Densities for Elliptic Curves over Global Function Fields
SPUR Final Paper, Summer 2022

Andrew Yao
Mentor: Hao Peng
Project Suggested By: Zhiyu Zhang

Abstract

Let K be a global function field. Using Haar measures, we compute the densities of the Kodiara types and Tamagawa numbers of elliptic curves over a completion of K. Also, we prove results about the number of iterations of Tate's algorithm that are completed when the algorithm is used on an elliptic curve over a completion of K.

1 Introduction

Let p be a prime and $q = p^n$ for a positive integer n. Let K be a finite extension of $\mathbb{F}_q(t)$. Define M_K as the set of places of K. Suppose $P \in M_K$. Let K_P be the completion of K at P and R_P be the valuation ring of K_P. Suppose E is an elliptic curve over K with equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

such that a_1, a_2, a_3, a_4, and a_6 are elements of K. E has a long Weierstrass form, and if $a_1 = a_2 = a_3 = 0$, E has a short Weierstrass form. We study densities for elliptic curves over K in long Weierstrass form.

As an elliptic curve over K_P, E has a Kodaira type, which describes its geometry. Particularly, E has a Tamagawa number $c_P = [E(K_P) : E_0(K_P)]$ over K_P. A method to determine the Kodaira type and Tamagawa number of an elliptic curve over K_P is Tate's algorithm ([6], [7]). The description of the algorithm in [6] is used in this paper to compute local densities. Often, steps from this description of the algorithm are referred to.

The papers [2] and [3] discuss densities of Kodaira types and Tamagawa products for elliptic curves over $\mathbb{Q}$. In these papers, the densities at the nonarchimedean places of $\mathbb{Q}$ are considered. In [2] and [3], the density is for elliptic curves in long and short Weierstrass forms, respectively. Moreover, [1] discusses densities of Kodaira types and Tamagawa products for elliptic curves over number fields in short Weierstrass form. Note that some of the methods for computing local densities with Tate's algorithm used in Section 4, Section 5, and Section 6 of this paper are similar to methods used in [1], [2], and [3].

Local densities over K_P can be obtained using the Haar measure. Let N be a positive integer. Note that K_P^N as an additive group is locally compact, and because of this, Haar's theorem can be used on K_P^N. Particularly, suppose μ_P is the Haar measure on K_P^N with $\mu_P(R_P^N) = 1$.

Let G_P be the set of curves $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ over K_P such that $a_1, a_2, a_3, a_4, a_6 \in R_P$. Because the discriminant of an elliptic curve must be nonzero, not all elements of G_P are elliptic curves. Also, note that G_P can be considered to be R_P^5. The local densities for G_P are obtained from the Haar measure on R_P^5.

Definition 1.1. For an elliptic curve $E \in G_P$, let $M_P(E)$ be the number of iterations of Tate's algorithm that are completed when the algorithm is used on E.

Suppose T is the set of Kodaira types. Let $\mathfrak{r}$ be an element of T and n be a positive integer. Define $\delta_K(\mathfrak{r}, n; P)$ to be the Haar measure of the set of elliptic curves E over K_P with coefficients in R_P such that E has Kodaira type $\mathfrak{r}$ and the Tamagawa number of E is n. For $k \geq 0$, define $\delta_K(\mathfrak{r}, n, k; P)$ to be the Haar measure of the set of elliptic curves E over K_P with coefficients in R_P such that E has Kodaira type $\mathfrak{r}$, the Tamagawa number of E is n, and $M_P(E) = k$.

In this paper, we often consider the number of iterations that Tate's algorithm completes when the algorithm is used on an elliptic curve over K_P. Note that in order to study this topic, Proposition 2.4 is useful. Next, we give an important result of the paper.

Theorem 1.2. For a Kodaira type $\mathfrak{r}$, positive integer n, and nonnegative integer k,

$$\delta_K(\mathfrak{r}, n, k; P) = \frac{1}{Q_P^{10k}} \delta_K(\mathfrak{r}, n, 0; P).$$

We prove Theorem 1.2 by considering the cases $p \geq 5$, $p = 3$, and $p = 2$. Note that the general method used to prove the theorem is to use translations. The proof of this result is given in Section 7.1.

Organization. The paper is organized as follows. In Section 2, we introduce elliptic curves and Tate's algorithm. Next, in Section 3, for a nonempty finite subset S of M_K and a positive integer N, we discuss how to obtain global densities for $\mathcal{O}_{K,S}^N$. Afterwards, in Section 4, Section 5, and Section 6, we compute the local densities if the characteristic p of K is at least 5, equal to 2, and equal to 3, respectively. Finally, in Section 7, we prove additional results about local and global densities.

Notation. Suppose P is a place of K. Let the degree of P be $[R_P/\pi_P R_P : \mathbb{F}_q]$. Also, let $Q_P = |R_P/\pi_P R_P|$. Let π_P be a uniformizer of P in K. Also, denote v_P to be the valuation v_{π_P} over K_P; note that v_P is also a valuation over K because $K \subset K_P$. Moreover for a nonnegative integer k, let $L_{P,k}$ be a set of representatives of the cosets of $R_P/\pi_P^k R_P$ such that $0 \in L_{P,k}$.

Suppose S is a finite nonempty subset of M_K. We let $\mathcal{O}_{K,S}$ be the set of $x \in K$ such that if $P \in S^C = M_K \backslash S$, $v_P(x) \geq 0$. Also, let W_S be the set of curves $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ such that $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_{K,S}$.

For $d \geq 1$, let T_d be the number of places of P with degree d. The zeta function of K is

$$\zeta_K(s) = \prod_{d=1}^{\infty} \left(1 - \frac{1}{q^{ds}}\right)^{-T_d}.$$

Suppose D is a divisor of K. Define $L(D)$ as the set of $x \in K$ such that $x = 0$ or $x \neq 0$ and $(x) + D \geq 0$.

Acknowledgements. This research was done in MIT SPUR. The author would like to thank Hao Peng for providing useful guidance. Also, the author would like to thank Zhiyu Zhang for suggesting the problem. Additionally, the author would like to thank David Jerison and Ankur Moitra for giving advice about the project.

2 Elliptic Curves and Global Densities

Suppose P is a place of K. An elliptic curve E over K_P has an equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

such that $a_1, a_2, a_3, a_4, a_6 \in K_P$. Additionally, using [6], for an elliptic curve E over K_P, define

$$b_2(E) = a_1^2 + 4a_2, b_4(E) = a_1a_3 + 2a_4, b_6(E) = a_3^2 + 4a_6,$$
$$b_8(E) = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Also, the discriminant of E is

$$\Delta(E) = -b_2(E)^2 b_8(E) - 8b_4(E)^3 - 27b_6(E)^2 + 9b_2(E)b_4(E)b_6(E).$$

Definition 2.1 ([7])**.** Elliptic curves E and F over K_P are *equivalent* if there exists $l, m, n, u \in K_P$ such that $u \neq 0$ and the equation for F can be obtained from the equation for E by first replacing x with $u^2x + n$ and y with $u^3y + lu^2x + m$ and then dividing by u^6.

Definition 2.2 ([7])**.** An elliptic curve E over K_P is *minimal* if the equation for E has coefficients in R_P and if there does not exist an elliptic curve F over K_P such that the equation for F has coefficients in R_P, F is equivalent to E, and $v_P(\Delta(F)) < v_P(\Delta(E))$.

The following proposition generalizes Theorem 3.2 of [7] to nonminimal equivalent elliptic curves. Note that the proposition is used later in the paper to compute local densities.

Proposition 2.3. Let E and F be elliptic curves over K_P that have equations with coefficients in R_P, are equivalent, and satisfy $v_P(\Delta(E)) = v_P(\Delta(F))$. Then, there exists $l, m, n, u \in R_P$ such that $v_P(u) = 0$ and the equation of F can be obtained from the equation of E by first replacing x with $u^2x + n$ and y with $u^3y + lu^2x + m$ and then dividing by u^6.

Proof. The proof of Theorem 3.2 of [7] can be used to prove this proposition. ∎

Proposition 2.4. Let k be a nonnegative integer. The elliptic curve E over K_P with coefficients in R_P has $M_P(E) \geq k$ if and only if $l, m, n \in R_P$ exist such that if x is replaced by $x + n$ and y is replaced by $y + lx + m$, the resulting elliptic curve

$$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

has $a_i' \equiv 0 \pmod{\pi_P^{ki}}$ for $i \in \{1, 2, 3, 4, 6\}$.

Proof. Suppose l, m, n exist. Then, $M_P(E) \geq k$ follows from replacing x with $x + n$ and y with $y + lx + m$ to get the curve $E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ such that for $i \in \{1, 2, 3, 4, 6\}$, π_P^{ik} divides a_i'. From Tate's algorithm, we have that $M_P(E) = M_P(E') \geq k$.

Next, we prove that if $M_P(E) \geq k$, l, m, and n exist using induction on k. The base case $k = 0$ is clear. Let a be a nonnegative integer and assume the result is true for $k = a$. We prove the result is true for $k = a + 1$. Assume $M_P(E) \geq a + 1$. Because $M_P(E) \geq a$, l, m, and n exist such that if x is replaced with $x + n$ and y is replaced with $y + lx + m$, the resulting curve $E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ has $a_i' \equiv 0 \pmod{\pi_P^{ia}}$ for $i \in \{1, 2, 3, 4, 6\}$. Using Tate's on E', E' after a iterations will be

$$F : y^2 + \frac{a_1'}{\pi_P^a}xy + \frac{a_3'}{\pi_P^{3a}}y = x^3 + \frac{a_2'}{\pi_P^{2a}}x^2 + \frac{a_4'}{\pi_P^{4a}}x + \frac{a_6'}{\pi_P^{6a}}.$$

We have that F is E with x replaced with $\pi_P^{2a}x + n$ and y replaced with $\pi_P^{3a}y + l\pi_P^{2a}x + m$ divided by π_P^{6a}.

Because $M_P(E') = M_P(E) \geq k + 1$, F will complete at least one more iteration. During this iteration, suppose x is replaced with $x + n'$ and y is replaced with $y + l'x + m'$. We have that the resulting elliptic curve

$$F' : y^2 + a_1''xy + a_3''y = x^3 + a_2''x^2 + a_4''x + a_6''$$

has $a_i'' \equiv 0 \pmod{\pi_P^i}$ for $i \in \{1, 2, 3, 4, 6\}$. Moreover, F' is E with x replaced with $\pi_P^{2a}x + n + \pi_P^{2a}n'$ and y replaced with $\pi_P^{3a}y + (l + l'\pi_P^a)\pi_P^{2a}x + m + m'\pi_P^{3a} + ln'\pi_P^{2a}$ divided by π_P^{6a}. Because $a_i'' \equiv 0 \pmod{\pi_P^i}$ for $i \in \{1, 2, 3, 4, 6\}$, we are done. ∎

Note that Tate's algorithm cannot be used on a curve in G_P with discriminant 0. However, this is not considered in the calculations of local densities later in the paper. Suppose $\mathfrak{r} \in T$, n is a positive integer, and k is a nonnegative integer. The set U of elliptic curves $E \in G_P$ with Kodaira type $\mathfrak{r}$, Tamagawa number n, and $M(E) = k$ is an open subset of G_P, because if $E \in U$, if multiples of π_P^M are added to the coefficients of E for sufficiently positive large integers M, the resulting curve will be an element of U. Particularly, the set of elliptic curves is an open subset of G_P. In the next proposition, we prove that the Haar measure of this set is 1; note that it follows that the Haar measure of the set of curves in G_P with discriminant 0 is 0.

Proposition 2.5. The Haar measure of the set of elliptic curves is 1.

