# The First Level of $\mathbb{Z}_p$-extensions and Compatibility of Heuristics

Larry Washington (joint with Debanjana Kundu)

University of Maryland

August 18, 2025

René 25

Université de la Polynésie Française

Fare ha'api'ira'a tuatoru nō Pōrinetia farāni

# $\mathbb{Z}_p$-extensions

- $p =$ (odd) prime

# $\mathbb{Z}_p$-extensions

- $p =$ (odd) prime
- $\zeta_{p^n} =$ primitive $p^n$th root of unity

# $\mathbb{Z}_p$-extensions

- $p =$ (odd) prime
- $\zeta_{p^n} =$ primitive $p^n$th root of unity
- $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset Q(\zeta_{p^{n+1}}) \subset \cdots$

## $\mathbb{Z}_p$-extensions

- $p =$ (odd) prime
- $\zeta_{p^n} =$ primitive $p^n$th root of unity
- $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset Q(\zeta_{p^{n+1}}) \subset \cdots$
- Take degree $p - 1$ off each field:
  $\mathbb{Q} \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \mathbb{Q}_\infty$

## $\mathbb{Z}_p$-extensions

- $p =$ (odd) prime
- $\zeta_{p^n} =$ primitive $p^n$th root of unity
- $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset Q(\zeta_{p^{n+1}}) \subset \cdots$
- Take degree $p-1$ off each field:
  $\mathbb{Q} \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \mathbb{Q}_\infty$
- $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$

## $\mathbb{Z}_p$-extensions

- $p =$ (odd) prime
- $\zeta_{p^n} =$ primitive $p^n$th root of unity
- $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset Q(\zeta_{p^{n+1}}) \subset \cdots$
- Take degree $p-1$ off each field: $\mathbb{Q} \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \mathbb{Q}_\infty$
- $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$
- Lift to a number field $K$:

$$K = K_0 \subset K_1 = K\mathbb{Q}_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty$$

## $\mathbb{Z}_p$-extensions

- $p =$ (odd) prime
- $\zeta_{p^n} =$ primitive $p^n$th root of unity
- $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset Q(\zeta_{p^{n+1}}) \subset \cdots$
- Take degree $p - 1$ off each field: $\mathbb{Q} \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \mathbb{Q}_\infty$
- $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$
- Lift to a number field $K$:

$$K = K_0 \subset K_1 = K\mathbb{Q}_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty$$

- $\mathrm{Gal}(K_n/K_0) \simeq \mathbb{Z}/p^n\mathbb{Z}, \qquad \mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p = p$-adic integers

# Iwasawa's Theorem

- $A_n$ = Sylow $p$-subgroup of ideal class group of $K_n$

## Iwasawa's Theorem

- $A_n$ = Sylow $p$-subgroup of ideal class group of $K_n$
- There exist $n_0$ and integers $\lambda, \mu \geq 0$ and $\nu$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

for all $n \geq n_0$.

# Iwasawa's Theorem

- $A_n$ = Sylow $p$-subgroup of ideal class group of $K_n$
- There exist $n_0$ and integers $\lambda, \mu \geq 0$ and $\nu$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

  for all $n \geq n_0$.
- Usually (conjecturally always) $\mu = 0$.

# Iwasawa's Theorem

- $A_n$ = Sylow $p$-subgroup of ideal class group of $K_n$
- There exist $n_0$ and integers $\lambda, \mu \geq 0$ and $\nu$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

  for all $n \geq n_0$.
- Usually (conjecturally always) $\mu = 0$.
- What can be said about $\lambda$ ?

# Iwasawa's Theorem

- $A_n$ = Sylow $p$-subgroup of ideal class group of $K_n$
- There exist $n_0$ and integers $\lambda, \mu \geq 0$ and $\nu$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

  for all $n \geq n_0$.
- Usually (conjecturally always) $\mu = 0$.
- What can be said about $\lambda$ ?
- When $K$ is imaginary quadratic, $\cup_{n \geq 0} A_n \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$.

