The negative Pell equation and the 8-rank of the class group

Peter Koymans
Max Planck Institute for Mathematics

Tel Aviv Number Theory Seminar

4 June 2020

History of Pell's equation

For a fixed squarefree integer $d > 0$, the equation

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

has been studied since at least the ancient Greeks.

History of Pell's equation

For a fixed squarefree integer $d > 0$, the equation

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

has been studied since at least the ancient Greeks.

Bhaskara II (12th century) gave an algorithm to find solutions of this equation.

History of Pell's equation

For a fixed squarefree integer $d > 0$, the equation

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

has been studied since at least the ancient Greeks.

Bhaskara II (12th century) gave an algorithm to find solutions of this equation.

Unbeknownst, Fermat challenged English mathematicians Brouncker and Wallis to solve the notorious case $d = 61$. The smallest non-trivial solution is

$$1766319049^2 - 61 \cdot 226153980^2 = 1.$$

Lagrange was the first to give an algorithm with proof of correctness.

A modern interpretation of Pell's equation

In modern terms, we know that

$$x^2 - dy^2 = 1$$

always has a non-trivial solution by Dirichlet's Unit Theorem.

A modern interpretation of Pell's equation

In modern terms, we know that

$$x^2 - dy^2 = 1$$

always has a non-trivial solution by Dirichlet's Unit Theorem.

Indeed, $\mathcal{O}_K^* \cong \langle \epsilon \rangle \oplus \langle -1 \rangle$ for a real quadratic field K.

A modern interpretation of Pell's equation

In modern terms, we know that

$$x^2 - dy^2 = 1$$

always has a non-trivial solution by Dirichlet's Unit Theorem.

Indeed, $\mathcal{O}_K^* \cong \langle \epsilon \rangle \oplus \langle -1 \rangle$ for a real quadratic field K.

The equation

$$x^2 - dy^2 = -1$$

is known as the negative Pell equation and is not always soluble.

A modern interpretation of Pell's equation

In modern terms, we know that

$$x^2 - dy^2 = 1$$

always has a non-trivial solution by Dirichlet's Unit Theorem.

Indeed, $\mathcal{O}_K^* \cong \langle \epsilon \rangle \oplus \langle -1 \rangle$ for a real quadratic field K.

The equation

$$x^2 - dy^2 = -1$$

is known as the negative Pell equation and is not always soluble.

Question: as we vary d, how often is the negative Pell equation soluble?

A criterion for solubility

Recall that the narrow class group $\mathrm{Cl}^+(K)$ is defined as the quotient of the ideal group I_K by the principal ideals P_K^+ admitting a totally positive generator, while the class group is the quotient by the principal ideals P_K.

A criterion for solubility

Recall that the narrow class group $\mathrm{Cl}^+(K)$ is defined as the quotient of the ideal group I_K by the principal ideals P_K^+ admitting a totally positive generator, while the class group is the quotient by the principal ideals P_K.

We have

$$\begin{aligned} x^2 - dy^2 = -1 \text{ is soluble } &\Leftrightarrow \text{ fundamental unit } \epsilon \text{ has negative norm} \\ &\Leftrightarrow (\sqrt{d}) \text{ is trivial in } \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})). \end{aligned}$$

A criterion for solubility

Recall that the narrow class group $\mathrm{Cl}^+(K)$ is defined as the quotient of the ideal group I_K by the principal ideals P_K^+ admitting a totally positive generator, while the class group is the quotient by the principal ideals P_K.

We have

$$\begin{aligned} x^2 - dy^2 = -1 \text{ is soluble } &\Leftrightarrow \text{ fundamental unit } \epsilon \text{ has negative norm} \\ &\Leftrightarrow (\sqrt{d}) \text{ is trivial in } \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})). \end{aligned}$$

There is a fundamental exact sequence

$$1 \to \frac{P_K}{P_K^+} \to \mathrm{Cl}^+(K) \to \mathrm{Cl}(K) \to 1$$

with $\left|\frac{P_K}{P_K^+}\right| \in \{1, 2\}$ and $\frac{P_K}{P_K^+}$ generated by $(\sqrt{d})$.

A criterion for solubility

Recall that the narrow class group $\mathrm{Cl}^+(K)$ is defined as the quotient of the ideal group I_K by the principal ideals P_K^+ admitting a totally positive generator, while the class group is the quotient by the principal ideals P_K.

