ON COMPUTATIONS OF SHANKS AND SCHMID

DAVID BRINK, PIETER MOREE AND ROBERT OSBURN

Abstract. In 1966, Shanks and Schmid investigated the asymptotic behavior of the number of positive integers less than or equal to x which are represented by the quadratic form X^2+nY^2, $n \geq 1$. Based on some numerical computations, they observed that the constant occurring in the main term appears to be the largest for $n=2$. In this paper, we prove that in fact this constant is unbounded as one runs through fundamental discriminants with a fixed number of distinct prime divisors.

1. Introduction

Let $f(X,Y) = aX^2+bXY+cY^2$ be a primitive integral binary quadratic form with discriminant $D = b^2-4ac$ and $B_f(x)$ count the number of positive integers $m \leq x$ which are represented by f. The problem of estimating $B_f(x)$ has attracted considerable attention over time. It is a classical result of Landau [9] that for $f(X,Y) = X^2+Y^2$,

$$B_f(x) \sim C(-4)\frac{x}{\sqrt{\log x}} \tag{1}$$

as $x \to \infty$. Here $C(-4)$ is an explicit constant, now called the Landau-Ramanujan constant, given by

$$C(-4) = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod 4} \left(\frac{1}{1-1/p^2}\right)^{1/2} = 0.78422365\ldots$$

Landau's result shows the asymptotical correctness of a later claim of Ramanujan who in his first letter to Hardy in 1913 stated he could prove that

$$B_f(x) = C(-4)\int_2^x \frac{dt}{\sqrt{\log t}} + O(x^{1/2+\epsilon}).$$

However, Shanks [12] showed that the latter error term is too optimistic and has to be replaced by $O(x\log^{-3/2}x)$.

Paul Bernays was a doctoral student of Landau's at Göttingen. In his 1912 thesis, he proved the following generalization of (1) (see page 59 and 115-116 in [2]). Namely, given a binary quadratic form f of discriminant D, we have

$$B_f(x) \sim C(D)\frac{x}{\sqrt{\log x}} \tag{2}$$

Date: March 8, 2010.

2000 *Mathematics Subject Classification.* Primary: 11E16, 11M20.

as $x \to \infty$.

In 1966, Shanks and Schmid [13] studied the family of binary quadratic forms $f(X,Y) = X^2 + nY^2$ and used indirect methods to compute $C(-4n)$ for $1 \le n \le 14$ and $n = 16, 20, 24, 27, 64, 96$ and 256. Specifically, we have the following table

n	b_n	b'_n
1	0.764223654	0.764223653589220662990698731 1
2	0.872887558	0.8728875581309146129200636834
3	0.638909405	0.6389094054453438822549426747
4	0.573167740	0.5731677401919154972430240483
5	0.535179999	0.5351799988649545413027199090
6	0.558357114	0.5583571140895246274460701041
7	0.543539641	0.5435396411014846926771211300
8	0.436443779	0.4364437790654573064600318417
9	0.424568696	0.4245686964384559238837215172
10	0.473558100	0.4735580999381557098419651553
11	≈ 0.677	0.6773880181341740551427831009
12	0.399318378	0.3993183784033399264093391717
13	≈ 0.420	0.4207205175783009914997595500
14	≈ 0.563	0.5634867715862649042931719141
16	0.334347848	0.3343478484452840400584306948
20	0.401384999	0.4013849991487159059770399317
24	0.279178557	0.2791785570447623137230350520
27	0.496929538	0.4969295375686007973093998581
64	0.274642876	0.2746428755086261757622823564
96	0.209383918	0.2093839177835717352922762890
256	0.259716632	0.2597166322744617096882452719

The second column in the above table gives the approximation b_n of $C(-4n)$ as computed by Shanks and Schmid in [13] to nine decimal places (for $n = 11$, 13 and 14, rough approximate values of $C(-4n)$ were given). The third column in the table gives the approximation b'_n of $C(-4n)$ using (3) and equation (3.2) in [11] (the precision is due to the fact that the discriminants are small). They then state (see page 561 of [13]) "We note, in passing, that of all binary forms $u^2 + nv^2$, $u^2 + 2v^2$ is the most populous, since b_2 is the largest of these constants."

