n-rank of class group of parameterized families quadratic fields

Azizul Hoque

Department of Mathematics
Rangapara College
Rangapara-784505
Assam, INDIA

@Seminars – Online Weekly Research Seminar

March 12, 2021

Contents

1. A number field K is a finite extension of $\mathbb{Q}$.

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.
3. The ring of integers; $\mathcal{O}_K \rightarrow$ set of all algebraic integers in K.

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.
3. The ring of integers; $\mathcal{O}_K \rightarrow$ set of all algebraic integers in K.
4. $$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.
3. The ring of integers; $\mathcal{O}_K \rightarrow$ set of all algebraic integers in K.
4. $$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

For $K := \mathbb{Q}(\sqrt{-5})$:

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.
3. The ring of integers; $\mathcal{O}_K \rightarrow$ set of all algebraic integers in K.
4. $$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

For $K := \mathbb{Q}(\sqrt{-5})$:

1. elements of $K \rightarrow a + b\sqrt{-5}$ with $a, b \in \mathbb{Q}$;

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.
3. The ring of integers; $\mathcal{O}_K \rightarrow$ set of all algebraic integers in K.
4. $$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

For $K := \mathbb{Q}(\sqrt{-5})$:

1. elements of $K \rightarrow a + b\sqrt{-5}$ with $a, b \in \mathbb{Q}$;
2. elements in $\mathcal{O}_K \rightarrow a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$;

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.
3. The ring of integers; $\mathcal{O}_K \rightarrow$ set of all algebraic integers in K.
4. $$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

For $K := \mathbb{Q}(\sqrt{-5})$:

1. elements of $K \rightarrow a + b\sqrt{-5}$ with $a, b \in \mathbb{Q}$;
2. elements in $\mathcal{O}_K \rightarrow a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$;
3. $\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$;

1. A number field K is a finite extension of $\mathbb{Q}$.
2. An algebraic integer is a complex number $\rightarrow$ a root of some monic polynomial in $\mathbb{Z}[x]$.
3. The ring of integers; $\mathcal{O}_K \rightarrow$ set of all algebraic integers in K.
4. $$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Example

For $K := \mathbb{Q}(\sqrt{-5})$:

1. elements of $K \rightarrow a + b\sqrt{-5}$ with $a, b \in \mathbb{Q}$;
2. elements in $\mathcal{O}_K \rightarrow a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$;
3. $\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$;
4. $$\begin{array}{ccc} \mathbb{Z}(\sqrt{-5}) & \subset & \mathbb{Q}(\sqrt{-5}) \\ \uparrow & & \uparrow \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Motivation

❀ $\mathbb{Z} \rightarrow$ has unique factorization of integers into primes. But, in $\mathcal{O}_K \rightarrow$ **not** necessarily has unique factorization of algebraic integers into primes (irreducibles).

Motivation

- $\mathbb{Z} \rightarrow$ has unique factorization of integers into primes. But, in $\mathcal{O}_K \rightarrow$ **not** necessarily has unique factorization of algebraic integers into primes (irreducibles).

- $K = \mathbb{Q}(\sqrt{-5})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In $\mathcal{O}_K$:

$$2 \times 3 = 6 = (1 + \sqrt{-5}) \times (1 - \sqrt{-5})$$

Now $2, 3, 1 \pm \sqrt{-5}$ are irreducibles in $\mathcal{O}_K \rightarrow$ 2 distinct factorizations of 6 $\Rightarrow \mathcal{O}_K$ is **not** UFD.

Class group

☆ Fractional ideal $\rightarrow$ a non-zero $\mathcal{O}_K$-module $\mathcal{I} \subset K$ such that $d\mathcal{I} \subset \mathcal{O}_K$ for some $d \in \mathcal{O}_K - \{0\}$.

Class group

- ★ Fractional ideal $\rightarrow$ a non-zero $\mathcal{O}_K$-module $\mathcal{I} \subset K$ such that $d\mathcal{I} \subset \mathcal{O}_K$ for some $d \in \mathcal{O}_K - \{0\}$.

