expected complexity of such an algorithm is identical to that of the deterministic algorithm, but in practice slower.

4.2. **Implementation.** The Github repository [AP20] includes an implementation of Algorithm 4.2 in [PARIGP]. This repository also contains an implementation in [Sage] of the Las Vegas algorithm discussed at the end of the previous section, for which we used the Jacobian arithmetic from [MJS20]. We note that this algorithm is still practical, but is slower by a constant factor due to Jacobian arithmetic being expensive.

In either case, the full algorithm for lifting is significantly faster than previous algorithms and has complexity $N \log(N)^{3+o(1)}$ when computing $Z_p(C, T)$ for almost all $p \leq N$. Our algorithm can also operate independently for fixed p when $L_p(C, T) \pmod{p}$ is already provided - this means we can speed up algorithms such as [ABCMT19] for a specific prime, since the most expensive lifting component is

now negligible. As a result, it can also be used to more efficiently compute $L_p(C, T)$ when p is large enough that computing $L_p(C, T)$ for almost all $p \leq N$ is impractical. For a given generic Picard curve over $\mathbb{Q}$, in Table 1 we report the average running time per prime over the primes $\leq N$ of Algorithm 4.2 with the implementation in [PARIGP].

TABLE 1. For the curves $C_1 : y^3 = x^4 + x + 1$ and $C_2 : y^3 = x^4 + 3x^2 + 2x + 1$, we display the average computation time spent per prime $p \leq N$ for [ABCMT19], [Sut20], and Algorithm 4.2 in milliseconds (ms). Bold numbers indicate new results from our algorithm. The timings are taken on a 3.40GHz Intel(R) Xeon(R) E5-2687W CPU. All computations were run with a single core.

N	2^{16}		2^{20}		2^{24}		2^{28}	
Algorithm	Old	New	Old	New	Old	New	Old	New
Full zeta function								
C_1	113.2	**0.31**	215.1	**0.69**	1152.7	**1.50**	5051.4	**4.76**
C_2	111.3	**0.33**	213.5	**0.71**	1152.9	**1.54**	5053.9	**4.87**
Lifting component								
C_1		**0.12**		**0.12**		**0.13**		**0.14**
C_2		**0.12**		**0.12**		**0.13**		**0.14**
Cartier–Manin matrix								
C_1	35.4	0.19	79.1	0.57	277.8	1.37	1368.3	4.63
C_2	34.4	0.20	77.6	0.59	276.7	1.41	1366.7	4.74

In Table 1, to compute these running times we ran each computation for $p \leq N$ three times and took the minimum of those attempts. The "New" columns have running times for our algorithm and [Sut20], since they are used together to compute the full zeta function. In the "Lifting component" section, we have put running times for Algorithm 4.2 and in the "Cartier–Manin matrix" section we have put running times for an implementation of [Sut20] in C. In the "Old" columns, we have the implementation of the algorithm [ABCMT19] in [Sage] computing the full zeta function. We have also used the Frobenius matrix method in [Sage] to compute a matrix which determines the Cartier–Manin matrix. These times are shown in "Old" columns of the "Full zeta function" and "Cartier–Manin" matrix sections respectively in Table 1. Running times for all of these algorithms have been given for two chosen generic curves $C_1 : y^3 = x^4 + x + 1$ and $C_2 : y^3 = x^4 + 3x^2 + 2x + 1$ (see [Upt09, §6.1.1, §6.2.2] for a proof of the genericity of these curves; we note that Zarhin's criterion recalled in Remark 4.4 also applies). For example, we can read off the table that for C_1 computing the zeta function with our algorithm for $p \leq 2^{28}$ takes an average of 4.76 ms per prime. Of this time, on average we spend 0.14 ms on the lifting component described in this paper and 4.63 ms on computing the Cartier–Manin matrices. In comparison, the implementation of [ABCMT19] takes roughly 5051.4 ms per prime.

