Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Tamagawa Products for Elliptic Curves Over Number Fields

par Yunseo CHOI, Sean LI, Apoorva PANIDAPU et Casia SIEGEL

RÉSUMÉ. Dans un article récent, Griffin, Ono et Tsai construisent une série L pour prouver que la proportion des courbes elliptiques de Weierstrass courtes sur $\mathbb{Q}$ dont le produit de Tamagawa est trivial est de $0,5054\ldots$ et que la valeur moyenne du produit de Tamagawa est de $1,8183\ldots$. Suite à leur travail, nous généralisons leur série L au cas où $\mathbb{Q}$ est remplacé par un corps de nombres quelconque K en posant

$$L_{\mathrm{Tam}}(K,s) := \sum_{m=1}^{\infty} \frac{P_{\mathrm{Tam}}(K,m)}{m^s},$$

où $P_{\mathrm{Tam}}(K,m)$ est la proportion des courbes elliptiques de Weierstrass courtes sur K dont le produit de Tamagawa est égal à m. Nous construisons ensuite des chaînes de Markov pour calculer les valeurs exactes de $P_{\mathrm{Tam}}(K,m)$ pour tous les corps de nombres K et tous les entiers positifs m. Comme corollaire, nous calculons également le produit de Tamagawa moyen $L_{\mathrm{Tam}}(K,-1)$. Nous utilisons ensuite ces résultats pour borner uniformément $P_{\mathrm{Tam}}(K,1)$ et $L_{\mathrm{Tam}}(K,-1)$ en fonction du degré de K. Enfin, nous montrons qu'il existe des suites de corps K pour lesquelles $P_{\mathrm{Tam}}(K,1)$ et $L_{\mathrm{Tam}}(K,-1)$ tendent respectivement vers 0 et l'infini, ainsi que des suites de K pour lesquelles $P_{\mathrm{Tam}}(K,1)$ et $L_{\mathrm{Tam}}(K,-1)$ tendent vers 1.

ABSTRACT. In recent work, Griffin, Ono, and Tsai constructs an L−series to prove that the proportion of short Weierstrass elliptic curves over $\mathbb{Q}$ with trivial Tamagawa product is $0.5054\ldots$ and that the average Tamagawa product is $1.8183\ldots$. Following their work, we generalize their L-series over arbitrary number fields K to be

$$L_{\mathrm{Tam}}(K,s) := \sum_{m=1}^{\infty} \frac{P_{\mathrm{Tam}}(K,m)}{m^s},$$

where $P_{\mathrm{Tam}}(K,m)$ is the proportion of short Weierstrass elliptic curves over K with Tamagawa product m. We then construct Markov chains to compute the exact values of $P_{\mathrm{Tam}}(K,m)$ for all number fields K and positive integers m.

As a corollary, we also compute the average Tamagawa product $L_{\mathrm{Tam}}(K, -1)$. We then use these results to uniformly bound $P_{\mathrm{Tam}}(K, 1)$ and $L_{\mathrm{Tam}}(K, -1)$ in terms of the degree of K. Finally, we show that there exist sequences of K for which $P_{\mathrm{Tam}}(K, 1)$ tends to 0 and $L_{\mathrm{Tam}}(K, -1)$ to ∞, as well as sequences of K for which $P_{\mathrm{Tam}}(K, 1)$ and $L_{\mathrm{Tam}}(K, -1)$ tend to 1.

1. Introduction

Although there are no elliptic curves $E/\mathbb{Q}$ with everywhere good reduction, *Tamagawa trivial curves* satisfy $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)] = 1$ for all primes p, where $E_0(\mathbb{Q}_p)$ is the subgroup consisting of the nonsingular points of $E(\mathbb{Q}_p)$ after reduction modulo p. For example, the curve

$$E/\mathbb{Q} : y^2 = x^3 + 3x + 1,$$

which has discriminant $-2^4 \cdot 3^3 \cdot 5$, satisfies $[E(\mathbb{Q}_2) : E_0(\mathbb{Q}_2)] = [E(\mathbb{Q}_3) : E_0(\mathbb{Q}_3)] = [E(\mathbb{Q}_5) : E_0(\mathbb{Q}_5)] = 1$. In recent work, Griffin, Ono, and Tsai [5, Corollary 1.2] prove that when the elliptic curves in short Weierstrass form are ordered by height, the proportion of elliptic curves that are Tamagawa trivial is $0.5054\ldots$.

For every elliptic curve over $\mathbb{Q}$, we associate the *Tamagawa product*

$$\mathrm{Tam}(E/\mathbb{Q}) := \prod_{p \text{ prime}} c_p,$$

where $c_p := [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is the *Tamagawa number* at p. Then $E/\mathbb{Q}$ is Tamagawa trivial if and only if $\mathrm{Tam}(E/\mathbb{Q}) = 1$. It is known that $\mathrm{Tam}(E/\mathbb{Q})$ can be arbitrarily large (see, for instance, [9, Table C.15.1]), and so it is natural to ask whether there is an average Tamagawa product for $E/\mathbb{Q}$. The numerics by Balakrishnan et al. [2, Figure A.14] suggest that the average Tamagawa product over $\mathbb{Q}$ exists and is in the neighborhood of 1.82. This speculation was confirmed by Griffin et al. [5, Theorem 1.3], who constructed a new L-function and proved that the exact average is $L_{\mathrm{Tam}}(-1) = 1.8183\ldots$.

It is then natural to ask about the values of the same arithmetic statistics over an arbitrary number field K. To this end, we define the Tamagawa product $\mathrm{Tam}(E/K)$ for an elliptic curve E/K. We let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, the ring of integers of K, that lies above a rational prime p. Recall that there is a unique extension $v := v_{\mathfrak{p}}$ to K corresponding to $\mathfrak{p}$. We let K_v be the completion of K with respect to v. Then the Tamagawa product for elliptic curves E/K is

$$\mathrm{Tam}(E/K) := \prod_{\mathfrak{p}} c_{\mathfrak{p}},$$

where $c_{\mathfrak{p}} := [E(K_v) : E_0(K_v)]$ is the Tamagawa number at $\mathfrak{p}$.

Generalizing the work of Griffin et al. [5], we compute the arithmetic statistics of Tamagawa products over arbitrary number fields K. Specifically, we compute the proportion of curves with fixed $\mathrm{Tam}(E/K)$ over short Weierstrass curves

$$E = E(a_4, a_6) : y^2 = x^3 + a_4 x + a_6,$$

where $a_4, a_6 \in \mathcal{O}_{K_v}$. We require a consistent way to count sets of elliptic curves to compute the proportion of curves with fixed $\mathrm{Tam}(E/K)$. To do so, we order E/K by their naive height. Recall [4] that the naive height of E/K is

$$\mathrm{ht}(E/K) := \prod_{\mathfrak{p} \in M_K} \max \left\{ 4|a_4|_{\mathfrak{p}}^3, 27|a_6|_{\mathfrak{p}}^2, 1 \right\},$$

where M_K contains all Archimedean and non-Archimedean places on K. To count the number of E/K with height $\leq X$, we introduce:

$$\mathcal{N}(K, X) := \#\{E := E(a_4, a_6) : \mathrm{ht}(E/K) \leq X\}.$$

Similarly, to count the number of E/K with Tamagawa product m and height $\leq X$, we define

$$\mathcal{N}_m(K, X) := \#\{E := E(a_4, a_6) : \mathrm{ht}(E/K) \leq X \text{ with } \mathrm{Tam}(E/K) = m\}.$$

We now formally define the proportion of elliptic curves $E(a_4, a_6)$ with Tamagawa number m to be

$$P_{\mathrm{Tam}}(K, m) := \lim_{X \to +\infty} \frac{\mathcal{N}_m(K, X)}{\mathcal{N}(K, X)}.$$

We compute the global statistic $P_{\mathrm{Tam}}(K, m)$ by computing the local statistics of Tamagawa numbers at each $\mathfrak{p}$. Namely, we let $\delta_{K,\mathfrak{p}}(c)$ be the local proportion of elliptic curves with Tamagawa number c at $\mathfrak{p}$ when the elliptic curves are ordered by height. The exact values of $\delta_{K,\mathfrak{p}}(c)$ are given in Propositions 3.3, 4.5 and 5.5. Using $\delta_{K,\mathfrak{p}}(c)$, we define an analogue of the L-function as presented in [5]:

$$L_{\mathrm{Tam}}(K, s) = \prod_{\mathfrak{p}} \left(\frac{\delta_{K,\mathfrak{p}}(1)}{1^s} + \frac{\delta_{K,\mathfrak{p}}(2)}{2^s} + \frac{\delta_{K,\mathfrak{p}}(3)}{3^s} + \dots \right).$$

Remark 1.1. All of the counts in this paper assume that the elliptic curves are ordered by height. But the congruence conditions are over bounded powers of π which are pairwise relatively prime for different prime ideals, so we can compute the L-series as the product above.

Our first result proves that $P_{\mathrm{Tam}}(K, m)$ are the Dirichlet coefficients of $L_{\mathrm{Tam}}(K, m)$.

Theorem 1.2. *If K is a number field, then $P_{\mathrm{Tam}}(K, m)$ are the Dirichlet coefficients of*

$$L_{\mathrm{Tam}}(K, s) = \sum_{m=1}^{\infty} \frac{P_{\mathrm{Tam}}(K, m)}{m^s}.$$

Remark 1.3. Theorem 1.2 gives $P_{\mathrm{Tam}}(K, m)$ for all number fields K and every positive integer m. In particular, the theorem makes no assumption on the class number h_K, the structure of the units in $\mathcal{O}_K^{\times}$, as well as the possible splitting types of primes in K.

Corollary 1.4. *If K is a number field, then the following are true.*

(1) *We have*

$$P_{\mathrm{Tam}}(K, 1) = \prod_{\mathfrak{p}} \delta_{K,\mathfrak{p}}(1).$$

(2) *The average Tamagawa product $L_{\mathrm{Tam}}(K, -1)$ is well-defined by absolute convergence.*

In the following example, we illustrate the results of Theorem 1.2 by computing $P_{\mathrm{Tam}}(K, 1)$ and $L_{\mathrm{Tam}}(K, -1)$ for all imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$ with class number 1. For the values of $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), m)$ with $m \geq 2$, refer to Section 7. For further examples, also refer to Section 7, where we compute $P_{\mathrm{Tam}}(K, m)$ and $L_{\mathrm{Tam}}(K, -1)$ for real quadratic fields $\mathbb{Q}(\sqrt{D})$ with squarefree $D < 10^4$ and a number field with Galois group S_4.

Example 1.5. Tables 1.1 and 1.2 display the convergence to $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), 1)$ and $L_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), -1)$ for class number 1 quadratic number fields.

TABLE 1.1. Convergence to $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), 1)$.

$\mathcal{N}_1(\mathbb{Q}(\sqrt{-D}), X)/\mathcal{N}(\mathbb{Q}(\sqrt{-D}), X)$								
X	$\sqrt{-1}$	$\sqrt{-2}$	$\sqrt{-3}$	$\sqrt{-7}$	$\sqrt{-11}$	$\sqrt{-19}$	$\sqrt{-43}$	$\sqrt{-67}$	$\sqrt{-163}$
10^4	0.542	0.488	0.663	0.357	0.609	0.620	0.657	0.560	0.450
10^5	0.539	0.460	0.665	0.359	0.599	0.678	0.716	0.711	0.636
10^6	0.528	0.468	0.660	0.343	0.586	0.667	0.726	0.744	0.728
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
∞	0.529	0.468	0.661	0.349	0.581	0.665	0.733	0.750	0.763

In Table 1.1, $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), 1)$ is noticeably smaller when $D = 7$. On the other hand, in Table 1.2, $L_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), -1)$ is noticeably larger when $D = 7$. The variance in $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), 1)$ and $L_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), -1)$ is due to the splitting type of small primes, since $\delta_{K,\mathfrak{p}}(1)$ is smaller and $\sum_{m=1}^{\infty} \delta_{K,\mathfrak{p}}(m)m$ is larger when $\mathfrak{p}$ has small norm (see Propositions 3.3, 4.5 and 5.5). Indeed, 2

TABLE 1.2. Convergence to $L_{\text{Tam}}(\mathbb{Q}(\sqrt{-D}), -1)$.

$\sum_{\text{ht}(\mathbb{Q}(\sqrt{-D}),E)\leq X} \text{Tam}(\mathbb{Q}(\sqrt{-D})), E)/N(\mathbb{Q}(\sqrt{-D}); X)$								
X	$\sqrt{-1}$	$\sqrt{-2}$	$\sqrt{-3}$	$\sqrt{-7}$	$\sqrt{-11}$	$\sqrt{-19}$	$\sqrt{-43}$	$\sqrt{-67}$	$\sqrt{-163}$
10^4	1.751	2.054	1.589	2.570	1.850	1.718	1.535	1.698	2.017
10^5	1.720	1.979	1.538	2.417	1.763	1.537	1.393	1.403	1.612
10^6	1.708	1.946	1.508	2.418	1.723	1.519	1.361	1.333	1.372
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
∞	1.678	1.904	1.487	2.376	1.708	1.480	1.331	1.300	1.277

splits only in $\mathbb{Q}(\sqrt{-7})$. For general number fields K, the possible splitting types of primes are determined by $d := \deg K$. It is then natural to ask whether $P_{\text{Tam}}(K, 1)$ and $L_{\text{Tam}}(\mathbb{Q}(\sqrt{-D}), -1)$ can be uniformly bounded as a function of d. We answer this question in the following corollary, where $\zeta(s)$ is the Riemann zeta-function and B_n is the nth Bernoulli number.

Corollary 1.6. *If K has degree d, then*

$$(0.5054)^d < P_{\text{Tam}}(\mathbb{Q}, 1)^d \leq P_{\text{Tam}}(K, 1) < (-1)^{d+1} \frac{2(2d)!}{B_{2d}(2\pi)^{2d}} = \frac{1}{\zeta(2d)}$$

and

$$\frac{\zeta(2d)}{\zeta(4d)} = (-1)^d \frac{B_{2d}(4d)!}{B_{4d}(2d)!(2\pi)^{2d}} < L_{\text{Tam}}(K, -1) \leq L_{\text{Tam}}(\mathbb{Q}, -1)^d < (1.8184)^d.$$

As $d \to \infty$ in Corollary 1.6, the given lower and upper bounds for $P_{\text{Tam}}(K, 1)$ tend to 0 and 1. We can then ask whether $P_{\text{Tam}}(K, 1)$ can be arbitrarily close to 0 or arbitrarily close to 1 as $d \to \infty$. More formally, let

$$t^-(d) := \inf_{\deg K = d} \{P_{\text{Tam}}(K, 1)\} \quad \text{and} \quad t^+(d) := \sup_{\deg K = d} \{P_{\text{Tam}}(K, 1)\}$$

to be the infimum and supremum of the Tamagawa trivial proportion over number fields K with degree d.

Similarly, from Corollary 1.6, as $d \to \infty$, the given lower and upper bounds for $L_{\text{Tam}}(K, -1)$ tend to 1 and ∞, respectively. Therefore, we similarly define

$$\mu^-(d) := \inf_{\deg K = d} \{L_{\text{Tam}}(K, -1)\} \quad \text{and} \quad \mu^+(d) := \sup_{\deg K = d} \{L_{\text{Tam}}(K, -1)\}$$

to be the infimum and supremum of the average Tamagawa product over number fields K with degree d.

Ono [7] conjecture that as $d \to \infty$, the limit infimum of $t^-(d)$ is 0, the limit supremum of $t^+(d)$ is 1, the limit infimum of $\mu^-(d)$ is 1, and the limit supremum of $\mu^+(d)$ is ∞. We confirm the conjecture in the following theorem.

Theorem 1.7. *We have*

$$\liminf_{d \to +\infty} t^-(d) = 0 \quad and \quad \limsup_{d \to +\infty} t^+(d) = 1,$$

and

$$\liminf_{d \to +\infty} \mu^-(d) = 1 \quad and \quad \limsup_{d \to +\infty} \mu^+(d) = \infty.$$

Remark 1.8. The proof of Theorem 1.7 is constructive. Namely, we provide a family of multiquadratic fields K for which $P_{\text{Tam}}(K, 1) \to 0$ and $L_{\text{Tam}}(K, -1) \to \infty$, and a family of cyclotomic fields K for which $P_{\text{Tam}}(K, 1) \to 1$ and $L_{\text{Tam}}(K, -1) \to 1$. In Section 7, we compute the values of $P_{\text{Tam}}(K, 1)$ and $L_{\text{Tam}}(K, -1)$ for example fields within these families.

The remainder of the paper is structured as follows: In Section 2, we introduce Tate's algorithm, a recursive procedure that computes the local invariants for elliptic curves, including the Tamagawa number of an elliptic curve E/K at $\mathfrak{p}$. Running Tate's algorithm at $\mathfrak{p} \nmid (6)$ is relatively straightforward, but additional challenges arise at $\mathfrak{p} \mid (3)$ and $\mathfrak{p} \mid (2)$ since E/K is cubic in x and quadratic in y. Therefore, we begin by running Tate's algorithm at $\mathfrak{p} \nmid (6)$ in Section 3, and then run Tate's algorithm for $\mathfrak{p} \mid (3)$ and $\mathfrak{p} \mid (2)$ in Sections 4 and 5, respectively. In Section 6, we prove our main theorems. In Section 7, we compute $P_{\text{Tam}}(K, m)$ and $L_{\text{Tam}}(K, -1)$ for example number fields to illustrate Theorem 1.2. For a classification of non-minimal short Weierstrass models at primes above 2 and 3, refer to Appendix A. For the exact proportions of Tamagawa numbers for primes above 2 and 3 with large ramification indices, refer to Appendix B of an extended version of the paper [3].

2. Tate's Algorithm Over $\mathcal{O}_K$

Tate's algorithm (see [8, Section 4.9]) is an iterative process that returns the Kodaira type and the Tamagawa number of an elliptic curve E/K at $\mathfrak{p}$, which allows us to compute $\delta_{K,\mathfrak{p}}(c)$. A single iteration of the algorithm consists of 11 steps. Select a uniformizer π and denote the corresponding valuation on K_v by v_π. If the model for E has minimal $v_\pi(\Delta)$ over the π-integral models for E, then the algorithm terminates during the first ten steps, which correspond to each of the ten Kodaira types. We refer to such elliptic curves as $\mathfrak{p}$-*minimal models*. However, if E is not $\mathfrak{p}$-minimal, then, at Step 11 of Tate's algorithm, we scale $(x, y) \mapsto (\pi^2 x, \pi^3 y)$. The substitutions from Steps 1 through 10 of Tate's algorithm guarantee that E is π-integral after Step 11. A non-minimal model E then loops back into Step 1 of Tate's algorithm. Tate's algorithm eventually terminates as the scaling at Step 11 decreases $v_\pi(\Delta)$ by 12. At the step in which the algorithm terminates, the Tamagawa number of E/K at $\mathfrak{p}$ is determined. After determining the

proportion of elliptic curves with a fixed Tamagawa number that terminate at each step, we sum these proportions over all steps to compute $\delta_{K,\mathfrak{p}}(c)$.

Griffin et al. [5] classify elliptic curves by $v_\pi(a_4), v_\pi(a_6)$, and $v_\pi(\Delta)$. They then apply distinct linear shifts to the curves in each case and parametrize a_4 and a_6 in terms of these shifts prior to running Tate's algorithm. Finally, they run the algorithm on each case separately. In our paper, we do not classify elliptic curves into cases before running Tate's algorithm. Instead, for each $\mathfrak{p}$, we run Tate's algorithm simultaneously for all $\mathfrak{p}$-minimal elliptic curves in the short Weierstrass form. These $\mathfrak{p}$-minimal elliptic curves are guaranteed to terminate during the first iteration of the algorithm. But when E is non-minimal, E passes through Step 11, then loops back into Step 1. For prime ideals $\mathfrak{p} \nmid (6)$, a non-minimal $E(a_4, a_6)$ is still in the short Weierstrass form after Step 11. But when $\mathfrak{p} \mid (3)$, the coefficient a_2 may be non-zero after Step 11, since E is cubic in x. Therefore, when $\mathfrak{p} \mid (3)$, we must study Tate's algorithm over

$$E(a_2, a_4, a_6): \quad y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

to understand how non-minimal curves loop back into Tate's algorithm. When $\mathfrak{p} \mid (2)$, the coefficients a_1 and a_3 may be nonzero after Step 11, since E is quadratic in y. Likewise, we must study Tate's algorithm over

$$E(a_1, a_3, a_4, a_6): \quad y^2 + a_1 xy + a_3 y = x^3 + a_4 x + a_6.$$

Therefore, to study how Tate's algorithm acts on non-minimal $E(a_4, a_6)$, we should study how Tate's algorithm acts on $E(a_1, a_2, a_3, a_4, a_6)$.

