An ergodic approach to an equdistribution result of Ferrero–Washington

Bharathwaj Palvannan

Random Geometry colloquium

Tata Institute of Fundamental Research

November 2022

joint work with Jungwon Lee

Irregular primes

- $\zeta(s) := \sum_{m=1}^{\infty} \frac{1}{m^s}$ converges absolutely for $\mathrm{Re}(s) > 1$.
- $\zeta(s)$ has an analytic continuation to the whole complex plane, except a simple pole at $s = 1$.
- At negative odd integers, $\zeta(-n) = -\frac{B_{n+1}}{n+1}$.
- $\zeta(-11) = \frac{1}{12} \times \frac{691}{2 \times 3 \times 5 \times 7 \times 13}$.
- $\zeta(-31) = \frac{1}{32} \times \frac{37 \times 683 \times 305065927}{2 \times 3 \times 5 \times 17}$.
- (Kummer) The primes dividing these numerators are precisely the irregular primes.

Irregular primes

- $\zeta(s) := \sum_{m=1}^{\infty} \frac{1}{m^s}$ converges absolutely for $\mathrm{Re}(s) > 1$.
- $\zeta(s)$ has an analytic continuation to the whole complex plane, except a simple pole at $s = 1$.
- At negative odd integers, $\zeta(-n) = -\frac{B_{n+1}}{n+1}$.
- $\zeta(-11) = \frac{1}{12} \times \frac{691}{2 \times 3 \times 5 \times 7 \times 13}$.
- $\zeta(-31) = \frac{1}{32} \times \frac{37 \times 683 \times 305065927}{2 \times 3 \times 5 \times 17}$.
- (Kummer) The primes dividing these numerators are precisely the irregular primes.

Irregular primes

- $\zeta(s) := \sum_{m=1}^{\infty} \frac{1}{m^s}$ converges absolutely for $\mathrm{Re}(s) > 1$.
- $\zeta(s)$ has an analytic continuation to the whole complex plane, except a simple pole at $s = 1$.
- At negative odd integers, $\zeta(-n) = -\frac{B_{n+1}}{n+1}$.
- $\zeta(-11) = \frac{1}{12} \times \frac{691}{2 \times 3 \times 5 \times 7 \times 13}$.
- $\zeta(-31) = \frac{1}{32} \times \frac{37 \times 683 \times 305065927}{2 \times 3 \times 5 \times 17}$.
- (Kummer) The primes dividing these numerators are precisely the irregular primes.

Irregular primes

- $\zeta(s) := \sum_{m=1}^{\infty} \frac{1}{m^s}$ converges absolutely for $\mathrm{Re}(s) > 1$.
- $\zeta(s)$ has an analytic continuation to the whole complex plane, except a simple pole at $s = 1$.
- At negative odd integers, $\zeta(-n) = -\frac{B_{n+1}}{n+1}$.
- $\zeta(-11) = \frac{1}{12} \times \frac{691}{2 \times 3 \times 5 \times 7 \times 13}$.
- $\zeta(-31) = \frac{1}{32} \times \frac{37 \times 683 \times 305065927}{2 \times 3 \times 5 \times 17}$.
- (Kummer) The primes dividing these numerators are precisely the irregular primes.

Irregular primes

- $\zeta(s) := \sum_{m=1}^{\infty} \frac{1}{m^s}$ converges absolutely for $\mathrm{Re}(s) > 1$.
- $\zeta(s)$ has an analytic continuation to the whole complex plane, except a simple pole at $s = 1$.
- At negative odd integers, $\zeta(-n) = -\frac{B_{n+1}}{n+1}$.
- $\zeta(-11) = \frac{1}{12} \times \frac{691}{2 \times 3 \times 5 \times 7 \times 13}$.
- $\zeta(-31) = \frac{1}{32} \times \frac{37 \times 683 \times 305065927}{2 \times 3 \times 5 \times 17}$.
- (Kummer) The primes dividing these numerators are precisely the irregular primes.

Irregular primes

Let $F = \mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$.

- The class group of $\mathbb{Q}(\zeta_p)$ is a finite abelian group.
- This group measures the failure of unique factorization of $\mathbb{Z}[\zeta_p]$.
- A: p-primary part of the class group.
- p is *regular* if $|A| = 1$.
- p is *irregular* otherwise.

Theorem (Kummer, 1847)

If p is an odd regular prime, then

$$x^p + y^p = z^p$$

has no non-trivial integer solutions.

Irregular primes

Let $F = \mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$.

- The class group of $\mathbb{Q}(\zeta_p)$ is a finite abelian group.
- This group measures the failure of unique factorization of $\mathbb{Z}[\zeta_p]$.
- A: p-primary part of the class group.
- p is *regular* if $|A| = 1$.
- p is *irregular* otherwise.

Theorem (Kummer, 1847)

If p is an odd regular prime, then

$$x^p + y^p = z^p$$

has no non-trivial integer solutions.

Irregular primes

Let $F = \mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$.

- The class group of $\mathbb{Q}(\zeta_p)$ is a finite abelian group.
- This group measures the failure of unique factorization of $\mathbb{Z}[\zeta_p]$.
- A: p-primary part of the class group.
- p is *regular* if $|A| = 1$.
- p is *irregular* otherwise.

Theorem (Kummer, 1847)

If p is an odd regular prime, then

$$x^p + y^p = z^p$$

has no non-trivial integer solutions.

Irregular primes

Let $F = \mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$.

- The class group of $\mathbb{Q}(\zeta_p)$ is a finite abelian group.
- This group measures the failure of unique factorization of $\mathbb{Z}[\zeta_p]$.
- A: p-primary part of the class group.
- p is *regular* if $|A| = 1$.
- p is *irregular* otherwise.

Theorem (Kummer, 1847)

If p is an odd regular prime, then

$$x^p + y^p = z^p$$

has no non-trivial integer solutions.

Irregular primes

Let $F = \mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$.

- The class group of $\mathbb{Q}(\zeta_p)$ is a finite abelian group.
- This group measures the failure of unique factorization of $\mathbb{Z}[\zeta_p]$.
- A: p-primary part of the class group.
- p is *regular* if $|A| = 1$.
- p is *irregular* otherwise.

Theorem (Kummer, 1847)

If p is an odd regular prime, then

$$x^p + y^p = z^p$$

has no non-trivial integer solutions.

Irregular primes

Let $F = \mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$.

- The class group of $\mathbb{Q}(\zeta_p)$ is a finite abelian group.
- This group measures the failure of unique factorization of $\mathbb{Z}[\zeta_p]$.
- A: p-primary part of the class group.
- p is *regular* if $|A| = 1$.
- p is *irregular* otherwise.

Theorem (Kummer, 1847)

If p is an odd regular prime, then

$$x^p + y^p = z^p$$

has no non-trivial integer solutions.

Irregular primes

Let $F = \mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$.

- The class group of $\mathbb{Q}(\zeta_p)$ is a finite abelian group.
- This group measures the failure of unique factorization of $\mathbb{Z}[\zeta_p]$.
- A: p-primary part of the class group.
- p is *regular* if $|A| = 1$.
- p is *irregular* otherwise.

Theorem (Kummer, 1847)

If p is an odd regular prime, then

$$x^p + y^p = z^p$$

has no non-trivial integer solutions.

Values of ζ at negative odd integers

$-n+1$	$\zeta(-n+1) = -\frac{B_n}{n}$	$-n+1$	$\zeta(-n+1) = -\frac{B_n}{n}$
-1	$\frac{-1}{2} \times \frac{1}{2\times 3},$	-3	$\frac{1}{4} \times \frac{1}{2\times 3\times 5},$
-5	$\frac{-1}{6} \times \frac{1}{2\times 3\times 7},$	-7	$\frac{1}{8} \times \frac{1}{2\times 3\times 5}$
-9	$\frac{-1}{2} \times \frac{1}{2\times 3\times 11}$	-11	$\frac{1}{12} \times \frac{691}{2\times 3\times 5\times 7\times 13}$
-13	$\frac{-1}{2} \times \frac{1}{2\times 3}$	-15	$\frac{1}{16} \times \frac{3617}{2\times 3\times 5\times 17}$

Values of ζ at negative odd integers

$-n+1$	$\zeta(-n+1) = -\frac{B_n}{n}$	$-n+1$	$\zeta(-n+1) = -\frac{B_n}{n}$
-17	$\frac{-1}{18} \times \frac{43867}{2\times3\times7\times19}$,	-19	$\frac{1}{20} \times \frac{283\times617}{2\times3\times5\times11}$,
-21	$\frac{-1}{2} \times \frac{131\times593}{2\times3\times23}$,	-23	$\frac{1}{24} \times \frac{103\times2294797}{2\times3\times5\times7\times13}$
-25	$\frac{-1}{2} \times \frac{657931}{2\times3}$	-27	$\frac{1}{4} \times \frac{9349\times362903}{2\times3\times5\times29}$
-29	$\frac{1}{6} \times \frac{1721\times1001259881}{2\times3\times7\times11\times31}$	-31	$\frac{1}{22} \times \frac{-37\times683\times305065927}{2\times3\times5\times17}$

Open questions

- What's known?

  There are infinitely many irregular primes.

- What's not known?

  Are there infinitely many regular primes?

- What's known? There's a periodicity in these mod p values

  (Kummer congruences) .

- Siegel's heuristic is that as $p \to \infty$, the $(p-3)/2$ values

$$\zeta(-1) \qquad \zeta(-3) \qquad \zeta(-5) \qquad \cdots \qquad \zeta(4-p).$$

  are "uniformly distributed" modulo p.

- If you believe Siegel's heuristic then, as $p \to \infty$, the probability that none of these values are 0 modulo p should be $e^{-1/2}$.

- (Open question)

  Are 60.65% of all primes regular?

Open questions

- What's known?

  There are infinitely many irregular primes.

- What's not known?

  Are there infinitely many regular primes?

- What's known? There's a periodicity in these mod p values

  (Kummer congruences) .

- Siegel's heuristic is that as $p \to \infty$, the $(p-3)/2$ values

$$\zeta(-1) \qquad \zeta(-3) \qquad \zeta(-5) \qquad \cdots \qquad \zeta(4-p).$$

  are "uniformly distributed" modulo p.

- If you believe Siegel's heuristic then, as $p \to \infty$, the probability that none of these values are 0 modulo p should be $e^{-1/2}$.

- (Open question)

  Are 60.65% of all primes regular?

Open questions

- What's known?

  There are infinitely many irregular primes.
- What's not known?

  Are there infinitely many regular primes?
- What's known? There's a periodicity in these mod p values

  (Kummer congruences) .
- Siegel's heuristic is that as $p \to \infty$, the $(p-3)/2$ values

$$\zeta(-1) \qquad \zeta(-3) \qquad \zeta(-5) \qquad \cdots \qquad \zeta(4-p).$$

  are "uniformly distributed" modulo p.
- If you believe Siegel's heuristic then, as $p \to \infty$, the probability that none of these values are 0 modulo p should be $e^{-1/2}$.
- (Open question)

  Are 60.65% of all primes regular?

Open questions

- What's known?

  There are infinitely many irregular primes.

- What's not known?

  Are there infinitely many regular primes?

- What's known? There's a periodicity in these mod p values

  (Kummer congruences) .

- Siegel's heuristic is that as $p \to \infty$, the $(p-3)/2$ values

$$\zeta(-1) \qquad \zeta(-3) \qquad \zeta(-5) \qquad \cdots \qquad \zeta(4-p).$$

  are "uniformly distributed" modulo p.

- If you believe Siegel's heuristic then, as $p \to \infty$, the probability that none of these values are 0 modulo p should be $e^{-1/2}$.
- (Open question)

  Are 60.65% of all primes regular?

Open questions

- What's known?

  There are infinitely many irregular primes.
- What's not known?