Proof. For a positive integer M, let E_M be the set of subsets of G_P of the form $(r_i + \pi_P^M)^5$ for $r_i \in L_{P,M}$ that are contained in the set of elliptic curves. For $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we see that the number of solutions to $\Delta(E) \equiv 0 \pmod{\pi_P^M}$ is $O(Q_P^{4M})$. Therefore, we have that $|E_M| = Q_P^{5M} - O(Q_P^{4M})$. However, the Haar measure of the union of the elements of E_M is $\frac{|E_M|}{Q_P^{5M}} = 1 - O\left(\frac{1}{Q_P^M}\right)$. The result follows from taking $M \to \infty$. ∎

3 Global Densities

Next, global densities are established. Definitions and theorems from [4] are used in this section.

Let S be a finite nonempty subset of M_K. Also, suppose N is a positive integer. Let $\mathrm{Div}(S)$ be the set of divisors

$$\sum_{P \in S} n_P P$$

such that for $P \in S$, n_P is a nonnegative integer, and there exists $P \in S$ such that $n_P > 0$. Suppose $U \subset \mathcal{O}_{K,S}^N$. The upper density of U at S is

$$\overline{d}_S(U) = \limsup_{D \in \mathrm{Div}(S)} \frac{|U \cap L(D)^N|}{|L(D)|^N},$$

and the lower density of U at S is

$$\underline{d}_S(U) = \liminf_{D \in \mathrm{Div}(S)} \frac{|U \cap L(D)^N|}{|L(D)|^N}.$$

If $\overline{d}_S(U) = \underline{d}_S(U)$, the density $d_S(U)$ of U at S exists, and equals $\overline{d}_S(U) = \underline{d}_S(U)$.

Theorem 3.1 ([4], Theorem 2.1)**.** For $P \in S^C$, let $U_P \subset K_P^N$ be a measurable set such that $\mu_P(\partial U_P) = 0$. For a positive integer M, let V_M be the set of $x \in \mathcal{O}_{K,S}^N$ such that $x \in U_P$ for some $P \in S^C$ with degree at least M. Suppose $\lim_{M\to\infty} \overline{d}_S(V_M) = 0$. Let $\mathcal{P} : \mathcal{O}_{K,S}^N \to 2^{S^C}, \mathcal{P}(a) = \{P \in S^C : a \in U_P\}$. Then:

1. $\sum_{P \in S^C} \mu_P(U_P)$ is convergent.
2. For $T \subset 2^{S^C}$, $\nu(T) := d_S(\mathcal{P}^{-1}(T))$ exists. Also, ν defines a measure on 2^{S^C}.
3. ν is concentrated at finite subsets of S^C, and for a finite set T of places in S^C,

$$\nu(\{T\}) = \prod_{P \in T} \mu_P(U_P) \prod_{P \in S^C \setminus T} (1 - \mu_P(U_P)).$$

Theorem 3.2 ([4], Theorem 2.2)**.** Let f and g be polynomials in $\mathcal{O}_{K,S}[x_1, \ldots, x_d]$ that are relatively prime. For $M \geq 1$, let V_M be the set of $x \in \mathcal{O}_{K,S}^N$ such that $f(x) \equiv g(x) \equiv 0 \pmod{\pi_P}$ for some $P \in S^C$ with degree at least M. Then, $\lim_{M\to\infty} \overline{d}_S(V_M) = 0$.

In this paper, we consider global densities for elliptic curves over K with coefficients in $\mathcal{O}_{K,S}$ in long Weierstrass form. We see that W_S can be considered to be $\mathcal{O}_{K,S}^5$, and particularly, the global density definitions from above for $\mathcal{O}_{K,S}^5$ can be used on W_S. Similar methods are used in [2] for elliptic curves over $\mathbb{Q}$ with coefficients in $\mathbb{Z}$. Note that an elliptic curve must have a nonzero discriminant, meaning that not all curves in W_S are elliptic curves. However, for $D \in \mathrm{Div}(S)$, the number of curves in W_S with discriminant 0 that are elements of $L(D)^5$, where W_S is considered to be $\mathcal{O}_{K,S}^5$, is $O(|L(D)|^4)$. Particularly, if proportions over elliptic curves in W_S is considered rather than the proportions over W_S, the density is not changed.

Proposition 3.3 is about the global density of nonminimal elliptic curves. Note that the lemma is used to prove Theorem 7.2.

Proposition 3.3. For a positive integer M, let V_M be the set of elliptic curves $E \in W_S$ such that there exists $P \in S^C$ with degree at least M such that $M_P(E) \geq 1$. Then, $\lim_{M\to\infty} \overline{d}_S(V_M) = 0$.

Proof. We prove this with casework on the characteristic p of K. Suppose that E is an elliptic curve in G_P with equation $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ for $a_1, a_2, a_3, a_4, a_6 \in R_P$ such that $M_P(E) \geq 1$.

Assume $p \geq 5$. We have that E can be translated to the curve

$$y^2 = x^3 + \left(-\frac{b_2^2}{48} + \frac{b_4}{2}\right) x - \frac{b_2^3}{864} - \frac{b_2b_4}{24} + \frac{b_6}{4}.$$

Because $M_P(E) \geq 1$, using Proposition 2.4, $-\frac{b_2^2}{48} + \frac{b_4}{2} \equiv 0 \pmod{\pi_P}$ and $-\frac{b_2^3}{864} - \frac{b_2b_4}{24} + \frac{b_6}{4} \equiv 0 \pmod{\pi_P}$. Then, Theorem 3.2 with $f(x_1, x_2, x_3, x_4, x_6) = -\frac{(x_1^2+4x_2)^2}{48} + \frac{x_1x_3+2x_4}{2}$ and $g(x_1, x_2, x_3, x_4, x_6) = -\frac{(x_1^2+4x_2)^3}{864} - \frac{(x_1^2+4x_2)(x_1x_3+2x_4)}{24} + \frac{x_3^2+4x_6}{4}$ proves the lemma for $p \geq 5$.

Next, assume $p = 3$. We have that E can be translated to the curve

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

Using Proposition 2.4, $\frac{b_2}{4} \equiv 0 \pmod{\pi_P}$ from the coefficient of x^2. Additionally, $\Delta(E) \equiv 0 \pmod{\pi_P}$. Next, Theorem 3.2 with $f(x_1, x_2, x_3, x_4, x_6) = -(x_1^2+x_2)^2(x_1^2x_6+x_2x_6-x_1x_3x_4+x_2x_3^2 - x_4^2) + (x_1x_3 + 2x_4)^3$ and $g(x_1, x_2, x_3, x_4, x_6) = x_1^2 + x_2$ proves the lemma for $p = 3$.

Suppose $p = 2$. Using Proposition 2.4, $a_1 \equiv 0 \pmod{\pi_P}$ from the coefficient of xy. Also, $\Delta(E) \equiv 0 \pmod{\pi_P}$. Therefore, Theorem 3.2 with $f(x_1, x_2, x_3, x_4, x_6) = x_1^4(x_1^2x_6+x_1x_3x_4+x_2x_3^2 + x_4^2) + x_3^4 + x_1^3x_3^3$ and $g(x_1, x_2, x_3, x_4, x_6) = x_1$ proves the lemma for $p = 2$. ■

4 Local Densities for $p \geq 5$

4.1 Setup

Suppose that the characteristic of K is $p \geq 5$. Let P be a place of K. We compute the local densities over K_P of Kodaira types $\mathfrak{r}$ and Tamagawa numbers n for elliptic curves in G_P. Let $G_P^{(1)}$ be the set of curves

$$y^2 = x^3 + a_4x + a_6$$

over K_P such that $a_4, a_6 \in R_P$. Note that $G_P^{(1)}$ can be considered to be R_P^2. Define $\varphi : G_P \to G_P^{(1)}$ as the function such that if E is the curve in G_P with equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $\varphi(E)$ is the curve

$$\varphi(E) : y^2 = x^3 + \left(-\frac{b_2^2}{48} + \frac{b_4}{2}\right) x - \frac{b_2^3}{864} - \frac{b_2b_4}{24} + \frac{b_6}{4}.$$

If E is an elliptic curve, $\varphi(E)$ is an elliptic curve equivalent to E.

Lemma 4.1. If U is an open subset of $G_P^{(1)}$, $\mu_P(\varphi^{-1}(U)) = \mu_P(U)$.

Proof. Let V be the set of $y^2 = x^3 + a_4'x + a_6'$ with $a_4' \in r_4 + \pi_P^{n_4} R_P$ and $a_6' \in r_6 + \pi_P^{n_6} R_P$. It suffices to prove that $\mu_P(\varphi^{-1}(V)) = \mu_P(V) = \frac{1}{Q^{n_4+n_6}}$ because all open subsets of $G_P^{(1)}$ can be written as a disjoint countable union of sets with the form of V. We want to find the set of $a_1, a_2, a_3, a_4, a_6 \in R_P$ such that $-\frac{b_2^2}{48} + \frac{b_4}{2} \in r_4 + \pi_P^{n_4} R_P$ and $-\frac{b_2^3}{864} - \frac{b_2 b_4}{24} + \frac{b_6}{4} \in r_6 + \pi_P^{n_6} R_P$. Let $M = \max(n_4, n_6)$. First, select a_1, a_2, a_3 modulo π_P^M. Each has Q_P^M possible residues. Afterwards, a_4 will have $Q_P^{M-n_4}$ residues modulo π_P^M; select the residue for a_4. Finally, a_6 has $Q_P^{M-n_6}$ residues modulo π_P^M. We see that if each of a_1, a_2, a_3, a_4, a_6 are taken modulo π_P^M, the number of combinations of residues is $Q_P^{5M-n_4-n_6}$. Also, because a_i is modulo π_P^M for $i \in \{1, 2, 3, 4, 6\}$, each combination of residues has a Haar measure of $\frac{1}{Q_P^{5M}}$. We are done. ■

4.2 Multiple Iterations

Let k be a nonnegative integer. Suppose S_k is the set of elliptic curves $E \in G_P^{(1)}$ such that $M_P(E) \geq k$.

Suppose E is an elliptic curve in $G_P^{(1)}$ with equation $E : y^2 = x^3 + a_4 x + a_6$. Assume $E \in S_k$. Then, using Proposition 2.4, $l, m, n \in R_P$ exist such that

$$\left(y + \frac{l}{\pi_P^k} x + \frac{m}{\pi_P^{3k}}\right)^2 - \left(x + \frac{n}{\pi_P^{2k}}\right)^3 - \frac{a_4}{\pi_P^{4k}}\left(x + \frac{n}{\pi_P^{2k}}\right) - \frac{a_6}{\pi_P^{6k}} \in R_P[x, y].$$

The coefficient of xy is $\frac{2l}{\pi_P^k}$, giving that $v_P(l) \geq k$, and the coefficient of y is $\frac{2m}{\pi_P^{3k}}$, giving that $v_P(m) \geq 3k$. Also, the coefficient of x^2 is $\frac{3n - l^2}{\pi_P^{2k}}$, giving that $v_P(n) \geq 2k$. From this, we have that $v_P(a_4) \geq 4k$ and $v_P(a_6) \geq 6k$.

Define the function $\phi_k : S_k \to S_0$, $y^2 = x^3 + a_4 x + a_6 \mapsto y^2 = x^3 + \frac{a_4}{\pi_P^{4k}} x + \frac{a_6}{\pi_P^{6k}}$. Note that $S_k \subset S_0 \subset G_P^{(1)}$. From Proposition 2.5 and Lemma 4.1, $\mu_P(S_0) = 1$. Next, we show how we can use ϕ_k to compute densities for S_k.

Lemma 4.2. If U is an open subset of $G_P^{(1)}$, $\mu_P(\phi_k^{-1}(U)) = \frac{1}{Q_P^{10k}} \mu_P(U)$.

