DOI:10.4153/S0008439520000090

PRIMITIVE POINTS IN RATIONAL POLYGONS

IMRE BÁRÁNY, GREG MARTIN, ERIC NASLUND, AND SINAI ROBINS

Abstract. Let $\mathcal{A}$ be a star-shaped polygon in the plane, with rational vertices, containing the origin. The number of primitive lattice points in the dilate $t\mathcal{A}$ is asymptotically $\frac{6}{\pi^2}\operatorname{Area}(t\mathcal{A})$ as $t \to \infty$. We show that the error term is both $\Omega_\pm\big(t\sqrt{\log\log t}\big)$ and $O(t(\log t)^{2/3}(\log\log t)^{4/3})$. Both bounds extend (to the above class of polygons) known results for the isosceles right triangle, which appear in the literature as bounds for the error term in the summatory function for Euler's $\phi(n)$.

1. Introduction

One of the fundamental problems in discrete geometry is to estimate the number of lattice points contained in a polygon. In this paper we concern ourselves with the set of *primitive lattice points*

$$\mathbb{P} = \{(m,n) \in \mathbb{Z}^2 \colon \gcd(m,n) = 1\}, \tag{1.1}$$

also known as lattice points visible from the origin. It is a classical result the number of primitive lattice points in a “reasonable” region in $\mathbb{R}^2$ is approximately $\frac{6}{\pi^2}$ times the area of the region. We shall be interested in the family $\{t\mathcal{A}\}$ of dilates of a fixed polygon $\mathcal{A}$, for which we define the error term

$$E_{\mathcal{A}}(t) = \#(t\mathcal{A} \cap \mathbb{P}) - \frac{6}{\pi^2}\operatorname{Area}(t\mathcal{A}) = \#(t\mathcal{A} \cap \mathbb{P}) - \frac{6}{\pi^2}t^2\operatorname{Area}(\mathcal{A}). \tag{1.2}$$

The fact that $\#(t\mathcal{A}\cap\mathbb{P}) \sim \frac{6}{\pi^2}t^2\operatorname{Area}(\mathcal{A})$, or equivalently that $E_{\mathcal{A}}(t) = o(t^2)$, was likely used as far back as Minkowski (see [16, page 998] or [5, Theorem 459]). Stronger upper bounds than $E_{\mathcal{A}}(t) = o(t^2)$ are relatively easy to obtain: we state the following result, which will be justified in the next section, as a benchmark for comparison.

Proposition 1.1. *If $\mathcal{A} \subset \mathbb{R}^2$ is a polygon, then*

$$E_{\mathcal{A}}(t) \ll t\log t$$

for $t \ge 2$, where the implicit constant may depend on $\mathcal{A}$.

The purpose of this paper is to improve this upper bound for any *rational polygon* (a polygon all of whose vertices have both coordinates rational), and show that it cannot be improved too much more by providing a strong $\Omega_\pm$ result for the error term.

It is instructive to consider the specific example $\mathcal{A} = \Delta$, where Δ is the isosceles right triangle with vertices $(0,0)$, $(1,0)$, and $(1,1)$ and thus area $\frac{1}{2}$. Then $\#(t\Delta\cap\mathbb{P})$ is the number

2010 *Mathematics Subject Classification.* Primary 11H06, 11P21; secondary 52C05.
Key words and phrases. Primitive points in polygons, visible points, Euler's Totient function, Error term, rational polygons.

of primitive points in the dilate $t\Delta = \{(x,y) \in \mathbb{R}^2 \colon 0 \le y \le x \le t\}$, that is,

$$\#(t\Delta \cap \mathbb{P}) = \sum_{0\le m\le t} \sum_{\substack{0\le n\le m \\ \gcd(m,n)=1}} 1 = 1 + \sum_{1\le m\le t} \phi(m) \tag{1.3}$$

(where the extra 1 comes from the fact that $\gcd(0,1) = 1$). It is well known that this summatory function of the Euler ϕ-function is asymptotic to $\frac{3}{\pi^2}t^2$, so we define

$$E_\Delta(t) = \sum_{1\le m\le t} \phi(m) - \frac{3}{\pi^2}t^2 + 1 = \#(t\Delta \cap \mathbb{P}) - \frac{3}{\pi^2}t^2. \tag{1.4}$$

Proposition 1.1 implies the estimate $E_\Delta(t) \ll t\log t$, which (when phrased in terms of the summatory function of the Euler ϕ-function) is a classical result of Mertens [9]. The best known unconditional upper bound for this error term $E_\Delta(t)$ is due to Walfisz [17, page 144, eq. (3)]: using methods related to exponential sums, he showed that

$$E_\Delta(t) \ll t(\log t)^{2/3}(\log\log t)^{4/3}. \tag{1.5}$$

As a consequence of our work, we can extend this bound from the isosceles right triangle Δ to all rational polygons.

Theorem 1.2. *Let $\mathcal{A} \subset \mathbb{R}^2$ be a rational polygon. Then*

$$E_{\mathcal{A}}(t) \ll t(\log t)^{2/3}(\log\log t)^{4/3},$$

where the implicit constant may depend on $\mathcal{A}$.

Prior to Walfisz's result, Chowla and Pillai [14] showed that these upper bounds cannot be improved too much by establishing the lower bound

$$\limsup_{t\to\infty} \frac{|E_\Delta(t)|}{t\log\log\log t} > 0,$$

that is, $E_\Delta(t) = \Omega(t\log\log\log t)$. Later, Erdős and Shapiro [4] obtained a slightly weaker quantitative lower bound but showed that $E_\Delta(t)$ oscillates in sign infinitely often. Both results were improved by Montgomery [10]:

Proposition 1.3. $E_\Delta(t) = \Omega_\pm(t\sqrt{\log\log t})$*; in other words,*

$$\limsup_{t\to\infty} \frac{E_\Delta(t)}{t\sqrt{\log\log t}} > 0 \quad \text{and} \quad \liminf_{t\to\infty} \frac{E_\Delta(t)}{t\sqrt{\log\log t}} < 0.$$

We use the term *origin-star-shaped* (star-shaped with respect to the origin) to refer to any domain $\mathcal{B}$ for which $\lambda\mathcal{B} \subset \mathcal{B}$ for all $\lambda \in [0,1]$; note that in particular, any origin-star-shaped domain contains the origin. The main result of this paper generalizes this lower bound of Montgomery to this class of polygons:

Theorem 1.4. *Let $\mathcal{A} \subset \mathbb{R}^2$ be a rational origin-star-shaped polygon. Then*

$$E_{\mathcal{A}}(t) = \Omega_\pm(t\sqrt{\log\log t}),$$

where the implicit constant may depend on $\mathcal{A}$.

In the process of applying an adaptation of Montgomery's argument to the general error term $E_{\mathcal{A}}(t)$ for the primitive point counting function for the lattice polygon $\mathcal{A}$, we found ourselves needing to establish the following "error term independence" result concerning the error term E_Δ for the summatory function of $\phi(n)$, which was defined in equation (1.4); this result may be of independent interest.

Theorem 1.5. *For any positive rational numbers $c_1, \dots, c_k$ and $f_1, \dots, f_k$,*

$$c_1 E_\Delta(f_1 x) + \cdots + c_k E_\Delta(f_k x) = \Omega_\pm\big(x\sqrt{\log\log x}\big),$$

where the implied constant may depend upon the c_j and f_j.

