Max-Planck-Institut für Mathematik
Bonn

Locally imprimitive points on elliptic curves

by

Nathan Jones
Francesco Pappalardi
Peter Stevenhagen

Max-Planck-Institut für Mathematik
Preprint Series 2023 (9)

Date of submission: May 28, 2023

Locally imprimitive points on elliptic curves

by

Nathan Jones
Francesco Pappalardi
Peter Stevenhagen

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics, Statistics
and Computer Science
University of Illinois at Chicago
851 S. Morgan St., 322 SEO
Chicago, IL 60607
USA

Dipartimento di Matematica
Università Roma Tre
Largo S. L. Murialdo 1
00146 Rome
Italy

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
The Netherlands

MPIM 23-9

LOCALLY IMPRIMITIVE POINTS ON ELLIPTIC CURVES

NATHAN JONES, FRANCESCO PAPPALARDI, AND PETER STEVENHAGEN

Abstract. Under GRH, any element in the multiplicative group of a number field K that is globally primitive (i.e., not a perfect power in K^*) is a primitive root modulo a set of primes of K of positive density.

For elliptic curves E/K that are known to have infinitely many primes $\mathfrak{p}$ of cyclic reduction, possibly under GRH, a globally primitive point $P \in E(K)$ may fail to generate any of the point groups $E(k_\mathfrak{p})$. We describe this phenomenon in terms of an associated Galois representation $\rho_{E/K,P} : G_K \to \mathrm{GL}_3(\widehat{\mathbf{Z}})$, and use it to construct non-trivial examples of global points on elliptic curves that are locally imprimitive.

1. Introduction

Under the Generalized Riemann Hypothesis (GRH), every non-zero rational number that is not -1 or a square is a primitive root modulo infinitely many primes p. This was proved in 1967 by Hooley [5], forty years after Artin had stated it as a conjecture. For general number fields K, there are counterexamples to the direct analogue of this statement, i.e., number fields K with non-torsion elements $x \in K^*$ that are not ℓ-th powers for any prime ℓ for which K contains a primitive ℓ-th root of unity, but that are nevertheless a primitive root in only finitely many residue class fields $k_\mathfrak{p}$. The direct analogue of Artin's conjecture does however hold for $x \in K^*$ that are *globally primitive*, i.e., not in $K^{*\ell}$ for any prime ℓ.

Theorem 1.1. *Let K be a number field and $x \in K^*$ globally primitive, and assume GRH. Then x is a primitive root modulo $\mathfrak{p}$ for a set primes $\mathfrak{p}$ of K of positive density.*

Informally stated: *globally primitive* elements in K^* are *locally primitive* in $k_\mathfrak{p}^*$ at infinitely many places $\mathfrak{p}$, with an element being 'primitive' in K^* or $k_\mathfrak{p}^*$ meaning that it generates a subgroup that is *not* contained in a strictly larger cyclic subgroup of K^* or $k_\mathfrak{p}^*$. Section 3 provides a proof of Theorem 1.1, and counterexamples to stronger statements.

Now replace the multiplicative group K^* by the point group $E(K)$ of an elliptic curve E/K, and the unit group $k_\mathfrak{p}^*$ of the residue class field at $\mathfrak{p}$ by the point group $E(k_\mathfrak{p})$ at the primes of good reduction $\mathfrak{p}$ of E. Then we can add two natural questions to Artin's to obtain the following three problems: for a number field K, determine the infinitude (or natural density) of the set of primes $\mathfrak{p}$ in K for which

I. (Artin) a given element $x \in K^*$ is a primitive root modulo $\mathfrak{p}$, i.e., $k_\mathfrak{p}^* = \langle \overline{x} \rangle$;
II. (Serre [15]) a given elliptic curve E/K has cyclic reduction modulo $\mathfrak{p}$;
III. (Lang-Trotter [8]) a given point $P \in E(K)$ generates the group $E(k_\mathfrak{p})$ at $\mathfrak{p}$.

Date: May 28, 2023.
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.
Key words and phrases. Elliptic curves, primitive points, Galois representation.

We will refer to the cases I, II, and III as the *multiplicative primitive root*, the *cyclic reduction* and the *elliptic primitive root* case, and denote the corresponding sets of primes by $S_{K,x}$, $S_{E/K}$, and $S_{E/K,P}$, respectively. By definition, the finitely many primes of bad reduction for which we have $\mathrm{ord}_{\mathfrak{p}}(x) \neq 0$ (in case I) or $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) \neq 0$ (in case II and III, with Δ_E the discriminant of E) are excluded from these sets. Note that we have an obvious inclusion $S_{E/K,P} \subset S_{E/K}$.

In each of the three cases, we have a group theoretical statement that can be checked prime-wise at the primes ℓ dividing the order of the groups $k_{\mathfrak{p}}^*$ and $E(k_{\mathfrak{p}})$ involved. The statement 'at ℓ' has a translation in terms of the splitting behavior of $\mathfrak{p}$ in a finite Galois extension $K \subset K_\ell$ that we describe in Section 2. Combining the requirements for all ℓ leads to (conjectural) density statements based on the Chebotarev density theorem [16].

Imposing infinitely many splitting conditions, one for each prime ℓ, leads to analytic problems with error terms that have been mastered under assumption of GRH in Cases I [1,5,9] and II [2,3,15], and that remain open in Case III. In each case, there is a conjectural density $\delta_{K,x}$, $\delta_{E/K}$, or $\delta_{E/K,P}$ that is an upper bound for the upper density of the set of primes $\mathfrak{p}$. Proving unconditionally that the set is infinite in case the conjectural density is positive is an open problem. If it is zero, we can however prove unconditionally that the corresponding set of primes is finite.

This paper focuses on the vanishing of $\delta_{E/K,P}$ in the elliptic primitive root case, which is much more subtle than the vanishing in the cases I and II. We call a global point $P \in E(K)$ *locally imprimitive* if it is a generator of the local point group $E(k_{\mathfrak{p}})$ for only finitely many primes $\mathfrak{p}$ of K. Our analysis will yield 'elliptic counterexamples' $(E/K, P)$ to Theorem 1.1, i.e., elliptic curves E/K for which the cyclic reduction density $\delta_{E/K}$ is positive but for which a globally primitive point $P \in E(K)$ is locally imprimitive.

Just as in the multiplicative primitive root and the cyclic reduction cases I and II, obstructions to local primitivity of a point $P \in E(K)$ become visible in an associated Galois representation. In the elliptic primitive root case, the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ of the number field K acts on the subgroup of $E(\overline{K})$ consisting of the points $Q \in E(\overline{K})$ satisfying $kQ \in \langle P \rangle \subset E(K)$ for some $k \in \mathbf{Z}_{\geq 1}$. This yields a representation $\rho_{E/K,P} : G_K \to \mathrm{GL}_3(\widehat{\mathbf{Z}})$. Just as in the two other cases [2], it suffices to consider the residual representation

$$\overline{\rho}_{E,P} : G_K \to \mathrm{GL}_3(\widehat{\mathbf{Z}}) \to \mathrm{GL}_3(\mathbf{Z}/N\mathbf{Z}) \tag{1}$$

modulo a suitable squarefree integer N that is divisible by all 'critical primes'.

Unlike the cases I and II, case III already allows non-trivial obstructions to local primitivity at prime level $N = \ell$. In the multiplicative case I, the index $[k_{\mathfrak{p}}^* : \langle \overline{x} \rangle]$ can only be divisible by ℓ for almost all $\mathfrak{p}$ for the 'trivial reason' that K contains an ℓ-th root of unity and x is an ℓ-th power in K^*. In the cyclic reduction case II, the group $E(k_{\mathfrak{p}})$ can only have a non-cyclic ℓ-part for almost all $\mathfrak{p}$ for the 'trivial reason' that the full ℓ-torsion of E/K is K-rational. In the elliptic primitive root case III however, there is a third reason why a point $P \in E(K)$ can be *locally ℓ-imprimitive*, meaning that ℓ divides the index $[E(k_{\mathfrak{p}}) : \langle \overline{P} \rangle]$ for all but finitely many $\mathfrak{p}$. It is a less obvious one, and it was numerically discovered in 2015 in the case $\ell = 2$ by Meleleo [11], who restricted himself to the basic case $K = \mathbf{Q}$.

Theorem 1.2. *Let $P \in E(K)$ be a non-torsion point of an elliptic curve E defined over a number field K, and ℓ a prime number. Then P is locally ℓ-imprimitive if and only if at least at least one of the following conditions holds*

A. *$E(K)$ contains a torsion point of order ℓ and $P \in \ell \cdot E(K)$;*
B. *E has complete rational ℓ-torsion over K;*
C. *there exists an isogeny $\phi : E' \to E$ defined over K with kernel generated by a torsion point of $E'(K)$ of order ℓ and $P \in \phi[E'(K)]$.*

Condition A in Theorem 1.2 is the analogue of the trivial condition from case I: if $E(K)$ has non-trivial ℓ-torsion, then almost all $E(k_\mathfrak{p})$ are groups of order divisible by ℓ, and for these $\mathfrak{p}$ a point $P \in \ell \cdot E(K)$ will have its reduction in the subgroup $\ell E(k_\mathfrak{p}) \subset E(k_\mathfrak{p})$ of index divisible by ℓ. Condition B bears no relation to P, and is well known from case II: non-cyclicity of the ℓ-part of the global torsion subgroup $E(K)^{\mathrm{tor}}$ implies non-cyclicity of the ℓ-part of $E(k_\mathfrak{p})$ at almost all $\mathfrak{p}$. At these $\mathfrak{p}$, no single point P can generate it.

Condition C has no analogue in the multiplicative primitive root case, and it is a truly different condition as it includes cases in which we have both $P \notin \ell \cdot E(K)$ and $E[\ell](K) = 0$. If it holds, the dual isogeny $\widehat{\phi} : E \to E'$ maps P into $\ell E'(K)$, and the pair (E, P) is ℓ-isogenous to the curve-point pair $(E', \widehat{\phi}(P))$ satisfying Condition A. We call a locally ℓ-imprimitive non-torsion point $P \in E(K)$ *non-trivial* if Condition C is satisfied, but *not* Condition A or B.

By Theorem 1.2, non-trivial locally 2-imprimitive points $P \in E(K)$ can only exist for E/K having a single K-rational point of order 2, i.e., a 2-torsion subgroup of order $\#E(K)[2] \neq 1, 4$. Examples of such points are actually surprisingly abundant.

Theorem 1.3. *Let E/K be any elliptic curve with $\#E(K)[2] = 2$. Then there are infinitely many quadratic twists of E over K that have a non-trivial locally 2-imprimitive point.*

The proof of this Theorem, which we give in Section 5, uses the fact that it is easy to create non-torsion points on twists of E, and exploits the particularly explicit description of K-rational 2-isogenies.

