p-adicity

Barbara T. Faires Allegheny Mountain Colloquium

Carl Wang-Erickson

University of Pittsburgh

November 12, 2024

In the beginning...

There was $\mathbb{Z}$. 0, 1, 2, 3, 4, ...

But what is $\mathbb{Z}$ *really?* Key structures:

- A ring: it has $+$ and $\cdot$ and they behave well
- Not just a ring but a domain: if $xy = 0$, then $x = 0$ or $y = 0$
- Ordered: has inequality $<$... $\rightsquigarrow$ notion of *positive*

Good! But so does $\mathbb{Q}$ = rationals... $\mathbb{R}$ = reals... and $\mathbb{Z}[\frac{1}{2}] = \left\{ \frac{a}{2^b} \right\}$

What sets $\mathbb{Z}$ apart: the *well-ordering principle*.

- Any non-empty subset of $\mathbb{Z}_{>0}$ has a least (minimum) element.

Elementary number theory:

- Prove there are no integers between 0 and 1 $\rightsquigarrow$ induction
- Unique factorization into primes

If $\mathbb{Z}$ is the beginning, what comes next?

The real numbers $\mathbb{R}$, right? Number line, continuum, measurements, ...

What is $\mathbb{R}$ *really?*

- An ordered field
- every non-empty subset of $\mathbb{R}$ that is bounded above has a supremum (least upper bound) in $\mathbb{R}$. This property is called completeness.

From $\mathbb{R}$, we go on to calculus, metrics and topologies, complex analysis, functional analysis; manifolds, geometric analysis, etc...

It's foundational to investigations of change, shapes, approximation, and much more.

Metric spaces

Metric spaces (like $\mathbb{R}^n$): a set X with a notion of $\mathbb{R}$-valued distance

$$d : X \times X \to \mathbb{R}_{\geq 0}$$

satisfying these *axioms of metric space*: $\forall\, x, y, z \in X$,

1. $d(x,y) = 0 \iff x = y$; and $d(x,y) = d(y,x)$
2. $\boxed{d(x,y) \leq d(x,z) + d(z,y)}$ – the triangle inequality

When X has a 0, then an *absolute value* or *norm* is distance from 0:

$$|\cdot| : X \to \mathbb{R}_{\geq 0}, \quad x \mapsto |x| := d(x,0).$$

Another perspective: $\mathbb{R}$ is a *completion* of $\mathbb{Q}$ according to the usual metric.

What if we did something else next, after $\mathbb{Z}$?

Question

Is there a metric on $\mathbb{Q}$ other than the usual one, and which respects the arithmetic structure "$+, \cdot$" of $\mathbb{Q}$?

Let's define "respects arithmetic structure."

Definition (Norm $|\cdot|_\star$ on $\mathbb{Q}$)

A function $|\cdot|_\star : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ *such that*

1. $|x|_\star = 0 \iff x = 0$
2. $|x + y|_\star \leq |x|_\star + |y|_\star$ *(triangle inequality)*
3. $|x \cdot y|_\star = |x|_\star \cdot |y|_\star$ *(multiplicativity)*

Note: norm $\rightsquigarrow$ metric, by $d_\star(x, y) = |x - y|_\star$.

Answer

"Yes" ... because of p-adicity.

p-adicity as seen on $\mathbb{Q}$

Let p be a prime number.

Definition (The standard p-adic norm $|\cdot|_p$ on $\mathbb{Q}$)

Let $\frac{a}{b} \in \mathbb{Q}$. Let $e \in \mathbb{Z}$ satisfy $\frac{a}{b} = p^e \cdot \frac{a'}{b'}$, where $p \nmid a'b'$. Define

$$\left|\frac{a}{b}\right|_p := p^{-e}.$$

Using words: p^e is the "p-part" of $\frac{a}{b}$ $\rightsquigarrow$ p-adic norm $=$ inverse p-part.

Intuitively: two rational numbers are p-adically
$\rightsquigarrow$ close together when their difference has numerator highly divisible by p
$\rightsquigarrow$ far away when their difference has denominator highly divisible by p.

