On a theorem of Jiang and Rallis

J. Hundley and Y. Rivera Vega

Abstract - Jiang and Rallis (1997) defined a family of local integrals attached to a cubic polynomial and proved explicit evaluations of them over a non-archimedean local field $\mathbf{F}$, when either $\mathbf{F}$ contains three third roots of unity, or the defining polynomial is reducible. The restriction on $\mathbf{F}$ allowed them, among other things, to reduce the case of irreducible polynomials of the form $x^3 - a$. Pleso (2009) began the work of removing the restriction on $\mathbf{F}$ by expressing the integral as a sum of 16 integrals for the cubic polynomial $x^3 - bx - c$, with $b, c \in \mathbf{F}$, and computing nine of them. In this work, we compute 15 of Pleso's integrals explicitly, and reduce the last to a conjecture about the number of points on a surface over a finite field, in the special case when $\mathbf{F}$ is the p-adic numbers ($\mathbf{F} = \mathbf{Q}_p$) and p is equivalent to 5 mod 6. The proof of this conjecture is provided in the appendix section. Our computations essentially complete Pleso's work in that special case. In the interim, Xiong (2020) has computed the integrals for an arbitrary non-archimedean local field by a totally different approach. Our direct approach might be more extendable to analogous integrals defined using quintic polynomials in a higher-rank setting.

Keywords : Dedekind zeta functions; zeta functions; L functions; adeles; p-adic numbers; G_2

Mathematics Subject Classification (2020) **:** 11S23

1 Introduction

In modern number theory, a lot of research is dedicated to the study of zeta functions and their analytic properties. The first and simplest example of such a function, and possibly still the most important, is the Riemann zeta function, $\zeta(s)$, defined for $s = \sigma + it \in \mathbf{C}$ with $\sigma > 1$ by the absolutely convergent Dirichlet series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

or by the absolutely convergent Euler product (over primes p)

$$\prod_p \left(1 - p^{-s}\right)^{-1},$$

but extending to an analytic function on $\mathbf{C} - \{1\}$, and satisfying the functional equation

$$\pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s) = \pi^{\frac{s-1}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s),$$

where Γ is the Gamma function, given, for $\Re(s) > 0$ by

$$\Gamma(s) = \int_0^\infty e^{-u} u^{s-1}\, du.$$

This idea was extended to number fields (i.e., finite extensions of $\mathbf{Q}$) by Dedekind, who defined a zeta function attached to such a field

$$\zeta_K(s) = \sum_{\mathfrak{a}} N\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1},$$

where the sum is over all ideals in the so-called ring of integers, $\mathfrak{o}_K$, of K, the product is over just the prime ideals, and for each ideal $\mathfrak{a}$, the norm $N\mathfrak{a}$ is just the index of $\mathfrak{a}$ in $\mathfrak{o}_K$, which is finite.

The same idea was extended in a different direction by Dirichlet, who introduced Dirichlet characters $\chi : \mathbf{Z} \to \mathbf{C}$, which satisfy

$$\chi(mn) = \chi(m)\chi(n), \qquad \chi(m+N) = \chi(m), \qquad \chi(n) = 0 \iff \gcd(n, N) \neq 1,$$

for some integer N. Dirichlet studied the L function

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{-s}} = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

The two extensions are related by quadratic reciprocity. Indeed, if K is any quadratic extension of $\mathbf{Q}$, then there is a unique Dirichlet character χ, which takes values in $\{-1, 0, 1\}$, such that

$$\zeta_K(s) = \zeta(s) L(s, \chi). \tag{1}$$

In more detail, for each prime p, one of three things happens:

1. There are two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in $\mathfrak{o}_K$ such that $N\mathfrak{p}_1 = N\mathfrak{p}_2 = p$, and $\chi(p) = 1$; in this case we get a factor of $(1-p^{-s})^{-2}$ in the Euler products on both sides of (1).

2. There is one prime ideal $\mathfrak{p}$ in $\mathfrak{o}_K$ such that $N\mathfrak{p} = p^2$, and $\chi(p) = -1$; in this case we get a factor of $(1 - p^{-2s})^{-1} = (1 - p^{-s})^{-1}(1 + p^{-s})^{-1}$ in the Euler products on both sides of (1).

3. There is one prime ideal $\mathfrak{p}$ in $\mathfrak{o}_K$ such that $N\mathfrak{p} = p$, and $\chi(p) = 0$; in this case we get a factor of $(1 - p^{-s})^{-1} = (1 - p^{-s})(1 - 0 \cdot p^{-s})$ in the Euler products on both sides of (1).

For example, if $K = \mathbf{Q}[i]$ then $\mathfrak{o}_K = \mathbf{Z}[i]$, which is a p.i.d., and χ is given by

$$\chi(n) = \begin{cases} 1, & n \equiv 1 \mod 4, \\ -1, & n \equiv 3 \mod 4, \\ 0, & n \text{ is even.} \end{cases}$$

There is an analogue of the identity (1) in the setting where K is a quadratic extension, not of $\mathbf{Q}$, but of another field F which is itself a finite extension of $\mathbf{Q}$. In this case ζ_K/ζ_F is attached to a Hecke character, which is like a Dirichlet character, but defined on $\mathfrak{o}_F$ rather than $\mathbf{Z}$. These and related facts are covered in most introductory algebraic number theory books, such as [10],[2].

There is also an analogue of the identity (1) in the setting where the extension is of degree > 2, but in this case ζ_K/ζ (or, more generally, ζ_K/ζ_F) is not a simple Dirichlet (or, more generally, Hecke) L function, but a product of L functions of a more mysterious type, known as an Artin L functions. Unlike Dirichlet and Hecke L functions, Artin L functions do not have analytic properties that are well understood.

In the paper [8], Jiang and Rallis introduced a new way to study the ratio ζ_K/ζ_F in the case when $[K : F] = 3$. The method is based on an integral over a group of matrices with entries in a ring called the adeles. The adele ring of a number field F is a natural object to use in the study of Euler products, because the adele ring itself is a type of product, with a factor for each prime, and a finite number of other factors. For example, in the case of $\mathbf{Q}$ there is one additional factor, and it corresponds to factor of $\pi^{-s/2}\Gamma(\frac{s}{2})$ which must be added to the original Euler product for $\zeta(s)$ in order to obtain a nice functional equation. We will describe the adele ring of $\mathbf{Q}$ in more detail below.

The integral $I^\sigma(s, f_s)$ of Jiang and Rallis depends on an element σ of F^4. This quadruple determines a polynomial g of degree at most three, and when g is cubic and irreducible, that provides the cubic extension of F. In their paper, Jiang and Rallis prove that the integral has nice analytic properties by relating it to a function called an Eisenstein series with known analytic properties. This Eisenstein series is defined on a group of matrices, with entries in the adele ring, which is known as G_2. The other parameter, f_s, on which the integral depends, is itself a certain type of function on this group which is used in the construction of the Eisenstein series.

Having established the analytic properties of their integral, Jiang and Rallis set out to calculate it. When σ determines a cubic extension K, the goal is to prove that the integral is equal to the product of $\zeta_K(3s-1)/\zeta_F(3s-1)$, and an additional factor, known as the "normalizing factor" of the Eisenstein series mentioned above, and given by

$$\frac{1}{\zeta_F(3s)\zeta_F(6s-2)\zeta_F(9s-3)}.$$

(They are also able to predict what the value of $I^\sigma(s, f_s)$ should be when the polynomial attached to σ is reducible, with distinct roots.) Using the product structure of the adele ring, Jiang and Rallis factor their integral as a product over primes, with a factor $I^\sigma_{\mathfrak{p}}(s, f_{s,\mathfrak{p}})$ for each prime ideal $\mathfrak{p}$ in $\mathfrak{o}_F$ and a finite number of other factors. The job is then to match the contribution from each prime with the corresponding factor in the Euler product for

$$\frac{\zeta_K(3s-1)}{\zeta_F(3s)\zeta_F(3s-1)\zeta_F(6s-2)\zeta_F(9s-3)}.$$

Jiang and Rallis were able to accomplish this goal only under two additional hypotheses:

- they restrict attention to primes which are "unramified." In essence this means that they assume that anything which only happens at a finite number of primes is *not* happening at the prime they are considering. (For example, if F is $\mathbf{Q}$, we might exclude any prime which divides the denominator of one of the elements of σ: there are only finitely many such primes.) This, in particular, forces the function $f_{s,\mathfrak{p}}$, on which the integral depends, to be one specific element, denoted $f^\circ_{s,\mathfrak{p}}$, of the space it varies in.

- they assume that the field F contains three cube roots of 1.

Note that this second technical hypothesis unfortunately excludes the case $F = \mathbf{Q}$!

Jiang and Rallis comment that the restriction on cube roots should be removable. A first step towards removing it was taken in the master's thesis of Joseph Pleso [12]. The hypothesis that F contains three cube roots of 1 is used in several different ways in [8], including in an argument which reduces the study of arbitrary irreducible cubic polynomials to the study of those of the form $x^3 - a$. Jiang and Rallis break the integral $I^\sigma_{\mathfrak{p}}(s, f^\circ_{s,\mathfrak{p}})$ into 16 pieces, and the complexity of these pieces is greater when there are more nonzero coefficients in the polynomial attached to σ. In [12], Pleso considers a polynomial of the form $x^2 - bx + c$, and computes the analogous 16 sub-integrals. He then evaluates nine of them.

In this paper, we restrict ourselves to the important special case $F = \mathbf{Q}$. In this case $\mathfrak{o}_F = \mathbf{Z}$. So, if $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}_F$, then $\mathfrak{p}$ is generated by an ordinary prime p. For each prime p, we obtain the field $\mathbf{Q}_p$ of p-adic numbers, which we discuss in more detail in the next section. The Jiang-Rallis integral $I_p(s, f^\circ_{s,p})$ is an integral over five copies of $\mathbf{Q}_p$, and is also described in more detail in the next section. If $p \equiv 1 \pmod 6$, then the field $\mathbf{Q}_p$ has three cube roots of 1. In this case, the value of $I_p(s, f^\circ_{s,p})$ can be deduced from the results of Jiang-Rallis, even though the field $\mathbf{Q}$ does not have three cube roots of 1.

Thus one, only has to handle $p = 2, p = 3$ and $p \equiv 5 \pmod 6$. In this paper, we let $p \equiv 5 \pmod 6$, compute six of the seven sub-integrals which Pleso did not compute, and reduce the last one to a conjecture about the number of integral solutions to a polynomial equation over $\mathbf{Z}/p\mathbf{Z}$.

Conjecture 2 *Let p be a prime, such that $p \equiv 5 \pmod 6$. Fix b and c in $\mathbf{Z}/p\mathbf{Z}^\times$ such that $g(u) := -u^3 + bu + c$ is irreducible. Then*

$$\{(r, y, u) \in (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z}) \mid g(u) \equiv 3uyr + y^3r^2 - r \mod p\}$$

has $p^2 - 1$ elements.

This conjecture has since been proved by Victor Scharaschkin, who has kindly permitted us to include his proof in an appendix to this paper. Our main theorem can be stated as follows.

Theorem 3 *Let $I^\sigma_p(s, f^\circ_{s,p})$ be the local integral of Jiang and Rallis at an unramified prime p. Assume that $p \equiv 5 \pmod 6$, and the polynomial g attached to σ is irreducible mod p. Then*

$$I^\sigma_p(s, f^\circ_{s,p}) = (1 - p^{-3s})(1 - p^{-3s+1})(1 - p^{-6s+2}).$$

The assumption that the polynomial g is irreducible mod p is a natural one. If g is reducible in the field $\mathbf{Q}_p$, then the integral has already been computed by Jiang and Rallis, who did not use their hypothesis on the cube roots of 1 in their treatment of this case. And, for any polynomial f with integer coefficients, the set of primes p such that f is reducible mod p but not in $\mathbf{Q}_p$ is finite.

So, by assuming that $p \equiv 5 \pmod 6$ and and that g is irreducible, we exclude only the cases already handled by Jiang-Rallis and a finite number of exceptions.

The right-hand side of our identity is the expected one. Indeed, when the polynomial attached to σ is irreducible mod p, and K is the cubic extension attached to it, there is a single prime ideal $\mathfrak{p}$ in $\mathfrak{o}_F$ such that $N\mathfrak{p} = p^3$. Thus, the contribution to the Euler product for $\zeta_F(3s-1)$ corresponding to the prime p is $(1-(p^3)^{-3s+1})^{-1}$, or $(1-p^{-9s+3})$, and so the contribution of the prime p to the Euler product for

$$\frac{\zeta_K(3s-1)}{\zeta(3s)\zeta(3s-1)\zeta(6s-2)\zeta(9s-3)}.$$

is

$$\frac{(1-p^{-9s+3})^{-1}}{(1-p^{-3s})^{-1}(1-p^{-3s+1})^{-1}(1-p^{-6s+2})^{-1}(1-p^{-9s+3})^{-1}},$$

which is precisely the right-hand side of our identity.

The integral $I^{\sigma}_{\mathfrak{p}}(s, f^{\circ}_{s,\mathfrak{p}})$ was previously computed by Xiong in [19] using a totally different method which works for any number field F. Thus, our "Conjecture 2" may actually be deduced from Xiong's result, using the results of this paper. Scharaschkin's elementary proof of conjecture 2 completes a second, more elementary proof of the special case $F = \mathbf{Q}$ of Xiong's result.

2 Background and Notation

2.1 The Field of p-adic Numbers

In this section we review some basic definitions about the field $\mathbf{Q}_p$ of p-adic numbes, where $p \in \mathbf{Z}$ is a prime number. Some references for a more detailed introduction to $\mathbf{Q}_p$ are [9], [13],[14],[15], [5].

2.1.1 Analytic Approach

The first, more analytic approach to defining $\mathbf{Q}_p$ is based on defining a non-standard absolute value on the field $\mathbf{Q}$ of rational numbers, which depends on a prime p. First, let $\mathrm{ord}_p : \mathbf{Q}^\times \to \mathbf{Z}$ be the unique function such that, for each element x of $\mathbf{Q}^\times$, we have $x = p^{\mathrm{ord}_p(x)}\frac{a}{b}$ for some $a, b \in \mathbf{Z}$, neither of which is divisible by p. It is conventional to set the $\mathrm{ord}_p(0) = +\infty$ to ensure ord_p satisfies all the axioms of a valuation. We then define the p-adic absolute value $\mathbf{Q} \to [0, \infty)$ by

$$|x|_p = \begin{cases} \frac{1}{p^{\mathrm{ord}_p(x)}} & \text{if } x \neq 0, \\ 0, & \text{if } x = 0. \end{cases}$$

This formula does indeed give a well-defined absolute value on $\mathbf{Q}$, and indeed, one which satisfies the "strong triangle inequality":

$$|a+b|_p \leq \max(|a|_p, |b|_p)$$

with equality whenever $|a|_p \neq |b|_p$. (Equivalently, $\mathrm{ord}_p(a+b) \geq \min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$, with equality whenever $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(b)$.) We may the define the field $\mathbf{Q}_p$ of p-adic numbers as the completion of $\mathbf{Q}$ with respect to $|\ |_p$; we define "Cauchy" and "convergent" using $|\ |_p$, show that having a difference which converges to 0 is an equivalence relation on Cauchy sequences, and let $\mathbf{Q}_p$ be the set of equivalence classes of Cauchy sequences, relative to this equivalence relation. Thus defined, $\mathbf{Q}_p$ is indeed a field, and addition, subtraction, multiplication, etc., as well as $|\ |_p$ have unique continuous extensions from $\mathbf{Q}$ to $\mathbf{Q}_p$ which we denote with the same symbols.

The ring of p-adic integers, $\mathbf{Z}_p$, may then be defined as $\{x \in \mathbf{Q}_p : |x| \leq 1\}$. This is indeed a subring of $\mathbf{Q}_p$, and it is also the closure of $\mathbf{Z}$ in the topology on $\mathbf{Q}_p$, and is compact in this topology. This ring has a unique maximal, ideal, namely $\{x \in \mathbf{Q}_p : |x| < 1\}$, which is principal and generated by p; its group of units $\mathbf{Z}_p^\times$ is thus $\{x \in \mathbf{Q}_p : |x| = 1\}$. Finally, $\mathbf{Q}_p - \mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x| > 1\}$.

The field $\mathbf{Q}_p$ possesses a measure, unique up to multiplication by a positive scalar, which assigns open sets positive measure, assigns compact sets finite measure, and is invariant under additive translation. We can pin it down uniquely by specifying that the measure of $\mathbf{Z}_p$ is 1. This measure is called the additive Haar measure and we denote it dx (or dy if the variable is y, etc).

2.1.2 Algebraic Approach

For each positive integer k, the set $\{x \in \mathbf{Z}_p : |x| \leq p^{-k}\}$ is the principal ideal $p^k\mathbf{Z}_p$ in $\mathbf{Z}_p$ generated by p^k. It satisfies $\mathbf{Z}_p/p^k\mathbf{Z}_p \cong \mathbf{Z}/p^k\mathbf{Z}$. This actually permits one to give an equivalent, algebraic definition of $\mathbf{Z}_p$ and $\mathbf{Q}_p$. Specifically, one may define $\mathbf{Z}_p$ as the projective limit $\varprojlim_k \mathbf{Z}/p^k\mathbf{Z}$ of the finite rings $\mathbf{Z}/p^k\mathbf{Z},\ k = 1, 2, 3\ldots$, i.e., the set of infinite sequences $(a_k)_{k=1}^\infty$ such that $a_k \in \mathbf{Z}/p^k\mathbf{Z}$ and if $\ell > k$ then a_k is the image of a_ℓ under the "reduction mod p^k" map $\mathbf{Z}/p^\ell\mathbf{Z} \to \mathbf{Z}/p^k\mathbf{Z}$. If this alternate definition of $\mathbf{Z}_p$ is used, then $\mathbf{Q}_p$ may be recovered as the field of fractions of $\mathbf{Z}_p$.

Via either approach, each nonzero element of $\mathbf{Q}_p$ has a unique p-adic expansion:

$$\sum_{n=N}^{\infty} d_n p^n, \qquad N \in \mathbf{Z}, \qquad d_n \in \{0, \ldots, p-1\},\ \text{each } n, \qquad d_N \neq 0.$$

Then $\sum_{n=N}^\infty d_n p^n$ lies in $\mathbf{Z}_p$ if and only if $N \geq 0$.

2.1.3 More on Haar Measure

As we have mentioned, the Haar measure is invariant under additive translation and assigns the ring $\mathbf{Z}_p$ a measure of 1. For each integer k the set

$$p^k\mathbf{Z}_p = \{p^k x : x \in \mathbf{Z}_p\}$$

is at once an additive subgroup of $\mathbf{Q}_p$, the closed ball of radius p^{-k} centered at 0, and the open ball of radius p^{1-k} centered at 0. For each other $a \in \mathbf{Q}_p$ the coset $a + p^k\mathbf{Z}_p$ is the closed ball of radius p^{-k} centered at a, and the open ball of radius p^{1-k} centered at a.

By invariance, the various cosets $a + p^k\mathbf{Z}_p$, as a varies, all have the same measure. If $k > 0$ then $\mathbf{Z}_p$ is a union of p^k cosets of $p^k\mathbf{Z}_p$. If $k < 0$ then $p^k\mathbf{Z}_p$ is a union of p^{-k} cosets of $\mathbf{Z}_p$. In either case we can deduce that the Haar measure of $a+p^k\mathbf{Z}_p$ is p^{-k} for all $k \in \mathbf{Z}$.

The cosets $a+p^k\mathbf{Z}_p,\ (a \in \mathbf{Q}_p, k \in \mathbf{Z})$ play a role in the theory of Haar measure on $\mathbf{Q}_p$ that is similar to the role played by intervals in the theory of Lebesgue measure on $\mathbf{R}$. For example the "step functions" used to define the integral are finite linear combinations of characteristic functions of these balls:

$$\sum_{i=1}^{n} c_i \mathbb{1}_{a_i+p^{k_i}\mathbf{Z}_p}. \tag{4}$$

(Here, and throughout this paper, $\mathbb{1}_X$ is the characteristic function of the set X.) Their integrals are completely determined by the volumes of these balls, which we just computed.

It follows that if X, and Y are two Haar-measurable subsets of $\mathbf{Q}_p$ and $\varphi : X \to Y$ is a function which maps each coset $a + p^k\mathbf{Z}_p$ to another coset $b + p^k\mathbf{Z}_p$ of the same size (i.e., with the same k), then φ preserves the Haar measure, so that

$$\int_X h(\varphi(x))\,dx = \int_Y h(y)\,dy,$$

for any measurable function h.

If X and Y happen to be subsets of $\mathbf{Z}_p$, then the cosets $a+p^k\mathbf{Z}_p$ are precisely the elements of the quotient ring $\mathbf{Z}/p^k\mathbf{Z}$, so the measure-preserving property can be interpreted as giving a well-defined bijection modulo p^k for each k.

In what follows, we shall make use not only of Haar measure on $\mathbf{Q}_p$ but also the product measure defined on several copies of $\mathbf{Q}_p$. In this context we shall frequently refer to the measure of a measurable set X as its volume, and denote it $\mathrm{Vol}(X)$.

