

ON IGUSA LOCAL ZETA FUNCTIONS OF ELLIPTIC CURVES

MARIANA CAMPBELL
ED DUBOIS
MICHAEL JOYCE
ANUSHKA KRISHNACHANDER
MARGARET ROBINSON
KIMBERLY SCHNEIDER
JASON SLEMONS

ABSTRACT. We introduce the Igusa local zeta function by describing its relationship to the Poincaré series, a generating function for the number of solutions of a polynomial in n variables mod p^e . Igusa's p -adic stationary phase formula is presented as a technique for computing local zeta functions, which are all rational functions. In this paper, we use Tate's algorithm to classify the reduction type of the special fiber of an elliptic curve by its Kodaira-Néron classification and then the p -adic stationary phase formula to explicitly determine local zeta functions for the finite reduction families: I_0 , II , III , IV , I_0^* , IV^* , III^* , II^* . The infinite families are determined in [?]. We also discuss properties of the zeta functions, such as patterns in the numerators. This work was completed as part of the Mount Holyoke Summer Mathematics Institute, an NSF funded REU Program.

1. INTRODUCTION

In 1964, Hironaka showed that a resolution of singularities always exists for an arbitrary polynomial in the characteristic 0 setting [?]. Hironaka received the Fields Medal in 1970 for this work. Using this result, Igusa showed in 1975 that the Igusa local zeta function is a rational function [?]. In 1994, Igusa introduced the p -adic stationary phase formula (SPF), a technique that allows one p -adic integral to be represented in terms of another often simpler integral [?]. This paper together with [?] proves that SPF is sufficient to determine the Igusa local zeta function for the class of non-singular algebraic curves known as elliptic curves.

2. INTRODUCTION TO THE p -ADICS

We will be interested in integrals over the p -adic numbers, \mathbb{Q}_p , and its ring of integers, \mathbb{Z}_p . The p -adic numbers arise from a peculiar p -adic absolute value on the rational numbers in exactly the same way that the real numbers arise from the usual absolute value. Hence the p -adic numbers are the completion of the rationals with respect to the p -adic absolute value.

Let p be any prime number. Then any rational number x can be represented in the following form:

$$x = a_0 p^k + a_1 p^{k+1} + a_2 p^{k+2} + \cdots, \quad \text{where } k \in \mathbb{Z}, a_i \in \mathbb{Z}/p\mathbb{Z}, \text{ and } a_0 \neq 0.$$

1991 *Mathematics Subject Classification*. Primary 11S40, 11G07.

Key words and phrases. Local zeta functions, elliptic curves.

This research is supported by the NSF, grant DMS-9732228.

We let k be called the order of x at p , $k = \text{ord}_p x$. The order of x at p is defined as the smallest power of p with a non-zero coefficient in the p -adic expansion of x . The p -adic absolute value is defined as:

$$|x|_p = \begin{cases} p^{-\text{ord}_p x} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

The p -adic absolute value induces the metric $d(x, y) = |x - y|_p$. The distance $d(x, y) \geq 0$ for all distinct rational numbers x, y as any power of p is positive. We can easily verify the metric properties of multiplicativity and the triangle inequality for $d(x, y)$. In fact, we can show that the p -adic metric has a stronger property called the ultra-metric property:

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

Since $\max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$, the triangle inequality follows from the ultra-metric property.

Completing the rationals with respect to this metric, we get the field of p -adic numbers, denoted \mathbb{Q}_p . We can show that each p -adic number can be uniquely represented by a convergent Cauchy sequence of rational numbers of the form

$$a_0 p^k + a_1 p^{k+1} + a_2 p^{k+2} + \dots \text{ with } a_i \in \mathbb{Z}/p\mathbb{Z}, k \in \mathbb{Z}.$$

Additionally, we define the p -adic integers, \mathbb{Z}_p , to be the subring of \mathbb{Q}_p of all elements which have $|x|_p \leq 1$, i.e., any p -adic number with an expansion of the form: $a_0 + a_1 p^1 + a_2 p^2 + \dots$.

3. THE IGUSA LOCAL ZETA FUNCTIONS OF ELLIPTIC CURVES

In this paper we compute the Igusa local zeta function

$$Z(t) = \int_{\mathbb{Z}_p^n} |f(x, y)|_p^s dx dy$$

where $f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$ is the Weierstrass equation of an elliptic curve for the finite reduction families in the Kodaira-Néron classification of elliptic curves modulo p . The measure that we use to integrate over \mathbb{Z}_p^n is the product measure of the Haar measures on \mathbb{Q}_p , which we normalize so that $\int_{\mathbb{Z}_p^2} dx dy = 1$. Igusa showed that this zeta function is related to a Poincaré series. Let f be the polynomial in the integrand of the zeta function. Then the Poincaré series associated to f is:

$$P(t) = \sum_{e=0}^{\infty} N_e p^{-2e} t^e$$

where N_e is the number of solutions to $f(x, y) \bmod p^e$. This series is a generating function for the N_e 's: when expanded, the coefficient of $p^{-2e} t^e$ is exactly N_e . Igusa showed that the connection between the zeta function and the Poincaré series is:

$$Z(t) = P(t) - \frac{1}{t}(P(t) - 1)$$

In 1975 when Igusa proved the rationality of his zeta function he also proved the rationality of this Poincaré series. As a result we know that the N_e 's, in general, have complicated recursive relations on them that allow the series to be summed. In this paper we will find zeta functions associated to elliptic curves which are

nonsingular cubic curves. We can then go back and find the Poincaré series via the relationship:

$$P(t) = \frac{1 - tZ(t)}{1 - t}.$$

4. THE STATIONARY PHASE FORMULA

In [?], Igusa introduced the p -adic Stationary Phase Formula (SPF), which takes its name from a similar formula in physics. Since we have the disjoint union

$$\mathbb{Z}_p^2 = \bigcup_{(a,b) \in \mathbb{F}_p^2} (a, b) + p\mathbb{Z}_p^2,$$

