Class number statistics for imaginary quadratic fields

Pär Kurlberg

Department of Matematics
Royal Institute of Technology (KTH)
Stockholm, Sweden
kurlberg@math.kth.se

Joint work with:
S. Holmin, N. Jones, C. McLeman, and K. Petersen.

CIRM, 16-03-31

Quadratic forms

Some notation:

- Q: binary quadratic form, $Q(x, y) = ax^2 + bxy + cy^2$.
- D_Q: discriminant of Q,

$$D_Q := b^2 - 4ac$$

Quadratic forms

Some notation:

- Q: binary quadratic form, $Q(x, y) = ax^2 + bxy + cy^2$.
- D_Q: discriminant of Q,

$$D_Q := b^2 - 4ac \equiv 0, 1 \mod 4$$

Quadratic forms

Some notation:

- Q: binary quadratic form, $Q(x, y) = ax^2 + bxy + cy^2$.
- D_Q: discriminant of Q,

$$D_Q := b^2 - 4ac \equiv 0, 1 \mod 4$$

- Say that two forms Q, Q' are *equivalent* if related by linear change of variables, i.e.,

$$Q'(x, y) = Q(\alpha x + \beta y, \gamma x + \delta y), \quad \alpha\delta - \beta\gamma \neq 0$$

Quadratic forms

Some notation:

- Q: binary quadratic form, $Q(x, y) = ax^2 + bxy + cy^2$.
- D_Q: discriminant of Q,

$$D_Q := b^2 - 4ac \equiv 0, 1 \mod 4$$

- Say that two forms Q, Q' are *equivalent* if related by linear change of variables, i.e.,

$$Q'(x, y) = Q(\alpha x + \beta y, \gamma x + \delta y), \quad \alpha\delta - \beta\gamma \neq 0$$

Examples (linear algebra):

- $\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{R}, D_Q \neq 0\}/GL_2(\mathbb{R}) = \{\pm x^2 + \pm y^2\}$

Quadratic forms

Some notation:

- Q: binary quadratic form, $Q(x,y) = ax^2 + bxy + cy^2$.
- D_Q: discriminant of Q,

$$D_Q := b^2 - 4ac \equiv 0, 1 \mod 4$$

- Say that two forms Q, Q' are *equivalent* if related by linear change of variables, i.e.,

$$Q'(x,y) = Q(\alpha x + \beta y, \gamma x + \delta y), \quad \alpha\delta - \beta\gamma \neq 0$$

Examples (linear algebra):

- $\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{R}, D_Q \neq 0\}/GL_2(\mathbb{R}) = \{\pm x^2 + \pm y^2\}$
- $\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{R}, D_Q \neq 0\}/O_2(\mathbb{R}) = \{\lambda_1 x^2 + \lambda_2 y^2, \lambda_1, \lambda_2 \in \mathbb{R}\}$

Number theory version

What if we only allow integer coefficients, i.e.,

$$\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q \neq 0\}/GL_2(\mathbb{Z}) = ???$$

Number theory version

What if we only allow integer coefficients, i.e.,

$$\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q \neq 0\}/GL_2(\mathbb{Z}) = ???$$

Turns out: $D_Q = D_{Q'}$ if Q' is $GL_2(\mathbb{Z})$-equivalent to Q.
Thus natural to fix $d < 0$ and consider:

$$H(d) := \{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q = d\}/GL_2(\mathbb{Z})$$

Number theory version

What if we only allow integer coefficients, i.e.,

$$\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q \neq 0\}/GL_2(\mathbb{Z}) = ???$$

Turns out: $D_Q = D_{Q'}$ if Q' is $GL_2(\mathbb{Z})$-equivalent to Q.
Thus natural to fix $d < 0$ and consider:

$$H(d) := \{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q = d\}/GL_2(\mathbb{Z})$$

Fact 1: the class number $h(d) := |H(d)|$ is **finite**.
Fact 2: we can make $H(d)$ into an abelian **group**.

Number theory version

What if we only allow integer coefficients, i.e.,

$$\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q \neq 0\}/GL_2(\mathbb{Z}) = ???$$

Turns out: $D_Q = D_{Q'}$ if Q' is $GL_2(\mathbb{Z})$-equivalent to Q.
Thus natural to fix $d < 0$ and consider:

$$H(d) := \{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q = d\}/GL_2(\mathbb{Z})$$

Fact 1: the class number $h(d) := |H(d)|$ is **finite**.
Fact 2: we can make $H(d)$ into an abelian **group**.
Fact 1: not so difficult. (Any Q is equivalent to "reduced form", only finite number of reduced ones.)

Number theory version

What if we only allow integer coefficients, i.e.,

$$\{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q \neq 0\}/GL_2(\mathbb{Z}) = ???$$

Turns out: $D_Q = D_{Q'}$ if Q' is $GL_2(\mathbb{Z})$-equivalent to Q.
Thus natural to fix $d < 0$ and consider:

$$H(d) := \{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, D_Q = d\}/GL_2(\mathbb{Z})$$

Fact 1: the class number $h(d) := |H(d)|$ is **finite**.
Fact 2: we can make $H(d)$ into an abelian **group**.
Fact 1: not so difficult. (Any Q is equivalent to "reduced form", only finite number of reduced ones.)
Fact 2: Gauss was a genious!

Gauss and class numbers/groups

Modern way to get fact 2 (group structure): roughly have

$$H(d) \simeq \{\text{ideals in } \mathbb{Z}_K\}/\{\text{principal ideals in } \mathbb{Z}_K\}$$

where $\mathbb{Z}_K$ is the ring of integers in $K = \mathbb{Q}(\sqrt{d})$.

Gauss and class numbers/groups

Modern way to get fact 2 (group structure): roughly have

$$H(d) \simeq \{\text{ideals in } \mathbb{Z}_K\}/\{\text{principal ideals in } \mathbb{Z}_K\}$$

where $\mathbb{Z}_K$ is the ring of integers in $K = \mathbb{Q}(\sqrt{d})$.
In particular: $h(d) = 1$ iff $\mathbb{Z}_K$ is a PID.

Gauss and class numbers/groups

Modern way to get fact 2 (group structure): roughly have

$$H(d) \simeq \{\text{ideals in } \mathbb{Z}_K\}/\{\text{principal ideals in } \mathbb{Z}_K\}$$

where $\mathbb{Z}_K$ is the ring of integers in $K = \mathbb{Q}(\sqrt{d})$.
In particular: $h(d) = 1$ iff $\mathbb{Z}_K$ is a PID.
Some conjectures on $h(d)$:

- Gauss conjectured: $h(d) \to \infty$ as $d \to -\infty$.