We note that [ABCMT19] is not fast enough to compute the full zeta function for all $p \leq N$ in a reasonable amount of time when N is very large, so we sampled one out of $10^2, 10^3, 10^4, 10^5$ primes respectively for $N = 2^{16}, 2^{20}, 2^{24}$ and 2^{28} to get estimates for the running times. The same was done for the computation of the

Frobenius matrices. Each computation was run on a single core in order to have a fair comparison. Algorithm 4.2 is used in the 'Lifting component' part of the table to compute the full zeta function once the algorithm from [Sut20] finishes. As can be seen from the table, the lifting component is always faster on average and performs better relative to computing $L_p(C, T) \pmod{p}$ as p becomes very large. There is some variation in the average running times between the two curves, but in each example this is $\approx 10^{-4}$ ms which is why it does not appear in the table.

As noted in the beginning of this section, Algorithm 4.2 also allows us to speed up [ABCMT19] on a Picard curve for a specific prime p by a constant factor. In particular, we need only compute $L_p(C, T) \pmod{p}$, and then lifting this takes a negligible amount of time. The time for the computating $L_p(C, T) \pmod{p}$ differs by a constant factor compared to computing $L_p(C, T)$ using [ABCMT19]. Using [Sage], we can estimate this constant factor to be about 8, for example from

```
sage: p=(2**40).next_prime()
sage: x = PolynomialRing(GF(p),"x").gen()
sage: CyclicCover(3, x^4 + x + 1).frobenius_matrix(1)
```

which takes a total of 3 min and 23 s, while using the algorithm to compute the full result $L_p(C, T)$ takes 24 min and 24 s. By applying Algorithm 4.2 after computing the Frobenius matrix modulo p we improve the running time by around a factor of 8, because for primes of this size our algorithm still takes on the order of a millisecond, which is negligible.

APPENDIX

by Andrew V. Sutherland[3]

In this appendix we give a constructive proof of the following theorem.

Theorem. *Let $p > 3$ be a prime congruent to 2 modulo 3, let $C_p \colon y^3 = f(x)$ be a Picard curve over $\mathbb{F}_p$ with L-polynomial $L_p \in \mathbb{Z}[T]$. The reduction of $L_p(T)$ modulo 2 can be computed (deterministically) in $O((\log p)^2 (\log \log p))$ time.*

Without loss of generality we may assume C_p is the reduction of a Picard curve $C \colon y^3 = f(x)$ over $\mathbb{Q}$. The Jacobian $J := k \operatorname{Jac}(C)$ is an abelian variety of dimension 3, thus the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $J[2]$ gives rise to a mod-2 Galois representation

$$\bar\rho_2 \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(J[2]) \simeq \operatorname{GSp}_6(\mathbb{F}_2) = \operatorname{Sp}_6(\mathbb{F}_2),$$

where we have used the Weil pairing to view $J[2] \simeq \mathbb{F}_2^6$ as a symplectic space. The endomorphism ring of the base change of J to $\mathbb{Q}(\zeta_3)$ contains $\mathbb{Z}[\zeta_3]$ and the prime 2 is inert in $\mathbb{Q}(\zeta_3)$; these facts imply that the restriction of $\bar\rho_2$ to $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_3))$ has image in $U(3, 2) = \operatorname{GU}(3, \mathbb{F}_4)$; see [Upt09, §2] for details.

Up to conjugacy, there is a unique subgroup $H \subseteq \operatorname{Sp}_6(\mathbb{F}_2)$ that is isomorphic to $\operatorname{GU}(3, \mathbb{F}_4)$, which has small group identifier $\langle 648, 533 \rangle$.[4] The endomorphism ring of $J/\mathbb{Q}$ does not contain $\mathbb{Z}[\zeta_3]$, so the image of $\bar\rho_2$ does not lie in H, in general. It lies in a subgroup of $\operatorname{Sp}_6(\mathbb{F}_2)$ isomorphic to $\operatorname{GU}(3, \mathbb{F}_4) \rtimes \operatorname{Gal}(\mathbb{F}_4/\mathbb{F}_2)$, with small group identifier $\langle 1296, 2891 \rangle$, which contains H with index 2. Up to conjugacy there is

[3]Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, MA 02139, USA; email: drew@math.mit.edu, URL: https://math.mit.edu/ drew

[4]In this appendix isomorphism classes of groups of order $n < 2048$ are identified by the label $\langle n, i \rangle$ assigned to them by the Small Groups Library [BEO01] used in GAP, Sage, and Magma.

