J. Aust. Math. Soc. (First published online 2024), page 1 of 20*
doi:10.1017/S1446788724000156
*Provisional—final page numbers to be inserted when paper edition is published

CLASS GROUP STATISTICS FOR TORSION FIELDS GENERATED BY ELLIPTIC CURVES

ANWESH RAY and TOM WESTON

(Received 20 December 2023; accepted 17 July 2024)

Communicated by Michael Coons

Abstract

For a prime p and a rational elliptic curve $E_{/\mathbb{Q}}$, set $K = \mathbb{Q}(E[p])$ to denote the torsion field generated by $E[p] := \ker\{E \xrightarrow{p} E\}$. The class group Cl_K is a module over $\mathrm{Gal}(K/\mathbb{Q})$. Given a fixed odd prime number p, we study the average nonvanishing of certain Galois stable quotients of the mod-p class group $\mathrm{Cl}_K / p\,\mathrm{Cl}_K$. Here, E varies over all rational elliptic curves, ordered according to *height*. Our results are conditional, since we assume that the p-primary part of the Tate–Shafarevich group is finite. Furthermore, we assume predictions made by Delaunay for the statistical variation of the p-primary parts of Tate–Shafarevich groups. We also prove results in the case when the elliptic curve $E_{/\mathbb{Q}}$ is fixed and the prime p is allowed to vary.

2020 *Mathematics subject classification*: primary 11G05; secondary 11R29, 11R32, 11R34, 11R45.

Keywords and phrases: torsion fields, class groups, Selmer groups of elliptic curves, arithmetic statistics.

1. Introduction

Given a family of number fields, it is natural to study the statistical variation of class groups in the family. Of significant interest is the family of imaginary quadratic extensions $K/\mathbb{Q}$. Such investigations go back to the work of Gauss, who was interested in the determination of all imaginary quadratic fields of a given class number h. The problem was solved for $h = 1$ by Baker, Heegner and Stark, for $h = 2$ by Baker and Stark, and for $h = 3$ by Oesterlé. Watkins in [Wat04] computed the imaginary quadratic fields for which $h \leq 100$. Soundararajan showed that the number of imaginary quadratic fields of class number $< x$ is asymptotically $3\zeta(2)/\zeta(3)x^2$ as $x \to \infty$. The story for real quadratic fields is significantly different. Predictions can be made for the distribution of class groups via Cohen–Lenstra heuristics for all quadratic number fields [CL84] and Cohen–Lenstra–Martinet heuristics for general

From September 2022 to September 2023, the first author's research is supported by the CRM Simons postdoctoral fellowship.

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

number fields [MC90]. We refer to [Woo16] for a survey of these methods. The study of class numbers on average in families of number fields has notably gained significant momentum in the following works [Bha05, DH71, EPW17, EV07, FK07, Won99]. However, there has been much interest in the study of the p-ranks of class groups of the cyclotomic extension $\mathbb{Q}(\mu_p)$. The Herbrand–Ribet theorem (see [Was97]) establishes a precise relationship between generalized Bernoulli numbers and the p-rank of the class group of $\mathbb{Q}(\mu_p)$. Ribet's converse relates congruences between Eisenstein series and cusp forms to the existence of p-cyclic unramified extensions of $\mathbb{Q}(\mu_p)$. The rank of the Eisenstein ideal is closely related to the Galois module structure of mod-p class groups that arise from certain families of number fields of the form $\mathbb{Q}(N^{1/p})$, where $N \equiv 1 \pmod p$ is a prime, see [Lec18, Maz77, SS19, WWE20]. It is however difficult to resolve distribution questions in this context, though there have been some computational experiments done (see [WWE20, Introduction]).

Motivated by such developments, we consider the family of number field extensions that are generated by the torsion in elliptic curves defined over $\mathbb{Q}$. To be specific, given an elliptic curve $E_{/\mathbb{Q}}$ and a prime p, we let $E[p]$ denote the p-torsion subgroup of $E(\bar{\mathbb{Q}})$. Let $K = \mathbb{Q}(E[p])$ be the field generated by $E[p]$, defined to be the fixed field of the residual representation

$$\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

on $E[p] \simeq \mathbb{F}_p \oplus \mathbb{F}_p$. The extension $K/\mathbb{Q}$ in general is a nonabelian extension that contains $\mathbb{Q}(\mu_p)$. Let Cl_K be the class group of K. Note that $G = \mathrm{Gal}(K/\mathbb{Q})$ acts on Cl_K and thus on the mod-p class group $\mathrm{Cl}_K / p\,\mathrm{Cl}_K$. We study Galois stable quotients of the $\mathrm{Cl}_K / p\,\mathrm{Cl}_K$ that are isomorphic to $E[p]$ as a G-module. In some sense, such investigations generalize the study of the p-rank of the class group of $\mathbb{Q}(\mu_p)$. To be precise, we study the following related questions.

(1) Let p be a fixed odd prime. As E varies over all elliptic curves defined over $\mathbb{Q}$, how often is $\mathrm{Hom}_G(\mathrm{Cl}_K / p\,\mathrm{Cl}_K, E[p])$ nonvanishing?

(2) Let $E_{/\mathbb{Q}}$ be a fixed elliptic curve. As p varies over all primes, how does the dimension of $\mathrm{Hom}_G(\mathrm{Cl}_K / p\,\mathrm{Cl}_K, E[p])$ vary?

In the context of the first question above, we order elliptic curves $E_{/\mathbb{Q}}$ according to *height*. We assume throughout that the p-primary part of the Tate–Shafarevich group is finite. Our results also rely on heuristics for the statistical behaviour of Tate–Shafarevich groups of elliptic curves. These heuristics were studied by Delaunay [Del07]. Let $\mathcal{E}_p$ be the set of elliptic curves $E_{/\mathbb{Q}}$ such that $\mathrm{Hom}_G(\mathrm{Cl}_K, E[p]) \neq 0$. Given $\Delta \in \mathbb{Z}_{<0}$ with $\Delta \equiv 0, 1 \pmod 4$, let $H(\Delta)$ be the Hurwitz class number, see Definition 3.10. Given a set of elliptic curves $\mathcal{S}$, we denote by $\underline{\mathfrak{d}}(\mathcal{S})$ the lower density of Weierstrass equations for elliptic curves in $\mathcal{S}$ (see (3-1) for the definition of $\underline{\mathfrak{d}}(\mathcal{S})$).

THEOREM (THEOREM 4.4). *Let p be an odd prime and assume that Conjecture 4.2 is satisfied. Then,*

$$\underline{\mathfrak{d}}(\mathcal{E}_p) > (p^{-1} + p^{-3} - p^{-4})(1 - p^{-1} - \mathfrak{d}_p - \mathfrak{d}'_p),$$

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

where

$$\mathfrak{d}_p = \begin{cases} \zeta(p) - 1 & \textit{if } p \geq 5, \\ (\zeta(3) - 1) + (\zeta(4) - 1) + (\zeta(7) - 1) & \textit{if } p = 3, \end{cases}$$

$$\mathfrak{d}'_p = \begin{cases} \left(\dfrac{p-1}{2p^2}\right) H(1 - 4p) & \textit{if } p \geq 7, \\ \left(\dfrac{p-1}{2p^2}\right)(H(1 - 4p) + H(p^2 + 1 - 6p)) & \textit{if } p \leq 5. \end{cases}$$

We obtain the following corollary to the above result.

Corollary (Corollary 4.5). *Let p be an odd prime and assume that Conjecture 4.2 is satisfied. Then,*

$$\underline{\mathfrak{d}}(\mathcal{E}_p) \geq p^{-1} + O(p^{-3/2+\epsilon}).$$

In other words, for any choice of $\epsilon > 0$, there is a constant $C > 0$, depending on ϵ and independent of p, such that

$$\underline{\mathfrak{d}}(\mathcal{E}_p) \geq p^{-1} - Cp^{-3/2+\epsilon}.$$

Next, we study the second question, where E is fixed and p varies. In this context, we prove two results.

