Simultaneous divisibility and indivisibility properties of class numbers of quadratic fields

Jaitra Chattopadhyay
Indian Institute of Technology, Guwahati
Guwahati - 781 039
Assam, India
e-mail : jaitra@iitg.ac.in

Indian Institute of Technology, Guwahati

May 14, 2021

• The ring $\mathbb{Z}$ is a principal ideal domain (PID) and hence a unique factorization domain (UFD).

- The ring $\mathbb{Z}$ is a principal ideal domain (PID) and hence a unique factorization domain (UFD).

- The ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is not a UFD.

- The ring $\mathbb{Z}$ is a principal ideal domain (PID) and hence a unique factorization domain (UFD).

- The ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is not a UFD.

- For an algebraic number field K, its ring of integers $\mathcal{O}_K$ is not always a PID.

- The ring $\mathbb{Z}$ is a principal ideal domain (PID) and hence a unique factorization domain (UFD).
- The ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is not a UFD.
- For an algebraic number field K, its ring of integers $\mathcal{O}_K$ is not always a PID.
- How do we "*measure*" the failure of unique factorization in the ring $\mathcal{O}_K$?

- Let $\mathfrak{F}(K)$ denote the group of fractional ideals of K.

- Let $\mathfrak{F}(K)$ denote the group of fractional ideals of K.

- Let $\mathfrak{P}(K)$ denote the subgroup of $\mathfrak{F}(K)$ consisting of the principal fractional ideals of K.

- Let $\mathfrak{F}(K)$ denote the group of fractional ideals of K.

- Let $\mathfrak{P}(K)$ denote the subgroup of $\mathfrak{F}(K)$ consisting of the principal fractional ideals of K.

- The quotient group $Cl_K := \mathfrak{F}(K)/\mathfrak{P}(K)$ is called the ideal class group of K.

- Let $\mathfrak{F}(K)$ denote the group of fractional ideals of K.
- Let $\mathfrak{P}(K)$ denote the subgroup of $\mathfrak{F}(K)$ consisting of the principal fractional ideals of K.
- The quotient group $Cl_K := \mathfrak{F}(K)/\mathfrak{P}(K)$ is called the ideal class group of K.
- The group Cl_K is a finite abelian group for all number fields K.

• Let $\mathfrak{F}(K)$ denote the group of fractional ideals of K.

• Let $\mathfrak{P}(K)$ denote the subgroup of $\mathfrak{F}(K)$ consisting of the principal fractional ideals of K.

• The quotient group $Cl_K := \mathfrak{F}(K)/\mathfrak{P}(K)$ is called the ideal class group of K.

• The group Cl_K is a finite abelian group for all number fields K.

• The order of the group Cl_K is called the class number of K and is denoted by h_K.

Example:- Diophantine equation

- **Question:** Find all $(x, y) \in \mathbb{Z}^2$ such that

$$y^2 = x^3 - 2.$$

Example:- Diophantine equation

- **Question:** Find all $(x, y) \in \mathbb{Z}^2$ such that

$$y^2 = x^3 - 2.$$

- Observe that both x and y are odd integers.

Example:- Diophantine equation

- **Question:** Find all $(x, y) \in \mathbb{Z}^2$ such that
$$y^2 = x^3 - 2.$$

- Observe that both x and y are odd integers.

- Write $x^3 = (y - \sqrt{-2})(y + \sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$.

- **Question:** Find all $(x, y) \in \mathbb{Z}^2$ such that
$$y^2 = x^3 - 2.$$

- Observe that both x and y are odd integers.
- Write $x^3 = (y - \sqrt{-2})(y + \sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$.
- We have $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ (Because $\mathbb{Z}[\sqrt{-2}]$ is a PID).

- **Question:** Find all $(x, y) \in \mathbb{Z}^2$ such that

$$y^2 = x^3 - 2.$$

- Observe that both x and y are odd integers.
- Write $x^3 = (y - \sqrt{-2})(y + \sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$.
- We have $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ (Because $\mathbb{Z}[\sqrt{-2}]$ is a PID).
- Equating the coefficients of $\sqrt{-2}$ from both sides, we get $1 = b(3a^2 - 2b^2)$.

- **Question:** Find all $(x, y) \in \mathbb{Z}^2$ such that
$$y^2 = x^3 - 2.$$
- Observe that both x and y are odd integers.
- Write $x^3 = (y - \sqrt{-2})(y + \sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$.
- We have $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ (Because $\mathbb{Z}[\sqrt{-2}]$ is a PID).
- Equating the coefficients of $\sqrt{-2}$ from both sides, we get $1 = b(3a^2 - 2b^2)$.
- This yields the solution $(a, b) = (\pm 1, 1)$.

