Computing the average root number of a one-parameter family of elliptic curves defined over $\mathbb{Q}$

Iakovos Jake Chinis

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Mathematics) at
Concordia University
Montreal, Quebec, Canada

August 2017

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: Iakovos Jake Chinis

Entitled: Computing the average root number of a one-parameter family of elliptic curves defined over $\mathbb{Q}$

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Hershy Kisilevsky

_____ Examiner
Dr. Giovanni Rosso

_____ Supervisor
Dr. Chantal David

Approved by _____
Yogendra P. Chaubey, Chair
Department of Mathematics and Statistics

_____ 2017

_____
André Roy, Dean
Faculty of Arts and Science

ABSTRACT

Computing the average root number of a one-parameter family of elliptic curves defined over $\mathbb{Q}$

Iakovos Jake Chinis

The root number w of an elliptic curve defined over $\mathbb{Q}$ has an intrinsic definition as an infinite product of *local root numbers* w_p, over all places p of $\mathbb{Q}$, with $w_p = \pm 1$ for all p and such that $w_p = 1$ for all but finitely-many p. By considering a one-parameter family of elliptic curves defined over $\mathbb{Q}$, we might ask ourselves if there is any bias in the distribution (or parity) of the root numbers at each specialization.

From the work of Helfgott in his Ph.D. thesis, we know (at least conjecturally) that the average root number of an elliptic curve defined over $\mathbb{Q}(T)$ is zero as soon as there is a place of multiplicative reduction over $\mathbb{Q}(T)$ other than $-\deg$.

In this paper, we are concerned with elliptic curves defined over $\mathbb{Q}(T)$ with no place of multiplicative reduction over $\mathbb{Q}(T)$, except possibly at $-\deg$. More precisely, we use the work of Helfgott to compute the average root number of an explicit family of elliptic curves defined over $\mathbb{Q}$ and show that this family is "parity-biased" infinitely-often.

Acknowledgments

First and foremost, I thank my supervisor, Chantal David, for her unwavering support over the last four years: from my first research experience, to my master's degree, and everything in between, Chantal has always believed in me, even when I did not, and I will always be indebted to her.

Then, in no particular order, I thank: Christophe Delaunay, for verifying my calculations with the use of the PARI/GP software [PAR16]; Hershy Kisilevsky, for a very useful discussion during a critical point in my work, for everything he's taught me over the years, and for his undeniable patience; my office mates in LB-936, for putting up with me and my insufferable pessimism and for listening to me vent and complain every other day for the last two years; consequently, I apologize to my office mates in LB-936, for putting up with me and my insufferable pessimism and for listening to me vent and complain every other day for the last two years; I especially thank Ryan Gibara, Patrick Meisner, and JB Nam, for their thoughts and comments on all my work.

Finally, I thank my family (both actual and metaphorical), for their support during all of my studies and without whom I might actually starve.

Contents

Chapter 1

Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. For every prime p, let $\tilde{E}_p$ denote the reduction of E modulo p and set $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$, where $\#\tilde{E}_p(\mathbb{F}_p)$ denotes the number of $\mathbb{F}_p$-points on $\tilde{E}_p$. The L-series associated to E is defined by the Euler product

$$L(s,E) := \prod_{\substack{p \text{ prime} \\ p|\Delta}} (1 - a_p p^{-s})^{-1} \prod_{\substack{p \text{ prime} \\ p\nmid\Delta}} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where Δ is the discriminant of E. It is well known that the product defining $L(s,E)$ converges and gives rise to an analytic function, provided $\Re(s) > \frac{3}{2}$, which follows from Hasse's bound: $|a_p| \leq 2\sqrt{p}$; we refer the reader to [Sil09]. The Modularity Theorem [Wil95] tells us that much more is true; namely,

$$\Lambda(s,E) := N_E^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(s,E),$$

has an analytic continuation to the entire complex plane and satisfies the functional equation

$$\Lambda(s,E) = w\Lambda(2-s,E),$$

for some $w = w_E = \pm 1$, where $N_E = N_{E/\mathbb{Q}}$ is the conductor of E and where $\Gamma(s) := \int_0^\infty t^{s-1}\,\mathrm{e}^{-t}\,dt$ is the Gamma function. We call w the *root number of* E.

In this paper, we use the techniques developed by Rizzo [Riz03] and generalized by Helfgott [Hel09] to compute the average root number of an explicit family of elliptic curves defined over $\mathbb{Q}$. To do so, we implement the methods outlined in [BDD16].

By a family of elliptic curves defined over $\mathbb{Q}$, we mean an elliptic curve defined over $\mathbb{Q}(T)$; equivalently, it is a one-parameter family of elliptic curves given by a Weierstrass equation

$$\mathcal{F} : y^2 = x^3 + a_2(T)x^2 + a_4(T)x + a_6(T),$$

for some $a_2(T), a_4(T), a_6(T) \in \mathbb{Z}[T]$. For every $t \in \mathbb{Z}$, we let $\mathcal{F}(t)$ denote the specialization of $\mathcal{F}$ at t and note that $\mathcal{F}(t)$ defines an elliptic curve for all but finitely-many t. Moreover, the map which sends $\mathcal{F}$ to $\mathcal{F}(t)$ is injective for all

but finitely-many t (Silverman's Specialization Theorem, [Sil83]). From here, we let

$$\varepsilon_{\mathcal{F}}(t) := \begin{cases} \text{the root number of } \mathcal{F}(t) & \text{if } \mathcal{F}(t) \text{ is an elliptic curve,} \\ 0 & \text{otherwise,} \end{cases}$$

and define the *average root number of $\mathcal{F}$ over $\mathbb{Z}$* by

$$\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) := \lim_{T\to\infty} \frac{1}{2T} \sum_{|t|\leq T} \varepsilon_{\mathcal{F}}(t),$$

provided the limit exists.

In [Hel09], Helfgott showed (conditionally, and unconditionally in some cases) that $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = 0$ whenever $\mathcal{F}$ has a place of multiplicative reduction over $\mathbb{Q}(T)$ other than $-\deg$. In order to make the statement precise, we first state the following conjectures:

Conjecture 1.0.1 (Chowla's Conjecture)**.** *Let P be a squarefree polynomial with integer coefficients. Then,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\leq N} \lambda(P(n)) = 0,$$

where $\lambda(n) := \prod_{p|n}(-1)^{\nu_p(n)}$ is Liouville's function and where $\nu_p(n)$ denotes the p-adic valuation of n.

Remark 1.0.1. *By "Strong Chowla's Conjecture" for a polynomial P, we mean that Chowla's Conjecture holds for $P(ax+b)$ for all $a, b \in \mathbb{Z}, a \neq 0$.*

Conjecture 1.0.2 (Squarefree Sieve Conjecture)**.** *Let P be a squarefree polynomial with integer coefficients. Then,*

$$\lim_{N\to\infty} \frac{1}{N} \#\{1 \leq n \leq N : \exists \text{ prime } p > \sqrt{N} \text{ s.t. } p^2 | P(n)\} = 0.$$

Proposition 1.0.1 ([Hel09])**.** *Let $\mathcal{F}$ be a family of elliptic curves defined over $\mathbb{Q}$. Let $M_{\mathcal{F}}(T)$ and $B_{\mathcal{F}}(T)$ be the polynomials defined by*

$$M_{\mathcal{F}}(T) := \prod_{\substack{\nu \text{ mult.} \\ \nu \neq -\deg}} Q_\nu(T), \qquad B_{\mathcal{F}}(T) := \prod_{\substack{\nu \text{ quite bad} \\ \nu \neq -\deg}} Q_\nu(T),$$

where the products are over all places ν of $\mathbb{Q}(T)$ for which $\mathcal{F}$ has multiplicative reduction over $\mathbb{Q}(T)$ and quite bad [1] reduction over $\mathbb{Q}(T)$, respectively, and where $Q_\nu(T)$ is the polynomial associated to ν. Then, for all but finitely-many $t \in \mathbb{Z}$,

$$\varepsilon_{\mathcal{F}}(t) = \mathrm{sgn}(g_\infty(t))\lambda(M_{\mathcal{F}}(t)) \prod_{p \text{ prime}} g_p(t),$$

where g_∞ is a polynomial, $\mathrm{sgn}(g_\infty(t))$ denotes the sign of g_∞ at t, and $g_p : \mathbb{Q}_p \to \{\pm 1\}$ are functions satisfying:

- *g_p are locally constant outside a finite set of points;*
- *for all but finitely-many primes p, $g_p(\tau) = 1$ whenever $\nu_p(B_{\mathcal{F}}(\tau)) < 2$.*

[1] ν is a place of quite bad reduction if no quadratic twist of $\mathcal{F}$ has good reduction at ν.

Moreover, if $\mathcal{F}$ has at least one place of multiplicative reduction over $\mathbb{Q}(T)$ other than $-\deg$, and if the Squarefree Sieve Conjecture holds for $B_{\mathcal{F}}(T)$ and Strong Chowla's Conjecture holds for $M_{\mathcal{F}}(T)$, then $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = 0$.

On the other hand, if $\mathcal{F}$ has no place of multiplicative reduction over $\mathbb{Q}(T)$, except possibly at $-\deg$, and if the Squarefree Sieve Conjecture holds for $B_{\mathcal{F}}(T)$, then

$$\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = \frac{c_- + c_+}{2} \prod_{p \text{ prime}} \int_{\mathbb{Z}_p} g_p(t)dt,$$

where dt denotes the usual p-adic measure and where $c_\pm = \lim_{x\to\pm\infty} \mathrm{sgn}(g_\infty(x))$.

Remark 1.0.2. *The above theorem is conditional on the Squarefree Sieve Conjecture as well as on Chowla's Conjecture, which are known to hold in some cases; namely, Chowla's Conjecture is known to hold for polynomials of degree 1, whereas the Squarefree Sieve Conjecture is known to hold for polynomials whose irreducible factors have degree less than or equal to 3 [Hel04].*

There has been little work dealing with the case where $\mathcal{F}$ has no place of multiplicative reduction over $\mathbb{Q}(T)$, except possibly at $-\deg$. In [Riz03], Rizzo showed that Washington's family [Was87] $\mathcal{W} : y^2 = x^3 + tx^2 - (t+3)x + 1$ has $\varepsilon_{\mathcal{W}}(t) = -1$ for all $t \in \mathbb{Z}$ (so that $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{W}})$ is trivially non-zero) and he also gave an example of a family of elliptic curves whose j-invariant is not constant and whose average root number is not equal to $\pm 1, 0$. There are other such isolated examples, see [BDD16] for a more thorough survey.

In [BDD16], the authors attempted to give a more systematic approach to describing families of elliptic curves defined over $\mathbb{Q}$ whose average root number is not zero: they classified all such "potentially parity-biased" families whose factors, in the parameter T, have degree less than or equal to 2. More precisely,

Definition 1.0.1. *Let $\mathcal{F}$ be an elliptic curve defined over $\mathbb{Q}(T)$, let $j_{\mathcal{F}}(T)$ denote the j-invariant of $\mathcal{F}$, and let $r_{\mathcal{F}}$ denote the rank of $\mathcal{F}$ over $\mathbb{Q}(T)$. Then,*

- *$\mathcal{F}$ is **potentially-parity biased over** $\mathbb{Z}$ if $\mathcal{F}$ has no place of multiplicative reduction over $\mathbb{Q}(T)$, except possibly at $-\deg$.*
- *$\mathcal{F}$ is **parity-biased over** $\mathbb{Z}$ if $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ exists and is non-zero.*
- *$\mathcal{F}$ is **non-isotrivial** if $j_{\mathcal{F}}(T)$ is non-constant; otherwise, $\mathcal{F}$ is **isotrivial**.*
- *$\mathcal{F}$ has **excess rank** if $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ exists and $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = -(-1)^{r_{\mathcal{F}}}$*

Remark 1.0.3. *As the authors in [BDD16] remark, there are many examples of isotrivial families. For example, quadratic twists of a fixed elliptic curve $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ defined over $\mathbb{Q}$ by a polynomial $d(T) \in \mathbb{Z}[T]$, $E^{d(T)} : d(T)y^2 = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{Z}, i = 2, 4, 6$. Furthermore, we have the following implications:*

$$\textit{Excess Rank} \Rightarrow \textit{Parity-Biased} \xrightarrow[Conj.]{Helfgott} \textit{Potentially Parity-Biased.}$$

In Theorems 7 and 8 of [BDD16], the authors show that there are essentially 6 different classes of non-isotrivial, potentially parity-biased families of elliptic curves defined over $\mathbb{Q}$ whose coefficients, in the parameter T, have degree

less than or equal to 2; namely,

$$\begin{aligned}
&\mathcal{F}_s(t) : y^2 = x^3 + 3tx^2 + 3sx + st, \text{ with } s \in \mathbb{Z}_{\neq 0};\\
&\mathcal{G}_w(t) : wy^2 = x^3 + 3tx^2 + 3tx + t^2, \text{ with } w \in \mathbb{Z}_{\neq 0};\\
&\mathcal{H}_w(t) : wy^2 = x^3 + (8t^2 - 7t + 3)x^2 - 3(2t - 1)x + (t + 1), \text{ with } w \in \mathbb{Z}_{\neq 0};\\
&\mathcal{I}_w(t) : wy^2 = x^3 + t(t - 7)x^2 - 6t(t - 6)x + 2t(5t - 27), \text{ with } w \in \mathbb{Z}_{\neq 0};\\
&\mathcal{J}_{m,w}(t) : wy^2 = x^3 + 3t^2x^2 - 3mtx + m^2, \text{ with } m, w \in \mathbb{Z}_{\neq 0};\\
&\mathcal{L}_{w,s,v}(t) : wy^2 = x^3 + 3(t^2 + v)x^2 + 3sx + s(t^2 + v), \text{ with } v \in \mathbb{Z}, s, w \in \mathbb{Z}_{\neq 0}.
\end{aligned}$$

The authors then compute the average root number for two subfamilies of $\mathcal{F}_s$,

$$\begin{aligned}
&\mathcal{W}_a(t) : y^2 = x^3 + tx^2 - a(t + 3a)x + a^3, \text{ with } a \in \mathbb{Z}_{\neq 0},\\
&\mathcal{V}_a(t) : y^2 = x^3 + 3tx^2 + 3atx + a^2t, \text{ with } a \in \mathbb{Z}_{\neq 0},
\end{aligned}$$

highlighting the key ideas in implementing Helfgott's and Rizzo's work (see also the "Sketch of the proof of Theorem 6" on pages 6-9 in [BDD16], where the authors give a general overview on the correct way to proceed).

Remark 1.0.4. *Note that* $\mathcal{W}_a(t) \cong \mathcal{F}_{-3^5 4a^2}(12t + 18a)$ *and* $\mathcal{V}_a(t) \cong \mathcal{F}_{4a^2}(4t - 2a)$.

In this paper, we complement the work of [BDD16] by computing $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}_s})$; that is, we prove the following:

Theorem 1.0.1. *Let* $\mathcal{F}_s$ *denote the family of elliptic curves defined over* $\mathbb{Q}$ *whose specializations are given by the Weierstrass equation*

$$\mathcal{F}_s(t) : y^2 = x^3 + 3tx^2 + 3sx + st, \text{ with } s \in \mathbb{Z}_{\neq 0}.$$

Then, $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}_s})$ *exists with*

$$\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}_s}) = -\prod_{p \text{ prime}} E_{\mathcal{F}_s}(p),$$

where the $E_{\mathcal{F}_s}(p)$ *are given by Propositions 3.2.1, 3.3.1, and 3.4.1, for* $p \geq 5$, $p = 3$, *and* $p = 2$, *respectively. In particular,* $\mathcal{F}_s$ *is parity biased over* $\mathbb{Z}$ *iff* $s \not\equiv 1, 3, 5 \pmod 8$.

1.1 Applications

In this section, we present some areas of mathematics where average root numbers play a role. We only briefly discuss the results here, leaving the rest to the imagination.

1.1.1 One-level density functions of elliptic surfaces

As mentioned in [BDD16], the average root numbers of elliptic surfaces defined over $\mathbb{Q}$ appear naturally in the study of elliptic curves and their associated L-functions. They show in upcoming work that the one-level density function

of an elliptic surface $\mathcal{F}$, denoted by $W_{\mathcal{F}}$, is equal to

$$W_{\mathcal{F}}(\tau) = r_{\mathcal{F}}\delta_0(\tau) + \frac{1+(-1)^{r_{\mathcal{F}}}\operatorname{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})}{2}W_{\text{SO(even)}}(\tau) + \frac{1-(-1)^{r_{\mathcal{F}}}\operatorname{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})}{2}W_{\text{SO(odd)}}(\tau),$$

where $r_{\mathcal{F}}$ is the rank of $\mathcal{F}$ over $\mathbb{Q}(T)$, δ_0 is the Dirac measure at 0, and $W_{\text{SO(even)}}$ (resp. $W_{\text{SO(odd)}}$) is the one-level density function of the special orthogonal group of even size (resp. odd size). For more on one-level densities and applications of Helfgott's work, see [Mil04].

1.1.2 Constructing families of elliptic curves with elevated rank

Assuming the Birch-Swinnerton-Dyer Conjecture, Silverman's Specialization Theorem [Sil83] tells us that

$$\operatorname{rank}(\mathcal{F}(t)(\mathbb{Q})) \geq r_{\mathcal{F}} + \frac{1}{2}(1-\varepsilon_{\mathcal{F}}(t)(-1)^{r_{\mathcal{F}}})$$

for all but finitely-many $t \in \mathbb{Q}$; in particular, the average root number of $\mathcal{F}$ provides a lower bound for the rank of each specialization. In [CCH05], the authors use this lower bound to construct families of elliptic curves with *elevated rank*; that is, to construct families of elliptic curves for which $r_{\mathcal{F}}$ is strictly less than $\operatorname{rank}(\mathcal{F}(t)(\mathbb{Q}))$ for all but finitely-many t.