We have

$$\begin{aligned} x^2 - dy^2 = -1 \text{ is soluble } &\Leftrightarrow \text{ fundamental unit } \epsilon \text{ has negative norm} \\ &\Leftrightarrow (\sqrt{d}) \text{ is trivial in } \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})). \end{aligned}$$

There is a fundamental exact sequence

$$1 \to \frac{P_K}{P_K^+} \to \mathrm{Cl}^+(K) \to \mathrm{Cl}(K) \to 1$$

with $\left|\frac{P_K}{P_K^+}\right| \in \{1, 2\}$ and $\frac{P_K}{P_K^+}$ generated by $(\sqrt{d})$.

Goal: study joint distribution of $(\mathrm{Cl}^+(K)[2^\infty], \mathrm{Cl}(K)[2^\infty])$.

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

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

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

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

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.

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.

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

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.

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.

Previous work on negative Pell

Define $\mathcal{D}$ to be the set of squarefree integers d such that $p \mid d$ implies $p \equiv 1, 2 \bmod 4$.

Previous work on negative Pell

Define $\mathcal{D}$ to be the set of squarefree integers d such that $p \mid d$ implies $p \equiv 1, 2 \bmod 4$.

By the Hasse-Minkowski Theorem we have

$$d \in \mathcal{D} \Leftrightarrow x^2 - dy^2 = -1 \text{ is soluble with } x, y \in \mathbb{Q}$$
$$\Leftrightarrow \mathrm{rk}_2 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_2 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})).$$

Example:

$$\mathrm{rk}_4\ \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} = 2$$
$$\mathrm{rk}_8\ \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} = 1.$$

Previous work on negative Pell

Define $\mathcal{D}$ to be the set of squarefree integers d such that $p \mid d$ implies $p \equiv 1, 2 \bmod 4$.

By the Hasse-Minkowski Theorem we have

$$d \in \mathcal{D} \Leftrightarrow x^2 - dy^2 = -1 \text{ is soluble with } x, y \in \mathbb{Q}$$
$$\Leftrightarrow \mathrm{rk}_2 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_2 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})).$$

Example:

$$\mathrm{rk}_4\ \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} = 2$$
$$\mathrm{rk}_8\ \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} = 1.$$

Fouvry and Klüners (2010) computed the asymptotic density of $d \in \mathcal{D}$ satisfying

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 0$$

and also those satisfying

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 1 + \mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})).$$

Further improvements on negative Pell

Fouvry and Klüners continued their investigations by computing the density of $d \in \mathcal{D}$ with

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = 1, \mathrm{rk}_8 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 0.$$

Further improvements on negative Pell

Fouvry and Klüners continued their investigations by computing the density of $d \in \mathcal{D}$ with

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = 1, \mathrm{rk}_8 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 0.$$

From their works they were able to deduce that

$$\frac{5\alpha}{4} \leq \liminf_{X \to \infty} \frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|} \leq \limsup_{X \to \infty} \frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|} \leq \frac{2}{3},$$

where $\alpha = \prod_{j=1}^{\infty}(1 + 2^{-j})^{-1} \approx 0.41942$.

Further improvements on negative Pell II

Together with S. Chan, D. Milovic and C. Pagano I computed the density of $d \in \mathcal{D}$ with

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = n, \quad \mathrm{rk}_8 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = m$$

for every $n \geq m$.

Further improvements on negative Pell II

Together with S. Chan, D. Milovic and C. Pagano I computed the density of $d \in \mathcal{D}$ with

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = n, \quad \mathrm{rk}_8 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = m$$

for every $n \geq m$.

Corollary 1 (Chan, K., Milovic, Pagano)

We have

$$\beta\alpha \leq \liminf_{X \to \infty} \frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|}, \quad \beta := \sum_{n=0}^{\infty} 2^{-n(n+3)/2} \approx 1.28325.$$

Further improvements on negative Pell II

Together with S. Chan, D. Milovic and C. Pagano I computed the density of $d \in \mathcal{D}$ with

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = n, \quad \mathrm{rk}_8 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = m$$

for every $n \geq m$.

Corollary 1 (Chan, K., Milovic, Pagano)

We have

$$\beta\alpha \leq \liminf_{X \to \infty} \frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|}, \quad \beta := \sum_{n=0}^{\infty} 2^{-n(n+3)/2} \approx 1.28325.$$

Further improvements to upper and lower bounds in recent work of K. and Pagano.

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.