- **Question:** Find all $(x, y) \in \mathbb{Z}^2$ such that

$$y^2 = x^3 - 2.$$

- Observe that both x and y are odd integers.
- Write $x^3 = (y - \sqrt{-2})(y + \sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$.
- We have $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ (Because $\mathbb{Z}[\sqrt{-2}]$ is a PID).
- Equating the coefficients of $\sqrt{-2}$ from both sides, we get $1 = b(3a^2 - 2b^2)$.
- This yields the solution $(a, b) = (\pm 1, 1)$.
- Hence $(x, y) = (3, \pm 5)$.

- **Question:** Find all primes p such that $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

- **Question:** Find all primes p such that $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

- From Class Field Theory, it is equivalent to the fact that p splits completely in the *Hilbert class field* of $\mathbb{Q}(\sqrt{-1})$.

• **Question:** Find all primes p such that $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

• From Class Field Theory, it is equivalent to the fact that p splits completely in the *Hilbert class field* of $\mathbb{Q}(\sqrt{-1})$.

• Since the class number of $\mathbb{Q}(\sqrt{-1})$ is 1, the Hilbert class field of $\mathbb{Q}(\sqrt{-1})$ is itself.

- **Question:** Find all primes p such that $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

- From Class Field Theory, it is equivalent to the fact that p splits completely in the *Hilbert class field* of $\mathbb{Q}(\sqrt{-1})$.

- Since the class number of $\mathbb{Q}(\sqrt{-1})$ is 1, the Hilbert class field of $\mathbb{Q}(\sqrt{-1})$ is itself.

- Now, p splits completely in $\mathbb{Q}(\sqrt{-1})$ if and only if $\left(\frac{-1}{p}\right) = 1$.

- **Question:** Find all primes p such that $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

- From Class Field Theory, it is equivalent to the fact that p splits completely in the *Hilbert class field* of $\mathbb{Q}(\sqrt{-1})$.

- Since the class number of $\mathbb{Q}(\sqrt{-1})$ is 1, the Hilbert class field of $\mathbb{Q}(\sqrt{-1})$ is itself.

- Now, p splits completely in $\mathbb{Q}(\sqrt{-1})$ if and only if $\left(\frac{-1}{p}\right) = 1$.

- Consequently, $p = x^2 + y^2$ has solutions $\iff p \equiv 1 \pmod 4$.

Theorem (Heegner, Baker and Stark)

Let $d > 0$ be a square-free integer. Then the quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number 1 precisely for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

Motivation and history (qualitative results)

Theorem (Heegner, Baker and Stark)

Let $d > 0$ be a square-free integer. Then the quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number 1 precisely for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

Gauss class number 1 conjecture

There exist infinitely many real quadratic fields of class number 1.

Theorem (Heegner, Baker and Stark)

Let $d > 0$ be a square-free integer. Then the quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number 1 precisely for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

Gauss class number 1 conjecture

There exist infinitely many real quadratic fields of class number 1.

Theorem (Nagell (1922), Ankeny and Chowla (1955))

Let $n \geq 2$ be an integer. Then there exist infinitely many imaginary quadratic fields K such that $n \mid h_K$.

Theorem (Heegner, Baker and Stark)

Let $d > 0$ be a square-free integer. Then the quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number 1 precisely for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

Gauss class number 1 conjecture

There exist infinitely many real quadratic fields of class number 1.

Theorem (Nagell (1922), Ankeny and Chowla (1955))

Let $n \geq 2$ be an integer. Then there exist infinitely many imaginary quadratic fields K such that $n \mid h_K$.

Theorem (Weinberger (1973))

Let $n \geq 2$ be an integer. Then there exist infinitely many real quadratic fields K such that $n \mid h_K$.

• **Question:-** What can we say about the divisibility of class numbers of two fields taken at a time?

• **Question:-** What can we say about the divisibility of class numbers of two fields taken at a time?

Scholz's reflection principle (1932)

Let $d > 1$ be a square-free integer. Let r and s be the 3-ranks of the ideal class groups of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$, respectively. Then

$$r \leq s \leq r + 1.$$

- **Question:-** What can we say about the divisibility of class numbers of two fields taken at a time?

Scholz's reflection principle (1932)

Let $d > 1$ be a square-free integer. Let r and s be the 3-ranks of the ideal class groups of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$, respectively. Then

$$r \leq s \leq r + 1.$$

- In particular, if $3 \mid h_{\mathbb{Q}(\sqrt{d})}$, then $3 \mid h_{\mathbb{Q}(\sqrt{-3d})}$.

Simultaneous divisibility by 3 (Quadratic field case)

• **Question:-** What can we say about the divisibility of class numbers of two fields taken at a time?