SPF breaks up the integral of the Igusa zeta function into three regions of integration, based on the finite number of points (x, y) where $x, y \in \mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$: the first where $f(x, y) \not\equiv 0 \pmod{p}$, the second where $f(x, y) \equiv 0 \pmod{p}$ but is nonsingular, and the third where $f(x, y) \equiv 0 \pmod{p}$ and is singular. The idea behind this dissection is that the integrals over the first two regions are simple to calculate, and often times the third can be carefully manipulated to reach the rational function for $Z(t)$. Once simplified, our SPF in two variables looks like this:

$$\begin{aligned} Z(t) = & (p^2 - |N|)(p^{-2}) + p^{-2}t(|N| - |S|) \frac{1 - p^{-1}}{1 - p^{-1}t} \\ & + \sum_{(a,b) \in S} \int_{(a+\mathbb{Z}_p) \times (b+\mathbb{Z}_p)} |f(x, y)|_p^s dx dy \end{aligned}$$

where $|N|$ is the cardinality of the set of points modulo p such that $f(x, y) \equiv 0 \pmod{p}$, and $|S|$ is the cardinality of the subset of points of N which are singular, i.e.:

$$\frac{\partial f}{\partial x}(x, y) \equiv 0 \pmod{p}, \quad \frac{\partial f}{\partial y}(x, y) \equiv 0 \pmod{p}.$$

This paper will show, using an algorithm of Tate, that SPF is sufficient to calculate the zeta function for all elliptic curves. An open problem is whether SPF is sufficient for all polynomials; no counterexample has yet been found, in part because it would be exceedingly difficult to prove without a shadow of a doubt that *no* possible manipulation of SPF will ever work.

4.1. The form of the p -adic Stationary Phase Formula. The p -adic Stationary Phase Formula gives a systematic way for computing the local zeta function. The process of SPF always takes one of the following four forms:

- The polynomial has no singular points.

The zeta function is therefore just the first two terms of the SPF. The zeta function is rational in this case because it is of the form:

$$Z(t) = (p^n - N)p^{-n} + (N - S)p^{-n}t \frac{1 - p^{-1}}{1 - p^{-1}t}$$

- The original zeta function appears as the singular integral.

The rationality of the zeta function is due to the fact that the original zeta function can be brought to the other side of the equation and solved for, leaving a rational function.

- A previously arrived at singular integral appears again as the singular integral

The rationality of the zeta function follow in a similar way to the previous case.

- The SPF process never terminates.

It is possible that the SPF process will require an infinite number of applications and will still yield a rational function. This happens in the case where we can sum the infinite series of first and second terms of SPF. If a pattern of f 's in the singular integral becomes apparent, then we should be able to find the sum.

4.2. Tate's algorithm. We have been interested primarily in the class of nonsingular (over \mathbb{Q}_p) cubic curves known as elliptic curves. A resolution modulo p is known for this class of curves. The resolution was known to Kodaira and an algorithm for classifying curves according to their mod p singularity type was given by Tate.

We begin by transforming any elliptic curve to its minimal Weierstrass form:

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$

moving its mod p singular point to $(0, 0)$ and defining the following associated quantities:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= (b_2b_6 - b_4^2)/4 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ P(T) &= T^3 + p^{-1}a_2T^2 + p^{-2}a_4T + p^{-3}a_6 \\ \text{Disc}(P) &= p^{-6}(-4a_2^3a_6 + a_2^2a_4^2 - 4a_4^3 - 27a_6^2 + 18a_2a_4a_6) \\ Q(Y) &= Y^2 + p^{-2}a_3Y - p^{-4}a_6 \end{aligned}$$

For a description of where these quantities come from, as well as a more complete understanding of this algorithm, see Silverman or Tate.

Tate's algorithm leads to the following classification scheme:

I_0	$p \nmid \Delta$
I_n	$p^n \Delta, p^{n+1} \nmid \Delta$ $p \nmid b_2, p a_3, a_4, a_6$
II	$p a_3, a_4, a_6, p b_2$ $p^2 \nmid a_6$
III	$p a_3, a_4, a_6, p b_2, p^2 a_6$ $p^3 \nmid b_8$
IV	$p a_3, a_4, a_6, p b_2, p^2 a_6, p^3 b_8$ $p^3 \nmid b_6$
I_0^*	$p a_3, a_4, a_6, p b_2, p^2 a_6, p^3 b_8, p^3 b_6$ $p a_1, a_2, p^2 a_3, a_4, p^3 a_6$ $p \nmid \text{Disc}(P)$
I_n^*	$p a_3, a_4, a_6, p b_2, p^2 a_6, p^3 b_8, p^3 b_6$ $p a_1, a_2, p^2 a_3, a_4, p^3 a_6$ $P(T)$ has a double root
IV*	$p a_3, a_4, a_6, p b_2, p^2 a_6, p^3 b_8, p^3 b_6$ $p a_1, a_2, p^2 a_3, a_4, p^3 a_6$ $P(T)$ has a triple root $p^2 a_2, p^3 a_4, p^4 a_6$ $Q(Y)$ has distinct roots
III*	$p a_3, a_4, a_6, p b_2, p^2 a_6, p^3 b_8, p^3 b_6$ $p a_1, a_2, p^2 a_3, a_4, p^3 a_6$ $P(T)$ has a triple root $p^2 a_2, p^3 a_4, p^4 a_6$ $Q(Y)$ has a double root $p^3 a_3, p^5 a_6$ $p^4 \nmid a_4$
II*	$p a_3, a_4, a_6, p b_2, p^2 a_6, p^3 b_8, p^3 b_6$ $p a_1, a_2, p^2 a_3, a_4, p^3 a_6$ $P(T)$ has a triple root $p^2 a_2, p^3 a_4, p^4 a_6$ $Q(Y)$ has a double root $p^3 a_3, p^5 a_6, p^4 a_4$ $p^6 \nmid a_6$

or, to represent it with a tree:



\dagger $p \nmid \text{Disc}(P)$, i.e. $P(t)$ has distinct roots

\ddagger $P(t)$ has a double root

\S $Q(y)$ has distinct roots

According to Tate's algorithm, any elliptic curve that ends up at (\star) has a discriminant that can have a factor of p^{12} removed from it through a translation, so the new transformed curve can be plugged through the algorithm again. Since a finite number of p 's factor out of the discriminant, the algorithm terminates.

5. THE IGUSA LOCAL ZETA FUNCTION FOR ALL REDUCTION TYPES

Type I_0 Reduction. We wish to compute the Igusa local zeta function for the polynomial $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. Hence, $f(x, y) = 0$ is an elliptic curve in Weierstrass normal form.