Remark 1.1.1. *Without assuming BSD, Silverman's Specialization Theorem tells us that $r_{\mathcal{F}} \leq \operatorname{rank}(\mathcal{F}(t)(\mathbb{Q}))$ for all but finitely-many $t \in \mathbb{Q}$.*

1.1.3 Generalizing the congruent number problem

Given an angle $\frac{\pi}{3} \leq \theta \leq \pi$, a squarefree integer n is called *θ-congruent* if there exists a triangle whose largest angle is θ, whose sides are all rational, and whose area is n. In [Rol11], the author gives an elliptic curve criterion for when a given integer is θ-congruent, he then uses the work of Helfgott [Hel09] to prove some density results concerning θ-congruent numbers.

1.2 Overview of this thesis

In this section, we provide a general overview of the work contained herein. Once again, our goal is to combine the work of Helfgott [Hel09] and Rizzo [Riz03], and then use the methods outlined in [BDD16], to compute the average root number of an explicit family of elliptic curves defined over $\mathbb{Q}$.

The main tool in proving Theorem 1.0.1 is the work of Helfgott; namely,

Proposition 1.2.1 ([Hel09], Proposition 7.7)**.** *Let S be a finite set of places of $\mathbb{Q}$, including the place at infinity. For every place $\nu \in S$, let $g_\nu : \mathbb{Q}_\nu \to \mathbb{C}$ be a bounded function that is locally constant almost everywhere. For every prime $p \notin S$, let $h_p : \mathbb{Q}_p \to \mathbb{C}$ be a function that is locally constant almost everywhere and such that $|h_p(x)| \leq 1$ for all x. Let $B(x) \in \mathbb{Z}[x]$ be a non-zero polynomial and assume that $h_p(x) = 1$ whenever $\nu_p(B(x)) < 2$. Let*

$$W(n) = \prod_{\nu \in S} g_\nu(n) \prod_{p \notin S} h_p(n).$$

If the Squarefree Sieve Conjecture holds for $B(x)$, then

$$\mathrm{Av}_{\mathbb{Z}}(W) = \frac{c_- + c_+}{2} \prod_{p \in S} \int_{\mathbb{Z}_p} g_p(x)dx \prod_{p \notin S} \int_{\mathbb{Z}_p} h_p(x)dx,$$

where $c_\pm = \lim_{x \to \pm\infty} g_\infty(x)$ and where $\mathrm{Av}_{\mathbb{Z}}(W) := \lim_{N \to \infty} \frac{1}{2N} \sum_{|n| \leq N} W(n)$.

Remark 1.2.1. *(i) When we say that a function is locally constant almost everywhere, we mean that it is locally constant outside a finite set of points. Recall further that a function f from topological space X into a set Y is locally constant if for every $x \in X$ there exists a neighbourhood U about x such that f is constant on U.*

(ii) We use ν to represent a place of $\mathbb{Q}$ that is either finite or infinite, so that $\mathbb{Q}_\nu = \mathbb{Q}_p$ is the field of p-adic numbers if $\nu = p$ is a (finite) prime and $\mathbb{Q}_\nu = \mathbb{R}$ if $\nu = \infty$ is the prime/place at infinity. The products indexed by p are over finite primes, under the respective conditions.

(iii) Note that a function $f : \mathbb{R} \to \mathbb{C}$ that is locally constant almost everywhere (that is, outside a finite set of points) is a step function with finitely-many discontinuities; in particular, $g_\infty(x)$ is constant for all x sufficiently large (sufficiently large and negative, respectively).

In order to use Proposition 1.2.1, our first goal is to write $\varepsilon_{\mathcal{F}}(t)$ as an infinite product: this is accomplished by writing the root number of $\mathcal{F}(t)$ as a product of *local root numbers* $w_p(t)$,

$$\varepsilon_{\mathcal{F}}(t) = - \prod_{p \text{ prime}} w_p(t).$$

Remark 1.2.2. *Alternatively, one may define the root number w of an elliptic curve $E/\mathbb{Q}$ to be the infinite product of local root numbers (independently of the functional equation associated to $L(s, E)$). The local root numbers are themselves defined by representations of the Weil-Deligne group of $\mathbb{Q}_p$ (with $w_\infty = -1$ for all elliptic curves defined over $\mathbb{R}$); we refer the reader to [Del73] and [Tat79].*

Sadly, the local root numbers do not, in general, satisfy the hypotheses of Proposition 1.2.1 (see section 1.2 of [Hel09]). In order to rectify this, we then express $\varepsilon_{\mathcal{F}}(t)$ as a product of modified local root numbers $w_\nu^*(t)$,

$$\varepsilon_{\mathcal{F}}(t) = -w_\infty^*(t) \prod_{p \text{ prime}} w_p^*(t),$$

with $w_\nu^*(t)$ satisfying the hypotheses of Proposition 1.2.1; our choice of $w_\nu^*(t)$ is a natural one (see Remark 3.1.2). At this point, computing the average root number of $\mathcal{F}$ amounts to computing the p-adic integrals $\int_{\mathbb{Z}_p} w_p^*(t)dt$, which we break into three sections (for $p \geq 5, p = 3, p = 2$), and we have that

$$\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = - \prod_{p \text{ prime}} \int_{\mathbb{Z}_p} w_p^*(t)dt,$$

as our choice of $w_\infty^*(t)$ is equal to 1 for all but finitely-many $t \in \mathbb{Z}$.

Remark 1.2.3. *In all that follows, the letter p will denote a (finite) prime and products over p are understood to be over all (finite) primes. In the case where a product involves the added "prime/place at infinity," we will make this explicit by writing the product over $p \leq \infty$. As usual, $\mathbb{Z}_p$ denotes the ring of p-adic integers and for all $n \in \mathbb{Z}_p$, $\nu_p(n)$ denotes the p-adic valuation of n. We use the identification $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ freely and set $n_p := np^{-\nu_p(n)}$ for all $n \in \mathbb{Z}_p \setminus \{0\}$.*

Chapter 2

Background on root numbers and p-adic integrals

In this chapter, we attempt to give as much background as possible on root numbers of elliptic curves and the basics of p-adic integration; we confine ourselves to what is needed for this thesis.

2.1 Root numbers: a history

In this section, we give a brief survey on root numbers of elliptic curves defined over $\mathbb{Q}$, beginning with the work of Deligne [Del73] and ending with the work of Rizzo [Riz03].

The *root number* w of an elliptic curve E defined over $\mathbb{Q}$ has an intrinsic definition as an infinite product of local root numbers w_p over all (finite) primes of $\mathbb{Q}$ and the prime at infinity $p = \infty$. In particular, $w_p = \pm 1$ for all primes p with $w_p = 1$ for all but finitely-many p, so that the expression

$$w := \prod_{p \leq \infty} w_p$$

is well-defined.

Defining local root numbers is quite a process; we mention the bare minimum here and refer back to the work of Deligne [Del73] and Tate [Tat79]. So, let E be an elliptic curve defined over $\mathbb{Q}$ and let p be a prime (either finite or infinite). The local root number w_p of E at p is defined by

$$w_p := \frac{\varepsilon(\sigma'_{E,p}, \psi, dx)}{|\varepsilon(\sigma'_{E,p}, \psi, dx)|},$$

where ψ is any non-trivial, unitary character on $\mathbb{Q}_p$, dx is any Haar measure on $\mathbb{Q}_p$, $\sigma'_{E,p}$ is some representation of the Weil-Deligne group of $\mathbb{Q}_p$, and $\varepsilon(\sigma'_{E,p}, \psi, dx)$ is the corresponding ε-factor as in [Del73] and [Tat79].

There are several classical results related to computing w_p for various p and for various $E/\mathbb{Q}$. For example, it is well-known that $w_\infty = -1$ for all $E/\mathbb{R}$, and that $w_p = 1$ whenever E has good reduction at p; see [Roh93] for a complete exposition of well-known results, or [Con94] for a more concise exposition.

In [Roh93], Rohrlich computed w_p for all $p \geq 5$ and for all $E/\mathbb{Q}$. For $p = 2, 3$, Rohrlich was only able to compute

w_p in the case where E has bad, potentially good reduction at p, with E abelian at p, $j \neq 0, 1728$. Unfortunately, Rohrlich's work for $p = 2, 3$ is not effective for computations, in the sense that his results are not explicit: for $p = 2, 3$, his work relies on finding a totally ramified cyclic extension K of $\mathbb{Q}_p$ and a nontrivial character μ on $\mathbb{Q}_p^*$ such that μ has order $[K : \mathbb{Q}_p]$, with μ trivial on the norm group $N_{K/\mathbb{Q}_p}(K^*)$. From there, he shows that $w_p = \mu(-1)$.

Connell [Con94] improved upon the work of Rohrlich in the case where E has bad, potentially good reduction at $p = 2, 3$, with E abelian at p, $j \neq 0, 1728$, by making Rohrlich's results explicit: Connell gave formulas for w_2, w_3 in terms of the covariants c_4, c_6, Δ, and the invariant j associated to E.

For $j = 0, 1728$, the local root numbers of E were computed by Birch-Stephens [BS66] and Liverance [Liv95].

Halberstadt [Hal98] then completed the study of local root numbers of elliptic curves defined over $\mathbb{Q}$ by considering the remaining cases at $p = 2, 3$. Again, the results are not effective for computations (at least when one considers a parametrized family of elliptic curves) as the work of Halberstadt gives values for w_2, w_3 which depend upon the coefficients of a minimal Weierstrass equation for E.

Rizzo [Riz03] brought the study of local root numbers full circle by revisiting the work of Halberstadt and removing the minimality condition for the Weierstrass equation defining E, thereby providing explicit formulas for the local root numbers of all elliptic curves defined over $\mathbb{Q}$ and for all p. For these reasons, we use [Riz03] for our computations.

Remark 2.1.1. *As the authors in [BDD16] remark, there are the following misprints in [Riz03]: in Table II, the line corresponding to* $(a, b, c) = (\geq 5, 6, 9)$ *should read* $c_6' + 2 \not\equiv 3c_{4,4} \pmod 9$*; in Table III, the second line should read* $(a, b, c) = (0, 0, \geq 0)$ *and the Kodaira symbol at* $(a, b, c) = (2, 3, 1)$ *should read* I_2^*.

2.2 p-adic analysis

In this section, we mention the basics of p-adic integration for complex-valued functions. All that follows is essentially an exercise in general measure theory, we use [Roy10] as a general reference.

We begin our study of p-adic analysis by "constructing" the *Haar measure* $\mu = \mu_{\text{Haar}}$ on $\mathbb{Z}_p$. For all $a \in \mathbb{Z}_p$ and all $n \in \mathbb{N}$, define $\mu_p(a + p^n \mathbb{Z}_p) := p^{-n}$; we extend μ_p to all compact-open subsets of $\mathbb{Z}_p$ by additivity, noting that all compact-open subsets of $\mathbb{Z}_p$ can be written as the disjoint union of a finite number of sets of the form $a + p^n \mathbb{Z}_p$. From here, we define the *outer-measure* μ_p^* *induced by* μ_p, by setting $\mu_p^*(\emptyset) = 0$ and by defining

$$\mu_p^*(\mathcal{O}) := \inf_{\{\mathcal{O}_k\}} \sum_k \mu_p(\mathcal{O}_k),$$

for all $\mathcal{O} \subset \mathbb{Z}_p$, where the infimum is taken over all countable sets of compact-open subsets of $\mathbb{Z}_p$ whose union covers $\mathcal{O}$. Now, let $\mathcal{M}$ denote the σ-algebra of μ_p^*-measurable sets of $\mathbb{Z}_p$; that is,

$$\mathcal{M} = \{\mathcal{O} \subset \mathbb{Z}_p : \mu_p^*(A) = \mu_p^*(A \bigcap \mathcal{O}) + \mu_p^*(A \bigcap \mathcal{O}^c) \text{ for all } A \subset \mathbb{Z}_p\}.$$

Finally, we let $\mu = \mu_{\text{Haar}}$ denote the restriction of μ_p^* on the Borel σ-algebra of subsets of $\mathbb{Z}_p$, $\mathcal{B} \subset \mathcal{M}$; i.e., $\mu = \mu_{p|\mathcal{B}}^*$.

We are now in a position to define p-adic integrals of the simplest kind, pun intended. Let $X \in \mathcal{B}$ and let f be a complex-valued function on X. Suppose further that f can be written as a finite linear combination of characteristic functions of pairwise disjoint, Borel subsets of X, say $f = \sum_{i=1}^n c_i \chi_{\mathcal{O}_i}$, for some $c_i \in \mathbb{C}, \mathcal{O}_i \subset X$. The *integral of* f

over X with respect to μ is then defined by

$$\int_X f(x)\mu(x) := \sum_{i=1}^{n} c_i \mu(\mathcal{O}_i).$$

Remark 2.2.1. *We often write $\int_X f(x)dx$ in place of $\int_X f(x)\mu(x)$.*

2.2.1 p-uniformly locally constant multiplicative functions and their p-adic integrals

In our work, we deal with functions Rizzo calls *p-uniformly locally constant multiplicative functions*. We will see that these functions are locally constant everywhere, except possibly at 0, which is what we need in order to apply Proposition 1.2.1.

Definition 2.2.1 ([Riz03], p.11)**.** *A function $f : \mathbb{Z}_p \to \mathbb{R}$ is a **p-uniformly locally constant multiplicative function** if there exists a positive integer η such that the value of f at $x \in \mathbb{Z}_p$ is completely determined by $\nu_p(x)$ and $x_p := xp^{-\nu_p(x)} \pmod{p^\eta}$. We call η a **uniformity constant** of f*

Remark 2.2.2. *Note that uniformity constants are not unique: if the value of f at x is determined by $\nu_p(x)$ and $x_p \pmod{p^\eta}$, then it is certainly determined by $\nu_p(x)$ and $x_p \pmod{p^{\eta'}}$ for any $\eta' \geq \eta$.*

From the definition above, it should be clear that all p-uniformly locally constant multiplicative functions are locally constant on $p^e\,\mathbb{Z}_p^* := \{x \in \mathbb{Z}_p : \nu_p(x) = e\}$ for all $e \geq 0$. To see this, let η be a uniformity constant of f, partition $p^e\,\mathbb{Z}_p^*$ into $p^{\eta-1}(p-1)$ disjoint balls of radius $p^{e+\eta}$,

$$p^e\,\mathbb{Z}_p^* = \bigcup_{\substack{\alpha_i=0,1,\ldots,p-1 \\ \alpha_0 \neq 0}} p^e(\alpha_0 + \alpha_1 p + \cdots + \alpha_{\eta-1}p^{\eta-1}) + p^{e+\eta}\,\mathbb{Z}_p,$$

and note that f is constant on each ball. From here, it is easy to see that

$$\int_{\nu_p(t)=e} f(t)dt := \int_{p^e\,\mathbb{Z}_p^*} f(t)dt = \sum_{d \in (\mathbb{Z}/p^\eta\,\mathbb{Z})^*} \frac{f(dp^e)}{p^{e+\eta}}.$$

We extend the above expression to all of $\mathbb{Z}_p$ by writing

$$\int_{\mathbb{Z}_p} f(t)dt = \sum_{e=0}^{\infty} \int_{\nu_p(t)=e} f(t)dt,$$

provided the sum converges absolutely.

Chapter 3

The family $\mathcal{F}_S$ and its average root number

In all that follows, we concern ourselves with the Weierstrass equation

$$\mathcal{F}_s(t) : y^2 = x^3 + 3tx^2 + 3sx + st,\ s \in \mathbb{Z}, s \neq 0,$$

for which we have

$$\begin{aligned} c_4(t) &= 2^4 3^2 (t^2 - s), \\ c_6(t) &= -2^6 3^3 t(t^2 - s), \\ \Delta(t) &= -2^6 3^3 s(t^2 - s)^2, \\ j(t) &= \frac{-2^6 3^3}{s}(t^2 - s). \end{aligned}$$

We prove the following:

Theorem 3.0.1. *Let*

$$\varepsilon_{\mathcal{F}_s}(t) = \begin{cases} \textit{the root number of } \mathcal{F}_s(t) & \textit{if } \mathcal{F}_s(t) \textit{ is an elliptic curve,} \\ 0 & \textit{otherwise.} \end{cases}$$

Then,

$$\begin{aligned} \mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}_s}) :&= \lim_{T\to\infty} \frac{1}{2T} \sum_{|t|\leq T} \varepsilon_{\mathcal{F}_s}(t) \\ &= -\prod_{p \textit{ prime}} E_{\mathcal{F}_s}(p), \end{aligned}$$

where the $E_{\mathcal{F}_s}(p)$ are given by Propositions 3.2.1, 3.3.1, and 3.4.1, for $p \geq 5$, $p = 3$, and $p = 2$, respectively; in particular, $\mathcal{F}_s$ is parity biased over $\mathbb{Z}$ iff $s \not\equiv 1, 3, 5$ (mod 8).

3.1 Finding local root numbers for the family $\mathcal{F}_s$

We begin by using tables I, II, and III of [Riz03] to find the local root numbers $w_p(t)$ of $\mathcal{F}_s(t)$. From there, we choose appropriate $w_p^*(t)$ so that

$$\varepsilon_{\mathcal{F}_s}(t) = -\prod_{p \text{ prime}} w_p(t) = -w_\infty^*(t) \prod_{p \text{ prime}} w_p^*(t),$$

with $w_p^*(t)$ satisfying the hypotheses of Proposition 1.2.1.

The local root numbers of $\mathcal{F}_s(t)$ for $p \geq 5$ are presented below. For $p = 2, 3$, similar calculations ensue, but we only present the final results in Appendix A.