# Iwasawa's Theorem

- $A_n$ = Sylow $p$-subgroup of ideal class group of $K_n$
- There exist $n_0$ and integers $\lambda, \mu \geq 0$ and $\nu$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

  for all $n \geq n_0$.
- Usually (conjecturally always) $\mu = 0$.
- What can be said about $\lambda$ ?
- When $K$ is imaginary quadratic, $\cup_{n \geq 0} A_n \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$.
- What can be said about $A_n$ for $n < n_0$ ?

# Imaginary Quadratic Fields

$K$ = imaginary quadratic field in which 3 does not split
$p = 3$

- Suppose $A_0$ is cyclic 3

# Imaginary Quadratic Fields

$K$ = imaginary quadratic field in which 3 does not split
$p = 3$

- Suppose $A_0$ is cyclic 3
- $A_1$ is one of the following:

# Imaginary Quadratic Fields

$K$ = imaginary quadratic field in which 3 does not split
$p = 3$

- Suppose $A_0$ is cyclic 3
- $A_1$ is one of the following:
- $3 \times 3 \times 3$

## Imaginary Quadratic Fields

$K$ = imaginary quadratic field in which 3 does not split
$p = 3$

- Suppose $A_0$ is cyclic 3
- $A_1$ is one of the following:
- $3 \times 3 \times 3$
- $3^{s+1} \times 3^s$ with $s \geq 1$

## Imaginary Quadratic Fields

$K =$ imaginary quadratic field in which 3 does not split
$p = 3$

- Suppose $A_0$ is cyclic 3
- $A_1$ is one of the following:
- $3 \times 3 \times 3$
- $3^{s+1} \times 3^s$ with $s \geq 1$
- $3^{s+1} \times 3^{s+1}$, with $s \geq 1$

# Imaginary Quadratic Fields

$K$ = imaginary quadratic field in which 3 does not split

$p = 3$

- Suppose $A_0$ is cyclic 3
- $A_1$ is one of the following:
- $3 \times 3 \times 3$
- $3^{s+1} \times 3^s$ with $s \geq 1$
- $3^{s+1} \times 3^{s+1}$, with $s \geq 1$
- 9

# Imaginary Quadratic Fields

$K$ = imaginary quadratic field in which 3 does not split
$p = 3$

- Suppose $A_0$ is cyclic 3
- $A_1$ is one of the following:
- $3 \times 3 \times 3$
- $3^{s+1} \times 3^s$ with $s \geq 1$
- $3^{s+1} \times 3^{s+1}$, with $s \geq 1$
- 9

9 is equivalent to $\lambda = 1$

The general case

- Suppose $K =$ imaginary quadratic field in which $p$ does not split

The general case

- Suppose $K =$ imaginary quadratic field in which $p$ does not split
- Assume $A_0$ is cyclic of order $p^m$ with $m \geq 1$.

The general case

- Suppose $K =$ imaginary quadratic field in which $p$ does not split
- Assume $A_0$ is cyclic of order $p^m$ with $m \geq 1$.
- **Theorem.** $A_1$ is one of the following:

$$(\mathbb{Z}/p^m\mathbb{Z})^p \,.$$

$$\left(\mathbb{Z}/p^{m-1}\mathbb{Z}\right) \times \left(\mathbb{Z}/p^{s+1}\mathbb{Z}\right)^a \times (\mathbb{Z}/p^s\mathbb{Z})^{p-1-a}$$

with $m \leq s$ and $1 \leq a \leq p-1$.

$$\left(\mathbb{Z}/p^{m+1}\mathbb{Z}\right) \times \left(\mathbb{Z}/p^{s+1}\mathbb{Z}\right)^b \times (\mathbb{Z}/p^s\mathbb{Z})^{p-1-b}$$

with $0 \leq s < m$ and $0 \leq b \leq p-2,$ and with $b \neq p-2$ if $m = s+1$.

# Main Ingredients

# Main Ingredients

- The natural map $A_0 \to A_1$ is injective.

# Main Ingredients

- The natural map $A_0 \to A_1$ is injective.
- The norm $A_1 \to A_0$ is surjective.

# Main Ingredients

- The natural map $A_0 \to A_1$ is injective.
- The norm $A_1 \to A_0$ is surjective.
- $G = \mathrm{Gal}(K_1/K_0)$ cyclic of order $p$. Write $G = \langle \sigma \rangle$.

