MATHEMATICA, 64 (87), N° 1, 2022, pp. 9–13

LEAST PRIMES WHICH SPLIT IN IMAGINARY QUADRATIC FIELDS

SAKHA A. ALKABOUSS, BOUALEM BENSEBA, OMAR KIHEL, and JESSE LARONE

Abstract. In this paper, we bound the least primes which split in an imaginary quadratic field in terms of its class number.

MSC 2010. Primary 11D85; Secondary 11Y50.

Key words. Class number, splitting primes, quadratic fields.

1. INTRODUCTION

In his treatise Disquistiones Arithmeticase, Gauss presented his class number problem. For a given positive integer n, this problem asks for a list all imaginary quadratic fields with class number n, although the original problem was stated in the language of binary quadractic forms. Gauss conjectured that $h(D)$, the number of classes of primitive positive definite quadratic forms of discriminant D, tends to infinity as $-D$ does.

This problem has a very long history, and it has been the main subject of research in works of many authors. Heilbronn [9] ineffectively resolved the general problem. Gauss's class number one problem, which refers to the case $n = 1$, was proved first by Heegner [8], although the proof contains some minor gaps. It was proved later by Baker [1] and Stark [12], who then jointly solved the problem for $n = 2$ [2].

Goldfeld [6] showed that the problem can be reduced to the existance of an elliptic curve with a Hasse-Weil L-function possessing a zero of order 3 at $s = 1$. Gross and Zagier [7] proved the existance of such an elliptic curve, reducing the problem to a finite number of computations. Oesterlé [11] generalised Goldfeld's theorem to the solve the problem for $n = 3$. Watkins [13] then modified Goldfeld's approach by considering Dirichlet L-functions possessing zeroes near the real line with low height, which solved the problem for $n \leq 100$.

Beckwith [3] provided an estimate for the number of negative fundamental discriminants whose corresponding class numbers $h(D)$ are indivisible by a given prime and whose imaginary quadratic fields satisfy a given set of local conditions.

The authors would like to thank the anonymous referees for their comments. The third author was supported by NSERC.

DOI: 10.24193/mathcluj.2022.1.02

Lamzouri, Li, and Soundararajan [10] proved, among other results, upper and lower bounds for $L(1,\chi)$ and $\zeta(1+it)$. They also deduced explicit bounds for the class number of imaginary quadratic fields assuming the generalised Riemann hypothesis.

The problem of bounding the smallest rational prime which splits in a number field has been previously explored. For example, Siegel's bound on the size of class numbers implies that $|D|^{1/2-\epsilon} \ll h(D) \ll |D|^{1/2+\epsilon}$, as discussed in [5]. Combined with the prime number theorem, one obtains that the h_K-th prime is asymptotically greater than $|D|^{1/2-\epsilon}\log|D|$.

The aim of this paper is to provide a lower bound on the least primes that split in an imaginary quadratic field in terms of its class number.

2. PRELIMINARY RESULTS

We first recall some terminology regarding quadratic forms. A binary quadratic form is given by

$$f(X,Y) = aX^2 + bXY + cY^2$$

for integers a, b, and c and discriminant $D = b^2 - 4ac$. An integer m is said to be represented by the quadratic form $f(X,Y)$ if and only if there exist integers x and y such that $m = f(x,y)$, and the representation is said to be proper if $\gcd(x,y) = 1$.

We will be interested only in positive definite quadratic forms, that is, those with negative discriminant and which represent only positive integers. Furthermore, we say that the quadratic form is primitive if and only if we have $\gcd(a,b,c) = 1$. Two forms $f(X,Y)$ and $g(X,Y)$ are said to be equivalent if there exist integers α,β,γ, and δ such that $f(X,Y) = g(\alpha X + \beta Y, \gamma X + \delta Y)$ and $\alpha\delta - \gamma\beta = \pm 1$. It is clear that this is an equivalence relation, that equivalent forms represent the same integers, and that equivalent forms have the same discriminant. The equivalence is said to be proper if $\alpha\delta - \gamma\beta = 1$, and we say that two forms are in the same class if and only if they are properly equivalent. Lastly, we recall that a primitive positive definite quadratic form $aX^2 + bXY + cY^2$ is reduced if $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

We will require the following four results, all of which can be found in Cox [4].

LEMMA 2.1. *Let $f(X,Y) = aX^2+bXY+cY^2$ be a reduced primitive positive definite quadratic form. Then, for any integers x and y,*

$$f(x,y) \geq (a - |b| + c)\min(x^2, y^2)\,.$$

LEMMA 2.2. *Let $f(X,Y) = aX^2+bXY+cY^2$ be a reduced primitive positive definite quadratic form. Then*

$$a \leq \sqrt{\frac{|D|}{3}}\,.$$

THEOREM 2.3. *Every primitive positive definite quadratic form is properly equivalent to a unique reduced quadratic form.*

Since we will be considering forms which are reduced with a fixed discriminant $D < 0$, we immediately have the fourth result due to Lemma 2.2 and Theorem 2.3:

THEOREM 2.4. *Let $D < 0$ be given. Then the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and it is equal to the number of reduced forms of discriminant D.*

3. MAIN RESULT

We prove the following theorem:

THEOREM 3.1. *Let $D < 0$ be an integer satisfying $D \equiv 0$ or $1 \pmod 4$, let $K = \mathbb{Q}(\sqrt{D})$, and let h_K the class number of K. If the least $h_K + 1$ odd prime numbers which split in K are denoted by $p_1, p_2, \ldots, p_{h_k+1}$ with $p_1 < p_2 < \cdots < p_{h_K+1}$, then*

$$p_{h_K+1} > \frac{1}{4}\sqrt{3|D|}\,.$$

Proof. Note that if $|D| < 23$, then the result holds trivially since

$$\frac{1}{4}\sqrt{3|D|} < 2.1\,.$$

As such, we assume in what follows that $|D| \geq 23$.