- ★ Ideal class group $\rightarrow$

$$\mathfrak{C}_K := \frac{\text{The group of all fractional ideals of K}}{\text{The group of all principal fractional ideals of K}}$$

Class group

- Fractional ideal $\rightarrow$ a non-zero $\mathcal{O}_K$-module $\mathcal{I} \subset K$ such that $d\mathcal{I} \subset \mathcal{O}_K$ for some $d \in \mathcal{O}_K - \{0\}$.

- Ideal class group $\rightarrow$

$$\mathfrak{C}_K := \frac{\text{The group of all fractional ideals of K}}{\text{The group of all principal fractional ideals of K}}$$

- Class number; h_K $\rightarrow$ order of $\mathfrak{C}_K$.

General problems

- $K \to$ number field
  $\mathfrak{C}_K \to$ Class group of K
  $h_K \to$ class number of K

General problems

- $K \rightarrow$ number field
  $\mathfrak{C}_K \rightarrow$ Class group of K
  $h_K \rightarrow$ class number of K

- Natural questions to ask:
  1. What is the size of $\mathfrak{C}_K$?

General problems

- $K \to$ number field
  $\mathfrak{C}_K \to$ Class group of K
  $h_K \to$ class number of K

- Natural questions to ask:
  1. What is the size of $\mathfrak{C}_K$?
  2. What is the structure of $\mathfrak{C}_K$?

General problems

- $K \rightarrow$ number field
  $\mathfrak{C}_K \rightarrow$ Class group of K
  $h_K \rightarrow$ class number of K

- Natural questions to ask:
  1. What is the size of $\mathfrak{C}_K$?
  2. What is the structure of $\mathfrak{C}_K$?
  3. Do these questions have a quantitative answer, depending, say, on the size of the discriminant of K?

Classical results on the size

- ☞ Assume that K runs through imaginary quadratic fields. In 1801, Gauss cojectured that:

$$\lim_{\mathrm{Disc(K)}\to -\infty} h_K = +\infty$$

Classical results on the size

- Assume that K runs through imaginary quadratic fields. In 1801, Gauss cojectured that:

$$\lim_{\text{Disc(K)}\to-\infty} h_K = +\infty$$

- In 1934, Heilbronn proved this conjecture.

Classical results on the size

☞ Assume that K runs through imaginary quadratic fields. In 1801, Gauss cojectured that:

$$\lim_{\mathrm{Disc(K)} \to -\infty} h_K = +\infty$$

☛ In 1934, Heilbronn proved this conjecture.

☞ LCNL: For given low class number (eg. 1, 2, and 3), Gauss gives lists of imaginary quadratic fields with the given class number and believed them to be complete. SOLVED COMPLETELY.

Classical results on the size

- Assume that K runs through imaginary quadratic fields. In 1801, Gauss cojectured that:

$$\lim_{\text{Disc(K)} \to -\infty} h_K = +\infty$$

- In 1934, Heilbronn proved this conjecture.
- LCNL: For given low class number (eg. 1, 2, and 3), Gauss gives lists of imaginary quadratic fields with the given class number and believed them to be complete. SOLVED COMPLETELY.
- Gauss also conjectured that there are ∞-ly many real quadratic fields with class number one. This problem is still open.

Gauss–Heilbronn

Carl Friedrich Gauss

Hans Arnold Heilbronn

A question about the structure

- ☆ If $n > 1$ is an integer and G is a finite abelian group, by n-rank of G, $rank_n G$, we mean the largest positive integer r such that G contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup.

A question about the structure

☆ If $n > 1$ is an integer and G is a finite abelian group, by n-rank of G, $rank_n G$, we mean the largest positive integer r such that G contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup.

Remark

For a given integer $n \geq 2$, $n \mid h_K \Leftrightarrow rank_n K \geq 1$.

A question about the structure

☆ If $n > 1$ is an integer and G is a finite abelian group, by n-rank of G, $rank_n G$, we mean the largest positive integer r such that G contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup.

