Integral points on quadratic equations

Peter Koymans
Max Planck Institute for Mathematics

MAX-PLANCK-GESELLSCHAFT

MAGIC Seminar

18 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 variant of Pell's equation

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

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

In this talk we study the equation

$$N_d(x, y) = \ell \text{ in } x, y \in \mathbb{Z}. \tag{1}$$

A variant of Pell's equation

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

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

In this talk we study the equation

$$N_d(x, y) = \ell \text{ in } x, y \in \mathbb{Z}. \tag{1}$$

We would like to know how often equation (1) is soluble as we vary d over squarefree integers.

A variant of Pell's equation

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

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

In this talk we study the equation

$$N_d(x, y) = \ell \text{ in } x, y \in \mathbb{Z}. \tag{1}$$

We would like to know how often equation (1) is soluble as we vary d over squarefree integers.

Equivalently, ℓ has residue field degree 1 in the *narrow Hilbert class field* of $\mathbb{Q}(\sqrt{d})$, denoted $H(\mathbb{Q}(\sqrt{d}))$.

A variant of Pell's equation

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

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

In this talk we study the equation

$$N_d(x, y) = \ell \text{ in } x, y \in \mathbb{Z}. \tag{1}$$

We would like to know how often equation (1) is soluble as we vary d over squarefree integers.

Equivalently, ℓ has residue field degree 1 in the *narrow Hilbert class field* of $\mathbb{Q}(\sqrt{d})$, denoted $H(\mathbb{Q}(\sqrt{d}))$.

Currently, the typical behavior of $H(\mathbb{Q}(\sqrt{d}))$ is poorly understood.

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

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

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

Genus theory

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

Genus theory

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

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

Genus theory

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

The group $\mathrm{Cl}(K)[2]$ has a 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

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

The group $\mathrm{Cl}(K)[2]$ has a 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 $\mathcal{O}_K$.

Indeed, 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.

Fouvry and Klüners dealt with the distribution of $2\mathrm{Cl}(K)[4]$.

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 $2\mathrm{Cl}(K)[4]$.

Theorem 1 (Smith, 2017)

Gerth's conjecture is true.

Back to our equation

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.

Back to our equation

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.

Equivalently, the unique ideal $\mathfrak{l}$ above ℓ splits completely in $H_2(\mathbb{Q}(\sqrt{d}))$.

Back to our equation

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.

Equivalently, the unique ideal $\mathfrak{l}$ above ℓ splits completely in $H_2(\mathbb{Q}(\sqrt{d}))$.

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 $x, y \in R$.

Back to our equation

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.

Equivalently, the unique ideal $\mathfrak{l}$ above ℓ splits completely in $H_2(\mathbb{Q}(\sqrt{d}))$.

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 $x, y \in R$.

By classical techniques in analytic number theory

$$|S_{\mathbb{Q},X,\ell}| \sim c_\ell \frac{X}{\sqrt{\log X}}.$$

Our results

Define

$$\eta_k := \prod_{j=1}^{k}(1 - 2^{-j}) \text{ with } k \in \mathbb{Z}_{\geq 0} \cup \{\infty\}, \quad \gamma := \sum_{j=0}^{\infty} \frac{2^{-j^2}\eta_\infty \eta_j^{-2}}{2^{j+1} - 1}.$$

Our results

Define

$$\eta_k := \prod_{j=1}^{k}(1-2^{-j}) \text{ with } k \in \mathbb{Z}_{\geq 0} \cup \{\infty\}, \quad \gamma := \sum_{j=0}^{\infty} \frac{2^{-j^2}\eta_\infty \eta_j^{-2}}{2^{j+1}-1}.$$

Theorem 2 (K.-Pagano)

Let ℓ be an integer such that $|\ell|$ is a prime 3 modulo 4. Then we have

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

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 3 (K.-Pagano)

Let $\ell > 3$ be a prime 3 modulo 4. Then we have

$$\begin{aligned}|\{0 < d < X \text{ squarefree} : H_{-\ell,d} = 2\}| &\sim |S_{\mathbb{Z},X,\ell}| + |S_{\mathbb{Z},X,-\ell}| \\ &\sim \gamma \cdot (c_\ell + c_{-\ell}) \cdot \frac{X}{\sqrt{\log X}}.\end{aligned}$$

A heuristical interpretation of γ

One can show that

$$x^2 - dy^2 = \ell \text{ is soluble with } x, y \in \mathbb{Q} \iff \ell \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$$

and we recall that

$$\gamma := \sum_{j=0}^{\infty} \frac{2^{-j^2} \eta_\infty \eta_j^{-2}}{2^{j+1} - 1}.$$

