The negative Pell equation and applications

Peter Koymans
University of Michigan

Canadian Mathematical Society winter meeting

5 December 2021

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 non-trivial 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 non-trivial solutions of this equation.

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

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

The negative Pell equation

The equation

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

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

The negative Pell equation

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?

The negative Pell equation

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?

Define $\mathcal{D}$ to be the set of squarefree integers having as odd prime divisors only primes $p \equiv 1 \bmod 4$ and define $\mathcal{D}^-$ to be the set of squarefree integers for which the negative Pell equation is soluble.

The negative Pell equation

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?

Define $\mathcal{D}$ to be the set of squarefree integers having as odd prime divisors only primes $p \equiv 1 \bmod 4$ and define $\mathcal{D}^-$ to be the set of squarefree integers for which the negative Pell equation is soluble.

By the Hasse-Minkowski Theorem we have for all squarefree d

$$d \in \mathcal{D} \Longleftrightarrow x^2 - dy^2 = -1 \text{ is soluble with } x, y \in \mathbb{Q},$$

so in particular $\mathcal{D}^- \subseteq \mathcal{D}$.

The negative Pell equation

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?

Define $\mathcal{D}$ to be the set of squarefree integers having as odd prime divisors only primes $p \equiv 1 \bmod 4$ and define $\mathcal{D}^-$ to be the set of squarefree integers for which the negative Pell equation is soluble.

By the Hasse-Minkowski Theorem we have for all squarefree d

$$d \in \mathcal{D} \Longleftrightarrow x^2 - dy^2 = -1 \text{ is soluble with } x, y \in \mathbb{Q},$$

so in particular $\mathcal{D}^- \subseteq \mathcal{D}$. Classical techniques in analytic number theory give a constant $C > 0$ such that

$$\#\{d \leq X : d \in \mathcal{D}\} \sim C \cdot \frac{X}{\sqrt{\log X}}.$$

The negative Pell equation

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?

Define $\mathcal{D}$ to be the set of squarefree integers having as odd prime divisors only primes $p \equiv 1 \bmod 4$ and define $\mathcal{D}^-$ to be the set of squarefree integers for which the negative Pell equation is soluble.

By the Hasse-Minkowski Theorem we have for all squarefree d

$$d \in \mathcal{D} \Longleftrightarrow x^2 - dy^2 = -1 \text{ is soluble with } x, y \in \mathbb{Q},$$

so in particular $\mathcal{D}^- \subseteq \mathcal{D}$. Classical techniques in analytic number theory give a constant $C > 0$ such that

$$\#\{d \leq X : d \in \mathcal{D}\} \sim C \cdot \frac{X}{\sqrt{\log X}}.$$

Refined question: what is the density of $\mathcal{D}^-$ inside $\mathcal{D}$?

Conjectures on the negative Pell equation

Nagell (1930s) conjectured that

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$.

Conjectures on the negative Pell equation

Nagell (1930s) conjectured that

$$\lim_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$.

Stevenhagen (1995) conjectured that

$$\lim_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} = 1 - \alpha,$$

where

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

Progress towards Stevenhagen's conjecture

Fouvry and Klüners (2010) proved that

$$\frac{5\alpha}{4} \leq \liminf_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \limsup_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \frac{2}{3}.$$

Progress towards Stevenhagen's conjecture

Fouvry and Klüners (2010) proved that

$$\frac{5\alpha}{4} \leq \liminf_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \limsup_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \frac{2}{3}.$$

Together with Stephanie Chan, Djordjo Milovic and Carlo Pagano, I improved the lower bound to

$$\alpha \cdot \sum_{n=0}^{\infty} 2^{-n(n+3)/2} \approx \alpha \cdot 1.28325.$$

Progress towards Stevenhagen's conjecture

Fouvry and Klüners (2010) proved that

$$\frac{5\alpha}{4} \leq \liminf_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \limsup_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \frac{2}{3}.$$

Together with Stephanie Chan, Djordjo Milovic and Carlo Pagano, I improved the lower bound to

$$\alpha \cdot \sum_{n=0}^{\infty} 2^{-n(n+3)/2} \approx \alpha \cdot 1.28325.$$

Theorem (K., Pagano (2021))

We have

$$\lim_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} = 1 - \alpha$$

in accordance with Stevenhagen's conjecture.

A criterion for solubility

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

We have

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

There is a basic exact sequence

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

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

A criterion for solubility

We have

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

There is a basic exact sequence

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

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

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

Genus theory

The group $\mathrm{Cl}^+(K)[2]$ has a very predictable behavior unlike $\mathrm{Cl}^+(K)[p]$ for p odd.

Genus theory

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

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 $\mathcal{O}_K$.

There is precisely one relation between the ramified primes.