Proposition 3.1.1. *For $p \geq 5$,*

- *if $0 \leq 2\nu_p(t) < \nu_p(s)$, then*

$$w_p(t) = \begin{cases} -\left(\frac{3t_p}{p}\right) & \text{if } \nu_p(t) \text{ is even,} \\ \left(\frac{-1}{p}\right) & \text{if } \nu_p(t) \text{ is odd;} \end{cases}$$

- *if $0 \leq \nu_p(s) < 2\nu_p(t)$, then*

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right)^{\frac{\nu_p(s)}{2}} & \text{if } \nu_p(s) \text{ is even,} \\ \left(\frac{-2}{p}\right) & \text{if } \nu_p(s) \text{ is odd;} \end{cases}$$

- *if $0 \leq 2\nu_p(t) = \nu_p(s)$, then*

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right) & \text{if } \nu_p(t) + \nu_p(t^2 - s) \equiv 1 \ (\textit{mod } 2), \\ \left(\frac{-3}{p}\right) & \text{if } \nu_p(t) + \nu_p(t^2 - s) \equiv 2, 4 \ (\textit{mod } 6), \\ 1 & \text{if } \nu_p(t) + \nu_p(t^2 - s) \equiv 0 \ (\textit{mod } 6). \end{cases}$$

Remark 3.1.1. $\left(\frac{\cdot}{p}\right)$ *represents the Legendre symbol.*

Proof. In order to find $w_p(t)$, it suffices to find the smallest triplet of non-negative integers (a, b, c) such that

$$\begin{aligned} \nu_p(c_4(t)) &\equiv a \pmod 4, \\ \nu_p(c_6(t)) &\equiv b \pmod 6, \\ \nu_p(\Delta(t)) &\equiv c \pmod{12}. \end{aligned}$$

Given such a triplet, we merely locate the corresponding value of $w_p(t)$ in Table I of [Riz03]. For the sake of simplicity, we write $\nu_p(c_4, c_6, \Delta)$ for the triplet $(\nu_p(c_4(t)), \nu_p(c_6(t)), \nu_p(\Delta(t)))$ and

$$(a, b, c) \sim (a', b', c'),$$

for non-negative integers a, b, c, if $a = a' + 4k, b = b' + 6k$, and $c = c' + 12k$, for some $k \in \mathbb{Z}$.

For $p \geq 5$,

$$\nu_p(c_4, c_6, \Delta) = (\nu_p(t^2 - s), \nu_p(t) + \nu_p(t^2 - s), \nu_p(s) + 2\nu_p(t^2 - s)).$$

From here, we consider three cases:

- If $0 \leq 2\nu_p(t) < \nu_p(s)$, then $\nu_p(t^2 - s) = \min(2\nu_p(t), \nu_p(s)) = 2\nu_p(t)$; in particular,

  $$\nu_p(c_4, c_6, \Delta) = (2\nu_p(t), 3\nu_p(t), \nu_p(s) + 4\nu_p(t)).$$

  Writing $\nu_p(t) = 2k + \lambda$, for some $k \in \mathbb{Z}_{\geq 0}$, $\lambda \in \{0, 1\}$, we have that

  $$\nu_p(c_4, c_6, \Delta) \sim (2\lambda, 3\lambda, \nu_p(s) - 4k + 4\lambda).$$

  Since $\nu_p(s) > 2\nu_p(t) = 4k + 2\lambda$,

  $$\nu_p(c_4, c_6, \Delta) \sim (2\lambda, 3\lambda, > 6\lambda).$$

  Looking into Table I of [Riz03],

  $$w_p(t) = \begin{cases} -\left(\frac{-c_6 p^{-\nu_p(c_6)}}{p}\right) & \text{if } \lambda = 0, \\ \left(\frac{-1}{p}\right) & \text{if } \lambda = 1. \end{cases}$$

  Moreover, $-c_6 p^{-\nu_p(c_6)} = 2^6 3^3 t(t^2 - s) p^{-3\nu_p(t)}$, as $\nu_p(c_6) = 3\nu_p(t)$. If we let $t_p = t p^{-\nu_p(t)}$, then

  $$\begin{aligned} \left(\frac{-c_6 p^{-\nu_p(c_6)}}{p}\right) &= \left(\frac{3t_p(t_p^2 - s p^{-2\nu_p(t)})}{p}\right) \\ &= \left(\frac{3t_p}{p}\right)\left(\frac{t_p^2 - s p^{-2\nu_p(t)}}{p}\right). \end{aligned}$$

  Finally, the assumption that $2\nu_p(t) < \nu_p(s)$ implies $s p^{-2\nu_p(t)}$ is divisible by p; and so,

  $$\left(\frac{t_p^2 - s p^{-2\nu_p(t)}}{p}\right) = \left(\frac{t_p^2}{p}\right) = 1,$$

  which is the desired result.

- If $0 \leq \nu_p(s) < 2\nu_p(t)$, then $\nu_p(t^2 - s) = \min(2\nu_p(t), \nu_p(s)) = \nu_p(s)$; in particular,

  $$\nu_p(c_4, c_6, \Delta) = (\nu_p(s), \nu_p(s) + \nu_p(t), 3\nu_p(s)).$$

  Writing $\nu_p(s) = 4k + \lambda$, for some $k \in \mathbb{Z}_{\geq 0}$, $\lambda \in \{0, 1, 2, 3\}$, we have that

  $$\nu_p(c_4, c_6, \Delta) \sim (\lambda, \nu_p(t) - 2k + \lambda, 3\lambda).$$

  Since $\nu_p(t) > \frac{\nu_p(s)}{2} = 2k + \frac{1}{2}\lambda$,

  $$\nu_p(c_4, c_6, \Delta) \sim (\lambda, > \frac{3}{2}\lambda, 3\lambda).$$

Looking into Table I of [Riz03], we have that

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right)^{\frac{\nu_p(s)}{2}} & \text{if } \lambda = 0, 2, \\ \left(\frac{-2}{p}\right) & \text{if } \lambda = 1, 3, \end{cases}$$

as claimed.

- If $0 \leq 2\nu_p(t) = \nu_p(s)$, then

$$\begin{aligned} v_p(c_4, c_6, \Delta) &= (v_p(t^2 - s), v_p(t) + v_p(t^2 - s), v_p(s) + 2(v_p(t^2 - s)) \\ &= (v_p(t^2 - s), v_p(t) + v_p(t^2 - s), 2(v_p(t) + v_p(t^2 - s)). \end{aligned}$$

Writing $v_p(t) + v_p(t^2 - s) = 6k + \lambda$, for some $k \in \mathbb{Z}_{\geq 0}, \lambda \in \{0, 1, 2, 3, 4, 5\}$,

$$v_p(c_4, c_6, \Delta) \sim (2k + \lambda - v_p(t), \lambda, 2\lambda).$$

Since $v_p(t^2 - s) \geq \min(2v_p(t), v_p(s)) = 2v_p(t)$, $6k + \lambda = v_p(t) + v_p(t^2 - s) \geq 3v_p(t)$; in particular, $2k \geq v_p(t) - \frac{1}{3}\lambda$. So,

$$v_p(c_4, c_6, \Delta) \sim (\geq \frac{2}{3}\lambda, \lambda, 2\lambda).$$

Looking into Table I of [Riz03],

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right) & \text{if } \lambda = 1, 3, 5, \\ \left(\frac{-3}{p}\right) & \text{if } \lambda = 2, 4, \\ 1 & \text{if } \lambda = 0, \end{cases}$$

which is the desired result.

□

So far, we have written the root number of $\mathcal{F}_s(t)$ as a product of local root numbers

$$\varepsilon_{\mathcal{F}_s}(t) = -\prod_{p \text{ prime}} w_p(t),$$

with $w_p(t)$ given by Proposition 3.1.1 for $p \geq 5$ and $w_3(t), w_2(t)$ given by Propositions A.0.1, A.0.2 in Appendix A, respectively. Our next goal is to modify the local root numbers in order to apply Proposition 1.2.1 (this is accomplished in the following lemma).

Lemma 3.1.1. *For $p \geq 5$, let $w_p^*(t) = w_p(t)\left(\frac{-1}{p}\right)^{\nu_p(t^2-s)}$, with $w_p(t)$ as in Proposition 3.1.1. For $p = 2, 3$, and for the prime at infinity, let $w_2^*(t), w_3^*(t), w_\infty^*(t) \in \{\pm 1\}$ be defined by*

$$\begin{aligned} w_2^*(t) &\equiv (t^2 - s)_2 w_2(t) \ (\textit{mod } 4), \\ w_3^*(t) &= (-1)^{\nu_3(t^2-s)} w_3(t), \\ w_\infty^*(t) &= \operatorname{sgn}(t^2 - s), \end{aligned}$$

where $w_2(t), w_3(t)$ are given by Propositions A.0.2, A.0.1, respectively. Then,

$$\varepsilon_{\mathcal{F}_s}(t) = -\prod_{p \text{ prime}} w_p(t) = -w_\infty^*(t) \prod_{p \text{ prime}} w_p^*(t). \tag{1}$$

Remark 3.1.2. *The choice of $w_p^*(t)$ is a natural one, more or less. We begin by assuming $p \geq 5$, $p \nmid s$, and $p|\Delta(t) = -2^6 3^3 s(t^2-s)^2$, so that $\nu_p(t^2-s) > 0$ (if $p \nmid \Delta$, then $w_p(t) = 1$ and this does not pose a problem in applying Proposition 1.2.1; similarly, the assumption that $p \nmid 6s$ throws away a finite number of primes, which will belong to the set S in Proposition 1.2.1). We have two cases to consider: $\nu_p(t) = \nu_p(s) = 0$ and $\nu_p(t) > \nu_p(s) = 0$. In the first case,*

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right) & \text{if } \nu_p(t^2-s) \equiv 1 \ (\text{mod } 2), \\ \left(\frac{-3}{p}\right) & \text{if } \nu_p(t^2-s) \equiv 2, 4 \ (\text{mod } 6), \\ 1 & \text{if } \nu_p(t^2-s) \equiv 0 \ (\text{mod } 6), \end{cases}$$

whereas, $w_p(t) = 1$ in the second case. Taking

$$w_p^*(t) = w_p(t)\left(\frac{-1}{p}\right)^{\nu_p(t^2-s)},$$

we see that $w_p^*(t) = 1$ whenever $p \nmid 6s$ and $\nu_p(t^2-s) \leq 1$. The choices of $w_2^*(t), w_3^*(t), w_\infty^*(t)$ are then made so that Equation 1 holds. Combining this remark together with Lemma 3.1.1 allows us to apply Proposition 1.2.1.

Proof. For p odd, $\left(\frac{-1}{p}\right) \equiv p \pmod 4$, so that

$$\begin{aligned} \prod_{p \neq 2,3} w_p^*(t) &= \prod_{p \neq 2,3} \left(\frac{-1}{p}\right)^{\nu_p(t^2-s)} \prod_{p \neq 2,3} w_p(t) \\ &\equiv \prod_{p \neq 2,3} p^{\nu_p(t^2-s)} \prod_{p \neq 2,3} w_p(t) \pmod 4 \\ &\equiv (-1)^{\nu_3(t^2-s)} \prod_{p \neq 2} p^{\nu_p(t^2-s)} \prod_{p \neq 2,3} w_p(t) \pmod 4 \\ &= (-1)^{\nu_3(t^2-s)} |(t^2-s)_2| \prod_{p \neq 2,3} w_p(t); \end{aligned}$$

thus,

$$-w_\infty^*(t) \prod_{p \text{ prime}} w_p^*(t) = -\prod_{p \text{ prime}} w_p(t).$$

□

Applying Proposition 1.2.1 with $S = \{p : p \nmid 6s\} \bigcup \{\infty\}$, $g_\nu = w_\nu^*$, $h_p = w_p^*$, and $B(x) = x^2 - s$, we have that

$$\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}_s}) = -\prod_{p \text{ prime}} \int_{\mathbb{Z}_p} w_p^*(t) dt,$$

as $w_\infty^*(t) = 1$ for all but finitely-many integers t.

Remark 3.1.3. *Recall that the Squarefree Sieve Conjecture (Conjecture 1.0.2) holds for all polynomials whose irreducible factors are of degree ≤ 3 [Hel04]. Since we are applying Proposition 1.2.1 with $B(x) = x^2 - s$, our results are unconditional.*

The next few sections are devoted to computing the p-adic integrals $\int_{\mathbb{Z}_p} w_p^*(t)dt$ for $p \geq 5, p = 3$, and $p = 2$, respectively.

3.2 Computing $\int_{\mathbb{Z}_p} w_p^*(t)dt$ for $p \geq 5$

During the calculations involved in computing $\int_{\mathbb{Z}_p} w_p^*(t)dt$ for $p \geq 5$, we will need to deal with integrals of the form

$$\int_{\substack{\nu_p(t)=\frac{\nu_p(s)}{2} \\ \nu_p(t^2-s)=\nu_p(s)+k}} 1dt,$$

for $k \in \mathbb{Z}_{\geq 0}$; this is accomplished in the following lemma,

Lemma 3.2.1. *For $k \in \mathbb{Z}_{\geq 0}$, let $S_k := \{t \in \mathbb{Z}_p : \nu_p(t) = \frac{\nu_p(s)}{2}, \nu_p(t^2 - s) = \nu_p(s) + k\}$. Then, S_k has measure*

$$\mu(S_k) = \begin{cases} 0 & \text{if } \nu_p(s) \text{ is odd,} \\ \begin{cases} \frac{p-1}{p^{\frac{\nu_p(s)}{2}+1}} & \text{if } \left(\frac{s_p}{p}\right) = -1 \text{ and } k = 0, \\ \frac{p-3}{p^{\frac{\nu_p(s)}{2}+1}} & \text{if } \left(\frac{s_p}{p}\right) = 1 \text{ and } k = 0, \\ 0 & \text{if } \left(\frac{s_p}{p}\right) = -1 \text{ and } k \geq 1, \\ \frac{2(p-1)}{p^{\frac{\nu_p(s)}{2}+k+1}} & \text{if } \left(\frac{s_p}{p}\right) = 1 \text{ and } k \geq 1, \end{cases} & \text{if } \nu_p(s) \text{ is even.} \end{cases}$$

Proof. We assume that $\nu_p(s)$ is even; otherwise, $S_k = \emptyset$ and there is nothing to prove. Let χ_k denote the characteristic function of S_k. For $t \in \mathbb{Z}_p$, $\chi_k(t) = 1$ iff $\nu_p(t) = \frac{\nu_p(s)}{2}$ and $t_p^2 \in s_p + p^k \mathbb{Z}_p^*$. Point is, χ_k is a p-uniformly locally constant multiplicative function with uniformity constant $\eta = k + 1$. Hence,

$$\begin{aligned} \mu(S_k) &:= \int_{\substack{\nu_p(t)=\frac{\nu_p(s)}{2} \\ \nu_p(t^2-s)=\nu_p(s)+k}} 1dt \\ &= \frac{1}{p^{\frac{\nu_p(s)}{2}+k+1}} \sum_{d \in (\mathbb{Z}/p^{k+1}\mathbb{Z})^*} \chi_k(dp^{\frac{\nu_p(s)}{2}}). \end{aligned}$$

We begin with the case $k = 0$ and treat the other cases separately.