Gauss and class numbers/groups

Modern way to get fact 2 (group structure): roughly have

$$H(d) \simeq \{\text{ideals in } \mathbb{Z}_K\}/\{\text{principal ideals in } \mathbb{Z}_K\}$$

where $\mathbb{Z}_K$ is the ring of integers in $K = \mathbb{Q}(\sqrt{d})$.
In particular: $h(d) = 1$ iff $\mathbb{Z}_K$ is a PID.
Some conjectures on $h(d)$:

- Gauss conjectured: $h(d) \to \infty$ as $d \to -\infty$.
- (Gauss) class number one problem: $h(d) = 1$ iff $d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\} \cup \{-12, -16, -27, -28\}$.

Gauss and class numbers/groups

Modern way to get fact 2 (group structure): roughly have

$$H(d) \simeq \{\text{ideals in } \mathbb{Z}_K\}/\{\text{principal ideals in } \mathbb{Z}_K\}$$

where $\mathbb{Z}_K$ is the ring of integers in $K = \mathbb{Q}(\sqrt{d})$.
In particular: $h(d) = 1$ iff $\mathbb{Z}_K$ is a PID.
Some conjectures on $h(d)$:

- Gauss conjectured: $h(d) \to \infty$ as $d \to -\infty$.
- (Gauss) class number one problem: $h(d) = 1$ iff $d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\} \cup \{-12, -16, -27, -28\}$.

Remark: Gauss only treated $Q(x, y) = ax^2 + 2bxy + cy^2$, and allowed "non-fundamental discriminants".

Gauss and class numbers/groups

Modern way to get fact 2 (group structure): roughly have

$$H(d) \simeq \{\text{ideals in } \mathbb{Z}_K\}/\{\text{principal ideals in } \mathbb{Z}_K\}$$

where $\mathbb{Z}_K$ is the ring of integers in $K = \mathbb{Q}(\sqrt{d})$.
In particular: $h(d) = 1$ iff $\mathbb{Z}_K$ is a PID.
Some conjectures on $h(d)$:

- Gauss conjectured: $h(d) \to \infty$ as $d \to -\infty$.
- (Gauss) class number one problem: $h(d) = 1$ iff $d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\} \cup \{-12, -16, -27, -28\}$.

Remark: Gauss only treated $Q(x, y) = ax^2 + 2bxy + cy^2$, and allowed "non-fundamental discriminants".
In what follows, will restrict to **fundamental discriminants**: $d \equiv 0, 1 \mod 4$ and $d = d_0$ or $d = 4d_0$ where d_0 is square free.

More on Gauss' conjectures

- Hecke (unpublished): if GRH is true, then $h(d) \to \infty$ as $d \to -\infty$.

More on Gauss' conjectures

- Hecke (unpublished): if GRH is true, then $h(d) \to \infty$ as $d \to -\infty$.
- Heilbronn: if GRH is **false(!!)**, then $h(d) \to \infty$ as $d \to -\infty$.

More on Gauss' conjectures

- Hecke (unpublished): if GRH is true, then $h(d) \to \infty$ as $d \to -\infty$.
- Heilbronn: if GRH is **false(!!)**, then $h(d) \to \infty$ as $d \to -\infty$.
- Siegel: $h(d) \gg_\epsilon |d|^{1/2-\epsilon}$ for all $\epsilon > 0$. PROBLEM: "horribly ineffective".

More on Gauss' conjectures

- Hecke (unpublished): if GRH is true, then $h(d) \to \infty$ as $d \to -\infty$.
- Heilbronn: if GRH is **false(!!)**, then $h(d) \to \infty$ as $d \to -\infty$.
- Siegel: $h(d) \gg_\epsilon |d|^{1/2-\epsilon}$ for all $\epsilon > 0$. PROBLEM: "horribly ineffective".
  Issue: by Dirichlet's class number formula,
  $$h(d) \gg L(1, \chi_d)|d|^{1/2}$$
  so ok if $L(1, \chi_d)$ not small. Problem: "Siegel zeros", i.e., $L(\sigma, \chi_d) = 0$ for σ very near 1.

More on Gauss' conjectures

- Hecke (unpublished): if GRH is true, then $h(d) \to \infty$ as $d \to -\infty$.
- Heilbronn: if GRH is **false(!!)**, then $h(d) \to \infty$ as $d \to -\infty$.
- Siegel: $h(d) \gg_\epsilon |d|^{1/2-\epsilon}$ for all $\epsilon > 0$. PROBLEM: "horribly ineffective".
  Issue: by Dirichlet's class number formula,

  $$h(d) \gg L(1, \chi_d)|d|^{1/2}$$

  so ok if $L(1, \chi_d)$ not small. Problem: "Siegel zeros", i.e., $L(\sigma, \chi_d) = 0$ for σ very near 1.
- Even though we know $h(d) \to \infty$, ineffectivity means we can't solve the class number one problem.

Class number one and beyond

- (Heegner)/Baker/Stark: class number one problem is solved by different methods. (Baker/Stark can also treat $h(d) = 2$.)

Class number one and beyond

- (Heegner)/Baker/Stark: class number one problem is solved by different methods. (Baker/Stark can also treat $h(d) = 2$.)
- Breakthrough by Goldfeld: **if** there is elliptic curve E such that $L_E(s)$ has high order of vanishing at $s = 1$, then have **effective** lower bound on $h(d)$.

Class number one and beyond

- (Heegner)/Baker/Stark: class number one problem is solved by different methods. (Baker/Stark can also treat $h(d) = 2$.)
- Breakthrough by Goldfeld: **if** there is elliptic curve E such that $L_E(s)$ has high order of vanishing at $s = 1$, then have **effective** lower bound on $h(d)$.
- Gross-Zagier: Such a curve exists!
- Oesterlé proved the explicit bound

$$h(d) > \frac{\log(|d|)}{7000} \prod_{p|d, p \neq d} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right),$$

and used this to find all d with $h(d) = 3$.

