Two-dimensional lattices with few distances

Pieter Moree and Robert Osburn

Abstract

We prove that of all two-dimensional lattices of covolume 1 the hexagonal lattice has asymptotically the fewest distances. An analogous result for dimensions 3 to 8 was proved in 1991 by Conway and Sloane. Moreover, we give a survey of some related literature, in particular progress on a conjecture from 1995 due to Schmutz Schaller.

1 Introduction

It is an old problem in combinatorial geometry how to place a given number of distinct points in n-dimensional Euclidean space so as to minimize the total number of distances they determine. Conway and Sloane [9] conjecture that, for all N sufficiently large, the optimal set of N points in n-dimensional space will be a subset of an n-dimensional lattice having minimal *Erdős number*. In real euclidean space $\mathbb{R}^n$ equipped with inner product $(v, w) = v \cdot w$, a lattice L consists of all integral linear combinations

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n,\ \ \lambda_i \in \mathbb{Z},$$

of n linearly independent vectors $v_1, \ldots, v_n$. The vectors $v_1, \ldots, v_n$ form an integral basis for L, and

$$f(\lambda) = (v, v) = \lambda A \lambda^{\mathrm{tr}},\ \ \lambda = (\lambda_1, \ldots, \lambda_n),\ \ A = (a_{ij}),\ \ a_{ij} = (v_i, v_j),$$

is the corresponding quadratic form. The various integral bases for L yield integrally equivalent quadratic forms. Suppose $n \geq 2$. The Erdős number of an n-dimensional lattice L is given by

$$E_L = F_L d^{1/n}, \tag{1}$$

where d is the determinant of the lattice and F_L, its *population fraction*, is given by

$$F_L = \lim_{x\to\infty} \frac{N_L(x)\sqrt{\log x}}{x} \text{ if } n = 2,\ \ F_L = \lim_{x\to\infty} \frac{N_L(x)}{x} \text{ if } n \geq 3,$$

where $N_L(x)$ is the *population function* associated to the corresponding quadratic form, i.e., the number of values not exceeding x taken by the form. The Erdős number is the population fraction when the lattice is normalized to have covolume 1. Conway and Sloane [9] proved that for $n \geq 3$ the lattices with minimal Erdős number are (up to a scale factor) the even lattices of minimal determinant. For $2 \leq n \leq 10$ the even lattices of minimal determinant are unique:

$$A_2,\ A_3 \cong D_3,\ D_4,\ D_5,\ E_6,\ E_7,\ E_8,\ E_8 \oplus A_1,\ E_8 \oplus A_2. \tag{2}$$

Mathematics Subject Classification (2000). 11N37, 11N69, 11R45

Actually Conway and Sloane also claimed the result for $n = 2$, relying on a preprint (in 1991) of Warren D. Smith [36]. However, the preprint was never published and this induced Schmutz Schaller [32, p. 200] to write 'the case $n = 2$ seems to be open'. It is the purpose of this paper to dispose of this case (in Theorem 1) and thus to 'complete' the Conway and Sloane result. In doing so, we have made use of results that have become available only very recently. In particular, we use an explicit formula for the number of genera of discriminant D representing a positive integer n (see Theorem 5) and an improved lower bound on the Euler phi function $\varphi(n)$ for n odd (see (24)).

Let Σ denote the hexagonal lattice of covolume 1, that is,

$$\Sigma = \sqrt{\frac{2}{\sqrt{3}}}\left(\mathbb{Z}\begin{pmatrix}1\\0\end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix}1/2\\\sqrt{3}/2\end{pmatrix}\right).$$

The associated quadratic form is $(X^2 + XY + Y^2)2/\sqrt{3}$.

Theorem 1 *If L is any two-dimensional lattice not isometric to Σ, then E_L, the Erdős number of L, satisfies*

$$E_L > E_\Sigma = 2^{-3/2}3^{1/4} \prod_{p\equiv 2 (\mathrm{mod}\ 3)} \frac{1}{\sqrt{1-1/p^2}} = 0.553311775832479\cdots \tag{3}$$

In other words, of all the two dimensional lattices of covolume 1, Σ has asymptotically the fewest distances. Moreover, given any real number r the set of non-homothetic lattices L such that $E_L < r$ is finite and can be explicitly determined.

In fact it turns out furthermore that if E_L is finite, then there is a homothetic lattice L' such that $E_L = E_{L'}$ and the quadratic form associated to L' has integer coefficients and is primitive (for Σ this is $X^2 + XY + Y^2$). Moreover, E_L only will depend on the discriminant D of the associated quadratic form. To stress this, we write $E(D)$ rather than E_L.

1.1 On a conjecture of Schmutz Schaller

In [32, p. 20] Schmutz Schaller, motivated by considerations from hyperbolic geometry, proposed for dimensions 2 to 8 a daring strengthening of Theorem 1 and (part of) the Conway and Sloane result:

Conjecture 1 *In dimensions 2 to 8 the even lattices with minimal determinant have 'maximal lengths', meaning that their length spectrum dominates the length spectrum of every other lattice of the same dimension and covolume at every position.*

Schmutz Schaller [31] proved an analogue of this conjecture in the hyperbolic case. Given any lattice L one can define the sequence $0 < d_1 < d_2 < ...$ of distances between lattice points that occur in this lattice (the *length spectrum*). (It is very important that in this definition we do not care about the multiplicities of these lengths.) The number d_k is called the *k-th length* of L. Given any other length spectrum $0 < l_1 < l_2 < \ldots$ we say that the former length spectrum *totally dominates* the latter if $d_i \geq l_i$ for every $i \geq 1$. This can be reformulated in terms of $N_L(x)$:

the length spectrum L_1 *totally dominates* that of L_2 iff $N_{L_1}(x) \leq N_{L_2}(x)$ for every $x > 0$.