It is not completely clear as to whether they meant that $C(-8)$ is the largest amongst the values computed or that the maximum value of $C(-4n)$ as n ranges over all positive integers is assumed for $n = 2$.

In any case, this quote motivates the following question: Is $C(-8)$ the maximum value? One can also wonder about the maximum of $C(D)$ as D runs over a set of fundamental discriminants. The purpose of this paper is to prove the following.

Theorem 1.1. *Let q be an odd prime. If Δ is a fixed negative fundamental discriminant, then $C(\Delta q)$, $q \equiv 1 \pmod 4$, is unbounded as $q \to \infty$. If Δ is a fixed positive fundamental discriminant or 1, then $C(-\Delta q)$, $q \equiv 3 \pmod 4$, is unbounded as $q \to \infty$.*

It is now straightforward via (4) to numerically find values of fundamental discriminants D with $C(D) > C(-8)$ when $D = -q$ where q is a prime congruent to 3 modulo 4:

D	$C(D)$
-47	0.891550...
-71	0.938541...
-167	0.951908...
-191	0.991028...
-239	1.004869...

The largest such value of $C(D)$ with $|D| < 10^9$ is

$$C(-984452999) = 1.527855...$$

Although it follows from Theorem 1.1 that $C(-4q)$ is unbounded as q runs through primes which are congruent to 1 modulo 4, finding such a q with $C(-4q) > C(-8)$ seems difficult. The problem is that (see [1])

$$L(1,\chi) < \frac{10}{3}\frac{\varphi(|D|)}{|D|}\log|D| + 1$$

and (5) both imply that $L(1,\chi)$ grows slowly. Here $L(s,\chi)$ is the Dirichlet L-series defined, for $\Re s > 1$ by

$$L(s,\chi) := \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} = \prod_p\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right),$$

and elsewhere by analytic continuation, where $\chi = \chi_D$ is the Kronecker character $\left(\frac{D}{\cdot}\right)$ and $\varphi(\cdot)$ is the Euler phi function. For example, if $D = -4q$ where $q = 13779962790518414129$, then

$$C(D) = 0.875985...$$

which is larger than $C(-8)$.

For $|D| < 10^6$, one can compute $C(D)$ using (3.2) in [11] for the Euler product and GP/PARI for $L(1,\chi_D)$. For $|D| < 10^{20}$, one can compute the Euler product by simply taking the product of roughly the first $100,000$ factors (since GP/PARI can not currently compute values of L-series for characters with moduli of this magnitude and thus one cannot use equation (3.2) in [11]) and $L(1,\chi_D)$ using the class number formula. This gives a precision of about six decimals in the latter case. It might be of computational interest to find other values of D with at least two distinct prime divisors such that $C(D) > C(-8)$. We do not address this topic here.

The paper is organized as follows. In Section 2, we recall some preliminaries on binary quadratic forms, in particular an explicit form for the constant $C(D)$. In Section 3, we prove Theorem 1.1 by making the appropriate adjustments to an analytic argument of Joshi [7].

2. Preliminaries

We first recall a general result concerning an explicit computation of the constant in the main term of the asymptotic expansion of $B_f(x)$. A nonsquare integer D with $D \equiv 0$ or $1 \pmod 4$ is called a *discriminant*. The *conductor* of the discriminant D is the largest positive integer α such that $d_0 := D/\alpha^2$ is a discriminant. If $\alpha = 1$, then D is said to be a *fundamental discriminant*. Using results of Kaplan and Williams [8] and Sun and Williams [14], the constant $C(D)$ in (2) was explicitly computed (see (2.5), (2.8) and (2.11) in [11]) as