Cohen–Lenstra–Gerth

Gerth adapted the Cohen–Lenstra conjectures to $p = 2$, i.e. we have

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

for every finite, abelian 2-group A.

Cohen–Lenstra–Gerth

Gerth adapted the Cohen–Lenstra conjectures to $p = 2$, i.e. we have

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

for every finite, abelian 2-group A.

Theorem (Alexander Smith (2017))

Gerth's conjecture is true.

Cohen–Lenstra–Gerth

Gerth adapted the Cohen–Lenstra conjectures to $p = 2$, i.e. we have

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

for every finite, abelian 2-group A.

Theorem (Alexander Smith (2017))

Gerth's conjecture is true.

Idea: adapt Smith's method to the family $\mathcal{D}$.

Two difficulties: $\mathcal{D}$ has density 0 in the set of squarefree integers, and $\mathcal{D}$ naturally ends up in the error term in Smith's proof!

Strategy for Stevenhagen's conjecture

Find for every integer $m \geq 1$, the density of $d \in \mathcal{D}$ for which

$$\mathrm{rk}_{2^k} \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_{2^k} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) > 0 \text{ for } 1 \leq k \leq m \text{ and}$$
$$\mathrm{rk}_{2^{m+1}} \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 0.$$

This gives better and better lower bounds for negative Pell.

Strategy for Stevenhagen's conjecture

Find for every integer $m \geq 1$, the density of $d \in \mathcal{D}$ for which

$$\mathrm{rk}_{2^k} \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_{2^k} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) > 0 \text{ for } 1 \leq k \leq m \text{ and}$$
$$\mathrm{rk}_{2^{m+1}} \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = 0.$$

This gives better and better lower bounds for negative Pell. Similarly, find for every integer $m \geq 1$, the density of $d \in \mathcal{D}$ for which

$$\mathrm{rk}_{2^k} \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_{2^k} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) > 0 \text{ for } 1 \leq k \leq m \text{ and}$$
$$\mathrm{rk}_{2^{m+1}} \mathrm{Cl}^+(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}_{2^{m+1}} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) + 1.$$

This gives better and better upper bounds for negative Pell.

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_1 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_1 is $2A[4]$ and right kernel is $2A^\vee[4]$.

Goal: in order to compute 4-rank, understand Art_1.

The Artin pairing

By class field theory we get a bijection

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

The Artin pairing

By class field theory we get a bijection

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

Under the earlier 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

By class field theory we get a bijection

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

Under the earlier 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. The Rédei matrix is

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

The Artin pairing

By class field theory we get a bijection

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

Under the earlier 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. The Rédei matrix is

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

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

Interlude: Stevenhagen's conjecture

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

Interlude: Stevenhagen's conjecture

Fact: 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.

Interlude: Stevenhagen's conjecture

Fact: 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 (Stevenhagen's conjecture)

We have

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

Interlude: Stevenhagen's conjecture

Fact: 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 (Stevenhagen's conjecture)

We have

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

Furthermore,

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

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 $\mathbb{Q}(\sqrt{d})$.

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 $\mathbb{Q}(\sqrt{d})$.

Fact: a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ with Galois group D_4.

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 $\mathbb{Q}(\sqrt{d})$.

Fact: a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ with Galois group D_4.

Such extensions are of the shape $\mathbb{Q}(\sqrt{d}, \sqrt{a}, \sqrt{\alpha})$, where

$$x^2 = ay^2 + \frac{d}{a}z^2 \text{ with } x, y, z \in \mathbb{Z} \text{ and } \gcd(x, y, z) = 1, \quad \alpha := x + y\sqrt{a}.$$

Reflection principles

In the literature there are many known results that compare different class groups. For example, we have

$$\mathrm{rk}_3 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \leq \mathrm{rk}_3 \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d})) \leq 1 + \mathrm{rk}_3 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})),$$

which is known as Scholz's reflection principle.

Reflection principles

In the literature there are many known results that compare different class groups. For example, we have

$$\mathrm{rk}_3\mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \leq \mathrm{rk}_3\mathrm{Cl}(\mathbb{Q}(\sqrt{-3d})) \leq 1 + \mathrm{rk}_3\mathrm{Cl}(\mathbb{Q}(\sqrt{d})),$$

which is known as Scholz's reflection principle.

The main algebraic result in Smith's work is in fact a reflection principle that compares Art_m of 2^m quadratic fields.

Reflection principles

In the literature there are many known results that compare different class groups. For example, we have

$$\mathrm{rk}_3 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \leq \mathrm{rk}_3 \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d})) \leq 1 + \mathrm{rk}_3 \mathrm{Cl}(\mathbb{Q}(\sqrt{d})),$$

which is known as Scholz's reflection principle.

The main algebraic result in Smith's work is in fact a reflection principle that compares Art_m of 2^m quadratic fields.

How can we find such reflection principles?