Let $S = \mathbb{Z}[i]$ denote the square lattice and $H = \mathbb{Z}[\zeta_3]$ the hexagonal lattice. Schmutz Schaller [32] conjectured that the hexagonal length spectrum should dominate that of the square lattice, that is he conjectured that $N_H(x) \leq N_S(x)$ for every $x > 0$, to make the point that even a partial version of his conjecture should be difficult to establish. Indeed, the first author and te Riele [22], refining techniques from [19], managed to prove this only after considerable effort, also numerical effort. Their approach, however, does not seem to offer any hope of establishing the general conjecture.

From the work of Korkine and Zolotareff (in the 19th century) and Blichfeldt (cf. [30, Chapter 9] and [4]) it follows that Conjecture 1 is true in the 1-length case, i.e., the lattices in (2) have maximal minimal positive length amongst those of the same dimension, after scaling to the same covolume. For a list of these lengths see, e.g. [30, p. 204].

A two-dimensional lattice is said to be *arithmetic* iff there exists a real number λ such that λL is isometric to a $\mathbb{Z}$-submodule of rank two in an imaginary quadratic number field, otherwise it is said to be *non-arithmetic*. Kühnlein [16] proved that a two-dimensional lattice is arithmetic iff there are at least 3 pairwise linearly independent vectors in it having the same length. As a consequence it is easy to show that $N_L(x) \sim c(L)x$ for some positive constant $c(L)$ in case L is non-arithmetic. It follows from this that a non-arithmetic lattice does not have a finite Erdős number. Kühnlein [16] proved furthermore that the length spectrum of Σ totally dominates the length spectrum of every non-arithmetic lattice of covolume 1. Thus in order to prove Conjecture 1 for dimension 2 it suffices to prove that the length spectrum of Σ totally dominates the length spectrum of every arithmetic lattice of covolume 1.

2 Population fraction of binary quadratic forms

Let $f(X,Y) = aX^2 + bXY + cY^2$ be a positive definite binary quadratic form with discriminant $D_f = b^2 - 4ac$ and a, b and c real numbers. Let $B_f(x)$ count the number of positive real numbers $r \le x$ that can be represented by f.

In the course of history the problem of estimating $B_f(x)$ has attracted considerable interest. A classical result of Landau [17] states that, as x tends to infinity,

$$B_{f_1}(x) \sim C(f_1)\frac{x}{\sqrt{\log x}},$$

where $C(f_1)$ is an explicit constant and $f_1(X,Y) = X^2 + Y^2$. Precisely, $C(f_1)$ is of the form

$$C(f_1) = \frac{1}{\sqrt{2}} \prod_{p\equiv 3 \pmod 4} (1-p^{-2})^{-1/2}.$$

Note that $B_{f_1}(x) = N_S(x)$.

A similar result was claimed by Srinivasa Ramanujan in his celebrated first letter to Hardy (written in 1912), cf. [21]. The constant $C(f_1)$ is now called the *Landau-Ramanujan constant*, cf. [11, Section 2.3]. Ramanujan even claimed that it ought to be true that

$$N_S(x) = C(f_1)\int_2^x \frac{dt}{\sqrt{\log t}} + O(x^{1/2+\epsilon}). \tag{4}$$

Note the analogy with the prime number theorem under assumption of the Riemann Hypothesis. This states that $\pi(x)$, the number of primes $p \le x$, satisfies $\pi(x) = \int_2^x dt/\log t + O(x^{1/2+\epsilon})$, on assumption of the Riemann Hypothesis. It was folklore that Landau's method could be easily adapted to show that $N_S(x)$ satisfies an asymptotic series expansion in the sense of Poincaré:

$$N_S(x) = C(f_1)\frac{x}{\sqrt{\log x}}\left(1 + \frac{r_1}{\log x} + \frac{r_2}{\log^2 x} + \cdots + \frac{r_n}{\log^m x} + O\left(\frac{1}{\log^{m+1} x}\right)\right), \tag{5}$$

where $m \geq 1$ is an arbitrary integer. A proof of this was finally written down by J.-P. Serre [33] for the larger class of so called Frobenian multiplicative functions. Note that Ramanujan's conjecture implies, by partial integration of the main term, that

$$N_S(x) = C(f_1)\frac{x}{\sqrt{\log x}}\left(1 + \frac{s_1}{\log x} + \frac{s_2}{\log^2 x} + \cdots + \frac{s_m}{\log^m x} + O\left(\frac{1}{\log^{m+1} x}\right)\right),$$

with $s_j = (2j-1)!/((j-1)!2^{2j-1})$ and $m \geq 1$ an arbitrary integer. Ramanujan's conjecture was shown to be false by Shanks [34] who proved that $s_1 \neq r_1$. In a celebrated unpublished (during his lifetime) paper on the partition and tau function [3], Ramanujan made conjectures similar to (4) concerning the divisiblity of the Ramanujan tau function by certain special primes. These conjectures were all shown to be false by the first author [20]. However, Rankin had shown earlier that asymptotically these conjectures are correct.

Paul Bernays (of later fame in logic and for many years assistant to Hilbert [28]) was a PhD student of Landau's at Göttingen. In his 1912 thesis Bernays [1] studied the question of finding an asymptotic formula similar to that of Landau's, but now in case f is a primitive positive definite binary quadratic form having negative discriminant D_f. Bernays' proved that, as x tends to infinity,

$$B_f(x) = C(f)\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{(\log x)^{1/2+\delta}}\right), \tag{6}$$

where the constant $C(f)$ is positive and depends only on the discriminant D_f of f and $\delta < \min(1/h, 1/4)$, where h denotes the number of reduced quadratic forms having the same discriminant as f. It turns out that the dependence of $C(f)$ on D_f is not very strong; $C(f) = D_f^{o(1)}$.

