

The Igusa Zeta Function in Arbitrary P-adic Fields

Neal Lima

July 26, 2007

What is a P-adic field?

The most common p-adic field is a result of taking \mathbb{Q} and completing the field with respect to some prime.

- ▶ We denote this \mathbb{Q}_p .

What is a P-adic field?

The most common p-adic field is a result of taking \mathbb{Q} and completing the field with respect to some prime.

- ▶ We denote this \mathbb{Q}_p .
- ▶ Every element of \mathbb{Q}_p can be expressed as a power series.

$$x \in \mathbb{Q}_p \Rightarrow x = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \dots + a_0 + a_1p + a_2p^2 \dots$$

where each $a_i \in \mathbb{F}_p$

What is a P-adic field?

The most common p-adic field is a result of taking \mathbb{Q} and completing the field with respect to some prime.

- ▶ We denote this \mathbb{Q}_p .
- ▶ Every element of \mathbb{Q}_p can be expressed as a power series.

$$x \in \mathbb{Q}_p \Rightarrow x = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \dots + a_0 + a_1p + a_2p^2 \dots$$

where each $a_i \in \mathbb{F}_p$

We set $|x| = p^{-n}$ where n is the smallest integer such that $a_n \neq 0$.

What is a P-adic field?

The most common p-adic field is a result of taking \mathbb{Q} and completing the field with respect to some prime.

- ▶ We denote this \mathbb{Q}_p .
- ▶ Every element of \mathbb{Q}_p can be expressed as a power series.

$$x \in \mathbb{Q}_p \Rightarrow x = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \dots + a_0 + a_1p + a_2p^2 \dots$$

where each $a_i \in \mathbb{F}_p$

We set $|x| = p^{-n}$ where n is the smallest integer such that $a_n \neq 0$.

- ▶ For example, in \mathbb{Q}_3 we have that $|15| = 3^{-1}$.

In the p-adic numbers we have the p-adic integers which we define to be

$$\begin{aligned}\mathbb{Z}_p &= \{x \in \mathbb{Q}_p : |x| \leq 1\} \\ &= \{x \in \mathbb{Q}_p : x = a_0 + a_1p + a_2p^2 \dots \text{ for } a_i \in \mathbb{F}_p\}\end{aligned}$$

Algebraic Structures within \mathbb{Q}_p

In the p-adic numbers we have the p-adic integers which we define to be

$$\begin{aligned}\mathbb{Z}_p &= \{x \in \mathbb{Q}_p : |x| \leq 1\} \\ &= \{x \in \mathbb{Q}_p : x = a_0 + a_1p + a_2p^2 \dots \text{ for } a_i \in \mathbb{F}_p\}\end{aligned}$$

In the ring \mathbb{Z}_p we have the maximal ideal

$$\begin{aligned}p\mathbb{Z}_p &= \{x \in \mathbb{Q}_p : |x| \leq 1\} \\ &= \{x \in \mathbb{Q}_p : x = b_1p + b_2p^2 \dots \text{ for } b_i \in \mathbb{F}_p\}\end{aligned}$$

Algebraic Structures within \mathbb{Q}_p

In the p-adic numbers we have the p-adic integers which we define to be

$$\begin{aligned}\mathbb{Z}_p &= \{x \in \mathbb{Q}_p : |x| \leq 1\} \\ &= \{x \in \mathbb{Q}_p : x = a_0 + a_1p + a_2p^2 \dots \text{ for } a_i \in \mathbb{F}_p\}\end{aligned}$$

In the ring \mathbb{Z}_p we have the maximal ideal

$$\begin{aligned}p\mathbb{Z}_p &= \{x \in \mathbb{Q}_p : |x| \leq 1\} \\ &= \{x \in \mathbb{Q}_p : x = b_1p + b_2p^2 \dots \text{ for } b_i \in \mathbb{F}_p\}\end{aligned}$$

We take $\mathbb{Z}_p/p\mathbb{Z}_p$ which we call *the residue field of \mathbb{Q}_p* and see that it is isomorphic to \mathbb{F}_p and can be thought of as the field of coefficients for all power series in \mathbb{Q}_p .

