Divisibility of class numbers of imaginary quadratic fields with discriminants of only three prime factors

Kostadinka Lapkova

Central European University
Budapest, Hungary

August 22, 2011

- $\mathbb{Q}(\sqrt{d})$, $d = -pqr < 0$
- Class group $Cl(d)$ = free group of fractional ideals/principal fractional ideals
- Class number $h(d)$ = the finite order of the class group

- $\mathbb{Q}(\sqrt{d})$, $d = -pqr < 0$
- Class group $Cl(d)$ = free group of fractional ideals/principal fractional ideals
- Class number $h(d)$ = the finite order of the class group

Theorem (Belabas,Fouvry, 1999)

There exists a positive density of primes p such that $h(p)$ is not divisible by 3.

- $\mathbb{Q}(\sqrt{d})$, $d = -pqr < 0$
- Class group $Cl(d)$ = free group of fractional ideals/principal fractional ideals
- Class number $h(d)$ = the finite order of the class group

Theorem (Belabas,Fouvry, 1999)

There exists a positive density of primes p such that $h(p)$ is not divisible by 3.

- Analogous result for negative discriminants that are pseudo primes.

- $\mathbb{Q}(\sqrt{d}), d = -pqr < 0$
- Class group $Cl(d)$ = free group of fractional ideals/principal fractional ideals
- Class number $h(d)$ = the finite order of the class group

Theorem (Belabas,Fouvry, 1999)

There exists a positive density of primes p such that $h(p)$ is not divisible by 3.

- Analogous result for negative discriminants that are pseudo primes.
- Divisibility of class numbers of quadratic fields whose discriminants have small number of prime divisors.

Theorem (Byeon,Lee,2008)

Let $\ell \geq 2$ be an integer. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of order 2ℓ and whose discriminant has only two prime divisors.

Theorem (Byeon,Lee,2008)

Let $\ell \geq 2$ be an integer. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of order 2ℓ and whose discriminant has only two prime divisors.

Theorem (K.L.,2011)

Let $\ell \geq 2$ and $k \geq 3$ be integers. There are infinitely many imaginary quadratic fields whose ideal class group has an element of order 2ℓ and whose discriminant has exactly k different prime divisors.

Motivation

Extending results of András Biró on Yokoi's conjecture ($d = n^2 + 4$):

Theorem (K.L.,2010)

If $d = (an)^2 + 4a$ is square-free for a and n – odd positive integers such that 43.181.353 divides n, then $h(d) > 1$.

Motivation

Extending results of András Biró on Yokoi's conjecture ($d = n^2 + 4$):

Theorem (K.L.,2010)

If $d = (an)^2 + 4a$ *is square-free for* a *and* n *– odd positive integers such that* $43.181.353$ *divides* n*, then* $h(d) > 1$*.*

The parameter 43.181.353 :

$$h(-43.181.353) = 2^9.3\,.$$

Motivation

Main identity

$$qh(-q)h(-qd) = \frac{n}{6}\left(a + \left(\frac{a}{q}\right)\right)\prod_{p|q}(p^2 - 1),$$

where $q \equiv 3 \pmod 4$ is squarefree, $q \mid n$, $(q, a) = 1$ and $h(d) = h((an)^2 + 4a) = 1$.

Motivation

Main identity

$$q\,h(-q)\,h(-qd) = \frac{n}{6}\left(a + \left(\frac{a}{q}\right)\right)\prod_{p\mid q}(p^2-1)\,,$$

where $q \equiv 3 \pmod 4$ is squarefree, $q \mid n$, $(q,a) = 1$ and $h(d) = h((an)^2 + 4a) = 1$.

Corollary

There exists an infinite family of parameters q, where q has exactly three distinct prime factors, with the following property. If $d = (an)^2 + 4a$ is square-free for a and n – odd positive integers, and q divides n, then $h(d) > 1$.

Sketch of the proof

The idea comes from treatment of an additive problem in

A. Balog and K. Ono
Ellements of class groups and Shafarevich-Tate groups of elliptic curves
Duke Math. J. **2003**, no.1, 35–63

Sketch of the proof

The idea comes from treatment of an additive problem in

A. Balog and K. Ono
Ellements of class groups and Shafarevich-Tate groups of elliptic curves
Duke Math. J. **2003**, no.1, 35–63

They need "Siegel-Walfisz sets".
(Number field generalization of the Siegel-Walfisz theorem for uniform distribution of primes in residue classes.)

Definition (Siegel-Walfisz set for Δ)

Let $\mathcal{P}$ be an infinite set of primes with density $0 < \gamma < 1$ and for $(q, b) = 1$ let $\mathcal{P}(x, q, b)$ be the number of primes $p \in \mathcal{P}$ with $p \leq x$ and $p \equiv b \pmod q$. Then $\mathcal{P}$ is a Siegel-Walfisz set for Δ if for any fixed integer $C > 0$

$$\mathcal{P}(x, q, b) = \frac{\gamma}{\varphi(q)}\pi(x) + \mathcal{O}(\frac{x}{\log^C x})$$

uniformly for all $(q, \Delta) = 1$ and all b coprime to q.