Bernays' result allows various generalisations: one could ask for simultaneous representation of n by various quadratic forms or by norm forms. A lot of work in this direction was carried out by Odoni, cf. [24, 25]. Blomer recently pointed out that Bernays' method can be used to disprove a conjecture of Erdős. The falsity of this conjecture was claimed earlier by Odoni [26], but his paper seems to contain some obscurities. Erdős conjectured that the number $V(x)$ of integers not exceeding x that are sums of two squareful integers satisfies $V(x) \asymp x/\sqrt{\log x}$, where an integer n is called squareful if $p|n$ implies that $p^2|n$ for all primes p. Since every squareful integer n can uniquely be written as $n = a^3b^2$ with $\mu(a) \neq 0$, one can write

$$V(x) = \#\{1 \leq n \leq x : \exists \mathbf{a} = (a_1, a_2) \in \mathbb{N}^2 : a_1^3X^2 + a_2^3Y^2 \text{ represents } n\}.$$

Thus one can estimate $V(x)$ if one can deal with $B_f(x)$ with some uniformity in f (or rather the discriminant of f). In Bernays' method the dependence on D can be made explicit. This yields $B_f(x) \gg_\epsilon |D|^{-\epsilon}x/\sqrt{\log x}$ uniformly at least in $D = O((\log\log x)^{1/2})$. This result can be used to show that Erdős' conjecture is false. By a more refined method Blomer [5, 6] even showed that $V(x) = x(\log x)^{-\alpha+\epsilon}$, where $\alpha = 1 - 2^{-1/3} = 0.206\cdots$. Moreover, Blomer and Granville [7] conjecture that $V(x) \asymp x(\log\log x)^{2^{2/3}-1}(\log x)^{2^{-1/3}-1}$ and prove the upper bound, failing to obtain the conjectured lower bound only by a power of $\log\log x$.

Bernays' result can be used to infer the following alternative characterisation of arithmetic lattices.

Proposition 1 *A two-dimensional lattice has a finite Erdős number iff it is arithmetic.*

Proof. We have already seen that a non-arithmetic lattice does not have a finite Erdős number. If the lattice is arithmetic then, possibly after scaling, the associated quadratic form has integer coefficients. The result then follows from Bernays' theorem and the definition (1) for $n = 2$. □

We say that the quadratic form $f = [a, b, c]$ is projectively equivalent with $g = [a', b', c']$ if the vectors (a, b, c) and (a', b', c') are projectively equivalent. If g is projectively equivalent to a binary quadratic form with integer coefficients and negative discriminant, say $g = [\lambda a', \lambda b', \lambda c']$, and $f = [a', b', c']$ with $\lambda > 0$, then Bernays' result (6) implies that, as x tends to infinity,

$$B_g(x) \sim C(g)\frac{x}{\sqrt{\log x}}.$$

It is easy to see that if L is any arithmetic lattice, then

$$E_L = \frac{\sqrt{|D_f|}}{2}C(f), \tag{7}$$

where f is a quadratic form associated to the lattice L. Note that if f and g are projectively equivalent, then $\sqrt{|D_f|}C(f) = \sqrt{|D_g|}C(g)$.

We now have:

Proposition 2 *Let L be a two-dimensional lattice. The assertion $E_L > E_\Sigma$ is equivalent with the assertion that the minimal value of $\sqrt{|D_f|}C(f)/2$, as f ranges over the primitive binary quadratic forms of negative discriminant, is assumed for $f = X^2 + XY + Y^2$.*

Proof. By Proposition 1 we can restrict ourselves to arithmetic lattices. The quadratic form associated to an arithmetic lattice is projectively equivalent with a primitive positive definite binary quadratic form of negative discriminant. Vice versa, to a quadratic form having integer coefficients there corresponds an arithmetic lattice. The proof is then completed on invoking (7) and noting that $X^2 + XY + Y^2$ is the primitive binary quadratic form associated to Σ. □

2.1 On computing the population fraction

Proposition 2 'reduces' our geometric problem to a problem in number theory, namely that of computing $C(f)$. We now discuss some historic results which are related to the explicit evaluation of $C(f)$ due to Bernays.

A nonsquare integer D with $D \equiv 0$ or $1 (\bmod 4)$ is called a *discriminant*. The conductor of the discriminant D is the largest positive integer f such that $d_0 := D/f^2$ is a discriminant. If $f = 1$, then D is said to be a *fundamental discriminant*. James [14] proved that the number $B_D(x)$ of positive integers $n \le x$ which are coprime to D and which are represented by some primitive integral form of discriminant $D \le -3$ satisfies

$$B_D(x) = J(D)\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{\log x}\right),$$

where $J(D)$ is the positive constant given by

$$\pi J(D)^2 = \frac{\varphi(|D|)}{|D|}L(1, \chi_D)\prod_{(\frac{D}{p})=-1}\frac{1}{1-\frac{1}{p^2}}, \tag{8}$$

and p runs over all primes such that $(\frac{D}{p}) = -1$. Here and in the remainder of the paper implicit constants depend at most on the discriminant D.

Just as for the characteristic function of $X^2 + Y^2$, the characteristic function corresponding to integers counted for some x by $B_D(x)$ is multiplicative. In both cases the associated Dirichlet series are very similar and this allowed James to essentially mimic Landau's original proof. In 1975 Williams [38] reproved James' result in a more elementary way (essentially along the lines of Rieger [29], who gave a more elementary proof of Landau's result). However, this reproof only gives a weaker error term. We like to point out that an even easier proof (but with an even weaker error term) can be obtained on invoking the following classical result of Wirsing [39].

