Class Numbers of Quadratic Fields

Ajit Bhand, M Ram Murty

Hardy-Ramanujan Journal 42 (2019), 17-25 submitted 08/07/2019, accepted 07/10/2019, revised 15/10/2019

Class Numbers of Quadratic Fields

Ajit Bhand and M. Ram Murty*

Dedicated to the memory of Alan Baker

Abstract. We present a survey of some recent results regarding the class numbers of quadratic fields

Keywords. class numbers, Baker's theorem, Cohen-Lenstra heuristics.
2010 Mathematics Subject Classification. Primary 11R42, 11S40, Secondary 11R29.

1. Introduction

The concept of *class number* first occurs in Gauss's *Disquisitiones Arithmeticae* written in 1801. In this work, we find the beginnings of modern number theory. Here, Gauss laid the foundations of the theory of binary quadratic forms which is closely related to the theory of quadratic fields. Motivated by the problem of representing natural numbers as the values of certain positive definite binary quadratic forms, he isolated the notions of *class number* and *genera*. Later, Dirichlet related the class number to special values $L(1,\chi)$ where χ is a quadratic (Dirichlet) character and $L(s,\chi)$ is the Dirichlet series attached to the character χ.

After the development of algebraic number theory through the works of Kummer and Dedekind, it became apparent that the failure of the unique factorization property in algebraic number fields is measured by the *ideal class group*. With Fermat's last theorem as the motivating muse, Kummer developed his theory of ideal numbers in the context of cyclotomic fields. But it was Dedekind who enunciated a larger theoretical framework that has now become part of the modern parlance. For any algebraic number field K, he introduced the *ring of integers* $\mathcal{O}_K$ and showed that every non-zero ideal of this ring has finite index and can be factored uniquely as a product of prime ideals. He also introduced what we now call the *Dedekind zeta function* $\zeta_K(s)$ which is defined for $\mathrm{Re}(s) > 1$ by the Dirichlet series

$$\sum_{\mathfrak{a}\neq 0} \frac{1}{\mathbb{N}\mathfrak{a}^s},$$

where $\mathbb{N}\mathfrak{a} := [\mathcal{O}_K : \mathfrak{a}]$. Dedekind's unique factorization theorem leads to the *Euler product*:

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathbb{N}\mathfrak{p}^s}\right)^{-1},$$

where the product is over all the non-zero prime ideals of $\mathcal{O}_K$. If $K = \mathbb{Q}$, then $\zeta_{\mathbb{Q}}(s)$ is the familiar Riemann zeta function and the above is the classical Euler product.

We say two non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_K$ are *equivalent* if there are elements $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. This defines an equivalence relation on the set of all ideals of $\mathcal{O}_K$ and one can even define an abelian group structure on the set of equivalence classes giving rise to the *ideal class group* $\mathfrak{C}_K$. That this ideal class group is a finite group is a famous theorem of Minkowski and his celebrated theory now called the *geometry of numbers* first arose in this context. The order of $\mathfrak{C}_K$ is called the *class number* and denoted h_K. Thus, $h_K = 1$ if and only if the ring $\mathcal{O}_K$ is a principal ideal domain (PID).

*The research of the second author was partially supported by an NSERC Discovery grant.
We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

2. Class numbers of imaginary quadratic fields

In his foundational work of 1801, Gauss conjectured that if K runs through imaginary quadratic fields, then the class number tends to infinity. In particular, he conjectured that there are only finitely many imaginary quadratic fields with class number one. In fact, he even predicted the complete list of such fields. They are $\mathbb{Q}(\sqrt{-d})$ where

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

This conjecture was finally proved independently by Alan Baker [Bak71] and Harold Stark [St66] in 1966. Baker developed his celebrated theory of linear forms in logarithms and applied his new theory to resolve this problem. Baker's method is applicable in a vast variety of Diophantine questions and so he was awarded the Fields Medal for this theory in 1968. Stark's method adapts an old method of Heegner using modular functions, but ultimately, the final step is resolved using linear forms in logarithms.

