A STUDY ON ‘t’-DIVISIBILITY OF CLASS NUMBERS OF CERTAIN FAMILY OF IMAGINARY QUADRATIC FIELDS.

SRILAKSHMI KRISHNAMOORTHY AND R. MUNEESWARAN

Abstract. We prove that for a given odd number \( m \geq 3 \), for all but finitely many primes ‘\( p \)’, class number of \( \mathbb{Q}(\sqrt{1-2mp}) \) is divisible by ‘\( p \)’ and this collection of fields is infinite for a fixed ‘\( m \)’. We also prove that the class number of \( \mathbb{Q}(\sqrt{1-2mp}) \) is divisible by ‘\( p \)’ whenever \( 2mp - 1 \) is a square-free integer. For the above two results we conclude some corollaries by replacing ‘\( p \)’ by an square-free odd integer \( t \geq 3 \). We prove that for any pair of twin primes \( p_1, p_2 = p_1 + 2 \), at least one of the \( p_i \) must divide the class number of \( \mathbb{Q}(\sqrt{1-2mp_i}) \). We give a corollary that settles a generalized version of Iizuka’s conjecture for the case \( n = 1 \) and odd square-free ‘\( t \)’.

1. Introduction

Let \( K \) be a number field. The class group of \( K \) is denoted by \( Cl_K \). Let \( h_K \) be the class number of \( K \). Cohen-Lenstra heuristics \[4\] predicts that, for a given \( n > 1 \), quadratic fields whose class numbers are divisible by ‘\( n \)’ has positive density in the set of all quadratic fields. Several authors proved that for any natural number \( n \), there are infinitely many quadratic fields whose class number is divisible by \( n \)[1], [14], [18], [17]. Gauss conjectured that there are only finitely many imaginary quadratic fields whose class number is equals to 1. He predicted that the complete list \( \mathbb{Q}(\sqrt{-d}) \) are \( d = 1, 2, 3, 7, 11, 19, 43, 67, 163 \). This was proved by Harold stark [16], also independently by Heegner(1852) [6] with an error and Baker (1966). There are results on non-divisibility of class numbers[2]. It follows from Gauss’s genus theory that, there are infinitely many imaginary quadratic fields with class number is not divisible by 2.

These divisibility properties are important for studying the structure of the class group. A.Hoque proved that, under certain conditions class number of \( \mathbb{Q}(\sqrt{a^2-4p^2}) \) is divisible by ‘\( n \)’ [7]. Many of the authors studied about the class number of \( \mathbb{Q}(\sqrt{1-\mu^2m^2}) \), \( \mu \in \{1, 2, \sqrt{2}\} \) [12], [11], [8], [13]. Stéphane Louboutin proved the following result on divisibility of class number of \( \mathbb{Q}(\sqrt{1-4U^k}) \) for \( U > 2 \) and odd \( n \) [12].

Theorem 1. If \( k \in \mathbb{Z}^+ \) be odd number, then for any integer \( U \geq 2 \) the ideal class groups of the imaginary quadratic fields \( \mathbb{Q}(\sqrt{1-4U^k}) \) contain an element of order \( k \).

We prove some theorems when \( \mu = \sqrt{2} \). The following result of 3 divisibility of the class number is proved by K.Chakraborty and A.Hoque[8].

Theorem 2. The class number of the imaginary quadratic field \( \mathbb{Q}(\sqrt{1-2m^3}) \) is divisible by 3 for any odd integer \( m \geq 3 \).

2010 Mathematics Subject Classification. Primary: 11R29, Secondary: 11R11.

Key words and phrases. Class number, ideal class group, imaginary quadratic fields, Diophantine equation.
The first author and Pasupulati extended the above theorem for all odd prime ‘p’ and odd prime power ‘m’ and proved the following theorem\[11\].

**Theorem 3.** For given odd primes \(p, q\) and a natural number \(r\) the class number of \(\mathbb{Q}(\sqrt{1-2mp})\) is divisible by \(p\), where \(m = q^r\). For a fixed prime \(p\) this collection is an infinite family of imaginary quadratic fields.

In this paper, we prove the following four theorems. Theorem 4 is an extension of theorem 3 with odd prime ‘\(p\)’ replaced by square-free integer ‘\(t\)’. Theorem 6 is a generalization of theorem 3 with odd prime power \(m\) is replaced by odd integer \(m\).

**Theorem 4.** For a given odd square-free integer ‘\(t\)’, odd prime ‘\(q\)’ and a natural number ‘\(r\)’ the class number of \(\mathbb{Q}(\sqrt{1-2mt})\) is divisible by ‘\(t\)’ where \(m = q^r\). For a fixed ‘\(t\)’ this collection will be an infinite family of imaginary quadratic fields.

**Corollary 5.** For a given odd square-free integer \(t\), there exist infinitely many \(d\) such that class number of \(\mathbb{Q}(\sqrt{d})\) and \(\mathbb{Q}(\sqrt{d+1})\) is divisible by \(t\).

**Theorem 6.** If \(m \geq 3\) be an odd integer, then for all but finitely many primes ‘\(p\)’ the class number of \(\mathbb{Q}(\sqrt{1-2mp})\) is divisible by ‘\(p\)’. For a fixed ‘\(m\)’ the collection of fields \(\mathbb{Q}(\sqrt{1-2mp})\) such that ‘\(p\)’ divides the class number of \(\mathbb{Q}(\sqrt{1-2mp})\) is infinite.