Remark

For a given integer $n \geq 2$, $n \mid h_K \Leftrightarrow rank_n K \geq 1$.

Conjecture (Folklore)

For an integer $n > 1$, the $rank_n \mathfrak{C}_K$ is unbounded when K runs through all quadratic fields.

Some notations

☆ x, y, n and $\mu \longrightarrow$ positive integers. We consider:

$$K_{x,y,n,\mu} = \mathbb{Q}(\sqrt{x^2 - \mu y^n})$$

with the conditions: $\gcd(x, y) = 1,\ y > 1$ and $x^2 \leq \mu y^n$.

Some notations

☆ x, y, n and $\mu \longrightarrow$ positive integers. We consider:

$$K_{x,y,n,\mu} = \mathbb{Q}(\sqrt{x^2 - \mu y^n})$$

with the conditions: $\gcd(x, y) = 1$, $y > 1$ and $x^2 \leq \mu y^n$.

☆ $s \longrightarrow$ the $+$ve integer such that

$$x^2 - y^n = -s^2 D.$$

Results of Ankeny-Chowla and Soundararajan

☞ Ankeny and Chowla[1] proved that $h_{K_{x,3,n,1}}$ is divisible by n if

1. $x > 0$ is an even;
2. n is a sufficiently large and even;
3. $0 < x < \sqrt{(2.3^{n-1})}$ and
4. $s = 1$.

[1] N. C. Ankeny & S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math., **5** (1955).

[2] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. **61** (2000), 681–690.

Results of Ankeny-Chowla and Soundararajan

- Ankeny and Chowla[1] proved that $h_{K_{x,3,n,1}}$ is divisible by n if
  1. $x > 0$ is an even;
  2. n is a sufficiently large and even;
  3. $0 < x < \sqrt{(2.3^{n-1})}$ and
  4. $s = 1$.

- K. Soundararajan[2] studied the divisibility of $h_{K_{x,y,n,1}}$ by n under the condition $s < \sqrt{(y^n - x^2)/(y^{n/2} - 1)}$.

[1] N. C. Ankeny & S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math., **5** (1955).

[2] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. **61** (2000), 681–690.

Ankeny-Chowla

Nesmith Cornett Ankeny

Sarvadaman D. S. Chowla

Two results

Theorem (KC, AH, YK, PPP)

Let n an odd integer, p and q be distinct odd primes with $q^2 < p^n$. Let d be the square-free part of $q^2 - p^n$. Assume that $q \not\equiv \pm 1 \pmod{|d|}$. Then $n | h_{K_{p,q,n,1}}$ if

$$p^{n/3} \neq (2q+1)/3, (q^2+2)/3$$

whenever both $d \equiv 1 \pmod 4$ and $3 \mid n$.

K. Chakraborty, A. Hoque, Y. Kishi and P. P. Pandey, Divisibility of the class numbers of imaginary quadratic fields, J. Number Theory, **185** (2018) 339–348.

Two results

Theorem (KC, AH, YK, PPP)

Let n an odd integer, p and q be distinct odd primes with $q^2 < p^n$. Let d be the square-free part of $q^2 - p^n$. Assume that $q \not\equiv \pm 1 \pmod{|d|}$. Then $n | h_{K_{p,q,n,1}}$ if

$$p^{n/3} \neq (2q+1)/3, (q^2+2)/3$$

whenever both $d \equiv 1 \pmod 4$ and $3 \mid n$.

Theorem (KC, AH, YK, PPP)

Let $n \geq 3$ be an odd integer not divisible by 3. For each odd prime q the class number of $K_{p,q,n,1}$ is divisible by n for all but finitely many p's.

K. Chakraborty, A. Hoque, Y. Kishi and P. P. Pandey, Divisibility of the class numbers of imaginary quadratic fields, J. Number Theory, **185** (2018) 339–348.

A question

For each odd prime $q \neq n$, let S_q denote the set odd primes $p \notin \{q, n\}$ such that $q^2 < p^n$ and the class number of $\mathbb{Q}(\sqrt{q^2 - p^n})$ is not divisible by n.