To prove: $|\cdot|_p$ satisfies the axioms of norm/metric.
Ostrowski's theorem.

Drawing $\mathbb{R}$-small integers and their p-adic distances

First fun phenomena of p-adicity on $\mathbb{Q}$

- $\mathbb{Z}$ is bounded in any p-adic metric
- $|\cdot|_p$ is *ultrametric* – that is, it satisfies the "strong triangle inequality"

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

  The opposite of ultrametric is "Archimedean", such as $|\cdot|$ on $\mathbb{R}$.

- In any ultrametric metric, every triangle is isoceles. In $\mathbb{Q}$:

$$|5-2|_3 = \frac{1}{3}, \quad |2-29|_3 = \frac{1}{27}, \quad |29-5|_3 = \frac{1}{3}.$$

- The series $\sum_{n=0}^{\infty} n!$ is Cauchy in any p-adic metric.
- In the 2-adic metric, the series $\sum_{n=0}^{\infty} 2^n$ converges. To what?

p-adic completion

Definition (Completion of $\mathbb{Q}$ with respect to a norm)

Given any norm $|\cdot|_\star$ on $\mathbb{Q}$, consider two Cauchy sequences $(a_n)_{n\geq 1}, (b_n)_{n\geq 1}$ in $\mathbb{Q}$ to be equivalent when their difference converges to zero, that is,

$$\lim_{n\to+\infty} a_n - b_n = 0; \qquad \textit{equivalently,} \quad \lim_{n\to+\infty} |a_n - b_n|_\star = 0.$$

The equivalence classes comprise the completion $\mathbb{Q}_\star$ of $\mathbb{Q}$ with respect to $|\cdot|_\star$.

Exercise: Because norms respect $+, \cdot$, $\mathbb{Q}_\star$ inherits $+, \cdot$.

Example: Usual $|\cdot|$ completes $\mathbb{Q}$ to $\mathbb{R}$ ...
while $|\cdot|_p$ completes $\mathbb{Q}$ to $\mathbb{Q}_p$, the p-adic numbers.

First fun phenomena in $\mathbb{Q}_p$

- If $a_n \to 0$ as $n \to +\infty$, then $\sum_{n=1}^{\infty} a_n$ converges in $\mathbb{Q}_p$. E.g.: $\sum_{n=0}^{\infty} n!$.

Idea: Ultrametric convergence is easier! Archimedean contrast: $\sum_{n=1}^{\infty} \frac{1}{n}$.

- Any $x \in \mathbb{Q}_p$ has a *unique* digit expansion

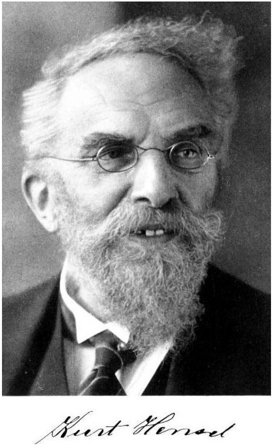
$$x = \sum_{n=m}^{\infty} x_i p^i, \qquad x_i \in \{0, 1, \dots, p-1\}$$

Idea: $p \leftrightarrow \frac{1}{10}$ as p-adic $\leftrightarrow$ decimal; and ultrametric $\Rightarrow$ uniqueness!

- $\mathbb{Z}$ completes to a subring $\mathbb{Z}_p \subset \mathbb{Q}_p$. *All* of the metric balls centered at 0 are: $\cdots \supset p^{-2}\mathbb{Z}_p \supset p^{-1}\mathbb{Z}_p \supset \mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \cdots$.

Idea: Balls have discrete radii, hence “closed = open” !

Kurt Hensel



In 1897, Hensel wrote down a p-adic digit expansion in *Über eine neue Begründung der Theorie der algebraischen Zahlen*.