Circle method

Find asymptotic formula for the solutions of

$$4m^\ell = p_1 + p_2 p_3$$

for $\ell \geq 2$, m–odd positive integer and $p_1 \in \mathcal{P}_1$, $p_2, p_3 \in \mathcal{P}_2$ for the Siegel-Walfisz sets for Δ:

- Every $p \in \mathcal{P}_1$ is $\equiv -5 \pmod{\Delta}$

Circle method

Find asymptotic formula for the solutions of

$$4m^{\ell} = p_1 + p_2 p_3$$

for $\ell \geq 2$, m–odd positive integer and $p_1 \in \mathcal{P}_1$, $p_2, p_3 \in \mathcal{P}_2$ for the Siegel-Walfisz sets for Δ:

- Every $p \in \mathcal{P}_1$ is $\equiv -5 \pmod{\Delta}$
- Every $r \in \mathcal{P}_2$ is $\equiv 3 \pmod{\Delta}$

Circle method

Find asymptotic formula for the solutions of

$$4m^{\ell} = p_1 + p_2 p_3$$

for $\ell \geq 2$, m–odd positive integer and $p_1 \in \mathcal{P}_1$, $p_2, p_3 \in \mathcal{P}_2$ for the Siegel-Walfisz sets for Δ:

- Every $p \in \mathcal{P}_1$ is $\equiv -5 \pmod{\Delta}$
- Every $r \in \mathcal{P}_2$ is $\equiv 3 \pmod{\Delta}$
- $p_1 \leq \sqrt{X}$; $X^{1/8} < p_2 \leq X^{1/4}, X^{3/8} < p_2 p_3 \leq \sqrt{X}$

Circle method

Find asymptotic formula for the solutions of

$$4m^{\ell} = p_1 + p_2 p_3$$

for $\ell \geq 2$, m–odd positive integer and $p_1 \in \mathcal{P}_1$, $p_2, p_3 \in \mathcal{P}_2$ for the Siegel-Walfisz sets for Δ:

- Every $p \in \mathcal{P}_1$ is $\equiv -5 \pmod{\Delta}$
- Every $r \in \mathcal{P}_2$ is $\equiv 3 \pmod{\Delta}$
- $p_1 \leq \sqrt{X}$; $X^{1/8} < p_2 \leq X^{1/4}, X^{3/8} < p_2 p_3 \leq \sqrt{X}$

Theorem

Let Δ, ℓ be positive integers for which $16\ell^2 \mid \Delta$ and $(15, \Delta) = 1$. If $R_d(X)$ denotes the number of positive integers $d \leq X$ of the form

$$d = p_1 p_2 p_3 = 4m^{2\ell} - n^2 ,$$

then

$$R_d(X) \gg \frac{X^{1/2+1/(2\ell)}}{\log^2 X} .$$

Apply a statement similar to:

Soundararajan,2000

Let $\ell \geq 2$ be an integer and $d \geq 63$ be a square-free integer for which

$$dt^2 = m^{2\ell} - n^2,$$

where m and n are integers with $(m, 2n) = 1$ and $m^\ell \leq d$. Then $Cl(-d)$ contains an element of order 2ℓ.

Apply a statement similar to:

Soundararajan,2000

Let $\ell \geq 2$ be an integer and $d \geq 63$ be a square-free integer for which

$$dt^2 = m^{2\ell} - n^2,$$

where m and n are integers with $(m, 2n) = 1$ and $m^\ell \leq d$. Then $Cl(-d)$ contains an element of order 2ℓ.

Corollary

Let $\ell \geq 2$ be an integer not divisible by 3 or 5. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of order 2ℓ and whose discriminant has exactly 3 different prime divisors.

Apply a statement similar to:

Soundararajan,2000

Let $\ell \geq 2$ be an integer and $d \geq 63$ be a square-free integer for which

$$dt^2 = m^{2\ell} - n^2,$$

where m and n are integers with $(m, 2n) = 1$ and $m^\ell \leq d$. Then $Cl(-d)$ contains an element of order 2ℓ.

Corollary

Let $\ell \geq 2$ be an integer not divisible by 3 or 5. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of order 2ℓ and whose discriminant has exactly 3 different prime divisors.

- $2m^\ell = p_1 + p_2 \dots p_k$

Apply a statement similar to:

Soundararajan,2000

Let $\ell \geq 2$ be an integer and $d \geq 63$ be a square-free integer for which

$$dt^2 = m^{2\ell} - n^2,$$

where m and n are integers with $(m, 2n) = 1$ and $m^\ell \leq d$. Then $Cl(-d)$ contains an element of order 2ℓ.

Corollary

Let $\ell \geq 2$ be an integer not divisible by 3 or 5. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of order 2ℓ and whose discriminant has exactly 3 different prime divisors.

- $2m^\ell = p_1 + p_2 \ldots p_k$
- Different Siegel-Walfisz sets $\mathcal{P}_1, \mathcal{P}_2$ for different k, ℓ.

Thank you for your attention!