On Class Number of Number Fields

Debopam Chakraborty

Visiting Scientist, ISI Delhi

December 17, 2016

Class Number

Class Number

Loosely speaking, class number of a number field measures the extent to which unique factorization fails in the ring of integers of an algebraic number field.

Class Number

Loosely speaking, class number of a number field measures the extent to which unique factorization fails in the ring of integers of an algebraic number field.

In 1801 Gauss proposed three conjectures regarding class number of quadratic number fields in his book "Disquisitiones Arithmeticae".

Class Number

Loosely speaking, class number of a number field measures the extent to which unique factorization fails in the ring of integers of an algebraic number field.

In 1801 Gauss proposed three conjectures regarding class number of quadratic number fields in his book "Disquisitiones Arithmeticae".

The conjecture about the existence of infinitely many real quadratic fields of class number one is yet to be answered.

Relative Class Number

Relative Class Number

In his 1856 paper, Dirichlet defined relative class number of a number field and asked about the existence of infinitely many real quadratic fields with relative class number as one for some conductor f.

Relative Class Number

In his 1856 paper, Dirichlet defined relative class number of a number field and asked about the existence of infinitely many real quadratic fields with relative class number as one for some conductor f.

Definition

The relative class number $H_d(f)$ of a real quadratic field $K = \mathbb{Q}(\sqrt{m})$ of discriminant d is defined to be the ratio of class numbers of $\mathcal{O}_f$ and $\mathcal{O}_K$, where $\mathcal{O}_K$ denotes the ring of integers of K and $\mathcal{O}_f$ is the order of conductor f given by $\mathbb{Z} + f\mathcal{O}_K$.

Dirichlet's Formula

Dirichlet's Formula

The following formula was obtained by Dirichlet himself;

Dirichlet's Formula

The following formula was obtained by Dirichlet himself;

Result

Let $\theta(f)$ be the smallest positive integer such that $\xi_m^{\theta(f)} \in \mathcal{O}_f$ and $\psi(f) = f \prod_{q|f} \left(1 - \left(\frac{d}{q}\right)\frac{1}{q}\right)$, where $\left(\frac{d}{q}\right)$ denotes the "Kronecker residue symbol" of d modulo a prime q. Then the relative class number for conductor f is given by

$$H_d(f) = \frac{\psi(f)}{\theta(f)}. \tag{1}$$

Fundamental Unit and Relative Class Number

Fundamental Unit and Relative Class Number

Let $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ be the fundamental unit of $\mathbb{Q}(\sqrt{m})$.

Fundamental Unit and Relative Class Number

Let $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ be the fundamental unit of $\mathbb{Q}(\sqrt{m})$.

If β_0 is divisible by a prime q, then $\theta(q) = 1$.

Fundamental Unit and Relative Class Number

Let $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ be the fundamental unit of $\mathbb{Q}(\sqrt{m})$.

If β_0 is divisible by a prime q, then $\theta(q) = 1$.

When the square-free integer m does not divide β_0, there exists a prime q dividing m such that β_0 is not divisible by q. Using $f = q$ in Dirichlet's formula, $\psi(q) = q$ and $\theta(q) \neq 1$ is a factor of $\psi(q)$. Hence $\theta(q) = \psi(q) = q$, and $H_d(q) = 1$.

The following results will lead us to an affirmative answer of the original question. The norm of ξ_m is assumed to be -1.

The following results will lead us to an affirmative answer of the original question. The norm of ξ_m is assumed to be -1.

Theorem

(i) If $p \equiv 1$ mod 4 is an odd prime not dividing m, then the relative class number for conductor p is not 1.
(ii) If $p \equiv 3$ mod 4 is an odd prime not dividing m, then the relative class number for conductor p is odd.

Sketch of the proof

Sketch of the proof

Suppose $p \equiv 1 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$.

Sketch of the proof

Suppose $p \equiv 1 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$.

$\xi_m^{\frac{p-1}{2}} = \alpha_1 + \beta_1\sqrt{m}$ has norm 1 as $\frac{p-1}{2}$ is even, so its inverse is $\xi_m^{-\frac{p-1}{2}} = \alpha_1 - \beta_1\sqrt{m}$.

Sketch of the proof

Suppose $p \equiv 1 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$.