$$C(D) = \frac{1}{2^{t(D)}} \left[\frac{\varphi(|D|)}{|D|} \frac{L(1,\chi)}{\pi} \prod_{(\frac{D}{p})=-1} \frac{1}{1-1/p^2} \right]^{1/2} v(D) \tag{3}$$

where $t(D)$ is given by (see [5] or [14])

$$t(D) = \begin{cases} \omega(D) & \text{if } D \equiv 0 \pmod{32}, \\ \omega(D) - 2 & \text{if } D \equiv 4 \pmod{16}, \\ \omega(D) - 1 & \text{otherwise} \end{cases}$$

and

$$v(D) = \frac{|D|}{\varphi(|D|)} \prod_{\substack{p|D \\ (\frac{d_0}{p})=-1}} \frac{1}{1+1/p} \sum_{m|\alpha} \frac{2^{t(D)-t(D/m^2)}}{m^2} \prod_{p|\alpha/m} \Big(1 - \frac{1}{p}\Big) \prod_{\substack{p|\alpha/m \\ (\frac{d_0}{p})=-1}} \Big(1 + \frac{1}{p}\Big).$$

One application of this explicit form for $C(D)$ is that of all the two-dimensional lattices of covolume 1, the hexagonal lattice has asymptotically the fewest distances (see Theorem 1 in [11]). If D is a fundamental discriminant, then

$$v(D) = \frac{|D|}{\varphi(|D|)}$$

and so

$$C(D) = \frac{1}{2^{t(D)}} \left[\frac{|D|}{\varphi(|D|)} \frac{L(1,\chi_D)}{\pi} \prod_{(\frac{D}{p})=-1} \frac{1}{1-1/p^2} \right]^{1/2}. \tag{4}$$

Note that

$$1 < \prod_{(\frac{D}{p})=-1} \frac{1}{1-1/p^2} < \prod_p \frac{1}{1-1/p^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} = 1.64\ldots$$

and thus the contribution of this Euler product to $C(D)$ is limited.

Assuming a suitable generalized Riemann hypothesis, Littlewood [10] showed

$$e^\gamma \leq \limsup_{D \to -\infty} \frac{L(1,\chi)}{\log\log|D|} \leq 2e^\gamma \tag{5}$$

with D running through negative fundamental discriminants. The left-hand inequality was shown unconditionally by Chowla [3] (see also the discussion in [1]). Recent work by Granville and Soundararajan [6] gives strong evidence via a probabilistic model that e^γ is in fact the true limit superior of $L(1,\chi)/\log\log|D|$.

In order to prove Theorem 1.1, we need an explicit lower bound estimate for $L(1,\chi)$ in which one can select D's with a fixed (or bounded) number of prime divisors. In this direction, Bateman, Erdös and Chowla [1] proved that

$$\limsup_{D\to-\infty} \frac{L(1,\chi)}{\log\log|D|} \geq \frac{e^\gamma}{18} \tag{6}$$

where D runs through fundamental discriminants of the form $D=-p$ where p is a prime congruent to 3 modulo 4. This implies that $C(D)$ is unbounded as D runs through (odd) negative fundamental discriminants, but says nothing about fundamental discriminants of the form $D=-4n$. Our main interest is in a result of Joshi [7] in which she improved (6) by removing the factor 18 (for a quantitative version of this result, see [4]). It turns out that one can make suitable adjustments to Joshi's proof in order to prove Theorem 1.1. This is the subject of the next section.

3. Proof of Theorem 1.1

As mentioned in Section 2, the proof of Theorem 1.1 will follow immediately from a lower bound estimate for $L(1,\chi)$. Specifically, we have

Theorem 3.1. *Let Δ be a fundamental discriminant or 1, c and d be coprime integers with d divisible by Δ and 8, q run through the primes congruent to c (mod d) and χ be the Kronecker character $\left(\frac{\Delta q^*}{\cdot}\right)$ with $q^*=\lambda q$, $\lambda=(-1)^{(c-1)/2}$. Then*

$$\limsup_{\substack{q\to\infty \\ q\equiv c\ (mod\ d)}} \frac{L(1,\chi)}{\log\log q} \geq e^\gamma \cdot \prod_{p|d} \frac{1-\frac{1}{p}}{1-\left(\frac{\Delta c^*}{p}\right)\frac{1}{p}},$$

where $c^*=\lambda c$ and γ is Euler's constant.