If p is an odd prime which splits in K, then $\left(\frac{D}{p}\right) = 1$, and p can be represented by a proper quadratic form of discriminant D. Hence, it can be represented by a positive definite quadratic form of discriminant $D < 0$ and, consequently, also by a reduced quadratic form of discriminant $D < 0$.

There exist h_K reduced forms of discriminant D. Of the $h_K + 1$ least prime numbers which do not split in K, at least two of them are then represented by the same reduced quadratic form of discriminant D. We let p_i and p_j be these two primes and $f(X, Y) = aX^2 + bXY + cY^2$ the form which represents them both. We additionally assume without loss of generality that $p_i < p_j$.

The form $f(X, Y)$ satisfies the conditions of Lemma 2.1, so for integers x and y we have $f(x, y) \geq (a - |b| + c)$, whenever $xy \neq 0$. Additionally, we have $|b| \leq a$ since $f(X, Y)$ is reduced. Thus, $f(x, y) \geq c$. If $|b| = c$, then we have $c = a = 1$. This imposes $|b| = c = 1$, so that

$$D = b^2 - 4ac = -3a^2 = -3.$$

Since we assume that $|D| \geq 23$, we must instead have $|b| \neq c$, in which case we have $f(x, y) \geq c$ and $f(x, y) > a$ whenever $xy \neq 0$. For $xy = 0$, we consider each possibility seperately. First, if $x = y = 0$ we have $f(0, 0) = 0$. Next, if $x = 0$ and $y \neq 0$, we have $f(0, y) = cy^2 \geq c$. Finally, if $x \neq 0$ and $y = 0$, we

have $f(x,0) = ax^2 \geq a$. Altogether, we have shown that the smallest positive integer that $f(x,y)$ may take is a, while the second smallest is c.

Since the smallest positive integer representable by $f(X,Y)$ is a, we have $p_i \geq a$. Since the second smallest positive integer representable by $f(X,Y)$ is c, and since $p_j > p_i$ is representable by $f(X,Y)$, we deduce that $p_j \geq c$.

The discriminant of f satisfies $D = b^2 - 4ac < 0$, so $-D = 4ac - b^2 > 0$. By Lemma 2.2, we have $a \leq \sqrt{\frac{|D|}{3}}$, hence

$$|D| = -D \leq 4c\sqrt{\frac{|D|}{3}}.$$

Therefore, we have

$$\frac{1}{4}\sqrt{3|D|} \leq c \leq p_j \leq p_{h_K+1}.$$

The left-most expression in the above inequality cannot be an integer, so we conclude that $\frac{1}{4}\sqrt{3|D|} < p_{h_K+1}$ as claimed. □

Example 3.2. Consider the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-163})$ which has class number $h_K = 1$. Let p_1 and p_2 be the two least odd prime numbers which split in K. If $p_1 < p_2$, then Theorem 3.1 asserts that $p_2 \geq \frac{1}{4}\sqrt{3(163)} \approx 5.528$. It is readily verified that each of the primes 2, 3, and 5 are in fact inert: $\mathcal{O}_K = \mathbb{Z}\left[\frac{-1+\sqrt{-163}}{2}\right]$ and each of the ideals (2), (3), and (5) are prime ideals of $\mathcal{O}_K$.

REFERENCES

[1] A. Baker, *Linear forms in the logarithm of algebraic number I, II, III*, Mathematika, **13** (1966), 204–216; ibid. **14** (1967), 102–107; ibid. **14** (1967), 220–228.

[2] A. Baker and H. Stark, *On a fundamental inequality in number theory*, Ann. of Math., **94** (1971), 190–199.

[3] O. Beckwith, *Indivisibility of class numbers of imaginary quadratic fields*, Res. Math. Sci., **4** (2017), Article 20, 1–11.

[4] D.A. Cox, *Primes of the Form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons, New Tork, 1989.

[5] H. Davenport, *Multiplicative Number Theory*, Third ed., Graduate Texts in Mathematics, Vol. 74, Springer-Verlag, New York, 2000.

[6] D. Goldfeld, *Gauss's class number problem of imaginary quadratic fields*, Bull. Amer. Math. Soc., **13** (1985), 23–37.

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

[8] K. Heegner, *Diophantische analysis und modulfunktionen*, Math. Z., **56** (1952), 227–253.

[9] H. Heilbronn, *On the class number in imaginary quadratic fields*, Q. J. Math., **5** (1934), 150–160.

[10] Y. Lamzouri, X. Li, and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp., **84** (2015), 907–938.

[11] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Seminaires Nicolas Bourbaki, Astérisque, **121-122** (1985), 309–323.

[12] H. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J., **14** (1967), 1–27.
[13] M. Watkins, *Class number of imaginary quadratic field*, Math. Comp., **73** (2003), 907–938.

Received March 8, 2020
Accepted May 12, 2021

Université Cheikh Anta Diop
Departement de Mathematiques
Sénégal
E-mail: sakha.alkabouss@ucad.edu.sn

Université des Sciences et de
la Technologie Houari Boumediene
Faculté de Mathematiques
Algiers, Algeria
E-mail: b.benseba@usthb.dz

Brock University
Department of Mathematics and Statistics
St. Catharines, Canada
E-mail: okihel@brocku.ca
E-mail: jlarone@brocku.ca