Duality of abelian groups

For a finite abelian group A, define

$$A^\vee := \mathrm{Hom}(A, \mathbb{C}^*).$$

Duality of abelian groups

For a finite abelian group A, define

$$A^\vee := \mathrm{Hom}(A, \mathbb{C}^*).$$

There is a natural pairing

$$\mathrm{Art}_1 : A[2] \times A^\vee[2] \to \{\pm 1\}, \quad (a, \chi) \mapsto \chi(a).$$

Duality of abelian groups

For a finite abelian group A, define

$$A^\vee := \mathrm{Hom}(A, \mathbb{C}^*).$$

There is a natural pairing

$$\mathrm{Art}_1 : A[2] \times A^\vee[2] \to \{\pm 1\}, \quad (a, \chi) \mapsto \chi(a).$$

Left kernel of Art is $2A[4]$ and right kernel is $2A^\vee[4]$.

Duality of abelian groups

For a finite abelian group A, define

$$A^\vee := \mathrm{Hom}(A, \mathbb{C}^*).$$

There is a natural pairing

$$\mathrm{Art}_1 : A[2] \times A^\vee[2] \to \{\pm 1\}, \quad (a, \chi) \mapsto \chi(a).$$

Left kernel of Art is $2A[4]$ and right kernel is $2A^\vee[4]$.

Goal: to compute 4-rank, it is enough to understand Art_1. We start by describing $\mathrm{Cl}^{+,\vee}(K)[2]$.

The dual class group

Theorem 2 (Class field theory)

We have an isomorphism

$$\mathrm{Cl}^+(K) \cong \mathrm{Gal}(H^+(K)/K)$$

given by sending a prime ideal $\mathfrak{p}$ *to* $\mathrm{Art}(\mathfrak{p})$. *Furthermore, if* K *is Galois, this isomorphism respects the natural Galois action of* $\mathrm{Gal}(K/\mathbb{Q})$ *on both sides.*

The dual class group

Theorem 2 (Class field theory)

We have an isomorphism

$$\mathrm{Cl}^+(K) \cong \mathrm{Gal}(H^+(K)/K)$$

given by sending a prime ideal $\mathfrak{p}$ *to* $\mathrm{Art}(\mathfrak{p})$*. Furthermore, if* K *is Galois, this isomorphism respects the natural Galois action of* $\mathrm{Gal}(K/\mathbb{Q})$ *on both sides.*

From this we get a bijection

$$\mathrm{Cl}^{+,\vee}(K)[2] \leftrightarrow \{\text{quadratic unramified extensions of } K\}.$$

The dual class group

Theorem 2 (Class field theory)

We have an isomorphism

$$\mathrm{Cl}^+(K) \cong \mathrm{Gal}(H^+(K)/K)$$

given by sending a prime ideal $\mathfrak{p}$ *to* $\mathrm{Art}(\mathfrak{p})$. *Furthermore, if* K *is Galois, this isomorphism respects the natural Galois action of* $\mathrm{Gal}(K/\mathbb{Q})$ *on both sides.*

From this we get a bijection

$$\mathrm{Cl}^{+,\vee}(K)[2] \leftrightarrow \{\text{quadratic unramified extensions of } K\}.$$

Indeed,

$$\mathrm{Cl}^{+,\vee}(K)[2] = \mathrm{Hom}(\mathrm{Cl}^+(K), \mathbb{C}^*)[2] \cong \mathrm{Hom}(\mathrm{Gal}(H^+(K)/K), \{\pm 1\}).$$

Given $\chi \in \mathrm{Hom}(\mathrm{Gal}(H^+(K)/K), \{\pm 1\})$, look at $H^+(K)^{\ker(\chi)}$.

The dual class group II

For quadratic K, $\mathrm{Gal}(K/\mathbb{Q})$ acts by -1 on $\mathrm{Cl}(K)$.

The dual class group II

For quadratic K, $\mathrm{Gal}(K/\mathbb{Q})$ acts by -1 on $\mathrm{Cl}(K)$.

Then it follows that any quadratic unramified extension of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ and must have Galois group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The dual class group II

For quadratic K, $\mathrm{Gal}(K/\mathbb{Q})$ acts by -1 on $\mathrm{Cl}(K)$.

Then it follows that any quadratic unramified extension of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ and must have Galois group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Get a diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{d}, \sqrt{a}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{a}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{d}) \arrow[d, dash] & \mathbb{Q}(\sqrt{d/a}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Unramified condition then implies that $a \mid d$.

The dual class group II

For quadratic K, $\mathrm{Gal}(K/\mathbb{Q})$ acts by -1 on $\mathrm{Cl}(K)$.