  Are there infinitely many regular primes?
- What's known? There's a periodicity in these mod p values

  (Kummer congruences) .
- Siegel's heuristic is that as $p \to \infty$, the $(p-3)/2$ values

$$\zeta(-1) \qquad \zeta(-3) \qquad \zeta(-5) \qquad \cdots \qquad \zeta(4-p).$$

  are "uniformly distributed" modulo p.
- If you believe Siegel's heuristic then, as $p \to \infty$, the probability that none of these values are 0 modulo p should be $e^{-1/2}$.
- (Open question)

  Are 60.65% of all primes regular?

Open questions

- What's known?

  There are infinitely many irregular primes.
- What's not known?

  Are there infinitely many regular primes?
- What's known? There's a periodicity in these mod p values

  (Kummer congruences) .
- Siegel's heuristic is that as $p \to \infty$, the $(p-3)/2$ values

$$\zeta(-1) \qquad \zeta(-3) \qquad \zeta(-5) \qquad \cdots \qquad \zeta(4-p).$$

  are "uniformly distributed" modulo p.
- If you believe Siegel's heuristic then, as $p \to \infty$, the probability that none of these values are 0 modulo p should be $e^{-1/2}$.
- (Open question)

  Are 60.65% of all primes regular?

Open questions

e.g. $p = 691$ divides

$$\zeta(1-12) \qquad \zeta(1-200)$$

- (open) In general, is the probability that p divides r such values equal to

$$e^{-1/2}\frac{(1/2)^r}{r!}?$$

Open questions

e.g. $p = 691$ divides

$$\zeta(1-12) \qquad \zeta(1-200)$$

- (open) In general, is the probability that p divides r such values equal to
$$e^{-1/2}\frac{(1/2)^r}{r!}?$$

Iwasawa invariants

- Let p be an odd prime number.

Consider the tower of field extensions

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \mathbb{Q}(\zeta_{p^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \bigcup \mathbb{Q}(\zeta_{p^n})$$

- A_n : the p-primary part of the class group of $\mathbb{Q}(\zeta_{p^n})$.
- Consider the mod-p cyclotomic character:

$$\omega : \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

- $A_{n,i}$: the ω^i- eigencomponent of A_n, for $0 \le i \le p-2$.

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

Iwasawa invariants

- Let p be an odd prime number.

Consider the tower of field extensions

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \mathbb{Q}(\zeta_{p^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \bigcup \mathbb{Q}(\zeta_{p^n})$$

- A_n : the p-primary part of the class group of $\mathbb{Q}(\zeta_{p^n})$.
- Consider the mod-p cyclotomic character:

$$\omega : \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

- $A_{n,i}$: the ω^i- eigencomponent of A_n, for $0 \le i \le p-2$.

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

Iwasawa invariants

- Let p be an odd prime number.

Consider the tower of field extensions

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \mathbb{Q}(\zeta_{p^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \bigcup \mathbb{Q}(\zeta_{p^n})$$

- A_n : the p-primary part of the class group of $\mathbb{Q}(\zeta_{p^n})$.
- Consider the mod-p cyclotomic character:

$$\omega : \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

- $A_{n,i}$: the ω^i- eigencomponent of A_n, for $0 \le i \le p-2$.

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

Iwasawa invariants

- Let p be an odd prime number.

Consider the tower of field extensions

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \mathbb{Q}(\zeta_{p^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \bigcup \mathbb{Q}(\zeta_{p^n})$$

- A_n : the p-primary part of the class group of $\mathbb{Q}(\zeta_{p^n})$.
- Consider the mod-p cyclotomic character:

$$\omega : \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

- $A_{n,i}$: the ω^i- eigencomponent of A_n, for $0 \le i \le p-2$.

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

Iwasawa invariants

- Let p be an odd prime number.

Consider the tower of field extensions

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \mathbb{Q}(\zeta_{p^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \bigcup \mathbb{Q}(\zeta_{p^n})$$

- A_n : the p-primary part of the class group of $\mathbb{Q}(\zeta_{p^n})$.
- Consider the mod-p cyclotomic character:

$$\omega : \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

- $A_{n,i}$: the ω^i- eigencomponent of A_n, for $0 \leq i \leq p-2$.

Theorem (Iwasawa)

Fix $0 \leq i \leq p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

Iwasawa invariants

- Let p be an odd prime number.

Consider the tower of field extensions

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \mathbb{Q}(\zeta_{p^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \bigcup \mathbb{Q}(\zeta_{p^n})$$

- A_n : the p-primary part of the class group of $\mathbb{Q}(\zeta_{p^n})$.
- Consider the mod-p cyclotomic character:

$$\omega : \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

- $A_{n,i}$: the ω^i- eigencomponent of A_n, for $0 \leq i \leq p-2$.

Theorem (Iwasawa)

Fix $0 \leq i \leq p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

Iwasawa's $\mu = 0$ conjecture

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

A Conjecture of Iwasawa, now a theorem of Ferrero–Washington, Sinnott

For all $0 \le i \le p-2$,

$$\mu_i = 0.$$

Remarks:

- Iwawsawa's theorem and conjecture are much more general. He states his conjecture for the cyclotomic $\mathbb{Z}_p$-extension of any number field. This conjecture is wide open.
- In the abelian case, one can consider more generally a tame level N:

$$\mathbb{Q}(\zeta_{Np}) \subset \mathbb{Q}(\zeta_{Np^2}) \subset \cdots \mathbb{Q}(\zeta_{Np^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{Np^\infty}) := \bigcup \mathbb{Q}(\zeta_{Np^n})$$

However, we prefer to fix the tame level N to be 1.

Iwasawa's $\mu = 0$ conjecture

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

A Conjecture of Iwasawa, now a theorem of Ferrero–Washington, Sinnott

For all $0 \le i \le p-2$,

$$\mu_i = 0.$$

Remarks:

- Iwawsawa's theorem and conjecture are much more general. He states his conjecture for the cyclotomic $\mathbb{Z}_p$-extension of any number field. This conjecture is wide open.
- In the abelian case, one can consider more generally a tame level N:

$$\mathbb{Q}(\zeta_{Np}) \subset \mathbb{Q}(\zeta_{Np^2}) \subset \cdots \mathbb{Q}(\zeta_{Np^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{Np^\infty}) := \bigcup \mathbb{Q}(\zeta_{Np^n})$$

However, we prefer to fix the tame level N to be 1.

Iwasawa's $\mu = 0$ conjecture

Theorem (Iwasawa)

Fix $0 \leq i \leq p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

A Conjecture of Iwasawa, now a theorem of Ferrero–Washington, Sinnott

For all $0 \leq i \leq p-2$,

$$\mu_i = 0.$$

Remarks:

- Iwawsawa's theorem and conjecture are much more general. He states his conjecture for the cyclotomic $\mathbb{Z}_p$-extension of any number field. This conjecture is wide open.
- In the abelian case, one can consider more generally a tame level N:

$$\mathbb{Q}(\zeta_{Np}) \subset \mathbb{Q}(\zeta_{Np^2}) \subset \cdots \mathbb{Q}(\zeta_{Np^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{Np^\infty}) := \bigcup \mathbb{Q}(\zeta_{Np^n})$$

However, we prefer to fix the tame level N to be 1.

Iwasawa's $\mu = 0$ conjecture

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

A Conjecture of Iwasawa, now a theorem of Ferrero–Washington, Sinnott

For all $0 \le i \le p-2$,

$$\mu_i = 0.$$

Remarks:

- Iwawsawa's theorem and conjecture are much more general. He states his conjecture for the cyclotomic $\mathbb{Z}_p$-extension of any number field. This conjecture is wide open.
- In the abelian case, one can consider more generally a tame level N:

$$\mathbb{Q}(\zeta_{Np}) \subset \mathbb{Q}(\zeta_{Np^2}) \subset \cdots \mathbb{Q}(\zeta_{Np^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{Np^\infty}) := \bigcup \mathbb{Q}(\zeta_{Np^n})$$

However, we prefer to fix the tame level N to be 1.

Iwasawa's $\mu = 0$ conjecture

Theorem (Iwasawa)

Fix $0 \le i \le p-2$.

$$|A_{n,i}| = p^{\lambda_i n + p^{\mu_i n} + \nu_i}, \qquad \forall n \gg 0.$$

A Conjecture of Iwasawa, now a theorem of Ferrero–Washington, Sinnott

For all $0 \le i \le p-2$,

$$\mu_i = 0.$$

Remarks:

- Iwawsawa's theorem and conjecture are much more general. He states his conjecture for the cyclotomic $\mathbb{Z}_p$-extension of any number field. This conjecture is wide open.
- In the abelian case, one can consider more generally a tame level N:

$$\mathbb{Q}(\zeta_{Np}) \subset \mathbb{Q}(\zeta_{Np^2}) \subset \cdots \mathbb{Q}(\zeta_{Np^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{Np^\infty}) := \bigcup \mathbb{Q}(\zeta_{Np^n})$$

However, we prefer to fix the tame level N to be 1.

Iwasawa algebra

- Let $G_n := \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)\right)$.

$$\mathbb{Z}_p[[T]] \xrightarrow{\cong} \mathbb{Z}_p[[G_\infty]] \cong \varprojlim_n \mathbb{Z}_p[G_n]$$

$$T+1 \leftrightarrow \gamma_0.$$

$$f(T) = p^\mu g(T) u(T).$$

- (**Weierstrass preparation theorem**) The λ_i and μ_i-invariants can also be gleaned from the characteristic power series $f_i(T)$ of an Iwasawa module.
- $\mu_i > 0$ iff p divides each coefficient of the power series $f_i(T)$.
- Via the isomorphism above, each element $f_i(T)$ can be viewed as a sequence of compatible elements $\theta_{i,n}$ in the group rings $\mathbb{Z}_p[G_n]$'s.
- $\mu_i > 0$ iff p divides each coefficient of the group ring element $\theta_{i,n}, \forall n$.
- $\mu_i > 0$ iff the image of $\theta_{i,n}$ in $\mathbb{F}_p[G_n]$ under the map $\mathbb{Z}_p[G_n] \to \mathbb{F}_p[G_n]$ equals zero.

Iwasawa algebra

- Let $G_n \coloneqq \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)\right)$.

$$\mathbb{Z}_p[[T]] \xrightarrow{\cong} \mathbb{Z}_p[[G_\infty]] \cong \varprojlim_n \mathbb{Z}_p[G_n]$$

$$T+1 \leftrightarrow \gamma_0.$$

$$f(T) = p^\mu g(T) u(T).$$

- (**Weierstrass preparation theorem**) The λ_i and μ_i-invariants can also be gleaned from the characteristic power series $f_i(T)$ of an Iwasawa module.
- $\mu_i > 0$ iff p divides each coefficient of the power series $f_i(T)$.
- Via the isomorphism above, each element $f_i(T)$ can be viewed as a sequence of compatible elements $\theta_{i,n}$ in the group rings $\mathbb{Z}_p[G_n]$'s.
- $\mu_i > 0$ iff p divides each coefficient of the group ring element $\theta_{i,n}, \forall n$.
- $\mu_i > 0$ iff the image of $\theta_{i,n}$ in $\mathbb{F}_p[G_n]$ under the map $\mathbb{Z}_p[G_n] \to \mathbb{F}_p[G_n]$ equals zero.

Iwasawa algebra

- Let $G_n := \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)\right)$.

$$\mathbb{Z}_p[[T]] \xrightarrow{\cong} \mathbb{Z}_p[[G_\infty]] \cong \varprojlim_n \mathbb{Z}_p[G_n]$$

$$T + 1 \leftrightarrow \gamma_0.$$

$$f(T) = p^\mu g(T) u(T).$$

- (**Weierstrass preparation theorem**) The λ_i and μ_i-invariants can also be gleaned from the characteristic power series $f_i(T)$ of an Iwasawa module.
- $\mu_i > 0$ iff p divides each coefficient of the power series $f_i(T)$.
- Via the isomorphism above, each element $f_i(T)$ can be viewed as a sequence of compatible elements $\theta_{i,n}$ in the group rings $\mathbb{Z}_p[G_n]$'s.
- $\mu_i > 0$ iff p divides each coefficient of the group ring element $\theta_{i,n}, \forall n$.
- $\mu_i > 0$ iff the image of $\theta_{i,n}$ in $\mathbb{F}_p[G_n]$ under the map $\mathbb{Z}_p[G_n] \to \mathbb{F}_p[G_n]$ equals zero.