2.2 Hensel's Lemma

Lemma 5 *For*

$$f(x) = \sum_{i=0}^{d} c_i x^i \in \mathbf{Z}_p[x],$$

let

$$f'(x) = \sum_{i=1}^{d} i c_i x^{i-1}$$

be the derivative. For $a_0 \in \mathbf{Z}_p$, suppose that

$$f(a_0) \equiv 0 \pmod{p}, \qquad \text{and} \qquad f'(a_0) \not\equiv 0 \pmod{p}.$$

Then

$$\{a \in \mathbf{Z}_p : a \equiv a_0 \pmod{p},\ \text{and } f(a) = 0\}$$

has exactly one element.

Proof. See [9], theorem 1.39. □

Corollary 6 *Take $f(x) \in \mathbf{Z}_p[x]$ and let $\overline{f}(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ be the polynomial obtained by reducing each of the coefficients of f modulo p. Suppose that f is irreducible, while $\overline{f}$ vanishes at $a \in \mathbf{Z}/p\mathbf{Z}$. Then a is actually a double zero of $\overline{f}$.*

2.3 Additive Characters

The function

$$e_p(x) = \begin{cases} \exp\left(-2\pi i \sum_{n=N}^{-1} d_n p^n\right), & x = \sum_{n=N}^{\infty} d_n p^n, \\ 1, & x \in \mathbf{Z}_p, \end{cases}$$

is a well-defined continuous homomorphism $\mathbf{Q}_p \to S^1 := \{z \in \mathbf{C} : |z| = 1\}$.

It should be noted that if F is a number field – that is, a finite extension of $\mathbf{Q}$ – then it is possible to define absolute values which are analogous to $|\ |_p$ on the field F and complete F with respect to these absolute values and obtain fields which share many of their properties with $\mathbf{Q}_p$. These fields are known as non-Archimedean local fields. Notably, many of the results of Jiang and Rallis are proved for any number field or for any non-Archimedean local field. Others are proved for any field in one of these classes which contains three cube roots of one– a technical hypothesis which excludes $\mathbf{Q}$, and excludes $\mathbf{Q}_p$ if $p \equiv 2 \pmod 3$.

2.4 The Adele Ring

In this section we briefly describe the so-called adele ring of $\mathbf{Q}$. It's worth noting that this theory may be extended to define adele rings attached to finite extensions of $\mathbf{Q}$ as well. Some good references are [10], [2], and [5].

In order to set up the definition, it is useful to mention an important fact. It follows from a theorem of Ostrowski (see [2], p. 45) that every nontrivial multiplicative absolute value on $\mathbf{Q}$ is either the standard one (which gives $\mathbf{R}$ as the completion of $\mathbf{Q}$), or the absolute value $|\ |_p$ for some prime p, or equivalent to $|\ |_p$ for some p in the sense that it induces the same topology on $\mathbf{Q}$. (Concretely, if we take $c \in (1, \infty)$, which is not equal to p, then replacing "$p^{-\operatorname{ord}_p(x)}$" by "$c^{-\operatorname{ord}_p(x)}$" in the definition of $|\ |_p$ produces an absolute value which is not the same as $|\ |_p$, but is equivalent to it.)

Thus, the set of topologically-distinct completions of $\mathbf{Q}$ consists of $\mathbf{R}$ and one element for each prime p. It is convenient to introduce an index set which consists of the primes and one additional element corresponding to $\mathbf{R}$. Historically, the most common choice for the index corresponding to the completion $\mathbf{R}$ is "∞." In keeping with this tradition, we let $\mathbf{Q}_\infty = \mathbf{R}$ and $|\ |_\infty : \mathbf{R} \to [0, \infty)$ be the usual absolute value.

We now consider the product of all the topologically-distinct completions of $\mathbf{Q}$:

$$\mathbf{R} \times \prod_p \mathbf{Q}_p.$$

An element of this ring can be thought of as an infinite sequence

$$x = (x_\infty, x_2, x_3, x_5, x_7, \ldots, x_p, \ldots)$$

such that $x_\infty \in \mathbf{R}$ while $x_p \in \mathbf{Q}_p$ for each prime p. The adele ring, $\mathbf{A}$ is then

$$\{x \in \mathbf{R} \times \prod_p \mathbf{Q}_p : \text{ the set of primes } p \text{ such that } x_p \notin \mathbf{Z}_p \text{ is finite}\}.$$

Notice that if a is an element of $\mathbf{Q}$ then a is an element of every completion of $\mathbf{Q}$ and hence $(a, a, a, a, a, \ldots, a, \ldots)$ is an element of $\mathbf{R} \times \prod_p \mathbf{Q}_p$. In fact, it is an element of $\mathbf{A}$ because $a \in \mathbf{Z}_p$ for any prime p which does not divide the denominator of a when written in lowest terms. We regard $\mathbf{Q}$ as a subring of $\mathbf{A}$ by identifying $a \in \mathbf{Q}$ with $(a, a, a, a, a, \ldots, a, \ldots) \in \mathbf{A}$.

The group $\mathbf{A}^\times$ of units of $\mathbf{A}$ is called the ideles. It is described explicitly as

$$\{x \in \mathbf{R}^\times \times \prod_p \mathbf{Q}_p^\times : \text{ the set of primes } p \text{ such that } x_p \notin \mathbf{Z}_p^\times \text{ is finite}\}.$$

Notice that if $a \in \mathbf{Q}^\times$ then $(a, a, a, a, a, \ldots, a, \ldots) \in \mathbf{A}^\times$, since $a \in \mathbf{Z}_p^\times$ for any prime p which divides neither the numerator nor the denominator of a (in lowest terms).

Like $\mathbf{Q}_p$, the ring $\mathbf{A}$ possesses a measure, called Haar measure, which is unique up to multiplication by a positive scalar, assigns open sets positive measure, assigns compact sets finite measure, and is invariant under additive translation. It can be pinned down uniquely by requiring that on each of the subsets

$$\mathbf{R} \times \prod_{p<T} \mathbf{Q}_p \times \prod_{p \geq T} \mathbf{Z}_p, \qquad (T \in (0, \infty)),$$

it is given by the product of Lebesgue measure on $\mathbf{R}$ and Haar measure on $\mathbf{Q}_p$ or $\mathbf{Z}_p$. (Notice that $\mathbf{A}$ is the union of these subsets.)

We shall also need to use the idelic absolute value, which is defined as follows. Suppose that $x \in \mathbf{A}^\times$. Let $S = \{p \text{ prime} \mid x_p \notin \mathbf{Z}_p^\times\}$. Then we define $|x| = |x_\infty|_\infty \cdot \prod_{p \in S} |x_p|_p$. Here $|x_\infty|_\infty$ is just the usual absolute value of x_∞, which is an element of $\mathbf{R}^\times$. Notice that if S' is any finite set which contains S then $|x| = |x_\infty| \cdot \prod_{p \in S'} |x_p|_p$ (since we've only added a finite number of 1's to the product). Indeed, the infinite product $|x_\infty| \cdot \prod_{\text{all primes } p} |x_p|_p$ converges to $|x|$ because all but finitely many terms in the product are 1. The idelic absolute value has the key properties that if $x, y \in \mathbf{A}^\times$ then $|xy| = |x||y|$, and that if $a \in \mathbf{Q}^\times$ then $|a| = 1$.

Finally, we would like to define a continuous homomorphism $\mathbf{A} \to S^1$ which is trivial on the embedded copy of $\mathbf{Q}$. Previously we introduced $e_p : \mathbf{Q}_p \to S^1$. Take $x = (x_\infty, x_2, x_3, \ldots, x_p, \ldots) \in \mathbf{A}$. Then, for all but a finite number of primes p, $x_p \in \mathbf{Z}_p$ and hence $e_p(x_p) = 1$. Hence

$$e(x) = e^{2\pi i x_\infty} \prod_p e_p(x_p) \tag{7}$$

does not have any convergence issues, and gives a well defined continuous homomorphism $\mathbf{A} \to S^1$. It can be shown that it is trivial on $\mathbf{Q}$.

2.5 The Group G_2

In this section we briefly introduce a certain matrix group which we call "G_2." Some references for this material are [4],[1],[6], [16],[17].

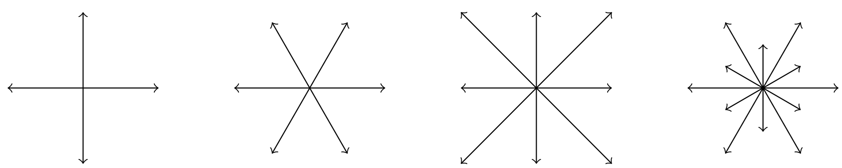
The name "G_2" applies, first and foremost, to a root system. A root system is a finite spanning set Φ in a real inner product space (one may take it to be $\mathbf{R}^n$ with the usual dot product) such that

1. the reflection $\alpha - 2\frac{\alpha\cdot\beta}{\beta\cdot\beta}\beta$ of α in the plane orthogonal to β is an element of Φ for all $\alpha, \beta \in \Phi$,
2. the quantity $2\frac{\alpha\cdot\beta}{\beta\cdot\beta}$ is an integer for all $\alpha, \beta \in \Phi$,
3. if $\alpha \in \Phi, k \in \mathbf{R}$ and $k\alpha \in \Phi$, then $k = 1$ or -1.

The elements of the set Φ are called roots. The second requirement has an interesting geometric consequence. Indeed, if α and β are two roots, and if θ is the angle between them then

$$\cos^2\theta = \frac{\alpha\cdot\beta}{\beta\cdot\beta}\frac{\alpha\cdot\beta}{\alpha\cdot\alpha} \in \{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1\}.$$

Up to rotation and scaling, there are only four root systems in $\mathbf{R}^2$. They are shown below.



The root system at the far right is G_2. It has 12 roots.

Root systems play an important role in the classification theory of various mathematical objects, including Lie groups, Lie algebras, and linear algebraic groups. For us, the important object is a linear algebraic group.

A linear algebraic group G over a field F is defined by a positive integer n and a finite set S of polynomial equations, with coefficients in F where the variables are the entries of an $n \times n$ matrix, and

$$G(R) := \{g \in GL_n(R) : S\}$$

is closed under matrix multiplication and inversion, i.e., a subgroup of $GL_n(R)$, for any commutative F-algebra with unity R. For example, if X is a fixed $n \times n$ matrix with entries in F then

$$\{g \in GL_n(R) : gXg^t = X\}$$

(here ^{t} denotes transpose) is well-defined a subgroup of $GL_n(R)$ for any commutative F-algebra with unity R. Thus G itself is not actually a group, but a mapping from F-algebras to groups.

In order to describe the results of Jiang, Rallis, and Pleso, we will not need to worry about the specific set of polynomial equations that defines G_2. The key point about our "G_2" being a linear algebraic group is that it is not a single group, but a mapping from $\mathbf{Q}$-algebras to groups, which we will use to define various groups: $G_2(\mathbf{Q})$, $G_2(\mathbf{Q}_p)$, $G_2(\mathbf{A})$, etc., and each subgroup of it which we introduce is a similar object.

2.6 Some Key Subgroups of G_2

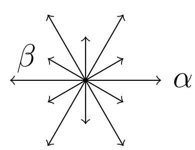
Without getting too bogged down in the details of how root systems are used in the classification of linear algebraic groups, let us briefly mention that our linear algebraic group G_2 has a one dimensional subgroup attached to each of the roots in the root system G_2. For example, if we use the same embedding of G_2 into GL_8 as Pleso [12], then one of the six long roots, which we denote α, is attached to the group of all matrices of the form

$$x_\alpha(a) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -a & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

and one of the six short roots, which we denote β, is attached to the group of all matrices of the form

$$x_\beta(b) = \begin{pmatrix} 1 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & b & b & -b^2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -b & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -b & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -b \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We may assume that the root system is embeeded in the plane so that α and β are as displayed below



Then the other ten roots are $\alpha+\beta, \alpha+2\beta, \alpha+3\beta, 2\alpha+3\beta$, and the negatives of the first six.

Bundling together five of these groups, we obtain another important group, which we denote N consisting of all matrices of the form

$$n(x,y,z,u,v) = x_{\alpha+3\beta}(x)x_{\alpha+2\beta}(y)x_{2\alpha+3\beta}(z)x_{\alpha+\beta}(u)x_{\alpha}(v)$$
$$= \begin{pmatrix} 1 & 0 & -u & -y & -y & -x & vx+2\,uy-z & -ux-y^2 \\ 0 & 1 & v & u & u & -y & -u^2+vy & -uy+z \\ 0 & 0 & 1 & 0 & 0 & 0 & y & x \\ 0 & 0 & 0 & 1 & 0 & 0 & -u & y \\ 0 & 0 & 0 & 0 & 1 & 0 & -u & y \\ 0 & 0 & 0 & 0 & 0 & 1 & -v & u \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Note that the function n is not a homomorphism, because the group N is not abelian. However it does give a bijection $R^5 \to N(R)$ for any $\mathbf{Q}$-algebra R. If $R = \mathbf{R}, \mathbf{Q}_p$ or $\mathbf{A}$, then this bijection with R^5 defines a measure on $N(R)$, which corresponds to product measure on R^5.

Abusing notation, we shall use the symbol n for a general element of N as well as for the above function from $R^5 \to N(R)$ for each R. So, for example, "$n \in N(\mathbf{A})$" means the same things as "$n = n(x,y,z,u,v)$ for some $x,y,z,u,v \in \mathbf{A}$."

The function n also has a lower-triangular analogue, which will also arise in the results of Jiang-Rallis and Pleso. It is given by

$$n^-(x,y,z,u,v) = x_{-\alpha}(x)x_{\alpha-\beta}(y)x_{-2\alpha-3\beta}(z)x_{-\alpha-2\beta}(u)x_{-\alpha-3\beta}(v)$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -y & x & 1 & 0 & 0 & 0 & 0 & 0 \\ -u & y & 0 & 1 & 0 & 0 & 0 & 0 \\ -u & y & 0 & 0 & 1 & 0 & 0 & 0 \\ -v & -u & 0 & 0 & 0 & 1 & 0 & 0 \\ vx+2\,uy-z & ux-y^2 & u & -y & -y & -x & 1 & 0 \\ -u^2-vy & -uy+z & v & u & u & y & 0 & 1 \end{pmatrix},$$

and its image is a subgroup of G_2 which is conjugate to N and denoted N^-. As we did with "n" we will also abuse notation with n^- by denoting a general element of the group $N^-(R)$ by n^- when we have no need to refer to its individual coordinates.

The next subgroup of G_2 is isomorphic to GL_2. Specifically, if $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then we define

$$m(g) = \begin{pmatrix} a & b & & & & & & \\ c & d & & & & & & \\ & & a^2/\Delta & ab/\Delta & ab/\Delta & -b^2/\Delta & & \\ & & ad/\Delta & ad/\Delta & bc/\Delta & -bd/\Delta & & \\ & & ad/\Delta & bc/\Delta & ad/\Delta & -bd/\Delta & & \\ & & -d^2/\Delta & -cd/\Delta & -cd/\Delta & d^2/\Delta & & \\ & & & & & & a/\Delta & -b/\Delta \\ & & & & & & -c/\Delta & d/\Delta \end{pmatrix},$$

where $\Delta = ad-bc$. Then $m : GL_2 \to GL_8$ is a homomorphism and its image is a subgroup of G_2 which we denote M.

The group M normalizes the group N, and the product of the groups N and M is denoted by P. For any $\mathbf{Q}$-algebra R, every element of $P(R)$ can be written uniquely as $m(g)n(x, y, z, u, v)$ for some $g \in GL_2(R)$ and $x, y, z, u, v \in R$. Since M normalizes N, the mapping $m(g)n(x, y, z, u, v) \to g$ is a homomorphism.

For any prime p we have $G_2(\mathbf{Q}_p) = P(\mathbf{Q}_p) \cdot G_2(\mathbf{Z}_p)$, that is, every element of $G_2(\mathbf{Q}_p)$ can be expressed as bk with $b \in P(\mathbf{Q}_p)$ and $k \in G_2(\mathbf{Z}_p)$. References for this fact include [7] Proposition 2.33. The expression is not unique, because $P(\mathbf{Q}_p) \cap G_2(\mathbf{Z}_p) = P(\mathbf{Z}_p)$ which is not trivial. But if $b_1k_1 = b_2k_2$, then there exists $\beta \in P(\mathbf{Z}_p)$ such that $b_2 = b_1\beta$ and $k_2 = \beta^{-1}k_1$.

2.7 Characters of N and Their Connection With Cubic Forms

We shall be working with continuous homomorphisms from $N(\mathbf{A})$ and $N(\mathbf{Q}_p)$ into the group $S^1 = \{z \in \mathbf{C} : |z| = 1\}$. Such homomorphisms are sometimes called "characters."

Let $\nu(n(x, y, z, u, v))$ be the row vector $\begin{bmatrix} x & y & u & v \end{bmatrix}$. It's not difficult to check that ν is a homomorphism $N(R) \to R^4$ for any $\mathbf{Q}$-algebra R. Its kernel is the group $Z(R)$ of all matrices of the form $n(0, 0, z, 0, 0)$. It's also not hard to check that

$$n(0, 0, 0, 0, z)n(1, 0, 0, 0, 0)n(0, 0, 0, 0, z)^{-1}n(1, 0, 0, 0, 0)^{-1} = n(0, 0, z, 0, 0).$$

This implies that, for any $\mathbf{Q}$-algebra R, and any abelian group A, every homomorphism from $N(R)$ to A must factor through ν.

Next, we need some key facts about the space of all continuous homomorphisms $R \to S^1$ when $R = \mathbf{R}, \mathbf{Q}_p$ or $\mathbf{A}$. See, for example [2],[10]. Let ψ be any fixed nontrivial continuous homomorphism $\mathbf{A} \to S^1$, which is trivial on $\mathbf{Q}$. (For example, the function e defined in (7).) Then every other continuous homomorphism $\mathbf{Q}\backslash\mathbf{A} \to S^1$, is of the form $\psi_a(x) = \psi(ax)$ for some $a \in \mathbf{Q}$. By restricting ψ to the copy of $\mathbf{R}$ inside $\mathbf{A}$ we get a nontrivial continuous homomorphism $\psi_\infty : \mathbf{R}^\times \to S^1$, and every other continuous homomorphism $\mathbf{R} \to S^1$, is of the form $\psi_{\infty,a}(x) = \psi_\infty(ax)$ for some $a \in \mathbf{R}$. Similarly, by restricting ψ to the copy of $\mathbf{Q}_p$ inside $\mathbf{A}$ we get a nontrivial continuous homomorphism $\psi_p : \mathbf{Q}_p \to S^1$, and every other continuous homomorphism $\mathbf{Q}_p \to S^1$, is of the form $\psi_{p,a}(x) = \psi_p(ax)$ for some $a \in \mathbf{Q}_p$.

It follows that every continuous homomorphism $N(\mathbf{A}) \to S^1$ which is trivial on $N(\mathbf{Q})$ has the form $n(x, y, z, u, v) \mapsto \psi(a_1x + a_2y + a_3u + a_4v)$ for some $a_1, a_2, a_3, a_4 \in \mathbf{Q}$, or, equivalently, $n \mapsto \psi(\nu(n) \cdot \sigma)$ for some $\sigma \in \mathbf{Q}^4$. Here $\cdot$ is the usual dot product. Moreover, every continuous homomorphism $N(\mathbf{Q}_p) \to S^1$ has the same form, with coefficients in $\mathbf{Q}_p$. In either case, we let ψ_σ be the mapping attached to the quadruple σ as above.

We have

$$\nu(m(g^{-1})n(x, y, z, u, v)m(g)) = \begin{bmatrix} x & y & u & v \end{bmatrix} \cdot \rho(g), \tag{8}$$

where

$$\rho\left(\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 0 & 0 & 0\\ -3a & 1 & 0 & 0\\ -3a^2 & 2a & 1 & 0\\ -a^3 & a^2 & a & 1\end{pmatrix},$$

$$\rho\left(\begin{pmatrix}1 & 0\\ a & 1\end{pmatrix}\right)=\begin{pmatrix}1 & -a & -a^2 & -a^3\\ 0 & 1 & 2a & 3a^2\\ 0 & 0 & 1 & 3a\\ 0 & 0 & 0 & 1\end{pmatrix},$$

$$\rho\left(\begin{pmatrix}t_1 & 0\\ 0 & t_2\end{pmatrix}\right)=\begin{pmatrix}t_2/t_1^2 & 0 & 0 & 0\\ 0 & t_1^{-1} & 0 & 0\\ 0 & 0 & t_2^{-1} & 0\\ 0 & 0 & 0 & t_1/t_2^2\end{pmatrix}.$$

From (8), it follows that for $\sigma \in \mathbf{Q}^4$ and $g \in GL_2(\mathbf{Q})$,

$$\psi_\sigma(m(g)^{-1}nm(g)) = \psi_{\sigma\cdot\rho(g)^t}(n).$$

The mapping $\rho : GL_2 \to GL_4$ is closely related to a certain action on homogeneous polynomials of degree at most 3 which we now explain. Key results are from [18]. If $\underline{c} = (c_1, c_2, c_3, c_4)$, then we define

$$F_{\underline{c}}([x, y]) = c_1x^3 + c_2x^2y + c_3xy^2 + c_4y^3.$$

For $g \in GL_2$ we define

$$g \cdot F([x, y]) = (\det g)^{-1}F([x, y]g).$$

Then we define $\varrho(g)$ to be the matrix such that

$$g \cdot F_{\underline{c}} = F_{\underline{c}\cdot\varrho(g)^t}.$$

It's easy to check that

$$\varrho\left(\begin{bmatrix}t_1 & 0\\ 0 & t_2\end{bmatrix}\right)=\begin{bmatrix}t_1^2/t_2 & & & \\ & t_1 & & \\ & & t_2 & \\ & & & t_2^2/t_1\end{bmatrix}$$

$$\varrho\left(\begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix}\right)=\begin{bmatrix}1 & a & a^2 & a^3\\ & 1 & 2a & 3a^2\\ & & 1 & 3a\\ & & & 1\end{bmatrix}$$

$$\varrho\left(\begin{bmatrix}1 & 0\\ a & 1\end{bmatrix}\right)=\begin{bmatrix}1 & & & \\ 3a & 1 & & \\ 3a^2 & 2a & 1 & \\ a^3 & a^2 & a & 1\end{bmatrix}$$

Then

$$\rho(g) = w_1 \varrho(\det g^{-1} g) w_1^{-1}, \qquad \text{where } w_1 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{9}$$

Indeed, it suffices to check this identity on matrices of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, and $\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix}$, because matrices of these three forms generate GL_2.