Class number one and beyond

- (Heegner)/Baker/Stark: class number one problem is solved by different methods. (Baker/Stark can also treat $h(d) = 2$.)
- Breakthrough by Goldfeld: **if** there is elliptic curve E such that $L_E(s)$ has high order of vanishing at $s = 1$, then have **effective** lower bound on $h(d)$.
- Gross-Zagier: Such a curve exists!
- Oesterlé proved the explicit bound

$$h(d) > \frac{\log(|d|)}{7000} \prod_{p|d, p \neq d} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right),$$

  and used this to find all d with $h(d) = 3$.
- Arno, Robinson-Wheeler, Wagner: $h(d) = N$ for $N \leq 7$, and odd $N \leq 23$.
- Watkins: $h(d) = N$ for $N \leq 100$. (Using low height zeros of $L(s, \chi)$ to "repel" Siegel zeros.) In particular, $h(d) > 100$ if $-d > 2.4 \cdot 10^6$.

Which class numbers/groups actually occur?

- Do all $h \in \mathbb{Z}^+$ **occur** as class numbers?
  - If occurring: how many times?

Which class numbers/groups actually occur?

- Do all $h \in \mathbb{Z}^+$ **occur** as class numbers?
  - If occurring: how many times?
- Do all abelian groups **occur** as class groups?
  - If occuring: how many times?

Which class numbers/groups actually occur?

- Do all $h \in \mathbb{Z}^+$ **occur** as class numbers?
  - If occurring: how many times?
- Do all abelian groups **occur** as class groups?
  - If occuring: how many times?
- Extreme case: fixed exponent and high rank.
  - Chowla: for $r \gg 1$, $(\mathbb{Z}/2\mathbb{Z})^r$ does **not** occur. (Ineffective!)
  - Boyd-Kisilevski, Weinberger, Heath-Brown: for $r \gg 1$ and $2 \leq n \leq 6$, $(\mathbb{Z}/n\mathbb{Z})^r$ does **not** occur. (Ineffective!)
  - Boyd-Kisilevski: on GRH, the exponent of $H(d)$ tends to infinity.

Which class numbers/groups actually occur?

- Do all $h \in \mathbb{Z}^+$ **occur** as class numbers?
  - If occurring: how many times?
- Do all abelian groups **occur** as class groups?
  - If occuring: how many times?
- Extreme case: fixed exponent and high rank.
  - Chowla: for $r \gg 1$, $(\mathbb{Z}/2\mathbb{Z})^r$ does **not** occur. (Ineffective!)
  - Boyd-Kisilevski, Weinberger, Heath-Brown: for $r \gg 1$ and $2 \leq n \leq 6$, $(\mathbb{Z}/n\mathbb{Z})^r$ does **not** occur. (Ineffective!)
  - Boyd-Kisilevski: on GRH, the exponent of $H(d)$ tends to infinity.
- Bounding $H(d)[l]$, the l-torsion part $H(d)$:
  - Pierce, Helfgott-Venkatesh, Ellenberg-Venkatesh:

$$|H(d)[3]| \ll |d|^{1/3+\epsilon}$$

  - Ellenberg-Venkatesh: on GRH, for $\ell > 3$

$$|H(d)[\ell]| \ll |d|^{1/2-1/2\ell+\epsilon}$$

Explicit groups that do **not** occur

What about some explicit examples of "missing" class groups?

- Watkins + pari computation: these groups do **not** occur:

$$(\mathbb{Z}/3\mathbb{Z})^3, \quad \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2, \quad (\mathbb{Z}/3\mathbb{Z})^4.$$

Explicit groups that do **not** occur

What about some explicit examples of "missing" class groups?

- Watkins + pari computation: these groups do **not** occur:

$$(\mathbb{Z}/3\mathbb{Z})^3, \quad \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2, \quad (\mathbb{Z}/3\mathbb{Z})^4.$$

- Note: rank r not that big, yet missing!

Explicit groups that do **not** occur

What about some explicit examples of “missing” class groups?

- Watkins + pari computation: these groups do **not** occur:

$$(\mathbb{Z}/3\mathbb{Z})^3, \quad \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2, \quad (\mathbb{Z}/3\mathbb{Z})^4.$$

- Note: rank r not that big, yet missing!
- For $h \in \mathbb{Z}^+$ and G a finite abelian group, define

$$F(h) := |\{d < 0 : h(d) = h\}|, \quad F(G) := |\{d < 0 : H(d) = G\}|$$

(recall: d always denotes fundamental discriminant.)

Explicit groups that do **not** occur

What about some explicit examples of "missing" class groups?

- Watkins + pari computation: these groups do **not** occur:

$$(\mathbb{Z}/3\mathbb{Z})^3, \quad \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2, \quad (\mathbb{Z}/3\mathbb{Z})^4.$$

- Note: rank r not that big, yet missing!
- For $h \in \mathbb{Z}^+$ and G a finite abelian group, define

$$F(h) := |\{d < 0 : h(d) = h\}|, \quad F(G) := |\{d < 0 : H(d) = G\}|$$

(recall: d always denotes fundamental discriminant.)
- Can we (conjecturally) determine growth of $F(h)$ or $F(G)$?

For simplicity, restrict to

- h odd, hence d **prime**. (2-rank of $H(d)$ given by $\omega(d) - 1$.)

For simplicity, restrict to

- h odd, hence d **prime**. (2-rank of $H(d)$ given by $\omega(d) - 1$.)
- G a p-group.

For simplicity, restrict to

- h odd, hence d **prime**. (2-rank of $H(d)$ given by $\omega(d) - 1$.)
- G a p-group.

Average of $F(h)$: prime discriminant analog of Soundararajan.

For simplicity, restrict to

- h odd, hence d **prime**. (2-rank of $H(d)$ given by $\omega(d) - 1$.)
- G a p-group.

Average of $F(h)$: prime discriminant analog of Soundararajan.

Theorem (Holmin-Jones-K.-McLeman-Petersen)

Assume GRH. For any $\epsilon > 0$,

$$\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h) = \frac{15}{4} \cdot \frac{H^2}{\log H} \left(1 + O\left(\frac{1}{(\log H)^{1/2-\epsilon}}\right)\right),$$

as $H \longrightarrow \infty$.

For simplicity, restrict to

- h odd, hence d **prime**. (2-rank of $H(d)$ given by $\omega(d)-1$.)
- G a p-group.

Average of $F(h)$: prime discriminant analog of Soundararajan.