Scholz's reflection principle (1932)

Let $d > 1$ be a square-free integer. Let r and s be the 3-ranks of the ideal class groups of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$, respectively. Then

$$r \leq s \leq r + 1.$$

• In particular, if $3 \mid h_{\mathbb{Q}(\sqrt{d})}$, then $3 \mid h_{\mathbb{Q}(\sqrt{-3d})}$.

• Combining Weinberger's theorem and Scholz's reflection principle, we obtain

• **Question:-** What can we say about the divisibility of class numbers of two fields taken at a time?

Scholz's reflection principle (1932)

Let $d > 1$ be a square-free integer. Let r and s be the 3-ranks of the ideal class groups of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$, respectively. Then

$$r \leq s \leq r + 1.$$

• In particular, if $3 \mid h_{\mathbb{Q}(\sqrt{d})}$, then $3 \mid h_{\mathbb{Q}(\sqrt{-3d})}$.

• Combining Weinberger's theorem and Scholz's reflection principle, we obtain

Proposition

There exist infinitely many pairs of quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$, with $d > 0$, such that

$$3 \mid h_{\mathbb{Q}(\sqrt{d})} \qquad \text{and} \qquad 3 \mid h_{\mathbb{Q}(\sqrt{-3d})}.$$

Recent results

Theorem (Komatsu (2002))

Let m be a non-zero integer. Then there exist infinitely many distinct pairs of quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{md})$, with $d > 0$, such that $3 \mid h_{\mathbb{Q}(\sqrt{d})}$ and $3 \mid h_{\mathbb{Q}(\sqrt{md})}$.

Recent results

Theorem (Komatsu (2002))

Let m be a non-zero integer. Then there exist infinitely many distinct pairs of quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{md})$, with $d > 0$, such that $3 \mid h_{\mathbb{Q}(\sqrt{d})}$ and $3 \mid h_{\mathbb{Q}(\sqrt{md})}$.

Theorem (Komatsu (2017))

Let $m \geq 2$ and $n \geq 2$ be integers. Then there exist infinitely many pairs of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{md})$ such that $n \mid h_{\mathbb{Q}(\sqrt{d})}$ and $n \mid h_{\mathbb{Q}(\sqrt{md})}$.

• Iizuka considered a slight variant of the above theorems and proved the following theorem.

• Iizuka considered a slight variant of the above theorems and proved the following theorem.

Theorem (Iizuka (2018))

There exist infinitely many pairs of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+1})$ with $d \in \mathbb{Z}$ such that $3 \mid h_{\mathbb{Q}(\sqrt{d})}$ and $3 \mid h_{\mathbb{Q}(\sqrt{d+1})}$.

• Iizuka considered a slight variant of the above theorems and proved the following theorem.

Theorem (Iizuka (2018))

There exist infinitely many pairs of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+1})$ with $d \in \mathbb{Z}$ such that $3 \mid h_{\mathbb{Q}(\sqrt{d})}$ and $3 \mid h_{\mathbb{Q}(\sqrt{d+1})}$.

• Iizuka also made the following conjecture.

• Iizuka considered a slight variant of the above theorems and proved the following theorem.

Theorem (Iizuka (2018))

There exist infinitely many pairs of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+1})$ with $d \in \mathbb{Z}$ such that $3 \mid h_{\mathbb{Q}(\sqrt{d})}$ and $3 \mid h_{\mathbb{Q}(\sqrt{d+1})}$.

• Iizuka also made the following conjecture.

Conjecture (Iizuka (2018))

Let $m \geq 1$ be an integer and let $\ell \geq 3$ be a prime number. Then there exist infinitely many tuples $\{\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \ldots, \mathbb{Q}(\sqrt{d+m})\}$ of quadratic fields (real or imaginary), with $d \in \mathbb{Z}$, such that ℓ divides the class numbers of all them.

Statement of Theorem 1

• We address a weaker version of the aforementioned conjecture and prove the following theorem.

• We address a weaker version of the aforementioned conjecture and prove the following theorem.

Theorem 1 (with M. Subramani)

Let $k \geq 1$ be a cube-free integer such that $k \equiv 1 \pmod 9$ and $\gcd(k, 7 \cdot 571) = 1$. Then there exist infinitely many triples of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{d+1})$ and $\mathbb{Q}(\sqrt{d+k^2})$ with $d \in \mathbb{Z}$ such that 3 divides $h_{\mathbb{Q}(\sqrt{d})}$, $h_{\mathbb{Q}(\sqrt{d+1})}$ and $h_{\mathbb{Q}(\sqrt{d+k^2})}$.

• We proved two parametric families of quadratic fields with class number divisible by 3.

Sketch of the proof

• We proved two parametric families of quadratic fields with class number divisible by 3.

