Indian J Pure Appl Math (2026) 57:338–343
https://doi.org/10.1007/s13226-024-00544-0

ORIGINAL RESEARCH

A note on the class number of certain real cyclotomic fields

Om Prakash

Received: 1 January 2023 / Accepted: 15 January 2024 / Published online: 25 January 2024

Abstract We construct an infinite family of real cyclotomic fields with non-trivial class group. This result generalizes some results of [6] in the sense that our family includes theirs.

Keywords Diophantine equation · Continued fraction · Class number · Quadratic field · Real cyclotomic field

Mathematics Subject Classification Primary: 11D09 · 11R29; Secondary: 11R11 · 11R18

1 Introduction & Set-up

The class number of cyclotomic fields have been studied since the time mathematicians established linkage between Fermat's last theorem and the unique factorization properties of cyclotomic integers more than a century ago. Throughout this article the class number of $\mathbb{Q}(\zeta_n)$, $\mathbb{Q}(\zeta_n)^+(:= \mathbb{Q}(\zeta_n + \zeta_n{}^{-1}))$ and $\mathbb{Q}(\sqrt{d})$ will be denoted by $\mathfrak{h}(n)$, $H(n)$ and $h(d)$ respectively. The class number $\mathfrak{h}(n)$ of cyclotomic field $\mathbb{Q}(\zeta_n)$ can be written as the product

$$\mathfrak{h}(n) = H(n)\mathfrak{h}(n)^-.$$

The class number of real cyclotomic field $\mathbb{Q}(\zeta_n)^+$ (also known as the 'plus part') remains one of the most enigmatic object to study.

The 'minus part' which we denote by $\mathfrak{h}(n)^-$, it is also known as the relative class number, is defined by the quotient

$$\mathfrak{h}(n)^- = \frac{\mathfrak{h}(n)}{H(n)}.$$

This is a tautology up to this point, but it is not tautological to note that $\mathfrak{h}(n)^-$ can be calculated quite explicitly by using the class number formula. On applying the class number formula to $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_n)^+$ and then taking the quotient, leaves us with the expression,

$$\mathfrak{h}(n)^- = \mathcal{Q}n \prod_{\chi} \left(\frac{-1}{2} B_{1,\chi} \right),$$

Communicated by Rahul Roy.

O. Prakash (✉)
Kerala School of Mathematics, Kozhikode, Kerala 673571, India
E-mail: omprakash@ksom.res.in

where the product runs over odd Dirichlet character χ; $B_{1,\chi}$ denotes the generalised Bernoulli numbers and

$$Q = \begin{cases} 1 & \text{if } n \text{ is a power of prime,} \\ 2 & \text{otherwise.} \end{cases}$$

On the other hand the 'plus part' is still a mystery. Their Minkowski bounds are too large to be effective for the fields with large n, and their discriminant are also far to large for Odlyzko's discriminant bound to treat their class number.

Ankeny et al. [8] showed that, if $p = (2nq)^2 + 1$ is a prime where q is also a prime and $n > 1$ is an integer then $h_p^+ > 1$. Lang [9] has also proved the same result for $p = \{(2n+1)q\}^2 + 4$ where q is a prime and $n \geq 1$ is an integer. In 1987, Osada [3] generalised the results of [8] and [9]. Some more interesting results along these lines can be found in [2] and [5].