A heuristical interpretation of γ

One can show that

$$x^2 - dy^2 = \ell \text{ is soluble with } x, y \in \mathbb{Q} \iff \mathfrak{l} \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$$

and we recall that

$$\gamma := \sum_{j=0}^{\infty} \frac{2^{-j^2} \eta_\infty \eta_j^{-2}}{2^{j+1} - 1}.$$

We have

$$\lim_{X \to \infty} \frac{|\{d \in S_{\mathbb{Q},X,\ell} : \dim_{\mathbb{F}_2} 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4] = j\}|}{|S_{\mathbb{Q},X,\ell}|} = 2^{-j^2} \eta_\infty \eta_j^{-2}.$$

A heuristical interpretation of γ

One can show that

$$x^2 - dy^2 = \ell \text{ is soluble with } x, y \in \mathbb{Q} \iff \mathfrak{l} \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$$

and we recall that

$$\gamma := \sum_{j=0}^{\infty} \frac{2^{-j^2} \eta_\infty \eta_j^{-2}}{2^{j+1} - 1}.$$

We have

$$\lim_{X \to \infty} \frac{|\{d \in S_{\mathbb{Q},X,\ell} : \dim_{\mathbb{F}_2} 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4] = j\}|}{|S_{\mathbb{Q},X,\ell}|} = 2^{-j^2} \eta_\infty \eta_j^{-2}.$$

From Gauss genus theory, we get a generating set for $2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$ of dimension $1 + \dim_{\mathbb{F}_2} 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$.

A heuristical interpretation of γ

One can show that

$$x^2 - dy^2 = \ell \text{ is soluble with } x, y \in \mathbb{Q} \iff \ell \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$$

and we recall that

$$\gamma := \sum_{j=0}^{\infty} \frac{2^{-j^2} \eta_\infty \eta_j^{-2}}{2^{j+1} - 1}.$$

We have

$$\lim_{X \to \infty} \frac{|\{d \in S_{\mathbb{Q},X,\ell} : \dim_{\mathbb{F}_2} 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4] = j\}|}{|S_{\mathbb{Q},X,\ell}|} = 2^{-j^2} \eta_\infty \eta_j^{-2}.$$

From Gauss genus theory, we get a generating set for $2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$ of dimension $1 + \dim_{\mathbb{F}_2} 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$.

Heuristic: every non-zero element in this generating set is equally likely to be trivial in $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$.

Reflection principles

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

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

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

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

which is known as Scholz's reflection principle.

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

Reflection principles

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

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

which is known as Scholz's reflection principle.

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

How can we find such reflection principles?

Intersections of Hilbert class fields

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

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

From Gauss genus theory we see that the quadratic unramified extensions of $\mathbb{Q}(\sqrt{d})$ are of the shape $\mathbb{Q}(\sqrt{d}, \sqrt{a})$ with $a \mid d$.

Intersections of Hilbert class fields

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

From Gauss genus theory we see that the quadratic unramified extensions of $\mathbb{Q}(\sqrt{d})$ are of the shape $\mathbb{Q}(\sqrt{d}, \sqrt{a})$ with $a \mid d$.

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

Intersections of Hilbert class fields

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

From Gauss genus theory we see that the quadratic unramified extensions of $\mathbb{Q}(\sqrt{d})$ are of the shape $\mathbb{Q}(\sqrt{d}, \sqrt{a})$ with $a \mid d$.

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

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

Intersections of Hilbert class fields II

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

Intersections of Hilbert class fields II

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

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

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

Intersections of Hilbert class fields II

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

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

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

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

Intersections of Hilbert class fields II

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

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

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

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

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

The Artin pairing

From class field theory and duality of abelian groups we get a natural pairing

$$\mathrm{Art}_{m,d} : 2^{m-1}\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^m] \times 2^{m-1}\mathrm{Gal}(H(\mathbb{Q}(\sqrt{d}))/\mathbb{Q}(\sqrt{d}))^\vee[2^m] \to \mathbb{F}_2$$

that sends $(\mathfrak{p}, \chi) \mapsto \psi(\mathrm{Frob}\ \mathfrak{p})$ with $2^{m-1}\psi = \chi$.