We compute $\delta_{K,\mathfrak{p}}(c)$ by first studying the $\mathfrak{p}$-minimal curves and then the non-minimal curves. Let $\delta'_{K,\mathfrak{p}}(T, c; \alpha_1, \alpha_2, \alpha_3)$ be the proportion of models $E(a_1, a_2, a_3, a_4, a_6)$ that are $\mathfrak{p}$-minimal with $v_\pi(a_i) = \alpha_i$ for $i = 1, 2, 3$, Kodaira type T, and Tamagawa number c. In Lemmas 3.1, 4.2 and 5.2, we compute $\delta'_{K,\mathfrak{p}}(T, c; \infty, \infty, \infty)$ for $\mathfrak{p} \nmid (6)$, $\delta'_{K,\mathfrak{p}}(T, c; \infty, \alpha_2, \infty)$ for $\mathfrak{p} \mid (3)$, and $\delta'_{K,\mathfrak{p}}(T, c; \alpha_1, \infty, \alpha_3)$ for $\mathfrak{p} \mid (2)$, respectively. These values of δ' accounts for the potentially nonzero coefficients after Step 11.

Then we study the form of non-minimal curves after Step 11. When $\mathfrak{p} \nmid (6)$, the elliptic curves that loop back are still in the short Weierstrass form, which we visualize in a simple Markov chain in Figure 3.1. When $\mathfrak{p} \mid (3)$ (resp. $\mathfrak{p} \mid (2)$) however, a non-minimal elliptic curve after Step 11 may not be short anymore, and so the underlying Markov chain structure is more complex as in Figure 4.1 (resp. Figure 5.1). Families, which are sets of elliptic curves that act as nodes in these Markov chain, are defined in Definition 4.1 and Definition 5.1. The edges are determined for $\mathfrak{p} \mid (3)$ (resp. $\mathfrak{p} \mid (2)$) in Lemma 4.4 (resp. Lemma 5.4).

Our analysis of Tate's algorithm boils down to studying congruences in terms of the coefficients a_1, a_2, a_3, a_4, a_6 modulo bounded powers of π. We often note that, when certain quantities like a_2, a_4, or $a_6 \pmod{\pi}$ are fixed,

there are a fixed number of choices for a_4 and a_6 modulo bounded powers of π. As such, an important quantity throughout our calculation is the ideal norm $q := N_{K/\mathbb{Q}}(\mathfrak{p})$, or the number of distinct residues in $\mathcal{O}_{K_v}$ modulo π. To further illustrate the connection between Tate's algorithm and these modular congruences, we generalize the results of Griffin et al. [5, Lemmas 2.2, 2.3] by classifying and counting the non-minimal short Weierstrass models at primes $\mathfrak{p} \mid (6)$ in Appendix A.

3. Classification for $\mathfrak{p} \nmid (6)$

In this section, we calculate $\delta_{K,\mathfrak{p}}(c)$ for $\mathfrak{p}$ above $p \geq 5$. We realize upon running Tate's algorithm for non-minimal short Weierstrass models (see Lemma 3.1) that the coefficients a_1, a_2, and a_3 remain invariant at 0. (This confirms the converse of non-minimality for char $k \neq 2, 3$ in [9].) Hence, we define $\varphi_{K,\mathfrak{p}}(T, c_{\mathfrak{p}}) := \delta'_{K,\mathfrak{p}}(T, c_{\mathfrak{p}}; \infty, \infty, \infty)$. We first calculate the values of $\varphi_{K,\mathfrak{p}}(T, c_{\mathfrak{p}})$ and the structure of the associated Markov chain.

Lemma 3.1. *Suppose that $\mathfrak{p} \nmid (6)$ is a prime ideal in K. Consider the family of Weierstrass models $E(a_4, a_6) : y^2 = x^3 + a_4 x + a_6$. Then the local densities $\varphi_{K,\mathfrak{p}}(T, c)$ are provided in Table 3.1.*

TABLE 3.1. The values of $\varphi_{K,\mathfrak{p}}(T, c)$ for $\mathfrak{p} \nmid (6)$. (Note: $\varepsilon(n) := ((-1)^n + 3)/2$.)

Type	$c_{\mathfrak{p}}$	$\varphi_{K,\mathfrak{p}}(T, c_{\mathfrak{p}})$	Type	$c_{\mathfrak{p}}$	$\varphi_{K,\mathfrak{p}}(T, c_{\mathfrak{p}})$	Type	$c_{\mathfrak{p}}$	$\varphi_{K,\mathfrak{p}}(T, c_{\mathfrak{p}})$
I_0	1	$\frac{q-1}{q}$	I_0^*	1	$\frac{1}{3}\frac{(q^2-1)}{q^7}$	III	2	$\frac{(q-1)}{q^4}$
I_1	1	$\frac{(q-1)^2}{q^3}$	I_0^*	2	$\frac{1}{2}\frac{(q-1)}{q^6}$	III^*	2	$\frac{(q-1)}{q^9}$
I_2	2	$\frac{(q-1)^2}{q^4}$	I_0^*	4	$\frac{1}{6}\frac{(q-1)(q-2)}{q^7}$	IV	1	$\frac{1}{2}\frac{(q-1)}{q^5}$
$I_{n\geq 3}$	$\varepsilon(n)$	$\frac{1}{2}\frac{(q-1)^2}{q^{n+2}}$	$I_{n\geq 1}^*$	2	$\frac{1}{2}\frac{(q-1)^2}{q^{7+n}}$	IV	3	$\frac{1}{2}\frac{(q-1)}{q^5}$
$I_{n\geq 3}$	n	$\frac{1}{2}\frac{(q-1)^2}{q^{n+2}}$	$I_{n\geq 1}^*$	4	$\frac{1}{2}\frac{(q-1)^2}{q^{7+n}}$	IV^*	1	$\frac{1}{2}\frac{(q-1)}{q^8}$
II	1	$\frac{(q-1)}{q^3}$	II^*	1	$\frac{(q-1)}{q^{10}}$	IV^*	3	$\frac{1}{2}\frac{(q-1)}{q^8}$

Proof. Recall that $q = N_{K/\mathbb{Q}}(\mathfrak{p})$ is the ideal norm of $\mathfrak{p}$. We run through Tate's algorithm over $E(a_4, a_6)$ to compute $\varphi_{K,\mathfrak{p}}(T, c)$.

Step 1. E terminates if $\pi \nmid \Delta = -16(4a_4^3 + 27a_6^2)$ or when $(a_4, a_6) \not\equiv (-3w^2, 2w^3) \pmod{\pi}$. Therefore, we have $q^2 - q$ choices of (a_4, a_6) modulo π. As a result, $\varphi_{K,\mathfrak{p}}(I_0, 1) = \frac{q-1}{q}$.

Step 2. Suppose that E is singular at $(u, 0)$ after reduction. We shift $x \mapsto x + u$; the new model is

$$y^2 = (x + u)^3 + a_4(x + u) + a_6.$$

We stop if $u \not\equiv 0 \pmod{\pi}$. We check that exactly half of the choices of u result in $T^2 - 3u$ splitting. By Hensel's lemma, these curves have a $\frac{(q-1)^2}{q^{n+2}}$ chance of satisfying $n = v_\pi(\Delta)$. Hence, we have $\delta_{K,\mathfrak{p}}(I_n, n) = \delta_{K,\mathfrak{p}}(I_n, \varepsilon(n)) = \frac{(q-1)^2}{2q^{n+2}}$. Henceforth, assume $u = 0$, which implies $\pi \mid a_4, a_6$.

Step 3. We stop if $\pi^2 \nmid a_6$. There is one choice for $a_4 \pmod{\pi}$ and $q - 1$ choices for $a_6 \pmod{\pi^2}$, whence $\delta_{K,\mathfrak{p}}(II, 1) = \frac{q-1}{q^3}$. Henceforth, assume $\pi^2 \mid a_6$.

Step 4. We stop when $\pi^2 \nmid a_4$. Thus, we have $q - 1$ choices for $a_4 \pmod{\pi^2}$ and one choice for $a_6 \pmod{\pi^2}$, so $\delta_{K,\mathfrak{p}}(III, 1) = \frac{q-1}{q^4}$. Henceforth, assume $\pi^2 \mid a_4$.

Step 5. We stop at Step 5 if $\pi^3 \nmid a_6$. Thus, we have one choice for $a_4 \pmod{\pi^2}$ and $q - 1$ choices for $a_6 \pmod{\pi^3}$. The Tamagawa number is 3 if $Y^2 - (\pi^{-2}a_6)^2$ splits modulo π, and 1 otherwise. Hence, $\delta_{K,\mathfrak{p}}(IV, 1) = \delta_{K,\mathfrak{p}}(IV, 3) = \frac{q-1}{2q^5}$. Henceforth, assume $\pi^3 \mid a_6$.

Step 6. In Steps 6 to 8, we study the polynomial $P(T) = T^3 + \frac{a_4}{\pi^2}T + \frac{a_6}{\pi^3} =: T^3 + A_4 T + A_6$. Note that A_4 and A_6 are equally distributed among the residues in k. The cubic $P(T)$ has discriminant $4A_4^3 + 27A_6^2$. We stop if $P(T)$ has three distinct roots, i.e., if $4A_4^3 + 27A_6^2 \not\equiv 0 \pmod{\pi}$. This accounts for $q^2 - q$ residue pairs as $(A_4, A_6) \not\equiv (-3w^2, 2w^3)$ modulo π.

We now classify $P(T)$ based on the number of its roots in k. First, if $c_\mathfrak{p} = 1$, then $P(T)$ must be irreducible. The linear map $\mathrm{Tr} : \mathbb{F}_{q^3} \to \mathbb{F}_q$ is surjective, so there are $q^3/q = q^2$ traceless elements of $\mathbb{F}_{q^3}$, one of which is in $\mathbb{F}_q$. Thus, there are $\frac{q^2-1}{3}$ such cubics. Next, if $c_\mathfrak{p} = 2$, then $P(T)$ factors into a linear term and an irreducible quadratic. There are $\frac{q^2-q}{2}$ irreducible quadratics and upon fixing this quadratic, the linear term is fixed as $P(T)$ is traceless. Finally, if $c_\mathfrak{p} = 4$, then $P(T)$ has three roots in k. There are $\binom{q}{3}$ ways to select three roots and $1/q$ of them have trace 0, so we have $\frac{(q-1)(q-2)}{6}$ such $P(T)$. In all, we have $\delta_{K,\mathfrak{p}}(I_0^*, 1) = \frac{q^2-1}{3q^7}$, $\delta_{K,\mathfrak{p}}(I_0^*, 2) = \frac{q-1}{2q^6}$, and $\delta_{K,\mathfrak{p}}(I_0^*, 4) = \frac{(q-1)(q-2)}{6q^7}$.

Step 7. We stop when $4A_4^3 + 27A_6^2 \equiv 0 \pmod{\pi}$ but $(A_4, A_6) \not\equiv (0, 0) \pmod{\pi}$. Let $r := \sqrt{A_4/3}$ that serves as the double root of $P(T)$. We accordingly shift $x \mapsto x + \pi r$:

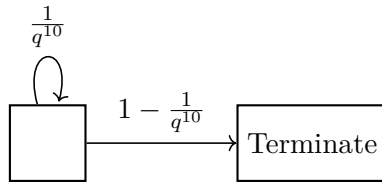(3.1) $\qquad y^2 = (x + \pi r)^3 + a_4(x + \pi r) + a_6 = x^3 + a_2' x^2 + a_6'.$

FIGURE 3.1. The Markov chain structure for short Weierstrass curves when $\mathfrak{p} \nmid (6)$.

Ultimately, the Kodaira type depends on $n := v_\pi(a_6') - 3$, which occurs with proportion $\frac{(q-1)^2}{q^{n+7}}$. The Tamagawa number depends on whether $\frac{a_6'}{\pi^{v_\pi(a_6')}}$ is a quadratic residue, which happens half of the time. Hence, $\delta_{K,\mathfrak{p}}(I_n^*, 2) = \delta_{K,\mathfrak{p}}(I_n^*, 4) = \frac{(q-1)}{2q^{n+7}}$.

Step 8. $P(T)$ is traceless. Therefore, its triple root must be 0, so henceforth $\pi^3 \mid a_4$ and $\pi^4 \mid a_6$. We stop if $Y^2 - \pi^{-4}a_6$ has distinct roots, i.e., if $\pi^{-4}a_6 \not\equiv 0 \pmod{\pi}$. We have one choice for $a_4 \pmod{\pi^3}$ and $q - 1$ choices for $a_6 \pmod{\pi^5}$, half of which cause $Y^2 - \pi^{-4}a_6$ to split. Thus, $\varphi_{K,\mathfrak{p}}(IV^*, 1) = \varphi_{K,\mathfrak{p}}(IV^*, 3) = \frac{q-1}{2q^8}$.

Step 9. We terminate if $\pi^4 \nmid a_4$. There are $q - 1$ choices for $a_4 \pmod{\pi^4}$ and one choice for $a_6 \pmod{\pi^5}$, whence $\varphi_{K,\mathfrak{p}}(III^*, 2) = \frac{q-1}{q^9}$.

Step 10. We stop if $\pi^6 \nmid a_6$. There is one choice for $a_4 \pmod{\pi^4}$ and $q - 1$ choices for $a_6 \pmod{\pi^6}$, whence $\varphi_{K,\mathfrak{p}}(II^*, 1) = \frac{q-1}{q^{10}}$.

Step 11. For E not to be $\mathfrak{p}$-minimal, it must be that $\pi^4 \mid a_4$ and $\pi^6 \mid a_6$, so the proportion of non-minimal E is $\frac{1}{q^{10}}$. □

Remark 3.2. The above local proportions $\varphi_{K,\mathfrak{p}}(T, c)$ exactly match the local proportions $\delta_p'(T, c)$ for $p \geq 5$ in Griffin et al. [5, Table 5] after replacing the rational prime p with the ideal norm q.

In the proof of Lemma 3.1, a non-minimal curve $E(a_4, a_6)$ transforms into $E'(a_4, a_6) := E(\pi^{-4}a_4, \pi^{-6}a_6)$. As we run through the non-minimal E, the family of E' is equivalent to that of E. Thus, we may rerun Lemma 3.1 on the new family E'. Figure 3.1 illustrates the resultant Markov chain.

Proposition 3.3. *If $\mathfrak{p} \nmid (6)$ is a prime ideal in K and $c \geq 1$, then letting $q := N_{K/\mathbb{Q}}(\mathfrak{p})$ we have*

$$\delta_{K,\mathfrak{p}}(c) = \begin{cases} 1 - \dfrac{q(6q^7 + 9q^6 + 9q^5 + 7q^4 + 8q^3 + 7q^2 + 9q + 6)}{6(q+1)^2(q^8 + q^6 + q^4 + q^2 + 1)} & \text{if } c = 1, \\[3mm] \dfrac{q(2q^7 + 2q^6 + q^5 + q^4 + 2q^3 + q^2 + 2q + 2)}{2(q+1)^2(q^8 + q^6 + q^4 + q^2 + 1)} & \text{if } c = 2, \\[3mm] \dfrac{q^2(q^4 + 1)}{2(q+1)(q^8 + q^6 + q^4 + q^2 + 1)} & \text{if } c = 3, \\[3mm] \dfrac{q^3(3q^2 - 2q - 1)}{6(q+1)(q^8 + q^6 + q^4 + q^2 + 1)} & \text{if } c = 4, \\[3mm] \dfrac{q^{10} - 2q^9 + q^8}{2q^c(q^{10} - 1)} & \text{if } c \geq 5. \end{cases}$$

Proof. Following the expressions for $\delta_{K,\mathfrak{p}}(c)$ in Lemma 3.1 and the Markov chain as illustrated in Figure 3.1, we have that

$$(3.2) \qquad \delta_{K,\mathfrak{p}}(c) = \left(1 + \frac{1}{q^{10}} + \frac{1}{q^{20}} + \dots\right) \sum_{c_{\mathfrak{p}} = n} \varphi_{K,\mathfrak{p}}(T, c_{\mathfrak{p}}). \qquad \square$$

Remark 3.4. When $K = \mathbb{Q}$, then $\mathfrak{p} = (p)$ for rational primes p and we recover the formulae over rationals found in [5]. Conversely, the expressions for the proportions over general K match that of $\mathbb{Q}$, except the rational prime p is replaced with the prime ideal norm q.

4. Classification for $\mathfrak{p} \mid (3)$

In this section, we derive $\delta_{K,\mathfrak{p}}(c)$ for $\mathfrak{p} \mid (3)$. Unlike in Section 3, Tate's algorithm may introduce a non-zero a_2-coefficient on non-minimal $E(a_4, a_6)$ that loops back into the algorithm. Therefore, to determine $\delta_{K,\mathfrak{p}}(c)$, we study the action of Tate's algorithm on a larger class of elliptic curves (namely, on $E(a_2, a_4, a_6)$, as defined in Section 2). The short Weierstrass elliptic curves are exactly the $E(a_2, a_4, a_6)$ with $\alpha_2 = \infty$. Naturally, we group elliptic curves into families depending on α_2 as follows.

Definition 4.1. The *3-family* $F(\alpha_2)$ refers to the set of models

$$F(\alpha_2) := \{E(a_2, a_4, a_6) : v_\pi(a_2) = \alpha_2; \ a_4, a_6 \text{ integral}\}.$$

The 3-family $F(\geq \alpha_2)$ refers to the set $\bigsqcup_{\alpha \geq \alpha_2} F(\alpha)$.

For brevity, we refer to 3-families as families for this section. We first run Tate's algorithm to calculate $\chi_{K,\mathfrak{p}}(T, c; \alpha_2) := \delta'_{K,\mathfrak{p}}(T, c; \infty, \alpha_2, \infty)$, which is the proportion of models that are $\mathfrak{p}$-minimal with Kodaira type T and Tamagawa number c for each family $F(\alpha_2)$.

Lemma 4.2. *Suppose that $\mathfrak{p} \subseteq K$ is above 3 with ramification index e. Then for $F(\alpha_2)$, the local densities $\chi_{K,\mathfrak{p}}(T, c; \alpha_2)$ is as provided in Table 4.1.*

TABLE 4.1. The values of $\chi_{K,\mathfrak{p}}(T, c; \alpha_2)$ for $\mathfrak{p} \mid (3)$.

Type	$c_{\mathfrak{p}}$	$e = 1$		$e \geq 2$		
		$\alpha_2 = 0$	$\alpha_2 \geq 1$	$\alpha_2 = 0$	$\alpha_2 = 1$	$\alpha_2 \geq 2$
I_0	1	$(q-1)/q$	$(q-1)/q$	$(q-1)/q$	$(q-1)/q$	$(q-1)/q$
I_1	1	$(q-1)/q^2$	0	$(q-1)/q^2$	0	0
I_2	2	$(q-1)/q^3$	0	$(q-1)/q^3$	0	0
$I_{n\geq3}$	n	$(q-1)/2q^{n+1}$	0	$(q-1)/2q^{n+1}$	0	0
$I_{n\geq3}$	$\varepsilon(n)$	$(q-1)/2q^{n+1}$	0	$(q-1)/2q^{n+1}$	0	0
II	1	0	$(q-1)/q^2$	0	$(q-1)/q^2$	$(q-1)/q^2$
III	2	0	$(q-1)/q^3$	0	$(q-1)/q^3$	$(q-1)/q^3$
IV	1	0	$(q-1)/2q^4$	0	$(q-1)/2q^4$	$(q-1)/2q^4$
IV	3	0	$(q-1)/2q^4$	0	$(q-1)/2q^4$	$(q-1)/2q^4$
I_0^*	1	0	$(q^2-1)/3q^6$	0	$1/3q^5$	$(q-1)/3q^5$
I_0^*	2	0	$(q-1)/2q^5$	0	$(q-1)/2q^6$	$(q-1)/2q^5$
I_0^*	4	0	$(q-1)(q-2)/6q^6$	0	$(q-3)/6q^6$	$(q-1)/6q^5$
$I_{n\geq1}^*$	2	0	$(q-1)^2/2q^{6+n}$	0	$(q-1)/2q^{5+n}$	0
$I_{n\geq1}^*$	4	0	$(q-1)^2/2q^{6+n}$	0	$(q-1)/2q^{5+n}$	0
IV^*	1	0	$(q-1)/2q^7$	0	0	$(q-1)/2q^6$
IV^*	3	0	$(q-1)/2q^7$	0	0	$(q-1)/2q^6$
III^*	2	0	$(q-1)/q^8$	0	0	$(q-1)/q^7$
II^*	1	0	$(q-1)/q^9$	0	0	$(q-1)/q^8$

Proof. We run Tate's algorithm over $F(\alpha_2)$ to compute $\chi_{K,\mathfrak{p}}(T, c; \alpha_2)$.