2.8 Some Results of Wright

Let k be an arbitrary field. Orbits for the action of $GL_2(k)$ on k^4 by ϱ^t were classified in [18].

Theorem 10 ([18]) *The orbits for the action of $GL_2(k)$ on k^4 by ϱ^t are as follows:*

1. *The set which contains only the zero vector is a singleton orbit.*
2. *The set which consists of all $\underline{c}$ such that $F_{\underline{c}}(x, y) = d(ax+by)^3$ for some (non-unique) $a, b, d \in k$ is a single orbit.*
3. *The set which consists of all $\underline{c}$ such that $F_{\underline{c}}(x, y) = (a_1x + b_2y)^2(a_2x + b_2y)$ for some (non-unique) $a_1, a_2, b_1, b_2 \in k$ is a single orbit.*
4. *For all other $\underline{c}$, let $K_{\underline{c}}$ be the smallest field extension of k such that $F_{\underline{c}}$ splits into linear factors over $K_{\underline{c}}$. Then $\underline{c}$ and $\underline{d} \in k^4$ lie in the same $GL_2(k)$-orbit if and only if $K_{\underline{c}} = K_{\underline{d}}$.*

Let $f_{\underline{c}}(x) = F_{\underline{c}}(1, x)$. We give a modest reformulation of the result.

Corollary 11 *Assume that k has more than two elements. Each nonzero orbit for the action of $GL_2(k)$ on k^4 by ϱ contains an element such that $f_{\underline{c}}$ has degree 3. To such an element $\underline{c}$ we can attach the quotient ring $k[x]/(f_{\underline{c}})$. Then two elements of k^4 are in the same orbit if and only if the attached quotient rings are isomorphic.*

Proof. Indeed, $f_{\underline{c}}$ has degree less than 3 if and only if x is a linear factor of $F_{\underline{c}}$. By Wright's result, the orbit of $\underline{c}$ determines the number and multiplicities of the linear factors of $F_{\underline{c}}$, but not what they are. So its possible to choose an element such that none of the linear factors is x, with only one exception– if k has two elements and $F_{\underline{c}}$ has three distinct linear factors, then one of them must be x because $k[x, y]$ only has three linear elements.

If $f_{\underline{c}}$ has distinct irreducible factors then, by the Chinese remainder theorem, $k[x]/(f_{\underline{c}}(x))$ is the direct sum of the quotients of $k[x]$ by the individual factors– that is, it's a single cubic field if $f_{\underline{c}}$ is irreducible, or $k \oplus K_{\underline{c}}$ if $f_{\underline{c}}$ is the product of a linear factor and a quadratic factor, and it's $k \oplus k \oplus k$ if $f_{\underline{c}}$ is the product of three distinct linear factors. Finally, if $f_{\underline{c}}$ has a repeated root r then, substituting $x \to x - r$ (which is an automorphism of $k[x]$), we can assume $r = 0$. Then $k[x] \cong k \oplus k[x]/(x^2)$ if 0 is a double root, or $k[x]/(x^3)$ if it's a triple root. No two of the rings thus obtained are isomorphic to each other. □

Remarks 12 *1. If we had defined $f_{\underline{c}}(x)$ as $F_{\underline{c}}(x,1)$ we would have gotten the same quotient ring for each orbit. Indeed, each orbit has an element which is divisible by neither x nor y. For such an element $F_{\underline{c}}(x,1)$ and $F_{\underline{c}}(1,x)$ are both cubic, and their roots are the inverses of one another.*

2. If $k[x]/(f_{\underline{c}}(x))$ is a cubic field, there are two possibilities for its relationship with the field $K_{\underline{c}}$ introduced earlier. Let α be any root of $f_{\underline{c}}(x)$. Then $k[x]/(f_{\underline{c}}(x)) \cong k(\alpha)$. If $k(\alpha)$ contains the other two roots of $f_{\underline{c}}(x)$, then $K_{\underline{c}} = k(\alpha) \cong k[x]/(f_{\underline{c}}(x))$. If not, then the two other roots of $f_{\underline{c}}$ lie in a quadratic extension of $k(\alpha)$, and this extension is $K_{\underline{c}}$. It is, of course, degree 6 over k.

This also enables us to compute the orbits for the action of $GL_2(k)$ on k^4 via ρ. Because of equation (9), which relates the actions by ρ and by ϱ, it is convenient to make the following definition. For $\sigma = (a_1, a_2, a_3, a_4) \in k^4$ let

$$g_\sigma = f_{\sigma \cdot w_1} = f_{(a_4, a_3, a_2, -a_1)} \in k[x].$$

Corollary 13 *Let k be any field. Take σ and $\tau \in k^4$. Then there exists $g \in GL_2(k)$ such that $\tau = \sigma\rho(g)^t$ if and only if*

$$k[x]/(g_\sigma) \cong k[x]/(g_\tau).$$

In what follows, it will also be useful to have a partial description of the orbits of $GL_2(\mathbf{Z}_p)$ acting on $\mathbf{Q}_p^4$ via ϱ. Before proceeding with this it will be useful to introduce a key fact from [18]. For k any field and $\underline{c} = (c_1, c_2, c_3, c_4) \in k^4$ let

$$P(\underline{c}) = c_2^2 c_3^2 + 18 c_1 c_2 c_3 c_4 - 4 c_2^3 c_4 - 4 c_1 c_3^3 - 27 c_1^2 c_4^2.$$

Lemma 14 *For all fields k, all $\underline{c} \in k^4$ and all $g \in GL(2,k)$, we have $P(\underline{c} \cdot \varrho(g)^t) = \det g^2 P(\underline{c})$.*

Proof. This appears near the top of p. 512 of [18]. □

If $f_{\underline{c}}$ is a cubic polynomial, with roots (possibly lying in an extension field) α_1, α_2 and α_3, then $P(\underline{c})$ is known as its discriminant, and is also given by the formula

$$P(\underline{c}) = c_4^4 \prod_{1 \le i < j \le 3} (\alpha_i - \alpha_j)^2.$$

In particular, it is zero if and only if $f_{\underline{c}}$ has a repeated root. See, for example, [3], pp. 610-612.

Proposition 15 *Take* $\underline{c}$ *and* $\underline{d} \in \mathbf{Q}_p^4$*. If* $\underline{c}$ *and* $\underline{d}$ *are in the same* $GL_2(\mathbf{Z}_p)$*-orbit, then* $K_{\underline{c}} = K_{\underline{d}}$, $|P(\underline{c})|_p = |P(\underline{d})|_p$, *and* $\max(|c_1|_p, |c_2|_p, |c_3|_p, |c_4|_p) = \max(|d_1|_p, |d_2|_p, |d_3|_p, |d_4|_p)$*. Moreover, for each relevant field* K

$$\{\underline{c} \in \mathbf{Z}_p^4 : |P(\underline{c})|_p = 1, \text{ and } K_{\underline{c}} = K\}$$

is a single $GL_2(\mathbf{Z}_p)$*-orbit.*

Remark 16 *For* $\underline{c} \in \mathbf{Q}_p^4$ *such that* $|P(\underline{c})| = 1$, $\underline{c} \in \mathbf{Z}_p^4 \iff \max(|c_1|_p, |c_2|_p, |c_3|_p, |c_4|_p) = 1$.

Proof. First assume that $\underline{c}$ and $\underline{d}$ are in the same $GL_2(\mathbf{Z}_p)$-orbit. Then $K_{\underline{c}} = K_{\underline{d}}$, because they are in the same $GL_2(\mathbf{Q}_p)$ orbit, and $|P(\underline{c})|_p = |P(\underline{d})|_p$, by lemma 14 (since the determinant of an element of $GL_2(\mathbf{Z}_p)$ lies in $\mathbf{Z}_p^\times$).

Now, $\max(|c_1|_p, |c_2|_p, |c_3|_p, |c_4|_p) = p^{-k}$ if and only if k is the smallest integer such that $\underline{c} \in p^k \cdot \mathbf{Z}_p^4$. From this description, it's clear that $\max(|d_1|_p, |d_2|_p, |d_3|_p, |d_4|_p) \leq \max(|c_1|_p, |c_2|_p, |c_3|_p, |c_4|_p)$ whenever $\underline{d} = \underline{c}h$ for some 4×4 matrix h with entries in $\mathbf{Z}_p$. In particular, equality holds when $h \in GL_4(\mathbf{Z}_p)$, and this includes the case $h = \rho(g)^t$ for some $g \in GL_2(\mathbf{Z}_p)$.

Now, take $\underline{c}, \underline{d} \in \mathbf{Z}_p^4$ such that $|P(\underline{c})|_p = |P(\underline{d})|_p = 1$ and $K_{\underline{c}} = K_{\underline{d}}$. We must prove that $\underline{c}$ and $\underline{d}$ are in the same orbit. There are three cases, depending on whether $f_{\underline{c}}$ is irreducible, the product of a linear factor by an irreducible quadratic, or the product of three linear factors. The case when $f_{\underline{c}}$ is irreducible is most challenging, and we tackle it in several steps.

The first step is to show that the element $\overline{f}_{\underline{c}}$ of $\mathbf{Z}/p\mathbf{Z}[x]$ obtained by reducing the coefficients of $f_{\underline{c}}$ mod p is also irreducible. Since $P(\underline{c}) \not\equiv 0 \pmod p$, it follows that $\overline{f}_{\underline{c}}$ can't have a double zero. If it had a simple zero, then, by Hensel's lemma, $f_{\underline{c}}$ would have a zero in $\mathbf{Z}_p$. Thus $\overline{f}_{\underline{c}}$ must be irreducible. This implies that c_1 and c_4 are in $\mathbf{Z}_p^\times$.

Since $K_{\underline{d}} = K_{\underline{c}}$, it follows that $f_{\underline{d}}$ must also be irreducible and remain irreducible mod p, and hence that d_1 and d_4 must also be units. Acting by a scalar matrix in $GL_2(\mathbf{Z}_p)$ we can multiply all entries of $\underline{c}$ (or $\underline{d}$) by any scalar in $\mathbf{Z}_p^\times$. From this, it follows that it suffices to treat the case when $f_{\underline{c}}$ and $f_{\underline{d}}$ are monic.

For the next step, we consider the finite extension $\mathbf{Q}_p[x]/(f_{\underline{c}}(x))$. It must contain a root of $f_{\underline{d}}$. Let $\beta = b_0 + b_1 x + b_2 x^2 + (f_{\underline{c}})$ be some such root. A priori, b_0, b_1, b_2 are in $\mathbf{Q}_p$. Our next step is to prove that they are actually in $\mathbf{Z}_p$ and that at least one of b_1, b_2 is in $\mathbf{Z}_p^\times$.

Suppose not. Then there is a unique positive integer k such that $p^k b_0, p^k b_1$, and $p^k b_2$ are all in $\mathbf{Z}_p$ and at least one of them is in $\mathbf{Z}_p^\times$. Reducing mod p gives a nonzero element of the finite field $\mathbf{Z}/p\mathbf{Z}(x)/(\overline{f}_{\underline{c}})$.

But β was a zero of $f_{\underline{d}}(x) = x^3 + d_3 x^2 + d_2 x + d_1$, so $p^k\beta$ is a zero of $x^3 + d_3 p^k x^2 + d_2 p^{2k} x + d_1 p^{3k}$. So, its image in $\mathbf{Z}/p\mathbf{Z}[x]/(\overline{f}_{\underline{c}})$ must be a zero of x^3 and this is a contradiction. Thus $b_0, b_1, b_2 \in \mathbf{Z}_p$.

If we reduce b_0, b_1, b_2 mod p we get a zero of $\overline{f}_{\underline{d}}$ in $\mathbf{Z}/p\mathbf{Z}[x]/(\overline{f}_{\underline{c}})$. Since $\overline{f}_{\underline{d}}$ is irreducible, it can't be in $\mathbf{Z}/p\mathbf{Z}$, so at least one of b_1, b_2 must be in $\mathbf{Z}_p^\times$.

Next, we prove that there exist $a_0, a_1, e_0, e_1 \in \mathbf{Z}_p$ such that $(a_0 + a_1 x) \cdot \beta \equiv (e_0 + e_1 x) \pmod{f_{\underline{c}}(x)}$. Indeed, $x^3 \equiv -(c_1 + c_2 x + c_3 x^2) \pmod{f_{\underline{c}}(x)}$, so for $a_0, a_1 \in \mathbf{Z}_p$ we have

$$(a_0+a_1x)\beta = a_0b_0 - a_1b_2c_1 + (a_1b_0 + b_1a_0 - a_1b_2c_2)x + (a_0b_2 + a_1b_1 - a_1b_2c_3)x^2 \pmod{f_{\underline{c}}(x)}.$$

If b_2 is a unit then we can take $a_1 = 1, a_0 = c_3 - b_1 b_2^{-1}$. And if $b_2 \in p\mathbf{Z}_p$ then $b_1 \in \mathbf{Z}_p^\times$. But then $b_1 - b_2 c_3$ is also in $\mathbf{Z}_p^\times$, and we can take $a_0 = 1$ and $a_1 = -b_2(b_1 - b_2 c_3)^{-1}$.

Now we are ready to prove that $\underline{c}$ and $\underline{d}$ are in the same $GL_2(\mathbf{Z}_p)$-orbit. Let α, ε, and γ be the images of $a_0 + a_1 x, e_0 + e_1 x$ and x in the quotient field $\mathbf{Q}_p[x]/(f_{\underline{c}}(x))$. Note that $(\alpha, \varepsilon) = (1, \gamma) g$ where $g = \left(\begin{smallmatrix} a_0 & e_0 \\ a_1 & e_1 \end{smallmatrix}\right)$. Also, $\beta = \alpha^{-1}\epsilon$. The matrix g has entries in $\mathbf{Z}_p$. We claim that it is in $GL_2(\mathbf{Z}_p)$. If it were not, its columns would be linearly dependent modulo, p. But if this were the case, then $\alpha^{-1}\epsilon$ would be an element of $\mathbf{Z}_p^\times$, and it's not. Since $f_{\overline{d}}$ vanishes at β, it follows that $F_{\overline{d}}$ vanishes at (α, ε). But then $F_{\overline{d} \cdot \varrho(g)^t}$ vanishes at $(1, \gamma)$, and $f_{\overline{d} \cdot \varrho(g)^t}$ vanishes at γ. This forces $\overline{d} \cdot \varrho(g)^t$ to be a scalar multiple of $\underline{c}$, so $\underline{c}$ and $\underline{d}$ are in the same orbit.

We are done in the case when $f_{\underline{c}}$ is irreducible. We now consider the case when it is reducible.

The first step is to prove that, whenever $f_{\underline{c}}$ is reducible, $\underline{c}$ is in the same orbit as an element of the form $(c_1', c_2' 1, 0)$. Assume $\min(|c_1|_p, |c_2|_p, |c_3|_p, |c_4|_p) = |P(\underline{c})|_p = 1$, and $F_{\underline{c}}$ factors as $(a_1 x + a_2 y)(b_1 x^2 + b_2 xy + b_3 y^2)$ with all coefficients in $\mathbf{Q}_p$. Then it's not hard to show that it has a factorization in the same form where all coefficients are in $\mathbf{Z}_p$ and there exists i, j such that a_i and b_j are in $\mathbf{Z}_p^\times$. But then $(a_1, a_2)^t$ is the first column of an element g of $GL_2(\mathbf{Z}_p)$. Acting by the inverse we may transform $(a_1 x + a_2 y)$ to x. Thus, any quadruple $\underline{c}$ such that $F_{\underline{c}}$ is reducible is in the same $GL_2(\mathbf{Z}_p)$ orbit as one where $c_4 = 0$. But if $c_4 = 0$, then $P(\underline{c}) = c_3^2(c_2^3 - 4c_1c_3)$. If all entries are in $\mathbf{Z}_p$ and this is in $\mathbf{Z}_p^\times$, then $c_3 \in \mathbf{Z}_p^\times$. Since each scalar matrix acts by the corresponding scalar, we deduce that any quadruple $\underline{c}$ such that $F_{\underline{c}}$ is reducible is in the same $GL_2(\mathbf{Z}_p)$ orbit as an element with $c_4 = 0, c_3 = 1$. So, suppose $F_{\underline{c}}(x, y) = x(c_1 x^2 + c_2 xy + y^2)$.

If $c_1 x^2 + c_2 xy + y^2$ factors in $\mathbf{Q}_p[x, y]$ then it factors as $(a_1 x + y)(a_2 x + y)$ where $a_1, a_2 \in \mathbf{Z}_p$. Acting by $\left(\begin{smallmatrix} 1 & -a_1 \\ 0 & 1 \end{smallmatrix}\right)$ transforms $a_1 x + y$ to y, while leaving x fixed. Thus, if $F_{\underline{c}}$ is a product of distinct linear factors, then it is in the same $GL_2(\mathbf{Z}_p)$-orbit as $(0, c_2', 1, 0)$ where $c_2' = a_2 - a_1$. Now, $P((0, c_2', 1, 0)) = (c_2')^2$, so $c_2' \in \mathbf{Z}_p^\times$. Then $\left(\begin{smallmatrix} 1 & 0 \\ 0 & c_2' \end{smallmatrix}\right)$ transforms $xy(c_2' x + y)$ to $xy(x + y)$. Thus, any tuple $\underline{c}$ such that $F_{\underline{c}}$ is a product of distinct linear factors is in the same $GL_2(\mathbf{Z}_p)$-orbit as $(0, 1, 1, 0)$.

Now suppose $c_1 x^2 + c_2 xy + y^2$ does not factor. If p is not 2 then we can act by $\left(\begin{smallmatrix} 1 & -c_2/2 \\ 0 & 1 \end{smallmatrix}\right)$ to get rid of c_2. That is, each $GL_2(\mathbf{Z}_p)$-orbit with a linear factor contains an element of the form $(c_1, 0, 1, 0)$. Since $P((c_1, 0, 1, 0)) = -4c_1$, we deduce (still under the assumption that $p \neq 2$) that $c_1 \in \mathbf{Z}_p^\times$. And since

$$(c_1, 0, 1, 0) \cdot \varrho \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = (a^2 c_1, 0, 1, 0),$$

it follows that two quadruples which generate the same quadratic extension are in the same $GL_2(\mathbf{Z}_p)$-orbit.

If $p = 2$ this approach doesn't work: for example, the $GL_2(\mathbf{Z}_p)$-orbit of $x^2 + xy + y^2$ does not contain any element of the form $cx^2 + y^2$ with $c \in \mathbf{Z}_2$. However, if $x^2 + c_2x + c_1$ and $x^2 + d_2x + d_1$ generate the same quadratic extension, then a simpler version of the argument given in the cubic case works. Take γ a zero of $x^2 + c_2x + c_1$ and β a zero of $x^2 + d_2x + d_1$ then $\beta = b_0 + b_1\gamma$ where $b_0 \in \mathbf{Z}_p$ and $b_1 \in \mathbf{Z}_p^\times$. Then $\underline{c}$ and $\underline{d} \cdot \varrho \left(\begin{smallmatrix} 1 & b_0 \\ 0 & b_1 \end{smallmatrix}\right)$ are unit scalar multiples of each other, and hence $\underline{c}$ and $\underline{d}$ are in the same orbit.

