Arithmetic statistics in the $n = p$ case

Peter Koymans
Max Planck Institute for Mathematics

MAX-PLANCK-GESELLSCHAFT

Glasgow Algebra and Number Theory Seminar

20 January 2021

Arithmetic statistics

The area of arithmetic statistics focuses on the behavior of arithmetic objects in families. Typical questions are:

Arithmetic statistics

The area of arithmetic statistics focuses on the behavior of arithmetic objects in families. Typical questions are:

- How many number fields are there with given Galois group G and discriminant bounded by some real number $X > 0$?

Arithmetic statistics

The area of arithmetic statistics focuses on the behavior of arithmetic objects in families. Typical questions are:

- How many number fields are there with given Galois group G and discriminant bounded by some real number $X > 0$?
- What is the average (analytic/algebraic/Selmer) rank of elliptic curves when ordered by discriminant?

Arithmetic statistics

The area of arithmetic statistics focuses on the behavior of arithmetic objects in families. Typical questions are:

- How many number fields are there with given Galois group G and discriminant bounded by some real number $X > 0$?
- What is the average (analytic/algebraic/Selmer) rank of elliptic curves when ordered by discriminant?
- How does $\mathrm{Cl}(K)$ behave in a family of number fields K ordered by discriminant (for example quadratic number fields)?

In this talk we shall mostly focus on the third question.

Reminder: class groups

Let K be a number field. Then every (fractional) ideal I can be factored uniquely as

$$I = \mathfrak{p}_1^{a_1} \cdot \ldots \cdot \mathfrak{p}_r^{a_r},$$

where $a_1, \ldots, a_r \in \mathbb{Z}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime ideals of the ring of integers $\mathcal{O}_K$.

Reminder: class groups

Let K be a number field. Then every (fractional) ideal I can be factored uniquely as

$$I = \mathfrak{p}_1^{a_1} \cdot \ldots \cdot \mathfrak{p}_r^{a_r},$$

where $a_1, \ldots, a_r \in \mathbb{Z}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime ideals of the ring of integers $\mathcal{O}_K$.

Define I_K to be the set of fractional ideals and let P_K be the set of fractional ideals I of the shape $I = x\mathcal{O}_K$ for some $x \in K^*$.

Reminder: class groups

Let K be a number field. Then every (fractional) ideal I can be factored uniquely as

$$I = \mathfrak{p}_1^{a_1} \cdot \ldots \cdot \mathfrak{p}_r^{a_r},$$

where $a_1, \ldots, a_r \in \mathbb{Z}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime ideals of the ring of integers $\mathcal{O}_K$.

Define I_K to be the set of fractional ideals and let P_K be the set of fractional ideals I of the shape $I = x\mathcal{O}_K$ for some $x \in K^*$.

The elements of P_K are called principal ideals. Define the class group

$$\mathrm{Cl}(K) = I_K / P_K$$

Reminder: class groups

Let K be a number field. Then every (fractional) ideal I can be factored uniquely as

$$I = \mathfrak{p}_1^{a_1} \cdot \ldots \cdot \mathfrak{p}_r^{a_r},$$

where $a_1, \ldots, a_r \in \mathbb{Z}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime ideals of the ring of integers $\mathcal{O}_K$.

Define I_K to be the set of fractional ideals and let P_K be the set of fractional ideals I of the shape $I = x\mathcal{O}_K$ for some $x \in K^*$.

The elements of P_K are called principal ideals. Define the class group

$$\mathrm{Cl}(K) = I_K/P_K$$

and the narrow class group as

$$\mathrm{Cl}(K) = I_K/P_K^+,$$

where P_K^+ is the set of fractional ideals I of the shape $I = x\mathcal{O}_K$ with x totally positive.

The Cohen-Lenstra heuristics

Let p be an odd prime. The group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

The Cohen-Lenstra heuristics

Let p be an odd prime. The group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

More formally, Cohen and Lenstra conjectured that

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian p-group A.

The Cohen-Lenstra heuristics

Let p be an odd prime. The group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

More formally, Cohen and Lenstra conjectured that

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian p-group A.

For real quadratic fields

$$\lim_{X\to\infty} \frac{\left|\left\{K \text{ re. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}^+(K)[p^\infty] \cong A\right\}\right|}{|\{K \text{ re. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=2}^{\infty}\left(1-\frac{1}{p^i}\right)}{|A||\mathrm{Aut}(A)|},$$

where $\mathrm{Cl}^+(K)[p^\infty]$ is now the quotient of a random abelian group.