# Main Ingredients

- The natural map $A_0 \to A_1$ is injective.
- The norm $A_1 \to A_0$ is surjective.
- $G = \mathrm{Gal}(K_1/K_0)$ cyclic of order $p$. Write $G = \langle \sigma \rangle$.
- $\mathbb{Z}_p[G]$ acts on $A_1$, where $\mathbb{Z}_p = p$-adic integers

# Main Ingredients

- The natural map $A_0 \to A_1$ is injective.
- The norm $A_1 \to A_0$ is surjective.
- $G = \mathrm{Gal}(K_1/K_0)$ cyclic of order $p$. Write $G = \langle\sigma\rangle$.
- $\mathbb{Z}_p[G]$ acts on $A_1$, where $\mathbb{Z}_p = p$-adic integers
- $A_1^G = A_0$

# Main Ingredients

- The natural map $A_0 \to A_1$ is injective.
- The norm $A_1 \to A_0$ is surjective.
- $G = \mathrm{Gal}(K_1/K_0)$ cyclic of order $p$. Write $G = \langle \sigma \rangle$.
- $\mathbb{Z}_p[G]$ acts on $A_1$, where $\mathbb{Z}_p = p$-adic integers
- $A_1^G = A_0$
- $A_0$ cyclic $\implies A_1 \simeq \mathbb{Z}_p[G]/I$ for some ideal $I$ of $\mathbb{Z}_p[G]$.

**Theorem**

*Let $p$ be an odd prime and let $G$ be the cyclic group of order $p$. Let $\mathbb{Z}_p[G]$ be the $p$-adic group ring of $G$. If $A_1$ is a non-trivial finite cyclic $\mathbb{Z}_p[G]$-module such that the Tate cohomology group $\widehat{H}^0(G, A_1) = 0$, then $A_1$ is isomorphic as an abelian group to one of the groups listed in the previous theorem.*

- Let $\zeta = \zeta_p$.

- Let $\zeta = \zeta_p$.
- $\pi = \zeta - 1$.

- Let $\zeta = \zeta_p$.
- $\pi = \zeta - 1$.
- The non-zero ideals of $\mathbb{Z}_p[\zeta]$ have the form $\pi^r \mathbb{Z}_p[\zeta]$.

- Let $\zeta = \zeta_p$.
- $\pi = \zeta - 1$.
- The non-zero ideals of $\mathbb{Z}_p[\zeta]$ have the form $\pi^r \mathbb{Z}_p[\zeta]$.
- $\mathbb{Z}_p[\zeta]/(\pi) \simeq \mathbb{F}_p$

# Reiner's Classification of Ideals of $\mathbb{Z}_p[G]$

$$\begin{array}{ccc} \mathbb{Z}_p[\sigma] & \xrightarrow{\epsilon} & \mathbb{Z}_p \\ \downarrow \phi & & \downarrow \text{mod } p \\ \mathbb{Z}_p[\zeta] & \xrightarrow[\text{mod } \pi]{} & \mathbb{F}_p \end{array}$$

where $\epsilon : \mathbb{Z}_p[\sigma] \to \mathbb{Z}_p$ is the map $\sum a_i \sigma^i \mapsto \sum a_i$ and $\phi(\sigma) = \zeta_p$.

# Reiner's Classification of Ideals of $\mathbb{Z}_p[G]$

$$\begin{array}{ccc} \mathbb{Z}_p[\sigma] & \xrightarrow{\epsilon} & \mathbb{Z}_p \\ \downarrow \phi & & \downarrow \text{mod } p \\ \mathbb{Z}_p[\zeta] & \xrightarrow[\text{mod } \pi]{} & \mathbb{F}_p \end{array}$$

where $\epsilon : \mathbb{Z}_p[\sigma] \to \mathbb{Z}_p$ is the map $\sum a_i \sigma^i \mapsto \sum a_i$ and $\phi(\sigma) = \zeta_p$.

$$\mathbb{Z}_p[\sigma] \simeq \{(x, y) \in \mathbb{Z}_p[\zeta] \times \mathbb{Z}_p \mid \phi(x) \text{ mod } \pi = \epsilon(y) \text{ mod } p \text{ in } \mathbb{F}_p\}.$$

