VISIBILITY IN THE PLANE

SUKUMAR DAS ADHIKARI AND ANDREW GRANVILLE

Abstract. We find the size of the smallest subset of the set of integer lattice points, such that every element of a given rectangular grid is visible from our subset, which in particular answers a question of Paul Erdős et al.

1. Introduction

If $D \geq 2$ we say that $\mathbf{a} \in \mathbb{Z}^D$ is *visible* from $\mathbf{b} \in \mathbb{Z}^D$ if there is no element of $\mathbb{Z}^D$ on the straight line segment in-between $\mathbf{a}$ and $\mathbf{b}$. One immediately deduces that (a, b) is visible from (c, d) if and only if $\gcd(c - a, d - b) = 1$, and, more generally, that $\mathbf{a}$ is visible from $\mathbf{b}$ if and only if the gcd of the co-ordinates of **a-b** equals 1. We say that $\mathcal{A} \subset \mathbb{Z}^D$ is visible from $\mathcal{B} \subset \mathbb{Z}^D$ if, for each point $a \in \mathcal{A}$ there is some $b \in \mathcal{B}$ such that a is visible from b.

In this paper we are interested in the size of the smallest $\mathcal{B} \subset \mathbb{Z}^D$ such that $\mathcal{A} \subset \mathbb{Z}^D$ is visible from $\mathcal{B}$. Research to date has focussed on the cases where $\mathcal{A}$ is the set of integer lattice points inside a cube with all sides equal and parallel to the axes (in two dimensions this is one of the list of problems compiled by (L. & W.) Moser, see also [6] (Section 10.4) and [9] (Problem F4)), or where $\mathcal{A}$ is the set of integer lattice points inside a rectangular cube with all sides parallel to the axes (see [11]). Herein we give an asymptotic formula for the size of that set $\mathcal{B}$:

Theorem 1. *For every integer $D \geq 2$, for any $\mathcal{A} \subset \mathbb{Z}^D$ which is the set of lattice points inside a rectangular box $\subset \mathbb{R}^D$ with all sides parallel to the axes and of shortest side length $N \geq 2$, the smallest $\mathcal{B} \subset \mathbb{Z}^D$ such that $\mathcal{A}$ is visible from $\mathcal{B}$ has size*

$$= \{1 + o_{N\to\infty}(1)\}\ \zeta(D)\ \frac{\log N}{\log\log N}, \tag{1}$$

where $\zeta(D) = \sum_{n\geq 1} 1/n^D$ is the Riemann zeta-function. Moreover $\mathcal{A}$ is visible from some $\mathcal{B}(A) \subset \{1, 2, \ldots, N\}^D \subset \mathcal{A}$ of this size.

In fact we obtain upper and lower bounds of the correct order of magnitude for all $N \geq 2$: This restriction is necessary, since if $\mathcal{A} = \{(m, 1) :\ 1 \leq m \leq M\}$ is visible from some $\mathcal{B} \subset \mathcal{A}$ then $|\mathcal{B}| \geq (M-1)/2$. The restriction is unnecessary if we allow the elements

Thanks are due to the astute referee for several useful remarks and observations, to Iosif Polterovich for some helpful remarks on the geometric problem in section 6, and to Anand Ramakrishnan for finding a typographic error.

of $\mathcal{B}$ to be close to $\mathcal{A}$, though not necessarily a subset; in our example $\mathcal{A}$ is visible from the singleton set $\{(1,0)\}$.

From Theorem 1 we immediately deduce

Corollary 2. *The smallest subset of $\mathbb{Z}^D$ from which $\{1,2,\dots,N\}^D$ is visible, has size* (1) *for each integer $D \geq 2$.*

Theorem 1 follows from two stronger results. Let

$$\mathcal{R}_D(N) := \{1,2,\dots,N\} \times \mathbb{Z}^{D-1}.$$

The first gives the lower bound in Theorem 1 since $\{1,2,\dots,N\}^D \subset \mathcal{A}$:

Proposition 3. *Fix integer $D \geq 2$. If $\{1,2,\dots,N\}^D$ is visible from $S \subset \mathbb{Z}^D$ then S has size*

$$\geq \{1 - o_{N\to\infty}(1)\}\ \zeta(D)\ \frac{\log N}{\log\log N}.$$

A more difficult result gives the upper bound in Theorem 1, since $\mathcal{A} \subset \mathcal{R}_D(N)$:

Proposition 4. *Fix integer $D \geq 2$. There exists a subset S of $\{1,2,\dots,N\}^D$ of size*

$$\leq \{1 + o_{N\to\infty}(1)\}\ \zeta(D)\ \frac{\log N}{\log\log N},$$

such that $\mathcal{R}_D(N)$ is visible from S.

(Henceforth, for notational convenience, we will replace "$= \{1 - o_{N\to\infty}(1)\}$" by "$\sim$" , "$\geq \{1 - o_{N\to\infty}(1)\}$" by "$\gtrsim$" , and "$\leq \{1 - o_{N\to\infty}(1)\}$" by "$\lesssim$".)

For an arbitrary compact, convex set $\mathcal{S} \subset \mathbb{R}^D$, one can ask for the size of the smallest $\mathcal{B} \subset \mathbb{Z}^D$ such that $\mathcal{S} \cap \mathbb{Z}^D$ is visible from $\mathcal{B}$. If one can find rectangular boxes $\mathcal{A}_-, \mathcal{A}_+$, with sides parallel to the axes such that $\mathcal{A}_- \subset \mathcal{S} \subset \mathcal{A}_+$ then the smallest such $\mathcal{B}$ has size in the range

$$\mathcal{L}_D(N_-) \lesssim |\mathcal{B}| \lesssim \mathcal{L}_D(N_+), \text{ where } \mathcal{L}_D(x) = \zeta(D)\frac{\log x}{\log\log x} \tag{2}$$

where $N_\pm$ is the shortest side length of $\mathcal{A}_\pm$, by Theorem 1, provided $N_- \geq 2$. We also have $\mathcal{B} \subset \mathcal{S}$. This yields an asymptotic provided $N_- \geq N_+^{1-o(1)}$ which will be the case unless $\mathcal{S}$ is oriented in a peculiar fashion. In particular if $\mathcal{H}$ is any fixed convex shape then the smallest set of lattice points from which all of $N\mathcal{H}$ is visible has size

$$\sim \mathcal{L}_D(N).$$

If M is a D-by-D matrix with integer entries of determinant ± 1 then $a \in \mathbb{Z}^D$ is visible from $b \in \mathbb{Z}^D$ if and only if $Ma \in \mathbb{Z}^D$ is visible from $Mb \in \mathbb{Z}^D$ (as is easily proven), so the orientation of $\mathcal{S}$ can be adjusted by a suitable invertible linear transformation without affecting visibility. For this reason one might guess that, in general, the smallest $\mathcal{B}$ from which the lattice points of $\mathcal{S}$ are visible, has size (1) where $N \geq 1$ is the smallest 1-dimensional thickness of $\mathcal{S}$. However this is far from true, even in two dimensions, as we show in the following results, which are proved in Section 6.