Iwasawa algebra

- Let $G_n := \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)\right)$.

$$\mathbb{Z}_p[[T]] \xrightarrow{\cong} \mathbb{Z}_p[[G_\infty]] \cong \varprojlim_n \mathbb{Z}_p[G_n]$$

$$T+1 \leftrightarrow \gamma_0.$$

$$f(T) = p^\mu g(T) u(T).$$

- (**Weierstrass preparation theorem**) The λ_i and μ_i-invariants can also be gleaned from the characteristic power series $f_i(T)$ of an Iwasawa module.
- $\mu_i > 0$ iff p divides each coefficient of the power series $f_i(T)$.
- Via the isomorphism above, each element $f_i(T)$ can be viewed as a sequence of compatible elements $\theta_{i,n}$ in the group rings $\mathbb{Z}_p[G_n]$'s.
- $\mu_i > 0$ iff p divides each coefficient of the group ring element $\theta_{i,n}, \forall n$.
- $\mu_i > 0$ iff the image of $\theta_{i,n}$ in $\mathbb{F}_p[G_n]$ under the map $\mathbb{Z}_p[G_n] \to \mathbb{F}_p[G_n]$ equals zero.

Iwasawa algebra

- Let $G_n \coloneqq \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)\right)$.

$$\mathbb{Z}_p[[T]] \xrightarrow{\cong} \mathbb{Z}_p[[G_\infty]] \cong \varprojlim_n \mathbb{Z}_p[G_n]$$

$$T + 1 \leftrightarrow \gamma_0.$$

$$f(T) = p^\mu g(T) u(T).$$

- (**Weierstrass preparation theorem**) The λ_i and μ_i-invariants can also be gleaned from the characteristic power series $f_i(T)$ of an Iwasawa module.
- $\mu_i > 0$ iff p divides each coefficient of the power series $f_i(T)$.
- Via the isomorphism above, each element $f_i(T)$ can be viewed as a sequence of compatible elements $\theta_{i,n}$ in the group rings $\mathbb{Z}_p[G_n]$'s.
- $\mu_i > 0$ iff p divides each coefficient of the group ring element $\theta_{i,n}, \forall n$.
- $\mu_i > 0$ iff the image of $\theta_{i,n}$ in $\mathbb{F}_p[G_n]$ under the map $\mathbb{Z}_p[G_n] \to \mathbb{F}_p[G_n]$ equals zero.

p-adic expansions and digits

- For every α in $\mathbb{Z}_p$, we can consider its p-adic expansion:

$$\alpha = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_n(\alpha)p^n + t_{n+1}(\alpha)p^{n+1} + \cdots,$$

  Here, the digits $t_n(\alpha)$'s belong to the set $\{0, 1, 2, \cdots, p-1\}$.

- Consider its associated partial sums for each $n \geq 1$:

$$s_{n-1}(\alpha) = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_{n-1}(\alpha)p^{n-1}.$$

  Notice that the element $\dfrac{s_{n-1}(\alpha)}{p^n}$ always belongs to the interval $[0, 1)$.

p-adic expansions and digits

- For every α in $\mathbb{Z}_p$, we can consider its p-adic expansion:

$$\alpha = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_n(\alpha)p^n + t_{n+1}(\alpha)p^{n+1} + \cdots,$$

  Here, the digits $t_n(\alpha)$'s belong to the set $\{0, 1, 2, \cdots, p-1\}$.

- Consider its associated partial sums for each $n \geq 1$:

$$s_{n-1}(\alpha) = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_{n-1}(\alpha)p^{n-1}.$$

  Notice that the element $\dfrac{s_{n-1}(\alpha)}{p^n}$ always belongs to the interval $[0, 1)$.

p-adic expansions and digits

- For every α in $\mathbb{Z}_p$, we can consider its p-adic expansion:

$$\alpha = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_n(\alpha)p^n + t_{n+1}(\alpha)p^{n+1} + \cdots,$$

Here, the digits $t_n(\alpha)$'s belong to the set $\{0, 1, 2, \cdots, p-1\}$.

- Consider its associated partial sums for each $n \geq 1$:

$$s_{n-1}(\alpha) = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_{n-1}(\alpha)p^{n-1}.$$

Notice that the element $\dfrac{s_{n-1}(\alpha)}{p^n}$ always belongs to the interval $[0, 1)$.

p-adic expansions and digits

- For every α in $\mathbb{Z}_p$, we can consider its p-adic expansion:

$$\alpha = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_n(\alpha)p^n + t_{n+1}(\alpha)p^{n+1} + \cdots,$$

  Here, the digits $t_n(\alpha)$'s belong to the set $\{0, 1, 2, \cdots, p-1\}$.

- Consider its associated partial sums for each $n \geq 1$:

$$s_{n-1}(\alpha) = t_0(\alpha) + t_1(\alpha)p^1 + t_2(\alpha)p^2 + \cdots + t_{n-1}(\alpha)p^{n-1}.$$

  Notice that the element $\dfrac{s_{n-1}(\alpha)}{p^n}$ always belongs to the interval $[0, 1)$.

Stickelberger elements

- Write
$$\Delta := \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$
$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times,$$
$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong G_n \times \Delta.$$
- We can identify Δ with the $(p-1)^{\mathrm{st}}$ roots of unity.
- We can identify G_n with the 1-units of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
- The Stickelberger element annihilates the minus part of the class group.
$$\sum_{\substack{u=1 \\ u\equiv 1 \bmod p}}^{p^n} \left(\sum_{\eta^{p-1}=1} \frac{s_{n-1}(u\eta)}{p^n} \sigma_\eta^{-1} \right) \sigma_u^{-1} \qquad \in \mathbb{Q}[\Delta][G_n]$$
- **Remark**: A compatible system of Stickelberger elements can be used to construct Kubota–Leopoldt p-adic L-functions.

Stickelberger elements

- Write

$$\Delta := \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times,$$
$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong G_n \times \Delta.$$

- We can identify Δ with the $(p-1)^{\mathrm{st}}$ roots of unity.
- We can identify G_n with the 1-units of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
- The Stickelberger element annihilates the minus part of the class group.

$$\sum_{\substack{u=1 \\ u\equiv 1 \bmod p}}^{p^n} \left(\sum_{\eta^{p-1}=1} \frac{s_{n-1}(u\eta)}{p^n}\, \sigma_\eta^{-1} \right) \sigma_u^{-1} \qquad \in \mathbb{Q}[\Delta][G_n]$$

- **Remark**: A compatible system of Stickelberger elements can be used to construct Kubota–Leopoldt p-adic L-functions.

Stickelberger elements

- Write

$$\Delta := \mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\big) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times,$$
$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\big) \cong G_n \times \Delta.$$

- We can identify Δ with the $(p-1)^{\text{st}}$ roots of unity.
- We can identify G_n with the 1-units of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
- The Stickelberger element annihilates the minus part of the class group.

$$\sum_{\substack{u=1\\ u\equiv 1 \bmod p}}^{p^n} \left(\sum_{\eta^{p-1}=1} \frac{s_{n-1}(u\eta)}{p^n}\, \sigma_\eta^{-1} \right) \sigma_u^{-1} \qquad \in \mathbb{Q}[\Delta][G_n]$$

- **Remark**: A compatible system of Stickelberger elements can be used to construct Kubota–Leopoldt p-adic L-functions.

Stickelberger elements

- Write
$$\Delta := \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$
$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times,$$
$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong G_n \times \Delta.$$
- We can identify Δ with the $(p-1)^{\text{st}}$ roots of unity.
- We can identify G_n with the 1-units of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
- The Stickelberger element annihilates the minus part of the class group.
$$\sum_{\substack{u=1 \\ u\equiv 1 \bmod p}}^{p^n} \left(\sum_{\eta^{p-1}=1} \frac{s_{n-1}(u\eta)}{p^n}\, \sigma_\eta^{-1} \right) \sigma_u^{-1} \qquad \in \mathbb{Q}[\Delta][G_n]$$
- **Remark**: A compatible system of Stickelberger elements can be used to construct Kubota–Leopoldt p-adic L-functions.

Stickelberger elements

- Write

$$\Delta := \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$

$$\begin{aligned}\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) &\cong (\mathbb{Z}/p^n\mathbb{Z})^\times,\\ \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) &\cong G_n \times \Delta.\end{aligned}$$

- We can identify Δ with the $(p-1)^{\mathrm{st}}$ roots of unity.
- We can identify G_n with the 1-units of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
- The Stickelberger element annihilates the minus part of the class group.

$$\sum_{\substack{u=1\\ u\equiv 1 \bmod p}}^{p^n} \left(\sum_{\eta^{p-1}=1} \frac{s_{n-1}(u\eta)}{p^n}\, \sigma_\eta^{-1} \right) \sigma_u^{-1} \qquad \in\ \mathbb{Q}[\Delta][G_n]$$

- **Remark**: A compatible system of Stickelberger elements can be used to construct Kubota–Leopoldt p-adic L-functions.

Stickelberger elements

- Write
$$\Delta := \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times.$$
$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times,$$
$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \cong G_n \times \Delta.$$
- We can identify Δ with the $(p-1)^{\mathrm{st}}$ roots of unity.
- We can identify G_n with the 1-units of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
- The Stickelberger element annihilates the minus part of the class group.
$$\sum_{\substack{u=1 \\ u\equiv 1 \bmod p}}^{p^n} \left(\sum_{\eta^{p-1}=1} \frac{s_{n-1}(u\eta)}{p^n}\, \sigma_\eta^{-1} \right) \sigma_u^{-1} \qquad \in \mathbb{Q}[\Delta][G_n]$$
- **Remark**: A compatible system of Stickelberger elements can be used to construct Kubota–Leopoldt p-adic L-functions.

Iwasawa's criterion

Proposition [Iwasawa, Ferrero–Washington]

The following statements are equivalent:

1. $\mu_i > 0$ for some $0 \le i \le p-2$.
2. There exists an odd integer $3 \le d \le p-2$ such that for all $n \ge 0$ and $\alpha \in \mathbb{Z}_p$, we have

$$\sum_{\eta^{p-1}=1} t_n(\alpha\eta)\eta^d \equiv 0 \pmod{p}. \tag{1}$$

- The restriction to the odd integers comes from an application of the reflection theorem.

Iwasawa's criterion

Proposition [Iwasawa, Ferrero–Washington]

The following statements are equivalent:

1. $\mu_i > 0$ for some $0 \le i \le p-2$.
2. There exists an odd integer $3 \le d \le p-2$ such that for all $n \ge 0$ and $\alpha \in \mathbb{Z}_p$, we have

$$\sum_{\eta^{p-1}=1} t_n(\alpha\eta)\eta^d \equiv 0 \pmod{p}. \tag{1}$$

- The restriction to the odd integers comes from an application of the reflection theorem.

Iwasawa's criterion

Proposition [Iwasawa, Ferrero–Washington]

The following statements are equivalent:

1. $\mu_i > 0$ for some $0 \le i \le p-2$.
2. There exists an odd integer $3 \le d \le p-2$ such that for all $n \ge 0$ and $\alpha \in \mathbb{Z}_p$, we have

$$\sum_{\eta^{p-1}=1} t_n(\alpha\eta)\eta^d \equiv 0 \pmod{p}. \tag{1}$$

- The restriction to the odd integers comes from an application of the reflection theorem.

Equidistribution result of Ferrero–Washington

- Let $\{\beta_1, \cdots, \beta_r\} \subset \mathbb{Z}_p$ be a linearly independent set over $\mathbb{Q}$.
- Let G_r be the set of all α in $\mathbb{Z}_p$ such that

$$\left\{ \left(\frac{s_{n-1}(\alpha\beta_1)}{p^n}, \dots, \frac{s_{n-1}(\alpha\beta_r)}{p^n} \right) \right\}_{n=0}^{\infty}$$

is equidistributed in $[0,1]^r$ with respect to the standard Borel measure.