[3] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387–398.

A question

For each odd prime $q \neq n$, let S_q denote the set odd primes $p \notin \{q, n\}$ such that $q^2 < p^n$ and the class number of $\mathbb{Q}(\sqrt{q^2 - p^n})$ is not divisible by n.

Question: Is $S_q \neq \phi$ for infinitely many q?

[3] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387–398.

A question

For each odd prime $q \neq n$, let S_q denote the set odd primes $p \notin \{q, n\}$ such that $q^2 < p^n$ and the class number of $\mathbb{Q}(\sqrt{q^2 - p^n})$ is not divisible by n.

Question: Is $S_q \neq \phi$ for infinitely many q?

Remark: Kohnen and Ono[3] gave an infinite family of imaginary quadratic fields with class number not divisible by a given prime number.

[3] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387–398.

Conjecture (Wada)

All the class groups of imaginary quadratic fields are either cyclic or of the type $C_{h_1} \times C_{h_2} \times C_{2^{r_1}} \times C_{2^{r_2}} \times \cdots \times C_{2^{r_k}}$.

H. Wada, *A table of ideal class groups of imaginary quadratic fields*, Proc. Japan Acad. **46** (1970), 401–403.

[4] K. Chakraborty and A. Hoque, Exponents of class groups of certain imaginary quadratic fields, *Czechoslovak Math. J.*, 70 (2020), no. 4, 1167–1178.

Conjecture (Wada)

All the class groups of imaginary quadratic fields are either cyclic or of the type $C_{h_1} \times C_{h_2} \times C_{2^{r_1}} \times C_{2^{r_2}} \times \cdots \times C_{2^{r_k}}$.

☆ We[4] consider:

$$K_{x,y,n,2} = \mathbb{Q}(\sqrt{x^2 - 2y^n}).$$

H. Wada, *A table of ideal class groups of imaginary quadratic fields*, Proc. Japan Acad. **46** (1970), 401–403.

[4] K. Chakraborty and A. Hoque, Exponents of class groups of certain imaginary quadratic fields, *Czechoslovak Math. J.*, 70 (2020), no. 4, 1167–1178.

Conjecture (Wada)

All the class groups of imaginary quadratic fields are either cyclic or of the type $C_{h_1} \times C_{h_2} \times C_{2^{r_1}} \times C_{2^{r_2}} \times \cdots \times C_{2^{r_k}}$.

- We[4] consider:

$$K_{x,y,n,2} = \mathbb{Q}(\sqrt{x^2 - 2y^n}).$$

- $\mathfrak{C}_{K_{5,11,27,2}} = C_{381006210618} \times C_6 \times C_6 \times C_2 \times C_2 \times C_2.$

H. Wada, *A table of ideal class groups of imaginary quadratic fields*, Proc. Japan Acad. **46** (1970), 401–403.

[4] K. Chakraborty and A. Hoque, Exponents of class groups of certain imaginary quadratic fields, *Czechoslovak Math. J.*, 70 (2020), no. 4, 1167–1178.

Conjecture (Wada)

All the class groups of imaginary quadratic fields are either cyclic or of the type $C_{h_1} \times C_{h_2} \times C_{2^{r_1}} \times C_{2^{r_2}} \times \cdots \times C_{2^{r_k}}$.

☆ We[4] consider:

$$K_{x,y,n,2} = \mathbb{Q}(\sqrt{x^2 - 2y^n}).$$

☆ $\mathfrak{C}_{K_{5,11,27,2}} = C_{381006210618} \times C_6 \times C_6 \times C_2 \times C_2 \times C_2$.

Conjecture (Chakraborty-Hoque)

Let p and q be two distinct odd primes. For each positive odd integer n and for each positive integer m such that m is not a n-root of any rational integer, there are infinitely many imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{p^2 - mq^n})$ *whose class number is divisible by n.*

H. Wada, *A table of ideal class groups of imaginary quadratic fields*, Proc. Japan Acad. **46** (1970), 401–403.

[4] K. Chakraborty and A. Hoque, Exponents of class groups of certain imaginary quadratic fields, *Czechoslovak Math. J.*, 70 (2020), no. 4, 1167–1178.

