On lattices, distinct distances, and the Elekes-Sharir framework*

Javier Cilleruelo† Micha Sharir‡ Adam Sheffer§

July 1, 2013

Abstract

In this note we consider distinct distances determined by points in an integer lattice. We first consider Erdős's lower bound for the square lattice, recast in the setup of the so-called Elekes-Sharir framework [5, 8], and show that, without a major change, this framework *cannot* lead to Erdős's conjectured lower bound. This shows that the upper bound of Guth and Katz [8] for the related 3-dimensional line-intersection problem is tight for this instance. The gap between this bound and the actual bound of Erdős arises from an application of the Cauchy-Schwarz inequality (which is an integral part of the Elekes-Sharir framework). Our analysis relies on two number-theoretic results by Ramanujan.

We also consider distinct distances in rectangular lattices of the form $\{(i,j) \mid 0 \le i \le n^{1-\alpha},\ 0 \le j \le n^{\alpha}\}$, for some $0 < \alpha < 1/2$, and show that the number of distinct distances in such a lattice is $\Theta(n)$. In a sense, our proof "bypasses" a deep conjecture in number theory, posed by Cilleruelo and Granville [4]. A positive resolution of this conjecture would also have implied our bound.

1 On the limitations of the Elekes-Sharir framework

Given a set $\mathcal{P}$ of n points in $\mathbb{R}^2$, let $D(\mathcal{P})$ denote the number of distinct distances that are determined by pairs of points from $\mathcal{P}$. Let $D(n) = \min_{|\mathcal{P}|=n} D(\mathcal{P})$; that is, $D(n)$ is the minimum number of distinct distances that any set of n points in $\mathbb{R}^2$ must always determine. In his celebrated 1946 paper [6], Erdős derived the bound $D(n) = O(n/\sqrt{\log n})$ by considering a $\sqrt{n} \times \sqrt{n}$ integer lattice. Recently, after 65 years and a series of increasingly larger lower bounds[1], Guth and Katz [8] provided an almost matching lower bound $D(n) = \Omega(n/\log n)$. For this, Guth and Katz simplified the Elekes-Sharir framework [5], developed by Elekes, and slightly refined by Sharir, for tackling the distinct distances problem, to

*Work by Javier Cilleruelo has been supported by grants MTM 2011-22851 of MICINN and ICMAT Severo Ochoa project SEV-2011-0087. Work by Adam Sheffer and Micha Sharir has been supported by Grant 338/09 from the Israel Science Fund, by the Israeli Centers of Research Excellence (I-CORE) program (Center No. 4/11), and by the Hermann Minkowski-MINERVA Center for Geometry at Tel Aviv University.

†Instituto de Ciencias Matematicas (CSIC-UAM-UC3M-UCM), and Departamento de Matematicas, Universidad Autónoma de Madrid, 28049 Madrid, Spain. *franciscojavier.cilleruelo@uam.es*

‡School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. *michas@tau.ac.il*

§School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. *sheffera@tau.ac.il*

[1]For a comprehensive list of the previous bounds, see [7] and `http://www.cs.umd.edu/~gasarch/erdos_dist/erdos_dist.html` (version of May 2013).

make it reduce this latter problem to a problem about line intersections in $\mathbb{R}^3$. To solve this problem, Guth and Katz developed several novel techniques, relying on tools from algebraic geometry and 19th century analytic geometry.

In this note, we examine the gap of $\Theta(\sqrt{\log n})$ between Erdős's upper bound and Guth and Katz's lower bound for the vertex set of the square lattice considered by Erdős. While it is conceivable that there exists a set of n points that spans $\Theta(n/\log n)$ distinct distances, the common belief is that $D(n) = \Theta(n/\sqrt{\log n})$. We prove that, even if this common belief is correct, the Elekes-Sharir framework cannot lead to the actual bound without a major improvement of the technique (more specifically, without replacing the use of the Cauchy-Schwarz inequality by some other technique).

We begin by recalling some of the basics of the Elekes-Sharir framework [5, 8]. Consider a set $\mathcal{P}$ of n points in the plane and put $x = D(\mathcal{P})$. The reduction revolves around the set

$$Q = \left\{(a, p, b, q) \in \mathcal{P}^4 \mid |ap| = |bq| > 0\right\};$$

The quadruples in Q are ordered, in the sense that (a, p, b, q), (b, p, a, q), (p, a, q, b), and the other possible permutations are all considered as distinct elements of Q. Also, in a quadruple $(a, p, b, q) \in Q$, the segments ap and bq are allowed to share vertices or even coincide.