For $k = 0$, $\chi_0(dp^{\frac{\nu_p(s)}{2}}) = 1$ iff $d^2 \not\equiv s_p \pmod{p}$. If s_p is not a square modulo p, then all $d \in (\mathbb{Z}/p\mathbb{Z})^*$ possess the preceding quality; on the other hand, if s_p is a square modulo p, exactly two $d \in (\mathbb{Z}/p\mathbb{Z})^*$ are such that $d^2 \equiv s_p \pmod{p}$. Therefore,

$$\mu(S_0) = \begin{cases} \frac{p-1}{p^{\frac{\nu_p(s)}{2}+1}} & \text{if } \left(\frac{s_p}{p}\right) = -1, \\ \frac{p-3}{p^{\frac{\nu_p(s)}{2}+1}} & \text{if } \left(\frac{s_p}{p}\right) = 1. \end{cases}$$

Now, suppose that $k \in \mathbb{N}$ and let $S_k^* := \{t \in \mathbb{Z}_p : \nu_p(t) = \frac{\nu_p(s)}{2}, \nu_p(t^2 - s) \geq \nu_p(s) + k\}$. Since $S_k = S_k^* \setminus S_{k+1}^*$,

with $\mu(S^*_{k+1}) < \infty$, $\mu(S_k) = \mu(S^*_k) - \mu(S^*_{k+1})$. Moreover, if we let χ^*_k denote the characteristic function of S^*_k, then χ^*_k is a p-uniformly locally constant multiplicative function with uniformity constant $\eta = k$. Therefore,

$$\mu(S^*_k) = \frac{1}{p^{\frac{\nu_p(s)}{2}+k}} \sum_{d \in (\mathbb{Z}/p^k\mathbb{Z})^*} \chi^*_k(dp^{\frac{\nu_p(s)}{2}}),$$

with $\chi^*_k(dp^{\frac{\nu_p(s)}{2}}) = 1$ iff $d^2 \equiv s_p \pmod{p^k}$. Since an integer a relatively prime to p is a square modulo p iff a is a square modulo p^n for every $n \in \mathbb{N}$, we have that

$$\mu(S^*_k) = \begin{cases} 0 & \text{if } \left(\frac{s_p}{p}\right) = -1, \\ \frac{2}{p^{\frac{\nu_p(s)}{2}+k}} & \text{if } \left(\frac{s_p}{p}\right) = 1; \end{cases}$$

and so,

$$\mu(S_k) = \mu(S^*_k) - \mu(S^*_{k+1}) = \begin{cases} 0 & \text{if } \left(\frac{s_p}{p}\right) = -1 \\ \frac{2(p-1)}{p^{\frac{\nu_p(s)}{2}+k+1}} & \text{if } \left(\frac{s_p}{p}\right) = 1, \end{cases}$$

as claimed. □

We are now in a position to prove the following:

Proposition 3.2.1. *For $p \geq 5$,*

$$\begin{aligned}
&\int_{\mathbb{Z}_p} w^*_p(t)dt \\
&= \begin{cases} \left(\frac{-1}{p}\right)^{\frac{\nu_p(s)}{2}} \frac{1}{p^{\frac{\nu_p(s)}{2}+1}} & \textit{if } \nu_p(s) \textit{ is even,} \\ \left(\frac{2}{p}\right) \frac{1}{p^{\frac{\nu_p(s)+1}{2}}} & \textit{if } \nu_p(s) \textit{ is odd,} \end{cases} \\
&+ \begin{cases} 0 & \textit{if } \nu_p(s) = 0,1,2, \\ \left(\frac{-1}{p}\right) \frac{p-1}{p^2} & \textit{if } \nu_p(s) = 3,4,5,6, \\ \left(\frac{-1}{p}\right) \frac{1}{p+1} \cdot \begin{cases} 1-p^{-2\alpha} & \textit{if } \nu_p(s) \equiv 2 \pmod 4, \\ 1-p^{-2\alpha-2} & \textit{otherwise,} \end{cases} & \textit{if } \nu_p(s) \geq 7, \end{cases} \\
&+ \begin{cases} 0 & \textit{if } \nu_p(s) \textit{ is odd,} \\ \left(\frac{-1}{p}\right)^{\frac{j}{2}} \frac{p-1}{p^{\frac{\nu_p(s)}{2}+1}} & \textit{if } \left(\frac{s_p}{p}\right) = -1, \\ \left(\frac{-1}{p}\right)^{\frac{j}{2}} \frac{p-1}{p^{\frac{\nu_p(s)}{2}+1}} & \textit{if } \left(\frac{s_p}{p}\right) = 1 \textit{ and } p \equiv 1 \pmod 3, \quad \textit{if } \nu_p(s) \textit{ is even,} \\ \left(\frac{-1}{p}\right)^{\frac{j}{2}} \frac{1}{p^{\frac{\nu_p(s)}{2}+1}} \left(p - (2j+1) - 4(-1)^{\frac{j}{2}} \frac{p^4+\frac{j}{2}p^3+p^2+\frac{j}{2}}{(p+1)(p^4+p^2+1)}\right) & \textit{if } \left(\frac{s_p}{p}\right) = 1 \textit{ and } p \equiv 2 \pmod 3, \end{cases}
\end{aligned}$$

where $\alpha = \lfloor \frac{\nu_p(s)-2}{4} \rfloor$ and $j \in \{0,2\}$ such that $\nu_p(s) \equiv j \pmod 4$ (for $\nu_p(s)$ even).

Remark 3.2.1. *In the case where $\nu_p(s) = 0$, such a hideous expression reduces to something quite nice; namely,*

$$\int_{\mathbb{Z}_p} w_p^*(t)dt = \begin{cases} 1 & \text{if } \left(\frac{s_p}{p}\right) = -1, \\ \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ 1 - 4\frac{p(p^2+1)}{(p+1)(p^4+p^2+1)} & \text{if } p \equiv 2 \pmod 3, \end{cases} & \text{if } \left(\frac{s_p}{p}\right) = 1. \end{cases}$$

Proof. By Proposition 3.1.1,

$$\begin{aligned} \int_{\mathbb{Z}_p} w_p^*(t)dt &= \int_{0\le 2\nu_p(t)<\nu_p(s)} w_p^*(t)dt + \int_{0\le\nu_p(s)<2\nu_p(t)} w_p^*(t)dt + \int_{0\le\nu_p(s)=2\nu_p(t)} w_p^*(t)dt \\ &= \int_{\substack{0\le 2\nu_p(t)<\nu_p(s) \\ 2|\nu_p(t)}} -\left(\frac{3t_p}{p}\right)dt + \int_{\substack{0\le 2\nu_p(t)<\nu_p(s) \\ 2\nmid\nu_p(t)}} \left(\frac{-1}{p}\right)dt \\ &\quad + \begin{cases} \int_{0\le\nu_p(s)<2\nu_p(t)} \left(\frac{-1}{p}\right)^{\frac{\nu_p(s)}{2}} dt & \text{if } \nu_p(s) \text{ is even}, \\ \int_{0\le\nu_p(s)<2\nu_p(t)} \left(\frac{2}{p}\right)dt & \text{if } \nu_p(s) \text{ is odd}, \end{cases} \\ &\quad + \sum_{k=0}^{\infty} \int_{\substack{0\le\nu_p(s)=2\nu_p(t) \\ \nu_p(t^2-s)=\nu_p(s)+k}} w_p^*(t)dt, \end{aligned}$$

where the infinite sum is simply a partition of $\int_{0\le\nu_p(s)=2\nu_p(t)} w_p^*(t)dt$. We consider each line separately, noting that the third line is the most difficult to deal with.

We begin by partitioning the first two integrals as a sum over all $t \in \mathbb{Z}_p$ with $\nu_p(t) = 2k$ and $\nu_p(t) = 2k+1$, respectively, to obtain

$$\begin{aligned} \int_{\substack{0\le 2\nu_p(t)<\nu_p(s) \\ 2|\nu_p(t)}} -\left(\frac{3t_p}{p}\right)dt &= \sum_{0\le k<\frac{\nu_p(s)}{4}} \int_{\nu_p(t)=2k} -\left(\frac{3t_p}{p}\right)dt \\ &= \sum_{0\le k<\frac{\nu_p(s)}{4}} -\left(\frac{3}{p}\right)\frac{1}{p^{2k+1}} \sum_{d\in(\mathbb{Z}/p\,\mathbb{Z})^*} \left(\frac{d}{p}\right) \end{aligned}$$

and

$$\begin{aligned} \int_{\substack{0\le 2\nu_p(t)<\nu_p(s) \\ 2\nmid\nu_p(t)}} \left(\frac{-1}{p}\right)dt &= \sum_{0\le k<\frac{\nu_p(s)-2}{4}} \int_{\nu_p(t)=2k+1} \left(\frac{-1}{p}\right)dt \\ &= \sum_{0\le k<\frac{\nu_p(s)-2}{4}} \left(\frac{-1}{p}\right)\mu(\{t\in\mathbb{Z}_p : \nu_p(t) = 2k+1\}). \end{aligned}$$

In the first case, $\int_{\substack{0\le 2\nu_p(t)<\nu_p(s) \\ 2|\nu_p(t)}} -\left(\frac{3t_p}{p}\right)dt = 0$: simply note that there are exactly $\frac{p-1}{2}$ squares and $\frac{p-1}{2}$ non-squares modulo p; i.e.,

$$\sum_{d\in(\mathbb{Z}/p\,\mathbb{Z})^*} \left(\frac{d}{p}\right) = 0$$

In the second case, $\mu(\{t \in \mathbb{Z}_p : \nu_p(t) = 2k+1\}) = \frac{p-1}{p^{2k+2}}$, so that

$$\begin{aligned}\int_{\substack{0 \le 2\nu_p(t) < \nu_p(s) \\ 2 \nmid \nu_p(t)}} \left(\frac{-1}{p}\right) dt &= \sum_{0 \le k < \frac{\nu_p(s)-2}{4}} \left(\frac{-1}{p}\right) \frac{p-1}{p^{2k+2}} \\ &= \left(\frac{-1}{p}\right) \frac{p-1}{p^2} \sum_{0 \le k < \frac{\nu_p(s)-2}{4}} (p^{-2})^k.\end{aligned}$$

Now, it is merely a matter of simplifying the geometric sum, taking into account the range of k: if $\nu_p(s) = 0, 1, 2$, then the sum is empty and the integral vanishes; if $\nu_p(s) = 3, 4, 5, 6$, then the only contribution comes from $k = 0$, so that the integral is equal to $\left(\frac{-1}{p}\right)\frac{p-1}{p^2}$; for the remaining cases, let $\alpha = \lfloor \frac{\nu_p(s)-2}{4} \rfloor$ and note that

$$\left(\frac{-1}{p}\right)\frac{p-1}{p^2} \sum_{0 \le k < \frac{\nu_p(s)-2}{4}} (p^{-2})^k = \left(\frac{-1}{p}\right)\frac{p-1}{p^2}\frac{1}{1-p^{-2}} \cdot \begin{cases} 1 - p^{-2\alpha} & \text{if } \nu_p(s) \equiv 2 \pmod 4, \\ 1 - p^{-2\alpha-2} & \text{otherwise.} \end{cases}$$

We have the following:

$$\int_{0 \le 2\nu_p(t) < \nu_p(s)} w_p^*(t)dt = \begin{cases} 0 & \text{if } \nu_p(s) = 0, 1, 2, \\ \left(\frac{-1}{p}\right)\frac{p-1}{p^2} & \text{if } \nu_p(s) = 3, 4, 5, 6, \\ \left(\frac{-1}{p}\right)\frac{1}{p+1} \cdot \begin{cases} 1 - p^{-2\alpha} & \text{if } \nu_p(s) \equiv 2 \pmod 4, \\ 1 - p^{-2\alpha-2} & \text{otherwise,} \end{cases} & \text{if } \nu_p(s) \ge 7. \end{cases}$$

For the integral over $\{t \in \mathbb{Z}_p : 0 \le \nu_p(s) < 2\nu_p(t)\}$, a quick calculation yields:

$$\begin{aligned}\int_{0 \le \nu_p(s) < 2\nu_p(t)} w_p^*(t)dt &= \begin{cases} \int_{0 \le \nu_p(s) < 2\nu_p(t)} \left(\frac{-1}{p}\right)^{\frac{\nu_p(s)}{2}} dt & \text{if } \nu_p(s) \text{ is even,} \\ \int_{0 \le \nu_p(s) < 2\nu_p(t)} \left(\frac{2}{p}\right) dt & \text{if } \nu_p(s) \text{ is odd,} \end{cases} \\ &= \begin{cases} \left(\frac{-1}{p}\right)^{\frac{\nu_p(s)}{2}} \frac{1}{p^{\frac{\nu_p(s)}{2}+1}} & \text{if } \nu_p(s) \text{ is even,} \\ \left(\frac{2}{p}\right) \frac{1}{p^{\frac{\nu_p(s)+1}{2}}} & \text{if } \nu_p(s) \text{ is odd.} \end{cases}\end{aligned}$$

Finally, for the integral over $\{t \in \mathbb{Z}_p : 0 \le 2\nu_p(t) = \nu_p(s)\}$, we assume $\nu_p(s)$ is even (otherwise, the domain of integration is empty and there is nothing to prove) and we have the following:

$$\int_{0 \le 2\nu_p(t) = \nu_p(s)} w_p^*(t)dt = \sum_{k=0}^{\infty} \int_{\substack{0 \le 2\nu_p(t) = \nu_p(s) \\ \nu_p(t^2 - s) = \nu_p(s) + k}} w_p^*(t)dt,$$

where, in this case,

$$w_p^*(t) = \begin{cases} \left(\frac{-1}{p}\right)^{k+1} & \text{if } k \equiv 1 - \frac{3\nu_p(s)}{2} \pmod 2, \\ \left(\frac{-3}{p}\right)\left(\frac{-1}{p}\right)^k & \text{if } k \equiv -\frac{3\nu_p(s)}{2} \pmod 2, \not\equiv 0 \pmod 3 \\ \left(\frac{-1}{p}\right)^k & \text{if } k \equiv -\frac{3\nu_p(s)}{2} \pmod 6. \end{cases}$$

Moreover,

$$\sum_{k=0}^{\infty}\int_{\substack{0\le\nu_p(s)=2\nu_p(t)\\ \nu_p(t^2-s)=\nu_p(s)+k}} w_p^*(t)dt$$
$$= \sum_{k\equiv 1-\frac{3\nu_p(s)}{2} \pmod 2} \left(\frac{-1}{p}\right)^{k+1}\mu(S_k) + \sum_{\substack{k\equiv\frac{-3\nu_p(s)}{2} \pmod 2\\ k\not\equiv 0 \pmod 3}} \left(\frac{-3}{p}\right)\left(\frac{-1}{p}\right)^{k}\mu(S_k) + \sum_{k\equiv\frac{-3\nu_p(s)}{2} \pmod 6} \left(\frac{-1}{p}\right)^{k}\mu(S_k),$$

with $\mu(S_k)$ as in Lemma 3.2.1. If we let $j\in\{0,2\}$ be such that $\nu_p(s)\equiv j \pmod 4$, this becomes

$$\left(\frac{-1}{p}\right)^{\frac{j}{2}}\left(\sum_{k\equiv 1-\frac{j}{2} \pmod 2}\mu(S_k) + \sum_{\substack{k\equiv\frac{j}{2} \pmod 2\\ k\not\equiv 0 \pmod 3}}\left(\frac{-3}{p}\right)\mu(S_k) + \sum_{k\equiv\frac{3j}{2} \pmod 6}\mu(S_k)\right).$$

In the case where $\left(\frac{s_p}{p}\right)=-1$,

$$\mu(S_k)=\begin{cases}\frac{p-1}{p^{\frac{\nu_p(s)}{2}+1}} & \text{if } k=0,\\ 0 & \text{if } k\ge 1;\end{cases}$$

in particular,

$$\int_{0\le\nu_p(s)=2\nu_p(t)} w_p^*(t)dt = \left(\frac{-1}{p}\right)^{\frac{j}{2}}\frac{p-1}{p^{\frac{\nu_p(s)}{2}+1}},$$

as the only contribution comes from $\mu(S_0)$. The case where $\left(\frac{s_p}{p}\right)=+1$ requires more work. We begin by recalling that

$$\mu(S_k)=\begin{cases}\frac{p-3}{p^{\frac{\nu_p(s)}{2}+1}} & \text{if } k=0,\\ \frac{2}{p^{\frac{\nu_p(s)}{2}+k+1}} & \text{if } k\ge 1.\end{cases}$$

By separating $\mu(S_0)$ from $\mu(S_k)$ for $k\ge 1$, we obtain

$$\int_{0\le\nu_p(s)=2\nu_p(t)} w_p^*(t)dt$$
$$= \left(\frac{-1}{p}\right)^{\frac{j}{2}}\left(\mu(S_{1-\frac{j}{2}}) + \mu(S_{\frac{3j}{2}}) + \left(\frac{-3}{p}\right)\left(\mu(S_{\frac{j}{2}}) - \mu(S_{\frac{3j}{2}})\right)\right.$$
$$\left. + \sum_{k=1}^{\infty}\mu(S_{2k+1-\frac{j}{2}}) + \sum_{k=1}^{\infty}\mu(S_{6k+\frac{3j}{2}}) + \left(\frac{-3}{p}\right)\left(\sum_{k=1}^{\infty}\mu(S_{2k+\frac{j}{2}}) - \sum_{k=1}^{\infty}\mu(S_{6k+\frac{3j}{2}})\right)\right),$$

where

$$\sum_{k=0}^{\infty}\mu(S_{2k+\frac{j}{2}}) - \sum_{k=0}^{\infty}\mu(S_{6k+\frac{3j}{2}}) = \sum_{\substack{k\equiv\frac{j}{2} \pmod 2\\ k\not\equiv 0 \pmod 3}}\mu(S_k).$$

For $k \geq 1$, $\mu(S_k) = \frac{2(p-1)}{p^{\frac{\nu_p(s)}{2}+k+1}}$ and it is easy to see that

$$\begin{aligned}
&\int_{0\leq\nu_p(s)=2\nu_p(t)} w_p^*(t)dt \\
&= \left(\frac{-1}{p}\right)^{\frac{j}{2}}\left(\mu(S_{1-\frac{j}{2}}) + \mu(S_{\frac{3j}{2}}) + \left(\frac{-3}{p}\right)\left(\mu(S_{\frac{j}{2}}) - \mu(S_{\frac{3j}{2}})\right)\right. \\
&\qquad \left. + \frac{2(p-1)}{p^{\frac{\nu_p(s)}{2}+1}}\left(\frac{1}{p^{1-\frac{j}{2}}(p^2-1)} + \frac{1}{p^{\frac{3j}{2}}(p^6-1)} + \left(\frac{-3}{p}\right)\left(\frac{1}{p^{\frac{j}{2}}(p^2-1)} - \frac{1}{p^{\frac{3j}{2}}(p^6-1)}\right)\right)\right).
\end{aligned}$$

If $p \equiv 1 \pmod 3$, then $\left(\frac{-3}{p}\right) = 1$ and we get that

$$\int_{0\leq\nu_p(s)=2\nu_p(t)} w_p^*(t)dt = \left(\frac{-1}{p}\right)^{\frac{j}{2}}\left(\mu(S_{1-\frac{j}{2}}) + \mu(S_{\frac{j}{2}}) + \frac{2(p-1)}{p^{\frac{\nu_p(s)}{2}+1}} \cdot \frac{p^{\frac{j}{2}} + p^{1-\frac{j}{2}}}{p(p^2-1)}\right).$$

Upon further simplification,

$$\int_{0\leq\nu_p(s)=2\nu_p(t)} w_p^*(t)dt = \left(\frac{-1}{p}\right)^{\frac{j}{2}} \frac{p-1}{p^{\frac{\nu_p(s)}{2}+1}}.$$

On the other hand, for $p \equiv 2 \pmod 3$, $\left(\frac{-3}{p}\right) = -1$; in particular,

$$\int_{0\leq\nu_p(s)=2\nu_p(t)} w_p^*(t)dt = \left(\frac{-1}{p}\right)^{\frac{j}{2}}\left(\mu(S_{1-\frac{j}{2}}) + 2\mu(S_{\frac{3j}{2}}) - \mu(S_{\frac{j}{2}}) + \frac{2(p-1)}{p^{\frac{\nu_p(s)}{2}+1}}\left(\frac{p^{\frac{j}{2}} - p^{1-\frac{j}{2}}}{p(p^2-1)} + \frac{2}{p^{\frac{3j}{2}}(p^6-1)}\right)\right).$$

Simplifying once again,

$$\int_{0\leq\nu_p(s)=2\nu_p(t)} w_p^*(t)dt = \left(\frac{-1}{p}\right)^{\frac{j}{2}} \frac{1}{p^{\frac{\nu_p(s)}{2}+1}}\left(p - (2j+1) - 4(-1)^{\frac{j}{2}} \frac{p^4 + \frac{j}{2}p^3 + p^2 + \frac{j}{2}}{(p+1)(p^4+p^2+1)}\right),$$

which is the desired result.

