hexagon:2611.00231v1

RATIONAL POINTS ON THE NON-SPLIT CARTAN MODULAR CURVE OF LEVEL 121

SANTIAGO ARANGO-PIÑEROS, FILIP NAJMAN, AND DAVID ZUREICK-BROWN

Abstract. We show that the modular curve $X_{\mathrm{ns}}^+(121)$, attached to the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/121\mathbb{Z})$, has exactly 7 rational points, all of them CM points. Together with the work of Rouse, Sutherland and Zureick-Brown, this completes the classification of the possible 11-adic images of Galois of elliptic curves over $\mathbb{Q}$ without complex multiplication. We do not use a model of $X_{\mathrm{ns}}^+(121)$, which has genus 511. Instead we use the map $X_{\mathrm{ns}}^+(121) \to X_{\mathrm{ns}}^+(11)$, whose target is an elliptic curve of rank 1, a descent with the cusps of $X_{\mathrm{ns}}^+(11)$ and a Mordell-Weil sieve to reduce the problem to 7 hyperelliptic curves of genus 5 over a number field of degree 15. We deal with these curves by a version of Stoll's Selmer group Chabauty method for the isogeny $1-\zeta_{11}$ of their Jacobians.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication (CM) and let ℓ be a prime. Serre [14] proved that the image of the ℓ-adic Galois representation $\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is open, and that the mod ℓ representation $\overline{\rho}_{E,\ell}$ is surjective for all but finitely many ℓ. He asked whether the primes ℓ for which $\overline{\rho}_{E,\ell}$ is not surjective can be bounded independently of E, and it is expected that over $\mathbb{Q}$ the bound 37 suffices (see [18]). For $\ell > 37$, by the work of Mazur [8], Serre [14] and Bilu, Parent and Rebolledo [3], if $\overline{\rho}_{E,\ell}$ is not surjective, then its image is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so this question becomes the question whether the modular curves $X_{\mathrm{ns}}^+(\ell)$ have non-CM rational points.

Rouse, Sutherland and Zureick-Brown [10] determined, for every prime ℓ, the possible ℓ-adic images of non-CM elliptic curves over $\mathbb{Q}$, apart from the images contained in the normalizer of a non-split Cartan subgroup of level $\ell \geq 19$ and apart from the images corresponding to rational points on finitely many explicit modular curves, whose rational points they could not determine: the curves $X_{\mathrm{ns}}^+(N)$ for $N = 27, 25, 49, 121$, and two curves of level 49 and genus 9 (see [10, Theorem 1.6]). Balakrishnan, Betts, Hast, Jha and Müller [2] have since determined the rational points on $X_{\mathrm{ns}}^+(27)$, Furio and Lombardo [6] the rational points on $X_{\mathrm{ns}}^+(49)$, and Arango-Piñeros and Zureick-Brown [1] showed that the two curves of level 49 and genus 9 have no non-CM rational points. The curve $X_{\mathrm{ns}}^+(121)$ has genus 511, and Rouse, Sutherland and Zureick-Brown did not compute a model of it. Using the map $\varphi : X_{\mathrm{ns}}^+(121) \to X_{\mathrm{ns}}^+(11)$ to an elliptic curve of rank 1, they showed with a Mordell-Weil sieve that a non-CM rational point on $X_{\mathrm{ns}}^+(121)$ would map to a multiple

2020 *Mathematics Subject Classification.* 11G05, 11G18, 14G05, 11F80.

Key words and phrases. modular curves, non-split Cartan subgroups, Galois representations, Selmer groups, Chabauty method.

F.N. was supported by the Croatian Science Foundation under the project no. IP-2022-10-5008, by the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027, and by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026, via an institutional grant of the University of Zagreb Faculty of Science, IK IA 1.1.3, Impact4Math.

kP of a generator P with $|k| \geq \operatorname{lcm}(1, 2, \ldots, 233)$, and hence its j-invariant would have height roughly $10^{7.92 \cdot 10^{202}}$ (see [10, Section 9.2]).

In this paper we determine the rational points on $X_{\mathrm{ns}}^+(121)$. Our main result is the following theorem.

Theorem 1.1. *The modular curve $X_{\mathrm{ns}}^+(121)$ has exactly 7 rational points. All of them are CM points, one for each of the discriminants*

$$D \in \{-3, -4, -12, -16, -27, -67, -163\}.$$

Note that these are all the discriminants of imaginary quadratic orders of class number 1 in which 11 is inert, so the rational points on $X_{\mathrm{ns}}^+(121)$ are the ones that the theory of complex multiplication predicts. We obtain the following corollary.

Corollary 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $\rho_{E,121}(G_{\mathbb{Q}})$ is not contained in a conjugate of the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/121\mathbb{Z})$. Hence $\rho_{E,11^\infty}(G_{\mathbb{Q}})$ is one of the groups described in* [10, Theorem 1.6 (i) and (ii)].

Proof. If $\rho_{E,121}(G_{\mathbb{Q}})$ were contained in such a group, then $j(E)$ would be the j-invariant of a non-CM rational point on $X_{\mathrm{ns}}^+(121)$, contradicting Theorem 1.1. The second statement now follows from [10, Theorem 1.6], as for $\ell = 11$ we have just excluded case (iii) of that theorem, and case (iv) occurs only for $\ell = 7$. □

Thus the 11-adic images of Galois of non-CM elliptic curves over $\mathbb{Q}$ are now completely determined. Of the curves listed in [10, Theorem 1.6], this leaves only $X_{\mathrm{ns}}^+(25)$. While writing this paper, we became aware that Eray Karabıyık has determined the rational points on $X_{\mathrm{ns}}^+(25)$ (private communication).

We now describe our methods. We never use a model of $X_{\mathrm{ns}}^+(121)$. The only information about $X_{\mathrm{ns}}^+(121)$ that we use is the moduli interpretation of the map $\varphi\colon X_{\mathrm{ns}}^+(121) \to X_{\mathrm{ns}}^+(11)$ of degree 121, at the cusps and at the CM points. The curve $X_{\mathrm{ns}}^+(11)$ is the elliptic curve

$$E\colon y^2 + y = x^3 - x^2 - 7x + 10$$

of rank 1, with $E(\mathbb{Q}) = \mathbb{Z}G$, where $G = (4, 5)$. Its 5 cusps are defined over $K = \mathbb{Q}(\zeta_{11})^+$, the maximal real subfield of $\mathbb{Q}(\zeta_{11})$, and they are points of order 11 on E. The proof has three steps.

The first step is a descent with the cusps. If $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$, then for every prime $\mathfrak{q}$ of K not above 11 and every cusp c of $X_{\mathrm{ns}}^+(11)$, the point $\varphi(\xi) \in E(\mathbb{Q})$ is congruent to c modulo $\mathfrak{q}^i$ only if it is congruent to c modulo $\mathfrak{q}^{11\lceil i/11 \rceil}$, i.e. the intersection number of $\varphi(\xi)$ and c at $\mathfrak{q}$ is divisible by 11 (Lemmas 4.2 and 4.3). This is the analogue for $X_{\mathrm{ns}}^+(121)$ of the condition, used by Schoof and Tzanakis [13] to determine the points on $X_{\mathrm{ns}}^+(11)$ with integral j-invariant, that $\varphi(\xi)$ does not meet the cusps at all. It follows that certain functions on E whose divisors are supported on the cusps and the origin take values in the finite group $K(S, 11)$, where S consists of the prime of K above 11. A Mordell-Weil sieve with 6 primes then shows that $\varphi(\xi) = nG$ with $n \equiv n_0 \pmod{4356}$ for some $n_0 \in \{-2, \ldots, 4\}$, and determines the values of these functions modulo 11-th powers (Proposition 4.7). The 7 values of n_0 correspond to the 7 CM points, and since 121 divides 4356, it follows that $n - n_0$ is divisible by 121.

The second step reduces the problem to curves of genus 5 (Section 5). The values from the first step show that $x(nG - 3s) = \alpha + \delta_{n_0} w^{11}$ with $w \in K$, where $s \in E(K)$ is a cusp and $\alpha, \delta_{n_0} \in K$ are explicit. Combined with a 2-descent on E over a cubic extension L of K, this gives a point on one of 7 hyperelliptic curves $\eta Y^2 = X^{11} + b^2$ of genus 5 over L, which is a number field of degree 15. The CM point gives the point with $w = 1$.

The third step deals with these curves. Over $F = L(\zeta_{11})$ their Jacobians J have the automorphism σ induced by $X \mapsto \zeta_{11} X$, and $\lambda = 1 - \sigma$ is an isogeny of degree 11. We use the idea of Stoll's *Selmer group Chabauty* [16, Theorem 2.1 and Remark 2.2] for the

isogeny λ. Since 121 divides $n-n_0$, the point $[P-P_0] \in J(F)$, where P is the point coming from ξ and P_0 the point coming from the CM point, is deep in the kernel of reduction at a prime v above 11. As long as a point is deep enough, its image under the local λ-Kummer map is 0, and since the localization at v of the λ-Selmer group turns out to be injective, the point is divisible by λ in $J(F)$. Repeating this, we arrive at a point of the kernel of reduction whose leading term we know. Its image under the local Kummer map is not in the image of the Selmer group, which is a contradiction (Propositions 8.3 and 9.2).

The method works because the curves $Y^2 = X^{11} + b^2$ have cuspidal reduction $Y^2 = (X+\bar{b}^2)^{11}$ at the primes above 11. As a consequence, the formal groups of their Jacobians at these primes are isomorphic to $\widehat{\mathbb{G}}_a^5$ via the formal logarithm (Lemma 6.1), and λ acts diagonally in the logarithmic coordinates, so the repeated divisions by λ can be followed explicitly. Note that our approach needs neither generators of the Mordell-Weil groups of the Jacobians (which have rank 5 over L for 3 of the 7 curves, see Remark 5.3) nor a bound on the height of the points. We do not assume the Generalized Riemann Hypothesis (GRH). It is used only to find generators of groups of S-units, which are then shown to be correct unconditionally.

We fix our notation in Section 2 and prove Theorem 1.1 in Section 10. The computations are described in Section 11.

All the code used in the paper can be found at

https://github.com/F-Najman/Xns-121-

Data availability and reproducibility. The repository contains the code, the logs and the certificates of all the computations in this paper, and a script that reruns all of them (in about 4 minutes). This paper refers to the revision `c12c8c3` of the repository, and the links in the paper point to this revision. The `README` file there lists, statement by statement, which script establishes each claim and which log it produced. In the digital form of this article, the words reporting a computation, such as "we compute", are hyperlinks to the script that carries it out.

AI disclosure and comments. The mathematical content of this paper was produced by AI models. Anthropic's Claude Opus 5.5, OpenAI's GPT-6.1 Sol and GPT-6 Astra produced almost all of the mathematics of the first versions of the proofs and carried out the computations. Claude Opus 5.5 also reviewed these proofs, reran all the computations, independently reimplemented the sieve, the Selmer group computations for the even classes, the determination of the rational points above the CM points and the computation of the genus, checked the references, wrote the manuscript and organized the code repository. We have not yet fully checked the proofs.

2. Notation and conventions

Throughout the paper ζ_{11} denotes a primitive 11-th root of unity, and $\pi = 1-\zeta_{11}$. For a number field k, a finite set S of primes of k and a prime p we write

$$k(S,p) = \{a \in k^\times/k^{\times p} : v_{\mathfrak{q}}(a) \equiv 0 \pmod{p} \text{ for all primes } \mathfrak{q} \notin S\}.$$

This is a finite dimensional $\mathbb{F}_p$-vector space, which we write additively. If k contains a primitive p-th root of unity and $\mathrm{Cl}(k)[p] = 0$, then $\dim_{\mathbb{F}_p} k(S,p) = r_1 + r_2 + \#S$, where (r_1, r_2) is the signature of k. For a finite extension l of $\mathbb{Q}_p$ we denote by v or v_l the valuation of l normalized by $v(l^\times) = \mathbb{Z}$, and by $\mathcal{O}_l$ its ring of integers.