But Gauss's class number problem and its final solution had a curious historical trajectory skirmishing around the generalized Riemann hypothesis! Although Dedekind introduced his celebrated zeta function, he was unable to derive an analytic continuation and functional equation similar to the Riemann zeta function. Using the newly created geometry of numbers, Weber was able to extend it to the region $\mathrm{Re}(s) > 1 - 1/[K : \mathbb{Q}]$, but the functional equation was elusive. It was Hecke who in 1918 used the theory of theta functions of several variables to show that $\zeta_K(s)$ extends analytically to the entire complex plane with a simple pole at $s = 1$ and satisfies a suitable functional equation similar to the one satisfied by $\zeta(s)$. One expects that all the non-trivial zeros of $\zeta_K(s)$ (that is, zeros with real part positive) to lie on the line $\mathrm{Re}(s) = 1/2$ and this is called the *generalized Riemann hypothesis* (GRH). If K is a quadratic field, then we have the factorization

$$\zeta_K(s) = \zeta(s)L(s, \chi)$$

where χ is the quadratic Dirichlet character (mod $|d_K|$), where d_K is the discriminant of K. One expects $L(s, \chi)$ to satisfy the Riemann hypothesis. Hecke noted that if $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field with class number $h(-d)$ and there is some constant $c > 0$ such that $L(s, \chi)$ has no real zero with real part greater than $1 - c/\log d$, then for some positive constant c_1, we have

$$h(d) > \frac{c_1\sqrt{d}}{\log d}.$$

In particular, the class number of imaginary quadratic fields tends to infinity and consequently, there are only finitely many imaginary quadratic fields with class number one. The reader will note that Hecke's hypothesis is substantially weaker than GRH and is certainly implied by it. It is surprising (and annoying to some) that we have been unable to show that this hypothesis always holds, an assertion which is far far away from the claim made by GRH. This is the problem of the so-called *Siegel zero*.

The years 1933 to 1935 saw a series of remarkable theorems related to this theme. Given Hecke's theorem, it was a surprise when Deuring proved in 1933 that the *falsity* of the classical Riemann hypothesis implies that $h(-d) \geq 2$ if d is sufficiently large. A year later, in 1934, Mordell proved that the *falsity* of the classical Riemann hypothesis also implies that $h(-d)$ tends to infinity. The final step came later that year when Heilbronn proved that the *falsity* of GRH implies $h(-d)$ tends to infinity. Thus, combining this strange mélange of theorems with the result of Hecke, we obtained an unconditional proof of Gauss's conjecture. We refer the reader to Chapter 21 of [Dav80] for the chronology of these puzzling sequence of discoveries.

Later in 1934, Heilbronn and Linfoot made their result partially *effective* in that they proved there is at most one more field in Gauss's list of imaginary quadratic fields with class number one.

Perhaps the most significant of these developments is the 1935 theorem of Siegel that states that for any $\epsilon > 0$, there is a constant $C(\epsilon) > 0$ such that

$$h(-d) > C(\epsilon) d^{1/2-\epsilon}.$$

We should compare this with Dirichlet's *class number formula* for imaginary quadratic fields

$$L(1, \chi) = \frac{2\pi h(-d)}{w\sqrt{|d_K|}}$$

where w is the number of roots of unity in K, d_K is the discriminant of K and χ is the Kronecker symbol $(d_K/\cdot)$, from which we can deduce

$$h(-d) \ll \sqrt{d} \log d.$$

Combining this with Siegel's theorem, we learn that $h(-d)$ "grows like" $\sqrt{d}$. More precisely,

$$\lim_{d\to\infty} \frac{\log h(-d)}{\log d} = \frac{1}{2}.$$

An important consequence of Siegel's theorem is that for any given value t there are only finitely many imaginary quadratic fields with class number t.

Siegel's theorem is *ineffective* in the sense that we do not know $C(\epsilon)$ explicitly. This ineffectivity does not facilitate an effective determination of all imaginary quadratic fields with a given class number. Although Baker and Stark could apply their methods to determine all imaginary quadratic fields with class number 2, their methods did not show us a way to tackle the general problem. In this direction, Goldfeld [Gol76] took a major step in 1976 when he related this problem to L-series attached to elliptic curves. Without going into too much detail, Goldfeld showed that if there is an elliptic curve E over $\mathbb{Q}$, whose associated L-series, $L_E(s)$ is entire and has a triple order zero at the point $s = 1/2$, then for any $\epsilon > 0$, there is an effectively computable constant $c(\epsilon) > 0$ such that

$$h(-d) > c(\epsilon)(\log d)^{1-\epsilon}.$$

In 1986, Gross and Zagier [GrZa86] showed that such an elliptic curve exists and thus completed the search for an effective theorem.