Proposition 1

Let t be an integer with $t \not\equiv 0 \pmod 3$. Then the class number of the quadratic field $\mathbb{Q}(\sqrt{3t(3888t^2 + 108t + 1)})$ is divisible by 3.

• We proved two parametric families of quadratic fields with class number divisible by 3.

Proposition 1

Let t be an integer with $t \not\equiv 0 \pmod 3$. Then the class number of the quadratic field $\mathbb{Q}(\sqrt{3t(3888t^2+108t+1)})$ is divisible by 3.

Proposition 2

Let $m \geq 1$ be an integer. Then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{1-2916m^3})$ is divisible by 3.

Sketch of the proof of Theorem 1

Theorem (Llorente and Nart)

Let $f(T) = T^3 - mT - n \in \mathbb{Z}[T]$ be an irreducible polynomial over $\mathbb{Q}$ with discriminant $D(f)$ and splitting field K_f over $\mathbb{Q}$. Assume that for each prime number p, either $v_p(m) < 2$ or $v_p(n) < 3$ holds. Let $k_f = \mathbb{Q}(\sqrt{D(f)})$ and let ℓ be a prime number.

(i) If $\ell \neq 3$, then K_f/k_f is ramified at a prime ideal $\wp$ above ℓ if and only if $1 \leq v_\ell(n) \leq v_\ell(m)$.

(ii) For $\ell = 3$, the extension K_f/k_f is ramified at a prime ideal $\wp$ above 3 if and only if one of the following three conditions holds.

1. $1 \leq v_3(n) \leq v_3(m)$,
2. $3 \nmid n$, $m \equiv 0, 6 \pmod 9$ and $n^2 \not\equiv m + 1 \pmod 9$,
3. $3 \nmid n$, $m \equiv 3 \pmod 9$ and $n^2 \not\equiv m + 1 \pmod{27}$.

Sketch of the proof of Theorem 1

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.

Sketch of the proof of Theorem 1

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.
- Let $t_0 \in \mathbb{Z}$ be such that f_t is irreducible for all integer $t > |t_0|$.

Sketch of the proof of Theorem 1

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.
- Let $t_0 \in \mathbb{Z}$ be such that f_t is irreducible for all integer $t > |t_0|$.
- Consider the discriminant $D(f_t) = 27 \cdot (2916t^3 - k^2)$.

Sketch of the proof of Theorem 1

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.
- Let $t_0 \in \mathbb{Z}$ be such that f_t is irreducible for all integer $t > |t_0|$.
- Consider the discriminant $D(f_t) = 27 \cdot (2916t^3 - k^2)$.
- Let $t_0' \in \mathbb{Z}$ be such that $D(f_t)$ is not a perfect square for all integers $t > |t_0'|$.

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.
- Let $t_0 \in \mathbb{Z}$ be such that f_t is irreducible for all integer $t > |t_0|$.
- Consider the discriminant $D(f_t) = 27 \cdot (2916t^3 - k^2)$.
- Let $t_0' \in \mathbb{Z}$ be such that $D(f_t)$ is not a perfect square for all integers $t > |t_0'|$.
- We set $T = \max\{|t_0|, |t_0'|\} + 1$.

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.
- Let $t_0 \in \mathbb{Z}$ be such that f_t is irreducible for all integer $t > |t_0|$.
- Consider the discriminant $D(f_t) = 27 \cdot (2916t^3 - k^2)$.
- Let $t_0' \in \mathbb{Z}$ be such that $D(f_t)$ is not a perfect square for all integers $t > |t_0'|$.
- We set $T = \max\{|t_0|, |t_0'|\} + 1$.
- Consider the following simultaneous congruences.

$$\begin{cases} x \equiv 2 \pmod{9}; \\ x \equiv 1 \pmod{k}. \end{cases} \tag{1}$$

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.
- Let $t_0 \in \mathbb{Z}$ be such that f_t is irreducible for all integer $t > |t_0|$.
- Consider the discriminant $D(f_t) = 27 \cdot (2916t^3 - k^2)$.
- Let $t_0' \in \mathbb{Z}$ be such that $D(f_t)$ is not a perfect square for all integers $t > |t_0'|$.
- We set $T = \max\{|t_0|, |t_0'|\} + 1$.
- Consider the following simultaneous congruences.

$$\begin{cases} x \equiv 2 \pmod 9; \\ x \equiv 1 \pmod k. \end{cases} \tag{1}$$

- Since $\gcd(k, 9) = 1$, by the Chinese remainder theorem, there exists a unique solution $x_0 \pmod{9k}$ to the system of congruences (1).