In other words, there can be no "magic cancellation" among the terms $E_\Delta(f_j x)$ that makes the oscillation of the sum significantly smaller than that of an individual term. Indeed, Theorem 1.5 holds more generally, when E_Δ is replaced $E_{\mathcal{A}}$ for any rational origin-star-shaped polygon $\mathcal{A}$ (see the remark following the statement of Theorem 2.5 below).

Furthermore, we conjecture that oscillations of the same size exist even when the c_i are allowed to be negative (where we require the f_i to be distinct in order to avoid trivial cancellations).

Conjecture 1.6. *Theorem 1.5 holds for any rational numbers c_i and any distinct positive rational numbers f_i.*

This conjectural generalization of Theorem 1.5 would imply a stronger version of Theorem 1.4 that holds for any rational polygon $\mathcal{A}$, not necessarily star-shaped or containing the origin:

Conjecture 1.7. *Let $\mathcal{A} \subset \mathbb{R}^2$ be a rational polygon. Then*

$$E_{\mathcal{A}}(t) = \Omega_\pm(t\sqrt{\log\log t}),$$

where the implicit constant may depend on $\mathcal{A}$.

The rest of the paper is divided into two sections. In the next section, we show (Theorem 2.5) that the error term $E_{\mathcal{A}}(t)$ may be rewritten as a linear combination of dilates of the totient error function $E_\Delta(t)$, thereby establishing Theorem 1.2 and reducing Theorem 1.4 to Theorem 1.5. We then establish this latter theorem in the final section.

2. Decomposing the error term

We begin by giving a proof of Proposition 1.1, not only for the sake of completeness, but also because the structure of the argument foreshadows how we will approach the main result of this section, namely Theorem 2.5 below. We use the term *pointed triangle* to mean a triangle which has the origin as a vertex.

Proof of Proposition 1.1. We begin by quoting a reasonably precise estimate [7, special case of Theorem 2.1] for the number of primitive points inside a domain $\mathcal{B}$: if $\mathcal{B}$ is convex and contains the origin, then

$$\#(\mathcal{B} \cap \mathbb{P}) - \frac{6}{\pi^2}\operatorname{Area}(\mathcal{B}) \ll \max\{1, \omega\log\omega\}, \tag{2.1}$$

where ω is the diameter of $\mathcal{B}$. In particular, if $\mathcal{C}$ is a convex polygon containing the origin and $\mathcal{B} = t\mathcal{C}$ is a dilate, then the diameter of $\mathcal{B}$ is a constant multiple of t and so

$$E_{\mathcal{C}}(t) \ll \max\{1, t\log t\}, \tag{2.2}$$

with the implicit constant depending on $\mathcal{C}$.

However, any polygon $\mathcal{A}$ can be partitioned into sums and differences of finitely many pointed triangles (by which we mean that the indicator function of the set $\mathcal{A}$ can be written as sums and differences of indicator functions of pointed triangles, up to inaccuracies on the edges of these triangles), simply by triangulating $\mathcal{A}$ and noting that any triangle $\mathcal{T}$ can be written as a sum and difference of three pointed triangles defined by the three edges of $\mathcal{T}$. Let $\{\mathcal{T}_j\}_{j=1}^n$ denote the set of these pointed triangles, and let $\epsilon_j \in \{1,-1\}$ indicate whether (the indicator function of) $\mathcal{T}_j$ is added or subtracted, so that $\operatorname{Area}(A) = \sum_{j=1}^n \epsilon_j \operatorname{Area}(\mathcal{T}_j)$. Even though these triangles have sides in common, the number of double-counted lattice points on the t-dilation of each side is at most $O(t)$; therefore the bound (2.2), valid since pointed triangles are certainly convex polygons containing the origin, implies

$$\begin{aligned} E_{\mathcal{A}}(t) = \#(t\mathcal{A} \cap \mathbb{P}) - \frac{6}{\pi^2}\operatorname{Area}(t\mathcal{A}) &= \left(\sum_{j=1}^n \epsilon_j \#(t\mathcal{T}_j \cap \mathbb{P}) + O(t)\right) - \frac{6}{\pi^2}\operatorname{Area}(t\mathcal{A}) \\ &= \sum_{j=1}^n \epsilon_j \left(\frac{6}{\pi^2}\operatorname{Area}(t\mathcal{T}_j) + E_{\mathcal{T}_j}(t)\right) + O(t) - \frac{6}{\pi^2}\operatorname{Area}(t\mathcal{A}) \\ &= \sum_{j=1}^n \epsilon_j E_{\mathcal{T}_j}(t) + O(t) \ll t\log t \end{aligned}$$

for $t \ge 2$, as desired. □

Remark. In [7], the bound (2.1) is stated without the hypothesis that $\mathcal{B}$ contain the origin; however, this hypothesis is actually necessary. One can easily construct, using the Chinese remainder theorem, a square $\mathcal{B}$ of diameter ω containing no primitive lattice points whatsoever. The area of such a square is a constant times ω^2, and therefore

$$\left|\#(\mathcal{B} \cap \mathbb{P}) - \frac{6}{\pi^2}\operatorname{Area}(\mathcal{B})\right| \gg \omega^2,$$

which is incompatible with the claimed bound $\omega \log \omega$.

The error in the proof of [7, Theorem 2.1] comes when applying Lemma 2.3, which requires $\omega \ge 1$, to a term of the form $\sum_{(\Delta/k)_1} f(kx)$; when $k > \omega$, the diameter of Δ/k is less than 1, and so Lemma 2.3 cannot be applied. However, if Δ is a set containing the origin, then these sets Δ/k are sets with diameter less than 1 that contain the origin, hence contain no primitive lattice points (indeed, no lattice points at all other than the origin). Therefore the sums over k in the proof of [7, Theorem 2.1] can be truncated at $k \le \omega$, and the rest of the argument goes through thereafter.

The remainder of this section is dedicated to proving Theorem 2.5, which asserts that the error term $E_{\mathcal{A}}(t)$ for any rational polygon $\mathcal{A}$ may be rewritten in terms of the totient error function $E_\Delta(t)$. We begin with a detailed investigation of this latter function.

Definition 2.1. Throughout this section, we employ the notation $\lfloor x \rfloor$ for the greatest integer not exceeding x and $\{x\} = x - \lfloor x \rfloor$ for the fractional part of x. We also employ the sawtooth function defined as

$$B(x) = \{x\} - \frac{1}{2}$$

for all real numbers x; this function is equal to the first periodic Bernoulli polynomial $\bar{B}_1(x)$ except at integer arguments.

Next we recall some well-known and useful estimates for sums involving the Möbius μ-function, which satisfies the key identity

$$\sum_{d\mid n}\mu(d)=\begin{cases}1, & \text{if } n=1,\\ 0, & \text{otherwise.}\end{cases} \tag{2.3}$$

For any real numbers $2\le x\le y$, we have:

$$\sum_{d\le x}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}+O\biggl(\frac{1}{x}\biggr); \tag{2.4}$$

$$\sum_{d\le y}\mu(d)\biggl\lfloor\frac{x}{d}\biggr\rfloor=1; \tag{2.5}$$

$$\biggl|\sum_{d\le x}\frac{\mu(d)}{d}\biggr|\ll 1. \tag{2.6}$$

The proofs of equations (2.4) and (2.6) are in [6], and the identity (2.5) can be found in [1] for instance. We are now ready to give a more precise formula for the totient error term $E_\Delta(t)$.