TYPE II REDUCTION

We now make the condition that $p^2 \nmid a_6$. We can change our region of integration by making the substitution $x = px_1$ and $y = py_1$. The singular integral over $p\mathbb{Z}_p \times p\mathbb{Z}_p$ now becomes an integral over $\mathbb{Z}_p \times \mathbb{Z}_p$. This change of variables leads to a change in measure of p^{-2} .

$$\begin{aligned} & \int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |f(x, y)|_p^s dx dy \\ &= p^{-2} \int_{\mathbb{Z}_p} \int_{\mathbb{Z}_p} |p^2y_1^2 + p^2a_1x_1y_1 + pa_3y_1 - p^3x_1^3 - p^2a_2x_1^2 - pa_4x_1 - a_6|_p^s dx_1 dy_1 \\ &= p^{-2}t \int_{\mathbb{Z}_p} |py_1^2 + pa_1x_1y_1 + a_3y_1 - p^2x_1^3 - pa_2x_1^2 - a_4x_1 - a_{6,1}|_p^s dx_1 dy_1 \end{aligned}$$

Reducing the integrand modulo p , our integral now becomes:

$$\int_{\mathbb{Z}_p \times \mathbb{Z}_p} |-a_{6,1}|_p^s = 1.$$

This gives us:

$$\int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |f(x, y)|_p^s dx dy = p^{-2}t$$

The zeta function for an elliptic curve of reduction type II has the following rational form:

$$\begin{aligned} Z(t) &= (p^2 - p)p^{-2} + (p - 1)p^{-2}t \frac{1 - p^{-1}}{1 - p^{-1}t} + p^{-2}t \\ &= \frac{1 - p^{-1} + p^{-3}t - p^{-3}t^2}{1 - p^{-1}t} \end{aligned}$$

TYPE III REDUCTION

We now impose the conditions: $p^2 \nmid a_6$ and $p^3 \nmid b_8$. From this we can see that $p^2 \nmid a_4$. This follows because $4b_8 = b_2b_6 - b_4^2$ where $p^2 \nmid b_6$ as $b_6 = a_3^2 + 4a_6$. Thus, if $p^2 \nmid b_4$, then $p^3 \nmid b_8$ which is a contradiction. Recall that $b_4 = a_1a_3 + 2a_4$. $p^2 \nmid a_4$ because if $p^2 \nmid a_4$ then $p^2 \nmid b_4$, also a contradiction. Consider the effect of these new

divisibility conditions on our singular integral.

$$\begin{aligned}
& \int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |f(x, y)|_p^s dx dy \\
&= p^{-2} \int_{\mathbb{Z}_p^2} |p^2 y_1^2 + p^2 a_1 x_1 y_1 + p a_3 y_1 - p^3 x_1^3 - p^2 a_2 x_1^2 - p a_4 x_1 - a_6|_p^s dx_1 dy_1 \\
&= p^{-2} t^2 \underbrace{\int_{\mathbb{Z}_p^2} |y_1^2 + a_1 x_1 y_1 + a_{3,1} y_1 - p x_1^3 - a_2 x_1^2 - a_{4,1} x_1 - a_{6,2}|_p^s dx_1 dy_1}_{\mathcal{I}_{S_1}}
\end{aligned}$$

Let the integrand be called $f_1(x_1, y_1)$. Consider $f_1(x_1, y_1)$ modulo p : $f_1(x_1, y_1) \equiv y_1^2 + a_{3,1} y_1 - a_{4,1} x_1 - a_{6,2}$. Let us now make the following change of variables: $\tilde{x} = y_1^2 + a_{3,1} y_1 - a_{4,1} x_1 - a_{6,2}$ and $\tilde{y} = y_1$.

Computing the Jacobian, our integral now reduces to:

$$\begin{aligned}
\mathcal{I}_{S_1} &= \int_{\mathbb{Z}_p^2} |\tilde{x}|_p^s d\tilde{x} d\tilde{y} \\
&= \int_{\mathbb{Z}_p} |\tilde{x}| d\tilde{x} \cdot \int_{\mathbb{Z}_p} d\tilde{y} \\
&= \frac{1 - p^{-1}}{1 - p^{-1}t}
\end{aligned}$$

The rational zeta function for the elliptic curve of type III reduction is:

$$\begin{aligned}
Z(t) &= (1 - p^{-1}) + (1 - p^{-1})p^{-1}t \frac{(1 - p^{-1})}{(1 - p^{-1}t)} + p^{-2}t^2 \frac{(1 - p^{-1})}{(1 - p^{-1}t)} \\
&= \frac{1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2}{1 - p^{-1}t}
\end{aligned}$$

TYPE IV REDUCTION

If we allow $p^3|b_8$, we then get $p^2|b_4$ and $p^2|a_4$. We will now consider elliptic curves with the following conditions on their coefficients: $p^2|a_6$, $p^3|b_8$, and $p^3 \nmid b_6$. Our singular integral now becomes:

$$\begin{aligned}
\int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |f(x, y)|_p^s dx dy &= p^{-2}t^2 \int_{\mathbb{Z}_p^2} |f_1(x_1, y_1)|_p^s dx_1 dy_1 \\
\mathcal{I}_{S_1} &= \int_{\mathbb{Z}_p^2} |f_1(x_1, y_1)|_p^s dx dy
\end{aligned}$$

where $f_1(x_1, y_1) \equiv y_1^2 + a_{3,1} y_1 - a_{6,2} \pmod{p}$. The discriminant of $f_1(x_1, y_1) \pmod{p}$ is precisely $a_{3,1}^2 + 4a_{6,2} = b_{6,2}$. Because $p^3 \nmid b_6$, we know that $f_1(x_1, y_1)$ is nonsingular. Therefore, $f_1(x_1, y_1)$ has distinct roots in the algebraic closure of \mathbb{Q}_p .

In \mathbb{Z}_p , $f_1(x_1, y_1)$ either has distinct roots or no roots. In the case where $b_{6,2}$ is a square modulo p , $N_1 = 2p$ and $S_1 = 0$. Applying SPF to \mathcal{I}_{S_1} :

$$\begin{aligned}\mathcal{I}_{S_1} &= (p^2 - 2p)p^{-2} + 2p^{-1}t \frac{1 - p^{-1}}{1 - p^{-1}t} \\ &= \frac{1 - 2p^{-1} + p^{-1}t}{1 - p^{-1}t}\end{aligned}$$

When $b_{6,2}$ is not a square mod p , $N_1 = 0$ and $S_1 = 0$. This gives $\mathcal{I}_{S_1} = 1$. The zeta function for case IV has two forms:

When $N_1 = 2p$:

$$Z(t) = \frac{1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - 2p^{-3}t^2 + p^{-3}t^3}{1 - p^{-1}t}$$

When $N_1 = 0$:

$$Z(t) = \frac{1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^3}{1 - p^{-1}t}$$