3. Class numbers of real quadratic fields

In his work on class numbers, Gauss also conjectured that there are infinitely many real quadratic fields with class number one. This conjecture is still unresolved as of today. Let $K = \mathbb{Q}(\sqrt{d})$, with $d > 1$ and square-free, and ϵ_d be the fundamental unit of K. The class number formula gives us

$$h(d) \log \epsilon_d = \sqrt{d_K} L(1, \chi).$$

In this case, the difficulty arises because it is not possible to separate the factor $\log \epsilon_d$ while finding bounds for $h(d)$. One may however consider real quadratic fields with a small fundamental unit. More precisely, one can consider real quadratic fields such that $\epsilon_d \asymp \log d$. In such cases, we get the existence of only finitely many $d > 0$ such that $h(d) = 1$, a result which mirrors the situation for imaginary quadratic fields.

It is not even known if there are infinitely many algebraic number fields with class number 1. There are some intriguing conjectures in this context. Let $\mathbb{B}_{p,n}$ denote the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, that is, the unique real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$ for odd primes p, and $\mathbb{Q}\left(\cos\left(\frac{2\pi}{2^{n+2}}\right)\right)$ for $p = 2$. Let $h_{p,n}$ be the class number of $\mathbb{B}_{p,n}$. In [Web1886], Weber showed that $h_{2,n}$ is odd for all $n \geq 1$. Subsequently, Iwasawa [Iwa56] generalized Weber's result to show that for all $n \geq 1$, the class number $h_{p,n}$ is not divisible by p. Then, in [FKM14], Fukuda and Komatsu proved that $h_{2,n}$ is not divisible by any prime less than 10^9. This led to the following conjecture, often called Weber's class number problem:

Conjecture 1. *Foe every positive integer n, the class number $h_{2,n}$ is 1.*

In [Co60], Cohn proved that $h_{2,3} = 1$. Since then many special cases have been verified to be true [Bau69, vdLin82, Mil15, Mil14] but the conjecture still remains elusive in general. Miller has conjectured that even a stronger statement should be true [Mil15] (see also [Coa12]):

Conjecture 2. *For any prime p and positive integer n, the class number $h_{p,n}$ is 1.*

Some progress in this direction was made by Buhler, Pomerance and Robertson [BPR04] who used an extension of Cohen-Lenstra heuristics (see Section 4. for details) to estimate the probability that $h_{p,n} > 1$. Consequently, they were led to the following conjecture.

Conjecture 3. *Let p be a prime and n be a positive integer. For all but finitely many pairs (p, n), the class number of the real cyclotomic field of conductor p^{n+1} is equal to the class number of the real cyclotomic field of conductor p^n. That is,*

$$h\left(\mathbb{Q}\left(\zeta_{p^{n+1}} + \zeta_{p^{n+1}}^{-1}\right)\right) = h\left(\mathbb{Q}\left(\zeta_{p^n} + \zeta_{p^n}^{-1}\right)\right).$$

Returning to quadratic fields, let $p = m^2 + 1$ be a prime and consider $\mathbb{Q}(\sqrt{p})$. In [ChFr76], Chowla and Friedlander conjectured that $m = 26$ is the largest value for which $h(p) = 1$. In other words, $h(p) > 1$ for $p > 677$. Mollin and Williams [MolWil88] proved this conjecture using the Generalized Riemann Hypothesis (GRH). They numerically verified that $h(p) > 1$ for $677 < p < 10^{13}$ and used a result of Cornell and Washington[CorWa85] which guarantees, under the assumption of GRH for the Dedekind zeta function of $\mathbb{Q}(\sqrt{p})$, that $h(p) > 1$ for $p > 10^{13}$. In [Bir03a], Biro provided an unconditional proof that $h(4m^2 + 1) > 1$ for $m > 13$. Let m be an odd, positive integer and $d = m^2 + 4$ be square-free. In [Bir03b], Biro also proved the so-called Yokoi conjecture, which states that $h(d) > 1$ for $m > 17$.

In [BKL07], Byeon, Kim and Lee prove that $h(\sqrt{n^2 - 4}) > 1$ for $n > 21$. Then, Byeon and Lee [ByeLee08] proved that there are exactly four quadratic fields of the form $\mathbb{Q}(\sqrt{m^2 + 1})$ with class number equal to 2.