To complete our proof, it suffices to sum our results, recalling that

$$\int_{\mathbb{Z}_p} w_p^*(t)dt = \left(\int_{0\leq 2\nu_p(t)<\nu_p(s)} + \int_{0\leq\nu_p(s)<2\nu_p(t)} + \int_{0\leq\nu_p(s)=2\nu_p(t)}\right) w_p^*(t)dt.$$

□

3.3 Computing $\int_{\mathbb{Z}_3} w_3^*(t)dt$

We begin by recalling that $w_3^*(t) = (-1)^{\nu_3(t^2-s)}w_3(t)$, with $w_3(t)$ given by Proposition A.0.1 in Appendix A. From here, we consider the usual cases: $0 \leq \nu_3(s) < 2\nu_3(t), 0 \leq 2\nu_3(t) < \nu_3(s), 0 \leq 2\nu_3(t) = \nu_3(s)$.

3.3.1 $0 \le \nu_3(s) < 2\nu_3(t)$

If $0 \le \nu_3(s) < 2\nu_3(t)$, then $\nu_3(t^2 - s) = \nu_3(s)$ and $w_3^*(t) = (-1)^{\nu_3(s)} w_3(t)$. Since $w_3(t)$ depends only on $\nu_3(t)$ and $t_3 \pmod 3$ (and possibly on $\nu_3(s)$ and s_3), $w_3(t)$ is a 3-uniformly locally constant multiplicative function with uniformity constant $\eta = 1$. Therefore,

$$\int_{0 \le \nu_3(s) < 2\nu_3(t)} w_3^*(t)dt = (-1)^{\nu_3(s)} \sum_{e > \frac{\nu_3(s)}{2}} \left(\frac{1}{3^{e+1}} \sum_{d \in (\mathbb{Z}/3\mathbb{Z})^*} w_3(d \cdot 3^e) \right)$$

and it is not hard to show that

$$\int_{0 \le \nu_3(s) < 2\nu_3(t)} w_3^*(t)dt = \begin{cases} \frac{1}{3^{\frac{\nu_3(s)}{2}+2}} & \text{if } \nu_3(s) \equiv 0 \pmod 2, \\ \frac{1-2\chi_3(s_3)}{3^{\frac{\nu_3(s)+3}{2}}} & \text{if } \nu_3(s) \equiv 1 \pmod 4, \\ \frac{-1}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s) \equiv 3 \pmod 4, \end{cases}$$

where χ_3 is the non-principal character modulo 3.

3.3.2 $0 \le 2\nu_3(t) < \nu_3(s)$

If $0 \le 2\nu_3(t) < \nu_3(s)$, then $\nu_3(t^2 - s) = 2\nu_3(t)$ and $w_3^*(t) = w_3(t)$. Once again, $w_3(t)$ is a 3-uniformly locally constant multiplicative function with uniformity constant $\eta = 1$. We begin by partitioning the integral $\int_{0 \le 2\nu_3(t) < \nu_3(s)} w_3^*(t)dt$ according to the cases in Proposition A.0.1:

$$\begin{aligned} &\int_{0 \le 2\nu_3(t) < \nu_3(s)} w_3^*(t)dt \\ &= \int_{\substack{\nu_3(s)-2\nu_3(t)=1 \\ 2 \mid \nu_3(t)}} w_3(t)dt + \int_{\substack{\nu_3(s)-2\nu_3(t)=2 \\ 2 \mid \nu_3(t)}} w_3(t)dt + \int_{\substack{\nu_3(s)-2\nu_3(t) \ge 3 \\ 2 \mid \nu_3(t)}} w_3(t)dt \\ &\quad + \int_{\substack{\nu_3(s)-2\nu_3(t)=1 \\ 2 \nmid \nu_3(t)}} w_3(t)dt + \int_{\substack{\nu_3(s)-2\nu_3(t)=2 \\ 2 \nmid \nu_3(t)}} w_3(t)dt + \int_{\substack{\nu_3(s)-2\nu_3(t)=3 \\ 2 \nmid \nu_3(t)}} w_3(t)dt + \int_{\substack{\nu_3(s)-2\nu_3(t) \ge 4 \\ 2 \nmid \nu_3(t)}} w_3(t)dt, \end{aligned}$$

From Proposition A.0.1,

$$\int_{\substack{\nu_3(s)-2\nu_3(t)=2 \\ 2 \mid \nu_3(t)}} w_3(t)dt, \int_{\substack{\nu_3(s)-2\nu_3(t)=2 \\ 2 \nmid \nu_3(t)}} w_3(t)dt, \int_{\substack{\nu_3(s)-2\nu_3(t) \ge 4 \\ 2 \nmid \nu_3(t)}} w_3(t)dt = 0,$$

whereas

$$\int_{\substack{\nu_3(s)-2\nu_3(t)=1\\ 2|\nu_3(t)}} w_3(t)dt = \begin{cases} \frac{2}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s)\equiv 1 \pmod 4 \text{ and } \nu_3(s)\geq 1,\\ 0 & \text{otherwise,}\end{cases}$$

$$\int_{\substack{\nu_3(s)-2\nu_3(t)\geq 3\\ 2|\nu_3(t)}} w_3(t)dt = \sum_{\substack{3\leq k\leq \nu_3(s)\\ k\equiv \nu_3(s) \pmod 4}} \frac{-2}{3^{\frac{\nu_3(s)-k}{2}+1}} = \begin{cases} \frac{1}{4}\left(\frac{3^{1-2\lfloor \frac{j}{3}\rfloor}}{3^{\frac{\nu_3(s)-j}{2}}}-3\right) & \text{if } \nu_3(s)\geq 3,\\ 0 & \text{otherwise,}\end{cases}$$

$$\int_{\substack{\nu_3(s)-2\nu_3(t)=1\\ 2\nmid\nu_3(t)}} w_3(t)dt = \begin{cases} \frac{2\chi_3(s_3)}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s)\equiv 3 \pmod 4 \text{ and } \nu_3(s)\geq 3,\\ 0 & \text{otherwise,}\end{cases}$$

$$\int_{\substack{\nu_3(s)-2\nu_3(t)=3\\ 2\nmid\nu_3(t)}} w_3(t)dt = \begin{cases} \frac{2}{3^{\frac{\nu_3(s)-1}{2}}} & \text{if } \nu_3(s)\equiv 1 \pmod 4 \text{ and } \nu_3(s)\geq 5,\\ 0 & \text{otherwise,}\end{cases}$$

where $j\in\{0,1,2,3\}$ such that $\nu_3(s)\equiv j \pmod 4$ and where χ_3 is the non-principal character modulo 3.

Summing the individual contributions,

$$\int_{0\leq 2\nu_3(t)<\nu_3(s)} w_3^*(t)dt = \begin{cases} 0 & \text{if } \nu_3(s)=0,\\ \frac{2}{3} & \text{if } \nu_3(s)=1,\\ 0 & \text{if } \nu_3(s)=2,\\ \frac{2(\chi_3(s_3)-3)}{9} & \text{if } \nu_3(s)=3,\\ \frac{-2}{3} & \text{if } \nu_3(s)=4,\\ \frac{1}{4}\left(\frac{3^{1-2\lfloor \frac{j}{3}\rfloor}}{3^{\frac{\nu_3(s)-j}{2}}}-3\right)+\begin{cases} 0 & \text{if } \nu_3(s)\equiv 0 \pmod 2,\\ \frac{8}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s)\equiv 1 \pmod 4,\\ \frac{2\chi_3(s_3)}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s)\equiv 3 \pmod 4,\end{cases} & \text{if } \nu_3(s)\geq 5,\end{cases}$$

where $j\in\{0,1,2,3\}$ such that $\nu_3(s)\equiv j \pmod 4$ and where χ_3 is the non-principal character modulo 3.

3.3.3 $0\leq 2\nu_3(t)=\nu_3(s)$

For $0\leq 2\nu_3(t)=\nu_3(s)$, we write $\nu_3(t^2-s)=\nu_3(s)+k$ with $k\geq 0$, so that

$$\int_{2\nu_3(t)=\nu_3(s)} w_3^*(t)dt = \sum_{k=0}^{\infty}(-1)^k \int_{\substack{0\leq 2\nu_3(t)=\nu_3(s)\\ \nu_3(t^2-s)=\nu_3(s)+k}} w_3(t)dt.$$

By splitting the contributions from $k=0, k\not\equiv 0 \pmod 3$, and $k\equiv 0 \pmod 3 (k\neq 0)$, we write

$$\begin{aligned}&\int_{2\nu_3(t)=\nu_3(s)} w_3^*(t)dt\\ &= \int_{\substack{0\leq 2\nu_3(t)=\nu_3(s)\\ \nu_3(t^2-s)=\nu_3(s)}} w_3(t)dt + \sum_{\substack{k\equiv 0 \pmod 3\\ k\neq 0}} (-1)^k \int_{\substack{0\leq 2\nu_3(t)=\nu_3(s)\\ \nu_3(t^2-s)=\nu_3(s)+k}} w_3(t)dt + \sum_{k\not\equiv 0 \pmod 3} (-1)^k \int_{\substack{0\leq 2\nu_3(t)=\nu_3(s)\\ \nu_3(t^2-s)=\nu_3(s)+k}} w_3(t)dt.\end{aligned}$$

Notice that if $2\nu_3(t) = \nu_3(s)$, then $\nu_3(t^2 - s) = \nu_3(s) + k$ iff $t_3^2 - s_3 \in 3^k \mathbb{Z}_3^*$; in other words, $\nu_3(t^2 - s) = \nu_3(s) + k$ iff

$$\begin{cases} t_3^2 \not\equiv s_3 \pmod 3 & \text{if } k = 0, \\ t_3^2 \equiv s_3 \pmod{3^k}, \not\equiv s_3 \pmod{3^{k+1}} & \text{if } k \geq 1. \end{cases}$$

Since $w_3^*(t) = (-1)^{\nu_3(t^2-s)} w_3(t)$ and since $w_3(t)$ depends only on $t_3(t_3^2 - s_3)_3 \pmod 9$ (and possibly on s_3 and $\nu_3(s)$), we have that

$$\int_{\substack{0 \leq 2\nu_3(t) = \nu_3(s) \\ \nu_3(t^2-s) = \nu_3(s)+k}} w_3(t)dt = \frac{1}{3^{\frac{\nu_3(s)}{2}+k+2}} \sum_{\substack{d \in (\mathbb{Z}/3^{k+2}\mathbb{Z})^* \\ d^2 \equiv s_3 \pmod{3^k} \\ d^2 \not\equiv s_3 \pmod{3^{k+1}}}} w_3(d \cdot 3^{\frac{\nu_3(s)}{2}}).$$

We consider two cases: $s_3 \equiv 1 \pmod 3$ and $s_3 \equiv 2 \pmod 3$.

In the case where $s_3 \equiv 2 \pmod 3$, s_3 is not a square modulo 3; in particular,

$$\sum_{\substack{d \in (\mathbb{Z}/3^{k+2}\mathbb{Z})^* \\ d^2 \equiv s_3 \pmod{3^k} \\ d^2 \not\equiv s_3 \pmod{3^{k+1}}}} w_3(d \cdot 3^{\frac{\nu_3(s)}{2}}) = 0$$

for all $k \geq 1$ (as the sums are empty). Therefore, if $s_3 \equiv 2 \pmod 3$,

$$\begin{aligned} \int_{2\nu_3(t) = \nu_3(s)} w_3^*(t)dt &= \frac{1}{3^{\frac{\nu_3(s)}{2}+2}} \sum_{\substack{d \in (\mathbb{Z}/3^2\mathbb{Z})^* \\ d^2 \not\equiv 2 \pmod 3}} w_3(d \cdot 3^{\frac{\nu_3(s)}{2}}) \\ &= \frac{1}{3^{\frac{\nu_3(s)}{2}+2}} \sum_{d \in (\mathbb{Z}/3^2\mathbb{Z})^*} w_3(d \cdot 3^{\frac{\nu_3(s)}{2}}). \end{aligned}$$

In this case, $w_3(d \cdot 3^{\frac{\nu_3(s)}{2}}) = 1$ iff $s_3 d \not\equiv 2, 4 \pmod 9$. Since s_3 is invertible modulo 9, as d varies over $(\mathbb{Z}/9\mathbb{Z})^*$, so does $s_3 d$; i.e.,

$$\sum_{d \in (\mathbb{Z}/3^2\mathbb{Z})^*} w_3(d \cdot 3^{\frac{\nu_3(s)}{2}}) = 2$$

with

$$\int_{2\nu_3(t) = \nu_3(s)} w_3^*(t)dt = \frac{2}{3^{\frac{\nu_3(s)}{2}+2}} \text{ if } s_3 \equiv 2 \pmod 3.$$

In the case where $s_3 \equiv 1 \pmod 3$, let $\pm\sqrt{s}_3$ denote the square roots of s_3 in $\mathbb{Z}_3$. Since s_3 is a square modulo 3, there exist exactly two d in $(\mathbb{Z}/3^k\mathbb{Z})^* \cong (\mathbb{Z}_3/3^k\mathbb{Z}_3)^*$ such that $d^2 \equiv s_3 \pmod{3^k}$ (namely, $\pm\sqrt{s}_3 + 3^k\mathbb{Z}_3$). Each such solution lifts in exactly three ways to solutions of $x^2 \equiv s_3 \pmod{3^k}$ in $(\mathbb{Z}/3^{k+1}\mathbb{Z})^*$; namely, $\pm(\sqrt{s}_3 + \alpha \cdot 3^k) + 3^{k+1}\mathbb{Z}_3$ with $\alpha \in \{0, 1, 2\}$. The condition that $x^2 \not\equiv s_3 \pmod{3^{k+1}}$ tells us to throw away two of our solutions (those corresponding to $\alpha = 0$). From here, we lift our solutions to $(\mathbb{Z}/3^{k+2}\mathbb{Z})^*$ by writing $\pm(\sqrt{s}_3 + \alpha \cdot 3^k + \beta \cdot 3^{k+1}) + 3^{k+2}\mathbb{Z}_3$ with $\beta \in \{0, 1, 2\}$. By working with the isomorphism $(\mathbb{Z}/3^{k+2}\mathbb{Z})^* \cong (\mathbb{Z}_3/3^{k+2}\mathbb{Z}_3)^*$ and choosing an appropriate representative for d, we have that there are exactly 12 solutions to $d \in (\mathbb{Z}/3^{k+2}\mathbb{Z})^*$ such that

$d^2 \equiv s_3 \pmod{3^k}, \not\equiv s_3 \pmod{3^{k+1}}$; namely,

$$d = \pm(\sqrt{s}_3 + \alpha \cdot 3^k + \beta \cdot 3^{k+1}) + 3^{k+2}\,\mathbb{Z}_3,$$

with $\alpha \in \{1, 2\}, \beta \in \{0, 1, 2\}$. Now, the value of $w_3(d \cdot 3^{\frac{\nu_3(s)}{2}})$ depends only on the value of $d(d^2 - s_3)_3$ modulo 9, with d as above (in the case where $k \equiv 0 \pmod 3$, the value of $w_3(d \cdot 3^{\frac{\nu_3(s)}{2}})$ depends only on $d(d^2 - s_3)_3$ modulo 3). But, if $d = \pm(\sqrt{s}_3 + \alpha \cdot 3^k + \beta \cdot 3^{k+1}) + 3^{k+2}\,\mathbb{Z}_3$, then, for $k \geq 1$,

$$d(d^2 - s_3)_3 \equiv \begin{cases} \pm 2s_3(\alpha + 3\beta) \pmod 9 & \text{if } k \equiv 0 \pmod 3, \\ \pm 2s_3\alpha \pmod 3 & \text{if } k \not\equiv 0 \pmod 3. \end{cases}$$

From here, it is easy to see that

$$\frac{1}{3^{\frac{\nu_3(s)}{2}+k+2}} \sum_{\substack{d \in (\mathbb{Z}/3^{k+2}\,\mathbb{Z})^* \\ d^2 \equiv s_3 \pmod{3^k} \\ d^2 \not\equiv s_3 \pmod{3^{k+1}}}} w_3(d \cdot 3^{\frac{\nu_3(s)}{2}}) = \begin{cases} 0 & \text{if } k \not\equiv 0 \pmod 3, \\ \frac{4}{3^{\frac{\nu_3(s)}{2}+k+2}} & \text{otherwise,} \end{cases}$$

whenever $k \geq 1$. When $k = 0$,

$$\int_{\substack{0 \leq 2\nu_3(t) = \nu_3(s) \\ \nu_3(t^2 - s) = \nu_3(s)}} w_3(t)dt = 0,$$

as the sum

$$\sum_{\substack{d \in (\mathbb{Z}/9\,\mathbb{Z})^* \\ d^2 \not\equiv s_3 \pmod 3}} w_3(d \cdot 3^{\frac{\nu_3(s)}{2}})$$

is empty (simply note that $d^2 \equiv 1 \pmod 3$ for all $d \in (\mathbb{Z}/9\,\mathbb{Z})^*$). Putting all of this together,

$$\int_{2\nu_3(t) = \nu_3(s)} w_3^*(t)dt = \sum_{\substack{k \equiv 0 \pmod 3 \\ k \neq 0}} (-1)^k \frac{4}{3^{\frac{\nu_3(s)}{2}+k+2}} = \frac{-1}{7} \cdot \frac{1}{3^{\frac{\nu_3(s)}{2}+2}};$$

that is,

$$\int_{0 \leq 2\nu_3(t) = \nu_3(s)} w_3^*(t)dt = \begin{cases} \begin{cases} \frac{2}{3^{\frac{\nu_3(s)}{2}+2}} & \text{if } s_3 \equiv 2 \pmod 3, \\ \frac{-1}{7} \cdot \frac{1}{3^{\frac{\nu_3(s)}{2}+2}} & \text{if } s_3 \equiv 1 \pmod 3, \end{cases} & \text{if } \nu_3(s) \equiv 0 \pmod 2, \\ 0 & \text{if } \nu_3(s) \equiv 1 \pmod 2. \end{cases}$$