$\mathbb{Z}_p$ is an *algebraic* limit

Notice that $p^m\mathbb{Z}_p$ consists of exactly those digital expansions of the form

$$\sum_{n=m}^{\infty} x_i p^i, \qquad x_i \in \{0, 1, \ldots, p-1\}$$

In fact $p^m\mathbb{Z}_p$ is an ideal of $\mathbb{Z}_p$ for $m \geq 0$, and we can compare:

$$\begin{array}{ccccccc}
\cdots \longrightarrow & \mathbb{Z}/p^3\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p \\
 & \downarrow \wr & & \downarrow \wr & & \downarrow \wr \\
\cdots \longrightarrow & \mathbb{Z}_p/p^3\mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p/p^2\mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p/p\mathbb{Z}_p
\end{array}$$

We call a system of choices in the upper line "$\varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$", which is another construction of $\mathbb{Z}_p$.

Hensel's lemma

To see algebraic and analytic ideas come together, we display Hensel's lemma for $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

Theorem (Hensel's lemma)

Let $f(x) \in \mathbb{Z}_p[x]$ be a monic polynomial and let $\bar{f}(x) \in \mathbb{F}_p[x]$ be its reduction modulo p. If $\bar{a} \in \mathbb{F}_p$ is a simple root of $\bar{f}(x)$, then there exists a unique $a \in \mathbb{Z}_p$ such that $\bar{a} = a \pmod{p}$ and $f(a) = 0$.

In words: a simple root $\bar{a} \pmod{p}$ *lifts* uniquely to a simple root $a \in \mathbb{Z}_p$.

Example

Because $\#\mathbb{F}_p^\times = p - 1$, the polynomial $x^{p-1} - 1$ has $p - 1$ distinct (thus, simple) roots in $\mathbb{F}_p$. Namely, the roots are $\mathbb{F}_p^\times$. By Hensel's lemma, $\mathbb{Z}_p$ contains the $p - 1$ roots of unity.

Proof method: "Newton's method always works" in $\mathbb{Z}_p$!

Helmut Hasse

Hasse

Theorem (The "Hasse principle", 1921)

A quadratic equation $0 = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$ *(*$a_{ij} \in \mathbb{Q}$*; indeterminants* x_i*) has a non-trivial solution in* $\mathbb{Q}$ *if and only if it has a non-trivial solution in* $\mathbb{R}$ *and in* $\mathbb{Q}_p$ *for all primes* p*.*

Brave new p-adic world ...

$\rightsquigarrow$ consider p-adic completion on par with Archimedean completion

p-adicity

p-adicity is a confluence of algebra, topology, and analysis.

$$p\text{-adic completion of } \mathbb{Z} \rightsquigarrow \mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

- metrics and topologies: adic things are first examples of *profinite* topologies
- analysis: the rest of this talk illustrates an example
- manifolds: some challenges and diverse progress over many decades in algebraic geometry and p-adic analytic geometry

p-adic notions are <u>ubiquitous</u> in number theory.

Recent number theory results using p-adic tools

Balakrishnan

Dogra

use the Chabauty–Kim (very p-adic!) method to determine $\mathbb{Q}$-points on algebraic curves

---

Caraiani

Scholze

use p-adic tools to study the geometry and cohomology of Shimura varieties

Dustin Clausen and Peter Scholze

Clausen

Scholze

Recently, Clausen and Scholze have proposed a new theory of *condensed mathematics* that is capable of encompassing p-adic analytic and real analytic geometry into a single framework.

A story from number theory: The Riemann zeta function

The RZF: $\zeta(s) = 1 + 2^{-s} + 3^{-s} + 4^{-s} + 5^{-s} + 6^{-s} + 7^{-s} + \cdots$

$$\begin{aligned} &= (1 + 2^{-s} + 4^{-s} + 8^{-s} + \cdots) \cdot (1 + 3^{-s} + 9^{-s} + \cdots) \\ &\quad \cdot (1 + 5^{-s} + 25^{-s} + \cdots) \cdot \ \cdots \\ &= \prod_{\ell:\ \text{prime}} (1 + \ell^{-s} + \ell^{-2s} + \ell^{-3s} + \cdots) \\ &= \prod_{\ell:\ \text{prime}} (1 - \ell^{-s})^{-1} \quad \leftarrow \text{ this is the Euler product.} \end{aligned}$$

Here are some key facts about $\zeta(s)$ in the *Archimedean* world.