Proposition 2.2. *For any real numbers $T\ge t\ge 2$,*

$$E_\Delta(t)=-t\sum_{d\le T}\frac{\mu(d)}{d}B\biggl(\frac{t}{d}\biggr)+O(T).$$

Proof. Starting from equation (1.3) and the key identity (2.3), we have

$$\begin{aligned}\#(t\Delta\cap\mathbb{P})&=1+\sum_{1\le m\le t}\sum_{\substack{1\le n\le m\\ \gcd(m,n)=1}}1=\sum_{m\le t}\sum_{\substack{n\le m\\ \gcd(m,n)=1}}\sum_{d\mid\gcd(m,n)}\mu(d)\\ &=\sum_{d\le t}\mu(d)\sum_{\substack{m\le t\\ d\mid m}}\sum_{\substack{n\le m\\ d\mid n}}1=\sum_{d\le t}\mu(d)\sum_{k\le t/d}\sum_{\ell\le k}1\\ &=\sum_{d\le t}\mu(d)\sum_{k\le t/d}k=\sum_{d\le t}\mu(d)\frac{1}{2}\biggl(\biggl\lfloor\frac{t}{d}\biggr\rfloor^2+\biggl\lfloor\frac{t}{d}\biggr\rfloor\biggr)\\ &=\frac{1}{2}\sum_{d\le t}\mu(d)\biggl\lfloor\frac{t}{d}\biggr\rfloor^2+\frac{1}{2}\end{aligned}$$

by equation (2.5). The last sum does not change if we extend its range from $d\le t$ to $d\le T$. Expanding $\lfloor\frac{t}{d}\rfloor^2=(\frac{t}{d}-\{\frac{t}{d}\})^2$, we obtain

$$\begin{aligned}\#(t\Delta\cap\mathbb{P})&=\frac{t^2}{2}\sum_{d\le T}\frac{\mu(d)}{d^2}-t\sum_{d\le T}\frac{\mu(d)}{d}\biggl\{\frac{t}{d}\biggr\}+\sum_{d\le T}\mu(d)\biggl\{\frac{t}{d}\biggr\}^2+\frac{1}{2}\\ &=\frac{t^2}{2}\biggl(\frac{6}{\pi^2}+O\biggl(\frac{1}{T}\biggr)\biggr)-t\sum_{d\le T}\frac{\mu(d)}{d}\biggl\{\frac{t}{d}\biggr\}+O(T)\end{aligned}$$

by equation (2.4) and a trivial bound. Therefore

$$\begin{aligned} E_\Delta(t) = \#(t\Delta \cap \mathbb{P}) - \frac{6}{\pi^2}t^2 \operatorname{Area}(\Delta) &= \frac{3}{\pi^2}t^2 - t\sum_{d\le T}\frac{\mu(d)}{d}\left\{\frac{t}{d}\right\} + O(T) - \frac{3}{\pi^2}t^2 \\ &= -t\sum_{d\le T}\frac{\mu(d)}{d}\left(B\left(\frac{t}{d}\right)+\frac{1}{2}\right) + O(T) = -t\sum_{d\le T}\frac{\mu(d)}{d}B\left(\frac{t}{d}\right) + O(T) \end{aligned}$$

by equation (2.6). □

Counting lattice points in the simplest way (each with weight 1) is problematic in our present context. First, we will be decomposing polygons into unions of triangles that share sides, and so double-counting lattice points on these shared boundaries would become an issue; second, any error term as large as the perimeter for counting lattice points in a triangle would result in an unacceptably large error term in the inclusion-exclusion method we use to detect primitive lattice points. Consquently, we employ a more convenient weighting in our lattice-point counting, namely the solid angle sum of a polygon.

Definition 2.3. For a point $p \in \mathbb{R}^2$, let $B(p;r) = \{q \in \mathbb{R}^2 \colon d(p-q) < r\}$ denote the ball of radius r centered at p. Let λ denote Lebesgue measure on $\mathbb{R}^2$, and define for any polygon $\mathcal{A}$ the solid angle at p:

$$\omega_{\mathcal{A}}(p) = \lim_{r\to 0}\frac{\lambda(B(p;r)\cap\mathcal{A})}{\lambda(B(p;r))}.$$

It follows directly from the definition that

$$\omega_{\mathcal{A}}(p) = \begin{cases} 0, & \text{if } p \notin \mathcal{A}, \\ 1, & \text{if } p \text{ is in the interior of } \mathcal{A}, \\ 1/2, & \text{if } p \text{ lies in the interior of an edge of } \mathcal{A}, \\ \theta_p/2\pi, & \text{if } p \text{ is a vertex of } \mathcal{A}, \end{cases}$$

where θ_p is the angle at the vertex p. Using this function, we define the solid angle sum of the t-dilate of the rational polygon $\mathcal{A}$ to be

$$A_{\mathcal{A}}(t) = \sum_{p\in\mathbb{Z}^2}\omega_{t\mathcal{A}}(p).$$

We also define the corresponding sum over primitive lattice points only:

$$\mathbb{P}_{\mathcal{A}}(t) = \sum_{p\in\mathbb{P}}\omega_{t\mathcal{A}}(p).$$

The benefit of this solid-angle weighting is that both of these functions are additive, in the sense that $A_{\mathcal{A}\cup\mathcal{B}}(t) = A_{\mathcal{A}}(t) + A_{\mathcal{B}}(t)$ and $\mathbb{P}_{\mathcal{A}\cup\mathcal{B}}(t) = \mathbb{P}_{\mathcal{A}}(t) + \mathbb{P}_{\mathcal{B}}(t)$ for any polygons $\mathcal{A}$ and $\mathcal{B}$ with disjoint interiors.

Proposition 2.4. *Let $\mathcal{A}$ be a rational polygon. There exist a real number C, a positive integer k, and rational numbers $c_1, \dots, c_k, f_1, \dots, f_k$ where $f_i > 0$ (all depending on $\mathcal{A}$) such that*

$$A_{\mathcal{A}}(t) = \operatorname{Area}(\mathcal{A})t^2 + Ct - t\sum_{j=1}^{k}c_jB(f_jt) + O(1), \tag{2.7}$$

where the implicit constant may depend upon $\mathcal{A}$. Furthermore, when $\mathcal{A}$ is an origin-star-shaped polygon the c_j may be taken to all be positive.

Proof. Le Quang and Robins [8] gave a precise formula for the solid angle sum of any rational pointed triangle $\mathcal{T}$:

$$A_{\mathcal{T}}(t) = \operatorname{Area}(\mathcal{T})t^2 + C(\mathcal{T})t - t\sum_{j=1}^{k(\mathcal{T})} c_j(\mathcal{T})B(f_j(\mathcal{T})t) + O(1) \tag{2.8}$$

where $C(\mathcal{T})$, $k(\mathcal{T})$, $c_j(\mathcal{T})$, $f_j(\mathcal{T})$ are constants depending on $\mathcal{T}$ with $k(\mathcal{T})$ a positive integer, and the $c_j(\mathcal{T})$ and $f_j(\mathcal{T})$ positive rational numbers. But the rational polygon $\mathcal{A}$ can be partitioned as a signed sum of a finite number of rational pointed triangles (as in the proof of Proposition 1.1). Simply summing the formula (2.8) over these finitely many triangles yields the desired formula (2.7), where C is the sum of the $C(\mathcal{T})$, and $\{f_j\}$ is the union of the $\{f_j(\mathcal{T})\}$, and so on. □

The following theorem results from a careful examination of $\mathbb{P}_{\mathcal{A}}(t)$, which can be related to the solid angle sum $A_{\mathcal{A}}(t)$ using the Möbius function as in the proof of Proposition 2.2.