TYPE I_n^* REDUCTION

We now allow $p^3|b_6$. From now on, it will be the case that $p^2|a_3$ and $p^3|a_6$. This can be seen as follows: $f_1(x_1, y_1) = y_1^2 + a_1x_1y_1 + a_{3,1}y_1 - px_1^3 - a_2x_1^2 - a_{4,1}x_1 - a_{6,2} \equiv y_1^2 + a_{3,1}y_1 - a_{6,2} \pmod{p}$. Completing the square yields: $f_1(x_1, y_1) \equiv (y_1 + \frac{a_{3,1}}{2})^2 - \frac{a_{3,1}^2}{4} - a_{6,2} \pmod{p}$. Let $\tilde{y}_1 = y_1 + \frac{a_{3,1}}{2}$ and $a_{6,2} = \frac{a_{3,1}^2}{4} + a_{6,2}$. Consider $a_{6,2} = a_{6,2} + \frac{a_{3,1}^2}{4} = \frac{4a_{6,2} + a_{3,1}^2}{4} = \frac{b_{6,2}}{4} \equiv 0 \pmod{p}$ as $p^3|b_6$. Thus, $p|a_{6,2}$ and $p^3|a_6$. Since $p^3|b_6$, $p^3|a_6$, and $b_6 = a_3^2 + 4a_6$ we can now see that $p^2|a_3$. Given an elliptic curve of reduction type I_n^* , we have shown it can always be transformed to get $p|a_{6,2}$ without affecting the divisibility conditions on the other coefficients. So, $f_1(x_1, y_1) \equiv y_1^2 \pmod{p}$. Setting $f_1(x_1, y_1)$ and its partials equal to zero mod p , we see that $N_1 = p$ and $S_1 = p$. Applying SPF we get:

$$\mathcal{I}_{S_1} = (p^2 - p)p^{-2} + \int_{\mathbb{Z}_p \times p\mathbb{Z}_p} |f_1(x_1, y_1)|_p^s dx_1 dy_1.$$

We change our region of integration from $\mathbb{Z}_p \times p\mathbb{Z}_p$ to $\mathbb{Z}_p \times \mathbb{Z}_p$ by making the change of variables: $x_1 \rightarrow x_2$ and $y_1 \rightarrow py_2$. This change of variables leads to a change in measure of p^{-1} . Our singular integral becomes:

$$\int_{\mathbb{Z}_p \times p\mathbb{Z}_p} |f_1(x_1, y_1)|_p^s dx_1 dy_1 = p^{-1}t \mathcal{I}_{S_2}$$

where

$$\begin{aligned}\mathcal{I}_{S_2} &= \int_{\mathbb{Z}_p^s} |p^2y_2^2 + pa_1x_2y_2 + pa_{3,1}y_2 - px_2^3 - a_2x_2^2 - a_{4,1}x_2 - a_{6,2}|_p^s dx_2 dy_2 \\ &= \int_{\mathbb{Z}_p^2} |f_2(x_2, y_2)|_p^s dx_2 dy_2\end{aligned}$$

where $f_2(x_2, y_2) = -x_2^3 - a_{2,1}x_2^2 - a_{4,2}x_2 - a_{6,3} \pmod{p}$.

Type I_0^* Reduction. The reduction type I_0^* is defined in Tate's algorithm as the case where $f_2(x_2, y_2) \bmod p$ has distinct roots in the algebraic closure of \mathbb{Q}_p . Therefore in \mathbb{Z}_p , $f_2(x_2, y_2)$ either has distinct roots or has no roots. That is, f_2 can take one of the following three forms with $A, B, C \in \mathbb{F}_p[x_2]$:

- $f_2(x_2, y_2) = (x_2 - A)(x_2 - B)(x_2 - C) \bmod p$
- $f_2(x_2, y_2) = (x_2 - A)(x_2^2 + Bx_2 + C) \bmod p$
- $f_2(x_2, y_2)$ is irreducible over $\mathbb{F}_p[x_2]$.

As $f_2(x_2, y_2)$ is nonsingular mod p , when we compute \mathcal{I}_{S_2} we will just get the first two terms of the SPF with the appropriate N_2 according to which of the three cases mentioned above we are in. That is,

$$\mathcal{I}_{S_2} = (p^2 - N_2)p^{-2} + N_2p^{-2}t \frac{1 - p^{-1}}{1 - p^{-1}t}$$

where $N_2 = 3p$ if f_2 has 3 distinct roots in \mathbb{Z}_p , $N_2 = p$ if f_2 has one root in \mathbb{Z}_p , and $N_2 = 0$ if f_2 is irreducible. The zeta functions for curves of reduction type I_0^* have the following three forms.

When $N_2 = 3p$:

$$Z(t) = \frac{1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 - 2p^{-4}t^3 + 2p^{-4}t^4}{1 - p^{-1}t}$$

When $N_2 = p$:

$$Z(t) = \frac{1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2}{1 - p^{-1}t}$$

When $N_2 = 0$:

$$Z(t) = \frac{1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 + p^{-4}t^3 - p^{-4}t^4}{1 - p^{-1}t}$$

Type I_1^* Reduction. The reduction type I_1^* is defined in Tate's algorithm as the case where $f_2(x_2, y_2)$ has a double root and a simple root mod p . Suppose that $f_2(x_2, y_2) = (x_2 - \alpha)^2(x_2 - \beta)$. Making the translation $x_2 \rightarrow x_2 + \alpha$ and $y_2 \rightarrow y_2$, we shift the root to $(0, y)$. From this translation, we discover that $p^3|a_4$ and $p^4|a_6$. Note that $f_2(x_2, y_2) \equiv x_2^3 + a_{2,1}x_2^2 + a_{4,2}x_2 + a_{6,3} \equiv x_2^2(x_2 - (\beta - \alpha)) \equiv x_2^3 - (\beta - \alpha)x_2^2$. By equating coefficients, we see that $a_{4,2} \equiv 0 \bmod p$ and $a_{6,3} \equiv 0 \bmod p$. If $p^2|a_2$, then f_2 would have a triple root, which is not considered in this case. For I_1^* reduction, $p^2 \nmid a_2$.

$$\mathcal{I}_{S_2} = \int_{\mathbb{Z}_p \times \mathbb{Z}_p} |f_2(x_2, y_2)|_p^s dx_2 dy_2$$

where $f_2(x_2, y_2) \equiv x_2^3 + a_{2,1}x_2^2 \bmod p$. Setting f_2 and its partials equal to zero mod p , we find $N_2 = 2p$ and $S_2 = p$. Applying SPF to \mathcal{I}_{S_2} yields:

$$\mathcal{I}_{S_2} = (p^2 - 2p)p^{-2} + p^{-1}t \frac{1 - p^{-1}}{1 - p^{-1}t} + \int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |f_2(x_2, y_2)|_p^s dx_2 dy_2$$