In a recent work, Mishra, Schoof and Washington [7] showed that, for a given finite abelian group G there exist infinitely many real cyclotomic fields with class group G. On the other hand Chakraborty and Hoque [6] has given explicit families of real cyclotomic fields having class number strictly bigger than 1. More precisely they proved the following:

Theorem 1.1 (K.Chakraborty and A. Hoque)

1. *Let* $p \equiv 1 \pmod 4$ *and let* $d = (2np)^2 - 1$ *with* $n \geq 1$ *being an integer. Then* $H(4d) > 1$.
2. *Let* $p \equiv \pm 1 \pmod 4$ *be a prime and let* $d = (2np)^2 + 3$ *with n being a positive integer and a multiple of* 3. *Then* $H(4d) > 1$.
3. *Let* $p \equiv \pm 1 \pmod 8$ *be a prime and let* $d = ((2n+1)p)^2 + 2$ *with n a positive integer. Then* $H(4d) > 1$.
4. *Let* $p \equiv 1, 3 \pmod 8$ *be a prime not equal to 3 and let* $d = ((2n+1)p)^2 - 2$ *with* $n \geq 1$ *an integer. Then* $H(4d) > 1$.

Their idea was to first prove that the equation $x^2 - dy^2 = \pm p$ has no solution for d of the form

$$d = \begin{cases} (2np)^2 - 1 & \text{with} \quad p \equiv 1 \pmod 4 \\ (2np)^2 + 3 & \text{with} \quad p \equiv \pm 1 \pmod 4 \\ ((2n+1)p)^2 + 2 & \text{with} \quad p \equiv \pm 1 \pmod 8 \\ ((2n+1)p)^2 - 2 & \text{with} \quad p \equiv 1, 3 \pmod 8 \end{cases}$$

where p is a prime and n is a positive integer. Then they lift the class group of the quadratic field to the real cyclotomic field using the following result of Yamaguchi [4].

Lemma 1.1 *Let h be the class number of quadratic field* $\mathbb{Q}(\sqrt{d})$, *if* $d > 0$ *is an integer with* $\phi(d) > 4$, *where* ϕ *is Euler's totient function, then* $h(d) | H(4d)$.

Let us recall that the continued fraction expression for $\sqrt{d}$ where d is a square-free integer has the form

$$\sqrt{d} = [a_0, \overline{a_1, a_2, ..., a_{t-1}, a_t = 2a_0}]$$

where $a_1, a_2, ..., a_{t-1}$ is a symmetric sequence.

Moreover, the converse of the above fact is also true. The following proposition describes the converse.

Proposition 1 [1] *Let* $a_1, a_2, ..., a_{t-1}$ $(t \geq 1)$ *be any symmetric sequence of positive integers. Define a sequence* q_i *for* $-1 \leq i \leq t$ *by the recurrence relation* $q_{i+1} = a_{i+1}q_i + q_{i-1}$, $q_{-1} = 0$, $q_0 = 1$. *Then the equation*

$$\sqrt{d} = [z, \overline{a_1, a_2, ..., a_{t-1}, 2z}], \; z = \lfloor d \rfloor \tag{1.1}$$

has infinitely many square-free positive solutions $d \equiv 2, 3 \pmod 4$ *if and only if* q_{t-1} *is odd or* q_{t-1} *and* $q_{t-2}q_{t-3}$ *are both even. When either of the condition is satisfied then all the solutions of* (1.1) *are given by*

$$d = d(n) = \alpha n^2 + \beta n + \gamma; \quad z(n) = \eta n + \mu,$$

for integers $n \geq 1$. *Here* $\alpha, \beta, \gamma, \eta, \mu$ *depend on* $a_1, a_2, ..., a_{t-1}$ *with* $\alpha \neq 0$ *is a square;* $\eta \neq 0$ *and the discriminant is*

$$\beta^2 - 4\alpha\gamma = (-1)^t \text{ or } 4(-1)^t \text{ or } 16(-1)^t.$$

Moreover, if $d(n)$ is square-free and $d \equiv 2, 3 \pmod 4$, the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has the form

$$\epsilon = p(n) + q\sqrt{d} \tag{1.2}$$

where p is a linear polynomial, $q = q_{t-1}$ and both p and q depend on the sequence $a_1, a_2, ..., a_{t-1}$.