Theorem (Holmin-Jones-K.-McLeman-Petersen)

Assume GRH. For any $\epsilon > 0$,

$$\sum_{\substack{h \le H \\ h \text{ odd}}} F(h) = \frac{15}{4} \cdot \frac{H^2}{\log H} \left(1 + O\left(\frac{1}{(\log H)^{1/2-\epsilon}}\right)\right),$$

as $H \longrightarrow \infty$.

Thus expect (in fact, conjectured by Soundararajan):

$$F(h) \asymp \frac{h}{\log h} \qquad (h \text{ odd})$$

Puzzling...

Initial numerics: find all d such that $h(d)$ odd and $\lessapprox 10^4$ — look at d up to $\sim 10^{12}$. (On GRH, using Lamzouri-Li-Soundararajan.)

Puzzling...

Initial numerics: find all d such that $h(d)$ odd and $\lessapprox 10^4$ — look at d up to $\sim 10^{12}$. (On GRH, using Lamzouri-Li-Soundararajan.)

Some data:

h	10001	10003	10005	10007	10009	10011	10013	10015
$F(h)$	10641	12154	**20661**	**10536**	10329	15966	12221	12975

Puzzling...

Initial numerics: find all d such that $h(d)$ odd and $\lessapprox 10^4$ — look at d up to $\sim 10^{12}$. (On GRH, using Lamzouri-Li-Soundararajan.)
Some data:

h	10001	10003	10005	10007	10009	10011	10013	10015
$F(h)$	10641	12154	**20661**	**10536**	10329	15966	12221	12975

- **Massive** swings — almost factor of two!

Puzzling...

Initial numerics: find all d such that $h(d)$ odd and $\lessapprox 10^4$ — look at d up to $\sim 10^{12}$. (On GRH, using Lamzouri-Li-Soundararajan.)
Some data:

h	10001	10003	10005	10007	10009	10011	10013	10015
$F(h)$	10641	12154	**20661**	**10536**	10329	15966	12221	12975

- **Massive** swings — almost factor of two!
- Troubling: using Theorem, i.e.,

$$\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h) \simeq \frac{15}{4} \cdot \frac{H^2}{\log H}$$

to predict local averages, say

$$\sum_{9500 \leq h \leq 9600, h \text{ odd}} F(h)$$

there is large bias compared to numerics (i.e., observed $F(h)$-values.)

Puzzling...

Initial numerics: find all d such that $h(d)$ odd and $\lesssim 10^4$ — look at d up to $\sim 10^{12}$. (On GRH, using Lamzouri-Li-Soundararajan.)
Some data:

h	10001	10003	10005	10007	10009	10011	10013	10015
$F(h)$	10641	12154	**20661**	**10536**	10329	15966	12221	12975

- **Massive** swings — almost factor of two!
- Troubling: using Theorem, i.e.,

$$\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h) \simeq \frac{15}{4} \cdot \frac{H^2}{\log H}$$

to predict local averages, say

$$\sum_{9500 \leq h \leq 9600, h \text{ odd}} F(h)$$

there is large bias compared to numerics (i.e., observed $F(h)$-values.) Prediction about 30% too high. WTF!?

"Unpuzzling"

- Better numerics: find all d such that $h(d)$ odd and $< 10^6$. Big computation — look at d up to 10^{15}. (Lucky: top 50 supercomputer at KTH!)

"Unpuzzling"

- Better numerics: find all d such that $h(d)$ odd and $< 10^6$. Big computation — look at d up to 10^{15}. (Lucky: top 50 supercomputer at KTH!)
- Higher order expansion for $\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h)$ in terms of powers of $1/\log h$. (Even though relative error is $O(1/\sqrt{\log h})$...)

"Unpuzzling"

- Better numerics: find all d such that $h(d)$ odd and $< 10^6$. Big computation — look at d up to 10^{15}. (Lucky: top 50 supercomputer at KTH!)
- Higher order expansion for $\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h)$ in terms of powers of $1/\log h$. (Even though relative error is $O(1/\sqrt{\log h})$...) Obtain "Archimedean" density $c_\infty(h)$ for $F(h)$.

"Unpuzzling"

- Better numerics: find all d such that $h(d)$ odd and $< 10^6$. Big computation — look at d up to 10^{15}. (Lucky: top 50 supercomputer at KTH!)
- Higher order expansion for $\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h)$ in terms of powers of $1/\log h$. (Even though relative error is $O(1/\sqrt{\log h})$...) Obtain "Archimedean" density $c_\infty(h)$ for $F(h)$.
- Capture small scale swings with local p-adic densities (Cohen-Lenstra!)

"Unpuzzling"

- Better numerics: find all d such that $h(d)$ odd and $< 10^6$. Big computation — look at d up to 10^{15}. (Lucky: top 50 supercomputer at KTH!)
- Higher order expansion for $\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h)$ in terms of powers of $1/\log h$. (Even though relative error is $O(1/\sqrt{\log h})$...) Obtain "Archimedean" density $c_\infty(h)$ for $F(h)$.
- Capture small scale swings with local p-adic densities (Cohen-Lenstra!)

Get "mass formula" (adelic/global density):

“Unpuzzling”

- Better numerics: find all d such that $h(d)$ odd and $< 10^6$. Big computation — look at d up to 10^{15}. (Lucky: top 50 supercomputer at KTH!)
- Higher order expansion for $\sum_{\substack{h \leq H \\ h \text{ odd}}} F(h)$ in terms of powers of $1/\log h$. (Even though relative error is $O(1/\sqrt{\log h})$...) Obtain “Archimedean” density $c_\infty(h)$ for $F(h)$.
- Capture small scale swings with local p-adic densities (Cohen-Lenstra!)