Genus theory

Recall that $p = 2$ is excluded from the Cohen–Lenstra conjectures. The reason for this is that the group $\mathrm{Cl}^+(K)[2]$ has a very predictable behavior unlike $\mathrm{Cl}^+(K)[p]$ for p odd.

Genus theory

Recall that $p = 2$ is excluded from the Cohen–Lenstra conjectures. The reason for this is that the group $\mathrm{Cl}^+(K)[2]$ has a very predictable behavior unlike $\mathrm{Cl}^+(K)[p]$ for p odd.

The description of $\mathrm{Cl}^+(K)[2]$ is due to Gauss and is known as genus theory. We have that

$$|\mathrm{Cl}^+(K)[2]| = 2^{\omega(D_K)-1}$$

and $\mathrm{Cl}^+(K)[2]$ is generated by the ramified prime ideals of $\mathcal{O}_K$.

Genus theory

Recall that $p = 2$ is excluded from the Cohen–Lenstra conjectures. The reason for this is that the group $\mathrm{Cl}^+(K)[2]$ has a very predictable behavior unlike $\mathrm{Cl}^+(K)[p]$ for p odd.

The description of $\mathrm{Cl}^+(K)[2]$ is due to Gauss and is known as genus theory. We have that

$$|\mathrm{Cl}^+(K)[2]| = 2^{\omega(D_K)-1}$$

and $\mathrm{Cl}^+(K)[2]$ is generated by the ramified prime ideals of $\mathcal{O}_K$.

If p divides the discriminant of $\mathbb{Q}(\sqrt{d})$, then p ramifies, so

$$\begin{array}{ccccc} \mathbb{Q}(\sqrt{d}) & \qquad & \mathfrak{p} & \qquad & \mathfrak{p}^2 = (p). \\ \Big| & & \Big| & & \\ \mathbb{Q} & & p & & \end{array}$$

There is precisely one relation between the ramified primes.

Gerth's modification

Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $(2\mathrm{Cl}(K))[2^\infty]$ that behaves randomly.

Gerth's modification

Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $(2\mathrm{Cl}(K))[2^\infty]$ that behaves randomly.

To be precise, Gerth conjectured the following

$$\lim_{X \to \infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, (2\mathrm{Cl}(K))[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty} \left(1 - \frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian 2-group A, and similarly for real quadratics.

Gerth's modification

Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $(2\mathrm{Cl}(K))[2^\infty]$ that behaves randomly.

To be precise, Gerth conjectured the following

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, (2\mathrm{Cl}(K))[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian 2-group A, and similarly for real quadratics.

This is referred to as the $n = p$ case (n standing for the degree of the number fields, p for the torsion we are studying in the class group).

Known results in the $n = p$ case

Fouvry and Klüners dealt with the distribution of $(2\mathrm{Cl}(K))[2]$.

Known results in the $n = p$ case

Fouvry and Klüners dealt with the distribution of $(2\mathrm{Cl}(K))[2]$.

The full Gerth conjecture was recently proven by Alexander Smith (2017) for imaginary quadratics.

Known results in the $n = p$ case

Fouvry and Klüners dealt with the distribution of $(2\mathrm{Cl}(K))[2]$.

The full Gerth conjecture was recently proven by Alexander Smith (2017) for imaginary quadratics.

In the same paper Smith proved that for an elliptic curve $E/\mathbb{Q} : y^2 = x^3 + ax + b$ satisfying some technical assumptions that

- 50% of the quadratic twists $E^{(d)} : dy^2 = x^3 + ax + b$ have 2^∞-Selmer rank 0,
- 50% of the quadratic twists $E^{(d)} : dy^2 = x^3 + ax + b$ have 2^∞-Selmer rank 1.

Known results in the $n = p$ case

Fouvry and Klüners dealt with the distribution of $(2\mathrm{Cl}(K))[2]$.

The full Gerth conjecture was recently proven by Alexander Smith (2017) for imaginary quadratics.

In the same paper Smith proved that for an elliptic curve $E/\mathbb{Q} : y^2 = x^3 + ax + b$ satisfying some technical assumptions that

- 50% of the quadratic twists $E^{(d)} : dy^2 = x^3 + ax + b$ have 2^∞-Selmer rank 0,
- 50% of the quadratic twists $E^{(d)} : dy^2 = x^3 + ax + b$ have 2^∞-Selmer rank 1.