# Reiner's Classification of Ideals of $\mathbb{Z}_p[G]$

$$\begin{array}{ccc} \mathbb{Z}_p[\sigma] & \xrightarrow{\epsilon} & \mathbb{Z}_p \\ \downarrow \phi & & \downarrow \text{mod } p \\ \mathbb{Z}_p[\zeta] & \xrightarrow[\text{mod } \pi]{} & \mathbb{F}_p \end{array}$$

where $\epsilon : \mathbb{Z}_p[\sigma] \to \mathbb{Z}_p$ is the map $\sum a_i \sigma^i \mapsto \sum a_i$ and $\phi(\sigma) = \zeta_p$.

$$\mathbb{Z}_p[\sigma] \simeq \{(x, y) \in \mathbb{Z}_p[\zeta] \times \mathbb{Z}_p \mid \phi(x) \text{ mod } \pi = \epsilon(y) \text{ mod } p \text{ in } \mathbb{F}_p\}.$$

$$
\begin{array}{ccc}
\mathbb{Z}_p[\sigma] & \xrightarrow{\ \epsilon\ } & \mathbb{Z}_p \\
\big\downarrow \phi & & \big\downarrow \text{mod } p \\
\mathbb{Z}_p[\zeta] & \xrightarrow[\text{mod } \pi]{} & \mathbb{F}_p
\end{array}
$$

$$
\begin{array}{ccc}
\mathbb{Z}_p[\sigma] & \xrightarrow{\epsilon} & \mathbb{Z}_p \\
\Big\downarrow \phi & & \Big\downarrow \text{mod } p \\
\mathbb{Z}_p[\zeta] & \xrightarrow[\text{mod } \pi]{} & \mathbb{F}_p
\end{array}
$$

- $\pi = \zeta_p - 1$
- $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1}$

$$
\begin{array}{ccc}
\mathbb{Z}_p[\sigma] & \xrightarrow{\ \epsilon\ } & \mathbb{Z}_p \\
\big\downarrow \phi & & \big\downarrow \text{mod } p \\
\mathbb{Z}_p[\zeta] & \xrightarrow[\text{mod } \pi]{} & \mathbb{F}_p
\end{array}
$$

- $\pi = \zeta_p - 1$
- $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1}$
- The action of $\mathbb{Z}_p[\sigma]$ is given by $\sigma(x, y) = (\zeta x, y)$. Therefore, $(\sigma - 1)(x, y) = (\pi x, 0)$ and $N(x, y) = (0, py)$.

**Reiner:** Let $I$ be an ideal of finite index greater than 1 in $\mathbb{Z}_p[G]$ such that $|N(\mathbb{Z}[G]/I)| = p^m > 1$. Then there are

(a) an integer $r \geq 1$,

(b) an integer $b \in p^m\mathbb{Z}_p/p^{m+1}\mathbb{Z}_p$

such that

$$I = \mathbb{Z}_p[\sigma](\pi^r, b) + \mathbb{Z}_p(0, p^{m+1}).$$

**Reiner:** Let $I$ be an ideal of finite index greater than 1 in $\mathbb{Z}_p[G]$ such that $|N(\mathbb{Z}[G]/I)| = p^m > 1$. Then there are

(a) an integer $r \geq 1$,

(b) an integer $b \in p^m\mathbb{Z}_p/p^{m+1}\mathbb{Z}_p$

such that

$$I = \mathbb{Z}_p[\sigma](\pi^r, b) + \mathbb{Z}_p(0, p^{m+1}).$$

Moreover,

$$|\mathbb{Z}_p[\sigma]/I| = p^{r+m}.$$

$$I = \mathbb{Z}_p[\sigma](\pi^r, b) + \mathbb{Z}_p(0, p^{m+1}).$$

$$I = \mathbb{Z}_p[\sigma](\pi^r, b) + \mathbb{Z}_p(0, p^{m+1}).$$

- Recall: $A_1^G = A_0$ and $A_0 = N(A_1)$.