For a given compact, convex set $\mathcal{S} \subset \mathbb{R}^2$, let P and Q be two points that are furthest apart in $\mathcal{S}$, and let $\alpha(\mathcal{S})$ be the slope of the line between them.

Let $N_+(\mathcal{S})$ be the distance between P and Q; and then let $N_-(\mathcal{S})$ be the smallest number such that every point in $\mathcal{S}$ lies within a distance $N_-(\mathcal{S})$ of the line joining P and Q (that is, $N_-(\mathcal{S})$ is the 1-dimensional thickness of $\mathcal{S}$).[1] Let $\mathcal{L}(x) = \mathcal{L}_2(x)$.

Theorem 5. *Fix $\alpha \in \mathbb{R}$.*

If $\alpha \in \mathbb{Q}$ then for all compact, convex sets $\mathcal{S} \subset \mathbb{R}^2$ with $\alpha(\mathcal{S}) = \alpha$, the smallest set of lattice points from which $\mathcal{A} = \mathcal{S} \cap \mathbb{Z}^2$ is visible has size $\sim \mathcal{L}(N_-)$.

If $\alpha \notin \mathbb{Q}$ then there exist arbitrarily large compact, convex sets $\mathcal{S} \subset \mathbb{R}^2$ with $\alpha(\mathcal{S}) = \alpha$ and $N_- = 1$, such that the smallest set of lattice points from which $\mathcal{A} = \mathcal{S} \cap \mathbb{Z}^2$ is visible has size $\gtrsim \frac{1}{4}\mathcal{L}(N_+)$.

(In the asymptotic results here, and in Theorems 6, 7 and 8, we have $o_{N_+ \to \infty}(1)$.)

For any α that is not too well approximable by rationals we can get close upper and lower bounds on the size of $\mathcal{B}$: Let

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \ldots$$

be the convergents in the continued fraction for α.

Theorem 6. *Suppose that $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ such that the convergents for α satisfy $\log q_{j+1} \sim \log q_j$ as $j \to \infty$. (This includes, for example, all irrational, algebraic α, by Roth's theorem). If $\mathcal{S} \subset \mathbb{R}^2$ is a compact, convex set with $\alpha(\mathcal{S}) = \alpha$, and $\mathcal{B}$ is the smallest set of lattice points from which $\mathcal{A} = \mathcal{S} \cap \mathbb{Z}^2$ is visible, then*

$$\frac{1}{2}\mathcal{L}(N_+) + \frac{1}{2}\mathcal{L}(N_-) \gtrsim |\mathcal{B}| \gtrsim \frac{1}{3}\mathcal{L}(N_+) + \frac{2}{3}\mathcal{L}(N_-).$$

Note that the upper and lower bounds here differ by a factor of at most 3/2.

Rather more generally we can prove that $|\mathcal{B}|$ is roughly of size $\mathcal{L}(N_+)$ unless α is very-well approximable by rationals.

Theorem 7. *Suppose that $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. For any given compact, convex set $\mathcal{S} \subset \mathbb{R}^2$ with $\alpha(\mathcal{S}) = \alpha$, let $\mathcal{B}(\mathcal{S})$ be the smallest set of lattice points from which $\mathcal{A} = \mathcal{S} \cap \mathbb{Z}^2$ is visible. We have $|\mathcal{B}(\mathcal{S})| \gg \mathcal{L}(N_+)$ for all such $\mathcal{S}$ if and only if $\log q_{j+1} \ll \log q_j$.*

Theorems 5, 6 and 7 are all extreme cases of a more general understanding of the size of $\mathcal{B}(\mathcal{S})$, which we now give. First though we must "normalize" our convex set: By translation we may assume that P is "close" to the origin and by reflections that the line joining P and Q has slope in $[0, 1]$ (it is easy to see that by reflections the line is in the positive quadrant; moreover if its slope is > 1 then we can reflect $\mathcal{S}$ in $x = y$ so that the slope is in $[0, 1]$). Next by the linear transformation $x \to x, y \to y + x$ we see that we may assume that the slope α of the line joining P and Q satisfies $1 \leq \alpha \leq 2$ (and hence

[1] It may be that there is more than one choice of P and Q and hence neither $\alpha(\mathcal{S})$ nor $N_-(\mathcal{S})$ are uniquely defined. Nonetheless the subsequent results work no matter which choice we make.

$\frac{p_1}{q_1} = 1$). Such a compact set $\mathcal{S}$, and the accompanying lattice points $\mathcal{A} = \mathcal{S} \cap \mathbb{Z}^2$, are called "normalized".

Theorem 8. *Let A be a normalized set of lattice points (inside a closed, compact subset of $\mathbb{R}^2$). We can determine $|\mathcal{B}(A)|$ up to a factor 2, as follows:*
If $i \geq 1$ and $q_i^2 \leq N_+/N_- < q_i q_{i+1}$

$$\mathcal{L}(N_- q_i) \gtrsim |\mathcal{B}(A)| \gtrsim \frac{1}{2}\mathcal{L}(N_- q_i). \tag{3}$$

If $i \geq 2$ and $q_{i-1} q_i \leq N_+/N_- < q_i^2$ then

$$\mathcal{L}(N_+/q_i) \gtrsim |\mathcal{B}(A)| \gtrsim \frac{1}{2}\mathcal{L}(N_+/q_i). \tag{4}$$

It would be worthwhile to generalize this result to higher dimensions, though one faces the difficulty of having to work with simultaneous approximations. It would be interesting to get an asymptotic for $|\mathcal{B}|$ here, something that we have been unable to do.