Theorem 2.5. *Let $\mathcal{A}$ be a rational polygon. There exist a positive integer k, rational numbers $r_1, \dots, r_k$, and positive rational numbers $f_1, \dots, f_k$ such that*

$$E_{\mathcal{A}}(t) = \sum_{j=1}^{k} r_j E_\Delta(f_j t) + O(t), \tag{2.9}$$

where the implicit constant may depend upon $\mathcal{A}$. Furthermore, if $\mathcal{A}$ is an origin-star-shaped polygon, then the r_j may all be taken to be positive as well.

Remark. Theorem 1.2 follows immediately from Theorem 2.5 in light of the known upper bound (1.5). In addition, Theorem 1.4 follows immediately from the combination of Theorem 2.5 and Theorem 1.5; the latter theorem is proved in the next section. Finally, we note that Theorem 2.5 automatically implies the generalization of Theorem 1.5 where the isosceles right triangle Δ is replaced by any rational origin-star-shaped polygon $\mathcal{A}$.

Proof. We commence by excluding the (non-primitive) origin and using the Möbius identity (2.3) to write

$$\mathbb{P}_{\mathcal{A}}(t) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \omega_{t\mathcal{A}}\big((m,n)\big) \sum_{d\mid\gcd(m,n)} \mu(d).$$

Interchanging the order of summation (valid since in reality there are only finitely many nonzero terms) and rescaling (which preserves solid angles),

$$\begin{aligned}\mathbb{P}_{\mathcal{A}}(t) &= \sum_{d=1}^{\infty} \mu(d) \sum_{\substack{(m,n)\in\mathbb{Z}^2\setminus(0,0)\\ d\mid m,\, d\mid n}} \omega_{t\mathcal{A}}\big((m,n)\big) = \sum_{d=1}^{\infty}\mu(d)\sum_{(x,y)\in\mathbb{Z}^2\setminus(0,0)} \omega_{\frac{t}{d}\mathcal{A}}\big((x,y)\big)\\ &= \sum_{d=1}^{\infty}\mu(d)\bigg(A_{\mathcal{A}}\Big(\frac{t}{d}\Big) - \omega_{\frac{t}{d}\mathcal{A}}\big((0,0)\big)\bigg)\end{aligned}$$

by the definition of $A_{\mathcal{A}}$, We may truncate the outer sum at any real number $T \geq t\,\mathrm{diam}(\mathcal{A})$: for larger values of d, the diameter of $\frac{t}{d}\mathcal{A}$ is less than 1, and hence $\frac{t}{d}\mathcal{A}$ (which contains the origin) cannot contain any other lattice points. Proposition 2.4 now implies

$$\begin{aligned}
\mathbb{P}_{\mathcal{A}}(t) &= \sum_{d\leq T} \mu(d)\biggl(\mathrm{Area}(\mathcal{A})\frac{t^2}{d^2} + C\frac{t}{d} - \frac{t}{d}\sum_{j=1}^{k} c_j B\Bigl(f_j\frac{t}{d}\Bigr) + O(1)\biggr) \\
&= \mathrm{Area}(\mathcal{A})t^2 \sum_{d\leq T}\frac{\mu(d)}{d^2} + Ct\sum_{d\leq T}\frac{\mu(d)}{d} \\
&\qquad - t\sum_{j=1}^{k} c_j \sum_{d\leq T}\frac{\mu(d)}{d} B\Bigl(f_j\frac{t}{d}\Bigr) + O\Bigl(\sum_{d\leq T}|\mu(d)|\Bigr) \\
&= \mathrm{Area}(\mathcal{A})t^2\Bigl(\frac{6}{\pi^2} + O\Bigl(\frac{1}{T}\Bigr)\Bigr) + O(|C|t\cdot 1) - t\sum_{j=1}^{k} c_j \sum_{d\leq T}\frac{\mu(d)}{d} B\Bigl(f_j\frac{t}{d}\Bigr) + O(T),
\end{aligned}$$

Using Proposition 2.2, we may rewrite the above in terms of $E_\Delta(t)$ and obtain

$$\mathbb{P}_{\mathcal{A}}(t) = \mathrm{Area}(\mathcal{A})\frac{6}{\pi^2}t^2 + \sum_{i=1}^{k}\frac{c_i}{f_i}E_\Delta(f_i t) + O(T) \tag{2.10}$$

for any $T \geq t\max\{1, \mathrm{diam}(\mathcal{A}), f_1, \ldots, f_k\}$.

The number of integer points on the boundary of $t\mathcal{A}$ is $O(t)$ since $t\mathcal{A}$ has finitely many sides, each of which has length $O(t)$. Consequently,

$$\mathbb{P}_{\mathcal{A}}(t) - \#(t\mathcal{A}\cap\mathbb{P}) \ll t,$$

and therefore equation (2.10) implies

$$\begin{aligned}
E_{\mathcal{A}}(t) &= \#(t\mathcal{A}\cap\mathbb{P}) - \mathrm{Area}(\mathcal{A})\frac{6}{\pi^2}t^2 \\
&= \mathbb{P}_{\mathcal{A}}(t) + O(t) - \mathrm{Area}(\mathcal{A})\frac{6}{\pi^2}t^2 = \sum_{j=1}^{k}\frac{c_j}{f_j}E_\Delta(f_j t) + O(T).
\end{aligned}$$

Upon setting $T = t\max\{1, \mathrm{diam}(\mathcal{A}), f_1, \ldots, f_k\}$ and $r_j = c_j/f_j$ for each $1 \leq j \leq k$, the theorem follows. □

3. Linear combinations of E_Δ

In this section we prove Theorem 1.5, showing that positive rational linear combinations of scaled copies of the totient error function E_Δ have oscillations as large as those known for E_Δ itself. We begin by recalling some of the components of Montgomery's argument [10] establishing the oscillations of E_Δ, after which we describe the strategy that led to our modifications.

Definition 3.1. Define

$$R_0(x) = \sum_{n\leq x}\frac{\phi(n)}{n} - \frac{6}{\pi^2}x.$$

Montgomery [10, Theorem 1] showed that the totient error function is closely connected to the above weighted error:

Lemma 3.2 (Montgomery)**.** $E_\Delta(x) = xR_0(x) + O\big(x\exp(-c\sqrt{\log x})\big)$.