□

2.9 The Results of Jiang and Rallis

In this section we briefly describe the main results of [8]. First, we take a continuous function $f : G_2(\mathbf{A}) \times \mathbf{C} \to \mathbf{C}$ such that

$$f_s(nm(g)h) = |\det g|^s f_s(h), \tag{17}$$

for all $g \in GL_2(\mathbf{A}), n \in N(\mathbf{A})$ and $h \in G_2(\mathbf{A})$. (Here, the value of f at $h \in G_2(\mathbf{A})$ and $s \in \mathbf{C}$ is denoted $f_s(h)$ rather than $f(h, s)$.) We also select a row vector $\sigma \in \mathbf{Q}^4$, and let

$$I^\sigma(s, f_s) := \int_{(\mathbf{Q}\backslash\mathbf{A})^5} f_s(w_0 n(x, y, z, u, v), s)\psi((v, u, y, x) \cdot \underline{\sigma})\, dn,$$

and

$$w_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Here, the integral over $(\mathbf{Q}/\mathbf{A})$ really means an integral over a measurable fundamental domain, and dn is the product measure. For $h_1 \in G_2(\mathbf{A})$, We define $R(h_1)f_s(h) = f_s(hh_1)$. Notice that $R(h_1)f_s$ is another function which satisfies (17) so $I^\sigma(s, R(h_1)f_s)$ is defined as well. Moreover, $I^\sigma(s, R(m(\gamma))f_s) = I^{\sigma\cdot\rho(\gamma)^t}(s, f_s)$, so it suffices to study $I^\sigma(s, f_s)$ for σ ranging over a set of representatives for the orbits of $GL_2(\mathbf{Q})$, acting on $\mathbf{Q}^4$ via ρ.

The first main result of Jiang and Rallis states that

$$I^\sigma(s, R(g).f_s) = \int_{N(\mathbf{Q})\backslash N(\mathbf{A})} E(ng, s; f_s)\psi_\sigma(n)\, dn,$$

provided that σ corresponds to a polynomial with distinct roots. Here $E(g, s, ; f_s)$ is a certain function $G_2(\mathbf{Q})\backslash G_2(\mathbf{A}) \times \mathbf{C} \to \mathbf{C}$ called an Eisenstein series. We won't go into the details of this part, but we mention it to motivate the following. From now on we shall only consider σ which are attached to polynomials with distinct roots.

To describe the next result, we assume not only that f_s satisfies (17), but also that f_s factors as a special type of product. For each prime p, we can define

$$f^\circ_{s,p}(nm(g)k) = |\det g|_p^s, \qquad g \in GL(2,\mathbf{Q}_p), n \in N(\mathbf{Q}_p), k \in G_2(\mathbf{Z}_p).$$

To see that this defines a function on all of $G_2(\mathbf{Q}_p)$ recall that any $h \in G_2(\mathbf{Q}_p)$ can be expressed as bk with $b \in P(\mathbf{Q}_p)$ and $k \in G_2(\mathbf{Z}_p)$. Then b can be expressed as $nm(g)$ for some $n \in N(\mathbf{Q}_p)$ and $g \in GL_2(\mathbf{Q}_p)$. The expression $h = bk$ is not unique, but if $b_1k_1 = b_2k_2$ then $b_2 = b_1\beta$ with $\beta \in P(\mathbf{Z}_p)$. It follows that, if $b_j = n_jm(g_j)$ for $j = 1,2$ then $g_2 = g_1\gamma$ for some $\gamma \in GL_2(\mathbf{Z}_p)$. But then $|\det \gamma|_p = 1$, so $|\det g_1|_p = |\det g_2|_p$.

We now assume that

$$f_s(h) = f_{s,\infty}(h_\infty) \prod_p f_{s,p}(h_p) \qquad \text{for } h = (h_\infty, h_2, h_3, \dots, h_p, \dots) \in G_2(\mathbf{A}),$$

and that the set of primes such that $f_{s,p} \neq f^\circ_{s,p}$ is finite. (Note that this second condition ensures that the infinite product is always convergent because all but finitely many of its factors are one.) This ensures that

$$I^\sigma(s, f_s) = I^\sigma_\infty(s, f_{s,\infty}) \cdot \prod_p I^\sigma_p(s, f_{s,p}),$$

where

$$I^\sigma_p(s, f_{s,p}) = \int_{\mathbf{Q}_p^5} f_{s,p}(w_0 n)\psi_p((v,u,y,x)\cdot \underline{\sigma})\, dn_p,$$

and I_∞ is defined analogously. Here, dn_p denotes the product measure on $\mathbf{Q}_p^5$.

The second main result of Jiang and Rallis is to compute $I^\sigma_p(s, f^\circ_{s,p})$ under some additional hypotheses.

Theorem 18 (Cf. [8],theorem 2) *Assume that ψ_p is trivial on $\mathbf{Z}_p$ but not on $p^{-1}\mathbf{Z}_p$.*

1. *If $\sigma = (0,1,1,0)$ then*

$$I^\sigma_p(s, f^\circ_{s,p}) = \frac{(1-p^{-3s})(1-p^{-3s+1})(1-p^{-6s+2})(1-p^{-9s+3})}{(1-p^{-3s+1})^3}.$$

2. *If $\sigma = (0,1,0,a)$ with $a \in \mathbf{Z}_p^\times$ such that $-a$ is not a square, then*

$$I^\sigma_p(s, f^\circ_{s,p}) = \frac{(1-p^{-3s})(1-p^{-3s+1})(1-p^{-6s+2})(1-p^{-9s+3})}{(1-p^{-3s+1})(1-p^{-6s+2})}.$$

3. *If $\sigma = (1,0,0,a)$ with $a \in \mathbf{Z}_p^\times$ which is not a cube, then*

$$I^\sigma_p(s, f^\circ_{s,p}) = \frac{(1-p^{-3s})(1-p^{-3s+1})(1-p^{-6s+2})(1-p^{-9s+3})}{(1-p^{-9s+3})}.$$

Remarks 19 *1. In each case the numerator is the same, and in each case, some part of it can be cancelled with the denominator but never the same part.*

2. *The result can also be expressed in terms of "zeta functions" of non-Archimedean local fields.*

3. *Jiang and Rallis actually prove the corresponding result for any non-Archimedean local field, not just* $\mathbf{Q}_p$.

4. *For* $k \in GL(2, \mathbf{Z}_p)$, *we have*

$$I_p^{\sigma \cdot \rho(k)^t}(s, f_{s,p}^{\circ}) = I_p^{\sigma}(s, f_{s,p}^{\circ}).$$

   So, the result actually determines the value of $I_p^{\sigma}(s, f_{s,p}^{\circ})$ *for any* $\sigma = \underline{c}w_1^{-1} \in \mathbf{Z}_p^4$ *such that* $P(\underline{c}) \neq 0$ *and* $K_{\underline{c}}$ *is either* $\mathbf{Q}_p$, *or the quadratic extension obtained by adjoining the square root of a unit, or the cubic extension obtained by adjoining the cube root of a unit.*

5. *The restriction to* $a \in \mathbf{Z}_p^{\times}$ *is not such a big deal. For any fixed* $\underline{c} \in \mathbf{Q}^4$ *with* $P(\underline{c}) \neq 0$, *we have* $P(\underline{c}) \in \mathbf{Z}_p^{\times}$ *for all but a finite number of* p. *If a quadruple* $\underline{c}$ *such that* $P(\underline{c}) \in \mathbf{Z}_p^{\times}$ *is in the same* $GL_2(\mathbf{Z}_p)$*-orbit as an element of the form* $(0, 1, 0, a)$ *or* $(1, 0, 0, a)$, *then* a *must be in* $\mathbf{Z}_p^{\times}$.

6. *The assumption that* ψ_p *is trivial on* $\mathbf{Z}_p$ *but not on* $\frac{1}{p}\mathbf{Z}_p$ *is a natural one. If* $\psi = \prod_v \psi_v$ *is any character of* $\mathbf{A}$, *then there are only finitely many* p *where it does not hold. And, since we work over* $\mathbf{Q}$ *rather than an arbitrary number field, we can take* ψ *to be the function* e *introduced before, and then the assumption is true for all* p.

7. *The restriction to cubic extensions which are obtained by adjoining the cube root of a unit is more restrictive. Indeed, if* $p \equiv 2 \pmod 3$ *then it follows from Hensel's lemma that every element of* $\mathbf{Z}_p^{\times}$ *is a cube.*

In order to motivate the results of Pleso, we briefly describe some of the methods in Jiang-Rallis. First, note that

$$w_0 n(x, y, z, u, v) w_0^{-1} = n^-(-x, y, z, u, -v).$$

It follows that

$$\begin{aligned} I_p^{\sigma}(s, f_{s,p}^{\circ}) = &\int_{\mathbf{Q}_p}\int_{\mathbf{Q}_p}\int_{\mathbf{Q}_p}\int_{\mathbf{Q}_p}\int_{\mathbf{Q}_p} \\ &\quad f_{s,p}^{\circ}(n^-(-x, y, z, u, -v))\psi_p((v, u, y, x) \cdot \sigma)\, dx\, dy\, dz\, du\, dv, \\ = &\; I_+ + I_-, \end{aligned}$$

where

$$I_+ = \int\limits_{\mathbf{Z}_p}\int\limits_{\mathbf{Q}_p}\int\limits_{\mathbf{Q}_p}\int\limits_{\mathbf{Q}_p}\int\limits_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x,y,z,u,-v))\psi_p((v,u,y,x)\cdot\sigma)\,dx\,dy\,dz\,du\,dv,$$

and I_- is the similar integral where v is integrated over $\mathbf{Q}_p - \mathbf{Z}_p$ and each of the other four variables is integrated over $\mathbf{Q}_p$. Now,

$$n^-(-x,y,z,u,-v) = n^-(-x,y,z,u,0)n^-(0,0,0,0,-v),$$

If $v \in \mathbf{Z}_p$, then $n^-(0,0,0,0,-v) \in G_2(\mathbf{Z}_p)$, so

$$f^\circ_{s,p}(n^-(-x,y,z,u,-v)) = f^\circ_{s,p}(n^-(-x,y,z,u,0)).$$

Moreover, if we assume $\sigma \in \mathbf{Z}_p^4$, then $v \in \mathbf{Z}_p$ implies $\psi_p(\sigma_1 v) = 1$. Hence,

$$I_+ = \int\limits_{\mathbf{Q}_p}\int\limits_{\mathbf{Q}_p}\int\limits_{\mathbf{Q}_p}\int\limits_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x,y,z,u,0))\psi_p((0,u,y,x)\cdot\sigma)\,dx\,dy\,dz\,du,$$

As we mentioned before, each of the roots of the G_2 root system corresponds to a one dimensional subgroup of the group G_2, and the groups N and N^- are each formed by bundling five of those groups together. For each root γ, we have made a choice of parametrization x_γ from R to the corresponding group.

Now, for each root γ there is a homomorphism $\varphi_\gamma : SL_2 \to G_2$ such that

$$x_\gamma(a) = \varphi_\gamma\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix} \qquad x_{-\gamma}(a) = \varphi_\gamma\begin{pmatrix}1 & 0\\ a & 1\end{pmatrix}.$$

If $v \in \mathbf{Q}_p - \mathbf{Z}_p$, then the following SL_2-identity

$$\begin{pmatrix}1 & 0\\ -v & 1\end{pmatrix} = \begin{pmatrix}v^{-1} & 0\\ 0 & v\end{pmatrix}\begin{pmatrix}1 & -v\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & v^{-1}\end{pmatrix}, \tag{20}$$

gives rise to a G_2-identity

$$x_{-\alpha-3\beta}(v) = h(1,v^{-1})x_{\alpha+3\beta}(-v)\varphi_{\alpha+3\beta}\begin{pmatrix}0 & 1\\ -1 & v^{-1}\end{pmatrix}.$$

Now, $\begin{pmatrix}0 & 1\\ -1 & v^{-1}\end{pmatrix} \in G_2(\mathbf{Z}_p)$ and

$$h(1,v)n^-(-x,y,z,u,0)h(1,v^{-1}) = n^-(-vx,y,v^{-1}z,v^{-1}u,0),$$

so

$$I_- = \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} f^\circ_{s,p}(h(1, v^{-1})n^-(-vx, y, v^{-1}z, v^{-1}u, 0)x_{\alpha+3\beta}(-v))\psi_p((0, u, y, x) \cdot \sigma)\, dx\, dy\, dz\, du,$$

$$= \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} |v|_p^{-3s+1} f^\circ_{s,p}(n^-(-x, y, z, u, 0)x_{\alpha+3\beta}(-v))\psi_p((0, uv, y, x/v) \cdot \sigma)\, dx\, dy\, dz\, du,$$

For the second identity, we used (17) and made changes of variable in x, u, and z.

Moreover,

$$n(-x, y, z, u, 0)x_{\alpha+3\beta}(-v) = x_{\alpha+3\beta}(-v)x_\beta(uv)n^-(-x + vz - 3uvy + u^3v^2, y - u^2v, z - u^3v, u, 0).$$

Making additional changes of variable, we obtain

$$I_- = \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} \int\limits_{\mathbf{Q}_p} |v|_p^{-3s+1} f^\circ_{s,p}(n^-(-x, y, z, u, 0)) \psi_p((0, uv, y + u^2v, x/v + z - 3uy - 3u^3v) \cdot \sigma)\, dx\, dy\, dz\, du.$$

The next step is to split each of the integrals I_+ and I_- into two pieces based on whether $u \in \mathbf{Z}_p$ or $u \in \mathbf{Q}_p - \mathbf{Z}_p$. After that, we can split on z and y, eventually obtaining an expression of the original $I_p^\sigma(s, f^\circ_{s,p})$ as a sum of sixteen integrals, I_{++++} to I_{----} each of which involves only $f^\circ_{s,p}(n^-(-x, 0, 0, 0, 0))$, at the expense of having a more complicated expression inside of ψ. For example I_{++++} corresponds to taking all variables in $\mathbf{Z}_p$, I_{+-++} corresponds to all in $\mathbf{Z}_p$ except u, which is in $\mathbf{Q}_p - \mathbf{Z}_p$, and so on. Following Pleso, we abbreviate $n^-(-x, 0, 0, 0, 0)$ to $n^-(-x)$.

2.10 The Results of Pleso

By restricting their attention to cubic extensions which were obtained by adjoining a cube root, Jiang and Rallis could benefit in two ways. First, they could assume that, in the case when σ was attached to a cubic extension, it was of the form $(1, 0, 0, a)$. This simplified the argument of ψ because some of the complicated expressions that would otherwise have entered were multiplied by 0. So, each of their sixteen integrals was simpler than it would have been if they'd considered the more general form $(1, 0, b, a)$. Second, the assumption assures that certain finite fields which arise in their calculations contains three cube roots of 1, and they were able to use this to their advantage in computing some of the sixteen sub-integrals.

In order to extend the results of Jiang and Rallis to the case when the roots of the polynomial g_σ attached to σ generate a cubic extension which can't be generated by adjoining a cube root, one has to do two things. First, one must re-do the bifurcation process, keeping track of the additional complexity that appears in the argument of ψ when $\sigma = (1, 0, b, a)$ with $b \neq 0$. Second, one must compute the sixteen generalized sub-integrals thus obtained. In some cases, this is a straightforward matter of checking that the arguments given by Jiang and Rallis in the $b = 0$ case still work. But in other cases, new ideas are required.

3 Some Technical Lemmas

Throughout our computations, we assume that ψ_p is a continuous homomorphism $\mathbf{Q}_p \to \mathbf{C}^\times$ which is trivial on $\mathbf{Z}_p$ but not on $p^{-1}\mathbf{Z}_p$. For simplicity, the reader may assume that it is e_p.

The following are some technical lemmas that are applicable to multiple cases in the computations.

Lemma 21 *For any $c \in \mathbf{C}$, $a \in \mathbf{Q}_p$, and $k \in \mathbf{Z}$,*

$$\int_{\{x \in \mathbf{Q}_p : |x-a|_p \le p^{-k}\}} c \quad dx = cp^{-k}.$$

Proof. Indeed, $\{x \in \mathbf{Q}_p : |x-a|_p \le p^{-k}\}$ is precisely the open ball $a + p^k\mathbf{Z}_p$. As discussed in the Haar measure section, this ball has measure p^{-k}. And, as with Lebesgue measure, the integral of a constant function over a measurable set is simply the constant times the measure of the set. □

Lemma 22 (Change of Variables) *Take $v \in \mathbf{Q}_p^\times$, and $c \in \mathbf{Q}_p$, and let $f : \mathbf{Q}_p \to \mathbf{C}$ be an integrable function. Then the functions g, h defined by $g(x) = f(vx)$ and $h(x) = f(x + c)$ are also integrable, and their integrals are given by*

$$\int_{\mathbf{Q}_p} f(vx)\, dx = |v|_p^{-1} \int_{\mathbf{Q}_p} f(z)\, dz,$$

and

$$\int_{\mathbf{Q}_p} f(x+c)\, dx = \int_{\mathbf{Q}_p} f(y)\, dy.$$

This is expressed by saying that if $z = vx$ then $dz = |v|_p\, dx$ and $dy = dx$.

Proof. The integral of an arbitrary measurable function is defined by approximating it with step functions as in (4), so it suffices to treat the case when f is a step function. Since both sides of each formula are linear in f it suffices to treat the case when f is the characteristic function $\mathbb{1}_{a+p^k\mathbf{Z}_p}$ for some a, k. Clearly, $x + c \in a + p^k\mathbf{Z}_p$ if and only if $x \in a - c + p^k\mathbf{Z}_p$. Then

$$\int_{\mathbf{Q}_p} f(x+c)\, dx = \int_{\mathbf{Q}_p} \mathbb{1}_{a-c+p^k} = \mathrm{Vol}(a - c + p^k) = p^{-k},$$

and

$$\int_{\mathbf{Q}_p} f(y)\,dy = \int_{\mathbf{Q}_p} \mathbb{1}_{a+p^k} = \mathrm{Vol}(a+p^k) = p^{-k}.$$

Notice that this is just the invariance property of the Haar measure. Similarly, $vx \in a + p^k\mathbf{Z}_p$ if and only if $x \in v^{-1}a + p^{k-\mathrm{ord}_p(v)}\mathbf{Z}_p$. Thus

$$\int_{\mathbf{Q}_p} f(vx)\,dx = \mathrm{Vol}(v^{-1}a + p^{k-\mathrm{ord}_p(v)}\mathbf{Z}_p) = p^{\mathrm{ord}_p(v)-k} = |v|_p^{-1}\int_{\mathbf{Q}_p} f(z)\,dz.$$

□

Lemma 23 *For any $a \in \mathbf{Q}_p$,*

$$\int_{\mathbf{Z}_p} \psi_p(ax)\,dx = \mathbb{1}_{\mathbf{Z}_p}(a).$$

This lemma is quite well-known, but the proof is short and nice, so we include it.
Proof. If $a \in \mathbf{Z}_p$ then $ax \in \mathbf{Z}_p$ for all x. But then $\psi(ax) = 1$ for all x, and we just get the measure of $\mathbf{Z}_p$, which is 1. If $a \notin \mathbf{Z}_p$ then ψ is not trivial on $a\mathbf{Z}_p$. Choose x_0 such that $\psi_p(ax_0) \neq 1$. Then

$$\int_{\mathbf{Z}_p} \psi_p(ax)\,dx = \int_{\mathbf{Z}_p} \psi_p(a(x+x_0))\,dx = \psi_p(ax_0)\int_{\mathbf{Z}_p} \psi_p(ax)\,dx,$$

which forces the integral to be 0. □

Lemma 24 *Let $\mathbb{1}_{\mathbf{Z}_p}$ be the characteristic function of $\mathbf{Z}_p$. That is, $\mathbb{1}_{\mathbf{Z}_p}(t)$ is 1, if $t \in \mathbf{Z}_p$ or 0 if $t \notin \mathbf{Z}_p$. Then*

$$\int_{\mathbf{Z}_p^\times} \psi_p(-xt)\,dx = \mathbb{1}_{\mathbf{Z}_p}(t) - p^{-1}\mathbb{1}_{\mathbf{Z}_p}(pt).$$

Proof. Express the left hand side as the integral over $\mathbf{Z}_p$ minus the integral over $p\mathbf{Z}_p$. Apply lemma 23 to the first integral. In the second integral, use lemma 22 to substitute $y = px$. As x ranges over $p\mathbf{Z}_p$, y ranges over $\mathbf{Z}_p$, and so lemma 23 can be applied again. □

Remark 25 *Replacing $\psi_p(-xt)$ by $\psi_p(xt)$ on the left hand side does not change the right hand side, since $\mathbb{1}_{\mathbf{Z}_p}$ is an even function.*

Corollary 26 *Let $a, b \in \mathbf{Z}$, $c \in \mathbf{Q}_p$, $u \in \mathbf{Q}_p - \mathbf{Z}_p$ and $u = \mu p^U$. Then*

$$\int_{\mathbf{Q}_p-\mathbf{Z}_p} |u|_p^{as+b}\psi_p(cu)\,du = \sum_{U=-\infty}^{-1} p^{-U(as+b+1)}\int_{\mathbf{Z}_p^\times} \psi_p(c\mu p^U)\,d\mu$$

$$\begin{cases} \frac{p^{as+b}}{1-p^{as+b}}\left[(1-|c|_p^{-as-b-1}) - p^{-1}(1-|c|_p^{-as-b-1}p^{as+b+1})\right], & c \in \mathbf{Z}_p, \\ 0, & c \notin \mathbf{Z}_p. \end{cases}$$

Proof. The first equation holds because $\mathbf{Q}_p - \mathbf{Z}_p$ is the countable disjoint union of the sets $p^U \mathbf{Z}_p^\times$, for U from -1 to $-\infty$. We plug in $u = p^U \mu$ and use lemma 22. Each of the μ integrals can then be computed using lemma 24, yielding

$$\sum_{U=-\infty}^{-1} p^{-U(as+b+1)} (\mathbb{1}_{\mathbf{Z}_p}(cp^U) - p^{-1}\mathbb{1}_{\mathbf{Z}_p}(cp^{U+1})).$$

Since cp^U (respectively, cp^{U+1}) is in $\mathbf{Z}_p$ if and only if $U \geq -\operatorname{ord}_p(c)$ (respectively $-\operatorname{ord}_p(c) - 1$), we obtain

$$\sum_{U=-\operatorname{ord}_p(c)}^{-1} p^{-U(as+b+1)} - p^{-1} \sum_{U=-\operatorname{ord}_p(c)-1}^{-1} p^{-U(as+b+1)}.$$

Summing these finite geometric series yields

$$\frac{p^{(as+b+1)} - p^{(as+b+1)(\operatorname{ord}_p(c)+1)}}{1 - p^{as+b+1}} - p^{-1} \frac{p^{(as+b+1)} - p^{(as+b+1)(\operatorname{ord}_p(c)+2)}}{1 - p^{as+b+1}}.$$

Plugging in $|c|_p = p^{-\operatorname{ord}_p(c)}$ and simplifying gives the second identity. □

Lemma 27 *For $s \in \mathbf{C}$, if $a \in \mathbf{Z}_p$, then*

$$\int_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x))\psi_p(ax)\, dx = \frac{1 - p^{-3s}}{1 - p^{1-3s}} (1 - |a|_p^{3s-1} p^{1-3s}).$$

Otherwise, the integral vanishes.