Theorem 2 *Suppose that $f(n)$ is a multiplicative function such that $f(n) \geq 0$, for $n \geq 1$, and such that there are constants γ_1 and γ_2, with $\gamma_2 < 2$, such that for every prime p and for every $\nu \geq 2$, $f(p^\nu) \leq \gamma_1 \gamma_2^\nu$. Assume that as $x \to \infty$,*

$$\sum_{p \leq x} f(p) \sim \tau \frac{x}{\log x},$$

where $\tau > 0$ is a constant. Then as x tends to infinity we have

$$\sum_{n \leq x} f(n) \sim \frac{e^{-\gamma\tau}}{\Gamma(\tau)} \frac{x}{\log x} \prod_{p \leq x} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right),$$

where γ is Euler's constant and $\Gamma(\tau)$ denotes the gamma-function.

Let ξ_D be the multiplicative function defined as follows:

$$\xi_D(p^e) = \begin{cases} 1 & \text{if } (\frac{D}{p}) = 1; \\ 1 & \text{if } (\frac{D}{p}) = -1 \text{ and } 2|e; \\ 0 & \text{otherwise.} \end{cases}$$

Let n be any integer coprime to D. Then $\xi_D(n) = 1$ iff n is represented by some primitive positive integral binary quadratic form of discriminant D. It follows that $B_D(x) = \sum_{n \leq x} \xi_D(n)$. It is a consequence of the law of quadratic reciprocity and the prime number theorem for arithmetic progressions that

$$\sum_{p \leq x} \xi_D(p) = \sum_{\substack{p \leq x \\ (\frac{D}{p})=1}} 1 \sim \frac{x}{2 \log x}. \tag{9}$$

Thus the conditions of Wirsing's theorem are satisfied and we find that

$$B_D(x) \sim \frac{e^{-\gamma/2}}{\Gamma(1/2)} \frac{x}{\log x} \prod_{\substack{p \leq x \\ (\frac{D}{p})=1}} \frac{1}{1 - \frac{1}{p}} \prod_{\substack{p \leq x \\ (\frac{D}{p})=-1}} \frac{1}{1 - \frac{1}{p^2}}.$$

By (6) of [38] we have the following estimate:

$$\prod_{\substack{p \leq x \\ (\frac{D}{p})=1}} \left(1 - \frac{1}{p}\right) = e^{-\gamma/2} \prod_{p|D} \left(1 - \frac{1}{p}\right)^{-1/2} \prod_{(\frac{D}{p})=-1} \left(1 - \frac{1}{p^2}\right)^{-1/2} \frac{L(1, \chi_D)^{-1/2}}{\sqrt{\log x}} + O\left(\frac{1}{\log^{3/2} x}\right).$$

On combining the latter formulae it then follows that $B_D(x) \sim J(D)x/\sqrt{\log x}$.

Indeed on using standard results from the asymptotic theory of arithmetical functions it is not difficult to improve on James' result. Estimate (9) can be easily sharpened to

$$\sum_{p \leq x} \xi_D(p) = \frac{1}{2} \int_2^x \frac{dt}{\log t} + O_m\left(\frac{x}{\log^m x}\right),$$

for every $m \geq 0$. This in combination with e.g. [21, Theorem 6] then shows the truth of the following result:

Theorem 3 *We have, for every $k \geq 1$,*

$$B_D(x) = J(D)\frac{x}{\sqrt{\log x}} + \sum_{j=1}^{k} c_k \frac{x}{\log^{j+1/2} x} + O_k(\frac{x}{\log^{k+3/2-\epsilon} x}),$$

where the constants $c_1, c_2, \ldots$ may depend on D.

James' counting function is artificial in the sense that one would like to drop the condition that n be coprime to D. This was achieved by Pall [27] who proved that the number $C_D(x)$ of positive integers $n \leq x$ which are which are represented by some primitive integral form of discriminant $D \leq -3$ satisfies

$$C_D(x) = P(D)\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{\log x}\right),$$

where $P(D)$, *Pall's constant*, is computed as follows. Let p be a prime dividing D. Let p' denote the primes which satisfy the following condition: if $p > 2$ and $p^2 \mid D$ or $p = 2$ and $D \equiv 0$ or $4 \bmod 16$. Then

$$P(D) = b_0 \prod_{p'} \left(1 - \frac{1}{p'^2}\right)^{-1} \prod \left(1 + \frac{1}{p^{2k+1}}\right),$$

where in the second product $D = p^{2k}D'$ where $p^2 \nmid D'$, $k \geq 1$, and $\left(\frac{D'}{p}\right) \neq -1$, and

$$b_0^2 = \frac{2h(D)}{w\sqrt{|D|}} \prod_{q} \left(1 - \frac{1}{q^2}\right)^{-1} \prod_{p'} \left(1 - \frac{1}{p'}\right) \prod_{\substack{p|D \\ p \neq p'}} \left(1 - \frac{1}{p}\right)^{-1},$$

where q runs over all primes such that $\left(\frac{D}{q}\right) = -1$.

Let us compute a specific example. If $D = -3$, then

$$P(-3)^2 = b_0^2 = \frac{1}{3} \cdot \frac{1}{\sqrt{3}} \cdot \alpha \cdot \frac{3}{2} = \frac{\alpha}{2\sqrt{3}},$$

where $\alpha = \prod_{q \equiv 2 (\text{mod } 3)} \left(1 - \frac{1}{q^2}\right)^{-1}$. Thus

$$P(-3) = \frac{1}{\sqrt{2}} \frac{1}{3^{1/4}} \prod_{q \equiv 2 (\text{mod } 3)} \left(1 - \frac{1}{q^2}\right)^{-1/2}.$$

Using Pall's result and the fact that $h(-3) = 1$, it then follows that E_Σ is as given in (3). Pall's result allows us to compute $C(f)$ in case the order associated to f has class number one.