Step 1. Suppose that E terminates at Step 1. If $E \in F(0)$, then $\Delta \equiv -a_2^3 a_6 + a_2^2 a_4^2 - a_4^3 \pmod{\pi}$. Thus, for $\pi \nmid \Delta$, there are $q - 1$ choices for a_6 modulo π for fixed a_2 and a_4. If $E \in F(1)$ or $E \in F(\geq 2)$, then $\Delta \equiv -a_4^3 \pmod{\pi}$. Therefore, there are $q - 1$ choices for a_4 modulo π for fixed a_2 and a_6. Thus, $\chi_{K,\mathfrak{p}}(I_0, 1; 0) = \chi_{K,\mathfrak{p}}(I_0, 1; 1) = \chi_{K,\mathfrak{p}}(I_0, 1; \geq 2) = \frac{q-1}{q}$. Moving forward, for curves that pass Step 1, in $F(0)$, the units digit of a_6 is fixed for fixed a_4 and a_2, and in $F(\geq 1)$ the units digit of a_4 is 0.

Step 2. Suppose that the singular point of E after reduction by π is at $(u, 0)$. Then, the translation $x \mapsto x + u$ yields the new model

(4.1) $y^2 = (x + u)^3 + a_2(x + u)^2 + a_4(x + u) + a_6.$

Curves in $F(0)$ always terminate as $\pi \nmid b_2 = a_2 + 3u$. By Hensel's lemma, exactly $\frac{q-1}{q^{n+1}}$ of curves within $F(0)$ satisfy $v_\pi(\Delta) = n$ as a_2 varies. We also check that half of these values make a_2 a quadratic residue modulo π. Thus, $\chi_{K,\mathfrak{p}}(I_n, n; 0) = \chi_{K,\mathfrak{p}}(I_n, \varepsilon(n); 0) = \frac{q-1}{2q^{n+1}}$.

However, if $E \in F(\geq 1)$, we always pass this step, so $\chi_{K,\mathfrak{p}}(I_n, n; 0) = \chi_{K,\mathfrak{p}}(I_n, \varepsilon(n); 0) = 0$. Since $(u, 0)$ lies on the curve after reduction and $v_\pi(a_4) \geq 1$ from Step 1, note $u^3 + a_6 \equiv 0 \pmod{\pi}$.

Step 3. If we stop at Step 3, $\pi^2 \nmid a_6 + a_4 u + a_2 u^2 + u^3$. From Step 2, we have that $\pi \mid a_6 + a_4 u + a_2 u^2 + u^3$. After fixing u, a_2, a_4, we have $q - 1$ choices for $a_6 \pmod{\pi^2}$. As a result, $\chi(II, 1; \geq 1) = \frac{q-1}{q^2}$.

Step 4. To terminate at Step 4, we must have $\pi^3 \nmid 4(a_2 + 3u)(a_6 + a_4 u + a_2 u^2 + u^3) - (3u^2 + 3a_2 u + a_4)^2$. From Steps 2 and 3 respectively, we have that $\pi \mid a_2 + 3u$ and $\pi^2 \mid a_6 + a_4 u + a_2 u + u^3$. As such, we stop if $\pi^2 \nmid 3u^2 + 3a_2 u + a_4$. We find that for fixed a_2 and u, there are $q(q - 1)$ choices for $a_4 \pmod{\pi^2}$ and one choice for $a_6 \pmod{\pi^2}$. Hence, $\chi_{K,\mathfrak{p}}(III, 2; \geq 1) = \frac{q-1}{q^3}$.

Step 5. To stop at Step 5, $\pi \nmid \pi^{-2}(a_6 + a_4 u + a_2 u^2 + u^3)$. For fixed a_2 and u, we have q choices for $a_4 \pmod{\pi^2}$ and $q - 1$ choices for $a_6 \pmod{\pi^3}$, half of which make $\pi^{-2}(a_6 + a_4 u + a_2 u^2 + u^3)$ a quadratic residue. Hence, $\chi_{K,\mathfrak{p}}(IV, 1; \geq 1) = \chi_{K,\mathfrak{p}}(IV, 3; \geq 1) = \frac{q-1}{2q^4}$. Moving forward, we have q choices for $a_4 \pmod{\pi^2}$ and $a_6 \pmod{\pi^3}$ for each choice of a_2, u, and the π^2-digit of a_4.

Step 6. We begin by writing $P(T) = T^3 + \frac{3u + a_2}{\pi} T^2 + \frac{3u^2 + 2a_2 u + a_4}{\pi^2} T + \frac{u^3 + a_2 u^2 + a_4 u + a_6}{\pi^3} =: T^3 + A_2 T^2 + A_4 T + A_6 \pmod{\pi}$. Note that fixing $A_4, A_6 \pmod{\pi}$ and a choice of a_2, u, and the π^3-digit of a_4 uniquely determines $a_4 \pmod{\pi^3}$ and $a_6 \pmod{\pi^4}$.

Suppose that we fix A_2 and consider $P(T)$ across (A_4, A_6) modulo π. For $P(T)$ to have 3 distinct roots, $P(T)$ and $P'(T) = 2A_2 x + A_4 \pmod{\pi}$ must not have a shared root. In other words, $A_4^3 + 2A_2^2 A_4^2 + A_6 A_2^3 \not\equiv 0 \pmod{\pi}$. As such, for a fixed A_2 modulo π, there are q choices for A_4 and $q - 1$ choices of A_6 modulo π such that $P(T)$ has three distinct roots. Suppose further that all three of $P(T)$'s roots are in $\mathbb{F}_q$. If $P(T)$ is traceless, i.e., $A_2 \equiv 0 \pmod{\pi}$, there are q choices for the first root and $q - 1$ choices for the second root. Then, the third root is guaranteed to be different from the first two. If $P(T)$ has a non-zero trace, however, then there are q choices for the first root and $q - 3$ choices for the second root to guarantee that the fixed third root is distinct from the first two. Now, suppose that $P(T)$ has exactly one root in $\mathbb{F}_q$. Then, once we fix an irreducible quadratic, the linear term is fixed. Therefore, no matter the trace, the number of $P(T)$ with exactly one root in $\mathbb{F}_q$ across (A_4, A_6) modulo π is $\frac{q^2 - q}{2}$. The last case is when $P(T)$ is irreducible. In $\mathbb{F}_{q^3}$, there are $\frac{q^2}{3}$ elements of a given trace as the linear map $\text{Tr} : \mathbb{F}_{q^3} \to \mathbb{F}_q$ is surjective. The elements of $\mathbb{F}_q$ all have

trace 0. Therefore, the number of irreducible $P(T)$ with zero trace is $\frac{q^2-q}{3}$, and the number of that with a non-zero trace is $\frac{q^2-q}{3}$.

We first discuss $e = 1$. Here, a fixed A_2 modulo π uniquely determines u—the units digit of a_6. We thus conclude from the aforementioned analysis that for $e = 1$, $\chi_{K,\mathfrak{p}}(I_0^*, 1; \geq 1) = \frac{q^2-1}{3q^6}$, $\chi_{K,\mathfrak{p}}(I_0^*, 2; \geq 1) = \frac{q-1}{2q^5}$, and $\chi_{K,\mathfrak{p}}(I_0^*, 4; \geq 1) = \frac{(q-1)(q-2)}{6q^6}$. We now repeat for $e \geq 2$ and $E \in F(1)$. Here, the trace is fixed and necessarily non-zero. As such, $\chi_{K,\mathfrak{p}}(I_0^*, 1; 1) = \frac{1}{3q^5}$, $\chi_{K,\mathfrak{p}}(I_0^*, 2; 1) = \frac{q-1}{2q^6}$, and $\chi_{K,\mathfrak{p}}(I_0^*, 4; 1) = \frac{q-3}{6q^6}$. Finally, we discuss $e \geq 2$ and $E \in F(\geq 2)$. Here, the trace is necessarily zero. Thus, $\chi_{K,\mathfrak{p}}(I_0^*, 1; \geq 2) = \frac{q-1}{3q^5}$, $\chi_{K,\mathfrak{p}}(I_0^*, 2; \geq 2) = \frac{q-1}{2q^5}$, and $\chi_{K,\mathfrak{p}}(I_0^*, 4; \geq 2) = \frac{q-1}{6q^5}$.

Step 7. If E stops at Step 7, $P(T)$ has a double root that is not a triple root. This implies that $A_2 \not\equiv 0 \pmod{\pi}$, but that $A_2^3 + 2A_2^2 A_4 + A_6 A_2^3 \equiv 0 \pmod{\pi}$. For $A_2 \not\equiv 0 \pmod{\pi}$, $\alpha_2 = 1$ and $e \geq 2$, or $\alpha_2 \geq 1$ and $e = 1$. Hence, $\chi_{K,\mathfrak{p}}(I_n^*, 2; \geq 1) = \chi_{K,\mathfrak{p}}(I_n^*, 4; \geq 1) = \frac{(q-1)^2}{2q^{6+n}}$ for $e = 1$. If $E \in F(1)$ and $e \geq 2$, E terminates at Step 7. Now suppose that $E \in F(\geq 2)$ and $e = 1$. Then, for $A_2^3 + 2A_2^2 A_4 + A_6 A_2^3 \equiv 0 \pmod{\pi}$, we have $q - 1$ choices for A_6 for each A_4. We then shift the double root of $P(T)$ to 0. The constant term of the shifted model is surjective over a_6. Therefore, the proportion of E with valuation $3 + n$ is $\frac{q-1}{q^n}$, half of which has $n = 2$ and half of which has $n = 4$. Hence, $\chi_{K,\mathfrak{p}}(I_n^*, 2; 1) = \chi_{K,\mathfrak{p}}(I_n^*, 4; 1) = \frac{q-1}{2q^{5+n}}$ and $\chi_{K,\mathfrak{p}}(I_n^*, 2; \geq 2) = \chi_{K,\mathfrak{p}}(I_n^*, 4; \geq 2) = 0$ for $e \geq 2$.

Step 8. If E reaches Step 8, $P(T)$ has a triple root. If so, then $e \geq 1$ and $E \in F(1)$, or $e \geq 2$ and $E \in F(\geq 2)$. Let the triple root of $P(T)$ be v, so $v^3 \equiv A_6 \pmod{\pi}$. We shift the triple root of $P(T)$ to 0 via $x \mapsto x + v\pi$. Letting $s := u + v\pi$, E becomes

$$(4.2) \qquad y^2 = (x+s)^3 + a_2(x+s)^2 + a_4(x+s) + a_6.$$

We stop if $\pi \nmid \pi^{-4}(s^3 + a_2 s^2 + a_4 s + a_6)$. We count by fixing a_2 and s $\pmod{\pi^2}$, the latter of which we have q choices for $e = 1$ and q^2 choices for $e \geq 2$. Resultantly, there is one choice for $a_4 \pmod{\pi^3}$ and $q - 1$ choices for $a_6 \pmod{\pi^5}$, half of which make $\pi^{-4}(s^3 + a_2 s^2 + a_4 s + a_6)$ a quadratic residue. Hence, we have $\chi_{K,\mathfrak{p}}(IV^*, 1; \geq 1) = \chi_{K,\mathfrak{p}}(IV^*, 3; \geq 1) = \frac{q-1}{2q^7}$ for $e = 1$, and $\chi_{K,\mathfrak{p}}(IV^*, 1; \geq 2) = \chi_{K,\mathfrak{p}}(IV^*, 3; \geq 2) = \frac{q-1}{2q^6}$ for $e \geq 2$.

Step 9. Suppose that E reaches Step 9. We stop if $\pi^4 \nmid 3s^2 + 2a_2 s + a_4$. As in Step 8, we first choose a_2 and s $\pmod{\pi^2}$, the latter of which we have q choices for $e = 1$ and q^2 choices for $e \geq 2$. These choices allow for $q - 1$ choices of $a_4 \pmod{\pi^4}$ and a unique choice of $a_6 \pmod{\pi^5}$ Hence, we have $\chi_{K,\mathfrak{p}}(III^*, 2; \geq 1) = \frac{q-1}{q^8}$ for $e = 1$, and $\chi_{K,\mathfrak{p}}(III^*, 2; \geq 2) = \frac{q-1}{q^7}$ for $e \geq 2$.

Step 10. We stop at Step 10 if $\pi \nmid \pi^{-5}(s^3 + a_2 s^2 + a_4 s + a_6)$. Once again, we first choose a_2 and s, the latter of which we have q choices for $e = 1$ and q^2 choices for $e \geq 2$. These choices give a unique choice of a_4 (mod π^4) and $q - 1$ choices of a_6 (mod π^6). Hence, we have $\chi_{K,\mathfrak{p}}(II^*, 1; \geq 1) = \frac{q-1}{q^9}$ for $e = 1$, and $\chi_{K,\mathfrak{p}}(II^*, 1; \geq 2) = \frac{q-1}{q^8}$ for $e \geq 2$.

Step 11. Suppose E is non-minimal. If s is fixed, then (a_4, a_6) is fixed up to modulo π^4 and π^6 respectively. When $e = 1$ and $E \in F(\geq 1)$, there are q choices of s modulo π^2. Therefore, $\frac{1}{q^9}$ of the curves are non-minimal. When $e \geq 2$ and $E \in F(\geq 2)$, there are q^2 choices for s. Hence, $\frac{1}{q^8}$ curves are non-minimal. $\qquad\square$

We now justify how we reclassify the non-minimal models of one family as another family of curves. We first note that the models in $F(\geq e)$ and $F(\infty)$ have the same local properties in the following sense.

Remark 4.3. Because linear transformations do not change the local data of an elliptic curve, instead of computing local densities on short Weierstrass models $F(\infty)$, we may compute the local densities on the set

$$(4.3) \qquad \{(E : y^2 = (x + t)^3 + a_4(x + t) + a_6) : t, a_4, a_6 \text{ integral}\}.$$

Since a_4 and a_6 are drawn uniformly from the residues modulo π^k for all k and the x^2-coefficient varies uniformly across multiples of 3, the set in (4.3) is precisely $F(\geq e)$.

Thus, moving forward, if $\alpha_2 \geq e$, then we work with the curves in $F(\geq e)$ instead of $F(\alpha_2)$. We first show that when $\alpha_2 < e$, the local densities at the non-minimal models of a family $F(\alpha_2)$ exactly match the local densities at the family $F(\alpha_2 - 2)$. To do this, we establish a map which sends a non-minimal model in $F(\alpha_2)$ to another isomorphic model in $F(\alpha_2 - 2)$, induced by the transformation at Step 11. Likewise, we demonstrate that the local densities at the non-minimal models of $F(\geq e)$ match the local densities at $F(\geq e - 2)$.

Lemma 4.4. *We have surjective, q^2-to-1 maps*
- *between the set of non-minimal models in $F(\alpha_2)$ and the set $F(\alpha_2 - 2)$ for each $\alpha_2 < e$ and*
- *between the set of non-minimal models in $F(\geq e)$ and the set $F(\geq e - 2)$*

that each sends E to its transformation E' after passing Step 11.

Proof. First, suppose that $\alpha_2 < e$. Then fix a set of q^2 representatives to be the residues modulo π^2. Recall that for non-minimal $E(a_2, a_4, a_6)$, Tate's algorithm produces a unique residue s (mod π^2) for which

$$(4.4) \qquad y^2 = (x + s)^3 + a_2(x + s)^2 + a_4(x + s) + a_6$$

has the coefficient of x^i divisible by π^i for $i = 2, 4, 6$. Hence, each non-minimal model $E(a_2, a_4, a_6) \in F(\alpha_2)$ is sent to

$$(4.5) \quad E\left(\frac{3s + a_2}{\pi^2}, \frac{3s^2 + 2a_2 s + a_4}{\pi^4}, \frac{s^3 + a_2 s^2 + a_4 s + a_6}{\pi^6}\right) \in F(\alpha_2 - 2),$$

and the map is well-defined.

Conversely, given a model $E(a'_2, a'_4, a'_6) \in F(\alpha_2 - 2)$, choosing s uniquely determines a_2, a_4, a_6, and moreover $v_{\pi(a_2)} = \alpha_2$. Hence, $E(a'_2, a'_4, a'_6)$ has exactly q^2 preimages in $F(\alpha_2)$, as we had sought.

The existence proof of a surjective, q^2-to-1 map between the set of non-minimal models in $F(\geq e)$ and the set $F(\geq e - 2)$ is analogous to that of the case $\alpha_2 < e$ and is thus omitted. $\qquad\square$

We now complete our classification for $\mathfrak{p} \mid (3)$ in Proposition 4.5. A key ingredient is the underlying Markov chain structure that helps us study how non-minimal curves loop back into Tate's algorithm. Lemma 4.4 allows us to identify the non-minimal curves of $F(0), F(1), \ldots, F(\geq e)$ to be identified with other families. In particular, we see from Lemma 4.4 that the non-minimal curves in $F(\alpha_2)$ for $\alpha < e$ are always transformed into curves in $F(\alpha_2 - 2)$, which as shown in Step 11 of the proof of Lemma 4.2 occurs with probability $\frac{1}{q^8}$. We also see from Lemma 4.4 that the non-minimal curves in $F(\geq e)$ with probability $\frac{1}{q^2}$ loop back to itself, with probability $\frac{q-1}{q^2}$ loop to $F(e-1)$, and with probability $\frac{q-1}{q}$ transform to $F(e-2)$. Thus, $F(\geq e)$ maps into the set $F(\geq e)$ with proportion $\frac{1}{q^8} \cdot \frac{1}{q^2} = \frac{1}{q^{10}}$, the set $F(e-1)$ with proportion $\frac{1}{q^8} \cdot \frac{q-1}{q^2} = \frac{q-1}{q^{10}}$, and the set $F(e-2)$ with proportion $\frac{1}{q^8} \cdot \frac{q-1}{q} = \frac{q-1}{q^9}$. Finally, Lemma 4.2 determines the local densities at each $F(\alpha_2)$ for $\alpha_2 = 1, 2, \ldots, e-1$, and the set $F(\geq e)$. We collate all of this information in Figure 4.1.

Proposition 4.5. *If $\mathfrak{p} \mid (3)$ is a prime ideal in K and $c \geq 1$, then letting $q := N_{K/\mathbb{Q}}(\mathfrak{p})$ and $e = 1$ we have*

$$\delta_{K,\mathfrak{p}}(c) = \begin{cases} 1 - \dfrac{(q-1)(6q^{10} + 9q^9 + 7q^8 + 8q^7 + 7q^6 + 9q^5 + 6q + 3)}{6q^2(q+1)(q^{10} - 1)} & \text{if } c = 1, \\[3ex] \dfrac{(q-1)(2q^{11} + 2q^{10} + q^9 + 2q^8 + q^7 + 2q^6 + 2q^5 + 2q^2 - 1)}{2q^3(q+1)(q^{10} - 1)} & \text{if } c = 2, \\[3ex] \dfrac{(q-1)(q^{10} + q^7 + q - 1)}{2q^4(q^{10} - 1)} & \text{if } c = 3, \\[3ex] \dfrac{(q-1)(q^{10} + q^9 + 3q - 3)}{6q^5(q^{10} - 1)} & \text{if } c = 4, \\[3ex] \dfrac{(q-1)^2}{2q^{c+1}(q^{10} - 1)} & \text{if } c \geq 5. \end{cases}$$
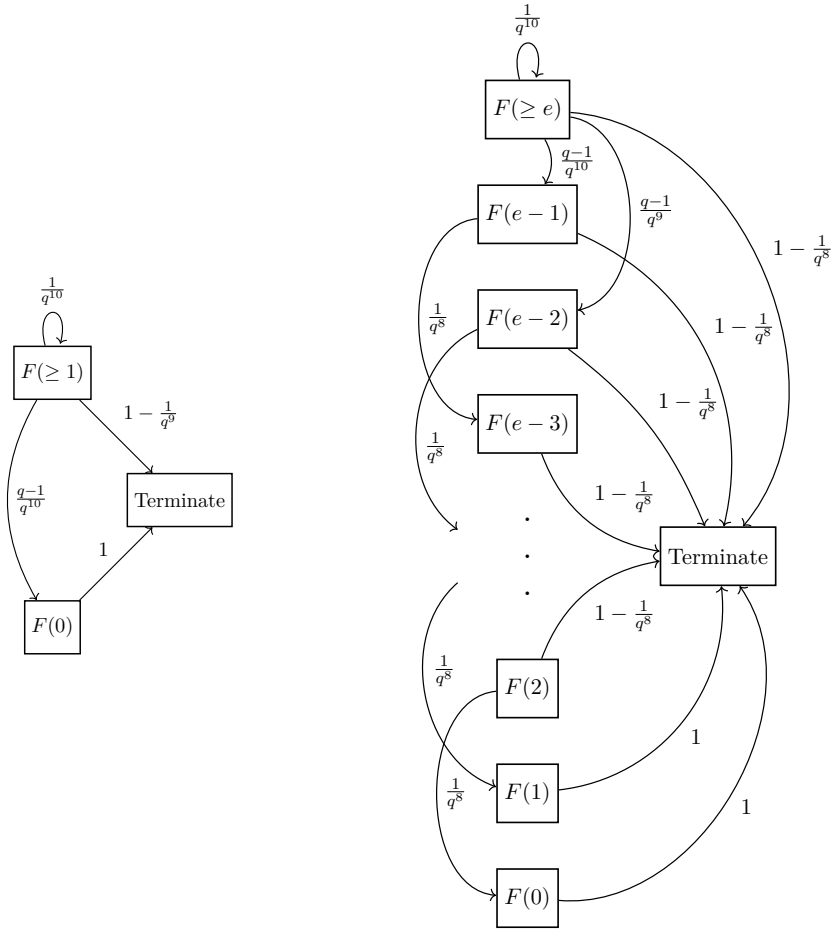
FIGURE 4.1. The Markov chain structure when $\mathfrak{p} \mid (3)$ for $e = 1$ (left) and $e \geq 2$ (right).