For primes $\ell > 2$, it is harder to obtain families of elliptic curves with points of infinite order that are locally ℓ-imprimitive in non-trivial ways. In Section 6 we provide an approach in the case $\ell = 3$. It can be extended to higher values of ℓ (Section 7), but the examples rapidly become unwieldy.

Non-torsion points that are locally imprimitive but not locally ℓ-imprimitive for any single prime ℓ do exist, but they are not easily found. They involve restrictions arising from reductions of $\rho_{E/K,P}$ of composite level caused by non-trivial *entanglement* between the fields K_ℓ. In the context of the easier cyclic reduction case II, this is discussed in [2], and we present a first type of examples for our Lang-Trotter case III in our final Section 8. Such higher level obstructions will be explored in more detail in a forthcoming paper.

Acknowledgements. *All authors received support from the Max-Planck-Institut für Mathematik in Bonn while working on this paper. They thank the institute for its financial support and for its very inspiring atmosphere.*

2. Characterization by splitting conditions

In each of the three cases discussed in the introduction, we can characterize the corresponding sets of primes $S_{K,x}$, $S_{E/K}$, and $S_{E/K,P}$ of K in terms of the splitting behaviour of their elements $\mathfrak{p}$ in suitable extensions $K \subset K_\ell$, with ℓ ranging over all prime numbers.

I. Multiplicative primitive root case. Let K be a number field and $x \in K^*$ non-torsion. Define $K_m = \mathbf{Q}(\zeta_m, \sqrt[m]{x})$ for $m \in \mathbf{Z}_{\geq 1}$ as the 'm-division field of x', i.e., the splitting field over K of the polynomial $X^m - x \in K[X]$. If $\mathfrak{p}$ is a prime of K of characteristic p for which x is a $\mathfrak{p}$-adic unit, the index $[k_\mathfrak{p}^* : \langle \overline{x} \rangle]$ is divisible by a prime $\ell \neq p$ if and only if $\mathfrak{p}$ splits completely in $K \subset K_\ell$.

Note that $[k_\mathfrak{p}^* : \langle \overline{x} \rangle]$ is never divisible by $p = \mathrm{char}(\mathfrak{p})$, even though $\mathfrak{p}$ may split completely in K_p. Example: $x = 17$ is a primitive root modulo the prime $\mathfrak{p}_3$ of norm 3 in $K = \mathbf{Q}(\sqrt{-21})$, but $\mathfrak{p}_3$ splits completely in the sextic extension

$$K \subset K_3 = K(\zeta_3, \sqrt[3]{17}) = K(\sqrt{7}, \sqrt[3]{17}).$$

This can however only happen for primes $\mathfrak{p}|2\Delta_K$, with Δ_K the discriminant of K, since $K \subset K_p$ is ramified at all $\mathfrak{p}|p$ for p coprime to $2\Delta_K$. In other words: for almost all $\mathfrak{p}$, the 'condition at ℓ' in the following Lemma is automatically satisfied at $\ell = \mathrm{char}\,\mathfrak{p}$.

Lemma 2.1. *For $\mathfrak{p}$ a prime of K outside the support of x, we have $k_\mathfrak{p}^* = \langle \overline{x} \rangle$ if and only if $\mathfrak{p}$ does not split completely in $K \subset K_\ell$ for any prime $\ell \neq \mathrm{char}\,\mathfrak{p}$.* □

By Lemma 2.1, the set $S_{K,x}$ of primes in K for which x is a primitive root is up to finitely many primes equal to the set of primes that do not split completely in $K \subset K_\ell$ for any prime ℓ. For $m \in \mathbf{Z}_{\geq 1}$, the set of primes $\mathfrak{p}$ of K that split completely in $K \subset K_m$ has natural density $1/[K_m : K]$. Under GRH, it follows from [9] that the set $S_{K,x}$ has a natural density that is given by the inclusion-exclusion sum

$$\delta_{K,x} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]} \tag{2}$$

that converges slowly, but that can be rewritten in 'factored form' as

$$\delta_{K,x} = \sum_{m|N} \frac{\mu(m)}{[K_m : K]} \cdot \prod_{\ell \nmid N \text{ prime}} (1 - \frac{1}{\ell(\ell-1)}). \tag{3}$$

Here we can take for N any integer divisible by the primes in some finite set of *critical primes*. One may take for this set the set of primes that are either in the support of x or divide $2\Delta_K$, together with those primes ℓ for which x is in $K^{*\ell}$. The essential feature of N is that the family $\{K_\ell\}_{\ell \nmid N}$ of 'ℓ-division fields of x outside N' is a linearly disjoint family over K with each K_ℓ having the full Galois group $\mathrm{Gal}(K_\ell/K) \cong \mathrm{Aff}_1(\mathbf{F}_\ell) = \mathbf{F}_\ell \rtimes \mathbf{F}_\ell^*$ of order $\ell(\ell-1)$, and that the compositum L of the fields in this family satisfies $L \cap K_N = K$.

II. Cyclic reduction case. For an elliptic curve E/K, we consider the set $S_{E/K}$ of primes of cyclic reduction of E, i.e., the primes $\mathfrak{p}$ of K for which E has good reduction and the reduced elliptic curve point group $E(k_\mathfrak{p})$ is cyclic. The condition that E have good reduction modulo $\mathfrak{p}$ only excludes the finitely many primes dividing the discriminant Δ_E of E.

For $m \in \mathbf{Z}_{\geq 1}$, we define $K_m = K(E[m](\overline{\mathbf{Q}}))$ in this case to be the m-division field of E over K. The following elementary lemma [2, Corollary 2.2] is the analogue of Lemma 2.1. It expresses the fact that a finite abelian group is cyclic if and only if its ℓ-primary part is cyclic for all primes ℓ.

Lemma 2.2. *A prime $\mathfrak{p}$ of good reduction of E/K is a prime of cyclic reduction if and only if $\mathfrak{p}$ does not split completely in $K \subset K_\ell$ for any prime $\ell \neq \operatorname{char} \mathfrak{p}$.* □

As in the multiplicative Case I, cyclicity of the p-primary part of the groups $E(k_\mathfrak{p})$ is automatic for $p = \operatorname{char}(\mathfrak{p})$. Also here, total splitting of $\mathfrak{p}$ in non-trivial extensions $K \subset K_p$ for $p = \operatorname{char} \mathfrak{p}$ does occur: it suffices to base change any elliptic curve E/K with $K \subset K_p = K[X]/(f)$ non-trivial by an extension $K \subset L = K[X]/(g)$ with f and g polynomials of the same degree that are $\mathfrak{p}$-adically close, but with g Eisenstein at a prime $\mathfrak{q}$ that is unramified in $K \subset K_p$. For E/L, the non-trivial extension $L \subset L_p$ will be totally split at all primes dividing $\mathfrak{p}$. Again, this can happen only at primes $\mathfrak{p}|2\Delta_K$, as otherwise $K \subset K_p$ will be ramified at all primes $\mathfrak{p}$ of characteristic p by the fact that K_p contains ζ_p. Thus, for almost all $\mathfrak{p}$, the 'condition at ℓ' in Lemma 2.2 is again automatically satisfied at $\ell = \operatorname{char} \mathfrak{p}$. The finitely many primes dividing $2\Delta_K$ are clearly irrelevant when dealing with the density of the set $S_{E/K}$, which, just like in the previous case, coincides up to finitely many primes with the set of primes $\mathfrak{p}$ of K that do not split completely in $K \subset K_\ell$ for any prime ℓ.

Under GRH, the density of $S_{E/K}$ is again given [2, Section 2] by an inclusion-exclusion sum that we already know from (2):

$$\delta_{E/K} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]}. \tag{4}$$

If E is without CM over $\overline{\mathbf{Q}}$, or has CM by an order $\mathcal{O} \subset K$, there is in each case a factorization of $\delta_{E/K}$ that is typographically identical to (2), provided that N is divisible by all primes from an appropriately defined finite set of critical primes [2, Theorems 1.1 and 1.2]. If E has CM by an order $\mathcal{O} \not\subset K$, there is a hybrid formula [2, Theorem 1.4] with different contributions from ordinary and supersingular primes.

A 'factorization formula' for $\delta_{K,x}$ and $\delta_{E/K}$ as in (3) shows that the vanishing of these densities is always caused by an obstruction at some finite level N. For such N, no element in $\operatorname{Gal}(K_N/K)$ restricts for all $\ell|N$ to a non-trivial element of $\operatorname{Gal}(K_\ell/K)$. As a consequence, there are no non-critical primes in $S_{K,x}$ or $S_{E/K}$: the Frobenius elements of such primes in $\operatorname{Gal}(K_N/K)$ cannot exist for group theoretical reasons.

An obstruction at prime level $N = \ell$, which means an equality $K = K_\ell$, amounts in the cases I and II to a 'trivial' reason that we already mentioned in the context of Conditions A and B in Theorem 1.2. For $K = \mathbf{Q}$, vanishing of $\delta_{\mathbf{Q},x}$ and $\delta_{E/\mathbf{Q}}$ only occurs if we have $K = K_\ell$ for a prime ℓ, which in this case has to be $\ell = 2$.

Over general number fields, vanishing may be caused by obstructions that occur *only* at composite levels. Typical examples can be constructed by base changing a non-vanishing example (K, x) or E/K to a suitable extension field $K \subset L$. Example 3.1 accomplishes vanishing of $\delta_{K,x}$ by an obstruction at level $30 = 2 \cdot 3 \cdot 5$ for the field $K = \mathbf{Q}(\sqrt{5})$ that does not arise at lower level by cleverly choosing x. In [2, Example 5.4] we find a base change of an elliptic curve $E/\mathbf{Q}$ to a field K of degree 48 with a similar level 30 obstruction to cyclic reduction.

III. Elliptic primitive root case. In addition to the elliptic curve E/K, we are now given a point $P \in E(K)$ of infinite order. We consider the set $S_{E/K,P}$ of primes $\mathfrak{p}$ of K for which E has cyclic reduction and the reduction of the point P modulo $\mathfrak{p}$ generates the group $E(k_\mathfrak{p})$. Note the obvious inclusion $S_{E/K,P} \subset S_{E/K}$.

For $m \in \mathbf{Z}_{\geq 1}$, we let $K_m = K(m^{-1}P)$ be the *m-division field of* P, i.e., the extension of K generated by the points of the subgroup of $E(\overline{K})$ defined as

$$\langle m^{-1}P \rangle = \{Q \in E(\overline{K}) : mQ \in \langle P \rangle\}.$$

Note that this extension K_m contains the m-division field of the elliptic curve E that we encountered in the cyclic reduction case II. The m-division field $K_m = K(m^{-1}P)$ of P is again unramified over K at primes $\mathfrak{p}$ of good reduction coprime to m. The proof of this fact is as for the m-division field of E: as the m-th roots $Q \in E(\overline{K})$ of P that generate K_m over K differ by m-torsion points, their reductions modulo a prime over $\mathfrak{p}$ remain different, so inertia acts trivially on the set of such Q.