Proposition [Ferrero–Washington]

G_r has full Haar measure in $\mathbb{Z}_p$.

- Ferrero–Washington apply this proposition to a linearly independent set of $(p-1)^{\text{st}}$ roots of unity.
- Ferrero–Washington use the Weyl criterion on $[0,1]^r$.

Equidistribution result of Ferrero–Washington

- Let $\{\beta_1, \cdots, \beta_r\} \subset \mathbb{Z}_p$ be a linearly independent set over $\mathbb{Q}$.
- Let G_r be the set of all α in $\mathbb{Z}_p$ such that

$$\left\{ \left(\frac{s_{n-1}(\alpha\beta_1)}{p^n}, \cdots, \frac{s_{n-1}(\alpha\beta_r)}{p^n} \right) \right\}_{n=0}^{\infty}$$

is equidistributed in $[0,1]^r$ with respect to the standard Borel measure.

Proposition [Ferrero–Washington]

G_r has full Haar measure in $\mathbb{Z}_p$.

- Ferrero–Washington apply this proposition to a linearly independent set of $(p-1)^{\text{st}}$ roots of unity.
- Ferrero–Washington use the Weyl criterion on $[0,1]^r$.

Equidistribution result of Ferrero–Washington

- Let $\{\beta_1, \cdots, \beta_r\} \subset \mathbb{Z}_p$ be a linearly independent set over $\mathbb{Q}$.
- Let G_r be the set of all α in $\mathbb{Z}_p$ such that

$$\left\{ \left(\frac{s_{n-1}(\alpha\beta_1)}{p^n}, \cdots, \frac{s_{n-1}(\alpha\beta_r)}{p^n} \right) \right\}_{n=0}^{\infty}$$

is equidistributed in $[0,1]^r$ with respect to the standard Borel measure.

Proposition [Ferrero–Washington]

G_r has full Haar measure in $\mathbb{Z}_p$.

- Ferrero–Washington apply this proposition to a linearly independent set of $(p-1)^{\text{st}}$ roots of unity.
- Ferrero–Washington use the Weyl criterion on $[0,1]^r$.

Equidistribution result of Ferrero–Washington

- Let $\{\beta_1, \cdots, \beta_r\} \subset \mathbb{Z}_p$ be a linearly independent set over $\mathbb{Q}$.
- Let G_r be the set of all α in $\mathbb{Z}_p$ such that

$$\left\{ \left(\frac{s_{n-1}(\alpha\beta_1)}{p^n}, \cdots, \frac{s_{n-1}(\alpha\beta_r)}{p^n} \right) \right\}_{n=0}^{\infty}$$

is equidistributed in $[0,1]^r$ with respect to the standard Borel measure.

Proposition [Ferrero–Washington]

G_r has full Haar measure in $\mathbb{Z}_p$.

- Ferrero–Washington apply this proposition to a linearly independent set of $(p-1)^{\text{st}}$ roots of unity.
- Ferrero–Washington use the Weyl criterion on $[0,1]^r$.

Equidistribution result of Ferrero–Washington

- Let $\{\beta_1, \cdots, \beta_r\} \subset \mathbb{Z}_p$ be a linearly independent set over $\mathbb{Q}$.
- Let G_r be the set of all α in $\mathbb{Z}_p$ such that

$$\left\{ \left(\frac{s_{n-1}(\alpha\beta_1)}{p^n}, \cdots, \frac{s_{n-1}(\alpha\beta_r)}{p^n} \right) \right\}_{n=0}^{\infty}$$

is equidistributed in $[0,1]^r$ with respect to the standard Borel measure.

Proposition [Ferrero–Washington]

G_r has full Haar measure in $\mathbb{Z}_p$.

- Ferrero–Washington apply this proposition to a linearly independent set of $(p-1)^{\text{st}}$ roots of unity.
- Ferrero–Washington use the Weyl criterion on $[0,1]^r$.

Ergodic preliminaries: Equidistribution

- Let X be a compact topological space.
- Let ν be a probability measure on the Borel sigma algebra of X.
- A sequence $\{x_n\}$ in X is said to be equidistributed if for all continuous functions $f : X \to \mathbb{R}$, we have

$$\lim_{M\to\infty} \frac{1}{M} \sum_{n=1}^{M} f(x_n) = \int_X f \, d\nu.$$

- Equidistribution is a property that involves an interplay between the topological and measure theoretic properties of a space.

Ergodic preliminaries: Equidistribution

- Let X be a compact topological space.
- Let ν be a probability measure on the Borel sigma algebra of X.
- A sequence $\{x_n\}$ in X is said to be equidistributed if for all continuous functions $f : X \to \mathbb{R}$, we have

$$\lim_{M\to\infty} \frac{1}{M} \sum_{n=1}^{M} f(x_n) = \int_X f \, d\nu.$$

- Equidistribution is a property that involves an interplay between the topological and measure theoretic properties of a space.

Ergodic preliminaries: Equidistribution

- Let X be a compact topological space.
- Let ν be a probability measure on the Borel sigma algebra of X.
- A sequence $\{x_n\}$ in X is said to be equidistributed if for all continuous functions $f : X \to \mathbb{R}$, we have

$$\lim_{M\to\infty} \frac{1}{M} \sum_{n=1}^{M} f(x_n) = \int_X f \, d\nu.$$

- Equidistribution is a property that involves an interplay between the topological and measure theoretic properties of a space.

Ergodic preliminaries: Equidistribution

- Let X be a compact topological space.
- Let ν be a probability measure on the Borel sigma algebra of X.
- A sequence $\{x_n\}$ in X is said to be equidistributed if for all continuous functions $f : X \to \mathbb{R}$, we have

$$\lim_{M\to\infty} \frac{1}{M} \sum_{n=1}^{M} f(x_n) = \int_X f \, d\nu.$$

- Equidistribution is a property that involves an interplay between the topological and measure theoretic properties of a space.

Ergodic preliminaries: Weyl criterion

Weyl criterion

The following statements are equivalent:

1. A sequence $\{\vec{x}_n\}$ is equidistributed in $[0,1]^r$.
2. For every non-zero vector $\vec{v}$ in $\mathbb{Z}^r$, we have

$$\lim_{M\to\infty} \frac{1}{M} \sum_{n=1}^{M} \exp(2\pi i \vec{v}\cdot\vec{x}_n) = 0.$$

- These exponential functions are called test functions.

Ergodic preliminaries: Weyl criterion

Weyl criterion

The following statements are equivalent:

1. A sequence $\{\vec{x}_n\}$ is equidistributed in $[0,1]^r$.
2. For every non-zero vector $\vec{v}$ in $\mathbb{Z}^r$, we have

$$\lim_{M\to\infty} \frac{1}{M} \sum_{n=1}^{M} \exp(2\pi i\, \vec{v}\cdot\vec{x}_n) = 0.$$

- These exponential functions are called test functions.

Ergodic preliminaries: Weyl criterion

Weyl criterion

The following statements are equivalent:

1. A sequence $\{\vec{x}_n\}$ is equidistributed in $[0,1]^r$.
2. For every non-zero vector $\vec{v}$ in $\mathbb{Z}^r$, we have

$$\lim_{M\to\infty} \frac{1}{M} \sum_{n=1}^{M} \exp(2\pi i \vec{v} \cdot \vec{x}_n) = 0.$$

- These exponential functions are called test functions.

Ergodic preliminaries: ergodic map

- We will consider a **dynamical system** (X, T, ν).
  - We have a self-map
    $$T : X \to X$$
    measurable wrt ν.
  - ν is a T-invariant measure, that is, for all Borel measurable sets B:
    $$\nu(B) = \nu\left(T^{-1}(B)\right).$$
- The map T is said to be ergodic if for all Borel measurable sets B, we have
  $$T^{-1}(B) = B \implies \nu(B) = 1, \text{ or } \nu(B) = 0.$$
- A point x is said to be a **generic point** for (X, T, ν) if the orbit $\left\{T^{[n]}(x)\right\}$ is equidistributed.

Ergodic preliminaries: ergodic map

- We will consider a **dynamical system** (X, T, ν).
  - We have a self-map
    $$T : X \to X$$
    measurable wrt ν.
  - ν is a T-invariant measure, that is, for all Borel measurable sets B:
    $$\nu(B) = \nu\left(T^{-1}(B)\right).$$
- The map T is said to be ergodic if for all Borel measurable sets B, we have
  $$T^{-1}(B) = B \implies \nu(B) = 1, \text{ or } \nu(B) = 0.$$
- A point x is said to be a **generic point** for (X, T, ν) if the orbit $\left\{T^{[n]}(x)\right\}$ is equidistributed.

Ergodic preliminaries: ergodic map

- We will consider a **dynamical system** (X, T, ν).
  - We have a self-map
    $$T : X \to X$$
    measurable wrt ν.
  - ν is a T-invariant measure, that is, for all Borel measurable sets B:
    $$\nu(B) = \nu\left(T^{-1}(B)\right).$$
- The map T is said to be ergodic if for all Borel measurable sets B, we have
  $$T^{-1}(B) = B \implies \nu(B) = 1, \text{ or } \nu(B) = 0.$$
- A point x is said to be a **generic point** for (X, T, ν) if the orbit $\left\{T^{[n]}(x)\right\}$ is equidistributed.

Ergodic preliminaries: ergodic map

- We will consider a **dynamical system** (X, T, ν).
  - We have a self-map
    $$T : X \to X$$
    measurable wrt ν.
  - ν is a T-invariant measure, that is, for all Borel measurable sets B:
    $$\nu(B) = \nu\left(T^{-1}(B)\right).$$
- The map T is said to be ergodic if for all Borel measurable sets B, we have
  $$T^{-1}(B) = B \implies \nu(B) = 1, \text{ or } \nu(B) = 0.$$
- A point x is said to be a **generic point** for (X, T, ν) if the orbit $\left\{T^{[n]}(x)\right\}$ is equidistributed.

Ergodic preliminaries: ergodic map

- We will consider a **dynamical system** (X, T, ν).
  - We have a self-map
    $$T : X \to X$$
    measurable wrt ν.
  - ν is a T-invariant measure, that is, for all Borel measurable sets B:
    $$\nu(B) = \nu\left(T^{-1}(B)\right).$$
- The map T is said to be ergodic if for all Borel measurable sets B, we have
  $$T^{-1}(B) = B \implies \nu(B) = 1, \text{ or } \nu(B) = 0.$$
- A point x is said to be a **generic point** for (X, T, ν) if the orbit $\left\{T^{[n]}(x)\right\}$ is equidistributed.

An ergodic approach (following Furstenberg)

- Using the Weyl criterion, one can show that if α is irrational, then $\{\lfloor n\alpha \rfloor\}_n$ is equidistributed in $[0,1]$.
- Consider the map

$$\begin{aligned} R_\alpha : [0,1] &\to [0,1], \\ x &\mapsto x + \alpha \pmod 1. \end{aligned}$$

- The map R_α is (uniquely) ergodic wrt the standard Borel measure.
- Every point x in $[0,1]$ is generic wrt R_α.
- Note that $R_\alpha^{[n]}(x) := x + n\alpha$.
- In particular, the orbit of 0

$$\{\lfloor n\alpha \rfloor\}_n$$

is equidistributed in $[0,1]$.

An ergodic approach (following Furstenberg)

- Using the Weyl criterion, one can show that if α is irrational, then $\{\lfloor n\alpha \rfloor\}_n$ is equidistributed in $[0,1]$.
- Consider the map

$$\begin{aligned} R_\alpha : [0,1] &\to [0,1], \\ x &\mapsto x+\alpha \pmod 1. \end{aligned}$$

- The map R_α is (uniquely) ergodic wrt the standard Borel measure.
- Every point x in $[0,1]$ is generic wrt R_α.
- Note that $R_\alpha^{[n]}(x) := x + n\alpha$.
- In particular, the orbit of 0

$$\{\lfloor n\alpha \rfloor\}_n$$

is equidistributed in $[0,1]$.

