On the 2-part of the class group of $\mathbb{Z}[\sqrt{-2p}]$ for $p \equiv -1 \bmod 4$

Djordjo Milovic

Institute for Advanced Study

September 26, 2016

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Example: $x^2 + y^2 = z^2 \rightsquigarrow$ Gaussian integers $\mathbb{Z}[i]$.

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Example: $x^2 + y^2 = z^2 \rightsquigarrow$ Gaussian integers $\mathbb{Z}[i]$.

Example: $x^p + y^p = z^p \rightsquigarrow$ cyclotomic integers $\mathbb{Z}[\zeta_p]$.

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Example: $x^2 + y^2 = z^2 \rightsquigarrow$ Gaussian integers $\mathbb{Z}[i]$.

Example: $x^p + y^p = z^p \rightsquigarrow$ cyclotomic integers $\mathbb{Z}[\zeta_p]$.

Unlike $\mathbb{Z}$, a number ring might **not** have unique prime factorization:

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Example: $x^2 + y^2 = z^2 \rightsquigarrow$ Gaussian integers $\mathbb{Z}[i]$.

Example: $x^p + y^p = z^p \rightsquigarrow$ cyclotomic integers $\mathbb{Z}[\zeta_p]$.

Unlike $\mathbb{Z}$, a number ring might **not** have unique prime factorization: for instance, in $\mathbb{Z}[\sqrt{-6}]$,

$$10 = 2 \cdot 5$$

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Example: $x^2 + y^2 = z^2 \rightsquigarrow$ Gaussian integers $\mathbb{Z}[i]$.

Example: $x^p + y^p = z^p \rightsquigarrow$ cyclotomic integers $\mathbb{Z}[\zeta_p]$.

Unlike $\mathbb{Z}$, a number ring might **not** have unique prime factorization: for instance, in $\mathbb{Z}[\sqrt{-6}]$,

$$10 = 2 \cdot 5 = (2 + \sqrt{-6}) \cdot (2 - \sqrt{-6}).$$

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Example: $x^2 + y^2 = z^2 \rightsquigarrow$ Gaussian integers $\mathbb{Z}[i]$.

Example: $x^p + y^p = z^p \rightsquigarrow$ cyclotomic integers $\mathbb{Z}[\zeta_p]$.

Unlike $\mathbb{Z}$, a number ring might **not** have unique prime factorization: for instance, in $\mathbb{Z}[\sqrt{-6}]$,

$$10 = 2 \cdot 5 = (2 + \sqrt{-6}) \cdot (2 - \sqrt{-6}).$$

However, a(n integrally closed) number ring always has **unique prime ideal factorization**:

Number rings

In number theory, Diophantine equations over $\mathbb{Z}$ are often solved in **number rings**.

Example: $x^2 + y^2 = z^2 \rightsquigarrow$ Gaussian integers $\mathbb{Z}[i]$.

Example: $x^p + y^p = z^p \rightsquigarrow$ cyclotomic integers $\mathbb{Z}[\zeta_p]$.

Unlike $\mathbb{Z}$, a number ring might **not** have unique prime factorization: for instance, in $\mathbb{Z}[\sqrt{-6}]$,

$$10 = 2 \cdot 5 = (2 + \sqrt{-6}) \cdot (2 - \sqrt{-6}).$$

However, a(n integrally closed) number ring always has **unique prime ideal factorization**:

$$(10) = \mathfrak{p}_2^2 \cdot (\mathfrak{p}_5 \mathfrak{p}_5') = (\mathfrak{p}_2 \mathfrak{p}_5) \cdot (\mathfrak{p}_2 \mathfrak{p}_5').$$

Class groups and units

Obstructions in passing from ideals to elements:

Class groups and units

Obstructions in passing from ideals to elements:

1. Non-principality $\rightsquigarrow$ **class group** $\mathrm{Cl} := \mathcal{I}/\mathcal{P}$.

Class groups and units

Obstructions in passing from ideals to elements:

1. Non-principality $\rightsquigarrow$ **class group** $\mathrm{Cl} := \mathcal{I}/\mathcal{P}$.

Example: In $\mathbb{Z}[\sqrt{-6}]$, $\mathfrak{p}_2 = (2, \sqrt{-6})$ is not principal and in fact $\mathrm{Cl} \cong \mathbb{Z}/2\mathbb{Z}$.