- Converges for $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 1$.
- Analytically continues to $\mathbb{C} \setminus \{1\}$, has Taylor series at $s = 1$

$$\zeta(s) = (s-1)^{-1} + a_0 + a_1(s-1) + \cdots$$

- Has a functional equation:

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s) \quad \text{satisfies} \quad \xi(s) = \xi(1-s).$$

Bernhard Riemann

Riemann

Riemann's 1859 paper *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* introduced the notation $\zeta(s)$, its analytic continuation, its functional equation, and the "Riemann hypothesis."

Meet the Riemann zeta function ($\mathbb{R}$-based perspective)

$$\zeta(s) = \prod_{\ell:\ \text{prime}} (1 - \ell^{-s})^{-1}.$$

- Analytically continues to $\mathbb{C} \smallsetminus \{1\}$.
- Has a functional equation:

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s) \quad \text{satisfies} \quad \xi(s) = \xi(1-s).$$

- The "zeros of ζ", which are those $\rho \in \mathbb{C}$ with $\zeta(\rho) = 0$, are: $-2, -4, -6, \ldots$, and values in the *critical strip*, $0 \leq \mathrm{Re}(\rho) \leq 1$
- Riemann hypothesis: Those ρ in the critical strip have $\mathrm{Re}(\rho) = \frac{1}{2}$.
- A further conjecture: these zeros are *simple*.

Bernoulli numbers and $\zeta(s)$

The values of the Riemann zeta function at non-positive integers are *rational* and determined by the sequence of Bernoulli numbers

$$\boxed{\zeta(1-n) = -\frac{B_n}{n}} \text{ for } n \in \mathbb{Z}_{\geq 1}.$$

$$B_0 = 1, \quad B_1 = \frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = B_5 = B_7 = \cdots = 0$$

$$B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2370}, \quad \cdots$$

... but what are the Bernoulli numbers *really*?

The Bernoulli numbers

What are Bernoulli numbers? They give the answer to this question.

Question (Power sum formula)

Let $x, k \in \mathbb{Z}_{\geq 1}$. What function of x calculates $P_k(x) := \sum_{n=1}^{x} n^k$?

Answer (A definition of Bernoulli numbers)

$$(k+1)P_k(x) = B_0 x^{k+1} + \binom{k+1}{1} B_1 x^k + \cdots + \binom{k+1}{k} B_k = \sum_{n=0}^{k} \binom{k+1}{n} B_n x^{k+1-n}.$$

For example, $P_4(x) = \frac{1}{5} \cdot \left(\boxed{1} x^5 + 5 \boxed{\frac{1}{2}} x^4 + 10 \boxed{\frac{1}{6}} x^3 + 5 \boxed{\frac{-1}{30}} x \right)$

A few other facts: $\dfrac{t}{1 - e^{-t}} = \sum_{n=0}^{\infty} \dfrac{B_n}{n!} t^n.$ $\qquad \sum_{n=0}^{k-1} \binom{k}{n} B_n = 0.$

Jacob Bernoulli and Seki Takakazu

Bernoulli

Takakazu

Bernoulli and Takakazu independently (both ∼1700, both published posthumously in 1710s) identified the constants B_n in terms of their role in power sums.

The Bernoulli numbers and arithmetic

Now let's start approaching B_n p-adically: the first step is divisibility by p.

Definition (Regular primes)

Call a prime regular if $p \nmid (\text{numerator of } B_n)$ for even n, $0 \leq n \leq p-3$.

Irregular primes: 37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, 307, 311, 347, 353, 379, 389, 401, 409, 421, 433, 461, 463, 467, 491, 523, 541, 547, 557, 577, 587, 593, 607, 613, 617, 619, 631, 647, 653, 659, 673, 677, 683, 691, ...