Theorem (Theorem 5.1). *Let $E_{/\mathbb{Q}}$ be an elliptic curve and assume that the following conditions are satisfied:*

(1) $\text{Ш}(E/\mathbb{Q})$ *is finite;*
(2) $\operatorname{rank} E(\mathbb{Q}) \leq 1$*;*
(3) *E does not have complex multiplication.*

Then, for 100% of primes p, we have that $\operatorname{Hom}_G(\operatorname{Cl}_K / p \operatorname{Cl}_K, E[p]) = 0$.

Theorem (Theorem 5.2). *Let $E_{/\mathbb{Q}}$ be an elliptic curve and assume that the following conditions are satisfied:*

(1) $\text{Ш}(E/\mathbb{Q})$ *is finite;*
(2) $\operatorname{rank} E(\mathbb{Q}) \geq 2$*;*
(3) *E does not have complex multiplication.*

Then, for 100% (that is, for a Dirichlet density-1 set) of primes p,

$$\dim \operatorname{Hom}_G(\operatorname{Cl}_K / p \operatorname{Cl}_K, E[p]) \geq \operatorname{rank} E(\mathbb{Q}) - 1.$$

Organization: In Section 2, we introduce preliminary notions and also recall results of Prasad and Shekhar [PS21] on the Galois module structure of the class group of the torsion field $\mathbb{Q}(E[p])$. In Section 3, we study the density of elliptic curves satisfying local conditions at a possibly infinite set of primes. Such results are crucially used in proving the main results of the article. In Section 4, we fix an odd prime p. The main results are Theorem 4.4 and Corollary 4.5, which establish that

$\mathrm{Hom}_G(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p])$ is nonvanishing for a positive density set of elliptic curves. Furthermore, we prove a lower bound for this density explicitly. These results are conditional since they rely on the heuristic of Delaunay. In Section 5, we fix an elliptic curve $E_{/\mathbb{Q}}$ that does not have complex multiplication and study the variation of the dimension of $\mathrm{Hom}_G(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p])$, where p varies over all prime numbers. Finally, in Section 6, we provide explicit computations for the prime $p = 3$. These computations do also illustrate cases of interest, when some of the hypotheses on E and p are relaxed.

2. Preliminaries

Fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and let E be an elliptic curve defined over $\mathbb{Q}$. Let p be a prime number and set $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ to denote the finite field with p elements. For $n \geq 1$, denote by $E[p^n]$ the kernel of the multiplication map $\times p^n : E(\bar{\mathbb{Q}}) \to E(\bar{\mathbb{Q}})$ and set $E[p^\infty] := \bigcup_n E[p^n]$. The absolute Galois group $\mathrm{G}_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E[p^n]$. Choosing an isomorphism $E[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$, let ρ_n be the associated Galois representation on $E[p^n]$,

$$\rho_n : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}).$$

Set $\rho := \varprojlim_n \rho_n$ to be the Galois representation on the p-adic Tate-module $\mathrm{T}_p(E) := \varprojlim_n E[p^n]$. Set $\bar{\rho}$ to denote the mod-p reduction of the characteristic-zero representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$. We refer to $\bar{\rho}$ as the *residual representation* and identify $\rho_1 : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ with $\bar{\rho}$. Let $\chi : \mathrm{G}_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character and $\bar{\chi} : \mathrm{G}_{\mathbb{Q}} \to \mathbb{F}_p^\times$ its mod-p reduction.

Given an integer r, set $\mathbb{Z}_p(r) := \mathbb{Z}_p(\chi^r)$ and given a $\mathbb{Z}_p[\mathrm{G}_{\mathbb{Q}}]$-module M, set $M(r) := M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi^r)$ to denote the *r th Tate-twist* of M. Note that if M is an $\mathbb{F}_p[\mathrm{G}_{\mathbb{Q}}]$-module, then, $M(r) = M \otimes_{\mathbb{F}_p} \mathbb{F}_p(r)$. Let $V_{\bar{\rho}} = E[p]$ be the underlying vector space for $\bar{\rho}$. Given $i, j \in \mathbb{Z}$ lying in the range $1 \leq i \leq (p-1)$ and $1 \leq j \leq (p-2)$, we set $V^{i,j} = V^{i,j}_{p,E}$ to denote $\mathrm{Sym}^i(V_{\bar{\rho}})(j)$. Throughout, we assume that $\bar{\rho}$ is irreducible. However, for the sake of discussion, let us consider the special case when $\bar{\rho}$ is surjective. Then, upon choosing a basis of $V_{\bar{\rho}} = E[p]$, we may identify the image of $\bar{\rho}$ with $\mathrm{GL}_2(\mathbb{F}_p)$ and thus the module $V^{i,j}$ is viewed as an irreducible representation of $\mathrm{GL}_2(\mathbb{F}_p)$. Note that any irreducible representation of $\mathrm{GL}_2(\mathbb{F}_p)$ over $\mathbb{F}_p$ is of the form $V^{i,j}$. A semisimple module M over $\mathbb{F}_p[\mathrm{G}_{\mathbb{Q}}]$ decomposes into a direct sum

$$M \simeq \bigoplus_{i,j} (V^{i,j})^{r_{i,j}(M)},$$

where $r_{i,j}(M) \geq 0$.

Let $K = \mathbb{Q}(E[p])$ be the *splitting field* of $\bar{\rho}$, taken to be the Galois extension of $\mathbb{Q}$ given by $K = \bar{\mathbb{Q}}^{\ker\bar{\rho}}$. Set $G := \mathrm{Gal}(K/\mathbb{Q})$ and identify G with the image of $\bar{\rho}$. Note that when $\bar{\rho}$ is surjective, G is identified with $\mathrm{GL}_2(\mathbb{F}_p)$. There is a natural action of G on the class group Cl_K, and thus on the mod-p class group $\mathrm{Cl}_K/p\,\mathrm{Cl}_K$. The study of the Galois

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

module structure of $\mathrm{Cl}_K/p\,\mathrm{Cl}_K$ is the primary focus of this paper. When $\bar{\rho}$ is surjective, its semisimplification decomposes into a direct sum of irreducible representations of $\mathrm{GL}_2(\mathbb{F}_p)$,

$$(\mathrm{Cl}_K/p\,\mathrm{Cl}_K)^{\mathrm{ss}} \simeq \bigoplus_{i,j} (V^{i,j})^{n_{i,j}}.$$

We are specifically interested in the space of homomorphisms $\mathrm{Hom}_G(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p])$. Note that $\mathrm{Hom}_G(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p]) \neq 0$ precisely when there is a G-stable quotient of $\mathrm{Cl}_K/p\,\mathrm{Cl}_K$ that is isomorphic to $E[p]$. By class field theory, this corresponds to the existence of an unramified $(\mathbb{Z}/p\mathbb{Z})^2$-extension L of K that is Galois over $\mathbb{Q}$, such that $\mathrm{Gal}(L/K) \simeq E[p]$ as a module over $G = \mathrm{Gal}(K/\mathbb{Q})$. We have that

$$n_{1,0} \geq \dim_{\mathbb{F}_p} \mathrm{Hom}_G(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p]),$$

with equality in the special case when the representation of G on $\mathrm{Cl}_K/p\,\mathrm{Cl}_K$ is semisimple.

Given a prime number ℓ, let $\mathcal{E}$ be the Néron model of E over $\mathbb{Z}_\ell$. Let $E^0(\mathbb{Q}_\ell)$ be the subset of points of $E(\mathbb{Q}_\ell) = \mathcal{E}(\mathbb{Z}_\ell)$ that reduce modulo ℓ to the identity component of $E_{/\mathbb{F}_\ell}$. Fix an absolute value $|\cdot|_p : \mathbb{Q}_p^\times \to \mathbb{Q}^\times$, normalized by $|p|_p^{-1} = p$. The *Tamagawa number* at ℓ is set to be $c_\ell(E) := [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)]$, and set $c_\ell^{(p)}(E) := |c_\ell(E)|_p^{-1}$. Therefore, $c_\ell(E)$ is a unit in $\mathbb{Z}_p$ if and only if $c_\ell^{(p)}(E) = 1$. We denote by $\mathrm{Sel}_p(E/\mathbb{Q})$ the p-Selmer group of E over $\mathbb{Q}$ defined by

$$\mathrm{Sel}_p(E/\mathbb{Q}) := \ker\Big\{H^1(\bar{\mathbb{Q}}/\mathbb{Q}, E[p]) \to \prod_\ell H^1(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell, E(\bar{\mathbb{Q}}_\ell))[p]\Big\},$$

where the restriction map for the prime ℓ is the composite

$$H^1(\bar{\mathbb{Q}}/\mathbb{Q}, E[p]) \to H^1(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell, E[p]) \to H^1(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell, E(\bar{\mathbb{Q}}_\ell))[p].$$

The Tate–Shafarevich group

$$Ш(E/\mathbb{Q}) := \ker\Big\{H^1(\bar{\mathbb{Q}}/\mathbb{Q}, E(\bar{\mathbb{Q}})) \to \prod_l H^1(\bar{\mathbb{Q}}_l/\mathbb{Q}_l, E(\bar{\mathbb{Q}}_l))\Big\},$$

fits into an exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0;$$

see [Coa00, page 8, (1)].