It had been shown that if $\{1, 2, \ldots, N\}^D$ is visible from $\mathcal{B}$ then $|\mathcal{B}| > \mathcal{L}_2(N)/2\zeta(2)$ when $D = 2$ by Abbott [1] in 1974, $|\mathcal{B}| \gg \mathcal{L}_D(N)$ when $D \geq 3$ by Adhikari and Chen [4] (see also [6]) in 1999, and the correct bound $|\mathcal{B}| \gtrsim \mathcal{L}_D(N)$ for all $D \geq 2$ by Chen and Cheng [7] in 2003, by an argument similar to ours.

Abbott [1] also proved that $\{1, 2, \ldots, N\}^D$ is visible from a set of size $< 4 \log N$ if N is sufficiently large, when $D = 2$, using a greedy construction. Adhikari and Chen [4] obtained $\ll \mathcal{L}_D(N)$ when $D \geq 3$, which was improved to $\lesssim \mathcal{L}_{D-1}(N)$ by Chen and Cheng [7]. In Corollary 2 we obtain $\lesssim \mathcal{L}_D(N)$ for all $D \geq 2$.

Erdős, Gruber and Hammer, in their monograph [8], remark: "*Abbott's proof is an existence proof and gives no indication how to construct small subsets from which any point of the set is visible. It would be of interest to construct such subsets of cardinality $O(\log N)$*". In 1996 Adhikari and Balasubramanian [3] did more than this by explicitly constructing a set of size $\ll \log N \log\log\log N/\log\log N$ from which $\{1, 2, \ldots, N\}^2$ is visible[2] (see also [2]). The sets that we produce in Corollary 2 are not explicitly constructed; rather we can use "almost all" sets inside a certain (constructible) class of sets of points. However, by slightly modifying Adhikari and Chen's method we show explicitly, in Section 4, how to find a set of size

$$\sim \frac{1}{(1 - \zeta^*(D-1))} \frac{\log N}{\log\log N} \quad \text{where} \quad \zeta^*(s) = \sum_p \frac{1}{p^s} \tag{5}$$

from which $\{1, 2, \ldots, N\}^D$ is visible, for each $D \geq 3$.

Finally we can ask a rather more general question: For any set $\mathcal{S} \subset \mathbb{Z}^D$ let $v(S)$ be the size of the smallest set of lattice points from which $\mathcal{S}$ is visible. What is

$$\nu_D(N) := \max_{\mathcal{S} \subset \mathbb{Z}^D,\ |\mathcal{S}| = N} v(S)\ ?$$

We prove the following result:

[2]Their implicit constant can be made explicit using [5].

Theorem 9. *Fix $D \geq 2$. If N is sufficiently large then*

$$\frac{\zeta(D)}{D} \frac{\log N}{\log\log N} \lesssim \nu_D(N) \lesssim \frac{\log N}{\log(1 + 1/(\zeta(D) - 1))}.$$

It would be good to close the gap between the upper and lower bounds here.

2. Lower bounds

Proof of Proposition 3 for $D = 2$. This is proved by using the Chinese Remainder Theorem. Suppose that $\{1, 2, \ldots, N\}^2$ is visible from $S_0 \subset \mathbb{Z}^2$.

Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes. For each k, $1 \leq k \leq K$ we select $i, j \pmod{p_k}$ so as to maximize the size of the set

$$\{(u, v) \in S_{k-1} : \ u \equiv i \pmod{p_k} \text{ and } v \equiv j \pmod{p_k}\}.$$

Call these values i_k, j_k and let T_k be this set. By definition $|T_k| \geq |S_{k-1}|/p_k^2$. Let $S_k = S_{k-1} \setminus T_k$ so that $|S_k| \leq (1 - 1/p_k^2)|S_{k-1}|$ and hence we have, by induction, that

$$|S_k| \leq \prod_{j=1}^{k}(1 - 1/p_j^2) \cdot |S_0| = \left(\frac{1}{\zeta(2)} + O\left(\frac{1}{p_k \log p_k}\right)\right)|S_0|.$$

We select K so that $p_K^2 \sim |S_0|/\zeta(2)$, which implies that $K = o((\sqrt{|S_0|})$ and $|S_K| \leq |S_0|/\zeta(2) + o(\sqrt{|S_0|})$.

Next write $S_K = \{(i_{K+\ell}, j_{K+\ell}) : \ 1 \leq \ell \leq |S_K|\}$, and let $r = K + |S_K|$ which, by the above, is $\leq |S_0|/\zeta(2) + o(\sqrt{|S_0|})$. Now let $m = \prod_{p \leq p_r} p$, and x and y be the least positive residues $\pmod{m}$ satisfying

$$x \equiv i_k \pmod{p_k} \text{ and } y \equiv j_k \pmod{p_k} \ \text{ for } 1 \leq k \leq r,$$

which is possible by the Chinese Remainder Theorem.

We see that (x, y) is invisible from each $s \in S_0$ for if $(u, v) \in S_0$ then there exists $k, 1 \leq k \leq r$ such that $u \equiv i_k \equiv x \pmod{p_k}$ and $v \equiv j_k \equiv y \pmod{p_k}$, so that $p_k | \gcd(u - x, y - v)$. Hence (by the definition of S_0), $N < \max\{x, y\} \leq m = r^{(1+o(1))r}$ by the prime number theorem, and so $r \geq (1 + o(1)) \log N/\log\log N$, from which the result follows.

Proof of Proposition 3 for $D \geq 3$. We proceed analogously to the proof of the lower bound for $D = 2$: For the primes p_k with $p_k^D \leq (1/\zeta(D))|S_0|$ we select the most popular residue class in S_{k-1} for $(i_k, j_k, \ldots, \ell_k) \pmod{p_k}$. For the larger primes we select one point in S_k per prime. The result follows by an analogous calculation.

3. More greediness: The proof of Theorem 9

The lower bound follows by assuming $\mathcal{S} \supset \{1, 2, \dots, M\}^D$ with $M = [N^{1/D}]$, and applying Proposition 3.