Proof. Let V be the set of $y^2 = x^3 + a_4'x + a_6'$ with $a_4' \in r_4 + \pi_P^{n_4} R_P$ and $a_6' \in r_6 + \pi_P^{n_6} R_P$. To prove the lemma, it suffices to prove that $\mu_P(\phi_k^{-1}(V)) = \mu_P(V) = \frac{1}{Q^{n_4+n_6+10}}$. We want to find a_4, a_6 such that $\frac{a_4}{\pi_P^{4k}} \in r_4 + \pi_P^{n_4} R_P$ and $\frac{a_6}{\pi_P^{6k}} \in r_6 + \pi_P^{n_6} R_P$. However, this is true if and only if $a_4 \in \pi_P^{4k} r_4 + \pi_P^{n_4+4k} R$ and $a_6 \in \pi_P^{6k} r_6 + \pi_P^{n_6+6k} R$. Moreover, because $\mu_P(S_0) = 1$, the density of curves $y^2 = x^3 + a_4 x + a_6$ with discriminant 0 such that $a_4 \in \pi_P^{4k} r_4 + \pi_P^{n_4+4k}$ and $a_6 \in \pi_P^{6k} r_6 + \pi_P^{n_6+6k}$ is 0. Because of this, $\mu_P(\phi_k^{-1}(V)) = \frac{1}{Q_P^{n_4+n_6+10}}$, completing the proof. ■

4.3 Density Calculations

Given a set A, the density of A means the Haar measure of A. In this subsection, we compute the density of the set of minimal elliptic curves with a given Kodaira type and Tamagawa number over $G_P^{(1)}$. From Lemma 4.2, the densities can be extended to all elliptic curves in $G_P^{(1)}$. Moreover, from Lemma 4.1, the densities of a given Koidara type and Tamagawa number over $G_P^{(1)}$ and over G_P are equal.

Suppose the discriminant is not divisible by π_P. We compute the density of this by considering a_4 and a_6 modulo π_P. Suppose $a_4 \in r_4 + \pi_P R_P$ and $a_6 \in r_6 + \pi_P R_P$. We find the number of pairs (r_4, r_6) in $L_{P,1}$ such that $\left(\frac{r_4}{3}\right)^3 + \left(\frac{r_6}{2}\right)^2 \equiv 0 \pmod{\pi_P}$. If $r_4 = 0$, r_6 has

1 choice, and if $-\frac{r_4}{3}$ is a square modulo π_P, r_6 has 2 choices. Otherwise, r_6 has 0 choices. We see that the number of pairs (r_4, r_6) is Q_P. Therefore, where each pair (r_4, r_6) has a density of $\frac{1}{Q_P^2}$, the density of the discriminant not being divisible by π_P is $\frac{Q_P-1}{Q_P}$. For this case, Tate's algorithm ends in step 1 and we get that $\delta_K(I_0, 1, 0; P) = \frac{Q_P-1}{Q_P}$.

Next, assume the discriminant is divisible by π_P. Furthermore, suppose $a_4, a_6 \not\equiv 0 \pmod{\pi_P}$. Because there are $Q_P - 1$ pairs (r_4, r_6) modulo π_P for this case, the total density is $\frac{Q_P-1}{Q_P^2}$. Let α be the element of $L_{P,1}$ such that $a_4 \equiv -3\alpha^2 \pmod{\pi_P}$ and $a_6 \equiv 2\alpha^3 \pmod{\pi_P}$. The singular point is $(\alpha, 0)$ and in step 2, x is replaced with $x+n$ where $n = \alpha$. Because $\alpha \not\equiv 0 \pmod{\pi_P}$, Tate's algorithm ends in step 2. The quadratic considered in step 2 is $T^2 - 3\alpha$. We see that for $\frac{Q_P-1}{2}$ values of α, this quadratic has roots in $R_P/\pi_P R_P$ and $c = v_P(\Delta(E))$. Otherwise, $c = 1$ if $v_P(\Delta(E))$ is odd and $c = 2$ if $v_P(\Delta(E))$ is even.

Let N be a positive integer. Suppose $a_4 \in r_4 + \pi_P^N R_P$ and $a_6 \in r_6 + \pi_P^N R_P$. We find the number of pairs (r_4, r_6) in $L_{P,1}$ such that $\left(\frac{r_4}{3}\right)^3 + \left(\frac{r_6}{2}\right)^2 \equiv 0 \pmod{\pi_P^N}$ and $r_4, r_6 \neq 0$. Because there are $\frac{Q_P^N - Q_P^{N-1}}{2}$ nonzero residues that are squares modulo π_P^M, we have that the number of pairs (r_4, r_6) is $Q_P^N - Q_P^{N-1}$. Therefore, the density of $v_P(\Delta(E)) \geq N$ for $a_4, a_6 \not\equiv 0 \pmod{\pi_P}$ is $\frac{Q_P-1}{Q_P^{N+1}}$.

Suppose N is a positive integer. The density of $v_P(\Delta(E)) = N$ is $\frac{Q_P-1}{Q_P^{N+1}} - \frac{Q_P-1}{Q_P^{N+2}} = \frac{(Q_P-1)^2}{Q_P^{N+2}}$.

We therefore have that $\delta_K(I_1, 1, 0; P) = \frac{(Q_P-1)^2}{Q_P^3}$, $\delta_K(I_2, 2, 0; P) = \frac{(Q_P-1)^2}{Q_P^4}$, and $\delta_K(I_N, N, 0; P) = \delta_K(I_N, 2\left\lfloor \frac{N}{2} \right\rfloor - N + 2, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+2}}$ for $N \geq 3$. Moreover, we have that $c = 1$ with density

$$\frac{(Q_P-1)^2}{Q_P^3} + \sum_{l=1}^{\infty} \frac{(Q_P-1)^2}{2Q_P^{2l+3}} = \frac{(Q_P-1)(2Q_P^2-1)}{2Q_P^3(Q_P+1)}$$

and similarly, $c = 2$ with density $\frac{(Q_P-1)(2Q_P^2-1)}{2Q_P^4(Q_P+1)}$. For $N \geq 3$, $c = N$ with density $\frac{(Q_P-1)^2}{2Q_P^{N+2}}$.

If $v_P(a_4), v_P(a_6) \geq 1$, the singular point is $(0, 0)$. The total density for this case is $\frac{1}{Q_P^2}$. If $v_P(a_6) = 1$, the algorithm ends in step 3. For this, we get $\delta_K(II, 1, 0; P) = \frac{Q_P-1}{Q_P^3}$.

Assume that $v_P(a_6) \geq 2$. The total density for this is $\frac{1}{Q_P^3}$. If $v_P(a_4) = 1$, the algorithm ends in step 4, and we get that $\delta_K(III, 2, 0; P) = \frac{Q_P-1}{Q_P^4}$.

Next, suppose $v_P(a_4) \geq 2$. The total density for this case is $\frac{1}{Q_P^4}$. If $v_P(a_6) = 2$, the algorithm ends in step 5. We have that from this, $\delta_K(IV, 1, 0; P) = \delta_K(IV, 3, 0; P) = \frac{Q_P-1}{2Q_P^5}$.

Suppose $v_P(a_6) \geq 3$. The total density for this case is $\frac{1}{Q_P^5}$. In step 6, the polynomial $P(T) \in (R_P/\pi_P R_P)[T]$ has coefficient of T^2 equal to 0. From adding multiples of π_P^2 to a_4, the choices for the coefficient of T are $L_{P,1}$. Also, from adding multiples of π_P^3 to a_6, the choices for the constant term are $L_{P,1}$. Then, we have that each polynomial $P(T) \in (R_P/\pi_P R_P)[T]$ with coefficient of T^2 equal to 0 corresponds to a density of $\frac{1}{Q_P^7}$ in $G_P^{(1)}$.

Assume $P(T)$ has distinct roots. The total number of $P(T)$ for this case is $Q_P^2 - Q_P$; therefore, the total density for this case is $\frac{Q_P-1}{Q_P^6}$. We have that Tate's algorithm ends in step 6 here. The number of $P(T)$ with 0, 1, and 3 roots in $R_P/\pi_P R_P$ are $\frac{Q_P^2-1}{3}$, $\frac{Q_P^2-Q_P}{2}$, and $\frac{Q_P^2-3Q_P+2}{6}$, respectively. With this, $\delta_K(I_0^*, 1, 0; P) = \frac{Q_P^2-1}{3Q_P^7}$, $\delta_K(I_0^*, 2, 0; P) = \frac{Q_P-1}{2Q_P^6}$, and $\delta_K(I_0^*, 4, 0; P) = \frac{Q_P^2-3Q_P+2}{6Q_P^7}$.

Next, assume that $P(T)$ has a double root and a simple root. For this case, the total number of $P(T)$ is $Q_P - 1$ and the total density is therefore $\frac{Q_P-1}{Q_P^7}$. Suppose N is a positive integer. We have that $\delta_K(I_N^*, 2, 0; P) = \delta_K(I_N^*, 4, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+7}}$. Moreover, $c = 2$ and $c = 4$ both have density $\frac{Q_P-1}{2Q_P^7}$. More details about computing local densities for the subprocedure are included in Section 4.4.

Assume $P(T)$ has a triple root. For this case, the total number of $P(T)$ is 1 and the total density is therefore $\frac{1}{Q_P^7}$. Because the coefficient of T^2 in $P(T)$ is 0, the triple root is 0. If $v_P(a_6) = 4$, the algorithm ends in step 8. For this, $\delta_K(IV^*, 1, 0; P) = \delta_K(IV^*, 3, 0; P) = \frac{Q_P-1}{2Q_P^8}$.

Next, assume that $v_P(a_6) \geq 5$. The total density for this case is $\frac{1}{Q_P^8}$. If $v_P(a_4) = 3$, the algorithm ends in step 9 and $\delta_K(III^*, 2, 0; P) = \frac{Q_P-1}{Q_P^9}$.

Suppose $v_P(a_4) \geq 4$. The total density for this case is $\frac{1}{Q_P^9}$. If $v_P(a_6) = 5$, the algorithm ends in step 10 and $\delta_K(II^*, 1, 0; P) = \frac{Q_P-1}{Q_P^{10}}$.

With density $\frac{1}{Q_P^{10}}$, we have that $v_P(a_4) \geq 4$ and $v_P(a_6) \geq 6$, meaning that the curve is not minimal. That is, the curve will complete iteration 1 and continue iteration 2. Note that the density of nonminimal curves calculated from the algorithm matches Lemma 4.2.

4.4 Subprocedure Density Calculations

We compute the subprocedure densities by studying the translation of x in Tate's algorithm. In the step 7 subprocedure, because initially the coefficient of y is 0, there will be no translations of y.

Let X be the set of elliptic curves $E \in G_P^{(1)}$ such that $M_P(E) = 0$ and Tate's algorithm enters the step 7 subprocedure when used on E. For $E \in X$, let $L(E)$ be the number of iterations of the step 7 subprocedure that are completed when Tate's algorithm is used on E. For a nonnegative integer N, let X_N be the set of $E \in X$ such that $L(E) \geq N$.

Suppose $N \geq 0$ is even. Iteration N of the step 7 subprocedure is completed if and only if $n \in R_P$ exists such that $v_P(n) = 1$, $v_P(a_4 + 3n^2) \geq \frac{N+6}{2}$, and $v_P(n^3 + 3na_4 + a_6) \geq N + 4$. Suppose $n = n_1$ satisfies this condition. Suppose $n = n_2$ also satisfies this condition. We then have that $n_1^2 \equiv n_2^2 \pmod{\pi_P^{\frac{N+6}{2}}}$. This gives that n_1 is equivalent to n_2 or $-n_2$ modulo $\pi_P^{\frac{N+4}{2}}$. However, because $n_1^3 + n_1 a_4 \equiv n_2^3 + n_2 a_4 \pmod{\pi_P^{N+4}}$, we have that $v_P(n_1 - n_2) \geq \frac{N+4}{2}$. Moreover, if $v_P(n_1 - n_2) \geq \frac{N+4}{2}$, $n = n_2$ works also.