Basically, the reduction is just double counting $|Q|$, and we now present the lower bound. We put $x = D(\mathcal{P})$, and denote the set of (nonzero) distinct distances that are determined by $\mathcal{P} \times \mathcal{P}$ as $\delta_1, \ldots, \delta_x$. Also, for $1 \le i \le x$, we set

$$E_i = \left\{(p, q) \in \mathcal{P}^2 \mid |pq| = \delta_i\right\}.$$

As before, we consider (p, q) and (q, p) as two distinct pairs in E_i. Notice that $\sum_{i=1}^{x} |E_i| = n^2 - n$ since every ordered pair of distinct points of $\mathcal{P} \times \mathcal{P}$ is contained in a unique set E_i. By applying the Cauchy-Schwarz inequality, we have

$$|Q| = \sum_{i=1}^{x} |E_i|^2 \ge \frac{1}{x}\left(\sum_{i=1}^{x} |E_i|\right)^2 = \frac{(n^2 - n)^2}{x}. \tag{1}$$

Guth and Katz [8] derive the upper bound $|Q| = O(n^3 \log n)$ which, combined with the above lower bound, immediately implies $x = \Omega(n/\log n)$. Deriving this upper bound is considerably more complicated, and we do not discuss it here. We show that, for the vertex set of the square lattice, Guth and Katz's bound is tight; that is, $|Q| = \Theta(n^3 \log n)$.

We next recall the full details of Erdős's lower bound [6]. We take $\mathcal{P} = \{(i, j) \mid 1 \le i, j \le \sqrt{n}\}$; that is, $\mathcal{P}$ is the vertex set of a $\sqrt{n} \times \sqrt{n}$ integer lattice, as depicted in Figure 1(a). We require the following theorem from number theory.

Theorem 1.1 (Landau-Ramanujan [1, 9]) *The number of positive integers smaller than n that are the sum of two squares is $\Theta(n/\sqrt{\log n})$.*

Every distance determined by a pair from $\mathcal{P} \times \mathcal{P}$ is of the form $\sqrt{i^2 + j^2}$ where $0 \le i, j \le \sqrt{n}$. The cases where $i = 0$ or $j = 0$ contribute negligible amounts to $D(\mathcal{P})$ and may thus be ignored. Therefore, Theorem 1.1 implies that $D(\mathcal{P}) = \Theta(n/\sqrt{\log n})$. This in turn implies that, for this special set $\mathcal{P}$, the value of the rightmost expression in (1) is $\Theta(n^3\sqrt{\log n})$.

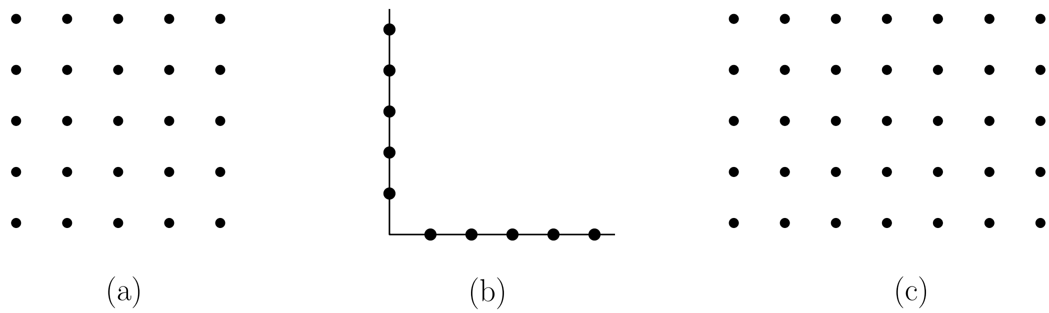

Figure 1: (a) A $\sqrt{n} \times \sqrt{n}$ integer lattice. (b) An L-shaped configuration. (c) A non-square integer lattice.

Notice that there is a gap of $\sqrt{\log n}$ between this bound and the upper bound $|Q| = O(n^3 \log n)$. To see where this gap comes from, we rely on another result by Ramanujan.