The quotient group $V_m = \langle m^{-1}P \rangle / \langle P \rangle$ is a free module of rank 3 over $\mathbf{Z}/m\mathbf{Z}$. It comes with a natural linear action of the absolute Galois group G_K of K, and this mod-m Galois representation induces an embedding

$$G_m = \mathrm{Gal}(K_m/K) \hookrightarrow \mathrm{GL}(V_m) \cong \mathrm{GL}_3(\mathbf{Z}/m\mathbf{Z}). \tag{5}$$

As G_K stabilizes the rank 2 subspace $U_m = E[m](\overline{K}) \subset V_m$, this is a 'reducible' representation. Write $V_m = U_m \oplus (\mathbf{Z}/m\mathbf{Z}) \cdot \overline{Q}$ with $\overline{Q} = (Q \bmod \langle P \rangle) \in V_m$ the image of a point $Q \in E(\overline{K})$ satisfying $mQ = P$. We then have a split exact sequence

$$0 \to U_m \longrightarrow V_m \longrightarrow \mathbf{Z}/m\mathbf{Z} \cdot \overline{Q} \to 0$$

of free $\mathbf{Z}/m\mathbf{Z}$-modules that is split as a sequence of $(\mathbf{Z}/m\mathbf{Z})[G_m]$-modules if and only if we have $P \in m \cdot E(K)$. After choosing an $\mathbf{Z}/m\mathbf{Z}$-basis $\{T_1, T_2\}$ of U_m and extending it by some $\overline{Q}$ as above to a $\mathbf{Z}/m\mathbf{Z}$-basis for V_m, the matrix representation of $\sigma \in G_m$ becomes

$$\sigma = \sigma_{A,b} = \begin{pmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ 0 & 0 & 1 \end{pmatrix}, \tag{6}$$

in which the linear action of σ on U_m with respect to some $\mathbf{Z}/m\mathbf{Z}$-basis $\{T_1, T_2\}$ of U_m is described by $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}(U_m)$, and

$$b = b_1T_1 + b_2T_2 = \sigma Q - Q$$

is the translation action of σ on some chosen 'm-th root' Q of P with respect to that same basis. In other words, V_m gives a Galois representation of G_K with image $G_m \subset \mathrm{GL}(V_m)$ that is contained in the 2-dimensional affine group

$$\mathrm{Aff}_2(\mathbf{Z}/m\mathbf{Z}) = (\mathbf{Z}/m\mathbf{Z})^2 \rtimes \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}).$$

In the important case where $m = \ell$ is prime, we are in the classical situation of a 3-dimensional Galois representation over the finite field $\mathbf{F}_\ell$.

The analogue in the elliptic primitive root case of the Lemmas 2.1 and 2.2 is a little bit more involved. We have to impose a condition on the Frobenius elements $\mathrm{Frob}_{\mathfrak{p},\ell} \in G_\ell$ at all primes $\ell \neq \mathrm{char}\,\mathfrak{p}$ different from being *equal* to the identity element $\mathrm{id}_\ell \in G_\ell$: in this case it only needs to be 'sufficiently close' to it.

Lemma 2.3. *For $P \in E(K)$ of infinite order and $\mathfrak{p}$ a prime of good reduction of E of characteristic different from ℓ we have*

$$\ell | [E(k_\mathfrak{p}) : \langle \overline{P} \rangle] \quad \Longleftrightarrow \quad \mathrm{rank}(\mathrm{Frob}_{\mathfrak{p},\ell} - \mathrm{id}_\ell) \leq 1.$$

Proof. As all V_ℓ are 3-dimensional over $\mathbf{F}_\ell$, the condition $\mathrm{rank}(\mathrm{Frob}_{\mathfrak{p},\ell} - \mathrm{id}_\ell) \leq 1$ means that $\mathrm{Frob}_{\mathfrak{p},\ell}$ is the identity on an $\mathbf{F}_\ell$-subspace of V_ℓ of dimension at least 2. If it equals U_ℓ, then $E(k_\mathfrak{p})$ has complete ℓ-torsion of order ℓ^2 and every cyclic subgroup $\langle \overline{P} \rangle$ has index divisible by ℓ. If not, it intersects U_ℓ in a 1-dimensional subspace, so we have a point of order ℓ in $E(k_\mathfrak{p})$ and a point $\overline{Q} \in E(k_\mathfrak{p})$ satisfying $\ell \overline{Q} = \overline{P}$. This also implies that $[E(k_\mathfrak{p}) : \langle \overline{P} \rangle]$ is divisible by ℓ.

Conversely, if ℓ divides $[E(k_\mathfrak{p}) : \langle \overline{P} \rangle]$ then either $E(k_\mathfrak{p})$ has complete ℓ-torsion or $E(k_\mathfrak{p})$ has a cyclic non-trivial ℓ-part and $\overline{P}$ is contained in $\ell \cdot E(k_\mathfrak{p})$. In both cases $\mathrm{Frob}_{\mathfrak{p},\ell}$ is the identity on a subspace of V_ℓ of dimension at least 2. □

Corollary 2.4. *Let $P \in E(K)$ be of infinite order and $\mathfrak{p}$ a prime of good reduction of E of prime norm $\mathrm{char}\, \mathfrak{p} > 5$ for which $\overline{P} \neq \overline{O} \in E(k_\mathfrak{p})$. Then we have*

$$E(k_\mathfrak{p}) = \langle \overline{P} \rangle \quad \Longleftrightarrow \quad \mathrm{rank}(\mathrm{Frob}_{\mathfrak{p},\ell} - \mathrm{id}_\ell) \geq 2 \textit{ for all primes } \ell.$$

Proof. By Lemma 2.3, the condition on the right side says that $p = \mathrm{char}\, \mathfrak{p}$ is the only possible prime divisor of the index $[E(k_\mathfrak{p}) : \langle \overline{P} \rangle]$. For a prime $\mathfrak{p}$ of degree one, i.e., of prime norm p, the index of a subgroup of $E(k_\mathfrak{p}) = E(\mathbf{F}_p)$ can only be divisible by p if it is the trivial subgroup, as we have $\# E(\mathbf{F}_p) < p + 1 + 2\sqrt{p} < 2p$ for $p > 5$. So we have $E(k_\mathfrak{p}) = \langle \overline{P} \rangle$ unless $\mathfrak{p}$ is a prime for which we have $\overline{P} = \overline{O} \in E(k_\mathfrak{p})$. As we have $P \neq O \in E(K)$, this happens only for finitely many $\mathfrak{p}$. □

In density questions, we can disregard any finite set of primes, and more generally a set of primes of density zero. The set of primes in a number field of degree bigger than one is such a zero density set. For this reason, the density of the set $S_{E/K,P}$ only depends on the primes of degree one outside any finite set of 'critical primes' that it contains. Thus, Corollary 2.4 can play the same role as the Lemmas 2.1 and 2.2.

In order to express the 'heuristical density' $\delta_{E/K,P}$ of $S_{E/K,P}$, we define the subset $S_\ell \subset G_\ell = \mathrm{Gal}(K_\ell/K)$ of 'bad' elements at the prime ℓ as

$$S_\ell = \{\sigma \in G_\ell : \mathrm{rank}_{\mathbf{F}_\ell}(\sigma - \mathrm{id}_\ell) \leq 1\}.$$

For arbitrary $m \in \mathbf{Z}_{\geq 1}$ and $\ell | m$ prime we let $\pi_{m,\ell} : G_m \to G_\ell$ be the natural restriction map, and define $S_m \subset G_m$ as

$$S_m = \bigcup_{\ell | m} \pi_{m,\ell}^{-1}[S_\ell].$$

With $s_m = \# S_m$ denoting the cardinality of S_m, the *elliptic primitive root density* is now given by the inclusion-exclusion sum

$$\delta_{E,P} = \sum_{m=1}^{\infty} \frac{\mu(m) s_m}{[K_m : K]}. \tag{7}$$

It is the elliptic analogue of the multiplicative primitive root density (2). It is an upper density for $S_{E/K,P}$ that has not been proven to be its true density in cases with $\delta_{E/K,P} > 0$, not even under GRH.

We can compute $\delta_{E/K,P}$ using the methods of [2]. This is not directly relevant for us, as our focus in this paper is on cases where $\delta_{E/K,P}$ vanishes in 'non-trivial' ways, so we will merely sketch this here. In order to obtain a factorization

$$\delta_{E/K,P} = \sum_{m|N} \frac{\mu(m)s_m}{[K_m : K]} \cdot \prod_{\ell\nmid N \text{ prime}} (1 - \frac{s_\ell}{[K_\ell : K]}). \tag{8}$$

as in (3), it suffices to have an 'open-image theorem' for the Galois representation $\rho_{E,P}$ arising from the action of G_K on the subgroup

$$R_P = \{Q \in E(\overline{K}) : mQ \in \langle P\rangle \text{ for some } m \in \mathbf{Z}_{\geq 1}\} \cong (\mathbf{Q}/\mathbf{Z})^2 \times \mathbf{Q}$$

of $E(\overline{K})$ generated by all the roots of P in $E(\overline{K})$. The Galois action of G_K on the quotient group $V = R_P/\langle P\rangle$, which is free of rank 3 over $\mathbf{Q}/\mathbf{Z}$, gives rise to a Galois representation

$$\rho_{E,P} : G_K \longrightarrow \mathrm{Aut}(V) \cong \mathrm{GL}_3(\widehat{\mathbf{Z}}),$$

which has (5) as its mod-m representation. It factors via $\mathrm{Gal}(K(R_P)/K)$, with $K(R_P) = \bigcup_m K_m \subset \overline{K}$ the compositum of all 'm-division fields' of P inside $\overline{K}$. The group $U = E(\overline{K})^{\mathrm{tor}} \cong (\mathbf{Q}/\mathbf{Z})^2$ is a direct summand of V, and if we choose a $\mathbf{Q}/\mathbf{Z}$-basis for $V = U \oplus \mathbf{Q}/\mathbf{Z}$ as we did for $V_m = U_m \oplus \mathbf{Z}/m\mathbf{Z} \cdot \overline{Q}$, the image of $\rho_{E,P}$ is in $\mathrm{Aff}_2(\widehat{\mathbf{Z}}) = \widehat{\mathbf{Z}}^2 \rtimes \mathrm{GL}_2(\widehat{\mathbf{Z}})$. For E without CM over $\overline{K}$, one deduces from Serre's open image theorem that this image is of finite index in $\mathrm{Aff}_2(\widehat{\mathbf{Z}})$, which yields (8) for any N divisible by some finite product $N_{E/K,P} \in \mathbf{Z}_{>0}$ of critical primes. As in [2], one deduces that all non-CM-densities $\delta_{E,P}$ are rational multiples of a universal constant. If E has CM over $\overline{K}$ by an order $\mathcal{O} \subset K$, one replaces $\mathrm{Aff}_2(\widehat{\mathbf{Z}})$ by $\mathrm{Aff}_1(\mathcal{O})$, and in the case of CM by an order $\mathcal{O} \not\subset K$, one separates the contribution of ordinary and supersingular primes of E/K as in [2].