Next, suppose $N \geq 0$ is odd. Iteration N of the subprocedure is completed if and only if $n \in R_P$ exists such that $v_P(n) = 1$, $v_P(a_4 + 3n_1^2) \geq \frac{N+5}{2}$, and $v_P(n^3 + na_4 + a_6) \geq N + 4$. Similarly, we have that if $n = n_1$ works, $n = n_2$ works if and only if $v_P(n_1 - n_2) \geq \frac{N+3}{2}$.

Suppose $N \geq 0$. Suppose n is an element of $L_{P,\lfloor \frac{N+4}{2} \rfloor}$ such that $v_P(n) = 1$. Let $Y_{n,N}$ be the set of curves $x^3 + 3nx^2 + a_4'x + a_6'$ such that $v_P(a_4') \geq \lfloor \frac{N+6}{2} \rfloor$ and $v_P(a_6') \geq N + 4$. Note that $Y_{n,N}$ can be considered to be an open subset of R_P^2.

For $E \in X_N$, let $n(E)$ be the unique value of $n \in L_{P,\lfloor \frac{N+4}{2} \rfloor}$ such that $v_P(n) = 1$, $v_P(a_4 + 3n^2) \geq \lfloor \frac{N+6}{2} \rfloor$, and $v_P(n^3 + na_4 + a_6) \geq N + 4$. Let θ_N be the function such that if $E : y^2 = x^3 + a_4 x + a_6$ is an element of X_N, $\theta_N(E) = (x + n(E))^3 + a_4(x + n(E)) + a_6$.

Lemma 4.3. Suppose N is a nonnegative integer and n is an element of $L_{P,\lfloor \frac{N+4}{2} \rfloor}$. If U is an open subset of $Y_{n,N}$, $\mu_P(\theta_N^{-1}(U)) = \mu_P(U)$.

Proof. Let $V \subset Y_{n,N}$ be the set of $E' : y^2 = x^3 + 3nx^2 + a_4'x + a_6'$ such that $a_4' \in r_4 + \pi_P^{n_4} R_P$ and $a_6' \in r_6 + \pi_P^{n_6} R_P$. Note that we have that $v_P(r_4), n_4 \geq \lfloor \frac{N+4}{2} \rfloor$ and $v_P(r_6), n_6 \geq N + 4$. It suffices to prove that $\mu_P(\theta_N^{-1}(V)) = \mu_P(V)$. Let $M = \max(n_4, n_6)$. Suppose $E : y^2 = x^3 + a_4 x + a_6$ is an elliptic curve. We have that $\theta_N(E) \in V$ if and only if

$$a_4 + 3n^2 \in r_4 + \pi_P^{n_4} R_P, na_4 + a_6 + n^3 \in \pi_P^{n_6} R_P.$$

Modulo π_P^M, there are $Q_P^{M-n_4}$ choices for the residue of a_4. After choosing a_4 modulo π_P^M, there are $Q_P^{M-n_6}$ choices for the residue of a_6 modulo π_P^M. Each of these combinations of residues modulo π_P^M for a_4 and a_6 has a density of $\frac{1}{Q_P^{2M}}$ in $G_P^{(1)}$. Note that the set of curves in $G_P^{(1)}$ with discriminant 0 is counted in these combinations, but the Haar measure of this set is 0. The Haar measure of the $Q_P^{2M-n_4-n_6}$ combinations is $\frac{1}{Q_P^{n_4+n_6}}$, which is $\mu_P(V)$. ■

Let N be a positive integer. We compute the density of I_N^*. Let n be an element of $L_{P,\lfloor \frac{N+3}{2} \rfloor}$ such that $v_P(n) = 1$. We have that the Haar measure of the set of $E \in Y_{n,N-1}$ that do not complete iteration N is $\frac{Q_P-1}{Q_P^{\lfloor \frac{N+5}{2} \rfloor + N+4}}$. With Lemma 4.3, because there are $(Q_P-1)Q_P^{\lfloor \frac{N-1}{2} \rfloor}$ values of n, the density of I_N^* is $\frac{(Q_P-1)^2}{Q_P^{N+7}}$. From adding multiples of π_P^{N+4} to a_6, $c=2$ and $c=4$ have equal density. Therefore,

$$\delta_K(I_N^*, 2, 0; P) = \delta_K(I_N^*, 4, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+7}}.$$

5 Local Densities for $p = 3$

5.1 Setup

Suppose that the characteristic of K is $p = 3$. Let P be a place of K and $G_P^{(2)}$ be the set of curves

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

over K_P such that $a_2, a_4, a_6 \in R_P$. Note that $G_P^{(2)}$ can be considered to be R_P^3. For a curve E in G_P with equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, let $\varphi(E)$ be the curve with equation

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}.$$

If E is an elliptic curve, $\varphi(E)$ is an elliptic curve equivalent to E.

Lemma 5.1. If U is an open subset of $G_P^{(2)}$, $\mu_P(\varphi^{-1}(U)) = \mu_P(U)$.

Proof. This can be proved similarly as Lemma 4.1. ■

5.2 Multiple Iterations

Let k be a nonnegative integer. Suppose S_k is the set of elliptic curves $E \in G_P^{(2)}$ such that $M_P(E) \geq k$.

Suppose $E \in S_k$ has equation $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$. From Proposition 2.4, $l, m, n \in R_P$ exist such that

$$\left(y + \frac{l}{\pi_P^k}x + \frac{m}{\pi_P^{3k}}\right)^2 = \left(x + \frac{n}{\pi_P^{2k}}\right)^3 + \frac{a_2}{\pi_P^{2k}}\left(x + \frac{n}{\pi_P^{2k}}\right)^2 + \frac{a_4}{\pi_P^{4k}}\left(x + \frac{n}{\pi_P^{2k}}\right) + \frac{a_6}{\pi_P^{6k}}$$

has coefficients in R_P. From the coefficient of xy, $v_P(l) \geq k$, and from the coefficient of y, $v_P(m) \geq 3k$. Therefore, we have that

$$y^2 = \left(x + \frac{n}{\pi_P^{2k}}\right)^3 + \frac{a_2}{\pi_P^{2k}}\left(x + \frac{n}{\pi_P^{2k}}\right)^2 + \frac{a_4}{\pi_P^{4k}}\left(x + \frac{n}{\pi_P^{2k}}\right) + \frac{a_6}{\pi_P^{6k}}$$

has coefficients in R_P. Note that $v_P(a_2) \geq 2k$ also.

For an elliptic curve $E \in G_P^{(2)}$ with equation $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$, let $A_k(E)$ be the set of $n \in R_P$ such that

$$y^2 = x^3 + \frac{a_2}{\pi_P^{2k}}x^2 + \frac{2na_2 + a_4}{\pi_P^{4k}}x + \frac{n^2a_2 + na_4 + a_6 + n^3}{\pi_P^{6k}}$$

has coefficients in R_P. The next proposition is useful for computing local densities for multiple iterations.

Proposition 5.2. Let E be an elliptic curve in $G_P^{(2)}$. $E \in S_k$ if and only if a unique element $n \in L_{P,k}$ exists such that $n \in A_k(E)$.

Proof. Assume a unique element $n \in L_{P,k}$ exists. Then, $A_k(E)$ is nonempty, and using Proposition 2.4, $E \in S_k$.

Next, assume $E \in S_k$. From Proposition 2.4, we have that $A_k(E)$ is nonempty. Let the equation of E be $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ for $a_2, a_4, a_6 \in R_P$.

Suppose $n \in A_k(E)$. From replacing x with $x + n'$ for $n' \in R_P$, we have that $n + n'\pi_P^{2k} \in A_k(E)$. Therefore, $n \in L_{P,k}$ exists such that $n \in A_k(E)$.

Next, we prove uniqueness. Assume $n_1, n_2 \in A_k(E) \cap L_{P,k}$. Suppose $a_2 \neq 0$. Let

$$F : y^2 = x^3 + \frac{a_2}{\pi_P^{2k}}x^2 + \frac{a_4}{\pi_P^{4k}}x + \frac{a_6}{\pi_P^{6k}}.$$

For $1 \leq i \leq 2$, let F_i be F with x replaced by $x + \frac{n_i}{\pi_P^{2k}}$. Note that $F_1, F_2 \in G_P^{(2)}$. Also, F_1 and F_2 are equivalent. Then, using Proposition 2.3, the equation of F_2 is the equation of F_1 with x replaced by $u^2x + n'$ and y replaced by $y = u^3y$ and dividing by u^6 for some $n', u \in R_P$ such that $v_P(u) = 0$. Then, we see that $u^2 = 1$ from the coefficient of x^2, and $\frac{n_1}{\pi_P^{2k}} + n' = \frac{n_2}{\pi_P^{2k}}$. Therefore, $n_1 \equiv n_2 \pmod{\pi_P^{2k}}$ and $n_1 = n_2$. Assume $a_2 = 0$. Afterwards, we have that $a_4 \equiv 0 \pmod{\pi_P^{4k}}$ and $(n_1 - n_2)^3 + (n_1 - n_2)a_4 \equiv 0 \pmod{\pi_P^{6k}}$, giving that $n_1 \equiv n_2 \pmod{\pi_P^{2k}}$ and $n_1 = n_2$. ∎

For $E \in S_k$, let $n(E)$ be the unique $n \in L_{P,2k}$ such that the curve $y^2 = x^3 + \frac{a_2}{\pi_P^{2k}}x^2 + \frac{2na_2+a_4}{\pi_P^{4k}}x + \frac{n^2a_2+na_4+a_6+n^3}{\pi_P^{6k}}$ has coefficients in R_P. Define $\phi_k : S_k \to S_0$ to be the function such that if $E \in S_k$ has equation $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$, $\phi_k(E) \in S_0$ have equation

$$\phi_k(E) : y^2 = x^3 + \frac{a_2}{\pi_P^{2k}}x^2 + \frac{2n(E)a_2 + a_4}{\pi_P^{4k}}x + \frac{n(E)^2a_2 + n(E)a_4 + a_6 + n(E)^3}{\pi_P^{6k}}.$$

Note that $S_k \subset S_0 \subset G_P^{(2)}$. Also, using Proposition 2.5 and Lemma 5.1, $\mu_P(S_0) = 1$. For $n \in L_{P,k}$, suppose $S_{k,n}$ is the set of $E \in S_k$ such that $n(E) = n$, and let $\phi_{k,n}$ be ϕ_k restricted to $S_{k,n}$.

Lemma 5.3. If U is an open subset of $G_P^{(2)}$, $\mu_P(\phi_k^{-1}(U)) = \frac{1}{Q_P^{10k}}\mu_P(U)$.

Proof. Suppose $n \in L_{P,k}$. We prove that for an open subset U of $G_P^{(2)}$, $\mu_P(\phi_{k,n}^{-1}(U)) = \frac{1}{Q_P^{12k}}\mu_P(U)$. Let V be the set of $y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$ such that $a_2' \in r_2 + \pi_P^{n_2}R_P$, $a_4' \in r_4 + \pi_P^{n_4}R_P$, and $a_6' \in r_6 + \pi_P^{n_6}R_P$. We compute the Haar measure of the set of $a_2, a_4, a_6 \in R_P$ such that $\frac{a_2}{\pi_P^{2k}} \in r_2 + \pi_P^{n_2}R_P$, $\frac{2na_2+a_4}{\pi_P^{4k}} \in r_4 + \pi_P^{n_4}R_P$, and $\frac{n^2a_2+na_4+a_6+n^3}{\pi_P^{6k}} \in r_6 + \pi_P^{n_6}R_P$. Let $M = \max(n_2 + 2k, n_4 + 4k, n_6 + 6k)$. There are $Q_P^{M-n_2-2k}$ ways to pick a_2 modulo π_P^M. Afterwards, a_4 will have $Q_P^{M-n_4-4k}$ choices for the residue modulo π_P^M; pick a_4 modulo π_P^M. Next, a_6 has $Q_P^{M-n_6-6k}$ choices for the residue modulo π_P^M. Select the residue for a_6. The number of combinations of residues is $Q_P^{3M-n_2-n_4-n_6-12k}$ and each combination of residues has a Haar measure of Q_P^{-3M}. Also, because $\mu_P(S_0) = 1$, the set of curves with discriminant 0 counted in these combinations of residues has a Haar measure 0. Therefore, $\mu_P(\phi_{k,n}^{-1}(V)) = \frac{1}{Q_P^{n_2+n_4+n_6+12k}}$. With this, $\mu_P(\phi_{k,n}^{-1}(U)) = \frac{1}{Q_P^{12k}}\mu_P(U)$ for all open subsets U of $G_P^{(2)}$.