**Corollary 7.** If \(m \geq 3\) be an odd integer, then there exist a finite number of primes say \(p_1, p_2, \ldots, p_n\) such that for any odd integer \(t \geq 3\) relatively prime to \(p_1p_2\ldots p_n\), the class number of \(\mathbb{Q}(\sqrt{1-2mt})\) is divisible by ‘\(p\)’ for all \(p \mid t\). In particular, if \(t \geq 3\) is an odd square-free integer relatively prime to \(p_1p_2\ldots p_n\), then the class number of \(\mathbb{Q}(\sqrt{1-2mt})\) is divisible by ‘\(t\)’.

**Theorem 8.** If \(m \geq 3\) is an odd number and ‘\(p\)’ is an odd prime such that \(2mp^r - 1\) is a square-free integer, then class number of \(\mathbb{Q}(\sqrt{1-2mp^r})\) is divisible by ‘\(p\)’.

**Corollary 9.** If \(m \geq 3\) be an odd integer and \(t \geq 3\) be an odd integer such that \(2mt^r - 1\) is a square-free integer, then the class number of \(\mathbb{Q}(\sqrt{1-2mt^r})\) is divisible by ‘\(p\)’ for all \(p \mid t\). In particular, if \(t \geq 3\) is an odd square-free integer such that \(2mt^r - 1\) is a square-free integer, then the class number of \(\mathbb{Q}(\sqrt{1-2mt^r})\) is divisible by ‘\(t\)’.

**Theorem 10.** If \(m \geq 3\) be an odd integer and \(p, p + 2\) is a pair of twin primes, then ‘\(p\)’ divides class number of \(\mathbb{Q}(\sqrt{1-2mp})\) or ‘\(p + 2\)’ divides the class number of \(\mathbb{Q}(\sqrt{1-2mp + 2})\).

We first prove \(\pm 2^{\frac{m-1}{2}}(1 + \sqrt{1-2mp^r})\) is not a \(p^{th}\) power in the ring of integers of \(\mathbb{Q}(\sqrt{1-2mp^r})\) and using this, we construct an element of order ‘\(p\)’ in the class group of \(\mathbb{Q}(\sqrt{1-2mp^r})\).

Birch Swinnerton-Dyer conjecture is elliptic curve analogue of the analytic class number formula. For any elliptic curve defined over \(\mathbb{Q}\) of rank zero and square-free conductor \(N\), if \(p \mid |E(\mathbb{Q})|\), under certain conditions on the Shafarevich-Tate group \(|\text{III}_E|\), the first author [10] showed that \(p \mid |\text{III}_E| \Leftrightarrow p \mid h_K\), \(K = \mathbb{Q}(\sqrt{-D})\).
2. Preliminaries

2.1. Iizuka’s conjecture. The following result on class numbers of imaginary quadratic fields is recently proved by Y. Iizuka in [8].

**Theorem 11.** There is an infinite family of pairs of imaginary quadratic fields \( \mathbb{Q}(\sqrt{d}) \) and \( \mathbb{Q}(\sqrt{d+1}) \) with \( d \in \mathbb{Z} \) whose class numbers are both divisible by 3.

Based on above theorem Iizuka conjectured the following

**Conjecture 12.** (Iizuka) For any prime \( p \) and any positive integer \( n \), there is an infinite family of \( n+1 \) successive real (or imaginary) quadratic fields

\[ \mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \ldots, \mathbb{Q}(\sqrt{d+n}) \]

with \( D \in \mathbb{Z} \) whose class numbers are divisible by \( p \).

A generalized version of the above conjecture is that the prime \( p \) can be replaced by any natural number ‘\( t \)’. Our corollary \([9]\) settles a generalized version of Iizuka’s conjecture for \( n = 1 \) odd square-free ‘\( t \)’.

**Definition 13.** Let \( K \) be a number field and let \( S \) be a finite set of valuations containing all the archimedean valuations. The set \( R_S = \{ x \in K : v(x) \geq 0, \forall v \notin S \} \) is called the set of \( S \)-integers.

**Theorem 14.** ([15], Chapter IX, Theorem 4.3). Let \( K \) be a number field and \( S \) be a finite set of valuations containing all the archimedean valuations on \( K \). Let \( f(x) \in K[x] \) be a polynomial of degree \( d \geq 3 \) with distinct roots in the algebraic closure \( \overline{K} \) of \( K \). Then the equation \( y^2 = f(x) \) has finitely many solutions in \( S \)-integers \( x, y \in R_S \).

**Corollary 15.** The collection of number fields \( \mathbb{Q}(\sqrt{1-2m^2}) \), where \( m \geq 3 \) is any odd positive integer is an infinite collection.

**Proof.** When \( K = \mathbb{Q} \) and \( S \) is the set of archimedean valuations on \( \mathbb{Q} \), the \( S \)-integers is \( \mathbb{Z} \). Consider the polynomial \( f(x) = \frac{1-2x \sqrt{d_0}}{d_0} \), \( d_0 \) is any square-free integer. It has distinct roots in the algebraic closure of \( \mathbb{Q} \).

Hence \( y^2 = \frac{1-2x \sqrt{d_0}}{d_0} \) has only finitely many solutions, \( x, y \in \mathbb{Z} \) by Siegel’s Theorem \([14]\). Therefore the collection \( \{ \mathbb{Q}(\sqrt{1-2m^2}) \} \) such that \( m \) is any odd positive integer and \( m > 1 \) is an infinite collection. \( \square \)

**Lemma 16.** (Lemma 2 of \([12]\)). The class number of an imaginary bi-quadratic field is either the product of the class numbers of the three quadratic subfields or half that number.