Get “mass formula” (adelic/global density):

$$F(h) \sim C \cdot \left(\prod_p c_p(h) \right) \cdot c_\infty(h)$$

$$\sim C \cdot c(h) \cdot \frac{h}{15} \cdot \mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2 \log(\pi h / L(1,\mathbb{Y}))} \right) \sim C \cdot c(h) \cdot \frac{h}{\log(\pi h)}$$

Two loose ends

Cohen-Lenstra prediction:

- Natural "measure" on how often a group should occur:

$$Pr(H(d) = G) \sim \frac{1}{\text{Aut}(G)}$$

Two loose ends

Cohen-Lenstra prediction:

- Natural "measure" on how often a group should occur:

$$Pr(H(d) = G) \sim \frac{1}{\mathrm{Aut}(G)}$$

  - $P(H(d) = \mathbb{Z}/p^2) \sim \frac{1}{\phi(p^2)} \simeq \frac{1}{p^2}$
  - $P(H(d) = \mathbb{Z}/p \times \mathbb{Z}/p) \sim \frac{1}{|GL_2(\mathbb{Z}/p\mathbb{Z})|} \simeq \frac{1}{p^4}$ — much rarer!
  - $P(3|h(d)) \simeq 0.43 \neq 1/3$

Two loose ends

Cohen-Lenstra prediction:

- Natural "measure" on how often a group should occur:

$$Pr(H(d) = G) \sim \frac{1}{\text{Aut}(G)}$$

  - $P(H(d) = \mathbb{Z}/p^2) \sim \frac{1}{\phi(p^2)} \simeq \frac{1}{p^2}$
  - $P(H(d) = \mathbb{Z}/p \times \mathbb{Z}/p) \sim \frac{1}{|GL_2(\mathbb{Z}/p\mathbb{Z})|} \simeq \frac{1}{p^4}$ — much rarer!
  - $P(3|h(d)) \simeq 0.43 \neq 1/3$

Recall Archimedean factor containing

$$\mathbb{E}\left(\frac{1}{L(1, \mathbb{Y})^2 \log(\pi h / L(1, \mathbb{Y}))}\right)$$

Two loose ends

Cohen-Lenstra prediction:

- Natural "measure" on how often a group should occur:

$$Pr(H(d) = G) \sim \frac{1}{\mathrm{Aut}(G)}$$

  - $P(H(d) = \mathbb{Z}/p^2) \sim \frac{1}{\phi(p^2)} \simeq \frac{1}{p^2}$
  - $P(H(d) = \mathbb{Z}/p \times \mathbb{Z}/p) \sim \frac{1}{|GL_2(\mathbb{Z}/p\mathbb{Z})|} \simeq \frac{1}{p^4}$ — much rarer!
  - $P(3|h(d)) \simeq 0.43 \neq 1/3$

Recall Archimedean factor containing

$$\mathbb{E}\left(\frac{1}{L(1,\mathbb{Y})^2 \log(\pi h/L(1,\mathbb{Y}))}\right)$$

Here $L(1,\mathbb{Y})$ is "random Euler product":

$$L(1,\mathbb{Y}) = \prod_p (1 - \mathbb{Y}_p/p)^{-1}$$

where $\mathbb{Y}_p = \pm 1$ (each with probability $1/2$.)

Our tweaked prediction:

$$\text{pred}(h) := C \cdot c(h) \cdot \frac{h}{\log(\pi h)} \cdot \left(1 + \frac{c_1}{\log(\pi h)} + \frac{c_2}{\log^2(\pi h)} + \frac{c_3}{\log^3(\pi h)}\right).$$

Our tweaked prediction:

$$\text{pred}(h) := C \cdot c(h) \cdot \frac{h}{\log(\pi h)} \cdot \left(1 + \frac{c_1}{\log(\pi h)} + \frac{c_2}{\log^2(\pi h)} + \frac{c_3}{\log^3(\pi h)}\right).$$

Relative error: $(F(h) - \text{pred}(h)) / \text{pred}(h)$

Our tweaked prediction:

$$\text{pred}(h) := C \cdot c(h) \cdot \frac{h}{\log(\pi h)} \cdot \left(1 + \frac{c_1}{\log(\pi h)} + \frac{c_2}{\log^2(\pi h)} + \frac{c_3}{\log^3(\pi h)}\right).$$

Relative error: $(F(h) - \text{pred}(h))/\,\text{pred}(h)$

h	10001	10003	10005	10007	10009	10011
$F(h)$	10641	12154	20661	10536	10329	15966
pred(h)	10598	12116	21074	10383	10385	16144
Rel. err.	+0.41%	+0.31%	−1.96%	+1.48%	−0.54%	−1.10%

h	100001	100003	100005	100007	100009	100011
$F(h)$	94623	85792	164289	86770	111948	142512
pred(h)	94213	85641	164806	86620	111210	142989
Rel. err.	+0.43%	+0.18%	−0.31%	+0.17%	+0.66%	−0.33%

h	999985	999987	999989	999991	999993	999995
$F(h)$	1064529	1095135	771805	791007	1093645	914482
pred(h)	1063376	1098842	769673	788871	1093732	911447
Rel. err.	+0.11%	−0.34%	+0.28%	+0.27%	−0.01%	+0.33%

For large h the prediction seems fairly good: relative error is $< 1\%$.

For large h the prediction seems fairly good: relative error is $< 1\%$.
In order to detect bias, look at *normalized fluctuations*

$$r(h) := \frac{F(h) - \text{pred}(h)}{\sqrt{\text{pred}(h)}}$$

for various subsets of the (odd) integers.

For large h the prediction seems fairly good: relative error is $< 1\%$.
In order to detect bias, look at *normalized fluctuations*

$$r(h) := \frac{F(h) - \text{pred}(h)}{\sqrt{\text{pred}(h)}}$$

for various subsets of the (odd) integers.
Audience guess: what kind of fluctuations?

For large h the prediction seems fairly good: relative error is $< 1\%$.
In order to detect bias, look at *normalized fluctuations*

$$r(h) := \frac{F(h) - \text{pred}(h)}{\sqrt{\text{pred}(h)}}$$

for various subsets of the (odd) integers.
Audience guess: what kind of fluctuations? Gaussian!?

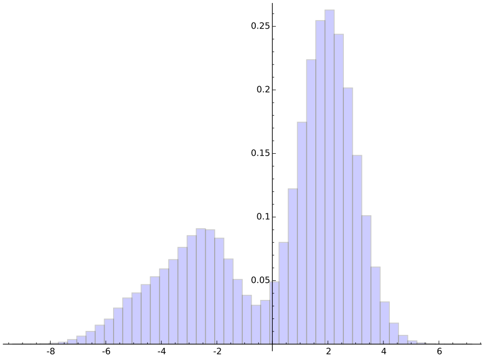

Figure: Histogram for $r(h)$, as h ranges over odd integers in $[500000, 1000000]$. $(\mu, \sigma) = (0.291561, 2.685280)$.