a unique such subgroup G; it is the normalizer of H in $\mathrm{Sp}_6(\mathbb{F}_2)$. Let $I := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $z_3 := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $s_2 := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and define

$$A := \begin{pmatrix} z_3 & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & z_3 \end{pmatrix}, \qquad B := \begin{pmatrix} 0 & 0 & z_3^2 \\ 0 & z_3^2 & z_3^2 \\ z_3^2 & z_3^2 & z_3 \end{pmatrix}, \qquad S_2 := \begin{pmatrix} s_2 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_2 \end{pmatrix}.$$

Then we can take $H = \langle A, B \rangle$ and $G = \langle A, B, S_2 \rangle$.

For each prime $p > 3$ of good reduction for C the representation $\bar{\rho}_2$ maps the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to a conjugacy class of $\mathrm{Sp}_6(\mathbb{F}_2)$ whose characteristic polynomial is the reduction of the characteristic polynomial $\chi_p \in \mathbb{Z}[T]$ of the Frobenius endomorphism π of $J_p := \mathrm{Jac}(C_p)$, equivalently, the characteristic polynomial of the endomorphism of $J_p[2] \simeq \mathbb{F}_2^6$ induced by π. The polynomials $\chi_p(T)$ and $L_p(T)$ are reciprocal, meaning that $L_p(T) = T^6 \chi_p(T^{-1})$, as are their reductions to $\mathbb{F}_2[T]$. The image of Frob_p under $\bar{\rho}_2$ lies H when p splits in $\mathbb{Q}(\zeta_3)$, and in the complement $G - H$ when p is inert in $\mathbb{Q}(\zeta_3)$, equivalently, when $p \equiv 2 \pmod 3$.

Thus to compute the reduction $\bar{L}_p \in \mathbb{F}_2[T]$ for $p \equiv 2 \pmod 3$, it suffices to determine the characteristic polynomial of $\bar{\rho}_2(\mathrm{Frob}_p) \in G - H$, for which there are only two possibilities:

$$T^6 + T^4 + T^2 + 1 \qquad \text{or} \qquad T^6 + 1.$$

The first occurs whenever $\bar{\rho}_2(\mathrm{Frob}_p)$ has order 2 or 8; the second occurs when $\bar{\rho}_2(\mathrm{Frob}_p)$ has order 6. It is an easy computation in [Sage] to verify this fact, and that every element of $G - H$ has order 2, 6, or 8.

The fixed field of the kernel of $\bar{\rho}_2$ is the 2-torsion field $\mathbb{Q}(J[2])$, and we have an isomorphism $\mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q}) \simeq \mathrm{Im}\,\bar{\rho}_2$. It follows that to compute $\bar{L}_p \in \mathbb{F}_2[T]$ it suffices to determine the order of the restriction of Frob_p to $\mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$. The group G contains a unique normal subgroup Z of order 3 generated by the matrix $Z_3 := \mathrm{diag}(z_3, z_3, z_3)$ which gives the action of $\zeta_3 \in \mathrm{End}(J_{\mathbb{Q}(\zeta_3)})$ on $J[2]$. The quotient G/Z is isomorphic to the general affine group $\mathrm{AGL}(3, 2)$, with small group identifier $\langle 432, 734 \rangle$; the projection $G \to G/Z$ does not change the order of elements of $G - H$.

The group $G/Z \simeq \mathrm{AGL}(3, 2)$ has a natural permutation representation of degree 9 corresponding to the transitive group with LMFDB label 9T26 [LMFDB]. This permutation representation can be realized via the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ζ_3-orbits of the 27 affine bitangents of a generic Picard curve.