In particular this implies that the set set of congruent numbers equal to 1, 2 or 3 modulo 8 have zero natural density.

More results in the $n = p$ case

There is a natural analogue of Smith's results for cyclic field extensions of prime degree. If $K/\mathbb{Q}$ is cyclic of degree ℓ, then $\mathrm{Cl}(K)[\ell^\infty]$ is a $\mathbb{Z}_\ell[\mathrm{Gal}(K/\mathbb{Q})]$-module killed by the norm, i.e. a $\mathbb{Z}_\ell[\zeta_\ell]$-module.

More results in the $n = p$ case

There is a natural analogue of Smith's results for cyclic field extensions of prime degree. If $K/\mathbb{Q}$ is cyclic of degree ℓ, then $\mathrm{Cl}(K)[\ell^\infty]$ is a $\mathbb{Z}_\ell[\mathrm{Gal}(K/\mathbb{Q})]$-module killed by the norm, i.e. a $\mathbb{Z}_\ell[\zeta_\ell]$-module.

Theorem 1 (Gerth's conjecture, K.-Pagano 2018)

Assume GRH and let ℓ be an odd prime. Then for all finitely generated, torsion $\mathbb{Z}_\ell[\zeta_\ell]$-modules A the limit

$$\lim_{X \to \infty} \frac{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X, ((1 - \zeta_\ell)\mathrm{Cl}(K))[\ell^\infty] \cong A\}|}{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X\}|}$$

exists,

More results in the $n = p$ case

There is a natural analogue of Smith's results for cyclic field extensions of prime degree. If $K/\mathbb{Q}$ is cyclic of degree ℓ, then $\mathrm{Cl}(K)[\ell^\infty]$ is a $\mathbb{Z}_\ell[\mathrm{Gal}(K/\mathbb{Q})]$-module killed by the norm, i.e. a $\mathbb{Z}_\ell[\zeta_\ell]$-module.

Theorem 1 (Gerth's conjecture, K.-Pagano 2018)

Assume GRH and let ℓ be an odd prime. Then for all finitely generated, torsion $\mathbb{Z}_\ell[\zeta_\ell]$-modules A the limit

$$\lim_{X\to\infty} \frac{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X, ((1-\zeta_\ell)\mathrm{Cl}(K))[\ell^\infty] \cong A\}|}{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X\}|}$$

exists, and is equal to

$$\frac{\prod_{i=2}^{\infty}\left(1-\frac{1}{\ell^i}\right)}{|A||\mathrm{Aut}_{\mathbb{Z}_\ell[\zeta_\ell]}(A)|}.$$

More results in the $n = p$ case

There is a natural analogue of Smith's results for cyclic field extensions of prime degree. If $K/\mathbb{Q}$ is cyclic of degree ℓ, then $\mathrm{Cl}(K)[\ell^\infty]$ is a $\mathbb{Z}_\ell[\mathrm{Gal}(K/\mathbb{Q})]$-module killed by the norm, i.e. a $\mathbb{Z}_\ell[\zeta_\ell]$-module.

Theorem 1 (Gerth's conjecture, K.-Pagano 2018)

Assume GRH and let ℓ be an odd prime. Then for all finitely generated, torsion $\mathbb{Z}_\ell[\zeta_\ell]$-modules A the limit

$$\lim_{X \to \infty} \frac{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X, ((1 - \zeta_\ell)\mathrm{Cl}(K))[\ell^\infty] \cong A\}|}{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X\}|}$$

exists, and is equal to

$$\frac{\prod_{i=2}^{\infty} \left(1 - \frac{1}{\ell^i}\right)}{|A||\mathrm{Aut}_{\mathbb{Z}_\ell[\zeta_\ell]}(A)|}.$$

The proof can easily be adapted to also handle real quadratic fields.

More results in the $n = p$ case

There is a natural analogue of Smith's results for cyclic field extensions of prime degree. If $K/\mathbb{Q}$ is cyclic of degree ℓ, then $\mathrm{Cl}(K)[\ell^\infty]$ is a $\mathbb{Z}_\ell[\mathrm{Gal}(K/\mathbb{Q})]$-module killed by the norm, i.e. a $\mathbb{Z}_\ell[\zeta_\ell]$-module.