4. Cohen-Lenstra Heuristics

In 1984, Cohen and Lenstra [CoLe84] made a number of conjectures about the structure of the class group and divisibility properties of class numbers of real and imaginary quadratic fields based on certain numerical computations. Let K be a quadratic field and $\mathfrak{C}_K^*$ be the odd part of the class group $\mathfrak{C}_K$, that is, the subgroup of ideal classes with odd orders. Given a finitely generated abelian group A and a prime p, define the *p-rank* of A as $\mathrm{Rk}_p(A) = \dim_{\mathbb{F}_p}(A/A^p)$. It is essentially the number of invariant factors of the p-part of A. Following [FouKlu06], if f is a real-valued function on the set of positive or negative discriminants d_K, we say that $f(d_K)$ has *average value* $a \in \mathbb{R}$ if, as $x \to \infty$, we have

$$\sum_{0<\pm d_K<x} f(d_K) = (a + o(1)) \sum_{0\pm d_K<x} 1.$$

In the case of imaginary quadratic fields, Cohen and Lenstra predict the following:

Conjecture 4. (Cohen-Lenstra) *Let K be an imaginary quadratic field and p be an odd prime. Then,*

(i) The probability that $p|h_K$ is

$$1 - \prod_{j=1}^{\infty}\left(1 - \frac{1}{p^j}\right).$$

(ii) The probability that $\mathrm{Rk}_p(\mathfrak{C}_K^*) = r$ *is*

$$p^{-r^2} \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^j}\right) \prod_{1 \leq k \leq r} \left(1 - \frac{1}{p^k}\right)^{-2}.$$

(iii) For a non-negative integer α*, the average value of*

$$\prod_{0 \leq i < \alpha} \left(p^{\mathrm{Rk}_p(\mathfrak{C}_K^*)} - p^i\right)$$

is one. In particular, the average value of $p^{\mathrm{Rk}_p(\mathfrak{C}_K^*)}$ *is two and that of* $p^{2\mathrm{Rk}_p(\mathfrak{C}_K^*)}$ *is* $p + 2$.

Due to the celebrated work of Davenport and Heilbronn [DavHei71], Conjecture 4(iii) is known to be true in the case $\alpha = 1$ and $p = 3$. They proved the following theorem on the number of 3-torsion elements in the class groups of quadratic fields with bounded discriminants.

Theorem 5. (Davenport and Heilbronn) *Let* d_K *denote the discriminant of a quadratic field* K *and* $\mathfrak{C}_3(K)$ *be the* 3*-torsion subgroup of the ideal class group* $\mathfrak{C}_K$*. Then*

$$\sum_{0 < d_K < x} \#\mathfrak{C}_3(K) = \frac{4}{3} \cdot \sum_{0 < d_K < x} 1 + o(x);$$
$$\sum_{-x < d_K < 0} \#\mathfrak{C}_3(K) = 2 \cdot \sum_{-x < d_K < 0} 1 + o(x).$$

It follows that the average value of $3^{\mathrm{Rk}_3(\mathfrak{C}_K^*)}$ is 2. In [BST13], Bhargava, Shankar and Tsimermann provided a simple proof of Theorem 5 and a precise form of the second main term. Other than these results, almost nothing is known about Conjecture 4 (except in the trivial case $\alpha = 0$ and any p). In the case of real quadratic fields, Cohen and Lenstra conjecture the following.

Conjecture 6. (Cohen-Lenstra) *Let* K *be a real quadratic field and* p *be an odd prime. Then,*

(i) The probability that $p | h_K$ *is*

$$1 - \prod_{j=2}^{\infty} \left(1 - \frac{1}{p^j}\right).$$

(ii) The probability that $\mathrm{Rk}_p(\mathfrak{C}_K^*) = r$ *is*

$$p^{-r(r+1)} \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^j}\right) \prod_{1 \leq k \leq r} \left(1 - \frac{1}{p^k}\right)^{-1} \prod_{1 \leq k \leq r+1} \left(1 - \frac{1}{p^k}\right)^{-1}.$$

(iii) For a non-negative integer α*, the average value of*

$$\prod_{0 \leq i < \alpha} \left(p^{\mathrm{Rk}_p(\mathfrak{C}_K^*)} - p^i\right)$$

is $p^{-\alpha}$*. In particular, the average value of* $p^{\mathrm{Rk}_p(\mathfrak{C}_K^*)}$ *is* $1 + p^{-1}$ *and that of* $p^{2\mathrm{Rk}_p(\mathfrak{C}_K^*)}$ *is* $2 + p^{-1} + p^{-2}$.