- For an integer $t \geq 1$, consider $f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X]$.
- Let $t_0 \in \mathbb{Z}$ be such that f_t is irreducible for all integer $t > |t_0|$.
- Consider the discriminant $D(f_t) = 27 \cdot (2916t^3 - k^2)$.
- Let $t_0' \in \mathbb{Z}$ be such that $D(f_t)$ is not a perfect square for all integers $t > |t_0'|$.
- We set $T = \max\{|t_0|, |t_0'|\} + 1$.
- Consider the following simultaneous congruences.

$$\begin{cases} x \equiv 2 \pmod{9}; \\ x \equiv 1 \pmod{k}. \end{cases} \tag{1}$$

- Since $\gcd(k, 9) = 1$, by the Chinese remainder theorem, there exists a unique solution $x_0 \pmod{9k}$ to the system of congruences (1).
- Let

$$\mathcal{N} = \{n \in \mathbb{Z} : n \equiv x_0 \pmod{9k} \text{ and } n > \max\{T, k\}\}.$$

- For $n \in \mathcal{N}$, we have

$$27 \cdot n \cdot (3888n^2 + 108n + 1) \equiv 3^3 \cdot 7 \cdot 571 \not\equiv 0 \pmod{k}. \tag{2}$$

• For $n \in \mathcal{N}$, we have

$$27 \cdot n \cdot (3888n^2 + 108n + 1) \equiv 3^3 \cdot 7 \cdot 571 \not\equiv 0 \pmod{k}. \tag{2}$$

• Now, for $n \in \mathcal{N}$, let $t_n = n \cdot (3888n^2 + 108n + 1)$ and we consider the polynomial $f_{t_n}(X) = X^3 - 27t_nX - k$ over $\mathbb{Q}$.

• For $n \in \mathcal{N}$, we have

$$27 \cdot n \cdot (3888n^2 + 108n + 1) \equiv 3^3 \cdot 7 \cdot 571 \not\equiv 0 \pmod{k}. \tag{2}$$

• Now, for $n \in \mathcal{N}$, let $t_n = n \cdot (3888n^2 + 108n + 1)$ and we consider the polynomial $f_{t_n}(X) = X^3 - 27t_nX - k$ over $\mathbb{Q}$.

• Since $n \in \mathcal{N}$, we have f_{t_n} is irreducible over $\mathbb{Q}$ and $D(f_{t_n})$ is not a perfect square.

• For $n \in \mathcal{N}$, we have

$$27 \cdot n \cdot (3888n^2 + 108n + 1) \equiv 3^3 \cdot 7 \cdot 571 \not\equiv 0 \pmod{k}. \tag{2}$$

• Now, for $n \in \mathcal{N}$, let $t_n = n \cdot (3888n^2 + 108n + 1)$ and we consider the polynomial $f_{t_n}(X) = X^3 - 27t_nX - k$ over $\mathbb{Q}$.

• Since $n \in \mathcal{N}$, we have f_{t_n} is irreducible over $\mathbb{Q}$ and $D(f_{t_n})$ is not a perfect square.

• By a result of Llorente and Nart, the splitting field E of f_{t_n} is an unramified extension of $\mathbb{Q}(\sqrt{D(f_{t_n})})$ and hence $3 \mid h_{\mathbb{Q}(\sqrt{D(f_{t_n})})}$.

- Since $\mathbb{Q}(\sqrt{D(f_{t_n})}) = \mathbb{Q}(\sqrt{27 \cdot (2916t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{3 \cdot (2916t_n^3 - k^2)})$ is a real quadratic field with $3 \mid h_{\mathbb{Q}(\sqrt{D(f_{t_n})})}$,

Sketch of the proof of Theorem 1

• Since $\mathbb{Q}(\sqrt{D(f_{t_n})}) = \mathbb{Q}(\sqrt{27 \cdot (2916 t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{3 \cdot (2916 t_n^3 - k^2)})$ is a real quadratic field with $3 \mid h_{\mathbb{Q}(\sqrt{D(f_{t_n})})}$,

• Scholz's reflection principle yields that 3 divides the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3 \cdot 3 \cdot (2916 t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{k^2 - 2916 t_n^3})$.

• Since $\mathbb{Q}(\sqrt{D(f_{t_n})}) = \mathbb{Q}(\sqrt{27 \cdot (2916t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{3 \cdot (2916t_n^3 - k^2)})$ is a real quadratic field with $3 \mid h_{\mathbb{Q}(\sqrt{D(f_{t_n})})}$,

• Scholz's reflection principle yields that 3 divides the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3 \cdot 3 \cdot (2916t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{k^2 - 2916t_n^3})$.

• By Proposition 1 and Proposition 2, we already have that 3 divides the class numbers of both $\mathbb{Q}(\sqrt{-2916t_n^3}) = \mathbb{Q}(\sqrt{-t_n})$ and $\mathbb{Q}(\sqrt{1 - 2916t_n^3})$.