Theorem 1 (Gerth's conjecture, K.-Pagano 2018)

Assume GRH and let ℓ be an odd prime. Then for all finitely generated, torsion $\mathbb{Z}_\ell[\zeta_\ell]$-modules A the limit

$$\lim_{X \to \infty} \frac{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X, ((1 - \zeta_\ell)\mathrm{Cl}(K))[\ell^\infty] \cong A\}|}{|\{K/\mathbb{Q} \text{ cyc. deg. } \ell : |D_K| < X\}|}$$

exists, and is equal to

$$\frac{\prod_{i=2}^{\infty} \left(1 - \frac{1}{\ell^i}\right)}{|A||\mathrm{Aut}_{\mathbb{Z}_\ell[\zeta_\ell]}(A)|}.$$

The proof can easily be adapted to also handle real quadratic fields.

Smith generalized this to arbitrary base fields.

The negative Pell equation

Another classical problem is the negative Pell equation

$$x^2 - dy^2 = -1 \text{ to be solved in } x, y \in \mathbb{Z}. \tag{1}$$

The negative Pell equation is soluble iff $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ and $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty]$ coincide iff $(\sqrt{d})$ is trivial in $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2]$.

The negative Pell equation

Another classical problem is the negative Pell equation

$$x^2 - dy^2 = -1 \text{ to be solved in } x, y \in \mathbb{Z}. \tag{1}$$

The negative Pell equation is soluble iff $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ and $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty]$ coincide iff $(\sqrt{d})$ is trivial in $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2]$.

How often is the above equation soluble as one varies over squarefree integers d?

The negative Pell equation

Another classical problem is the negative Pell equation

$$x^2 - dy^2 = -1 \text{ to be solved in } x, y \in \mathbb{Z}. \tag{1}$$

The negative Pell equation is soluble iff $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ and $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty]$ coincide iff $(\sqrt{d})$ is trivial in $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2]$.

How often is the above equation soluble as one varies over squarefree integers d?

The answer is 0% of the time, since solubility with $x, y \in \mathbb{Q}$ is equivalent to every prime divisor p of d satisfying $p \equiv 1, 2 \bmod 4$.

Current results on negative Pell

Define $\mathcal{D}$ to be the set of squarefree integers d with $p \mid d$ implies $p \equiv 1, 2 \bmod 4$ and $\mathcal{D}^- \subseteq \mathcal{D}$ the subset for which negative Pell is soluble.

Current results on negative Pell

Define $\mathcal{D}$ to be the set of squarefree integers d with $p \mid d$ implies $p \equiv 1, 2 \bmod 4$ and $\mathcal{D}^- \subseteq \mathcal{D}$ the subset for which negative Pell is soluble.

Theorem 2 (Fouvry-Klüners, 2010)

We have

$$0.52475 \approx \frac{5}{4} \prod_{j=1}^{\infty} (1 + 2^{-j})^{-1} \leq \liminf_{X \to \infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \limsup_{X \to \infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \frac{2}{3}.$$

Current results on negative Pell

Define $\mathcal{D}$ to be the set of squarefree integers d with $p \mid d$ implies $p \equiv 1, 2 \bmod 4$ and $\mathcal{D}^- \subseteq \mathcal{D}$ the subset for which negative Pell is soluble.

Theorem 2 (Fouvry-Klüners, 2010)

We have

$$0.52475 \approx \frac{5}{4}\prod_{j=1}^{\infty}(1+2^{-j})^{-1} \leq \liminf_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \limsup_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \frac{2}{3}.$$

The lower bound was improved by Chan–K.–Milovic–Pagano (2019).

Current results on negative Pell

Define $\mathcal{D}$ to be the set of squarefree integers d with $p \mid d$ implies $p \equiv 1, 2 \bmod 4$ and $\mathcal{D}^- \subseteq \mathcal{D}$ the subset for which negative Pell is soluble.

Theorem 2 (Fouvry-Klüners, 2010)

We have

$$0.52475 \approx \frac{5}{4}\prod_{j=1}^{\infty}(1+2^{-j})^{-1} \leq \liminf_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \limsup_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \frac{2}{3}.$$

The lower bound was improved by Chan–K.–Milovic–Pagano (2019).