Again, by the work of Davenport and Heilbronn [DavHei71], Conjecture 6 (iii) is known to be true for $\alpha = 1$ and $p = 3$. In [Ger87], Gerth has extended the Cohen-Lenstra conjectures to include the case $p = 2$ by considering the group $\mathfrak{C}_K^2 := \{a^2 : a \in \mathfrak{C}_K\}$ and in [FouKlu07], Fouvry and Kluners have proved the corresponding modifications of Conjecture 1(iii) and Conjecture 2(iii) in the case $p = 2$ and $\alpha \geq 0$,

5. Divisibility of class numbers

5.A. Quantitative results

Cohen and Lenstra predict that the quadratic fields with class number divisible by n should have positive density among all quadratic fields. To state quantitative results in this direction, for a square-free positive integer d, we define

$$N_n(x) = \#\{d : \ n|h(-d), \text{ and } |d_K| \le x\}.$$

Then, according to Cohen-Lenstra heuristics, we must have

$$N_n(x) \sim c_n x$$

for a positive constant c_n. In particular, for an odd prime p they predict that

$$c_p = \begin{cases} \frac{6}{\pi^2}\left(1 - \prod_{j=2}^{\infty}\left(1 - \frac{1}{p^j}\right)\right), & \text{real quadratic fields} \\ \frac{6}{\pi^2}\left(1 - \prod_{j=1}^{\infty}\left(1 - \frac{1}{p^j}\right)\right), & \text{imaginary quadratic fields.} \end{cases}$$

In [Mur97], Ram Murty proved, using the ABC conjecture, that for an integer $g \ge 3$, at least $\gg x^{1/g-\epsilon}$ imaginary quadratic fields with absolute discriminant $\le x$ have an element of order g in their class group. That is, $N_g(x) \gg x^{1/g-\epsilon}$. In the real quadratic case, he found a lower bound of $N_g(x) \gg x^{1/(2g)-\epsilon}$ for such quadratic fields. Later in [Mur99], Murty gave stronger results without using the ABC conjecture. He proved that $N_g(x) \gg x^{\frac{1}{2}+\frac{1}{g}}$ for $g \ge 3$. For real quadratic fields, he proved that $N_g(x) \gg x^{\frac{1}{2g}-\epsilon}$ for any ϵ, and g odd, where the implied constant may depend on ϵ.

For imaginary quadratic fields, Soundararajan [Sou00] improved Murty's bounds to $N_g(x) \gg x^{\frac{1}{2}+\frac{2}{g}-\epsilon}$ when $g \equiv 0 \pmod 4$ and $N_g(x) \gg x^{\frac{1}{2}+\frac{3}{g+2}-\epsilon}$ when $g \equiv 2 \pmod 4$. Note that his result contains bounds for $N_d(x)$ when d is odd since $N_g(x) \ge N_{2g}(x)$. In these results, the exponent is still asymptotic to $\frac{1}{2}$ as g goes to infinity. Some substantially new idea is needed to break through the "$\frac{1}{2}$" barrier in this problem.

In the case of real quadratic fields, Murty's bounds were improved by Luca [Luc03] to $N_g(x) \gg x^{\frac{1}{g}}/\log x$ for g even and by Yu [Yu02] to $N_g(x) \gg x^{\frac{1}{g}-\epsilon}$ for g odd. Inspite of these encouraging results, we seem to be still far away from any resolution of the Cohen-Lenstra conjectures.

5.B. Certain infinite families of quadratic fields

We first consider the following family of quadratic fields. For an integer $n > 1$ let

$$K_{x,y,n} := \mathbb{Q}\left(\sqrt{x^2 - y^n}\right), \quad x, y \in \mathbb{Z}.$$

In [AnCh55] Ankeny and Chowla studied the family $K_{x,3,n}$ and proved the following result.