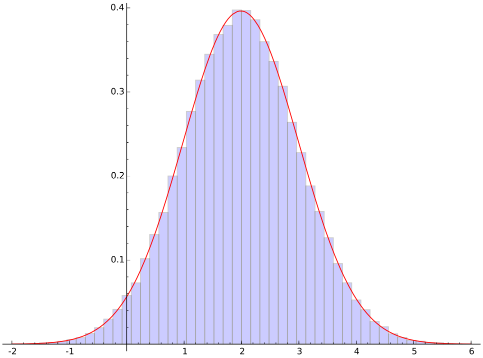

Figure: Histogram for $r(h)$, as $h \not\equiv 0 \mod 3$ ranges over odd integers in $[500000, 1000000]$. $(\mu, \sigma) = (1.987995, 1.006428)$.

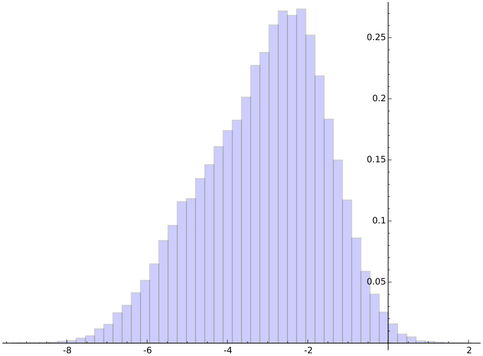

Figure: Histogram for $r(h)$, as $h \equiv 0 \mod 3$ ranges over odd integers in $[500000, 1000000]$. $(\mu, \sigma) = (-3.101265, 1.529449)$.

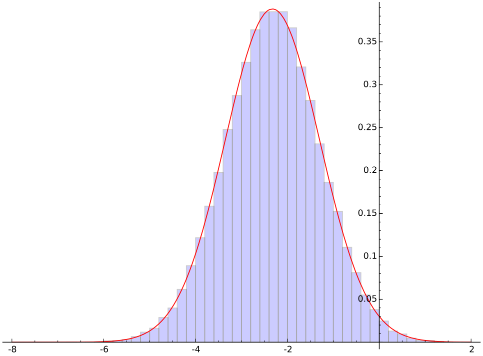

Figure: Histogram for $r(h)$, for odd h in (500000,1000000), $3||h$. $(\mu, \sigma) = (-2.326289, 1.027387)$.

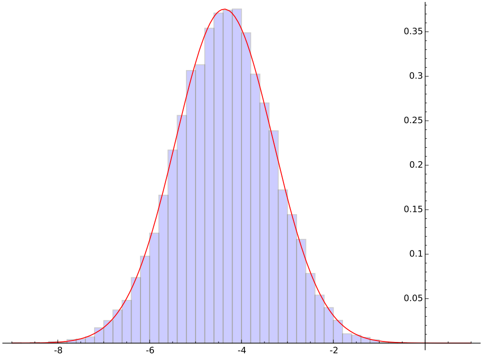

Figure: Histogram for $r(h)$, for odd h in (500000,1000000), $3^2 || h$. $(\mu, \sigma) = (-4.372185, 1.062480)$.

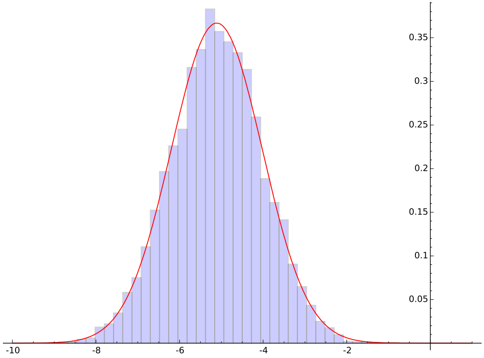

Figure: Histogram for $r(h)$, for odd h in (500000,1000000), $3^3 || h$. $(\mu, \sigma) = (-5.110585, 1.087463)$.

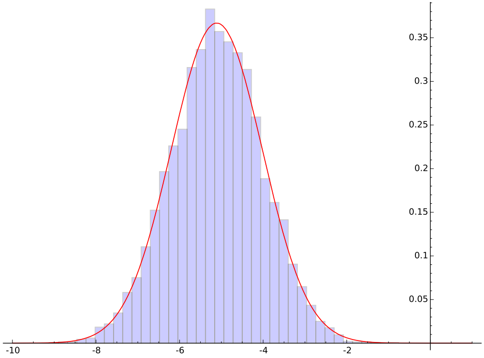

Figure: Histogram for $r(h)$, for odd h in (500000,1000000), $3^3 || h$. $(\mu, \sigma) = (-5.110585, 1.087463)$.

Seems to be systematic bias coming from 3-divisibility. Most likely similar to Davenport-Heilbronn bias:

- Main term: pole at $s = 1$
- Secondary term: pole at $s = 5/6$. (Mysterious!)

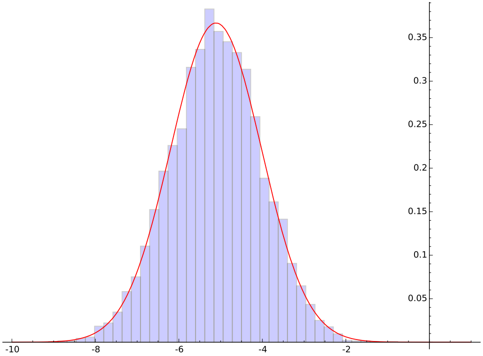

Figure: Histogram for $r(h)$, for odd h in (500000,1000000), $3^3 || h$. $(\mu, \sigma) = (-5.110585, 1.087463)$.

Seems to be systematic bias coming from 3-divisibility. Most likely similar to Davenport-Heilbronn bias:

- Main term: pole at $s = 1$
- Secondary term: pole at $s = 5/6$. (Mysterious!)

Note: we don't see similar bias for ℓ-divisibility, $\ell > 3$ small odd

Upshot of $F(h)$ prediction. And what groups occur?

- Very good fit with numerics ($< 1\%$ relative error.)

Upshot of $F(h)$ prediction. And what groups occur?

- Very good fit with numerics ($< 1\%$ relative error.)
- Puzzling "three divisibility bias".

Upshot of $F(h)$ prediction. And what groups occur?

- Very good fit with numerics ($< 1\%$ relative error.)
- Puzzling "three divisibility bias".
- Separating out h so that $3^a || h$, normalized fluctuations seem Gaussian (with variance very close to one!)

Upshot of $F(h)$ prediction. And what groups occur?

- Very good fit with numerics ($< 1\%$ relative error.)
- Puzzling "three divisibility bias".
- Separating out h so that $3^a || h$, normalized fluctuations seem Gaussian (with variance very close to one!)