$N(3, r, x) \longrightarrow$ The # of quadratic fields whose class group has 3-rank at least r and absolute discriminant $\leq x$.

Theorem (−)

$N(3, 3, x) \gg x^{\frac{1}{3}}$.

A. Hoque, *Parameterized families of quadratic fields with class groups of 3-rank at least* 3, Preprint

$N(3, r, x) \longrightarrow$ The # of quadratic fields whose class group has 3-rank at least r and absolute discriminant $\leq x$.

Theorem (−)

$N(3, 3, x) \gg x^{\frac{1}{3}}$.

Outline of the proof:

1. Utilization of Hilbert class field theory.

A. Hoque, *Parameterized families of quadratic fields with class groups of 3-rank at least* 3, Preprint

$N(3, r, x) \longrightarrow$ The # of quadratic fields whose class group has 3-rank at least r and absolute discriminant $\leq x$.

Theorem (−)

$N(3, 3, x) \gg x^{\frac{1}{3}}$.

Outline of the proof:

1. Utilization of Hilbert class field theory.
2. Construction of 3 cyclic, cubic, unramified extensions L_1, L_2, L_3 of $K = \mathbb{Q}(\sqrt{d})$.

A. Hoque, *Parameterized families of quadratic fields with class groups of 3-rank at least* 3, Preprint

$N(3, r, x) \longrightarrow$ The # of quadratic fields whose class group has 3-rank at least r and absolute discriminant $\leq x$.

Theorem (−)

$N(3, 3, x) \gg x^{\frac{1}{3}}$.

Outline of the proof:

1. Utilization of Hilbert class field theory.
2. Construction of 3 cyclic, cubic, unramified extensions L_1, L_2, L_3 of $K = \mathbb{Q}(\sqrt{d})$.
3. $L_1 \neq L_2 \neq L_3$.

A. Hoque, *Parameterized families of quadratic fields with class groups of 3-rank at least* 3, Preprint

$N(3,r,x) \longrightarrow$ The # of quadratic fields whose class group has 3-rank at least r and absolute discriminant $\leq x$.

Theorem (–)

$N(3,3,x) \gg x^{\frac{1}{3}}$.

Outline of the proof:

1. Utilization of Hilbert class field theory.
2. Construction of 3 cyclic, cubic, unramified extensions L_1, L_2, L_3 of $K = \mathbb{Q}(\sqrt{d})$.
3. $L_1 \neq L_2 \neq L_3$.
4. Counting such fields.

A. Hoque, *Parameterized families of quadratic fields with class groups of 3-rank at least* 3, Preprint

$N(3, r, x) \longrightarrow$ The # of quadratic fields whose class group has 3-rank at least r and absolute discriminant $\leq x$.

Theorem (−)

$N(3, 3, x) \gg x^{\frac{1}{3}}$.

Outline of the proof:

① Utilization of Hilbert class field theory.

② Construction of 3 cyclic, cubic, unramified extensions L_1, L_2, L_3 of $K = \mathbb{Q}(\sqrt{d})$.

③ $L_1 \neq L_2 \neq L_3$.

④ Counting such fields.

For suitable integers m, n, b and c, define $f(m, n, b, c) = 2nc(4m^3 - 216b^2nc)$. Assume that d is the square-free parts of $f(m, n, b, c)$. Then $rank_3\mathbb{Q}(\sqrt{d}) \geq 3$. $\Rightarrow$ ② and ③.