To get the upper bound, suppose that we are given a set $\mathcal{S}$ of N points in $\mathbb{Z}^D$. We now construct a point from which $> N/\zeta(D)$ of these N points are visible:

Fix $y > N^{1/(D-1)}$. Select the residue class $(a_{1,1}, a_{1,2}, \dots, a_{1,D}) \pmod 2$ containing the fewest elements of $\mathcal{S}$; so that it contains $\leq |\mathcal{S}|/2^D$ elements. Let S_1 equal $\mathcal{S}$ minus these elements. The points in S_1 are visible from any point in our residue class, at least if we only consider the prime 2. Now we select the residue class $(a_{2,1}, a_{2,2}, \dots, a_{2,D}) \pmod 3$ containing the fewest elements of $\mathcal{S}_1$, and define $\mathcal{S}_2$ analogously, and keep on going with this construction for all primes $p \leq y$. Hence there is some residue class mod $m = \prod_{p \leq y} p$ such that every element of S_k, where $k = \pi(y)$, is visible from any point in our residue class, at least if we only consider the primes $\leq y$. Now, for each prime $p > y$, the proportion of elements of our residue class which do not see some element of S_k because of the prime p is $\leq |S_k|/p^D$. Hence the proportion of elements of our residue class which do not see some element of S_k because of some prime $p > y$ is $\leq \sum_{p>y} |S_k|/p^D \leq N \sum_{n>y} 1/n^D \leq N/y^{D-1} < 1$; in other words there are points in our residue class from which S_k is visible. Select any such point and note that $|S_k| \geq N \prod_{p \leq y}(1 - 1/p^D) > N/\zeta(D)$.

The idea then is to start with a set $\mathcal{S}$ of N points, select a point P_1 from which the most elements of $\mathcal{S}$ are visible, and then repeat the process on the set $S_1 = \mathcal{S} \setminus P_1$. After selecting k points at most $N(1 - 1/\zeta(D))^k$ points of $\mathcal{S}$ are not visible from at least one of $P_1, P_2, \dots, P_k$. The result follows.

4. First upper bounds: The construction yielding (5)

(We more-or-less follow the proof of [4].) Let

$$S := \{(2, 2, \dots, , 2)\} \cup \{(a_1, a_2, \dots, a_k, 1) : 1 \leq a_j \leq M\} ,$$

with $k = D-1$. Notice that every point with Dth co-ordinate 1 is visible from $(2, 2, \dots, , 2)$. Moreover, the number of points in $S \setminus \{(2, 2, \dots, , 2)\}$ from which $(x_1, x_2, \dots, x_D)$ is invisible, when $x_D > 1$, is

$$\leq \sum_{1 \leq a_1, a_2, \dots, a_k \leq M} \ \sum_{\substack{p \text{ prime}, \ p | (x_D - 1) \\ p | (x_j - a_j) \text{ for } 1 \leq j \leq k}} 1 = \sum_{\substack{p \text{ prime} \\ p | (x_D - 1)}} \prod_{j=1}^{k} \sum_{\substack{a_j = 1 \\ p | (x_j - a_j)}}^{M} 1 \leq \sum_{p \leq y(N)} \left(\frac{M}{p} + 1 \right)^k ,$$

where $y = y(N) = \{1 + o(1)\} \log N$ denotes the largest prime for which $\prod_{p \leq y} p < N$, since $M/p + 1$ is a decreasing function in p. If we expand this last term using the binomial theorem then, for each $j \geq 2$, we get an upper bound

$$\leq \sum_{i=0}^{k-2} \binom{k}{k-i} \zeta^*(k-i) M^{k-i} + kM(\log \log y + O(1)) + \pi(y).$$

Selecting M so that $M^k = (1+\epsilon)\pi(y)/(1-\zeta^*(k))$, the above is $\leq \zeta^*(k)M^k + \pi(y) + O_k(M^{k-1}) < M^k$, and so there must be an element of S from which $(x_1, x_2, \ldots, x_D)$ is visible. The result follows letting $\epsilon \to 0$. Note that S is explicitly given as claimed.

5. More difficult upper bounds: Proposition 4

We believe that $\{1, 2, \ldots, N\}^2$ should be visible from a rectangular set of the shape

$$\left\{(i,j) : \ 1 \leq i \leq k, \ 1 \leq j \leq \{\zeta(2)+o(1)\} \ \frac{\log N}{k \log\log N}\right\}.$$

To prove this one needs to show that for every $n, r \leq N$ there exists i and j in these ranges for which $\gcd(n-i, r-j) = 1$. Handling the possible "small" common prime factors is a straightforward technical issue, but we have been unable to handle the possibility of a grand co-incidence of large prime factors. A straightforward heuristic suggests that such a co-incidence is extremely unlikely so, although we cannot rule it out, we can do so "on average". In other words if we keep the same choice of j's and instead select the "rows" i at random (in a suitable sense) then a grand co-incidence of large prime factors can be ruled out, and we have a set $\mathcal{B}$ that gives us the upper bound in Corollary 2 for $D = 2$. Indeed this construction is also suitable for the upper bounds in Theorem 1 and for Proposition 4 for $D = 2$, and is easily generalized to also obtain these results for all $D \geq 3$.

Let $\omega(m)$ denote the number of distinct prime factors of integer m. Fix $C > \zeta(2)$, and let

$$k = [\log\log N], \quad y = \frac{C \log N}{k \log\log N} \quad \text{and} \quad z = \left[\frac{1}{2}\log\log\log N\right]$$

with $m = \prod_{p \leq y} p$ and $R = \prod_{p \leq z} p$, so that $R = o(k)$, and $2^k \leq m^k \leq e^{O(ky)} = N^{o(1)}$. We will show that $\mathcal{R}_2(N)$ is visible from $S = \{(i_j, l) : \ 1 \leq j \leq k, \ 1 \leq l \leq y\}$, for various choices of $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, N\}$.

Lemma 1. Suppose that N is large and y, z, m and R are as above. Suppose that n is an integer $\leq N$ with $\gcd(n, R) = d$. The number of integers in an interval of length y that are coprime with n is

$$\geq y\left(\frac{\phi(d)}{d} - \sum_{\substack{z<p\leq y \\ p|n}} \frac{1}{p}\right) - 2^{\omega(d)} - \omega(n).$$

Proof. The number of integers in a given interval of length y that are divisible by g is $y/g + r_g$ where $|r_g| \leq 1$. Therefore, by inclusion-exclusion, the number of integers in a given interval of length y that are coprime with d is

$$\sum_{g|d} \mu(g)\left(\frac{y}{g} + r_g\right) = \frac{\phi(d)}{d} \ y + \sum_{g|d} \mu(g) r_g \geq \frac{\phi(d)}{d} \ y - 2^{\omega(d)}.$$

To get a lower bound on the number coprime to n we simply bound the number of integers in the interval divisible by prime factors of n that are $> z$: This is $\leq y/p+1$ if $z<p\leq y$ and ≤ 1 if $p>y$. The result follows.