Note that $\dim_{\mathbb{F}_p} E(\mathbb{Q})/pE(\mathbb{Q}) = \operatorname{rank} E(\mathbb{Q}) + \dim_{\mathbb{F}_p} E(\mathbb{Q})[p]$, and since $\bar{\rho}$ is irreducible, $E(\mathbb{Q})[p] = 0$, and thus, $\dim_{\mathbb{F}_p} E(\mathbb{Q})/pE(\mathbb{Q}) = \operatorname{rank} E(\mathbb{Q})$. Hence, we find that

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/\mathbb{Q}) = \operatorname{rank} E(\mathbb{Q}) + \dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p].$$

Due to the Cassels–Tate pairing, the $\mathbb{F}_p$-dimension of $Ш(E/\mathbb{Q})[p]$ is even. The following result shows that there is an explicit relationship between $\mathrm{Cl}_K/p\,\mathrm{Cl}_K$ and the

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

p-torsion in the Tate–Shafarevich group $Ш(E/\mathbb{Q})$, and is key to constructing quotients of $\mathrm{Cl}_K/p\,\mathrm{Cl}_K$ that are isomorphic to $E[p]$.

THEOREM 2.1 (Prasad and Shekhar). *Let E be an elliptic curve over $\mathbb{Q}$ and p be an odd prime number at which E has good reduction. With respect to the notation above, suppose that the following assumptions hold:*

(1) $c_\ell^{(p)}(E) = 1$ *for all primes* $\ell \neq p$*;*
(2) $E(\mathbb{Q}_p)[p] = 0$.

Then,

$$\dim_{\mathbb{F}_p} \mathrm{Hom}_G(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p]) \geq \mathrm{rank}\, E(\mathbb{Q}) + \dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p] - 1. \qquad (2\text{-}1)$$

In particular, under the above assumptions, if $Ш(E/\mathbb{Q})[p] \neq 0$*, or* $\mathrm{rank}\, E(\mathbb{Q}) \geq 2$*, then,* $\mathrm{Hom}(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p])$ *is nonzero.*

PROOF. Equation (2-1) follows from [PS21, Theorem 3.1]. The second assertion follows from Corollary 3.2 of *loc. cit.* □

DEFINITION 2.2. Let $\mathcal{I} = \mathcal{I}_p(E)$ be the set of primes $\ell \neq p$ such that:

- E has split multiplicative reduction at ℓ and $E(\mathbb{Q}_\ell)[p]$ has rank 1;
- E has nonsplit multiplicative reduction at ℓ and $E(\mathbb{Q}_\ell)[p]$, and $E(\mathbb{Q}_\ell^{\mathrm{nr}})[p]$ has rank 1.

THEOREM 2.3 (Prasad and Shekhar). *Let $E_{/\mathbb{Q}}$ be an elliptic curve and p an odd prime at which the conditions of Theorem 2.1 are satisfied. Let $\mathcal{I}$ be the finite set from Definition 2.2. Then, the following bound is satisfied*

$$\dim_{\mathbb{F}_p} \mathrm{Hom}(\mathrm{Cl}_K/p\,\mathrm{Cl}_K, E[p]) \leq \mathrm{rank}\, E(\mathbb{Q}) + \dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p] - 1 + \#\mathcal{I}.$$

PROOF. The above result is [PS21, Theorem 4.2]. □

Theorem 2.1 is crucially used in the proof of Theorem 4.4, which is our main result. However, both Theorems 2.1 and 2.3 are applied to prove results in the case when E is a fixed elliptic curve and p varies over all primes at which E has good reduction; see Section 5.

3. Density results for Weierstrass equations with local conditions

In this section, we recall results due to Cremona and Sadek [CS23] for the density of elliptic curves $E_{/\mathbb{Q}}$ satisfying local conditions at a prescribed set of primes. This set of primes may in fact be infinite. The results in this section are used to study the proportion of elliptic curves $E_{/\mathbb{Q}}$, ordered according to *height*, that satisfy the conditions of Theorem 2.1. As always, we fix an odd prime p. Given a tuple of integers $a = (a_1, a_2, a_3, a_4, a_6)$, we have an associated elliptic curve E_a defined by the long Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

The *height* of E_a is defined as follows:

$$\mathrm{ht}(a) = \mathrm{ht}(E_a) := \max_i\{|a_i|^{1/i}\}.$$

We let

$$b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$\Delta(a) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Given a ring R, we let

$$\mathcal{W}(R) = R^5 = \{a = (a_1, a_2, a_3, a_4, a_6) \,|\, a_i \in R\},$$

and let $\Delta(a) = \Delta(E_a)$ be the associated discriminant. Given a prime ℓ, let $\mathcal{W}_M(\mathbb{Z}_\ell)$ be the subset of $\mathcal{W}(\mathbb{Z}_\ell)$ consisting of equations that are *minimal* in the sense of [Sil09, Section VII.1]. Recall that if E is an elliptic curve over $\mathbb{Q}_\ell$, the *Kodaira type* is one of the following choices:

- I_0 if E has good reduction;
- $\mathrm{I}_{\geq 1}$ if E has bad multiplicative reduction, of type I_m for some $m \geq 1$;
- finally, if E has bad additive reduction, we have the following choices: II, III, IV, II^*, III^*, IV^*, I_0^*, $\mathrm{I}_{\geq 1}^*$, the latter meaning type I_m^* for some $m \geq 1$.

We refer to [Sil94, IV, Section 9] for a comprehensive study of Kodaira types and how they may be detected via Tate's algorithm. For $a \in \mathcal{W}(\mathbb{Z}_\ell)$, we say that a has Kodaira type T if the associated elliptic curve E_a has Kodaira type T. Note that this definition applies to nonminimal Weierstrass equations as well. Given a Kodaira type T, let $\mathcal{W}^T(\mathbb{Z}_\ell)$ be the subset of $\mathcal{W}(\mathbb{Z}_\ell)$ of tuples a of Kodaira type T and set $\mathcal{W}_M^T(\mathbb{Z}_\ell) = \mathcal{W}^T(\mathbb{Z}_\ell) \cap \mathcal{W}_M(\mathbb{Z}_\ell)$. Let μ be the Haar measure on $\mathcal{W}(\mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell^5$ and set $\rho^M(\ell) := \mu(\mathcal{W}_M(\mathbb{Z}_\ell))$. Given a Kodaira type T at the prime ℓ, set

$$\rho_T^M(\ell) := \mu(\mathcal{W}_M^T(\mathbb{Z}_\ell)),$$
$$\rho_T(\ell) := \mu(\mathcal{W}^T(\mathbb{Z}_\ell)).$$

According to [CS23, Proposition 2.6], we have that $\rho_T(\ell) = (1 - \ell^{-10})^{-1}\rho_T^M(\ell)$. These local densities are calculated in *loc. cit.*, and these calculations are summarized here.