$\xi_m^{\frac{p-1}{2}} = \alpha_1 + \beta_1\sqrt{m}$ has norm 1 as $\frac{p-1}{2}$ is even, so its inverse is $\xi_m^{-\frac{p-1}{2}} = \alpha_1 - \beta_1\sqrt{m}$.

It follows

$$2\beta_1\sqrt{m} = \xi_m^{\frac{p-1}{2}} - \xi_m^{-\frac{p-1}{2}} = \xi_m^{-\frac{p-1}{2}}(\xi_m^{p-1} - 1) \in p\mathcal{O}_K.$$

Sketch of the proof

Suppose $p \equiv 1 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$.
$\xi_m^{\frac{p-1}{2}} = \alpha_1 + \beta_1\sqrt{m}$ has norm 1 as $\frac{p-1}{2}$ is even, so its inverse is $\xi_m^{-\frac{p-1}{2}} = \alpha_1 - \beta_1\sqrt{m}$.
It follows

$$2\beta_1\sqrt{m} = \xi_m^{\frac{p-1}{2}} - \xi_m^{-\frac{p-1}{2}} = \xi_m^{-\frac{p-1}{2}}(\xi_m^{p-1} - 1) \in p\mathcal{O}_K.$$

From $2\beta_1\sqrt{m} \in p\mathcal{O}_K$ it follows that $2m\beta_1 = \sqrt{m} \cdot 2\beta_1\sqrt{m} \in p\mathcal{O}_K$.
Hence, $2m\beta_1 \in p\mathbb{Z}$, so $p \mid \beta_1$, since $2m$ is invertible modulo p.

Proposition

When $\mathbb{Q}(\sqrt{m})$ *has fundamental unit of norm* -1 *the relative class number for conductor* 3 *must be* 1.

Proposition

When $\mathbb{Q}(\sqrt{m})$ *has fundamental unit of norm* -1 *the relative class number for conductor* 3 *must be* 1.

Corollary

There are infinitely many real quadratic fields of relative class number 1 *for the conductor* 3.

Fundamental Unit of a Cubic Field and its Class Number

Fundamental Unit of a Cubic Field and its Class Number

By Dirichlet's Unit Theorem, the group of units in the ring of integers of a pure cubic or real quadratic field is of rank one, and the smallest unit > 1 is referred to as the fundamental unit.

Fundamental Unit of a Cubic Field and its Class Number

By Dirichlet's Unit Theorem, the group of units in the ring of integers of a pure cubic or real quadratic field is of rank one, and the smallest unit > 1 is referred to as the fundamental unit.

We will now describe our results relating the class number of number field of degree 2 to congruence relations satisfied by the fundamental unit of cubic and quadratic field.

The following proposition gives a simple but effective representation of the fundamental unit of a cubic field.

The following proposition gives a simple but effective representation of the fundamental unit of a cubic field.

Proposition

Let $q \neq m$ be a prime that ramifies in $K = \mathbb{Q}(\sqrt[3]{m})$. If $3 \nmid h_m$ then either ξ_m or ξ_m^2 can be written as $\frac{\alpha^3}{q}$ for some $\alpha \in K$.

The following proposition gives a simple but effective representation of the fundamental unit of a cubic field.

Proposition

Let $q \neq m$ be a prime that ramifies in $K = \mathbb{Q}(\sqrt[3]{m})$. If $3 \nmid h_m$ then either ξ_m or ξ_m^2 can be written as $\frac{\alpha^3}{q}$ for some $\alpha \in K$.

The proof follows from the fact that a principal ideal can only be a cube of another principal ideal.

Similar argument for quadratic fields yields in the following proposition;

Similar argument for quadratic fields yields in the following proposition;

Proposition

Let $\xi_d = x + y\sqrt{d} > 1$ *be the fundamental unit of* $\mathbb{Q}(\sqrt{d})$.
1. *If* $d = p$ *or* $2p$ *where* p *is a prime congruent to* 3 *mod* 4, *then* $2\xi_d = {u_d}^2$ *for some* $u_d \in \mathcal{O}_K$.
2. *If* $d = p_1 p_2$, *where* p_1 *and* p_2 *are two distinct primes congruent to* $\equiv 3$ *mod* 4, *then* $p_1\xi_d = {u_d}^2$ *for some* $u_d \in \mathcal{O}_K$.