Reflection principles

In the literature there are many known results that compare different class groups. For example, we have

$$\mathrm{rk}_3\mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \leq \mathrm{rk}_3\mathrm{Cl}(\mathbb{Q}(\sqrt{-3d})) \leq 1 + \mathrm{rk}_3\mathrm{Cl}(\mathbb{Q}(\sqrt{d})),$$

which is known as Scholz's reflection principle.

The main algebraic result in Smith's work is in fact a reflection principle that compares Art_m of 2^m quadratic fields.

How can we find such reflection principles?

Smith's idea is to look for situations where the compositum of various Hilbert class fields is in some sense *small*.

Intersections of Hilbert class fields

Take primes p_1, p_2, q_1, q_2. Now suppose that we have a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{dp_i q_j})$ each lifting the character χ_a.

Intersections of Hilbert class fields

Take primes p_1, p_2, q_1, q_2. Now suppose that we have a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{dp_iq_j})$ each lifting the character χ_a.

Recall that we then get $\alpha_{i,j} \in \mathbb{Q}(\sqrt{a})$ with

$$\mathrm{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\alpha_{i,j}) = \frac{dp_iq_j}{a} z_{i,j}^2.$$

Intersections of Hilbert class fields

Take primes p_1, p_2, q_1, q_2. Now suppose that we have a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{dp_iq_j})$ each lifting the character χ_a.

Recall that we then get $\alpha_{i,j} \in \mathbb{Q}(\sqrt{a})$ with

$$\text{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\alpha_{i,j}) = \frac{dp_iq_j}{a} z_{i,j}^2.$$

Then we see that the norm of $\alpha_{1,1}\alpha_{1,2}\alpha_{2,1}\alpha_{2,2}$ is a square.

Intersections of Hilbert class fields

Take primes p_1, p_2, q_1, q_2. Now suppose that we have a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{dp_iq_j})$ each lifting the character χ_a.

Recall that we then get $\alpha_{i,j} \in \mathbb{Q}(\sqrt{a})$ with

$$\mathrm{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\alpha_{i,j}) = \frac{dp_iq_j}{a} z_{i,j}^2.$$

Then we see that the norm of $\alpha_{1,1}\alpha_{1,2}\alpha_{2,1}\alpha_{2,2}$ is a square.

In other words, part of $H_2(\mathbb{Q}(\sqrt{dp_2q_2}))$ is contained in the other $H_2(\mathbb{Q}(\sqrt{dp_iq_j}))$.

Intersections of Hilbert class fields

Take primes p_1, p_2, q_1, q_2. Now suppose that we have a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{dp_i q_j})$ each lifting the character χ_a.

Recall that we then get $\alpha_{i,j} \in \mathbb{Q}(\sqrt{a})$ with

$$\mathrm{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\alpha_{i,j}) = \frac{dp_i q_j}{a} z_{i,j}^2.$$

Then we see that the norm of $\alpha_{1,1}\alpha_{1,2}\alpha_{2,1}\alpha_{2,2}$ is a square.

In other words, part of $H_2(\mathbb{Q}(\sqrt{dp_2 q_2}))$ is contained in the other $H_2(\mathbb{Q}(\sqrt{dp_i q_j}))$. This implies

$$\mathrm{Art}_{2,dp_1q_1}(b, \chi_a) + \mathrm{Art}_{2,dp_1q_2}(b, \chi_a) + \mathrm{Art}_{2,dp_2q_1}(b, \chi_a) + \mathrm{Art}_{2,dp_2q_2}(b, \chi_a) = 0$$

for $b \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{dp_i q_j}))[4]$ a fixed divisor of d.

Intersections of Hilbert class fields

Take primes p_1, p_2, q_1, q_2. Now suppose that we have a degree 4 unramified, abelian extension of $\mathbb{Q}(\sqrt{dp_iq_j})$ each lifting the character χ_a.

Recall that we then get $\alpha_{i,j} \in \mathbb{Q}(\sqrt{a})$ with

$$\mathrm{Norm}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\alpha_{i,j}) = \frac{dp_iq_j}{a} z_{i,j}^2.$$

Then we see that the norm of $\alpha_{1,1}\alpha_{1,2}\alpha_{2,1}\alpha_{2,2}$ is a square.

In other words, part of $H_2(\mathbb{Q}(\sqrt{dp_2q_2}))$ is contained in the other $H_2(\mathbb{Q}(\sqrt{dp_iq_j}))$. This implies

$$\mathrm{Art}_{2,dp_1q_1}(b, \chi_a) + \mathrm{Art}_{2,dp_1q_2}(b, \chi_a) + \mathrm{Art}_{2,dp_2q_1}(b, \chi_a) + \mathrm{Art}_{2,dp_2q_2}(b, \chi_a) = 0$$

for $b \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{dp_iq_j}))[4]$ a fixed divisor of d.