We change the region of integration from $p\mathbb{Z}_p \times \mathbb{Z}_p$ to $\mathbb{Z}_p \times \mathbb{Z}_p$ by making the change of variables $x_2 \rightarrow px_3$ and $y_2 \rightarrow y_3$ which cause a change in measure of p^{-1} . Now

our singular integral is equal to:

$$\begin{aligned} & p^{-1} \int_{\mathbb{Z}_p \times \mathbb{Z}_p} |py_3^2 + pa_1x_3y_3 + a_{3,1}y_3 - p^3x_3^3 - p^2a_{2,1}x_3^2 - pa_{4,2}x_3 - a_{6,3}|_p^s dx_3 dy_3 \\ &= p^{-1}t \int_{\mathbb{Z}_p^s} |y_3^2 + a_1x_3y_3 + a_{3,2}y_3 - p^2x_3^3 - pa_{2,1}x_3^2 - a_{4,2}x_3 - a_{6,4}|_p^s dx_3 dy_3 \end{aligned}$$

We will call $f_3(x_3, y_3) = y_3^2 + a_1x_3y_3 + a_{3,2}y_3 - p^2x_3^3 - pa_{2,1}x_3^2 - a_{4,2}x_3 - a_{6,4} \equiv y_3^2 + a_{3,2}y_3 - a_{6,4} \pmod{p}$. We will let \mathcal{I}_{S_3} be the integral of f_3 over the region \mathbb{Z}_p^2 . Tate's algorithm states that I_1^* is the case where $f_3(x_3, y_3)$ has distinct roots in the algebraic closure of \mathbb{Q}_p . Over \mathbb{Z}_p , it either has distinct roots or no roots. In either case, f_3 is nonsingular. Therefore,

$$\mathcal{I}_{S_3} = (p^2 - N_3)p^{-2} + N_3p^{-2}t \frac{1 - p^{-1}}{1 - p^{-1}t}$$

where $N_3 = 2p$ if f_3 has distinct roots and $N_3 = 0$ if f_3 is irreducible. The zeta function for the case of distinct roots is:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ (p - 1)p^{-2}t(1 - p^{-1} + p^{-2}t^2((p^{-2}p^2 - p) \\ &+ p^{-1}t((p^{-2}(p^2 - 2p)) + \frac{(2p - p)p^{-2}t(1 - p^{-1})}{1 - p^{-1}t} \\ &+ p^{-1}t((p^2 - 2p)p^{-2} + \frac{((2p)p^{-2}t)(1 - p^{-1})}{1 - p^{-1}t}))))). \end{aligned}$$

The zeta function for the case of no roots is:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ \frac{(p - 1)p^{-2}t(1 - p^{-1})}{1 - p^{-1}t} + p^{-2}t^2((p^{-2} - (p^2 - p)) \\ &+ p^{-1}t((p^2 - 2p) + \frac{(2p - p)p^{-2}t(1 - p^{-1})}{1 - p^{-1}t} + p^{-1}t)). \end{aligned}$$

Type I_2^* Reduction. I_2^* will be the case where $f_3 \equiv y_3^2 + a_{3,2}y_3 - a_{6,4}$ has a double root. Make the translation $y_3 \rightarrow y_4 + \beta$ and $x_3 \rightarrow x_4$ to get $f_3 \equiv y_4^2 \pmod{p}$. Equating coefficients we see that $p^3|a_3$ and $p^5|a_6$. Recall that $f_3(x_3, y_3) = y_3^2 + a_1x_3y_3 - p^2x_3^3 - a_{2,1}px_3^2 + a_{3,2}y_3 - a_{4,2}x_3 - a_{6,4}$. Make the change of variables $x_3 \rightarrow x_4$ and $y_3 \rightarrow py_4$. Our singular integral, \mathcal{I}_{S_3} now becomes:

$$p^{-1}t \int_{\mathbb{Z}_p^2} |py_4^2 + a_1x_4y_4 - px_4^3 - a_{2,1}x_4^2 + a_{3,2}y_4 - a_{4,3}x_4 - a_{6,5}| dx_4 dy_4$$

We will call the integrand $f_4(x_4, y_4)$ and we will consider it mod p . $f_4(x_4, y_4) = -a_{2,1}x_4^2 - a_{4,3}x_4 - a_{6,5} \pmod{p}$. As $f_4 \pmod{p}$ is a quadratic in x_4 , we consider the two cases: f_4 has distinct roots mod p and f_4 has no roots mod p . If f_4 has distinct roots, then $N_3 = 2p$ and $S_3 = 0$. If f_4 has no roots, then $N_3 = 0$ and $S_3 = 0$.

The zeta function for the case of distinct roots is:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ \frac{(p - 1)p^{-2}t(1 - p^{-1})}{1 - p^{-1}t} + p^{-2}t^2(p^{-2}(p^2 - p) \\ &+ p^{-1}t((p^2 - p)p^{-2} + p^{-1}t((p^2 - 2p)p^{-2} \\ &+ 2p^{-1}t \frac{(1 - p^{-1})}{1 - p^{-1}t}))) \end{aligned}$$

In the case where f_4 has no roots, then the zeta function is:

$$\begin{aligned} Z(t) &= (p^2 - p)p^{-2} + \frac{(p-1)p^{-2}(1-p^{-1})}{1-p^{-1}t} + p^{-2}t^2(p^{-2}(p^2 - p) \\ &+ p^{-1}t((p^2 - p)p^{-2} + p^{-1}t)). \end{aligned}$$

If we continue to look at the cases of distinct roots and no roots versus double roots in the alternating quadratic equations in x and y , we will get the general form for the zeta function in the I_n^* case. In both cases, the denominator of the zeta function will be $1 - p^{-1}t$. The numerator for the case of no roots is: $1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 - p^{-4}t^3 + p^{-4}t^4 + p^{-5}t^4 - p^{-5}t^5 + \dots + (p^{-(n+4)}t^{(n+3)} - p^{-(n+4)}t^{(n+4)})$. The numerator of the zeta function for the case $N = 2p$ is: $1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 - p^{-4}t^3 + p^{-4}t^4 + p^{-5}t^4 - p^{-5}t^5 + \dots + (-p^{-(n+4)}t^{(n+3)} + p^{-(n+4)}t^{(n+4)})$.