An ergodic approach (following Furstenberg)

- Using the Weyl criterion, one can show that if α is irrational, then $\{\lfloor n\alpha \rfloor\}_n$ is equidistributed in $[0,1]$.
- Consider the map

$$\begin{aligned} R_\alpha : [0,1] &\to [0,1], \\ x &\mapsto x + \alpha \pmod 1. \end{aligned}$$

- The map R_α is (uniquely) ergodic wrt the standard Borel measure.
- Every point x in $[0,1]$ is generic wrt R_α.
- Note that $R_\alpha^{[n]}(x) := x + n\alpha$.
- In particular, the orbit of 0

$$\{\lfloor n\alpha \rfloor\}_n$$

is equidistributed in $[0,1]$.

An ergodic approach (following Furstenberg)

- Using the Weyl criterion, one can show that if α is irrational, then $\{\lfloor n\alpha \rfloor\}_n$ is equidistributed in $[0,1]$.
- Consider the map

$$\begin{aligned} R_\alpha : [0,1] &\to [0,1], \\ x &\mapsto x + \alpha \pmod 1. \end{aligned}$$

- The map R_α is (uniquely) ergodic wrt the standard Borel measure.
- Every point x in $[0,1]$ is generic wrt R_α.
- Note that $R_\alpha^{[n]}(x) := x + n\alpha$.
- In particular, the orbit of 0

$$\{\lfloor n\alpha \rfloor\}_n$$

is equidistributed in $[0,1]$.

An ergodic approach (following Furstenberg)

- Using the Weyl criterion, one can show that if α is irrational, then $\{\lfloor n\alpha \rfloor\}_n$ is equidistributed in $[0,1]$.
- Consider the map

$$\begin{aligned} R_\alpha : [0,1] &\to [0,1], \\ x &\mapsto x + \alpha \pmod 1. \end{aligned}$$

- The map R_α is (uniquely) ergodic wrt the standard Borel measure.
- Every point x in $[0,1]$ is generic wrt R_α.
- Note that $R_\alpha^{[n]}(x) := x + n\alpha$.
- In particular, the orbit of 0

$$\{\lfloor n\alpha \rfloor\}_n$$

is equidistributed in $[0,1]$.

An ergodic approach (following Furstenberg)

- Using the Weyl criterion, one can show that if α is irrational, then $\{\lfloor n\alpha \rfloor\}_n$ is equidistributed in $[0,1]$.
- Consider the map

$$\begin{aligned} R_\alpha : [0,1] &\to [0,1], \\ x &\mapsto x + \alpha \pmod 1. \end{aligned}$$

- The map R_α is (uniquely) ergodic wrt the standard Borel measure.
- Every point x in $[0,1]$ is generic wrt R_α.
- Note that $R_\alpha^{[n]}(x) := x + n\alpha$.
- In particular, the orbit of 0

$$\{\lfloor n\alpha \rfloor\}_n$$

is equidistributed in $[0,1]$.

Ergodic preliminaries: generic points of an ergodic map

- In general, ergodic maps aren't necessarily uniquely ergodic.
- In general, not every point will be a generic point.
- However, we have the following theorem:

Theorem

Suppose $T : X \to X$ is ergodic. Then,

$$\nu\left(\left\{x \in X,\ \textit{such that } x \textit{ is a generic point}\right\}\right) = 1.$$

- If we want to establish that a particular point is generic, we may need to use the Weyl criterion. However, this can be difficult in practice. This theorem will be useful if one is satisfied with slightly less specific statements involving sets of generic points having full measure.
- There is precedence in applying ergodic tools to Iwasawa theory. For example, Cornut and Vatsal (independently) use Ratner's theorems to obtain results in anticyclotomic Iwasawa theory.

Ergodic preliminaries: generic points of an ergodic map

- In general, ergodic maps aren't necessarily uniquely ergodic.
- In general, not every point will be a generic point.
- However, we have the following theorem:

Theorem

Suppose $T : X \to X$ is ergodic. Then,

$$\nu\left(\left\{x \in X,\ \textit{such that } x \textit{ is a generic point}\right\}\right) = 1.$$

- If we want to establish that a particular point is generic, we may need to use the Weyl criterion. However, this can be difficult in practice. This theorem will be useful if one is satisfied with slightly less specific statements involving sets of generic points having full measure.
- There is precedence in applying ergodic tools to Iwasawa theory. For example, Cornut and Vatsal (independently) use Ratner's theorems to obtain results in anticyclotomic Iwasawa theory.

Ergodic preliminaries: generic points of an ergodic map

- In general, ergodic maps aren't necessarily uniquely ergodic.
- In general, not every point will be a generic point.
- However, we have the following theorem:

Theorem

Suppose $T : X \to X$ is ergodic. Then,

$$\nu\left(\left\{x \in X,\ \textit{such that } x \textit{ is a generic point}\right\}\right) = 1.$$

- If we want to establish that a particular point is generic, we may need to use the Weyl criterion. However, this can be difficult in practice. This theorem will be useful if one is satisfied with slightly less specific statements involving sets of generic points having full measure.
- There is precedence in applying ergodic tools to Iwasawa theory. For example, Cornut and Vatsal (independently) use Ratner's theorems to obtain results in anticyclotomic Iwasawa theory.

Ergodic preliminaries: generic points of an ergodic map

- In general, ergodic maps aren't necessarily uniquely ergodic.
- In general, not every point will be a generic point.
- However, we have the following theorem:

Theorem

Suppose $T : X \to X$ is ergodic. Then,

$$\nu\left(\left\{x \in X,\ \textit{such that } x \textit{ is a generic point}\right\}\right) = 1.$$

- If we want to establish that a particular point is generic, we may need to use the Weyl criterion. However, this can be difficult in practice. This theorem will be useful if one is satisfied with slightly less specific statements involving sets of generic points having full measure.
- There is precedence in applying ergodic tools to Iwasawa theory. For example, Cornut and Vatsal (independently) use Ratner's theorems to obtain results in anticyclotomic Iwasawa theory.

Ergodic preliminaries: generic points of an ergodic map

- In general, ergodic maps aren't necessarily uniquely ergodic.
- In general, not every point will be a generic point.
- However, we have the following theorem:

Theorem

Suppose $T : X \to X$ is ergodic. Then,

$$\nu\left(\left\{x \in X,\ \textit{such that } x \textit{ is a generic point}\right\}\right) = 1.$$

- If we want to establish that a particular point is generic, we may need to use the Weyl criterion. However, this can be difficult in practice. This theorem will be useful if one is satisfied with slightly less specific statements involving sets of generic points having full measure.
- There is precedence in applying ergodic tools to Iwasawa theory. For example, Cornut and Vatsal (independently) use Ratner's theorems to obtain results in anticyclotomic Iwasawa theory.

Ergodic preliminaries: Bernoulli shifts

- Let $A = \{a_1, \cdots, a_n\}$ be an "alphabet" space.
- Let $\vec{p} = (v_1, \cdots v_n)$ be a probability vector, that is $\sum_{i=0}^{n} v_i = 1$.
- The vector $\vec{p}$ defines a probability measure on A.
- Let Σ denote $A^{\mathbb{Z}}$ or $A^{\mathbb{N}}$.
- We equip Σ with the product topology and the product measure ν on the Borel sigma algebra.
- We consider a dynamical system $(\Sigma, \nu) \xrightarrow{T} (\Sigma, \nu)$ as follows
- If $\Sigma = A^{\mathbb{Z}}$, the system is a 2-sided Bernoulli shift.

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots, \right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots \right).$$

- If $\Sigma = A^{\mathbb{N}}$, the system is a 1-sided Bernoulli shift.

$$(a_0, a_1, a_2, \cdots,) \mapsto (a_1, a_2, a_3 \cdots).$$

Ergodic preliminaries: Bernoulli shifts

- Let $A = \{a_1, \cdots, a_n\}$ be an "alphabet" space.
- Let $\vec{p} = (v_1, \cdots v_n)$ be a probability vector, that is $\sum_{i=0}^{n} v_i = 1$.
- The vector $\vec{p}$ defines a probability measure on A.
- Let Σ denote $A^{\mathbb{Z}}$ or $A^{\mathbb{N}}$.
- We equip Σ with the product topology and the product measure ν on the Borel sigma algebra.
- We consider a dynamical system $(\Sigma, \nu) \xrightarrow{T} (\Sigma, \nu)$ as follows
- If $\Sigma = A^{\mathbb{Z}}$, the system is a 2-sided Bernoulli shift.

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots, \right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots\right).$$

- If $\Sigma = A^{\mathbb{N}}$, the system is a 1-sided Bernoulli shift.

$$(a_0, a_1, a_2, \cdots,) \mapsto (a_1, a_2, a_3 \cdots).$$

Ergodic preliminaries: Bernoulli shifts

- Let $A = \{a_1, \cdots, a_n\}$ be an "alphabet" space.
- Let $\vec{p} = (v_1, \cdots v_n)$ be a probability vector, that is $\sum_{i=0}^{n} v_i = 1$.
- The vector $\vec{p}$ defines a probability measure on A.
- Let Σ denote $A^{\mathbb{Z}}$ or $A^{\mathbb{N}}$.
- We equip Σ with the product topology and the product measure ν on the Borel sigma algebra.
- We consider a dynamical system $(\Sigma, \nu) \xrightarrow{T} (\Sigma, \nu)$ as follows
- If $\Sigma = A^{\mathbb{Z}}$, the system is a 2-sided Bernoulli shift.

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots, \right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots \right).$$

- If $\Sigma = A^{\mathbb{N}}$, the system is a 1-sided Bernoulli shift.

$$(a_0, a_1, a_2, \cdots,) \mapsto (a_1, a_2, a_3 \cdots).$$

Ergodic preliminaries: Bernoulli shifts

- Let $A = \{a_1, \cdots, a_n\}$ be an "alphabet" space.
- Let $\vec{p} = (v_1, \cdots v_n)$ be a probability vector, that is $\sum_{i=0}^{n} v_i = 1$.
- The vector $\vec{p}$ defines a probability measure on A.
- Let Σ denote $A^{\mathbb{Z}}$ or $A^{\mathbb{N}}$.
- We equip Σ with the product topology and the product measure ν on the Borel sigma algebra.
- We consider a dynamical system $(\Sigma, \nu) \xrightarrow{T} (\Sigma, \nu)$ as follows
- If $\Sigma = A^{\mathbb{Z}}$, the system is a 2-sided Bernoulli shift.

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots, \right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots \right).$$

- If $\Sigma = A^{\mathbb{N}}$, the system is a 1-sided Bernoulli shift.

$$(a_0, a_1, a_2, \cdots,) \mapsto (a_1, a_2, a_3 \cdots).$$

Ergodic preliminaries: Bernoulli shifts

- Let $A = \{a_1, \cdots, a_n\}$ be an "alphabet" space.
- Let $\vec{p} = (v_1, \cdots v_n)$ be a probability vector, that is $\sum_{i=0}^{n} v_i = 1$.
- The vector $\vec{p}$ defines a probability measure on A.
- Let Σ denote $A^{\mathbb{Z}}$ or $A^{\mathbb{N}}$.
- We equip Σ with the product topology and the product measure ν on the Borel sigma algebra.
- We consider a dynamical system $(\Sigma, \nu) \xrightarrow{T} (\Sigma, \nu)$ as follows
- If $\Sigma = A^{\mathbb{Z}}$, the system is a 2-sided Bernoulli shift.

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots, \right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots \right).$$

- If $\Sigma = A^{\mathbb{N}}$, the system is a 1-sided Bernoulli shift.

$$(a_0, a_1, a_2, \cdots,) \mapsto (a_1, a_2, a_3 \cdots).$$

Ergodic preliminaries: Bernoulli shifts

- Let $A = \{a_1, \cdots, a_n\}$ be an "alphabet" space.
- Let $\vec{p} = (v_1, \cdots v_n)$ be a probability vector, that is $\sum_{i=0}^{n} v_i = 1$.
- The vector $\vec{p}$ defines a probability measure on A.
- Let Σ denote $A^{\mathbb{Z}}$ or $A^{\mathbb{N}}$.
- We equip Σ with the product topology and the product measure ν on the Borel sigma algebra.
- We consider a dynamical system $(\Sigma, \nu) \xrightarrow{T} (\Sigma, \nu)$ as follows
- If $\Sigma = A^{\mathbb{Z}}$, the system is a 2-sided Bernoulli shift.