Class groups and units

Obstructions in passing from ideals to elements:

1. Non-principality $\rightsquigarrow$ **class group** $\mathrm{Cl} := \mathcal{I}/\mathcal{P}$.

Example: In $\mathbb{Z}[\sqrt{-6}]$, $\mathfrak{p}_2 = (2, \sqrt{-6})$ is not principal and in fact $\mathrm{Cl} \cong \mathbb{Z}/2\mathbb{Z}$.

2. Principal ideals may have infinitely many generators.

Class groups and units

Obstructions in passing from ideals to elements:

1. Non-principality $\rightsquigarrow$ **class group** $\mathrm{Cl} := \mathcal{I}/\mathcal{P}$.

Example: In $\mathbb{Z}[\sqrt{-6}]$, $\mathfrak{p}_2 = (2, \sqrt{-6})$ is not principal and in fact $\mathrm{Cl} \cong \mathbb{Z}/2\mathbb{Z}$.

2. Principal ideals may have infinitely many generators.

Example: In $\mathbb{Z}[\sqrt{2017}]$,

Class groups and units

Obstructions in passing from ideals to elements:

1. Non-principality $\rightsquigarrow$ **class group** $\mathrm{Cl} := \mathcal{I}/\mathcal{P}$.

Example: In $\mathbb{Z}[\sqrt{-6}]$, $\mathfrak{p}_2 = (2, \sqrt{-6})$ is not principal and in fact $\mathrm{Cl} \cong \mathbb{Z}/2\mathbb{Z}$.

2. Principal ideals may have infinitely many generators.

Example: In $\mathbb{Z}[\sqrt{2017}]$, if $(a, b) =$

$$(10651529913260318450384444, 2371696115380807559791481),$$

Class groups and units

Obstructions in passing from ideals to elements:

1. Non-principality $\rightsquigarrow$ **class group** $\mathrm{Cl} := \mathcal{I}/\mathcal{P}$.

Example: In $\mathbb{Z}[\sqrt{-6}]$, $\mathfrak{p}_2 = (2, \sqrt{-6})$ is not principal and in fact $\mathrm{Cl} \cong \mathbb{Z}/2\mathbb{Z}$.

2. Principal ideals may have infinitely many generators.

Example: In $\mathbb{Z}[\sqrt{2017}]$, if $(a, b) =$

$$(10651529913260318450384444, 237169611538080755979 1481),$$

then

$$(a + b\sqrt{2017}) \cdot (a - b\sqrt{2017}) = -1.$$

A conjecture

A conjecture

Gauss proved that the class group of $\mathbb{Z}[\sqrt{-2p}]$ is of the form

$$\mathrm{Cl}(-8p) \cong \mathbb{Z}/2^r\mathbb{Z} \times (\text{odd}),$$

with $r \geq 1$.

A conjecture

Gauss proved that the class group of $\mathbb{Z}[\sqrt{-2p}]$ is of the form

$$\mathrm{Cl}(-8p) \cong \mathbb{Z}/2^r\mathbb{Z} \times (\text{odd}),$$

with $r \geq 1$. We focus on the case $p \equiv -1 \bmod 4$.

A conjecture

Gauss proved that the class group of $\mathbb{Z}[\sqrt{-2p}]$ is of the form

$$\mathrm{Cl}(-8p) \cong \mathbb{Z}/2^r\mathbb{Z} \times (\text{odd}),$$

with $r \geq 1$. We focus on the case $p \equiv -1 \bmod 4$. Let

$$N(2^k, X) = \#\{p \leq X : p \equiv -1 \bmod 4,\ 2^k \mid \#\mathrm{Cl}(-8p)\}.$$

A conjecture

Gauss proved that the class group of $\mathbb{Z}[\sqrt{-2p}]$ is of the form

$$\mathrm{Cl}(-8p) \cong \mathbb{Z}/2^r\mathbb{Z} \times (\text{odd}),$$

with $r \geq 1$. We focus on the case $p \equiv -1 \bmod 4$. Let

$$N(2^k, X) = \#\{p \leq X : p \equiv -1 \bmod 4,\ 2^k \mid \#\mathrm{Cl}(-8p)\}.$$