Going beyond Pall's work requires genus theory. Let $H(D)$ denote the group of strict equivalence classes of primitive, positive-definite, integral, binary quadratic forms of discriminant D under Gaussian composition. Let $G(D)$ denote the genus group of $H(D)$, that is, $G(D) = H(D)/H(D)^2$. The order $|G(D)|$ of $G(D)$ is a power of 2 so that there exists a non-negative integer $t(D)$ such that $|G(D)| = 2^{t(D)}$. The latter quantity is the number of classes whose order divides 2, that is, the number of ambiguous classes in $H(D)$. The value of $t(D)$ is given as follows (see [10] or [37]):

$$t(D) = \begin{cases} \omega(D) & \text{if } D \equiv 0 (\text{mod } 32); \\ \omega(D) - 2 & \text{if } D \equiv 4 (\text{mod } 16); \\ \omega(D) - 1 & \text{otherwise,} \end{cases} \tag{10}$$

where $\omega(D)$ denotes the number of distinct prime factors in D. For example, if $D = -3 \equiv 1 \bmod 4$, then $\omega(D) = 1$ and so there is one genus of forms of discriminant -3. Note that if D is fundamental, then $t(D) = \omega(D) - 1$. We say that n is represented by the genus G of $G(D)$ if it is represented by at least one class in G. By $g(n, D)$ we denote the number of genera of discriminant D representing n. We now turn to the explicit evaluation of $C(f)$ (see page 59 and 115-116 in [1]) which is due to Bernays. Namely, we have the following.

Theorem 4 (Bernays' Theorem). *Let f be a positive definite binary quadratic form having discirminant D. Then*

$$C(f) = \frac{J(D)}{2^{t(D)}} \sum_{n|D^\infty} \frac{g(n, D)}{n}, \tag{11}$$

where $n \mid D^\infty$ means that n divides some arbitrary power of D.

It is a classical fact that if n is represented by a class of discriminant D and $(n, D) = 1$, then $g(n, D) = 1$. It is rather more complicated to determine the value of $g(n, D)$ in case $(n, D) > 1$. This was recently achieved by Kaplan and Williams in [15] and Sun and Williams in [37]. In [15] they showed that if $g(n, D) > 0$, then $g(n, D) = 2^{t(D)-t(D/m^2)}$, where m is the largest integer such that $m^2|n$ and $m|f$. Note that m^2 is the largest square dividing (n, f^2). This result together with Theorem 6.1 of [37] then yields the following result. Here $\nu_p(n)$ denotes the largest power of the prime p dividing the nonzero integer n.

Theorem 5 *Let D be a discriminant with conductor f, $d_0 = D/f^2$ and n a natural number. If (n, f^2) is not a square, or there exists a prime p such that $\nu_p(n)$ is odd and $(\frac{d_0}{p}) = -1$, then $g(n, d) = 0$. Suppose (n, f^2) is a square and $(\frac{d_0}{p}) = 0, 1$ for every prime p with $\nu_p(n)$ is odd. Then $g(n, D) = 2^{t(D)-t(D/(n,f^2))}$.*

Using Theorem 5 one can evaluate more explicitly the sum

$$v(D) := \sum_{n|D^\infty} \frac{g(n, D)}{n}. \tag{12}$$

By Theorem 5 we have

$$v(D) = \sum_{m|f} \frac{2^{t(D)-t(D/m^2)}}{m^2} {\sum}' \frac{1}{n_0}, \tag{13}$$

where the dash indicates that the sum is over those n_0 dividing D^∞ such that $(n_0, f/m) = 1$ and there is no prime p such that $2 \nmid \nu_p(n_0)$ and $(\frac{d_0}{p}) = -1$. Note that if $g(n, D) > 0$ we can write, by Theorem 5, $(n, f^2) = m^2$, with $m|f$ and thus we have $n = n_0 m^2$, where $(n_0, f/m) = 1$. Furthermore note that $2 \nmid \nu_p(n)$ iff $2 \nmid \nu_p(n_0)$. On evaluating the double sum in (13) we obtain

$$v(D) = \frac{|D|}{\varphi(|D|)} \prod_{\substack{p|D \\ (\frac{d_0}{p})=-1}} \frac{1}{1+1/p} \sum_{m|f} \frac{2^{t(D)-t(D/m^2)}}{m^2} \prod_{p|f/m} \left(1 - \frac{1}{p}\right) \prod_{\substack{p|f/m \\ (\frac{d_0}{p})=-1}} \left(1 + \frac{1}{p}\right). \quad (14)$$

Using (10) the sum $v(D)$ can be explicitly computed using this formula. Note that it always is a positive rational number. Also note that if D is a fundamental discriminant, then

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

`Example`. Take $D = -1984 = -2^6 \cdot 31$. There are $2^{t(D)} = 4$ genera of discriminant -1984. We have $G(-1984) = \{I, A, B, AB\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where

$$\begin{aligned} I &= \{[1,0,496],[20,\pm 4,25]\}, \\ A &= \{[4,4,125],[5,\pm 4,100]\}, \\ B &= \{[16,0,31],[7,\pm 2,71]\}, \\ AB &= \{[16,16,35],[19,\pm 12,28]\}. \end{aligned}$$