Hence,

Proposition 3.3.1.

$$\int_{\mathbb{Z}_3} w_3^*(t)dt = \begin{cases} \frac{1}{3^{\frac{\nu_3(s)}{2}+2}} & \text{if } \nu_3(s) \equiv 0 \pmod 2, \\ \frac{1-2\chi_3(s_3)}{3^{\frac{\nu_3(s)+3}{2}}} & \text{if } \nu_3(s) \equiv 1 \pmod 4, \\ \frac{-1}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s) \equiv 3 \pmod 4, \end{cases}$$

$$+ \begin{cases} 0 & \text{if } \nu_3(s) = 0, \\ \frac{2}{3} & \text{if } \nu_3(s) = 1, \\ 0 & \text{if } \nu_3(s) = 2, \\ \frac{2(\chi_3(s_3)-3)}{9} & \text{if } \nu_3(s) = 3, \\ \frac{-2}{3} & \text{if } \nu_3(s) = 4, \\ \frac{1}{4}\left(\frac{3^{1-2\lfloor \frac{j}{3} \rfloor}}{3^{\frac{\nu_3(s)-j}{2}}} - 3\right) + \begin{cases} 0 & \text{if } \nu_3(s) \equiv 0 \pmod 2, \\ \frac{8}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s) \equiv 1 \pmod 4, \\ \frac{2\chi_3(s_3)}{3^{\frac{\nu_3(s)+1}{2}}} & \text{if } \nu_3(s) \equiv 3 \pmod 4, \end{cases} & \text{if } \nu_3(s) \geq 5, \end{cases}$$

$$+ \begin{cases} \begin{cases} \frac{2}{3^{\frac{\nu_3(s)}{2}+2}} & \text{if } s_3 \equiv 2 \pmod 3, \\ \frac{-1}{7} \cdot \frac{1}{3^{\frac{\nu_3(s)}{2}+2}} & \text{if } s_3 \equiv 1 \pmod 3, \end{cases} & \text{if } \nu_3(s) \equiv 0 \pmod 2, \\ 0 & \text{if } \nu_3(s) \equiv 1 \pmod 2, \end{cases}$$

where $j \in \{0,1,2,3\}$ such that $\nu_3(s) \equiv j \pmod 4$ and where χ_3 is the non-principal character modulo 3.

3.4 Computing $\int_{\mathbb{Z}_2} w_2^*(t)dt$

We begin by recalling that $w_2^*(t) \in \{\pm 1\}$ with $w_2^*(t) \equiv (t^2 - s)_2 w_2(t) \pmod 4$. We consider the usual cases: $0 \leq \nu_2(s) < 2\nu_2(t), 0 \leq 2\nu_2(t) < \nu_2(s)$, and $0 \leq 2\nu_2(t) = \nu_2(s)$.

3.4.1 $0 \leq \nu_2(s) < 2\nu_2(t)$

If $0 \leq \nu_2(s) < 2\nu_2(t)$, then $\nu_2(t^2 - s) = \nu_2(s)$ and $2\nu_2(t) = \nu_2(s) + k$, for some $k \geq 1$; in particular,

$$\begin{aligned} (t^2 - s)_2 &= (t^2 - s)2^{-\nu_2(s)} \\ &= t_2^2 \cdot 2^k - s_2 \\ &\equiv \begin{cases} s_2 \pmod 4 & \text{if } k = 1, \\ -s_2 \pmod 4 & \text{if } k \geq 2. \end{cases} \end{aligned}$$

Therefore,

$$\int_{2\nu_2(t)-\nu_2(s)=k} w_2^*(t)dt = \int_{2\nu_2(t)-\nu_2(s)=k} w_2(t)dt \cdot \begin{cases} \chi_4(s_2) & \text{if } k = 1, \\ -\chi_4(s_2) & \text{if } k \geq 2, \end{cases}$$

where χ_4 is the non-principal character modulo 4.

Since $w_2(t)$ depends only on $\nu_2(t)$ and $t_2 \pmod 4$ (and possibly on $\nu_2(s)$ and s_2), we have that $w_2(t)$ is a 2-uniformly locally constant multiplicative function with uniformity constant $\eta = 2$; i.e.,

$$\int_{2\nu_2(t)-\nu_2(s)=k} w_2(t)dt = \frac{1}{2^{\frac{\nu_2(s)+k}{2}+2}} \sum_{d\in(\mathbb{Z}/4\,\mathbb{Z})^*} w_2(d\cdot 2^{\frac{\nu_2(s)+k}{2}}).$$

Putting all of this together,

$$\int_{0\le\nu_2(s)<2\nu_2(t)} w_2^*(t)dt = \chi_4(s_2)\cdot \begin{cases} -\sum_{k=1}^{\infty}\int_{\nu_2(t)=\frac{\nu_2(s)}{2}+k} w_2(t)dt & \text{if } \nu_2(s)\equiv 0 \pmod 2,\\ \int_{\nu_2(t)=\frac{\nu_2(s)+1}{2}} w_2(t)dt - \sum_{k=1}^{\infty}\int_{\nu_2(t)=\frac{\nu_2(s)+1}{2}+k} w_2(t)dt & \text{if } \nu_2(s)\equiv 1 \pmod 2, \end{cases}$$

where χ_4 is the non-principal character modulo 4 and with $\int_{\nu_2(t)=e} w_2(t)dt$ as above.

From here, a tedious, but straightforward, computation yields:

$$\int_{0\le\nu_2(s)<2\nu_2(t)} w_2^*(t)dt = \begin{cases} 0 & \text{if } \nu_2(s)\equiv 0 \pmod 2,\\ \frac{(-1)^{\frac{\nu_2(s)-1}{2}}}{2^{\frac{\nu_2(s)+3}{2}}}\cdot \begin{cases} 1 & \text{if } s_2\equiv 1,7 \pmod 8,\\ -1 & \text{if } s_2\equiv 3,5 \pmod 8, \end{cases} & \text{if } \nu_2(s)\equiv 1 \pmod 2. \end{cases}$$

3.4.2 $0 \le 2\nu_2(t) < \nu_2(s)$

If $0 \le 2\nu_2(t) < \nu_2(s)$, then $\nu_2(t^2-s) = 2\nu_2(t)$ and $\nu_2(s) = 2\nu_2(t)+k$, for some $k \ge 1$; in particular,

$$\begin{aligned} (t^2-s)_2 &= (t^2-s)2^{-2\nu_2(t)}\\ &= t_2^2 - s_2\cdot 2^k\\ &\equiv \begin{cases} -1 \pmod 4 & \text{if } k=1,\\ 1 \pmod 4 & \text{if } k\ge 2. \end{cases} \end{aligned}$$

Therefore,

$$\int_{\nu_2(s)-2\nu_2(t)=k} w_2^*(t)dt = \int_{\nu_2(s)-2\nu_2(t)=k} w_2(t)dt \cdot \begin{cases} -1 & \text{if } k=1,\\ 1 & \text{if } k\ge 2. \end{cases}$$

Since $w_2(t)$ depends only on $\nu_2(t)$ and $t_2 \pmod 8$ (and possibly on $\nu_2(s)$ and s_2), $w_2(t)$ is a 2-uniformly locally constant multiplicative function with uniformity constant $\eta = 3$; that is,

$$\int_{\nu_2(s)-2\nu_2(t)=k} w_2(t)dt = \frac{1}{2^{\frac{\nu_2(s)-k}{2}+3}} \sum_{d\in(\mathbb{Z}/8\,\mathbb{Z})^*} w_2(d\cdot 2^{\frac{\nu_2(s)-k}{2}}),$$

with

$$\begin{aligned}
&\int_{0\le 2\nu_2(t)<\nu_2(s)} w_2^*(t)dt \\
&= -\int_{\substack{\nu_2(s)-2\nu_2(t)=1\\ 2|\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)=2\\ 2|\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)=3\\ 2|\nu_2(t)}} w_2(t)dt \\
&+ \int_{\substack{\nu_2(s)-2\nu_2(t)=4\\ 2|\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)=5\\ 2|\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)=6\\ 2|\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)\ge 7\\ 2|\nu_2(t)}} w_2(t)dt \\
&- \int_{\substack{\nu_2(s)-2\nu_2(t)=1\\ 2\nmid\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)=2\\ 2\nmid\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)=3\\ 2\nmid\nu_2(t)}} w_2(t)dt + \int_{\substack{\nu_2(s)-2\nu_2(t)\ge 4\\ 2\nmid\nu_2(t)}} w_2(t)dt,
\end{aligned}$$

where we partitioned the integral according to the cases in Proposition A.0.2. From Proposition A.0.2, it is also easy to see that

$$\begin{aligned}
&\int_{\substack{\nu_2(s)-2\nu_2(t)=1\\ 2|\nu_2(t)}} w_2(t)dt, \int_{\substack{\nu_2(s)-2\nu_2(t)=3\\ 2|\nu_2(t)}} w_2(t)dt, \int_{\substack{\nu_2(s)-2\nu_2(t)=6\\ 2|\nu_2(t)}} w_2(t)dt, \\
&\int_{\substack{\nu_2(s)-2\nu_2(t)=1\\ 2\nmid\nu_2(t)}} w_2(t)dt, \int_{\substack{\nu_2(s)-2\nu_2(t)=2\\ 2\nmid\nu_2(t)}} w_2(t)dt, \int_{\substack{\nu_2(s)-2\nu_2(t)\ge 4\\ 2\nmid\nu_2(t)}} w_2(t)dt = 0,
\end{aligned}$$

whereas

$$\int_{\substack{\nu_2(s)-2\nu_2(t)=2\\ 2|\nu_2(t)}} w_2(t)dt = \begin{cases} \frac{1}{2^{\frac{\nu_2(s)}{2}+1}} \cdot \begin{cases} 1 & \text{if } s_2 \equiv 1 \pmod 4, \\ -2 & \text{if } s_2 \equiv 3 \pmod 4, \end{cases} & \text{if } \nu_2(s) \equiv 2 \pmod 4 \text{ and } \nu_2(s) \ge 2, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{\substack{\nu_2(s)-2\nu_2(t)=4\\ 2|\nu_2(t)}} w_2(t)dt = \begin{cases} \frac{1}{2^{\frac{\nu_2(s)}{2}}} & \text{if } \nu_2(s) \equiv 0 \pmod 4 \text{ and } \nu_2(s) \ge 4, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{\substack{\nu_2(s)-2\nu_2(t)=5\\ 2|\nu_2(t)}} w_2(t)dt = \begin{cases} \frac{1}{2^{\frac{\nu_2(s)-1}{2}}} & \text{if } \nu_2(s) \equiv 1 \pmod 4 \text{ and } \nu_2(s) \ge 5, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{\substack{\nu_2(s)-2\nu_2(t)\ge 7\\ 2|\nu_2(t)}} w_2(t)dt = \sum_{\substack{7\le k\le \nu_2(s)\\ k\equiv \nu_2(s) \pmod 4}} \frac{-2}{2^{\frac{\nu_2(s)-k}{2}+3}} = \begin{cases} \frac{1}{3}\left(\frac{2^{2\lceil \frac{7-j}{4}\rceil}}{2^{\frac{\nu_2(s)-j}{2}+2}} - 1\right) & \text{if } \nu_2(s) \ge 7, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{\substack{\nu_2(s)-2\nu_2(t)=3\\ 2\nmid\nu_2(t)}} w_2(t)dt = \begin{cases} \frac{-\chi_4(s_2)}{2^{\frac{\nu_2(s)-1}{2}}} & \text{if } \nu_2(s) \equiv 1 \pmod 4 \text{ and } \nu_2(s) \ge 5, \\ 0 & \text{otherwise.} \end{cases}$$

Summing the individual contributions,

$$\int_{0\le 2\nu_2(t)<\nu_2(s)} w_2^*(t)dt$$

$$= \begin{cases} 0 & \text{if } \nu_2(s)=0,\\ 0 & \text{if } \nu_2(s)=1,\\ \frac{1}{4}\cdot\begin{cases}1 & \text{if } s_2\equiv 1 \pmod 4,\\ -2 & \text{if } s_2\equiv 3 \pmod 4,\end{cases} & \text{if } \nu_2(s)=2,\\ 0 & \text{if } \nu_2(s)=3,\\ \frac{1}{4} & \text{if } \nu_2(s)=4,\\ \frac{1-\chi_4(s_2)}{4} & \text{if } \nu_2(s)=5,\\ \frac{1}{16}\cdot\begin{cases}1 & \text{if } s_2\equiv 1 \pmod 4,\\ -2 & \text{if } s_2\equiv 3 \pmod 4,\end{cases} & \text{if } \nu_2(s)=6,\\ \frac{1}{3}\left(\frac{2^{2\lceil\frac{7-j}{4}\rceil}}{2^{\frac{\nu_2(s)-j}{2}+2}}-1\right)+\frac{1}{2^{\frac{\nu_2(s)-j}{2}}}\begin{cases}1 & \text{if } \nu_2(s)\equiv 0 \pmod 4,\\ 1-\chi_4(s_2) & \text{if } \nu_2(s)\equiv 1 \pmod 4,\\ \begin{cases}\frac{1}{4} & \text{if } s_2\equiv 1 \pmod 4,\\ \frac{-1}{2} & \text{if } s_2\equiv 3 \pmod 4,\end{cases} & \text{if } \nu_2(s)\equiv 2 \pmod 4,\\ 0 & \text{if } \nu_2(s)\equiv 3 \pmod 4,\end{cases} & \text{if } \nu_2(s)\ge 7,\end{cases}$$

where $j\in\{0,1,2,3\}$ such that $\nu_2(s)\equiv j \pmod 4$ and where χ_4 is the non-principal character modulo 4.

3.4.3 $0\le 2\nu_2(t)=\nu_2(s)$

To deal with the case where $0\le 2\nu_2(t)=\nu_2(s)$, we first write

$$\int_{0\le 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt=\sum_{k=0}^{\infty}\int_{\substack{2\nu_2(t)=\nu_2(s)\\ \nu_2(t^2-s)=\nu_2(s)+k}} w_2^*(t)dt,$$

with $w_2^*(t)\in\{\pm 1\}$ such that

$$w_2^*(t)\equiv (t^2-s)_2 w_2(t) \pmod 4,$$

where $w_2(t)$ is given by Proposition A.0.2 in Appendix A.