Proof. We split the domain of integration into two pieces: $\mathbf{Z}_p$ and $\mathbf{Q}_p - \mathbf{Z}_p$. If $x \in \mathbf{Z}_p$ then $n^-(-x) \in G_2(\mathbf{Z}_p)$ and hence $f^\circ_{s,p}(n^-(-x)) = 1$. By Lemma 23, we get

$$\int_{\mathbf{Z}_p} f^\circ_{s,p}(n^-(-x))\psi_p(ax)\, dx = \mathbb{1}_{\mathbf{Z}_p}(a)\, dx.$$

If $|x|_p > 1$ then we use the identity (20) and an embedding $SL_2 \to G_2$ to check that $f^\circ_{s,p}(n^-(-x)) = |x|_p^{-3s}$. We can then apply corollary 26 to compute this part.

Combining the two parts gives

$$\int_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x))\psi_p(ax)\, dx = \frac{p^{-(3s-1)} - p^{-(3s-1)}|a|_p^{3s-1}}{1 - p^{-(3s-1)}} - p^{-3s}|a|_p^{3s-1} + 1.$$

Now we find a common denominator, expand and simplify the expression to have

$$\int_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x))\psi_p(ax)\, dx$$
$$= \frac{1 - p^{-(3s-1)} - p^{-3s}|a|_p^{3s-1} + p^{-(6s-1)}|a|_p^{3s-1} + p^{-(3s-1)} - p^{-(3s-1)}|a|_p^{3s-1}}{1 - p^{-(3s-1)}}$$

$$= \frac{1 - p^{-3s}|a|_p^{3s-1} + p^{-(6s-1)}|a|_p^{3s-1} - p^{-(3s-1)}|a|_p^{3s-1}}{1 - p^{-(3s-1)}} = \frac{1 - p^{-3s}}{1 - p^{1-3s}}(1 - |a|_p^{3s-1}p^{1-3s}).$$

□

Lemma 28 *Let $h \in \mathbf{Z}_p[r, y, u]$ be a polynomial in three variables with coefficients in $\mathbf{Z}_p$, and for any negative integer V, let*

$$S(V) = \{(r, y, u) \in (\mathbf{Z}/p^{-V}\mathbf{Z}) \times (\mathbf{Z}/p^{-V}\mathbf{Z}) \times (\mathbf{Z}/p^{-V}\mathbf{Z}) \mid h(r, y, u) = 0\}.$$

Then, for each V, reduction mod p^{-V} gives a well-defined function $\rho : S(V-1) \to S(V)$.

Proof. Indeed, if (r_1, y_1, u_1) and (r_2, y_2, u_2) are equivalent modulo $-V+1$, then they are equivalent modulo $-V$, and if $h(r, y, u)$ is 0 modulo $-V+1$, then it is zero modulo V. □

Remark 29 *In some of our applications one or more of the variables is restricted to $(\mathbf{Z}/p^{-V}\mathbf{Z})^\times$. The lemma remains true in this context with the same proof, since an element of $\mathbf{Z}/p^{-V+1}\mathbf{Z}$ is a unit if and only if its image in $\mathbf{Z}/p^{-V}\mathbf{Z}$ is.*

Lemma 30 *Let h, V and $S(V)$ be as in lemma 28. Let $\overline{h}$ be the image of $(h_r(t), h_y(t), h_u(t))$ in $(\mathbf{Z}/p\mathbf{Z})^3$, and suppose that it is not zero. Here h_r is the partial derivative of h with respect to the variable r and so on. Then, for all $t \in S(V)$,*

$$\#\{a \in S(V-1) | \rho(a) = t\} = p^2.$$

Proof. Fix $t = (r_0, y_0, u_0) \in S(V)$. The number of $a \in (\mathbf{Z}/p^{-V+1}\mathbf{Z})^3$ such that $\rho(a) = t$ is p^3, and we can express each element uniquely as $a = (r_0 + p^{-V}\alpha, y_0 + p^{-V}\beta, u_0 + p^{-V}\gamma)$, with $\alpha, \beta, \gamma \in \mathbf{Z}/p\mathbf{Z}$. We can plug in a Taylor expansion in each variable, and higher order terms vanish modulo p^{-2V}. Hence

$$h(a) \equiv h(t) + p^{-V}(\alpha h_r(t) + \beta h_y(t) + \gamma h_u(t)) \mod p^{-2V}.$$

Since $h(r_0, y_0, u_0)$, is divisible by p^{-V}, we can write it as $-p^{-V}d$, for some $d \in \mathbf{Z}_p$. Then

$$h(a) \equiv 0 \mod p^{-V+1} \iff (\alpha h_r(t) + \beta h_y(t) + \gamma h_u(t)) \equiv -d \mod p.$$

This expression can be written as a matrix representation;

$$(\overline{h}) \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = d$$

This is a linear equation in three variables over the field with p elements. If $d = 0$, then its solution is a two dimensional subspace of $(\mathbf{Z}/p\mathbf{Z})^3$. If not, it's a coset of that subspace. In either case, it has p^2 elements. □

Corollary 31 *Let $S(V)$ be defined as in lemma 30, using a polynomial h such that $\overline{h}$, defined as in lemma 30 is nonzero. Let $N(V)$ be the number of elements in $S(V)$. Then $N(V-1) = p^2 N(V)$.*

Proof. Notice that by Lemma 30, $\#\{a \in S(V-1) | \rho(a) = t\} = p^2$, for each element of $S(V)$. So the number of elements in $S(V-1)$ is simply the number of elements in $S(V-1)$ that map to each element in $S(V)$, p^2, times the amount of elements in $S(V)$, $N(V)$. Therefore $N(V-1) = p^2 N(V)$. □

4 Computations

We compute all 16 pieces of $I_p^\sigma(s, f_{s,p}^\circ)$ when $\sigma = (1, 0, b, c)$ with $b, c \in \mathbf{Z}_p^\times$ such that $g_\sigma(u) = -u^3 + bu + c$ is irreducible, and all $p \equiv 5 \mod 6$. Some of our results do not need all of these conditions to be satisfied. Throughout this section, σ is fixed, and we denote g_σ simply as g.

We remark that the values of $I_{++++}, I_{+++-}, I_{++-+}, I_{++--}, I_{+-+-}, I_{+--+}, I_{+---}, I_{-++-}$, and I_{-+--} were already computed by Pleso in [12]. We include them here for the sake of completeness. The first four may reasonably be attributed to Jiang and Rallis in [8], since, as Pleso points out, the coefficient b, which is zero in Jiang-Rallis and nonzero here, does not appear at all in them.

Case 1 (I_{++++})

$$\mathbf{I}_{++++} = \int_{\mathbf{Q}_p} f_{s,p}^\circ(n^-(-x))\psi_p(x)\,dx.$$

Applying Lemma 27, notice that since $|1|_p = 1, 1 \in \mathbf{Z}_p$, so the solution to the integral is as follows:

$$\mathbf{I}_{++++} = \int_{\mathbf{Q}_p} f_{s,p}^\circ(n^-(-x))\psi_p(x)\,dx = \frac{1-p^{-3s}}{1-p^{-3s+1}}(1 - |1|_p^{3s-1} p^{-3s+1}) = 1 - p^{-3s}.$$

Case 2 (I_{+++-})

$$\mathbf{I}_{+++-} = \int_{\mathbf{Q}_p - \mathbf{Z}_p} |y|_p^{-9s+3} \int_{\mathbf{Q}_p} f_{s,p}^\circ(n^-(-x))\psi_p(xy^3)\,dx\,dy.$$

Notice that since $|y|_p > 1$, then $|y^3|_p > 1$, which implies that $y^3 \notin \mathbf{Z}_p$. By Lemma 27, the integral vanishes.

Case 3 (I_{++-+})

$$\mathbf{I}_{++-+} = \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{\mathbf{Z}_p} |z|_p^{-6s+2}\psi_p(-z^2y^3) \int_{\mathbf{Q}_p} f_{s,p}^\circ(n^-(-x))\psi_p(xz)\,dx\,dy\,dz.$$

Notice that since $|z|_p > 1$ then $z \notin \mathbf{Z}_p$. By Lemma 27, the integral vanishes.

Case 4 (I_{++--})

$$\mathbf{I}_{++--} = \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} f^{\circ}_{s,p}(n^-(-x))|y|_p^{-9s+3}|z|_p^{-6s+2}\psi_p(-z^2y^3) \int\limits_{\mathbf{Q}_p} \psi_p(xy^3z)\, du\, dy\, dz.$$

Notice that since $|y|_p > 1$ and $|z|_p > 1$, then $|y^3z|_p > 1$ which implies that $y^3z \notin \mathbf{Z}_p$. By Lemma 27, the integral vanishes.

Case 5 (I_{+-++})

$$\mathbf{I}_{+-++} = \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} |u|_p^{-9s+4}\psi_p(bu - u^3z^2 - 3uy^2 - 3u^2yz) \int\limits_{\mathbf{Q}_p} f^{\circ}_{s,p}(n^-(-x))\psi_p(x)\, dx\, dz\, dy\, du.$$

Notice that the integral with respect to x is identical to the integral with respect to x in Case 1 (I_{++++}). Let $\psi_1(a,d) = a^2 + 3ad + 3d^2$. Then,

$$\mathbf{I}_{+-++} = (1 - p^{-3s}) \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} |u|_p^{-9s+4}\psi_p(bu - u\psi_1(uz, y))\, dz\, dy\, du.$$

Applying Corollary 26 we get,

$$\mathbf{I}_{+-++} = (1 - p^{-3s}) \sum_{U=-\infty}^{-1} p^{-U(-9s+5)} \int\limits_{\mathbf{Z}_p^{\times}} \int\limits_{\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} \psi_p(b\mu p^U - \mu p^U \psi_1(\mu p^U z, y))\, dz\, dy\, d\mu.$$

Let $w = \mu p^U z \to z = \mu^{-1}p^{-U}w$. Then, $z \in \mathbf{Z}_p \iff w \in p^U\mathbf{Z}_p$. Also, by Lemma 22 $dz = p^U\, dw$. So,

$$\mathbf{I}_{+-++} = (1 - p^{-3s}) \sum_{U=-\infty}^{-1} p^{-U(-9s+4)} \int\limits_{\mathbf{Z}_p^{\times}} \int\limits_{\mathbf{Z}_p} \int\limits_{p^U\mathbf{Z}_p} \psi_p(\mu p^U(b - \psi_1(w, y)))\, dw\, dy\, d\mu.$$

Applying Lemma 24,

$$\mathbf{I}_{+-++} = (1 - p^{-3s}) \sum_{U=-\infty}^{-1} p^{-U(-9s+4)} \int\limits_{\mathbf{Z}_p} \int\limits_{p^U\mathbf{Z}_p} \mathbb{1}_{\mathbf{Z}_p}(p^U(b - \psi_1(w, y)))$$

$$-p^{-1}\mathbb{1}_{\mathbf{Z}_p}(p^{U+1}(b - \psi_1(w, y)))\, dw\, dy.$$

For $k \in \mathbf{Z}, k \geq 0$, let

$$S_{k,b} = \{(w, y) \in \mathbf{Z}_p^2 : b - \psi_1(w, y) \in p^k\mathbf{Z}_p\}.$$

Notice that, for any nonpositive integer U,

$$S_{k,b} = \{(w,y) \in p^U\mathbf{Z}_p \times \mathbf{Z}_p : b - \psi_1(w,y) \in p^k\mathbf{Z}_p\}.$$

That is, allowing w to range over the larger set $p^U\mathbf{Z}_p$ does not add any elements for if $\mathrm{ord}_p(w) = W < 0$, then $\psi_1(w,y)$, and hence also $b-\psi_1(w,y)$, will have order $2W < 0 \le k$. Now, the set $S_{k,b}$ is a union of $p^k\mathbf{Z}_p \times p^k\mathbf{Z}_p$ cosets, since the truth or falsity of the statement "$b - \psi_1(w,y) \in p^k\mathbf{Z}_p$" only depends on the image of w, and y in the quotient ring $\mathbf{Z}_p/p^k\mathbf{Z}_p = \mathbf{Z}/p^k\mathbf{Z}$. Thus if

$$V(k,b) := \mathrm{Vol}(S_{k,b}) = \int_{\mathbf{Z}_p}\int_{\mathbf{Z}_p} \mathbb{1}_{\mathbf{Z}_p}(p^{-k}(b - \psi_1(w,y)))\,dw\,dy,$$

then for $k \ge 1$,

$$V(k,b) = p^{-2k}\#\{(w_1,y_1) \in (\mathbf{Z}/p^k\mathbf{Z})^2 : \psi_1(w_1,y_1) = b \mod p^k\}, \tag{32}$$

since each coset of $p^k\mathbf{Z}_p \times p^k\mathbf{Z}_p$ has volume p^{-2k}. Further,

$$\mathbf{I}_{+-++} = (1 - p^{-3s}) \sum_{U=-\infty}^{-1} p^{-U(-9s+4)} \; (V(-U,b) - p^{-1}V(-U-1,b)).$$

Proposition 33 *Let p be a prime such that $p \equiv 5 \pmod 6$. Then for any positive integer k $\#\{(w_1,y_1) \in (\mathbf{Z}/p^k\mathbf{Z})^2 : \psi_1(w,y) = b\} = (p+1)p^{k-1}$.*

Proof.

Since $p \equiv 5 \pmod 6$, the finite field $\mathbf{Z}/p\mathbf{Z}$ contains no nontrivial cube roots of 1. so the polynomial x^2+x+1 is irreducible over $\mathbf{Z}/p\mathbf{Z}$ and a zero α of it generates the unique quadratic extension $\mathbf{F}_{p^2}$. Note that if α is one of the zeros of x^2+x+1, then the other one is α^p, which is also α^2, because $\alpha^3 = 1$ and $p \equiv 2 \mod 3$. Each element of $\mathbf{F}_{p^2}$ has the form $c + d\alpha$ for $c,d \in \mathbf{Z}/p\mathbf{Z}$, and the **norm**

$$N(c+d\alpha) = (c+d\alpha)(c+d\alpha^p) = (c+d\alpha)^{p+1} = c^2 - cd + d^2$$

maps $\mathbf{F}_{p^2}$ to $(\mathbf{Z}/p\mathbf{Z})$. For $y,w \in \mathbf{Z}/p\mathbf{Z}$, we can now recognize $\psi_1(y,w)$ as the norm of $y + w - w\alpha$. So, when $k = 1$ we are counting the number of elements of $\mathbf{F}_{p^2}$ of norm b. Since $\mathbf{F}_{p^2}^\times$ is a cyclic group of order p^2-1, whose unique subgroup of order $p-1$ is $(\mathbf{Z}/p\mathbf{Z})^\times$, and since $N(\xi) = \xi^{p+1}$, it follows that each element of $(\mathbf{Z}/p\mathbf{Z})^\times$, is the norm of precisely $p+1$ elements of $\mathbf{F}_{p^2}^\times$. This completes the case $k = 1$.

We now proceed by induction. Note that

$$\psi_1(w_1 + w_2p^k, y_1 + y_2p^k) \equiv \psi_1(w_1,w_2) + p^k((2w_1+3y_1)w_2 + (3w_1+6y_1)y_2) \mod p^{k+1}.$$

Also, if $\psi_1(w_1,y_1) \equiv b \ne 0 \mod p^k$ with $k \ge 1$, then $(w_1,y_1) \ne 0 \mod p$. But then $(2w_1+3y_1, 3w_1+6y_1) \ne 0 \mod p$, since $\left[\begin{smallmatrix}2 & 3\\ 3 & 6\end{smallmatrix}\right]$ is nonsingular $\mod p$. But then

$$(w_2,y_2) \mapsto (2w_1+3y_1)w_2 + (3w_1+6y_1)y_2$$

is a nontrivial linear map $\mathbf{Z}/p\mathbf{Z}^2 \to \mathbf{Z}/p\mathbf{Z}$, so it is surjective and each of its fibers has p elements. It follows that the number of solutions to $\psi_1(w, y) = b \mod p^{k+1}$ is precisely p times the number of solutions mod k. This completes the proof. □

Combining proposition 33 with equation (32), and noting that when $k = 0$, the set $S_{k,b}$ is clearly all of $\mathbf{Z}_p^2$, which has volume one, we obtain.

$$V(k, b) = \begin{cases} 1, & k = 0, \\ (1 + p^{-1})p^{-k}, & k \geq 1. \end{cases}$$

Hence, $V(k, b) - p^{-1}V(k-1, b)$ is equal to

$$\begin{cases} (1 + p^{-1})p^{-1} - p^{-1}(1) = p^{-1} + p^{-2} - p^{-1} = p^{-2}, & k = 1, \\ (1 + p^{-1})p^{-k} - p^{-1}(1 + p^{-1})p^{-k+1} = (1 + p^{-1})(p^{-k} - p^{-k+1-1}) = 0, & k \geq 2. \end{cases}$$

Going back to the integral, we now know $V(-U, b) - p^{-1}V(-U-1, b) = p^{-2}$ if $U = -1$, and zero otherwise.

Therefore,

$$\mathbf{I}_{+-++} = (1 - p^{-3s})p^{-9s+4}p^{-2} = (1 - p^{-3s})p^{-9s+2}.$$

Case 6 (I_{+-+-})

$$\mathbf{I}_{+-+-} = \int_{\mathbf{Z}_p}\int_{\mathbf{Z}_p}\int_{\mathbf{Q}_p - \mathbf{Z}_p} |y|_p^{-9s+3}|u|_p^{-9s+4}\psi_p(-3uy(y + uz) - u^3z^2)\int_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x))\psi_p(xy^3)\, dx\, du\, dy\, dz.$$

Notice that the integral with respect to x is identical to the integral with respect to x in Case 2 (I_{+++-}), and we've proven it vanishes. Therefore the integral vanishes.

Case 7 (I_{+--+})

$$\mathbf{I}_{+--+} = \int_{\mathbf{Z}_p}\int_{\mathbf{Q}_p - \mathbf{Z}_p}\int_{\mathbf{Q}_p - \mathbf{Z}_p} |u|_p^{-9s+4}|z|_p^{-6s+2}\psi_p(-u^3z^2 - y^3z^2 - 3u^2yz^2 - 3uy^2z^2)\int_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x))\psi_p(xz)\, dx\, du\, dy\, dz.$$

Notice that the integral with respect to x is identical to the integral with respect to x in Case 3 (I_{++-+}), and we've proven it vanishes. Therefore the integral vanishes.

Case 8 (I_{+---})

$$\mathbf{I}_{+---} = \int_{\mathbf{Q}_p - \mathbf{Z}_p}\int_{\mathbf{Q}_p - \mathbf{Z}_p}\int_{\mathbf{Q}_p - \mathbf{Z}_p} |u|_p^{-9s+4}|z|_p^{-6s+2}|y|_p^{-3s+1}\psi_p(-u^3z^2 - y^3z^2 - 3u^2yz^2 - 3uy^2z^2)$$

$$\int_{\mathbf{Q}_p} f^\circ_{s,p}(n^-(-x))\psi_p(xy^3z)\, dx\, du\, dy\, dz.$$

Notice that the integral with respect to x is identical to the integral with respect to x in Case 3 (I_{++--}), and we've proven it vanishes. Therefore the integral vanishes.