Then it follows that any quadratic unramified extension of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ and must have Galois group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Get a diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{d}, \sqrt{a}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{a}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{d}) \arrow[d, dash] & \mathbb{Q}(\sqrt{d/a}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Unramified condition then implies that $a \mid d$.
Example for ramification at 2: $d \equiv 1 \bmod 4$, $a \equiv 3 \bmod 4$ a prime.

The dual class group II

For quadratic K, $\mathrm{Gal}(K/\mathbb{Q})$ acts by -1 on $\mathrm{Cl}(K)$.

Then it follows that any quadratic unramified extension of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ and must have Galois group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Get a diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{d}, \sqrt{-a}) \arrow[dl, dash] \arrow[d, dash, "\infty \text{ ram.}"] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-a}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{d}) \arrow[d, dash] & \mathbb{Q}(\sqrt{-d/a}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Unramified condition then implies that $a \mid d$.
Example for ramification at 2: $d \equiv 1 \bmod 4$, $a \equiv 3 \bmod 4$ a prime.

The Artin pairing

Under the identifications, we have that

$$\mathrm{Art}_1 : \mathrm{Cl}^+(K)[2] \times \mathrm{Cl}^{+,\vee}(K)[2] \to \{\pm 1\}, \quad (\mathfrak{p}, \chi) \mapsto \chi(\mathrm{Art}\ \mathfrak{p}).$$

The Artin pairing

Under the identifications, we have that

$$\mathrm{Art}_1 : \mathrm{Cl}^+(K)[2] \times \mathrm{Cl}^{+,\vee}(K)[2] \to \{\pm 1\}, \quad (\mathfrak{p}, \chi) \mapsto \chi(\mathrm{Art}\ \mathfrak{p}).$$

Let $p_1, \ldots, p_t$ be the prime divisors of d. Define χ_m to be the quadratic character of $\mathbb{Q}(\sqrt{m})$. The Rédei matrix is

$$\begin{array}{ccccc}
 & \chi_{p_1} & \chi_{p_2} & \cdots & \chi_{p_t} \\
p_1 & * & \left(\frac{p_2}{p_1}\right) & \cdots & \left(\frac{p_t}{p_1}\right) \\
p_2 & \left(\frac{p_1}{p_2}\right) & * & \cdots & \left(\frac{p_t}{p_2}\right) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
p_t & \left(\frac{p_1}{p_t}\right) & \left(\frac{p_2}{p_t}\right) & \cdots & *
\end{array}.$$

Left kernel gives generating set for $2\mathrm{Cl}^+(K)[4]$.

Interlude: Stevenhagen's conjecture

For $d \in \mathcal{D}$, we have $(\sqrt{d}) \in 2\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[4]$.

Interlude: Stevenhagen's conjecture

For $d \in \mathcal{D}$, we have $(\sqrt{d}) \in 2\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[4]$.

Heuristic assumption: every non-zero element in the generating set of $2\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[4]$ is equally likely to be trivial.

Conjecture 1 (Stevenhagen's conjecture)

We have

$$\lim_{X \to \infty} \frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|} = \sum_{j=0}^{\infty} \frac{\mathbb{P}(4-\textit{rank of } d \in \mathcal{D} \textit{ equals } j)}{2^{j+1}-1} \approx 0.581.$$

Interlude: Stevenhagen's conjecture

For $d \in \mathcal{D}$, we have $(\sqrt{d}) \in 2\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[4]$.

Heuristic assumption: every non-zero element in the generating set of $2\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[4]$ is equally likely to be trivial.

Conjecture 1 (Stevenhagen's conjecture)

We have

$$\lim_{X \to \infty} \frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|} = \sum_{j=0}^{\infty} \frac{\mathbb{P}(4-\textit{rank of } d \in \mathcal{D} \textit{ equals } j)}{2^{j+1}-1} \approx 0.581.$$

Furthermore,

$$\mathbb{P}(4\text{−rank of } d \in \mathcal{D} \text{ equals } j) = \lim_{t \to \infty} \mathbb{P}(t \times t\text{−symm. matrix ker. of dim. } j).$$

The second Artin pairing

There is a natural pairing

$$\mathrm{Art}_2 : 2A[4] \times 2A^\vee[4] \to \{\pm 1\}, \quad (a, \chi) \mapsto \psi(a),\ 2\psi = \chi.$$

Left kernel is $4A[8]$ and right kernel is $4A^\vee[8]$.

The second Artin pairing

There is a natural pairing

$$\mathrm{Art}_2 : 2A[4] \times 2A^\vee[4] \to \{\pm 1\}, \quad (a, \chi) \mapsto \psi(a),\ 2\psi = \chi.$$

Left kernel is $4A[8]$ and right kernel is $4A^\vee[8]$.