Recall the expression $\sum_{i=1}^{x} |E_i|^2$ from (1) just before applying the Cauchy-Schwarz inequality. For a positive integer k, we set $r(k) = \left|\{(i,j) \in \mathbb{N}^2 \mid i^2 + j^2 = k\}\right|$, and also $\hat{r}(k) = \sum_{i=1}^{k} r(i)^2$. Consider a distance $1 \le \delta \le \sqrt{n}/10$, say, such that $\delta = \sqrt{i^2 + j^2}$ for some $i, j \in \mathbb{N}$. Clearly, every point of $\mathcal{P}$ lies at distance δ from $r(\delta^2)$ other points of $\mathcal{P}$. This implies that

$$\sum_{i:\delta_i < \sqrt{n}/10} |E_i|^2 = \Omega(n^2 \hat{r}(n/100)).$$

Theorem 1.2 (Ramanujan [10]). *$\hat{r}(k) = \Theta\left(k \log k\right)$.*

By combining Theorem 1.2 with the above reasoning, we obtain

$$\sum_{i=1}^{x} |E_i|^2 = \Omega(n^2 \hat{r}(n/100)) = \Omega(n^3 \log n).$$

Thus, by applying the Cauchy-Schwarz inequality, we lose a factor of $\sqrt{\log n}$ which prevents the framework from implying the correct bound $D(\mathcal{P}) = \Theta(n/\sqrt{\log n})$. Moreover, since we obtain the lower bound of $|Q| = \Omega(n^3 \log n)$, Guth and Katz's upper bound on the number of line intersections is tight in this case.

Remarks. (i) The fact that the Cauchy-Schwarz inequality forms a gap in this case indicates that the sizes of the sets E_i are highly non-uniform. Note that $E_i = \Theta(nr(\delta_i^2))$ (as long as δ_i is not too close to $\sqrt{n}$). Since there are only $x = \Theta(n/\sqrt{\log n})$ such sets (by Theorem 1.1), and since $\sum_{i=1}^{x} |E_i| = \Theta(n^2)$, the average size of these sets is $\Theta(n\sqrt{\log n})$. That is, the average value of the quantities $r(\delta_i^2)$, for $i = 1, \ldots, x$, is $\Theta(\sqrt{\log n})$, but the average of their squares is $\dfrac{1}{x}\sum_{i=1}^{x} r(\delta_i^2)^2 = \Theta\left((\log n)^{3/2}\right)$ (by Theorem 1.2). This indicates that the values $r(\delta_i^2)$ form a rather non-uniform sequence, for which the Cauchy-Schwarz inequality is too weak.

(ii) One might also compare this with Erdős's lower bound construction for the *repeated distances problem* [6], which relied on the property that for infinitely many values $r(\delta_i^2)$ can be as high as $n^{c/\log\log n}$ (for some universal constant c).

The case of an L-shaped configuration. We next consider a different configuration, in which the Cauchy-Schwarz inequality yields a surprisingly large gap of $\Theta(n/\sqrt{\log n})$. We set $\mathcal{P}_1 = \{(1,0),(2,0),\ldots,(n,0)\}$, a set of n evenly spaced points on the x-axis, and similarly, define $\mathcal{P}_2 = \{(0,1),(0,2),\ldots,(0,n)\}$ on the y-axis. Figure 1(b) illustrates the configuration $\mathcal{P}' = \mathcal{P}_1 \cup \mathcal{P}_2$. Every distance determined by $\mathcal{P}'$ is the square root of a sum of two squares, where each such sum is between 0 and $2n^2$. Thus, Theorem 1.1 implies $D(\mathcal{P}') = \Theta(n^2/\sqrt{\log n})$.

We define Q as before and repeat the analysis in (1), which implies the lower bound $|Q| = \Omega(n^4/D(\mathcal{P}')) = \Omega(n^2\sqrt{\log n})$. However, the value of the expression from (1) before applying the Cauchy-Schwarz inequality is $\Theta(n^3)$. To see why, let d_i, for $i = 1,\ldots,n-1$, denote the number of pairs in $\mathcal{P}'^2$ that span a distance of i (not to be confused with δ_i).