Theorem 3 (K.-Pagano, 2020)

We have

$$0.54302 \leq \liminf_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq \limsup_{X\to\infty} \frac{|\mathcal{D}^-(X)|}{|\mathcal{D}(X)|} \leq 0.59944.$$

A variant of the negative Pell equation

Fix a prime number $\ell \equiv 3 \bmod 4$. Define for squarefree $d > 0$

$$N_d(x, y) = \begin{cases} x^2 + xy - \frac{d-1}{4}y^2 & \text{if } d \equiv 1 \bmod 4 \\ x^2 - dy^2 & \text{otherwise.} \end{cases}$$

A variant of the negative Pell equation

Fix a prime number $\ell \equiv 3 \bmod 4$. Define for squarefree $d > 0$

$$N_d(x, y) = \begin{cases} x^2 + xy - \frac{d-1}{4}y^2 & \text{if } d \equiv 1 \bmod 4 \\ x^2 - dy^2 & \text{otherwise.} \end{cases}$$

We now consider the equation

$$N_d(x, y) = \ell \text{ in } x, y \in \mathbb{Z}, \tag{2}$$

where d only varies over squarefree integers divisible by ℓ. Equation (2) is soluble iff the unique ideal $\mathfrak{l}$ above ℓ is trivial in $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2]$.

A variant of the negative Pell equation

Fix a prime number $\ell \equiv 3 \bmod 4$. Define for squarefree $d > 0$

$$N_d(x, y) = \begin{cases} x^2 + xy - \frac{d-1}{4} y^2 & \text{if } d \equiv 1 \bmod 4 \\ x^2 - dy^2 & \text{otherwise.} \end{cases}$$

We now consider the equation

$$N_d(x, y) = \ell \text{ in } x, y \in \mathbb{Z}, \tag{2}$$

where d only varies over squarefree integers divisible by ℓ. Equation (2) is soluble iff the unique ideal $\mathfrak{l}$ above ℓ is trivial in $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2]$.

For a ring R, write $S_{R,X,\ell}$ for the set of squarefree integers $0 < d < X$ that are divisibly by ℓ and equation (2) is soluble with $x, y \in R$.

A variant of the negative Pell equation

Fix a prime number $\ell \equiv 3 \bmod 4$. Define for squarefree $d > 0$

$$N_d(x, y) = \begin{cases} x^2 + xy - \frac{d-1}{4}y^2 & \text{if } d \equiv 1 \bmod 4 \\ x^2 - dy^2 & \text{otherwise.} \end{cases}$$

We now consider the equation

$$N_d(x, y) = \ell \text{ in } x, y \in \mathbb{Z}, \tag{2}$$

where d only varies over squarefree integers divisible by ℓ. Equation (2) is soluble iff the unique ideal $\mathfrak{l}$ above ℓ is trivial in $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2]$.

For a ring R, write $S_{R,X,\ell}$ for the set of squarefree integers $0 < d < X$ that are divisibly by ℓ and equation (2) is soluble with $x, y \in R$.

Theorem 4 (K.-Pagano, 2020)

There exists $0 < C < 1$ *such that*

$$\lim_{X \to \infty} \frac{|S_{\mathbb{Z},X,\ell}|}{|S_{\mathbb{Q},X,\ell}|} = C.$$

An application to the Hasse Unit Index

For a biquadratic field $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, the Hasse Unit Index is defined to be

$$H_{a,b} := \left[\mathcal{O}^*_{\mathbb{Q}(\sqrt{a},\sqrt{b})} : \mathcal{O}^*_{\mathbb{Q}(\sqrt{a})}\mathcal{O}^*_{\mathbb{Q}(\sqrt{b})}\mathcal{O}^*_{\mathbb{Q}(\sqrt{ab})}\right].$$

If the biquadratic field is totally complex, then $H_{a,b} \in \{1, 2\}$.

An application to the Hasse Unit Index

For a biquadratic field $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, the Hasse Unit Index is defined to be

$$H_{a,b} := \left[\mathcal{O}^*_{\mathbb{Q}(\sqrt{a},\sqrt{b})} : \mathcal{O}^*_{\mathbb{Q}(\sqrt{a})}\mathcal{O}^*_{\mathbb{Q}(\sqrt{b})}\mathcal{O}^*_{\mathbb{Q}(\sqrt{ab})}\right].$$

If the biquadratic field is totally complex, then $H_{a,b} \in \{1, 2\}$.