Theorem 7. (Ankeny-Chowla) *Let n be an even positive integer and let $d := x^2 - 3^n < 0$ be a square-free integer with x even and $0 < x < \sqrt{2 \cdot 3^{n-1}}$, then n divides the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$.*

In [GrRoh78], Gross and Rohrlich proved that the class number of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{1 - 4a^n}\right)$ is divisible by n for any odd integer $n \ge 3$ and any integer $a \ge 2$. In the case of real quadratic fields, a similar result was obtained by Ichimura [Ich03], who showed that the class number of $\mathbb{Q}\left(\sqrt{a^{2n} + 4}\right)$ is divisible by any integer $n \ge 2$ and any odd integer $a \ge 3$. Cohn [Cohn01] proved that for $n > 2$ and $n \ne 6$, the class number of $K_{1,2,n}$ is divisible by $(n-2)$ if $2^n - 1$ is not a square. In [Ki09], Kishi proved that, for $x = 2^k$, $k \ge 1$, Theorem 7 is true for all n such that $2^{2k} < 3^n$. Kishi

[Ki10] also proved that if $n \geq 3$ is odd then the class number of $K_{2,3,n}$ is divisible by 3. Subsequently, there have been further generalisations of these results by Ito [Ito11] as well as Chakraborty, Hoque, Kishi and Pandey [CHKP18]. An important ingredient in these proofs is a result by Bugeuad and Shorey [BugSh01] on the number of solutions in positive integers of the generalized Ramanujan-Nagell equation.

6. Non-divisibility of class numbers of quadratic fields

6.A. Imaginary quadratic fields

It follows from Gauss' genus theory that there are infinitely many imaginary quadratic fields with class number not divisible by 2. In [Har74], Hartung showed that given an odd prime p, there are infinitely many imaginary quadratic fields K for which $p \nmid h_K$. To state further results in this direction, we require the following terminology. Let p be a fixed prime and let $\mathbb{Z}_p$ be the p-adic integer ring. Let K be a finite algebraic number field with class number h_K. Further, we denote by $\lambda_p(K)$ and $\mu_p(K)$ respectively, the Iwasawa λ- and $\mu-$invariants associated to the basic $\mathbb{Z}_p$ extension over K (see [Mur02] for more details). In [Hor87], Horie used a modification of Hartung's approach to prove that given a prime p, there are infinitely many imaginary quadratic fields K for which $p \nmid h_K$ and in which p is not split. It then follows from Iwasawa's criterion [Iwa56] that there exist infinitely many imaginary quadratic fields K with $\lambda_K = \mu_K$. The proof is based on the Eichler-Selberg trace formula as well as the p-adic Galois representation associated to the Jacobian of the modular curve $X_0(p)$.

Let p be a prime number and let P_1, P_{-1} and P_0 be finite mutually disjoint subsets of the set of primes numbers such that $2 \notin P_1 \cup P_{-1}$. In [Hor90], Horie proved that for sufficient large p, there exist infinitely many imaginary quadratic fields K such that $p \nmid h_K$ and $\left(\frac{d_K}{m}\right) = j$ for $m \in P_j$, $j = \{0, 1, 2\}$. Here $\left(\frac{\cdot}{\cdot}\right)$ is the usual Legendre symbol. Next, let $\epsilon = -1, 0$ or 1. In [HorOni88], Horie and Onishi proved that, given a prime $p \geq 5$, there exist infinitely many imaginary quadratic fields K such that $p \nmid h_K$ and $\left(\frac{d_K}{p}\right) = \epsilon$.

In [KoOno99], Kohnen and Ono proved that for a prime $p > 3$ and $\epsilon > 0$, the following lower bound exists for the number of quadratic fields whose class number is not divisible by p and whose absolute discriminant is less than x.

$$\#\left\{-x < -d < 0 \text{ fundamental } : p \nmid h(-d)\right\} \geq \left(\frac{2(p-2)}{\sqrt{3}(p-1)} - \epsilon\right) \frac{\sqrt{x}}{\log x}.$$

6.B. Real quadratic fields

By the work of Davenport and Heilbronn [DavHei71], it is know that for $\epsilon > 0$, we have

$$\frac{\#\{0 < d < x : \ 3 \nmid h(d)\}}{\#\{0 < d < x\}} \geq \frac{5}{6} - \epsilon.$$

The non-divisibility of class number of real quadratic fields K is closely related to the Greenberg conjecture which says that for every prime p and totally real number field K, we must have $\lambda_p(K) = 0 = \mu_p(K)$. From the work of Ferrero and Washington, it is know that for $K = \mathbb{Q}(\sqrt{d})$ we have $\mu_p(K) = 0$. However, the conjecture that $\lambda_p(\mathbb{Q}(\sqrt{d})) = 0$ has not been resolved yet. In this direction, Ono [Ono99] and Byeon [Bye01] have shown that for each prime p, there exist infinitely many real quadratic fields $\mathbb{Q}(\sqrt{d})$ such that $\lambda_p(\mathbb{Q}(\sqrt{d})) = 0$.