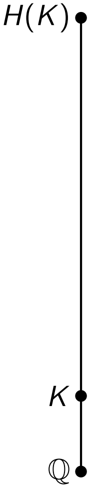
A. Hoque, *Parameterized families of quadratic fields with class groups of 3-rank at least* 3, Preprint

HCF

$K \rightarrow$ a number field

$$
\begin{array}{c}
K \\
| \\
\mathbb{Q}
\end{array}
$$

HCF



$K \rightarrow$ a number field

$H(K) \rightarrow$ Hilbert class field of K

HCF

$$\begin{array}{c} H(K) \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

$K \rightarrow$ a number field

$H(K) \rightarrow$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

HCF

$$\begin{tikzcd}
H(K) \arrow[d, dash] \\
L \arrow[d, dash] \\
K \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

$K \rightarrow$ a number field

$H(K) \rightarrow$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

$L \rightarrow$ unramified abelian extension

HCF

$$
\begin{array}{c}
H(K) \\
| \\
L \\
| \\
K \\
| \\
\mathbb{Q}
\end{array}
$$

$K \to$ a number field

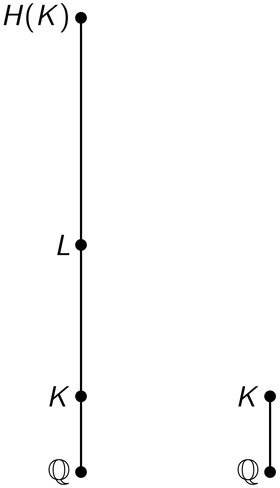
$H(K) \to$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

$L \to$ unramified abelian extension

$|L : K| \mid \mathrm{Ord}(Gal(H(K)/K)) = h_K$

HCF



$K \rightarrow$ a number field

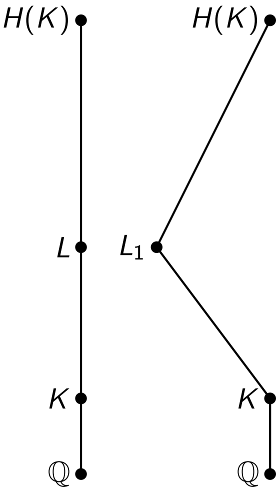
$H(K) \rightarrow$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

$L \rightarrow$ unramified abelian extension

$|L : K| \mid \text{Ord}(Gal(H(K)/K)) = h_K$

HCF



$K \rightarrow$ a number field

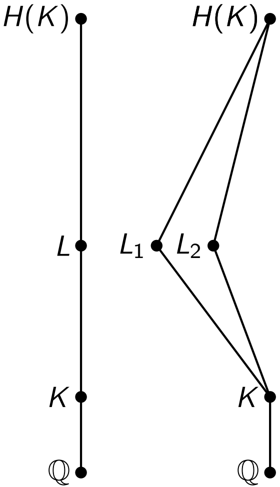
$H(K) \rightarrow$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

$L \rightarrow$ unramified abelian extension

$|L : K| \mid \text{Ord}(Gal(H(K)/K)) = h_K$

HCF



$K \rightarrow$ a number field

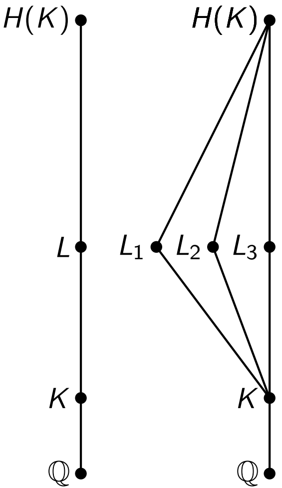
$H(K) \rightarrow$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

$L \rightarrow$ unramified abelian extension

$|L : K| \mid \mathrm{Ord}(Gal(H(K)/K)) = h_K$

HCF



$K \rightarrow$ a number field

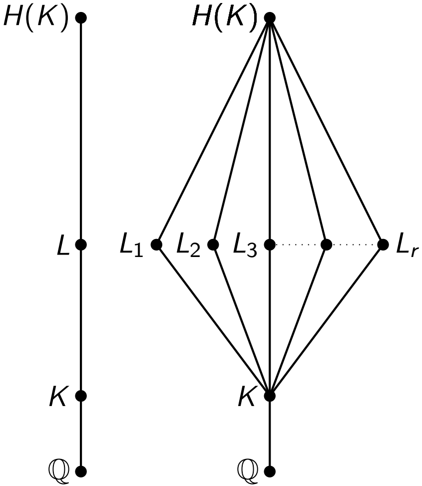
$H(K) \rightarrow$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