3. Multiplicative primitivity

Before focusing on the Lang-Trotter case III, we first settle the multiplicative primitive root case: under GRH, globally primitive elements $x \in K^*$ are locally primitive for a set of primes of positive density $\delta_{K,x}$.

Proof of Theorem 1.1. Let $x \in K^*$ be globally primitive. As we assume GRH, the primitive root density for $x \in K^*$ exists and is equal to $\delta_{K,x}$ defined in (2), by the results of [9]. We need to show that $\delta_{K,x}$ does not vanish. In view of the factorization formula (3), it suffices to show that for any squarefree integer $N > 1$, the fraction $\sum_{m|N} \mu(m)[K_m : K]^{-1}$ of elements in $\mathrm{Gal}(K_N/K)$ that have non-trivial restriction to K_ℓ for all primes $\ell|N$ does not vanish.

As x is not an ℓ-th power in K^*, the polynomial $X^\ell - x$ is irreducible in $K[X]$. It therefore gives rise to an extension $K \subset K_\ell = \mathrm{Split}_K(X^\ell - x) = K(\zeta_\ell, \sqrt[\ell]{x})$ of degree $\ell \cdot c_\ell$, with c_ℓ a divisor of $\ell - 1$. If ℓ is the largest prime dividing the squarefree number N, we conclude that $K_{N/\ell} \subset K_N$ is Galois of degree divisible by ℓ.

Showing that $\mathrm{Gal}(K_N/K)$ contains an element of the required type is now easily done by induction on the number of of primes dividing the squarefree integer $N > 1$. If N is prime, then $\mathrm{Gal}(K_N/K)$ contains a non-trivial element of order N. If not, we let ℓ be the largest prime dividing N and observe that an automorphism of the required type in $\mathrm{Gal}(K_{N/\ell}/K)$, which exists by the induction hypothesis, always possesses an extension to the compositum K_N of $K_{N/\ell}$ and K_ℓ that is non-trivial on K_ℓ. □

The assumption of global primitivity in Theorem 1.1 cannot be weakened to the assumption $K \neq K_\ell$ for all prime number ℓ. The resulting stronger statement is correct for $K = \mathbf{Q}$, but counterexamples to it exist for general number fields K, as the cyclotomic extensions $K \subset K(\zeta_\ell)$ for different ℓ may all be non-trivial, but 'entangled' over K. The following counterexample takes K to be quadratic.

Example 3.1. The quadratic field $K = \mathbf{Q}(\sqrt{5})$ has fundamental unit $\varepsilon = \frac{1+\sqrt{5}}{2}$. The element $\pi = \varepsilon^2 - 4 = \frac{-5+\sqrt{5}}{2} \in K$ has norm 5 and is a square modulo 4. The field $K(\sqrt{\pi})$, which is cyclic of degree 4 over $\mathbf{Q}$ and unramified outside 5, is therefore equal to $K(\zeta_5)$. Take $y = -3\pi \in K$ and choose $x = y^{15}$. We then have

$$K_3 = K(\zeta_3) = K(\sqrt{-3}) \qquad \text{and} \qquad K_5 = K(\zeta_5) = K(\sqrt{\pi}),$$

so $K_2 = K(\sqrt{x}) = K(\sqrt{y}) = K(\sqrt{-3\pi})$ and K_3 and K_5 are three different quadratic extensions of K contained in the biquadratic extension $K \subset K_6 = K_{10} = K_{15} = K_{30}$. We have $\mu_K = \{\pm 1\}$ and, even though x is not a square in K^*, there is exactly one prime of K modulo which x is a primitive root: (2). For the primes $\mathfrak{p} = (3)$ and $\mathfrak{p} = (\sqrt{5})$ the element x is not in $k_\mathfrak{p}^*$, and for all primes of characteristic $p > 5$ the index $[\mathbf{F}_p : \langle \overline{x} \rangle]$ is divisible by at least one of 2, 3 or 5. Indeed, no prime can be inert in all three quadratic subfields of an extension with group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

The simple observation that no prime $\mathfrak{p}$ of a number field K can be inert in all three quadratic subextensions of an extension $K \subset L$ with group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ underlies many 'entanglement obstructions', including the one in our final Section 8.

4. Proof of Theorem 1.2

In the Lang-Trotter situation, Lemma 2.3 shows that a point $P \in E(K)$ will generate a subgroup of the local point group $E(k_\mathfrak{p})$ of index divisible by ℓ when $\mathrm{Frob}_{\mathfrak{p},\ell} \in G_\ell$ pointwise fixes a 2-dimensional subspace of the 3-dimensional $\mathbf{F}_\ell$-vector space V_ℓ. Vanishing of the density $\delta_{E/K,P}$ can therefore occur 'because of K_ℓ' in cases where $G_\ell = \mathrm{Gal}(K_\ell/K)$ is non-trivial, but only contains elements that pointwise fix a 2-dimensional subspace of V_ℓ.

Our proof of Theorem 1.2 is based on a general lemma that we phrase and prove in the generality that was suggested to us by Hendrik Lenstra. It describes the linear group actions on vector spaces of finite dimension over arbitrary fields that have 'many fixpoints' in the sense of the 3-dimensional example V_ℓ that we have at hand.

Let V be any vector space on which a group G acts linearly, and denote by

$$V^G = \{v \in V : \sigma v = v \text{ for all } \sigma \in G\} \qquad \text{and} \qquad V_G = V/(\textstyle\sum_{\sigma \in G} (\sigma - 1)V)$$

the maximal subspace and quotient space of V on which G acts trivially. For every $\sigma \in G$, we have an exact sequence of vector spaces

$$0 \longrightarrow V^{\langle \sigma \rangle} \longrightarrow V \xrightarrow{\sigma - 1} V \longrightarrow V/(\sigma - 1)V \to 0$$

showing that for V of finite dimension n, we have

$$\dim V^{\langle \sigma \rangle} \geq n - 1 \quad \Longleftrightarrow \quad \dim(\sigma - 1)V \leq 1. \tag{9}$$

Lemma 4.1. *Let G be a group acting linearly on a vector space V of dimension $n \in \mathbf{Z}_{\geq 0}$. Then the following are equivalent:*

(1) $\dim V^{\langle\sigma\rangle} \geq n-1$ *for all* $\sigma \in G$*;*
(2) $\dim V^G \geq n-1$ *or* $\dim V_G \geq n-1$.

Proof. The implication (2) ⇒ (1) is immediate, as the inequality $\dim V_G \geq n-1$ implies that, for all $\sigma \in G$, we have $\dim(\sigma-1)V \leq 1$ and, by (9), $\dim V^{\langle\sigma\rangle} \geq n-1$.

For (1) ⇒ (2), we can assume there exists $\sigma \in G$ acting non-trivially on V, and define subgroups $A_\sigma, B_\sigma \subset G$ by

$$A_\sigma = \{\tau \in G \colon V^{\langle\tau\rangle} \supset V^{\langle\sigma\rangle}\} \qquad \text{and} \qquad B_\sigma = \{\tau \in G \colon (\tau-1)V \subset (\sigma-1)V\}.$$

The equality $A_\sigma = G$ implies that $V^G = V^{\langle\sigma\rangle}$ has dimension $n-1$, and the equality $B_\sigma = G$ implies that $V_G = V/(\sigma-1)V$ has dimension $n-1$. In order to show that we have one of these equalities, and therefore (2), we argue by contradiction. Assume A_σ and B_σ are *strict* subgroups of G, and pick $\tau \in G$ outside $A_\sigma \cup B_\sigma$. Then there exist $s \in V^{\langle\sigma\rangle} \setminus V^{\langle\tau\rangle}$ and $t \in V^{\langle\tau\rangle} \setminus V^{\langle\sigma\rangle}$, and $(\sigma-1)V$ and $(\tau-1)V$ are *different* 1-dimensional subspaces of V spanned by $(\sigma-1)t$ and $(\tau-1)s$, respectively.

The subspace $(\tau\sigma-1)V$ is 1-dimensional and spanned by $(\tau\sigma-1)s = (\tau-1)s$, so it equals $(\tau-1)V$. It contains $(\tau\sigma-1)t = \tau(\sigma-1)t$, but since τ acts on $(\sigma-1)t \notin (\tau-1)V$ by translation along a vector in $(\tau-1)V$, we have $\tau(\sigma-1)t \notin (\tau-1)V$. Contradiction. □

For those who like to think of Lemma 4.1 in terms of matrices, Condition (1) means that every element of G has a matrix representation with respect to a suitable basis that, according to (9), can be given in one of the equivalent forms

$$\left(\begin{array}{ccc|c} & & & * \\ & I_{n-1} & & \vdots \\ & & & * \\ \hline 0 & \cdots & 0 & * \end{array}\right) \qquad \text{or} \qquad \left(\begin{array}{c|ccc} * & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{array}\right). \tag{10}$$

The first form shows $n-1$ linearly independent vectors in $V^{\langle\sigma\rangle}$, the second starts from a vector spanning $(\sigma-1)V$. The lemma then states that under this condition, a *single* basis for V can be chosen such that either all elements of G have a matrix representation of the first form, or they all have one of the second form.

Example 4.2. For an elliptic curve E/K, we can apply Lemma 4.1 to the action of the Galois group G of the ℓ-division field of E over K on the 2-dimensional $\mathbf{F}_\ell$-vector space $V = E[\ell](\overline{K})$ of ℓ-torsion points of E. In this case the point group $E(k_\mathfrak{p})$ at a prime $\mathfrak{p} \nmid \ell$ of good reduction is of order divisible by ℓ if and only if $\mathrm{Frob}_\mathfrak{p} \in G$ pointwise fixes a 1-dimensional subspace of V. We find that almost all local point groups $E(k_\mathfrak{p})$ are of order divisible by ℓ if and only if the Galois representation $\rho_{E/K,\ell}$ of G_K on the group of ℓ-torsion points of E can be given in matrix form as

$$\rho_{E/K,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \qquad \text{or} \qquad \rho_{E/K,\ell} \sim \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

In words: either $E(K)$ contains an ℓ-torsion point, or it is ℓ-isogenous over K to an elliptic curve with a K-rational ℓ-torsion point. Moreover, for E/K of the first kind, with a point $T \in E(K)$ of order ℓ, the quotient curve $E' = E/\langle T\rangle$ is of the second kind, with the dual isogeny $E' \to E$ being the ℓ-isogeny in question. This is a well-known fact that occurs as the very first exercise in [14, p. I-2].