2^k	$N(2^k, 10^6)$	$N(2^k, 10^6)/\pi(10^6)$
2	39322	50.09%
4	19669	25.06%
8	9837	12.53%
16	5027	6.40%
32	2482	3.16%
64	1271	1.62%

A conjecture

Gauss proved that the class group of $\mathbb{Z}[\sqrt{-2p}]$ is of the form

$$\mathrm{Cl}(-8p) \cong \mathbb{Z}/2^r\mathbb{Z} \times (\text{odd}),$$

with $r \geq 1$. We focus on the case $p \equiv -1 \bmod 4$. Let

$$N(2^k, X) = \#\{p \leq X : p \equiv -1 \bmod 4,\ 2^k \mid \#\mathrm{Cl}(-8p)\}.$$

2^k	$N(2^k, 10^6)$	$N(2^k, 10^6)/\pi(10^6)$
2	39322	50.09%
4	19669	25.06%
8	9837	12.53%
16	5027	6.40%
32	2482	3.16%
64	1271	1.62%

Conjecture

$N(2^k, X) \sim 2^{-k}\pi(X)$ as $X \to +\infty$ for all $k \geq 1$.

Some results

Some results

Theorem (Rédei, 1934)

$N(4, X) \sim \frac{1}{4}\pi(X)$ *as* $X \to +\infty$.

Some results

Theorem (Rédei, 1934)
$N(4, X) \sim \frac{1}{4}\pi(X)$ *as* $X \to +\infty$.

Theorem (Hasse, 1969)
$N(8, X) \sim \frac{1}{8}\pi(X)$ *as* $X \to +\infty$.

Some results

Theorem (Rédei, 1934)
$N(4, X) \sim \frac{1}{4}\pi(X)$ *as* $X \to +\infty$.

Theorem (Hasse, 1969)
$N(8, X) \sim \frac{1}{8}\pi(X)$ *as* $X \to +\infty$.

Theorem (M., 2015)
$N(16, X) \sim \frac{1}{16}\pi(X)$ *as* $X \to +\infty$.

Criteria for divisibility by powers of 2

$$4 | \#\mathrm{Cl}(-8p) \iff p \equiv -1 \bmod 8 \qquad \text{(Rédei, 1934)}$$

Criteria for divisibility by powers of 2

$$\begin{aligned} 4 \mid \#\mathrm{Cl}(-8p) &\iff p \equiv -1 \bmod 8 \qquad \text{(Rédei, 1934)} \\ &\iff \mathrm{Frob}(p; \mathbb{Q}(\zeta_8)/\mathbb{Q}) \equiv -1 \bmod 8 \end{aligned}$$

Criteria for divisibility by powers of 2

$$
\begin{aligned}
4 \mid \#\mathrm{Cl}(-8p) \quad &\iff \quad p \equiv -1 \bmod 8 \qquad &&\text{(Rédei, 1934)}\\
&\iff \quad \mathrm{Frob}(p; \mathbb{Q}(\zeta_8)/\mathbb{Q}) \equiv -1 \bmod 8 &&\\
8 \mid \#\mathrm{Cl}(-8p) \quad &\iff \quad p \equiv -1 \bmod 16 \qquad &&\text{(Hasse, 1969)}
\end{aligned}
$$

Criteria for divisibility by powers of 2

$$
\begin{aligned}
4 \mid \#\mathrm{Cl}(-8p) &\iff p \equiv -1 \bmod 8 \qquad \text{(Rédei, 1934)}\\
&\iff \mathrm{Frob}(p; \mathbb{Q}(\zeta_8)/\mathbb{Q}) \equiv -1 \bmod 8\\
8 \mid \#\mathrm{Cl}(-8p) &\iff p \equiv -1 \bmod 16 \qquad \text{(Hasse, 1969)}\\
&\iff \mathrm{Frob}(p; \mathbb{Q}(\zeta_{16})/\mathbb{Q}) \equiv -1 \bmod 16
\end{aligned}
$$