Let $\varepsilon = 2$, which is not a square modulo 11. The non-split Cartan subgroup $C_{\mathrm{ns}}(121)$ of $\mathrm{GL}_2(\mathbb{Z}/121\mathbb{Z})$ is the group of invertible matrices of the form

$$\begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}, \quad a, b \in \mathbb{Z}/121\mathbb{Z},$$

which is the unit group of the subring $\mathbb{Z}/121\mathbb{Z}[\sqrt{\varepsilon}] \simeq \mathbb{Z}_{11}[\sqrt{\varepsilon}]/(121)$ of the matrix ring, and its normalizer $N_{\mathrm{ns}}(121)$ is generated by $C_{\mathrm{ns}}(121)$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The modular curve $X_{\mathrm{ns}}^+(121)$ is the modular curve attached to $N_{\mathrm{ns}}(121)$, and $X_{\mathrm{ns}}^+(11)$ is defined in the same way. Since $-I \in N_{\mathrm{ns}}(121)$ and $\det N_{\mathrm{ns}}(121) = (\mathbb{Z}/121\mathbb{Z})^\times$, for an elliptic curve $E'/\mathbb{Q}$ with $j(E') \neq 0, 1728$ the j-invariant $j(E')$ is the image of a rational point on $X_{\mathrm{ns}}^+(121)$ if and only if $\rho_{E',121}(G_{\mathbb{Q}})$ is contained in a conjugate of $N_{\mathrm{ns}}(121)$ (see [18, Proposition 3.3]). More generally, the points of $X_{\mathrm{ns}}^+(121)$ above $j(E')$ (for any $j(E')$) correspond to the subrings of $\mathrm{End}(E'[121])$ that are conjugate to $\mathbb{Z}/121\mathbb{Z}[\sqrt{\varepsilon}]$, modulo the action of $\mathrm{Aut}(E')$, and $G_{\mathbb{Q}}$ acts on them through $\rho_{E',121}$ (see [10, Section 2.3]).

We will denote by $\varphi\colon X_{\mathrm{ns}}^+(121) \to X_{\mathrm{ns}}^+(11)$ the natural map, which is of degree 121.

For computations we use Magma [5].

3. The curve $X_{\mathrm{ns}}^+(11)$ and the CM points

Ligozat [7] showed (see [13, Section 4]) that $X_{\mathrm{ns}}^+(11)$ is isomorphic to the elliptic curve

$$E\colon y^2 + y = x^3 - x^2 - 7x + 10,$$

which is the curve 121b1 in Cremona's tables and 121.b2 in the LMFDB [17]. We compute that $E(\mathbb{Q}) = \mathbb{Z}G$, where $G = (4, 5)$ is a point of infinite order. We use the j-map $j\colon E \to \mathbb{P}^1$ of degree 55 from the LMFDB (the modular curve with label 11.55.1.b.1). It can be written as

$$j = \frac{\mathcal{A}(x) + \mathcal{B}(x)y}{u^{11}}, \quad u = (x-4)(y-5) - 11,$$

where $\mathcal{A}, \mathcal{B} \in \mathbb{Z}[x]$ have degrees 27 and 26 and are given in `code/compact_jmap.m`. Note that after the substitution $x \mapsto x + 4$, $y \mapsto y + 5$ the function u becomes the function $xy - 11$ which appears in [13, Theorem 4.1].

Let $K = \mathbb{Q}(z)$, where $z^5 + z^4 - 4z^3 - 3z^2 + 3z + 1 = 0$. This is the field $\mathbb{Q}(\zeta_{11})^+$, and the unique prime $\mathfrak{p}$ of K above 11 is generated by $2 - z$. Put

$$s = \left(-z^4 - z^3 + 2z^2 + 3z + 3,\ -2z^4 - 4z^3 + 6z^2 + 11z + 1\right) \in E(K)$$

and let $R = \{1, 3, 4, 5, 9\}$ be the set of non-zero squares modulo 11.

Proposition 3.1. a) *The point s has order 11, the cusps of $E \simeq X_{\mathrm{ns}}^+(11)$ are the 5 points rs, $r \in R$, and the function j has a pole of order 11 at each cusp. The divisor of u is $\sum_{r\in R}(rs) - 5(O)$.*

b) *For every $r \in R$, the element $(\mathcal{A} + \mathcal{B}y)(rs) \in K$ is a unit at all the primes of K not above 11.*

c) *For $n \in \{-2, \dots, 4\}$ the point nG is the unique rational point of E above $j(nG)$, and $j(nG)$ is the j-invariant of the CM order of discriminant D given in Table 1.*

Proof. We compute a) and b), and we compute c) (see also `code/model.m`). □

Table 1. The points nG with $n \in \{-2, \dots, 4\}$ and the corresponding CM points.

n	nG	D	$j(nG)$
-2	$(2, -1)$	-27	$-2^{15} \cdot 3 \cdot 5^3$
-1	$(4, -6)$	-16	$2^3 \cdot 3^3 \cdot 11^3$
0	O	-12	$2^4 \cdot 3^3 \cdot 5^3$
1	$(4, 5)$	-67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
2	$(2, 0)$	-4	$2^6 \cdot 3^3$
3	$(5/4, 7/8)$	-3	0
4	$(-2, 3)$	-163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Remark 3.2. We compute, from the action of $\mathrm{SL}_2(\mathbb{Z})$ on the cosets of $N_{\mathrm{ns}}(121)$ in $\mathrm{GL}_2(\mathbb{Z}/121\mathbb{Z})$, that $\varphi\colon X_{\mathrm{ns}}^+(121) \to X_{\mathrm{ns}}^+(11)$ has degree 121 and that $X_{\mathrm{ns}}^+(121)$ has 55 cusps, 67 elliptic points of order 2, 1 elliptic point of order 3 and genus 511, in agreement with [10, Table 2].

Lemma 3.3. *Let $\mathcal{O}$ be an imaginary quadratic order in which 11 is inert, let $E_0/\mathbb{Q}$ be an elliptic curve with CM by $\mathcal{O}$, and let $A_0 \subset \mathrm{End}(E_0[121])$ be the image of $\mathcal{O}$, and put $\overline{A}_0 = A_0/11A_0 \simeq \mathbb{F}_{121}$. Let ξ_0 be the point of $X_{\mathrm{ns}}^+(121)$ given by A_0. Let $g \in \mathbb{F}_{121}^\times$ with $g^{5\#\mathcal{O}^\times} \neq 1$, and suppose that an element of $G_{\mathbb{Q}}$ acts on $E_0[121]$ through an element of $A_0^\times$ whose image in $\overline{A}_0$ is g. Then ξ_0 is the only point of $X_{\mathrm{ns}}^+(121)$ above $\varphi(\xi_0)$ which is fixed by this element.*

Proof. The points of $X_{\mathrm{ns}}^+(121)$ above $\varphi(\xi_0)$ correspond to the subrings $A \subset \mathrm{End}(E_0[121])$ conjugate to A_0 with $A \equiv A_0 \pmod{11}$, modulo the action of $\mathrm{Aut}(E_0) = \mathcal{O}^\times$. For $c \in \overline{A}_0$ write $\overline{c} = c^{11}$ for its conjugate. Then $M_2(\mathbb{F}_{11}) = \overline{A}_0 \oplus \overline{A}_0\iota$ for some ι with $\iota c \iota^{-1} = \overline{c}$ for $c \in \overline{A}_0$. Every such A is of the form $(1+11X)A_0(1+11X)^{-1}$, where X is a lift of an element of $\overline{A}_0\iota \simeq M_2(\mathbb{F}_{11})/\overline{A}_0$ (as the normalizer of A_0 surjects onto the normalizer of $\overline{A}_0$), and this element is uniquely determined by A, since $(1+11X)A_0(1+11X)^{-1} = A_0$ if and only if X commutes with $\overline{A}_0$ modulo 11. If $h \in A_0^\times$ has image $c \in \overline{A}_0$, then $h(1+11X)A_0(1+11X)^{-1}h^{-1}$ corresponds to cXc^{-1}, and for $X = y\iota$ with $y \in \overline{A}_0$ we have $cXc^{-1} = (c/\overline{c})X$.

It follows that a point corresponding to $X \neq 0$ is fixed by an element of $G_{\mathbb{Q}}$ acting through an element of $A_0^\times$ with image g only if $g/\overline{g} = u/\overline{u}$ for some $u \in \mathcal{O}^\times$. Since $\overline{u} = u^{11}$ and $\mathcal{O}^\times$ is cyclic of order $\#\mathcal{O}^\times \in \{2,4,6\}$, the elements $u/\overline{u} = u^{-10}$ form the group of $(\#\mathcal{O}^\times/2)$-th roots of unity, and $g/\overline{g} = g^{-10}$. Hence this happens only if $g^{5\#\mathcal{O}^\times} = 1$, which is not the case. □

Lemma 3.4. *Let $n_0 \in \{-2,\dots,4\}$. There is exactly one rational point on $X_{\mathrm{ns}}^+(121)$ above n_0G, and it is a CM point with discriminant D as in Table 1.*

Proof. Let $E_0/\mathbb{Q}$ be an elliptic curve with $j(E_0) = j(n_0G)$. It has CM by the order $\mathcal{O}$ of discriminant D, and 11 is inert in $\mathcal{O}$. The subring $A_0 = \mathcal{O}/121\mathcal{O}$ of $\mathrm{End}(E_0[121])$ is conjugate to $\mathbb{Z}/121\mathbb{Z}[\sqrt{\varepsilon}]$, and it is normalized by $\rho_{E_0,121}(G_{\mathbb{Q}})$, since $G_{\mathbb{Q}(\sqrt{D})}$ acts through $A_0^\times$ and complex conjugation acts on $\mathcal{O}$ as the non-trivial automorphism. Hence A_0 gives a rational point ξ_0 on $X_{\mathrm{ns}}^+(121)$ above $j(E_0)$. Its image in $X_{\mathrm{ns}}^+(11)$ is a rational point above $j(E_0)$, so it is n_0G by Proposition 3.1 c).

For each n_0 we find a prime p which splits in $\mathbb{Q}(\sqrt{D})$ such that the Frobenius element $g \in \mathbb{F}_{121}$ of p, a root of $x^2 - a_p(E_0)x + p$, satisfies $g^{5\#\mathcal{O}^\times} \neq 1$. The primes are $p = 7,5,7,5,7,17,41$ for $D = -3,-4,-12,-16,-27,-67,-163$, respectively (see `code/cm_lifts.m`). Note that this condition does not depend on the choice of E_0, as a twist changes g by an element of $\mathcal{O}^\times$. A Frobenius element at p acts on $E_0[121]$ through an element of $A_0^\times$ with image g in $\mathbb{F}_{121}$, so by Lemma 3.3 the point ξ_0 is the only rational point above n_0G. □

4. Descent with the cusps

Lemma 4.1. *Let $a \in \mathbb{Z}/121\mathbb{Z}$. If the matrix $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/121\mathbb{Z})$ to an element of $N_{\mathrm{ns}}(121)$, then $a = 0$.*

Proof. Let $U = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Suppose first that $11 \nmid a$. Then U reduces to an element of order 11 of a conjugate of $N_{\mathrm{ns}}(11)$, which is impossible as $\#N_{\mathrm{ns}}(11) = 240$. Suppose now that

$a = 11a'$ with $11 \nmid a'$. Then $U = I + 11M$ with $M = \begin{pmatrix} 0 & a' \\ 0 & 0 \end{pmatrix}$, which is non-zero and nilpotent modulo 11. Since $U \equiv I \pmod{11}$, and the elements of $N_{\mathrm{ns}}(121)$ not in $C_{\mathrm{ns}}(121)$ are not congruent to I modulo 11, a conjugate of U lies in the kernel $I + 11 \cdot \mathbb{F}_{11}[\sqrt{\varepsilon}]$ of the reduction $C_{\mathrm{ns}}(121) \to C_{\mathrm{ns}}(11)$. This is impossible, as $\mathbb{F}_{11}[\sqrt{\varepsilon}] \simeq \mathbb{F}_{121}$ contains no non-zero nilpotent elements. □

Lemma 4.2. *Let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$ be a non-cuspidal point and let $p \neq 11$ be a prime with $v_p(j(\xi)) < 0$. Then 121 divides $v_p(j(\xi))$.*

Proof. Let $E'/\mathbb{Q}$ be an elliptic curve with $j(E') = j(\xi)$. Since $v_p(j(E')) < 0$, we have $j(E') \neq 0, 1728$, so $\rho_{E',121}(G_{\mathbb{Q}})$ is contained in a conjugate of $N_{\mathrm{ns}}(121)$. Over $\mathbb{Q}_p$, the curve E' is a quadratic twist of a Tate curve with parameter q satisfying $v_p(q) = -v_p(j(\xi))$. As $p \neq 11$, inertia at p acts on the 121-torsion of the Tate curve through the matrices $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $a \in v_p(q)\mathbb{Z}/121\mathbb{Z}$, and all of these occur. Since the twist changes the action by ± 1, the image of inertia contains $\pm \begin{pmatrix} 1 & v_p(q) \\ 0 & 1 \end{pmatrix}$, and hence its square $\begin{pmatrix} 1 & 2v_p(q) \\ 0 & 1 \end{pmatrix}$. By Lemma 4.1, 121 divides $2v_p(q)$, and hence $v_p(q)$. □

We denote by $t = x/y$ the usual parameter of E at O. For a prime $\mathfrak{q}$ of K not above 11, the curve E has good reduction at $\mathfrak{q}$. For points $P, Q \in E(K)$ we denote by $(P \cdot Q)_{\mathfrak{q}}$ the intersection number of the sections P and Q on the smooth model of E over $\mathcal{O}_{K,\mathfrak{q}}$ (the largest integer i such that $P \equiv Q$ modulo $\mathfrak{q}^i$).