• Since $\mathbb{Q}(\sqrt{D(f_{t_n})}) = \mathbb{Q}(\sqrt{27 \cdot (2916t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{3 \cdot (2916t_n^3 - k^2)})$ is a real quadratic field with $3 \mid h_{\mathbb{Q}(\sqrt{D(f_{t_n})})}$,

• Scholz's reflection principle yields that 3 divides the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3 \cdot 3 \cdot (2916t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{k^2 - 2916t_n^3})$.

• By Proposition 1 and Proposition 2, we already have that 3 divides the class numbers of both $\mathbb{Q}(\sqrt{-2916t_n^3}) = \mathbb{Q}(\sqrt{-t_n})$ and $\mathbb{Q}(\sqrt{1 - 2916t_n^3})$.

• By letting $D_n = -2916t_n^3$, we get

$$3 \mid h_{\mathbb{Q}(\sqrt{D_n})}, 3 \mid h_{\mathbb{Q}(\sqrt{D_n+1})} \text{ and } 3 \mid h_{\mathbb{Q}(\sqrt{D_n+k^2})}.$$

$\square$

- **Trivial fact:** $h_K = 1 \iff h_K \not\equiv 0 \pmod{p}$ for all prime number p.

Indivisibility of class numbers

- **Trivial fact:** $h_K = 1 \iff h_K \not\equiv 0 \pmod{p}$ for all prime number p.
- Motivation comes from the *Gauss class number 1 conjecture*.

- **Trivial fact:** $h_K = 1 \iff h_K \not\equiv 0 \pmod{p}$ for all prime number p.
- Motivation comes from the *Gauss class number 1 conjecture*.
- Indivisibility result as the complement of the divisibility results.

- **Trivial fact:** $h_K = 1 \iff h_K \not\equiv 0 \pmod{p}$ for all prime number p.
- Motivation comes from the *Gauss class number 1 conjecture*.
- Indivisibility result as the complement of the divisibility results.
- What is known towards the direction of *simultaneous indivisibility* of class numbers of quadratic fields?

Motivation from Byeon's work

- In 2004, Byeon proved the following theorem.

- In 2004, Byeon proved the following theorem.

Theorem (Byeon (2004))

Let t be a square-free integer. Then there exist a positive proportion of fundamental discriminants $D > 0$ such that the class numbers of both $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{tD})$ are indivisible by 3.

- In 2004, Byeon proved the following theorem.

Theorem (Byeon (2004))

Let t be a square-free integer. Then there exist a positive proportion of fundamental discriminants $D > 0$ such that the class numbers of both $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{tD})$ are indivisible by 3.

- Motivated by the conjecture by Iizuka, we ask the following question.

- In 2004, Byeon proved the following theorem.

Theorem (Byeon (2004))

Let t be a square-free integer. Then there exist a positive proportion of fundamental discriminants $D > 0$ such that the class numbers of both $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{tD})$ are indivisible by 3.

- Motivated by the conjecture by Iizuka, we ask the following question.

Question

Let $\ell \geq 3$ be a prime number and let t be a non-zero integer. Do there exist infinitely many pairs of real (or imaginary) quadratic fields of the form $\{\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+t})\}$ such that the class numbers of all of them are indivisible by ℓ?

Theorem 2 (With A. Saikia)

Let $t \geq 1$ be an integer with $t \equiv 0 \pmod 4$. Then there exist infinitely many fundamental discriminants $D > 0$ with positive density such that the class numbers of the real quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{D+t})$ are all indivisible by 3.

Lemma 1 (Horie and Nakagawa (1988))

Lemma 1 (Horie and Nakagawa)

Let $m \geq 1$ and $N \geq 1$ be two integers satisfying the following two conditions.

1. If p is an odd prime number such that $p \mid \gcd(m, N)$, then $N \equiv 0 \pmod{p^2}$ and $m \not\equiv 0 \pmod{p^2}$.
2. If N is an even integer, then either $N \equiv 0 \pmod 4$ and $m \equiv 1 \pmod 4$ or $N \equiv 0 \pmod{16}$ and $m \equiv 8, 12 \pmod{16}$.