As shown in [BTW05, §2.2], each point of order 2 in $J_p(\mathbb{F}_p)$ corresponds to the class of an ideal of the form $\langle s, u+y \rangle$ in the ring $\mathbb{F}_p[x, y]/(y^3 - f(x))$, with $s, u \in \mathbb{F}_p[x]$ satisfying $\deg u < \deg s \leq 3$, with s monic and $s^2 = u^3 + f$. Those with $\deg s = 2$ correspond to divisors of the form $P_1 + P_2 - 2\infty$ arising from the 27 bitangents that intersect the curve at the affine points P_1, P_2, where $s(x) = (x - x(P_1))(x - x(P_2))$ and the linear polynomial u is determined by $u(x(P_i)) = y(P_i)$. If we assume $f(x) = x^4 + f_2 x^2 + f_1 x + f_0$ and let $s(x) = x^2 + s_1 x + s_0$ and $u(x) = u_1 x + u_0$, equating coefficients on both sides of the equation $s^2 = u^3 + f$ yields the system

$$2s_1 = u_1^3, \quad 2s_0 = f_2 + 3u_0 u_1^2 - s_1^2, \quad 2s_0 s_1 = f_1 + 3u_0^2 u_1, \quad s_0^2 = f_0 + u_0^3.$$

A Groebner basis calculation over $\mathbb{Q}(f_0, f_1, f_2)$ shows that s_1 must be a root of

$$\psi_f(x) := x^9 + 24f_2 x^7 - 168f_1 x^6 + (1080f_0 - 78f_2^2)x^5 + 336f_1 f_2 x^4$$
$$+ (1728f_0 f_2 - 636f_1^2 + 80f_2^3)x^3 + (-864f_0 f_1 - 168f_1 f_2^2)x^2$$
$$+ (-432f_0^2 + 216f_0 f_2^2 - 120f_1^2 f_2 - 27f_2^4)x - 8f_1^3,$$

and s_0 can be written as a polynomial in s_1 whose coefficients are rational functions of f_0, f_1, f_2. Each of the 9 possibilities for (s_0, s_1) gives rise to 3 possibilities for (u_0, u_1) that differ only by a cube root of unity and comprise a single ζ_3-orbit. The 27 possible values of u_1 are the roots of $\psi_f(x^3/2)$, each of which determines rational values for u_0, s_0, s_1. The discriminant of ψ_f has the form $-2^{24}3^{27}D_f^2$ with $D_f \in \mathbb{Z}[f_0, f_1, f_2]$, a fact we will use in the proof of the lemma below.

This calculation of $\psi_f(x)$ is valid over any field k whose characteristic is not 2 or 3, and we can define ψ_f for any Picard curve $y^3 = f(x)$ over k by putting f in the form $x^4 + f_2 x^2 + f_1 x + f_0$ as follows: if $f = \sum f_i x^i \in k[x]$ with $f_4 \neq 1$ then replace f with $f_4^3 f(x/f_4)$ and if $f_4 = 1$ and $f_3 \neq 0$ replace f with $f(x - f_3/4)$.

Lemma. *Let $C \colon y^3 = f(x)$ be a Picard curve over k with $\mathrm{char}(k) \neq 2, 3$ and let $J := \mathrm{Jac}(C)$. Then $k(J[2])$ is the splitting field K of $\psi_f(x^3/2)$ over k, and when $k = \mathbb{F}_p$ with $p \equiv 2 \pmod 3$ this is also the splitting field K' of $\psi_f(x)$.*

Proof. The points in $J[2]$ corresponding to bitangents are defined over K, so $J(K)[2]$ has order at least 27 and must be 32 or 64, since $J[2] \simeq (\mathbb{Z}/2\mathbb{Z})^6$. The three cuberoots of unity in $\bar{k}$ lie in K (take ratios of appropriate roots of $\psi(x^3/2)$), so $\mathbb{Z}[\zeta_3] \subseteq \mathrm{End}(J_K)$. The endomorphism ζ_3 acts bijectively on the points of order 2 in $J(K)[2]$, with ζ_3-orbits of size 3. We cannot have $\#J(K)[2] = 32$ because 3 does not divide 31. Thus $\#J(K)[2] = 64$ and $K = k(J[2])$.