Proof. The theorem is a generalization of [7, Theorem 2] which corresponds to the case $\Delta=1$. As the proof is a modification of Joshi's argument, we give the necessary changes.

Fix some (small) $\epsilon>0$. It suffices to show that for every (large) x there exists a prime $q\leq x$, $q\equiv c \pmod d$, such that

$$\begin{aligned} \log L(1,\chi) \quad &\geq \quad \log\log\log x + \gamma + \sum_{p|d}\log\left(1-\frac{1}{p}\right) \\ &\quad -\sum_{p|d}\log\left(1-\left(\frac{\Delta c^*}{p}\right)\frac{1}{p}\right) + \log(1-2\epsilon) + o(1). \end{aligned} \tag{7}$$

We prove (7) by constructing a set $\Sigma=\Sigma(x)$ of primes $q\leq x$, $q\equiv c \pmod d$, with $S=|\Sigma|$ and showing

$$\begin{aligned} \sum_{q\in\Sigma}\log L(1,\chi) \quad &\geq \quad S\left(\log\log\log x + \gamma + \sum_{p|d}\log\left(1-\frac{1}{p}\right)\right. \\ &\quad \left. -\sum_{p|d}\log\left(1-\left(\frac{\Delta c^*}{p}\right)\frac{1}{p}\right) + \log(1-2\epsilon)\right) + o(S). \end{aligned} \tag{8}$$

Put

$$y = (\log x)^{1-2\epsilon}$$

and let $p_1, \ldots, p_m$ be the primes not greater than y and not dividing d. Define r as in [7, p. 64], and let $k = dp_1 \cdots p_{r-1}p_{r+1} \cdots p_m$. For each $i \neq r$, let g_i (respectively h_i) be a quadratic residue (respectively non-residue) modulo p_i. Let $l \leq k$ be the unique positive integer satisfying $l \equiv c \pmod{d}$ and

$$l \equiv \begin{cases} g_i \pmod{p_i} & \text{for } \left(\frac{\lambda\Delta}{p_i}\right) = 1,\ i \neq r \\ h_i \pmod{p_i} & \text{for } \left(\frac{\lambda\Delta}{p_i}\right) = -1,\ i \neq r. \end{cases}$$

Define

$$\Sigma = \{q \text{ prime} \mid \sqrt{x} \leq q \leq x,\ q \equiv l \pmod{k}\}.$$

Then every $q \in \Sigma$ satisfies $q \equiv c \pmod{d}$ and $\chi(p_i) = 1$ for $i \neq r$ since

$$\chi(p_i) = \left(\frac{\Delta q^*}{p_i}\right) = \left(\frac{\lambda\Delta}{p_i}\right)\left(\frac{q}{p_i}\right) = \left(\frac{\lambda\Delta}{p_i}\right)\left(\frac{l}{p_i}\right) = 1.$$

So far, the only difference compared with Joshi's proof is the definition of l and χ (in [7], χ is the character $\left(\frac{\cdot}{q}\right) = \left(\frac{q^*}{\cdot}\right)$ corresponding to $\Delta = 1$). The different definition of l plays no role other than guaranteeing that we still have $\chi(p_i) = 1$, cf. [7, p. 65]. Hence, as in [7, (24)], we get

$$\begin{aligned} \sum_{q\in\Sigma} \log L(1,\chi) \quad \geq \quad & S\Bigg(\log\log\log x + \gamma + \sum_{p|d} \log\left(1 - \frac{1}{p}\right) \\ & - \sum_{p|d} \log\left(1 - \left(\frac{\Delta c^*}{p}\right)\frac{1}{p}\right) + \log(1-2\epsilon)\Bigg) + R + o(S) \end{aligned}$$