Lemma 4.3. *Let $\mathfrak{q}$ be a prime of K not above 11 and let $P \in E(K)$ be a point which is not a cusp. If P does not meet a cusp at $\mathfrak{q}$, then $v_{\mathfrak{q}}(j(P)) \geq 0$. If P meets the cusp rs at $\mathfrak{q}$ for some $r \in R$, then $v_{\mathfrak{q}}(j(P)) = -11(P \cdot rs)_{\mathfrak{q}}$.*

Proof. The functions x, y, u, $\mathcal{A}(x)$ and $\mathcal{B}(x)$ have integral Laurent expansions in t, and the leading coefficient of u is ± 1. Hence the divisor of u on the smooth model of E over $\mathcal{O}_{K,\mathfrak{q}}$ has no vertical component, and it is equal to $\sum_{r \in R}(rs) - 5(O)$ by Proposition 3.1 a). The cusps are distinct modulo $\mathfrak{q}$, since they differ by points of order 11. The expansion of $j = (\mathcal{A}(x) + \mathcal{B}(x)y)t^{55}/(ut^5)^{11}$ at O is integral, so $v_{\mathfrak{q}}(j(P)) \geq 0$ if $P \equiv O \pmod{\mathfrak{q}}$. Otherwise P is $\mathfrak{q}$-integral, $v_{\mathfrak{q}}(u(P)) = \sum_{r \in R}(P \cdot rs)_{\mathfrak{q}}$, and if P meets the cusp rs, then $(\mathcal{A} + \mathcal{B}y)(P) \equiv (\mathcal{A} + \mathcal{B}y)(rs) \pmod{\mathfrak{q}}$ is a $\mathfrak{q}$-unit by Proposition 3.1 b). The lemma follows. □

For $m \in \{1, 2, 3\}$ and $r \in R$ let $a_{m,r} \in \{1, \dots, 10\}$ be such that $a_{m,r} \equiv r^m \pmod{11}$. We have $\sum_{r \in R} a_{m,r} = 22$ and $\sum_{r \in R} a_{m,r} r \equiv \sum_{r \in R} r^{m+1} \equiv 0 \pmod{11}$, so the divisors

$$\sum_{r \in R} a_{m,r}(rs) - 22(O) \quad \text{and} \quad 11(s) - 11(O)$$

are principal. Let f_1, f_2, f_3 and f_T be the functions in $K(E)$ with these divisors, normalized by the condition that the leading coefficient of their expansions in t is 1. We will need the following well-known lemma.

Lemma 4.4. *Let k be a field of characteristic 0, E'/k an elliptic curve, t_0 a parameter of E' at O, $T_0 \in E'(k)$ a point of order m, and $f \in k(E')$ a function with divisor $m(T_0) - m(O)$ such that the leading coefficient of the expansion of f in t_0 is in $k^{\times m}$. Then the map $E'(k) \setminus \{O, T_0\} \to k^\times/k^{\times m}$, $P \mapsto f(P)k^{\times m}$, extends to a homomorphism $E'(k) \to k^\times/k^{\times m}$.*

Proof. Multiplying f by an m-th power, we may assume that the leading coefficient of f is 1. The divisor $[m]^*(T_0) - [m]^*(O)$ is defined over k and principal, so it is the divisor of some $g \in k(E')$, and $g^m = cf \circ [m]$ for some $c \in k^\times$. Since g has a simple pole at O

and $f \circ [m]$ has the leading coefficient m^{-m}, it follows that $c \in k^{\times m}$, so we may choose g such that $g^m = f \circ [m]$. Let $P \in E'(k) \setminus \{O, T_0\}$ and $Q \in E'(\bar{k})$ with $mQ = P$. Then $f(P) = g(Q)^m$, and for $\tau \in G_k$ we have

$$\frac{\tau(g(Q))}{g(Q)} = \frac{g(Q+Q_\tau)}{g(Q)} = e_m(Q_\tau, T_0), \quad \text{where } Q_\tau = \tau(Q) - Q \in E'[m]$$

and e_m is the Weil pairing (see [15, Section III.8]). Hence the image of $f(P)$ in $H^1(k, \boldsymbol{\mu}_m) \simeq k^\times/k^{\times m}$ is the image of the Kummer class of P under the map $H^1(k, E'[m]) \to H^1(k, \boldsymbol{\mu}_m)$ induced by the G_k-equivariant homomorphism $e_m(\cdot, T_0)$, and the lemma follows. □

Corollary 4.5. *Let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$ and $P = \varphi(\xi)$. Then $P \in E(\mathbb{Q})$, and if $P \neq O$, then $f_m(P) \in K(S, 11)$ for $m \in \{1, 2, 3\}$, where $S = \{\mathfrak{p}\}$.*

Proof. The cusps of $X_{\mathrm{ns}}^+(121)$ map to cusps of $X_{\mathrm{ns}}^+(11)$, which are not rational, so ξ is not a cusp. Let $\mathfrak{q}$ be a prime of K not above 11. By the normalization, the divisor of f_m on the smooth model of E over $\mathcal{O}_{K,\mathfrak{q}}$ has no vertical component, so

$$v_\mathfrak{q}(f_m(P)) = \sum_{r \in R} a_{m,r}(P \cdot rs)_\mathfrak{q} - 22(P \cdot O)_\mathfrak{q}.$$

If $(P \cdot rs)_\mathfrak{q} > 0$, then $v_\mathfrak{q}(j(P)) = -11(P \cdot rs)_\mathfrak{q}$ by Lemma 4.3, and as 11 is the only prime that ramifies in K, 121 divides $v_p(j(\xi)) = v_\mathfrak{q}(j(P))$ by Lemma 4.2, where p is the rational prime below $\mathfrak{q}$. It follows that 11 divides $(P \cdot rs)_\mathfrak{q}$, and $v_\mathfrak{q}(f_m(P)) \equiv 0 \pmod{11}$. □

For $P \in E(\mathbb{Q})$ with $f_m(P) \in K(S, 11)$ we denote by $\gamma_m(P) \in K(S, 11)$ the class of $f_m(P)$, and we put $\gamma_m(O) = 0$. The group $K(S, 11)$ has dimension 5, with basis $2 - z$ and the fundamental units of K.

Let $\mathfrak{l}$ be a prime of K not above 11 such that 11 divides $\#\mathbb{F}_\mathfrak{l}^\times$, where $\mathbb{F}_\mathfrak{l}$ is the residue field of $\mathfrak{l}$. Fixing a primitive 11-th root of unity in $\mathbb{F}_\mathfrak{l}$, the 11-th power residue symbol defines a homomorphism $\chi_\mathfrak{l} \colon \mathbb{F}_\mathfrak{l}^\times \to \mathbb{F}_{11}$, and since every element of $K(S, 11)$ has a representative which is a unit at $\mathfrak{l}$, also a linear map $\chi_\mathfrak{l} \colon K(S, 11) \to \mathbb{F}_{11}$.

Lemma 4.6. *Let $\mathfrak{l}$ be a prime of K not above 11 such that 11 divides $\#\mathbb{F}_\mathfrak{l}^\times$, let $m \in \{1, 2, 3\}$, and let $P \in E(\mathbb{Q})$ be such that $f_m(P) \in K(S, 11)$ or $P = O$. Denote by $\overline{P}$ the reduction of P modulo $\mathfrak{l}$.*

a) *If $\overline{P}$ is neither O nor the reduction of a cusp, then $\chi_\mathfrak{l}(\gamma_m(P)) = \chi_\mathfrak{l}(\overline{f}_m(\overline{P}))$, where $\overline{f}_m$ is the reduction of f_m modulo $\mathfrak{l}$.*
b) *If $\overline{P} = O$, then $\chi_\mathfrak{l}(\gamma_m(P)) = 0$.*

Proof. Part a) is clear, as $f_m(P)$ is a unit at $\mathfrak{l}$. For b) we may assume $P \neq O$. Then $t(P)$ has positive valuation at $\mathfrak{l}$, and since $f_m t^{22}$ is a power series in t with $\mathfrak{l}$-integral coefficients and constant term 1, we have $f_m(P) = t(P)^{-22} w$ with $w \equiv 1 \pmod{\mathfrak{l}}$. The class $\gamma_m(P)$ is represented by $w = f_m(P)(t(P)^2)^{11}$, and $\chi_\mathfrak{l}(w) = 0$. □

Proposition 4.7. *Let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$ and write $\varphi(\xi) = nG$. Then there exists $n_0 \in \{-2, \ldots, 4\}$ such that $n \equiv n_0 \pmod{4356}$ and $\gamma_m(nG) = \gamma_m(n_0 G)$ for $m \in \{1, 2, 3\}$.*

Proof. Let $\ell \in \{23, 53, 353, 3301, 12101, 15731\}$. All these primes split completely in K, except 53, which is inert, and 11 divides $\#\mathbb{F}_\mathfrak{l}^\times$ for every prime $\mathfrak{l}$ of K above ℓ. The orders of G modulo these 6 primes are 33, 12, 11, 33, 1089 and 726, respectively, and their least common multiple is $4356 = 2^2 \cdot 3^2 \cdot 11^2$. By Corollary 4.5 and Lemma 4.6, for each prime $\mathfrak{l}$ above ℓ and each m, either nG reduces modulo $\mathfrak{l}$ to a cusp, or $\chi_\mathfrak{l}(\gamma_m(nG))$ is a value which depends only on n modulo the order of G modulo ℓ, and which we can compute. For a fixed residue class of n modulo 4356, these conditions, for all the 26 primes $\mathfrak{l}$ above the 6 primes ℓ, form 3 systems of linear equations over $\mathbb{F}_{11}$ for the coordinates of $\gamma_1(nG), \gamma_2(nG), \gamma_3(nG)$ in our basis of $K(S, 11)$. We compute that for $n \not\equiv -2, \ldots, 4$

(mod 4356) at least one of these systems has no solution, and that for $n \equiv n_0 \pmod{4356}$ with $n_0 \in \{-2, \dots, 4\}$ each of the 3 systems has a unique solution, equal to the coordinates of $\gamma_m(n_0 G)$. □

Remark 4.8. Lemma 4.6 b) is essential here. If we do not use it, and impose no condition at the primes $\mathfrak{l}$ at which nG reduces to O, then the same 6 primes leave 10 residue classes modulo 4356, namely those of $-396, -2, -1, 0, 1, 2, 3, 4, 1782$ and 2178 (see `code/sieve_bruteforce.m`).