In our case, we are going to consider t to be even so that the norm of the fundamental unit, $Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\epsilon) = 1$. Also $a_1, a_2, ..., a_{s-1}$ be any symmetric sequence of positive integers such that q_{t-1} is odd. Note that such class of symmetric sequences will be non-empty because if we take $t = 2$ and consider symmetric sequence $a_1 = 1$, in this case $q_1 = 1$ is odd. Hence by Proposition 1, the equation

$$\sqrt{d} = [z, \overline{a_1, a_2, ..., a_{s-1}, 2z}], z = \lfloor d \rfloor$$

has infinitely many square-free positive integer solutions $d \equiv 3 \pmod 4$. For example, if we take the same sequence $a_1 = 1$ as above then we can see that there are infinitely many d's with $d \equiv 3 \pmod 4$. We aren't interested in $d \equiv 2 \pmod 4$ for reasons which would be clear when we prove non-triviality of the class number. Therefore for us d has the form:

$$d = \alpha n^2 + \beta n + \gamma.$$

If d is square-free, the fundamental unit of $\mathbb{Q}(\sqrt{d})$ is of the form:

$$\epsilon = p(n) + q\sqrt{d}.$$

In this article, we obtain an infinite family of d's with non-trivial class number for real cyclotomic fields $\mathbb{Q}(\zeta_{4d})^+$. We now state the main result of this note.

Theorem 1.2 *There are infinitely many $d \equiv 3 \pmod 4$ of the form $d = \alpha n^2 + \beta n + \gamma$ such that $H(4d) > 1$.*

Here α, β and γ are as stated in the Proposition 1.

2 Solvability of a Diophantine equation

Lemma 2.1 *Given a prime p, there are infinitely many d of the form $d = \alpha n^2+\beta n+\gamma$ for which the Diophantine equation*

$$x^2 - dy^2 = \pm p$$

has no integer solution.

Proof First we consider

$$x^2 - dy^2 = p. \tag{2.1}$$

If possible let us assume that (2.1) has an integer solution (x_0, y_0) and without loss of generality we assume that it is the smallest solution with $y_0 \geq 1$. Then,

$$x_0^2 - dy_0^2 = p. \tag{2.2}$$

We rewrite it as

$$Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x_0 - y_0\sqrt{d}) = p.$$

The above equation can written as (since ϵ is a unit)

$$p = Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}((x_0 - y_0\sqrt{d})\epsilon),$$

which can be further reduced to,

$$\begin{aligned} p &= Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}((x_0 - y_0\sqrt{d})(p(n) + q\sqrt{d})). \\ &= Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}((p(n)x_0 - dqy_0) + (x_0q - p(n)y_0)\sqrt{d}). \\ &= (p(n)x_0 - dqy_0)^2 - (x_0q - p(n)y_0)^2d. \end{aligned}$$

Now by the minimality of y_0, we have,

$$y_0 \leq |x_0q - p(n)y_0|.$$

Case 1 *If* $y_0 \le x_0 q - p(n) y_0$.
Then,

$$(1 + p(n)) y_0 \le x_0 q.$$

We use (2.2) *and set* $p(n) = x_1 n + x_2$. *This leads to*

$$\{(1 + x_1 n + x_2)^2 - q^2 d\} y_0^2 \le q^2 p.$$
$$\{(1 + x_1 n + x_2)^2 - q^2 (\alpha n^2 + \beta n + \gamma)\} y_0^2 \le q^2 p.$$

Also

$$(x_1^2 - q^2 \alpha) n^2 + (2x_1 + 2x_1 x_2 - q^2 \beta) n + (x_2^2 + 2x_2 + 1 - q^2 \gamma) \le \frac{q^2 p}{y_0^2}. \tag{2.3}$$

Since $x_1, x_2, p, q, \alpha, \beta, \gamma, y_0$ *are fixed integers, therefore,* (2.3) *implies that there are finitely many* $n's$, *which further implies that there are finitely many* $d's$. *We may remove those finitely many* $d's$.