The divisors n of D^∞ such that $g(n,D) > 0$ are precisely the numbers of the form $31^a, 4 \cdot 31^a, 16 \cdot 31^a$ and $64 \cdot 31^a \cdot 2^b$, where $a, b \geq 0$ are arbitrary integers. By Theorem 5 we have $g(n,D) = 1, 2, 4$ and respectively 4 for these cases. Indeed, if $n = 31^a$, then the corresponding genera are I and B, depending on whether a is even or odd. If $n = 4 \cdot 31^a$, then the corresponding genera are I and A, and B and AB depending on whether a is even or odd. In case $n = 16 \cdot 31^a$ and $n = 64 \cdot 31^a \cdot 2^b$ the corresponding genera are I, A, B and AB. For example, if $n = 4 \cdot 31^{2a+1}$, then n is represented by $[16, 16, 35]$ on taking $x = 31^a$ and $y = -2 \cdot 31^a$ and thus is represented by AB. It follows that

$$v(D) = \sum_{n|D^\infty} \frac{g(n,D)}{n} = \left(1 + \frac{2}{4} + \frac{4}{16} + \frac{4}{64} \sum_{b=0}^{\infty} \frac{1}{2^b}\right) \sum_{a=0}^{\infty} \frac{1}{31^a} = \frac{31}{16}.$$

Note that formula (14) also yields that $v(D) = 31/16$.

`Remark`. Fomenko [12] has given an alternative proof of Bernays' asymptotic result using modular forms in which the constant $C(f)$ is explicitly computed in case D is a fundamental discriminant. Namely, we have (see [12, Theorem 4]) for a fundamental discriminant D,

$$B_f(x) \sim \frac{P(D)}{2^{t(D)}} \frac{x}{\sqrt{\log x}}, \quad (15)$$

where $P(D)$ is Pall's constant. Is there a modular forms approach which computes $C(f)$ for arbitrary discriminant D?

`Remark`. It might be of some interest to recover $C(f)$ in general following Iwaniec's approach to the half-dimensional sieve. Using this sieve (see [13]), the constant $C(f_1)$ was verified for $f_1 = X^2 + Y^2$.

3 On explicitly computing the Erdős number

The explicit formula (14) for $\nu(D)$ allows one to explicitly compute the Erdős number $E(D)$. Note that from (7), (4) and (8) it follows that

$$E(D) = \frac{\nu(D)}{2^{t(D)+1}}\sqrt{\frac{L(1,\chi_D)\varphi(|D|)}{\pi}}\prod_{(\frac{D}{p})=-1}\Big(1-\frac{1}{p^2}\Big)^{-1/2}, \tag{16}$$

where $\nu(D)$ is explicitly given by (14).

The latter formula unfortunately does not allow one to compute $E(D)$ with more that a few decimals of accuracy. A problem in doing is that the Euler product involved on direct evaluation (by multiplying consecutive terms together) can be evaluated with roughly six digit precision only. However, it turns out that it is possible to express these Euler products in terms of L-series evaluated at integer arguments. To this end note that for $\Re(s) > 1/2$,

$$\prod_{(\frac{D}{q})=-1}(1-q^{-2s})^{-2} = \frac{\zeta(2s)}{L(2s,\chi_D)}\prod_{(\frac{D}{q})=0}(1-q^{-2s})\prod_{(\frac{D}{q})=-1}(1-q^{-4s})^{-1}. \tag{17}$$

By recursion we then find from (16) and (17) the following formula:

$$E(D) = \frac{\nu(D)}{2^{t(D)+1}}\sqrt{\frac{L(1,\chi_D)\varphi(|D|)}{\pi}}\prod_{n=1}^{\infty}\Big(\frac{\zeta(2^n)}{L(2^n,\chi_D)}\prod_{(\frac{D}{q})=0}(1-q^{-2^n})\Big)^{1/2^{n+1}}. \tag{18}$$

This approach was already known to Ramanujan [2, pp. 60–66] and, independently, Shanks [34, p. 78]. It can also be used to deal with more elementary Euler products of the form $\prod_{p>p_0}(1-f(p)/g(p))$, where f and g are polynomials such that $\deg(f)+2 \le \deg(g)$, see e.g. [18]. In the latter case only values of $\zeta(s)$ at integers are required.

We note that in case D is a fundamental discriminant $\nu(D) = |D|/\varphi(|D|)$ and $t(D) = \omega(D) - 1$ and hence

$$E(D) = \frac{|D|}{2^{\omega(D)}}\sqrt{\frac{L(1,\chi_D)}{\pi\varphi(|D|)}}\prod_{n=1}^{\infty}\Big(\frac{\zeta(2^n)}{L(2^n,\chi_D)}\prod_{(\frac{D}{q})=0}(1-q^{-2^n})\Big)^{1/2^{n+1}}. \tag{19}$$

4 Some computations of Shanks and Schmid revisited

We demonstrate our above approach in computing the Erdős number (and hence by (7) the Bernays constant $C(f)$), by recomputing the entries in Table 1 from a paper by Shanks and Schmid [35]. They put $C(X^2 + nY^2) = b_n$ and we will follow their notation. The second column in the following table corresponds to the values of b_n as computed in [35] to nine decimal places (for $n = 11$, $n = 13$ and $n = 14$, approximate values of b_n were given). The third column in the table is the computation of b_n using (7) and (18).

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

5 Proof of Theorem 1

The idea of the proof is to use a lower bound estimate for $\varphi(|D|)$ combined with an upper bound estimate for $\omega(D)$ to show that $E(D) > E(-3)$ for all $|D| \geq D_0$, with D_0 an explicit number. In the range $|D| < D_0$ one then determines those D for which the quickly computed lower bound for $E(D)^2$ given in (21) does not exceed $E(-3)^2$. For these values of D one then computes $E(D)$ using (18) and compares with $E(-3)$.