Proof of Proposition 4 for $D=2$**.** We will show that there are $o((N/m)^k)$ k-tuples of integers $(i_1,i_2,\dots,i_k)$, with each $i_j\leq N$ and $i_j\equiv j \pmod m$, such that there exists an integer n for which $\gcd(n-i_j,l)>1$ for every integer l in some given interval of length y. Then, for almost all of the k-tuples of integers $(i_1,i_2,\dots,i_k)$ with each $i_j\leq N$ and $i_j\equiv j \pmod m$, for every integer $n\leq N$ and every integer r, there exists an integer l, $1\leq l\leq y$ such that $\gcd(n-i_j,r-l)=1$. In other words, $\mathcal{R}_2(N)$ is visible from $S=\{(i_j,l):\ 1\leq j\leq k,\ 1\leq l\leq y\}$, as claimed.

So, for a given integer n, suppose that $\gcd(n-i_j,l)>1$ for every integer l in some given interval of length y. By Lemma 1, with $d=\gcd(n-i_j,R)$, this implies that

$$\omega(n-i_j)\geq y\left(\frac{\phi(d)}{d}-\sum_{\substack{z<p\leq y\\ p|(n-i_j)}}\frac{1}{p}\right)-2^{\omega(d)}\geq y\left(\frac{\phi(d)}{d}-\sum_{\substack{z<p\leq y\\ p|(n-i_j)}}\frac{1}{p}+o(1)\right). \tag{6}$$

Now suppose that we are given a k-tuple of integers $(i_1,i_2,\dots,i_k)$ with each $i_j\leq N$ and $i_j\equiv j \pmod m$. Let J be the set of j, $1\leq j\leq k$ for which $\sum_{z<p\leq y,\ p|(n-i_j)}1/p\geq 1/\log z$, so that $\omega(n-i_j)\geq\left(\frac{\phi(d)}{d}+o(1)\right)y$ if $j\notin J$, by (6). Now

$$\begin{aligned}\frac{|J|}{\log z}\leq\sum_{j=1}^{k}\sum_{\substack{p|(n-i_j)\\ z<p\leq y}}\frac{1}{p} &= \sum_{z<p\leq y}\frac{1}{p}\,\#\{j:\ 1\leq j\leq k \text{ and } j\equiv i_j\equiv n \pmod p\}\\ &\leq \sum_{z<p\leq y}\frac{1}{p}\left(\frac{k}{p}+1\right)\leq k\sum_{z<p\leq y}\frac{1}{p^2}+\sum_{z<p\leq y}\frac{1}{p}\ll\frac{k}{z\log z},\end{aligned}$$

so that $|J|\ll k/z$.

Now fix $J\subset\{1,2,\dots,k\}$ with $|J|\ll k/z$. A famous result of Hardy and Ramanujan states that the number of integers $\leq N$ with exactly r distinct prime factors is

$$\ll\frac{N}{\log N}\frac{(\log\log N+O(1))^{r-1}}{(r-1)!}.$$

Hence the number of k-tuples of integers $(i_1,i_2,\dots,i_k)$ with each $i_j\leq N$ and $i_j\equiv j \pmod m$, such that $\gcd(n-i_j,l)>1$ for every integer l in some given interval of length y, and where the set of j, $1\leq j\leq k$ for which $\sum_{z<p\leq y,\ p|(n-i_j)}1/p\geq 1/\log z$ is precisely

J, is less than N to the power

$$
\begin{aligned}
& \sum_{\substack{1\le j\le k\\ d=\gcd(n-j,R)\\ j\notin J}} \left(1-\frac{C}{k}\left(\frac{\phi(d)}{d}+o(1)\right)\right)+\sum_{j\in J}1 \\
= \;& k-\frac{C}{k}\sum_{\substack{1\le j\le k\\ d=\gcd(n-j,R)}}\frac{\phi(d)}{d}+o(1)=k-\frac{C}{k}\left(\frac{k}{R}+O(1)\right)\sum_{\substack{1\le j\le R\\ d=\gcd(n-j,R)}}\frac{\phi(d)}{d}+o(1). \\
= \;& k-\frac{C}{R}\sum_{d|R}\phi(R/d)\frac{\phi(d)}{d}+o(1)=k-C\prod_{p\le z}\frac{1}{p}\left(p-1+1-\frac{1}{p}\right)+o(1) \qquad (7)\\
= \;& k-C\prod_{p\le z}\left(1-\frac{1}{p^2}\right)+o(1)=k-\frac{C}{\zeta(2)}+o(1)
\end{aligned}
$$

Now the number of possible such sets J is $\le 2^k < N^{o(1)}$. Therefore, since $C>\zeta(2)$, the number of k-tuples of integers $(i_1,i_2,\dots,i_k)$ with each $i_j\le N$ and $i_j\equiv j \pmod m$ such that there exists an integer n for which $\gcd(n-i_j,l)>1$ for every integer l in some given interval of length y, is

$$\le N\cdot N^{k-C/\zeta(2)+o(1)}=o((N/m)^k),$$

since $m^k\le N^{o(1)}$, which was the result stated at the start of the proof.

Sketch of the proof of Proposition 4 for $D\ge 3$. Keep k,z,m and R as above. Consider the sets

$$S=\{(i_j,x_2,x_3,\dots,x_D):\ 1\le j\le k,\ 1\le x_i\le y\},\ \text{where } y:=\left(\frac{C\log N}{k\log\log N}\right)^{\frac{1}{D-1}}.$$

The analogy to Lemma 1 is that for any given integers $v_2,\dots,v_D$ the number of elements $(x_2,x_3,\dots,x_D)$, with each x_i an integer in $[1,y]$, for which $(n,x_2-v_2,x_3-v_3,\dots,x_D-v_D)=1$, is

$$\ge y^{D-1}\left(\prod_{p|d}\left(1-\frac{1}{p^{D-1}}\right)-o(1)\right)-\omega(n).$$

One proves this, analogously, by noting that the number of such elements for which $\gcd(n,x_2-v_2,x_3-v_3,\dots,x_D-v_D)$ is divisible by d is $(y/d+O(1))^{D-1}=(y/d)^{D-1}+O((y/d)^{D-2})$ if $d\le y$; moreover this number of elements is $\le (y/d+1)^{D-1}\le(2y/d)^{D-1}$ if $d\le y$, and ≤ 1 if $d>y$. In the calculation one majorizes the additional term $2^{D-1}\sum_{z<p\le y,\ p|n}1/p^{D-1}\ll_D 1/z=o(1)$, which simplifies the subsequent argument since the (analogy to the) set J is now empty.