Case 2 *If* $y_0 \le p(n) y_0 - x_0 q$.
Then,

$$x_0 q \le (p(n) - 1) y_0.$$

Again, using (2.2) *and setting* $p(n) = x_1 n + x_2$, *we get,*

$$q^2 p \le \{(x_1 n + x_2 - 1)^2 - q^2 d\} y_0^2.$$

This leads to

$$q^2 p \le \{(x_1 n + x_2 - 1)^2 - q^2 (\alpha n^2 + \beta n + \gamma)\} y_0^2$$

and

$$q^2 (\alpha n^2 + \beta n + \gamma) - (x_1 n + x_2 - 1)^2 \le \frac{-q^2 p}{y_0^2}.$$

Thus

$$(q^2 \alpha - x_1^2) n^2 + (q^2 \beta - 2x_1 - 2x_1 x_2) n + (q^2 \gamma - x_2^2 - 2x_2 - 1) \le \frac{-q^2 p}{y_0^2}. \tag{2.4}$$

By the same argument as in case (1), we have finitely many $d's$.

Next, we consider

$$x^2 - dy^2 = -p. \tag{2.5}$$

Suppose that (2.5) has an integer solution. Without loss of generality assume that (x_0, y_0) is the smallest solution with $y_0 \ge 1$.

Then,

$$x_0^2 - y_0^2 = -p. \tag{2.6}$$

We rewrite

$$Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} (x_0 - y_0 \sqrt{d}) = -p. \tag{2.7}$$

The above equation can written as (since ϵ is a unit)

$$-p = Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} ((x_0 - y_0 \sqrt{d}) \epsilon),$$

which is,

$$\begin{aligned} -p &= Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} ((x_0 - y_0 \sqrt{d})(p(n) + q\sqrt{d})). \\ &= Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} ((p(n) x_0 - dq y_0) + (x_0 q - p(n) y_0)\sqrt{d}). \\ &= (p(n) x_0 - dq y_0)^2 - (x_0 q - p(n) y_0)^2 d. \end{aligned}$$

Now by the minimality of y_0, we have,

$$y_0 \le |x_0 q - p(n) y_0|.$$

Case 3 *If $y_0 \le x_0 q - p(n) y_0$. Then,*

$$(1 + p(n)) y_0 \le x_0 q.$$

We use (2.6) *and set* $p(n) = x_1 n + x_2$. *This leads to*

$$\begin{aligned} -q^2 p &\ge \{(1 + x_1 n + x_2)^2 - q^2 d\} y_0^2 \\ &\ge \{(1 + x_1 n + x_2)^2 - q^2(\alpha n^2 + \beta n + \gamma)\} y_0^2. \end{aligned}$$

This implies

$$\frac{-q^2 p}{y_0^2} \ge (x_1^2 - q^2 \alpha) n^2 + (2x_1 + 2x_1 x_2 - q^2 \beta) n + (x_2^2 + 2x_2 + 1 - q^2 \gamma),$$

which implies finitely many $d's$.

Case 4 *If $y_0 \le p(n) y_0 - x_0 q$.*
Then,

$$x_0 q \le (p(n) - 1) y_0.$$

We use (2.6) *and set* $p(n) = x_1 n + x_2$. *This leads to*

$$\begin{aligned} -q^2 p &\le \{(x_1 n + x_2 - 1)^2 - q^2 d\} y_0^2. \\ -q^2 p &\le \{(x_1 n + x_2 - 1)^2 - q^2(\alpha n^2 + \beta n + \gamma)\} y_0^2. \\ \frac{q^2 p}{y_0^2} &\ge q^2(\alpha n^2 + \beta n + \gamma) - (x_1 n + x_2 - 1)^2. \end{aligned}$$

This implies

$$(q^2 \alpha - x_1^2) n^2 + (q^2 \beta - 2x_1 - 2x_1 x_2) n + (q^2 \gamma - x_2^2 - 2x_2 - 1) \le \frac{q^2 p}{y_0^2},$$

which implies finitely many $d's$.