Since $w_2^*(t)$ depends only on $\nu_2(t)$, $t_2 \pmod 8$, and $(t^2-s)_2 \pmod 8$, we have that

$$\int_{\substack{2\nu_2(t)=\nu_2(s)\\ \nu_2(t^2-s)=\nu_2(s)+k}} w_2^*(t)dt=\frac{1}{2^{\frac{\nu_2(s)}{2}+k+3}}\sum_{\substack{d\in(\mathbb{Z}/2^{k+3}\mathbb{Z})^*\\ d^2\equiv s_2 \pmod{2^k}\\ d^2\not\equiv s_2 \pmod{2^{k+1}}}}(d^2-s_2)_2' w_2(d\cdot 2^{\frac{\nu_2(s)}{2}}),$$

where the $\prime$ indicates that we take $(d^2-s_2)_2'$ in $\{\pm 1\}$ such that $(d^2-s_2)_2 \equiv (d^2-s_2)_2' \pmod 4$; hence,

$$\int_{0\leq 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt = \sum_{k=0}^{\infty} \frac{1}{2^{\frac{\nu_2(s)}{2}+k+3}} \sum_{\substack{d\in(\mathbb{Z}/2^{k+3}\mathbb{Z})^* \\ d^2\equiv s_2 \pmod{2^k} \\ d^2\not\equiv s_2 \pmod{2^{k+1}}}} (d^2-s_2)_2' w_2(d\cdot 2^{\frac{\nu_2(s)}{2}}). \tag{2}$$

From here, we consider various cases:

(1) $s_2 \equiv 3 \pmod 4$: Let $d \in (\mathbb{Z}/2^{k+3}\mathbb{Z})^*$ and suppose that $d^2 \equiv s_2 \pmod{2^k}$, with $k \geq 2$. Then, $d^2 \equiv s_2 \pmod 4$. Under the assumption that $s_2 \equiv 3 \pmod 4$, we have that $d^2 \equiv 3 \pmod 4$, a contradiction, as all $d \in (\mathbb{Z}/2^{k+3}\mathbb{Z})^*$ have squares equivalent to 1 modulo 4; and so, the sums

$$\sum_{\substack{d\in(\mathbb{Z}/2^{k+3}\mathbb{Z})^* \\ d^2\equiv s_2 \pmod{2^k} \\ d^2\not\equiv s_2 \pmod{2^{k+1}}}} (d^2-s_2)_2' w_2(d\cdot 2^{\frac{\nu_2(s)}{2}})$$

are empty for all $k \geq 2$. Similarly, there are no $d \in (\mathbb{Z}/8\mathbb{Z})^*$ with $d^2 \not\equiv 1 \pmod 2$, so that the above sum is also empty for $k=0$. On the other hand, all $d \in (\mathbb{Z}/16\mathbb{Z})^*$ are such that $d^2 \equiv 1 \pmod 2, \not\equiv 3 \pmod 4$; that is,

$$\sum_{\substack{d\in(\mathbb{Z}/16\mathbb{Z})^* \\ d^2\equiv s_2 \pmod 2 \\ d^2\not\equiv s_2 \pmod 4}} (d^2-s_2)_2' w_2(d\cdot 2^{\frac{\nu_2(s)}{2}}) = \sum_{d\in(\mathbb{Z}/16\mathbb{Z})^*} (d^2-s_2)_2' w_2(d\cdot 2^{\frac{\nu_2(s)}{2}}).$$

It now follows that the only contribution to Equation 2, when $s_2 \equiv 3 \pmod 4$, comes from $k=1$; in other words,

$$\int_{0\leq 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt = \frac{1}{2^{\frac{\nu_2(s)}{2}+4}} \sum_{d\in(\mathbb{Z}/16\mathbb{Z})^*} (d^2-s_2)_2' w_2(d\cdot 2^{\frac{\nu_2(s)}{2}}).$$

By considering $(d^2-s_2)_2$ for $s_2 \equiv 3,7,11,15 \pmod{16}$ and as d varies over $(\mathbb{Z}/16\mathbb{Z})^*$, we get that

$$\int_{0\leq 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt = \begin{cases} \begin{cases} 0 & \text{if } s_2 \equiv 3 \pmod 8, \\ \frac{-1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 7 \pmod{16}, \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 15 \pmod{16}, \end{cases} & \text{if } \nu_2(s) \equiv 0 \pmod 4, \\ 0 & \text{if } \nu_2(s) \equiv 2 \pmod 4. \end{cases}$$

(2) $s_2 \equiv 5 \pmod 8$: Similarly to the case above, let $d \in (\mathbb{Z}/2^{k+3}\mathbb{Z})^*$ and suppose that $d^2 \equiv s_2 \pmod{2^k}$, with $k \geq 3$. Then, $d^2 \equiv s_2 \pmod 8$. Under the assumption that $s_2 \equiv 5 \pmod 8$, we have that $d^2 \equiv 5 \pmod 8$, a contradiction, as all $d \in (\mathbb{Z}/2^{k+3}\mathbb{Z})^*$ have squares equivalent to 1 modulo 8. So, the sums

$$\sum_{\substack{d\in(\mathbb{Z}/2^{k+3}\mathbb{Z})^* \\ d^2\equiv s_2 \pmod{2^k} \\ d^2\not\equiv s_2 \pmod{2^{k+1}}}} (d^2-s_2)_2' w_2(d\cdot 2^{\frac{\nu_2(s)}{2}})$$

are empty for all $k \geq 3$. Similarly, there are no $d \in (\mathbb{Z}/8\mathbb{Z})^*$ (resp. $(\mathbb{Z}/16\mathbb{Z})^*$) with $d^2 \not\equiv 1 \pmod 2$ (resp.

$d^2 \equiv 1 \pmod 2, \not\equiv 1 \pmod 4$), so that the above sums are also empty for $k = 0, 1$. On the other hand, all $d \in (\mathbb{Z}/32\,\mathbb{Z})^*$ are such that $d^2 \equiv 1 \pmod 4, \not\equiv 5 \pmod 8$; that is,

$$\sum_{\substack{d\in(\mathbb{Z}/32\,\mathbb{Z})^* \\ d^2\equiv s_2 \pmod 4 \\ d^2\not\equiv s_2 \pmod 8}} (d^2 - s_2)_2' w_2(d \cdot 2^{\frac{\nu_2(s)}{2}}) = \sum_{d\in(\mathbb{Z}/32\,\mathbb{Z})^*} (d^2 - s_2)_2' w_2(d \cdot 2^{\frac{\nu_2(s)}{2}}).$$

It now follows that the only contribution to Equation 2, when $s_2 \equiv 5 \pmod 8$, comes from $k = 2$; i.e.,

$$\int_{0\le 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt = \frac{1}{2^{\frac{\nu_2(s)}{2}+5}} \sum_{d\in(\mathbb{Z}/32\,\mathbb{Z})^*} (d^2 - s_2)_2' w_2(d \cdot 2^{\frac{\nu_2(s)}{2}}).$$

By considering $(d^2 - s_2)_2$ for $s_2 \equiv 5, 13 \pmod{16}$, $d \in (\mathbb{Z}/32\,\mathbb{Z})^*$, it is also not hard to show that

$$\int_{0\le 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt = \begin{cases} 0 & \text{if } \nu_2(s) \equiv 0 \pmod 4, \\ \begin{cases} \frac{1}{2^{\frac{\nu_2(s)}{2}+2}} & \text{if } s_2 \equiv 5 \pmod{16}, \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 13 \pmod{16}, \end{cases} & \text{if } \nu_2(s) \equiv 2 \pmod 4. \end{cases}$$

(3) $s_2 \equiv 1 \pmod 8$: In the case where $s_2 \equiv 1 \pmod 8$, we apply a less barbaric approach to computing $\int_{0\le 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt$. Firstly, notice that there are no $d \in (\mathbb{Z}/2^{k+3}\,\mathbb{Z})^*$ such that $d^2 \equiv 1 \pmod{2^k} \not\equiv 1 \pmod{2^{k+1}}$ for $k = 0, 1, 2$; that is,

$$\int_{0\le 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt = \sum_{k=3}^{\infty} \frac{1}{2^{\frac{\nu_2(s)}{2}+k+3}} \sum_{\substack{d\in(\mathbb{Z}/2^{k+3}\,\mathbb{Z})^* \\ d^2\equiv s_2 \pmod{2^k} \\ d^2\not\equiv s_2 \pmod{2^{k+1}}}} (d^2 - s_2)_2' w_2(d \cdot 2^{\frac{\nu_2(s)}{2}}).$$

Our next goal is to characterize all $d \in (\mathbb{Z}/2^{k+3}\,\mathbb{Z})^*$ such that $d^2 \equiv s_2 \pmod{2^k}, \not\equiv s_2 \pmod{2^{k+1}}$, for $k \ge 3$. We begin by noting that all integers congruent to 1 modulo 8 admit a square root in $\mathbb{Z}_2$ (this follows from Hensel's Lemma). So, let $\pm\sqrt{s_2}$ denote the square roots of s_2 in $\mathbb{Z}_2$ and consider

$$d = d(\alpha_1, \alpha_2) = \pm(\sqrt{s_2} + 2^{k-1}(1 + \alpha_1 \cdot 2 + \alpha_2 \cdot 2^2 + \alpha_3 \cdot 2^3)) + 2^{k+3}\,\mathbb{Z}_2 \tag{3}$$

$$\in (\mathbb{Z}_2/2^{k+3}\,\mathbb{Z}_2)^* \cong (\mathbb{Z}/2^{k+3}\,\mathbb{Z})^*, \tag{4}$$

where $\alpha_i \in \{0, 1\}, i = 1, 2, 3$. Then, $d^2 \equiv s_2 \pmod{2^k}, \not\equiv s_2 \pmod{2^{k+1}}$. Moreover,

$$(d^2 - s_2)_2 \equiv \begin{cases} 2(1 + 2\alpha_1) + \sqrt{s_2}(1 + 2\alpha_1 + 4\alpha_2) \pmod 8 & \text{if } k = 3, \\ 4 + \sqrt{s_2}(1 + 2\alpha_1 + 4\alpha_2) \pmod 8 & \text{if } k = 4, \\ \sqrt{s_2}(1 + 2\alpha_1 + 4\alpha_2) \pmod 8 & \text{if } k \ge 5. \end{cases}$$

Remark 3.4.1. *The reason we label d above as $d(\alpha_1, \alpha_2)$ will become apparent. Essentially, we only care for the values of $d, (d^2 - s_2)_2$ modulo 8, so that the value of α_3 is irrelevant in our calculations: from Proposition A.0.2, $w_2(t)$ is completely determined by $\nu_2(t)$ and $t_2, (t_2^2 - s_2)_2$ (mod 8).*

What's important to note is that the value of $(d^2 - s_2)_2'$ depends only on α_1. Furthermore, the values of

$(d^2-s_2)'_2$ at $\alpha_1=0$ and $\alpha_1=1$ are negatives of one another! We claim further that Equation 3 characterizes all $d\in(\mathbb{Z}/2^{k+3}\mathbb{Z})^*$ such that $d^2\equiv s_2 \pmod{2^k}, \not\equiv s_2 \pmod{2^{k+1}}$: this follows from a simple counting argument. First note that there are exactly four $d\in(\mathbb{Z}/2^k\mathbb{Z})^*$ such that $d^2\equiv s_2 \pmod{2^k}$, each of which lifts in exactly two ways to $d\in(\mathbb{Z}/2^{k+1}\mathbb{Z})^*$ such that $d^2\equiv s_2 \pmod{2^k}$. Of these eight solutions, exactly four satisfy $d^2\equiv s_2 \pmod{2^{k+1}}$; that is, there are exactly four $d\in(\mathbb{Z}/2^{k+1}\mathbb{Z})^*$ such that $d^2\equiv s_2 \pmod{2^k}, \not\equiv s_2 \pmod{2^{k+1}}$, each of which lifts in exactly four ways to $d\in(\mathbb{Z}/2^{k+3}\mathbb{Z})^*$ such that $d^2\equiv s_2 \pmod{2^k}, \not\equiv s_2 \pmod{2^{k+1}}$.

By the preceding remarks, we may write

$$\sum_{\substack{d\in(\mathbb{Z}/2^{k+3}\mathbb{Z})^*\\ d^2\equiv s_2 \pmod{2^k}\\ d^2\not\equiv s_2 \pmod{2^{k+1}}}} (d^2-s_2)'_2 w_2(d\cdot 2^{\frac{\nu_2(s)}{2}})$$

as

$$(2\chi_{k=3}(k)+\sqrt{s_2})'\Bigg(\Big(w_2(d(0,0)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(0,0)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(d(0,1)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(0,1)\cdot 2^{\frac{\nu_2(s)}{2}})\Big)$$
$$-\Big(w_2(d(1,0)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(1,0)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(d(1,1)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(1,1)\cdot 2^{\frac{\nu_2(s)}{2}})\Big)\Bigg).$$

A case by case analysis then shows that, for $s_2\equiv 1 \pmod 8$,

$$\int_{0\le 2\nu_2(t)=\nu_2(s)} w_2^*(t)dt = \begin{cases} 0 & \text{if } \nu_2(s)\equiv 0 \pmod 4,\\ \frac{-1}{2^{\frac{\nu_2(s)}{2}+2}} & \text{if } \nu_2(s)\equiv 2 \pmod 4.\end{cases}$$

For the sake of completeness, we say a few more words. We deal with the case where $\nu_2(s)\equiv 0 \pmod 4$, the case where $\nu_2(s)\equiv 2 \pmod 4$ being eerily similar. Firstly, recall that $k\ge 3$.

If $k\equiv 0,2,3,4 \pmod 6, k\neq 2,3$, then $w_2(d\cdot 2^{\frac{\nu_2(s)}{2}})=1$ iff $d\equiv (d^2-s_2)_2 \pmod 4$; in particular, $w_2(d\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d\cdot 2^{\frac{\nu_2(s)}{2}})=0$ for all d. Therefore, the sums over $k\equiv 0,2,3,4 \pmod 6, k\neq 2,3,4$ are all equal to 0.

If $k\equiv 1,5 \pmod 6, k\neq 1,5$, then $w_2(d\cdot 2^{\frac{\nu_2(s)}{2}})=-1$ for all d; in this case,

$$w_2(d(0,0)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(0,0)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(d(0,1)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(0,1)\cdot 2^{\frac{\nu_2(s)}{2}})$$
$$=w_2(d(1,0)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(1,0)\cdot 2^{\frac{\nu_2(s)}{2}}))+w_2(d(1,1)\cdot 2^{\frac{\nu_2(s)}{2}})+w_2(-d(1,1)\cdot 2^{\frac{\nu_2(s)}{2}}).$$

Again, the sums over $k\equiv 1,5 \pmod 6, k\neq 1,5$, are equal to 0.

For $k=3$, $w_2(d\cdot 2^{\frac{\nu_2(s)}{2}})=1$ iff $d\equiv 1 \pmod 4$ and $d(d^2-s_2)_2\equiv 5,7 \pmod 8$ or $d\equiv 3 \pmod 4$ and $d(d^2-s_2)_2\equiv 3,5 \pmod 8$. Since $d\equiv\pm\sqrt{s_2} \pmod 4$ and since

$$d(d^2-s_2)_2\equiv\pm\begin{cases} 6\sqrt{s_2}+1 & \text{if } \alpha_1=0,\alpha_2=0,\\ 6\sqrt{s_2}+5 & \text{if } \alpha_1=0,\alpha_2=1,\\ 6\sqrt{s_2}+3 & \text{if } \alpha_1=1,\alpha_2=0,\\ 6\sqrt{s_2}+7 & \text{if } \alpha_1=1,\alpha_2=1,\end{cases}$$

it is easy to see that the sum at $k = 3$ is also 0.

Similarly, for the sum at $k = 5$, $w_2(d \cdot 2^{\frac{\nu_2(s)}{2}}) = 1$ iff $d(d^2 - s_2)_2 \equiv 1, 3, 7 \pmod 8$. In this case,

$$d(d^2 - s_2)_2 = \pm \begin{cases} 1 & \text{if } \alpha_1 = 0, \alpha_2 = 0, \\ 5 & \text{if } \alpha_1 = 0, \alpha_2 = 1, \\ 3 & \text{if } \alpha_1 = 1, \alpha_2 = 0, \\ 7 & \text{if } \alpha_1 = 1, \alpha_2 = 1; \end{cases}$$

in particular, the sum at $k = 5$ is 0.

To summarize this subsection,

$$\int_{0 \le 2\nu_2(t) = \nu_2(s)} w_2^*(t)dt = \begin{cases} 0 & \text{if } \nu_2(s) \equiv 1 \pmod 2, \\ \begin{cases} 0 & \text{if } s_2 \equiv 1, 3, 5 \pmod 8, \\ \frac{-1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 7 \pmod{16}, \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 15 \pmod{16}, \end{cases} & \text{if } \nu_2(s) \equiv 0 \pmod 4, \\ \begin{cases} 0 & \text{if } s_2 \equiv 3 \pmod 4, \\ \frac{-1}{2^{\frac{\nu_2(s)}{2}+2}} & \text{if } s_2 \equiv 1 \pmod 8, \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+2}} & \text{if } s_2 \equiv 5 \pmod{16}, \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 13 \pmod{16}, \end{cases} & \text{if } \nu_2(s) \equiv 2 \pmod 4. \end{cases}$$

Combining the results of the previous three subsections,

Proposition 3.4.1.

$$\int_{\mathbb{Z}_2} w_2^*(t)dt$$

$$= \begin{cases} 0 & \text{if } \nu_2(s) \equiv 0 \ (mod\ 2), \\ \frac{(-1)^{\frac{\nu_2(s)-1}{2}}}{2^{\frac{\nu_2(s)+3}{2}}} \begin{cases} 1 & \text{if } s_2 \equiv 1,7 \ (mod\ 8), \\ -1 & \text{if } s_2 \equiv 3,5 \ (mod\ 8), \end{cases} & \text{if } \nu_2(s) \equiv 1 \ (mod\ 2), \end{cases}$$

$$+ \begin{cases} 0 & \text{if } \nu_2(s) = 0, \\ 0 & \text{if } \nu_2(s) = 1, \\ \frac{1}{4} \cdot \begin{cases} 1 & \text{if } s_2 \equiv 1 \ (mod\ 4), \\ -2 & \text{if } s_2 \equiv 3 \ (mod\ 4), \end{cases} & \text{if } \nu_2(s) = 2, \\ 0 & \text{if } \nu_2(s) = 3, \\ \frac{1}{4} & \text{if } \nu_2(s) = 4, \\ \frac{1-\chi_4(s_2)}{4} & \text{if } \nu_2(s) = 5, \\ \frac{1}{16} \cdot \begin{cases} 1 & \text{if } s_2 \equiv 1 \ (mod\ 4), \\ -2 & \text{if } s_2 \equiv 3 \ (mod\ 4), \end{cases} & \text{if } \nu_2(s) = 6, \\ \frac{1}{3}\left(\frac{2^{2\lceil \frac{7-j}{4} \rceil}}{2^{\frac{\nu_2(s)-j}{2}+2}} - 1 \right) + \frac{1}{2^{\frac{\nu_2(s)-j}{2}}} \begin{cases} 1 & \text{if } \nu_2(s) \equiv 0 \ (mod\ 4), \\ 1-\chi_4(s_2) & \text{if } \nu_2(s) \equiv 1 \ (mod\ 4), \\ \begin{cases} \frac{1}{4} & \text{if } s_2 \equiv 1 \ (mod\ 4), \\ \frac{-1}{2} & \text{if } s_2 \equiv 3 \ (mod\ 4), \end{cases} & \text{if } \nu_2(s) \equiv 2 \ (mod\ 4), \\ 0 & \text{if } \nu_2(s) \equiv 3 \ (mod\ 4),. \end{cases} & \text{if } \nu_2(s) \geq 7, \end{cases}$$

$$+ \begin{cases} 0 & \text{if } \nu_2(s) \equiv 1 \ (mod\ 2), \\ \begin{cases} 0 & \text{if } s_2 \equiv 1,3,5 \ (mod\ 8), \\ \frac{-1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 7 \ (mod\ 16), \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 15 \ (mod\ 16), \end{cases} & \text{if } \nu_2(s) \equiv 0 \ (mod\ 4), \\ \begin{cases} 0 & \text{if } s_2 \equiv 3 \ (mod\ 4), \\ \frac{-1}{2^{\frac{\nu_2(s)}{2}+2}} & \text{if } s_2 \equiv 1 \ (mod\ 8), \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+2}} & \text{if } s_2 \equiv 5 \ (mod\ 16), \\ \frac{1}{2^{\frac{\nu_2(s)}{2}+1}} & \text{if } s_2 \equiv 13 \ (mod\ 16), \end{cases} & \text{if } \nu_2(s) \equiv 2 \ (mod\ 4), \end{cases}$$

where $j \in \{0,1,2,3\}$ such that $\nu_2(s) \equiv j \ (mod\ 4)$ and where χ_4 is the non-principal character modulo 4.