Igusa Function over \mathbb{Q}_p

We let μ be a Haar measure on \mathbb{Z}_p which we scale so that $\mu(\mathbb{Z}_p) = 1$ and for a measurable set $A \subseteq \mathbb{Z}_p$ we say that

$$\mu(A) = \int_A dx$$

Igusa Function over \mathbb{Q}_p

We let μ be a Haar measure on \mathbb{Z}_p which we scale so that $\mu(\mathbb{Z}_p) = 1$ and for a measurable set $A \subseteq \mathbb{Z}_p$ we say that

$$\mu(A) = \int_A dx$$

With this we can define the Igusa Zeta Function over \mathbb{Q}_p for some function f to be

$$Z_I(s) = \int_{\mathbb{Z}_p} |f(x)|^s dx$$

Igusa Function over \mathbb{Q}_p

We let μ be a Haar measure on \mathbb{Z}_p which we scale so that $\mu(\mathbb{Z}_p) = 1$ and for a measurable set $A \subseteq \mathbb{Z}_p$ we say that

$$\mu(A) = \int_A dx$$

With this we can define the Igusa Zeta Function over \mathbb{Q}_p for some function f to be

$$Z_I(s) = \int_{\mathbb{Z}_p} |f(x)|^s dx$$

To compute this, one must break up $\mathbb{Z}_p = A_1 \cup A_2 \cup \dots$ where each A_i is measurable, and $|f(x)|$ is constant over each A_i . In this case

$$Z_I(s) = \sum_i |f(a_i)|^s \mu(A_i)$$

Main Goal

We want to define the Igusa Zeta Function over all finite extensions of \mathbb{Q}_p . To do this we will need:

We want to define the Igusa Zeta Function over all finite extensions of \mathbb{Q}_p . To do this we will need:

- ▶ An understanding of what the elements in a finite extension of \mathbb{Q}_p look like.

We want to define the Igusa Zeta Function over all finite extensions of \mathbb{Q}_p . To do this we will need:

- ▶ An understanding of what the elements in a finite extension of \mathbb{Q}_p look like.
- ▶ A ring of integers in this extension.

We want to define the Igusa Zeta Function over all finite extensions of \mathbb{Q}_p . To do this we will need:

- ▶ An understanding of what the elements in a finite extension of \mathbb{Q}_p look like.
- ▶ A ring of integers in this extension.
- ▶ A maximal ideal in this ring.

Main Goal

We want to define the Igusa Zeta Function over all finite extensions of \mathbb{Q}_p . To do this we will need:

- ▶ An understanding of what the elements in a finite extension of \mathbb{Q}_p look like.
- ▶ A ring of integers in this extension.
- ▶ A maximal ideal in this ring.
- ▶ And lastly, a Haar measure on this ring.

The Elements of a Finite Extension

We take our finite extension K/\mathbb{Q}_p and a basis for this extension $\{v_1, \dots, v_d\}$. Then for $x \in K$ we have that

$$x = b_1 v_1 + \dots + b_d v_d$$

Where $b_i \in \mathbb{Q}_p$.

The Elements of a Finite Extension

We take our finite extension K/\mathbb{Q}_p and a basis for this extension $\{v_1, \dots, v_d\}$. Then for $x \in K$ we have that

$$x = b_1 v_1 + \dots + b_d v_d$$

Where $b_i \in \mathbb{Q}_p$.

Because each b_i has a p-adic expansion, we can then express x p-adically as well,

$$x = (a_{-m,1} v_1 + \dots + a_{-m,d} v_d) p^{-m} + \dots + (a_{0,1} v_1 + \dots + a_{0,d} v_d) + (a_{1,1} v_1 + \dots + \dots)$$

where each $a_{i,j} \in \mathbb{F}_p$.

The Elements of a Finite Extension

We take our finite extension K/\mathbb{Q}_p and a basis for this extension $\{v_1, \dots, v_d\}$. Then for $x \in K$ we have that

$$x = b_1 v_1 + \dots + b_d v_d$$

Where $b_i \in \mathbb{Q}_p$.

Because each b_i has a p -adic expansion, we can then express x p -adically as well,

$$x = (a_{-m,1} v_1 + \dots + a_{-m,d} v_d) p^{-m} + \dots + (a_{0,1} v_1 + \dots + a_{0,d} v_d) + (a_{1,1} v_1 + \dots + \dots)$$

where each $a_{i,j} \in \mathbb{F}_p$.

We can then define the ring of integers in K to be

$$O_K = \{x \in K : x = \alpha_0 + \alpha_1 p^1 + \dots \text{ where } \alpha_i = a_{i,1} v_1 + \dots + a_{i,d} v_d \text{ and } a_{i,j} \in \mathbb{F}_p\}$$

- ▶ It can be shown that \mathbb{Z}_p is a PID where every ideal is of the form $p^n\mathbb{Z}_p$ for some integer n .