This completes the proof of Lemma 2.1 □

3 Proof of the Theorem (1.2)

Let $p \equiv 1 \pmod 4$ be a prime. There are infinitely many $d \equiv 3 \pmod 4$ such that the Legendre symbol

$$\left(\frac{d}{p}\right) = 1.$$

We consider those $d's$.
This implies, p splits completely in $\mathbb{Q}(\sqrt{d})$, i.e. $p = \mathfrak{P}\mathfrak{P}'$, where $\mathfrak{P}$ and $\mathfrak{P}'$ are prime ideals. We also have $Nm(\mathfrak{P}) = Nm(\mathfrak{P}') = p$.

Suppose if possible the class number $h(d)$ of $\mathbb{Q}(\sqrt{d})$ is 1. Then $\mathfrak{P}$ is a principal ideal in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, say $\mathfrak{P} = \langle a + b\sqrt{d} \rangle$. Thus, we have

$$p = Nm(\mathfrak{P}) = Nm_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = |a^2 - db^2|.$$

This implies

$$a^2 - db^2 = \pm p, \tag{3.1}$$

which contradicts the lemma (2.1). Hence $h(d) \ne 1$. Except for finitely many $d's$, we have $\phi(d) > 4$, therefore $h(d) | H(4d)$ (by Lemma 1.1). Since $h(d) > 1$, we have $H(4d) > 1$.

4 Concluding remarks

As mentioned earlier, if we consider the sequence $a_1 = 1$ for $t = 2$, then in this case $d = (z+1)^2 - 1$. Suppose z is even, say, $z = 2n$, then

$$\begin{aligned} d &= (2n+1)^2 - 1 \\ &= 4n(n+1). \end{aligned}$$

So, for d to be square-free z has to be odd. Hence d has to be of the form $(2np)^2 - 1$, which is precisely the family considered in [6]. Thus, we get a more generalized and larger family.

Acknowledgements This article is a part of author's master thesis; the author would like to extend his heartfelt thanks to Prof. Kalyan Chakraborty for supervising the thesis and his continuous support, suggestions, remarks throughout.The author would also like to thank Mohit Mishra for going through the article and his continuous support in the completion of this article. The author is thankful to the anonymous referee for his/her suggestions/corrections which has immensely helped improving the manuscript. The scenic ambience of KSoM and support of the colleagues played an important role in completing the work.

References

1. A. Dahl and V. Kala, Distribution of class numbers in continued fraction families of real quadratic fields *Proc. Edinb. Math. Soc. (2)*, **61** (2018), 1193–1212.
2. A. Hoque and H. k. Saikia, On the class-number of the maximal real subfield of a cyclotomic field *Quaesty Math.*, **39** (2016), 889–894.
3. H. Osada, Note on class number of maximal real subfield of cyclotomic field, *Manuscripta Math.*, **58** (1987), 215–227.
4. I. Yamaguchi, On the class number of real subfield of cyclotomic field, *J. Reine Angrew. Math.*, **272** , (1975), 217–220.
5. J. C. Miller, Class number of totally real fiels and applications to the Weber class number problem, *Acta Arith.*, **164** , (2014), 381–397.
6. K.Chakraborty and A. Hoque, Pell-type equations and class number of the maximal real subfield of a cyclotomic field *Ramanujan J.*, **46** (2018), 727–742.
7. M. Mishra, R. Schoof and L. Washington, Class groups of real cyclotomic fields, *Monatsh. Math.*, **195** (2021), 489–496.
8. N. C. Ankeny, S. Chowla and H. Hasse, On the class number of the maximal real subfield of a cyclotomic field, *J. Reine Angrew. Math.*, **217** (1965), 217–220.
9. S. D. Lang, Note on the class number of the maximal real subfield of a cyclotomic field, *J. Reine Angrew. Math.*, **290** (1977), 70–72.