Put $\alpha = x(2s) = z^4 - z^3 - 3z^2 + 3z + 2$ and, for $n_0 \in \{-2, \dots, 4\}$,

$$\delta_{n_0} = x(n_0 G - 3s) - \alpha \in K^\times.$$

Corollary 4.9. *Let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$, $\varphi(\xi) = nG$, and let n_0 be as in Proposition 4.7. Then there is a $w \in K^\times$ such that*

$$x(nG - 3s) = \alpha + \delta_{n_0} w^{11}. \tag{4.1}$$

We have $w = 1$ if and only if $n = n_0$.

Proof. We compute that there is a function $h \in K(E)$, with divisor supported on the cusps and O, such that

$$\frac{x(P - 3s) - \alpha}{x(3s) - \alpha} = f_1^7 f_2^{10} f_3^6 f_T^3 h^{11}$$

as functions of $P \in E$, and that both sides take the value 1 at O. The left-hand side has divisor $(s) + (5s) - 2(3s)$. The function f_T satisfies the conditions of Lemma 4.4 with $m = 11$ and the parameter t, and since 11 divides $n - n_0$, the classes of $f_T(nG)$ and $f_T(n_0 G)$ in $K^\times / K^{\times 11}$ are equal (if $n_0 = 0$, the class of $f_T(nG)$ is trivial). Evaluating the identity at nG and at $n_0 G$ (and taking leading coefficients at O if one of them is O), and using Proposition 4.7, we obtain that $x(nG - 3s) - \alpha$ and $x(n_0 G - 3s) - \alpha = \delta_{n_0}$ have the same class modulo $K^{\times 11}$. Note that $x(nG - 3s) \neq \alpha$, as $nG - 3s \neq \pm 2s$.

Finally, $w = 1$ if and only if $nG - 3s = \pm(n_0 G - 3s)$. As $6s \notin E(\mathbb{Q})$, this happens only if $n = n_0$. □

5. The curves of genus 5

Let $\theta \in \overline{\mathbb{Q}}$ be a root of $x^3 - x^2 - 7x + 41/4$. Then $(\theta, -1/2)$ is a point of order 2 on E. Let $L = K(\theta)$. We compute that L is a number field of degree 15 with discriminant $-2^{10} \cdot 11^{13}$, that $4 - \theta$ is not a square in L, and that $\alpha - \theta = \beta^2$ for some $\beta \in L$. For $n_0 \in \{-2, \dots, 4\}$ put $\eta_{n_0} = 1$ if n_0 is even and $\eta_{n_0} = 4 - \theta$ if n_0 is odd. We compute that

$$x(n_0 G - 3s) - \theta = \eta_{n_0} \rho_{n_0}^2$$

for some $\rho_{n_0} \in L$, and we put

$$a = \delta_{n_0} / \beta^2 \in L, \quad b = a^5, \quad C_{n_0} \colon \eta_{n_0} Y^2 = X^{11} + b^2.$$

The curve C_{n_0} is a hyperelliptic curve of genus 5 over L. We suppress the dependence of a and b on n_0 from the notation.

Let $F = L(\zeta_{11})$ and $B = F(\sqrt{4 - \theta})$. We compute that F is a number field of degree 30 with discriminant $-2^{20} \cdot 11^{27}$, that it has a unique prime above 2 and 3 primes above 11, whose completions are all isomorphic to $\mathbb{Q}_{11}(\zeta_{11})$, and that the ideal generated by a in F is the square of the prime above 2. In particular, a and b are units at all the primes of F not above 2. The field B is a number field of degree 60 with discriminant $2^{60} \cdot 11^{56}$, and it has a unique prime above 2 and 3 primes above 11. At 2 of the 3 primes v of F above 11 we have $v(4 - \theta) = 5$, and B/F is ramified, and at the third one $v(4 - \theta) = 10$, and B/F is unramified. As B has only 3 primes above 11, it follows that $4 - \theta$ is not a square in F_v for any prime v of F above 11.

Let k be a field of characteristic 0 containing ζ_{11} and let $b \in k^\times$. We denote by C the curve $Y^2 = X^{11}+b^2$ over k, by J its Jacobian, by σ the automorphism $(X,Y) \mapsto (\zeta_{11}X, Y)$ of C, and we put $\lambda = 1-\sigma$. As $C/\langle\sigma\rangle \simeq \mathbb{P}^1$, we have $1+\sigma+\cdots+\sigma^{10} = 0$ on J, so $\mathbb{Z}[\sigma] \simeq \mathbb{Z}[\zeta_{11}]$ acts on J, and λ is an isogeny of degree 11. The point $T = [(0,b)-\infty] \in J(k)$ is fixed by σ and is non-zero, so $J[\lambda] = \langle T\rangle$. For a non-square $\eta \in k^\times$ we denote by J^η the Jacobian of the quadratic twist $\eta Y^2 = X^{11}+b^2$ of C, by τ the non-trivial automorphism of $k(\sqrt{\eta})/k$, and we identify $J^\eta(k)$ with $\{D \in J(k(\sqrt{\eta})) : \tau(D) = -D\}$. The isogeny λ commutes with τ and induces an isogeny of J^η, which we also denote by λ. For a field $k \supseteq F$ we always take b to be the element a^5 defined above, and $\eta = 4-\theta$. Then $C = C_{n_0}$ if n_0 is even, and J^η is the Jacobian of C_{n_0} if n_0 is odd. For $k = F$ the automorphism τ is the non-trivial automorphism of B/F.

Proposition 5.1. *Let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$, $\varphi(\xi) = nG$, and let n_0 and w be as in Corollary 4.9. Then there exists $\rho \in L^\times$ such that*

$$P = \left(aw, \frac{a^5\rho}{\beta}\right) \in C_{n_0}(L),$$

and $X(P) = a$ if and only if $n = n_0$. The point

$$P_0 = \left(a, \frac{a^5\rho_{n_0}}{\beta}\right)$$

lies on C_{n_0}. If n_0 is even, then $[P-P_0] \in J(F)$. If n_0 is odd, then the images of P and P_0 under the isomorphism $C_{n_0} \to C$, $(X,Y) \mapsto (X, \sqrt{\eta}\,Y)$, over B, which we again denote by P and P_0, satisfy $[P-P_0] \in J^\eta(F)$.

Proof. The function $x-\theta$ has divisor $2(\theta,-1/2)-2(O)$ and leading coefficient 1, so by Lemma 4.4, $Q \mapsto x(Q)-\theta$ induces a homomorphism $E(L) \to L^\times/L^{\times 2}$. Since $n \equiv n_0 \pmod 2$, the points $nG-3s$ and n_0G-3s differ by an element of $2E(L)$, so $x(nG-3s)-\theta = \eta_{n_0}\rho^2$ for some $\rho \in L^\times$. Combining this with (4.1) we get

$$\eta_{n_0}\rho^2 = \beta^2 + \delta_{n_0}w^{11} = \beta^2(1+aw^{11}),$$

and multiplying by a^{10}/β^2 we obtain that $P \in C_{n_0}(L)$. The claim about P_0 is the case $n = n_0$, and $X(P) = a$ if and only if $w = 1$, so the second statement follows from Corollary 4.9. If n_0 is even, then $C_{n_0} = C$ and $[P-P_0] \in J(L) \subseteq J(F)$. If n_0 is odd, then $\tau(P)$ and $\tau(P_0)$ are the images of P and P_0 under the hyperelliptic involution, so $\tau([P-P_0]) = -[P-P_0]$. □

Lemma 5.2. *Let k be a field of characteristic 0 containing ζ_{11}, let $b \in k^\times$, let J be the Jacobian of $C\colon Y^2 = X^{11}+b^2$ over k, let $\lambda = 1-\sigma$, where $\sigma(X,Y) = (\zeta_{11}X, Y)$, and let $T = [(0,b)-\infty]$.*

a) *The map*

$$\mu_k\colon J(k)/\lambda J(k) \to k^\times/k^{\times 11}, \quad \Big[\sum_i n_iP_i\Big] \mapsto \prod_i (Y(P_i)-b)^{n_i},$$

where $\sum_i n_iP_i$ runs through the divisors of degree 0 whose support does not contain $(0,b)$, and where $Y-b$ takes the value 1 at ∞, is a well-defined injective homomorphism, and $\mu_k(T)$ is the class of $1/(2b)$.

b) *Let $\eta \in k^\times$ be a non-square, let J^η be the Jacobian of $\eta Y^2 = X^{11}+b^2$, let τ be the non-trivial automorphism of $k(\sqrt{\eta})/k$, and identify $J^\eta(k)$ with $\{D \in J(k(\sqrt{\eta})) : \tau(D) = -D\}$. Then $J^\eta[\lambda](k) = 0$, and $\mu_{k(\sqrt{\eta})}$ induces an injective homomorphism*

$$\mu_k\colon J^\eta(k)/\lambda J^\eta(k) \to \left(k(\sqrt{\eta})^\times/k(\sqrt{\eta})^{\times 11}\right)^-,$$

where the superscript $-$ denotes the subspace on which τ acts as -1.

Proof. The curve C is the cyclic cover $X^{11} = (Y-b)(Y+b)$ of the Y-line, and the function $Y-b$ has divisor $11((0,b))-11(\infty)$ and leading coefficient 1 with respect to the parameter X^5/Y at ∞. Hence the first statement of a) is [12, Theorem 2.3 and Section 3] (with the roles of X and Y interchanged, and with the polynomial $Y^2 - b^2$ of degree 2, which is prime to 11). Since $T = -[(0,-b) - \infty]$ and -1 is an 11-th power, $\mu_k(T)$ is the class of $1/(2b)$.

For b), note that $\tau(T) = T$, so if $hT \in J^\eta(k)$ for some $h \in \mathbb{Z}$, then $hT = -hT$, and hence $hT = 0$. The map $\mu_{k(\sqrt{\eta})}$ commutes with τ, as $b \in k$, so it maps $J^\eta(k)$ to the subspace on which τ acts as -1. If $D \in J^\eta(k)$ and $\mu_{k(\sqrt{\eta})}(D) = 0$, then $D = \lambda D'$ with $D' \in J(k(\sqrt{\eta}))$ by a), so $2D = \lambda(D' - \tau(D'))$ with $D' - \tau(D') \in J^\eta(k)$. Since 11 is divisible by λ in $\mathbb{Z}[\sigma]$, we have $11D \in \lambda J^\eta(k)$, and it follows that $D = 6 \cdot 2D - 11D \in \lambda J^\eta(k)$. □

For a field $k \supseteq F$ we call the maps μ_k of Lemma 5.2 (for our b and $\eta = 4 - \theta$) the *Kummer maps*. For a number field $k \supseteq F$ we denote by $\mathrm{Sel}^\lambda(J/k) \subseteq k^\times/k^{\times 11}$ the λ-Selmer group, which is the set of classes whose localizations lie in the images of the local Kummer maps at all places. It contains $\mu_k(J(k)/\lambda J(k))$. The curve C has good reduction at all the primes not above 2 and 11, since b is a unit at these primes, so $\mathrm{Sel}^\lambda(J/k) \subseteq k(S_k, 11)$, where S_k is the set of primes of k above 2 and 11. For odd n_0 we define $\mathrm{Sel}^\lambda(J^\eta/F)$ in the same way, and it is contained in $B(S_B, 11)^-$.

Remark 5.3. Our arguments do not use the ranks of $J(F)$ and $J^\eta(F)$, but we can determine some of them. For odd n_0 the Selmer group $\mathrm{Sel}^\lambda(J^\eta/F)$ has dimension 1 and contains the non-zero class $\mu_F([P_0 - \infty])$ (Proposition 7.3). As $J^\eta(F)$ is a $\mathbb{Z}[\zeta_{11}]$-module with no λ-torsion, it follows that it has rank 1 over $\mathbb{Z}[\zeta_{11}]$ and rank 10 over $\mathbb{Z}$. The non-trivial automorphism of F/L acts on the 1-dimensional $\mathbb{Q}(\zeta_{11})$-vector space $J^\eta(F) \otimes \mathbb{Q}$ semilinearly with respect to $\zeta_{11} \mapsto \zeta_{11}^{-1}$, so its fixed space $J^\eta(L) \otimes \mathbb{Q}$ has dimension 5 over $\mathbb{Q}$, and the Jacobian of C_{n_0} has rank 5 over L. For even n_0 we get that the rank of $J(F)$ is at most 40, 40, 30 and 30 for $n_0 = -2, 0, 2, 4$ (Proposition 7.4).