If $e \geq 2$ is even, we have

$$
\delta_{K,\mathfrak{p}}(c) = \begin{cases}
1 - (q-1)\left[\dfrac{(6q^{14} + 9q^{13} + 13q^{12} + 16q^{11} + 22(q^{10} + q^9 + q^8))}{6(q+1)(q^2+1)(q^4+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{10}}\right)\right] & \textit{if } c = 1, \\[4ex]
\dfrac{(q-1)(2q^{13} + 3q^{11} + 5q^9 + 5q^7 + 5q^5 + 3q^3 + 2q)}{2(q^2+1)(q^4+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{4e+3}}\right) & \textit{if } c = 2, \\[4ex]
\dfrac{(q-1)(q^{4e+8} + q^{4e+6} + q^{4e+4} + q^{4e+2} + q^{4e} - q^6 + q^4 - q^2)}{2q^{4e-2}(q^4+1)(q^{10}-1)} & \textit{if } c = 3, \\[4ex]
\dfrac{(q-1)(q^{11} + q^9 + q^7 + q^5 + q^3)}{6(q^2+1)(q^4+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{4e+4}}\right) & \textit{if } c = 4, \\[4ex]
\dfrac{(q-1)^2}{2q^{4e+c-8}(q^{10}-1)} & \textit{if } c \geq 5.
\end{cases}
$$

If $e > 2$ is odd, we have

$$\delta_{K,\mathfrak{p}}(c) = \begin{cases} 1 - (q-1)\left[\dfrac{(6q^{14} + 9q^{13} + 13q^{12} + 16q^{11} + 22(q^{10} + q^9 + q^8))}{6(q+1)(q^2+1)(q^4+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{10}}\right)\right] & \text{if } c = 1, \\[18pt] \dfrac{(q-1)(2q^{13} + 3q^{11} + 5q^9 + 5q^7 + 5q^5 + 3q^3)}{2(q^2+1)(q^4+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{4e-2}}\right) & \text{if } c = 2, \\[18pt] \dfrac{(q-1)(q^{10} + q^8 + q^6 + q^4 + q^2)}{2(q^4+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{4e-1}}\right) & \text{if } c = 3, \\[18pt] \dfrac{(q-1)(q^{11} + q^9 + q^7 + q^5 + q^3)}{6(q^2+1)(q^4+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{4e+1}}\right) & \text{if } c = 4, \\[18pt] \dfrac{(q-1)^2}{2q^{4e+c-3}(q^{10}-1)} & \text{if } c \geq 5. \end{cases}$$

The exact proportions are given in Proposition B.1 of the extended version of the paper [3].

Proof. Refer to Figure 4.1. Because we begin with a short Weierstrass form, we start at the node $F(\geq e)$. Fix a Kodaira type T and Tamagawa number c over which we compute the local density of curves with this data. We perform casework on the family we terminate in.

First, suppose that $e = 1$. The proportion of curves that terminate in $F(\geq 1)$ with Kodaira type T and Tamagawa number c is

$$\left(1 + \frac{1}{q^{10}} + \frac{1}{q^{20}} + \dots\right)\chi_{K,\mathfrak{p}}(T, c; \geq 1).$$

On the other hand, the proportion of curves that terminate in $F(0)$ with our prescribed local data is

$$\left(1 + \frac{1}{q^{10}} + \frac{1}{q^{20}} + \dots\right)\frac{q-1}{q^{10}}\chi_{K,\mathfrak{p}}(T, c; 0).$$

Now, suppose that $e \geq 2$. The proportion of curves that terminate in $F(2), F(3), \dots, F(\geq e)$ with Kodaira type T and Tamagawa number c is

$$\left(1 + \frac{1}{q^{10}} + \frac{1}{q^{20}} + \dots\right)\left(1 + \sum_{k=0}^{\lfloor(e-1)/2\rfloor} \frac{q-1}{q^{8k+10}} + \sum_{k=0}^{\lfloor(e-2)/2\rfloor} \frac{q-1}{q^{8k+9}}\right)\chi_{K,\mathfrak{p}}(T, c; \geq 2).$$

Second, the proportion of curves that terminate in $F(1)$ with our prescribed local data is

$$\begin{cases} \left(1 + \dfrac{1}{q^{10}} + \dfrac{1}{q^{20}} \dots\right)\dfrac{q-1}{q^{4e+2}}\chi_{K,\mathfrak{p}}(T, c; 1) & \text{if } 2 \mid e \\[14pt] \left(1 + \dfrac{1}{q^{10}} + \dfrac{1}{q^{20}} \dots\right)\dfrac{q-1}{q^{4e-3}}\chi_{K,\mathfrak{p}}(T, c; 1) & \text{if } 2 \nmid e. \end{cases}$$

Finally, the proportion of curves that terminate in $F(0)$ with our prescribed local data is

$$
\begin{cases}
\left(1 + \dfrac{1}{q^{10}} + \dfrac{1}{q^{20}} \cdots \right) \dfrac{q-1}{q^{4e+1}} \chi_{K,\mathfrak{p}}(T,c;0) & \text{if } 2 \mid e \\[2ex]
\left(1 + \dfrac{1}{q^{10}} + \dfrac{1}{q^{20}} \cdots \right) \dfrac{q-1}{q^{4e+6}} \chi_{K,\mathfrak{p}}(T,c;0) & \text{if } 2 \nmid e.
\end{cases}
$$

The values $\delta_{K,\mathfrak{p}}(T,c)$ are provided in Lemma 4.2. We sum these proportions over all Kodaira types T with Tamagawa number c to get the total density $\delta_{K,\mathfrak{p}}(c)$. $\qquad\square$

5. Classification for $\mathfrak{p} \mid (2)$

In this section, we calculate $\delta_{K,\mathfrak{p}}(c_\mathfrak{p})$ for $\mathfrak{p} \mid (2)$. Unlike in Section 3 and in Section 4, Tate's algorithm may introduce a non-zero a_1, a_2, and a_3 coefficient on non-minimal $E(a_4, a_6)$ that loops back into the algorithm. However, even if E is transformed after Step 11 into $E'(a_1', a_2', a_3', a_4', a_6')$, as in Section 2, with $a_2' \neq 0$, the translation $x \mapsto x - a_2/3$ eliminates the a_2 coefficient of E' without changing the local data of the curve. Therefore, to study how $\mathfrak{p}$-non-minimal elliptic curves loop back into Tate's algorithm, we study the action of Tate's algorithm on the larger class of elliptic curves $E = E(a_1, a_3, a_4, a_6)$, defined as in Section 2. By convention, we re-eliminate the a_2 coefficient after passing Step 11 before re-running Tate's algorithm.

Upon running Tate's algorithm, we find that the sets of elliptic curves $E(a_1, a_3, a_4, a_6)$ across (a_4, a_6) with fixed a_1 and a_3 behave similarly if they have the same $\alpha_1 := v_\pi(a_1)$ and $\alpha_3 := v_\pi(a_3)$. Moreover, the short Weierstrass elliptic curve are exactly the $E(a_1, a_3, a_4, a_6)$ with $\alpha_1 = \alpha_3 = \infty$. We thus group elliptic curves entering Tate's algorithm into families depending on α_1 and α_3 as follows.

Definition 5.1. The *2-family* $F(\alpha_1, \alpha_3)$ refers to the set of models

$$
F(\alpha_1, \alpha_3) := \{ E(a_1, a_3, a_4, a_6) : v_\pi(a_1) = \alpha_1, v_\pi(a_3) = \alpha_3; \ a_4, a_6 \text{ integral}\}.
$$

The 2-family $F(\geq \alpha_1, \geq \alpha_3)$ refers to the set $\bigsqcup_{\alpha \geq \alpha_1} \bigsqcup_{\beta \geq \alpha_3} F(\alpha, \beta)$.

For brevity, refer to 2-families as families for the rest of this section. The rest of the section is structured similarly to Section 4. In Lemma 5.2, we run Tate's algorithm to calculate $\psi_{K,\mathfrak{p}}(T,c;\alpha_1,\alpha_3) := \delta'_{K,\mathfrak{p}}(T,c;\alpha_1,\infty,\alpha_3)$, which is the proportion of $\mathfrak{p}$-minimal models with Kodaira type T and Tamagawa number c for each family $F(\alpha_1, \alpha_3)$. Then, we show in Lemma 5.4 that the non-minimal models from certain families may themselves be viewed as a family. The analysis of non-minimal models in this section is more involved than the analysis in Section 4 for two reasons: there are now two relevant valuations α_1 and α_3, and we have to incorporate the shift $x \mapsto x - a_2/3$ after Step 11. Finally, in Proposition 5.5, we leverage

these lemmas to form a Markov chain whose nodes are families and whose edges represent the reclassification of non-minimal models, which we use to compute the local proportion $\delta_{K,\mathfrak{p}}(c)$.

Lemma 5.2. *Suppose that $\mathfrak{p} \subseteq K$ is above 2 with ramification index e. Then for $F(\alpha_1, \alpha_3)$, the local densities $\psi_{K,\mathfrak{p}}(T, c_{\mathfrak{p}}; \alpha_1, \alpha_3)$ is as provided in Table 5.1 for $e = 1, 2$ and Table 5.2 for $e \geq 3$.*

TABLE 5.1. The values of $\psi_{K,\mathfrak{p}}(T, c; \alpha_1, \infty, \alpha_3)$ for $\mathfrak{p} \mid (2)$.

Type	$c_{\mathfrak{p}}$	$e = 1$			$e = 2$				
		$\alpha_1 = 0$	$\alpha_1 \geq 1$ $\alpha_3 = 0$	$\alpha_1 \geq 1$ $\alpha_3 \geq 1$	$\alpha_1 = 0$	$\alpha_1 \geq 1$ $\alpha_3 = 0$	$\alpha_1 = 1$ $\alpha_3 \geq 1$	$\alpha_1 \geq 2$ $\alpha_3 = 1$	$\alpha_1 \geq 2$ $\alpha_3 \geq 2$
I_0	1	$\frac{q-1}{q}$	1	0	$\frac{q-1}{q}$	1	0	0	0
I_1	1	$\frac{q-1}{q^2}$	0	0	$\frac{q-1}{q^2}$	0	0	0	0
I_2	2	$\frac{q-1}{q^3}$	0	0	$\frac{q-1}{q^3}$	0	0	0	0
$I_{n \geq 3}$	n	$\frac{q-1}{2q^{n+1}}$	0	0	$\frac{q-1}{2q^{n+1}}$	0	0	0	0
$I_{n \geq 3}$	$\varepsilon(n)$	$\frac{q-1}{2q^{n+1}}$	0	0	$\frac{q-1}{2q^{n+1}}$	0	0	0	0
II	1	0	0	$\frac{q-1}{q}$	0	0	$\frac{q-1}{q}$	$\frac{q-1}{q}$	$\frac{q-1}{q}$
III	2	0	0	$\frac{q-1}{q^2}$	0	0	$\frac{q-1}{q^2}$	$\frac{q-1}{q^2}$	$\frac{q-1}{q^2}$
IV	1	0	0	$\frac{q-1}{2q^3}$	0	0	$\frac{q-1}{2q^3}$	$\frac{1}{2q^2}$	0
IV	3	0	0	$\frac{q-1}{2q^3}$	0	0	$\frac{q-1}{2q^3}$	$\frac{1}{2q^2}$	0
I_0^*	1	0	0	$\frac{q^2-1}{3q^5}$	0	0	$\frac{q^2-1}{3q^5}$	0	$\frac{q^2-1}{3q^4}$
I_0^*	2	0	0	$\frac{q-1}{2q^4}$	0	0	$\frac{q-1}{2q^4}$	0	$\frac{q-1}{2q^3}$
I_0^*	4	0	0	$\frac{(q-1)(q-2)}{6q^5}$	0	0	$\frac{(q-1)(q-2)}{6q^5}$	0	$\frac{(q-1)(q-2)}{6q^4}$
$I_{n \geq 1}*$	2	0	0	$\frac{(q-1)^2}{2q^{5+n}}$	0	0	$\frac{(q-1)^2}{2q^{5+n}}$	0	$\frac{(q-1)^2}{2q^{4+n}}$
$I_{n \geq 1}*$	4	0	0	$\frac{(q-1)^2}{2q^{5+n}}$	0	0	$\frac{(q-1)^2}{2q^{5+n}}$	0	$\frac{(q-1)^2}{2q^{4+n}}$
$IV*$	1	0	0	$\frac{q-1}{2q^6}$	0	0	$\frac{q-1}{2q^6}$	0	$\frac{q-1}{2q^5}$
$IV*$	3	0	0	$\frac{q-1}{2q^6}$	0	0	$\frac{q-1}{2q^6}$	0	$\frac{q-1}{2q^5}$
$III*$	2	0	0	$\frac{q-1}{q^7}$	0	0	$\frac{q-1}{q^7}$	0	$\frac{q-1}{q^6}$
$II*$	1	0	0	$\frac{q-1}{q^8}$	0	0	$\frac{q-1}{q^8}$	0	$\frac{q-1}{q^7}$

Proof. We run through Tate's algorithm to compute $\psi_{\mathfrak{p},K}(T, c_{\mathfrak{p}}; \alpha_1, \alpha_3)$. Recall that $q = N_{K/\mathbb{Q}}(\mathfrak{p})$ is the norm of $\mathfrak{p}$.

Step 1. E terminates at Step 1 if $\pi \nmid \Delta$. By definition, $\Delta \equiv b_2^2 b_8 + b_6^2 + b_2 b_4 b_6$ (mod π), where $b_2 \equiv a_1^2$ (mod π), $b_4 \equiv a_1 a_3$ (mod π), $b_6 \equiv a_3^2$ (mod π), and $b_8 \equiv a_1^2 a_6 - a_1 a_3 a_4 - a_4^2$ (mod π). Therefore, $\Delta \equiv a_1^6 a_6 - a_1^5 a_3 a_4 - a_1^4 a_4^2 + a_3^4 + a_1^3 a_3^3$ (mod π). If $\alpha_1 \geq 1$, then $\Delta \equiv a_3^4$ (mod π). As such, $\psi_{K,\mathfrak{p}}(I_0, 1; \alpha_1, \alpha_3) = 1$ if $\alpha_3 = 0$ and 0 if $\alpha_3 \geq 1$. Now, suppose that $\alpha_1 = 0$, in which case Δ is then linear in terms of a_6. Therefore, for each a_1 and a_3,

TABLE 5.2. The values of $\psi_{K,\mathfrak{p}}(T, c; \alpha_1, \infty, \alpha_3)$ for $\mathfrak{p} \mid (2)$.

			$e \geq 3$					
Type	$c_\mathfrak{p}$	$\alpha_1 = 0$	$\alpha_1 \geq 1$ $\alpha_3 = 0$	$\alpha_1 = 1$ $\alpha_3 \geq 1$	$\alpha_1 \geq 2$ $\alpha_3 = 1$	$\alpha_1 = 2$ $\alpha_3 \geq 2$	$\alpha_1 \geq 3$ $\alpha_3 = 2$	$\alpha_1 \geq 3$ $\alpha_3 \geq 3$
I_0	1	$\frac{q-1}{q}$	1	0	0	0	0	0
I_1	1	$\frac{q-1}{q^2}$	0	0	0	0	0	0
I_2	2	$\frac{q-1}{q^3}$	0	0	0	0	0	0
$I_{n \geq 3}$	n	$\frac{q-1}{2q^{n+1}}$	0	0	0	0	0	0
$I_{n \geq 3}$	$\varepsilon(n)$	$\frac{q-1}{2q^{n+1}}$	0	0	0	0	0	0
II	1	0	0	$\frac{q-1}{q}$	$\frac{q-1}{q}$	$\frac{q-1}{q}$	$\frac{q-1}{q}$	$\frac{q-1}{q}$
III	2	0	0	$\frac{q-1}{q^2}$	$\frac{q-1}{q^2}$	$\frac{q-1}{q^2}$	$\frac{q-1}{q^2}$	$\frac{q-1}{q^2}$
IV	1	0	0	$\frac{q-1}{2q^3}$	$\frac{1}{2q^2}$	0	0	0
IV	3	0	0	$\frac{q-1}{2q^3}$	$\frac{1}{2q^2}$	0	0	0
I_0^*	1	0	0	$\frac{q^2-1}{3q^5}$	0	$\frac{q^2-1}{3q^4}$	$\frac{q^2-1}{3q^4}$	$\frac{q^2-1}{3q^4}$
I_0^*	2	0	0	$\frac{q-1}{2q^4}$	0	$\frac{q-1}{2q^3}$	$\frac{q-1}{2q^3}$	$\frac{q-1}{2q^3}$
I_0^*	4	0	0	$\frac{(q-1)(q-2)}{6q^5}$	0	$\frac{(q-1)(q-2)}{6q^4}$	$\frac{(q-1)(q-2)}{6q^4}$	$\frac{(q-1)(q-2)}{6q^4}$
$I_{n \geq 1}*$	2	0	0	$\frac{(q-1)^2}{2q^{5+n}}$	0	$\frac{(q-1)^2}{2q^{4+n}}$	$\frac{(q-1)^2}{2q^{4+n}}$	$\frac{(q-1)^2}{2q^{4+n}}$
$I_{n \geq 1}*$	4	0	0	$\frac{(q-1)^2}{2q^{5+n}}$	0	$\frac{(q-1)^2}{2q^{4+n}}$	$\frac{(q-1)^2}{2q^{4+n}}$	$\frac{(q-1)^2}{2q^{4+n}}$
$IV*$	1	0	0	$\frac{q-1}{2q^6}$	0	$\frac{q-1}{2q^5}$	$\frac{1}{2q^4}$	0
$IV*$	3	0	0	$\frac{q-1}{2q^6}$	0	$\frac{q-1}{2q^5}$	$\frac{1}{2q^4}$	0
$III*$	2	0	0	$\frac{q-1}{q^7}$	0	$\frac{q-1}{q^6}$	0	$\frac{q-1}{q^5}$
$II*$	1	0	0	$\frac{q-1}{q^8}$	0	$\frac{q-1}{q^7}$	0	$\frac{q-1}{q^6}$

there is one choice of a_6 modulo π such that E terminates at Step 1. We thus have $\psi_{K,\mathfrak{p}}(I_0, 1; 0, \geq 0) = \frac{q-1}{q}$.

Step 2. Suppose that the singular point of E is at (s, u) after reduction by π; accordingly, we shift the singular point to $(0, 0)$ by $(x, y) \mapsto (x+s, y+u)$. Our model is now:

$$(5.1) \quad (y + u)^2 + a_1(x + s)(y + u) + a_3(y + u) = (x + s)^3 + a_4(x + s) + a_6.$$

To stop at Step 2, we require that $\pi \nmid b_2 = a_1^2 + 12s$. Therefore, if $\alpha_1 = 0$, then we always stop. By Hensel's lemma, exactly $\frac{q-1}{q^{n+1}}$ of curves have $v_\pi(\Delta) = n$. Also, for exactly half of E, $T^2 + a_1 T - 3s$ splits in k. Hence, $\psi_{K,\mathfrak{p}}(I_n, n; 0, \geq 0) = \psi_{K,\mathfrak{p}}(I_n, \varepsilon(n); 0, \geq 0) = \frac{q-1}{2q^{n+1}}$. If $\alpha_1 \geq 1$, then $\alpha_3 \geq 1$ by Step 1. In this case, we always pass. Thus, $\psi_{K,\mathfrak{p}}(I_n, c_\mathfrak{p}; \alpha_1, \alpha_3) = 0$ for all $\alpha_1, \alpha_3 \geq 1$. Henceforth, $\alpha_1, \alpha_3 \geq 1$. By taking partial derivatives of (5.1), we find that $s^2 \equiv a_4 \pmod{\pi}$ and $u^2 \equiv a_6 \pmod{\pi}$.