The Artin pairing

From class field theory and duality of abelian groups we get a natural pairing

$$\mathrm{Art}_{m,d} : 2^{m-1}\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^m] \times 2^{m-1}\mathrm{Gal}(H(\mathbb{Q}(\sqrt{d}))/\mathbb{Q}(\sqrt{d}))^\vee[2^m] \to \mathbb{F}_2$$

that sends $(\mathfrak{p}, \chi) \mapsto \psi(\mathrm{Frob}\ \mathfrak{p})$ with $2^{m-1}\psi = \chi$.

The left kernel of $\mathrm{Art}_{m,d}$ is $2^m\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^{m+1}]$, so knowing all the Artin pairings gives $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$.

The Artin pairing

From class field theory and duality of abelian groups we get a natural pairing

$$\mathrm{Art}_{m,d} : 2^{m-1}\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^m] \times 2^{m-1}\mathrm{Gal}(H(\mathbb{Q}(\sqrt{d}))/\mathbb{Q}(\sqrt{d}))^\vee[2^m] \to \mathbb{F}_2$$

that sends $(\mathfrak{p}, \chi) \mapsto \psi(\mathrm{Frob}\ \mathfrak{p})$ with $2^{m-1}\psi = \chi$.

The left kernel of $\mathrm{Art}_{m,d}$ is $2^m\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^{m+1}]$, so knowing all the Artin pairings gives $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$.

Idea: relation between the ψ will give a relation between the Artin pairings. Previous slide then becomes

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

This is not enough for equidistribution!

Intersections of Hilbert class fields again

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

Intersections of Hilbert class fields again

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

From the conics

$$x^2 = ap_1y^2 + \frac{dq_1}{a}z^2, \quad x^2 = ap_1y^2 + \frac{dq_2}{a}z^2$$

we get a solution to $x^2 = ap_1y^2 + q_1q_2z^2$. Doing this one more time gives a solution to

$$x^2 = p_1p_2y^2 + q_1q_2z^2.$$

Intersections of Hilbert class fields again

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

From the conics

$$x^2 = ap_1y^2 + \frac{dq_1}{a}z^2, \quad x^2 = ap_1y^2 + \frac{dq_2}{a}z^2$$

we get a solution to $x^2 = ap_1y^2 + q_1q_2z^2$. Doing this one more time gives a solution to

$$x^2 = p_1p_2y^2 + q_1q_2z^2.$$

In this case we get that

$$\mathrm{Art}_{2,dp_1q_1}(b, ap_1) + \mathrm{Art}_{2,dp_1q_2}(b, ap_1) + \mathrm{Art}_{2,dp_2q_1}(b, ap_2) + \mathrm{Art}_{2,dp_2q_2}(b, ap_2) = K_{p_1p_2,q_1q_2}(\mathrm{Frob}\ b),$$

where $K_{p_1p_2,q_1q_2}$ is a certain D_4-extension containing $\mathbb{Q}(\sqrt{p_1p_2}, \sqrt{q_1q_2})$.

Sketch: equidistribution of Art_2

Pick some small primes $\{p_1, \ldots, p_M\}$ and $\{q_1, \ldots, q_M\}$ with M also small. For $1 \leq i, j, k, l \leq M$, we get linear equations for Art_2 of the shape

$$\mathrm{Art}_{2,dp_iq_k}(b, ap_i) + \mathrm{Art}_{2,dp_iq_l}(b, ap_i) + \\ \mathrm{Art}_{2,dp_jq_k}(b, ap_2) + \mathrm{Art}_{2,dp_jq_l}(b, ap_i) = K_{p_ip_j,q_kq_l}(\mathrm{Frob}\ b).$$

Sketch: equidistribution of Art_2

Pick some small primes $\{p_1, \ldots, p_M\}$ and $\{q_1, \ldots, q_M\}$ with M also small. For $1 \leq i, j, k, l \leq M$, we get linear equations for Art_2 of the shape

$$\mathrm{Art}_{2,dp_iq_k}(b, ap_i) + \mathrm{Art}_{2,dp_iq_l}(b, ap_i) + \\ \mathrm{Art}_{2,dp_jq_k}(b, ap_2) + \mathrm{Art}_{2,dp_jq_l}(b, ap_i) = K_{p_ip_j,q_kq_l}(\mathrm{Frob}\ b).$$

We now vary b and apply the Chebotarev Density Theorem to the compositum of the $K_{p_ip_j,q_kq_l}$. Then the RHS of the linear system appears equally often.