6. Formal groups

Let l be a finite extension of $\mathbb{Q}_{11}$ containing ζ_{11} and with residue field $\mathbb{F}_{11}$, and let $b \in \mathcal{O}_l^\times$. For such a pair (l, b) we use the following notation, with C, J, σ and λ as in Section 5. Let ϖ be a uniformizer of l and $e = v(\pi)$, so $v(11) = 10e$. Let $\mathcal{C}$ be the closure of C in the weighted projective plane $\mathbb{P}(1,6,1)$ over $\mathcal{O}_l$. This is a proper flat model of C over $\mathcal{O}_l$. Its special fiber is the curve $Y^2 = (X + \bar{b}^2)^{11}$, which is geometrically integral and has a unique singular point $(-\bar{b}^2, 0)$, and the point ∞ is a smooth point of both fibers. The differentials

$$\omega_j = \frac{X^{j-1}dX}{2Y}, \quad j = 1, \dots, 5,$$

form a basis of $H^0(\mathcal{C}, \omega_{\mathcal{C}/\mathcal{O}_l})$, and $\sigma^*\omega_j = \zeta_{11}^j \omega_j$.

The identity component of the relative Picard functor of $\mathcal{C}$ over $\mathcal{O}_l$ is represented by a smooth separated group scheme, whose generic fiber is J (see [4, 9.3/1], which applies as $\mathcal{C}$ is projective and flat over $\mathcal{O}_l$ with geometrically reduced and irreducible fibers). Let $\widehat{J}$ be its formal group, which is a formal group of dimension 5 over $\mathcal{O}_l$ whose invariant differentials correspond to the ω_j. Its points $\widehat{J}(\varpi\mathcal{O}_l)$ form an open subgroup of finite index of $J(l)$. The automorphism σ of $\mathcal{C}$ acts on $\widehat{J}$, and since σ is the identity on $\mathcal{C}$ modulo π, its action on $\widehat{J}$ is the identity modulo π.

Lemma 6.1. *Let l be a finite extension of $\mathbb{Q}_{11}$ containing ζ_{11} and with residue field $\mathbb{F}_{11}$, and let $b \in \mathcal{O}_l^\times$.*

a) *The formal logarithm* $\log = (\log_1, \dots, \log_5)$ *of* $\widehat{J}$*, normalized by* $d\log_j = \omega_j$*, has coefficients in* $\mathcal{O}_l$ *(with respect to suitable formal coordinates over* $\mathcal{O}_l$*), and*

$$\log\colon \widehat{J}(\varpi\mathcal{O}_l) \to (\varpi\mathcal{O}_l)^5$$

is an isomorphism of groups.

b) *For* $m \geq 1$ *put* $H_m = \log^{-1}((\varpi^m\mathcal{O}_l)^5)$*. Then* λ *acts on the logarithm by* $\log_j \mapsto (1-\zeta_{11}^j)\log_j$*, and* λ *maps* H_m *isomorphically onto* H_{m+e}*.*

c) *The logarithm extends uniquely to a homomorphism* $\log\colon J(l) \to l^5$*, whose kernel is the torsion subgroup of* $J(l)$*, which is finite. For points* P, Q *in a disc of* $C(l)$ *on which the integrals of the* ω_j *converge,* $\log[P-Q] = \int_Q^P(\omega_1, \dots, \omega_5)$*.*

Proof. Choose formal coordinates $Z_1, \dots, Z_5$ of $\widehat{J}$ over $\mathcal{O}_l$ such that dZ_j and ω_j agree at the origin. The power series of $[\sigma]$ is congruent to the identity modulo π, so all the coefficients of the power series of $[\lambda] = [1-\sigma]$ are divisible by π. Since $11/\pi^{10}$ is a unit of $\mathbb{Z}[\zeta_{11}]$, the endomorphism $[11]$ is the composition of $[\lambda]^{10}$ with an automorphism of $\widehat{J}$, and as the composition of power series without constant terms whose coefficients are divisible by π^i and $\pi^{i'}$ has coefficients divisible by $\pi^{i+i'}$, all the coefficients of $[11]$ are divisible by π^{10}, and hence by 11. Write $[11](Z) = 11\,g(Z)$, where $g(Z) = Z + (\text{higher terms})$ has coefficients in $\mathcal{O}_l$.

We prove that the coefficients c_I of log (where I is a multi-index) are integral by induction on the total degree $|I|$, the case $|I| = 1$ being clear. Comparing the terms of total degree $M \geq 2$ in $\log(11g(Z)) = 11\log(Z)$, we get

$$(11 - 11^M)c_I = \sum_{|I'|<M} 11^{|I'|}c_{I'} \cdot (\text{integral coefficients}),$$

and the right-hand side is divisible by 11 by the induction hypothesis. As $(11-11^M)/11$ is a unit, c_I is integral. Since $\log(Z) = Z + (\text{higher terms})$, its inverse exp also has integral coefficients, so log is an isomorphism of formal groups $\widehat{J} \to \widehat{\mathbb{G}}_a^5$ over $\mathcal{O}_l$, and in particular $\log\colon \widehat{J}(\varpi\mathcal{O}_l) \to (\varpi\mathcal{O}_l)^5$ is an isomorphism. This proves a). As $\sigma^*\omega_j = \zeta_{11}^j\omega_j$, the endomorphism λ acts on $\log_j$ by $1-\zeta_{11}^j$, which has valuation e, and b) follows.

As $\widehat{J}(\varpi\mathcal{O}_l)$ has finite index in $J(l)$ and is torsion free by a), the logarithm extends uniquely to a homomorphism $J(l) \to l^5$, whose kernel is the torsion subgroup of $J(l)$, and this subgroup injects into $J(l)/\widehat{J}(\varpi\mathcal{O}_l)$. For P, Q in a disc on which the integrals converge, both sides of the last formula vanish for $P = Q$ and have the same derivative, which proves c). □

Note that by Lemma 6.1, $H_m/H_{m+1} \simeq \mathbb{F}_{11}^5$ via $D \mapsto \log(D)/\varpi^m \bmod \varpi$. We call the image of $D \in H_m \setminus H_{m+1}$ in $\mathbb{F}_{11}^5$ its *leading vector*, and m its *depth*. Note also that $(1-\zeta_{11}^j)/\pi = 1 + \zeta_{11} + \cdots + \zeta_{11}^{j-1} \equiv j \pmod{\pi}$.

Lemma 6.2. *Let* l *be a finite extension of* $\mathbb{Q}_{11}$ *containing* ζ_{11} *and with residue field* $\mathbb{F}_{11}$*, let* $b \in \mathcal{O}_l^\times$*, let* $f(X) = X^{11} + b^2$*, and let* $Q = (X_Q, Y_Q) \in C(l)$ *with* $X_Q, Y_Q \in \mathcal{O}_l$*.*

a) *Suppose* $Y_Q \in \mathcal{O}_l^\times$*. Let* $P \in C(l)$ *be such that* $X_P \equiv X_Q$ *and* $Y_P \equiv Y_Q \pmod{\varpi}$*, and put* $t = X_P - X_Q$ *and* $d = v(t)$*. Then* $[P-Q] \in H_d$ *and*

$$\log[P-Q] \equiv t\left(\frac{X_Q^{j-1}}{2Y_Q}\right)_{j=1,\dots,5} \pmod{\varpi^{2d}}.$$

b) *Suppose* $e = 2$, $v(Y_Q) = 1$ *and* $X_Q \equiv -\bar{b}^2 \pmod{\varpi}$. *Let* $P = (X_Q + t, Y_P) \in C(l)$ *with* $d = v(t) \geq 28$ *and* $Y_P/Y_Q \equiv 1 \pmod{\varpi}$. *Then* $[P - Q] \in H_{d-1} \setminus H_d$ *and*

$$\log[P - Q] \equiv \frac{t}{2Y_Q} \left(X_Q^{j-1}\right)_{j=1,\dots,5} \pmod{\varpi^d}.$$

Proof. For a) note that Q and P are $\mathcal{O}_l$-points of the smooth locus of $\mathcal{C}$ with the same reduction, so the class of the line bundle $\mathcal{O}(P - Q)$ is trivial on the special fiber, and $[P - Q] \in \widehat{J}(\varpi\mathcal{O}_l)$. The function $X - X_Q$ is a parameter of $\mathcal{C}$ at the reduction of Q, and the map $P \mapsto [P - Q]$ from the residue disc of Q to $\widehat{J}$ is given by power series in t with coefficients in $\mathcal{O}_l$. Thus $\log[P - Q] = \sum_{h \geq 1} g_h t^h$ with $g_h \in \mathcal{O}_l^5$, and $g_1 = (X_Q^{j-1}/(2Y_Q))_j$ is the value of $(\omega_j/dX)_j$ at Q. This proves a).

For b), Q reduces to the singular point of the special fiber, so we argue analytically. Put $\Delta(t) = (f(X_Q + t) - f(X_Q))/Y_Q^2$. Since $v(\binom{11}{h}) = 20$ for $1 \leq h \leq 10$ and $v(Y_Q^2) = 2$, the coefficient of t^h in Δ has valuation at least 18 for $h \leq 10$ and is Y_Q^{-2} for $h = 11$. For $v(t) \geq 1$ the series $Y(t) = Y_Q(1 + \Delta(t))^{1/2}$ converges, and it gives the points of C near Q with $Y/Y_Q \equiv 1 \pmod{\varpi}$. The binomial coefficients of $(1 + \Delta)^{-1/2}$ are 11-integral, so the coefficient of t^h in $(X_Q + t)^{j-1}/(2Y(t))$ has valuation at least $-2h - 1$. Integrating term by term, the term with t^{h+1} in $I_j(t) = \int_0^t (X_Q + u)^{j-1} du/(2Y(u))$ has valuation at least

$$(h + 1)d - 2h - 1 - 20v_{11}(h + 1) > d - 1 \quad \text{for } h \geq 1,$$

since $d \geq 28$ and $20v_{11}(h + 1) \leq 2h$. Hence $I(t) = (I_1(t), \dots, I_5(t)) \in (\varpi^{d-1}\mathcal{O}_l)^5$ and $I(t) \equiv (t/(2Y_Q))(X_Q^{j-1})_j \pmod{\varpi^d}$. By Lemma 6.1 a), $\exp(I(t)) \in H_{d-1}$. By Lemma 6.1 c), $\log[P - Q] = I(t) = \log \exp(I(t))$, so the maps $t \mapsto [P - Q]$ and $t \mapsto \exp(I(t))$, which are rigid analytic on the disc $v(t) \geq 28$ and take the value 0 at $t = 0$, differ by a torsion point of $J(l)$. As the torsion of $J(l)$ is finite, the two maps are equal. The first coordinate of $I(t)$ has valuation $d - 1$, so $[P - Q] \notin H_d$. □

Lemma 6.3. *Let* l *be a finite extension of* $\mathbb{Q}_{11}$ *containing* ζ_{11} *and with residue field* $\mathbb{F}_{11}$, *and let* $b \in \mathcal{O}_l^\times$.