Conjecture (Siegel)

The proportion of primes that are regular is $e^{-\frac{1}{2}} \approx 60.6\%$.

Unfortunately, not even the infinitude of regular primes is known.

Ernst Kummer: Bernoulli numbers and arithmetic

Kummer

Theorem ("Kummer's criterion", 1850)

A prime p is irregular if and only if there exists an ideal I in the ring $\mathbb{Z}[e^{2\pi i/p}]$ such that I is not principal and I^p is principal.

Theorem (Kummer's work on Fermat's last theorem)

If p is regular, then Fermat's last theorem for the exponent p can be proven using 19th century technology. $\rightsquigarrow$ *$x^p + y^p = z^p$ has no $\mathbb{Z}$-solution*

The Kummer congruences

Remarkably, the Bernoulli numbers are p-adically continuous as follows.

Theorem (von Staudt – Clausen: denominators are under control!)

$$B_{2n} + \sum_{\substack{(p-1)|2n \\ p:\ \text{prime}}} \frac{1}{p} \in \mathbb{Z};\ \textit{in particular},\ \mathrm{denominator}(B_{2n}) = \prod_{(p-1)|2n} p.$$

Ex: $B_2 = \frac{1}{2}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66}$

Theorem (Kummer congruences: p-adic continuity)

Let $m, n \in \mathbb{Z}_{\geq 1}$, not divisible by $(p-1)$. Let $a \in \mathbb{Z}_{\geq 0}$.

- *If $(p-1) \mid m-n$, then $\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}$.*
- *If $(p-1)p^a \mid m-n$, then $(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \pmod{p^{a+1}}$*

Ex: $p = 5, \quad 2 \equiv 10 \pmod{(5-1)}, \quad \frac{B_2}{2} - \frac{B_{10}}{10} = \frac{65}{264}$

The Kummer congruences for values of $\zeta(s)$

Theorem (Kummer congruences)

Let $m, n \in \mathbb{Z}_{\geq 1}$, not divisible by $(p-1)$. Let $a \in \mathbb{Z}_{\geq 0}$.

- *If $(p-1)p^a \mid m-n$, then $(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \pmod{p^{a+1}}$*

Let's say the same thing using $\zeta(s)$ and $\zeta(1-n) = -\frac{B_n}{n}$.

Theorem (Kummer congruences, $\zeta(s)$ version)

Let $s, t \in \mathbb{Z}_{\leq 0}$ such that $s, t \not\equiv 1 \pmod{(p-1)}$. Let $a \in \mathbb{Z}_{\geq 0}$.

- *If $(p-1)p^a \mid s-t$, then $(1-p^{-s})\zeta(s) \equiv (1-p^{-t})\zeta(t) \pmod{p^{a+1}}$.*

Remember that $\zeta(s) = \prod_{\ell:\text{ prime}}(1-\ell^{-s})^{-1}$ ...

Thus the Kummer congruences say: when you *remove* the Euler factor $(1-p^{-s})^{-1}$ from $\zeta(s)$, you get a p-adically continuous function on $\mathbb{Z}_{\leq 0}$.

Summing up the story of $\zeta : \mathbb{Z}_{\leq 0} \to \mathbb{Q}$ so far...

1. $\zeta(s) = \prod_{\ell\text{: prime}} (1 - \ell^{-s})^{-1}$ extends, using complex analysis, to all $s \in \mathbb{C} \setminus \{1\}$.
2. The values $\zeta(1-n)$ of the zeta-function at non-positive integers are given by Bernoulli numbers, $\zeta(1-n) = -\frac{B_n}{n}$.
3. The function $\zeta_p(s) := \zeta(s) \cdot (1 - p^{-s}) = \prod_{\ell\text{: prime}, \ell \neq p} (1 - \ell^{-s})^{-1}$ is p-adically continuous* as a function $\mathbb{Z}_{\leq 0} \to \mathbb{Q}$.