Proof of Theorem 1. Note that $h(D) \geq 2^{t(D)}$, $v(D) \geq 1$ and that the Euler product in (16) exceeds one. Using these trivial lower bounds and (16) we infer that

$$E(D) \geq \left(\frac{1}{2^{t(D)+1} w(D)} \frac{\varphi(|D|)}{|D|^{1/2}} \right)^{1/2}, \tag{20}$$

where we used that $L(1, \chi_D) = 2\pi h(D)/(w(D)\sqrt{|D|})$. It is well-known that in case D is a fundamental discriminant $w(D) \neq 2$ if and only if $D = -3$ or $D = -4$. Using the observation that that order for the discriminant D is the $\mathbb{Z}$-module generated by 1 and $f(D + \sqrt{D})/2$ (cf. [10, Lemma 7.2]), where f is the conductor, one sees that $w(D) = 2$ unless $D = -4$ or $D = -3$. In the rest of the proof we assume that $|D| \geq 5$. Then

$$E(D)^2 \geq \frac{\varphi(|D|)}{2^{t(D)+2}\sqrt{|D|}}. \tag{21}$$

Put $g(n) = \varphi(n)/(2^{\omega(n)}\sqrt{n})$. Note that g is a multplicative function of n. If $n = \prod_{i=1}^m q_i^{e_i}$ denotes the canonical factorisation of n, then

$$g(n) = \prod_{i=1}^m \frac{1}{2} q_i^{e_i/2-1}(q_i - 1) \geq \prod_{i=1}^m \frac{1}{2}(\sqrt{q_i} - \frac{1}{\sqrt{q_i}}).$$

We let $p_1 = 2,\ p_2 = 3, \cdots$ denote the consecutive primes. Note that $\sqrt{x} - \frac{1}{\sqrt{x}}$ is strictly increasing with x. It thus follows that

$$g(n) \geq \prod_{i=1}^{m} \frac{1}{2}(\sqrt{p_i} - \frac{1}{\sqrt{p_i}}).$$

If n is odd, then we similarly have

$$g(n) \geq \prod_{i=2}^{m+1} \frac{1}{2}(\sqrt{p_i} - \frac{1}{\sqrt{p_i}}). \tag{22}$$

From (10) and (21) one infers that

$$E(D)^2 \geq \alpha(D) g(D_{\text{odd}}), \tag{23}$$

where

$$\alpha(D) = \begin{cases} 1/4 & \text{if } D \equiv 12 (\text{mod } 16); \\ 1/2\sqrt{2} & \text{if } D \equiv 8 (\text{mod } 16) \text{ or } D \equiv 0 (\text{mod } 32); \\ 1/2 & \text{if } D \equiv 1 (\text{mod } 4),\ D \equiv 0 (\text{mod } 16) \text{ or } D \equiv 4 (\text{mod } 16), \end{cases}$$

and D_{odd} denotes the largest odd divisor of D.

First assume that $D \equiv 1(\text{mod } 4)$ (thus $\alpha(D) = 1/2$ and $t(D) = \omega(D) - 1$). Then, from (23) and (22) we infer that

$$2E(D)^2 \geq \prod_{i=2}^{\omega(D)+1} \frac{1}{2}(\sqrt{p_i} - \frac{1}{\sqrt{p_i}}).$$

If $\omega(D) > 3$ it follows from the latter inequality that $E(D) > 0.66 > E(-3)$. So let us assume that $\omega(D) \leq 3$. It now follows, using that

$$\varphi(n) > e^{-\gamma} \frac{n}{\log\log n}, \tag{24}$$

for all odd integers $n \geq 17$ (see [8]), that for $|D| \geq 19$ we have

$$E(D)^2 \geq \frac{\varphi(|D|)}{16\sqrt{|D|}} \geq \frac{e^{-\gamma}}{16} \frac{\sqrt{|D|}}{\log\log|D|}.$$

From this estimate one infers that $E(D) > E(-3)$ for $|D| \geq 217$. For the D with $D \equiv 1(\text{mod } 4)$ and $7 \leq |D| \leq 215$ one checks that

$$\left(\frac{\varphi(|D|)}{2^{\omega(D)+1}\sqrt{|D|}} \right)^{1/2} > 0.6 > E(-3),$$

except for $D = -15$. A direct computation shows that $E(-15) = 0.9719612\cdots > E(-3)$.

The remaining cases are dealt with similarly: on noting that the right hand side of (22) is monotonically increasing for $m \geq 2$ one uses (23) to obtain an upper bound for $\omega(D)$. From this upper bound, (21) and (24), one then finds an integer D_0 such that if $E(D) > E(-3)$, then $|D| < D_0$. For the discriminants D with $|D| < D_0$ one then computes the discriminants D for which the left hand side of (21) does not exceed $E(-3)^2$. For these D values one then computes $E(D)$ using (18). One finds that for all these values of D one has $E(D) > E(-3)$. In this way it is seen that $E(D)$ is minimal for $D = -3$.

To prove the second assertion note that in the above argument one can replace $E(-3)$ with any real number r. In the end one is left with a finite list of D for which $E(D) < r$. $\square$

`Example`. If $r = 1$, then one finds the following list.

D	$E(D)$
-3	0.55331177583247955595155817776
-4	0.76422365358922066299069873311
-7	0.95871381203988677071780434483
-15	0.97196125963599060498175629880

Thus the second smallest lattice is given by the maximal order with $D = -4$ (the square lattice) and the third and fourth smallest lattices by $D = -7$ and $D = -15$ respectively.

`Remark`. The inequality (24) is quite subtle. Let $N_k = 2 \cdot 3 \cdots p_k$ be the product of the first k primes, then if the Riemann Hypothesis is true (24) is false for every integer n with $n = N_k$. On the other hand, if the Riemann Hypothesis is false then there are infinitely many integers k for which $n = N_k$ does satisfy (24). See Nicolas [23] for a proof of this interesting result.