For a positive real number X, let $S_+(X)$ stand for the set of positive fundamental discriminants $D < X$ and let

$$S_+(X, m, N) = \{D \in S_+(X) : D \equiv m \pmod{N}\}.$$

For a fundamental discriminant $D > 0$, let $r_3(D)$ be the 3-rank of the ideal class group $Cl_{\mathbb{Q}(\sqrt{D})}$ of $\mathbb{Q}(\sqrt{D})$. Then we have

$$\lim_{X \to \infty} \frac{\sum\limits_{D \in S_+(X,m,N)} 3^{r_3(D)}}{|S_+(X, m, N)|} = \frac{4}{3}. \tag{3}$$

Lemma 2 (Byeon (2004))

Lemma 2 (Byeon (2004))

Let m and N be two positive integers satisfying the hypotheses of Lemma 1 and let D be a fundamental discriminant. Then

$$\liminf_{X\to\infty} \frac{|\{D \in S_+(X,m,N) : h(D) \not\equiv 0 \pmod 3\}|}{|S_+(X,m,N)|} \geq \frac{5}{6}. \tag{4}$$

Lemma 3 (Prachar (1958))

Lemma 3 (Prachar (1958))

Let $k \geq 1$ and $\ell \geq 1$ be two integers with $\gcd(k, \ell) = 1$. For a large positive real number X, let

$$\mathcal{Q}(X, k, \ell) = |\{m \in \mathbb{N} : m \leq X, m \equiv \ell \pmod{k} \text{ and } \mu(m) \neq 0\}|.$$

Then for any real number $\varepsilon > 0$, we have

$$\mathcal{Q}(X, k, \ell) = \frac{6}{k\pi^2} \prod_{p|k} \left(1 - \frac{1}{p^2}\right)^{-1} X + O(X^{\frac{1}{2}} k^{-\frac{1}{4}+\varepsilon} + k^{\frac{1}{2}+\varepsilon}), \tag{5}$$

and the error term is uniform in k.

- Let $t \geq 1$ be a given integer with $t \equiv 0 \pmod 4$.

Proof of Theorem 2

- Let $t \geq 1$ be a given integer with $t \equiv 0 \pmod 4$.

- Choose positive integers m and N such that $\gcd(m, N) = \gcd(m + t, N) = 1$, $m \equiv 1 \pmod 4$ and $N \equiv 0 \pmod 4$.

Proof of Theorem 2

- Let $t \geq 1$ be a given integer with $t \equiv 0 \pmod 4$.

- Choose positive integers m and N such that $\gcd(m, N) = \gcd(m + t, N) = 1$, $m \equiv 1 \pmod 4$ and $N \equiv 0 \pmod 4$.

- For real number $X > 0$, let

$$L(X) = \{D \leq X : D \equiv m \pmod N, \mu(D) \neq 0 \text{ and } h(D) \not\equiv 0 \pmod 3\}$$

and

$$L_t(X) = \{D \leq X : D \equiv m \pmod N, \mu(D+t) \neq 0 \text{ and } h(D+t) \not\equiv 0 \pmod 3\}.$$

Proof of Theorem 2

- Let $t \geq 1$ be a given integer with $t \equiv 0 \pmod 4$.

- Choose positive integers m and N such that $\gcd(m, N) = \gcd(m+t, N) = 1$, $m \equiv 1 \pmod 4$ and $N \equiv 0 \pmod 4$.

- For real number $X > 0$, let

$$L(X) = \{D \leq X : D \equiv m \pmod N, \mu(D) \neq 0 \text{ and } h(D) \not\equiv 0 \pmod 3\}$$

and

$$L_t(X) = \{D \leq X : D \equiv m \pmod N, \mu(D+t) \neq 0 \text{ and } h(D+t) \not\equiv 0 \pmod 3\}.$$

- Note that $D \equiv m \equiv 1 \pmod 4$ and $D + t \equiv m + t \equiv 1 \pmod 4$.

• Let $t \geq 1$ be a given integer with $t \equiv 0 \pmod 4$.

• Choose positive integers m and N such that $\gcd(m, N) = \gcd(m+t, N) = 1$, $m \equiv 1 \pmod 4$ and $N \equiv 0 \pmod 4$.

• For real number $X > 0$, let

$$L(X) = \{D \leq X : D \equiv m \pmod N, \mu(D) \neq 0 \text{ and } h(D) \not\equiv 0 \pmod 3\}$$

and

$$L_t(X) = \{D \leq X : D \equiv m \pmod N, \mu(D+t) \neq 0 \text{ and } h(D+t) \not\equiv 0 \pmod 3\}.$$

• Note that $D \equiv m \equiv 1 \pmod 4$ and $D + t \equiv m + t \equiv 1 \pmod 4$.

• Therefore, the integers in the sets $L(X)$ and $L_t(X)$ are fundamental discriminants.

Proof of Theorem 2 continued...

- Let $\mathcal{S}(X) = \{D \leq X : D \equiv m \pmod{N}\}$.

- Let $\mathcal{S}(X) = \{D \leq X : D \equiv m \pmod{N}\}$.
- Since $\gcd(m, N) = 1$, by Lemma 3, we have

Proof of Theorem 2 continued...