Criteria for divisibility by powers of 2

$$\begin{aligned}
4|\#\mathrm{Cl}(-8p) &\iff p \equiv -1 \bmod 8 \qquad \text{(Rédei, 1934)} \\
&\iff \mathrm{Frob}(p; \mathbb{Q}(\zeta_8)/\mathbb{Q}) \equiv -1 \bmod 8 \\
8|\#\mathrm{Cl}(-8p) &\iff p \equiv -1 \bmod 16 \qquad \text{(Hasse, 1969)} \\
&\iff \mathrm{Frob}(p; \mathbb{Q}(\zeta_{16})/\mathbb{Q}) \equiv -1 \bmod 16
\end{aligned}$$

Theorem (Čebotarev, 1922, + La Vallée Poussin, 1899)

Let $M/\mathbb{Q}$ be a normal extension with Galois group G. Let C be a union of conjugacy classes in G. Then, as $X \to +\infty$,

$$\begin{aligned}
\pi(X; M/\mathbb{Q}, C) &:= \#\{p \leq X : \mathrm{Frob}(p; M/\mathbb{Q}) \subset C\} \\
&= \frac{\#C}{\#G}\pi(X) + O\left(X \exp(-c_2\sqrt{\log X})\right)
\end{aligned}$$

for some $c > 0$ that depends only on $M/\mathbb{Q}$.

Governing fields

Conjecture (Cohn-Lagarias, 1983)

Let D be an integer and let $k \geq 1$. Then there exists a normal extension $M_D/\mathbb{Q}$ such that the 2^k-rank of $\mathrm{Cl}(Dp)$ (when Dp is a fundamental discriminant) is determined by $\mathrm{Frob}(p; M_D/\mathbb{Q})$.

Governing fields

Conjecture (Cohn-Lagarias, 1983)

Let D be an integer and let $k \geq 1$. Then there exists a normal extension $M_D/\mathbb{Q}$ such that the 2^k-rank of $\mathrm{Cl}(Dp)$ (when Dp is a fundamental discriminant) is determined by $\mathrm{Frob}(p; M_D/\mathbb{Q})$. The field M_D is called a governing field for the 2^k-rank in the family $\{\mathbb{Q}(\sqrt{Dp})\}_p$.

Governing fields

Conjecture (Cohn-Lagarias, 1983)

Let D be an integer and let $k \geq 1$. Then there exists a normal extension $M_D/\mathbb{Q}$ such that the 2^k-rank of $\mathrm{Cl}(Dp)$ (when Dp is a fundamental discriminant) is determined by $\mathrm{Frob}(p; M_D/\mathbb{Q})$. The field M_D is called a governing field for the 2^k-rank in the family $\{\mathbb{Q}(\sqrt{Dp})\}_p$.

Theorem (Stevenhagen, 1989)

Governing fields for the 8-rank exist.

Governing fields

Conjecture (Cohn-Lagarias, 1983)

Let D be an integer and let $k \geq 1$. Then there exists a normal extension $M_D/\mathbb{Q}$ such that the 2^k-rank of $\mathrm{Cl}(Dp)$ (when Dp is a fundamental discriminant) is determined by $\mathrm{Frob}(p; M_D/\mathbb{Q})$. The field M_D is called a governing field for the 2^k-rank in the family $\{\mathbb{Q}(\sqrt{Dp})\}_p$.

Theorem (Stevenhagen, 1989)

Governing fields for the 8-rank exist.

No governing field for the 16-rank has ever been found.

Governing fields

Conjecture (Cohn-Lagarias, 1983)

Let D be an integer and let $k \geq 1$. Then there exists a normal extension $M_D/\mathbb{Q}$ such that the 2^k-rank of $\mathrm{Cl}(Dp)$ (when Dp is a fundamental discriminant) is determined by $\mathrm{Frob}(p; M_D/\mathbb{Q})$. The field M_D is called a governing field for the 2^k-rank in the family $\{\mathbb{Q}(\sqrt{Dp})\}_p$.

Theorem (Stevenhagen, 1989)

Governing fields for the 8-rank exist.