TYPE IV* REDUCTION

Suppose now that $f_2(x_2, y_2)$ has a triple root. So, $f_2(x_2, y_2)$ factors as $(x - \alpha)^3$ which is congruent to $-x_2^3 - a_{2,1}x_2^2 - a_{4,2}x_2 - a_{6,3}$ modulo p . Make the translation $x_2 \rightarrow x_2 + \alpha$ and $y_2 \rightarrow y_2$ which gives us $f_2 \equiv -x_2^3 \pmod{p}$. Equating coefficients, we see that $p^2|a_2, p^3|a_4$, and $p^4|a_6$. In terms of $f_2(x_2, y_2)$, the singular integral is now:

$$\mathcal{I}_{S_2} = \int_{\mathbb{Z}_p \times \mathbb{Z}_p} |py_2^2 + a_1x_2y_2 + a_{3,1}y_2 - x_2^3 - a_{2,1}x_2^2 - a_{4,2}x_2 - a_{6,3}|_p^s dx_2 dy_2$$

By considering f_2 and its partials congruent to 0 mod p , we learn that $N_2=p$ and there are p singular points. Therefore the middle term of the SPF vanishes. Making the substitution $x_2 = px_3$ and $y_2 = y_3$ changes the region of integration for the singular integral to \mathbb{Z}_p^2 and causes a change in measure of p^{-1} . Our integral is:

$$\begin{aligned} &\int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |f_2(x_2, y_2)|_p^s dx_2 dy_2 \\ &= p^{-1} \int_{\mathbb{Z}_p^2} |py_3^2 + pa_1x_3y_3 + a_{3,1}y_3 - p^3x_3^3 \\ &\quad - p^2a_{2,1}x_3^2 - pa_{4,2}x_3 - a_{6,3}|_p^s dx_3 dy_3 \\ &= p^{-1}t \int_{\mathbb{Z}_p^2} |y_3^2 + a_1x_3y_3 + a_{3,2}y_3 - p^2x_3^3 \\ &\quad - pa_{2,1}x_3^2 - a_{4,2}x_3 - a_{6,4}|_p^s dx_3 dy_3 \end{aligned}$$

where $f_3(x_3, y_3) = y_3^2 + a_1x_3y_3 + a_{3,2}y_3 - p^2x_3^3 - pa_{2,1}x_3^2 - a_{4,2}x_3 - a_{6,3}$. Let \mathcal{I}_{S_3} be:

$$\int_{\mathbb{Z}_p \times \mathbb{Z}_p} |f_3(x_3, y_3)|_p^s dx_3 dy_3$$

where $f_3 \equiv y_3^2 + a_{3,2}y_3 - a_{6,4} \pmod{p}$. If $f_3(x_3, y_3)$ has no roots or distinct roots, then we are in the case of IV* where: $N_3 = 0$ in the case of no roots and $N_3 = 2p$ in the case of distinct roots. Therefore, our singular integral can be evaluated as:

$$\mathcal{I}_{S_3} = (p^2 - N_3)p^{-2} + N_3p^{-2}t \frac{1 - p^{-1}}{1 - p^{-1}t}$$

Our zeta function associated to reduction of type IV* (distinct roots) is:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ (p-1)p^{-2}t \frac{1-p^{-1}}{1-p^{-1}t} \\ &+ p^{-2}t^2((p^2-p)p^{-2} + p^{-1}t((p^2-p)p^{-2} \\ &+ p^{-1}t((p^2-2p)p^{-2} + 2p^{-1}t \frac{(1-p^{-1})}{1-p^{-1}t}))) \end{aligned}$$

The zeta function associated to reduction of type IV* (no roots) is:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ (p-1)p^{-2}t \frac{(1-p^{-1})}{1-p^{-1}t} \\ &+ p^{-2}t^2((p^2-p)p^{-2} \\ &+ p^{-1}t((p^2-p)p^{-2} + p^{-1}t)) \end{aligned}$$

If we assume that $f_3(x_3, y_3) = y_3^2 + a_{3,2}y_3 - a_{6,4}$ has a double root (which we will translate to the origin $y=0$) we get the divisibility conditions: $p^3|a_3$ and $p^5|a_6$ by equating coefficients. If, in addition, we assume that $p^4 \nmid a_4$, then we are in case III*

TYPE III* REDUCTION

With our new divisibility conditions, $f_3 \equiv y_3^2 + a_{3,2}y_3 - a_{6,4} \equiv y_3^2 \pmod{p}$. $N_3 = p$ and we also have that $S_3 = p$ by considering f_3 and its partial derivatives. Make the change of variables: $x_3 = x_4$ and $y_3 = py_4$ to get:

$$\begin{aligned} p^{-1} \int_{\mathbb{Z}_p \times \mathbb{Z}_p} &|p^2y_4^2 + a_1px_4y_4 - p^2x_4^3 - pa_{2,1}x_4^2 + a_{3,2}py_4 - a_{4,2}x_4 - a_{6,4}|_p^s dx_4 dy_4 \\ p^{-1}t \int_{\mathbb{Z}_p \times \mathbb{Z}_p} &|py_4^2 + a_1x_4y_4 - px_4^3 - a_{2,1}x_4^2 + a_{3,2}y_4 - a_{4,3}x_4 - a_{6,5}|_p^s dx_4 dy_4 \end{aligned}$$

Let \mathcal{I}_{S_4} be the integral above. Is \mathcal{I}_{S_4} a singular integral? Consider the integrand, $f_4(x_4, y_4)$, modulo p . $f_4(x_4, y_4) = -a_{4,3}x_4 - a_{6,5} \pmod{p}$. Considering the partials of f_4 , we note that the partial of f_4 with respect to x_4 is $-a_{4,3}$ which is never congruent to zero mod p because $p^4 \nmid a_4$. So our integral is not singular. Therefore, we get the first two terms of SPF with $N_4 = p$. The zeta function associated to type III* reduction is:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ (p-1)p^{-2}t \frac{(1-p^{-1})}{1-p^{-1}t} + p^{-2}t^2((p^2-p)p^{-2} \\ &+ p^{-1}t((p^2-p)p^{-2} + p^{-2} + p^{-1}t((p^2-p)p^{-2} \\ &+ p^{-1}t((p^2-p)p^{-2} + p^{-1}t \frac{1-p^{-1}}{1-p^{-1}t}))))). \end{aligned}$$

TYPE II* REDUCTION

If we make the condition that $p^4|a_4$ but $p^6 \nmid a_6$, then we are in case II*. Consider \mathcal{I}_{S_4} :

$$\mathcal{I}_{S_4} = \int_{\mathbb{Z}_p \times \mathbb{Z}_p} |py_4^2 + a_1x_4y_4 - px_4^3 - a_{2,1}x_4^2 + a_{3,2}y_4 - a_{4,3}x_4 - a_{6,5}|_p^s dx_4 dy_4$$