We state some results proved by Yann Bugeaud and T.N. Shorey on solutions of Diophantine equation \( D_1x^2 + D_2 = \lambda^2m^\nu \) \([3]\), where gcd\((D_1, D_2) = \gcd(D_1D_2, m) = 1 \), \( m \geq 2 \) and \( \lambda = 1, 2, \sqrt{2} \) such that \( \lambda = 2 \) when \( m \) is even.

Let us denote \( F_i \) to be the Fibonacci sequence defined by \( F_0 = 0, F_1 = 1 \) and \( F_i = F_{i-1} + F_{i-2} \), and \( L_i \) denote the Lucas sequence defined by \( L_0 = 2, L_1 = 1 \) and \( L_i = L_{i-1} + L_{i-2}, i \geq 2 \). We define subsets \( F, G, H \) of \( \mathbb{N} \times \mathbb{N} \times \mathbb{N} \) by

\[ F = \{(F_{i-2\epsilon}, L_{i+\epsilon}, F_i) : i \geq 2, \epsilon \in \{\pm 1\}\} \]
\[ G = \{(1, 4m^r - 1, m) : m \geq 2, r \geq 1\}, \]
\[ H = \{(D_1, D_2, m) : \exists r, s \in \mathbb{N} \ni D_1s^2 + D_2 = \lambda^2m^r \text{ and } 3D_1s^2 - D_2 = \pm \lambda^2\}. \]

Define \( N(\lambda, D_1, D_2, m) \) to be the number of \((x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+\) such that \( D_1x^2 + D_2 = \lambda^2m^r \). Let \( S = \{(2, 2, 3), (4, \sqrt{2}, 7, 11), (\sqrt{2}, 1, 1, 5), (\sqrt{2}, 1, 1, 13), (2, 1, 3, 7), (1, 1, 19, 55), (1, 1, 341, 377), (1, 2, 1, 3), (2, 7, 1, 2)\}. \) By Theorem 2 of [3], if \((\lambda, D_1, D_2, m) \in S\), then \( N(\lambda, D_1, D_2, m) = 2\), which is a finite number.

**Theorem 17.** (Corollary 1 of [3]). Apart from the elements corresponding to the elements in the infinite families \( F, G, H \) and the examples in the set \( S \), the equation \( D_1x^2 + D_2 = \lambda^2m^r \) has at most \( 2^{\omega(m)-1} \) solutions, here \( \omega(m) = \text{number of distinct prime divisors of } m \).

**Theorem 18.** (Page 65 of [3]). The Diophantine equation \( x^2 + 1 = 2y^n \) with odd \( n > 1 \) and odd \( y > 1 \) has no solution.

**Lemma 19.** For any integer \( m \geq 3 \) and a positive integer \( D \) and \( \text{gcd}(D, m) = 1 \), the number of solutions of the Diophantine equation \( Dx^2 + 1 = 2m^y \) is finite.

**Proof.** Let \( D_1 = D, D_2 = 1, \lambda = \sqrt{2} \). From Theorem 17, the Diophantine equation \( Dx^2 + 1 = 2m^y \) has finite number of solutions if \((D_1, D_2, m) = (D, 1, m) \notin F \cup G \cup H \). If \((D, 1, m) \in F\), then \((D, 1, m) = (F_{i-2}, L_{i+\epsilon}, F_i)\) for some \( i, \epsilon \). By comparing the second coordinates, we get \( 1 = L_{i+\epsilon} \). Hence \( i = 2 \) and \( \epsilon = -1 \), which implies \( F_i = 1 \). By comparing the third coordinates, we get, \( m = F_i = 1 \), which is a contradiction to \( m \geq 3 \). If \((D, 1, m) \in G\), then \((D, 1, m) = (1, 4m^r - 1, m)\). Hence \( 4m^r - 1 = 1 \), which is a contradiction to \( m \) is an integer. If \((D, 1, m) \in H\), then \( \exists r, s \in \mathbb{N} \ni D_2s^2 + 1 = 2m^r, 3D_2s^2 - 1 = \pm 2 \). Suppose \( 3D_2s^2 - 1 = 2\), then \( D_2s^2 = 1 \) hence \( 2m^r - 1 = 1 \), thus \( m = 1 \), which is not possible. Suppose \( 3D_2s^2 - 1 = -2\), then \( D = \frac{-1}{3^2} \), which is a contradiction to \( D \) is an integer. Thus \((D, 1, m) \notin F \cup G \cup H \). Hence the lemma follows. \( \square \)

**Lemma 20.** For every integer \( m \geq 3 \) the equation \((2m - 1)x^2 + 1 = 2m^y \) has at most \( 2^{\omega(m)-1} \) solutions \((x, y) \in \mathbb{N} \times \mathbb{N}\).