No governing field for the 16-rank has ever been found. Instead, write

$$p = u^2 - 2v^2$$

where u and v are positive integers and $u \equiv 1 \bmod 16$.

Governing fields

Conjecture (Cohn-Lagarias, 1983)

Let D be an integer and let $k \geq 1$. Then there exists a normal extension $M_D/\mathbb{Q}$ such that the 2^k-rank of $\mathrm{Cl}(Dp)$ (when Dp is a fundamental discriminant) is determined by $\mathrm{Frob}(p; M_D/\mathbb{Q})$. The field M_D is called a governing field for the 2^k-rank in the family $\{\mathbb{Q}(\sqrt{Dp})\}_p$.

Theorem (Stevenhagen, 1989)

Governing fields for the 8-rank exist.

No governing field for the 16-rank has ever been found. Instead, write

$$p = u^2 - 2v^2$$

where u and v are positive integers and $u \equiv 1 \bmod 16$. Then

$$16 | \#\mathrm{Cl}(-8p) \iff \left(\frac{v}{u}\right) = 1. \qquad \text{(Leonard-Williams, 1982)}$$

The main result

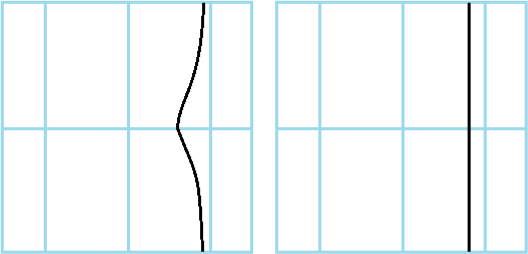
As $X \to \infty$, we have

$$\sum_{\substack{p \le X \\ p \equiv -1 \bmod 16}} \left(\frac{v}{u}\right) \ll X^{\frac{199}{200}}.$$

The main result

As $X \to \infty$, we have

$$\sum_{\substack{p \leq X \\ p \equiv -1 \bmod 16}} \left(\frac{v}{u}\right) \ll X^{\frac{199}{200}}.$$



$$\sigma \leq 1 - \frac{c}{\log t} \qquad \sigma \leq 1 - \delta$$

$$\ll X \exp(-c'\sqrt{\log X}) \qquad \ll_\epsilon X^{1-\delta+\epsilon}$$

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \le X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X\to+\infty} \delta(X)$ and $\delta^+ = \limsup_{X\to+\infty} \delta(X)$.

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \leq X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X \to +\infty} \delta(X)$ and $\delta^+ = \limsup_{X \to +\infty} \delta(X)$.
Stevenhagen (1992) conjectured that $\delta^- = \delta^+ = \frac{1}{3}$.

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \leq X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X \to +\infty} \delta(X)$ and $\delta^+ = \limsup_{X \to +\infty} \delta(X)$. Stevenhagen (1992) conjectured that $\delta^- = \delta^+ = \frac{1}{3}$. The best known bounds are

$$\frac{5}{16} \leq \delta^- \leq \delta^+ \leq \frac{3}{8},$$

and they follow from results available in the 1930's.

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \leq X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X \to +\infty} \delta(X)$ and $\delta^+ = \limsup_{X \to +\infty} \delta(X)$. Stevenhagen (1992) conjectured that $\delta^- = \delta^+ = \frac{1}{3}$. The best known bounds are

$$\frac{5}{16} \leq \delta^- \leq \delta^+ \leq \frac{3}{8},$$

and they follow from results available in the 1930's. To make progress on the upper bound and obtain $\delta^+ \leq \frac{3}{8} - \frac{1}{32} = \frac{11}{32}$:

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \leq X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X \to +\infty} \delta(X)$ and $\delta^+ = \limsup_{X \to +\infty} \delta(X)$. Stevenhagen (1992) conjectured that $\delta^- = \delta^+ = \frac{1}{3}$. The best known bounds are

$$\frac{5}{16} \leq \delta^- \leq \delta^+ \leq \frac{3}{8},$$

and they follow from results available in the 1930's. To make progress on the upper bound and obtain $\delta^+ \leq \frac{3}{8} - \frac{1}{32} = \frac{11}{32}$: in the case that p is a prime number that splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})/\mathbb{Q}$,