With our new divisibility conditions, we see: $f_4(x_4, y_4) \equiv a_{6,5} \pmod{p}$. Because $p^6 \nmid a_6$, $|a_{6,5}|=1$. This implies that $|\int_{\mathbb{Z}_p^2} dx_4 dy_4| = 1$. The zeta function associated to type II* reduction is:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ (p-1)p^{-2}t \frac{(1-p^{-1})}{1-p^{-1}t} \\ &+ p^{-2}t^2((p^2-p)p^{-2} + p^{-1}t((p^2-p)p^{-2} \\ &+ p^{-1}t((p^2-p)p^{-2} + p^{-1}t))) \end{aligned}$$

We have entirely worked our way through Tate's algorithm. If $p^6|a_6$, then the equation we started with was not minimal and we could repeat the above algorithm. Since only finitely many p 's can be factored out of the discriminant, Tate's algorithm will terminate. Therefore, we have found the Igusa local zeta functions associated to elliptic curves of all possible mod p singularity types.

6. THE END OF TATE'S ALGORITHM

We have a curve $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ with the conditions: $p|a_1$, $p^3|a_3$, $p^2|a_2$, $p^4|a_4$, $p^6|a_6$. We make the change of variables so that: $f(x, y) = y^2 - 4x^3 - b_2x^2 - 2b_4x - b_6$. When we do this, we change our region of integration. We must apply SPF appropriately to the integral that results from this change of variables to determine what factor should be in front of the integral when we go through Tate's algorithm with the new polynomial. From our divisibility conditions, we see that: $p^2|b_2$, $p^4|b_4$, $p^6|b_6$. We apply SPF for the first time to the integral:

$$(6.1) \quad Z(t) = \int_{\mathbb{Z}_p^2} |y^2 - 4x^3 - b_2x^2 - 2b_4x - b_6|_p^s dx dy$$

Considering the integrand modulo p , we have: $y^2 - 4x^3 \equiv 0$. There are p solutions to this equation, one of which is singular. It is obvious that $(0,0)$ is the only singular solution. There are $p-1$ other values of x ($1, \dots, p-1$). For $(p-1)/2$ of these values, x is not a square mod p , while $4x^2$ clearly is a square, so $4x^3$ will not be a square mod p , and thus each of these $(p-1)/2$ x values gives no solution. For the other $(p-1)/2$ values, x is a square mod p . Let $x = a^2$. Then $4x^3 = (2x)^2 = a^2(2a^2)^2 = 4a^6$, so this x value gives two solutions: $(a^2, 2a^3)$, $(a^2, -2a^3)$. This gives $p-1$ more solutions. The above argument is the explanation for why there are p solutions to $y^2 - 4x^3 = 0$ modulo p , with one of them being singular.

So, now we use SPF to see:

$$\begin{aligned} Z(t) = (p^2 - p)p^{-2} &+ (p-1)p^{-2}t \frac{1-p^{-1}}{1-p^{-1}t} \\ &+ \int_{(p\mathbb{Z}_p)^2} |y^2 - 4x^3 - b_2x^2 - 2b_4x - b_6|_p^s dx dy \end{aligned}$$

We let $x = px_1$ and $y = py_1$ to get the following zeta function:

$$\begin{aligned} Z(t) &= (1 - p^{-1}) + (1 - p^{-1})p^{-1}t \frac{1 - p^{-1}}{1 - p^{-1}t} \\ &\quad + p^{-2}t^2 \int_{\mathbb{Z}_p^2} |y_1^2 - 4px_1^3 - b_2x_1^2 - 2b_{4,1}x_1 - b_{6,2}|_p^s dx dy \\ &= A_1 + p^{-2}t^2 \mathcal{I}_1. \end{aligned}$$

where

$$A_1 = 1 - p^{-1} + (1 - p^{-1})p^{-1}t \frac{1 - p^{-1}}{1 - p^{-1}t}$$

is the first two terms of the SPF and

$$\mathcal{I}_1 = \int_{\mathbb{Z}_p^2} |y_1^2 - 4px_1^3 - b_2x_1^2 - 2b_{4,1}x_1 - b_{6,2}|_p^s dx_1 dy_1$$

is our new integral to evaluate, having pulled two p 's out of the integral after our change of variables. We can now apply SPF a second time for \mathcal{I}_1 . Our equation is $y_1^2 \equiv 0 \pmod{p}$. There are p solutions to this equation— $(x, 0)$, where x ranges over \mathbb{F}_p . All of the solutions are singular. Note that $|N| - |S| = 0$ and therefore the second term of this SPF vanishes. Now, \mathcal{I}_1 becomes:

$$\mathcal{I}_1 = (1 - p^{-1}) + p^{-1}t \int_{\mathbb{Z}_p \times p\mathbb{Z}_p} |y_1^2 - 4px_1^3 - b_2x_1^2 - 2b_{4,1}x_1 - b_{6,2}|_p^s dx_1 dy_1$$

Note that our region of integration for the singular integral is $\mathbb{Z}_p \times p\mathbb{Z}_p$ because all x 's give a singular point when $y \equiv 0 \pmod{p}$. We make the change of variables $y_1 = py_2$ to get the following integral:

$$\mathcal{I}_1 = (1 - p^{-1}) + p^{-1}t \int_{\mathbb{Z}_p^2} |py_2^2 - 4x_2^3 - b_{2,1}x_2^2 - 2b_{4,2}x_2 - b_{6,3}|_p^s dx_2 dy_2.$$

So

$$\begin{aligned} Z(t) &= A_1 + p^{-2}t^2 \mathcal{I}_1 \\ &= A_1 + A_2 + p^{-3}t^3 \mathcal{I}_2 \end{aligned}$$

where

$$A_2 = p^{-2}t^2(1 - p^{-1})$$

and

$$\mathcal{I}_2 = \int_{\mathbb{Z}_p^2} |py_2^2 - 4x_2^3 - b_{2,1}x_2^2 - 2b_{4,2}x_2 - b_{6,3}|_p^s dx_2 dy_2$$

We now apply SPF for a third time to evaluate \mathcal{I}_2 . Our integrand becomes $-4x_2^3 \equiv 0 \pmod{p}$. There are p solutions to this equation: $(0, y)$ and all of them are singular. Therefore,

$$\mathcal{I}_2 = (p^2 - p)p^{-2} + \int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |py_2^2 - 4x_2^3 - b_{2,1}x_2^2 - 2b_{4,2}x_2 - b_{6,3}|_p^s dx_2 dy_2$$