Case 9 (I_{-+++})

$$\mathbf{I}_{-+++} = \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{\mathbf{Z}_p} |v|_p^{-3s+1} \psi_p(cv - u^3 v + buv) \int_{\mathbf{Q}_p} f_{s,p}^{\circ}(n^-(-x)) \psi_p(xv^{-1})\, dx\, du\, dv.$$

Notice that since $|v|_p > 1$, then $\mathrm{ord}_p\, v < 0$. Considering v^{-1}, notice $|v^{-1}|_p = p^{\mathrm{ord}_p v} < 1$. So this implies that $v^{-1} \in \mathbf{Z}_p$. By Lemma 27,

$$\begin{aligned}
\mathbf{I}_{-+++} &= \left(\frac{1-p^{-3s}}{1-p^{-3s+1}}\right) \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{\mathbf{Z}_p} |v|_p^{-3s+1} (1 - |v^{-1}|_p^{3s-1} p^{-3s+1}) \psi_p(cv - u^3 v + buv)\, du\, dv \\
&= \left(\frac{1-p^{-3s}}{1-p^{-3s+1}}\right) \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{\mathbf{Z}_p} (|v|_p^{1-3s} - |v|_p^{2-6s} p^{-3s+1}) \psi_p(cv - u^3 v + buv)\, du\, dv. \\
&= \frac{1-p^{-3s}}{1-p^{-3s+1}} [H(1-3s) - p^{1-3s} H(2-6s)],
\end{aligned}$$

where

$$H(\lambda) = \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{\mathbf{Z}_p} |v|_p^{\lambda} \psi_p(cv - u^3 v + buv)\, du\, dv.$$

Applying Corollary 26,

$$H(\lambda) = \int_{\mathbf{Z}_p} \sum_{V=-\infty}^{-1} p^{-V(\lambda+1)} \int_{\mathbf{Z}_p^{\times}} \psi_p(p^V \nu (c - u^3 + bu))\, d\nu\, du.$$

Applying Lemma 24,

$$H(\lambda) = \sum_{V=-\infty}^{-1} p^{-V(\lambda+1)} \int_{\mathbf{Z}_p} \mathbb{1}_{\mathbf{Z}_p}(p^V(u^3 - bu - c)) - p^{-1} \mathbb{1}_{\mathbf{Z}_p}(p^{V+1}(u^3 - bu - c))\, du.$$

For a nonpositive integer V, let

$$h(V) = \int_{\mathbf{Z}_p} \mathbb{1}_{\mathbf{Z}_p}(p^V(u^3 - bu - c))\, du = \mathrm{Vol}(\{u \in \mathbf{Z}_p : |u^3 - bu - c|_p \leq p^V\}).$$

Then,

$$H(\lambda) = \sum_{V=-\infty}^{-1} p^{-V(\lambda+1)} \, (h(V) - p^{-1} h(V+1)).$$

By Lemma 21,

$$h(V) = \begin{cases} \mathrm{Vol}(\mathbf{Z}_p) = 1, & V = 0, \\ N(b,c)p^V, & V < 0, \end{cases}$$

where $N(b,c) \in \{0,1,3\}$ is the number of zeros of $g(u) = -u^3 + bu + c \bmod p$. In particular, $N(b,c) = 0$ when g is irreducible. Thus,

$$h(V) - p^{-1}h(V+1) = \begin{cases} N(b,c)p^{-1} - p^{-1}, & V = -1, \\ 0, & V < -1, \end{cases}$$

and hence

$$\begin{aligned} H(\lambda) &= p^{\lambda+1}(N(b,c)-1)p^{-1} \\ &= p^{\lambda}(N(b,c)-1). \end{aligned}$$

Therefore,

$$\mathbf{I}_{-+++} = \frac{1-p^{-3s}}{1-p^{-3s+1}}[p^{-3s+1}(N(b,c)-1) - p^{-3s+1}p^{-6s+2}(N(b,c)-1)]$$

$$= (1-p^{-3s})(N(b,c)-1)(\frac{1-p^{-6s+2}}{1-p^{-3s+1}})p^{-3s+1} = (1-p^{-3s})(N(b,c)-1)(1+p^{-3s+1})p^{-3s+1}$$

$$= (1-p^{-3s})(N(b,c)-1)(p^{-3s+1}+p^{-6s+2}).$$

In particular, when g is irreducible,

$$I_{-+++} = -p^{-3s+1}(1-p^{-3s})(1+p^{-3s+1}).$$

Case 10 (I_{-++-})

$$\mathbf{I}_{-++-} = \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Q}_p - \mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} |v|_p^{-3s+1}|y|_p^{-9s+3}\psi_p(cv - u^3v - 3uy + buv) \int\limits_{\mathbf{Q}_p} f^{\circ}_{s,p}(n^-(-x))\psi_p(xv^{-1}y^3)\, dx\, du\, dv\, dy.$$

If $v^{-1}y^3 \notin \mathbf{Z}_p$ then the x integral vanishes. So Lemma 27, yields a new integral where the condition $|y^3|_p \leq |v|_p$ must be incorporated into the domain of integration:

$$\mathbf{I}_{-++-} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Z}_p} \iint\limits_{|v|_p \geq |y^3|_p > 1} |v|_p^{-3s+1}|y|_p^{-9s+3}\psi_p(cv + buv - u^3v - 3uy)(1 - |v^{-1}y^3|_p^{3s-1}p^{-3s+1})\, dv\, dy\, du = \frac{1-p^{-3s}}{1-p^{-3s+1}}(H(1-3s, 3-9s) - p^{1-3s}H(2-6s, 0)),$$

where

$$H(\lambda,\mu) = \int\limits_{\mathbf{Z}_p} \iint\limits_{|v|_p \geq |y^3|_p > 1} |y|_p^{\mu}|v|_p^{\lambda}\psi_p(-3uy + (c + bu - u^3)v)\, dv\, dy\, du.$$

Applying Corollary 26 in both y and v,

$$H(\lambda,\mu) = \int\limits_{\mathbf{Z}_p} \sum_{Y=-\infty}^{-1} \sum_{V=-\infty}^{3Y} p^{Y(\mu+1)+V(\lambda+1)} \int\limits_{\mathbf{Z}_p^{\times}} \psi_p(3up^Y\gamma)\, d\gamma \int\limits_{\mathbf{Z}_p^{\times}} \psi_p((c+bu-u^3)p^V\nu)\, d\nu\, du.$$

Applying Lemma 24

$$H(\lambda,\mu) = \sum_{Y=-\infty}^{-1} \sum_{V=-\infty}^{3Y} p^{Y(\mu+1)+V(\lambda+1)} \int_{\mathbf{Z}_p} (\mathbb{1}_{\mathbf{Z}_p}(3up^Y) - p^{-1}\mathbb{1}_{\mathbf{Z}_p}(3up^{Y+1})$$

$$(\mathbb{1}_{\mathbf{Z}_p}((c+bu-u^3)p^V) - p^{-1}\mathbb{1}_{\mathbf{Z}_p}((c+bu-u^3)p^{V+1})\, du.$$

We now make use of the assumption that $g(u)$ is irreducible $\mod p$. It follows from this assumption that $g(u) \in \mathbf{Z}_p^\times$ for all $u \in \mathbf{Z}_p$. Also, it follows that $\mathbb{1}_{\mathbf{Z}_p}(g(u)p^V) = \mathbb{1}_{\mathbf{Z}_p}(g(u)p^{v+1}) = 0$ for all $V < 3Y \leq -3$.

Therefore $H(\lambda,\mu) = 0$, so the integral vanishes.

Case 11 (I_{-+-+})

$$\mathbf{I}_{-+-+} = \int_{\mathbf{Q}_p-\mathbf{Z}_p} \int_{\mathbf{Z}_p} \int_{\mathbf{Q}_p-\mathbf{Z}_p} \int_{\mathbf{Z}_p} |v|_p^{-3s+1}|z|_p^{-6s+2}\psi_p(z+cv-u^3v+buv-3uyz-v^{-1}y^3z^2)$$

$$\int_{\mathbf{Q}_p} f_{s,p}^\circ(n^-(-x))\psi_p(v^{-1}xz)\, dx\, du\, dv\, dy\, dz.$$

By Lemma 27,

$$\mathbf{I}_{-+-+} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \iint_{|v|_p \geq |z|_p > 1} \int_{\mathbf{Z}_p} \int_{\mathbf{Z}_p} |v|_p^{-3s+1}|z|_p^{-6s+2}(1-|v^{-1}z|_p^{3s-1}p^{-3s+1})$$

$$\psi_p(z+cv+buv-u^3v-3uyz-v^{-1}y^3z^2)\, du\, dy\, dv\, dz.$$

Let $z = rv$. Then by Lemma 24, $dz = |v|_p dr$. So

$$\mathbf{I}_{-+-+} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \iint_{|v^{-1}|_p < |r|_p \leq 1} \int_{\mathbf{Z}_p} \int_{\mathbf{Z}_p} |v|_p^{-9s+4}|r|_p^{-6s+2}(1-|r|_p^{3s-1}p^{-3s+1})$$

$$\psi_p(v(r+c+bu-u^3-3uyr-y^3r^2))\, du\, dy\, dv\, dr.$$

Applying Corollary 26,

$$\mathbf{I}_{-+-+} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int_{\mathbf{Z}_p} \int_{\mathbf{Z}_p} \int_{\mathbf{Z}_p} \sum_{V=-\infty}^{-\mathrm{ord}(r)-1} |r|_p^{-6s+2} p^{-V(-9s+5)}(1-|r|_p^{3s-1}p^{-3s+1})$$

$$\int_{\mathbf{Z}_p^\times} \psi_p(\nu p^V(c+bu-u^3+r-3uyr-y^3r^2))\, d\nu\, du\, dy\, dr.$$

Applying Lemma 24,

$$\mathbf{I}_{-+-+} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int_{\mathbf{Z}_p}\int_{\mathbf{Z}_p}\int_{\mathbf{Z}_p} \sum_{V=-\infty}^{-\mathrm{ord}(r)-1} |r|_p^{-6s+2} p^{-V(-9s+5)} (1-|r|_p^{3s-1}p^{-3s+1})$$

$$\left(\mathbb{1}_{\mathbf{Z}_p}(p^V(g(u)-h(u,y,r))) - p^{-1}\mathbb{1}_{\mathbf{Z}_p}(p^{V+1}(g(u)-h(u,y,r)))\right) du\, dy\, dr,$$

where $g(u) = -u^3+bu+c$ and $h(u,y,r) = 3uyr+y^3r^2-r$. There are two possibilities: either $r \in \mathbf{Z}_p^\times$ or not.

Consider first $r \notin \mathbf{Z}_p^\times$. Then $r \in \mathbf{Z}_p - p\mathbf{Z}_p$. Since $u, y \in \mathbf{Z}_p$ then $h(u,y,r) \in p\mathbf{Z}_p$. However since $g(u) \in \mathbf{Z}_p^\times$ then $g(u)-h(u,y,r) \in \mathbf{Z}_p^\times$. Therefore $\mathbb{1}_{\mathbf{Z}_p}(p^{-k}(g(u)-h(u,y,r))) = 0$, for all $k > 0$.

Now consider $r \in \mathbf{Z}_p^\times$. Define

$$N(V) = \#\{(r,y,u) \in (\mathbf{Z}/p^{-V}\mathbf{Z})^\times \times (\mathbf{Z}/p^{-V}\mathbf{Z}) \times (\mathbf{Z}/p^{-V}\mathbf{Z}) \mid g(u)-h(r,y,u) \equiv 0 \mod p^{-V}\},$$

$$H(V) = \int_{\mathbf{Z}_p}\int_{\mathbf{Z}_p}\int_{\mathbf{Z}_p^\times} \mathbb{1}_{\mathbf{Z}_p}(p^V(g(u)-h(u,y,r)))\, dr\, du\, dy$$

$$= \mathrm{Vol}\{(r,y,u) \in \mathbf{Z}_p^\times \times \mathbf{Z}_p \times \mathbf{Z}_p | p^{-V}(g(u)-h(r,y,u)) \in \mathbf{Z}_p\}.$$

Then, $H(V) = p^{3V}N(V)$, and

$$\mathbf{I}_{-+-+} = (1-p^{-3s}) \sum_{V=-\infty}^{-1} p^{-V(-9s+5)}(H(V)-p^{-1}H(V+1)).$$

Conjecture 34 *For all primes $p \equiv 2 \mod 3$, $N(-1) = p^2-1$ (for all b, c in $\mathbf{Z}$ such that g is irreducible mod p).*

This restates conjecture 2 from the introduction, and is proved by Scharaschkin in the appendix.

Corollary 35 *If $p \equiv 2 \mod 3$, k an integer, $k \leq 0$, then*

$$H(k) = \mathrm{Vol}\{(r,y,u) \in \mathbf{Z}_p^\times \times \mathbf{Z}_p \times \mathbf{Z}_p \mid p^k(g(u)-h(r,y,u))) \in \mathbf{Z}_p\} = \begin{cases} \frac{p-1}{p}, & \text{if } k = 0, \\ \frac{p^2-1}{p^3}(p^{k+1}), & \text{if } k \leq -1. \end{cases}$$

Proof. Let us show first that when $k = 0$, $H(k) = \frac{p-1}{p}$. Notice that for all p, the volume of the set $\mathbf{Z}_p$ is 1 and the volume of the set $\mathbf{Z}_p^\times$ is simply $\frac{p-1}{p}$. Then the volume of the Cartesian product $\mathbf{Z}_p^\times \times \mathbf{Z}_p \times \mathbf{Z}_p$ is just $(\frac{p-1}{p})(1)(1) = \frac{p-1}{p}$. Now we must show the case where $k \leq -1$. Notice that by conjecture 34, $H(k) = p^{3k}N(k)$ implies $H(-1) = p^{3(-1)}(p^2-1) = \frac{p^2-1}{p^3} = (\frac{p^2-1}{p^3})(p^{-1+1})$. So the base case where $k = -1$ is satisfied. Assume the statement is true for all $k \in \{-1, -2, ..., k'\}$, i.e. $H(k) = p^{3k}N(k) = (\frac{p^2-1}{p^3})(p^{k+1})$.

Then the next case by definition is, $H(k'-1) = p^{3(k'-1)}N(k'-1)$. By Corollary 31, $N(k-1) = p^2 N(k)$, for all $k \leq -1$. Therefore,

$$\begin{aligned} H(k'-1) &= p^{3(k'-1)}(p^2)N(k') = p^{3k'}p^{-3}p^2N(k') = p^{-1}(p^{3k'}N(k')) \\ &= p^{-1}(\frac{p^2-1}{p^3})(p^{k'+1}) = (\frac{p^2-1}{p^3})(p^{(k'-1)+1}). \end{aligned}$$

Hence, case $k = k'-1$ is also satisfied. By the Principle of Strong Mathematical Induction, for all $k \leq -1$, $H(k) = (\frac{p^2-1}{p^3})(p^{k+1})$. □

Therefore assuming $p \equiv 2 \mod 3$, we can apply Corollary 35.

$$H(V) - p^{-1}H(V+1) = \begin{cases} (\frac{p^2-1}{p^3}) - p^{-1}\frac{p-1}{p} = \frac{p-1}{p^3}, & \text{if } V=-1, \\ (\frac{p^2-1}{p^3})(p^{V+1}) - p^{-1}(\frac{p^2-1}{p^3})(p^{V+2})) = 0, & \text{if } V < -1. \end{cases}$$

Therefore,

$$\mathbf{I}_{-+-+} = (1-p^{-3s})p^{-9s+5}(\frac{p-1}{p^3}) = (1-p^{-3s})(1-p^{-1})p^{-9s+3} = (1-p^{-3s})(p^{-9s+3}-p^{-9s+2}).$$

Before moving on to the next case, we remark that, even without conjecture 34 we can say that $H(k) = p^{-1}H(k+1)$ for $k < -1$, and hence that

$$H(V) - p^{-1}H(V+1) = \begin{cases} \frac{N(-1)-p^2+p}{p^3}, & V=-1 \\ 0, & V < -1, \end{cases}$$

and

$$\mathbf{I}_{-+-+} = (1-p)^{-3s}p^{-9s+3}(1-p+\frac{N(-1)}{p}).$$

Thus, conjecture 34 can actually be deduced from Xiong's result, by way of our results on the other fifteen sub-integrals.

Case 12 (I_{-+--})

$$\mathbf{I}_{-+--} = \int_{\mathbf{Q}_p-\mathbf{Z}_p}\int_{\mathbf{Q}_p-\mathbf{Z}_p}\int_{\mathbf{Q}_p-\mathbf{Z}_p}\int_{\mathbf{Z}_p} \psi_p(z+cv-u^3v+buv-3uyz-v^{-1}y^3z^2)$$
$$|v|_p^{-3s+1}|z|_p^{-6s+2}|y|_p^{-9s+3}\int_{\mathbf{Q}_p} f^{\circ}_{s,p}(n^-(-x))\psi_p(v^{-1}xy^3z)\,dx\,du\,dz\,dv\,dy.$$

By Lemma 27, if $v^{-1}y^3z \notin \mathbf{Z}_p$ then the x integral vanishes. Hence we obtain a new integral where the domain of integration includes the constraint $v^{-1}y^3z \in \mathbf{Z}_p$.

$$\mathbf{I}_{-+--} = \frac{1-p^{-3s}}{1-p^{-3s+1}}\int_{\mathbf{Q}_p-\mathbf{Z}_p}\int_{\mathbf{Q}_p-y^3\mathbf{Z}_p}\int_{y^{-3}v\mathbf{Z}_p-\mathbf{Z}_p}\int_{\mathbf{Z}_p}|v|_p^{-3s+1}|z|_p^{-6s+2}|y|_p^{-9s+3}$$

$$\psi_p(z + cv - u^3v + buv - 3uyz - v^{-1}y^3z^2 + v^{-1}xy^3z)(1 - |\frac{y^3z}{v}|_p^{3s-1}p^{-3s+1})\, du\, dz\, dv\, dy.$$

Let $z = rv$, then $dz = |v|_p dr$. This implies that $|rv|_p > 1 \iff |r|_p > |v|_p^{-1}$, $|y^3r|_p \leq 1 \iff |r|_p \leq |y|_p^{-3}$. Therefore $|y|_p^3 < |v|_p$. Hence,

$$\mathbf{I}_{-+--} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{|v|_p>|y|_p^3} \int\limits_{|v|_p^{-1}<|r|_p\leq|y|_p^{-3}} \int\limits_{\mathbf{Z}_p} |v|_p^{4-9s}|r|_p^{2-6s}|y|_p^{3-9s}(1-|y^3r|_p^{3s-1}p^{-3s+1})$$

$$\psi_p(v(r + c - u^3 + bu - 3uyr - y^3r^2))\, du\, dr\, dv\, dy.$$

Notice that $|y^3r^2|_p \leq |r|_p \leq |y|_p^{-3} \leq p^{-3}$, which implies that $|yr|_p \leq |y|_p|y|_p^{-3} \leq |y|_p^{-2} \leq p^{-2}$. Let $v = p^V\nu$ and $y = p^Y\gamma$, with $\nu, \gamma \in \mathbf{Z}_p^\times$. By Lemma 22, $dv = p^{-V}d\nu$ and $dy = p^{-Y}d\gamma$. Applying Corollary 26,

$$\mathbf{I}_{-+--} = \sum_{Y=-\infty}^{-1} \sum_{V=-\infty}^{3Y-1} p^{-V(5-9s)-Y(4-9s)} \int\limits_{p^V<|r|_p\leq p^{3Y}} |r|_p^{2-6s}$$

$$\int\limits_{\mathbf{Z}_p}\int\limits_{\mathbf{Z}_p^\times}\int\limits_{\mathbf{Z}_p^\times} \psi_p(p^V\nu(r + c - u^3 + bu - 3up^Y\gamma r - (p^Y\gamma)^3r^2))\, d\nu\, d\gamma\, du\, dr.$$

By Lemma 24,

$$\int\limits_{\mathbf{Z}_p^\times} \psi_p(p^V\nu(r + c - u^3 + bu - 3up^Y\gamma r - (p^Y\gamma)^3r^2))\, d\nu$$

$$= \mathbb{1}_{\mathbf{Z}_p}(p^V\nu(r + c - u^3 + bu - 3up^Y\gamma r - (p^Y\gamma)^3r^2)) - p^{-1}\mathbb{1}_{\mathbf{Z}_p}(p^{V+1}\nu(r + c - u^3 + bu - 3up^Y\gamma r - (p^Y\gamma)^3r^2)).$$

Assuming that $u^3 - bu - c$ is irreducible mod p ($b, c \in \mathbf{Z}_p^\times$) and $p > 3$ makes $p^V\nu(r + c - u^3 + bu - 3up^Y\gamma r - (p^Y\gamma)^3r^2) \notin p^{-1}\mathbf{Z}_p$. Therefore $\mathbb{1}_{\mathbf{Z}_p}(p^V\nu(r + c - u^3 + bu - 3up^Y\gamma r - (p^Y\gamma)^3r^2)) = 0$ and the integral vanishes.

Case 13 (I_{--++})

$$\mathbf{I}_{--++} = \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p}\int\limits_{\mathbf{Q}_p-\mathbf{Z}_p}\int\limits_{\mathbf{Z}_p}\int\limits_{\mathbf{Z}_p} \psi_p(vg(u) - (2uz + 3y)u^2 - \frac{(u^2z^2 + 3y^2 + 3uyz)u}{v})$$

$$|v|_p^{-3s+1}|u|_p^{-9s+4} \int\limits_{\mathbf{Q}_p} f_{s,p}^\circ(n^-(-x))\psi_p(v^{-1}x)\, dx\, dz\, dy\, du\, dv,$$

where $g(u) = c + bu - u^3$.