Definition 3.3. Define

$$K(q,\alpha) = -\sum_{d|q} \frac{\mu(d)}{d} B\bigg(\frac{\alpha}{d}\bigg),$$

where the sawtooth function $B(x)$ was defined in Definition 2.1, and

$$C(q,\alpha) = K(q,\alpha)\frac{6}{\pi^2}\prod_{p|q}\bigg(1-\frac{1}{p^2}\bigg)^{-1}.$$

Lemma 3.4. *If b is relatively prime to q, then*

$$K(qb,\alpha b) = \sum_{d_1d_2=b} \frac{\mu(d_1)}{d_1} K(q,\alpha d_2).$$

Proof. Since every divisor of qb can be written uniquely as a divisor of b times a divisor of q,

$$K(qb,\alpha b) = -\sum_{d|qb}\frac{\mu(d)}{d}B\bigg(\frac{\alpha b}{d}\bigg) = -\sum_{a|b}\frac{\mu(a)}{a}\sum_{c|q}\frac{\mu(c)}{c}B\bigg(\frac{\alpha b}{ac}\bigg) = \sum_{a|b}\frac{\mu(a)}{a}K\bigg(q,\frac{\alpha b}{a}\bigg),$$

which is equivalent to the statement of the lemma. □

The above quantities appear [10, Lemma 4] in a key part of Montgomery's argument, which displays a bias in the values of R_0 sampled on an arithmetic progression:

Lemma 3.5 (Montgomery)**.** *There exists a positive real number c such that if α is a non-integral real number with $0 < \alpha < q$, then*

$$\sum_{n=1}^{N} R_0(nq+\alpha) = C(q,\alpha)N + O\big(N\exp(-c\sqrt{\log N})\big)$$

uniformly for $q \le e^{c\sqrt{\log N}}$.

The proof of Lemma 3.5 is based on the following ancient identity due to Raabe [15] for a sum of $B(x)$ over an arithmetic progression of points: for all real numbers x,

$$\sum_{j=1}^{J} B\bigg(x+\frac{j}{J}\bigg) = B(Jx).$$

The relevance to the problem at hand is due to the fact [10, Lemma 1] that

$$R_0(x) = -\sum_{d\le x}\frac{\mu(d)}{d}B\bigg(\frac{x}{d}\bigg) + O(1).$$

To exploit Lemma 3.5, Montgomery chose $\alpha = q/4$, so that for all divisors d of q the quantity $B(\alpha/d)$ equals $\pm\frac{1}{4}$, with the sign depending only upon the residue class of d modulo 4. On the other hand, he chose q to be the product of many primes congruent to 3 modulo 4; for any divisor d of this q, the residue class of d (mod 4) depends only on the number of prime factors of d. With these choices, the sign of $B(\alpha/d)$ correlates exactly with the sign of

$\mu(d)$, making the quantity $K(q,\alpha)$ large in absolute value. Choosing $\alpha = 3q/4$ instead again makes $K(q,\alpha)$ large but with the opposite sign.

One of our key observations is that we may work modulo a suitably chosen prime P rather than working modulo 4. Instead of choosing q to be the product of many primes congruent to 3 (mod 4), we instead choose q to be the product of many primes that are quadratic nonresidues modulo P. The sign of $B(\alpha/d)$ will not be perfectly correlated with $\mu(d)$, but there will be enough of a systematic bias in the signs of $B(\alpha/d)$ (due to the imperfect distribution of quadratic residues and nonresidues modulo P) that we can still force $K(q,\alpha)$ to be large in absolute value. If we choose the prime P carefully, we can even force all of the different $K(qb_i, \alpha b_i)$ to be large in absolute value and have the same sign.

We introduce the following function, whose oscillations we will want to establish. For the rest of this section, we use boldface variables such as $\mathbf{a}$ to indicate the dependence of various quantities on k-tuples $(a_1,\dots,a_k)$ of variables.

Definition 3.6. Given real numbers $a_1,\dots,a_k$ and $b_1,\dots,b_k$, define

$$G_{\mathbf{a},\mathbf{b}}(x) = a_1 R_0(b_1 x) + \cdots + a_k R_0(b_k x).$$

The starting point of our modification of Montgomery's method is the following easy consequence of Lemma 3.5.

Lemma 3.7. *Let $a_1,\dots,a_k$ and $b_1,\dots,b_k > 0$ be real numbers. There exists a positive real number c such that: if $\alpha \in (0,q)$ is a real number such that none of the αb_j is an integer, then*

$$\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nq+\alpha) = N \sum_{j=1}^{k} a_j C(qb_j, \alpha b_j) + O_{\mathbf{a},\mathbf{b}}(N \exp(-c\sqrt{\log N}))$$

uniformly for $\max\{b_1,\dots,b_k\} < q \le e^{c\sqrt{\log N}}$.

We now state our oscillation result for $G_{\mathbf{a},\mathbf{b}}$, after which we show how Theorem 1.5 is implied by it. Thereafter our only remaining goal will be to establish this proposition:

Proposition 3.8. *Let $a_1,\dots,a_k$ and $b_1,\dots,b_k$ be fixed positive integers. There exists a constant $\kappa_{\mathbf{a},\mathbf{b}} > 0$, and sequences $Q_{N,\mathbf{b}} \le e^{\sqrt{\log N}}$ and $0 < \alpha_N^+, \alpha_N^- < Q_{N,\mathbf{b}}$ defined for positive integers N, for which $Q_{N,\mathbf{b}}$ tends to infinity with N and*

$$\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nQ_{N,\mathbf{b}} + \alpha_N^+) = \kappa_{\mathbf{a},\mathbf{b}} N \sqrt{\log\log N} + O_{\mathbf{a},\mathbf{b}}(N)$$

and

$$\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nQ_{N,\mathbf{b}} + \alpha_N^-) = -\kappa_{\mathbf{a},\mathbf{b}} N \sqrt{\log\log N} + O_{\mathbf{a},\mathbf{b}}(N).$$

Proof of Theorem 1.5 assuming Proposition 3.8. By Lemma 3.2,

$$\sum_{j=1}^{k} r_j E_\Delta(s_j x) = x \sum_{j=1}^{k} r_j s_j R_0(s_j x) + O_{\mathbf{r},\mathbf{s}}\big(x \exp(-c\sqrt{\log x})\big).$$

Let $D_{\mathbf{s}}$ be the least common denominator of the rational numbers $s_1, \dots, s_k$, and set $a_j = D_{\mathbf{s}} r_j s_j$ and $b_j = D_{\mathbf{s}} s_j$. Replacing x by $D_{\mathbf{s}} x$, we obtain

$$\sum_{j=1}^{k} r_j E_\Delta(s_j D_{\mathbf{s}} x) = x G_{\mathbf{a},\mathbf{b}}(x) + O_{\mathbf{r},\mathbf{s}}\big(x \exp(-c\sqrt{\log x})\big). \tag{3.1}$$