**Proof.** Consider \( D_1 = 2m - 1, D_2 = 1, \lambda = \sqrt{2} \). We see that \((\lambda, D_1, D_2, m) = (\sqrt{2}, 2m - 1, 1, m) \notin S \). Clearly \( \text{gcd}(D_1, D_2) = \text{gcd}(2m - 1, 1) = 1, \text{gcd}(D_1, D_2, m) = \text{gcd}(2m - 1, m) = 1 \) and \( m \geq 3 \). As in the proof of Lemma 19, \((2m - 1, 1, m) \notin F \cup G \cup H \). Hence the equation \((2m - 1)x^2 + 1 = 2m^y \) has at most \( 2^{\omega(m)-1} \) solutions \((x, y) \in \mathbb{N} \times \mathbb{N}\) by Theorem 17. \( \square \)

3. **Proof of main theorems**

**Proposition 21.** If \( m \geq 3 \) is an odd integer and ‘\( p \)’ be an odd prime, then for all but finitely many odd primes \( p \), \( \pm 2^{\frac{p-1}{2}} (1 + \sqrt{1 - 2m^p}) \) is not a \( p\)th power in the ring of integers of \( \mathbb{Q}(\sqrt{1 - 2m^p}) \).

**Proof.** Let \( \{p_i\} \) be the set of all odd primes. Let \( d_i \) be the square-free part of \( 1 - 2m^{p_i} \) with the same sign. Let \( 1 - 2m^{p_i} = n_i^2d_i, n_i \in \mathbb{N} \) and \( K_i = \mathbb{Q}(\sqrt{1 - 2m^{p_i}}) \).

\begin{equation}
1 - 2m^{p_i} \equiv 3 \pmod{4} \implies O_{K_i} = \mathbb{Z}[(\sqrt{d_i})].
\end{equation}
Let $a_i = 1 + \sqrt{1 - 2m^p}$. We claim that $\pm 2^{\frac{p-1}{2}}(1 + \sqrt{1 - 2m^p})$ is not $p_i^{th}$ power of any element in $O_{K_i}$ for all but finitely many $p_i$. Note $2^{\frac{p-1}{2}}(1 + \sqrt{1 - 2m^p})$ is $p_i^{th}$ power if and only if $-2^{\frac{p-1}{2}}(1 + \sqrt{1 - 2m^p})$ is $p_i^{th}$ power. Hence it is enough to prove that $2^{\frac{p-1}{2}}(1 + \sqrt{1 - 2m^p})$ is not the $p_i^{th}$ power except finitely many $p_i$. Suppose $2^{\frac{p-1}{2}}(1 + \sqrt{1 - 2m^p}) = (a_i + b_i\sqrt{d_i})^{p_i}, a_i + b_i\sqrt{d_i} \in \mathbb{Z}[d_i]$ for every $p_i$.

Using binomial expansion we get,

\begin{equation}
2^{\frac{p_i-1}{2}} (1 + \sqrt{1 - 2m^p}) = \sum_{j=0}^{\frac{p_i-1}{2}} \binom{p_i}{2j} a_i^{p_i-2j} b_i^{2j} d_i^j + \sum_{j=0}^{\frac{p_i-1}{2}} \binom{p_i}{2j+1} a_i^{p_i-(2j+1)} b_i^{2j+1} d_i^j \sqrt{d_i}.
\end{equation}

\begin{equation}
2^{\frac{p_i-1}{2}} (1 + n_i \sqrt{d_i}) = a_i \sum_{j=0}^{\frac{p_i-1}{2}} \binom{p_i}{2j} a_i^{p_i-2j-1} b_i^{2j} d_i^j + b_i \sum_{j=0}^{\frac{p_i-1}{2}} \binom{p_i}{2j+1} a_i^{p_i-(2j+1)} b_i^{2j+1} d_i^j \sqrt{d_i}.
\end{equation}

From the above expression, we can conclude that $a_i \mid 2^{\frac{p_i-1}{2}}$ and $b_i \mid 2^{\frac{p_i-1}{2}} n_i$. Let $2^{\frac{p_i-1}{2}} n_i = b_i y_i$, for some $y_i \in \mathbb{Z}$. From $a_i \mid 2^{\frac{p_i-1}{2}}$ we can observe that $a_i$ is even or $a_i = \pm 1$. We claim that ‘$a_i$’ is even is not possible.

Suppose ‘$a_i$’ is even, Consider

\begin{equation}
2^{\frac{p_i-1}{2}} (1 + \sqrt{1 - 2m^p}) = (a_i + b_i \sqrt{d_i})^{p_i}.
\end{equation}

Applying norm on both sides we get,

\begin{equation}
2^{p_i} m^p = (a_i^2 - b_i^2 d_i)^{p_i}.
\end{equation}

\begin{equation}
2m - a_i^2 = -b_i^2 d_i.
\end{equation}

The left hand side $2m - a_i^2$ is even. Hence right hand side $-b_i^2 d_i$ must be even. Since $d_i$ is odd, $b_i$ must be even. Hence the right hand side of the equation (3.6) is divisible by 4. Thus left hand side is also divisible by 4. Thus 2 divides ‘m’, which is a contradiction to ‘m’ is odd. Hence $a_i$ is not even. Which implies $a_i = \pm 1$. Thus the equation (3.6) becomes,

\begin{equation}
2m - 1 = -b_i^2 d_i.
\end{equation}

Multiplying by $y_i^2$ on both sides of the above equation we get,

\begin{equation}
2my_i^2 - y_i^2 = -(b_i y_i)^2 d_i.
\end{equation}

put $b_i y_i = 2^{\frac{p_i-1}{2}} n_i$ in equation (3.8) we get,

\begin{equation}
(2m - 1)y_i^2 = -2^{p_i-1} n_i^2 d_i.
\end{equation}

By comparing both sides of the above equation and by using $2m - 1$ is odd, we get $2^{p_i-1} \mid y_i^2$. Rewriting the equation above we get,

\begin{equation}
(2m - 1) \left( \frac{y_i}{2^{\frac{p_i-1}{2}}} \right)^2 = -n_i^2 d_i = 2m^p - 1.
\end{equation}

\begin{equation}
(2m - 1) \left( \frac{y_i}{2^{\frac{p_i-1}{2}}} \right)^2 + 1 = 2m^p.
\end{equation}
From the above equation, \( \left( \frac{\mu}{2^{m-1}}, p_i \right) \) is a solution for the equation \((2m-1)x^2 + 1 = 2m^y\). By Lemma 20, the equation has at most \(2^{\omega(m)-1}\) solutions in \(N \times N\).