THEOREM 3.1 (Cremona and Sadek). *Let ℓ be a prime, then $\rho^M(\ell) = 1 - \ell^{-10}$. For each Kodaira type T, the local density $\rho_T^M(\ell)$ is given by the values in Table 1.*

PROOF. The above result follows from [CS23, Propositions 2.1(3), 2.2, 2.5]. □

Let $\mathcal{S}$ be a subset of $\mathcal{W}(\mathbb{Z}) \simeq \mathbb{Z}^5$, the *density* of $\mathcal{S}$ is taken to be the following limit

$$\begin{aligned}\mathfrak{d}(\mathcal{S}) &:= \lim_{x\to\infty} \frac{\#\{a \in \mathcal{S} \mid \mathrm{ht}(a) < x\}}{\#\{a \in \mathbb{Z}^5 \mid \mathrm{ht}(a) < x\}},\\ &= \lim_{x\to\infty} 2^{-5}x^{-16}\#\{a \in \mathcal{S} \mid |a_i| < x^i \text{ for } i = 1, 2, 3, 4, 6\}. \qquad (3\text{-}1)\end{aligned}$$

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

TABLE 1. Local densities: Kodaira types.

T	$\rho_T^M(\ell)$
I_0	$(\ell-1)/\ell$
II	$(\ell-1)/\ell^3$
III	$(\ell-1)/\ell^4$
IV	$(\ell-1)/\ell^5$
I_0^*	$(\ell-1)/\ell^6$
$\mathrm{I}_{\geq 1}^*$	$(\ell-1)/\ell^7$
IV^*	$(\ell-1)/\ell^8$
III^*	$(\ell-1)/\ell^9$
II^*	$(\ell-1)/\ell^{10}$
I_m	$(\ell-1)^2/\ell^{m+2}$
$\mathrm{I}_{\geq m}$	$(\ell-1)/\ell^{m+1}$.

Note that the above limit may not exist. We let $\overline{\mathfrak{d}}(\mathcal{S})$ and $\underline{\mathfrak{d}}(\mathcal{S})$ be the upper and lower limits, respectively. Note that $\overline{\mathfrak{d}}(\mathcal{S})$ and $\underline{\mathfrak{d}}(\mathcal{S})$ are defined by replacing the limit by lim sup and lim inf, respectively, and that these limits do exist unconditionally. If $\mathcal{S}$ is a set of elliptic curves $E_{/\mathbb{Q}}$, we by abuse of notation denote by $\mathcal{S}$ the subset of $\mathcal{W}(\mathbb{Z})$ consisting of all tuples $a = (a_1, a_2, a_3, a_4, a_6)$ such that $E_a \in \mathcal{S}$. Note that since we work with long Weierstrass equations, the choice of a for a given isomorphism class of elliptic curves is not unique. According to [CS23, Theorem 1.1], the proportion of integral Weierstrass equations that are globally minimal is $1/\zeta(10) = 93\,555/\pi^{10} \approx 99.99\%$. Let Φ be a possibly infinite set of prime numbers and for each prime $\ell \in \Phi$, let U_ℓ be a subset of $\mathcal{W}(\mathbb{Z}_\ell)$ defined by a set of congruence classes. In other words, U_ℓ is the inverse image of a subset of $\mathcal{W}(\mathbb{Z}/\ell^M\mathbb{Z})$ for some integer $M > 0$. Let U be the family of conditions $\{U_\ell \mid \ell \in \Phi\}$. Given $N > 0$, let

$$Z_N(U) := \{a \in \mathcal{W}(\mathbb{Z}) \mid a \in U_\ell \text{ for some prime } \ell > N\}.$$

DEFINITION 3.2. The family $U = \{U_\ell \mid \ell \in \Phi\}$ is said to be *admissible* if

$$\lim_{N\to\infty} \mathfrak{d}(Z_N(U)) = 0.$$

Let $\mathcal{W}_U$ be the set of integral Weierstrass equations $a \in \mathcal{W}(\mathbb{Z})$ not satisfying U_ℓ at any prime $\ell \in \Phi$.

PROPOSITION 3.3. *Let U be an admissible family and $s_\ell = \mu(U_\ell)$. Then, $\sum_{\ell\in\Phi} s_\ell$ converges and*

$$\mathfrak{d}(\mathcal{W}_U) = \prod_{\ell\in\Phi}(1 - s_\ell).$$

PROOF. The above result follows from [CS23, Proposition 3.4]. □

DEFINITION 3.4. Given a Kodaira type T, let $U(T)$ be the family of conditions on the set of primes $\ell \neq p$, where U_ℓ consists of local Weierstrass equations $a \in \mathcal{W}(\mathbb{Z}_\ell)$ satisfying T. Thus, $\mathcal{W}_{U(T)}$ consists of integral Weierstrass equations $a \in \mathcal{W}(\mathbb{Z})$ such that E_a does not satisfy T at any prime $\ell \neq p$.

LEMMA 3.5. *Let T be a Kodaira type such that $U(T)$ is admissible, then, the density of $\mathcal{W}_{U(T)}$ exists and equals*

$$\mathfrak{d}(\mathcal{W}_{U(T)}) = \prod_{\ell \neq p}(1 - \rho_T(\ell)) \geq 1 - \sum_{\ell \neq p} \rho_T(\ell).$$

PROOF. The result follows directly from Proposition 3.3. □

THEOREM 3.6. *Let p and ℓ be distinct prime numbers, and E an elliptic curve over $\mathbb{Q}_\ell$. The following assertions hold.*

(1) *Suppose that $p \geq 5$, then, $p|c_\ell(E)$ if and only if E has Kodaira type $T = \mathrm{I}_{pm}$ for $m \in \mathbb{Z}_{\geq 1}$.*
(2) *Suppose that $p = 3$, then, $p|c_\ell(E)$ if and only if E has Kodaira type $T = \mathrm{I}_{3m}$ for $m \in \mathbb{Z}_{\geq 1}$, or $T = \mathrm{IV}$, or $T = \mathrm{IV}^*$.*

PROOF. The result is well known, see [Sil94, Table 4.1, page 365]. □

We come to the main result of this section, which is subsequently used in the proof of our main result in the next section.

DEFINITION 3.7. Recall that p is a fixed prime number. Let $\mathcal{S}_p$ be the set of elliptic curves $E_{/\mathbb{Q}}$ such that $p|c_\ell(E)$ for some prime $\ell \neq p$.

THEOREM 3.8. *Let E be an elliptic curve and p an odd prime number. We have the following assertions:*

(1) *if $p \geq 5$, then,*

$$\bar{\mathfrak{d}}(\mathcal{S}_p) < \zeta(p) - 1;$$

(2) *if $p = 3$, then,*

$$\bar{\mathfrak{d}}(\mathcal{S}_p) < (\zeta(3) - 1) + (\zeta(4) - 1) + (\zeta(7) - 1).$$

PROOF. We prove the result on a case by case basis.

(1) First, we consider the case when $p \geq 5$. Then, by Theorem 3.6(1), we have that $p|c_\ell(E)$ if and only if the Kodaira type T is I_{mp} for some integer $m \geq 1$. Let $U = U(\mathrm{I}_{\geq p})$ be the datum such that $U_\ell = I_{\geq p}$ at every prime $\ell \neq p$. It follows directly from the proof of [CS23, Theorem 4.6] that the datum $U(\mathrm{I}_{\geq 2})$ is admissible, and hence, so is U. From Lemma 3.5,

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

$$\begin{aligned}\mathfrak{d}(\mathcal{W}_U) &= \prod_{\ell\neq p}(1-(1-\ell^{-10})^{-1}(1-\ell^{-1})\ell^{-p})\\ &\geq \prod_{\ell\neq p}(1-\ell^{-p})\\ &\geq 1-\sum_{\ell\neq p}\ell^{-p}.\end{aligned}$$

Since $\mathcal{S}_p$ is contained in the complement of $\mathcal{W}_U$, we find that

$$\overline{\mathfrak{d}}(\mathcal{S}_p) \leq \sum_{\ell\neq p}\ell^{-p} < \zeta(p)-1.$$

(2) We now consider the case when $p = 3$. By Theorem 3.6(2), we have that $3|c_\ell(E)$ if and only if the Kodaira type T is I_{3m} for some integer $m \geq 1$, or, $T = \mathrm{IV}$ or $T = \mathrm{IV}^*$. Let U be such that U_ℓ is the subset of $\mathcal{W}(\mathbb{Z}_\ell)$ with Kodaira type $\mathrm{I}_{\geq 3}$, IV or IV^*, respectively. Note that ℓ^2 divides Δ for such reduction types. Admissibility is a direct consequence of the proof of [CS23, Theorem 4.6].