Proof of Theorem 1.2. Let E/K be an elliptic curve, and $P \in E(K)$ a non-torsion point that is locally ℓ-imprimitive. We define $K_\ell = K(\ell^{-1}P)$ as in Section 2, and view $G_\ell = \mathrm{Gal}(K_\ell/K) \subset \mathrm{GL}(V_\ell)$ as a group of $\mathbf{F}_\ell$-linear automorphisms of the 3-dimensional vector space $V_\ell = \langle \ell^{-1}P\rangle/\langle P\rangle$. As every element of G_ℓ occurs as the Frobenius of infinitely many primes of good reduction, it follows from Lemma 2.3 that all elements of G_ℓ leave a 2-dimensional subspace of V_ℓ pointwise invariant. We can now apply our Lemma 4.1 for $n = 3$ with $G = G_\ell$ and $V = V_\ell$ to conclude that at least one of the following occurs: either G_ℓ acts trivially on a 2-dimensional subspace of V_ℓ, or G_ℓ acts trivially on a 2-dimensional quotient space of V_ℓ.

In the first case, if $U_\ell = E[\ell](\overline{K}) \subset V_\ell$ is a subspace with trivial G_ℓ-action, then $E(K)$ has complete ℓ-torsion and Condition B is satisfied. If G_ℓ acts trivially on a different 2-dimensional subspace $S_\ell \subset V_\ell$, than S_ℓ is spanned by a non-zero vector in $U_\ell \cap S_\ell$ and the non-zero image of a point of infinite order $Q \in \langle \ell^{-1}P\rangle$ in the $\mathbf{F}_\ell$-vector space V_ℓ. In other words: $E(K)$ contains a torsion point of order ℓ and a point Q with $\ell Q = mP$ for some $m \in \mathbf{Z}$ that is not divisible by ℓ. Writing $am + b\ell = 1$ in $\mathbf{Z}$, the point $Q' = aQ + bP \in E(K)$ satisfies $\ell Q' = a\ell Q + b\ell P = amP + b\ell P = P$, so Condition A is satisfied.

In the second case, where G_ℓ acts trivially on a 2-dimensional quotient space V_ℓ/T_ℓ, it acts on V_ℓ by translation along the 1-dimensional subspace T_ℓ. We will assume that G_ℓ does not act trivially on the subspace U_ℓ, as this would bring us back in the first case, with Condition B holding. As $U_\ell = E[\ell](\overline{K}) \subset V_\ell$ is G_ℓ-stable, we have strict inclusions $0 \subsetneq T_\ell \subsetneq U_\ell$ of $\mathbf{F}_\ell[G_\ell]$-modules, so T_ℓ is a K-rational subgroup of $E(\overline{K})$ of order ℓ. The corresponding isogeny $E \to E' = E/T_\ell$ is defined over K, and identifies the $\mathbf{F}_\ell[G_\ell]$-module U_ℓ/T_ℓ, which has trivial G_ℓ-action, with the subgroup of $E'(K)$ of order ℓ that is the kernel of the isogeny $\phi : E' \to E$ dual to $\widehat{\phi} : E \to E' = E/T_\ell$. If $Q \in E(\overline{K})$ satisfies $\ell Q = P$, then $P' = \widehat{\phi}(Q)$ is in $E'(K)$, as it is the image of any point in the Galois orbit $G_\ell \cdot Q \subset Q + T_\ell$. Moreover, we have $\phi(P') = \phi\widehat{\phi}(Q) = \ell Q = P$, so Condition C of Theorem 1.2 is satisfied.

Conversely, each of the Conditions A, B, and C guarantees that $P \in E(K)$ is locally ℓ-imprimitive. For A and B this is immediate. If Condition C holds, we have an ℓ-isogeny $\phi : E' \to E$ defined over K and a point $P' \in E'(K)$ with $\phi(P') = P$. Pick $Q' \in E'(\overline{K})$ with $\ell Q' = P'$ and put $Q = \phi(Q') \in E(\overline{K})$. Writing $\widehat{\phi} : E \to E'$ for the dual isogeny, we are in the situation of Example 4.2, and we have

$$\ell Q = \phi(\ell Q') = \phi(P') = P \qquad \text{and} \qquad \widehat{\phi} Q = \widehat{\phi}\phi Q' = \ell Q' = P' \in E'(K).$$

As Q is in the fibre $\widehat{\phi}^{-1}(P')$, the G_ℓ-action on $Q \bmod \langle P\rangle \in V_\ell$, which is by translation over ℓ-torsion points, gives rise to a Galois orbit of length dividing ℓ. If the length is 1, then Condition A is satisfied, and $P \in E(K)$ is locally ℓ-imprimitive. If the length is ℓ, then G_ℓ acts on V_ℓ by translation along the K-rational subgroup $T_\ell = \ker \widehat{\phi} \subset U_\ell = E[\ell](\overline{K})$, and the matrix representation of G_ℓ on V_ℓ with respect to the filtration $T_\ell \subset U_\ell \subset V_\ell$ is

$$\rho_{E/K,\ell} \sim \begin{pmatrix} * & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

By Lemma 2.3, we find that we have $\ell|[E(k_{\mathfrak{p}}) : \langle\overline{P}\rangle]$ for every prime $\mathfrak{p}$ of good reduction of E that is of characteristic different from ℓ, so $P \in E(K)$ is locally ℓ-imprimitive. □

5. Locally 2-imprimitive points

A *non-trivial* locally ℓ-imprimitive point on an elliptic curve E/K is a non-torsion point $P \in E(K)$ for which Condition C of Theorem 1.2 holds, but not Conditions A or B. If P is such a point, E admits a K-rational ℓ-isogeny $E \to E'$, and the Galois representation $\overline{\rho}_{E,\ell}$ of G_K on $U_\ell = E[\ell](\overline{K})$ is non-trivial, with image contained in a Borel subgroup of $\mathrm{GL}(U_\ell)$.

Let $P \in E(K)$ be a non-trivial locally 2-imprimitive point. As a Borel subgroup of $\mathrm{GL}(U_2) \cong \mathrm{GL}_2(\mathbf{F}_2)$ has order 2, the representation $\overline{\rho}_{E,2}$ is a non-trivial quadratic character, and as a Weierstrass model for E we can take

$$E : y^2 = x(x^2 + ax + b) \qquad \text{with } b, d = a^2 - 4b \in K^*. \tag{11}$$

Here $(0,0)$ is the K-rational point of order 2, and $\overline{\rho}_{E,2}$ corresponds to the 2-division field of E over K, which equals $K(\sqrt{d})$. Addition by $(0,0)$ induces an involution

$$(x, y) \mapsto (x_1, y_1) = (b/x, -by/x^2)$$

on the function field $K(E) = K(x,y)$ of E, and the invariant field $K(x+x_1, y+y_1)$ is the function field of the 2-isogenous curve $E' = E/\langle(0,0)\rangle$. Choosing $u = x+x_1+a$ and $v = y + y_1$ as generators for $K(E')$, we obtain a Weierstrass model

$$E' : v^2 = u(u^2 - 2au + d) \qquad \text{with } d, d' = (-2a)^2 - 4d = 16b \in K^* \tag{12}$$

for E' that is of the same form (11), and an explicit 2-isogeny $\varphi : E \to E'$ given by

$$\varphi : (x, y) \longmapsto (u, v) = (x + x_1 + a, y + y_1) = \left(\frac{y^2}{x^2}, (1 - \frac{b}{x^2})y\right). \tag{13}$$

An affine point $(u, v) \in E'(K)$ different from $(0,0)$ is in the image of $E(K)$ under this isogeny if and only if $u \in K^*$ is a square. The point $(0,0)$ is in the image if and only if d is a square in K^*, which amounts to saying that $E(K)$ has full 2-torsion. This not the case for our E.

As E' is again of the form (11), one sees that the isogeny $\widehat{\varphi} : E' \to E$ dual to φ is given by

$$\widehat{\varphi} : (u, v) \longmapsto \left(\frac{v^2}{4u^2}, (1 - \frac{b}{u^2})\frac{v}{8}\right). \tag{14}$$

Proof of Theorem 1.3. Let E/K be an elliptic curve with $\#E(\overline{K}) = 2$. We take $(0,0)$ as the point of order 2 in a Weierstrass model of E in order to obtain an equation $E : y^2 = x(x^2 + ax + b)$ as in (11), with $d = a^2 - 4b \in K^* \setminus K^{*2}$. Any quadratic twist of E over K is of the form

$$E_D : y^2 = x(x^2 + aDx + bD^2)$$

for some $D \in K^*$ that we may still rescale by squares in K^*, and we can define the 2-isogeny $\varphi : E_D \to E'_D = E/\langle(0,0)\rangle$ as above by replacing (a, b) in (11), (12), and (13) by (aD, bD^2). Any point $P \in E_D(K)$ satisfying Condition C from Theorem 1.2 is in the image $\widehat{\varphi}(E'_D(K))$ of the isogeny $\widehat{\varphi} : E'_D \to E_D$ dual to φ. This means that its x-coordinate is a square in K^*, which we can take to be 1 after rescaling the model of E over K. Thus, the twists that are relevant for us are those for which the point $P = (1, \pm Y) \in E_D(\overline{K})$ is K-rational.