Thus if \(2^{\frac{m-1}{2}}\) is a \(p_i\text{th}\) power, then corresponding to that \(p_i\), we get a solution in integers for the equation \((2m-1)x^2 + 1 = 2m^y\) with \(y = p_i\). Hence if \(2^{\frac{m-1}{2}}\) is a \(p_i\text{th}\) power for more than \(2^{\omega(m)-1}\) number of primes, then it is a contradiction to the equation \((2m-1)x^2 + 1 = 2m^y\) has at most \(2^{\omega(m)-1}\) solutions. Hence for all but finitely many odd primes \(p\), \(\pm 2^{\frac{m-1}{2}}(1 + \sqrt{1-2m^y})\) is not a \(p\text{th}\) power in the ring of integers of \(\mathbb{Q}(\sqrt{1-2m^y})\).

Proposition 22. If \(m \geq 3\) be an odd integer and ‘\(p\)’ be an odd prime such that \(2m^p - 1\) is a square-free integer, then \(\pm 2^{\frac{m-1}{2}}(1 + \sqrt{1-2m^y})\) is not a \(p\text{th}\) power in the ring of integers of \(\mathbb{Q}(\sqrt{1-2m^y})\).

Proof. Let \(d = 1 - 2m^p\). Let \(K = \mathbb{Q}(\sqrt{d})\) and \(O_K\) be the ring of integers of \(K\).

\[1 - 2m^p \equiv 3 \pmod{4}\] (mod 4). Hence \(d \equiv 3 \pmod{4}\). Thus \(O_K = \mathbb{Z}[\sqrt{d}]\).

Note that \(-2^{\frac{m-1}{2}}\) is \(p\text{th}\) power if and only if \(+2^{\frac{m-1}{2}}\) is \(p\text{th}\) power, where \(\alpha = 1 + \sqrt{1-2m^y}\). Hence it is enough to prove \(2^{\frac{m-1}{2}}\) is not \(p\text{th}\) power.

suppose \(2^{\frac{m-1}{2}} = (a + b\sqrt{d})^p\), \(a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]\). Expanding the above expression using binomial expansion and comparing the real and imaginary parts and using \(2m^p - 1\) is square-free we get, \(a \mid 2^{\frac{m-1}{2}}\) and \(b \mid 2^{\frac{m-1}{2}}\).

Similar way like the proof of proposition 21 we can conclude that ‘\(a\)’ is not even and ‘\(a\)’ must be equals to \(\pm 1\). Using all of these observations we get,

\[2^{\frac{m-1}{2}}(1 + \sqrt{1-2m^y}) = (\pm 1 + b\sqrt{d})^p.\]

Applying norm on both sides we get,

\[2^p m^p = (1 - b^2 d)^p \text{ implies } b^2 d = 1 - 2m.\]

From the above expression, we observe that ‘\(b\)’ must be odd. We know \(b \mid 2^{\frac{m-1}{2}}\). Hence \(b = \pm 1\). Substituting \(b = \pm 1\) in (3.13) we get,

\[d = 1 - 2m.\]

Since \(2m^p - 1\) is square-free and \(d = 1 - 2m^p\), from (3.14) we get, \(1 - 2m^p = 1 - 2m\). Hence \(p = 1\), which is a contradiction to ‘\(p\)’ is a prime number. Hence \(2^{\frac{m-1}{2}}(1 + \sqrt{1-2m^y})\) is not a \(p\text{th}\) power in the ring of integers of \(\mathbb{Q}(\sqrt{1-2m^y})\).

Proposition 23. If \(m \geq 3\) be an odd integer and \(p, p + 2\) be a pair of twin primes, then \(\pm 2^{\frac{m-1}{2}}(1 + \sqrt{1-2m^y})\) is not a \(p\text{th}\) power in the ring of integers of \(\mathbb{Q}(\sqrt{1-2m^y})\) or \(\pm 2^{\frac{m-1}{2}}(1 + \sqrt{1-2m^{p+2}})\) is not a \((p + 2)\text{th}\) power in the ring of integers of \(\mathbb{Q}(\sqrt{1-2m^{p+2}})\).

Proof. Let \(p + 2 = q\). Let \(d, d'\) be square-free part of \(-2m^p\) and \(-2m^q\) respectively with the same sign. Let \(1 - 2m^p = n_1^2 d\) and \(1 - 2m^q = n_2^2 d'\), for some \(n_1, n_2 \in \mathbb{N}\). Let \(K = \mathbb{Q}(\sqrt{1-2m^p}), K' = \mathbb{Q}(\sqrt{1-2m^q})\).

\[1 - 2m^p \equiv 3 \pmod{4}\] (mod 4) and \(1 - 2m^q \equiv 3 \pmod{4}\).