As before, class field theory gives that this pairing becomes

$$(\mathfrak{p}, \chi) \mapsto \psi(\mathrm{Art}\ \mathfrak{p}),\ 2\psi = \chi.$$

Goal: understand cyclic degree 4 unramified extensions of $\mathbb{Q}(\sqrt{d})$.

Cyclic degree 4 extensions

A cyclic degree 4 unramified extension L of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ with Galois group D_4.

Cyclic degree 4 extensions

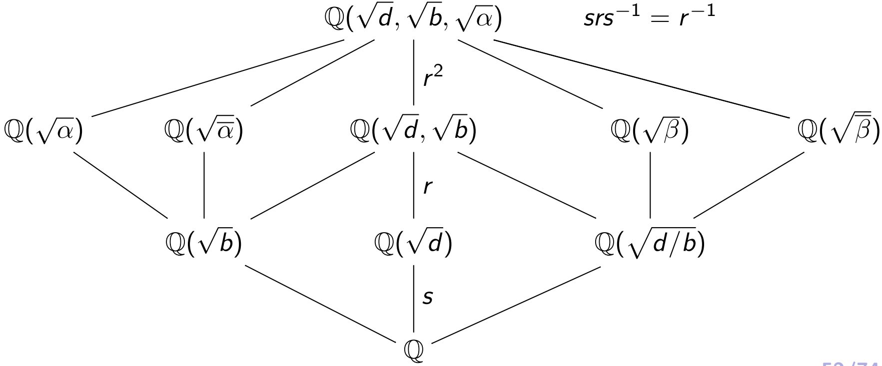
A cyclic degree 4 unramified extension L of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ with Galois group D_4.

From basic Galois theory any D_4-extension is of the following shape, where $\alpha := x + y\sqrt{b}$ and $x^2 = by^2 + \frac{d}{b}z^2$ with $x, y, z \in \mathbb{Q}$ non-trivial

Cyclic degree 4 extensions

A cyclic degree 4 unramified extension L of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ with Galois group D_4.

From basic Galois theory any D_4-extension is of the following shape, where $\alpha := x + y\sqrt{b}$ and $x^2 = by^2 + \frac{d}{b}z^2$ with $x, y, z \in \mathbb{Q}$ non-trivial



Unramified degree 4 extensions

To make the extension unramified, we need to find a *primitive* solution

$$x^2 = by^2 + \frac{d}{b}z^2 \text{ with } x, y, z \in \mathbb{Z}, \gcd(x, y, z) = 1.$$

Such solutions exist since $\gcd(b, d/b) = 1$.

Unramified degree 4 extensions

To make the extension unramified, we need to find a *primitive* solution

$$x^2 = by^2 + \frac{d}{b}z^2 \text{ with } x, y, z \in \mathbb{Z}, \gcd(x, y, z) = 1.$$

Such solutions exist since $\gcd(b, d/b) = 1$.

To understand the splitting in dihedral extensions, let us work in greater generality. Suppose that

$$(a, b)_v = (b, c)_v = (a, c)_v = 1, \quad \gcd(a, b, c) = 1.$$

We define the Rédei symbol

$$[a, b, c] \in \mathbb{F}_2 \cong \mathrm{Gal}(L_{a,b}/\mathbb{Q}(\sqrt{a}, \sqrt{b}))$$

to be the splitting of $\mathfrak{c}$ in a *minimally ramified* degree 4 cyclic extension $L_{a,b}$ of $\mathbb{Q}(\sqrt{ab})$, where $\mathfrak{c}$ is an ideal in $\mathbb{Q}(\sqrt{ab})$ of norm c.

Facts:

- $L_{a,b}$ minimally ramified means unramified outside the primes dividing a or b;
- can change such $L_{a,b}$ only by twisting α to $p\alpha$ with p dividing ab;
- every $p \mid c$ splits or ramifies in $\mathbb{Q}(\sqrt{ab})$, hence $\mathfrak{c}$ exists;
- every $\mathfrak{p}$ dividing $\mathfrak{c}$ splits in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$;
- $[a, b, c] := \mathrm{Art}(L_{a,b}/\mathbb{Q}(\sqrt{ab}), \mathfrak{c}) \in \mathrm{Gal}(L_{a,b}/\mathbb{Q}(\sqrt{a}, \sqrt{b}))$.