Hence in place of (7) we obtain

$$\begin{aligned} &= k - \frac{C}{R}\sum_{d|R}\phi(R/d)\prod_{p|d}\left(1-\frac{1}{p^{D-1}}\right)+o(1) \\ &= k - C\prod_{p\le z}\frac{1}{p}\left(p-1+1-\frac{1}{p^{D-1}}\right)+o(1) = k-\frac{C}{\zeta(D)}+o(1), \end{aligned}$$

and the rest of the proof goes through analogously taking $C > \zeta(D)$.

6. Irrational orientation in 2-dimensions

In this section we will prove Theorem 8, which shows that the visibility properties of thin convex bodies that are irrationally oriented, are quite different from the visibility properties of thin convex bodies that are rationally oriented.

We begin with a lemma that shows that we need only study visibility for the lattice points inside rectangular boxes

Lemma 10. *For any bounded, closed convex body $\mathcal{A} \subset \mathbb{R}^2$ there exist rectangular boxes $\mathcal{B}_1 \subset \mathcal{A} \subset \mathcal{B}_2$, with parallel sides, such that each side length in $\mathcal{B}_1$ is one-third the length of the parallel side in $\mathcal{B}_2$.*

Remark: Hadwiger [10] showed that for any bounded, closed convex body $\mathcal{A} \subset \mathbb{R}^d$ there exist such rectangular boxes $\mathcal{B}_1 \subset \mathcal{A} \subset \mathcal{B}_2$ with $\mathrm{Vol}(B_2) \le d!d^d\,\mathrm{Vol}(B_1)$. On the other hand if A is a sphere then one can easily show that one must have $\mathrm{Vol}(B_2) \ge d^{d/2}\,\mathrm{Vol}(B_1)$. It remains to determine the "best possible" constant in d-dimensions.

Proof. Select two points of $\mathcal{A}$ at maximal distance from one another, say P_1 and P_2, and draw a line $\mathcal{L}$ between them. On each side of $\mathcal{L}$, find a point at maximal distance from $\mathcal{L}$. Call these two points Q_1 and Q_2. Let $\mathcal{B}_2$ be the box with two sides parallel to $\mathcal{L}$ going through Q_1 and Q_2, and then two sides perpendicular to $\mathcal{L}$ going through P_1 and P_2; evidently $\mathcal{A} \subset \mathcal{B}_2$ by convexity.

Let $\mathcal{L}_j$ be the line perpendicular to $\mathcal{L}$ going through Q_j, for $j = 1, 2$, and then let R_j be the intersection point of $\mathcal{L}$ and $\mathcal{L}_j$. The triangle formed by P_i, Q_j, R_j lies inside $\mathcal{A}$ by convexity. Let $P_{i,j}$ be the point one-third of the way between P_i and R_j; and then let $Q_{i,j}$ be the point on the line joining P_i and Q_j such that the line joining $P_{i,j}$ and $Q_{i,j}$ is perpendicular to $\mathcal{L}$. Note that the distance between $P_{i,j}$ and $Q_{i,j}$ is one third the distance between Q_j and R_j, by similarity. Hence the rectangle, $S_{i,j}$, with one side the segment of $\mathcal{L}$ between $P_{i,j}$ and R_j, and a second side the line segment between $P_{i,j}$ and $Q_{i,j}$, lies in $\mathcal{A}$, by convexity. Next we join the rectangles $S_{1,j}$ and $S_{2,j}$, to get a new rectangle which lies inside $\mathcal{A}$: This contains S_j, one side of which is the middle third of the line segment between P_1 and P_2, and has width one third of the distance between Q_j and R_j, in the direction of Q_j. (That this lies inside $S_{1,j} \cup S_{2,j}$ follows since $P_{1,j}$ is one third of the way between P_1 and R_j, so at most one third of the way between P_1 and P_2). Then $\mathcal{B}_1 = S_1 \cup S_2$.

Proposition 11. *Let A be a normalized set of lattice points with the notation of Theorem 8, and let $\mathcal{B} \subset \mathbb{Z}^2$ be the smallest set of lattice points from which $\mathcal{A}$ is visible. If $N_- \geq N_+^{1-o(1)}$ then $|\mathcal{B}| \sim \mathcal{L}(N_+)$. So, now assume that $N_- \leq N_+^{1-\epsilon}$, and select $i, j \geq 1$ so that $N_+/N_- \in [q_{j-1}q_j^2, q_jq_{j+1}^2) \cap [q_{i-1}q_i, q_iq_{i+1})$. We have the following lower bounds:*
(i) If $N_+/N_- \in [q_{j-1}q_j^2, q_j^2q_{j+1})$ then $|\mathcal{B}| \gtrsim \mathcal{L}(N_-q_j)$; and
(ii) If $N_+/N_- \in [q_j^2q_{j+1}, q_jq_{j+1}^2)$ then $|\mathcal{B}| \gtrsim \mathcal{L}(N_+/q_jq_{j+1})$.
And we have the following upper bounds:
(iii) If $N_+/N_- \in [q_{i-1}q_i, q_i^2)$ then $|\mathcal{B}| \lesssim \mathcal{L}(N_+/q_i)$; and
(iv) If $N_+/N_- \in [q_i^2, q_iq_{i+1})$ then $|\mathcal{B}| \lesssim \mathcal{L}(N_-q_i)$.

Proof: By definition $N_- \leq N_+$. One can deduce from the proof of Lemma 10 that there exist squares $\mathcal{B}_1', \mathcal{B}_2'$ with sides parallel to the axes, of side lengths $N_-/2$ and N_+, respectively, such that $\mathcal{B}_1' \subset \mathcal{B}_1 \subset \mathcal{A} \subset \mathcal{B}_2 \subset \mathcal{B}_2'$. It follows from Theorem 1 that the smallest set $\mathcal{B}$ from which all of $\mathcal{A}$ is visible, satisfies $\mathcal{L}(N_-) \lesssim |\mathcal{B}| \lesssim \mathcal{L}(N_+)$. In particular if $N_- \geq N_+^{1-o(1)}$ then $|\mathcal{B}| \sim \mathcal{L}(N_+)$.