(3.15) \(\text{Which implies } O_K = \mathbb{Z}[d]\) and \(O_{K'} = \mathbb{Z}[d']\).
Let us take $\alpha = 1 + \sqrt{1 - 2m^2}$ and $\beta = 1 + \sqrt{1 - 2m^2}$.

Suppose $\pm 2^{\frac{d-1}{2}}$ is $p^{th}$ power in $O_K$ and $\pm 2^{\frac{d-1}{2}}$ is $q^{th}$ power in $O_K^*$, 

\[(3.17) \quad 2^{\frac{d-1}{2}} = (a_1 + b_1 \sqrt{d})^p \text{ and } 2^{\frac{d-1}{2}} = (a_2 + b_2 \sqrt{d})^q, \quad a_1, a_2, b_1, b_2 \in \mathbb{Z}.
\]

Expanding the above expressions using binomial expansion we get, $a_1 \mid 2^{\frac{d-1}{2}}$, $b_1 \mid 2^{\frac{d-1}{2}} n_1$, $a_2 \mid 2^{\frac{d-1}{2}}$ and $b_2 \mid 2^{\frac{d-1}{2}} n_2$. Hence $2^{\frac{d-1}{2}} n_1 = b_1 y_1$ and $2^{\frac{d-1}{2}} n_2 = b_2 y_2$, for some $y_1, y_2 \in \mathbb{Z}$.

Similar way like the proof of proposition 21 we can conclude that \[(2 \mid m - 1) \text{ implies } (2 \mid n - 1 - (2m^p - 1)).
\]

\begin{align*}
(2m - 1) & | (2m^p - 1) \text{ and } (2m - 1) | (2m^q - 1) \implies (2m - 1) | (2m^q - 1 - (2m^p - 1)). \\
(2m - 1) & \mid 2m^p(m^2 - 1).
\end{align*}

We have $2m - 1$ and $2m^p$ are relatively prime hence we get,

\begin{align*}
(2m - 1) & \mid (m^2 - 1) \text{ implies } (2m - 1) | (m - 1)(m + 1). \\
\text{Hence } (2m - 1) \mid (m + 1).
\end{align*}

We can write $2m - 1 = 2(m - 1) + 1$. Thus $2m - 1$ and $m - 1$ are relatively prime.

\begin{align*}
\text{Hence } (2m - 1) \mid (m + 1). \\
\text{From the above } 2m - 1 \leq m + 1, \text{ thus } m \leq 2.
\end{align*}

Which is a contradiction to $m \geq 3$. Hence the proposition follows.

\begin{proposition}
Suppose $m \geq 3$ be an odd number and $p$ be an odd prime, If $\pm 2^{\frac{d-1}{2}}(1 + \sqrt{1 - 2m^p})$ is not a $p^{th}$ power of an element in the ring of integers of $\mathbb{Q}(\sqrt{1 + 2m^p})$, then $p$ divides the order of the class group of $\mathbb{Q}(\sqrt{1 - 2m^p})$.
\end{proposition}

\begin{proof}
Let $d$ be the square-free part of $1 - 2m^p$ with the same sign, then $d \equiv 3 \pmod{4}$ and $K = \mathbb{Q}(\sqrt{d})$.

Put $\alpha = 1 + \sqrt{1 - 2m^2}$, then $N_{K/\mathbb{Q}}(\alpha) = 2m^p$. Since $d \equiv 3 \pmod{4}$ the ideal $(2)$ is ramified, there exist a prime ideal $P$ such that $(2) = P^2$. Let $m = \prod_{i=1}^{n} p_i^{t_i}$, each $p_i$ is an odd prime. Clearly each $p_i$ is splits.

Since $N_{K/\mathbb{Q}}(\alpha) = 2m^p = 2p_1^{r_1}p_2^{r_2}...p_n^{r_n}$, the prime decomposition of $\langle \alpha \rangle$ is given by $\langle \alpha \rangle = P Q_1^{r_1} Q_2^{r_2}...Q_n^{r_n}$, where each $Q_i$ is a prime ideal lies above $p_i$ and each $t_i$ is a positive integer. Since $p_i$ splits over $K$, we can say that $N(Q_i) = p_i$ for all ‘$i$’. Hence $N(\langle \alpha \rangle) = 2p_1^{r_1}p_2^{r_2}...p_n^{r_n}$. We know that
\end{proof}
\( N(\langle \alpha \rangle) = N_{K/Q}(\alpha) \). This gives \( t_i = r_i p \). Consider the ideal \( I = PQ_1^{t_1}Q_2^{t_2}...Q_n^{t_n} \) of \( O_K \).

We have,
\[
(3.27) \quad I^p = P^Q_1Q_2^{t_2}...Q_n^{t_n} = (2)^{\frac{n-1}{2}} \quad PQ_1^{t_1}Q_2^{t_2}...Q_n^{t_n} = (2)^{\frac{n-1}{2}} (\alpha) = \langle 2^{\frac{n-1}{2}} \alpha \rangle.
\]

We claim that the order of the ideal \( I \) in the ideal class group is \( p \). If \( I \) is not of order \( 'p' \), then \( I = \langle \beta \rangle \) for some \( \beta \in O_K \).

\[
(3.28) \quad \langle \beta^p \rangle = \langle \beta \rangle^p = I^p = \langle 2^{\frac{n-1}{2}} \alpha \rangle.
\]

By the Theorem (18) we get \( Q(\sqrt{1 - 2mp}) \neq Q(\sqrt{-1}) \). Hence the only units of \( O_K \) are 1 and -1. This implies that \( \beta^p = \pm 2^{\frac{n-1}{2}} \alpha \), which is a contradiction to \( \pm 2^{\frac{n-1}{2}} \alpha \) is not a \( p^h \) power in \( O_K \). Hence class group of \( Q(\sqrt{1 - 2mp}) \) has an element \( I \) of order \( 'p' \). Thus \( 'p' \) divides the order of the class group of \( Q(\sqrt{1 - 2mp}) \).