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \leq X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X \to +\infty} \delta(X)$ and $\delta^+ = \limsup_{X \to +\infty} \delta(X)$. Stevenhagen (1992) conjectured that $\delta^- = \delta^+ = \frac{1}{3}$. The best known bounds are

$$\frac{5}{16} \leq \delta^- \leq \delta^+ \leq \frac{3}{8},$$

and they follow from results available in the 1930's. To make progress on the upper bound and obtain $\delta^+ \leq \frac{3}{8} - \frac{1}{32} = \frac{11}{32}$: in the case that p is a prime number that splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})/\mathbb{Q}$, one would need to find a criterion "conducive to analytic number theory"

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \leq X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X \to +\infty} \delta(X)$ and $\delta^+ = \limsup_{X \to +\infty} \delta(X)$. Stevenhagen (1992) conjectured that $\delta^- = \delta^+ = \frac{1}{3}$. The best known bounds are

$$\frac{5}{16} \leq \delta^- \leq \delta^+ \leq \frac{3}{8},$$

and they follow from results available in the 1930's. To make progress on the upper bound and obtain $\delta^+ \leq \frac{3}{8} - \frac{1}{32} = \frac{11}{32}$: in the case that p is a prime number that splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})/\mathbb{Q}$, one would need to find a criterion "conducive to analytic number theory" for the unique unramified at finite primes C_8-extension $H_8/\mathbb{Q}(\sqrt{2p})$ to be totally real.

A related open problem

For a real number $X > 3$, let

$$\delta(X) = \#\{p \leq X : x^2 - 2py^2 = -1 \text{ is solvable}\} \cdot \pi(X)^{-1}.$$

Let $\delta^- = \liminf_{X\to+\infty} \delta(X)$ and $\delta^+ = \limsup_{X\to+\infty} \delta(X)$. Stevenhagen (1992) conjectured that $\delta^- = \delta^+ = \frac{1}{3}$. The best known bounds are

$$\frac{5}{16} \leq \delta^- \leq \delta^+ \leq \frac{3}{8},$$

and they follow from results available in the 1930's. To make progress on the upper bound and obtain $\delta^+ \leq \frac{3}{8} - \frac{1}{32} = \frac{11}{32}$: in the case that p is a prime number that splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})/\mathbb{Q}$, one would need to find a criterion "conducive to analytic number theory" for the unique unramified at finite primes C_8-extension $H_8/\mathbb{Q}(\sqrt{2p})$ to be totally real. One approach: non-abelian class field theory over $\mathbb{Q}(\sqrt{2})$.

Thank you for your attention!

A result of Friedlander, Iwaniec, Mazur, and Rubin (2013)

$\{a_\mathfrak{n}\}_\mathfrak{n} \subset \mathbb{C}$. If there exist two real numbers $0 < \theta_1, \theta_2 < 1$ such that

$$A_\mathfrak{d}(X) := \sum_{\substack{\mathrm{Norm}(\mathfrak{n}) \leq X \\ \mathfrak{n} \equiv 0 \bmod \mathfrak{d}}} a_\mathfrak{n} \ll_\epsilon X^{1-\theta_1+\epsilon}$$

and

$$B(M,N) := \sum_{\mathrm{Norm}(\mathfrak{m}) \leq M} \sum_{\mathrm{Norm}(\mathfrak{n}) \leq N} \alpha_\mathfrak{m} \beta_\mathfrak{n} a_{\mathfrak{m}\mathfrak{n}} \ll_\epsilon (M+N)^{\theta_2} (MN)^{1-\theta_2+\epsilon},$$

then

$$S(X) := \sum_{\mathrm{Norm}(\mathfrak{p}) \leq X} a_\mathfrak{p} \ll_\epsilon X^{1-\frac{\theta_1\theta_2}{2+\theta_2}+\epsilon}.$$

Power-saving bounds for **linear** and **bilinear** sums in $a_\mathfrak{n}$ imply a **power-saving** bound for sums over **primes**.