For $1 \le i \le n/2$, we have $d_i = \Theta(n)$ (most of these distances are realized in $(\mathcal{P}_1 \times \mathcal{P}_1) \cup (\mathcal{P}_2 \times \mathcal{P}_2)$). Reconsidering the analysis in (1), we have

$$|Q| = \sum_{i=1}^{x} |E_i|^2 > \sum_{i=1}^{n/2} d_i^2 = \Omega(n^3).$$

That is, if we perform the rest of the analysis as in the Elekes-Sharir framework, we only obtain (at best) the weak lower bound $D(\mathcal{P}') = \Omega(n)$. The reason for this discrepancy is that the "trivial" distances $1,2,\ldots,n/2$ generate $\Omega(n^3)$ quadruples in Q, whereas the "real" inter-line distances generate only a nearly quadratic number of quadruples. The discrepancy would have been much lower if the analysis could have discarded the trivial distances, for example, by considering the *bipartite* version of the problem, which only takes into account the distinct distances in $\mathcal{P}_1 \times \mathcal{P}_2$; see [11] for a study of this variant. The non-bipartite situation is another instance in which the values $|E_i|$ are (significantly more) non-uniformly distributed.

2 Distinct distances in rectangular lattices

In the second part of this note we consider the number of distinct distances that are determined by an $n^{1-\alpha} \times n^{\alpha}$ integer lattice, for some $0 < \alpha \le 1/2$. We denote this number by $D_\alpha(n)$.

The case $\alpha = 1/2$ is the case of the square $\sqrt{n} \times \sqrt{n}$ lattice, which determines $D_{1/2}(n) = \Theta(n/\sqrt{\log n})$ distinct distances, as reviewed in Section 1. Surprisingly, we show here a different estimate for $\alpha < 1/2$.

Theorem 2.1 *For $\alpha < 1/2$ we have $D_\alpha(n) = \Theta(n)$.*

Proof. We consider the rectangular lattice

$$R_\alpha(n) = \{(i,j) \mid 0 \le i \le n^{1-\alpha},\ 0 \le j \le n^{\alpha}\},$$

and its sublattice,

$$R'_\alpha(n) = \{(i,j) \mid 2n^{\alpha} \le i \le n^{1-\alpha},\ 0 \le j \le n^{\alpha}\};$$

since $\alpha < 1/2$, $R'_\alpha(n) \neq \emptyset$ for $n \geq n_0(\alpha)$, a suitable constant depending on α. We also consider the functions

$$r(m) = \left|\{(i,j) \in R'_\alpha(n) \;\mid\; i^2 + j^2 = m\}\right|,$$
$$d(m) = \left|\{(i,j) \in R'_\alpha(n) \;\mid\; i^2 - j^2 = m\}\right|.$$

Observe that the smallest (resp., largest) value of m for which $d(m) \neq 0$ is $3n^{2\alpha}$ (resp., $n^{2-2\alpha}$).

We have the identities

$$\sum_m r(m) = \sum_m d(m), \tag{2}$$

$$\sum_m r^2(m) = \sum_m d^2(m). \tag{3}$$

The identity (2) is trivial. To see (3) we observe that the sum $\sum_m r^2(m)$ counts the number of ordered quadruples (i,j,i',j'), for $(i,j),(i',j') \in R'_\alpha(n)$, such that $i^2 + j^2 = i'^2 + j'^2$. But this quantity also counts the number of those ordered quadruples (i,j,i',j'), for $(i,j'),(i',j) \in R'_\alpha(n)$, such that $i^2 - j'^2 = i'^2 - j^2$, which is the value of the sum $\sum_m d^2(m)$. Putting (2) and (3) together we have

$$\sum_m \binom{r(m)}{2} = \sum_m \binom{d(m)}{2}. \tag{4}$$

It is clear that $D_\alpha(n) \leq |R_\alpha(n)| = n + O(n^{1-\alpha})$. In the rest of the proof we derive a matching lower bound for $D_\alpha(n)$.

Writing M_k for the set of those m with $r(m) = k$, we have $\sum_k k|M_k| = |R'_\alpha(n)|$. On the other hand,

$$\begin{aligned} D_\alpha(n) &\geq \sum_{k\geq 1} |M_k| \\ &= \sum_{k\geq 1} k|M_k| - \sum_{k\geq 1}(k-1)|M_k| \\ &= |R'_\alpha(n)| - \sum_{k\geq 2}(k-1)|M_k|. \end{aligned}$$

Thus $D_\alpha(n) \geq n - O(n^{2\alpha}) - \sum_{k\geq 2}(k-1)|M_k|$. Using the inequality $k - 1 \leq \binom{k}{2}$ and (4), we have

$$\sum_{k\geq 2}(k-1)|M_k| \leq \sum_{k\geq 2}\binom{k}{2}|M_k| = \sum_m \binom{r(m)}{2} = \sum_m \binom{d(m)}{2}.$$

Theorem 2.1 is therefore a trivial consequence of the following proposition. ◻

Proposition 2.2

$$\sum_m \binom{d(m)}{2} = O\left(n^{2\alpha}\log^2 n\right).$$

Proof. We need the following easy lemma.