Now assume k is a finite field $\mathbb{F}_p$ with $p > 3$ and $p \equiv 2 \pmod 3$. The discriminant $-2^{24}3^{27}D_f^2$ of ψ_f is a square in its splitting field K', thus $\mathbb{F}_p \subsetneq \mathbb{F}_p(\zeta_3) \subseteq K'$. The action of the Frobenius endomorphism π on $J[2]$ is given by a matrix M in the group $G := \langle A, B, S_2 \rangle \subseteq \mathrm{Sp}_6(\mathbb{F}_2)$ defined above that does not lie in the index 2 subgroup $H := \langle A, B \rangle$. For any such M, its order n is unchanged in the quotient G/Z_3 which gives the action of π on the ζ_3-orbits of $J[2]$. This action is determined by (and has the same order as) the action of π on the ζ_3-orbits of the points in $J[2]$ arising from bitangents of C, which coincides with the action of the p-power Frobenius automorphism on the roots of $\psi_f(x)$. The p-power Frobenius automorphisms of $\mathbb{F}_p(J[2])$ and K' thus have the same order n, so $\mathbb{F}_p(J[2]) = K'$. $\square$

Corollary. *Let $y^3 = f(x)$ be a Picard curve over $\mathbb{F}_p$ with $p \neq 2, p \equiv 2 \pmod 3$. Let $\bar{L}_p \in \mathbb{F}_2[T]$ be the reduction of its L-polynomial modulo 2. Then*

$$\bar{L}_p(T) = \begin{cases} T^6 + T^4 + T^2 + 1 & \text{if } \psi_f(x) \text{ has an } \mathbb{F}_p\text{-rational root,} \\ T^6 + 1 & \text{if } \psi_f(x) \text{ has no } \mathbb{F}_p\text{-rational roots.} \end{cases}$$

These cases can be distinguished in $O((\log p)^2 \log \log p)$ time by computing the degree of $\gcd(x^p - x, \psi_f(x))$.

Proof. Let $J := \mathrm{Jac}(C)$. Then $\bar{L}_p(T)$ is reciprocal to the characteristic polynomial of the Frobenius endomorphism π as an element of $\mathrm{End}(J[2])$, corresponding to a matrix M in the group $G := \langle A, B, S_2 \rangle \subseteq \mathrm{Sp}_6(\mathbb{F}_2)$ defined above that does not lie in the index two subgroup $H := \langle A, B \rangle$. As noted above, the two possibilities for $\bar{L}_p(T)$ are those listed in the statement of the corollary; the first occurs when M

has order 2 or 8, while the second occurs when M has order 6. The order of M is equal to the order of $\mathrm{Gal}(\mathbb{F}_p(J[2])/\mathbb{F}_p) = \mathrm{Gal}(K'/\mathbb{F}_p)$, where K' is the splitting field of $\psi_f(x)$ over $\mathbb{F}_p$. The Galois group of $\psi_f(x)$ over $\mathbb{F}_p$ is a cyclic subgroup of the transitive group `9T26` whose generator σ does not lie in the unique index 2 subgroup (we note that this is true even if $\psi_f(X)$ is not squarefree). The cycle structure of the degree 9 permutation σ must be one of $2^3 1^3$, $8^1 1^1$, or $6^1 3^1$, the last of which has order 6 and occurs if and only if $\psi_f(x)$ has no $\mathbb{F}_p$-rational roots.

As is well known, the roots of $\gcd(x^p - x, \psi_f(x))$ are the distinct $\mathbb{F}_p$-rational roots of $\psi_f(x)$; the degree of this polynomial is nonzero if and only if $\psi_f(x)$ has an $\mathbb{F}_p$-rational root. To efficiently compute $\gcd(x^p - x, \psi_f(x))$ one computes x^p in the ring $\mathbb{F}_p[x]/(\psi_f(x))$ via binary exponentiation to obtain a polynomial $g \in \mathbb{F}_p[x]$ of degree less than $\deg \psi_f = 9$ and then computes $\gcd(g(x) - x, \psi_f(x))$. This involves $O(\log p)$ ring operations in $\mathbb{F}_p[x]/(\psi_f(x))$, each of which can be computed using $O(1)$ ring operations and a Euclidean division in $\mathbb{F}_p[x]$, followed by a GCD computation on polynomials of degree $O(1)$, which requires $O(1)$ ring operations and Euclidean divisions in $\mathbb{F}_p[x]$ using the standard Euclidean algorithm.