$$
\begin{tikzcd}
 & & L_{a,b} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt{\alpha}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{\overline{\alpha}}) \arrow[d, dash] & \mathbb{Q}(\sqrt{a}, \sqrt{b})\ \mathfrak{c}' \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{\beta}) \arrow[d, dash] & \mathbb{Q}(\sqrt{\overline{\beta}}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{a}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{ab})\ \ \mathfrak{c} \arrow[d, dash] & \mathbb{Q}(\sqrt{b}) \arrow[dl, dash] & \\
 & & \mathbb{Q}\ \ c & &
\end{tikzcd}
$$

Rédei symbols in a diagram

Facts:

- $L_{a,b}$ minimally ramified means unramified outside the primes dividing a or b;
- can change such $L_{a,b}$ only by twisting α to $p\alpha$ with p dividing ab;
- every $p \mid c$ splits or ramifies in $\mathbb{Q}(\sqrt{ab})$, hence $\mathfrak{c}$ exists;
- every $\mathfrak{p}$ dividing $\mathfrak{c}$ splits in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$;
- $[a, b, c] := \mathrm{Art}(L_{a,b}/\mathbb{Q}(\sqrt{ab}), \mathfrak{c}) \in \mathrm{Gal}(L_{a,b}/\mathbb{Q}(\sqrt{a}, \sqrt{b}))$.

$$
\begin{tikzcd}
 & & L_{a,b} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt{\alpha}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{\overline{\alpha}}) \arrow[d, dash] & \mathbb{Q}(\sqrt{a}, \sqrt{b})\ \mathfrak{c}' \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{\beta}) \arrow[d, dash] & \mathbb{Q}(\sqrt{\overline{\beta}}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{a}) \arrow[dr, dash, red] & \mathbb{Q}(\sqrt{ab})\ \ \mathfrak{c} \arrow[d, dash] & \mathbb{Q}(\sqrt{b}) \arrow[dl, dash, red] & \\
 & & \mathbb{Q}\ \ c & &
\end{tikzcd}
$$

Rédei symbols in a diagram

Facts:

- $L_{a,b}$ minimally ramified means unramified outside the primes dividing a or b;
- can change such $L_{a,b}$ only by twisting α to $p\alpha$ with p dividing ab;
- every $p \mid c$ splits or ramifies in $\mathbb{Q}(\sqrt{ab})$, hence $\mathfrak{c}$ exists;
- every $\mathfrak{p}$ dividing $\mathfrak{c}$ splits in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$;
- $[a, b, c] := \mathrm{Art}(L_{a,b}/\mathbb{Q}(\sqrt{ab}), \mathfrak{c}) \in \mathrm{Gal}(L_{a,b}/\mathbb{Q}(\sqrt{a}, \sqrt{b}))$.

$$\begin{tikzcd}
 & & L_{a,b} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt{\alpha}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{\overline{\alpha}}) \arrow[d, dash] & \mathbb{Q}(\sqrt{a}, \sqrt{b})\ \mathfrak{c}' \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{\beta}) \arrow[d, dash] & \mathbb{Q}(\sqrt{\overline{\beta}}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{a}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{ab})\ \ \mathfrak{c} \arrow[d, dash] & \mathbb{Q}(\sqrt{b}) \arrow[dl, dash] & \\
 & & \mathbb{Q}\ \ c & &
\end{tikzcd}$$

Rédei symbols in a diagram

Facts:

- $L_{a,b}$ minimally ramified means unramified outside the primes dividing a or b;
- can change such $L_{a,b}$ only by twisting α to $p\alpha$ with p dividing ab;
- every $p \mid c$ splits or ramifies in $\mathbb{Q}(\sqrt{ab})$, hence $\mathfrak{c}$ exists;
- every $\mathfrak{p}$ dividing $\mathfrak{c}$ splits in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$;
- $[a, b, c] := \mathrm{Art}(L_{a,b}/\mathbb{Q}(\sqrt{ab}), \mathfrak{c}) \in \mathrm{Gal}(L_{a,b}/\mathbb{Q}(\sqrt{a}, \sqrt{b}))$.

$$\begin{tikzcd}
& & & & L_{a,b} \arrow[dllll, dash] \arrow[dll, dash] \arrow[d, dash, red] \arrow[drr, dash] \arrow[drrrr, dash] & & & & \\
\mathbb{Q}(\sqrt{\alpha}) \arrow[drr, dash] & & \mathbb{Q}(\sqrt{\overline{\alpha}}) \arrow[d, dash] & & \mathbb{Q}(\sqrt{a}, \sqrt{b})\ \mathfrak{c}' \arrow[dll, dash] \arrow[d, dash, red] \arrow[drr, dash] & & \mathbb{Q}(\sqrt{\beta}) \arrow[d, dash] & & \mathbb{Q}(\sqrt{\overline{\beta}}) \arrow[dll, dash] \\
& & \mathbb{Q}(\sqrt{a}) \arrow[drr, dash, red] & & \mathbb{Q}(\sqrt{ab}) \arrow[d, dash] & \mathfrak{c} & \mathbb{Q}(\sqrt{b}) \arrow[dll, dash, red] & & \\
& & & & \mathbb{Q} & c & & &
\end{tikzcd}$$