Step 3. Suppose that E reaches Step 3. We stop if $\pi \nmid \pi^{-1}(s^3 + a_4 s + a_6 - u^2 - a_1 su - a_3 u)$. For fixed a_1, a_3, and a_4, there are $q(q-1)$ choices of a_6 modulo π^2. Hence, $\psi_{K,\mathfrak{p}}(II, 1; \alpha_1, \alpha_3) = \frac{q-1}{q}$ for each $\alpha_1, \alpha_3 \geq 1$.

Step 4. E terminates at this step if $\pi^3 \nmid (3s)(2u + a_1 s + a_3)^2 - (3s^2 + a_4 - a_1 u)^2$. By Step 2, we know that $\pi^2 \mid (3s)(2u + a_1 s + a_3)^2 - (3s^2 + a_4 - a_1 u)^2$. Thus, we want $\pi \nmid \pi^{-2}(3s(2u + a_1 s + a_3)^2 + (3s^2 + a_4 - a_1 u)^2)$. Therefore, for fixed a_1 and a_3, there are $q(q-1)$ choices for a_4 modulo π^2 and q choices for a_6 modulo π^2. Thus, $\psi_{K,\mathfrak{p}}(III, 2; \alpha_1, \alpha_3) = \frac{q-1}{q^2}$ for $\alpha_1, \alpha_3 \geq 1$.

Step 5. For an elliptic curve to terminate at Step 5, it must be that $\pi \nmid \pi^{-1}(2u + a_3 + a_1 s)$. If $e = 1$, for fixed a_1 and a_3, we have q choices of a_4 modulo π^2 and $q-1$ choices of a_6 modulo π^2. Now, the Tamagawa number depends on whether the polynomial $Y^2 + \frac{2u + a_3 + a_1}{\pi} Y - \frac{a_6 + a_4 s + s^3 - u^2 - a_1 su - a_3 u}{\pi^2}$ modulo π factors over $\mathbb{F}_q$. To count, we will fix a_1, a_3, and a_4 and count over the $q(q-1)$ possible a_6 modulo π^3. Suppose that the polynomial has a root in $\mathbb{F}_q$ and fix one of the roots. Then, since the trace is fixed, the other root is fixed. Because $\pi^{-1}(2u + a_3 + a_1)$ is non-zero modulo π, the two roots must be distinct. Therefore, there are $\frac{q(q-1)}{2}$ choices of a_6 modulo π^3 that each results in Tamagawa number 1 and 3. Thus, $\psi_{K,\mathfrak{p}}(IV, 1; \geq 1, \geq 1) = \psi_{K,\mathfrak{p}}(IV, 3; \geq 1, \geq 1) = \frac{q-1}{2q^3}$ when $e = 1$. Now, suppose that $e \geq 2$. First, if $\alpha_1 = 1$, then we have $q-1$ choices of a_4 modulo π^2 and q choices for a_6 modulo π^2. With the same argument as above, we conclude that for $\frac{q^2}{2}$ choices of a_6 modulo π^3, the Tamagawa number is 1, and for the same number of choices, the Tamagawa number is 3. Now, suppose that $\alpha_1 \geq 2$. If $\alpha_3 = 1$, then the elliptic curves always terminate at this step. Again, we have that for half of the choices of a_6, the Tamagawa number is 1 and that for the other half, the Tamagawa number is 3. Therefore, we have that $\psi_{K,\mathfrak{p}}(IV, 1; \geq 2, 1) = \psi_{K,\mathfrak{p}}(IV, 3; \geq 2, 1) = \frac{1}{2q^2}$. Conversely, if $\alpha_3 \geq 2$, then no curves terminate at this step. Therefore, $\psi_{K,\mathfrak{p}}(IV, 1; \geq 2, \geq 2) = \psi_{K,\mathfrak{p}}(IV, 3; \geq 2, \geq 2) = 0$.

Step 6. Let $t^2 \equiv s \pmod{\pi}$ and $\beta^2 \equiv \pi^{-2}(s^3 + a_4 s + a_6 - u^2 - a_1 su - a_3 u)$ $\pmod{\pi}$, and define $v := u + \beta\pi$. Following the shifts outlined in Step 6 of Tate's algorithm, we have

$$(5.2) \quad (y + tx + v)^2 + a_1(x + t^2)(y + tx + v) + a_3(y + tx + v)$$
$$= (x + t^2)^3 + a_4(x + t^2) + a_6.$$

We study

$$P(T) = T^3 + \frac{2t^2 - a_1 t}{\pi} T^2 + \frac{3t^4 + a_4 - 2tv - a_1 t^3 - a_1 v - a_3 t}{\pi^2} T$$
$$+ \frac{t^6 + a_4 t^2 + a_6 - v^2 - a_1 t^2 v - a_3 v}{\pi^3}.$$

Define A_2, A_4, and A_6 such that $P(Y) \equiv T^3 + A_2 T^2 + A_4 T + A_6 \pmod{\pi}$. Now, suppose that we fix a_4 modulo π^2 and a_6 modulo π^3. There then exists a bijective map between the π possible values of a_4 modulo π^3 and A_4 modulo π and between the π possible values of a_6 modulo π^4 and A_6 modulo π. For E to terminate at Step 6, $P(T)$ must have three distinct roots. If so, $P(T)$ and $P'(T) \equiv 3T^2 + A_4 \equiv 0 \pmod{\pi}$ should not have shared roots. Therefore, for $P(T)$ to have three distinct roots, $A_2 A_4 \not\equiv A_6$ $\pmod{\pi}$. Thus, for each A_2 modulo π, there are $q(q-1)$ choices of (A_4, A_6) modulo π. We also note that when $P(T)$ has three distinct roots, none of the roots can be A_2 as if so, the remaining two roots must be the same; a contradiction to $P(T)$ having distinct roots.

We now fix A_2 and count the number of $P(T)$ with three distinct roots that have three, one, and no roots in $\mathbb{F}_q$ over (A_4, A_6) modulo π. Because we fix A_2 modulo π, the trace of $P(T)$ is fixed. We first count the number of $P(T)$ that have all three roots in $\mathbb{F}_q$ with fixed trace. We have $q-1$ choices for the first root, $q-2$ choices for the second root, and a fixed choice for the third root, because as long as none of the roots are congruent to A_2 modulo π, the three roots are distinct. Therefore, for fixed A_2, there are $\frac{(q-1)(q-2)}{6}$ choices of (A_4, A_6) modulo π that allows for $P(T)$ to have three distinct roots, all of which are in $\mathbb{F}_q$. We now proceed to count the number of $P(T)$ with three distinct roots with exactly one root in $\mathbb{F}_q$ with fixed a_2. We start by choosing one of $\frac{q^2-q}{2}$ irreducible quadratics. The root in $\mathbb{F}_q$ is then fixed as the trace of $P(T)$ is fixed. Therefore, there are a total of $\frac{q^2-q}{2}$ choices of $P(T)$ with three distinct roots, exactly one root of which is in $\mathbb{F}_q$. Lastly, we count the number of irreducible cubics with three distinct roots. Out of the q^3 elements in $\mathbb{F}_{q^3}$, q are in $\mathbb{F}_q$. Because the traces are equally distributed, for a fixed trace, there are $\frac{q^3-q}{q} = q^2 - 1$ elements with that fixed trace. Since $P(T)$ is a cubic, there are $\frac{q^2-1}{3}$ irreducible cubics with trace A_2.

Now, suppose that $e = 1$. From Steps 1 and 2, we have that $\alpha_1, \alpha_3 \geq 1$. Now, for each fixed $(a_4, \frac{a_1}{\pi})$ modulo π, we have $\frac{(q-1)(q-2)}{6}$ $P(T)$ with three distinct roots all in $\mathbb{F}_q$, $\frac{q(q-1)}{2}$ $P(T)$ with exactly one of the three distinct roots in $\mathbb{F}_q$, and $\frac{q^2-1}{2}$ $P(T)$ with three distinct roots, none of which are in $\mathbb{F}_q$. Thus, we have that for $\psi_{K,\mathfrak{p}}(I_0^*, 4; \geq 1, \geq 1) = \frac{(q-1)(q-2)}{6q^5}$, $\psi_{K,\mathfrak{p}}(I_0^*, 2;$

$\geq 1, \geq 1) = \frac{(q-1)}{2q^4}$, and $\psi_{K,\mathfrak{p}}(I_0^*, 1; \geq 1, \geq 1) = \frac{q^2-1}{3q^5}$. Suppose that $e \geq 2$. If $\alpha_1 = 1$, then $\alpha_3 \geq 1$ from Step 1. Then, A_2 modulo π forms a bijective map with $\frac{a_1}{\pi}$ modulo π. Therefore, by our aforementioned counting of $P(T)$ with three distinct roots, a fixed number of which are in $\mathbb{F}_q$, we have that for $\psi_{K,\mathfrak{p}}(I_0^*, 4; 1, \geq 1) = \frac{(q-1)(q-2)}{6q^5}$, $\psi_{K,\mathfrak{p}}(I_0^*, 2; 1, \geq 1) = \frac{(q-1)}{2q^4}$, and $\psi_{K,\mathfrak{p}}(I_0^*, 1; 1, \geq 1) = \frac{q^2-1}{3q^5}$. If $\alpha_1 \geq 2$, then $\alpha_3 \geq 2$ from Step 6. Then, $A_2 \equiv 0$ (mod π). Therefore, by our aforementioned counting of $P(T)$ with a fixed number of roots in $\mathbb{F}_q$, we have that for $\psi_{K,\mathfrak{p}}(I_0^*, 4; \alpha_1, \alpha_3) = \frac{(q-1)(q-2)}{6q^4}$, $\psi_{K,\mathfrak{p}}(I_0^*, 2; \alpha_1, \alpha_3) = \frac{(q-1)}{2q^3}$, and $\psi_{K,\mathfrak{p}}(I_0^*, 1; \alpha_1, \alpha_3) = \frac{q^2-1}{3q^4}$ for $\alpha_1, \alpha_3 \geq 2$.

Step 7. E terminates at Step 7 if $A_2 A_4 \equiv A_6$ (mod π) and $(A_4, A_6) \not\equiv (A_2^2, A_2^3)$ (mod π). We study the interaction between quadratics $R(Y) = Y^2 + a'_{3,*}Y - a'_{6,*}$ and $S(X) = a'_{2,*}X^2 + a'_{4,*}X + a'_{6,*}$, translating the curve as we move between them. Note that by varying a_6, the quantity $a'_{6,*}$ is surjective modulo π. As before, since a_2, a_3, a_4, a_6 are equidistributed, by Hensel's lemma, there are $\frac{q-1}{q^n}$ residues for which we have Kodaira type I_n, and moreover, half of these cause the quadratic in question to split. Hence, $\psi_{K,\mathfrak{p}}(I_n^*, 1; \geq 1, \geq 1) = \psi_{K,\mathfrak{p}}(I_n^*, 3; \geq 1, \geq 1) = \frac{q-1}{2q^{5+n}}$ for $e = 1$ and $\psi_{K,\mathfrak{p}}(I_n^*, 1; \geq 2, \geq 2) = \psi_{K,\mathfrak{p}}(I_n^*, 3; \geq 2, \geq 2) = \frac{q-1}{2q^{4+n}}$ for $e \geq 2$.

Step 8. Suppose that E reaches Step 8. Then $(A_2, A_4, A_6) \equiv (A_2, A_2^2, A_2^3)$ (mod π). Perform $x \mapsto x + \pi A_2 = x + (2t^2 - a_1 t)$ and let $v' := v + 2t^3 - a_1 t^2$ to get the penultimate model

$$(y + tx + v')^2 + a_1(x + 3t^2 - a_1 t)(y + tx + v') + a_3(y + tx + v')$$
$$= (x + 3t^2 - a_1 t)^3 + a_4(x + 3t^2 - a_1 t) + a_6.$$

We stop if $\pi \nmid \pi^{-2}(2v' + 3a_1 t^2 - a_1^2 t + a_3)$. We notice that if we fix a_1, a_4, and a_6, then a_3 modulo π^2 is fixed such that $2v' + 3a_1 t^2 - a_1^2 t + a_3$ is a multiple of π^2. We then notice that $\pi^{-2}(2v' + 3a_1 t^2 - a_1^2 t + a_3)$ modulo π forms a bijective map with the q possible values of a_3 modulo π^3.

First, suppose that $e = 1$. From Steps 1 and 2, we have that $\alpha_1, \alpha_3 \geq 1$. For each a_3 modulo π^2, we see that for $\frac{q}{2}$ possible values of a_3 modulo π^3, E terminates with Tamagawa number 1 and that for $\frac{q}{2}$ choices for a_3 moudlo π^3, E terminates with Tamagawa number 3. Therefore, when $e \geq 1$, $\psi_{K,\mathfrak{p}}(IV^*, 1; \geq 1, \geq 1) = \psi_{K,\mathfrak{p}}(IV^*, 3; \geq 1, \geq 1) = \frac{q-1}{2q^6}$. For the same reasons, we conclude that when $e = 2$ and $\alpha_1 = 1$ and $\alpha_3 \geq 1$, $\psi_{K,\mathfrak{p}}(IV^*, 1; 1, \geq 1) = \psi_{K,\mathfrak{p}}(IV^*, 3; 1, \geq 1) = \frac{q-1}{2q^6}$. We also see in the same way that $\psi_{K,\mathfrak{p}}(IV^*, 1; \geq 2, \geq 2) = \psi_{K,\mathfrak{p}}(IV^*, 3; \geq 2, \geq 2) = \frac{q-1}{2q^5}$.

Now, suppose that $e \geq 3$. When $\alpha_1 = 1$ and $\alpha_3 \geq 1$, we conclude as we did in the previous paragraph that $\psi_{K,\mathfrak{p}}(IV^*, 1; 1, \geq 1) = \psi_{K,\mathfrak{p}}(IV^*, 3; 1, \geq 1) = \frac{q-1}{2q^6}$. We also see in the same way that $\psi_{K,\mathfrak{p}}(IV^*, 1; \geq 2, \geq 2) = \psi_{K,\mathfrak{p}}(IV^*, 3; \geq 2, \geq 2) = \frac{q-1}{2q^6}$. Similarly, when $\alpha_1 = 2$ and $\alpha_3 \geq 2$, we have that $\psi_{K,\mathfrak{p}}(IV^*, 1; 2, \geq 2) = \psi_{K,\mathfrak{p}}(IV^*, 3; 2, \geq 2) = \frac{q-1}{2q^5}$. But when $\alpha_1 \geq 3$ and $\alpha_3 = 2$, then E necessarily terminates at Step 8. Then depending on $\frac{a_3}{\pi^2}$, E has Tamagawa number 1 and 3 with equal proportions. Therefore, we have that $\psi_{K,\mathfrak{p}}(IV^*, 1; \geq 3, 2) = \psi_{K,\mathfrak{p}}(IV^*, 3; \geq 3, 2) = \frac{1}{2q^4}$. If $\alpha_1, \alpha_3 \geq 3$, however, no E terminates at this step. Therefore, $\psi_{K,\mathfrak{p}}(IV^*, 1; \geq 3, 2) = \psi_{K,\mathfrak{p}}(IV^*, 3; \geq 3, 2) = 0$.

Step 9. Let $w^2 \equiv \pi^{-4}((3t^2 - a_1 t)^3 + a_4(3t^2 - a_1 t) + a_6 - v'^2 + a_1^2 tv' - a_3 v')$ (mod π) and let $w := \pi^2 w' + v'$. Then, we have the final model

$$(5.3) \quad (y + tx + w)^2 + a_1(x + 3t^2 - a_1 t)(y + tx + w) + a_3(y + tx + w)$$
$$= (x + 3t^2 - a_1 t)^3 + a_4(x + 3t^2 - a_1 t) + a_6.$$

We terminate at this case if $\pi^4 \nmid -2tw - a_1 w - a_1^2 t^2 - a_3 t + 3(3t^2 - a_1 t)^2 + a_4$. From Step 8, we have that $\pi^3 \mid -2tw - a_1 w - a_1^2 t^2 - a_3 t + 3(3t^2 - a_1 t)^2 + a_4$. Therefore, we want $\pi \mid \pi^{-3}(-2tw - a_1 w - a_1^2 t^2 - a_3 t + 3(3t^2 - a_1 t)^2 + a_4)$. For fixed a_4 modulo π^3, $\pi^{-3}(-2tw - a_1 w - a_1^2 t^2 - a_3 t + 3(3t^2 - a_1 t)^2 + a_4)$ forms a bijective map with the q possible values of a_4 modulo π^4. When $e = 1$, $\alpha_1, \alpha_3 \geq 1$ from Steps 1 and 2. Therefore, $\psi_{K,\mathfrak{p}}(III^*, 2; \geq 1, \geq 1) = \frac{q-1}{q^7}$. When $e = 2$, we have from Steps 1, 2 and 5 that either $\alpha_1 = 1$ and $\alpha_3 \geq 1$ or $\alpha_1, \alpha_3 \geq 2$. We thus conclude, $\psi_{K,\mathfrak{p}}(III^*, 2; 1, \geq 1) = \frac{q-1}{q^7}$ and $\psi_{K,\mathfrak{p}}(III^*, 2; \geq 2, \geq 2) = \frac{q-1}{q^6}$. Lastly, when $e \geq 3$, we have that either $\alpha_1 = 1$ and $\alpha_3 \geq 1$, $\alpha_1 = 2$ and $\alpha_3 \geq 2$, and $\alpha_1 \geq 3$ and $\alpha_3 \geq 3$. We similarly conclude that $\psi_{K,\mathfrak{p}}(III^*, 2; 1, \geq 1) = \frac{q-1}{q^7}$, $\psi_{K,\mathfrak{p}}(III^*, 2; 2, \geq 2) = \frac{q-1}{q^6}$, and $\psi_{K,\mathfrak{p}}(III^*, 2; \geq 3, \geq 3) = \frac{q-1}{q^5}$.

Step 10. E terminates at Step 10 if $\pi^6 \nmid -w^2 + a_1^2 tw - a_3 w + (3t^2 - a_1 t)^3 - a_1 a_4 t + a_6$. From Step 9, we have that $\pi^5 \mid -w^2 + a_1^2 tw - a_3 w + (3t^2 - a_1 t)^3 - a_1 a_4 t + a_6$. Therefore, we want that $\pi \mid \pi^{-5}(-w^2 + a_1^2 tw - a_3 w + (3t^2 - a_1 t)^3 - a_1 a_4 t + a_6)$. Fix a_6 modulo π^5. Then, note that $\pi^{-5}(-w^2 + a_1^2 tw - a_3 w + (3t^2 - a_1 t)^3 - a_1 a_4 t + a_6)$ modulo π forms a bijective map with the q possible values of a_6 modulo π^6. For $q - 1$ of the q possible values of a_6 modulo π^6, E terminates at Step 10. When $e = 1$, $\alpha_1, \alpha_3 \geq 1$ from Steps 1 and 2. Therefore, $\psi_{K,\mathfrak{p}}(II^*, 1; \geq 1, \geq 1) = \frac{q-1}{q^8}$. When $e = 2$, we have from Steps 1, 2 and 5 that either $\alpha_1 = 1$ and $\alpha_3 \geq 1$ or $\alpha_1, \alpha_3 \geq 2$. We thus conclude, $\psi_{K,\mathfrak{p}}(II^*, 1; 1, \geq 1) = \frac{q-1}{q^8}$ and $\psi_{K,\mathfrak{p}}(II^*, 2; \geq 2, \geq 2) = \frac{q-1}{q^7}$. Lastly, when $e \geq 3$, we have that either $\alpha_1 = 1$ and $\alpha_3 \geq 1$, $\alpha_1 = 2$ and $\alpha_3 \geq 2$, and

$\alpha_1 \geq 3$ and $\alpha_3 \geq 3$. We similarly conclude that $\psi_{K,\mathfrak{p}}(II^*, 1; 1, \geq 1) = \frac{q-1}{q^8}$, $\psi_{K,\mathfrak{p}}(II^*, 1; 2, \geq 2) = \frac{q-1}{q^7}$, and $\psi_{K,\mathfrak{p}}(II^*, 1; \geq 3, \geq 3) = \frac{q-1}{q^6}$.

Step 11. For E to reach Step 11, it must not have terminated at a previous step. Therefore, we check that when $e = 1$, $\alpha_1, \alpha_3 \geq 1$, the proportion of non-minimal curves is $\frac{1}{q^8}$, when $e = 2$, $\alpha_1 = 1$, and $\alpha_3 \geq 1$, the proportion of non-minimal curves is $\frac{1}{q^8}$ as well, and that when $e = 2$ and $\alpha_1, \alpha_3 \geq 2$, the proportion of non-minimal curves is $\frac{1}{q^7}$. When $e \geq 3$, the proportion of non-minimal curves equal $\frac{1}{q^8}$ when $\alpha_1 = 1$ and $\alpha_3 \geq 1$, $\frac{1}{q^7}$ when $\alpha_1 = 2$ and $\alpha_3 \geq 2$, and $\frac{1}{q^6}$ when $\alpha_1, \alpha_3 \geq 3$. □

We now show how we reclassify the non-minimal models of one family as another family of curves. As in Section 4, we first note that the models in $F(\geq e, \geq e)$ and $F(\infty, \infty)$ have the same local properties in the following sense.