Our short survey should convince the reader that this topic is a fertile area of research with many open questions. It is a confluence of several branches of number theory that will inspire further investigation for generations to come.

Acknowledgement. We thank the referee for helpful comments on an earlier version of this paper.

References

[AnCh55] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324.

[Bak71] A. Baker, *On the class number of imaginary quadratic fields*, Bulletin of the American Math. Society **77** (1971), 678–684.

[Bau69] H. Bauer, *Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkrper*, J. Number Theory **1** (1969), 161–162.

[BelFou99] K. Belabas and E. Fouvry, *On the 3-rank of quadratic fields with prime or almost prime discriminant*, Duke Math. J. **98** (1999), 217–268.

[BST13] M. Bhargava, A. Shankar and J. Tsimermann, *On the Davenport-Heilbronn theorems and second order terms. (English summary)*, Invent. Math. **193** (2013), 439–499.

[Bir03a] A. Biró, *Chowla's conjecture*, Acta Arith. **107** (2003), 179–194.

[Bir03b] A. Biró, *Yokoi's conjecture*, Acta Arith. **106** (2003), 85–104.

[BugSh01] Y. Bugeaud and T. N. Shorey, *On the number of solutions of the generalized Ramanujan-Nagell equation*, J. Reine Angew. Math. **539** (2001), 55–74.

[BPR04] J. Buhler, C. Pomerance, and L. Robertson, *Heuristics for class numbers of prime-power real cyclotomic fields*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, in: Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 149–157.

[Bye01] D. Byeon. *Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields*, Compositio Math. **126** (2001), 249–256.

[BKL07] D. Byeon, M. Kim and J. Lee, *Mollin's conjecture*, Acta Arith. **126** (2007), 99–114.

[ByeLee08] D. Byeon, J. Lee, *Class number 2 problem for certain real quadratic fields of Richaud-Degert type*, J. Number Theory **128** (2008), 865–883.

[CHKP18] K. Chakraborty, A. Hoque, Y. Kishi and P. P. Pandey, *Divisibility of the class numbers of imaginary quadratic fields*, J. Number Theory **185** (2018), 339–348.

[CoLe84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Lecture Notes in Mathematics 1068 (Springer, 1984), 33–62.

[Co60] H. Cohn, *A numerical study of Weber's real class number of calculation I*, Numer. Math. **2** (1960), 347–362.

[Cohn01] J. E. H. Cohn, *On the class number of certain imaginary quadratic fields*, Proc. Amer. Math. Soc. **130** (2001), 1275–1277.

[ChFr76] S. Chowla and J. Friedlander, *Class numbers and quadratic residues*, Glasgow Math. J. **17** (1976), 47–52.

[Coa12] J. Coates, *The enigmatic Tate-Shafarevich group*, Fifth International Congress of Chinese Mathematicians, Parts 1, 2, in: AMS/IP Stud. Adv. Math. vol. 2, 51, pt. 1, Amer. Math. Soc., Providence, RI, 2012, pp. 43–50.

[CorWa85] G. Cornell and L. C. Washington, *Class numbers of cyclotomic fields*, J. Number Theory **21** (1985), 260–274.

[Dav80] H. Davenport, *Multiplicative Number Theory, Graduate Texts in Mathematics*, **74**, Second edition, Springer-Verlag, 1980.

[DavHei71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.

[FeWa79] B. Ferrero and L. C. Washington, *The Iwasawa invariants λ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[FouKlu06] E. Fouvry and J. Kluners, *Cohen-Lenstra heuristics of quadratic number fields*, Algorithmic number theory, 40–55, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006.

[FouKlu07] E. Fouvry and J. Kluners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), 455–513.

[FKM14] T. Fukuda, K. Komatsu and T. Morisawa, *Weber's class number one problem*, Iwasawa Theory 2012, in: Contrib. Math. Comput. Sci., vol. 7, Springer, Heidelberg, 2014.

[Ger87] F. Gerth Ill, *Extension of conjectures of Cohen and Lenstra*, Expo. Math. **5** (1987), 181–184.