$$I = \mathbb{Z}_p[\sigma](\pi^r, b) + \mathbb{Z}_p(0, p^{m+1}).$$

- Recall: $A_1^G = A_0$ and $A_0 = N(A_1)$.

$$(\mathbb{Z}_p[\sigma]/I)^G = (N)\,(\mathbb{Z}_p[\sigma]/I) \iff b \not\equiv 0 \pmod{p^{m+1}}.$$

$$I = \mathbb{Z}_p[\sigma](\pi^r, b) + \mathbb{Z}_p(0, p^{m+1}).$$

- Recall: $A_1^G = A_0$ and $A_0 = N(A_1)$.

$$(\mathbb{Z}_p[\sigma]/I)^G = (N)\,(\mathbb{Z}_p[\sigma]/I) \Longleftrightarrow b \not\equiv 0 \pmod{p^{m+1}}.$$

- The ideals that yield possibilities for $A_1$ have the form

$$I = \mathbb{Z}_p[\sigma](\pi^r, b_1 p^m) + \mathbb{Z}_p(0, p^{m+1}),\ \text{with } r \geq 1 \text{ and } 1 \leq b_1 \leq p-1.$$

- Analyzing the structure of $\mathbb{Z}_p[G]/I$ yields the theorem.

## Heuristics

- The following are equivalent:

# Heuristics

- The following are equivalent:
  - $\lambda = 1$

## Heuristics

- The following are equivalent:
  - $\lambda = 1$
  - $A_0$ and $A_1$ are non-trivial cyclic

# Heuristics

- The following are equivalent:
  - $\lambda = 1$
  - $A_0$ and $A_1$ are non-trivial cyclic
  - $|A_1|/|A_0| = p$

## Heuristics

- The following are equivalent:
  - $\lambda = 1$
  - $A_0$ and $A_1$ are non-trivial cyclic
  - $|A_1|/|A_0| = p$
- The Ellenberg-Jain-Venkatesh heuristics predict that the probability the Iwasawa invariant $\lambda = 1$ is

$$p^{-1}\prod_{j=2}^{\infty}(1-p^{-j}).$$

# Heuristics

- The following are equivalent:
  - $\lambda = 1$
  - $A_0$ and $A_1$ are non-trivial cyclic
  - $|A_1|/|A_0| = p$
- The Ellenberg-Jain-Venkatesh heuristics predict that the probability the Iwasawa invariant $\lambda = 1$ is

$$p^{-1}\prod_{j=2}^{\infty}(1-p^{-j}).$$

- The Cohen-Lenstra heuristics predict that the probability $A_0$ is cyclic is

$$p^{-1}(1-p^{-1})^{-2}\prod_{j=1}^{\infty}(1-p^{-j}).$$

- We know that

$$\lambda = 1 \iff \exists m \geq 1 \text{ such that } A_0 \simeq \mathbb{Z}/p^m\mathbb{Z} \text{ and } A_1 \simeq \mathbb{Z}/p^{m+1}\mathbb{Z}.$$

- We know that

$$\lambda = 1 \iff \exists m \geq 1 \text{ such that } A_0 \simeq \mathbb{Z}/p^m\mathbb{Z} \text{ and } A_1 \simeq \mathbb{Z}/p^{m+1}\mathbb{Z}.$$

- The conditional probability that $\lambda = 1$ given that $A_0$ is cyclic equals
  the conditional probability that $A_1$ is cyclic given that $A_0$ is cyclic.

- We know that

$$\lambda = 1 \Longleftrightarrow \exists m \geq 1 \text{ such that } A_0 \simeq \mathbb{Z}/p^m\mathbb{Z} \text{ and } A_1 \simeq \mathbb{Z}/p^{m+1}\mathbb{Z}.$$

- The conditional probability that $\lambda = 1$ given that $A_0$ is cyclic equals
  the conditional probability that $A_1$ is cyclic given that $A_0$ is cyclic.
- Combining the CL and EJV heuristics yields

$$\text{Prob}(\lambda = 1 \mid A_0 \text{ is cyclic}) = \frac{\text{Prob}(\lambda = 1)}{\text{Prob}(A_0 \text{ is cyclic})} = \frac{p-1}{p}.$$

# EJV from CL

A different approach

# EJV from CL

A different approach

- If $A_0$ is cyclic, we know the possibilities for $A_1$.
- Weight the possibilities for $A_1$ by the inverse of the sizes of their automorphism groups as $\mathbb{Z}_p[\sigma]$-modules.