Acknowledgement

This paper owes much to an inspiring discussion with Prof. Don Zagier in which he convinced the first author that proving Theorem 1 should be doable. The authors would like to thank Valentin Blomer for his helpful comments regarding Bernays' thesis and K.S. Williams for making his preprint [37] available. It is also a pleasure to thank UCD graduate student Raja Mukherji for his suggestions which greatly improved the efficiency of the GP/PARI program which was used in Sections 4 and 5. Finally, the authors thank the Max-Planck-Institut für Mathematik in Bonn for its hospitality and support during the preparation of this paper.

References

[1] 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/`

[2] B.C. Berndt, *Ramanujan's notebooks.* Part IV, Springer-Verlag, New York, 1994.

[3] B.C. Berndt and K. Ono, Ramanujan's unpublished manuscript on the partition and tau functions with proofs and commentary. The Andrews Festschrift (Maratea, 1998), *Sém. Lothar. Combin.* **42** (1999), Art. B42c, 63 pp.

[4] H.F. Blichfeldt, The minimum values of positive quadratic forms in six, seven and eight variables, *Math. Z.* **39** (1935), 1–15.

[5] V. Blomer, Binary quadratic forms with large discriminants and sums of two squareful numbers, *J. Reine Angew. Math.* **569** (2004), 213–234.

[6] V. Blomer, Binary quadratic forms with large discriminants and sums of two squareful integers II, *J. London Math. Soc.* **71** (2005), 69–84.

[7] V. Blomer and A. Granville, Estimates for representation numbers of quadratic forms, to appear in Duke Math. J.

[8] Y.-J. Choie, N. Lichiardopol, P. Moree and P. Solé, On Robin's criterion for the Riemann Hypothesis, arXiv:math.NT/0604163, submitted.

[9] J.H. Conway and N.J.A. Sloane, Lattices with few distances, *J. Number Theory* **39** (1991), 75–90.

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

[11] S.R. Finch, *Mathematical constants*, Encyclopedia of Mathematics and its Applications **94**, Cambridge University Press, Cambridge, 2003.

[12] O.M. Fomenko, Distribution of values of Fourier coefficients of modular forms of weight 1, *J. Math. Sci. (New York)* **89** (1998), 1050–1071.

[13] H. Iwaniec, The half dimensional sieve, *Acta Arith.* **29** (1976), 69–95.

[14] R.D. James, The distribution of integers represented by quadratic forms, *Amer. J. Math.* **60** (1938), 737–744.

[15] P. Kaplan and K.S. Williams, The genera representing a positive integer, *Acta Arith* **102** (2002), no. 4, 353–361.

[16] S. Kühnlein, Partial solution of a conjecture of Schmutz, *Arch. Math.* **67** (1996), 164–172.

[17] 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.

[18] P. Moree, Approximation of singular series and automata, *Manuscripta Math.* **101** (2000), 385–399.

[19] P. Moree, Chebyshev's bias for composite numbers with restricted prime divisors, *Math. Comp.* **73** (2004), 425–449.

[20] P. Moree, On some claims in Ramanujan's 'unpublished' manuscript on the partition and tau functions, *Ramanujan J.* **8** (2004), 317–330.

[21] P. Moree and J. Cazaran, On a claim of Ramanujan in his first letter to Hardy, *Exposition. Math.* **17** (1999), 289–311.

[22] P. Moree and H.J.J. te Riele, The hexagonal versus the square lattice, *Math. Comp.* **73** (2004), 451–473.

[23] J.-L. Nicolas, Petites valeurs de la fonction d'Euler, *J. Number Theory* **17** (1983), 375–388.

[24] R.W.K. Odoni, Representations of algebraic integers by binary quadratic forms and norm forms from full modules of extension fields, *J. Number Theory* **10** (1978), 324–333.

[25] R.W.K. Odoni, The distribution of integral and prime-integral values of systems of full-norm polynomials and affine-decomposable polynomials, *Mathematika* **26** (1979), 80–87.

[26] R.W.K. Odoni, A problem of Erdős on sums of two squarefull numbers, *Acta Arith.* **39** (1981), 145–162

[27] G. Pall, The distribution of integers represented by binary quadratic forms, *Bull. Amer. Math. Soc.* **49** (1943), 447–449.

[28] C. Reid, *Hilbert*, Springer-Verlag, New York-Berlin, 1970.

[29] G.J. Rieger, Zur Satz von Landau über die Summe aus zwei Quadraten, *J. Reine Angew. Math.* **244** (1970), 198–200.

[30] W. Scharlau and H. Opolka, *Von Fermat bis Minkowski. Eine Vorlesung über Zahlentheorie und ihre Entwicklung*, Springer-Verlag, Berlin-New York, 1980.

[31] P. Schmutz, Arithmetic groups and the length spectrum of Riemann surfaces, *Duke Math. J.* **84** (1996), 199–215.

[32] P. Schmutz Schaller, Geometry of Riemann surfaces based on closed geodesics, *Bull. Amer. Math. Soc. (N.S.)* **35** (1998), 193–214.

[33] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, *Enseignement Math.* **22** (1976), 227–260.

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

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

[36] W.D. Smith, Few-distance sets and the second Erdös number, unpublished preprint (1990).

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

[38] K.S. Williams, Note on integers representable by binary quadratic forms, *Canad. Math. Bull.* **18** (1975), 123–125.

[39] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen, *Math. Ann.* **143** (1961), 75–102.

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.
e-mail: `moree@mpim-bonn.mpg.de`

School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland.
e-mail: `robert.osburn@ucd.ie`