$L \rightarrow$ unramified abelian extension

$|L : K| \mid \mathrm{Ord}(Gal(H(K)/K)) = h_K$

HCF



$K \rightarrow$ a number field

$H(K) \rightarrow$ Hilbert class field of K

$Gal(H(K)/K) \cong Cl(K)$

$L \rightarrow$ unramified abelian extension

$|L : K| \mid \mathrm{Ord}(Gal(H(K)/K)) = h_K$

Construction of unramified extensions

Theorem (Kishi-Miyanke)

For any integer u and v, let $g(Z) = Z^3 - uvZ - u^2$. If

(i) *$d = 4uv^3 - 27u^2$ is not a square in $\mathbb{Z}$,*

(ii) $\gcd(u, v) = 1$,

(iii) *$g(Z)$ is irreducible,*

(iv) *one of the following conditions holds:*

- (iv.a) $3 \nmid v$,
- (iv.b) $3 \mid v$, $\quad uv \not\equiv 3 \pmod 9$, $\quad u \equiv v \pm 1 \pmod 9$,
- (iv.c) $3 \mid v$, $\quad uv \equiv 3 \pmod 9$, $\quad u \equiv v \pm 1 \pmod{27}$,

then the normal closure of $\mathbb{Q}(\alpha)$, where α is a root of $g(Z)$, is a cyclic, cubic and unramified extension of $K = \mathbb{Q}(\sqrt{d})$; in particular, the class number of K is divisible by 3.

Y. Kishi and K. Miyake, *Parametrization of the quadratic fields whose class numbers are divisible by three*, J. NumberTheory **80** (2000), 209–217.

Splitting of primes

Lemma (–)

Let $g(Z) = Z^3 - uvZ - u^2 \in \mathbb{Z}[Z]$ *and* α *a root of* $g(Z)$.

(i) *If* $p \geq 3$ *is a prime such that* $p^{2r} \mid\mid u$ *and* $p \nmid v$, *then* p *splits in* $\mathbb{Q}(\alpha)$ *as* $p = \mathfrak{pqr}$ *or* $\mathfrak{pq}$ *according as* $\left(\frac{w}{p}\right) = 1$ *or* -1, *where* $w = uv/p^{2r}$.

(ii) *If* $p \geq 5$ *is prime and* $\Delta = 4uv^3 - 27u^2$ *such that* $p \nmid v\Delta$, *then* p *decomposes in* $\mathbb{Q}(\alpha)$ *as follows:*

$$(p) = \begin{cases} \mathfrak{pqr} & \textit{when } \left(\frac{\Delta}{p}\right) = 1 \textit{ and } f(x) \pmod{p} \textit{ has a root}, \\ \mathfrak{p} & \textit{when } \left(\frac{\Delta}{p}\right) = 1 \textit{ and } f(x) \pmod{p} \textit{ has no root}, \\ \mathfrak{pq} & \textit{when } \left(\frac{\Delta}{p}\right) = -1. \end{cases}$$

(iii) 3 *is inert in* $\mathbb{Q}(\alpha)$ *if* $uv \equiv 1 \pmod{3}$.

Square-free sieve

Let $F(X,Y) = a_0X^r + a_1X^{r-1}Y + \cdots + a_{r-1}XY^{r-1}a_rY^r \in \mathbb{Z}[X,Y]$. Assume that M, N and T are integers with $T \geq 1$. For any positive real number x, let $R(x)$ denote the number of square-free integers d with $|d| \leq x$ for which there are integers m, n and z satisfying $m \equiv M \pmod{T}$, $n \equiv N \pmod{T}$ and $F(m,n) = dz^2$.