Rédei symbols in a diagram

Facts:

- $L_{a,b}$ minimally ramified means unramified outside the primes dividing a or b;
- can change such $L_{a,b}$ only by twisting α to $p\alpha$ with p dividing ab;
- every $p \mid c$ splits or ramifies in $\mathbb{Q}(\sqrt{ab})$, hence $\mathfrak{c}$ exists;
- every $\mathfrak{p}$ dividing $\mathfrak{c}$ splits in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$;
- $[a, b, c] := \mathrm{Art}(L_{a,b}/\mathbb{Q}(\sqrt{ab}), \mathfrak{c}) \in \mathrm{Gal}(L_{a,b}/\mathbb{Q}(\sqrt{a}, \sqrt{b}))$.

$$
\begin{tikzcd}
 & & L_{a,b} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt{\alpha}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{\overline{\alpha}}) \arrow[d, dash] & \mathbb{Q}(\sqrt{a}, \sqrt{b})\ \mathfrak{c}' \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{\beta}) \arrow[d, dash] & \mathbb{Q}(\sqrt{\overline{\beta}}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{a}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{ab}) \quad \mathfrak{c} \arrow[d, dash] & \mathbb{Q}(\sqrt{b}) \arrow[dl, dash] & \\
 & & \mathbb{Q} \quad c & &
\end{tikzcd}
$$

An example

Take $a = 5$, $b = 41$ and $c = 59$. We have

$$11^2 = 5 \cdot 4^2 + 41 \cdot 1^2, \quad \alpha := 11 + 4\sqrt{5}.$$

To compute the splitting of 59 in $L_{a,b}$ (or equivalently in $\mathbb{Q}(\sqrt{\alpha})$ or in $\mathbb{Q}(\sqrt{\overline{\alpha}})$), need to compute if

$$11 + 4\sqrt{5} \equiv \square \bmod 59.$$

An example

Take $a = 5$, $b = 41$ and $c = 59$. We have

$$11^2 = 5 \cdot 4^2 + 41 \cdot 1^2, \quad \alpha := 11 + 4\sqrt{5}.$$

To compute the splitting of 59 in $L_{a,b}$ (or equivalently in $\mathbb{Q}(\sqrt{\alpha})$ or in $\mathbb{Q}(\sqrt{\overline{\alpha}})$), need to compute if

$$11 + 4\sqrt{5} \equiv \square \bmod 59.$$

This is independent of the choice of $\sqrt{5}$ in $\mathbb{Z}/59\mathbb{Z}$, since

$$(11 + 4\sqrt{5}) \cdot (11 - 4\sqrt{5}) = 41 \equiv \square \bmod 59$$

by the assumptions. The choices of $\sqrt{5}$ are $\{8, 51\}$, so need to check

$$43 \equiv \square \bmod 59 \text{ or equivalently } 51 \equiv \square \bmod 59.$$

Answer is no.

Rédei reciprocity

We have the following fundamental theorem, which follows from Hilbert reciprocity applied to a suitable quadratic extension of $\mathbb{Q}$.

Theorem 3 (Rédei reciprocity)

The Rédei symbol is trilinear and symmetric in all its entries

$$[a, b, c] = [b, a, c] = [a, c, b].$$

Governing fields

We will use Rédei reciprocity to study the 8-rank. Fix a squarefree integer d, and look at the family $\mathbb{Q}(\sqrt{dp})$ as p varies over primes.

Governing fields

We will use Rédei reciprocity to study the 8-rank. Fix a squarefree integer d, and look at the family $\mathbb{Q}(\sqrt{dp})$ as p varies over primes.

Restrict further to p with a given congruence class m modulo $8d$. Then the Rédei matrix is constant as p varies in such a family.

Governing fields

We will use Rédei reciprocity to study the 8-rank. Fix a squarefree integer d, and look at the family $\mathbb{Q}(\sqrt{dp})$ as p varies over primes.

Restrict further to p with a given congruence class m modulo $8d$. Then the Rédei matrix is constant as p varies in such a family.