a) *Suppose* $e = 1$, *so* $l \simeq \mathbb{Q}_{11}(\zeta_{11})$, *take* $\varpi = \pi$, *suppose that* $\bar{b}^2 = 1$, *and let* μ_l *be the map of Lemma 5.2 a). Then* $\mu_l(H_2) = 0$, *and for* $D \in H_1$ *with leading vector* $(c_1, \dots, c_5)$ *we have*

$$\mu_l(D) = -\frac{1}{2\bar{b}} \left(\sum_{j=1}^{5} \ell_{j-1} c_j \right) \kappa_l,$$

where κ_l *is the class of* $1 + \pi^{11}$ *in* $l^\times/l^{\times 11}$ *and*

$$\ell_0 + \ell_1 X + \cdots + \ell_4 X^4 = \prod_{h \in \{2,3,4,8\}} \frac{X - h}{-h} = 1 + 2X + 2X^2 + X^3 + 9X^4 \in \mathbb{F}_{11}[X].$$

b) *Suppose that* $l = k(\sqrt{\eta})$, *where* $k \simeq \mathbb{Q}_{11}(\zeta_{11})$, $\eta, b \in k$ *and* $v_k(\eta)$ *is odd, so* $e = 2$. *Let* τ *be the non-trivial automorphism of* l/k, *let* J^η *be the Jacobian of* $\eta Y^2 = X^{11} + b^2$, *with* $J^\eta(k)$ *identified with* $\{D \in J(l) : \tau(D) = -D\}$, *and let* μ_k *be the map of Lemma 5.2 b) for* J^η *over* k. *Choose* ϖ *with* $\tau(\varpi) = -\varpi$, *and put* $H_m^- = \{D \in H_m : \tau(D) = -D\}$. *Then* $H_2^- = H_3^- = \lambda H_1^-$, $\mu_k(H_2^-) = 0$, *and the restriction of* μ_k *to* H_1^- *factors through the isomorphism* $H_1^-/H_2^- \simeq \mathbb{F}_{11}^5$ *given by the leading vector.*

Proof. a) By Lemma 6.1 b), $H_2 = \lambda H_1 \subseteq \lambda J(l)$, so $\mu_l(H_2) = 0$. Let $Q_0 = (0, -b)$ and $Q_i = (X_i, Y_i)$ for $(X_1, \dots, X_4) = (2, 3, 4, 8)$, where $Y_i \in \mathcal{O}_l$ is a square root of $X_i^{11} + b^2$, which exists as $X_i + 1$ is a square modulo 11. For $t = (t_0, \dots, t_4) \in (\pi\mathcal{O}_l)^5$ let $Q_i(t_i)$ be

the point of $C(l)$ with X-coordinate $X(Q_i)+t_i$ in the residue disc of Q_i. By Lemma 6.2 a), the map $t \mapsto \log \sum_i [Q_i(t_i) - Q_i]$ is given by integral power series whose linear part is $t \mapsto \sum_i t_i (X(Q_i)^{j-1}/(2Y(Q_i)))_j$, which is invertible modulo π (as the $X(Q_i)$ are distinct modulo π). Hence $t \mapsto \sum_i [Q_i(t_i) - Q_i]$ is a bijection $(\pi\mathcal{O}_l)^5 \to H_1$, and the leading vector c of $\sum_i [Q_i(t_i) - Q_i]$ satisfies $\sum_i \overline{u}_i (X(Q_i)^{j-1}/(2Y(Q_i)))_j = c$, where $t_i = \pi u_i$. Using Lagrange interpolation we get $\overline{u}_0 = 2\overline{Y}(Q_0) \sum_j \ell_{j-1} c_j = -2\bar{b} \sum_j \ell_{j-1} c_j$.

We have $\mu_l(\sum_i [Q_i(t_i) - Q_i]) = \prod_i (Y(Q_i(t_i)) - b)/(Y(Q_i) - b)$. For $i \geq 1$,

$$f(X_i + \pi u_i) - f(X_i) \equiv \pi^{11} \left(\frac{11}{\pi^{10}} X_i^{10} u_i + u_i^{11} \right) \equiv \pi^{11}(-\overline{u}_i + \overline{u}_i) \equiv 0 \pmod{\pi^{12}},$$

where $f(X) = X^{11} + b^2$, as $11/\pi^{10} \equiv -1 \pmod{\pi}$ and $v(\binom{11}{h}\pi^h) \geq 12$ for $2 \leq h \leq 10$. Since $Y(Q_i)$ and $Y(Q_i) - b$ are units, it follows that $(Y(Q_i(t_i)) - b)/(Y(Q_i) - b) \equiv 1 \pmod{\pi^{12}}$. For $i = 0$ we have $Y(Q_0(t_0)) = -b(1 + t_0^{11}/b^2)^{1/2}$, so

$$\frac{Y(Q_0(t_0)) - b}{-2b} \equiv 1 + \frac{\pi^{11} u_0^{11}}{4b^2} \equiv 1 + \pi^{11} \frac{\overline{u}_0}{4\bar{b}^2} \pmod{\pi^{12}}.$$

Finally, $1 + \pi^{12}\mathcal{O}_l \subseteq l^{\times 11}$ (using log and exp on $1 + \pi^2\mathcal{O}_l$), and the class of $1 + \pi^{11} y$ is $\overline{y}\kappa_l$ for $y \in \mathcal{O}_l$. Putting these together proves a).

b) Since the model $\mathcal{C}$ and the differentials ω_j are defined over $\mathcal{O}_k$, the logarithm commutes with τ. If $\log D = \varpi^m y$, then $\log \tau(D) = (-1)^m \varpi^m \tau(y) \equiv (-1)^m \varpi^m y \pmod{\varpi^{m+1}}$, as τ acts trivially on the residue field. Thus τ acts as $(-1)^m$ on H_m/H_{m+1}. If $D \in H_2^-$, then the image of D in H_2/H_3 equals its negative, so $D \in H_3$. By Lemma 6.1 b), λ maps H_1 isomorphically onto H_3, and it commutes with τ, so $H_3^- = \lambda H_1^-$, and $\mu_k(H_3^-) = 0$. Finally, the map $H_1^- \to H_1/H_2$ is surjective, since for $D \in H_1$ the element $6(D - \tau(D)) \in H_1^-$ has the same image in H_1/H_2 as $12D$, which is the image of D. Its kernel is H_2^-. □

7. Selmer groups

Lemma 7.1. *Let S_F and S_B be the sets of primes of F and of B above 2 and 11.*

a) *The 11-parts of the class groups of F and B are trivial.*

b) *We have $\dim F(S_F, 11) = 19$, $\dim B(S_B, 11) = 34$ and $\dim B(S_B, 11)^- = 15$, where the superscript $-$ denotes the subspace on which the non-trivial automorphism τ of B/F acts as -1.*

Proof. The root discriminants of F and B are $(2^{20} \cdot 11^{27})^{1/30} < 19$ and $(2^{60} \cdot 11^{56})^{1/60} < 19$. Suppose M is an unramified cyclic extension of degree 11 of F or of B. Then M is a totally complex field of degree $N \geq 330$ with the same root discriminant, which is less than 19. On the other hand, the unconditional bound of Odlyzko [9, Table 4], with the parameter $b = 9$, gives $|d_M| > 20.710^N e^{-24.001}$ (the constants in the table are rounded in the safe direction, see the description of the tables in [9]), so the root discriminant of M is larger than

$$20.710\, e^{-24.001/330} > 20.710 \left(1 - \frac{24.001}{330}\right) > 19,$$

which is a contradiction. We verify the discriminants and the inequalities. This proves a).

The fields F and B are totally complex of degrees 30 and 60, they contain ζ_{11}, and S_F and S_B both have 4 elements (see Section 5). By a) we get $\dim F(S_F, 11) = 15 + 4 = 19$ and $\dim B(S_B, 11) = 30 + 4 = 34$. Since $[B : F] = 2$, the subspace of $B(S_B, 11)$ fixed by τ is the image of $F(S_F, 11)$, so $\dim B(S_B, 11)^- = 15$. □

For a place v of a number field k and a class $c \in k^\times/k^{\times 11}$ we denote by $\mathrm{loc}_v(c)$ its image in $k_v^\times/k_v^{\times 11}$.

Lemma 7.2. *Let $n_0 \in \{-2, \dots, 4\}$ and let v be a prime of F above 11. Then the image of the Kummer map μ_{F_v} of J has dimension 6. If n_0 is odd, then the image of the Kummer map μ_{F_v} of J^η, where $\eta = 4 - \theta$, has dimension 5.*

Proof. For an isogeny $\psi\colon V \to V$ of an abelian variety over a finite extension k of $\mathbb{Q}_p$ we have

$$\#V(k)/\psi V(k) = \#V[\psi](k) \cdot |\det \psi'(0)|_k^{-1},$$

where $\psi'(0)$ is the action of ψ on the tangent space at the origin and $|\cdot|_k$ is the normalized absolute value. This is [11, Lemma 3.8] in the case of an isogeny from V to itself, in which the orders of the groups of components that appear there cancel. We have $F_v \simeq \mathbb{Q}_{11}(\zeta_{11})$ (see Section 5), and the determinant of λ on the tangent space of J and of J^η is $\prod_{j=1}^5 (1 - \zeta_{11}^j)$, which has valuation 5 in F_v. As $J[\lambda](F_v) = \langle T \rangle$, and as $J^\eta[\lambda](F_v) = 0$ by Lemma 5.2 b) ($4 - \theta$ is not a square in F_v), the lemma follows from the injectivity of the Kummer maps (Lemma 5.2). □

Proposition 7.3. *Let $n_0 \in \{-1, 1, 3\}$ and $\eta = 4 - \theta$. For a prime v of F above 11 let $\tilde{v}$ be the prime of B above v, and let $W_v \subseteq (B_{\tilde{v}}^\times / B_{\tilde{v}}^{\times 11})^-$ be the image of the Kummer map of J^η over F_v. Let*

$$\mathcal{S} = \{c \in B(S_B, 11)^- : \mathrm{loc}_{\tilde{v}}(c) \in W_v \text{ for all } v \mid 11\}.$$

a) *We have $\mathrm{Sel}^\lambda(J^\eta/F) \subseteq \mathcal{S}$, and $\mathcal{S}$ is 1-dimensional, spanned by $\mu_F([P_0 - \infty])$.*
b) *Let v be one of the two primes of F above 11 with $v(4 - \theta)$ odd, and let $\kappa_v^- \in W_v$ be the image under the Kummer map of an element of H_1^- with leading vector $(1, 4, 9, 6, 3)$, where H_1^- and the leading vectors are taken for the pair $(B_{\tilde{v}}, b)$ and a uniformizer ϖ of $B_{\tilde{v}}$ with $\tau(\varpi) = -\varpi$ (see Lemma 6.3 b)). Then $\kappa_v^- \neq 0$, $\mathrm{loc}_{\tilde{v}}(\mathcal{S})$ is 1-dimensional, and $\kappa_v^- \notin \mathrm{loc}_{\tilde{v}}(\mathcal{S})$.*

Proof. The inclusion in a) is clear from the definitions. We compute the rest as follows. We find 15 elements of $B(S_B, 11)^-$ of the form $g/\tau(g)$, with g an S-unit in one of the fields $L(\sqrt{4 - \theta})$ and $L(\sqrt{-11(4 - \theta)})$ of degree 30 (computed under GRH), and we check that their valuations outside S_B are divisible by 11 and that their localizations at the 3 primes above 11 are linearly independent. By Lemma 7.1 b), they form a basis of $B(S_B, 11)^-$, and this does not depend on GRH. At each of the 3 primes v above 11 we compute the images of the classes $6[P - \tau(P)]$ for points $P \in C(B_{\tilde{v}})$ until they span a space of dimension 5, which is then equal to W_v by Lemma 7.2. Then we compute $\mathcal{S}$ and check that it contains the class $\mu_F([P_0 - \infty])$, which is non-zero. For b) we construct an explicit element of H_1^- with the given leading vector, as in the proof of Lemma 6.3 a). We take $6 \sum_i [Q_i^+ - Q_i^-]$, where $Q_i^\pm$ are the points of $C(B_{\tilde{v}})$ with X-coordinates $h_i \pm \varpi u_i$, for $h_i \in \{0, 2, 3, 4, 8\}$, such that $\tau(Q_i^+) = Q_i^-$, and where the u_i are chosen such that the leading vector is $(1, 4, 9, 6, 3)$. We compute its image κ_v^- under the Kummer map, and check that $\kappa_v^- \neq 0$ and $\kappa_v^- \notin \mathrm{loc}_{\tilde{v}}(\mathcal{S})$. □