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots, \right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots \right).$$

- If $\Sigma = A^{\mathbb{N}}$, the system is a 1-sided Bernoulli shift.

$$(a_0, a_1, a_2, \cdots,) \mapsto (a_1, a_2, a_3 \cdots).$$

Ergodic preliminaries: Bernoulli shifts

- One can also consider an r-fold product

$$(\Sigma^r, \nu^r) \xrightarrow{T^r} (\Sigma^r, \nu^r).$$

Theorem

The dynamical system (Σ^r, T^r, ν^r) is ergodic.

- **Remark**: By contrast, an 2-fold product R_α^2 of the rotation-by-α map is not ergodic.

Ergodic preliminaries: Bernoulli shifts

- One can also consider an r-fold product

$$(\Sigma^r, \nu^r) \xrightarrow{T^r} (\Sigma^r, \nu^r).$$

Theorem

The dynamical system (Σ^r, T^r, ν^r) is ergodic.

- **Remark**: By contrast, an 2-fold product R_α^2 of the rotation-by-α map is not ergodic.

Ergodic preliminaries: Bernoulli shifts

- One can also consider an r-fold product

$$(\Sigma^r, \nu^r) \xrightarrow{T^r} (\Sigma^r, \nu^r).$$

Theorem

The dynamical system (Σ^r, T^r, ν^r) is ergodic.

- **Remark**: By contrast, an 2-fold product R_α^2 of the rotation-by-α map is not ergodic.

Ergodic preliminaries: Normal numbers in base p

- Let $\Sigma = \{0, 1, \cdots, p-1\}^{\mathbb{N}}$.
- Let $\vec{v} = (1/p, \cdots, 1/p)$.
- We have a topological and a measurable isomorphism

$$\Sigma \xrightarrow{\cong} \mathbb{Z}_p,$$
$$(a_0, a_1, \cdots) \mapsto \sum_{n=0}^{\infty} a_n p^n.$$

- We have the shift map $(a_0, a_1, \cdots) \overset{T}{\mapsto} (a_1, a_2, \cdots)$.

Definition

A p-adic number β is called **normal** if it is a generic point for T.

Definition

An r-tuple $(\beta_1, \cdots, \beta_r)$ is called **jointly normal** if it is a generic point for T^r.

Ergodic preliminaries: Normal numbers in base p

- Let $\Sigma = \{0, 1, \cdots, p-1\}^{\mathbb{N}}$.
- Let $\vec{v} = (1/p, \cdots, 1/p)$.
- We have a topological and a measurable isomorphism

$$\Sigma \xrightarrow{\cong} \mathbb{Z}_p,$$
$$(a_0, a_1, \cdots) \mapsto \sum_{n=0}^{\infty} a_n p^n.$$

- We have the shift map $(a_0, a_1, \cdots) \overset{T}{\mapsto} (a_1, a_2, \cdots)$.

Definition

A p-adic number β is called **normal** if it is a generic point for T.

Definition

An r-tuple $(\beta_1, \cdots, \beta_r)$ is called **jointly normal** if it is a generic point for T^r.

Ergodic preliminaries: Normal numbers in base p

- Let $\Sigma = \{0, 1, \cdots, p-1\}^{\mathbb{N}}$.
- Let $\vec{v} = (1/p, \cdots, 1/p)$.
- We have a topological and a measurable isomorphism

$$\Sigma \xrightarrow{\cong} \mathbb{Z}_p,$$
$$(a_0, a_1, \cdots) \mapsto \sum_{n=0}^{\infty} a_n p^n.$$

- We have the shift map $(a_0, a_1, \cdots) \overset{T}{\mapsto} (a_1, a_2, \cdots)$.

Definition

A p-adic number β is called **normal** if it is a generic point for T.

Definition

An r-tuple $(\beta_1, \cdots, \beta_r)$ is called **jointly normal** if it is a generic point for T^r.

Ergodic preliminaries: Normal numbers in base p

- Let $\Sigma = \{0, 1, \cdots, p-1\}^{\mathbb{N}}$.
- Let $\vec{v} = (1/p, \cdots, 1/p)$.
- We have a topological and a measurable isomorphism

$$\Sigma \xrightarrow{\cong} \mathbb{Z}_p,$$
$$(a_0, a_1, \cdots) \mapsto \sum_{n=0}^{\infty} a_n p^n.$$

- We have the shift map $(a_0, a_1, \cdots) \overset{T}{\mapsto} (a_1, a_2, \cdots)$.

Definition

A p-adic number β is called **normal** if it is a generic point for T.

Definition

An r-tuple $(\beta_1, \cdots, \beta_r)$ is called **jointly normal** if it is a generic point for T^r.

Ergodic preliminaries: Normal numbers in base p

- The map

$$\begin{aligned} [0,1] &\to [0,1], \\ x &\mapsto px \pmod 1. \end{aligned}$$

  is also ergodic.
- It can be viewed as a shift map by considering expansions of $[0,1]$ in base p.
- The generic points of $\times p$ map are also called normal numbers in base p.
- It is possible to artificially construct some normal numbers.
- Rational numbers are not normal.
- But given a general irrational number, it seems hard to figure out if it is normal or not.
- (Folklore conjecture?) Every algebraic irrational number is normal.

Ergodic preliminaries: Normal numbers in base p

- The map
$$\begin{aligned}[0,1] &\to [0,1],\\ x &\mapsto px \pmod 1.\end{aligned}$$
is also ergodic.
- It can be viewed as a shift map by considering expansions of $[0,1]$ in base p.
- The generic points of $\times p$ map are also called normal numbers in base p.
- It is possible to artificially construct some normal numbers.
- Rational numbers are not normal.
- But given a general irrational number, it seems hard to figure out if it is normal or not.
- (Folklore conjecture?) Every algebraic irrational number is normal.

Ergodic preliminaries: Normal numbers in base p

- The map
$$\begin{aligned}[0,1] &\to [0,1],\\ x &\mapsto px \pmod 1.\end{aligned}$$
is also ergodic.
- It can be viewed as a shift map by considering expansions of $[0,1]$ in base p.
- The generic points of $\times p$ map are also called normal numbers in base p.
- It is possible to artificially construct some normal numbers.
- Rational numbers are not normal.
- But given a general irrational number, it seems hard to figure out if it is normal or not.
- (Folklore conjecture?) Every algebraic irrational number is normal.

Ergodic preliminaries: Normal numbers in base p

- The map

$$\begin{aligned}[0,1] &\to [0,1],\\ x &\mapsto px \pmod 1.\end{aligned}$$

  is also ergodic.
- It can be viewed as a shift map by considering expansions of $[0,1]$ in base p.
- The generic points of $\times p$ map are also called normal numbers in base p.
- It is possible to artificially construct some normal numbers.
- Rational numbers are not normal.
- But given a general irrational number, it seems hard to figure out if it is normal or not.
- (Folklore conjecture?) Every algebraic irrational number is normal.

Ergodic preliminaries: Normal numbers in base p

- The map
$$\begin{aligned}[0,1] &\to [0,1],\\ x &\mapsto px \pmod 1.\end{aligned}$$
is also ergodic.
- It can be viewed as a shift map by considering expansions of $[0,1]$ in base p.
- The generic points of $\times p$ map are also called normal numbers in base p.
- It is possible to artificially construct some normal numbers.
- Rational numbers are not normal.
- But given a general irrational number, it seems hard to figure out if it is normal or not.
- (Folklore conjecture?) Every algebraic irrational number is normal.

Ergodic preliminaries: Normal numbers in base p

- The map
$$\begin{aligned}[0,1] &\to [0,1],\\ x &\mapsto px \pmod 1.\end{aligned}$$
is also ergodic.
- It can be viewed as a shift map by considering expansions of $[0,1]$ in base p.
- The generic points of $\times p$ map are also called normal numbers in base p.
- It is possible to artificially construct some normal numbers.
- Rational numbers are not normal.
- But given a general irrational number, it seems hard to figure out if it is normal or not.
- (Folklore conjecture?) Every algebraic irrational number is normal.

Ergodic preliminaries: Normal numbers in base p

- The map
$$\begin{aligned} [0,1] &\to [0,1], \\ x &\mapsto px \pmod 1. \end{aligned}$$
is also ergodic.
- It can be viewed as a shift map by considering expansions of $[0,1]$ in base p.
- The generic points of $\times p$ map are also called normal numbers in base p.
- It is possible to artificially construct some normal numbers.
- Rational numbers are not normal.
- But given a general irrational number, it seems hard to figure out if it is normal or not.
- (Folklore conjecture?) Every algebraic irrational number is normal.

Historical remark / an observation of Ralph Greenberg

Proposition [Ferrero–Washington]

Let G_r be the set of all α in $\mathbb{Z}_p$ such that

$$\left\{ \left(\frac{s_{n-1}(\alpha\beta_1)}{p^n}, \dots, \frac{s_{n-1}(\alpha\beta_r)}{p^n} \right) \right\}_{n=0}^{\infty}$$

is equidistributed in $[0,1]^r$ with respect to the standard Borel measure. Then, G_r has full Haar measure in $\mathbb{Z}_p$.

- (Hearsay): An initial approach was to prove that a linearly independent set of $(p-1)^{\mathrm{st}}$ roots of unity is jointly normal (?)

p-adic expansions and p-ary expansions

- One important observation is that the map

$$\mathbb{Z}_p \to [0,1],$$
$$\sum_{n=0}^{\infty} a_n p^n \mapsto \sum_{n=0}^{\infty} \frac{a_n}{p^{n+1}}.$$

from a p-adic expansion to a base p expansion is continuous and surjective.

- It is one-one except at rational numbers of the form $\frac{a}{p^n}$ that have two base p-expansions.
- For example, the image of the map (essentially) from the 2-adic expansion to the base 3-expansion gives us the Cantor set.

$$\mathbb{Z}_2 \to [0,1],$$
$$\sum_{n=0} t_n 2^n \mapsto 2\sum_{n=0}^{\infty} \left(\frac{t_n}{3^{n+1}}\right).$$

p-adic expansions and p-ary expansions

- One important observation is that the map

$$\mathbb{Z}_p \to [0,1],$$
$$\sum_{n=0}^{\infty} a_n p^n \mapsto \sum_{n=0}^{\infty} \frac{a_n}{p^{n+1}}.$$

  from a p-adic expansion to a base p expansion is continuous and surjective.

- It is one-one except at rational numbers of the form $\dfrac{a}{p^n}$ that have two base p-expansions.

- For example, the image of the map (essentially) from the 2-adic expansion to the base 3-expansion gives us the Cantor set.

$$\mathbb{Z}_2 \to [0,1],$$
$$\sum_{n=0} t_n 2^n \mapsto 2\sum_{n=0}^{\infty} \left(\frac{t_n}{3^{n+1}}\right).$$

p-adic expansions and p-ary expansions

- One important observation is that the map
$$\begin{aligned} \mathbb{Z}_p &\to [0,1], \\ \sum_{n=0}^{\infty} a_n p^n &\mapsto \sum_{n=0}^{\infty} \frac{a_n}{p^{n+1}}. \end{aligned}$$
from a p-adic expansion to a base p expansion is continuous and surjective.
- It is one-one except at rational numbers of the form $\dfrac{a}{p^n}$ that have two base p-expansions.
- For example, the image of the map (essentially) from the 2-adic expansion to the base 3-expansion gives us the Cantor set.
$$\begin{aligned} \mathbb{Z}_2 &\to [0,1], \\ \sum_{n=0} t_n 2^n &\mapsto 2\sum_{n=0}^{\infty} \left(\frac{t_n}{3^{n+1}}\right). \end{aligned}$$

p-adic solenoid

- The p-adic extension to $\mathbb{R}/\mathbb{Z}$

$$\frac{\mathbb{Z}_p \times \mathbb{R}}{\mathbb{Z}} \cong \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$

  is called the **p-adic solenoid**.