We want (D, Y) to be a K-rational point on the conic $Y^2 = 1 + aD + bD^2$ different from $(0, \pm 1)$. Such points are obtained as the second point of intersection of this conic with the line $Y - 1 = \lambda D$ through $(0, 1)$ with slope $\lambda \in K$. We find that the twists $E_\lambda = E_{D_\lambda}$ of E by

$$D_\lambda = \frac{a - 2\lambda}{\lambda^2 - b} \qquad \text{with } \lambda \in K \setminus \{a/2, \pm\sqrt{b}\} \tag{15}$$

come by construction with a K-rational point

$$P_\lambda = (1, Y_\lambda) = \left(1, \frac{\lambda^2 - a\lambda + b}{\lambda^2 - b}\right) \in E_\lambda(K). \tag{16}$$

We can find $K_2 = K(\frac{1}{2}P_\lambda)$ by solving $2Q = \widehat{\varphi}(\varphi Q) = P_\lambda$ in $E_\lambda(\overline{K})$. The equation $\widehat{\varphi}(u, v) = P_\lambda$ has 2 solutions in $E'_\lambda(K)$, since we chose for the first coordinate of P_λ the square value 1. By (14), these are the K-rational points (u, v) different from $(0, 0)$ that have $v^2 = 4u^2$ and satisfy the equation

$$v^2 = u(u^2 - 2aD_\lambda u + dD_\lambda^2)$$

defining E'_λ. With $d = a^2 - 4b$, the resulting equation

$$u^2 - 2aD_\lambda u - 4u + dD_\lambda^2 = (u - aD_\lambda - 2)^2 - 4(1 + aD_\lambda + bD_\lambda^2) = 0$$

for u yields two solutions $u_1, u_2 = aD_\lambda + 2 \pm Y_\lambda \in K$ with product $u_1 u_2 = dD_\lambda^2$. Writing D_λ and P_λ as in (15) and (16), we find $aD_\lambda + 2 - Y_\lambda = d/(\lambda^2 - b)$, so the minimal extension $K \subset K_2$ for which the corresponding points are in $\varphi[E(K_2)]$ is

$$K_2 = K(\tfrac{1}{2}P_\lambda) = K(\sqrt{u_1}, \sqrt{u_2}) = K(\sqrt{d}, \sqrt{\lambda^2 - b}).$$

If we avoid the values $\lambda \in K$ for which $\lambda^2 - b$ is either a square or d times a square in K–this includes the 3 values excluded in (15)–then K_2 is a biquadratic extension of K which, unsurprisingly, has the 2-division field $K(\sqrt{d})$ of E/K as one of its quadratic subextensions. For these λ, our matrix representation from (5) and (6) of $G_2 = \mathrm{Gal}(K_2/K)$ becomes

$$\mathrm{Gal}(K_2/K) = \left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : x, y \in \mathbf{F}_2 \right\},$$

which implies that $P_\lambda \in E_\lambda(K)$ is globally 2-primitive, but locally 2-imprimitive.

There is still the possibility that P_λ, though globally 2-primitive, is a torsion point of even order $m > 2$. Examples: the point $(1, -3)$ on $y^2 = x(x^2 - 7x + 3)$ has order 4, and the point $(1, 1)$ on $y^2 = x(x^2 + 3x - 3)$ has order 6. However, for fixed K there are only finitely many possibilities for m by Merel's theorem. For every given even m, the point P_λ is of order m if and only if the m-th division polynomial $\psi_m(x) = y^{-1}f(x, E_\lambda)$ vanishes at $x = 1$. This happens for only finitely many values of λ, as $f(1, E_\lambda)$ is a non-constant rational function of λ if we fix $a, b \in K$. □

Our understanding of local 2-imprimitivity is more or less complete, as every nontrivial 2-locally imprimitive point on an elliptic curve arises as in the construction in the proof of Theorem 1.3. Indeed, the hypothesis $\#E[2](\overline{K}) = 2$ implies that E has a model as in (11), and as the x-coordinate of a point P satisfying Condition C of Theorem 1.2 is a square, the model can be scaled over K to have $P = (1, y) \in E(K)$.

6. Locally 3-imprimitive points

By Theorem 1.2, every pair (E, P) of an elliptic curve E/K with a non-trivial locally ℓ-imprimitive point $P \in E(K)$ arises as the ℓ-isogenous image of a K-rational curve-point-pair (E', P') for which the kernel $E' \to E$ is generated by an ℓ-torsion point $T \in E'(K)$. In this situation, the Galois representations of G_K on the ℓ-torsion subgroups of E' and $E = E'/\langle T\rangle$ are, with respect to a suitable basis, of the form

$$\rho_{E'/K,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & \omega_\ell \end{pmatrix} \qquad \text{and} \qquad \rho_{E/K,\ell} \sim \begin{pmatrix} \omega_\ell & * \\ 0 & 1 \end{pmatrix}. \tag{17}$$

Here ω_ℓ is the cyclotomic character corresponding to the extension $K \subset K(\zeta_\ell)$. For $\ell > 2$, the K-rationality of ℓ-torsion points of E is not preserved under twisting of E, so there is no direct analogue of Theorem 1.3 for $\ell \neq 2$. In this section we focus on the case $\ell = 3$.

Lemma 6.1. *Let E/K be an elliptic curve of discriminant Δ_E for which the Galois representation $\rho_{E/K,3}$ on $U_3 = E[3](\overline{K})$ is of one of the two forms in (17). Then the 3-division field of E over K equals the splitting field of the polynomial $X^3 - \Delta_E$.*

Proof. Let $H_3 = \mathrm{Gal}(K(E[3])/K) \subset \mathrm{GL}(U_3) \cong \mathrm{GL}_2(\mathbf{F}_3)$ be the image of $\rho_{E/K,3}$, and denote by $\psi_3 = \prod_{i=1}^4 (X - x_i) \in K[X]$ the 3-division polynomial of E over K. The quartic polynomial ψ_3 comes with a Galois resolvent $\delta_3 \in K[X]$, a cubic having

$$\alpha_1 = x_1x_2 + x_3x_4, \qquad \alpha_2 = x_1x_3 + x_2x_4, \qquad \alpha_3 = x_1x_4 + x_2x_3$$

as its roots. Under the permutation action of $\mathrm{GL}(U_3)/\langle -1\rangle = S_4$ on the roots of ψ_3, the normal subgroup $V_4 \lhd S_4$ of order 4 fixes each of these 3 roots α_i. The two natural surjections of Galois groups

$$H_3 \to \mathrm{Gal}(\psi_3) \to \mathrm{Gal}(\delta_3) \tag{18}$$

are isomorphisms as they arise as a restriction to suitable subgroups of the generic group theoretical maps

$$\mathrm{GL}(U_3) \to \mathrm{GL}(U_3)/\langle -1\rangle = S_4 \to S_4/V_4 = S_3.$$

More precisely, the first surjection in (18) is injective as we have $-1 \notin H_3$ for H_3 as in (17), and the second is because we have $\mathrm{Gal}(\psi_3) \cap V_4 = 1$ in S_4: the x-coordinate of the 3-torsion point spanning the Galois invariant subspace corresponding to the first column of the matrices is fixed by $\mathrm{Gal}(\psi_3)$. Viewing H_3 as $\mathrm{Gal}(\delta_3)$, we may finish the proof by quoting a classical formula [13, p. 305] that expresses the three cube roots of Δ_E as $b_4 - 3\alpha_i$ $(i = 1, 2, 3)$, with $b_i \in K$ a coefficient from the Weierstrass model of E. This yields $K(E[3]) = \mathrm{Split}_K(g) = \mathrm{Split}_K(X^3 - \Delta_E)$. □

From Lemma 6.1, we see that for the representations in (17), the subgroup $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ corresponds to the extension $K(\zeta_3) \subset K(\zeta_3, \sqrt[3]{\Delta})$ for the discriminant values $\Delta = \Delta_{E'}$ and Δ_E.

We can write the curve E' in Deuring normal form [6, p. 89] as

$$E' : y^2 + axy + by = x^3 \qquad \text{with } a, b \in K \text{ and } \Delta_{E'} = b^3(a^3 - 27b) \in K^*. \tag{19}$$

Here $T = (0, 0) \in E'(K)$ is the point of order 3, and the quotient curve $E = E'/\langle T\rangle$ has Weierstrass equation

$$E : y^2 + axy + by = x^3 - 5abx - (a^3 + 7b)b, \tag{20}$$

with the explicit formula for the 3-isogeny $\varphi_3 : E' \to E = E'/\langle T\rangle$ being given by

$$\varphi_3(x,y) = \left(\frac{x^3+abx+b^2}{x^2}, \frac{y(x^3-abx-2b^2)-b(ax+b)^2}{x^3}\right). \tag{21}$$

As E has discriminant $\Delta_E = b(a^3-27b)^3$, the 3-division field $K(E[3])$ over K equals $K(\zeta_3)$ if and only if $b \in K^*$ is a cube and different from $(a/3)^3$.

If a is non-zero, we can rescale $(x,y) \mapsto (a^2x, a^3y)$ and simplify (19) to

$$E'_b : y^2 + xy + by = x^3. \tag{22}$$

For K a number field, we have infinitely many pairwise different 3-isogenous images $(E_b, P_b) = \varphi_3[(E'_b, P'_b)]$ for which $P_b \in E_b(K)$ is non-trivially locally 3-imprimitive.

Theorem 6.2. *For K a number field, take $b = b(X) = (1-X-X^2)/X \in K(X)$ and define the associated elliptic curve over $K(X)$ as*

$$E_b : y^2 + xy + by = x^3 - 5bx - (1+7b)b.$$

Then for infinitely many $t \in K^*$, the specialization $E_{b(t)}$ of E_b is an elliptic curve over K for which

$$\left(\frac{(t^2+t)(t^2-1)+1}{t^2}, \frac{(1-t^2)\left(t^4+2t^3+t-1\right)}{t^3}\right) \in E_{b(t)}(K) \tag{23}$$

is a non-trivial locally 3-imprimitive point.

Proof. For the curve E'_b in (22) with $b \in K(X)$ as defined, the point $P'_b = (1, X)$ lies on E'_b by the very choice of b: it satisfies $X^2 + X + bX = 1$. Under the 3-isogeny $\varphi_3 : E'_b \to E_b$ from (21) to the curve E_b obtained by putting $a = 1$ in (20), it is mapped to

$$P_b = (1 + b + b^2, (1 - b - 2b^2)X - b(1 + b)^2) \in E_b(K(X)).$$

Under the specialization $X = t \in K^*$, we obtain a point $P_{b(t)}$, on the curve $E_{b(t)}$ defined over K that is given by (23). We are only interested in those specializations for which $E_{b(t)}$ is an elliptic curve. As these are all $t \in K^*$ for which $b(t) \notin \{0, 1/27\}$, at most 4 'bad' values of t are excluded. Also, by the same argument as we gave for P_λ in the case $\ell = 2$, there are only finitely many $t \in K^*$ for which P_t is torsion point. These finitely many t we also exclude as 'bad' values.