We develop two new reflection principles. Unlike Smith's work, they make essential use of Hilbert reciprocity in multiquadratic fields.

Bonus slide: new reflection principles

For the Artin pairing with dp_iq_j we have (following Smith's ideas)

$$\mathrm{Art}_{2,dp_1q_1}(dp_1q_1,\chi_{ap_1}) + \mathrm{Art}_{2,dp_1q_2}(dp_1q_2,\chi_{ap_1}) +$$
$$\mathrm{Art}_{2,dp_2q_1}(dp_2q_1,\chi_{ap_2}) + \mathrm{Art}_{2,dp_2q_2}(dp_2q_2,\chi_{ap_2}) = \mathrm{Frob}_{K_{p_1p_2,q_1q_2}/\mathbb{Q}}(\infty).$$

Bonus slide: new reflection principles

For the Artin pairing with dp_iq_j we have (following Smith's ideas)

$$\mathrm{Art}_{2,dp_1q_1}(dp_1q_1,\chi_{ap_1})+\mathrm{Art}_{2,dp_1q_2}(dp_1q_2,\chi_{ap_1})+$$
$$\mathrm{Art}_{2,dp_2q_1}(dp_2q_1,\chi_{ap_2})+\mathrm{Art}_{2,dp_2q_2}(dp_2q_2,\chi_{ap_2})=\mathrm{Frob}_{K_{p_1p_2,q_1q_2}/\mathbb{Q}}(\infty).$$

Our reciprocity law shows that

$$\mathrm{Frob}_{K_{p_1p_2,q_1q_2}/\mathbb{Q}}(\infty)=\mathrm{Frob}_{K_{p_1p_2,-1}/\mathbb{Q}}(q_1)+\mathrm{Frob}_{K_{p_1p_2,-1}/\mathbb{Q}}(q_2).$$

Bonus slide: new reflection principles

For the Artin pairing with dp_iq_j we have (following Smith's ideas)

$$\mathrm{Art}_{2,dp_1q_1}(dp_1q_1, \chi_{ap_1}) + \mathrm{Art}_{2,dp_1q_2}(dp_1q_2, \chi_{ap_1}) +$$
$$\mathrm{Art}_{2,dp_2q_1}(dp_2q_1, \chi_{ap_2}) + \mathrm{Art}_{2,dp_2q_2}(dp_2q_2, \chi_{ap_2}) = \mathrm{Frob}_{K_{p_1p_2,q_1q_2}/\mathbb{Q}}(\infty).$$

Our reciprocity law shows that

$$\mathrm{Frob}_{K_{p_1p_2,q_1q_2}/\mathbb{Q}}(\infty) = \mathrm{Frob}_{K_{p_1p_2,-1}/\mathbb{Q}}(q_1) + \mathrm{Frob}_{K_{p_1p_2,-1}/\mathbb{Q}}(q_2).$$

For the pairing between a and χ_a we also develop a new reflection principle.

Potential applications

Some potential applications of these new techniques

- non-vanishing of $L(1/2, \chi)$ for 100% of the quadratic characters χ of $\mathbb{F}_q(t)$;

Potential applications

Some potential applications of these new techniques

- non-vanishing of $L(1/2, \chi)$ for 100% of the quadratic characters χ of $\mathbb{F}_q(t)$;
- prove Greenberg's conjecture for the cyclotomic $\mathbb{Z}_2$-extension for 100% of the real quadratic fields;

Potential applications

Some potential applications of these new techniques

- non-vanishing of $L(1/2, \chi)$ for 100% of the quadratic characters χ of $\mathbb{F}_q(t)$;
- prove Greenberg's conjecture for the cyclotomic $\mathbb{Z}_2$-extension for 100% of the real quadratic fields;
- many new cases of the strong form of Malle's conjecture;

Potential applications

Some potential applications of these new techniques

- non-vanishing of $L(1/2, \chi)$ for 100% of the quadratic characters χ of $\mathbb{F}_q(t)$;
- prove Greenberg's conjecture for the cyclotomic $\mathbb{Z}_2$-extension for 100% of the real quadratic fields;
- many new cases of the strong form of Malle's conjecture;
- extend Smith's result (on the distribution of 2^k-Selmer groups) to elliptic curves with a rational 4-torsion point.

Potential applications

Some potential applications of these new techniques

- non-vanishing of $L(1/2, \chi)$ for 100% of the quadratic characters χ of $\mathbb{F}_q(t)$;
- prove Greenberg's conjecture for the cyclotomic $\mathbb{Z}_2$-extension for 100% of the real quadratic fields;
- many new cases of the strong form of Malle's conjecture;
- extend Smith's result (on the distribution of 2^k-Selmer groups) to elliptic curves with a rational 4-torsion point.

Thank you for your attention!