Lemma 2.3 *If m can be written as the product of two integers in two different ways, say $m = m_1 m_2 = m_3 m_4$, then there exists a quadruple of positive integers (s_1, s_2, s_3, s_4) satisfying*

$$m_1 = s_1 s_2, \quad m_2 = s_3 s_4, \quad m_3 = s_1 s_3, \quad m_4 = s_2 s_4.$$

Proof. Since m_1 divides $m_3 m_4$, we have $m_1 = s_1 s_2$ for some $s_1 \mid m_3$ and some $s_2 \mid m_4$. Putting $s_3 = m_3/s_1$ and $s_4 = m_4/s_2$, we have $m_2 = s_3 s_4$, $m_3 = s_1 s_3$, and $m_4 = s_2 s_4$. ◻

We write

$$\sum_m \binom{d(m)}{2} = \sum_{1 \le l \le n^{1-2\alpha}} \sum_{m \in I_l} \binom{d(m)}{2},$$

where $I_l = [l^2 n^{2\alpha}, (l+1)^2 n^{2\alpha})$. We observe that the union of the intervals, namely $[n^{2\alpha}, (1+n^{1-2\alpha})^2 n^{2\alpha})$, covers all the possible m with $d(m) \neq 0$.

Now we estimate $\sum_{m \in I_l} \binom{d(m)}{2}$ for a fixed l. Let $a^2 - b^2 = c^2 - d^2$ ($a > c$ and $b > d$) be a pair of distinct representations of some m, which is counted in the above sum $\sum_{m \in I_l} \binom{d(m)}{2}$. Since $m \in I_l$ we have

$$l^2 n^{2\alpha} \le a^2 - b^2 < (l+1)^2 n^{2\alpha}.$$

Thus,

$$l^2 n^{2\alpha} \le a^2 < (l+1)^2 n^{2\alpha} + b^2 \le ((l+1)^2 + 1) n^{2\alpha} < (l+2)^2 n^{2\alpha}.$$

The same inequality holds for c, so we have

$$l n^\alpha \le a, c < (l+2) n^\alpha. \tag{5}$$

Applying Lemma 2.3 to $(a-c)(a+c) = (b-d)(b+d)$, we obtain a quadruple (s_1, s_2, s_3, s_4) satisfying

$$\begin{aligned} s_1 s_2 &= a - c, & s_3 s_4 &= a + c, \\ s_1 s_3 &= b - d, & s_2 s_4 &= b + d. \end{aligned}$$

Using (5) and $0 \le b, d \le n^\alpha$ we have the following inequalities:

$$\begin{aligned} 1 \le s_1 s_2,\ s_1 s_3,\ & s_2 s_4 \le 2n^\alpha, \\ 2ln^\alpha \le & s_3 s_4 < (2l+4) n^\alpha. \end{aligned} \tag{6}$$

It is clear from the above inequalities that $s_i \le 2n^\alpha$, for $i = 1, \ldots, 4$. From $s_2 s_4 \le 2n^\alpha$, $s_1 s_3 \le 2n^\alpha$, and $2ln^\alpha \le s_3 s_4$, we also deduce that

$$1 \le s_2 \le \frac{s_3}{l} \qquad \text{and} \qquad 1 \le s_1 \le \frac{s_4}{l}. \tag{7}$$

Choose s_3 between 1 and $2n^\alpha$. Then choose s_4, according to (6), in the range $[\frac{2ln^\alpha}{s_3}, \frac{(2l+4)n^\alpha}{s_3})$. Then choose s_1 and s_2, according to (7), in $\frac{s_3}{l} \cdot \frac{s_4}{l} \le \frac{(2l+4)n^\alpha}{l^2}$ ways. The overall number of quadruples (s_1, s_2, s_3, s_4) under consideration is thus at most

$$\sum_{1 \le s_3 \le 2n^\alpha} \frac{4n^\alpha}{s_3} \cdot \frac{(2l+4)n^\alpha}{l^2} = O\left(\frac{n^{2\alpha} \log n}{l}\right).$$