We find that

$$\begin{aligned}\mathfrak{d}(\mathcal{W}_U) &\geq \prod_{\ell\neq p}(1-\rho_{\mathrm{I}_{\geq 3}}(\ell)-\rho_{\mathrm{IV}}(\ell)-\rho_{\mathrm{IV}^*}(\ell))\\ &\geq \prod_{\ell\neq p}(1-(1-\ell^{-10})^{-1}(1-\ell^{-1})(\ell^{-3}+\ell^{-4}+\ell^{-7}))\\ &\geq \prod_{\ell\neq p}(1-(\ell^{-3}+\ell^{-4}+\ell^{-7}))\\ &\geq 1-\sum_{\ell\neq p}\ell^{-3}-\sum_{\ell\neq p}\ell^{-4}-\sum_{\ell\neq p}\ell^{-7}.\\ &> 1-(\zeta(3)-1)-(\zeta(4)-1)-(\zeta(7)-1).\end{aligned}$$

Thus, we find that

$$\overline{\mathfrak{d}}(\mathcal{S}_p) < (\zeta(3)-1)+(\zeta(4)-1)+(\zeta(7)-1). \qquad \square$$

Definition 3.9. Denote by $\mathcal{S}'_p$ the set of elliptic curves E for which $p \nmid \Delta(E)$ and $E(\mathbb{Q}_p)[p] \neq 0$. Note that for such elliptic curves and $p > 2$, $\widetilde{E}(\mathbb{F}_p)[p] \neq 0$, where $\widetilde{E}$ is the reduction of E.

Let $\Delta \in \mathbb{Z}_{<0}$ with $\Delta \equiv 0, 1 \pmod 4$, and set

$$B(\Delta) := \{ax^2+bxy+cy^2 \in \mathbb{Z}[x,y] \mid a>0, b^2-4ac=\Delta\}.$$

The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{Z}[x,y]$, where a matrix $\sigma = \left(\begin{smallmatrix} p & q\\ r & s\end{smallmatrix}\right)$ sends $x \mapsto (px+qy)$ and $y \mapsto (rx+sy)$. Thus, if $f = ax^2+bxy+cy^2$, the matrix σ acts by

$$f\circ\sigma = a(px+qy)^2+b(px+qy)(rx+sy)+c(rx+sy)^2.$$

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

We note that $B(\Delta)$ is stable under the action of $\mathrm{SL}_2(\mathbb{Z})$ and $B(\Delta)/\,\mathrm{SL}_2(\mathbb{Z})$ is finite; see [Sch87] for additional details.

DEFINITION 3.10. The *Hurwitz class number* $H(\Delta)$ is the order of $B(\Delta)/\,\mathrm{SL}_2(\mathbb{Z})$.

Let $d(p)$ be the number of tuples $a \in \mathcal{W}(\mathbb{F}_p)$ such that $E_a(\mathbb{F}_p)[p] \neq 0$. Note that

$$\frac{d(p)}{\#\mathcal{W}(\mathbb{F}_p)} = \frac{d(p)}{p^5}.$$

LEMMA 3.11. *With respect to the notation above,* $\overline{\mathfrak{d}}(\mathcal{S}'_p) \leq d(p)/p^5$.

PROOF. Given $a \in \mathcal{W}(\mathbb{F}_p)$, let $\mathcal{S}_a$ be the set of $\tilde{a} \in \mathcal{W}(\mathbb{Z})$ that reduce to a. It is easy to see that $\mathfrak{d}(\mathcal{S}_a) = 1/p^5$. Note that $\mathcal{S}'_p$ is contained in the disjoint union $\bigsqcup_a \mathcal{S}_a$, where a ranges over the tuples in $\mathcal{W}(\mathbb{F}_p)$ such that $E_a(\mathbb{F}_p)[p] \neq 0$. The result follows from this. □

PROPOSITION 3.12. *With respect to the notation above,*

$$\overline{\mathfrak{d}}(\mathcal{S}'_p) \leq \begin{cases} \left(\dfrac{p-1}{2p^2}\right) H(1-4p) & \text{if } p \geq 7, \\ \left(\dfrac{p-1}{2p^2}\right)(H(1-4p) + H(p^2+1-6p)) & \text{if } p \leq 5. \end{cases}$$

PROOF. The number of isomorphism classes of elliptic curves E over $\mathbb{F}_p$ such that $E(\mathbb{F}_p)[p] \neq 0$ is

$$\begin{cases} H(1-4p) & \text{if } p \geq 7, \\ H(1-4p) + H(p^2+1-6p) & \text{if } p \leq 5; \end{cases}$$

see [RS23, Corollary 3.11] for additional details. Given $a \in \mathcal{W}(\mathbb{F}_p)$ and associated integral Weierstrass model E_a, then, after a transformation $(X, Y) \mapsto (X + r, Y + sX + t)$, we obtain an elliptic curve with a short Weierstrass equation. Note that two elliptic curves

$$E_{c,d} : Y^2 = X^3 + cX + d$$
$$E_{c',d'} : Y^2 = X^3 + c'X + d'$$

are isomorphic over $\mathbb{F}_p$ if there exists $s \in \mathbb{F}_p^\times$ such that

$$c' = s^4 c \quad \text{and} \quad d' = s^6 d.$$

It is thus easy to see that the number of Weierstrass equations in a given isomorphism class is at most $p^3((p-1)/2)$. Thus, we find that

$$d(p) \leq \begin{cases} p^3\left(\dfrac{p-1}{2}\right) H(1-4p) & \text{if } p \geq 7, \\ p^3\left(\dfrac{p-1}{2}\right)(H(1-4p) + H(p^2+1-6p)) & \text{if } p \leq 5. \end{cases}$$ □

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

4. Results for a fixed prime and varying elliptic curve

In this section, we prove our main results. Throughout, we fix an odd prime number p. Given a set of rational elliptic curves $\mathcal{S}$, we obtain a subset of $\mathcal{W}(\mathbb{Z})$ consisting of all a such that $E_a \in \mathcal{S}$. By abuse of notation, we refer to this set as $\mathcal{S}$ as well. The density $\mathfrak{d}(\mathcal{S})$ is defined as in (3-1). Recall that the upper and lower densities, denoted $\overline{\mathfrak{d}}(\mathcal{S})$ and $\underline{\mathfrak{d}}(\mathcal{S})$, are always defined even if $\mathfrak{d}(\mathcal{S})$ need not be. Let $\mathcal{E}_p$ be the set of elliptic curves $E_{/\mathbb{Q}}$ such that $\operatorname{Hom}_G(\operatorname{Cl}_K, E[p]) \neq 0$. Note that for $E \in \mathcal{E}_p$, we have in particular that $p \mid \# \operatorname{Cl}_K$.

Recall from Definition 3.7 that $\mathcal{S}_p$ is the set of elliptic curves $E_{/\mathbb{Q}}$ such that $p|c_\ell(E)$ for some prime $\ell \neq p$. Recall from Definition 3.9 that $\mathcal{S}'_p$ is the set of elliptic curves E for which $p \nmid \Delta(E)$ and $E(\mathbb{Q}_p)[p] \neq 0$. Denote by $\mathcal{S}''_p$ the set of elliptic curves $E_{/\mathbb{Q}}$ with bad reduction at p. Let $\mathfrak{T}_p$ be the elliptic curves E such that $\text{Ш}(E/\mathbb{Q})[p^\infty]$ is finite and $\text{Ш}(E/\mathbb{Q})[p] \neq 0$.