Let U be an open subset of $G_P^{(2)}$ We have that $\phi_k^{-1}(U) = \sqcup_{n \in L_{P,k}} \phi_{k,n}^{-1}(U)$. Then,

$$\mu_P(\phi_k^{-1}(U)) = \sum_{n \in L_{P,k}} \mu_P(\phi_{k,n}^{-1}(U)) = \frac{1}{Q_P^{10k}}\mu_P(U),$$

completing the proof. ■

5.3 Density Calculations for $v_P(a_2) = 0$

Suppose $v_P(a_2) = 0$. The density for this over $G_P^{(2)}$ is $\frac{Q_P-1}{Q_P}$. The discriminant is $-a_2^3a_6 + a_2^2a_4^2 - a_4^3$.

From adding multiples of π_P to a_6, the set of curves with discriminant not divisible by π_P has density $\frac{(Q_P-1)^2}{Q_P^2}$. For this case, we have that $c = 1$. Also, we add $\frac{(Q_P-1)^2}{Q_P^2}$ to $\delta_K(I_0, 1, 0; P)$.

Assume the discriminant is divisible by π_P. The algorithm ends in step 2. Because $v_P(a_2) = 0$, the coefficient of a_6 in the discriminant is not divisible by π_P. Then, we see that for $N \geq 0$, the density over $G_P^{(2)}$ of curves such that $v_P(a_2) = 0$ and $v_P(\Delta(E)) = N$ is $\frac{(Q_P-1)^2}{Q_P^{N+2}}$. If $a_2 \equiv r_2 \pmod{\pi_P}$ for $r_2 \in L_{P,1}$ such that $r_2 \neq 0$, $T^2 + a_2$ is irreducible over $R_P/\pi_P R_P$ for $\frac{Q_P-1}{2}$ values of r_2.

Using step 2 of Tate's algorithm, we have that $\delta_K(I_1, 1, 0; P) = \frac{(Q_P-1)^2}{Q_P^3}$, $\delta_K(I_2, 2, 0; P) = \frac{(Q_P-1)^2}{Q_P^4}$, and $\delta_K(I_N, N, 0; P) = \delta_K(I_N, 2\left\lfloor\frac{N}{2}\right\rfloor - N + 2, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+2}}$ for $N \geq 3$. Moreover, $c = 1$ with density $\frac{(Q_P-1)(2Q_P^2-1)}{2Q_P^3(Q_P+1)}$ and $c = 2$ with density $\frac{(Q_P-1)(2Q_P^2-1)}{2Q_P^4(Q_P+1)}$. For $N \geq 3$, $c = N$ with density $\frac{(Q_P-1)^2}{2Q_P^{N+2}}$.

5.4 Density Calculations for $v_P(a_2) \geq 1$

Next, suppose $v_P(a_2) \geq 1$. The density for this is $\frac{1}{Q_P}$ and modulo π_P, the discriminant is $-a_4^3$.

Assume the discriminant is not divisible by π_P. This occurs if and only if a_4 is not divisible by π_P, and the density of this case is $\frac{Q_P-1}{Q_P^2}$. Adding this density to $\delta_K(I_0, 1, 0; P)$ gives that $\delta_K(I_0, 1, 0; P) = \frac{Q_P-1}{Q_P}$.

Next, assume the discriminant is divisible by π_P. The total density for these cases will be $\frac{1}{Q_P^2}$. Suppose α_1 is an element of $L_{P,1}$ such that $a_6 + \alpha_1^3 \equiv 0 \pmod{\pi_P}$. A singular point is $(\alpha_1, 0)$. We have that x is replaced with $x + n$ where $n = \alpha_1$. The resulting curve has equation

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

We have that $n^2a_2 + na_4 + a_6 + n^3$ is not divisible by π_P^2 with density $\frac{Q_P-1}{Q_P^3}$ by adding multiples of π_P to a_6. Here, $\delta_K(II, 1, 0; P) = \frac{Q_P-1}{Q_P^3}$.

Assume $n^2a_2 + na_4 + a_6 + n^3$ is divisible by π_P^2. The total density for this case is $\frac{1}{Q_P^3}$. The density of $v_P(2na_2 + a_4) = 1$ is $\frac{Q_P-1}{Q_P^4}$ from replacing a_4 with $a_4 + \pi_P d$ and a_6 with $a_6 - \alpha_1\pi_P d$ for $d \in L_{P,1}$. If $v_P(2na_2 + a_4) = 1$, the algorithm ends in step 4. We then have that $\delta_K(III, 2, 0; P) = \frac{Q_P-1}{Q_P^4}$.

Assume $2na_2 + a_4$ is divisible by π_P^2. The total density for this case is $\frac{1}{Q_P^4}$. We have that $v_P(n^2a_2 + na_4 + a_6 + n^3) = 2$ with density $\frac{Q_P-1}{Q_P^5}$ from adding multiples of π_P^2 to a_6. If this is true, the algorithm ends in step 5. Afterwards, we have that $\delta_K(IV, 1, 0; P) = \delta_K(IV, 3, 0; P) = \frac{Q_P-1}{2Q_P^5}$.

Suppose $v_P(n^2a_2 + na_4 + a_6 + n^3) \geq 3$. The total density for this case is $\frac{1}{Q_P^5}$. In step 6, there is no translation. Suppose a_2 is replaced by $a_2 + d_1\pi_P$, a_4 is replaced with $a_4 - 2\alpha_1 d_1\pi_P$, and a_6 is replaced with $a_6 + \alpha_1^2 d_1\pi_P$ for $d_1 \in L_{P,1}$. Note that the previous parts of the algorithm will not be changed. However, this changes the coefficient of x^2 from a_2 to $a_2 + d_1\pi_P$, which changes the coefficient of T^2 of $P(T)$ in step 6. Next, replace a_4 with $a_4 + d_2\pi_P^2$ and a_6 with $a_6 - \alpha_1 d_2\pi_P^2$ for $d_2 \in \pi_P$. Similarly, this does not change the previous parts of the algorithm. However, $d_2\pi_P^2$ will be added to the coefficient of x, which adds d_2 to the coefficient of T of $P(T)$. Afterwards, replace a_6 with $a_6 + d_3\pi_P^3$ for $d_3 \in L_{P,1}$. This adds d_3 to the constant term $P(T)$. With this, the choices for $P(T)$ are the monic polynomials with degree 3 in $(R_P/\pi_P R_P)[T]$; each choice for $P(T)$ corresponds to a density of $\frac{1}{Q_P^8}$. Moreover, the number of $P(T)$ with a double root and triple root are $Q_P(Q_P - 1)$ and Q_P, respectively.

Assume $P(T)$ has distinct roots. We have that the algorithm ends in step 6, with $\delta_K(I_0^*, 1, 0; P) = \frac{Q_P^2-1}{3Q_P^7}$, $\delta_K(I_0^*, 2, 0; P) = \frac{Q_P-1}{2Q_P^6}$, and $\delta_K(I_0^*, 4, 0; P) = \frac{Q_P^2-3Q_P+2}{6Q_P^7}$.

Assume $P(T)$ has a double root. For this case, Tate's algorithm ends in step 7 and the total density is $\frac{Q_P-1}{Q_P^7}$. For a positive integer N, we have that $\delta_K(I_N^*, 2, 0; P) = \delta_K(I_N^*, 4, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+7}}$. Also, it can be proven that $c = 2$ and $c = 4$ both have density $\frac{Q_P-1}{2Q_P^7}$. More details are in Section 5.5.

Now, assume $P(T)$ has a triple root. The density for this case is $\frac{1}{Q_P^7}$. Let α_2 be the element of $L_{P,1}$ such that

$$n^2a_2 + na_4 + a_6 + n^3 \equiv -\pi_P^3\alpha_2^3 \pmod{\pi_P^4}.$$

Then, for the translation in step 8, we let $n = \alpha_1 + \alpha_2\pi_P$. Suppose $v_P(n^2a_2 + na_4 + a_6 + n^3) = 4$. This occurs with density $\frac{Q_P-1}{Q_P^8}$ by adding multiples of π_P^4 to a_6. In this case, Tate's algorithm ends in step 8, and $\delta_K(IV^*, 1, 0; P) = \delta_K(IV^*, 3, 0; P) = \frac{Q_P-1}{2Q_P^8}$.

Next, assume $v_P(n^2a_2 + na_4 + a_6 + n^3) \geq 5$. The total density for this case is $\frac{1}{Q_P^8}$. Consider replacing a_4 with $a_4 + d\pi_P^3$ and a_6 with $a_6 - (\alpha_1 + \alpha_2\pi_P)d\pi_P^3$ for $d \in L_{P,1}$. This does not change previous parts of the algorithm but adds $d\pi_P^3$ to the coefficient of x. Therefore, $v_P(2na_2 + a_4) = 3$ with density $\frac{Q_P-1}{Q_P^9}$. For this, we have that Tate's algorithm ends in step 9 and $\delta_K(III^*, 2, 0; P) = \frac{Q_P-1}{Q_P^9}$.

Suppose $v_P(2na_2 + a_4) \geq 4$. The total density of this case is $\frac{1}{Q_P^9}$. From adding multiples of π_P^6 to a_6, $v_P(n^3 + a_2n^2 + a_4n + a_6) = 5$ with density $\frac{Q_P-1}{Q_P^{10}}$. Also, if $v_P(n^3 + a_2n^2 + a_4n + a_6) = 5$, the algorithm ends in step 10. This gives that $\delta_K(II^*, 1, 0; P) = \frac{Q_P-1}{Q_P^{10}}$.

5.5 Subprocedure Density Calculations

Let X be the set of elliptic curves $E \in G_P^{(2)}$ such that $M_P(E) = 0$ and Tate's algorithm enters the step 7 subprocedure when used on E. For $E \in X$, let $L(E)$ be the number of iterations of the step 7 subprocedure that are completed when Tate's algorithm is used on E. For a nonnegative integer N, let X_N be the set of $E \in X$ such that $L(E) \geq N$.

Assume $N \geq 0$ is even. Iteration N of the step 7 subprocedure is completed if and only if $n \in R_P$ exists such that $v_P(a_2) = 1$, $v_P(2na_2 + a_4) \geq \frac{N+6}{2}$, and $v_P(n^3 + n^2a_2 + na_4 + a_6) \geq N + 4$. Assume $n = n_1$ satisfies the condition. Suppose $n = n_2$ satisfies the condition also.

Because $v_P(a_2) = 1$, $v_P(n_1 - n_2) \geq \frac{N+4}{2}$. Next, assume $v_P(n_1 - n_2) \geq \frac{N+4}{2}$. We show that $n = n_2$ also satisfies the condition. Clearly, $v_P(2n_2a_2 + a_4) \geq \frac{N+6}{2}$. Moreover, we have that

$$n_2^2a_2 + n_2a_4 = n_1^2a_2 + n_1a_4 + \frac{1}{2}(n_2 - n_1)((2n_1a_2 + a_4) + (2n_2a_2 + a_4)).$$

Therefore, $v_P(n_2^3 + n_2^2a_2 + n_2a_4 + a_6) \geq N + 4$. We have that $n = n_2$ satisfies the condition if and only if $v_P(n_1 - n_2) \geq \frac{N+4}{2}$.