Finally we have

$$\sum_m \binom{d(m)}{2} \le \sum_{1\le l\le n^{1-2\alpha}} \sum_{m\in I_l} \binom{d(m)}{2} = O\left(\sum_{l\le n^{1-2\alpha}} \frac{n^{2\alpha}\log n}{l} \right) = O\left(n^{2\alpha}\log^2 n\right).$$

$\square$

Discussion. Theorem 2.1 is closely related to a special case of a fairly deep conjecture in number theory, stated as Conjecture 13 in Cilleruelo and Granville [4]. This special case, given in [4, Eq. (5.1)], asserts that, for any integer N, and any fixed $\beta < 1/2$,

$$\left|\{(a,b) \mid a^2+b^2 = N,\ |b| < N^\beta\}\right| \le C_\beta,$$

where C_β is a *constant* that depends on β (but not on N). A simple geometric argument shows that this is true for $\beta \le 1/4$ but it is unknown for any $1/4 < \beta < 1/2$. If that latter conjecture were true, a somewhat weaker version of Theorem 2.1 would follow. Indeed, let N be an integer that can be written as $i^2 + j^2$, for $\frac{1}{2}n^{1-\alpha} \le i \le n^{1-\alpha}$ and $j \le n^\alpha$. Then $N = \Theta(n^{2(1-\alpha)})$, and $j = O(N^\beta)$, for $\beta = \alpha/(2(1-\alpha)) < 1/2$.

Conjecture 13 of [4] would then imply that the number of pairs (i,j) as above is at most the constant C_β. In other words, each of the $\Theta(n)$ distances in the portion of $R_\alpha(n)$ with $i \ge \frac{1}{2}n^{1-\alpha}$, interpreted as a distance from the origin $(0,0)$, can be attained at most C_β times. Hence $D_\alpha(n) = \Theta(n)$, as asserted in Theorem 2.1.

The general form of conjecture 13 [4] asserts that the number of integer lattice points on an arc of length N^β on the circle $a^2+b^2 = N$ is bounded by some constant C_β, for any $\beta < 1/2$. Cilleruelo and Córdoba [3] have proved this for $\beta < 1/4$. See also Bourgain and Rudnick [2] for some consequences of this conjecture.

Acknowledgements. The authors would like to thank Zeev Rudnick for useful discussions on some of the number-theoretic issues. The third author would like to thank Orit Raz and Joshua Zahl for several helpful discussions.

References

[1] B. C. Berndt and R. A. Rankin, *Ramanujan: Letters and Commentary*, Amer. Math. Soc., Providence, RI, 1995.

[2] J. Bourgain and Z. Rudnick, On the Geometry of the Nodal Lines of Eigenfunctions of the Two-Dimensional Torus, *Annales Henri Poincaré*, **12** (2011), 1027–1053.

[3] J. Cilleruelo and A. Córdoba, Trigonometric polynomials and lattice points, *Proc. Amer. Math. Soc.* **115** (1992), 899–905.

[4] J. Cilleruelo and A. Granville, Lattice points on circles, squares in arithmetic progressions and sumsets of squares, in *Additive Combinatorics*, CRM Proceedings and Lecture Notes, Vol. 43, Amer. Math. Soc. Press, RI, 2007, 241–262.

[5] G. Elekes and M. Sharir, Incidences in three dimensions and distinct distances in the plane, *Combinat. Probab. Comput.* **20** (2011), 571–608.

[6] P. Erdős, On sets of distances of n points, *Amer. Math. Monthly* **53** (1946), 248–250.

[7] J. Garibaldi, A. Iosevich, and S. Senger, *The Erdős Distance Problem*, Student Math. Library, Vol. 56, Amer. Math. Soc., Providence, RI, 2011.

[8] L. Guth and N. H. Katz, On the Erdős distinct distances problem in the plane, in arXiv:1011.4105.

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

[10] S. Ramanujan, Some formulae in the analytic theory of numbers, *Messenger of Mathematics* **46** (1916), 81–84.

[11] M. Sharir, A. Sheffer, and J. Solymosi, Distinct distances on two lines, *J. Combinat. Theory A*, **120** (2013), 1732–1736.