Let's switch gears — which **groups** occur?

Upshot of $F(h)$ prediction. And what groups occur?

- Very good fit with numerics ($< 1\%$ relative error.)
- Puzzling "three divisibility bias".
- Separating out h so that $3^a || h$, normalized fluctuations seem Gaussian (with variance very close to one!)

Let's switch gears — which **groups** occur?

- For simplicity, only consider p-groups.
  - Too much data if we keep all groups.
  - Numeric speedup by looking for (noncyclic) p-groups.

Upshot of $F(h)$ prediction. And what groups occur?

- Very good fit with numerics ($< 1\%$ relative error.)
- Puzzling "three divisibility bias".
- Separating out h so that $3^a || h$, normalized fluctuations seem Gaussian (with variance very close to one!)

Let's switch gears — which **groups** occur?

- For simplicity, only consider p-groups.
  - Too much data if we keep all groups.
  - Numeric speedup by looking for (noncyclic) p-groups.
- Independence assumption: given abelian group G,

$$P\Big(H(d) = G\Big) = P\Big(h(d) = |G|\Big) \cdot P\Big(H(d) = G \Big| h(d) = |G|\Big)$$

Upshot of $F(h)$ prediction. And what groups occur?

- Very good fit with numerics ($< 1\%$ relative error.)
- Puzzling "three divisibility bias".
- Separating out h so that $3^a || h$, normalized fluctuations seem Gaussian (with variance very close to one!)

Let's switch gears — which **groups** occur?

- For simplicity, only consider p-groups.
  - Too much data if we keep all groups.
  - Numeric speedup by looking for (noncyclic) p-groups.
- Independence assumption: given abelian group G,

$$P\Big(H(d) = G\Big) = P\Big(h(d) = |G|\Big) \cdot P\Big(H(d) = G \Big| h(d) = |G|\Big)$$

  - Use $F(h)$-prediction for first term.
  - Use Cohen-Lenstra prediction for second term.

"Types" of p-groups of order p^2:

- Partitions of 2:
  - $2 = 2$:
  - $2 = 1 + 1$:
- Corresponding groups:
  - $G = \mathbb{Z}/p^2$
  - $G = \mathbb{Z}/p \times \mathbb{Z}/p$ (rare, zero "cyclicity index".)

"Types" of p-groups of order p^2:

- Partitions of 2:
  - $2 = 2$:
  - $2 = 1 + 1$:
- Corresponding groups:
  - $G = \mathbb{Z}/p^2$
  - $G = \mathbb{Z}/p \times \mathbb{Z}/p$ (rare, zero "cyclicity index".)

Groups of order p^3:

- Partitions of 3:
  - $3 = 3$:
  - $3 = 2 + 1$:
  - $3 = 1 + 1 + 1$:
- Corresponding groups:
  - $G = \mathbb{Z}/p^3$
  - $G = \mathbb{Z}/p^2 \times \mathbb{Z}/p$
  - $G = \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p$ (very rare, negative "cyclicity index".)

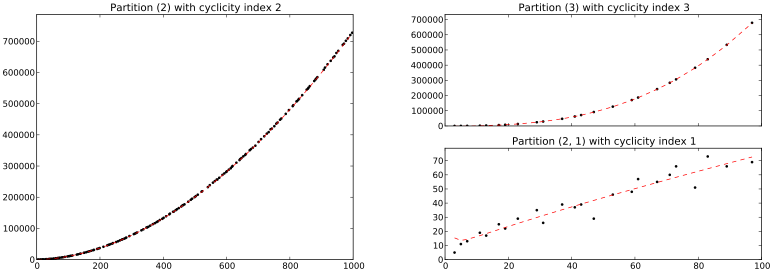

Figure: Partitions of 2 and 3 with cyclicity index > 0. Corresponding groups: $\mathbb{Z}/p^2$, $\mathbb{Z}/p^3$, and $\mathbb{Z}/p^2 \times \mathbb{Z}/p$.

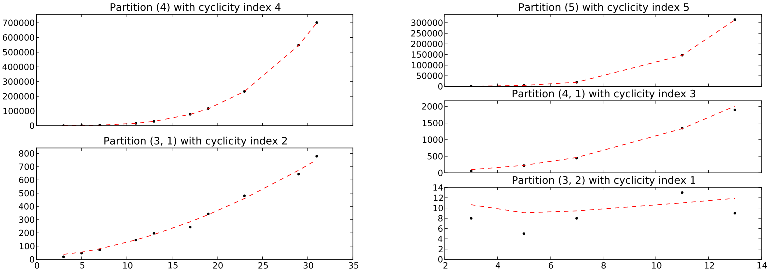

Figure: Partitions of 4 and 5. Corresponding groups: $\mathbb{Z}/p^4$, $\mathbb{Z}/p^3 \times \mathbb{Z}/p$, $\mathbb{Z}/p^5$, $\mathbb{Z}/p^4 \times \mathbb{Z}/p$ $\mathbb{Z}/p^2 \times \mathbb{Z}/p$, and $\mathbb{Z}/p^3 \times \mathbb{Z}/p^2$.

"Sporadic" groups

Each of the groups

$$\frac{\mathbb{Z}}{5^3\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^2, \qquad \frac{\mathbb{Z}}{3^4\mathbb{Z}} \times \frac{\mathbb{Z}}{3^2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \left(\frac{\mathbb{Z}}{3^3\mathbb{Z}}\right)^2 \times \frac{\mathbb{Z}}{3\mathbb{Z}},$$

$$\frac{\mathbb{Z}}{3^4\mathbb{Z}} \times \frac{\mathbb{Z}}{3^3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \frac{\mathbb{Z}}{3^5\mathbb{Z}} \times \frac{\mathbb{Z}}{3^3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \frac{\mathbb{Z}}{3^7\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{3^2\mathbb{Z}}\right)^2,$$

$$\frac{\mathbb{Z}}{3^6\mathbb{Z}} \times \frac{\mathbb{Z}}{3^4\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}, \qquad \frac{\mathbb{Z}}{3^8\mathbb{Z}} \times \frac{\mathbb{Z}}{3^2\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)^2$$

occurs exactly **once** as an imaginary quadratic class group, though partition has negative cyclicity index.

“Completely missing” families of groups

We haven’t seen **any** groups of the form

$$(\mathbb{Z}/p\mathbb{Z})^r$$

for $p > 2$ and $r \geq 3$. (Cyclicity index < 0.)