where

$$R = \sum_{q\in\Sigma}\sum_{p>y} \chi(p)\frac{1}{p}.$$

We now show $R = o(S)$ and hence (8) by splitting the summation over p into five intervals $I_1, \ldots, I_5$ and thus writing $R = R_1 + \cdots + R_5$ with

$$R_i = \sum_{q\in\Sigma}\sum_{p\in I_i} \chi(p)\frac{1}{p}.$$

The estimation of R_1 and R_2 is practically the same as in Joshi's paper, only one has to replace $\left(\frac{\lambda}{p}\right)$ by $\left(\frac{\lambda\Delta}{p}\right)$ in [7, (27)] and the equation below that, which makes no difference since the sign of that factor plays no role anyway. The estimation of R_3 is exactly the same since it relies on the majorization

$$\left|\sum_{p\in I_3} \chi(p)\frac{1}{p}\right| \leq \sum_{p\in I_3} \frac{1}{p}.$$

The estimation of R_4 requires some more care since it relies on the large sieve as stated in [7, Lemma 1] which works only for prime moduli. Put $\beta = 2 + \epsilon^{-1}$ and subdivide I_4 into intervals

J_t each containing Z_t primes as in [7, p. 70]. Then [7, (30)] remains valid, i.e.

$$\sum_{q\in\Sigma}\sum_{p\in J_t}\chi(p)\frac{1}{p}-\frac{1}{t}\sum_{q\in\Sigma}\sum_{p\in J_t}\chi(p)=O\left(\frac{S}{(\log x)^{2\beta}}\right). \tag{9}$$

Let J_t^+ and J_t^- denote the sets of primes in J_t with $\left(\frac{\Delta}{p}\right)=1$ and $\left(\frac{\Delta}{p}\right)=-1$, respectively. Then $Z_t=Z_t^++Z_t^-$ where Z_t^+ and Z_t^- are defined analogously. Also, let $Z_t(a,q)$ be the number of p in J_t which are congruent to a modulo q, and similarly write $Z_t(a,q)=Z_t^+(a,q)+Z_t^-(a,q)$. Then a computation using the large sieve, cf. [7, p. 71], shows

$$\begin{aligned}\left|\frac{1}{t}\sum_{q\in\Sigma}\sum_{p\in J_t^+}\left(\frac{p}{q}\right)\right|^2 &= \frac{1}{t^2}\left|\sum_{q\in\Sigma}\sum_{j=1}^{q-1}\left(\frac{j}{q}\right)\left(Z_t^+(j,q)-\frac{Z_t^+}{q}\right)\right|^2\\ &\leq \frac{S^2}{(\log x)^{4\beta}},\end{aligned}$$

and similarly with the summation over $p\in J_t^-$. Since $\chi(p)=\left(\frac{\Delta}{p}\right)\left(\frac{p}{q}\right)$, we now get

$$\begin{aligned}\left|\frac{1}{t}\sum_{q\in\Sigma}\sum_{p\in J_t}\chi(p)\right| &\leq \left|\frac{1}{t}\sum_{q\in\Sigma}\sum_{p\in J_t^+}\chi(p)\right|+\left|\frac{1}{t}\sum_{q\in\Sigma}\sum_{p\in J_t^-}\chi(p)\right|\\ &= \left|\frac{1}{t}\sum_{q\in\Sigma}\sum_{p\in J_t^+}\left(\frac{p}{q}\right)\right|+\left|\frac{1}{t}\sum_{q\in\Sigma}\sum_{p\in J_t^-}\left(\frac{p}{q}\right)\right|\\ &\leq 2\cdot\frac{S}{(\log x)^{2\beta}}\\ &= O\left(\frac{S}{(\log x)^{2\beta}}\right). \qquad (10)\end{aligned}$$