Therefore, henceforth, we may assume that $N_- \leq N_+^{1-\epsilon}$. Moreover, via the construction in Lemma 10, and since $\mathcal{A}$ is normalized, we may assume, up to a bounded factor in each dimension, that we are studying the lattice points inside the region

$$\mathcal{T} = \mathcal{T}_\alpha(N_+, N_-) := \{0 \leq x, y \leq N_+ : \ |y - \alpha x| \leq N_-\}, \tag{8}$$

where $1 \leq \alpha \leq 2$.

The convergents of a continued fraction satisfy several properties. First $p_{2k+1}/q_{2k+1} \to \alpha$ from below, and $p_{2k}/q_{2k} \to \alpha$ from above, as $k \to \infty$. We will show that $|\alpha - \frac{p_i}{q_i}| \asymp \frac{1}{q_iq_{i+1}}$: One has that $|\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}}| = \frac{1}{q_{i-1}q_i}$. We deduce the upper bound $|\alpha - \frac{p_i}{q_i}| \leq |\frac{p_i}{q_i} - \frac{p_{i+1}}{q_{i+1}}| = \frac{1}{q_iq_{i+1}}$, and then the lower bound $|\alpha - \frac{p_i}{q_i}| \geq |\frac{p_i}{q_i} - \frac{p_{i+1}}{q_{i+1}}| - |\alpha - \frac{p_{i+1}}{q_{i+1}}| \geq \frac{1}{q_iq_{i+1}} - \frac{1}{q_{i+1}q_{i+2}} \geq \frac{1}{2q_iq_{i+1}}$, since there exists an integer $a_i \geq 1$ such that $q_{i+2} = a_iq_{i+1} + q_i \geq q_{i+1} + q_i \geq 2q_i$.

Lower bounds: In the proof of Proposition 3 for $D = 2$, we saw that for any finite set of lattice points, S, there exist integers $1 \leq a, b \leq m = \prod_{p \leq y} p$ such that any lattice point $(x, y) \in \mathbb{Z}^2$ with $x \equiv a \pmod m$ and $y \equiv b \pmod m$ is invisible from S. Here $\pi(y) = r$ where $r \sim |S|/\zeta(2)$.

We will suppose $p/q = p_i/q_i$ and $Q = q_{i+1}$ for some i, and assume that

$$\frac{m}{N_+} \ll \left|\alpha - \frac{p}{q}\right| \leq \frac{N_-}{qm}. \tag{9}$$

The distance between the consecutive numbers $mn(p - q\alpha), n \in \mathbb{Z}$ is precisely $m|q\alpha - p|$ which is $\leq N_-$, so at least two such multiples lie within a distance N_- of $\alpha b - a$. For such a multiple, $(a + mnp, b + mnq)$ is invisible from S by the discussion in the previous paragraph, and $|(a + mnp) - \alpha(b + mnq)| \leq N_-$. Now

$$|a + mnp|, |\alpha(b + mnq)| \ll mn|\alpha q| \ll \frac{|\alpha b - a|}{|p - q\alpha|} \cdot |q| \ll \frac{m}{|p/q - \alpha|} \ll N_+$$

using (9) and the bounded range for α, so that $(a+mnp, b+mnq) \in \mathcal{T}_\alpha(N_+, N_-)$.

Now $|\alpha - p/q| \asymp 1/qQ$. Hence the above construction works provided (9) holds, that is

$$m \ll M_- := \min\left\{ QN_-,\ \frac{N_+}{qQ} \right\},$$

and therefore, taking m as large as possible in this range,

$$|\mathcal{B}| \gtrsim \zeta(2)r \sim \zeta(2)\frac{y}{\log y} \sim \mathcal{L}(m) \sim \mathcal{L}(M_-).$$

Upper bounds: We make a unitary linear transformation on the region $\mathcal{T}_\alpha(N_+, N_-)$, so that visibility is preserved:

$$X = q_i y - p_i x,\ Y = q_{i-1}y - p_{i-1}x,$$

Then $X = q_i(y - \alpha x) - (p_i - \alpha q_i)x$ so that

$$|X| \le q_i|y - \alpha x| - |p_i - \alpha q_i|x \le q_i N_- + \frac{N_+}{q_{i+1}}$$

By Proposition 4 we deduce that $|\mathcal{B}| \lesssim \mathcal{L}(q_i N_- + \frac{N_+}{q_{i+1}})$.

Deduction of Theorem 8: We compare the upper and lower bounds of Proposition 11: Suppose that $N_+/N_- \in [q_i^2, q_i q_{i+1}) \cap [q_{j-1}q_j^2, q_j^2 q_{j+1})$. In this range $q_i q_{i+1} \ge q_{j-1}q_j^2 > q_{j-1}q_j$, and so $i \ge j$. If $i = j$ then $|\mathcal{B}| \sim \mathcal{L}(N_- q_j)$ (note that, in this case $q_{i+1} \ge q_i q_{i-1}$). If $i \ge j+1$ then $q_j^2 q_{j+1} \ge q_i^2 \ge q_{j+1}^2$ so that $q_j^2 \ge q_{j+1}$, and thus $(N_- q_j)^4 \ge N_-^4 q_j^2 q_{j+1} \ge N_-^3 N_+ \ge N_-^4 q_i^2$, so that $\mathcal{L}(N_- q_j) \gtrsim \frac{1}{2}\mathcal{L}(N_- q_i)$. Hence by (i) and (iv) we have (3).

If $N_+/N_- \in [q_i^2, q_i q_{i+1}) \cap [q_j^2 q_{j+1}, q_j q_{j+1}^2)$ then $q_i q_{i+1} \ge q_j^2 q_{j+1} > q_j q_{j+1}$, so that $i \ge j+1$. If $q_{j+1} < q_j^2 N_-^2$ then $N_+^3 > (N_- q_j^2 q_{j+1})^3 (q_{j+1} q_j^2 N_-^2) = N_-(q_j q_{j+1})^4$, whence $(N_+/q_j q_{j+1})^4 > N_+ N_- \ge (N_- q_i)^2$. If $q_{j+1} \ge q_j^2 N_-^2$ then $(N_+/q_j q_{j+1})^2 \ge N_-^2 N_+^2 / q_{j+1}^3 \ge N_-^4 q_i^4 / q_{j+1}^3 \ge N_-^4 q_i \ge N_- q_i$. Hence we recover (3) from (ii) and (iv).