Each Euclidean division in $\mathbb{F}_p[x]$ can be accomplished using $O(1)$ ring operations in $\mathbb{F}_p[x]$ via Newton iteration [GG13, Thm. 9.6], and each ring operation in $\mathbb{F}_p[x]$ involving polynomials of degree $O(1)$ can be achieved using $O(1)$ ring operations in $\mathbb{Z}$ via Kronecker substitution and Euclidean division in $\mathbb{Z}$. The entire computation of $\gcd(x^p - x, \psi_f(x))$, including the cost of deriving $\psi_f(x)$ from $f(x)$, reduces to $O(\log p)$ ring operations on integers with $n = O(\log p)$ bits. Applying the $O(n \log n)$ bound for integer multiplication [HvdH21] completes the proof. $\square$

ACKNOWLEDGMENTS

REFERENCES

[ABCMT19]   Vishal Arul, Alex J. Best, Edgar Costa, Richard Magner, and Nicholas Triantafil-lou, *Computing zeta functions of cyclic covers in large characteristic*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 37–53. MR3952003

[Abe18]   S. Abelard, *Counting points on hyperelliptic curves in large characteristic: algorithms and complexity*, PhD diss., Université de Lorraine, France, 2018.

[AH19]   Jeffrey D. Achter and Everett W. Howe, *Hasse-Witt and Cartier-Manin matrices: a warning and a request*, Arithmetic geometry: computation and applications, Contemp. Math., vol. 722, Amer. Math. Soc., Providence, RI, [2019] ©2019, pp. 1–18, DOI 10.1090/conm/722/14534. MR3896846

[AP20]   S. Asif, D. Pentland, *Computing Picard*, Github repository containing Sage code, https://github.com/sualehasif/computingPicard.

[Aru21]   Vishal Arul, *Division by $1 - \zeta$ on superelliptic curves and Jacobians*, Int. Math. Res. Not. IMRN **4** (2021), 3143–3185, DOI 10.1093/imrn/rnaa075. MR4218349

[BEO01]   Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644, DOI 10.1142/S0218196702001115. MR1935567

[BTW05]   Mark Bauer, Edlyn Teske, and Annegret Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), no. 252, 1983–2005, DOI 10.1090/S0025-5718-05-01758-8. MR2164107

[CDF20]   E. Costa, R. Donepudi, R. Fernando, V. Karemaker, C. Springer, and M. West, *Restrictions on Weil polynomials of Jacobians of hyperelliptic curves*, to appear in Arithmetic geometry, number theory, and computation, Simons Symp., `arXiv:2002.02067v2`, 2020.

[CFADLNV05] Christophe Doche, *Finite field arithmetic*, Handbook of elliptic and hyperelliptic curve cryptography, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. 201–237. MR2162727

[FKRS12]   Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), no. 5, 1390–1442, DOI 10.1112/S0010437X12000279. MR2982436

[FKS21]   Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland, *Sato–Tate groups of abelian threefolds: A preview of the classification*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 770, Amer. Math. Soc., Providence, RI, 2021, pp. 103–129, DOI 10.1090/conm/770/15432. MR4280389

[Fit20]   F. Fité, *Ordinary primes for some varieties with extra endomorphisms*, `arXiv:2005.10185v1`, 2020.

[FO04]   Stéphane Flon and Roger Oyono, *Fast arithmetic on Jacobians of Picard curves*, Public key cryptography—PKC 2004, Lecture Notes in Comput. Sci., vol. 2947, Springer, Berlin, 2004, pp. 55–68, DOI 10.1007/978-3-540-24632-9_5. MR2095638

[GG13]   Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, 3rd ed., Cambridge University Press, Cambridge, 2013, DOI 10.1017/CBO9781139856065. MR3087522

[Har14]   David Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. (2) **179** (2014), no. 2, 783–803, DOI 10.4007/annals.2014.179.2.7. MR3152945

[Har15]   David Harvey, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 6, 1379–1401, DOI 10.1112/plms/pdv056. MR3447797

[HvdH21]   David Harvey and Joris van der Hoeven, *Integer multiplication in time $O(n \log n)$*, Ann. of Math. (2) **193** (2021), no. 2, 563–617, DOI 10.4007/annals.2021.193.2.4. MR4224716

[HMS16]   David Harvey, Maike Massierer, and Andrew V. Sutherland, *Computing L-series of geometrically hyperelliptic curves of genus three*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 220–234, DOI 10.1112/S1461157016000383. MR3540957

[HS14]   David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 257–273, DOI 10.1112/S1461157014000187. MR3240808

[HS16]   David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147, DOI 10.1090/conm/663/13352. MR3502941

[Kat73]   N. M. Katz, *Une formule de congruence pour la fonction ζ*. In Groupes de monodromie en géométrie algébrique. II, Lecture Notes in Mathematics, Vol. **340**, pages 401–438. Springer-Verlag, Berlin–New York, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), dirigé par P. Deligne et N. Katz.