Suppose $N \geq 0$ is odd. Iteration N of the step 7 subprocedure is completed if and only if $n \in R_P$ exists such that $v_P(n^2a_2 + na_4 + a_6 + n^3) \geq N + 4$ and $v_P(2na_2 + a_4) \geq \frac{N+5}{2}$. Assume $n = n_1$ satisfies the condition. Similarly to when N is even, we have that $n = n_2$ also satisfies the condition if and only if $v_P(n_1 - n_2) \geq \frac{N+3}{2}$.

Suppose N is a nonnegative integer. Let Y_N be the set of curves $y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$ with $v_P(a_2') = 1$, $v_P(a_4') \geq \lfloor \frac{N+6}{2} \rfloor$, and $v_P(a_6') \geq N + 4$. For $E \in X_N$, let $n_N(E)$ be the unique value of n in $L_{P,\lfloor \frac{N+4}{2} \rfloor}$ from above. Suppose $\theta_N(E)$, with $\theta_N : X_N \to Y_N$, is the curve

$$\theta_N(E) : y^2 = (x + n_N(E))^3 + a_2(x + n_N(E))^2 + a_4(x + n_N(E)) + a_6.$$

Lemma 5.4. If U is an open subset of Y_N, $\mu_P(\theta_N^{-1}(U)) = Q_P^{\lfloor \frac{N+4}{2} \rfloor}\mu_P(U)$.

Proof. Suppose $n \in L_{P,\lfloor \frac{N+4}{2} \rfloor}$. Let $X_{N,n}$ be the set of $E \in X_N$ with $n_N(E) = n$ and $\theta_{N,n}$ be θ_N restricted to $X_{N,n}$. Note that if $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ is an element of $X_{N,n}$, $\theta_N(E) = \theta_{N,n}(E)$ is $y^2 = x^3 + a_2x^2 + (na_2 + a_4)x + n^2a_2 + na_4 + a_6 + n^3$. Particularly, $\theta_{N,n}(E)$ is invertible. We then have that $\mu_P(\theta_{N,n}^{-1}(U)) = \mu_P(U)$. Because there are $Q_P^{\lfloor \frac{N+4}{2} \rfloor}$ values of n, the result follows. ■

Suppose N is a positive integer. Using Lemma 5.4, we can compute the density of the curves E with $M_P(E) = 0$ that have type I_N^* and Tamagawa number 2 or 4. The Haar measure of the curves in Y_{N-1} that end in iteration N is $\frac{(Q_P-1)^2}{Q_P^{N+6+\lfloor \frac{N+5}{2} \rfloor}}$. With Lemma 4.1, we have that $\delta_K(I_N^*, 2, 0; P) = \delta_K(I_N^*, 4, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+7}}$.

6 Local Densities for $p = 2$

6.1 Setup

Suppose that the characteristic of K is $p = 2$. Let P be a place of K and $G_P^{(3)}$ be the set of curves

$$y^2 + a_1xy + a_3y = x^3 + a_4x + a_6$$

over K_P such that $a_1, a_3, a_4, a_6 \in R_P$. Note that $G_P^{(3)}$ can be considered to be R_P^4. For a curve $E \in G_P$ with equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, let $\varphi(E)$ be the curve with equation

$$\varphi(E) : y^2 + a_1xy + \left(a_3 - \frac{a_1a_2}{3}\right)y = x^3 + \left(a_4 - \frac{a_2^2}{3}\right)x + \frac{2a_2^3}{27} - \frac{a_2a_4}{3} + a_6.$$

If E is an elliptic curve, $\varphi(E)$ is an elliptic curve equivalent to E.

Lemma 6.1. If U is an open subset of $G_P^{(3)}$, $\mu_P(\varphi^{-1}(U)) = \mu_P(U)$.

Proof. This can be proved similarly as Lemma 4.1. ■

6.2 Multiple Iterations

Let k be a nonnegative integer. Suppose S_k is the set of elliptic curves $E \in G_P^{(3)}$ such that $M_P(E) \geq k$.

For an elliptic curve $E \in G_P^{(3)}$ with equation $E : y^2 + a_1xy + a_3y = x^3 + a_4x + a_6$, let $A_k(E)$ be the set of $(l, m, n) \in R_P^3$ such that if $X = x + \frac{n}{\pi_P^{2k}}$ and $Y = y + \frac{l}{\pi_P^k}x + \frac{m}{\pi_P^{3k}}$,

$$Y^2 + \frac{a_1}{\pi_P^k}XY + \frac{a_3}{\pi_P^{3k}}Y - X^3 - \frac{a_4}{\pi_P^{4k}}X - \frac{a_6}{\pi_P^{6k}} \in R_P[x, y].$$

Proposition 6.2. Let E be an elliptic curve in $G_P^{(3)}$. $E \in S_k$ if and only if a unique pair $(l, m) \in L_{P,k} \times L_{P,3k}$ exists such that $(l, m, l^2 + a_1l) \in A_k(E)$.

Proof. Suppose a unique pair (l, m) satisfying the conditions exists. Because $A_k(E)$ is nonempty, $E \in S_k$ from Proposition 2.4.

Assume $E \in S_k$. Then, using Proposition 2.4, $A_k(E)$ is nonempty. Let the equation of E be $E : y^2 + a_1xy + a_3y = x^3 + a_4x + a_6$ for $a_1, a_3, a_4, a_6 \in R_P$.

From replacing y with $y + l'x$ for $l' \in R_P$, if $(l, m, n) \in A_k(E)$, $(l + l'\pi_P^k, m, n) \in A_k(E)$. Therefore, there exist $l \in L_{P,k}$ and $m, n \in R_P$ such that $(l, m, n) \in A_k(E)$. Moreover, if $(l, m, n) \in A_k(E)$, $l^2 + a_1l + n \equiv 0 \pmod{\pi_P^{2k}}$. With this, from replacing x with $x + \frac{l^2+a_1l+n}{\pi_P^{2k}}$, if $(l, m, n) \in A_k(E)$, $(l, m + l(l^2 + a_1l + n), l^2 + a_1l) \in A_k(E)$. Therefore, there exist $l \in L_{P,k}$ and $m \in R_P$ such that $(l, m, l^2 + a_1l)$. Next, from replacing y with $y + m'$ for $m' \in R_P$, there exists $l \in L_{P,k}$ and $m \in L_{P,3k}$ such that $(l, m, l^2 + a_1l) \in A_k(E)$.

Next, we prove that (l, m) is unique. Assume that $(l_1, m_1), (l_2, m_2) \in L_{P,k} \times L_{P,3k}$ and $(l_1, m_1, l_1^2 + a_1l_1), (l_2, m_2, l_2^2 + a_1l_2) \in A_k(E)$. We prove that $(l_1, m_1) = (l_2, m_2)$.

Suppose $a_1 \neq 0$. Let F be the curve

$$F : y^2 + \frac{a_1}{\pi_P^k}xy + \frac{a_3}{\pi_P^{3k}} = x^3 + \frac{a_4}{\pi_P^k}x + \frac{a_6}{\pi_P^{6k}}.$$

For $1 \leq i \leq 2$, let F_i be F with x replaced by $x + \frac{l_i^2+a_1l_i}{\pi_P^{2k}}$ and y replaced by $y + \frac{l_i}{\pi_P^k}x + \frac{m_i}{\pi_P^{3k}}$. Note that $F_1, F_2 \in G_P^{(3)}$. Also, F_1 and F_2 are equivalent. Then, using Proposition 2.3, let the translation from the equation of F_1 to the equation of F_2 replace x with $u^2x + n'$ and y with $u^3y + l'u^2x + m'$, where $u, l', m', n' \in R_P$ and $v_P(u) = 0$. The coefficient of xy after this translation is $\frac{a_1}{u\pi_P^k}$; therefore, $u = 1$ and $a_1 \equiv 0 \pmod{\pi_P^k}$. Afterwards, from the coefficient of x^2, $l_1^2 + a_1l_1 + n'\pi_P^{2k} = l_2^2 + a_1l_2$. Therefore, $l_1 \equiv l_2 \pmod{\pi_P^k}$ and $l_1 = l_2$. Particularly, $n' = 0$. Following this, $m_2 = m_1 + m'\pi_P^{2k}$ and $m_1 = m_2$.

Assume $a_1 = 0$. We then have that $a_3 \equiv 0 \pmod{\pi_P^{3k}}$, and from the coefficient of x, $l_1^4 + a_3l_1 \equiv l_2^4 + a_3l_2 \pmod{\pi_P^{4k}}$. From this, we clearly have that $l_1 = l_2$. Afterwards, from the constant terms, $m_1^2 + a_3m_1 \equiv m_2^2 + a_3m_2 \pmod{\pi_P^6}$ and $m_1 = m_2$. ■

For $E \in S_k$, let the unique pair $(l, m) \in L_{P,k} \times L_{P,3k}$ such that $(l, m, l^2 + a_1l) \in A_k(E)$ be $(l(E), m(E))$. Define $\phi_k : S_k \to S_0$ to be the function such that if $E \in S_k$ has equation $E : y^2 + a_1xy + a_3y = x^3 + a_4x + a_6$, $\phi_k(E)$ has equation

$$\phi_k(E) : Y^2 + \frac{a_1}{\pi_P^k}XY + \frac{a_3}{\pi_P^{3k}}Y = X^3 + \frac{a_4}{\pi_P^{4k}}X + \frac{a_6}{\pi_P^{6k}},$$

with $X = x + \frac{l(E)^2+a_1l(E)}{\pi_P^{2k}}$ and $Y = y + \frac{l(E)}{\pi_P^k}x + \frac{m(E)}{\pi_P^{3k}}$. Note that $S_0 \subset G_P^{(3)}$, and from Proposition 2.5 and Lemma 6.1, $\mu_P(S_0) = 1$. For $l \in L_{P,k}$ and $m \in L_{P,3k}$, let $S_{k,l,m}$ be the set of $E \in S_k$ such that $l(E) = l$ and $m(E) = m$. Assume that $\phi_{k,l,m}$ is ϕ_k restricted to $S_{k,l,m}$.

Lemma 6.3. If U is an open subset of $G_P^{(3)}$, $\mu_P(\phi_k^{-1}(U)) = \frac{1}{Q_P^{10k}}\mu_P(U)$.

Proof. Note that there are Q_P^k values of l and Q_P^{3k} values of m. Similarly, it suffices to prove that for open subsets U of $G_P^{(3)}$, $\mu_P(\phi_{k,l,m}^{-1}(U)) = \frac{1}{Q_P^{14k}}\mu_P(U)$. Let V be the set of curves $y^2 + a_1'xy + a_3'y = x^3 + a_4'x + a_6'$ with $a_i' \in r_i + \pi_P^{n_i}R_P$ for $i \in \{1,3,4,6\}$. We find $\phi_{k,l,m}^{-1}(V)$. Let $M = \max(n_1+k, n_3+3k, n_4+4k, n_6+6k)$. Note that $a_1 \in \pi_P^k r_1 + \pi_P^{n_1+k}R_P$, and there are $Q_P^{M-n_1-k}$ choices for the residue of a_1 modulo π_P^M. After choosing the residue of a_1, there are $Q_P^{M-n_3-3k}$ choices for the residue of a_3. Continuing this process for a_4 and a_6 and adding over the Q_P^{4k} pairs (l,m) gives the result. Similarly, the set of curves counted in these combinations of residues with discriminant 0 has a Haar measure of 0. ∎

6.3 Density Calculations for $v_P(a_1) = 0$

Suppose that $v_P(a_1) = 0$. This case has density $\frac{Q_P-1}{Q_P}$. The discriminant is

$$a_1^4(a_1^2a_6 + a_1a_3a_4 + a_4^2) + a_3^4 + a_1^3a_3^3.$$

Note that by considering a_6 modulo π_P, the discriminant is not divisible by π_P with density $\frac{(Q_P-1)^2}{Q_P^2}$. For this case, the algorithm ends in step 1 and $c = 1$. Then, we add $\frac{(Q_P-1)^2}{Q_P^2}$ to $\delta_K(I_0, 1, 0; P)$.