If $N_+/N_- \in [q_{i-1}q_i, q_i^2) \cap [q_j^2 q_{j+1}, q_j q_{j+1}^2)$ then $q_i^2 > q_j^2 q_{j+1} \ge q_j^2$ so that $i \ge j+1$. Now $N_- q_j^2 q_{j+1} \ge N_+$ and so $(N_- q_j)^2 \ge N_- N_+ / q_{j+1} \ge N_- N_+ / q_i \ge N_+ / q_i$. Hence we have (4) by (i) and (iii).

If $N_+/N_- \in [q_{i-1}q_i, q_i^2) \cap [q_j^2 q_{j+1}, q_j q_{j+1}^2)$ then $q_i^2 > q_j^2 q_{j+1} \ge q_j^2$ so that $i \ge j+1$. Now $(N_+/q_j q_{j+1})^2 \ge N_- N_+ / q_{j+1} \ge N_- N_+ / q_i \ge N_+ / q_i$, we recover (4) from (ii) and (iii).

We can be more precise for small N_+/N_- $(\le q_2^2)$: If $N_+/N_- \le q_2$ then $|\mathcal{B}| \sim \mathcal{L}(N_-)$; and if $q_2 \le N_+/N_- < q_2^2$ then $|\mathcal{B}| \sim \mathcal{L}(N_+/q_2)$.

Before deducing Theorems 5, 6 and 7, we should note that act of "normalizing" $\mathcal{S}$, that is applying the map $\alpha \to 1 + 1/\alpha$ if $\alpha > 1$, has little effect on the convergents p_j/q_j:

Deduction of Theorem 5: If $\alpha \in \mathbb{Q}$ we simply perform an invertible linear transformation (with integer coefficients) to obtain a new convex body with $\alpha = 0$, and then apply Theorem 1. If $\alpha \notin \mathbb{Q}$ apply Theorem 8 with $N_+ = q_i^2$.

Deduction of Theorem 6: Since $q_{k+1} = q_k^{1+o(1)}$, Proposition 11 gives us that if $N_- \leq N_+^{1-\epsilon}$, $N_+/N_- = q_j^{3+o(1)}$ and $N_+/N_- = q_i^{2+o(1)}$ then $|\mathcal{B}| \gtrsim \mathcal{L}(N_- q_j) \sim \frac{1}{3}\mathcal{L}(N_+) + \frac{2}{3}\mathcal{L}(N_-)$ and $|\mathcal{B}| \lesssim \mathcal{L}(N_- q_i) \sim \frac{1}{2}\mathcal{L}(N_+) + \frac{1}{2}\mathcal{L}(N_-)$. The result follows.

Deduction of Theorem 7: If $\log N_- \gg \log N_+$ then $|\mathcal{B}(A)| \asymp \mathcal{L}(N_+)$ by Theorem 8; so henceforth we will assume $\log N_- = o(\log N_+)$. Now if $\log q_j \geq c \log q_{j+1}$ for all $j \geq 2$ then, in the first case of Theorem 8 we have $N_- q_i \geq N_-(q_i q_{i+1})^{\frac{c}{c+1}} \geq N_-(N_+/N_-)^{\frac{c}{c+1}}$, and $N_+/q_i \geq N_- q_{i-1} \geq N_- q_i^c \geq N_-(N_+/N_-)^{c/2}$ in the second case, so that $|\mathcal{B}(A)| \gg \mathcal{L}(N_+)$.

Now suppose that $\log q_j = o(\log q_{j+1})$ for some infinite sequence of integers j, let $N_- = 1$ and $N_+ = q_{j+1}$, so the first case of Theorem 8 yields that $|\mathcal{B}(A)| \lesssim \mathcal{L}(q_j) = o(\mathcal{L}(q_{j+1})) = o(\mathcal{L}(N_+))$.

References

[1] H. L. Abbott, *Some results in combinatorial Geometry*, Discrete Mathematics **9**, 199–204 (1974).

[2] S. D. Adhikari, *Some questions regarding visibility of integer lattice points in $\mathbb{R}^d$*, Proceedings of the Session in Analytic Number Theory and Diophantine Equations (Bonn, January – June 2002) (Eds. D. R. Heath-Brown and B. Z. Moroz), Bonner Mathematische Schriften, **Nr. 360**.

[3] S. D. Adhikari and R. Balasubramanian, *On a question regarding visibility of lattice points*, Mathematika **43**, 155–158 (1996).

[4] S. D. Adhikari and Yong-Gao Chen, *On a question regarding visibility of lattice points-II*, Acta Arithmetica **89**, no. 3, 279–282 (1999).

[5] S. D. Adhikari and Yong-Gao Chen, *On a question regarding visibility of lattice points-III*, Discrete Mathematics, **259**, no. 1-3, 251–256 (2002).

[6] Peter Brass, William Moser and János Pach, *Research Problems in Discrete Geometry*, Springer, 2005.

[7] Y. -G. Chen and L. -F. Cheng, *Visibility of lattice points*, Acta Arithmetica **107**, no. 3, 203–207 (2003).

[8] P. Erdős, P. M. Gruber and J. Hammer, *Lattice Points*, Pitman Monographs and Surveys in Pure and Applied Mathematics **39**, John Wiley and Sons, New York, 1989.

[9] Richard K. Guy, *Unsolved Problems in Number Theory*, Third Edition, Springer, 2004.

[10] H. Hadwiger, *Volumschätzung für die einen Eikörper überdeckenden und unterdeckenden Parallelotope*, Elem. Math. **10**, 122–124 (1955).

[11] Joshua Laison and Michelle Schick, *Seeing dots: visibility of lattice points*, Math. Mag., **80**, no. 4, 274–282 (2007).

Sukumar Das Adhikari (*adhikari@mri.ernet.in*),
Harish-Chandra Research Institute,
Chhatnag Road, Jhusi, Allahabad 211019, India.

Andrew Granville (*andrew@dms.umontreal.ca*),
Départment de Mathématiques et de Statistique,

Université de Montréal, C. P. 6128,
Succ. Centre-Ville, Montréal, QC H3C 3J7, Canada.