Proposition 4.1. *Let p be an odd prime. Then,*

$$\underline{\mathfrak{d}}(\mathcal{E}_p) \geq \underline{\mathfrak{d}}(\mathfrak{T}_p \backslash (\mathcal{S}_p \cup \mathcal{S}'_p \cup \mathcal{S}''_p)).$$

Proof. Suppose E is an elliptic curve in $\mathfrak{T}_p \backslash (\mathcal{S}_p \cup \mathcal{S}'_p \cup \mathcal{S}''_p)$, then, since $E \in \mathfrak{T}_p$, we have that $\text{Ш}(E/\mathbb{Q})[p] \neq 0$, and since $E \notin \mathcal{S}_p \cup \mathcal{S}'_p \cup \mathcal{S}''_p$, we have that $p \nmid c_\ell(E)$ for all primes $\ell \neq p$, and $E(\mathbb{Q}_p)[p] = 0$. So long as the residual representation on $E[p]$ is irreducible, it follows from Theorem 2.1 that $\operatorname{Hom}_G(\operatorname{Cl}_K, E[p]) \neq 0$. As a result, E is contained in $\mathcal{E}_p$. By a well-known result of Duke [Duk97], the residual representation on $E[p]$ is irreducible for 100% of elliptic curves, and the result follows. □

Throughout, we assume that for any elliptic curve $E_{/\mathbb{Q}}$, the p-primary part of the Tate–Shafarevich group $\text{Ш}(E/\mathbb{Q})[p^\infty]$ is finite. The density of elliptic curves $E_{/\mathbb{Q}}$ such that $\text{Ш}(E/\mathbb{Q})[p^\infty] \neq 0$ was studied by Delaunay [Del07].

Conjecture 4.2 (Delaunay). *With respect to the notation above,*

$$\underline{\mathfrak{d}}(\mathfrak{T}_p) \geq 1 - \prod_{i \geq 1} (1 - p^{-(2i-1)}) > p^{-1} + p^{-3} - p^{-4}.$$

Moreover, given a set $\mathcal{E}$ of elliptic curves defined by local congruence conditions,

$$\underline{\mathfrak{d}}(\mathfrak{T}_p \cap \mathcal{E}) = \underline{\mathfrak{d}}(\mathfrak{T}_p)\mathfrak{d}(\mathcal{E}).$$

Remark 4.3. For the purposes of this article, we use only the second lower bound predicted by the above conjecture: that is, we assume that

$$\underline{\mathfrak{d}}(\mathfrak{T}_p \cap \mathcal{E}) > (p^{-1} + p^{-3} - p^{-4})\mathfrak{d}(\mathcal{E}),$$

where $\mathcal{E}$ is taken to be the complement of $\mathcal{S}_p \cup \mathcal{S}'_p \cup \mathcal{S}''_p$.

Theorem 4.4. *Let p be an odd prime and assume the above conjecture. Then,*

$$\underline{\mathfrak{d}}(\mathcal{E}_p) > (p^{-1} + p^{-3} - p^{-4})(1 - p^{-1} - \mathfrak{d}_p - \mathfrak{d}'_p),$$

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

where

$$\mathfrak{d}_p = \begin{cases} \zeta(p) - 1 & \textit{if } p \geq 5, \\ (\zeta(3) - 1) + (\zeta(4) - 1) + (\zeta(7) - 1) & \textit{if } p = 3, \end{cases}$$

$$\mathfrak{d}'_p = \begin{cases} \Big(\dfrac{p-1}{2p^2}\Big) H(1-4p) & \textit{if } p \geq 7, \\ \Big(\dfrac{p-1}{2p^2}\Big)(H(1-4p) + H(p^2+1-6p)) & \textit{if } p \leq 5. \end{cases}$$

PROOF. Let $\mathcal{E}$ be the set of elliptic curves in the complement of $\mathcal{S}_p \cup \mathcal{S}'_p \cup \mathcal{S}''_p$. We have from Theorem 3.8 (respectively Proposition 3.12) that $\mathfrak{d}(\mathcal{S}_p) = \mathfrak{d}_p$ (respectively $\mathfrak{d}(\mathcal{S}'_p) = \mathfrak{d}'_p$). Furthermore, we have from Theorem 3.1 and Proposition 3.3 that $\mathfrak{d}(\mathcal{S}''_p) = 1/p$. From Proposition 4.1, we have that $\underline{\mathfrak{d}}(\mathcal{E}_p) \geq \underline{\mathfrak{d}}(\mathfrak{T}_p \backslash (\mathcal{S}_p \cup \mathcal{S}'_p \cup \mathcal{S}''_p))$. According to our assumption,

$$\begin{aligned} \underline{\mathfrak{d}}(\mathfrak{T}_p \backslash (\mathcal{S}_p \cup \mathcal{S}'_p \cup \mathcal{S}''_p)) &= \underline{\mathfrak{d}}(\mathfrak{T}_p \cap \mathcal{E}) \\ &\geq \Big(1 - \prod_{i \geq 1} (1 - p^{-(2i-1)})\Big) \mathfrak{d}(\mathcal{E}) \\ &> (p^{-1} + p^{-3} - p^{-4}) \mathfrak{d}(\mathcal{E}) \\ &= (p^{-1} + p^{-3} - p^{-4})(1 - p^{-1} - \mathfrak{d}_p - \mathfrak{d}'_p), \end{aligned}$$

and the result follows. □

COROLLARY 4.5. *Assume Conjecture 4.2. Then,*

$$\underline{\mathfrak{d}}(\mathcal{E}_p) \geq p^{-1} + O(p^{-3/2+\epsilon}).$$

In other words, for any choice of $\epsilon > 0$, there is a constant $C > 0$, depending on ϵ and independent of p, such that

$$\underline{\mathfrak{d}}(\mathcal{E}_p) \geq p^{-1} - Cp^{-3/2+\epsilon}.$$

PROOF. According to Theorem 4.4,

$$\begin{aligned} \underline{\mathfrak{d}}(\mathcal{E}_p) &> (p^{-1} + p^{-3} - p^{-4})(1 - p^{-1} - \mathfrak{d}_p - \mathfrak{d}'_p) \\ &> p^{-1} - p^{-1}(p^{-1} + \mathfrak{d}_p + \mathfrak{d}'_p). \end{aligned}$$

We have that

$$\zeta(p) - 1 = 2^{-p} + \sum_{n \geq 3} n^{-p} < 2^{-p} + \int_2^\infty x^{-p} dx = 2^{-p} \Big(\frac{p+1}{p-1}\Big),$$

and hence,

$$\mathfrak{d}_p = O(2^{-p}) = O(p^{-1/2+\epsilon}).$$

However, it follows from known results that

$$\mathfrak{d}'_p = O(p^{-1/2} \log p (\log\log p)^2) = O(p^{-1/2+\epsilon}),$$

(see [LJ87, Proposition 1.9]) and the result follows. □

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

5. Results for a fixed elliptic curve and varying prime

In this section, we prove results for a fixed elliptic curve $E_{/\mathbb{Q}}$ and varying prime p. We assume throughout that E does not have complex multiplication, and that the Tate–Shafarevich group $Ш(E/\mathbb{Q})$ is finite. Given a prime p, we let $K_p = \mathbb{Q}(E[p])$. We make a number of observations with regards to the variation of $\mathrm{Cl}_{K_p}/p\,\mathrm{Cl}_{K_p}$, where p varies over all primes p.

Theorem 5.1. *Let $E_{/\mathbb{Q}}$ be an elliptic curve; assume that the following conditions are satisfied:*

(1) *$Ш(E/\mathbb{Q})$ is finite;*
(2) *$\operatorname{rank} E(\mathbb{Q}) \le 1$;*
(3) *E does not have complex multiplication.*

Then, for 100% of primes p, we have that $\mathrm{Hom}_G(\mathrm{Cl}_{K_p}/p\,\mathrm{Cl}_{K_p}, E[p]) = 0$.

Proof. Note that for all but finitely many primes p:

(1) E has good reduction at p;
(2) $E(\mathbb{Q}_\ell)[p] = 0$ for all primes ℓ at which E has bad reduction;
(3) $Ш(E/\mathbb{Q})[p] = 0$;
(4) the representation on $E[p]$ is irreducible;
(5) $c_\ell^{(p)}(E) = 1$ for all primes ℓ at which E has bad reduction.