“Completely missing” families of groups

We haven’t seen **any** groups of the form

$$(\mathbb{Z}/p\mathbb{Z})^r$$

for $p > 2$ and $r \geq 3$. (Cyclicity index < 0.)
In particular, $(\mathbb{Z}/p\mathbb{Z})^3$ does not seem to occur.

"Completely missing" families of groups

We haven't seen **any** groups of the form

$$(\mathbb{Z}/p\mathbb{Z})^r$$

for $p > 2$ and $r \geq 3$. (Cyclicity index < 0.)
In particular, $(\mathbb{Z}/p\mathbb{Z})^3$ does not seem to occur.

Conjecture

No such group occurs as an imaginary quadratic class group.

“Completely missing” families of groups

We haven't seen **any** groups of the form

$$(\mathbb{Z}/p\mathbb{Z})^r$$

for $p > 2$ and $r \geq 3$. (Cyclicity index < 0.)
In particular, $(\mathbb{Z}/p\mathbb{Z})^3$ does not seem to occur.

Conjecture

No such group occurs as an imaginary quadratic class group.

Remark: probabilistic model suggests that “expected” number for $h > 10^6$ is $< 10^{-4}$.

"Completely missing" families of groups

We haven't seen **any** groups of the form

$$(\mathbb{Z}/p\mathbb{Z})^r$$

for $p > 2$ and $r \geq 3$. (Cyclicity index < 0.)
In particular, $(\mathbb{Z}/p\mathbb{Z})^3$ does not seem to occur.

Conjecture

No such group occurs as an imaginary quadratic class group.

Remark: probabilistic model suggests that "expected" number for $h > 10^6$ is $< 10^{-4}$.

Theorem

For a positive integer n, we have

$$\frac{\#\{\text{partitions of } n \text{ with cyclicity index} > 0\}}{\#\{\text{partitions of } n\}} \ll n^{3/4} e^{(2-\sqrt{\frac{2}{3}}\pi)\sqrt{n}}.$$

In particular, ratio $\to 0$: most p-groups likely to be "missing"!

Zero cyclicity index

Intermediate case: infinitely many groups in the family should occur, and infinitely many should not.

Zero cyclicity index

Intermediate case: infinitely many groups in the family should occur, and infinitely many should not.
Data quite limited, restrict to the family $G = (\mathbb{Z}/p\mathbb{Z})^2$.

Zero cyclicity index

Intermediate case: infinitely many groups in the family should occur, and infinitely many should not.
Data quite limited, restrict to the family $G = (\mathbb{Z}/p\mathbb{Z})^2$.

n	All primes $p < 1000$ such that $\mathcal{F}((\mathbb{Z}/p\mathbb{Z})^2) = n$
0	11, 19, 37, 79, 89, 97, 103, 139, 151, 167, 181, 191, 193, 227, 229, 233, 241, 251, 271, 281, 283, 311, 313, 317, 349 409, 433, 443, 463, 467, 479, 491, 499, 523, 563, 571, 587, 601, 619, 631, 643, 673, 701, 709, 733, 757, 769, 787, 907, 919, 929, 947, 953, 977, 983
1	3, 17, 23, 41, 43, 47, 61, 67, 73, 107, 109, 113, 127, 131, 137, 157, 163, 173, 179, 199, 239, 257, 263, 269, 277, 293 367, 373, 379, 397, 419, 439, 457, 487, 503, 509, 521, 547, 557, 577, 599, 613, 617, 641, 653, 659, 677, 683, 691, 761, 797, 811, 821, 823, 839, 853, 857, 859, 863, 881, 937, 941, 971, 991, 997
2	5, 7, 29, 31, 53, 59, 71, 83, 101, 197, 211, 223, 389, 431, 449, 461, 569, 593, 607, 647, 661, 827, 883, 911
3	149, 421, 541, 751, 967
4	773
5	13

Seems to support intermediate behaviour.

Zero cyclicity index

Intermediate case: infinitely many groups in the family should occur, and infinitely many should not.
Data quite limited, restrict to the family $G = (\mathbb{Z}/p\mathbb{Z})^2$.

n	All primes $p < 1000$ such that $\mathcal{F}((\mathbb{Z}/p\mathbb{Z})^2) = n$
0	11, 19, 37, 79, 89, 97, 103, 139, 151, 167, 181, 191, 193, 227, 229, 233, 241, 251, 271, 281, 283, 311, 313, 317, 349 409, 433, 443, 463, 467, 479, 491, 499, 523, 563, 571, 587, 601, 619, 631, 643, 673, 701, 709, 733, 757, 769, 787, 907, 919, 929, 947, 953, 977, 983
1	3, 17, 23, 41, 43, 47, 61, 67, 73, 107, 109, 113, 127, 131, 137, 157, 163, 173, 179, 199, 239, 257, 263, 269, 277, 293 367, 373, 379, 397, 419, 439, 457, 487, 503, 509, 521, 547, 557, 577, 599, 613, 617, 641, 653, 659, 677, 683, 691, 761, 797, 811, 821, 823, 839, 853, 857, 859, 863, 881, 937, 941, 971, 991, 997
2	5, 7, 29, 31, 53, 59, 71, 83, 101, 197, 211, 223, 389, 431, 449, 461, 569, 593, 607, 647, 661, 827, 883, 911
3	149, 421, 541, 751, 967
4	773
5	13

Seems to support intermediate behaviour.
Remark: predicted "probability" that $\mathbb{Z}/p \times \mathbb{Z}/p$ occurs is about

$$1/\log p,$$

so most of these groups are "missing".

Zero cyclicity, comparing cumulants

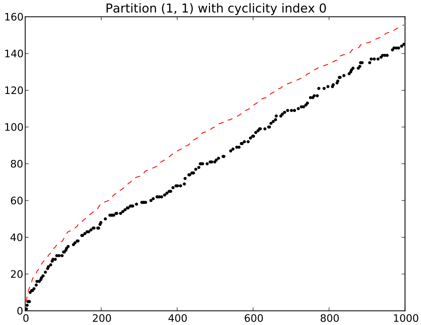

Figure: *Cumulative* observed values $\sum_{p<x} F(G_{(1,1)}(p))$ (black dots) compared to *cumulative* predicted values $\sum_{p<x} P(G_{(1,1)}(p))\,\mathrm{pred}(p^2)$ (red dashed line), for each prime $x < 1000$.

Happy Birthday Igor!