Let $0 < \varepsilon < \kappa_{\mathbf{a},\mathbf{b}}$. If there existed an x_0 such that $G_{\mathbf{a},\mathbf{b}}(x) < (\kappa_{\mathbf{a},\mathbf{b}} - \varepsilon)\sqrt{\log\log(D_{\mathbf{s}} x)}$ for all $x > x_0$, then we would have

$$\begin{aligned}\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nQ_N + \alpha_N^+) &< (\kappa_{\mathbf{a},\mathbf{b}} - \varepsilon) N \sqrt{\log\log(D_{\mathbf{s}}(NQ_N + \alpha_N^+))} + O(x_0 \max_{1 \le t \le x_0} G_{\mathbf{a},\mathbf{b}}(t)) \\ &= (\kappa_{\mathbf{a},\mathbf{b}} - \varepsilon) N \bigg(\sqrt{\log\log N} + O_{\mathbf{s}}\bigg(\frac{1}{\sqrt{\log N}}\bigg)\bigg) + O_{\varepsilon,\mathbf{a},\mathbf{b}}(1)\end{aligned}$$

by the bounds $0 < \alpha_N^+ < Q_{N,\mathbf{b}}$; for large N (and hence for large $Q_{N,\mathbf{b}}$) this would contradict Proposition 3.8. Therefore no such x_0 can exist, in which case equation (3.1) implies that there are arbitrarily large values of x for which

$$\sum_{j=1}^{k} r_j E_\Delta(s_j D_{\mathbf{s}} x) \ge x(\kappa_{\mathbf{a},\mathbf{b}} - \varepsilon)\sqrt{\log\log(D_{\mathbf{s}} x)} + O_{\mathbf{r},\mathbf{s}}\big(x \exp(-c\sqrt{\log x})\big).$$

In other words,

$$\limsup_{x \to \infty} \frac{r_1 E_\Delta(s_1 x) + \cdots + r_k E_\Delta(s_k x)}{x\sqrt{\log\log x}} \ge \frac{\kappa_{\mathbf{a},\mathbf{b}}}{D_{\mathbf{s}}},$$

and the analogous argument using the values $G(nQ_N + \alpha_N^-)$ gives

$$\liminf_{x \to \infty} \frac{r_1 E_\Delta(s_1 x) + \cdots + r_k E_\Delta(s_k x)}{x\sqrt{\log\log x}} \le -\frac{\kappa_{\mathbf{a},\mathbf{b}}}{D_{\mathbf{s}}},$$

completing the derivation of Theorem 1.5 from Proposition 3.8. □

Before addressing Proposition 3.8 directly, we record some preliminary facts about the distribution of primes in residue classes and the associated L-values.

Lemma 3.9. *Let $P \equiv 3 \pmod 4$ be a prime exceeding 3, and let $\chi_1(\cdot) = \big(\frac{\cdot}{P}\big)$ denote the quadratic character modulo P. Then the class number $h(-P)$ of the field $\mathbb{Q}(\sqrt{-P})$ equals*

$$h(-P) = \frac{\sqrt{P}}{\pi} L(1, \chi_1) = -\frac{1}{P}\sum_{a=1}^{P-1} a\chi_1(a).$$

Proof. These results are classical; see for example [3, Chapter 6, equations (15) and (19)]. □

Lemma 3.10. *Let $P \equiv 3 \pmod 4$ be a prime exceeding 3. If χ_0 denotes the principal character $\pmod P$, then*

$$\prod_{\substack{p \le y \\ (\frac{p}{P}) = -1}} \bigg(1 + \frac{\chi_0(p)}{p}\bigg) = c_P\sqrt{\log y} + O_P(1),$$

where

$$c_P = \left(\frac{e^\gamma}{\pi}\frac{P-1}{h(-P)\sqrt{P}}\prod_{(\frac{p}{P})=-1}\left(1-p^{-2}\right)\right)^{1/2}. \tag{3.2}$$

On the other hand, for any nonprincipal character $\chi \pmod{P}$,

$$\prod_{\substack{p\le y\\ (\frac{p}{P})=-1}}\left(1+\frac{\chi(p)}{p}\right) \ll_P 1.$$

Proof. Again let $\chi_1(\cdot) = \left(\frac{\cdot}{P}\right)$ denote the quadratic character (mod P). For any character $\chi \pmod{P}$ we can write

$$\Bigg(\prod_{\substack{p\le y\\ (\frac{p}{P})=-1}}\left(1+\frac{\chi(p)}{p}\right)\Bigg)^2 = \prod_{p\le y}\left(1-\frac{\chi(p)}{p}\right)^{-1}\prod_{p\le y}\left(1-\frac{\chi(p)\chi_1(p)}{p}\right)\prod_{\substack{p\le y\\ (\frac{p}{P})=-1}}\left(1-\frac{\chi^2(p)}{p^2}\right). \tag{3.3}$$

The last product is absolutely convergent uniformly in P; indeed,

$$\Bigg|\prod_{\substack{p>y\\ (\frac{p}{P})=-1}}\left(1-\frac{\chi^2(p)}{p^2}\right)\Bigg| \le \prod_{\substack{p>y\\ (\frac{p}{P})=-1}}\left(1+\frac{1}{p^2}\right) < \prod_{n>y}\left(1+\frac{1}{n^2}\right) < \prod_{n>y}\left(1-\frac{1}{n^2}\right)^{-1} = 1+\frac{1}{\lceil y\rceil},$$

and so the last product equals $\prod_{(\frac{p}{P})=-1}\left(1-\chi^2(p)p^{-2}\right)\left(1+O\left(\frac{1}{y}\right)\right)$ and in particular is uniformly bounded. When χ is nonprincipal, we know [11, Theorem 4.11(d)] that

$$\prod_{p\le y}\left(1-\frac{\chi(p)}{p}\right)^{-1} = L(1,\chi)+O_\chi\left(\frac{1}{\log y}\right) = L(1,\chi)\left(1+O_P\left(\frac{1}{\log y}\right)\right),$$

since $L(1,\chi)\ne 0$ [11, Theorem 4.9]. (Better error terms are available but are not relevant for us.) In particular, when neither χ nor $\chi\chi_1$ is principal, the first two products on the right-hand side of equation (3.3) are $L(1,\chi)\left(1+O_P\left(\frac{1}{\log y}\right)\right)$ and $L(1,\chi\chi_1)^{-1}\left(1+O_P\left(\frac{1}{\log y}\right)\right)$, respectively; in particular, both are $\ll_P 1$. This estimate establishes the lemma when χ is neither principal nor equal to χ_1.

When $\chi = \chi_1$, the first and third factors are still bounded, while now the second factor actually diverges to 0, hence in particular is still bounded. Finally, when $\chi = \chi_0$ is principal, the second factor converges to $1/L(1,\chi_1) = \sqrt{P}/\pi h(-P)$ by Lemma 3.9, while the first factor on the left-hand side of equation (3.3) is

$$\prod_{p\le y}\left(1-\frac{\chi_0(p)}{p}\right)^{-1} = \prod_{\substack{p\le y\\ p\ne P}}\left(1-\frac{1}{p}\right)^{-1} = \frac{P-1}{P}(e^\gamma\log y)\left(1+O\left(\frac{1}{\log y}\right)\right)$$

by Mertens's formula [11, Theorem 2.7(e)]. This asymptotic evaluation of the right-hand side of equation (3.3) establishes the lemma when χ is principal, indeed with the stronger error term $O_P\left(\frac{1}{\sqrt{\log y}}\right)$. □

We can now define the modulus $Q_{N,\mathbf{b}}$ appearing in the statement of Proposition 3.8, in terms of a companion prime $P_{\mathbf{b}}$.