Notice that $v \notin \mathbf{Z}_p$ which implies that $ord_p(v) < 0$, and hence that $v^{-1} \in \mathbf{Z}_p$. By Lemma 27,

$$\mathbf{I}_{--++} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} |v|_p^{-3s+1} |u|_p^{-9s+4} (1 - |v^{-1}|_p^{3s-1} p^{-3s+1})$$
$$\psi_p(vg(u) - (2uz+3y)u^2 - \frac{(u^2z^2+3y^2+3uyz)u}{v})\, dz\, dy\, du\, dv.$$

Let $y = vy_1$, $z = vz_1$. By Lemma 22, $dy = |v|_p\, dy_1$ and $dz = |v|_p\, dz_1$.

$$\mathbf{I}_{--++} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{v^{-1}\mathbf{Z}_p} \int\limits_{v^{-1}\mathbf{Z}_p} |v|_p^{-3s+3} |u|_p^{-9s+4} (1 - |v^{-1}|_p^{3s-1} p^{-3s+1})$$
$$\psi_p(v(g(u) - (2uz_1+3y_1)u^2 - ((uz_1)^2 + 3y_1^2 + 3uy_1z_1)u))\, dy_1\, dz_1\, du\, dv.$$

Lemma 36 *For all u, y_1, z_1 in the domain of integration, the order of $g(u) - (2uz_1 + 3y_1)u^2 - ((uz_1)^2 + 3y_1^2 + 3uy_1z_1)u$ is equal to $3\,\mathrm{ord}_p(u)$. In particular, it is at most -3.*

Proof. Since $ord_p(u) < 0$ it follows from the strong triangle inequality that $\mathrm{ord}_p(g(u)) = \mathrm{ord}_p(u^3) = 3\,\mathrm{ord}_p(u)$. We claim that this is the minimal order among the three summands.

First, notice that since $y_1, z_1 \in v^{-1}\mathbf{Z}_p$, it is true that both $\mathrm{ord}_p(z_1)$ and $\mathrm{ord}_p(y_1)$ are positive, so $\mathrm{ord}_p(u)$ is strictly smaller to them. Using this, it is sufficient to show the order of the first summand is smaller than the other two. We will only show the case of the second summand, since the third follows analogously. Since 2 and 3 have zero order, then $\mathrm{ord}_p(2(uz_1)u^2) = \mathrm{ord}_p(u^3z_1) = 3\,\mathrm{ord}_p(u) + \mathrm{ord}_p(z_1) > 3\,\mathrm{ord}_p(u)$. Similarly, $\mathrm{ord}_p(3y_1u^2) = \mathrm{ord}_p(y_1u^2) = \mathrm{ord}_p(y_1) + 2\,\mathrm{ord}_p(u) \geq 2\,\mathrm{ord}_p(u) > 3\,\mathrm{ord}_p(u)$ (again because the $\mathrm{ord}_p(u)$ is negative). Then $\mathrm{ord}_p((2uz_1 + 3y_1)u^2) = \mathrm{ord}_p(u^3z_1 + y_1u^2) = \mathrm{ord}_p(u^3z_1) + \mathrm{ord}_p(y_1u^2) > 3\,\mathrm{ord}_p(u)$. Therefore, the order of the first summand is smaller than the orders of the other two, and that means $3\,\mathrm{ord}_p(u)$ is the order of the sum. □

In view of Lemma 36, it follows from Corollary 26 and Lemma 24 that I_{--++} vanishes.

Case 14 (I_{--+-})

$$\mathbf{I}_{--+-} = \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} |v|_p^{-3s+1} |y|_p^{-9s+3} |u|_p^{-9s+4}$$

$$\psi_p(vg(u) - (2uz+3y)u^2 - \frac{(u^2z^2+3y^2+3uyz)u}{v}) \int\limits_{\mathbf{Z}_p} f^{\circ}_{s,p}(n^-(-x))\psi_p(v^{-1}xy^3)\, dx\, dz\, dy\, du\, dv.$$

where $g(u) = c + bu - u^3$.

If $v^{-1}y^3 \notin \mathbf{Z}_p$ the x integral vanishes. Note that $v^{-1}y^3 \in \mathbf{Z}_p$ is equivalent to $|y|_p^3 \leq |v|_p$. By Lemma 27,

$$\mathbf{I}_{--+-} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \iint\limits_{|v|_p \geq |y|_p^3 > 1} \int\limits_{\mathbf{Z}_p} |v|_p^{-3s+1} |y|_p^{-9s+3} |u|_p^{-9s+4}$$

$$\psi_p(vg(u) - (2uz+3y)u^2 - \frac{(u^2z^2+3y^2+3uyz)u}{v})(1-|v^{-1}y^3|_p^{3s-1}p^{-3s+1})\, dz\, dv\, dy\, du.$$

Let $y = vy_1$, $z = vz_1$. Then $z_1 \in v^{-1}\mathbf{Z}_p$, and $|v|_p^{-2} \geq |y_1|_p^3 > |v|_p^{-3}$. Also, by Lemma 22, $dy = |v|_p\, dy_1$ and $dz = |v|_p\, dz_1$. Hence,

$$\mathbf{I}_{--+-} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-p\mathbf{Z}_p} \int\limits_{|v|_p^{-2} \geq |y_1|_p^3 > |v|_p^{-3}} \int\limits_{v^{-1}\mathbf{Z}_p} |v|_p^{-3s+3} |y|_p^{-9s+4} |u|_p^{-9s+4} (1-|v^{-1}y^3|_p^{3s-1}p^{-3s+1})$$

$$\psi_p(v(g(u) - (2uz_1+3y_1)u^2 - ((uz_1)^2+3y_1^2+3uy_1z_1)u))\, dz_1\, dy_1\, dv\, du.$$

Notice that, inside of ψ_p, we have the same function as in I_{--++}. Let's check if Lemma 36 is still true. First, note that each of the variables z_1, y_1 ranges over a subset of $p\mathbf{Z}_p$ which depends on v, while u ranges over $\mathbf{Q}_p - \mathbf{Z}_p$. Hence, $\operatorname{ord}_p(z_1) \geq 1 > \operatorname{ord}_p(u)$. Then $\operatorname{ord}_p(2(uz_1)u^2) = \operatorname{ord}_p(u^3z_1) = 3\operatorname{ord}_p(u) + \operatorname{ord}_p(z_1) > 3\operatorname{ord}_p(u)$ and $\operatorname{ord}_p(3y_1u^2) = \operatorname{ord}_p(u^2y_1) = 2\operatorname{ord}_p(u) + \operatorname{ord}_p(y_1) > 2\operatorname{ord}_p(u) - 2/3\operatorname{ord}_p(v) > 2\operatorname{ord}_p(u) > 3\operatorname{ord}_p(u)$ (Since the order of both u, v is negative). So, $\operatorname{ord}_p((2uz_1+3y_1)u^2) \geq \min(\operatorname{ord}_p(u^3z_1), \operatorname{ord}_p(u^2y_1)) > 3\operatorname{ord}_p(u)$. An analogous argument can also be made for the third summand. Once again, the order of the first summand is smaller than the orders of the other two, so Lemma 36 holds.

In view of Lemma 36, it follows from Corollary 26 and Lemma 24 that I_{--+-} vanishes.

Case 15 (I_{---+})

$$\mathbf{I}_{---+} = \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} |v|_p^{-3s+1} |u|_p^{-9s+4} |z|_p^{-6s+2}$$

$$\psi_p(cv - u^3v - 2u^3z + buv - u^3v^{-1}z^2 - 3u^2yz - v^{-1}y^3z^2 - 3u^2v^{-1}yz^2 - 3uv^{-1}y^2z^2)$$

$$\int\limits_{\mathbf{Q}_p} f_{s,p}^{\circ}(n^-(-x))\psi_p(v^{-1}zx)\, dx\, dy\, du\, dv\, dz.$$

By Lemma 27, and the fact that $v^{-1}z \in \mathbf{Z}_p \iff z \in v\mathbf{Z}_p$,

$$\mathbf{I}_{---+} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{v\mathbf{Z}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Z}_p} |v|_p^{-3s+1} |u|_p^{-9s+4} |z|_p^{-6s+2}$$

$$\psi_p(cv - u^3v - 2u^3z + buv - u^3v^{-1}z^2 - 3u^2yz - v^{-1}y^3z^2 - 3u^2v^{-1}yz^2 - 3uv^{-1}y^2z^2)(1 - |v^{-1}z|_p^{3s-1}p^{-3s+1})\, dy\, dz\, dv\, du.$$

Let $z = rv$. Then by Lemma 22, $dz = |v|_p dr$. Rearranging the terms inside ψ_p, we get the following:

$$\mathbf{I}_{---+} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int_{\mathbf{Q}_p - \mathbf{Z}_p} \iint_{1 \geq |r|_p > |v|_p^{-1}} \int_{\mathbf{Z}_p} (1 - |r|_p^{3s-1}p^{-3s+1})|v|_p^{-9s+4}|u|_p^{-9s+4}|r|_p^{-6s+2}$$

$$\psi_p(v(-u^3(r+1)^2 - u^2(3yr(r+1)) + u(b - 3y^2r^2) + (c - r^2y^3)))\, dy\, dr\, dv\, du.$$

Since y, r, b and c are all in $\mathbf{Z}_p$, it follows that

$$\text{ord}_p(-u^3(r+1)^2 - u^2(3yr(r+1)) + u(b-3y^2r^2) + (c - r^2y^3)) = \text{ord}_p(-u^3(r+1)^2) \leq -3,$$

whenever $\text{ord}_p(u(r+1)) < 0$. On the other hand, if $\text{ord}_p(u(r+1)) \geq 0$, then $\text{ord}_p(r+1) > 0$, and hence $\text{ord}_p(r) = 1$. The constraint $|r|_p > |v|_p^{-1}$ becomes $v \in \mathbf{Q}_p - \mathbf{Z}_p$ for all such r. We obtain

$$\mathbf{I}_{---+} = (1-p^{-3s}) \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{|r+1|_p \leq |u|_p^{-1}} \int_{\mathbf{Z}_p} |uv|_p^{-9s+4}$$

$$\psi_p(v(-u^3(r+1)^2 - u^2(3yr(r+1)) + u(b - 3y^2r^2) + (c - r^2y^3)))\, dy\, dr\, dv\, du.$$

Now let $y_1 = y/u$. Since $y \in \mathbf{Z}_p$, then $|y_1|_p \leq |u|_p^{-1}$. Then by Lemma 22, $dy = |u|_p dy_1$. Rearranging again the terms inside ψ_p, we get the following:

$$\mathbf{I}_{---+} = (1-p^{-3s}) \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{|r+1|_p \leq |u|_p^{-1}} \int_{|y_1|_p \leq |u|_p^{-1}} |v|_p^{-9s+4}|u|_p^{-9s+5}$$

$$\psi_p(v(c + bu - u^3(1 + r(3y_1+2) + r^2(y_1+1)^3)))\, dy_1\, dr\, dv\, du.$$

Let $v_1 = vu^3$. Since $v \in \mathbf{Q}_p - \mathbf{Z}_p$, then $|v_1|_p > |u|_p^3$. Then by Lemma 22, $dv = |u|_p^{-3}dv_1$. So,

$$\mathbf{I}_{---+} = (1-p^{-3s}) \int_{\mathbf{Q}_p - \mathbf{Z}_p} \int_{|v_1|_p > |u|_p^3} \int_{|r+1|_p \leq |u|_p^{-1}} \int_{|y_1|_p \leq |u|_p^{-1}} |v_1|_p^{-9s+4}|u|_p^{18s-10}$$

$$\psi_p(\frac{v_1}{u^3}(c+bu) - v_1(1 + r(3y_1+2) + r^2(y_1+1)^3))\, dy_1\, dr\, dv_1\, du.$$

Let $u_1 = u^{-1}$. By Lemma 22, $\frac{du}{|u|_p} = \frac{du_1}{|u_1|_p}$, so $du = |u_1|_p^2 du_1$. As u ranges over $\mathbf{Q}_p - \mathbf{Z}_p$, its inverse, u_1, ranges over $p\mathbf{Z}_p - \{0\}$. Since the measure of $\{0\}$ is 0, we obtain,

$$\mathbf{I}_{---+} = (1-p^{-3s}) \int\limits_{p\mathbf{Z}_p} \int\limits_{|v_1|_p>|u|_p^3} \int\limits_{|r+1|_p \le |u|_p^{-1}} \int\limits_{|y_1|_p \le |u|_p^{-1}} |v_1|_p^{-9s+4} |u_1|_p^{-18s+8}$$

$$\psi_p(v_1(u_1^3 c + u_1^2 b) - v_1(1 + r(3y_1+2) + r^2(y_1+1)^3))\, dy_1\, dr\, dv_1\, du_1$$

$$= (1-p^{-3s}) \sum_{U=1}^{\infty} \int\limits_{|u_1|_p = p^{-U}} \int\limits_{|v_1|_p > p^{3U}} \int\limits_{|r+1|_p \le p^{-U}} \int\limits_{|y_1|_p \le p^{-U}} |v_1 u_1^2|_p^{-9s+4}$$

$$\psi_p(v_1(u_1^3 c + u_1^2 b) - v_1(1 + r(3y_1+2) + r^2(y_1+1)^3))\, dy_1\, dr\, dv_1\, du_1.$$

Let $u_1 = p^U u_2, u_2 \in \mathbf{Z}_p^\times$. Then by Lemma 2, $du_1 = p^{-U} du_2$. Applying Corollary 26,

$$= (1-p^{-3s}) \sum_{U=1}^{\infty} p^{U(18s-9)} \int\limits_{\mathbf{Z}_p^\times} \psi_p(v_1(u_2^3 p^{3U} c + u_2^2 p^{2U} b))\, du_2$$

$$\int\limits_{|v_1|_p > p^{3U}} |v_1|_p^{-9s+4} \int\limits_{|r+1|_p \le p^{-U}} \int\limits_{|y_1|_p \le p^{-U}} \psi_p(-v_1(1 + r(3y_1+2) + r^2(y_1+1)^3))\, dy_1\, dr\, dv_1.$$

We will focus on the u_2 integral and show it vanishes. For $a, d \in \mathbf{Q}_p$, define $H(d)$ and $H_1(d,a)$ as the following:

$$H_1(d,a) = \int\limits_{\mathbf{Z}_p^\times} \psi_p(d(x^2 + ax^3))\, dx, \qquad H(d) = H_1(d,0) = \int\limits_{\mathbf{Z}_p^\times} \psi_p(dx^2)\, dx.$$

Lemma 37 *If $a \in p\mathbf{Z}_p$, then $H_1(d,a) = H(d)$, and if $\operatorname{ord}(d) < -1$, then $H(d) = 0$.*

This can be proven by fixing $x_0 \in \{1, ..., p-1\}$ and considering $\varphi_a = x^2 + ax^3$. Notice that $\varphi_a : \mathbf{Z}_p \to \mathbf{Z}_p$, for $a \in \mathbf{Z}_p$.

Lemma 38 *For $a \in p\mathbf{Z}_p$, the function φ_a is a bijection*

$$\{x \in (\mathbf{Z}/p^k\mathbf{Z})^\times | x \equiv x_0 \mod p\} \to \{y \in (\mathbf{Z}/p^k\mathbf{Z})^\times | y \equiv \varphi_a(x_0) \mod p\},$$

for any positive integer k, and hence a measure-preserving bijection $x_0 + p\mathbf{Z}_p \to x_0^2 + p\mathbf{Z}_p$, for each $x_0 \in \mathbf{Z}_p^\times$.

Proof. We will prove this statement by induction. If $k = 1$ then we have nothing to prove. Take $k \ge 1$ and write $x = x_1 + p^k x_2$. Then $\varphi_a(x) \equiv \varphi_a(x_1) + p^k(2x_1x_2) \mod p^{k+1}$. Since $p \ne 2$ and $x_1 \in (\mathbf{Z}/p\mathbf{Z})^\times$ the mapping $x_2 \mapsto 2x_1x_2$ is a bijection $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$. It follows that

$$x_1 + p^k x_2 \mapsto \varphi_a(x_1) + p^k(2x_1x_2)$$

is a bijection

$$\{x \in (\mathbf{Z}/p^{k+1}\mathbf{Z})^\times : x \equiv x_1 \mod p^k\} \to \{y \in (\mathbf{Z}/p^{k+1}\mathbf{Z})^\times : y \equiv \varphi_a(x_1) \mod p^k\}.$$

Thus our bijection at level k extends to a bijection at level $k+1$, completing the proof by induction. □

We can now prove Lemma 37.

Proof. [Proof of Lemma 37]

$$H_1(d,a) = \int_{\mathbf{Z}_p^\times} \psi_p(d\varphi_a(x))\,dx = \sum_{x_0=1}^{p-1} \int_{x_0+p\mathbf{Z}_p} \psi_p(d\varphi_a(x))\,dx = \sum_{x_0=1}^{p-1} \int_{\varphi_a(x_0)+p\mathbf{Z}_p} \psi_p(dy)\,dy, \text{ Corollary 38}$$

Notice that $\varphi_a(x_0) + p\mathbf{Z}_p = x_0^2 + pax_0^3 + p\mathbf{Z}_p = x_0^2 + p\mathbf{Z}_p$

$$H_1(d,a) = \sum_{x_0=1}^{p-1} \int_{x_0^2+p\mathbf{Z}_p} \psi_p(dy)\,dy = H_1(d,0) = H(d).$$

Moreover, for each x_0 we have

$$\int_{\varphi_a(x_0)+p\mathbf{Z}_p} \psi_p(dy)\,dy = p^{-1}\int_{\mathbf{Z}_p} \psi_p(d(\varphi_a(x_0)+py_1))\,dy_1 = p^{-1}\psi_p(d\varphi_a(x_0))\int_{\mathbf{Z}_p} \psi_p(dpy_1)\,dy_1,$$

by lemma 22. If $\mathrm{ord}_p(d) < -1$, then the last integral is zero by lemma 23. □

Coming back to the u_2 integral,

$$\int_{\mathbf{Z}_p^\times} \psi_p(v_1(u_2^3p^{3U}c + u_2^2p^{2U}b))\,du_2 = H_1(v_1p^2Ub, p^Ucb^{-1}), \text{ provided } b \neq 0.$$

We know $u > 0$, so p^Ucb^{-1} is always divisible by p. By Lemma 37, $H_1(v_1p^2Ub, p^Ucb^{-1}) = H(v_1p^{2U}b)$. Since $|v_1|_p > p^{3U}$ and $b \in \mathbf{Z}_p^\times$, we have $|v_1p^{2U}b|_p = |v_1p^{2U}|_p > p^U > 1$. Therefore $\mathrm{ord}_p(v_1p^{2U}b) < -1$, so $H(v_1p^{2U}b) = 0$ and the integral vanishes.

Note: Jiang-Rallis, showed that $\mathbf{I}_{---+}$ has a nonzero solution in the case $b = 0$.

Case 16 (I_{----})

$$\mathbf{I}_{----} = \int_{\mathbf{Q}_p-\mathbf{Z}_p}\int_{\mathbf{Q}_p-\mathbf{Z}_p}\int_{\mathbf{Q}_p-\mathbf{Z}_p}\int_{\mathbf{Q}_p-\mathbf{Z}_p} |v|_p^{-3s+1}|u|_p^{-9s+4}|z|_p^{-6s+2}|y|_p^{-9s+3}$$

$$\psi_p(vg(u) - (2u+3y)u^2z - \frac{(u+y)^3z^2}{v})$$

$$\int_{\mathbf{Q}_p} f_{s,p}^\circ(n^-(-x))\psi_p(v^{-1}xy^3z)\,dx\,du\,dv\,dy\,dz$$

where $g(u) = c + bu - u^3$.

If $v^{-1}y^3z \notin \mathbf{Z}_p$ the x integral vanishes. If not then z lies in $v^{-1}y^3\mathbf{Z}_p - \mathbf{Z}_p$. Notice that this is only nonempty if $3\operatorname{ord}_p(y) > \operatorname{ord}_p(v)$, i.e. $v \in \mathbf{Q}_p - y^3\mathbf{Z}_p$. By Lemma 27,

$$\mathbf{I}_{----} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-y^3\mathbf{Z}_p} \int\limits_{\frac{v}{y^3}\mathbf{Z}_p-\mathbf{Z}_p} |v|_p^{-3s+1}|u|_p^{-9s+4}|z|_p^{-6s+2}|y|_p^{-9s+3}(1-|v^{-1}y^3z|_p^{3s-1}p^{-3s+1})$$

$$\psi_p(vg(u) - (2u+3y)u^2z - \frac{(u+y)^3z^2}{v})\, dz\, dv\, dy\, du.$$

Let $z = vr$. By Lemma 22, $dz = |v|dr$, and

$$\mathbf{I}_{----} = \frac{1-p^{-3s}}{1-p^{-3s+1}} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-\mathbf{Z}_p} \int\limits_{\mathbf{Q}_p-y^3\mathbf{Z}_p} \int\limits_{y^{-3}\mathbf{Z}_p-v^{-1}\mathbf{Z}_p} |v|_p^{-9s+4}|u|_p^{-9s+4}|r|_p^{-6s+2}|y|_p^{-9s+3}(1-|y^3r|_p^{3s-1}p^{-3s+1})$$

$$\psi_p(v[g(u) - (2u+3y)u^2r - (u+y)^3r^2])\, dr\, dv\, dy\, du.$$

Lemma 39 *For all u, y, r in the domain of integration, the order of $g(u) - (2u+3y)u^2r - (u+y)^3r^2$ is equal to $3\operatorname{ord}_p(u)$. In particular, it is at most -3.*

Proof. Since $\operatorname{ord}_p(u) < 0$ it follows from the strong triangle inequality that $\operatorname{ord}_p(g(u)) = \operatorname{ord}_p(u^3) = 3\operatorname{ord}_p(u)$. We claim that this is the minimal order among the three summands.