We make the change of variables $x_2 = px_3$ to get the following integral:

$$\mathcal{I}_2 = (1 - p^{-1}t) + p^{-1}t \int_{\mathbb{Z}_p^2} |y_3^2 - 4p^2x_3^3 - b_2x_3^2 - 2b_{4,2}x_3 - b_{6,4}|_p^s dx_3 dy_3.$$

So,

$$\begin{aligned} Z(t) &= A_1 + A_2 + p^{-3}t^3\mathcal{I}_2 \\ &= A_1 + A_2 + A_3 + p^{-4}t^4\mathcal{I}_3 \end{aligned}$$

with

$$\begin{aligned} A_3 &= p^{-3}t^3(1 - p^{-1}) \quad \text{and} \\ \mathcal{I}_3 &= \int_{\mathbb{Z}_p^2} |y_3^2 - 4p^2x_3^3 - b_2x_3^2 - 2b_{4,2}x_3 - b_{6,4}|_p^s dx_3 dy_3 \end{aligned}$$

We apply SPF a fourth and final time for \mathcal{I}_3 . Our integrand is $y_3^2 \equiv 0 \pmod{p}$. So we have p solutions, all singular. This gives:

$$\mathcal{I}_3 = (p^2 - p)p^{-2} + \int_{\mathbb{Z}_p \times p\mathbb{Z}_p} |y_3^2 - 4p^2x_3^3 - b_2x_3^2 - 2b_{4,2}x_3 - b_{6,4}|_p^s dx_3 dy_3$$

We change our variables so that $y_3 = py_4$ to get the following:

$$\mathcal{I}_3 = (1 - p^{-1}) + p^{-1}t^2 \int_{\mathbb{Z}_p^2} |y_4^2 - 4x_4^3 - b_{2,2} - 2b_{4,4}x_4 - b_{6,6}|_p^s dx_4 dy_4$$

Therefore,

$$\begin{aligned} Z(t) &= A_1 + A_2 + A_3 + p^{-4}t^4\mathcal{I}_3 \\ &= A_1 + A_2 + A_3 + A_4 + p^{-5}t^6\mathcal{I}_4 \end{aligned}$$

where

$$\mathcal{I}_4 = \int_{\mathbb{Z}_p^2} |y_4^2 - 4x_4^3 - b_{2,2}x_4^2 - 2b_{4,4}x_4 - b_{6,6}|_p^s dx_4 dy_4$$

is the integral we were originally looking for. Let us now rename \mathcal{I}_4 as Z^* . Z^* will be our zeta function for when we factor out p 's in our coefficients as Tate's algorithm directs us. This gives us:

$$Z(t) = A_1 + A_2 + A_3 + A_4 + p^{-5}t^6Z^*$$

If we substitute in the values of the A_i , we get:

$$\begin{aligned} Z(t) &= (1 - p^{-1})\left(1 + \frac{(1 - p^{-1})p^{-1}t}{1 - p^{-1}t}\right) + p^{-2}t^2 + p^{-3}t^3 \\ &\quad + p^{-4}t^4 + p^{-5}t^6Z^* \end{aligned}$$

Thus, we can recover our zeta function from the one with smaller coefficients via this recursion formula.

7. NUMERATORS OF THE ZETA FUNCTIONS

Now that we have shown it is possible to find the zeta functions associated with elliptic curves using only the SPF method, we would like to study properties of the

numerators of the zeta functions we found. Here is a summary of the numerators of the zeta functions obtained for all reduction types modulo p .

$$\begin{aligned}
I_0 : Z(t) &= 1 - p^{-1}t - p^{-2}N + p^{-2}tN \\
II : Z(t) &= 1 - p^{-1} + p^{-3}t - p^{-3}t^2 \\
III, III^* : Z(t) &= 1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 \\
IVa) : Z(t) &= 1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^3 \text{ when } ac(b_6) \text{ is not a square modulo } p \\
&\text{or} \\
IVb) : Z(t) &= 1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - 2p^{-3}t^2 + p^{-3}t^3 \text{ when } ac(b_6) \text{ is a square modulo } p \\
IV^*a) : Z(t) &= 1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 + p^{-5}t^4 - p^{-5}t^5 \text{ when } ac(b_6) \text{ is not a square modulo } p \\
&\text{or} \\
IV^*b) : Z(t) &= 1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 - p^{-5}t^4 + p^{-5}t^5 \text{ when } ac(b_6) \text{ is a square modulo } p \\
II^* : Z(t) &= 1 - p^{-1} - p^{-2}t + p^{-2}t^2 + p^{-3}t - p^{-3}t^2 + p^{-6}t^5 - p^{-6}t^6
\end{aligned}$$

8. WILL SPF ALWAYS SUFFICE?

Hironaka's result in 1964 addresses the existence of a resolution of singularities in the characteristic 0 setting. His proof only supplied the existence and not an algorithm for finding the resolutions. Historically, resolutions for algebraic curves have been known since the middle of the last century. These resolutions are given by the process of "blowing up" the singular points. Currently, there is no known algorithm for finding resolutions for general polynomials modulo p . It is believed that if an algorithm exists for finding resolutions modulo p , then SPF will suffice for finding the Igusa local zeta function.

REFERENCES

- [1] H. Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero. I-II, *Ann. Math.*, 79 (1964), 109-326.
- [2] J.-I. Igusa, Complex powers and asymptotic expansions. I, *Crelles J. Math.*, 268/269 (1974), 110-130; II, *ibid.*, 278/279 (1975), 307-321.
- [3] J.-I. Igusa, *A stationary phase formula for p-adic integrals and its applications*, Algebraic geometry and its applications, Springer-Verlag, (1994), 175-194
- [4] D. Meuser, *On the poles of a local zeta function for curves*, *Invent. Math.* **73** (1983), 445-465.
- [5] D. Meuser and M. Robinson, *The Igusa local zeta function of elliptic curves*, *Math. Comp.*, to appear.
- [6] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag (1994).
- [7] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, *Modular Functions of One Variable IV*, Lect. Notes in Math. 476, B.J. Birch and W. Kuyk, eds., Springer-Verlag, Berlin (1975), 33-52
- [8] W. Veys, *On the poles of Igusa's local zeta function for curves*, *J. London Math. Soc.* **41** (1990), 27-32.

MOUNT HOLYOKE COLLEGE, SOUTH HADLEY, MA 01075

E-mail address: robinson@mtholyoke.edu