From (9) and (10) follows

$$\left|\sum_{q\in\Sigma}\sum_{p\in J_t}\chi(p)\frac{1}{p}\right|=O\left(\frac{S}{(\log x)^{2\beta}}\right),$$

and thus

$$R_4=\sum_{q\in\Sigma}\sum_{p\in I_4}\chi(p)\frac{1}{p}=o(S).$$

Finally, the estimation of R_5 can be carried out by writing

$$\sum_{v<p\leq w}\chi(p)\frac{1}{p}=\sum_{j=1}^{|\Delta q|}\chi(j)\sum_{\substack{v<p\leq w\\ p\equiv j \pmod{|\Delta q|}}}\frac{1}{p},$$

and using the uniform prime number theorem, cf. [7, p. 72].

$\square$

Remark 3.2. Theorem 3.1 is close to being best possible (see (5)).

Proof of Theorem 1.1. If Δ is a negative fundamental discriminant, then let $c = 1$ and d be divisible by Δ and 8. Hence Theorem 3.1 implies that for $\chi = \chi_D$, $D = \Delta q$, we have

$$\sup_{\substack{q \to \infty \\ q \equiv c \pmod d}} L(1, \chi) = \infty.$$

Applying this to (4) yields the first statement. If Δ is a positive fundamental discriminant or 1, let $c = -1$ and d be divisible by Δ and 8. Applying Theorem 3.1 with $D = -\Delta q$ to (4) implies the second statement. □

Acknowlegements

The first author was supported by grant 272-08-0323 from the Danish Agency for Science, Technology and Innovation while the third author was partially supported by Science Foundation Ireland 08/RFP MTH1081. The third author would like to thank the Institut des Hautes Études Scientifiques for their hospitality and support during the preparation of this paper and Greg Martin and Olivier Ramaré for their comments.

References

[1] P. Bateman, S. Chowla and P. Erdös, Remarks on the size of $L(1, \chi)$, *Publ. Math. Debrecen* **1** (1950), 165–182.

[2] P. Bernays, Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht-quadratischen Diskriminante, Dissertation, Göttingen, 1912, available at `http://www.math.uni-bielefeld.de/~rehmann/DML/`

[3] S. Chowla, On the class-number of the corpus $P(\sqrt{-k})$, *Proc. Nat. Acad. Sci. India* **13** (1947), 197–200.

[4] R. Cook, A note on character sums, *J. Number Theory* **11** (1979), 505–515.

[5] D. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley & Sons, Inc, New York, 1989.

[6] A. Granville and K. Soundararajan, The distribution of values of $L(1, \chi_d)$, *Geom. Funct. Anal.* **13** (2003), 992–1028.

[7] P. Joshi, The size of $L(1, \chi)$ for real nonprincipal residue characters χ with prime modulus, *J. Number Theory* **2** (1970), 58–73.

[8] P. Kaplan and K. Williams, The genera representing a positive integer, *Acta Arith.* **102** (2002), 353–361.

[9] E. Landau, Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der mindest Anzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate, *Arch. der Math. und Phys. (3)* **13** (1908), 305–312.

[10] J. Littlewood, On the class-number of the corpus $P(\sqrt{-k})$, *Proc. London Math. Soc. (2)* **27** (1928), 358–372.

[11] P. Moree and R. Osburn, Two-dimensional lattices with few distances, *Enseignement Math.* **52** (2006), 361–380.

[12] D. Shanks, The second order term in the asymptotic expansion of $B(x)$, *Math. Comp.* **18** (1964), 75–86.

[13] D. Shanks and L. Schmid, Variations on a theorem of Landau. I, *Math. Comp.* **20** (1966), 551–569.

[14] Z. Sun and K. Williams, On the number of representations of n by $ax^2 + bxy + cy^2$, *Acta Arith.* **122** (2006), 101–171.

School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany

E-mail address: `david.brink@ucd.ie`

E-mail address: `moree@mpim-bonn.mpg.de`

E-mail address: `robert.osburn@ucd.ie`