- ▶ It can be shown that \mathbb{Z}_p is a PID where every ideal is of the form $p^n\mathbb{Z}_p$ for some integer n .
- ▶ Furthermore, it can also be shown that O_K is a PID where every ideal is of the form $\pi^n O_K$.

- ▶ It can be shown that \mathbb{Z}_p is a PID where every ideal is of the form $p^n\mathbb{Z}_p$ for some integer n .
- ▶ Furthermore, it can also be shown that O_K is a PID where every ideal is of the form $\pi^n O_K$.
- ▶ We then have that the ideal $\mathfrak{p}O_K$ is generated by π^e for some $\pi \in K$ and $e \in \mathbb{Z}^+$.

- ▶ It can be shown that \mathbb{Z}_p is a PID where every ideal is of the form $p^n \mathbb{Z}_p$ for some integer n .
- ▶ Furthermore, it can also be shown that O_K is a PID where every ideal is of the form $\pi^n O_K$.
- ▶ We then have that the ideal $\mathfrak{p} O_K$ is generated by π^e for some $\pi \in K$ and $e \in \mathbb{Z}^+$.
- ▶ We call e the ramification index of K .

- ▶ If $e = 1$ then K is *unramified* Example: $K = \mathbb{Q}_p(\sqrt{2})$.

Ramification

- ▶ If $e = 1$ then K is *unramified* Example: $K = \mathbb{Q}_p(\sqrt{2})$.
- ▶ If $e > 1$ then K is *ramified*. Example: $K = \mathbb{Q}_p(\sqrt{2}, \sqrt{p})$.

Ramification

- ▶ If $e = 1$ then K is *unramified* Example: $K = \mathbb{Q}_p(\sqrt{2})$.
- ▶ If $e > 1$ then K is *ramified*. Example: $K = \mathbb{Q}_p(\sqrt{2}, \sqrt{p})$.
- ▶ If $e = d = [K : \mathbb{Q}_p]$ then K is *totally ramified*. Example:
 $K = \mathbb{Q}_p(\sqrt[d]{p})$

Structure of K

Surprisingly, K looks like \mathbb{Q}_p because now we can write all elements of K as a unique power series around π . We can also define a ring of integers in K to be

$$O_K = \{x \in K : x = a_0 + a_1\pi + a_2\pi^2 + \dots \text{ where } a_i \in \mathbb{F}_{p^f}\}$$

Structure of K

Surprisingly, K looks like \mathbb{Q}_p because now we can write all elements of K as a unique power series around π . We can also define a ring of integers in K to be

$$O_K = \{x \in K : x = a_0 + a_1\pi + a_2\pi^2 + \dots \text{ where } a_i \in \mathbb{F}_{p^f}\}$$

The maximal ideal in O_K is

$$\pi O_K = \{x \in K : x = a_1\pi + a_2\pi^2 + \dots \text{ where } a_i \in \mathbb{F}_{p^f}\}$$

Structure of K

Surprisingly, K looks like \mathbb{Q}_p because now we can write all elements of K as a unique power series around π . We can also define a ring of integers in K to be

$$O_K = \{x \in K : x = a_0 + a_1\pi + a_2\pi^2 + \dots \text{ where } a_i \in \mathbb{F}_{p^f}\}$$

The maximal ideal in O_K is

$$\pi O_K = \{x \in K : x = a_1\pi + a_2\pi^2 + \dots \text{ where } a_i \in \mathbb{F}_{p^f}\}$$

Our coefficients of K are now coming from $O_K/\pi O_K \cong \mathbb{F}_{p^f}$ for some integer f . We call f the residue degree of K and it plays a major role in defining $Z_f(s)$ in K .

Fundamental Identity of Ramification

We have

- ▶ $d = [K : \mathbb{Q}_p]$
- ▶ $f = [O_K/\pi O_K : \mathbb{Z}_p/p\mathbb{Z}_p]$
- ▶ e such that $\pi^e = p$ in K

Fundamental Identity of Ramification

We have

- ▶ $d = [K : \mathbb{Q}_p]$
- ▶ $f = [O_K/\pi O_K : \mathbb{Z}_p/p\mathbb{Z}_p]$
- ▶ e such that $\pi^e = p$ in K

Theorem

$$ef = d$$

Fundamental Identity of Ramification

We have

- ▶ $d = [K : \mathbb{Q}_p]$
- ▶ $f = [O_K/\pi O_K : \mathbb{Z}_p/p\mathbb{Z}_p]$
- ▶ e such that $\pi^e = p$ in K

Theorem

$$ef = d$$

- ▶ We then have that f is completely determined by e and d .