Lemma (Stewart–Top)

Let M, N and T be integers with $T \geq 1$. Let F be defined as above with non-vanishing discriminant and degree $r \geq 3$. Assume that the largest degree of an irreducible factor of F over $\mathbb{Q}$ is at most 6. Then for any large positive real number x, there exists a sufficiently large positive constant c, which depends on T and F, such that $R(x) > cx^{\frac{2}{r}}$.

C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

Completion of the proof

Recall that $f(m,n,b,c) = 2nc(4m^3 - 216b^2nc)$. Then $f(m,n,43,-553n) = 2n(m^2 - 9954mn + 33027372n^2)(4m^3 - 399384m^2n + 3975468336mn^2 - 13190603938848n^3)$.

Completion of the proof

Recall that $f(m,n,b,c) = 2nc(4m^3 - 216b^2nc)$. Then $f(m,n,43,-553n) = 2n(m^2 - 9954mn + 33027372n^2)(4m^3 - 399384m^2n + 3975468336mn^2 - 13190603938848n^3)$.
Finally, we choose $m \equiv 530881 \pmod{713370}$ and $n \equiv 120401 \pmod{713370}$ to complete the proof.

- Construction of small degree number fields with large class groups.

- Construction of small degree number fields with large class groups.
- Large n-rank of quadratic/higher degree number fields.

- Construction of small degree number fields with large class groups.
- Large n-rank of quadratic/higher degree number fields.
- For any integer $n > 1$, Kishi conjectured the following:
  (i) If x and y are both odd positive integers with $\gcd(x, y) = 1$, then the class number of $\mathbb{Q}(\sqrt{x^{2n} + y^{2n}})$ is divisible by n.

- Construction of small degree number fields with large class groups.
- Large n-rank of quadratic/higher degree number fields.
- For any integer $n > 1$, Kishi conjectured the following:
  - (i) If x and y are both odd positive integers with $\gcd(x, y) = 1$, then the class number of $\mathbb{Q}(\sqrt{x^{2n} + y^{2n}})$ is divisible by n.
  - (ii) If x is an odd positive integer and y is any positive integer with $\gcd(x, y) = 1$, then the class number of $\mathbb{Q}(\sqrt{x^{2n} + 4y^{2n}})$ is divisible by n.

- Construction of small degree number fields with large class groups.
- Large n-rank of quadratic/higher degree number fields.
- For any integer $n > 1$, Kishi conjectured the following:
    - (i) If x and y are both odd positive integers with $\gcd(x, y) = 1$, then the class number of $\mathbb{Q}(\sqrt{x^{2n} + y^{2n}})$ is divisible by n.
    - (ii) If x is an odd positive integer and y is any positive integer with $\gcd(x, y) = 1$, then the class number of $\mathbb{Q}(\sqrt{x^{2n} + 4y^{2n}})$ is divisible by n.
- Parameterization of all quadratic fields with class number divisible by a given integer $n > 3$. Further, it would be also interesting to parameterize all higher degree numbers fields with class number divisible by a given integer $n \geq 3$.

- Construction of small degree number fields with large class groups.
- Large n-rank of quadratic/higher degree number fields.
- For any integer $n > 1$, Kishi conjectured the following:
  (i) If x and y are both odd positive integers with $\gcd(x, y) = 1$, then the class number of $\mathbb{Q}(\sqrt{x^{2n} + y^{2n}})$ is divisible by n.
  (ii) If x is an odd positive integer and y is any positive integer with $\gcd(x, y) = 1$, then the class number of $\mathbb{Q}(\sqrt{x^{2n} + 4y^{2n}})$ is divisible by n.
- Parameterization of all quadratic fields with class number divisible by a given integer $n > 3$. Further, it would be also interesting to parameterize all higher degree numbers fields with class number divisible by a given integer $n \geq 3$.
- The Diophantine equations $cx^2 + d^m = \mu y^n, x, y \geq 1, m, n \geq 1$, $\mu \in \{1, 2, 4\}$, where c and d are fixed positive integers.


Thank
you !!!