Thus, it follows from Theorem 2.3 that we have that $\mathrm{Hom}_G(\mathrm{Cl}_{K_p}/p\,\mathrm{Cl}_{K_p}, E[p]) = 0$ provided $E(\mathbb{Q}_p)[p] = 0$. Let $\widetilde{E}$ be the reduction of E over $\mathbb{F}_p$. The formal group $\widehat{E}(\mathbb{Z}_p)$ of E at p has no nontrivial p-torsion. Thus, if p is a prime of good reduction, the natural map $E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$ induces an injection

$$E(\mathbb{Q}_p)[p] \to \widetilde{E}(\mathbb{F}_p)[p].$$

A prime p at which E has good reduction is called an *anomalous prime* if $\widetilde{E}(\mathbb{F}_p)[p] \neq 0$. It is well known that for a non-CM elliptic curve, 100% of primes are nonanomalous (see for instance [Mur97]). Thus, $E(\mathbb{Q}_p)[p] = 0$ for 100% of primes p, and thus the result follows. □

Theorem 5.2. *Let $E_{/\mathbb{Q}}$ be an elliptic curve and assume that the following conditions are satisfied:*

(1) *$Ш(E/Q)$ is finite;*
(2) *$\operatorname{rank} E(\mathbb{Q}) \ge 2$;*
(3) *E does not have complex multiplication.*

Then, for 100% of primes p,

$$\dim \mathrm{Hom}_G(\mathrm{Cl}_{K_p}/p\,\mathrm{Cl}_{K_p}, E[p]) \ge \operatorname{rank} E(\mathbb{Q}) - 1.$$

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

PROOF. It follows from the proof of Theorem 5.1 that for 100% of primes p, all of the following conditions are satisfied:

(1) E has good reduction at p;
(2) the representation on $E[p]$ is irreducible;
(3) $c_\ell^{(p)}(E) = 1$ for all primes ℓ at which E has bad reduction;
(4) $E(\mathbb{Q}_p)[p] = 0$.

It follows from Theorem 2.1 that

$$\dim \operatorname{Hom}_G(\mathrm{Cl}_{K_p} / p\,\mathrm{Cl}_{K_p}, E[p]) \geq \operatorname{rank} E(\mathbb{Q}) - 1. \qquad \square$$

6. Computational results

In this section, we present some computations of $\mathrm{Cl}_K / 3\,\mathrm{Cl}_K$, where $K = \mathbb{Q}(E[3])$, for certain families of elliptic curves E. Due to the difficulty of computing statistics for larger extensions, we primarily restrict ourselves to the case where $\mathrm{Gal}(K/\mathbb{Q}) \subset \mathrm{GL}_2(\mathbb{F}_3)$ is the normalizer of a split Cartan subgroup. This is the smallest irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. We include also a few additional calculations where the Galois group is the normalizer of a nonsplit Cartan subgroup.

We note that the hypotheses of [PS21] are often violated in these cases. Specifically, a majority of such E has bad reduction at 3. In addition, all ramification at 3 is tame as the Galois group has order prime to 3: thus, any such E for which $a_3(E) \equiv 1 \pmod 3$ has 3 as a local torsion prime. We computed our examples without regard to these considerations. We have verified that every computation violating the lower bound of [PS21] does not satisfy their hypotheses.

6.1. Normalizer of a split Cartan: varying *j*-invariants. We use the formula of Zywina [Zyw15, Theorem 1.2],

$$j_2(t) = 27\frac{(t+1)^3(t-3)^3}{t^3}$$

such that any elliptic curve with such a j-invariant has $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ contained in the normalizer of a split Cartan subgroup. For any t, let E_t denote the elliptic curve of smallest conductor with j-invariant $j_2(t)$ and let K_t denote the field $\mathbb{Q}(E_t[3])$. We computed $\mathrm{Sel}_3(E_t/\mathbb{Q})$ as well as the Galois module structure of $\mathrm{Cl}_{K_t}/3$ for the 599 elliptic curves in the set

$$S_0 = \{E_{a/b} \mid |a| \leq 50, 1 \leq b \leq 10, [K_t : \mathbb{Q}] = 8\}.$$

Let L_t denote the unique biquadratic subfield of K_t; note that L_t necessarily contains $\mathbb{Q}(\sqrt{-3})$. In each case, there was $d_t \geq 0$ such that there was an isomorphism

$$\mathrm{Cl}_{K_t}/3 \cong \mathrm{Cl}_{L_t}/3 \oplus E_t[3]^{d_t}$$

as $\mathrm{Gal}(K_t/\mathbb{Q})$-modules. Note that $\mathrm{Gal}(K_t/\mathbb{Q})$ acts on $\mathrm{Cl}_{L_t}/3$ via its abelianization.

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

TABLE 2. Mod 3 class group data.

$\dim \mathrm{Cl}_{L_t}/3$	$\# t$
0	447
1	123
2	28
3	1

TABLE 3. 3 Selmer group data (i).

$\dim \mathrm{Sel}_3(E_t/\mathbb{Q})$	d_t	$\# t$
0	0	103
0	1	26
1	0	228
1	1	52
1	2	2
2	0	95
2	1	74
2	2	2
3	0	4
3	1	12
3	2	1

Our interest here is primarily in comparing $\mathrm{Sel}_3(E_t/\mathbb{Q})$ and d_t. We briefly report the data for $\mathrm{Cl}_{L_t}/3$ in Table 2. The only curve in our sample with $\dim \mathrm{Cl}_{L_t}/3 = 3$ was $E_{-46/3}$ with $L_t = \mathbb{Q}(\sqrt{-3}, \sqrt{2917})$.

Please see Table 3 for the other quantities.

We remark that the restriction to E with specified 3-torsion fields obviously biases the distribution of 3-Selmer groups. Although it is unwise to extrapolate too much from this limited data, we note that for t with $\dim \mathrm{Sel}_3(E_t/\mathbb{Q}) \leq 1$, the dimension of $\mathrm{Cl}_{K_t}/3$ appears to be roughly the same (being nonzero around 19% of the time) whether the Selmer group has dimension zero or one. By contrast, for Selmer groups of dimension two, the proportion having $d_t \geq 1$ is much larger at 44%. For Selmer groups of dimension three, it is much larger than that in this limited sample.

Granting the limits of this data set, it certainly appears that $\mathrm{Sel}_3(E_t/\mathbb{Q})$ has a significant effect on d_t, but there are additional influences as well that are not currently clear.

6.2. Normalizer of a split Cartan: fixed *j*-invariants. We also investigated two quadratic twist families. Let E_1 denote the elliptic curve

$$y^2 + xy + y = x^3 - 141x + 624$$

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

TABLE 4. 3 Selmer group data (ii).

$\dim \mathrm{Sel}_3(E_{1,t}/\mathbb{Q})$	$d_{1,t}$	$\# t$
0	0	341
0	1	1
1	0	74
1	1	31
1	2	2
2	1	140
2	2	18
3	2	1

with $j(E_1) = 857\,375/8$ and conductor $10\,082 = 2 \cdot 71^2$. For any squarefree t, let $E_{1,t}$ denote the quadratic twist of E_1 by t and let $K_{1,t}$ denote the field $\mathbb{Q}(E_{1,t}[3])$. Then, $\mathrm{Gal}(K_{1,t}/\mathbb{Q})$ is the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. We note that each $K_{1,t}$ contains the biquadratic field $L_1 = \mathbb{Q}(\sqrt{-3}, \sqrt{-71})$, which has trivial 3-class group.

Consider the set of 608 elliptic curves

$$S_1 = \{E_{1,t} \mid 1 \leq t \leq 1000, t \text{ squarefree}\}.$$

In each case, we computed a $\mathrm{Gal}(K_{1,t}/\mathbb{Q})$-isomorphism

$$\mathrm{Cl}_{K_{1,t}}/3 \cong E_{1,t}[3]^{d_{1,t}}$$

for some $d_{1,t}$. We computed the data as seen in Table 4.

We note here that the dependence of $d_{1,t}$ on $\mathrm{Sel}_3(E_{1,t}/\mathbb{Q})$ is more clear than in the case of varying j-invariants: the lower bound of [PS21] (although, as noted, the hypotheses are often violated in this data set) appears to control most of the behaviour of $d_{1,t}$.