[KM74]   Nicholas M. Katz and William Messing, *Some consequences of the Riemann hypothesis for varieties over finite fields*, Invent. Math. **23** (1974), 73–77, DOI 10.1007/BF01405203. MR332791

[KS08]   Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 312–326, DOI 10.1007/978-3-540-79456-1_21. MR2467855

[KS09]   Kiran S. Kedlaya and Andrew V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*, Arithmetic, geometry, cryptography and coding theory,

Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, pp. 119–162, DOI 10.1090/conm/487/09529. MR2555991

[LMFDB]   The LMFDB Collaboration, *The L-functions and modular forms database*, 2021, available at `http://www.lmfdb.org`.

[Mac19]   E. MacNeil, $C_{3,4}$ *curves*, Github repository containing Sage code, available at `https://github.com/emmacneil/c34-curves`.

[MJS20]   E. MacNeil, M. Jacobson, and R. Scheidler, *Divisor class group arithmetic on* $C_{3,4}$ *curves*. Master's thesis, University of Calgary, Canada, 2019, available at `https://prism.ucalgary.ca/handle/1880/111659`.

[PARIGP] H. Cohen et al., *PARI/GP mathematics software, version 2.11.4*, available at `https://pari.math.u-bordeaux.fr`.

[Pil90]   J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763, DOI 10.2307/2008445. MR1035941

[Rib76]   Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804, DOI 10.2307/2373815. MR457455

[Sage]   W. A. Stein et al., *Sage mathematics software, version 6.3*, available at http://www.sagemath.org.

[Saw16]   William F. Sawin, *Ordinary primes for Abelian surfaces* (English, with English and French summaries), C. R. Math. Acad. Sci. Paris **354** (2016), no. 6, 566–568, DOI 10.1016/j.crma.2016.01.025. MR3494322

[Sch98]   Edward F. Schaefer, *Erratum: "Computing a Selmer group of a Jacobian using functions on the curve" [Math. Ann.* **310** *(1998), no. 3, 447–471; MR1612262]*, Math. Ann. **339** (2007), no. 1, 1, DOI 10.1007/s00208-007-0091-5. MR2317759

[Sch85]   René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494, DOI 10.2307/2007968. MR777280

[Ser58]   Jean-Pierre Serre, *Sur la topologie des variétés algébriques en caractéristique p* (French), Symposium internacional de topología algebraica International symposium on algebraic topology, Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958, pp. 24–53. MR0098097

[Ser12]   Jean-Pierre Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012. MR2920749

[Sut11]   Andrew V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*, Math. Comp. **80** (2011), no. 273, 477–500, DOI 10.1090/S0025-5718-10-02356-2. MR2728991

[Sut20]   A. V. Sutherland, *Counting points on superelliptic curves in average polynomial time*, Fourteenth Algorithmic Number Theory Symposium (ANTS XIV), Open Book Ser. **4** (2020), 403–422.

[Upt09]   M. G. Upton, *Galois representations attached to Picard curves*, J. Algebra **322** (2009), no. 4, 1038–1059, DOI 10.1016/j.jalgebra.2009.04.021. MR2537671

[Zar18]   Yuri G. Zarhin, *Endomorphism algebras of abelian varieties with special reference to superelliptic Jacobians*, Geometry, algebra, number theory, and their information technology applications, Springer Proc. Math. Stat., vol. 251, Springer, Cham, 2018, pp. 477–528, DOI 10.1007/978-3-319-97379-1_22. MR3880401

Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, Massachusetts 02139

Email address: sualeh@mit.edu

URL: https://sualehasif.me/

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, Massachusetts 02139

Email address: ffite@mit.edu

URL: https://www-math.mit.edu/~ffite/

Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, Massachusetts 02139

Email address: dylanp@mit.edu