- The p-adic solenoid is equipped with the Haar measure.
- The space $\mathbb{Z}_p \times [0,1]$ is a choice of fundamental domain for the p-adic solenoid.
- That is, we have a surjection

$$\mathbb{Z}_p \times [0,1] \twoheadrightarrow \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$

  that is a homeomorphism outside the boundary $\mathbb{Z}_p \times \{0,1\}$.

- The fundamental domain is equipped with the measure Haar $\times$ Std Borel.

p-adic solenoid

- The p-adic extension to $\mathbb{R}/\mathbb{Z}$
$$\frac{\mathbb{Z}_p \times \mathbb{R}}{\mathbb{Z}} \cong \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$
  is called the ***p*-adic solenoid**.
- The p-adic solenoid is equipped with the Haar measure.
- The space $\mathbb{Z}_p \times [0,1]$ is a choice of fundamental domain for the p-adic solenoid.
- That is, we have a surjection
$$\mathbb{Z}_p \times [0,1] \twoheadrightarrow \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$
  that is a homeomorphism outside the boundary $\mathbb{Z}_p \times \{0,1\}$.
- The fundamental domain is equipped with the measure $\mathrm{Haar} \times \mathrm{Std\ Borel}$.

p-adic solenoid

- The p-adic extension to $\mathbb{R}/\mathbb{Z}$

$$\frac{\mathbb{Z}_p \times \mathbb{R}}{\mathbb{Z}} \cong \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$

  is called the p-**adic solenoid**.

- The p-adic solenoid is equipped with the Haar measure.

- The space $\mathbb{Z}_p \times [0,1]$ is a choice of fundamental domain for the p-adic solenoid.

- That is, we have a surjection

$$\mathbb{Z}_p \times [0,1] \twoheadrightarrow \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$

  that is a homeomorphism outside the boundary $\mathbb{Z}_p \times \{0,1\}$.

- The fundamental domain is equipped with the measure Haar $\times$ Std Borel.

p-adic solenoid

- The p-adic extension to $\mathbb{R}/\mathbb{Z}$
$$\frac{\mathbb{Z}_p \times \mathbb{R}}{\mathbb{Z}} \cong \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$
is called the **p-adic solenoid**.
- The p-adic solenoid is equipped with the Haar measure.
- The space $\mathbb{Z}_p \times [0,1]$ is a choice of fundamental domain for the p-adic solenoid.
- That is, we have a surjection
$$\mathbb{Z}_p \times [0,1] \twoheadrightarrow \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$
that is a homeomorphism outside the boundary $\mathbb{Z}_p \times \{0,1\}$.
- The fundamental domain is equipped with the measure Haar $\times$ Std Borel.

p-adic solenoid

- The p-adic extension to $\mathbb{R}/\mathbb{Z}$

$$\frac{\mathbb{Z}_p \times \mathbb{R}}{\mathbb{Z}} \cong \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$

  is called the ***p*-adic solenoid**.

- The p-adic solenoid is equipped with the Haar measure.
- The space $\mathbb{Z}_p \times [0,1]$ is a choice of fundamental domain for the p-adic solenoid.
- That is, we have a surjection

$$\mathbb{Z}_p \times [0,1] \twoheadrightarrow \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$

  that is a homeomorphism outside the boundary $\mathbb{Z}_p \times \{0,1\}$.

- The fundamental domain is equipped with the measure $\text{Haar} \times \text{Std Borel}$.

p-adic solenoid

- The p-adic extension to $\mathbb{R}/\mathbb{Z}$
$$\frac{\mathbb{Z}_p \times \mathbb{R}}{\mathbb{Z}} \cong \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$
is called the ***p*-adic solenoid**.
- The p-adic solenoid is equipped with the Haar measure.
- The space $\mathbb{Z}_p \times [0,1]$ is a choice of fundamental domain for the p-adic solenoid.
- That is, we have a surjection
$$\mathbb{Z}_p \times [0,1] \twoheadrightarrow \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}$$
that is a homeomorphism outside the boundary $\mathbb{Z}_p \times \{0,1\}$.
- The fundamental domain is equipped with the measure Haar $\times$ Std Borel.

Symbolic coding for the p-adic solenoid

- Using the p-adic and base p expansions, we have a surjection

$$\{0,1,\cdots,p-1\}^{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}_p \times [0,1],$$
$$\left(\cdots,a_{-2},a_{-1}\middle|a_0,a_1,\cdots\right) \mapsto \left(\sum a_n p^n,\ \sum_{n=0}^{\infty}\frac{a_{-n-1}}{p^{n+1}}\right).$$

- We equip $\{0,1,\cdots,p-1\}^{\mathbb{Z}}$ with the probability measure corresponding to the uniform probability vector $\left(\frac{1}{p},\cdots,\frac{1}{p}\right)$.

Symbolic coding for the p-adic solenoid

- Using the p-adic and base p expansions, we have a surjection

$$\{0, 1, \cdots, p-1\}^{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}_p \times [0,1],$$
$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots\right) \mapsto \left(\sum a_n p^n, \sum_{n=0}^{\infty} \frac{a_{-n-1}}{p^{n+1}}\right).$$

- We equip $\{0, 1, \cdots, p-1\}^{\mathbb{Z}}$ with the probability measure corresponding to the uniform probability vector $\left(\frac{1}{p}, \cdots, \frac{1}{p}\right)$.

A Hecke map, a skew-product map, a shift map

- We have a map on the p-adic solenoid:

$$\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]} \xrightarrow{T} \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]},$$
$$(x, y) \to \left(\frac{x}{p}, \frac{y}{p}\right).$$

- We have a map on its fundamental domain:

$$\mathbb{Z}_p \times [0,1] \xrightarrow{T} \mathbb{Z}_p \times [0,1],$$
$$(x, y) \mapsto \left(\frac{x - t_0(x)}{p}, \frac{y + t_0(x)}{p}\right).$$

- We have the 2-sided shift map on $\{0, 1, \cdots, p-1\}^{\mathbb{Z}}$:

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots, \right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots \right).$$

A Hecke map, a skew-product map, a shift map

- We have a map on the p-adic solenoid:

$$\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]} \xrightarrow{T} \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]},$$
$$(x, y) \to \left(\frac{x}{p}, \frac{y}{p}\right).$$

- We have a map on its fundamental domain:

$$\mathbb{Z}_p \times [0,1] \xrightarrow{T} \mathbb{Z}_p \times [0,1],$$
$$(x, y) \mapsto \left(\frac{x - t_0(x)}{p}, \frac{y + t_0(x)}{p}\right).$$

- We have the 2-sided shift map on $\{0, 1, \cdots, p-1\}^{\mathbb{Z}}$:

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots,\right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots\right).$$

A Hecke map, a skew-product map, a shift map

- We have a map on the p-adic solenoid:

$$\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]} \xrightarrow{T} \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]},$$
$$(x, y) \to \left(\frac{x}{p}, \frac{y}{p}\right).$$

- We have a map on its fundamental domain:

$$\mathbb{Z}_p \times [0,1] \xrightarrow{T} \mathbb{Z}_p \times [0,1],$$
$$(x, y) \mapsto \left(\frac{x - t_0(x)}{p}, \frac{y + t_0(x)}{p}\right).$$

- We have the 2-sided shift map on $\{0, 1, \cdots, p-1\}^{\mathbb{Z}}$:

$$\left(\cdots, a_{-2}, a_{-1} \middle| a_0, a_1, \cdots,\right) \mapsto \left(\cdots, a_{-2}, a_{-1}, a_0 \middle| a_1, a_2, \cdots\right).$$

An ergodic map between measurably isomorphic spaces

$$\begin{tikzcd}
\left(\{0,1,\cdots,p-1\}^{\mathbb{Z}}\right)^r \arrow[r, "\text{2-sided shift}"] \arrow[d, two heads] & \left(\{0,1,\cdots,p-1\}^{\mathbb{Z}}\right)^r \arrow[d, two heads] \\
\left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[r, "\text{skew product}"] \arrow[d, two heads] & \left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[d, two heads] \\
\left(\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[r, "\times 1/p"] & \left(\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r.
\end{tikzcd}$$

Generic points for the 1-sided and 2-sided shifts

$$\begin{tikzcd}
\left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[r, "\text{skew product}"] \arrow[d] & \left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[d] \\
\left(\mathbb{Z}_p\right)^r \arrow[r, "\text{1-sided shift}"] & \left(\mathbb{Z}_p\right)^r,
\end{tikzcd}$$

We prove the following proposition:

Proposition 1

The following statements are equivalent

- For every $(x_1, \cdots, x_r)$ in $[0,1]^r$, the element $\left((\gamma_1, x_1), (\gamma_2, x_2), \cdots, (\gamma_r, x_r)\right)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $\left((\gamma_1, 0), (\gamma_2, 0), \cdots, (\gamma_r, 0)\right)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the 1-sided shift.

Generic points for the 1-sided and 2-sided shifts

$$\begin{tikzcd}
\left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[r, "\text{skew product}"] \arrow[d] & \left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[d] \\
\left(\mathbb{Z}_p\right)^r \arrow[r, "\text{1-sided shift}"] & \left(\mathbb{Z}_p\right)^r,
\end{tikzcd}$$

We prove the following proposition:

Proposition 1

The following statements are equivalent

- For every $(x_1, \cdots, x_r)$ in $[0,1]^r$, the element $\left(\left(\gamma_1, x_1\right), \left(\gamma_2, x_2\right), \cdots, \left(\gamma_r, x_r\right)\right)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $\left(\left(\gamma_1, 0\right), \left(\gamma_2, 0\right), \cdots, \left(\gamma_r, 0\right)\right)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the 1-sided shift.

Generic points for the 1-sided and 2-sided shifts

$$\begin{tikzcd}
\left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[r, "\text{skew product}"] \arrow[d] & \left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[d] \\
\left(\mathbb{Z}_p\right)^r \arrow[r, "\text{1-sided shift}"] & \left(\mathbb{Z}_p\right)^r,
\end{tikzcd}$$

We prove the following proposition:

Proposition 1

The following statements are equivalent

- For every $(x_1, \cdots, x_r)$ in $[0,1]^r$, the element $\left((\gamma_1, x_1), (\gamma_2, x_2), \cdots, (\gamma_r, x_r)\right)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $\left((\gamma_1, 0), (\gamma_2, 0), \cdots, (\gamma_r, 0)\right)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the 1-sided shift.

Generic points for the 1-sided and 2-sided shifts

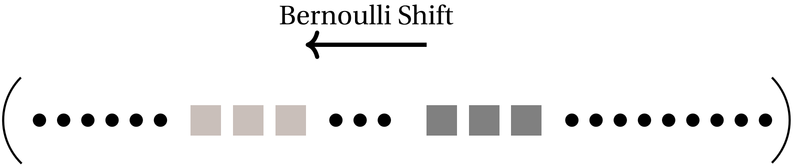
$$\begin{tikzcd} \left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[r, "\text{skew product}"] \arrow[d] & \left(\mathbb{Z}_p \times [0,1]\right)^r \arrow[d] \\ \left(\mathbb{Z}_p\right)^r \arrow[r, "\text{1-sided shift}"] & \left(\mathbb{Z}_p\right)^r, \end{tikzcd}$$

We prove the following proposition:

Proposition 1

The following statements are equivalent

- For every $(x_1, \cdots, x_r)$ in $[0,1]^r$, the element $\big((\gamma_1, x_1), (\gamma_2, x_2), \cdots, (\gamma_r, x_r)\big)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $\big((\gamma_1, 0), (\gamma_2, 0), \cdots, (\gamma_r, 0)\big)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the 1-sided shift.