Fundamental Identity of Ramification

We have

- ▶ $d = [K : \mathbb{Q}_p]$
- ▶ $f = [O_K/\pi O_K : \mathbb{Z}_p/p\mathbb{Z}_p]$
- ▶ e such that $\pi^e = p$ in K

Theorem

$$ef = d$$

- ▶ We then have that f is completely determined by e and d .
- ▶ K is determined by π and the coefficients of all π -adic expansions, so K is also completely determined by e and d .

Fundamental Identity of Ramification

We have

- ▶ $d = [K : \mathbb{Q}_p]$
- ▶ $f = [O_K/\pi O_K : \mathbb{Z}_p/p\mathbb{Z}_p]$
- ▶ e such that $\pi^e = p$ in K

Theorem

$$ef = d$$

- ▶ We then have that f is completely determined by e and d .
- ▶ K is determined by π and the coefficients of all π -adic expansions, so K is also completely determined by e and d .
- ▶ In particular, there is only one unramified extension of degree d over \mathbb{Q}_p we call K_d , with ring of integers O_d .

Fundamental Identity of Ramification

We have

- ▶ $d = [K : \mathbb{Q}_p]$
- ▶ $f = [O_K/\pi O_K : \mathbb{Z}_p/p\mathbb{Z}_p]$
- ▶ e such that $\pi^e = p$ in K

Theorem

$$ef = d$$

- ▶ We then have that f is completely determined by e and d .
- ▶ K is determined by π and the coefficients of all π -adic expansions, so K is also completely determined by e and d .
- ▶ In particular, there is only one unramified extension of degree d over \mathbb{Q}_p we call K_d , with ring of integers O_d .
- ▶ Note that $K_d \leq K_n$ if and only if $d|n$.

Fundamental Identity of Ramification

We have

- ▶ $d = [K : \mathbb{Q}_p]$
- ▶ $f = [O_K/\pi O_K : \mathbb{Z}_p/p\mathbb{Z}_p]$
- ▶ e such that $\pi^e = p$ in K

Theorem

$$ef = d$$

- ▶ We then have that f is completely determined by e and d .
- ▶ K is determined by π and the coefficients of all π -adic expansions, so K is also completely determined by e and d .
- ▶ In particular, there is only one unramified extension of degree d over \mathbb{Q}_p we call K_d , with ring of integers O_d .
- ▶ Note that $K_d \leq K_n$ if and only if $d|n$.
- ▶ In K_d we let $\pi = p$.

A Measure on O_K

We now take μ to be a Haar measure on O_K scaling $\mu(O_K) = 1$

A Measure on O_K

We now take μ to be a Haar measure on O_K scaling $\mu(O_K) = 1$

- ▶ Once again $\mu(A) = \int_A dx$

A Measure on O_K

We now take μ to be a Haar measure on O_K scaling $\mu(O_K) = 1$

- ▶ Once again $\mu(A) = \int_A dx$
- ▶ We can show that $\mu(\pi^n O_K) = p^{-nf}$
- ▶ Based on our measure we set $|\pi| = p^{-f}$

A Measure on O_K

We now take μ to be a Haar measure on O_K scaling $\mu(O_K) = 1$

- ▶ Once again $\mu(A) = \int_A dx$
- ▶ We can show that $\mu(\pi^n O_K) = p^{-nf}$
- ▶ Based on our measure we set $|\pi| = p^{-f}$
- ▶ Now that we have a measure and absolute value on O_K we can define the Igusa Zeta function over K to be

$$Z_I(s) = \int_{O_K} |f(x)|^s dx$$

Ramification, What is it good for?

We let $E \in \mathbb{Q}_p[x, y]$ be an elliptic curve. We studied the *resolution of singularities mod p* which depend on what E looks like modulo p .

- ▶ In an unramified field, p is no longer prime so we must look at E modulo π .

Ramification, What is it good for?

We let $E \in \mathbb{Q}_p[x, y]$ be an elliptic curve. We studied the *resolution of singularities mod p* which depend on what E looks like modulo p .