Remark 5.3. Because linear transformations do not change the local data of an elliptic curve, without loss of generality, instead of computing the local density on short Weierstrass forms $F(\infty, \infty)$, we can compute the local density at the set

(5.4)
$$\left\{ \left(E : (y + tx + s)^2 = \left(x + \frac{t^2}{3} \right)^3 + a_4 \left(x + \frac{t^2}{3} \right) + a_6 \right) : s, t, a_4, a_6 \text{ integral} \right\}.$$

By the surjectivity of a_4 and a_6, the set in (5.4) is precisely $F(\geq e, \geq e)$.

Thus, moving forward, if $\alpha_1, \alpha_3 \geq e$, then we work with the curves in $F(\geq e, \geq e)$ instead of $F(\alpha_1, \alpha_3)$. Similarly, if $\alpha_1 \geq e > \alpha_3$, then we work with the curves in $F(\geq e, \alpha_3)$ and if $\alpha_3 \geq e > \alpha_1$, then we work with the curves in $F(\alpha_1, \geq e)$. We first show that, for $\alpha_3, \alpha_1 < e$, the local densities at the non-minimal models of a family $F(\alpha_1, \alpha_3)$ exactly match the local densities at the family $F(\alpha_1 - 1, \alpha_3 - 3)$. To do this, we establish a map which sends a non-minimal model in $F(\alpha_1, \alpha_3)$ to another isomorphic model in $F(\alpha_1 - 1, \alpha_3 - 3)$, induced by the transformation at Step 11 followed by the shift $x \mapsto x - a_2/3$. Likewise, we show that for $\alpha_1 \geq e > \alpha_3$ (resp. $\alpha_3 \geq e > \alpha_1$ and $\alpha_1, \alpha_3 \geq e$), the local densities at the non-minimal models of a family $F(\geq e, \alpha_3)$ (resp. $F(\alpha_1, \geq e)$ and $F(\geq e, \geq e)$) exactly match the local densities at the family $F(\geq e - 1, \alpha_3 - 3)$ (resp. $F(\alpha_1 - 1, \geq e - 3)$ and $F(\geq e - 1, \geq e - 3)$).

Lemma 5.4. *We have surjective, q^4-to-1 maps between*

- *the set of non-minimal models in $F(\alpha_1, \alpha_3)$ and the set $F(\alpha_1 - 1, \alpha_3 - 3)$ for each $\alpha_1, \alpha_3 < e$,*

- *the set of non-minimal models in $F(\geq e, \alpha_3)$ and the set $F(\geq e - 1,$ $\alpha_3 - 3)$ for each $\alpha_1 \geq e > \alpha_3$*
- *the set of non-minimal models in $F(\alpha_1, \geq e)$ and the set $F(\alpha_1 - 1,$ $\geq e - 3)$ for each $\alpha_3 \geq e > \alpha_1$*
- *the non-minimal models in $F(\geq e, \geq e)$ and the set $F(\geq e - 1,$ $\geq e - 3)$*

that each sends E to its transformation E' after passing Step 11.

Proof. First, suppose that $\alpha_1, \alpha_3 < e$. Recall from Step 11 of Tate's algorithm that for non-minimal $E(a_1, a_2, a_3, a_4, a_6)$, Tate's algorithm produces a unique residue $t \pmod{\pi}$ and $w \pmod{\pi^3}$ for which

$$(y + tx + w)^2 + a_1(x + 3t^2 - a_1 t)(y + tx + w) + a_3(y + tx + w)$$
$$= (x + 3t^2 - a_1 t)^3 + a_4(x + 3t^2 - a_1 t) + a_6$$

has the coefficient of y and xy divisible by π and π^3, respectively, and the coefficient of x^i divisible by π^i for $i = 2, 4, 6$. Hence, each non-minimal model $E(a_1, a_2, a_3, a_4, a_6) \in F(\alpha_1, \alpha_3)$ is sent to

$$\widehat{E}(a_1, a_2, a_3, a_4, a_6) := E\left(\frac{a_1 + 2t}{\pi}, \frac{8t^2 - 4a_1 t}{\pi^2}, \frac{2w + 3a_1 t^2 - a_1^2 t + a_3}{\pi^3}, \right.$$
$$\frac{-2tw - a_1 w - 3a_1 t^3 + a_1^2 t^2 - a_3 t + 3(3t^2 - a_1 t^2) + a_4}{\pi^4},$$
$$\left. \frac{-w^2 - a_1 w(3t^2 - a_1 t) - a_3 w + (3t^2 - a_1 t)^3 + a_4(3t^2 - a_1 t) + a_6}{\pi^6} \right),$$

with $v_\pi(2t + a_1) = v_\pi(a_1) = \alpha_1$ and $v_\pi(2w + 3a_1 t^2 - a_1^2 t + a_3) = v_\pi(a_3) = \alpha_3$. Now, let $\widehat{E}(a_1, a_2, a_3, a_4, a_6) = E(\widehat{a_1}, \widehat{a_2}, \widehat{a_3}, \widehat{a_4}, \widehat{a_6})$. Then we perform $x \to x - \frac{\widehat{a_2}}{3}$ to $\widehat{E}$ and transform $\widehat{E}$ to E' :

$$E'(a_1, a_2, a_3, a_4, a_6) := y^2 + \widehat{a_1}\left(x - \frac{\widehat{a_2}}{3}\right)y + \widehat{a_3}y$$
$$= \left(x - \frac{\widehat{a_2}}{3}\right)^3 + \widehat{a_2}\left(x - \frac{\widehat{a_2}}{3}\right)^2 + \widehat{a_4}\left(x - \frac{\widehat{a_2}}{3}\right) + \widehat{a_6}.$$

We now have

$$E'(a_1, a_2, a_3, a_4, a_6)$$
$$= E\left(\widehat{a_1}, -\frac{\widehat{a_1}\widehat{a_2}}{3} + \widehat{a_3}, \frac{-\widehat{a_2}^2}{3} + \widehat{a_4}, \frac{2\widehat{a_2}^3}{27} - \frac{\widehat{a_2}\widehat{a_4}}{3} + \widehat{a_6} \right) \in F(\alpha_1 - 1, \alpha_3 - 3).$$

The two transformations are well-defined, so the map is also well-defined.

Conversely, given a model $E(a_1', a_3', a_4', a_6') \in F(\alpha_1 - 1, \alpha_3 - 3)$, pick a pair of residues $t \pmod{\pi}$ and $w \pmod{\pi^3}$. Then, there is a unique choice of a_2' for which

$$E(\widehat{a_1}, \widehat{a_2}, \widehat{a_3}, \widehat{a_4}, \widehat{a_6}) := y^2 + a_1'\left(x + \frac{a_2'}{3}\right)y + a_3'y$$

$$= \left(x + \frac{a_2'}{3}\right)^3 + a_4'\left(x + \frac{a_2'}{3}\right) + a_6'$$

and $(\widehat{a_1}, \widehat{a_2}) = \left(\frac{a_1 + 2t}{\pi}, \frac{8t^2 - 4a_1 t}{\pi^2}\right)$ for some a_1 so that $E(\widehat{a_1}, \widehat{a_2}, \widehat{a_3}, \widehat{a_4}, \widehat{a_6})$ has some preimage $E \in F(\alpha_1, \alpha_3)$. In fact, there is a unique preimage E for which $E \mapsto E(\widehat{a_1}, \widehat{a_2}, \widehat{a_3}, \widehat{a_4}, \widehat{a_6})$ after Step 11. Hence, after varying t and w across a set of q and q^3 representatives, respectively, we have shown the aforementioned map is q^4-to-1, as we had sought. The proof of the statement of the lemma when $\alpha_1 \geq e$ or $\alpha_3 \geq e$ follows in the same way and is thus omitted. $\qquad\square$

We now finish by using our lemmas to compute $\delta_{K,\mathfrak{p}}(c)$ by forming a Markov chain amongst families of curves. Lemma 5.4 establish the edges between these families, while Lemma 5.2 establishes the local densities at each node. This information is collated in Figures 5.1 to 5.3.
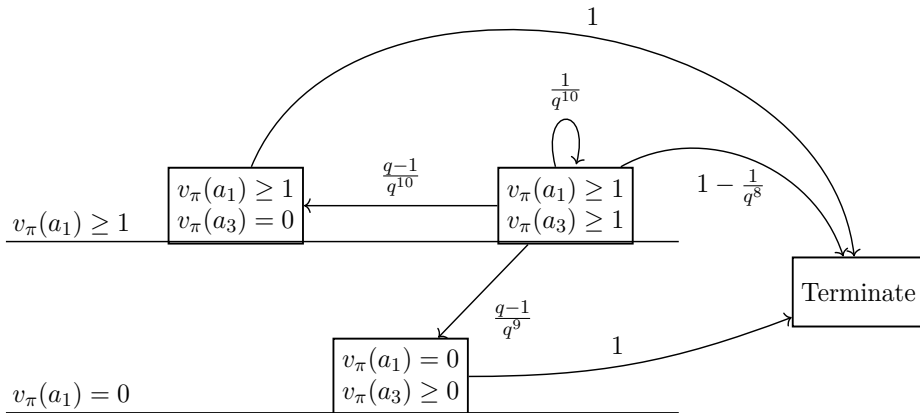

FIGURE 5.1. The Markov Chain structure when $\mathfrak{p} \mid (2)$ for $e = 1$.
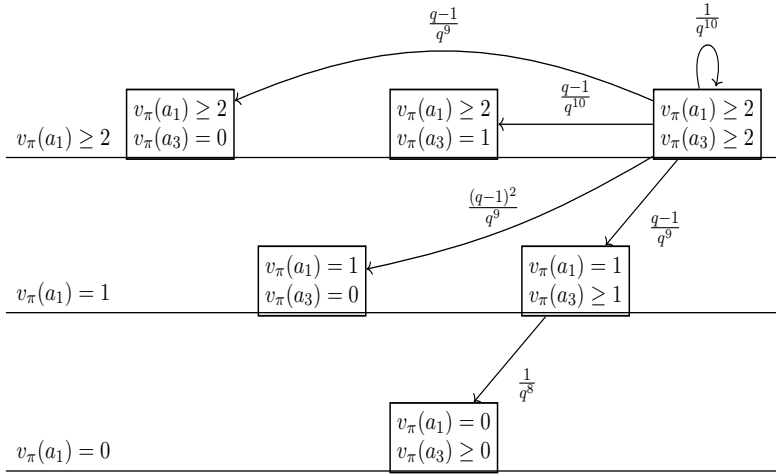
FIGURE 5.2. The Markov Chain structure when $\mathfrak{p} \mid (2)$ for $e = 2$.

Proposition 5.5. *For $\mathfrak{p} \mid (2)$ is a prime ideal in K and $c \geq 1$, let $q := N_{K/\mathbb{Q}}(\mathfrak{p})$. If $e = 1$, we have*

$$
\delta_{K,\mathfrak{p}}(c) = \begin{cases}
1 - \dfrac{(q-1)(6q^{10} + 9q^9 + 7q^8 + 8q^7 + 7q^6 + 9q^5 + 6q^4 + 6q + 3)}{6q(q+1)(q^{10}-1)} & \text{if } c = 1, \\[3mm]
\dfrac{(q-1)(2q^{11} + 2q^{10} + q^9 + 2q^8 + q^7 + 2q^6 + 2q^5 + 2q^2 - 1)}{2q^2(q+1)(q^{10}-1)} & \text{if } c = 2, \\[3mm]
\dfrac{(q-1)(q^{10} + q^7 + q - 1)}{2q^3(q^{10}-1)} & \text{if } c = 3, \\[3mm]
\dfrac{(q-1)(q^{10} + q^9 + 3q - 3)}{6q^4(q^{10}-1)} & \text{if } c = 4, \\[3mm]
\dfrac{(q-1)^2}{2q^c(q^{10}-1)} & \text{if } c \geq 5.
\end{cases}
$$

If $e = 2$, we have

$$
\delta_{K,\mathfrak{p}}(c) = \begin{cases}
1 - \dfrac{(q-1)(6q^{18} + 10q^{17} + 8q^{16} + 7q^{15} + 9q^{14} + 6q^{13} + 6q^{10} + 9q^9)}{6q^9(q+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{11}}\right) & \text{if } c = 1, \\[3mm]
\dfrac{(q-1)(2q^{19} + 3q^{18} + 2q^{17} + q^{16} + 2q^{15} + 2q^{14} + 2q^{11} + 2q^{10}))}{2q^{10}(q+1)(q^{10}-1)} + O\left(\dfrac{1}{q^{11}}\right) & \text{if } c = 2, \\[3mm]
\dfrac{(q-1)(q^2+1)(q^4 - q^2 + 1)(q^{10} + q - 1)}{2q^{11}(q^{10}-1)} & \text{if } c = 3, \\[3mm]
\dfrac{(q-1)(q^{19} + q^{18} + q^{10} - q^8 + 3q - 3)}{6q^{12}(q^{10}-1)} & \text{if } c = 4, \\[3mm]
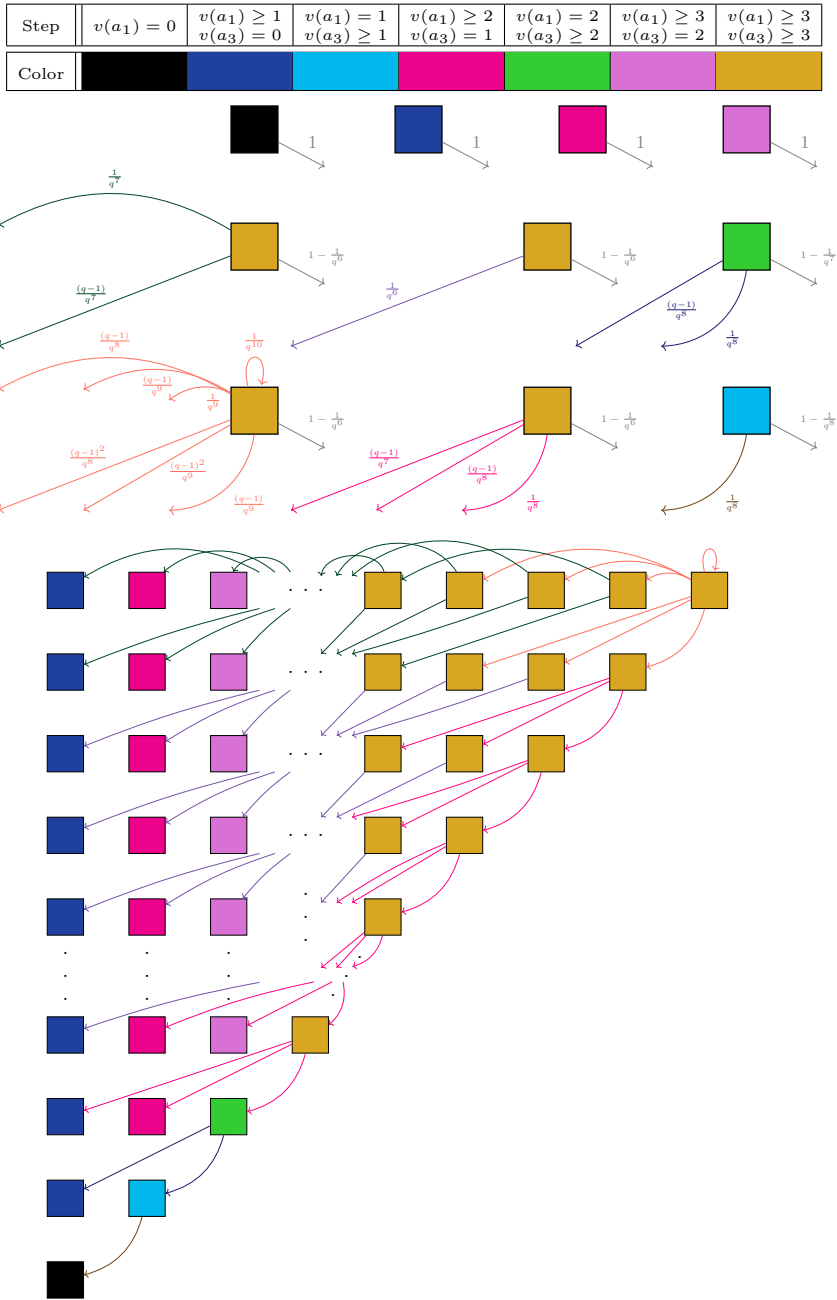\dfrac{(q-1)^2}{2q^{8+c}(q^{10}-1)} & \text{if } c \geq 5.
\end{cases}
$$

Step	$v(a_1) = 0$	$v(a_1) \geq 1$ $v(a_3) = 0$	$v(a_1) = 1$ $v(a_3) \geq 1$	$v(a_1) \geq 2$ $v(a_3) = 1$	$v(a_1) = 2$ $v(a_3) \geq 2$	$v(a_1) \geq 3$ $v(a_3) = 2$	$v(a_1) \geq 3$ $v(a_3) \geq 3$
Color							

FIGURE 5.3. The Markov Chain structure when $\mathfrak{p} \mid (2)$ for $e \geq 3$.

The exact proportions for $e = 2$ and the proportions for $e \geq 3$ are given in Proposition B.2 of the extended version of the paper [3].

Proof. The proof is very similar to Proposition 4.5: we compute the proportion of curves which reach each of the $(e+1)(e+2)/2$ non-terminal nodes, then sum and scale the proportions by $\frac{q^{10}}{q^{10}-1}$ to account for curves which initially loop back to $F(\geq e, \geq e)$. □

6. Proofs of the Main Results

In this section, we make use of the computed local densities to prove our main results.

Proof of Theorem 1.2. That

$$(6.1) \qquad \prod_{\mathfrak{p}} \left(\frac{\delta_{K,\mathfrak{p}}(1)}{1^s} + \frac{\delta_{K,\mathfrak{p}}(2)}{2^s} + \frac{\delta_{K,\mathfrak{p}}(3)}{3^s} + \dots \right) = \sum_{m=1}^{\infty} \frac{P_{\mathrm{Tam}}(K, m)}{m^s}$$

follows directly from expansion of the product over $\mathfrak{p}$, but for $P_{\mathrm{Tam}}(K, m)$ to be well-defined, we must additionally show that its value given by the left hand side of (6.1) converges. From Proposition 3.3, for a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \nmid (6)$, we have that $1 - \frac{1}{q^2} < \delta_{K,\mathfrak{p}}(1) < 1$, where $q := N_{K/\mathbb{Q}}(\mathfrak{p})$. Therefore, the convergence of $P_{\mathrm{Tam}}(K, m)$ follows from the convergence of $\zeta(2)$. □

Proof of Corollary 1.4. By Theorem 1.2,

$$(6.2) \qquad \prod_{\mathfrak{p}} \left(\frac{\delta_{K,\mathfrak{p}}(1)}{1^s} + \frac{\delta_{K,\mathfrak{p}}(2)}{2^s} + \frac{\delta_{K,\mathfrak{p}}(3)}{3^s} + \dots \right) = \sum_{m=1}^{\infty} \frac{P_{\mathrm{Tam}}(K, m)}{m^s}.$$

Thus, the expansion of the left hand side gives $P_{\mathrm{Tam}}(K, 1) = \prod_{\mathfrak{p}} \delta_{K,\mathfrak{p}}(1)$, which converges as shown in the proof of Theorem 1.2.