Corollary 5 (K.-Pagano)

Let $\ell > 3$ be a prime 3 modulo 4. Then there is $C > 0$ such that

$$|\{0 < d < X \text{ squarefree} : H_{-\ell,d} = 2\}| \sim C\frac{X}{\sqrt{\log X}}.$$

Governing fields

Arithmetic statistics in the $n = p$ case has traditionally been studied through the viewpoint of *governing fields*.

Governing fields

Arithmetic statistics in the $n = p$ case has traditionally been studied through the viewpoint of *governing fields*.

Example 1

Let q be an odd prime number and write h_q for the class number of $\mathbb{Q}(\sqrt{-q})$. Then

$$\begin{aligned} 2 \mid h_q &\iff q \text{ splits in } \mathbb{Q}(i) \\ 4 \mid h_q &\iff q \text{ splits in } \mathbb{Q}(\zeta_8) \\ 8 \mid h_q &\iff q \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}). \end{aligned}$$

Governing fields

Arithmetic statistics in the $n = p$ case has traditionally been studied through the viewpoint of *governing fields*.

Example 1

Let q be an odd prime number and write h_q for the class number of $\mathbb{Q}(\sqrt{-q})$. Then

$$\begin{aligned} 2 \mid h_q &\iff q \text{ splits in } \mathbb{Q}(i) \\ 4 \mid h_q &\iff q \text{ splits in } \mathbb{Q}(\zeta_8) \\ 8 \mid h_q &\iff q \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}). \end{aligned}$$

Chebotarev Density Theorem then implies density results for the 2, 4 and 8-torsion of $\mathrm{Cl}(\mathbb{Q}(\sqrt{-q}))$.

Governing fields: formal definition

For a finite abelian group A, we define $\mathrm{rk}_{2^k}(A) := \dim_{\mathbb{F}_2} 2^{k-1}A/2^kA$.

Governing fields: formal definition

For a finite abelian group A, we define $\mathrm{rk}_{2^k}(A) := \dim_{\mathbb{F}_2} 2^{k-1}A/2^kA$.

Example 2

Take

$$A = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Then we have $\mathrm{rk}_2(A) = 3$, $\mathrm{rk}_4(A) = \mathrm{rk}_8(A) = 1$ *and* $\mathrm{rk}_{2^k}(A) = 0$ *for every integer* $k \geq 4$.

Governing fields: formal definition

For a finite abelian group A, we define $\mathrm{rk}_{2^k}(A) := \dim_{\mathbb{F}_2} 2^{k-1}A/2^kA$.

Example 2

Take

$$A = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Then we have $\mathrm{rk}_2(A) = 3$, $\mathrm{rk}_4(A) = \mathrm{rk}_8(A) = 1$ *and* $\mathrm{rk}_{2^k}(A) = 0$ *for every integer* $k \geq 4$*.*

Conjecture 1 (Cohn–Lagarias, 1980's)

For each integer $k \geq 1$ *and each integer* $d \not\equiv 2 \bmod 4$*, there exists a normal field extension* $M_{d,k}$ *over* $\mathbb{Q}$ *and a class function* $\phi_{d,k} : \mathrm{Gal}(M_{d,k}/\mathbb{Q}) \to \mathbb{Z}_{\geq 0}$ *such that*

$$\phi_{d,k}(\mathrm{Frob}_{M_{d,k}/\mathbb{Q}}(p)) = \mathrm{rk}_{2^k}\mathrm{Cl}(\mathbb{Q}(\sqrt{dp}))$$

for all primes p *coprime with* $2d$*.*

The Cohn and Lagarias conjecture

Theorem 6 (Stevenhagen, 1989)

The Cohn and Lagarias conjecture is true for all values of d and all values of $1 \leq k \leq 3$.

The Cohn and Lagarias conjecture

Theorem 6 (Stevenhagen, 1989)

The Cohn and Lagarias conjecture is true for all values of d and all values of $1 \leq k \leq 3$.

No progress since then! It is still an open problem if $M_{d,k}$ exists for any value of k with $k > 3$. However, we have the following.

The Cohn and Lagarias conjecture

Theorem 6 (Stevenhagen, 1989)

The Cohn and Lagarias conjecture is true for all values of d and all values of $1 \leq k \leq 3$.

No progress since then! It is still an open problem if $M_{d,k}$ exists for any value of k with $k > 3$. However, we have the following.