[Gol76] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Sc. Norm. Super. Pisa **3** (1976), 623–663.

[GrZa86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Inventiones Math. **84** (1986), 225–320.

[GrRoh78] B. H. Gross and D. E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201–224.

[Har74] P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3*, J. Number Th. **6** (1974), 276–278.

[HerLu04] S. Hernndez and F. Luca, *Divisibility of exponents of class groups of pure cubic number fields*, High primes and misdemeanours: Lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., 41, Amer. Math. Soc., Providence, RI, 2004, pp. 237–244.

[Hers36] A. Herschfeld, *The equation* $2^x - 3^y = d$, Bull. Amer. Math. Soc. **42** (1936), 231–234.

[Hor87] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. **88** (1987), 31–38.

[Hor90] K. Horie, *Trace formulae and imaginary quadratic fields*, Math. Ann. **288** (1990), 605–612.

[HorOni88] K. Horie and Y. Onishi, *The existence of certain infinite families of imaginary quadratic fields*, J. Reine und ange. Math. **390** (1988), 97–133.

[Ich03] H. Ichimura, *Note on the class numbers of certain real quadratic fields*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 281–288.

[Ito11] A. Ito, *Remarks on the divisibility of the class numbers of imaginary quadratic fields* $\mathbb{Q}\sqrt{2^{2k} - q^n}$, Glasgow Math. J. **53** (2011), 379–389.

[Iwa56] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[Ki09] Y. Kishi, *Note on the divisibility of the class number of certain imaginary quadratic fields*, Glasgow Math. J. **51** (2009), 187–191.

[Ki10] Y. Kishi, *On the ideal class group of certain quadratic fields*, Glasgow Math. J. **52** (2010), 575–581.

[KoOno99] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387–398.

[Mol96] R. A. Mollin, *Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields*, Glasgow Math. J. **38** (1996), 195–197.

[MolWil88] R. A. Mollin and H. C. Williams, *A conjecture of S. Chowla via the generalized Riemann hypothesis*, Proc. Amer. Math. Soc. **102** (1988), 794–796.

[Luc03] F. Luca, *A note on the divisibility of class numbers of real quadratic fields*, C. R. Math. Acad. Sci. Soc. R. Can. **25** (2003), 71–75.

[Mil15] J. C. Miller, *Class numbers in cyclotomic* $\mathbb{Z}_p$*-extensions*, J. Number Theory **150** (2015), 47–73.

[Mil14] J. C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, Acta Arith. **164** (2014), 381–398.

[Mur97] M. Ram Murty, *The ABC conjecture and exponents of quadratic fields*, Cont. Math. **210** (1997), pp. 85–95, in Number Theory, edited by V. Kumar Murty and Michel Waldschmidt, Amer. Math. Soc., Providence.

[Mur99] M. Ram Murty, *Exponents of class groups of quadratic number fields*, Topics in Number Theory (University Park, PA, 1997) Kluwer Acad. Publ., Dordrecht (1999), 229–239.

[Mur02] M. Ram Murty, *Introduction to p-adic analytic number theory*, AMS/IP Studies in Advanced Mathematics, 27. American Mathematical Society, Providence, RI; International Press, Somerville, MA, 2002.

[Ono99] K. Ono, *indivisibility of the class numbers of real quadratic fields*, Composito Math. **199** (1999), 1–11.

[OnoSki98] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651–660.

[Sou00] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. **61** (2000), 681–690.

[St66] H. M. Stark, *On complex quadratic fields with class-number equal to one*, Transactions of the Amer. Math. Society **122** (1966), 112–119.

[vdLin82] F. J. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), 693–707.

[Web1886] H. Weber, *Theorie der Abel'schen Zahlkrper*, Acta Math. **8** (1886), 193–263.

[Yu02] G. Yu, *A note on the divisibility of class numbers of real quadratic fields*, J. Number Theory **97** (2002), 35–44.

Ajit Bhand
Department of Mathematics
Indian Institute of Science Education and Research Bhopal
Bhopal Bypass Road, Bhauri, Bhopal 462 066
Madhya Pradesh, India
e-mail: abhand@iiserb.ac.in

M. Ram Murty
Department of Mathematics and Statistics
Queen's University, Kingston
Ontario, Canada, K7L 3N6
e-mail: murty@queensu.ca