**Proof of Theorem (3)** Let \( q \) be an odd prime number, \( t \geq 3 \) be an odd square-free integer and \( m = q^r \) for some natural number \( 'r' \). Write \( t = q_1q_2...q_t \) where each \( q_i \) is a prime. Let \( m_i = q^r \Pi_{j \neq i} q_j = m \Pi_{j \neq i} q_j \), which implies \( m^t = m^{\Pi_{j \neq i} q_j} \). Hence by this Theorem (2) class number of \( Q(\sqrt{1 - 2m^t}) \) is divisible by \( q_i \). We also have \( Q(\sqrt{1 - 2m^t}) \) \( = Q(\sqrt{1 - 2m_i^t}) \). This implies the class number of \( Q(\sqrt{1 - 2m^t}) \) is divisible by every \( q_i \). Hence \( t \) divides the class number of \( Q(\sqrt{1 - 2m^t}) \). By corollary (15) this collection is infinite.

**Proof of Corollary (5)** It follows from Theorem (3) any odd square-free \( t \) divides the class number of \( K = Q(\sqrt{4(1 - 2m^t)t}) = Q(\sqrt{(1 - 2m^t)}) \) for \( m = q^r \), where \( q \) is any odd prime.

Let \( U = 2m^t - 1 \). Then \( U \geq 2 \). Furthermore Theorem (1) implies that \( t \) divides the class number of \( Q(\sqrt{1 - 4U^t}) \). Now look at
\[
Q(\sqrt{1 - 4U^t}) = Q(\sqrt{1 - 4(2m^t - 1)^t}) = Q(\sqrt{4(1 - 2m^t)^t + 1}).
\]

Let \( d = 4(1 - 2m^t)^t \). The square-free integer \( t \) divides class numbers of \( Q(\sqrt{d}), Q(\sqrt{d + 1}) \).

Infiniteness of \( d \) comes from the infiniteness of Theorem (3). Hence the result follows.

**Corollary 25.** For any odd square-free integer \( t \geq 3 \), there exist infinitely many imaginary bi-quadratic fields whose class number is divisible by \( t \).

**Proof.** Fix an odd square-free integer \( t \geq 3 \), consider the set \( S_1 = \{ m \in \mathbb{Z}^+ : m \) is not a square, \( m \equiv 1 \pmod{4} \) and the class number of \( Q(\sqrt{1 - 2m^t}) \) is divisible by \( t \} \). By Siegel’s Theorem, Theorem (3) and Dirichlet’s Theorem on arithmetic progression, \( S_1 \) contains infinitely many primes \( q \) with \( q \equiv 1 \pmod{4} \), which implies that \( S_1 \) is an infinite set. For \( m \in S_1 \), consider the bi-quadratic field \( K_m = Q(\sqrt{1 - 2m^t}, \sqrt{m}) \). Denote \( L^1_m = Q(\sqrt{1 - 2m^t}), L^2_m = Q(\sqrt{m}) \), and \( L^3_m = Q(\sqrt{1 - 2m^t} \sqrt{m}) \).

Since \( m \) is not a square, \( L^2_m \) is a quadratic field. Observe that \( L^1_m \neq L^2_m \) because \( 1 - 2m^t \equiv 3 \pmod{4} \). Thus \( L^1_m, L^2_m \) and \( L^3_m \) are three quadratic sub fields of \( K_m \). Let \( h_m, h^1_m, h^2_m, h^3_m \) be the class numbers of \( K_m, K^1_m, K^2_m, K^3_m \) respectively. Then by Lemma (16) we have \( h_m = \frac{h^1_m h^2_m h^3_m}{2} \), \( i = 0, 1 \). Since \( m \in S_1 \),
the odd square-free integer \( t \) divides the class number of \( h_m^1 \). Since \( t \) is odd, \( t \) must divides \( h_m \). The infiniteness of the set \( \{ K_m : m \in S_1 \} \) follows from infiniteness of the set \( S_1 \) and Siegel’s Theorem. \( \square \)

**Proof of Theorem 6.** Using Proposition 21 and Proposition 24 we can say that for a given odd integer \( m \geq 3 \) the class number of \( \mathbb{Q}(\sqrt{1-2m^p}) \) is divisible by \( 'p' \) for all but finitely many odd primes \( 'p' \). In lemma 19 choosing \( D \) is any positive square-free integer and \( k = m \), we can say that for only finitely many prime \( 'p' \), \( D \) can be square-free part of \( 2m^p - 1 \). Hence the collection \( \{ p : p \text{ is a prime and } p | h_{\mathbb{Q}(\sqrt{1-2m^p})} \} \) is infinite set and a positive square-free integer \( D \) can be square-free part of \( 2m^p - 1 \) for only finitely many primes \( 'p' \). Hence for a fixed \( 'm' \) the collection of fields \( \mathbb{Q}(\sqrt{1-2m^p}) \) whose class number is divisible by \( 'p' \) is infinite.