Now, setting $m = -1$ in Theorem 1.2, the average Tamagawa number $L_{\mathrm{Tam}}(K, -1)$ is given as

$$L_{\mathrm{Tam}}(K, -1) = \sum_{m=1}^{\infty} P_{\mathrm{Tam}}(K, m) m$$

$$= \prod_{\mathfrak{p}} \left(\delta_{K,\mathfrak{p}}(1) + 2\delta_{K,\mathfrak{p}}(2) + 3\delta_{K,\mathfrak{p}}(3) + \dots \right).$$

By Proposition 3.3, for prime ideal $\mathfrak{p}$ with $\mathfrak{p} \nmid (6)$ and $q := N_{K/\mathbb{Q}}(\mathfrak{p})$, we have that $\delta_{K,\mathfrak{p}}(1) = 1 - \frac{1}{q^2} + O(1/q^3)$ and $0 < c\delta_{K,\mathfrak{p}}(c) < \frac{c}{q^c}$ for $c \geq 2$. Since $\sum_{c=2}^{\infty} \frac{c}{q^c} = \frac{2q-1}{(q-1)^2 q} = \frac{2}{q^2} + O(\frac{1}{q^3})$, we obtain

$$(6.3) \qquad \sum_{c=1}^{\infty} c\delta_{K,\mathfrak{p}}(c) = 1 + \frac{1}{q^2} + O\left(\frac{1}{q^3}\right).$$

From Propositions 4.5 and 5.5, when $\mathfrak{p} \mid (6)$, letting $q := N_{K/\mathbb{Q}}(\mathfrak{p})$, we have

$$(6.4) \quad \sum_{c \geq 1} c\delta_{K,\mathfrak{p}}(c) \leq \delta_{K,\mathfrak{p}}(1) + \sum_{k=1}^{\infty} (4+k)(1 - \delta_{K,\mathfrak{p}}(1))\frac{q-1}{q^k}$$

$$= 5 - 4\delta_{K,\mathfrak{p}}(1) + \frac{(1 - \delta_{K,\mathfrak{p}}(1))}{q-1}.$$

Therefore, $L_{\text{Tam}}(K, -1)$ must converge as sought. □

Proof of Corollary 1.6. We begin by establishing bounds on $P_{\text{Tam}}(K, 1)$ with respect to d. Recall from Corollary 1.4 that

$$(6.5) \quad P_{\text{Tam}}(K, 1) = \prod_{\mathfrak{p}} \delta_{K,\mathfrak{p}}(1).$$

We first establish a lower bound on $P_{\text{Tam}}(K, 1)$ with respect to d. From Propositions 3.3, 4.5 and 5.5, $\delta_{K,\mathfrak{p}}(1)$ is at least when each $\mathfrak{p}$ is unramified and has residue field degree 1. If $\mathfrak{p}$ is unramified and has residue field degree 1, then $q = N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ and

$$(6.6) \quad P_{\text{Tam}}(\mathbb{Q}, 1)^d \leq P_{\text{Tam}}(K, 1).$$

From [5], $P_{\text{Tam}}(\mathbb{Q}, 1) = 0.5054\ldots$. Therefore,

$$(6.7) \quad (0.5054)^d < P_{\text{Tam}}(\mathbb{Q}, 1)^d \leq P_{\text{Tam}}(K, 1).$$

Next, we establish a lower bound on $P_{\text{Tam}}(K, 1)$ with respect to d. Again, from Propositions 3.3, 4.5 and 5.5, $\delta_{K,\mathfrak{p}}$ is at most when each p is inert. When p is inert, $q := N_{K/\mathbb{Q}}(\mathfrak{p}) = p^d$. Furthermore, from Propositions 3.3 and 4.5, when $\mathfrak{p} \nmid (2)$,

$$(6.8) \quad \delta_{K,\mathfrak{p}}(1) \leq 1 - \frac{1}{q^2} + \frac{1}{q^3} = 1 - \frac{1}{p^{2d}} + \frac{1}{p^{3d}}$$

and from Proposition 5.5, when $\mathfrak{p} \mid (2)$,

$$(6.9) \quad \delta_{K,\mathfrak{p}}(1) \leq 1 - \frac{1}{q} + \frac{1}{q^2} = 1 - \frac{1}{2^d} + \frac{1}{2^{2d}}.$$

Now collecting (6.5), (6.8), and (6.9), we have that

$$(6.10) \quad P_{\text{Tam}}(K, 1) = \prod_{\mathfrak{p}} \delta_{K,\mathfrak{p}}(1) \leq \left(1 - \frac{1}{2^d} + \frac{1}{2^{2d}}\right) \prod_{p \geq 3 \text{ prime}} \left(1 - \frac{1}{p^{2d}} + \frac{1}{p^{3d}}\right).$$

Because $\prod_{p \text{ prime}} \left(1 - \frac{1}{p^{2d}}\right) = \frac{1}{\zeta(2d)}$ [6], the upper bound on $P_{\text{Tam}}(K, 1)$ in the theorem statement follows from (6.10) if

$$(6.11) \quad \left(1 - \frac{1}{2^d} + \frac{1}{2^{2d}}\right) \prod_{p \geq 3 \text{ prime}} \left(1 - \frac{1}{p^{2d}} + \frac{1}{p^{3d}}\right) \leq \prod_{p \text{ prime}} \left(1 - \frac{1}{p^{2d}}\right).$$

By combining the denominators of the terms within each parenthesis of (6.11), we can rewrite (6.11) as

$$(6.12) \quad \left(\frac{2^{2d} - 2^d + 1}{2^{2d}}\right) \prod_{p \geq 3 \text{ prime}} \left(\frac{p^{3d} - p^d + 1}{p^{3d}}\right) \leq \prod_{p \text{ prime}} \left(\frac{p^{2d} - 1}{p^{2d}}\right).$$

Dividing each side of (6.12) by $\left(\frac{2^{2d} - 2^d + 1}{2^{2d}}\right) \prod_{p \geq 3 \text{ prime}} \left(\frac{p^{2d} - 1}{p^{2d}}\right)$ gives

$$(6.13) \quad \prod_{p \geq 3 \text{ prime}} \left(\frac{p^{3d} - p^d + 1}{p^d(p^{2d} - 1)}\right) = \prod_{p \geq 3 \text{ prime}} \left(1 + \frac{1}{p^{3d} - p^d}\right)$$

$$\leq \frac{2^{2d} - 1}{2^{2d} - 2^d + 1} = 1 + \frac{2^d - 2}{2^{2d} - 2^d + 1}.$$

Now, because

$$(6.14) \quad \prod_{p \geq 3 \text{ prime}} \left(1 + \frac{1}{p^{3d} - p^d}\right) \leq \prod_{p \text{ prime}} \left(1 + \frac{1}{p^{3d-1} - 1}\right) = \zeta(3d - 1),$$

and

$$(6.15) \quad \zeta(3d - 1) \leq 1 + \frac{1}{2^{3d-1}} + \int_2^\infty \frac{1}{x^{3d-1}} \, dx$$

$$= 1 + \frac{1}{2^{3d-1}} + \frac{1}{(3d - 2)2^{3d-2}} \leq 1 + \frac{2^d - 2}{2^{2d} - 2^d + 1},$$

(6.13) holds true. Therefore, (6.11) holds true. Thus, combining (6.10) and (6.11), we have that

$$(6.16) \quad P_{\text{Tam}}(K, 1) \leq \frac{1}{\zeta(2d)} = (-1)^{d+1} \frac{2(2d)!}{B_{2d}(2\pi)^{2d}},$$

where the last equality follows from a well-known result by Euler [1].

We now establish bounds on $L_{\text{Tam}}(K, -1)$ with respect to d. Recall from Corollary 1.4 that

$$(6.17) \quad L_{\text{Tam}}(K, -1) = \prod_{\mathfrak{p}} \sum_{m=1}^\infty \delta_{K,\mathfrak{p}}(m)m.$$

We begin by establishing an upper bound on $L_{\text{Tam}}(K, -1)$ with respect to d. From Propositions 3.3, 4.5 and 5.5, $L_{\text{Tam}}(K, -1)$ is at most when each p splits completely. When p splits completely, $q := N_{K/\mathbb{Q}}(\mathfrak{p}) = p$, and

$$(6.18) \quad L_{\text{Tam}}(K, -1) \leq L_{\text{Tam}}(\mathbb{Q}, -1)^d.$$

From [5], $L_{\text{Tam}}(\mathbb{Q}, -1) = 1.8184\ldots$ Therefore,

$$(6.19) \quad L_{\text{Tam}}(K, -1) \leq L_{\text{Tam}}(\mathbb{Q}, -1)^d < (1.8184)^d.$$

We now establish a lower bound on $L_{\text{Tam}}(K, -1)$ with respect to d. Again, from Propositions 3.3, 4.5 and 5.5, $L_{\text{Tam}}(K, -1)$ is at least when

each p is inert. When p is inert, $q := N_{K/\mathbb{Q}}(\mathfrak{p}) = p^d$. Now, because for each $\mathfrak{p}$,

$$(6.20) \qquad \delta_{K,\mathfrak{p}}(1) + 2(1 - \delta_{K,\mathfrak{p}}(1)) = 2 - \delta_{K,\mathfrak{p}}(1) \leq \sum_{m=1}^{\infty} \delta_{K,\mathfrak{p}}(m)m,$$

from Propositions 3.3, 4.5 and 5.5, we have that

$$(6.21) \qquad \left(1 + \frac{1}{2^d} - \frac{1}{2^{2d}}\right) \prod_{p \geq 3 \text{ prime}} \left(1 + \frac{1}{p^{2d}} - \frac{1}{p^{3d}}\right) \leq L_{\text{Tam}}(K, -1).$$

Now, because $\prod_{p \text{ prime}}\left(1 + \frac{1}{p^{2d}}\right) = \frac{\zeta(2d)}{\zeta(4d)}$, if we show that

$$(6.22) \qquad \prod_{p \text{ prime}} \left(1 + \frac{1}{p^{2d}}\right) \leq \left(1 + \frac{1}{2^d} - \frac{1}{2^{2d}}\right) \prod_{p \geq 3 \text{ prime}} \left(1 + \frac{1}{p^{2d}} - \frac{1}{p^{3d}}\right),$$

then the statement of the theorem follows from (6.21). Now, combining the denominator across the terms within the parentheses of (6.22), we can rewrite (6.22) as

$$(6.23) \qquad \prod_{p \text{ prime}} \left(\frac{p^{2d} + 1}{p^{2d}}\right) \leq \left(\frac{2^{2d} + 2^d - 1}{2^{2d}}\right) \prod_{p \geq 3 \text{ prime}} \left(\frac{p^{3d} + p^d - 1}{p^{3d}}\right).$$

Dividing each side by $\frac{2^{2d}+2^d-1}{2^{2d}} \prod_{p \geq 3 \text{ prime}}\left(\frac{p^{2d}+1}{p^{2d}}\right)$, (6.23) is equivalent to

$$(6.24) \quad \frac{2^{2d}+1}{2^{2d}+2^d-1} = 1 - \frac{2^d - 2}{2^{2d} + 2^d - 1}$$

$$\leq \prod_{p \geq 3 \text{ prime}} \left(\frac{p^{3d} + p^d - 1}{p^{3d} + p^d}\right) = \prod_{p \geq 3 \text{ prime}} \left(1 - \frac{1}{p^{3d} + p^d}\right).$$

Now, because

$$(6.25) \qquad \frac{1}{\zeta(3d)} = \prod_{p \geq 3 \text{ prime}} \left(1 - \frac{1}{p^{3d}}\right) \leq \prod_{p \geq 3 \text{ prime}} \left(1 - \frac{1}{p^{3d} + p^d}\right),$$

(6.24) follows if we show that

$$(6.26) \qquad 1 - \frac{2^d - 2}{2^{2d} + 2^d - 1} \leq \frac{1}{\zeta(3d)}.$$

Now, because

$$(6.27) \qquad \zeta(3d) \leq 1 + \frac{1}{2^{3d}} + \int_2^{\infty} \frac{1}{x^{3d}} \, \mathrm{d}x = 1 + \frac{1}{2^{3d}} + \frac{1}{(3d-1)2^{3d-1}}$$

and

$$1 - \frac{2^d - 2}{2^{2d} + 2^d - 1} \le 1 - \frac{3d + 1}{2^{3d}(3d - 1) + 3d + 1}$$

$$= \frac{2^{3d}(3d - 1)}{(2^{3d} + 1)(3d - 1) + 2} = \frac{1}{1 + \frac{1}{2^{3d}} + \frac{1}{2^{3d-1}(3d-1)}},$$

(6.26) holds true. Now, combining (6.21) and (6.22), we have that

$$(6.28) \qquad \frac{\zeta(2d)}{\zeta(4d)} = (-1)^d \frac{B_{2d}(4d)!}{B_{4d}(2d)!(2\pi)^{2d}} \le L_{\mathrm{Tam}}(K, -1),$$

where the equality follows from Euler [1]. □

Proof of Theorem 1.7. It suffices to explicitly construct a family of multi-quadratic fields whose Tamagawa trivial proportions tend to 0 and a family of cyclotomic fields whose proportions tend to 1.

We begin by proving $\liminf_{d \to +\infty} t^-(d) = 0$. Let $p_1 < p_2 < p_3 < \ldots$ be an infinite sequence of 1 (mod 8) primes. Consider the sequence of multi-quadratic field extensions

$$K_1 = \mathbb{Q}(\sqrt{p_1}),$$
$$K_2 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}),$$
$$K_3 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}),$$
$$\vdots$$

Fix a field K_i. Since 2 is a quadratic residue modulo p_i for $1 \le j \le i$, (2) splits completely in the number fields $\mathbb{Q}(\sqrt{p_j})$. Hence the ideal (2) also splits completely in the composite field K_i. In particular, there are 2^i distinct prime ideals above (2), each with inertial degree and ramification index 1. Recall from Proposition 5.5 that for norm 2 unramified prime ideals $\mathfrak{p}$ we have $\delta_{K,\mathfrak{p}}(1) = 241/396$. Hence, we have an upper bound

$$(6.29) \quad t^-(2^i) \le P_{\mathrm{Tam}}(K_i; 1) = \prod_{\mathfrak{p}} \delta_{K_i,\mathfrak{p}}(1) \le \prod_{\mathfrak{p}|(2)} \delta_{K_i,\mathfrak{p}}(1) = (241/396)^{2^i},$$

which tends to 0 as i grows large. Thus, $\liminf_{d \to +\infty} t^-(d) = 0$.

In fact, this sequence of fields also show that $\limsup_{d \to +\infty} \mu^+(d) = \infty$. For each $\mathfrak{p}$ above 2, we may compute $\sum_{m=1}^{\infty} \delta_{K,\mathfrak{p}}(m)m > 1.49$, whence

$$(6.30) \qquad \mu^+(2^i) \ge \prod_{\mathfrak{p}} \sum_{m=1}^{\infty} \delta_{K_i,\mathfrak{p}}(m)m \ge \prod_{\mathfrak{p}|(2)} \sum_{m=1}^{\infty} \delta_{K_i,\mathfrak{p}}(m)m > (1.49)^{2^i}.$$

The right-hand side tends to infinity as $i \to \infty$, from which the claim follows.

We now prove that $\limsup_{d \to +\infty} t^+(d) = 1$ for the sequence of fields $K = \mathbb{Q}(\xi_a)$, where a is some increasing sequence of odd primes and $\xi_a =$

$e^{2\pi i/a}$. By Propositions 3.3 and 4.5, a prime ideal $\mathfrak{p} \nmid (2)$ satisfies the bound $\delta_{K,\mathfrak{p}}(1) \geq 1 - (N_{K/\mathbb{Q}}(\mathfrak{p}))^{-1.5}$. Hence, letting $\zeta_{\mathbb{Q}(\xi_a)}$ be the Dedekind zeta function of $\mathbb{Q}(\xi_a)$, we have the lower bound

$$(6.31) \qquad t^+(a-1) \geq P_{\mathrm{Tam}}(K;1) = \prod_{\mathfrak{p}} \delta_{K,\mathfrak{p}}(1)$$

$$(6.32) \qquad \geq \frac{\left(1 - 2^{-\operatorname{ord}_a(2)}\right)^{\frac{a-1}{\operatorname{ord}_a(2)}}}{\left(1 - 2^{-1.5\operatorname{ord}_a(2)}\right)^{\frac{a-1}{\operatorname{ord}_a(2)}}} \frac{1}{\zeta_{\mathbb{Q}(\xi_a)}(1.5)}$$

$$(6.33) \qquad \geq \frac{\left(1 - 2^{-\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}}{\left(1 - 2^{-1.5\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}} \frac{1}{\zeta_{\mathbb{Q}(\xi_a)}(1.5)},$$

where the last inequality follows from $\operatorname{ord}_a(2) \geq \log_a(2)$. It now remains to show that as $a \to \infty$, (6.33) converges to 1.

First, it is straightforward that

$$(6.34) \quad 1 \geq \lim_{a\to\infty} \left(\frac{1 - 2^{-\log_2(a)}}{1 - 2^{-1.5\log_2(a)}}\right)^{\frac{a-1}{\log_2(a)}} = \lim_{a\to\infty} \frac{\left(1 - a^{-1}\right)^{\frac{a-1}{\log_2(a)}}}{\left(1 - a^{-1.5}\right)^{\frac{a-1}{\log_2(a)}}} = 1.$$

Next,

$$(6.35) \quad \log \zeta_{\mathbb{Q}(\zeta_a)}(1.5) = -\sum_{\mathfrak{p}} \log\left(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{1.5}\right) = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{1}{k N_{K/\mathbb{Q}}(\mathfrak{p})^{1.5k}}$$

$$(6.36) \qquad \leq \sum_{\mathfrak{p}} \frac{a-1}{N_{K/\mathbb{Q}}(\mathfrak{p})^{1.5}} + \sum_{\mathfrak{p}} \sum_{k=2}^{\infty} \frac{1}{k N_{K/\mathbb{Q}}(\mathfrak{p})^{1.5k}},$$

where the last inequality follows from at most $a-1$ primes having the same norm in $\mathbb{Q}(\zeta_a)$.

Now, taking the limit of each side,

$$(6.37) \qquad \limsup_{a\to\infty} \log \zeta_{\mathbb{Q}(\zeta_a)}(1.5) \leq \limsup_{a\to\infty} \sum_{\mathfrak{p}} \frac{a-1}{N_{K/\mathbb{Q}}(\mathfrak{p})^{1.5}}$$

Now, by Theorem 2.13 in [10], $N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \pmod{a}$ for all $\mathfrak{p}$ unless $\mathfrak{p}^{a-1} = (a)$. Therefore,

$$(6.38) \quad \limsup_{a\to\infty} \log \zeta_{\mathbb{Q}(\zeta_a)}(1.5) \leq \limsup_{a\to\infty} \sum_{\mathfrak{p}} \frac{a-1}{N_{K/\mathbb{Q}}(\mathfrak{p})^{1.5}}$$

$$(6.39) \qquad \leq \limsup_{a\to\infty} \frac{a-1}{a^{1.5}} + \limsup_{a\to\infty} \sum_{\mathfrak{p} \nmid (a)} \frac{a-1}{N_{K/\mathbb{Q}}(\mathfrak{p})^{1.5}}$$

$$(6.40) \qquad \leq \limsup_{a \to \infty} \sum_{k=1}^{\infty} \frac{a-1}{(ak)^{1.5}}$$

$$(6.41) \qquad \leq \limsup_{a \to \infty} \frac{a-1}{a^{1.5}} \frac{1}{1.5 - 1} = 0.$$

Thus,

$$(6.42) \qquad \limsup_{a \to \infty} \zeta_{\mathbb{Q}(\zeta_a)}(1.5) = 1.$$

Now, from (6.34), and (6.42), we have that

$$(6.43) \qquad \limsup_{a \to \infty} \frac{\left(1 - 2^{-\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}}{\left(1 - 2^{-1.5\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}} \frac{1}{\zeta_{\mathbb{Q}(\xi_a)}(1.5)} = 1.$$

Thus, by (6.33), it holds that $\limsup_{d \to +\infty} t^+(d) = 1$.

Next, we show that the same sequence of fields $K = \mathbb{Q}(\xi_a)$ satisfies $\liminf_{d \to +\infty} \mu^-(d) = 1$. By Propositions 3.3 and 4.5, for $\mathfrak{p} \nmid (2)$, we have that

$$(6.44) \qquad \sum_{m=1}^{\infty} \delta_{K,\mathfrak{p}}(m)m \leq 1 + 2N_{K/\mathbb{Q}}(\mathfrak{p})^{-1.95} \leq \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-1.5}}.$$

In addition, from Proposition 5.5, for $\mathfrak{p} \mid (2)$, we have that

$$(6.45) \qquad \sum_{m=1}^{\infty} \delta_{K,\mathfrak{p}}(m)m \leq 1 + 2N_{K/\mathbb{Q}}(\mathfrak{p})^{-0.95} \leq \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-1}}.$$

Thus, by (6.44) and (6.45),

$$(6.46) \qquad \mu^-(a-1) \leq \prod_{\mathfrak{p}} \sum_{m=1}^{\infty} \delta_{K,\mathfrak{p}}(m)m$$

$$(6.47) \qquad \leq \frac{\left(1 - 2^{-1.5\operatorname{ord}_a(2)}\right)^{\frac{a-1}{\operatorname{ord}_a(2)}}}{\left(1 - 2^{-\operatorname{ord}_a(2)}\right)^{\frac{a-1}{\log_2(a)}}} \zeta_{\mathbb{Q}(\xi_a)}(1.5)$$

$$(6.48) \qquad \leq \frac{\left(1 - 2^{-1.5\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}}{\left(1 - 2^{-\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}} \zeta_{\mathbb{Q}(\xi_a)}(1.5),$$

where the last inequality follows from the naive bound $\log_2(a) \leq \operatorname{ord}_a(2)$.