First suppose that $\operatorname{ord}_p(u) \le \operatorname{ord}_p(y)$. Then $\operatorname{ord}_p(u^2(3u+3y))$ and $\operatorname{ord}_p(u+y)^3$ are at least $\operatorname{ord}_p(u^3)$. But $\operatorname{ord}_p(r) \ge \operatorname{ord}_p(y^{-3}) \ge 3$, so $\operatorname{ord}_p(g(u))$ is indeed strictly smaller than the other two, and hence the order to the sum.

Now suppose that $\operatorname{ord}_p(y) < \operatorname{ord}_p(u)$. Then $\operatorname{ord}_p(u+y) = \operatorname{ord}_p(2u+3y) = \operatorname{ord}_p(y)$. Then

$$\operatorname{ord}_p((2u+3y)u^2r) = \operatorname{ord}_p(yu^2r) > \operatorname{ord}_p(y^3r) \ge 0 > \operatorname{ord}_p(u^3),$$

and

$$\operatorname{ord}_p((u+y)^3r^2) = \operatorname{ord}_p(y^3r^2) \ge \operatorname{ord}_p(r) > 0 > \operatorname{ord}_p(u^3).$$

Once again, the order of the first summand is strictly smaller than the orders of the other two, and that means it is the order of the sum. □

In view of Lemma 39, it follows from corollary 26 and Lemma 24 that I_{----} vanishes.

5 Summary of Results

Now that we have the result of all 16 cases we can deduce the following propositions.

Proposition 40

$$I_{+++-} = I_{++-+} = I_{++--} = I_{+-+-} = I_{+--+} = I_{+---} = 0,$$

$$I_{--++} = I_{--+-} = I_{----} = 0. \textit{ (New Result)}$$

Proposition 41 *If g is irreducible mod p, $p > 3$, then $I_{-++-} = I_{-+--} = 0$.*

Proposition 42 *If g is irreducible mod p, $p \equiv 2 \mod 3$, then $I_{---+} = 0$. (New Result)*

Proposition 43 $I_+ = (1 - p^{-3s})(1 + p^{-9s+2})$.

Proof. We know that $I_+ = I_{++++} + I_{+-++} + I_{+++-} + I_{++-+} + I_{++--} + I_{+--+} + I_{+-+-} + I_{+---}$. By Proposition 40, $I_+ = I_{++++} + I_{+-++}$. Then,
$I_+ = (1 - p^{-3s}) + (1 - p^{-3s})p^{-9s+2} = (1 - p^{-3s})(1 + p^{-9s+2})$. □

Proposition 44 *If g is irreducible mod p, then*
$I_- = (1 - p^{-3s})(-p^{-3s+1} - p^{-6s+2} + p^{-9s+3} - p^{-9s+2})$. *(New result)*

Proof. We know that $I_- = I_{----} + I_{-+--} + I_{---+} + I_{--+-} + I_{--++} + I_{-++-} + I_{-+-+} + I_{-+++}$. By Proposition 40 and 42, $I_- = I_{-+++} + I_{-+-+}$. Assuming g is irreducible mod p makes $N(b, c) = 0$ in I_{-+++}. Therefore, $I_- = (1 - p^{-3s})(-p^{-3s+1} - p^{-6s+2}) + (1 - p^{-3s})(p^{-9s+3} - p^{-9s+2}) = (1 - p^{-3s})(-p^{-3s+1} - p^{-6s+2} + p^{-9s+3} - p^{-9s+2})$. □

Theorem 45 (Main Theorem) *If Conjecture 34 is valid in I_{-+-+}, then*

$$I_p^\sigma(s, f_{s,p}^\circ) = (1 - p^{-3s})(1 - p^{-3s+1})(1 - p^{-6s+2}).$$

Proof. $I_p^\sigma(s, f_{s,p}^\circ) = I_+ + I_- = (1-p^{-3s})(1+p^{-9s+2} - p^{-3s+1} - p^{-6s+2} + p^{-9s+3} - p^{-9s+2}) = (1 - p^{-3s})((1 - p^{-6s+2}) - p^{3s+1}(1 - p^{-6s+2})) = (1 - p^{-3s})(1 - p^{-3s+1})(1 - p^{-6s+2})$. □

6 Directions for Future Work

There are a number of natural directions for future work. One of them is to generalize the result to the context of an arbitrary non-Archimedean local field F of characteristic zero, which contains only one cube root of 1.

Another natural direction is to relax the assumption that all data is unramified. For example, we have assumed that b and c are in $\mathbf{Z}_p^\times$ because, for any $b, c \in \mathbf{Q}^\times$, the set of primes p such that b and c are not in $\mathbf{Z}_p^\times$ is finite. Nevertheless, if we hope to get the correct Euler factor at every place, we must handle the finite set of exceptional primes. This will require considering functions $f_{s,p} \neq f_{s,p}^\circ$.

As noted before, the local integral $I_v^\sigma(s, f_{s,v})$ of Jiang and Rallis was defined in the context of an arbitrary local field of characteristic zero. This includes the two Archimedean local fields, $\mathbf{R}$ and $\mathbf{C}$. As far as we know the Archimedean zeta integrals have not been considered. One would expect that they would be related to the Gamma factors which appear in the functional equations of the zeta functions obtained from the non-Archimedean contributions.

Finally, it is worth noting as Jiang and Rallis did, that the exceptional groups F_4 and E_8 have unipotent subgroups, analogous to our group N, but with field extensions of degree 4 (in the F_4 case) or 5 (in the E_8 case) playing the role that field extensions of degree 3 have played here. The quintic case is particularly tantalizing because this would be the first time an extension with a non-solvable Galois group could appear. It is also noteworthy that Xiong's approach is based on the "Exceptional Θ correspondence" of Magaard-Savin [11], and an embedding $G_2 \times PGL_3$ into the exceptional group E_6. It is reasonable to hope that it may extend to the F_4 case. The exceptional Θ correspondence also includes an embedding of $G_2 \times F_4$ into E_8 [11]. But it's not clear how to embed a product of the form $E_8 \times H$ into something even bigger in a similar way. With that being said, it must be noted that, if N' and N'' are the analogues of N in F_4 and E_8 respectively, then $\dim N' = 20$ and $\dim N'' = 104$. Thus, the method of repeated bifurcation which produced $16 = 2^4$ sub-integrals from an integral over 5 dimensional N, would result in 2^{19} or 2^{103} sub-integrals in these cases. Thus, any feasible approach along these lines would require automating the analysis of most of the integrals.

Appendix: Proof of Conjecture 2

by V. Scharaschkin

We prove Conjecture 2. See also Conjecture 34 and the preceding text for an explanation of how the polynomial f_1 arises.

We make a slight change of notation: put $r = v$ and $y = w$.

Let $p \equiv 5 \pmod 6$ be prime, and let b, $c \in \mathbb{F}_p$. Define

$$g(z) = z^3 - bz - c, \qquad f_1(u,v,w) = v^2w^3 + 3uvw + u^3 - bu - v - c$$

$$X_1 = \big\{(u,v,w) \mid f_1(u,v,w) = 0\big\}.$$

Assume g is irreducible over $\mathbb{F}_p$ from now on. We prove:

Theorem 46 *The affine variety X_1 is a rational surface, and $|X_1(\mathbb{F}_p)| = p^2 - 1$.*

Observe that as immediate consequences of our assumptions on p and g,

(a) -3 is not a square in $\mathbb{F}_p$.

(b) The cubing map on $\mathbb{F}_p$ is a bijection.

(c) $g(a) \neq 0$ for any $a \in \mathbb{F}_p$.

(d) $b \neq 0$.

The condition $p \equiv 5 \pmod 6$ is used in (a) and (b). Part (d) follows from (b) since $x^3 - c$ is always reducible.

We give an elementary proof of Theorem 46. This is a little ungainly, so collect the notation here for reference. Let

$$\begin{aligned}
f_1(u,v,w) &= v^2w^3 + 3uvw + u^3 - bu - v - c \\
f_2(u,v,w) &= w \\
f_3(u,v,w) &= \tfrac{1}{v}\Big[g\big(u + vw^2\big) - f_1\Big] \;=\; v^2w^6 + 3uvw^4 + 3u^2w^2 - vw^3 - 3uw - bw^2 + 1
\end{aligned}$$

$$
\begin{aligned}
f_4(u,v,w) &= w^3\cdot g\big(u-\tfrac{1}{w}\big) = u^3w^3-3u^2w^2-buw^3-cw^3+3uw+bw^2-1
\end{aligned}
$$

$$
\begin{aligned}
h_1(x,y) &= 3x^2+y^2-4b\\
h_2(x,y) &= -x^3+xy^2+4c\\
h_3(x,y) &= 8\,g\big(\tfrac{y-x}{2}\big) = (y-x)^3-4b(y-x)-8c\\
h_4(x,y) &= -8\,g\big(\tfrac{-y-x}{2}\big) = (x+y)^3-4b(x+y)+8c
\end{aligned}
$$

Check the following identities:

$$4g(x)+h_2 = x\,h_1 \tag{47}$$
$$f_3+f_4 = w^3 f_1 \tag{48}$$
$$bh_1^2h_2+ch_1^3-h_2^3 = -g(x)h_3h_4 \tag{49}$$
$$8g(x)+6h_2+h_3 = h_4 \tag{50}$$
$$4g(x)+3h_2+h_3 = y\,h_1 \tag{51}$$
$$g\big(u+vw^2\big) = f_1+v\cdot f_3 \tag{52}$$
$$w^2\cdot h_1\big(u-\tfrac{1}{w},\ 2vw^2+3u-\tfrac{1}{w}\big) = 4f_3 \tag{53}$$
$$w^2\cdot h_2\big(u-\tfrac{1}{w},\ 2vw^2+3u-\tfrac{1}{w}\big) = 4(uf_3-w^2f_1) \tag{54}$$
$$w^3\cdot g\big(u-\tfrac{1}{w}\big) = f_4 \tag{55}$$

For each f_j and h_j above, define sets (affine varieties)

$$
\begin{aligned}
X_j &= \{(u,v,w)\in\mathbb{F}_p^3 \mid f_j(u,v,w)=0\}\\
X_{j,k} &= X_j\cap X_k\\
Y_j &= \{(x,y)\in\mathbb{F}_p^2 \mid h_j(x,y)=0\}
\end{aligned}
$$

Since $f_3(u,v,0)=1$ we have

$$X_{2,3}(\mathbb{F}_p)=\varnothing.$$

Since g never vanishes, equations (52) and (55) show

$$X_{1,3}(\mathbb{F}_p)=\varnothing=X_{1,4}(\mathbb{F}_p). \tag{56}$$

also.

We shall define a bijection

$$X_1\setminus X_{1,2}\to\mathbb{F}_p^2\setminus Y_1. \tag{57}$$

Equation (57) implies

$$|X_1(\mathbb{F}_p)| = p^2-|Y_1(\mathbb{F}_p)|+|X_{1,2}(\mathbb{F}_p)|. \tag{58}$$

Clearly $f_1(u,v,w)=f_2(u,v,w)=0 \iff g(u)=v$, so for each u there is a unique v with $(u,v,w)\in X_{1,2}$, so

$$|X_{1,2}|=p.$$

Since $b \neq 0$, Y_1 is a (non-degenerate) conic. The projective closure of Y_1 has $p+1$ points over $\mathbb{F}_p$. (It always has at least one point by the Cauchy–Davenport theorem,[1] and this gives a bijection with $\mathbb{P}^1$.) Points at ∞ would only occur where $3X^2 + Y^2 - 4bZ^2 = 0$ with $Z = 0$, that is, when $Y^2 = -3X^2$. So condition (a) above implies

$$|Y_1| = p + 1$$

also. Thus from (58) we obtain

$$|X_1| = p^2 - p - 1 + p = p^2 - 1.$$

It remains to establish (57).

Define $\theta\colon \mathbb{F}_p^3 \setminus X_2 \to \mathbb{F}_p^2$ by

$$\theta(u, v, w) = \Big(u - \tfrac{1}{w},\ 2vw^2 + 3u - \tfrac{1}{w}\Big). \tag{59}$$

From (53) $\;[w \neq 0 \text{ and } f_3(u, v, w) \neq 0] \implies [\,\theta(u, v, w) \text{ is defined and } h_1\big(\theta(u, v, w)\big) \neq 0\,]$. Thus

$$\theta\colon \mathbb{F}_p^3 \setminus (X_2 \cup X_3) \to \mathbb{F}_p^2 \setminus Y_1.$$

From (56) $X_{1,3} = \varnothing$, so θ restricts to a map

$$\theta\colon X_1 \setminus X_{1,2} \to \mathbb{F}_p^2 \setminus Y_1. \tag{60}$$

Define $\sigma\colon \mathbb{F}_p^2 \setminus Y_1 \to \mathbb{F}_p^3 \setminus X_2$ by

$$\sigma(x, y) = \left(\ \frac{h_2}{h_1},\ \frac{8g(x)^2 h_3}{h_1^3},\ -\frac{h_1}{4g(x)}\ \right). \tag{61}$$

This is well defined off Y_1 since g never vanishes, and $h_1 \neq 0$ implies $\sigma(x, y) \notin X_2$. We show that $(x, y) \in \mathbb{F}_p^2 \setminus Y_1 \implies f_1 \circ \sigma(x, y) = 0$ so $\sigma(x, y) \in X_1$. Writing g for $g(x)$,

$$\begin{aligned}
-h_1^3 \cdot (f_1 \circ \sigma) \quad &= \quad -h_1^3 \cdot f_1\Big(\frac{h_2}{h_1}, \frac{8g^2 h_3}{h_1^3}, -\frac{h_1}{4g}\Big) \\
&= \quad -h_1^3 \cdot \frac{8g^2 h_3}{h_1^3}\left[\frac{-h_3 - 6h_2 - 8g}{8g}\right] - h_2^3 + bh_1^2 h_2 + ch_1^3 \\
&= \quad gh_3\big[h_3 + 6h_2 + 8g\big] - h_2^3 + bh_1^2 h_2 + ch_1^3 \\
&\overset{(50),\,(49)}{=} \quad 0.
\end{aligned}$$

So

$$\sigma\colon \mathbb{F}_p^2 \setminus Y_1 \to X_1 \setminus X_{1,2}. \tag{62}$$

[1] Let $Q = \{3x^2 \mid x \in \mathbb{F}_p\}$, $R = \{y^2 \mid y \in \mathbb{F}_p\}$. Then $|Q| + |R| \geq p + 1$ implies every element of $\mathbb{F}_p$ (in particular $4b$) is of the form $q + r$ for some $q \in Q$, $r \in R$.

Finally we show that the maps θ and σ in equations (60), (62) are mutually inverse:

$$\theta\big(\sigma(x,y)\big) = \theta\left(\frac{h_2}{h_1},\ \ \frac{8g^2h_3}{h_1^3},\ \ -\frac{h_1}{4g(x)}\right) \ = \ \left(\frac{4g+h_2}{h_1},\ \ \frac{4g+3h_2+h_3}{h_1}\right) \overset{(47,51)}{=} \big(x,\ y\big).$$

Let $(U,V,W) = \big(\sigma\circ\theta\big)(u,v,w) = \sigma\big(u-\frac{1}{w},\ 2vw^2+3u-\frac{1}{w}\big)$. Here $(u,v,w)\in X_1\setminus X_{1,2}$ so $w\neq 0$ and $f_3(u,v,w)$ and $f_4(u,v,w)\neq 0$ also, from (56). A (rather tedious) calculation yields:

$$U = \frac{h_2}{h_1}\Big(u-\tfrac{1}{w},\ \ 2vw^2+3u-\tfrac{1}{w}\Big) \overset{(53,54)}{=} \frac{uf_3-w^2f_1}{f_3} = u - f_1\frac{w^2}{f_3},$$

$$\begin{aligned} V = \frac{8g^2h_3}{h_1^3}\Big(u-\tfrac{1}{w},\ \ 2vw^2+3u-\tfrac{1}{w}\Big) &\overset{(52),(53),(55)}{=} \frac{f_1f_4^2+vf_3f_4^2}{f_3^3} \\ &= \ v+\frac{f_1f_4^2+vf_3f_4^2-vf_3^3}{f_3^3} \ \overset{(48)}{=} \ v+f_1\frac{[f_4^2+vw^3f_3\cdot(f_4-f_3)]}{f_3^3}, \end{aligned}$$

and

$$W = -\frac{h_1}{4g}\Big(u-\tfrac{1}{w},\ 2vw^2+3u-\tfrac{1}{w}\Big) \overset{(53),(55)}{=} -\frac{wf_3}{f_4} \ = \ w \ - \ w\cdot\left(1+\frac{f_3}{f_4}\right) \overset{(48)}{=} w-f_1\frac{w^4}{f_4}.$$

So

$$(U,V,W) = \left(u-f_1\frac{w^2f_1}{f_3},\quad v+f_1\frac{[f_4^2+vw^3f_3\cdot(f_4-f_3)]}{f_3^3},\quad w-f_1\frac{w^4}{f_4}\right).$$

On X_1 where f_1 vanishes, $\big(\sigma\circ\theta\big)(u,v,w) = (U,V,W) = (u,v,w)$ as required. This completes the proof.

Acknowledgments

We would like to acknowledge the Alfred P. Sloan Foundation (SLOAN) for funding the project initially as a summer research in 2023 (G2021-17076).

References

[1] A. Borel, *Linear algebraic groups*, Graduate Texts in Mathematics **126**, Second edition, Springer-Verlag, New York, 1991.

[2] J.W.S. Cassels, A. Fröhlich, *Algebraic number theory*, Academic Press, London, 1986.

[3] D.S. Dummit, R.M. Foote, *Abstract algebra*, Third edition, John Wiley & Sons, Hoboken, NJ, 2004.

[4] W. Fulton, J. Harris, *Representation theory*, Graduate Texts in Mathematics **129**, Springer-Verlag, New York, 1991.

[5] D. Goldfeld, J. Hundley, *Automorphic representations and L-functions for the general linear group. Volume I*, Cambridge Studies in Advanced Mathematics **129**, Cambridge University Press, Cambridge, 2011.

[6] J.E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics **21**, Springer-Verlag, New York-Heidelberg, 1975.

[7] N. Iwahori, H. Matsumoto, On some Bruhat decomposition and the structure of the Hecke rings of $\mathfrak{p}$-adic Chevalley groups, *Inst. Hautes Études Sci. Publ. Math.*, **25** (1965), 5–48.

[8] D. Jiang, S. Rallis, Fourier coefficients of Eisenstein series of the exceptional group of type G_2, *Pacific J. Math.*, **181** (1997), 281–314.

[9] S. Katok, *p-adic analysis compared with real*, Student Mathematical Library **37**, American Mathematical Society, Providence, RI, 2007.

[10] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics **110**, Second edition, Springer-Verlag, New York, 1994.

[11] K. Magaard, G. Savin, Exceptional Θ-correspondences. I, *Compositio Math.*, **107** (1997), 89–123.

[12] J.F. Pleso, *Integrals Over an Interesting Unipotent Subgroup*, Master's thesis, Southern Illinois University Carbondale, 2009.

[13] P.J. Sally Jr., *Fundamentals of mathematical analysis*, Pure and Applied Undergraduate Texts **20**, American Mathematical Society, Providence, RI, 2013.

[14] P.J. Sally Jr., An introduction to p-adic fields, harmonic analysis and the representation theory of SL_2, *Lett. Math. Phys.*, **46** (1998), 1–47.

[15] P.J. Sally Jr., *Tools of the trade*, American Mathematical Society, Providence, RI, 2008.

[16] T.A. Springer, *Linear algebraic groups*, Modern Birkhäuser Classics, Second edition, Birkhäuser Boston, Boston, MA, 2009.

[17] M. Weissman, What is ... G_2?, available online at the URL: `http://martyweissman.com/WhatIsG2.pdf`.

[18] D.J. Wright, The adelic zeta function associated to the space of binary cubic forms. I. Global theory, *Math. Ann.*, **270** (1985), 503–534.

[19] W. Xiong, On certain Fourier coefficients of Eisenstein series on G_2, *Pacific J. Math.*, **289** (2017), 235–255.

Joseph Hundley
SUNY University at Buffalo
134 Jacobs Hl,
Buffalo, NY 14260
E-mail: `jahundle@buffalo.edu`

Yaniel Rivera Vega
University of Wisconsin-Madison
500 Lincoln Dr,
Madison, WI 53706
E-mail: `riveravega@wisc.edu`

Victor Scharaschkin
E-mail: `vscharaschkin@gmail.com`

Received: June 2, 2025 **Accepted**: December 2, 2025
Communicated by Daniel Vallières