Similar argument for quadratic fields yields in the following proposition;

Proposition

Let $\xi_d = x + y\sqrt{d} > 1$ *be the fundamental unit of* $\mathbb{Q}(\sqrt{d})$.
1. *If* $d = p$ *or* $2p$ *where* p *is a prime congruent to* 3 *mod* 4, *then* $2\xi_d = {u_d}^2$ *for some* $u_d \in \mathcal{O}_K$.
2. *If* $d = p_1 p_2$, *where* p_1 *and* p_2 *are two distinct primes congruent to* $\equiv 3$ *mod* 4, *then* $p_1\xi_d = {u_d}^2$ *for some* $u_d \in \mathcal{O}_K$.

The following result is classically known, but we can also deduce it from the above propsition.

Similar argument for quadratic fields yields in the following proposition;

Proposition

Let $\xi_d = x + y\sqrt{d} > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{d})$.
1. *If $d = p$ or $2p$ where p is a prime congruent to 3 mod 4, then $2\xi_d = {u_d}^2$ for some $u_d \in \mathcal{O}_K$.*
2. *If $d = p_1 p_2$, where p_1 and p_2 are two distinct primes congruent to $\equiv 3$ mod 4, then $p_1\xi_d = {u_d}^2$ for some $u_d \in \mathcal{O}_K$.*

The following result is classically known, but we can also deduce it from the above propsition.

Corollary

If $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field with discriminant having at least three prime factors then the class number of K is even.

Sketch of the proof

Sketch of the proof

Suppose $K = \mathbb{Q}(\sqrt{d})$ is the real quadratic field under question. The given condition implies that at least 3 distinct rational primes p, q and r ramify in K.

Sketch of the proof

Suppose $K = \mathbb{Q}(\sqrt{d})$ is the real quadratic field under question.
The given condition implies that at least 3 distinct rational primes p, q and r ramify in K.
Hence both p and pq ramify in K, but none of them is a square in K.

Sketch of the proof

Suppose $K = \mathbb{Q}(\sqrt{d})$ is the real quadratic field under question.
The given condition implies that at least 3 distinct rational primes p, q and r ramify in K.
Hence both p and pq ramify in K, but none of them is a square in K.
If ξ_d denotes the fundamental unit of K and the class number of K is not divisible by 2, then we can write $\xi_d = \frac{\alpha^2}{p} = \frac{\beta^2}{pq}$ by previous proposition. Then $\sqrt{q} \in K$, a contradiction.

Let $\xi_m = x + yt + zt^2$, where $t = \sqrt[3]{m} \in \mathbb{R}$, be the fundamental unit of K.

Let $\xi_m = x + yt + zt^2$, where $t = \sqrt[3]{m} \in \mathbb{R}$, be the fundamental unit of K.

Theorem

Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field with a power integral basis (i.e., m square-free natural number and $m \not\equiv \pm 1 \bmod 9$). If 3 does not divide h_m, then m must be either p or $3p$ for some prime p.

Let $\xi_m = x + yt + zt^2$, where $t = \sqrt[3]{m} \in \mathbb{R}$, be the fundamental unit of K.

Theorem

Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field with a power integral basis (i.e., m square-free natural number and $m \not\equiv \pm 1 \bmod 9$). If 3 does not divide h_m, then m must be either p or $3p$ for some prime p.

Corollary

For any composite number $m \equiv 2, 4, 5$ or $7 \pmod 9$, the class number of $\mathbb{Q}(\sqrt[3]{m})$ is divisible by 3.

Let $\xi_m = x + yt + zt^2$, where $t = \sqrt[3]{m} \in \mathbb{R}$, be the fundamental unit of K.

Theorem

Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field with a power integral basis (i.e., m square-free natural number and $m \not\equiv \pm 1 \bmod 9$). If 3 does not divide h_m, then m must be either p or $3p$ for some prime p.

Corollary

For any composite number $m \equiv 2, 4, 5$ or $7 \pmod 9$, the class number of $\mathbb{Q}(\sqrt[3]{m})$ is divisible by 3.