Now, by (6.43),

$$(6.49) \quad \limsup_{a \to \infty} \mu^-(a-1) \leq \limsup_{a \to \infty} \frac{\left(1 - 2^{-1.5\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}}{\left(1 - 2^{-\log_2(a)}\right)^{\frac{a-1}{\log_2(a)}}} \zeta_{\mathbb{Q}(\xi_a)}(1.5) = 1$$

as sought. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

7. Examples

In this section, we offer numerical examples that illustrate the results in this paper.

Example 7.1. There are finitely many imaginary quadratic fields of class number 1. As briefly discussed in the introduction, in Table 1.1, we calculated the following values for their proportion of Tamagawa trivial curves. Then Tables 7.1 and 7.2 shows the convergence of $P_{Tam}(\mathbb{Q}(\sqrt{-D}), 2)$ and $P_{Tam}(\mathbb{Q}(\sqrt{-D}), 3)$ respectively. Lastly, in Table 1.2 we have average Tamagawa product for each of the imaginary quadratic fields, as shown below.

TABLE 7.1. Convergence to $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), 2)$.

$\mathcal{N}_2(X, K)/\mathcal{N}(X, K)$								
X	$\sqrt{-1}$	$\sqrt{-2}$	$\sqrt{-3}$	$\sqrt{-7}$	$\sqrt{-11}$	$\sqrt{-19}$	$\sqrt{-43}$	$\sqrt{-67}$	$\sqrt{-163}$
10^4	0.353	0.351	0.248	0.354	0.255	0.278	0.260	0.284	0.283
10^5	0.360	0.387	0.253	0.369	0.277	0.231	0.220	0.218	0.207
10^6	0.377	0.382	0.266	0.382	0.298	0.256	0.228	0.211	0.215
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
∞	0.378	0.384	0.264	0.370	0.299	0.265	0.226	0.216	0.206

TABLE 7.2. Convergence to $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{-D}), 3)$.

$\mathcal{N}_3(X, K)/\mathcal{N}(X, K)$								
X	$\sqrt{-1}$	$\sqrt{-2}$	$\sqrt{-3}$	$\sqrt{-7}$	$\sqrt{-11}$	$\sqrt{-19}$	$\sqrt{-43}$	$\sqrt{-67}$	$\sqrt{-163}$
10^4	0.008	0.023	0.015	0.074	0.018	0.027	0.019	0.069	0.100
10^5	0.015	0.026	0.029	0.078	0.035	0.029	0.035	0.040	0.089
10^6	0.017	0.025	0.027	0.078	0.035	0.024	0.021	0.025	0.031
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
∞	0.018	0.026	0.032	0.082	0.038	0.028	0.024	0.024	0.024

Example 7.2. Figure 7.1 (resp. Figure 7.2) displays the spread of the proportion of Tamagawa trivial curves (resp. the average Tamagawa product) across square-free real quadratic fields $\mathbb{Q}(\sqrt{D})$ for $2 \leq D < 10^4$.

In Figure 7.1, one can see that $P_{\mathrm{Tam}}(\mathbb{Q}(\sqrt{D}), 1)$ does not have a normal distribution, nor does it resemble a skewed normal distribution. Instead,
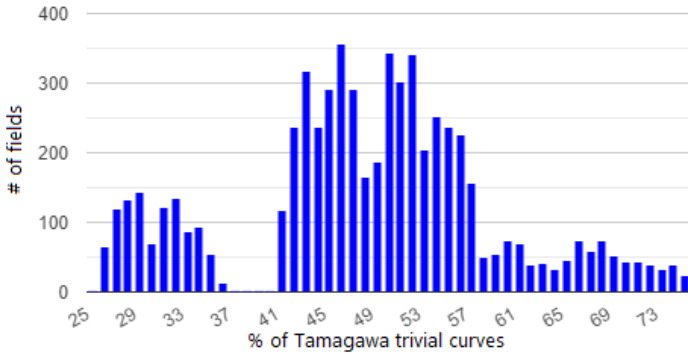
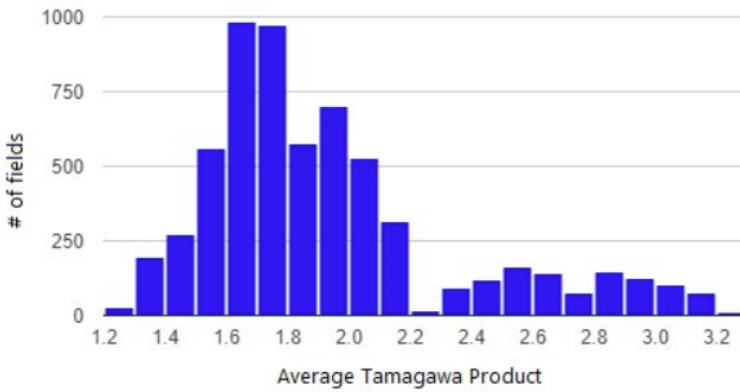FIGURE 7.1. Distribution of $P_{\mathrm{Tam}}(K, 1)$ for real quadratic number fields.

FIGURE 7.2. Distribution of $L_{\mathrm{Tam}}(K, -1)$ for real quadratic number fields.

there appear to be three distinct sections, from ≈ 0.26 to ≈ 0.36, from ≈ 0.41 to ≈ 0.57, and from ≈ 0.58 to ≈ 0.75. These three distinct regions correspond to how 2 behaves at any particular field. The left-most section corresponds to fields where 2 splits, the middle section corresponds to fields where 2 ramifies, and the right-most section corresponds to fields where 2 is inert. This leads us to many possible questions. Is the distribution uniform or random among each section? Are the proportions dense on any interval? How might these generalize over different degree fields? Are there always gaps between the sections? In Figure 7.2, we see that $L_{\mathrm{Tam}}(Q(\sqrt{D}), -1)$ also

does not have a normal distribution, but instead has two distinct sections. This leads to further questions, such as how do these sections relate to those for $P_{\text{Tam}}(Q(\sqrt{D}), 1)$?

Example 7.3. From Theorem 1.7 we have

$$\liminf_{d \to +\infty} t^-(d) = 0 \quad \text{and} \quad \limsup_{d \to +\infty} t^+(d) = 1,$$

and

$$\liminf_{d \to +\infty} \mu^-(d) = 1 \quad \text{and} \quad \limsup_{d \to +\infty} \mu^+(d) = \infty.$$

In Table 7.3, we have an example of a sequence of fields with the proportion of Tamagawa trivial curves decreasing to zero, and the corresponding average Tamagawa products heading off to infinity. The sequence follows the sequence of fields constructed in the proof of Theorem 1.7.

TABLE 7.3. The proportion of Tamagawa trivial curves in multiquadratic fields.

K	$\mathbb{Q}(\sqrt{17})$	$\mathbb{Q}(\sqrt{17}, \sqrt{41})$	$\mathbb{Q}(\sqrt{17}, \sqrt{41}, \sqrt{73})$	$\mathbb{Q}(\sqrt{17}, \sqrt{41}, \sqrt{73}, \sqrt{89})$
$P_{\text{Tam}}(K, 1)$	0.35585	0.13273	0.01778	0.00031
$L_{\text{Tam}}(K, -1)$	2.32335	5.14423	26.22779	686.87874

Similarly, in Figure 7.3, the sequence of fields $\mathbb{Q}(\zeta_p)$ for primes $p < 258$ excluding $p = 5, 7, 31$, and 127 have the proportion of Tamagawa trivial curves heading to 1.
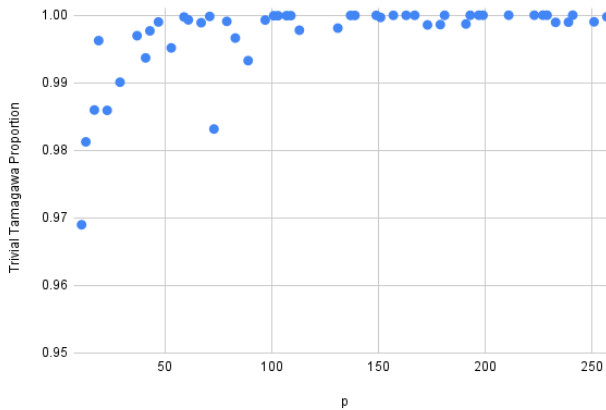

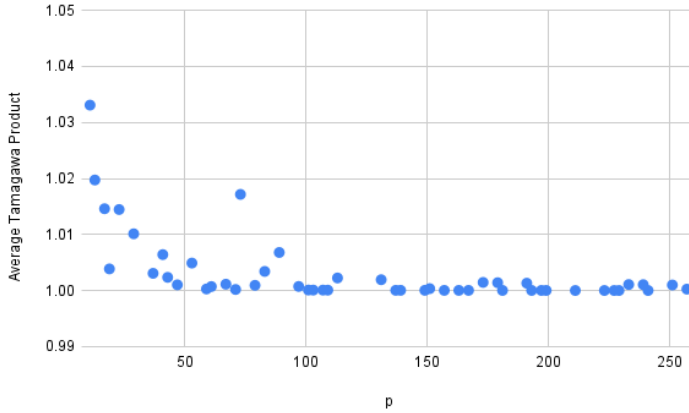FIGURE 7.3. $P_{\text{Tam}}(\mathbb{Q}(\zeta_p), 1)$ for primes $p < 258$ excluding $p = 5, 7, 31$, and 127.

FIGURE 7.4. $L_{\text{Tam}}(\mathbb{Q}(\zeta_p), -1)$ for primes $p < 258$ excluding $p = 5, 7, 31$, and 127.

In Figure 7.4, we see that for the same sequence of fields, the average Tamagawa products converge to 1. Note that as displayed in Table 7.4, the data points for $p = 5, 7, 31$, and 127 are outliers. For the latter three p, it is hinted in the proof of Theorem 1.7 that the reason is small $\text{ord}_p(2)$.

TABLE 7.4. Omitted values for $P_{\text{Tam}}(\mathbb{Q}(\zeta_p), 1)$ and $L_{\text{Tam}}(\mathbb{Q}(\zeta_p), -1)$

p	5	7	31	127
$P_{\text{Tam}}(\mathbb{Q}(\zeta_p), 1)$	$0.867\ldots$	$0.753\ldots$	$0.827\ldots$	$0.868\ldots$
$L_{\text{Tam}}(\mathbb{Q}(\zeta_p), -1)$	$1.155\ldots$	$1.309\ldots$	$1.205\ldots$	$1.151\ldots$

Example 7.4. Many of the above examples are of simpler fields, however in our paper we are able to calculate trivial Tamagawa proportions and average Tamagawa products for all fields, regardless of class number or degree. Thus, even for a more complicated field such as $\mathbb{Q}(x^4 + 5x^2 - 6x + 3)$ with Galois group S_4, we can even determine the trivial Tamagawa proportion. Note that $\mathbb{Q}(x^4 + 5x^2 - 6x + 3)$ has $\Delta = 32880$, and thus the primes $2, 3, 5$, and 137 all ramify. More specifically, we have that $2 = (-8\alpha^3 - \alpha^2 - 37\alpha + 47)^2$, $3 = (-\alpha)^2(2\alpha^3 + 9\alpha - 13)(\alpha - 1)$, $5 = (-\alpha^3 + \alpha - 1)(-2\alpha^2 + 2\alpha - 1)^2$, and $137 = (44\alpha^3 + 33\alpha^2 + 235\alpha - 100)(-\alpha^3 - 4\alpha^2 - 9\alpha - 17)^2$. By knowing how these primes ramify, we can calculate that $P_{\text{Tam}}(\mathbb{Q}(x^4 + 5x^2 - 6x + 3), 1) = 0.526\ldots$.

Appendix A. Classification of non-minimal models

In this section, we classify the non-minimal short Weierstrass models at prime ideals $\mathfrak{p} \mid (3)$ and $\mathfrak{p} \mid (2)$. These results generalize the work of Griffin et al. [5, Lemmas 2.2, 2.3], who classify the non-minimal short Weierstrass rational elliptic curves for primes $p = 2, 3$. The conditions for non-minimality can be written as a set of modular equations for bounded powers of π, which allows for a parametrization for the non-minimal curves. Since we are working with primes modulo powers of π, our results depend on the size of e.

Lemma A.1. *Let $\mathfrak{p} \subseteq K$ have ramification index e over (3). The curve $E(a_4, a_6)$ is not $\mathfrak{p}$-minimal if and only if some residues r $(\mathrm{mod}\ \pi^{\min\{2,e\}})$ and w $(\mathrm{mod}\ \pi^2)$ satisfy*

$$a_4 \equiv -3\pi^{\max\{0,4-2e\}}r^2 + \pi^4 w \pmod{\pi^6}$$

and

$$a_6 \equiv 2\pi^{\max\{0,6-3e\}}r^3 - \pi^{\max\{4,6-e\}}rw \pmod{\pi^6}.$$

Moreover, across a_4 modulo π^4 and a_6 modulo π^6 such that $E(a_4, a_6)$ is non-minimal, the choice of (r, w) from their respective residue classes is unique, i.e., there are exactly q^3 (resp. q^4) classes (a_4, a_6) $(\mathrm{mod}\ \pi^6)$ of non-minimal models for $e = 1$ (resp. $e \geq 2$).

Proof. Suppose that E/K is not $\mathfrak{p}$-minimal. Throughout Steps 1 to 10 of Tate's algorithm, we potentially translate (x, y) in the original curve to $(x + R, y + Vx + U)$. If the starting curve is non-minimal, we must reach Step 11, and the new coefficients a_i of the curve after Tate's algorithm must be divisible by π^i for $i = 1, 2, 3, 4, 6$. Translating this into equations, the restrictions on a_4, a_6, R, V, U are as follows:

$$(A.1) \qquad\qquad\qquad 2V \equiv 0 \pmod{\pi}$$

$$(A.2) \qquad\qquad\qquad 3R - V^2 \equiv 0 \pmod{\pi^2}$$

$$(A.3) \qquad\qquad\qquad 2U \equiv 0 \pmod{\pi^3}$$

$$(A.4) \qquad\qquad 3R^2 + a_4 - 2UV \equiv 0 \pmod{\pi^4}$$

$$(A.5) \qquad R^3 + a_4 R + a_6 - U^2 \equiv 0 \pmod{\pi^6}$$

Regardless of $\mathfrak{p}$, (A.1) and (A.3) imply that $V \equiv 0$ $(\mathrm{mod}\ \pi)$ and $U \equiv 0$ $(\mathrm{mod}\ \pi^3)$. As such, U and V vanish from the remaining equations.

From (A.2), we have that $R \equiv 0$ $(\mathrm{mod}\ \pi^{\max\{0,2-e\}})$. Therefore, suppose that $R = \pi^{\max\{0,2-e\}}r$ for some π-adic integer r. Then, from (A.4), we have $a_4 \equiv -3\pi^{\max\{0,4-2e\}}r^2$ $(\mathrm{mod}\ \pi^4)$. We therefore write $a_4 = -3\pi^{\max\{0,4-2e\}}r^2 + \pi^4 w$. Then, (A.5) is equivalent to $a_6 \equiv -R^3 - a_4 R \equiv 2\pi^{\max\{0,6-3e\}}r^3 - \pi^{\max\{4,6-e\}}rw$ $(\mathrm{mod}\ \pi^6)$.

To determine (a_4, a_6) up to $\pmod{\pi^6}$, r should be determined up to $\pmod{\pi^{\max\{3, e+1\}}}$ and w should be determined up to π^2. Yet, we contend, in order for the map between $(a_4, a_6) \pmod{\pi^6}$ and (r, w) to be bijective, the residues r and w must be selected modulo $\pi^{\min\{2, e\}}$ and modulo π^2, respectively. To show injectivity, we note that the resulting (a_4, a_6) $\pmod{\pi^6}$ from (r, w) and $(r + k\pi^{\min\{2, e\}}, w + \frac{6}{\pi^{\min\{2, e\}}} \alpha k + 3k^2)$ are equivalent. To show surjectivity, suppose that for some (r, w) and (r', w'), the resulting (a_4, a_6) are equivalent $\pmod{\pi^6}$, i.e.,

$$(A.6) \quad -3\pi^{\max\{0, 4-2e\}} r^2 + \pi^4 w \equiv -3\pi^{\max\{0, 4-2e\}} r'^2 + \pi^4 w' \pmod{\pi^6},$$

and

$$(A.7) \quad 2\pi^{\max\{0, 6-3e\}} r^3 - \pi^{\max\{4, 6-e\}} rw$$
$$\equiv 2\pi^{\max\{0, 6-3e\}} r'^3 - \pi^{\max\{4, 6-e\}} r'w' \pmod{\pi^6}.$$

From (A.7), $r \equiv r' \pmod{\pi^{\min\{2, e\}}}$. Then, from (A.6), $w \equiv w' \pmod{\pi^2}$ as we had sought. $\square$

Lemma A.2. *Let $\mathfrak{p}$ have ramification index e over (2). The curve $E(a_4, a_6)$ is not $\mathfrak{p}$-minimal if and only some residues $u \pmod{\pi^{\min\{3, e\}}}$, $v \pmod{\pi}$, and $w \pmod{\pi^2}$ satisfy*

$$a_4 \equiv 2\pi^{\max\{0, 3-e\}} uv - 3v^4 + \pi^4 w \pmod{\pi^6}$$

and

$$a_6 \equiv \pi^{\max\{0, 6-2e\}} u^2 - v^6 - a_4 v^2 \pmod{\pi^6}.$$

For each (a_4, a_6), the choice of (u, v, w) from their respective residue classes is unique, i.e., there exists exactly q^4 (resp. q^5 and q^6) classes (a_4, a_6) $\pmod{\pi^6}$ of non-minimal models for $e = 1$ (resp. $e = 2$ and $e \geq 3$).

Proof. Suppose that E is not $\mathfrak{p}$-minimal in K. Following the same steps as in the proof of Lemma A.1, we have (A.1), (A.2), (A.3), (A.4), (A.5) as restrictions on R, U, V and a_4, a_6. From here, we check that (R, U, V) and $(R + k\pi^2, U + k\pi^2 V, V)$ give rise to the same (a_4, a_6) modulo π^6. Hence, by choosing a suitable value of k, we assume $R = -V^2$.

To begin, (A.3) yields $U \equiv 0 \pmod{\pi^{\max\{0, 3-e\}}}$. Therefore, we suppose that $U = \pi^{\max\{0, 3-e\}} u$ for some π-adic integer u. From (A.4), we get $a_4 = 2\pi^{\max\{0, 3-e\}} uV - 3V^4$, whence we write $a_4 = (2\pi^{\max\{0, 3-e\}} uV - 3V^4) + \pi^4 w$ for some π-adic integer w. Finally, (A.5) gives $a_6 \equiv \pi^{\max\{0, 6-2e\}} u^2 - V^6 - V^2 a_4 \pmod{\pi^6}$.

By the analogous reasoning as in the proof of Lemma A.1, it can be shown that selecting u, v, w as representatives modulo $\pi^{\min\{3, e\}}$, π, and π^2 respectively forms a bijective map between u, v, w and (a_4, a_6) as we had sought. $\square$

References

[1] R. Ayoub, "Euler and the Zeta Function", *Am. Math. Mon.* **81** (1974), p. 1067-1086.

[2] J. S. Balakrishnan, W. Ho, N. Kaplan, S. Spicer, W. Stein & J. Weigandt, "Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks", *LMS J. Comput. Math.* **19A** (2016), p. 351-370.

[3] Y. Choi, S. Li, A. Panidapu & C. Siegel, "Tamagawa Products for Elliptic Curves Over Number Fields", `https://arxiv.org/abs/2108.13625v1`, 2021.

[4] J. E. Cremona & M. Sadek, "Local and global densities for Weierstrass models of elliptic curves", *Math. Res. Lett.* **30** (2020), no. 2, p. 413-461.

[5] M. Griffin, K. Ono & W.-L. Tsai, "Tamagawa products of elliptic curves over $\mathbb{Q}$", *Q. J. Math.* **72** (2021), no. 4, p. 1517-1543.

[6] B. Mazur & W. Stein, *Prime Numbers and the Riemann Hypothesis*, Cambridge University Press, 2016, xi+142 pages.

[7] K. Ono, "Personal communication", 2021.

[8] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 51, Springer, 1994.

[9] ———, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 2009, xx+513 pages.

[10] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Studies in Mathematics, vol. 83, Springer, 1996, xiv+487 pages.

Yunseo Choi
84 Brattle Street
Cambridge, MA, USA
E-mail: `ychoi@college.harvard.edu`

Sean Li
182 Memorial Drive
Cambridge, MA, USA
E-mail: `seanjli@mit.edu`

Apoorva Panidapu
458 Lagunita Drive
Stanford, CA, USA
E-mail: `panidapu@stanford.edu`

Casia Siegel
200 D. W. Brooks Drive
Athens, GA, USA
E-mail: `casia.Siegel@uga.edu`