Sketch: equidistribution of Art_2

Pick some small primes $\{p_1, \ldots, p_M\}$ and $\{q_1, \ldots, q_M\}$ with M also small. For $1 \leq i, j, k, l \leq M$, we get linear equations for Art_2 of the shape

$$\mathrm{Art}_{2,dp_iq_k}(b, ap_i) + \mathrm{Art}_{2,dp_iq_l}(b, ap_i) + \mathrm{Art}_{2,dp_jq_k}(b, ap_2) + \mathrm{Art}_{2,dp_jq_l}(b, ap_i) = K_{p_ip_j,q_kq_l}(\mathrm{Frob}\ b).$$

We now vary b and apply the Chebotarev Density Theorem to the compositum of the $K_{p_ip_j,q_kq_l}$. Then the RHS of the linear system appears equally often.

The key combinatorial result is then that for *almost all* choices of the RHS, *any function F* from $\{p_1, \ldots, p_M\} \times \{q_1, \ldots, q_M\} \to \mathbb{F}_2$ satisfying the equations

$$F(p_i, q_k) + F(p_i, q_l) + F(p_j, q_k) + F(p_j, q_l) = RHS,$$

is such that F is 0 roughly 50% of the time (hence also 1 roughly 50% of the time).

Dealing with Art_m

Proceed similarly: sum 2^m Artin pairings to get

$$K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}(\mathrm{Frob}\ b),$$

where $K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}$ is a multiquadratic unramified extension of

$$\mathbb{Q}(\sqrt{p_{1,1}p_{1,2}},\ldots,\sqrt{p_{m,1}p_{m,2}}).$$

Dealing with Art_m

Proceed similarly: sum 2^m Artin pairings to get

$$K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}(\mathrm{Frob}\ b),$$

where $K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}$ is a multiquadratic unramified extension of

$$\mathbb{Q}(\sqrt{p_{1,1}p_{1,2}},\ldots,\sqrt{p_{m,1}p_{m,2}}).$$

This is a rough description of Smith's strategy. What happens if we try to apply it to our family?

The ideal $\mathfrak{l}$

Recall that $\mathfrak{l} \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$.

The ideal $\mathfrak{l}$

Recall that $\mathfrak{l} \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$.

We need to compute $\mathrm{Art}_m(I, a)$. The reflection principle gives

$$K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}(\text{Frob } \ell).$$

The ideal $\mathfrak{l}$

Recall that $\mathfrak{l} \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$.

We need to compute $\mathrm{Art}_m(I, a)$. The reflection principle gives

$$K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}(\mathrm{Frob}\ \ell).$$

Since ℓ is fixed, Chebotarev does no longer work.

The ideal $\mathfrak{l}$

Recall that $\mathfrak{l} \in 2\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[4]$.

We need to compute $\mathrm{Art}_m(I, a)$. The reflection principle gives

$$K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}(\mathrm{Frob}\ \ell).$$

Since ℓ is fixed, Chebotarev does no longer work.

How do we prove equidistribution of $K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}(\mathrm{Frob}\ \ell)$?

Higher Rédei Reciprocity

The key new ingredient in the paper is a new *reciprocity law*.

Higher Rédei Reciprocity

The key new ingredient in the paper is a new *reciprocity law*.

This reciprocity law is a generalization of Rédei reciprocity (in turn a generalization of quadratic reciprocity).

Higher Rédei Reciprocity

The key new ingredient in the paper is a new *reciprocity law*.

This reciprocity law is a generalization of Rédei reciprocity (in turn a generalization of quadratic reciprocity).

The reciprocity law yields that under favorable circumstances

$$K_{p_{1,1}p_{1,2},\ldots,p_{m,1}p_{m,2}}(\text{Frob } \ell) = K_{p_{1,1}p_{1,2},\ldots,p_{m-1,1}p_{m-1,2},\ell}(\text{Frob } p_{m,1}p_{m,2}).$$

We can now apply Chebotarev again.

Higher Rédei Reciprocity

The key new ingredient in the paper is a new *reciprocity law*.

This reciprocity law is a generalization of Rédei reciprocity (in turn a generalization of quadratic reciprocity).

The reciprocity law yields that under favorable circumstances

$$K_{p_{1,1}p_{1,2},\dots,p_{m,1}p_{m,2}}(\mathrm{Frob}\ \ell) = K_{p_{1,1}p_{1,2},\dots,p_{m-1,1}p_{m-1,2},\ell}(\mathrm{Frob}\ p_{m,1}p_{m,2}).$$

We can now apply Chebotarev again.

We prove the reciprocity law by an application of Hilbert reciprocity in the field $\mathbb{Q}(\sqrt{p_{1,1}p_{1,2}}, \dots, \sqrt{p_{m-1,1}p_{m-1,2}})$.

That's it!

Thank you for your attention!