- Let $\mathcal{S}(X) = \{D \leq X : D \equiv m \pmod{N}\}$.
- Since $\gcd(m, N) = 1$, by Lemma 3, we have

$$\lim_{X \to \infty} \frac{\mathcal{Q}(X, N, m)}{|\mathcal{S}(X)|} = \frac{6}{\pi^2} \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right)^{-1} \geq \frac{6}{\pi^2}. \tag{6}$$

- Let $\mathcal{S}(X) = \{D \leq X : D \equiv m \pmod{N}\}$.
- Since $\gcd(m, N) = 1$, by Lemma 3, we have

$$\lim_{X\to\infty} \frac{\mathcal{Q}(X, N, m)}{|\mathcal{S}(X)|} = \frac{6}{\pi^2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right)^{-1} \geq \frac{6}{\pi^2}. \tag{6}$$

- Therefore, from equation (6) and Lemma 2, we get

- Let $\mathcal{S}(X) = \{D \leq X : D \equiv m \pmod{N}\}$.
- Since $\gcd(m, N) = 1$, by Lemma 3, we have

$$\lim_{X\to\infty} \frac{\mathcal{Q}(X, N, m)}{|\mathcal{S}(X)|} = \frac{6}{\pi^2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right)^{-1} \geq \frac{6}{\pi^2}. \tag{6}$$

- Therefore, from equation (6) and Lemma 2, we get

$$\liminf_{X\to\infty} \frac{|L(X)|}{|\mathcal{S}(X)|} \geq \frac{5}{6} \cdot \frac{6}{\pi^2} = \frac{5}{\pi^2}. \tag{7}$$

- Similarly, for $L_t(X)$, we obtain

- Similarly, for $L_t(X)$, we obtain

$$\liminf_{X\to\infty} \frac{|L_t(X)|}{|\mathcal{S}(X)|} \geq \frac{5}{6} \cdot \frac{6}{\pi^2} = \frac{5}{\pi^2}. \tag{8}$$

- Similarly, for $L_t(X)$, we obtain

$$\liminf_{X\to\infty} \frac{|L_t(X)|}{|\mathcal{S}(X)|} \geq \frac{5}{6}\cdot\frac{6}{\pi^2} = \frac{5}{\pi^2}. \tag{8}$$

- Now, the principle of inclusion-exclusion yields

$$\frac{|L(X)\cap L_t(X)|}{|\mathcal{S}(X)|} = \frac{|L(X)|}{|\mathcal{S}(X)|} + \frac{|L_t(X)|}{|\mathcal{S}(X)|} - \frac{|L(X)\cup L_t(X)|}{|\mathcal{S}(X)|}. \tag{9}$$

- Since $\dfrac{|L(X) \cup L_t(X)|}{|\mathcal{S}(X)|}$ can be at most 1, we conclude that

- Since $\frac{|L(X) \cup L_t(X)|}{|\mathcal{S}(X)|}$ can be at most 1, we conclude that

$$\begin{aligned} \liminf_{X \to \infty} \frac{|L(X) \cap L_t(X)|}{|\mathcal{S}(X)|} &\geq \frac{5}{\pi^2} + \frac{5}{\pi^2} - 1 \\ &= \frac{10 - \pi^2}{\pi^2} > 0. \end{aligned}$$

- Since $\dfrac{|L(X) \cup L_t(X)|}{|\mathcal{S}(X)|}$ can be at most 1, we conclude that

$$\begin{aligned} \liminf_{X \to \infty} \frac{|L(X) \cap L_t(X)|}{|\mathcal{S}(X)|} &\geq \frac{5}{\pi^2} + \frac{5}{\pi^2} - 1 \\ &= \frac{10 - \pi^2}{\pi^2} > 0. \end{aligned}$$

- This completes the proof of Theorem 2. $\square$

Y. Iizuka, *On the class number divisibility of pairs of imaginary quadratic fields*, J. Number Theory, **184** (2018), 122-127.

J. Chattopadhyay and A. Saikia, *Simultaneous indivisibility of class numbers of pairs of real quadratic fields*, Ramanujan J., To appear.

J. Chattopadhyay and M. Subramani, *On the simultaneous* 3*-divisibility of class numbers of triples of imaginary quadratic fields*, Acta Arithmetica, **197** (2021), 105-110.

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

T. Komatsu, *An infinite family of pairs of quadratic fields* $\mathbb{Q}(\sqrt{D})$ *and* $\mathbb{Q}(\sqrt{mD})$ *whose class numbers are both divisible by* 3, Acta Arith., **104** (2002), 129–136.

T. Komatsu, *An infinite family of pairs of imaginary quadratic fields with ideal classes of a given order*, Int. J. Number Theory, **13** (2017), 253-260.

A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math., **166** (1932), 201-203.

THANK YOU