Proposition 7.4. *Let $n_0 \in \{-2, 0, 2, 4\}$. For a prime v of F above 11 let $W_v \subseteq F_v^\times / F_v^{\times 11}$ be the image of the Kummer map of J over F_v, and let*

$$\mathcal{S} = \{c \in F(S_F, 11) : \mathrm{loc}_v(c) \in W_v \text{ for all } v \mid 11\}.$$

a) *We have $\mathrm{Sel}^\lambda(J/F) \subseteq \mathcal{S}$, and $\dim \mathcal{S} = 5, 5, 4, 4$ for $n_0 = -2, 0, 2, 4$, respectively.*
b) *Let v be one of the two primes of F above 11 with $v(4 - \theta)$ odd, and let κ_v be the class of $1 + \pi^{11}$ in $F_v^\times / F_v^{\times 11}$. Then loc_v is injective on $\mathcal{S}$, and $\kappa_v \notin \mathrm{loc}_v(\mathcal{S})$.*

Proof. The inclusion in a) is clear from the definitions. We compute the rest. We find 19 generators of $F(S_F, 11)$ under GRH, and we check that their valuations outside S_F are divisible by 11 and that their localizations at the primes above 11 are linearly independent, so they form a basis by Lemma 7.1 b). At each of the 3 primes v above 11 we compute

the images $Y(P) - b$ of the classes $[P - \infty]$ for points $P \in C(F_v)$, together with $\mu_{F_v}(T)$, until they span a space of dimension 6, which is then equal to W_v by Lemma 7.2. Then we compute $\mathcal{S}$, and check b). □

Remark 7.5. Imposing also the local conditions at the prime of F above 2 does not make the spaces $\mathcal{S}$ of Proposition 7.4 smaller (see `code/even_selmer.m`). In Propositions 7.3 and 7.4 the statements b) hold for both primes v with $v(4-\theta)$ odd, but not for the third prime above 11 (for $n_0 = 2$, the localization at the third prime is not injective on $\mathcal{S}$).

Lemma 7.6. *Let A be an abelian variety over a number field k, let ψ be an isogeny from A to itself defined over k, and let v be a place of k. Suppose that the map $A(k)/\psi A(k) \to A(k_v)/\psi A(k_v)$ is injective and that $A[\psi](k_v) = A[\psi](k)$. If $D \in A(k)$ and $D' \in A(k_v)$ satisfy $\psi D' = D$, then $D' \in A(k)$.*

Proof. The image of D in $A(k_v)/\psi A(k_v)$ is 0, so by the injectivity $D = \psi D_0$ for some $D_0 \in A(k)$. Then $D_0 - D' \in A[\psi](k_v) = A[\psi](k)$, so $D' = D_0 - (D_0 - D') \in A(k)$. □

Lemma 7.7. *Let v be one of the two primes of F above 11 with $v(4-\theta)$ odd.*

a) *If $n_0 \in \{-2, 0, 2, 4\}$, then the Jacobian J over F, the isogeny λ and the place v satisfy the hypotheses of Lemma 7.6.*

b) *If $n_0 \in \{-1, 1, 3\}$, then the Jacobian J^η over F, where $\eta = 4 - \theta$, the isogeny λ and the place v satisfy the hypotheses of Lemma 7.6.*

Proof. a) Let $D \in J(F)$ be such that its image in $J(F_v)$ lies in $\lambda J(F_v)$. Then $\mathrm{loc}_v(\mu_F(D)) = \mu_{F_v}(D) = 0$. Since $\mu_F(D) \in \mathrm{Sel}^\lambda(J/F) \subseteq \mathcal{S}$, where $\mathcal{S}$ is as in Proposition 7.4, and loc_v is injective on $\mathcal{S}$ by Proposition 7.4 b), we get $\mu_F(D) = 0$, so $D \in \lambda J(F)$ by Lemma 5.2 a). As $J[\lambda] = \langle T \rangle$ and $T \in J(F)$, we have $J[\lambda](F_v) = J[\lambda](F)$.

b) Let $D \in J^\eta(F)$ be such that its image in $J^\eta(F_v)$ lies in $\lambda J^\eta(F_v)$, and let $\tilde{v}$ be the prime of B above v. Then $\mathrm{loc}_{\tilde{v}}(\mu_F(D)) = \mu_{F_v}(D) = 0$. Since $\mu_F(D) \in \mathrm{Sel}^\lambda(J^\eta/F) \subseteq \mathcal{S}$, where $\mathcal{S}$ is as in Proposition 7.3, and $\mathcal{S}$ and $\mathrm{loc}_{\tilde{v}}(\mathcal{S})$ are both 1-dimensional by Proposition 7.3, we get $\mu_F(D) = 0$, so $D \in \lambda J^\eta(F)$ by Lemma 5.2 b). As $4 - \theta$ is not a square in F_v, Lemma 5.2 b) gives $J^\eta[\lambda](F_v) = J^\eta[\lambda](F) = 0$. □

8. The odd classes

Let $v_\mathfrak{p}$ be the valuation of K at the prime $\mathfrak{p}$ above 11. Then $v_\mathfrak{p}(2-z) = 1$ and $v_\mathfrak{p}(11) = 5$.

Lemma 8.1. *Let $n_0 \in \{-2, \dots, 4\}$, let $n \equiv n_0 \pmod{4356}$ with $n \neq n_0$, and let $w \in K^\times$ be such that $x(nG - 3s) = \alpha + \delta_{n_0} w^{11}$. Put $\nu = v_{11}(n - n_0) \geq 2$. Then*

$$v_\mathfrak{p}(w-1) = \begin{cases} 5\nu - 3 & \text{if } n_0 \text{ is odd,} \\ 5\nu - 4 & \text{if } n_0 \text{ is even.} \end{cases}$$

Proof. Over the completion $K_\mathfrak{p}$, put $x' = (x-4)/(2-z)^2$ and $y' = (y + 1/2)/(2-z)^3$. Then

$$y'^2 = x'^3 + \frac{11}{(2-z)^2}x'^2 + \frac{33}{(2-z)^4}x' + \frac{121}{4(2-z)^6}$$

is a Weierstrass model of E with integral coefficients. Let $t' = -x'/y'$. We have $t'(2G) = 4(2-z)$ (see `code/even_geometry.m`), so $2G$ lies in the kernel of reduction of this model. As $1 > v_\mathfrak{p}(11)/10$, the formal logarithm is an isomorphism preserving valuations on the points with $v_\mathfrak{p}(t') \geq 1$ (see [15, Section IV.6]), and since $n - n_0 = 4m$ with $v_{11}(m) = \nu$, we get $v_\mathfrak{p}(t'((n-n_0)G)) = v_\mathfrak{p}(t'(2G)) + v_\mathfrak{p}(2m) = 1 + 5\nu$.

Let $q_0 = n_0 G - 3s$. Writing the addition law in the formal parameter, $x'(q_0 + Q)$ is a power series in $t'(Q)$ with coefficients in $\mathbb{Z}[x'(q_0), y'(q_0), 11/(2-z)^2, 33/(2-z)^4, 121/(4(2-z)^6)]$ whose linear term is $2y'(q_0)t'(Q)$. We compute that $v_\mathfrak{p}(x'(q_0)) = v_\mathfrak{p}(y'(q_0)) = 1$ and

$v_{\mathfrak{p}}(\delta_{n_0}) = 2$ if n_0 is odd, and we compute that $v_{\mathfrak{p}}(x'(q_0)) = v_{\mathfrak{p}}(y'(q_0)) = 0$ and $v_{\mathfrak{p}}(\delta_{n_0}) = 2$ if n_0 is even. Hence for $Q = (n - n_0)G$,

$$v_{\mathfrak{p}}\big(x(nG - 3s) - x(q_0)\big) = 2 + v_{\mathfrak{p}}\big(x'(q_0 + Q) - x'(q_0)\big) = \begin{cases} 5\nu + 4 & \text{if } n_0 \text{ is odd,} \\ 5\nu + 3 & \text{if } n_0 \text{ is even,} \end{cases}$$

as the higher terms have valuation at least $2(1+5\nu)$. By assumption, $x(nG-3s)-x(q_0) = \delta_{n_0}(w^{11} - 1)$, so $v_{\mathfrak{p}}(w^{11} - 1)$ equals $5\nu + 2$ or $5\nu + 1$. In particular $w \equiv 1 \pmod{\mathfrak{p}}$, and if $v_{\mathfrak{p}}(w - 1) = h$, then in the expansion of $w^{11} - 1$ in powers of $w - 1$ the term $11(w - 1)$, of valuation $5 + h$, has smaller valuation than all the others, so $v_{\mathfrak{p}}(w^{11} - 1) = 5 + h$. The lemma follows. □

Lemma 8.2. *Let $n_0 \in \{-1, 1, 3\}$ and $\eta = 4-\theta$, let v be one of the two primes of F above 11 with $v(4-\theta)$ odd, let $k = F_v$, and let $l = B_{\tilde{v}}$ be the completion of B at the prime $\tilde{v}$ above v. Let H_1 and the leading vectors be taken for the pair (l, b) and a uniformizer ϖ of l with $\tau(\varpi) = -\varpi$, and let $H_1^- = \{D \in H_1 : \tau(D) = -D\}$. Then there is no $D \in J^\eta(F)$ whose image in $J^\eta(k)$ lies in H_1^- and has leading vector a non-zero multiple of $(1, 4, 9, 6, 3)$.*

Proof. Suppose the opposite, and let D be such a point. Changing the uniformizer ϖ to another one with the same property multiplies ϖ by an element of $\mathcal{O}_k^\times$, and hence the leading vectors of the elements of H_1^- by a non-zero scalar, so we may assume that ϖ is the uniformizer used in Proposition 7.3 b). By Lemma 6.3 b), $\mu_k(D)$ is a non-zero multiple of κ_v^-. On the other hand, $\mu_k(D) = \mathrm{loc}_{\tilde{v}}(\mu_F(D)) \in \mathrm{loc}_{\tilde{v}}(\mathcal{S})$, as $\mu_F(D) \in \mathrm{Sel}^\lambda(J^\eta/F) \subseteq \mathcal{S}$. This contradicts Proposition 7.3 b). □

Proposition 8.3. *Let $n_0 \in \{-1, 1, 3\}$, let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$, and suppose $\varphi(\xi) = nG$ with $n \equiv n_0 \pmod{4356}$. Then $n = n_0$.*

Proof. Suppose the opposite, that $n \neq n_0$, and let $\nu = v_{11}(n-n_0)$. Let v be one of the two primes of F above 11 with $v(4-\theta)$ odd, let $k = F_v$, and let $l = B_{\tilde{v}}$ be the completion of B at the prime $\tilde{v}$ above v. Then $l = k(\sqrt{\eta})$ is a ramified quadratic extension of $k \simeq \mathbb{Q}_{11}(\zeta_{11})$, so $e = 2$ for the pair (l, b), and $\varpi = \sqrt{\eta}/\pi^2$ is a uniformizer of l with $\tau(\varpi) = -\varpi$.

Let P and P_0 be the points of $C(B)$ from Proposition 5.1, and put $D = [P - P_0] \in J^\eta(F)$. We compute that $a \equiv -1 \pmod{v}$ (so $\overline{b}^2 = \overline{a}^{10} = 1$ and $X(P_0) \equiv -\overline{b}^2$) and that $v_l(Y(P_0)) = 1$. Replacing ρ by $-\rho$ in Proposition 5.1 if necessary, which replaces P by its image under the hyperelliptic involution, we may assume that $Y(P)/Y(P_0) \equiv 1 \pmod{\varpi}$, as $Y(P)^2 - Y(P_0)^2 = f(X(P)) - f(a)$, where $f(X) = X^{11} + b^2$, has valuation larger than 2. By Corollary 4.9 and Lemma 8.1,

$$d := v_l(X(P) - a) = v_l(a(w - 1)) = 4(5\nu - 3) = 20\nu - 12 \geq 28,$$

so by Lemma 6.2 b), the image of D in $J^\eta(k)$ lies in H_{d-1}^- and $\log D \equiv (t/(2Y(P_0)))(a^{j-1})_j \pmod{\varpi^d}$, where $t = X(P) - a$.