We saw already that E_b has 3-division field $K(\zeta_3, \sqrt[3]{b})$, and an explicit computation shows that the 3-division field of the point $P_b \in E_b(K(X))$ equals

$$K(X)(\tfrac{1}{3}P_b) = K(\zeta_3, \sqrt[3]{b}, \sqrt[3]{X}) = K(\zeta_3, \sqrt[3]{X}, \sqrt[3]{X^2+X-1}).$$

Over $K(\zeta_3, X)$, the elements X and $X^2 + X - 1$ have 'independent' cube roots – it suffices look at their ramification locus. It follows that the Galois group of the 3-division field of P_b over $K(X)$ may be described as

$$\mathrm{Gal}(K(X)(\tfrac{1}{3}P_b)/K(X)) = \left\{ \begin{bmatrix} \omega_3 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : x, y \in \mathbf{F}_3 \right\},$$

with ω_3 denoting the $\mathbf{F}_3^*$-valued character corresponding to the (possibly trivial) extension $K(X) \subset K(X, \zeta_3)$. By Hilbert irreducibility, it follows that for infinitely many $t \in K^*$ outside the finite set of 'bad' values, the 3-division field of the point $P_{b(t)} \in E_{b(t)}(K)$ has the 'same' Galois group over K, making it into a point that is globally 3-primitive, but locally 3-imprimitive. As $E_{b(t)}$ does not have complete

3-torsion over K, we conclude that the point $P_{b(t)}$ given in (23) is a non-trivial locally 3-imprimitive point. □

Remark 6.3. The construction in the proof of Theorem 6.2 excludes all specializations for which $b = b(t) \in K^*$ is a cube and the elliptic curve in (22) has 3-division field $K(\zeta_3)$. In this special case, we can also equip $E = E_b$ with a non-trivial locally 3-imprimitive point for infinitely many $b \in K^{*3}$. We first write $b = c^{-3}$ and transform the curve under $(x, y) \mapsto (c^{-2}x, c^{-3}y)$ into $E' : y^2 + cxy + y = x^3$. As in the previous case, we have $P' = (1, t) \in E'(K)$ for $c = (-t^2 - t + 1)/t$, and the image of P' under the map

$$\varphi : E' \to E = E'/\langle(0,0)\rangle : y^2 + cxy + y = x^3 - 5cx - (c^3 + 7)$$

is the point $P = \varphi_3(P') = ((-t^2 + t + 1)/t, (t^2 - 1)/t^2) \in E(K)$, for which the 3-division field $K(\frac{1}{3}P)$ is equal to $K(\zeta_3, \sqrt[3]{t})$. For almost all $t \notin K^{*3}$, this makes P into a globally 3-primitive point that is locally 3-imprimitive.

We conclude our discussion for $\ell = 3$ with the remaining case in which the curve E' in (19) has $a = 0$. In this case E' has j-invariant 0, and writing $c = b/2$ we may rescale the equation by $y \mapsto y - c$ to the more familiar shape $E' : y^2 = x^3 + c^2$, with 3-torsion point $T = (0, c)$ and CM by $\mathbf{Z}[\zeta_3]$. We equip E' with a K-rational point $(c, c\sqrt{c+1})$ by putting $c = s^2 - 1$ with $s \in K$. This leads to a 1-parameter family of 3-isogenies

$$\begin{aligned} \varphi_3 : E'_s : y^2 = x^3 + (s^2-1)^2 &\longrightarrow E_s : y^2 = x^3 - 27(s^2-1)^2 \\ P'_s = (s^2 - 1, s(s^2-1)) &\longmapsto P_s = (s^2 + 3, s(s^2 - 9)) \end{aligned}$$

between CM-curves with j-invariant 0. In this case the 3-division field of E_s over K is $K(\zeta_3, \sqrt[3]{2(s^2-1)})$, and the 3-division field of P_s over K equals

$$K(\zeta_3, \sqrt[3]{2(s^2-1)}, \sqrt[3]{4(s+1)}).$$

Again, for $s \in K$ outside a thin set, the point $P_s \in E_s(K)$ is globally 3-primitive but locally 3-imprimitive.

7. Further examples

Over $K = \mathbf{Q}$, non-trivial locally ℓ-imprimitive points can only occur for primes $\ell \leq 7$. Examples for $\ell = 5$ and also $\ell = 7$ can be found by the techniques that we employed for $\ell = 3$, but the formulas and resulting curves rapidly become less suitable for presentation on paper.

7.1. **Curves with a locally 5-imprimitive point.** In this case, we start from Tate's normal form

$$E' : y^2 + (1-c)xy - cy = x^3 - cx^2 \tag{24}$$

that parametrises elliptic curves with $(0, 0)$ as a 5-rational point (see Kulesz [7]). It has further points $(0, c)$, $(c, 0)$ and (c, c^2) of order 5, and its discriminant equals $\Delta_{E'} = c^5\left(c^2 - 11c - 1\right)$. Using Vélu's formula [18] or invoking Pari-GP, we compute the Weierstrass equation for the 5-isogenous curve $E = E'/\langle(0,0)\rangle$

$$\begin{aligned} E = E_c : \quad y^2 &+ (1-c)xy - cy = \\ &x^3 - cx^2 - 5c(c^2 + 2c - 1)x - c(c^4 + 10c^3 - 5c^2 + 15c - 1), \end{aligned}$$

and also the explicit 5-isogeny $\varphi_5 : E' \to E$. The discriminants involved are $\Delta_{E'} = c^5(c^2 - 11c - 1)$ and $\Delta_E = c(c^2 - 11c - 1)^5$, much like we saw for $\ell = 3$. The 5-torsion representations of E' and E are as in (17), and even though the proof of Lemma 6.1 for $\ell = 3$ does not generalize to $\ell = 5$, we found by a direct calculation that the 5-division fields are $K(E'[5]) = K(\zeta_5, \sqrt[5]{c^2 - 11c - 1})$ and $K(E[5]) = K(\zeta_5, \sqrt[5]{c})$: generated over $K(\zeta_5)$ by the 5-th root of the discriminant.

We can equip E' with a K-rational point $P'_t = (t, t)$ by putting $c = t(2 - t)$, and compute its image $P_t = \varphi_5(P') \in E_{t(2-t)}(K)$ as

$$P_t = \left(\tfrac{2t^4-8t^3+11t^2-6t+2}{(t-1)^2}, -\tfrac{t^8-7t^7+19t^6-23t^5+4t^4+23t^3-31t^2+19t-4}{(t-1)^3}\right).$$

The corresponding 5-division field of P_t is

$$K(\tfrac{1}{5}P_t) = K(\zeta_5, \sqrt[5]{t}, \sqrt[5]{t-2}).$$

If this is an extension of degree 5 of $K(\zeta_5, \sqrt[5]{c}) = K(\zeta_5, \sqrt[5]{t(t-2)})$, then P_t is a globally 5-primitive but locally 5-imprimitive point in $E_{t(2-t)}(K)$.

Example 7.1. Take $K = \mathbf{Q}$. For $t = 1$ the point P_t above is the zero point as P'_t is 5-torsion, for $t = 2$ we have $c = 0$ and E is singular, while for $t = 3$ and 4 we encounter the 'accidents' $t = -c$ and $tc = 2^5$ leading to points $P_t \in 5E_{t(2-t)}(\mathbf{Q})$. For $t = 5$ we obtain the point $P_5 = (497/16, -73441/64)$ on

$$E_{-15} : y^2 + 16xy + 15y = x^3 + 15x^2 + 14550x + 232860,$$

which is the curve 5835.c2 in the LMFDB-database. Note that for $c = -15$ we have

$$c(c^2 - 11c - 1) = -5835 = -3 \cdot 5 \cdot 389.$$

The locally 5-imprimitive point P_5 is a generator of $E_{-15}(\mathbf{Q}) \cong \mathbf{Z}$. In fact, P_t will be globally 5-primitive but locally 5-imprimitive in $E_{t(2-t)}(\mathbf{Q})$ for all $t \in \mathbf{Z}_{\geq 5}$ that are not a fifth power or a fifth power plus 2, as for these t the subgroup of $\mathbf{Q}^*/\mathbf{Q}^{*5}$ generated by t and $t - 2$ has order 25.

7.2. **Curves with a locally 7-imprimitive point.** Again we start from the Tate's normal equation

$$E' : y^2 + (1 - c)xy - by = x^3 - bx^2$$

but now we do not impose $b = c$ as for $\ell = 5$, but instead

$$c = d^2 - d \quad \text{ and } b = d^3 - d^2.$$

The curve $E' = E'_d$ parametrizes [7] elliptic curves with $(0, 0)$ as point of order 7. A Weierstrass equation for the 7-isogenous curve $E = E'/\langle(0, 0)\rangle$ is

$$\begin{gathered}
E : y^2 + (1 - c)xy - by = x^3 - bx^2 - 5\left(2b^2 + b\left(c^2 - 3c - 2\right) + c\left(c^2 + 4c + 1\right)\right)x \\
-b^2\left(12c^2 + c + 24\right) - 6b^3 + b\left(-c^4 + 9c^3 + 46c^2 + 24c + 2\right) - \\
c\left(c^4 + 16c^3 + 36c^2 + 16c + 1\right).
\end{gathered}$$

It has discriminant $\Delta_E = d(d - 1)(d^3 - 8d^2 + 5d + 1)^7$, and this time we find its 7-division field to be $K(E[7]) = K(\zeta_7, \sqrt[7]{d(d - 1)^2})$.

We equip E' with a K-rational point $P'_t = (d^2t, d^3t)$ by putting $d = d(t) = (t + 1)/(t^2 - t + 1)$. The image of P'_t under the 7-isogeny $E' \to E$ is

$$P_t = \left(-\frac{C(t)}{(2t - 1)^2(t - 1)^2\left(t^2 - t + 1\right)^4}, \frac{D(t)}{(t - 1)^3(2t - 1)^3\left(t^2 - t + 1\right)^6}\right) \in E(K)$$

for certain polynomials $C(t)$ and $D(t)$ in $\mathbf{Z}[t]$ of degree 12 and 18. In terms of t, the 7-division field is $K(E[7]) = K(\zeta_7, \sqrt[7]{t^2(t+1)(t-2)^2(t^2-t+1)^4})$, and the 7-division field of P_t is

$$K(\tfrac{1}{7}P_t) = K(E[7])\left(\sqrt[7]{\tfrac{t(t+1)}{t-2}}\right) = K\left(\zeta_7, \sqrt[7]{\tfrac{t(t^2-t+1)}{(t+1)}}, \sqrt[7]{\tfrac{t(t+1)}{(t-2)}}\right).$$

The point P_t is a globally 7-primitive but locally 7-imprimitive point when the extension $K(\zeta_7) \subset K(\frac{1}{7}P_t)$ has its generic degree 7^2.

Example 7.2. Take $K = \mathbf{Q}$. For $t = 1$ the point P_t above is the zero point as P'_t is 7-torsion, and for $t = 2$ the curve E' is singular. For $t = 3$ and $d = \frac{4}{7}$ however we obtain the point $P_3 = (286019/490^2, 15951227/490^3)$ on

$$E : y^2 + \tfrac{61}{7^2}xy + \tfrac{48}{7^3}y = x^3 + \tfrac{48}{7^3}x^2 - \tfrac{774780}{7^7}x - \tfrac{1047829260}{7^{11}},$$

which is the curve 20622.j1 with minimal model

$$E_0 : y^2 + xy = x^3 - 5455771x - 5039899603,$$

in the LMFDB-database. Our locally 7-imprimitive point P_3 is a generator of $E(\mathbf{Q}) \cong \mathbf{Z}$. On E_0 the corresponding generator is $(328219/10^2, 109777927/10^3)$.