Assume the discriminant is divisible by π_P. Let (α_1, α_2) be the singular point modulo π_P; it can be proven that $\alpha_1, \alpha_2 \in R_P$. Also, $\alpha_1 \equiv -\frac{a_3}{a_1} \pmod{\pi_P}$. In step 2, replace x by $x+n$ and y by $y+m$ with $n = \alpha_1$ and $m = \alpha_2$. Afterwards, the coefficient of xy is a_1, which is not divisible by π_P. The algorithm then ends in step 2.

We see that the discriminant is linear in a_6. Therefore, we have that $v_P(a_1) = 0$ and $v_P(\Delta(E)) = N$ with density $\frac{(Q_P-1)^2}{Q_P^{N+2}}$ for $N \geq 0$. Note that the polynomial considered in step 2 is $T^2 + a_1T + \alpha_1$. Suppose $a_1 \equiv r_1 \pmod{\pi_P}$ and $a_3 \equiv r_3 \pmod{\pi_P}$ for $r_1, r_3 \in L_{P,1}$ such that $r_1 \neq 0$. Given r_1, $T^2 + a_1T + \alpha_1$ is irreducible over R_P/π_PR_P for $\frac{Q_P}{2}$ values of r_3. Afterwards, using step 2 of Tate's algorithm, we get that in this case, $\delta_K(I_1, 1, 0; P) = \frac{(Q_P-1)^2}{Q_P^3}$, $\delta_K(I_2, 2, 0; P) = \frac{(Q_P-1)^2}{Q_P^4}$, and $\delta_K(I_N, N, 0; P) = \delta_K(I_N, 2\left\lfloor\frac{N}{2}\right\rfloor - N + 2, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+2}}$ for $N \geq 3$. Moreover, $c = 1$ with density $\frac{(Q_P-1)(2Q_P^2-1)}{2Q_P^3(Q_P+1)}$, $c = 2$ with density $\frac{(Q_P-1)(2Q_P^2-1)}{2Q_P^4(Q_P+1)}$, and for $N \geq 3$, $c = N$ with density $\frac{(Q_P-1)^2}{2Q_P^{N+2}}$.

6.4 Density Calculations for $v_P(a_1) \geq 1$

In this subsection, we assume that $v_P(a_1) \geq 1$. The density for this is $\frac{1}{Q_P}$, and the discriminant modulo π_P is a_3^4.

Suppose $v_P(a_3) = 0$. The density for this case is $\frac{Q_P-1}{Q_P^2}$. Here, the discriminant is not divisible by π_P. Tate's algorithm then ends in step 1, and we add $\frac{Q_P-1}{Q_P^2}$ to $\delta_K(I_0, 1, 0; P)$. We therefore have that $\delta_K(I_0, 1, 0; P) = \frac{Q_P-1}{Q_P}$.

Next, assume that $v_P(a_3) \geq 1$. The total density for this is $\frac{1}{Q_P^2}$. The singular point modulo π_P is $(x, y) = (\alpha_1, \alpha_2)$ for $\alpha_1, \alpha_2 \in L_{P,1}$ such that $a_4 \equiv \alpha_1^2 \pmod{\pi_P}$ and $a_6 \equiv \alpha_2^2 \pmod{\pi_P}$. We replace x with $x+n$ and y with $y+m$, where $n = \alpha_1$ and $m = \alpha_2$. The curve is

$$(y+m)^2 + a_1(x+n)(y+m) + a_3(y+m) = (x+n)^3 + a_4(x+n) + a_6.$$

If π_P^2 does not divide $mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3$, the algorithm ends in step 3. By adding multiples of π_P to a_6, this occurs with density $\frac{Q_P-1}{Q_P^3}$. We have that $\delta_K(II, 1, 0; P) = \frac{Q_P-1}{Q_P^3}$.

Assume π_P^2 divides $mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3$. The total density for this case is $\frac{1}{Q_P^3}$. We have that

$$b_8 = n(na_1 + a_3)^2 + (ma_1 + a_4 + n^2)^2.$$

If b_8 is not divisible by π_P^3, the algorithm ends in step 4. By adding multiples of π_P to a_4, we have that $\delta_K(III, 2, 0; P) = \frac{Q_P-1}{Q_P^4}$.

Assume that b_8 is divisible by π_P^3. The total density for this case is $\frac{1}{Q_P^4}$. If $v_P(na_1+a_3) = 1$, the algorithm ends in step 5. Assume $a_4 \equiv 0 \pmod{\pi_P}$. Then, replace a_3 with $a_3 + d\pi_P$ and a_4 with $a_4 + \beta d\pi_P$ for $\beta, d \in L_{P,1}$ such that $\beta^2 \equiv \alpha_1 \pmod{\pi_P}$. This will not affect previous parts of the algorithm; particularly, this will not change b_8 modulo π_P^3. However, $na_1 + a_3$ will be increased by $d\pi_P$. Therefore, we have that $v_P(na_1 + a_3) = 1$ with density $\frac{Q_P-1}{Q_P^5}$. From this, $\delta_K(IV, 1, 0; P) = \delta_K(IV, 3, 0; P) = \frac{Q_P-1}{2Q_P^5}$.

Assume $v_P(na_1 + a_3) \geq 2$. The total density for this case is $\frac{1}{Q_P^5}$. Assume α_3 is the element of $L_{P,1}$ such that $n \equiv \alpha_3^2 \pmod{\pi_P}$. Also, let α_4 be the element of $L_{P,1}$ such that $mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3 \equiv \alpha_4^2\pi_P^2 \pmod{\pi_P^3}$. After the transformation in step 6, let the equation of the curve be

$$\begin{aligned}&(y + lx + m)^2 + a_1(x + n)(y + lx + m) + a_3(y + lx + m)\\ &= (x + n)^3 + a_4(x + n) + a_6.\end{aligned}$$

Here, $l = \alpha_3$ and $m = \alpha_2 + \alpha_4\pi_P$. Suppose that in step 6, the polynomial $P(T) \in (R_P/\pi_P R_P)[T]$ is $P(T) = T^3 + w_2T^2 + w_1T + w_0$.

Suppose $a_4 \equiv 0 \pmod{\pi_P}$. Because $0 \in L_{P,1}$, we have that $n = l = 0$, and $w_2 = 0$. Then, we can replace a_4 with $a_4 + d_1\pi_P^2$ for $d_1 \in L_{P,1}$, and the previous parts of the algorithm will not be changed. With this, the choices for w_1 modulo π_P are the elements of $L_{P,1}$. Following this, by replacing a_6 with $a_6 + d_2\pi_P^3$ for $d_2 \in L_{P,1}$, the choices for w_0 modulo π_P are the elements of $L_{P,1}$. We have that the number of $P(T)$ with a double root and no roots are $Q_P - 1$ and 1, respectively. Moreover, we have that the number of $P(T)$ with three distinct roots in $\overline{R_P/\pi_P R_P}$ with 0 roots, 1 root, and 3 roots in $R_P/\pi_P R_P$ are $\frac{Q_P^2-1}{3}$, $\frac{Q_P^2-Q_P}{2}$, and $\frac{Q_P^2-3Q_P+2}{6}$, respectively.

Suppose $a_4 \not\equiv 0 \pmod{\pi_P}$. Consider the translation of replacing a_1 with $a_1 + d_1\pi_P$, a_3 with $a_3 + \alpha_1 d_1\pi_P$, a_4 with $a_4 + (\alpha_2 + \alpha_4\pi_P)d_1\pi_P$, and a_6 with $a_6 + \alpha_1(\alpha_2 + \alpha_4\pi_P)d_1\pi_P$ for $d_1 \in L_{P,1}$. After this, the parts of the algorithm before step 6 do not change. In step 6, w_0 and w_1 do not change. However, w_2 increases by $\alpha_3 d_1$. Because $\alpha_3 \neq 0$, the choices for w_2 are the elements of $L_{P,1}$. Next, replace a_6 with $a_6 + d_2\pi_P^3$ for $d_2 \in L_{P,1}$. With this, the choices for w_0 are also the elements of $L_{P,1}$. The number of $P(T)$ with a double root and no roots are the same as above. Also, the number of $P(T)$ with three distinct roots in $\overline{R_P/\pi_P R_P}$ with 0 roots, 1 root, and 3 roots in $R_P/\pi_P R_P$ are the same as above.

Suppose $P(T)$ has distinct roots. For this case, the total density is $\frac{Q_P-1}{Q_P^6}$ and Tate's algorithm ends in step 6. We see that $\delta_K(I_0^*, 1, 0; P) = \frac{Q_P^2-1}{3Q_P^7}$, $\delta_K(I_0^*, 2, 0; P) = \frac{Q_P-1}{2Q_P^6}$, and $\delta_K(I_0^*, 4, 0; P) = \frac{Q_P^2-3Q_P+2}{6Q_P^7}$.

Assume $P(T)$ has a double root and a simple root. For this case, the total density is $\frac{Q_P-1}{Q_P^7}$ and Tate's algorithm ends in step 7. We have that for positive integers N, $\delta_K(I_N^*, 2, 0; P) = \delta_K(I_N^*, 4, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+7}}$. More details for calculating these densities are in Section 6.5.

Next, suppose $P(T)$ has a triple root. For this case, the density is $\frac{1}{Q_P^7}$, and the root of $P(T)$ is $\sqrt{w_1}$ modulo π_P. If $a_4 \equiv 0 \pmod{\pi_P}$, the triple root is 0 modulo π_P. Let α_5 be an element of $L_{P,1}$ such that

$$(m + ln)a_1 + la_3 + a_4 + n^2 \equiv \alpha_5^2\pi_P^2 \pmod{\pi_P^3}.$$

Then, the translation in step 8 sets n to be $n = \alpha_1 + \alpha_5\pi_P$.

Suppose $a_4 \equiv 0 \pmod{\pi_P}$. Replace a_3 with $a_3 + d\pi_P^2$ and a_6 with $a_6 + (\alpha_2 + \alpha_4\pi_P)d\pi_P^2$ for some $d \in L_{P,1}$. Then, note that the previous parts of the algorithm, including $P(T)$, are unchanged. However, the coefficient of y increases by $d\pi_P^2$. We have that for one value of d, the coefficient of y is divisible by π_P^3. Next, suppose $a_4 \not\equiv 0 \pmod{\pi_P}$. Replace a_1 with $a_1 + d\pi_P^2$ and a_4 with $a_4 + (\alpha_2 + \alpha_4\pi_P)d\pi_P^2$ for some $d \in L_{P,1}$. The previous parts of the algorithm, including $P(T)$, are unchanged. However, the coefficient of y increases by $(\alpha_1 + \alpha_5\pi_P)d\pi_P^2$. Similarly, we have that for one value of d, the coefficient of y is divisible by π_P^3. From this, we get that the coefficient of y is not divisible by π_P^3 and the algorithm ends in step 8 with density $\frac{Q_P-1}{Q_P^8}$. We then have that $\delta_K(IV^*, 1, 0; P) = \delta_K(IV^*, 3, 0; P) = \frac{Q_P-1}{2Q_P^8}$.