- ▶ In an unramified field, p is no longer prime so we must look at E modulo π .
- ▶ Also, if a function g has a singular point in O_d then it will also have a singular point in O_{nd} for all $n \in \mathbb{Z}^+$.
- ▶ A result due to Igusa relates a curves zeta function to it's singularities. In these two previous examples the Igusa zeta function will change and not change based on the ramification index of K .

Ramification, What is it good for?

We let $E \in \mathbb{Q}_p[x, y]$ be an elliptic curve. We studied the *resolution of singularities mod p* which depend on what E looks like modulo p .

- ▶ In an unramified field, p is no longer prime so we must look at E modulo π .
- ▶ Also, if a function g has a singular point in O_d then it will also have a singular point in O_{nd} for all $n \in \mathbb{Z}^+$.
- ▶ A result due to Igusa relates a curves zeta function to it's singularities. In these two previous examples the Igusa zeta function will change and not change based on the ramification index of K .

Example

- ▶ Take any polynomial f and find $Z_I(s)$ over \mathbb{Q}_p . Then $Z_I(s)$ will be the same over all totally ramified extensions of \mathbb{Q}_p .

Example

- ▶ Take any polynomial f and find $Z_I(s)$ over \mathbb{Q}_p . Then $Z_I(s)$ will be the same over all totally ramified extensions of \mathbb{Q}_p .
- ▶ Take $f(x) = x - 2$ in \mathbb{Q}_p for $p > 2$. Then $Z_I(s) = \frac{1-p^{-1}}{1-p^{-1}p^{-s}}$.

Example

- ▶ Take any polynomial f and find $Z_I(s)$ over \mathbb{Q}_p . Then $Z_I(s)$ will be the same over all totally ramified extensions of \mathbb{Q}_p .
- ▶ Take $f(x) = x - 2$ in \mathbb{Q}_p for $p > 2$. Then $Z_I(s) = \frac{1-p^{-1}}{1-p^{-1}p^{-s}}$.
- ▶ Let K be any totally ramified field ($e = d$) with prime π . Then $Z_I(s) = \frac{1-p^{-1}}{1-p^{-1}p^{-s}}$.

Another Example

- ▶ Let $g(x) = x^2 - 1$ and p such that $2 \not\equiv \square \pmod{p}$. Then g has a root in K_d if and only if d is even. In this case

$$Z_I(s) = \frac{1 - 2p^{-d} + p^{-d}t^2}{1 - p^{-dt}}$$

Another Example

- ▶ Let $g(x) = x^2 - 1$ and p such that $2 \not\equiv \square \pmod{p}$. Then g has a root in K_d if and only if d is even. In this case

$$Z_I(s) = \frac{1 - 2p^{-d} + p^{-d}t^2}{1 - p^{-dt}}$$

- ▶ If d is odd, then $Z_I(s) = 1$.

Another Example

- ▶ Let $g(x) = x^2 - 1$ and p such that $2 \not\equiv \square \pmod{p}$. Then g has a root in K_d if and only if d is even. In this case

$$Z_I(s) = \frac{1 - 2p^{-d} + p^{-d}t^2}{1 - p^{-dt}}$$

- ▶ If d is odd, then $Z_I(s) = 1$.
- ▶ Take L to be any field such that $K_2 \leq L$. Then

$$Z_I(s) = \frac{1 - 2p^{-f} + p^{-f}t^2}{1 - p^{-ft}}$$

where $f = \frac{d}{e}$

Conclusion and Thanks

- ▶ We now see how we can fix a polynomial f and let our base field vary and how this will effect $Z_I(s)$.

Conclusion and Thanks

- ▶ We now see how we can fix a polynomial f and let our base field vary and how this will effect $Z_I(s)$.
- ▶ Using the fact that $ef = d$ and the work of the 1999 REU we can ask how an elliptic curve's reduction type will change in arbitrary extensions of \mathbb{Q}_p .

Conclusion and Thanks

- ▶ We now see how we can fix a polynomial f and let our base field vary and how this will effect $Z_I(s)$.
- ▶ Using the fact that $ef = d$ and the work of the 1999 REU we can ask how an elliptic curve's reduction type will change in arbitrary extensions of \mathbb{Q}_p .
- ▶ Lastly, I'd like to thank Zeb Engberg, Sohini Mahapatra, Sam Ruth, Hillary Sackett, Mount Holyoke College, and especially Margaret Robinson, for all their support this summer.