Pick a generating set for $2\mathrm{Cl}^{+}(\mathbb{Q}(\sqrt{dp}))[4]$ and $2\mathrm{Cl}^{+,\vee}(\mathbb{Q}(\sqrt{dp}))[4]$ not supported by p (use the ideal $(\sqrt{d})$ to achieve this).

Governing fields

We will use Rédei reciprocity to study the 8-rank. Fix a squarefree integer d, and look at the family $\mathbb{Q}(\sqrt{dp})$ as p varies over primes.

Restrict further to p with a given congruence class m modulo $8d$. Then the Rédei matrix is constant as p varies in such a family.

Pick a generating set for $2\mathrm{Cl}^{+}(\mathbb{Q}(\sqrt{dp}))[4]$ and $2\mathrm{Cl}^{+,\vee}(\mathbb{Q}(\sqrt{dp}))[4]$ not supported by p (use the ideal $(\sqrt{d})$ to achieve this).

Then if we have two primes p and p' with $p \equiv p' \equiv m \bmod 8d$, we have

$$\begin{aligned}\mathrm{Art}_{2,\mathbb{Q}(\sqrt{dp})}(a, \chi_b) + \mathrm{Art}_{2,\mathbb{Q}(\sqrt{dp'})}(a, \chi_b) &= [a, dp/a, b] + [a, dp'/a, b] \\ &= [a, b, pp'].\end{aligned}$$

Idea: the splitting of p in the compositum of the $L_{a,b}$ determines the 8-rank. Now apply the Chebotarev density theorem.

Avoiding GRH

Approach above needs GRH.

Avoiding GRH

Approach above needs GRH.

Instead vary two primes, say p and q. Then we get that the sum of the four Artin pairings

$$\mathrm{Art}_{2,dpq}(ap,\chi_b)+\mathrm{Art}_{2,dp'q}(ap',\chi_b)+\mathrm{Art}_{2,dpq'}(ap,\chi_b)+\mathrm{Art}_{2,dp'q'}(ap',\chi_b)$$

equals

$$[aq,b,pp']+[aq',b,pp']=[pp',qq',b].$$

Avoiding GRH

Approach above needs GRH.

Instead vary two primes, say p and q. Then we get that the sum of the four Artin pairings

$$\mathrm{Art}_{2,dpq}(ap,\chi_b)+\mathrm{Art}_{2,dp'q}(ap',\chi_b)+\mathrm{Art}_{2,dpq'}(ap,\chi_b)+\mathrm{Art}_{2,dp'q'}(ap',\chi_b)$$

equals

$$[aq,b,pp']+[aq',b,pp']=[pp',qq',b].$$

If p and q are small, we can apply Chebotarev. However, we no longer have direct control over Art_2. Use combinatorial ideas to overcome this.

Beyond the 8-rank

No "governing fields" have been found for the 16-rank.

Beyond the 8-rank

No "governing fields" have been found for the 16-rank.

The key idea of Smith to deal with the higher ranks is that of a *relative* governing field. If one adds several Artin pairings, then one actually does get a symbol that can be attacked using the Chebotarev density theorem.

Beyond the 8-rank

No "governing fields" have been found for the 16-rank.

The key idea of Smith to deal with the higher ranks is that of a *relative* governing field. If one adds several Artin pairings, then one actually does get a symbol that can be attacked using the Chebotarev density theorem.

K. and Pagano found a generalization of the Rédei reciprocity law for these *relative* governing fields. This allows us to compute the density of $d \in \mathcal{D}$ with

$$\mathrm{rk}_4\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_4\mathrm{Cl}(\mathbb{Q}(\sqrt{d})), \quad \mathrm{rk}_8\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 1 + \mathrm{rk}_8\mathrm{Cl}(\mathbb{Q}(\sqrt{d})).$$

Beyond the 8-rank

No "governing fields" have been found for the 16-rank.

The key idea of Smith to deal with the higher ranks is that of a *relative* governing field. If one adds several Artin pairings, then one actually does get a symbol that can be attacked using the Chebotarev density theorem.

K. and Pagano found a generalization of the Rédei reciprocity law for these *relative* governing fields. This allows us to compute the density of $d \in \mathcal{D}$ with

$$\mathrm{rk}_4 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})), \quad \mathrm{rk}_8 \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 1 + \mathrm{rk}_8 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})).$$

Theorem 4 (K., Pagano)

We have

$$\limsup_{X \to \infty} \frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|} \leq 0.61.$$

That's it!

Thank you for your attention!