Upshot: because $\mathbb{Z}_{\leq 0} \subset \mathbb{Z}_p$ is dense,

there is a unique continuous* extension $\zeta_p : \mathbb{Z}_p \to \mathbb{Q}_p$.

(*): p-adically continuous $\zeta_{p,i}$ defined on $s \in (i + (p-1)\mathbb{Z}) \cap \mathbb{Z}_{\leq 0}$.

The Kubota–Leopoldt p-adic zeta function

Corollary (Construction of the p-adic zeta function, 1964)

There is a list $\zeta_{p,i}$, $i = 1, \ldots, p-1$, of meromorphic functions $\zeta_{p,i} : \mathbb{Z}_p \to \mathbb{Q}_p$ characterized by the equality, for $s \in \mathbb{Z}_{\leq 0}$,

$$(1 - p^{-s})\zeta(s) = \zeta_{p,i}(s) \quad \text{for } s \equiv i \pmod{(p-1)}.$$

The $\zeta_{p,i}$ are analytic other than $\zeta_{p,1}$ having a single simple pole at $s = 1$.

Kubota

Leopoldt

What we ask about this new world of zeta-functions

Compare with Riemann's Archimedean-analytic study:

- Analytic continuation: Radius of convergence of $\zeta_{p,i}$ goes beyond $\mathbb{Z}_p$, which is the ball of radius 1
- $\zeta_{p,i}$ has a zero (for some i) $\iff$ p is *irregular*
  - In the p-adic world, the existence of zeros of power series can be detected modulo p
- Folklore conjecture: the zeros of ζ_p are simple.

Question

What do the zeros of ζ_p mean?

As Kummer's criterion suggests, there is a connection:

$\exists$ zeros of $\zeta_{p,i} \Leftrightarrow p$ is irregular $\Leftrightarrow$ arithmetic of $\mathbb{Z}[e^{2\pi i/p}]$ more complicated

Arithmetic meaning of zeros of ζ_p: Iwasawa theory

Each $\zeta_{p,i}$ can be considered to be an element of $\Lambda := \mathbb{Z}_p[\![s]\!]$.

The (i-part of the) p-power part of the finite abelian ideal class groups X_n of the cyclotomic fields $\mathbb{Q}(e^{2\pi i/p^n})$ as $n \to \infty$ can be considered to be a module X_∞ over the ring $\Lambda = \mathbb{Z}_p[\![s]\!]$.

The main conjecture of Iwasawa theory (Theorem of Mazur–Wiles)

Up to a finite defect, $X_\infty \simeq \Lambda/f_1\Lambda \oplus \cdots \oplus \Lambda/f_s\Lambda$ for some f_j $(1 \leq j \leq s)$ such that $\prod_{j=1}^{s} f_j = \zeta_{p,i}$.

In other words: the Iwasawa main conjecture dictates that the zeros of ζ_p are determined by the arithmetic of $\mathbb{Q}(e^{2\pi i/p^\infty})$.

Kenkichi Iwasawa, Barry Mazur, Kenneth Ribet, and Andrew Wiles


Iwasawa


Ribet


Mazur


Wiles

Iwasawa formulated the main conjecture in the 1960s. Mazur and Wiles proved it in a paper published in 1980, building upon methods that Ribet instigated in a paper published in 1976.

p-adicity in modern number theory

Ways that p-adicity appears:

1. If a collection of mathematical objects is defined over $\mathbb{Q}$ or $\mathbb{Z}$, interpolate them p-adically.

2. If a mathematical object is defined over $\mathbb{Q}$ or $\mathbb{Z}$, use its behavior over $\mathbb{Q}_p$ (and $\mathbb{R}$) to gain insight into its behavior over $\mathbb{Q}$.

3. Build a mathematical object over $\mathbb{Z}_p$ by taking a limit over $\mathbb{Z}/p^n\mathbb{Z}$.

Thank you for your attention!

Feel free to reach out to me at carl.wang-erickson@pitt.edu!

Web: https://sites.pitt.edu/~caw203/