We computed analogous data for the elliptic curve E_2 given by

$$y^2 = x^3 - 83\,667\,346\,875x - 10\,711\,930\,420\,406\,250$$

with $j(E_2) = -42\,875/8$ and conductor $6962 = 2 \cdot 59^2$. With notation as above, we consider the set of 608 quadratic twists

$$S_2 = \{E_{2,t} \mid 1 \leq t \leq 1000, t \text{ squarefree}\}.$$

Each 3-division field field $K_{2,t}$ has Galois group the normalizer of a split Cartan subgroup and contains the biquadratic field $L_2 = \mathbb{Q}(\sqrt{-3}, \sqrt{-59})$. This field has class group $\mathbb{Z}/3$, and for each t, we computed a $\mathrm{Gal}(K_{2,t}/\mathbb{Q})$-isomorphism

$$\mathrm{Cl}_{K_{2,t}}/3 \cong \mathrm{Cl}_{L_2}/3 \oplus E_{2,t}[3]^{d_{2,t}}$$

for some $d_{2,t}$ (see Table 5).

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

TABLE 5. 3 Selmer group data (iii).

$\dim \mathrm{Sel}_3(E_{2,t}/\mathbb{Q})$	$d_{2,t}$	# t
0	0	54
0	1	18
1	0	332
1	1	165
2	0	18
2	1	13
2	2	2
3	2	6

TABLE 6. 3 Selmer group data (iv).

$\dim \mathrm{Sel}_3(E_{3,t}/\mathbb{Q})$	$d_{3,t}$	# t
0	0	18
0	1	2
1	0	18
1	1	14
1	2	1
2	1	8

This behaviour appears somewhat less straightforward than for S_1. The distribution of $\mathrm{Sel}_3(E_{2,t}/\mathbb{Q})$ is obviously quite different from that of $\mathrm{Sel}_3(E_{1,t}/\mathbb{Q})$ and the effect on $d_{2,t}$ is less clear. We do note that the distributions of $d_{1,t}$ and $d_{2,t}$ ignoring Selmer groups are similar, which is somewhat curious.

6.3. Normalizer of a nonsplit Cartan: fixed *j*-invariant. We compiled very limited data in one case where the mod 3 Galois image is the normalizer of a nonsplit Cartan subgroup. Consider the elliptic curve E_3 given by

$$y^2 = x^3 + x^2 - 2x - 8$$

with $j(E_3) = -64$ and conductor $1568 = 2^5 \cdot 7^2$. We consider its set of 61 twists

$$S_3 = \{E_{3,t} \mid 1 \leq t \leq 100, t \text{ squarefree}\}.$$

For each t, we have an isomorphism of $\mathrm{Gal}(K_{3,t}/\mathbb{Q})$-modules

$$\mathrm{Cl}_{K_{3,t}}/3 \cong E_{3,t}[3]^{d_{3,t}}$$

for some $d_{3,t}$ (see Table 6).

There is too little data here to provide anything more than wild speculations; unfortunately the computations rapidly became very time consuming beyond this point.

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

References

[Bha05] M. Bhargava, 'The density of discriminants of quartic rings and fields', *Ann. of Math. (2)* **162** (2005), 1031–1063.

[CL84] H. Cohen and H. W. Lenstra, 'Heuristics on class groups of number fields', in: *Number Theory Noordwijkerhout 1983* (ed. H. Jager) (Springer, Berlin–Heidelberg, 1984), 33–62.

[Coa00] J. H. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, Lecture Notes at the Tata Institute of Fundamental Research, 88 (Narosa, New Delhi, 2000).

[CS23] J. E. Cremona and M. Sadek, 'Local and global densities for Weierstrass models of elliptic curves', *Math. Res. Lett.* **30**(2) (2023), 413–461.

[Del07] C. Delaunay, 'Heuristics on class groups and on Tate–Shafarevich groups: the magic of the Cohen–Lenstra heuristics', in *Ranks of Elliptic Curves and Random Matrix Theory*, London Mathematical Society Lecture Note Series, 341 (eds. J. B. Conrey, D. W. Farmer, F. Mezzadri and N. C. Snaith) (Cambridge University Press, Cambridge, 2007), 323–340.

[DH71] H. Davenport and H. A. Heilbronn, 'On the density of discriminants of cubic fields. II', *Proc. Roy. Soc. Lond. A* **322**(1551) (1971), 405–420.

[Duk97] W. Duke, 'Elliptic curves with no exceptional primes', *C. R. Acad. Sci. Sér. 1* **325**(8) (1997), 813–818.

[EPW17] J. Ellenberg, L. Pierce and M. Wood, 'On ℓ-torsion in class groups of number fields', *Algebra Number Theory* **11**(8) (2017), 1739–1778.

[EV07] J. S. Ellenberg and A. Venkatesh, 'Reflection principles and bounds for class group torsion', *Int. Math. Res. Not. IMRN* **2007** (2007), Article no. 002.

[FK07] É. Fouvry and J. Klüners, 'On the 4-rank of class groups of quadratic number fields', *Invent. Math.* **167**(3) (2007), 455–513.

[Lec18] E. Lecouturier, 'On the Galois structure of the class group of certain Kummer extensions', *J. Lond. Math. Soc. (2)* **98**(1) (2018), 35–58.

[LJ87] H. W. Lenstra Jr, 'Factoring integers with elliptic curves', *Ann. of Math. (2)* **126** (1987), 649–673.

[Maz77] B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* **47** (1978), 33–186; 1977. With an appendix by Mazur and M. Rapoport.

[MC90] J. Martinet and H. Cohen, 'Étude heuristique des groupes de classes des corps de nombres', *J. reine angew. Math.*, **404** (1990), 455–513.

[Mur97] V. K. Murty, 'Modular forms and the Chebotarev density theorem II', in: *Analytic Number Theory*, London Mathematical Society Lecture Note Series, 247 (ed. Y. Motohashi) (Cambridge University Press, Cambridge, 1997), 287–308.

[PS21] D. Prasad and S. Shekhar, 'Relating the Tate–Shafarevich group of an elliptic curve with the class group', *Pacific J. Math.* **312**(1) (2021), 203–218.

[RS23] A. Ray and R. Sujatha, 'Arithmetic statistics for the fine Selmer group in Iwasawa theory', *Res. Number Theory* **9**(3) (2023), Paper no. 59, 25 pages.

[Sch87] R. Schoof, 'Nonsingular plane cubic curves over finite fields', *J. Combin. Theory Ser. A* **46**(2) (1987), 183–211.

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151 (Springer-Verlag, New York, 1994).

[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edn, Graduate Texts in Mathematics, 106 (Springer, Dordrecht, 2009).

[SS19] K. Schaefer and E. Stubley, 'Class groups of Kummer extensions via cup products in Galois cohomology', *Trans. Amer. Math. Soc.* **372**(10) (2019), 6927–6980.

[Was97] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edn, Graduate Texts in Mathematics, 83 (Springer-Verlag, New York, 1997).

[Wat04] M. Watkins, 'Class numbers of imaginary quadratic fields', *Math. Comp.* **73**(246) (2004), 907–938.

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press

[Won99] S. Wong, ‘On the rank of ideal class groups’, in: *Number Theory: Fifth Conference of the Canadian Number Theory Association*, CRM Proceedings and Lecture Notes, 19 (eds. R. Gupta and K. J. Williams) (American Mathematical Society, Providence, RI, 1999), 377–383.

[Woo16] M. M. Wood, ‘Asymptotics for number fields and class groups’, in: *Directions in Number Theory*, Association for Women in Mathematics Series, 3 (eds. E. E. Eischen, L. Long, R. Pries and K. E. Stange) (Springer, Cham, 2016), 291–339.

[WWE20] P. Wake and C. Wang-Erickson, ‘The rank of Mazur’s Eisenstein ideal’, *Duke Math. J.* **169**(1) (2020), 31–115.

[Zyw15] D. Zywina, ‘On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$’, Preprint, 2015, arXiv:1508.07660.

ANWESH RAY, Chennai Mathematical Institute, H1, SIPCOT IT Park,
Kelambakkam, Siruseri, Tamil Nadu 603103, India
e-mail: ar2222@cornell.edu

TOM WESTON, Department of Mathematics,
University of Massachusetts, Amherst, MA, USA
e-mail: weston@math.umass.edu

https://doi.org/10.1017/S1446788724000156 Published online by Cambridge University Press