# EJV from CL

A different approach

- If $A_0$ is cyclic, we know the possibilities for $A_1$.
- Weight the possibilities for $A_1$ by the inverse of the sizes of their automorphism groups as $\mathbb{Z}_p[\sigma]$-modules.
- Recall $I$ can have the form $\mathbb{Z}_p[\sigma](\pi^r, b_1 p^m) + \mathbb{Z}_p(0, p^m)$ with $1 \leq b_1 \leq p-1$.
- The automorphism group of $\mathbb{Z}_p[\sigma]/I$ is $(\mathbb{Z}_p[\sigma]/I)^\times$.

# EJV from CL

A different approach

- If $A_0$ is cyclic, we know the possibilities for $A_1$.
- Weight the possibilities for $A_1$ by the inverse of the sizes of their automorphism groups as $\mathbb{Z}_p[\sigma]$-modules.
- Recall $I$ can have the form $\mathbb{Z}_p[\sigma](\pi^r, b_1 p^m) + \mathbb{Z}_p(0, p^m)$ with $1 \leq b_1 \leq p-1$.
- The automorphism group of $\mathbb{Z}_p[\sigma]/I$ is $(\mathbb{Z}_p[\sigma]/I)^\times$.
- If $\mathbb{Z}_p[\sigma]/I$ has order $p^{m+r}$, the order of its automorphism group is $(p-1)p^{m+r-1}$.

- If $\mathbb{Z}_p[\sigma]/I$ has order $p^{m+r}$, the order of its automorphism group is $(p-1)p^{m+r-1}$.

- If $\mathbb{Z}_p[\sigma]/I$ has order $p^{m+r}$, the order of its automorphism group is $(p-1)p^{m+r-1}$.
- There are $p-1$ ideals $I$ with $\mathbb{Z}_p[\sigma]/I$ of order $p^{m+r}$:

$$I = \mathbb{Z}_p[\sigma](\pi^r, b_1 p^m) + \mathbb{Z}_p(0, p^m) \text{ with } 1 \le b_1 \le p-1.$$

- If $\mathbb{Z}_p[\sigma]/I$ has order $p^{m+r}$, the order of its automorphism group is $(p-1)p^{m+r-1}$.
- There are $p-1$ ideals $I$ with $\mathbb{Z}_p[\sigma]/I$ of order $p^{m+r}$:

$$I = \mathbb{Z}_p[\sigma](\pi^r, b_1 p^m) + \mathbb{Z}_p(0, p^m) \text{ with } 1 \leq b_1 \leq p-1.$$

- $$\sum_{A_1 \text{ such that } A_0 \text{ cyclic } p^m} \frac{1}{|\mathrm{Aut}(A_1)|} = \sum_{r=1}^{\infty} \frac{p-1}{(p-1)p^{r+m-1}} = \frac{1}{(p-1)p^{m-1}}.$$

- If $\mathbb{Z}_p[\sigma]/I$ has order $p^{m+r}$, the order of its automorphism group is $(p-1)p^{m+r-1}$.
- There are $p-1$ ideals $I$ with $\mathbb{Z}_p[\sigma]/I$ of order $p^{m+r}$:

$$I = \mathbb{Z}_p[\sigma](\pi^r, b_1 p^m) + \mathbb{Z}_p(0, p^m) \text{ with } 1 \le b_1 \le p-1.$$

- $$\sum_{A_1 \text{ such that } A_0 \text{ cyclic } p^m} \frac{1}{|\mathrm{Aut}(A_1)|} = \sum_{r=1}^{\infty} \frac{p-1}{(p-1)p^{r+m-1}} = \frac{1}{(p-1)p^{m-1}}.$$

- The $p-1$ in the numerator comes from the $p-1$ choices for $b_1$.

- There are $p-1$ ideals that yield $A_1$ cyclic of order $p^{m+1}$.