Theorem 7 (K.-Milovic, 2018)

Assume a short character sum conjecture. Then $M_{-4,4}$ does not exist.

The Cohn and Lagarias conjecture

Theorem 6 (Stevenhagen, 1989)

The Cohn and Lagarias conjecture is true for all values of d *and all values of* $1 \leq k \leq 3$.

No progress since then! It is still an open problem if $M_{d,k}$ exists for any value of k with $k > 3$. However, we have the following.

Theorem 7 (K.-Milovic, 2018)

Assume a short character sum conjecture. Then $M_{-4,4}$ *does not exist.*

Theorem 8 (K., 2018)

The density of prime numbers p *for which* $16 \mid \mathrm{Cl}(\mathbb{Q}(\sqrt{-p}))$ *is* $\frac{1}{16}$.

Reflection principles

What to do in absence of governing fields?

Reflection principles

What to do in absence of governing fields?

Compare different class groups. Such results are known as *reflection principles*.

Reflection principles

What to do in absence of governing fields?

Compare different class groups. Such results are known as *reflection principles*.

Theorem 9 (Scholz, 1930's)

We have for $d > 1$

$$\dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[3] \leq \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d}))[3] \leq 1 + \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[3].$$

Reflection principles

What to do in absence of governing fields?

Compare different class groups. Such results are known as *reflection principles*.

Theorem 9 (Scholz, 1930's)

We have for $d > 1$

$$\dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[3] \leq \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d}))[3] \leq 1 + \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[3].$$

This was one of the key ingredients in giving pointwise upper bounds for $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[3]$ (Ellenberg–Venkatesh).

Reflection principles for the 8-rank

Let h_n be the class number of $\mathbb{Q}(\sqrt{n})$, and h_n^+ the narrow class number.

Reflection principles for the 8-rank

Let h_n be the class number of $\mathbb{Q}(\sqrt{n})$, and h_n^+ the narrow class number.

Theorem 10 (Stevenhagen, 1993)

Let $p \equiv 1 \bmod 8$ *be a prime. Then*

$$\begin{aligned} 8 \mid h_{-p} &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}) \\ 8 \mid h_{-2p} &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt[4]{-2}) \\ 8 \mid h_{2p}^+ &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}, \sqrt[4]{-2}) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2}). \end{aligned}$$

Reflection principles for the 8-rank

Let h_n be the class number of $\mathbb{Q}(\sqrt{n})$, and h_n^+ the narrow class number.

Theorem 10 (Stevenhagen, 1993)

Let $p \equiv 1 \bmod 8$ *be a prime. Then*

$$
\begin{aligned}
8 \mid h_{-p} &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}) \\
8 \mid h_{-2p} &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt[4]{-2}) \\
8 \mid h_{2p}^+ &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}, \sqrt[4]{-2}) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2}).
\end{aligned}
$$

Unsurprising part: 8-rank is given by splitting conditions (recall that governing fields exist for the 8-rank).

Reflection principles for the 8-rank

Let h_n be the class number of $\mathbb{Q}(\sqrt{n})$, and h_n^+ the narrow class number.

Theorem 10 (Stevenhagen, 1993)

Let $p \equiv 1 \bmod 8$ *be a prime. Then*

$$\begin{aligned} 8 \mid h_{-p} &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}) \\ 8 \mid h_{-2p} &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt[4]{-2}) \\ 8 \mid h_{2p}^+ &\iff p \text{ splits in } \mathbb{Q}(\zeta_8, \sqrt{1+i}, \sqrt[4]{-2}) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2}). \end{aligned}$$

Unsurprising part: 8-rank is given by splitting conditions (recall that governing fields exist for the 8-rank).

Surprising part: $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ is the compositum of $\mathbb{Q}(\zeta_8, \sqrt{1+i})$ and $\mathbb{Q}(\zeta_8, \sqrt[4]{-2})$. The various governing fields are related!

Reflection principles for the 16-rank

How does a reflection principle for the 16-rank look like? Recall that we do not expect there to be a governing field in this case.

Reflection principles for the 16-rank

How does a reflection principle for the 16-rank look like? Recall that we do not expect there to be a governing field in this case.