Definition 3.11. Let $P_{\mathbf{b}}$ be the smallest prime satisfying $P_{\mathbf{b}} \equiv -1 \pmod{8b_1 \dots b_k}$. Note that $P_{\mathbf{b}} \equiv 7 \pmod 8$, and so -1 is a quadratic nonresidue $\pmod{P_{\mathbf{b}}}$ while 2 is a quadratic residue $\pmod{P_{\mathbf{b}}}$. Furthermore, if p is any odd prime dividing one of the b_j, then by quadratic reciprocity [12, Theorem 3.1] we have, since $P_{\mathbf{b}} \equiv 3 \pmod 4$ and $P_{\mathbf{b}} \equiv -1 \pmod p$,

$$\left(\frac{p}{P_{\mathbf{b}}}\right) = (-1)^{(p-1)/2}\left(\frac{P_{\mathbf{b}}}{p}\right) = (-1)^{(p-1)/2}\left(\frac{-1}{p}\right) = 1.$$

Consequently, each prime dividing every b_j is a quadratic residue $\pmod{P_{\mathbf{b}}}$.

Now define, for any integer $N \geq 1$,

$$Q_{N,\mathbf{b}} = \prod_{\substack{p \leq c\sqrt{\log N} \\ \left(\frac{p}{P_{\mathbf{b}}}\right) = -1}} p,$$

where c is the constant from Lemma 3.7. Since

$$\log Q_{N,\mathbf{b}} = \sum_{\substack{1 \leq a \leq P_{\mathbf{b}} \\ \left(\frac{a}{P_{\mathbf{b}}}\right) = -1}} \sum_{\substack{p \leq c\sqrt{\log N} \\ p \equiv a \pmod{P_{\mathbf{b}}}}} \log p = \sum_{\substack{1 \leq a \leq P_{\mathbf{b}} \\ \left(\frac{a}{P_{\mathbf{b}}}\right) = -1}} \theta\big(c\sqrt{\log N}; P_{\mathbf{b}}, a\big),$$

where the sum on the right-hand side is over $\phi(P_{\mathbf{b}})/2$ reduced residue classes modulo $P_{\mathbf{b}}$, the prime number theorem for arithmetic progressions to a fixed modulus (see [11, Corollary 11.21]) implies that

$$\log Q_{N,\mathbf{b}} \sim \frac{1}{2}c\sqrt{\log N}.$$

In particular, $Q_{N,\mathbf{b}}$ tends to infinity with N, and $Q_{N,\mathbf{b}} < e^{c\sqrt{\log N}}$ when N is large enough.

Note also that $Q_{N,\mathbf{b}}$ is squarefree and relatively prime to $P_{\mathbf{b}}$ and to each b_j, since every prime $p \mid b_j$ satisfies $\big(\frac{p}{P_{\mathbf{b}}}\big) = 1$. Finally, note that any divisor d of $Q_{N,\mathbf{b}}$ has the convenient (and, for us, crucial) property that $\big(\frac{d}{P_{\mathbf{b}}}\big) = \mu(d)$, since both quantities equal $(-1)^{\#\{p \mid d\}}$.

Lemma 3.12. *For any $1 \leq b \leq P-1$, we have*

$$\sum_{\substack{d \mid Q_{N,\mathbf{b}} \\ d \equiv b \pmod{P_{\mathbf{b}}}}} \frac{1}{d} = \frac{c_{P_{\mathbf{b}}}}{\sqrt{2}(P_{\mathbf{b}} - 1)}\sqrt{\log\log N} + O_{\mathbf{b}}(1),$$

where c_P was defined in equation (3.2).

Proof. From the orthogonality of the characters modulo $P_{\mathbf{b}}$,

$$\begin{aligned}\sum_{\substack{d|Q_{N,\mathbf{b}}\\ d\equiv b \pmod{P_{\mathbf{b}}}}} \frac{1}{d} &= \frac{1}{P_{\mathbf{b}}-1} \sum_{\chi \pmod{P_{\mathbf{b}}}} \bar{\chi}(b) \sum_{d|Q_{N,\mathbf{b}}} \frac{\chi(d)}{d} \\ &= \frac{1}{P_{\mathbf{b}}-1} \sum_{\chi \pmod{P_{\mathbf{b}}}} \bar{\chi}(b) \prod_{p|Q_{N,\mathbf{b}}} \left(1+\frac{\chi(p)}{p}\right) \\ &= \frac{1}{P_{\mathbf{b}}-1} \sum_{\chi \pmod{P_{\mathbf{b}}}} \bar{\chi}(b) \prod_{\substack{p\le c\sqrt{\log N}\\ \left(\frac{p}{P_{\mathbf{b}}}\right)=-1}} \left(1+\frac{\chi(p)}{p}\right) \\ &= \frac{1}{P_{\mathbf{b}}-1} c_{P_{\mathbf{b}}} \sqrt{\log(c\sqrt{\log N})} + O_{P_{\mathbf{b}}}(1)\end{aligned}$$

by Lemma 3.10. The statement of the lemma follows upon noting that $\log(c\sqrt{\log N}) = \frac{1}{2}\log\log N + O(1)$. □

Lemma 3.13. *For any integer m that is not a multiple of $P_{\mathbf{b}}$ and for any integer $N \ge 3$,*

$$K\left(Q_{N,\mathbf{b}}, \frac{mQ_{N,\mathbf{b}}}{P_{\mathbf{b}}}\right) = \left(\frac{m}{P_{\mathbf{b}}}\right)\left(\frac{Q_{N,\mathbf{b}}}{P_{\mathbf{b}}}\right) \frac{c_{P_{\mathbf{b}}} h(-P_{\mathbf{b}})}{\sqrt{2}(P_{\mathbf{b}}-1)} \sqrt{\log\log N} + O_{\mathbf{b}}(1).$$

Remark. The exact value of the leading constant is not as important for us as the fact that its dependence on m is only in the term $\left(\frac{m}{P_{\mathbf{b}}}\right)$, so that the sign of the leading constant depends on whether m is a quadratic residue or nonresidue modulo $P_{\mathbf{b}}$.

Proof. By Definition 3.3 and the coincidence between the Legendre symbol and the Möbius function on divisors of $Q_{N,\mathbf{b}}$ (as noted at the end of Definition 3.11), we have

$$\begin{aligned}-K\left(Q_{N,\mathbf{b}}, \frac{mQ_{N,\mathbf{b}}}{P_{\mathbf{b}}}\right) &= \sum_{d|Q_{N,\mathbf{b}}} \frac{\mu(d)}{d} B\left(\frac{mQ_{N,\mathbf{b}}}{dP_{\mathbf{b}}}\right) \\ &= \sum_{d|Q_{N,\mathbf{b}}} \left(\frac{d}{P_{\mathbf{b}}}\right)\frac{1}{d} B\left(\frac{mQ_{N,\mathbf{b}}}{dP_{\mathbf{b}}}\right) \\ &= \sum_{d|Q_{N,\mathbf{b}}} \left(\frac{mQ_{N,\mathbf{b}}}{P_{\mathbf{b}}}\right)\left(\frac{mQ_{N,\mathbf{b}}/d}{P_{\mathbf{b}}}\right)\frac{1}{d} B\left(\frac{mQ_{N,\mathbf{b}}}{dP_{\mathbf{b}}}\right) \\ &= \left(\frac{mQ_{N,\mathbf{b}}}{P_{\mathbf{b}}}\right) \sum_{a=1}^{P_{\mathbf{b}}-1} \left(\frac{a}{P_{\mathbf{b}}}\right) B\left(\frac{a}{P_{\mathbf{b}}}\right) \sum_{\substack{d|Q_{N,\mathbf{b}}\\ mQ_{N,\mathbf{b}}d^{-1}\equiv a \pmod{P_{\mathbf{b}}}}} \frac{1}{d}.\end{aligned}$$