- There are $p-1$ ideals that yield $A_1$ cyclic of order $p^{m+1}$.
- The automorphism groups have order $(p-1)p^m$.

- There are $p-1$ ideals that yield $A_1$ cyclic of order $p^{m+1}$.
- The automorphism groups have order $(p-1)p^m$.
- We obtain the heuristic prediction

$$\begin{aligned}
&\mathrm{Prob}(A_1 \text{ is cyclic} \mid A_0 \text{ cyclic } p^m) \\
&\qquad = \frac{\text{Total weight of cyclic } A_1}{\text{Total weight of all } A_1 \text{ with } A_0 \text{ cyclic } p^m} \\
&\qquad = \frac{(p-1)/(p-1)p^m}{1/(p-1)p^{m-1}} \\
&\qquad = \frac{p-1}{p}.
\end{aligned}$$

- There are $p-1$ ideals that yield $A_1$ cyclic of order $p^{m+1}$.
- The automorphism groups have order $(p-1)p^m$.
- We obtain the heuristic prediction

$$\begin{aligned}
&\text{Prob}(A_1 \text{ is cyclic} \mid A_0 \text{ cyclic } p^m) \\
&\qquad = \frac{\text{Total weight of cyclic } A_1}{\text{Total weight of all } A_1 \text{ with } A_0 \text{ cyclic } p^m} \\
&\qquad = \frac{(p-1)/(p-1)p^m}{1/(p-1)p^{m-1}} \\
&\qquad = \frac{p-1}{p}.
\end{aligned}$$

- Therefore, the EJV heuristics for $\lambda = 1$ are compatible with the CL heuristics.

This also indicates that all the possible groups listed in the theorem should occur.

| | # of $d$ | 9 | $9\times3$ | $3\times3\times3$ | $9\times9$ | $27\times9$ | $27\times27$ |
|---|---|---|---|---|---|---|---|
| $3\nmid d$ | 18315 | .6669 | .1118 | .1104 | .0728 | .0267 | .0079 |
| $3\mid d$ | 12096 | .6685 | .1132 | .1122 | .0703 | .0227 | .0091 |
| Predicted | | .6667 | .1111 | .1111 | .0741 | .0247 | .0082 |

| $81\times27$ | $81\times81$ | $3^5\times3^4$ | $3^5\times3^5$ | $3^6\times3^5$ |
|---|---|---|---|---|
| .0023 | .0008 | .0003 | .0001 | .0001 |
| .0027 | .0010 | .0003 | .0000 | .0000 |
| .0027 | .0009 | .0003 | .0001 | .0000 |

Table: $A_0$ is cyclic of order 3. Distribution of 3-parts of $A_1$ for fundamental discriminants of the form $-1-3j$ for $10^6\le j\le 10^6+2\times10^5$ (the line $3\nmid d$ and of the form $-3j$ for $10^6\le j\le 10^6+2\times10^5$ (the line $3\mid d$).

| | Number of $d$ | 25 | $25 \times 5$ | $25 \times 5 \times 5$ | $25 \times 5 \times 5 \times 5$ |
|---|---|---|---|---|---|
| $-2-5k$ | 588 | .8078 | .1582 | .0272 | .0051 |
| $-3-5k$ | 561 | .7843 | .1765 | .0196 | .0143 |
| $-5k$ | 482 | .8050 | .1515 | .0353 | .0083 |
| Predicted | | .8000 | .1600 | .0320 | .0048 |

| $5\times5\times5\times5\times5$ | $25 \times 25 \times 5 \times 5$ | $25 \times 25 \times 25 \times 5$ | $25 \times 25 \times 25 \times 25$ |
|---|---|---|---|
| .0000 | .0017 | .0000 | .0000 |
| .0018 | .0018 | .0000 | .0018 |
| .0000 | .0000 | .0000 | .0000 |
| .0016 | .0013 | .0003 | .0001 |

Table: $A_0$ is cyclic of order 5. Distribution of 5-parts of $A_1$ for fundamental discriminants of the form $-2-5k$, $-3-5k$, and $-5k$ for $10^6 \leq k < 10^6 + 10^4$.

Māuruuru