Let $N = 10\nu - 7$, so $d - 1 - 2N = 1$. By Lemma 6.1 b), with $e = 2$, for $0 \leq i \leq N$ there is a unique $D_i' \in H_{d-1-2i}$ with $\lambda^i D_i' = D$, and $\lambda D_{i+1}' = D_i'$. The logarithm commutes with τ, as $\mathcal{C}$ and the ω_j are defined over $\mathcal{O}_k$, so $\tau(D_i') \in H_{d-1-2i}$, and as $\lambda^i \tau(D_i') = \tau(D) = -D$, the uniqueness gives $\tau(D_i') = -D_i'$. Hence $D_i' \in J^\eta(k)$. By Lemmas 7.6 and 7.7 b), applied N times, D_N' is the image of a point of $J^\eta(F)$, and it lies in H_1^-. By Lemma 6.1 b),

$$\log_j D_N' = (1 - \zeta_{11}^j)^{-N} \log_j D \equiv \frac{t}{2Y(P_0)\pi^N}\, j^{-N}(-1)^{j-1} \pmod{\varpi^2},$$

using $(1-\zeta_{11}^j)/\pi \equiv j \pmod{\pi}$, $a \equiv -1 \pmod{\varpi}$ and $v_l(t/(2Y(P_0)\pi^N)) = d-1-2N = 1$. As $N \equiv 3 \pmod{10}$, the leading vector of D_N' is a non-zero multiple of

$$\big((-1)^{j-1} j^{-3}\big)_{j=1,\ldots,5} = (1, 4, 9, 6, 3) \in \mathbb{F}_{11}^5,$$

which contradicts Lemma 8.2. □

9. The even classes

Lemma 9.1. *Let $n_0 \in \{-2,0,2,4\}$, let v be one of the two primes of F above 11 with $v(4-\theta)$ odd, and let $l = F_v$, with H_m and the leading vectors taken for the pair (l,b) and $\varpi = \pi$. Let $D \in J(F)$ be such that its image in $J(l)$ lies in $H_1 \setminus H_2$ and has leading vector $(c_1,\dots,c_5)$. Then $\sum_{j=1}^5 \ell_{j-1}c_j = 0$, where $\ell_0,\dots,\ell_4$ are as in Lemma 6.3 a).*

Proof. As $b = a^5$, where a is a unit at v, and the residue field of l is $\mathbb{F}_{11}$, we have $\overline{b}^2 = \overline{a}^{10} = 1$. By Lemma 6.3 a), $\mu_l(D) = -(2\overline{b})^{-1}(\sum_j \ell_{j-1}c_j)\kappa_v$. On the other hand, $\mu_l(D) = \mathrm{loc}_v(\mu_F(D)) \in \mathrm{loc}_v(\mathcal{S})$, where $\mathcal{S}$ is as in Proposition 7.4, as $\mu_F(D) \in \mathrm{Sel}^\lambda(J/F) \subseteq \mathcal{S}$. Since $\kappa_v \notin \mathrm{loc}_v(\mathcal{S})$ by Proposition 7.4 b), and in particular $\kappa_v \neq 0$, it follows that $\sum_j \ell_{j-1}c_j = 0$. □

Proposition 9.2. *Let $n_0 \in \{-2,0,2,4\}$, let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$, and suppose $\varphi(\xi) = nG$ with $n \equiv n_0 \pmod{4356}$. Then $n = n_0$.*

Proof. Suppose the opposite, that $n \neq n_0$, and let $\nu = v_{11}(n-n_0)$. Let v be one of the two primes of F above 11 with $v(4-\theta)$ odd and let $l = F_v \simeq \mathbb{Q}_{11}(\zeta_{11})$, so $e = 1$ for the pair (l,b) and we can take $\varpi = \pi$. Let $P, P_0 \in C(F)$ be as in Proposition 5.1 and $D = [P - P_0] \in J(F)$. We compute that $a \equiv 8 \pmod{v}$ and that $Y(P_0)$ is a unit at v. As $Y(P)^2 - Y(P_0)^2 = f(X(P)) - f(a)$, where $f(X) = X^{11} + b^2$, has positive valuation, replacing ρ by $-\rho$ in Proposition 5.1 if necessary, we may assume that $Y(P) \equiv Y(P_0) \pmod{\pi}$. By Corollary 4.9 and Lemma 8.1,

$$d := v(X(P) - a) = 2(5\nu - 4) = 10\nu - 8 \geq 12,$$

so by Lemma 6.2 a), $D \in H_d$ and $\log D \equiv (t/(2Y(P_0)))(a^{j-1})_j \pmod{\pi^{2d}}$, where $t = X(P) - a$.

By Lemma 6.1 b), with $e = 1$, for $0 \leq i \leq d-1$ there is a unique $D'_i \in H_{d-i}$ with $\lambda^i D'_i = D$, and $\lambda D'_{i+1} = D'_i$. By Lemmas 7.6 and 7.7 a), applied $d-1$ times, D'_{d-1} is the image of a point of $J(F)$, and it lies in H_1. By Lemma 6.1 b),

$$\log_j D'_{d-1} = (1-\zeta_{11}^j)^{-(d-1)} \log_j D \equiv \frac{t}{2Y(P_0)\pi^{d-1}}\, j^{-(d-1)} 8^{j-1} \pmod{\pi^2},$$

and $v(t/(2Y(P_0)\pi^{d-1})) = 1$. As $d - 1 = 10\nu - 9 \equiv 1 \pmod{10}$, the image D'_{d-1} lies in $H_1 \setminus H_2$, and its leading vector is a non-zero multiple of $(8^{j-1}/j)_j$. Since

$$\sum_{j=1}^{5} \ell_{j-1} \frac{8^{j-1}}{j} = 1 + 8 + 6 + 7 + 5 = 5 \neq 0 \quad \text{in } \mathbb{F}_{11},$$

this contradicts Lemma 9.1. □

10. Proof of Theorem 1.1

Let $\xi \in X_{\mathrm{ns}}^+(121)(\mathbb{Q})$. By Corollary 4.5 ξ is not a cusp, and $\varphi(\xi) = nG$ for some $n \in \mathbb{Z}$. By Proposition 4.7 there is an $n_0 \in \{-2,\dots,4\}$ with $n \equiv n_0 \pmod{4356}$, and by Propositions 8.3 and 9.2 we have $n = n_0$. By Lemma 3.4, ξ is the unique rational point above $n_0 G$, which is a CM point with the discriminant D given in Table 1. Conversely, by Lemma 3.4 these 7 CM points are rational, which proves the theorem.

11. Computations

All the computations were done in Magma V2.30-1 [5], on the *Mordell* server at the Department of Mathematics, University of Zagreb, which has an AMD EPYC 9175F processor with 16 cores (32 threads) and 384 GB of RAM. All of them can be rerun with the script `run_all.sh`, which also checks that every computation reaches its success

marker, in about 4 minutes of wall time and 10 minutes of CPU time (with at most 3 Magma processes at a time). The longest computations are the Selmer groups for the odd classes (2 minutes for all 3 classes at the 11-adic precision of 160 digits) and the supplementary checks below (2 minutes).

The local computations at the primes above 11 were done with p-adic precision 160, and the Selmer groups for the odd classes also with precision 80, with the same results. We use the image of a local element under the Kummer map only when we know it to relative precision at least $2v(11)+2$. This is enough, since $1+\varpi^m\mathcal{O}_l \subseteq l^{\times 11}$ for $m > 11v(11)/10$.

GRH was used only to find the generators of the groups $F(S_F, 11)$ and of the groups of S-units of the degree 30 subfields of B. As explained in the proofs of Propositions 7.3 and 7.4, these generators are then shown to be correct unconditionally, using Lemma 7.1.

The first version of the proof and of the computations was done with different code, which is archived in the repository. We have rerun all of these computations with Magma V2.30-1 and obtained the same results. Independently of them, we have recomputed the sieve of Proposition 4.7 with a different implementation. In the first version the functions f_m were recomputed over each residue field and the residue classes modulo 4356 were lifted one prime at a time, while in `code/sieve_bruteforce.m` we reduce the functions f_m computed over K and run through all the residue classes modulo 4356. We have also recomputed the Selmer groups of Proposition 7.4 using only the standard Magma intrinsics, while the first version used a modified copy of Magma's implementation of descent on cyclic covers [12]. Both computations of the even Selmer groups give the same dimensions $5, 5, 4, 4$. The Selmer groups of Proposition 7.3 were computed only once, with the code `code/odd_selmer.m`, but with two different precisions.

We also ran the following supplementary checks, which the proofs do not need. For $n_0 \in \{-1, 1, 3\}$ and $n = n_0 + 4356$ and $n = n_0 + 11 \cdot 4356$ we computed the solutions w of (4.1) in the completions of K, and checked that the valuations of $X(P) - a$ and the leading vectors after the divisions by λ in the proof of Proposition 8.3 are as predicted (see `code/odd_depth_examples.m`). We checked that the points $[P_0 - \infty]$ have infinite order (see `code/nontorsion.m`).

References

[1] S. Arango-Piñeros and D. Zureick-Brown, *7-adic Galois representations of elliptic curves over the rationals via Kummer descent*, 2026. preprint, https://arxiv.org/abs/2610.06521.

[2] J. S. Balakrishnan, L. A. Betts, D. R. Hast, A. Jha, and J. S. Müller, *Rational points on the non-split Cartan modular curve of level 27 and quadratic Chabauty over number fields*, (2025). preprint, https://arxiv.org/abs/2501.07833.

[3] Y. Bilu, P. Parent, and M. Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble), 63 (2013), pp. 957–984.

[4] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, vol. 21 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Springer-Verlag, Berlin, 1990.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265.

[6] L. Furio and D. Lombardo, *On 7-adic Galois representations for elliptic curves over $\mathbb{Q}$*, Proc. Lond. Math. Soc. (3), 133 (2026), p. Paper No. e70193.

[7] G. Ligozat, *Courbes modulaires de niveau 11*, in Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), vol. 601 of Lecture Notes in Math., Springer, Berlin, 1977, pp. 149–237.

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

[9] A. M. Odlyzko, *Discriminant bounds*, 1976. Unpublished tables, November 29, 1976. Table 4: https://www-users.cse.umn.edu/~odlyzko/unpublished/discr.bound.table4, description: https://www-users.cse.umn.edu/~odlyzko/unpublished/discr.bound.tables.txt.

[10] J. Rouse, A. V. Sutherland, and D. Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight)*, Forum Math. Sigma, 10 (2022), pp. Paper No. e62, 63 pp.

[11] E. F. Schaefer, *Class groups and Selmer groups*, J. Number Theory, 56 (1996), pp. 79–114.
[12] ———, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann., 310 (1998), pp. 447–471.
[13] R. Schoof and N. Tzanakis, *Integral points of a modular curve of level 11*, Acta Arith., 152 (2012), pp. 39–49.
[14] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., 15 (1972), pp. 259–331.
[15] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106 of Graduate Texts in Mathematics, Springer, Dordrecht, second ed., 2009.
[16] M. Stoll, *Chabauty without the Mordell–Weil group*, in Algorithmic and experimental methods in algebra, geometry, and number theory, Springer, Cham, 2017, pp. 623–663.
[17] The LMFDB Collaboration, *The L-functions and modular forms database*, 2026. https://www.lmfdb.org.
[18] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, 2015. preprint, https://arxiv.org/abs/1508.07660.

Department of Mathematics, University of Massachusetts Amherst, Amherst, MA 01003, USA
Email address: santiago.arango.pineros@gmail.com

University of Zagreb Faculty of Science, Department of Mathematics, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: fnajman@math.hr

Department of Mathematics, Amherst College, 31 Quadrangle Dr., Amherst, MA 01002, USA
Email address: dzureickbrown@amherst.edu