Table : $m \neq p, 3p$, $m \not\equiv \pm 1 \bmod 9$ & m square-free

m	14	22	30	34	38	42	58	60	65
h_m	3	3	3	3	3	3	3	3	18
m	66	74	77	78	85	86	92	94	95
h_m	6	3	3	9	3	3	3	3	3

Theorem

Suppose $m = 3p$ *where* p *is any prime other than* 3. *Let* $\xi_m = x + yt + zt^2$ *be the fundamental unit of the field* $K = \mathbb{Q}(t)$ $(t = \sqrt[3]{m})$. *If* 3 *does not divide* h_m *then* $x^2 \equiv 1 \ mod\ 27p$ *and* $y \equiv z \equiv 0 \ mod\ 3$.

Theorem

Suppose $m = 3p$ where p is any prime other than 3. Let $\xi_m = x + yt + zt^2$ be the fundamental unit of the field $K = \mathbb{Q}(t)$ $(t = \sqrt[3]{m})$. If 3 does not divide h_m then $x^2 \equiv 1$ mod $27p$ and $y \equiv z \equiv 0$ mod 3.

Table : $m = 3p$, where $p \neq 3$ is a prime

m	x^2 mod 27	x^2 mod p	y mod 3	z mod 3	h_m
21	$1705^2 \not\equiv 1$	$1705^2 \not\equiv 1$	$618 \equiv 0$	$224 \equiv 0$	3
39	$529^2 \not\equiv 1$	$529^2 \not\equiv 1$	$156 \equiv 0$	$46 \not\equiv 0$	6
57	$1460968^2 \not\equiv 1$	$1460968^2 \equiv 1$	$379620 \equiv 0$	$98641 \not\equiv 0$	6

Elliptic curves and unramified quadratic extensions of bi-quadratic fields

Elliptic curves and unramified quadratic extensions of bi-quadratic fields

It is well known from class field theory that the ideal class group is also the Galois group of the maximal unramified abelian extension of K.

Elliptic curves and unramified quadratic extensions of bi-quadratic fields

It is well known from class field theory that the ideal class group is also the Galois group of the maximal unramified abelian extension of K.

There are many results regarding the relations between class numbers of number fields and points on elliptic curves.

Elliptic curves and unramified quadratic extensions of bi-quadratic fields

It is well known from class field theory that the ideal class group is also the Galois group of the maximal unramified abelian extension of K.

There are many results regarding the relations between class numbers of number fields and points on elliptic curves.

R. Soleng gave a construction of families of quadratic number fields from an elliptic curve having ideal class group isomorphic to the torsion group of the curve.

Elliptic curves and unramified quadratic extensions of bi-quadratic fields

It is well known from class field theory that the ideal class group is also the Galois group of the maximal unramified abelian extension of K.

There are many results regarding the relations between class numbers of number fields and points on elliptic curves.

R. Soleng gave a construction of families of quadratic number fields from an elliptic curve having ideal class group isomorphic to the torsion group of the curve.

A. Sato constructed quadratic number fields with class number divisible by 5 from points on elliptic curves.

F. Lemmermeyer showed a method for constructing unramified quadratic extension of cubic fields using points on suitable elliptic curves, which implied that the parity of the class number is even.

F. Lemmermeyer showed a method for constructing unramified quadratic extension of cubic fields using points on suitable elliptic curves, which implied that the parity of the class number is even.

The following theorem took the inspiration from Lemmermeyer's method and give a construction for infinitely many bi-quadratic number fields with even class number from the points of an elliptic curve of rank at least one.

Theorem

Let $m \neq 0, 1$ be a square-free integer which is divisible by 3 if it is positive. Let $P_0 = \left(\frac{r_0}{t_0^2}, \frac{s_0}{t_0^3}\right)$ be any non-torsion point of the elliptic curve $y^2 = x^3 + m$ such that r_0 is odd and non-square. Let $\left(\frac{r_i}{t_i^2}, \frac{s_i}{t_i^3}\right)$ $= 2^i P_0$ for each natural number i. Then the bi-quadratic field K_i $= \mathbb{Q}(\sqrt{r_i}, \sqrt{m})$ has an everywhere unramified quadratic extension $K_i(\sqrt{\beta_i})$, where β_i is either $\pm(s_i + t_i^3\sqrt{m})$ or $3(s_i + t_i^3\sqrt{m})$.

Sketch of the proof

Sketch of the proof

The following results lead to the proof of the theorem.

Sketch of the proof

The following results lead to the proof of the theorem.