8. A composite level obstruction

So far we have focused on non-trivial obstructions to local primitivity at prime level ℓ, as this is a new phenomenon in the elliptic primitive root case III that does not arise in the multiplicative primitive root case I and the cyclic reduction case II.

In all three cases, there exist obstructions of different nature at composite levels that arise from the *entanglement* between finitely many of the corresponding division fields K_ℓ. These obstructions do not arise over $K = \mathbf{Q}$, and most examples in the cases I and II are created by base changing to a well-chosen finite extension of the fields of definition $\mathbf{Q}(x)$ and $\mathbf{Q}(j_E)$. Again, case III is different here, as entanglement obstructions already occur over $\mathbf{Q}$. In this Section we construct a level 6 obstruction.

Let E/K be an elliptic curve with $\#E[2](K) = 2$, and $P \in E(K)$ a point of infinite order. Then the 2 division field $K(E[2](\overline{K}))$ is a quadratic extension of K. Assume that the 2-division field $K(\frac{1}{2}P)$ of P is of maximal degree 4 over it. Then $G_2 = \mathrm{Gal}(K(\frac{1}{2}P)/K)$ is a dihedral group of order 8 for which the matrix representation (6) on $V_2 = \langle\frac{1}{2}P\rangle/\langle P\rangle$ has the form

$$G_2 = \left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbf{F}_2 \right\} \subset \mathrm{GL}_3(\mathbf{F}_2). \tag{25}$$

There is a unique subfield of $L \subset K(\frac{1}{2}P)$ with Galois group over K isomorphic to the Klein 4-group $V_4 = C_2 \times C_2$, and we can view a and b in the matrix representation (25) of G_2 as $\mathbf{F}_2$-valued quadratic characters on G_2 that generate the character group of the quotient $\mathrm{Gal}(L/K) \cong V_4$ of G_2.

For a prime $\mathfrak{p} \nmid 2\Delta_E$, the point P generates a subgroup of odd index in $E(k_\mathfrak{p})$ if and only if for its Frobenius $\mathrm{Frob}_{\mathfrak{p},2} \in G_2$, viewed as a matrix as in (25), the endomorphism $(\mathrm{Frob}_{\mathfrak{p},2} - \mathrm{id}_2) : V_2 \to V_2$ has $\mathbf{F}_2$-rank at least 2 (Lemma 2.3). We obtain the criterion

$$2 \nmid [E(k_\mathfrak{p}) : \langle\overline{P}\rangle] \quad \Longleftrightarrow \quad a(\mathrm{Frob}_{\mathfrak{p},2}) = b(\mathrm{Frob}_{\mathfrak{p},2}) = 1 \in \mathbf{F}_2. \tag{26}$$

More precisely, $a(\mathrm{Frob}_{\mathfrak{p},2}) = 1$ implies that $E(k_\mathfrak{p})$ does not have full 2-torsion, and $b(\mathrm{Frob}_{\mathfrak{p},2}) = 1$ implies that P is not only not in $2E(k_\mathfrak{p})$, but also not a 2-isogenous image as in Condition C of Theorem 1.2.

Suppose further that E has a K-rational 3-torsion subgroup T, and let $\varphi_3 : E' \to E$ be the isogeny dual to the quotient map $\phi : E \to E' = E/T$. Assume that the point P is in $\varphi_3[E'(K)]$ but not in $3E(K)$. Then the 3-division field $K(\frac{1}{3}P)$ of P has Galois group $G_3 = \mathrm{Gal}(K(\frac{1}{3}P)/K)$ for which the matrix representation on $V_3 = \langle \frac{1}{3}P\rangle/\langle P\rangle$ will 'generically' be the group

$$G_3 = \left\{ \begin{bmatrix} d & e & f \\ 0 & g & 0 \\ 0 & 0 & 1 \end{bmatrix} : \quad d, g \in \mathbf{F}_3^*, e, f \in \mathbf{F}_3 \right\} \subset \mathrm{GL}_3(\mathbf{F}_3) \tag{27}$$

of order 36. In this case d and g can be viewed as a quadratic characters $G_3 \to \mathbf{F}_3^*$, and another application of Lemma 2.3 shows that for primes $\mathfrak{p} \nmid 3\Delta_E$, we have

$$g(\mathrm{Frob}_{\mathfrak{p},3}) = 1 \in \mathbf{F}_3^* \quad \Longrightarrow \quad 3|[E(k_\mathfrak{p}) : \langle \overline{P}\rangle]. \tag{28}$$

Thus, for primes $\mathfrak{p} \nmid 6\Delta_E$, a necessary condition for $\overline{P} \in E(k_\mathfrak{p})$ to be an elliptic primitive root is that the three quadratic characters a, b and g occurring in (26) and (28) do not vanish on the Frobenius automorphism of $\mathfrak{p}$ in $K_6 = K(\frac{1}{6}P)$. In other words: the prime $\mathfrak{p}$ has to be inert in the quadratic extensions K_a, K_b and K_g of K corresponding to these 3 characters.

Primes $\mathfrak{p}$ satisfying the condition above exist if the quadratic extensions K_a, K_b and K_g are linearly disjoint over K, but *not* if they are the three quadratic subfields of a V_4-extension $K \subset K_aK_bK_g$. In the latter case, we have a splitting obstruction to local primitivity of P in K_6 that does not exist in one of the smaller fields $K(\frac{1}{2}P)$ or $K(\frac{1}{3}P)$: it has level 6, but not 2 or 3, making it an obstruction caused by *entanglement* of division fields.

Example 8.1. An example is provided by the elliptic curve $E/\mathbf{Q}$ with label 12100.j1 in the LMFDB data base. The curve E has discriminant

$$\Delta_E = 2^4 \cdot 5^9 \cdot 11^6,$$

and if we take $(0, 0)$ to be its unique $\mathbf{Q}$-rational 2-torsion point it has Weierstrass model

$$E : y^2 = x^3 + 605x^2 - 3025x.$$

For this curve we have $E(\mathbf{Q}) = \langle T_2\rangle \times \langle P\rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}$ with $T_2 = (0, 0)$ of order 2 and $P = (\frac{-13475}{36}, \frac{1249325}{216})$ a generator of infinite order. We have $K_a = \mathbf{Q}(E[2]) = \mathbf{Q}(\sqrt{\Delta_E}) = \mathbf{Q}(\sqrt{5})$, and over this field the 2-division field $\mathbf{Q}(\frac{1}{2}P)$ of P is the V_4 extension

$$\mathbf{Q}(E[2]) = \mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\tfrac{1}{2}P) = \mathbf{Q}(\sqrt{5}, \sqrt{\pi}, \sqrt{\overline{\pi}})$$

generated by the square roots of $\pi = 3 + 2\sqrt{5}$ and its conjugate. From $\pi\overline{\pi} = -11$ we see that $\mathbf{Q}(\frac{1}{2}P)$ is cyclic of degree 4 over $\mathbf{Q}(\sqrt{-55})$, and that we have $K_b = \mathbf{Q}(\sqrt{-11})$.

As E acquires a 3-torsion point $T_3 = (\frac{55}{3}, \frac{275}{9}\sqrt{165})$ over the quadratic field $\mathbf{Q}(\sqrt{165}) = \mathbf{Q}(\sqrt{-3 \cdot -55})$ that generates a $\mathbf{Q}$-rational torsion subgroup of order 3, the 3-division field of E has quadratic subfields $K_d = \mathbf{Q}(\sqrt{165})$ and $K_g = \mathbf{Q}(\sqrt{-55})$, making K_g the third quadratic subfield in the V_4-extension $\mathbf{Q} \subset K_aK_b$. Over the full 3-division field of E, the 3-division field of P is the cubic extension

$$\mathbf{Q}(E[3]) = \mathbf{Q}(\sqrt{-3}, \sqrt{-55}, \sqrt[3]{2}) \subset \mathbf{Q}(\tfrac{1}{3}P) = \mathbf{Q}(E[3], \sqrt[3]{\alpha})$$

generated by a cube root of an element $\alpha = (3 + \sqrt{-55})/2 \in K_g$ of norm 16, which shows that its Galois group over $\mathbf{Q}$ is the group G_3 in (27). We conclude that P is a locally never-primitive point of $E(\mathbf{Q})$ as the index of $\langle \overline{P} \rangle$ in $E(\mathbf{F}_p)$ is always divisible by 2 or 3.

An upcoming paper will have further details on obstructions to primitivity of composite level, and on how to find explicit examples.

References

[1] George Cooke and Peter J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to* SL_2, Comm. Algebra **3** (1975), 481–524.

[2] Francesco Campagna and Peter Stevenhagen, *Cyclic reduction densities for elliptic curves*, ArXiv preprint 2001.00028, submitted.

[3] Rajiv Gupta and M. Ram Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), no. 1, 225–235.

[4] ———, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), no. 1, 13–44.

[5] Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[6] Dale Husemöller, *Elliptic curves, 2nd edition*, Springer Verlag, New York, 2004.

[7] Leopoldo Kulesz, *Families of elliptic curves of high rank with nontrivial torsion group over* **Q**, Acta Arith. **108** (2003), no. 4, 339–356.

[8] Serge Lang and Hale Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292.

[9] H. W. Lenstra Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224.

[10] H. W. Lenstra Jr., P. Stevenhagen, and P. Moree, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. **157** (2014), no. 3, 489–511.

[11] Giulio Meleleo, *Questions related to Primitive Points on Elliptic Curves and Statistics for Biquadratic Curves over Finite Fields*, Tesi di Dottorato, Università Roma Tre (2015).

[12] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449 (French).

[13] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[14] ———, *Abelian ℓ-adic representations and elliptic curves*, Benjamin, New York, 1968.

[15] ———, *Résumé des cours de 1977-1978*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2013. Reprint of the 2003 edition [of the 1986 original MR0926691].

[16] Peter Stevenhagen and Hendrik Lenstra, *Chebotarev and his density theorem*, The Mathematical Intelligencer **18** (1996), no. 2, 26–37.

[17] Peter Stevenhagen, *The correction factor in Artin's primitive root conjecture*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 383–391 (English, with English and French summaries). Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[18] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241 (French).

Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, IL 60607, USA

Dipartimento di Matematica, Università Roma Tre, Largo S. L. Murialdo 1, I–00146 Rome, Italy

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands

Email address: ncjones@uic.edu, pappa@mat.uniroma3.it, psh@math.leidenuniv.nl