Theorem 11 (Stevenhagen, 1993)

Let p be a prime that splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$, so that $8 \mid h_{-p}, h_{-2p}, h_{2p}^{+}$. Then one has

$$16 \mid h_{2p}^{+} \Longleftrightarrow 16 \mid h_{-2p} \text{ and } 16 \mid h_{-p}$$

if p splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{1+\zeta_8})$,

Reflection principles for the 16-rank

How does a reflection principle for the 16-rank look like? Recall that we do not expect there to be a governing field in this case.

Theorem 11 (Stevenhagen, 1993)

Let p be a prime that splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$, so that $8 \mid h_{-p}, h_{-2p}, h_{2p}^{+}$. Then one has

$$16 \mid h_{2p}^{+} \Longleftrightarrow 16 \mid h_{-2p} \text{ and } 16 \mid h_{-p}$$

if p splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{1+\zeta_8})$, and

$$16 \mid h_{2p}^{+} \Longleftrightarrow 16 \mid h_{-2p} \text{ and } 8 \parallel h_{-p}$$

if p does not split completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{1+\zeta_8})$.

Reflection principles for the 16-rank

How does a reflection principle for the 16-rank look like? Recall that we do not expect there to be a governing field in this case.

Theorem 11 (Stevenhagen, 1993)

Let p be a prime that splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$, so that $8 \mid h_{-p}, h_{-2p}, h_{2p}^{+}$. Then one has

$$16 \mid h_{2p}^{+} \iff 16 \mid h_{-2p} \text{ and } 16 \mid h_{-p}$$

if p splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{1+\zeta_8})$, and

$$16 \mid h_{2p}^{+} \iff 16 \mid h_{-2p} \text{ and } 8 \parallel h_{-p}$$

if p does not split completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}, \sqrt{1+\zeta_8})$.

The relation between different class groups is now governed by a splitting condition.

Proof sketch of Smith's result

Smith's main algebraic result is a reflection principle in the style of Stevenhagen.

Proof sketch of Smith's result

Smith's main algebraic result is a reflection principle in the style of Stevenhagen.

For a finite abelian 2-group A, there is for every integer $k \geq 1$ a natural pairing

$$\mathrm{Art} : 2^{k-1}A[2^k] \times 2^{k-1}A^\vee[2^k] \to \mathbb{F}_2, \quad (a, \chi) \mapsto \psi(a), 2^{k-1}\psi = \chi$$

with left kernel $2^k A[2^{k+1}]$ and right kernel $2^{k+1}A^\vee[2^{k+1}]$.

Proof sketch of Smith's result

Smith's main algebraic result is a reflection principle in the style of Stevenhagen.

For a finite abelian 2-group A, there is for every integer $k \geq 1$ a natural pairing

$$\mathrm{Art} : 2^{k-1}A[2^k] \times 2^{k-1}A^\vee[2^k] \to \mathbb{F}_2, \quad (a, \chi) \mapsto \psi(a), 2^{k-1}\psi = \chi$$

with left kernel $2^k A[2^{k+1}]$ and right kernel $2^{k+1}A^\vee[2^{k+1}]$.

Under favorable circumstances, the sum of 2^k Artin pairings (of class groups of different fields) is given by the splitting of an auxiliary prime in a number field.

Proof sketch of Smith's result II

Smith's reflection principle gives many linear equations for the Artin pairings.

Proof sketch of Smith's result II

Smith's reflection principle gives many linear equations for the Artin pairings.

However, the system of linear equations is *underdetermined*, but only barely.

Proof sketch of Smith's result II

Smith's reflection principle gives many linear equations for the Artin pairings.

However, the system of linear equations is *underdetermined*, but only barely.

But the Chebotarev Density Theorem shows that every RHS occurs roughly equally often.

Proof sketch of Smith's result II

Smith's reflection principle gives many linear equations for the Artin pairings.

However, the system of linear equations is *underdetermined*, but only barely.

But the Chebotarev Density Theorem shows that every RHS occurs roughly equally often.

For some choices of RHS we will not be able to deduce equidistribution of Art, but for most choices we can.

Proof sketch of Smith's result II

Smith's reflection principle gives many linear equations for the Artin pairings.

However, the system of linear equations is *underdetermined*, but only barely.

But the Chebotarev Density Theorem shows that every RHS occurs roughly equally often.

For some choices of RHS we will not be able to deduce equidistribution of Art, but for most choices we can.

Hence we get equidistribution of the Artin pairing, and this implies Gerth's conjecture.

Questions?

Thank you for your attention!

Thank you for your attention!

Questions?