Appendix A

Local root numbers of $\mathcal{F}_s(t)$ at $p = 2, 3$

Recall that

$$\mathcal{F}_s(t) : y^2 = x^3 + 3tx^2 + 3sx + st,\ s \in \mathbb{Z}, s \neq 0,$$

with

$$\begin{aligned} c_4(t) &= 2^4 3^2 (t^2 - s), \\ c_6(t) &= -2^6 3^3 t(t^2 - s), \\ \Delta(t) &= -2^6 3^3 s(t^2 - s)^2, \\ j(t) &= \frac{-2^6 3^3}{s}(t^2 - s). \end{aligned}$$

Proposition A.0.1. *The local root number of $\mathcal{F}_s(t)$ at $p = 3$ is given by:*

- *if* $0 \leq \nu_3(s) < 2\nu_3(t)$, *then*
  - *if* $\nu_3(s) \equiv 0 \pmod 4$, *then*
    - *if* $\nu_3(t) = \frac{\nu_3(s)}{2} + 1$, *then* $w_3(t) = 1$ *iff* $t_3 \equiv 1 \pmod 3$;
    - *if* $\nu_3(t) > \frac{\nu_3(s)}{2} + 1$, *then* $w_3(t) = 1$;
  - *if* $\nu_3(s) \equiv 1 \pmod 4$, *then*
    - *if* $\nu_3(t) = \frac{\nu_3(s)}{2} + \frac{1}{2}$, *then* $w_3(t) = 1$ *iff* $s_3 \equiv 1 \pmod 3$;
    - *if* $\nu_3(t) > \frac{\nu_3(s)}{2} + \frac{1}{2}$, *then* $w_3(t) = -1$;
  - *if* $\nu_3(s) \equiv 2 \pmod 4$, *then*
    - *if* $\nu_3(t) = \frac{\nu_3(s)}{2} + 1$, *then* $w_3(t) = 1$ *iff* $t_3 \not\equiv s_3 \pmod 3$;
    - *if* $\nu_3(t) > \frac{\nu_3(s)}{2} + 1$, *then* $w_3(t) = 1$;
  - *if* $\nu_3(s) \equiv 3 \pmod 4$, *then* $w_3(t) = 1$;
- *if* $0 \leq 2\nu_3(t) < \nu_3(s)$, *then*
  - *if* $\nu_3(t) \equiv 0 \pmod 2$, *then*

    - *if* $\nu_3(s) - 2\nu_3(t) = 1$, *then* $w_3(t) = 1$;
    - *if* $\nu_3(s) - 2\nu_3(t) = 2$, *then* $w_3(t) = 1$ *iff* $t_3 \equiv s_3 \pmod 3$;
    - *if* $\nu_3(s) - 2\nu_3(t) \geq 3$, *then* $w_3(t) = -1$;
  - *if* $\nu_3(t) \equiv 1 \pmod 2$, *then*
    - *if* $\nu_3(s) - 2\nu_3(t) = 1$, *then* $w_3(t) = 1$ *iff* $s_3 \equiv 1 \pmod 3$;
    - *if* $\nu_3(s) - 2\nu_3(t) = 2$, *then* $w_3(t) = 1$ *iff* $t_3 \equiv 2 \pmod 3$;
    - *if* $\nu_3(s) - 2\nu_3(t) = 3$, *then* $w_3(t) = 1$;
    - *if* $\nu_3(s) - 2\nu_3(t) \geq 4$, *then* $w_3(t) = 1$ *iff* $t_3 \equiv 2 \pmod 3$;
- *if* $0 \leq 2\nu_3(t) = \nu_3(s)$, *then*
  - *if* $\nu_3(s) \equiv 0 \pmod 4$, *then*
    - *if* $\nu_3(t^2 - s) = \nu_3(s)$, *then* $w_3(t) = 1$ *iff* $s_3 \equiv 2 \pmod 3$ *and* $s_3 t_3 \not\equiv 2, 4 \pmod 9$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 0 \pmod 6, \nu_3(t^2 - s) \neq \nu_3(s)$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \not\equiv 7, 8 \pmod 9$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 1, 2 \pmod 6$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \equiv 1 \pmod 3$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 3 \pmod 6$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \not\equiv 1, 2 \pmod 9$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 4, 5 \pmod 6$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \equiv 2 \pmod 3$;
  - *if* $\nu_3(s) \equiv 2 \pmod 4$, *then*
    - *if* $\nu_3(t^2 - s) = \nu_3(s)$, *then* $w_3(t) = 1$ *iff* $s_3 \equiv 2 \pmod 3$ *and* $s_3 t_3 \not\equiv 2, 4 \pmod 9$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 0 \pmod 6, \nu_3(t^2 - s) \neq \nu_3(s)$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \not\equiv 1, 2 \pmod 9$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 1, 2 \pmod 6$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \equiv 2 \pmod 3$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 3 \pmod 6$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \not\equiv 7, 8 \pmod 9$;
    - *if* $\nu_3(t^2 - s) - \nu_3(s) \equiv 4, 5 \pmod 6$, *then* $w_3(t) = 1$ *iff* $t_3(t_3^2 - s_3)_3 \equiv 1 \pmod 3$.

Proposition A.0.2. *The local root number of* $\mathcal{F}_s(t)$ *at* $p = 2$ *is given by:*

- *if* $0 \leq \nu_2(s) < 2\nu_2(t)$, *then*
  - *if* $\nu_2(s) \equiv 0 \pmod 4$, *then*
    - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} = 1$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 3 \pmod 4$ *or* $s_2 \equiv 1, 13 \pmod{16}$ *and* $t_2 \equiv 3 \pmod 4$ *or* $s_2 \equiv 5, 9 \pmod{16}$ *and* $t_2 \equiv 1 \pmod 4$;
    - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} = 2$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 5, 9 \pmod{16}$;
    - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} \geq 3$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1, 13 \pmod{16}$;
  - *if* $\nu_2(s) \equiv 1 \pmod 4$, *then*
    - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} = \frac{1}{2}$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1, 3 \pmod 8$ *and* $t_2 \equiv 3 \pmod 4$ *or* $s_2 \equiv 5, 7 \pmod 8$ *and* $t_2 \equiv 1 \pmod 4$;
    - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} \geq 1$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 5, 7 \pmod 8$;
  - *if* $\nu_2(s) \equiv 2 \pmod 4$, *then*
    - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} = 1$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1 \pmod 4$ *or* $s_2 \equiv 3, 7 \pmod{16}$ *and* $t_2 \equiv 1 \pmod 4$ *or* $s_2 \equiv 11, 15 \pmod{16}$ *and* $t_2 \equiv 3 \pmod 4$;

        - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} = 2$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 7, 11 \pmod{16}$;
        - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} \geq 3$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 3, 15 \pmod{16}$;
    - *if* $\nu_2(s) \equiv 3 \pmod{4}$, *then*
        - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} = \frac{1}{2}$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1, 7 \pmod{8}$ *and* $t_2 \equiv 1 \pmod{4}$ *or* $s_2 \equiv 3, 5 \pmod{8}$ *and* $t_2 \equiv 3 \pmod{4}$;
        - *if* $\nu_2(t) - \frac{\nu_2(s)}{2} \geq 1$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1, 3 \pmod{8}$;
- *if* $0 \leq 2\nu_2(t) < \nu_2(s)$, *then*
    - *if* $\nu_2(t)$ *is even, then*
        - *if* $\nu_2(s) - 2\nu_2(t) = 1$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1 \pmod{4}$ *and* $t_2 \equiv 1, 7 \pmod{8}$ *or* $s_2 \equiv 3 \pmod{4}$ *and* $t_2 \equiv 1, 3 \pmod{8}$;
        - *if* $\nu_2(s) - 2\nu_2(t) = 2$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1 \pmod{8}$ *and* $t_2 \equiv 3, 5, 7 \pmod{8}$ *or* $s_2 \equiv 5 \pmod{8}$ *and* $t_2 \equiv 1, 3, 7 \pmod{8}$;
        - *if* $\nu_2(s) - 2\nu_2(t) = 3$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 1 \pmod{4}$ *and* $t_2 \equiv 3, 5 \pmod{8}$ *or* $s_2 \equiv 3 \pmod{4}$ *and* $t_2 \equiv 1, 3 \pmod{8}$;
        - *if* $\nu_2(s) - 2\nu_2(t) = 4$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 1 \pmod{4}$ *or* $s_2 \equiv 1 \pmod{4}$ *and* $t_2 \equiv 3 \pmod{8}$ *or* $s_2 \equiv 3 \pmod{4}$ *and* $t_2 \equiv 7 \pmod{8}$;
        - *if* $\nu_2(s) - 2\nu_2(t) = 5$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 1 \pmod{4}$ *or* $t_2 \equiv 7 \pmod{8}$;
        - *if* $\nu_2(s) - 2\nu_2(t) = 6$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 3 \pmod{4}$;
        - *if* $\nu_2(s) - 2\nu_2(t) \geq 7$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 7 \pmod{8}$;
    - *if* $\nu_2(t)$ *is odd, then*
        - *if* $\nu_2(s) - 2\nu_2(t) = 1$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv s_2, s_2 + 2 \pmod{8}$;
        - *if* $\nu_2(s) - 2\nu_2(t) = 2$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv s_2 \pmod{4}$;
        - *if* $\nu_2(s) - 2\nu_2(t) = 3$, *then* $w_2(t) = 1$ *iff* $s_2 \equiv 3 \pmod{4}$;
        - *if* $\nu_2(s) - 2\nu_2(t) \geq 4$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 3 \pmod{4}$.
- *if* $0 \leq 2\nu_2(t) = \nu_2(s)$, *then*
    - *if* $\nu_2(s) \equiv 0 \pmod{4}$, *then*
        - *if* $\nu_2(t^2 - s) - \nu_2(s) \equiv 0 \pmod{6}$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
        - *if* $\nu_2(t^2 - s) - \nu_2(s) = 1$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 1 \pmod{4}$ *and* $t_2(t^2 - s)_2 \equiv 1, 7 \pmod{8}$ *or* $t_2 \equiv 3 \pmod{4}$ *and* $t_2(t^2 - s)_2 \equiv 5, 7 \pmod{8}$;
        - *if* $\nu_2(t^2 - s) - \nu_2(s) \equiv 1 \pmod{6}$ *and* $\nu_2(t^2 - s) - \nu_2(s) > 1$, *then* $w_2(t) = -1$;
        - *if* $\nu_2(t^2 - s) - \nu_2(s) = 2$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 3 \pmod{4}$;
        - *if* $\nu_2(t^2 - s) - \nu_2(s) \equiv 2 \pmod{6}$ *and* $\nu_2(t^2 - s) - \nu_2(s) > 2$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
        - *if* $\nu_2(t^2 - s) - \nu_2(s) = 3$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv 1 \pmod{4}$ *and* $t_2(t^2 - s)_s \equiv 5, 7 \pmod{8}$ *or* $t_2 \equiv 3 \pmod{4}$ *and* $t_2(t^2 - s)_2 \equiv 3, 5 \pmod{8}$;
        - *if* $\nu_2(t^2 - s) - \nu_2(s) \equiv 3 \pmod{6}$ *and* $\nu_2(t^2 - s) - \nu_2(s) > 3$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
        - *if* $\nu_2(t^2 - s) - \nu_2(s) \equiv 4 \pmod{6}$, *then* $w_2(t) = 1$ *iff* $t_2 \equiv (t^2 - s)_2 \pmod{4}$;

- *if* $\nu_2(t^2-s)-\nu_2(s)=5$, *then* $w_2(t)=1$ *iff* $t_2(t^2-s)_2\equiv 1,3,7\ (mod\ 8)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)\equiv 5\ (mod\ 6)$ *and* $\nu_2(t^2-s)-\nu_2(s)>5$, *then* $w_2(t)=-1$.

◦ *if* $\nu_2(s)\equiv 2\ (mod\ 4)$, *then*

- *if* $\nu_2(t^2-s)-\nu_2(s)\equiv 0\ (mod\ 6)$, *then* $w_2(t)=1$ *iff* $t_2\equiv(t^2-s)_2\ (mod\ 4)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)=1$, *then* $w_2(t)=1$ *iff* $t_2\equiv 3\ (mod\ 8)$ *or* $t_2\equiv 1\ (mod\ 8)$ *and* $(t^2-s)_2\equiv 1,5\ (mod\ 8)$ *or* $t_2\equiv 5\ (mod\ 8)$ *and* $(t^2-s)_2\equiv 3,7\ (mod\ 8)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)\equiv 1\ (mod\ 6)$ *and* $\nu_2(t^2-s)-\nu_2(s)>1$, *then* $w_2(t)=1$ *iff* $t_2\equiv(t^2-s)_2\ (mod\ 4)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)=2$, *then* $w_2(t)=1$ *iff* $t_2\equiv(t^2-s)_2\equiv 1\ (mod\ 4)$ *or* $t_2\equiv 7\ (mod\ 8)$ *and* $(t^2-s)_2\equiv 1\ (mod\ 4)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)\equiv 2\ (mod\ 6)$ *and* $\nu_2(t^2-s)-\nu_2(s)>2$, *then* $w_2(t)=-1$;
- *if* $\nu_2(t^2-s)-\nu_2(s)=3$, *then* $w_2(t)=1$ *iff* $(t^2-2)_2\equiv 3\ (mod\ 4)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)\equiv 3\ (mod\ 6)$ *and* $\nu_2(t^2-s)-\nu_2(s)>3$, *then* $w_2(t)=1$ *iff* $t_2\equiv(t^2-s)_2\ (mod\ 4)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)=4$, *then* $w_2(t)=1$ *iff* $t_2\equiv 1\ (mod\ 4)$ *and* $t_2(t^2-s)_2\equiv 3,5,7\ (mod\ 8)$ *or* $t_2\equiv 3\ (mod\ 4)$ *and* $t_2(t^2-s)_2\equiv 1,3,7\ (mod\ 8)$;
- *if* $\nu_2(t^2-s)-\nu_2(s)\equiv 4\ (mod\ 6)$ *and* $\nu_2(t^2-s)-\nu_2(s)>4$, *then* $w_2(t)=-1$;
- *if* $\nu_2(t^2-s)-\nu_2(s)\equiv 5\ (mod\ 6)$, *then* $w_2(t)=1$ *iff* $t_2\equiv(t^2-s)_2\ (mod\ 4)$.

Bibliography

[BDD16] Sandro Bettin, Chantal David, and Christophe Delaunay. Families of elliptic curves with non-zero average root number. Preprint, 2016.

[BS66] Bryan J. Birch and Nelson M. Stephens. The parity of the rank of the mordell-weil group. *Topology*, 5:295–299, 1966.

[CCH05] Brian Conrad, Keith Conrad, and Harald A. Helfgott. Root numbers and ranks in positive characteristic. *Adv. Math.*, 198(2):684–731, 2005.

[Con94] Ian Connell. Calculating root numbers of elliptic surfaces over $\mathbb{Q}$. *Manuscripta Math.*, 82:93–104, 1994.

[Del73] Pierre Deligne. Les constantes des équations fonctionelles des fonctions L. In *Modular functions of one variable, II, SLN 349*, pages 501–595. Springer-Verlag, New York, 1973.

[Hal98] Emmanuel Halberstadt. Signes locaux des courbes elliptiques en 2 et 3. *C. R. Acad. Sci. Paris, Sér. I Math.*, 326:1047–1052, 1998.

[Hel04] Harald A. Helfgott. On the square-free sieve. *Acta Airth.*, 115(4):349–402, 2004.

[Hel09] Harald A. Helfgott. On the behaviour of root numbers in families of elliptic curves. Preprint, arXiv:math/0408141v3, 2009.

[Liv95] Eric Liverance. A formula for the root number of a family of elliptic curves. *J. Number Theory*, 51(2):288–305, 1995.

[Mil04] Steven J. Miller. One- and two-level densities for rational families of elliptic curves: evidence for the underlying group symmetries. *Compos. Math.*, 140(4):952–992, 2004.

[PAR16] Group PARI. PARI/GP, version 2.8.1. *Bordeaux*, 2016.

[Riz03] Ottavio G. Rizzo. Average root numbers for a nonconstant family of elliptic curves. *Compos. Math.*, 136:1–23, 2003.

[Roh93] David E. Rohrlich. Variation of the root number in families of elliptic curves. *Compos. Math.*, 87(2):119–151, 1993.

[Rol11] Larry Rolen. A generalization of the congruent number problem. *Int. J. Number Theory*, 7(8):2237–2247, 2011.

[Roy10] Halsey L. Royden. *Real analysis*. Prentice Hall, Boston, 2010.

[Sil83] Joseph H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, 342:197–211, 1983.

[Sil09] Joseph H. Silverman. *The airthmetic of elliptic curves*. Springer, Dordrecht, 2009.

[Tat79] John Tate. Number theoretic background. In *Automorphic forms, representations, and L-functions (Proc. Symp. Pure Math., Vol. 33-Part 2)*, pages 3–26. Amer. Math. Soc., Providence, R.I., 1979.

[Was87] Lawrence C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.*, 48(177):371–384, 1987.

[Wil95] Andrew J. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.