Handling the unit of infinite order

For $u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ with u odd and positive, define

$$[u + v\sqrt{2}] := \left(\frac{v}{u}\right).$$

Lemma

Let $u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that u is odd and positive. Let $\varepsilon = 1 + \sqrt{2}$. Then

$$[u + v\sqrt{2}] = [\varepsilon^8(u + v\sqrt{2})].$$

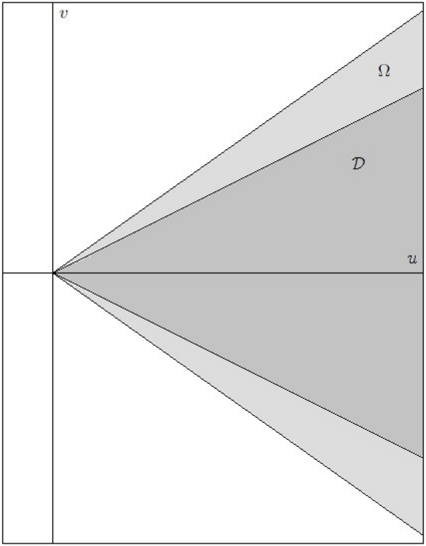
This allows us to define

$$a_{\mathfrak{n}} := [w] + [\varepsilon^2 w] + [\varepsilon^4 w] + [\varepsilon^6 w],$$

where w is any totally positive generator of $\mathfrak{n}$.

A fundamental domain for the action of ε

Let $\mathcal{D} := \{(u, v) \in \mathbb{R}^2 : u > 0, -u < 2v \leq u\}$.



Lemma

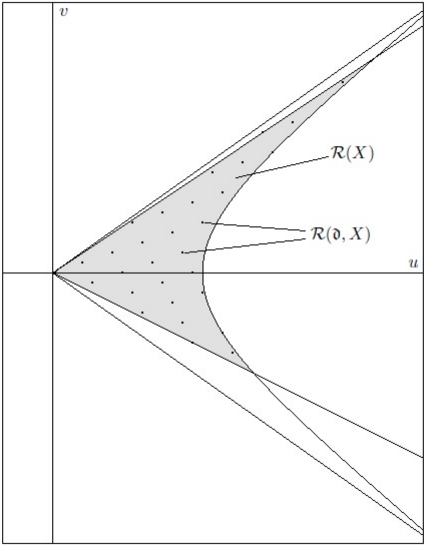
Suppose that $\mathfrak{n}$ is a non-zero ideal of $\mathbb{Z}[\sqrt{2}]$. Then $\mathfrak{n}$ has a unique generator $u + v\sqrt{2}$ such that $(u, v) \in \mathcal{D}$.

Bounding linear sums

Recall that

$$A_{\mathfrak{d}}(X) = \sum_{\substack{\mathrm{Norm}(\mathfrak{n}) \le X \\ \mathfrak{n} \equiv 0 \bmod \mathfrak{d}}} a_{\mathfrak{n}}.$$

We sum $\left(\frac{v}{u}\right)$ over $\mathcal{R}(\mathfrak{d}, X)$ using machinery of **short character sums**.



We obtain

$$A_{\mathfrak{d}}(X) \ll_{\epsilon} X^{\frac{5}{6}+\epsilon},$$

i.e. cancellation with $\theta_1 = \frac{1}{6}$.

Bounding bilinear sums

Recall that $B(M,N) = \sum_{w\in\mathcal{D}(M)} \sum_{z\in\mathcal{D}(N)} \alpha_w \beta_z [wz]$.

Lemma

Let $w = a + b\sqrt{2}$ and $z = c + d\sqrt{2}$ be two primitive, totally positive, odd elements of $\mathbb{Z}[\sqrt{2}]$. Then

$$[wz] \sim [w][z]\gamma(w,z),$$

where

$$\gamma(w,z) := \left(\frac{c + 2bd/a}{a^2 - 2b^2}\right).$$

Hence we are left to bound

$$Q(M,N) := \sum_{w\in\mathcal{D}(M)} \sum_{z\in\mathcal{D}(N)} \alpha_w \beta_z \gamma(w,z).$$

This is a result about **double oscillation**. Get cancellation with $\theta_2 = \frac{1}{12}$.