Assume the coefficient of y is divisible by π_P^3. The total density of this case is $\frac{1}{Q_P^8}$. Let α_6 be the element of $L_{P,1}$ such that

$$mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3 \equiv \alpha_6^2\pi_P^4 \pmod{\pi_P^5}.$$

Then, m is set to $m = \alpha_2 + \alpha_4\pi_P + \alpha_6\pi_P^2$ in step 9. If π_P^4 does not divide the x coefficient of this curve, the algorithm ends in step 9. Consider the translation of replacing a_4 with $a_4 + d\pi_P^3$ and a_6 with $a_6 + (\alpha_1 + \alpha_5\pi_P)d\pi_P^3$ for $d \in L_{P,1}$. The previous parts of the algorithm do not change, but the coefficient of x is increased by $d\pi_P^3$. Therefore, π_P^4 does not divide the x coefficient with density $\frac{Q_P-1}{Q_P^9}$. We have that $\delta_K(III^*, 2, 0; P) = \frac{Q_P-1}{Q_P^9}$

Assume π_P^4 divides the coefficient of x of the curve. The total density for this case is $\frac{1}{Q_P^9}$. If π_P^6 does not divide $mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3$, Tate's algorithm ends in step 10. This occurs with density $\frac{Q_P-1}{Q_P^{10}}$ from adding multiples of π_P^6 to a_6. We then have that $\delta_K(II^*, 1, 0; P) = \frac{Q_P-1}{Q_P^{10}}$.

6.5 Subprocedure Density Calculations

We calculate the density of Kodaira types $\mathfrak{r} = I_N^*$ for $N \geq 1$ and Tamagawa numbers $n = 2, 4$. Note that previously, the curve was reduced by removing a_2 with a translation on x to obtain $G_P^{(3)}$. However, here the density is calculated in G_P without the reduction. That is, the density is calculated for curves in long Weierstrass form.

Let X be the set of elliptic curves $E \in G_P$ such that $M_P(E) = 0$ and Tate's algorithm enters the step 7 subprocedure when used on E. For $E \in X$, let $L(E)$ be the number of iterations of the step 7 subprocedure that are completed when Tate's algorithm is used on E. For a nonnegative integer N, let X_N be the set of $E \in X$ such that $L(E) \geq N$.

We consider when $N \geq 0$ is even. Suppose $N = 0$. In iteration $N = 0$, there is a translation. Note that the double root of $P(T)$ is the squareroot of w_1. Because of this, in step 7, we add $\gamma_0\pi_P$ to n and $l\gamma_0\pi_P$ to m for some $\gamma_0 \in L_{P,1}$ such that

$$(m + ln)a_1 + la_3 + a_4 + n^2 \equiv \gamma_0^2\pi_P^2 \pmod{\pi_P^3}$$

Next, assume $N \geq 2$ is even. If iteration N of the step 7 subprocedure is reached and the quadratic has a double root,

$$v_P((m + ln)a_1 + la_3 + a_4 + n^2) \geq \frac{N+6}{2}.$$

Also, we add $\gamma_N\pi_P^{\frac{N+2}{2}}$ to n and $l\gamma_N\pi_P^{\frac{N+2}{2}}$ to m for some $\gamma_N \in L_{P,1}$ such that

$$mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3 \equiv (la_1 + a_2 + n + l^2)\gamma_N^2\pi_P^{N+2} \pmod{\pi_P^{N+4}}.$$

Note that $v_P(la_1 + a_2 + n + l^2) = 1$.

Suppose $N \geq 0$ is odd. If iteration N of the step 7 subprocedure is reached and the quadratic has a double root, $v_P(na_1 + a_3) \geq \frac{N+5}{2}$. Also, $\gamma_N \pi_P^{\frac{N+3}{2}}$ is added to m for some $\gamma_N \in L_{P,1}$ such that

$$mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3 \equiv \gamma_N^2 \pi_P^{N+3} \pmod{\pi_P^{N+4}}$$

Let N be a nonnegative integer. Let Y_N be the set of curves $y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ with $v_P(a_1') \geq 1$, $v_P(a_2') = 1$, $v_P(a_3') \geq \lfloor \frac{N+5}{2} \rfloor, v_P(a_4') \geq \lfloor \frac{N+6}{2} \rfloor$, and $v_P(a_6') \geq N+4$.

Suppose $E \in X_N$ and that the translations of Tate's algorithm when it is used on E are α_1, α_2, α_3, α_4, γ_0, γ_1, ..., γ_N. Let $T(E) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \gamma_0, \gamma_1, \ldots, \gamma_N)$. Note that because the characteristic of K is $p = 2$, $T(E)$ is well defined. Also, let $\theta_N(E) : X_N \to Y_N$ be E with x replaced by $x + n$ and y replaced by $y + lx + m$, where

$$n = \alpha_1 + \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \gamma_{2i} \pi_P^{i+1}, l = \alpha_3, m = \alpha_2 + \alpha_4 \pi_P + \alpha_3 \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \gamma_{2i} \pi_P^{i+1} + \sum_{i=0}^{\lfloor \frac{N-1}{2} \rfloor} \gamma_{2i+1} \pi_P^{i+2}.$$

Lemma 6.4. If U is an open subset of Y_N, $\mu_P(\theta_N^{-1}(U)) = Q_P^{N+5} \mu_P(U)$.

Proof. Let $a = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \gamma_0, \gamma_1, \ldots, \gamma_N)_{0 \leq i \leq N}$. Assume that $X_{N,a}$ is the set of $E \in X_N$ such that $T(E) = a$. Let $\theta_{N,a}$ be θ_N restricted to $X_{N,a}$. From a, we obtain l, m, n. We have that if $E \in X_{N,a}$, $\theta_{N,a}(E)$ is $E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$, where

$$a_1' = a_1, a_2' = la_1 + a_2 + n + l^2, a_3' = na_1 + a_3, a_4' = (m + ln)a_1 + la_3 + a_4 + n^2,$$
$$a_6' = mna_1 + ma_3 + na_4 + a_6 + m^2 + n^3.$$

It is clear that $\theta_{N,a}$ is a bijection.

Let V be the set of $E' \in Y_N$ such that $a_i' \in r_i + \pi_P^{n_i} R_P$ for $i \in \{1, 2, 3, 4, 6\}$. Let $M = \max_{i \in \{1,2,3,4,6\}} n_i$. Similarly, we can consider combinations of residues of the a_i, $i \in \{1, 2, 3, 4, 6\}$, modulo π_P^M to obtain that $\mu_P(\theta_{N,a}^{-1}(V)) = \mu_P(V)$, with the set of curves with discriminant 0 counted in the combinations of residues having a Haar measure of 0. Because there are Q_P^{N+5} choices of a, the result follows. ∎

Suppose N is a positive integer. With Lemma 6.4, we can compute the density for curves that enter step 7 in the first iteration and have type I_N^*. We have that $\mu_P(Y_{N-1}) = \frac{Q_P - 1}{Q_P^{2N+10}}$, and the Haar measure in $G_P^{(3)}$ of curves that have type I_N^* is then $\frac{(Q_P-1)^2}{Q_P^{N+7}}$. Particularly, $\delta_K(I_N^*, 2, 0; P) = \delta_K(I_N^*, 4, 0; P) = \frac{(Q_P-1)^2}{2Q_P^{N+7}}$.

7 Local and Global Density Results

In Section 4, Section 5, and Section 6, we computed the local densities of Koidara types and Tamagawa numbers for $p \geq 5$, $p = 3$, and $p = 2$, respectively. The methods we used involved first removing some terms from the equations of elliptic curves with translations, and then using translations to compute the local densities. Moreover, the local densities can be expressed as rational functions. Let $\mathfrak{r}$ be a Koidara type and n be a positive integer. There exists a rational function $f(x)$ such that $\delta_K(\mathfrak{r}, n; P) = f(Q_P)$ for all $P \in M_K$. Note that $f(x)$ is the same for all global function fields K. Additionally, in [3], the rational function calculated for the local density of $\mathfrak{r}$ and n for elliptic curves in short Weierstrass form over $\mathbb{Q}_r$ for primes $r \geq 5$ is $f(x)$. In [1], the rational function calculated for the local density of $\mathfrak{r}$ and n for elliptic curves in short Weierstrass form over completions of a number field at places that lie above a prime $r \geq 5$ is also $f(x)$.

Next, we will discuss some results about local and global density, including a proof of Theorem 1.2. Particularly, we compute the density of completing at most $k \geq 0$ iterations of Tate's algorithm.

7.1 Proof of Theorem 1.2

Let U and V be the sets of elliptic curves $E \in G_P$ with Kodaira type $\mathfrak{r}$ and Tamagawa number n such that $M_P(E) = 0$ and $M_P(E) = k$, respectively. We have that U and V are open sets. Moreover, $\varphi(U)$ and $\varphi(V)$ are open sets. With this, we have that $\mu_P(U) = \mu_P(\varphi(U))$ and $\mu_P(V) = \mu_P(\varphi(V))$ for all characteristics p from Lemma 4.1, Lemma 5.1, and Lemma 6.1. Therefore, it suffices to prove that

$$\mu_P(\varphi(V)) = \frac{1}{Q_P^{10k}} \mu_P(\varphi(U)).$$

However, observe that $\varphi(U) = \phi_k(\varphi(V))$. The result then follows from Lemma 4.2, Lemma 5.3, and Lemma 6.3.

7.2 Density for Multiple Iterations

Let k be a nonnegative integer. For $P \in M_K$, let U_P^k denote the set of elliptic curves E in G_P such that $M_P(E) \geq k+1$. The following proposition is important for the proof of Theorem 7.2.

Proposition 7.1. For a nonnegative integer k and $P \in M_K$, $\mu_P(U_P^k) = \frac{1}{Q_P^{10(k+1)}}$.

Proof. From Lemma 4.2, Lemma 5.3, and Lemma 6.3 with $k+1$ as k and G_P as U, we have that

$$\mu_P(U_P^k) = \frac{1}{Q_P^{10(k+1)}} \mu_P(G_P) = \frac{1}{Q_P^{10(k+1)}}.$$

■

Theorem 7.2. Let U be the set of elliptic curves in W_S such that $M_P(E) \leq k$ for all $P \in S^C$. Then,

$$d_S(U) = \frac{1}{\zeta_K(10(k+1))} \cdot \prod_{P \in S} \left(\frac{Q_P^{10(k+1)}}{Q_P^{10(k+1)} - 1} \right).$$

Proof. For a positive integer M, let V_M be the set of elliptic curves $E \in W_S$ such that there exists $P \in S^C$ with degree at least M such that $E \in U_P^k$. From Proposition 3.3, we have that $\lim_{M\to\infty} \overline{d}_S(V_M) = 0$. Therefore, we can use Theorem 3.1 with U_P^k as U_P for $P \in S^C$. The result follows from Proposition 7.1. ■

Example 7.3. We given an example of Theorem 7.2. Let k be a nonnegative integer. Let $K = \mathbb{F}_q(t)$. Suppose P_∞ is the infinite place of $\mathbb{F}_q(t)$ and let $S = \{P_\infty\}$. Let U be the set of elliptic curves in W_S such that $M_P(E) \leq k$ for all $P \in S^C$. From Theorem 5.9 of [5], because the genus of K is 0, we have that $\zeta_K(10(k+1)) = \frac{q^{20k+19}}{(q^{10k+9}-1)(q^{10k+10}-1)}$. Because P_∞ has degree 1, from Theorem 7.2, $d_S(U) = 1 - \frac{1}{q^{10k+9}}$.

References

[1] Yunseo Choi, Sean Li, Apoorva Panidapu, and Casia Siegel, *Tamagawa products for elliptic curves over number fields*, arXiv, 2021.

[2] John Cremona and Mohammad Sadek, *Local and global densities for Weierstrass models of elliptic curves*, arXiv, 2020.

[3] Michael Griffin, Ken Ono, and Wei-Lun Tsai, *Tamagawa products of elliptic curves over* $\mathbb{Q}$, The Quarterly Journal of Mathematics **72** (2021), no. 4, 1517–1543.

[4] Giacomo Micheli, *A local to global principle for densities over function fields*, arXiv, 2017.

[5] Michael Rosen, *Number theory in function fields*, 1st ed., Springer, 2002.

[6] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, 1st ed., Springer, 1994.

[7] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV, 1975, pp. 33–52.