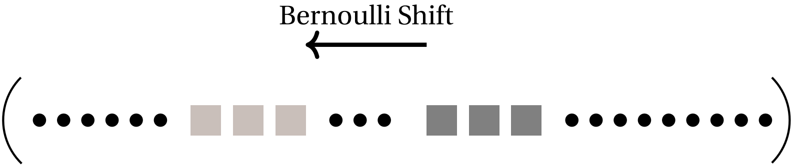


Proposition 1

The following statements are equivalent

- For every $(x_1, \cdots, x_r)$ in $[0,1]^r$, the element $\big((\gamma_1, x_1), (\gamma_2, x_2), \cdots, (\gamma_r, x_r)\big)$ in $\big(\mathbb{Z}_p \times [0,1]\big)^r$ is a generic point.
- $\big((\gamma_1, 0), (\gamma_2, 0), \cdots, (\gamma_r, 0)\big)$ in $\big(\mathbb{Z}_p \times [0,1]\big)^r$ is a generic point.
- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the 1-sided shift.

Generic points for the 1-sided and 2-sided shifts



Proposition 1

The following statements are equivalent

- For every $(x_1, \cdots, x_r)$ in $[0,1]^r$, the element $\big((\gamma_1, x_1), (\gamma_2, x_2), \cdots, (\gamma_r, x_r)\big)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $\big((\gamma_1, 0), (\gamma_2, 0), \cdots, (\gamma_r, 0)\big)$ in $\left(\mathbb{Z}_p \times [0,1]\right)^r$ is a generic point.
- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the 1-sided shift.

Orbit of generic points

- The orbit of $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is given by the set
$$\left\{\left(\left(\frac{\gamma_1 - s_{n-1}(\gamma_1)}{p^n}, \frac{s_{n-1}(\gamma_1)}{p^n}\right), \ldots, \left(\frac{\gamma_r - s_{n-1}(\gamma_r)}{p^n}, \frac{s_{n-1}(\gamma_r)}{p^n}\right)\right)\right\}$$

- If $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is a generic point, then the set above is equidistributed in $\left(\mathbb{Z}_p \times [0,1]\right)^r$.

- Consider the continuous map
$$\left(\mathbb{Z}_p \times [0,1]\right)^r \twoheadrightarrow [0,1]^r.$$

- If $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is a generic point, then the set
$$\left\{\left(\frac{s_{n-1}(\gamma_1)}{p^n}, \ldots, \frac{s_{n-1}(\gamma_r)}{p^n}\right)\right\}_{n=1}^{\infty}$$
must be equidistributed in $[0,1]^r$.

Orbit of generic points

- The orbit of $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is given by the set
$$\left\{\left(\left(\frac{\gamma_1 - s_{n-1}(\gamma_1)}{p^n}, \frac{s_{n-1}(\gamma_1)}{p^n}\right), \dots, \left(\frac{\gamma_r - s_{n-1}(\gamma_r)}{p^n}, \frac{s_{n-1}(\gamma_r)}{p^n}\right)\right)\right\}$$
- If $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is a generic point, then the set above is equidistributed in $\left(\mathbb{Z}_p \times [0,1]\right)^r$.
- Consider the continuous map
$$\left(\mathbb{Z}_p \times [0,1]\right)^r \twoheadrightarrow [0,1]^r.$$
- If $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is a generic point, then the set
$$\left\{\left(\frac{s_{n-1}(\gamma_1)}{p^n}, \dots, \frac{s_{n-1}(\gamma_r)}{p^n}\right)\right\}_{n=1}^{\infty}$$
must be equidistributed in $[0,1]^r$.

Orbit of generic points

- The orbit of $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is given by the set
$$\left\{\left(\left(\frac{\gamma_1-s_{n-1}(\gamma_1)}{p^n},\frac{s_{n-1}(\gamma_1)}{p^n}\right),\dots,\left(\frac{\gamma_r-s_{n-1}(\gamma_r)}{p^n},\frac{s_{n-1}(\gamma_r)}{p^n}\right)\right)\right\}$$
- If $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is a generic point, then the set above is equidistributed in $\left(\mathbb{Z}_p\times[0,1]\right)^r$.
- Consider the continuous map
$$\left(\mathbb{Z}_p\times[0,1]\right)^r\twoheadrightarrow[0,1]^r.$$
- If $\big((\gamma_1,0),(\gamma_2,0),\cdots,(\gamma_r,0)\big)$ is a generic point, then the set
$$\left\{\left(\frac{s_{n-1}(\gamma_1)}{p^n},\dots,\frac{s_{n-1}(\gamma_r)}{p^n}\right)\right\}_{n=1}^{\infty}$$
must be equidistributed in $[0,1]^r$.

A group-theoretic reduction step to the $r = 1$ case

For every non-zero vector $\vec{m}$ in $\mathbb{Z}^r$, we have a commutative diagram:

$$\begin{tikzcd}
\left(\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[r, "\times 1/p"] \arrow[d, "(-\cdot \vec{m})"] & \left(\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[d, "(-\cdot \vec{m})"] \\
\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]} \arrow[r, "\times 1/p"] & \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}
\end{tikzcd}$$

- This reduction step requires us to work with the p-adic solenoid.
- Using this observation, we can deduce the following:

Proposition 2

The following are equivalent:

- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the (r-fold) 1-sided shift.
- For every non-zero vector $\vec{m}$, the linear combination $m_1\gamma_1 + \cdots + m_r\gamma_r$ is a generic point for the 1-sided shift.

A group-theoretic reduction step to the $r = 1$ case

For every non-zero vector $\vec{m}$ in $\mathbb{Z}^r$, we have a commutative diagram:

$$\begin{tikzcd}
\left(\dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[r, "\times 1/p"] \arrow[d, "(-\cdot\vec{m})"] & \left(\dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[d, "(-\cdot\vec{m})"] \\
\dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]} \arrow[r, "\times 1/p"] & \dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}
\end{tikzcd}$$

- This reduction step requires us to work with the p-adic solenoid.
- Using this observation, we can deduce the following:

Proposition 2

The following are equivalent:

- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the (r-fold) 1-sided shift.
- For every non-zero vector $\vec{m}$, the linear combination $m_1\gamma_1 + \cdots + m_r\gamma_r$ is a generic point for the 1-sided shift.

A group-theoretic reduction step to the $r = 1$ case

For every non-zero vector $\vec{m}$ in $\mathbb{Z}^r$, we have a commutative diagram:

$$\begin{tikzcd}
\left(\dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[r, "\times 1/p"] \arrow[d, "(-\cdot \vec{m})"] & \left(\dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[d, "(-\cdot \vec{m})"] \\
\dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]} \arrow[r, "\times 1/p"] & \dfrac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}
\end{tikzcd}$$

- This reduction step requires us to work with the p-adic solenoid.
- Using this observation, we can deduce the following:

Proposition 2

The following are equivalent:

- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the (r-fold) 1-sided shift.
- For every non-zero vector $\vec{m}$, the linear combination $m_1\gamma_1 + \cdots + m_r\gamma_r$ is a generic point for the 1-sided shift.

A group-theoretic reduction step to the $r = 1$ case

For every non-zero vector $\vec{m}$ in $\mathbb{Z}^r$, we have a commutative diagram:

$$\begin{tikzcd}
\left(\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[r, "\times 1/p"] \arrow[d, "(-\cdot \vec{m})"] & \left(\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}\right)^r \arrow[d, "(-\cdot \vec{m})"] \\
\frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]} \arrow[r, "\times 1/p"] & \frac{\mathbb{Q}_p \times \mathbb{R}}{\mathbb{Z}[1/p]}
\end{tikzcd}$$

- This reduction step requires us to work with the p-adic solenoid.
- Using this observation, we can deduce the following:

Proposition 2

The following are equivalent:

- $(\gamma_1, \cdots, \gamma_r)$ is a generic point for the (r-fold) 1-sided shift.
- For every non-zero vector $\vec{m}$, the linear combination $m_1\gamma_1 + \cdots + m_r\gamma_r$ is a generic point for the 1-sided shift.

Final remarks

- The Ferrero–Washington equidistribution result can now be deduced using the characterization of generic points for the r-fold 2-sided Bernoulli shifts afforded by Propositions 1 and 2.
- The linear independence of the β_i's comes into play while applying Proposition 2.
- One also uses the measure-theoretic fact a countable intersection of full measure sets has full measure.
- The reduction step from a general r to $r = 1$ is purely group-theoretic.
- No explicit analysis involved.
- This suggests the entire ergodic nature of the situation is encapsulated in the $r = 1$ case.

Final remarks

- The Ferrero–Washington equidistribution result can now be deduced using the characterization of generic points for the r-fold 2-sided Bernoulli shifts afforded by Propositions 1 and 2.
- The linear independence of the β_i's comes into play while applying Proposition 2.
- One also uses the measure-theoretic fact a countable intersection of full measure sets has full measure.
- The reduction step from a general r to $r = 1$ is purely group-theoretic.
- No explicit analysis involved.
- This suggests the entire ergodic nature of the situation is encapsulated in the $r = 1$ case.

Final remarks

- The Ferrero–Washington equidistribution result can now be deduced using the characterization of generic points for the r-fold 2-sided Bernoulli shifts afforded by Propositions 1 and 2.
- The linear independence of the β_i's comes into play while applying Proposition 2.
- One also uses the measure-theoretic fact a countable intersection of full measure sets has full measure.
- The reduction step from a general r to $r = 1$ is purely group-theoretic.
- No explicit analysis involved.
- This suggests the entire ergodic nature of the situation is encapsulated in the $r = 1$ case.

Final remarks

- The Ferrero–Washington equidistribution result can now be deduced using the characterization of generic points for the r-fold 2-sided Bernoulli shifts afforded by Propositions 1 and 2.
- The linear independence of the β_i's comes into play while applying Proposition 2.
- One also uses the measure-theoretic fact a countable intersection of full measure sets has full measure.
- The reduction step from a general r to $r = 1$ is purely group-theoretic.
- No explicit analysis involved.
- This suggests the entire ergodic nature of the situation is encapsulated in the $r = 1$ case.

Final remarks

- The Ferrero–Washington equidistribution result can now be deduced using the characterization of generic points for the r-fold 2-sided Bernoulli shifts afforded by Propositions 1 and 2.
- The linear independence of the β_i's comes into play while applying Proposition 2.
- One also uses the measure-theoretic fact a countable intersection of full measure sets has full measure.
- The reduction step from a general r to $r = 1$ is purely group-theoretic.
- No explicit analysis involved.
- This suggests the entire ergodic nature of the situation is encapsulated in the $r = 1$ case.

Final remarks

- The Ferrero–Washington equidistribution result can now be deduced using the characterization of generic points for the r-fold 2-sided Bernoulli shifts afforded by Propositions 1 and 2.
- The linear independence of the β_i's comes into play while applying Proposition 2.
- One also uses the measure-theoretic fact a countable intersection of full measure sets has full measure.
- The reduction step from a general r to $r = 1$ is purely group-theoretic.
- No explicit analysis involved.
- This suggests the entire ergodic nature of the situation is encapsulated in the $r = 1$ case.

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Generalizations and vague ideas

- What sort of generalizations can one consider? (GL_2-generalization)
  - The case of real quadratic fields itself will itself be interesting.
  - Elliptic curves, modular forms.
    - There are *Stickelberger-type* elements constructed using modular symbols.
    - The analog of Iwasawa's criterion goes back to the thesis of Hae-Sang Sun.
    - The analogue of the uniform distribution results are conjectural (Mazur–Rubin–Stein).
    - Average versions of these uniform distribution conjectures are known due to Petridis–Risager and Lee-Sun.
    - Lee–Sun use the dynamics of continued fractions.
    - The connection to topological dynamics is more explicit.
  - In our work, we want to highlight the connection to symbolic dynamics.
    - The connection to symbolic dynamics in the GL_2-situation dates back to the relationship between continued fractions and symbolic coding of geodesics on the modular curve.
    - We have more ergodic tools at our disposal to study geodesics.
    - Is there a geometric description to p-adic (extensions of) continued fractions?

Thank you.