Lemma

Consider the duplication formula for the point $P = (\frac{r}{t^2}, \frac{s}{t^3})$ *on* $y^2 = x^3 + m$*:*

$$\left(\frac{r(2P)}{t(2P)^2}, \frac{s(2P)}{t(2P)^3}\right) = 2P = \left(\frac{r(9r^3 - 8s^2)}{(2st)^2}, \frac{27r^6 - 36r^3s^2 + 8s^4}{(2st)^3}\right) \tag{2}$$

Suppose m *is square-free and* r *is odd. If* $3 \nmid s$*, the fractions on the right hand side of the above equation are already in their reduced form. When* $s = 3s'$ *the fractions on the right hand side above reduces to*

$$\left(\frac{r(2P)}{t(2P)^2}, \frac{s(2P)}{t(2P)^3}\right) = 2P = \left(\frac{r(r^3 - 8s'^2)}{(2s't)^2}, \frac{r^6 - 12r^3s'^2 + 24s'^4}{(2s't)^3}\right). \tag{3}$$

Lemma

Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ be a non-torsion point of the elliptic curve E_m with t even. Then α and its conjugate $\bar{\alpha}$ over $\mathbb{Q}(\sqrt{r})$ generate coprime ideals in the ring $\mathcal{O}_K$ of integers in K. Moreover, there exists an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $\langle\alpha\rangle := \alpha\mathcal{O}_K = \mathfrak{a}^2$.

Lemma

Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ be a non-torsion point of the elliptic curve E_m with t even. Then α and its conjugate $\bar{\alpha}$ over $\mathbb{Q}(\sqrt{r})$ generate coprime ideals in the ring $\mathcal{O}_K$ of integers in K. Moreover, there exists an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $\langle\alpha\rangle := \alpha\mathcal{O}_K = \mathfrak{a}^2$.

Lemma

The extension $K(\sqrt{\beta})$ over $K = \mathbb{Q}(\sqrt{r}, \sqrt{m})$ is quadratic and unramified at all finite primes.

Lemma

Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ be a non-torsion point of the elliptic curve E_m with t even. Then α and its conjugate $\bar{\alpha}$ over $\mathbb{Q}(\sqrt{r})$ generate coprime ideals in the ring $\mathcal{O}_K$ of integers in K. Moreover, there exists an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $\langle\alpha\rangle := \alpha\mathcal{O}_K = \mathfrak{a}^2$.

Lemma

The extension $K(\sqrt{\beta})$ over $K = \mathbb{Q}(\sqrt{r}, \sqrt{m})$ is quadratic and unramified at all finite primes.

Using all the above results the theorem follows. In fact, an infinite family of such bi-quadratic fields of even class number can be constructed by using the same method.

References

[1] D. Chakraborty and A. Saikia. *Congruence relations for the fundamental unit of a pure cubic field and its class number*. Journal of Number Theory, 166: 76 – 84, 2016.

[2] D. Chakraborty and A. Saikia. *Another look at real quadratic fields of relative class number* 1. Acta Arithmetica, 163: 371 – 378, 2014.

[3] D. Chakraborty and A. Saikia. *An explicit construction for unramified quadratic extensions of bi-quadratic fields*. Acta Arithmetica, Accepted, 2016.

[4] H. Cohn. *A numerical study of the relative class numbers of the real quadratic integral domains*. Math. Comp, 16: 127 – 140, 1962.

[5] A. Furness and E. A. Parker. *On Dirichlet's conjecture on relative class number one*. Journal of Number Theory, 7: 1398 – 1403, 2012.

[6] F. Gerth. *Cubic fields whose class number are not divisible by* 3. Illinois. J. Math., 20: 486 – 493, 1976.

[7] F. Lemmermeyer. *Why the class number of* $\mathbb{Q}(\sqrt[3]{11})$ *is even?* Math. Bohem., 138: 149 – 163, 2013.

[8] A. Sato. *On the class numbers of certain number fields obtained from points on elliptic curves III*. Osaka. J. Math., 48: 809 – 826, 2011.

[9] R. Soleng. *Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields*. Journal of Number Theory, 46: 214 – 229, 1994.

[10] Z. Zhang and Q. Yue. *Fundamental unit of real quadratic fields of odd class number*. Journal of Number Theory, 137: 122129, 2014.