**Proof of Corollary 7.** Let \( J = \{ p_1, p_2, ..., p_n \} \) be the set of primes which are the exceptional cases arising by Theorem 6. Consider an odd integer \( t \geq 3 \) relatively prime to \( p_1p_2...p_n \). Let \( p \) be a prime which divides \( t \). Clearly \( p \) is relatively prime to \( p_1p_2...p_n \). Consider \( \mathbb{Q}(\sqrt{1-2m^t}) = \mathbb{Q}(\sqrt{1-2(m^t)^p}) \). By the Theorem 6 we can say that \( p \) divides the class number of \( \mathbb{Q}(\sqrt{1-2(m^t)^p}) \) which is \( \mathbb{Q}(\sqrt{1-2m^t}) \).

Hence if \( p \) divides \( t \), then \( p \) divides the class number of \( \mathbb{Q}(\sqrt{1-2m^t}) \). In particular if \( t \) is a square-free odd number relatively prime to \( p_1p_2...p_n \), then clearly \( t \) divides class number of \( \mathbb{Q}(\sqrt{1-2m^t}) \).

**Proof of Theorem 8.** Assume that \( 2m^p - 1 \) is square-free for an odd prime \( 'p' \) and \( m \geq 3 \) an odd number. Using the Proposition 22 and Proposition 24 we can say that \( 'p' \) divides the class number of \( \mathbb{Q}(\sqrt{1-2m^t}) \).

**Proof of Corollary 9.** Choose \( 'p' \) is an arbitrary prime divisor of an odd integer \( t \geq 3 \) and assume that \( 2m^t - 1 \) also square-free. Here \( 2m^t - 1 = 2(m^t)^p - 1 \) which gives \( \mathbb{Q}(\sqrt{1-2m^t}) = \mathbb{Q}(\sqrt{1-2(m^t)^p}) \). Also \( 2(m^t)^p - 1 \) is a square-free integer. Hence using Theorem 8 we can say that \( 'p' \) divides class number of \( \mathbb{Q}(\sqrt{1-2(m^t)^p}) = \mathbb{Q}(\sqrt{1-2m^t}) \). Since \( 'p' \) is an arbitrary prime divisor of \( 't' \), we conclude that if \( t \) is odd square-free, then \( 't' \) divides the class of \( \mathbb{Q}(\sqrt{1-2m^t}) \). Hence the proof.

**Proof of Theorem 10.** Proposition 23 and Proposition 24 implies Theorem 10.

**Remark 26.** Twin prime conjecture states that there are infinitely many twin primes. If the twin prime conjecture is true, then for each pair of twin primes we can have at least one prime \( 'p' \) which divides class number of \( \mathbb{Q}(\sqrt{1-2m^t}) \). This shows that there are infinitely many primes \( 'p' \) which divides class number of \( \mathbb{Q}(\sqrt{1-2m^t}) \).

**Acknowledgement**

We thank IISER, TVM for providing the excellent working conditions. We would like to thank Azizul Hoque and Sunil Kumar Pasupulati for helpful discussions and suggestions. We also wanted to thank Jaitra Chattopadhyay for helpful comments.

**References**

1. N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. 5 (1955), 321–324.
2. Ajit Bhand and M. Ram Murty, *Class numbers of quadratic fields*, Hardy-Ramanujan J. **42** (2019), 17–25.

3. Yann Bugeaud and T. N. Shorey, *On the number of solutions of the generalized Ramanujan-Nagell equation*, J. Reine Angew. Math. **539** (2001), 55–74.

4. H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

5. Gary Cornell, *A note on the class group of composita*, J. Number Theory **39** (1991), no. 1, 1–4.

6. Kurt Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.

7. Azizul Hoque, *On the exponents of class groups of some families of imaginary quadratic fields*, Mediterr. J. Math. **18** (2021), no. 4, Paper No. 153, 13.

8. Azizul Hoque and Kalyan Chakraborty, *Divisibility of class numbers of certain families of quadratic fields*, J. Ramanujan Math. Soc. **34** (2019), no. 3, 281–289.

9. Yoshichika Izuka, *On the class number divisibility of pairs of imaginary quadratic fields*, J. Number Theory **184** (2018), 122–127.

10. Srilakshmi Krishnamoorthy, *A note on the Fourier coefficients of a Cohen-Eisenstein series*, Int. J. Number Theory **12** (2016), no. 5, 1149–1161.

11. Srilakshmi Krishnamoorthy and Sunil Kumar Pasupulati, *Note on the p-divisibility of class numbers of an infinite family of imaginary quadratic fields*, Glasgow Mathematical Journal (2021), 1–6.

12. Stéphane R. Louboutin, *On the divisibility of the class number of imaginary quadratic number fields*, Proc. Amer. Math. Soc. **137** (2009), no. 12, 4025–4028.

13. M. Ram Murty, *Exponents of class groups of quadratic fields*, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 229–239.

14. Trygve Nagel, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), no. 1, 140–150.

15. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

16. Harold Stark, *On complex quadratic fields with class number equal to one*, Trans. Amer. Math. Soc. **122** (1966), 112–119.

17. P. J. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory **5** (1973), 237–241.

18. Yoshihiko Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka Math. J. **7** (1970), 57–76.