The last congruence is equivalent to d being in the reduced residue class $mQ_{N,\mathbf{b}}a^{-1} \pmod{P_\mathbf{b}}$, and so Lemma 3.12 applies:

$$\begin{aligned}-K\Big(Q_{N,\mathbf{b}}, \frac{mQ_{N,\mathbf{b}}}{P_\mathbf{b}}\Big) &= \Big(\frac{mQ_{N,\mathbf{b}}}{P_\mathbf{b}}\Big)\sum_{a=1}^{P_\mathbf{b}-1}\Big(\frac{a}{P_\mathbf{b}}\Big)B\Big(\frac{a}{P_\mathbf{b}}\Big)\Big(\frac{c_{P_\mathbf{b}}}{\sqrt{2}(P_\mathbf{b}-1)}\sqrt{\log\log N} + O_\mathbf{b}(1)\Big)\\ &= \Big(\frac{mQ_{N,\mathbf{b}}}{P_\mathbf{b}}\Big)\frac{c_{P_\mathbf{b}}}{\sqrt{2}(P_\mathbf{b}-1)}\sqrt{\log\log N}\sum_{a=1}^{P_\mathbf{b}-1}\Big(\frac{a}{P_\mathbf{b}}\Big)B\Big(\frac{a}{P_\mathbf{b}}\Big) + O_\mathbf{b}(1).\end{aligned}$$

By the definition of the Bernoulli polynomial B, this sum equals

$$\sum_{a=1}^{P_\mathbf{b}-1}\Big(\frac{a}{P_\mathbf{b}}\Big)B\Big(\frac{a}{P_\mathbf{b}}\Big) = \frac{1}{P_\mathbf{b}}\sum_{a=1}^{P_\mathbf{b}-1}a\Big(\frac{a}{P_\mathbf{b}}\Big) - \frac{1}{2}\sum_{a=1}^{P_\mathbf{b}-1}\Big(\frac{a}{P_\mathbf{b}}\Big) = -h(-P_\mathbf{b}) - 0$$

by Lemma 3.9, which completes the proof of the lemma. □

We now have all the tools we need to establish Proposition 3.8 and hence our main theorems.

Proof of Proposition 3.8. Given a sufficiently large integer N, define two numbers

$$\alpha_N^\pm = \frac{m^\pm Q_{N,\mathbf{b}}}{P_\mathbf{b}},$$

where the integers $1 \le m^\pm \le P_\mathbf{b} - 1$ satisfy $m^\pm \equiv \pm Q_{N,\mathbf{b}} \pmod{P_\mathbf{b}}$; note that none of the numbers $\alpha_N^\pm b_j$ is an integer, since neither $Q_{N,\mathbf{b}}$ nor any of the b_j is a multiple of the prime $P_\mathbf{b}$. Since we confirmed in Definition 3.11 that $Q_{N,\mathbf{b}} < e^{c\sqrt{\log N}}$, we may invoke Lemma 3.7:

$$\begin{aligned}\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nQ_{N,\mathbf{b}} + \alpha_N^+) &= N\sum_{j=1}^{k} a_j C(Q_{N,\mathbf{b}}b_j, \alpha_N^+ b_j) + O\big(N\exp(-c\sqrt{\log N})\big)\\ &= N\sum_{j=1}^{k} a_j K(Q_{N,\mathbf{b}}b_j, \alpha_N^+ b_j)\frac{6}{\pi^2}\prod_{p\mid Q_{N,\mathbf{b}}b_j}\Big(1-\frac{1}{p^2}\Big)^{-1} + O(N).\end{aligned}$$

As noted in Definition 3.11, each b_j is relatively prime to $Q_{N,\mathbf{b}}$. Thus by Lemma 3.4 with our choice of $\alpha_N^\pm$,

$$\begin{aligned}&\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nQ_{N,\mathbf{b}} + \alpha_N^\pm) = O(N)\\ &\qquad + \frac{6}{\pi^2}N\prod_{p\mid Q_{N,\mathbf{b}}}\Big(1-\frac{1}{p^2}\Big)^{-1}\sum_{j=1}^{k}a_j\prod_{p\mid b_j}\Big(1-\frac{1}{p^2}\Big)^{-1}\sum_{d_1d_2=b_j}\frac{\mu(d_1)}{d_1}K\Big(Q_{N,\mathbf{b}}, \frac{m^\pm d_2 Q_{N,\mathbf{b}}}{P_\mathbf{b}}\Big).\end{aligned}$$

By Lemma 3.13,

$$\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nQ_{N,\mathbf{b}}+\alpha_N^{\pm}) = O(N) + \frac{6}{\pi^2}N\prod_{p|Q_{N,\mathbf{b}}}\left(1-\frac{1}{p^2}\right)^{-1}\sum_{j=1}^{k}a_j\prod_{p|b_j}\left(1-\frac{1}{p^2}\right)^{-1}$$
$$\times\sum_{d_1d_2=b_j}\frac{\mu(d_1)}{d_1}\left(\left(\frac{m^{\pm}d_2}{P_{\mathbf{b}}}\right)\left(\frac{Q_{N,\mathbf{b}}}{P_{\mathbf{b}}}\right)\frac{c_{P_{\mathbf{b}}}h(-P_{\mathbf{b}})}{\sqrt{2}(P_{\mathbf{b}}-1)}\sqrt{\log\log N}+O_{\mathbf{b}}(1)\right).$$

As noted in Definition 3.11, every prime dividing b_j is a quadratic residue modulo $P_{\mathbf{b}}$, which implies that $\big(\frac{d_2}{P_{\mathbf{b}}}\big)=1$ always. Moreover, $m^+\equiv Q_{N,\mathbf{b}} \pmod{P_{\mathbf{b}}}$, so the product of Legendre symbols $\big(\frac{m^+}{P_{\mathbf{b}}}\big)\big(\frac{Q_{N,\mathbf{b}}}{P_{\mathbf{b}}}\big)$ equals 1; on the other hand, since -1 is a quadratic nonresidue modulo $P_{\mathbf{b}}$, the product of Legendre symbols $\big(\frac{m^-}{P_{\mathbf{b}}}\big)\big(\frac{Q_{N,\mathbf{b}}}{P_{\mathbf{b}}}\big)$ equals -1. Consequently,

$$\sum_{n=1}^{N} G_{\mathbf{a},\mathbf{b}}(nQ_{N,\mathbf{b}}+\alpha_N^{\pm}) = \pm\frac{6}{\pi^2}\frac{c_{P_{\mathbf{b}}}h(-P_{\mathbf{b}})}{\sqrt{2}(P_{\mathbf{b}}-1)}N\sqrt{\log\log N}\prod_{p|Q_{N,\mathbf{b}}}\left(1-\frac{1}{p^2}\right)^{-1}\sum_{j=1}^{k}a_j$$
$$\times\prod_{p|b_j}\left(1-\frac{1}{p^2}\right)^{-1}\sum_{d_1d_2=b_j}\frac{\mu(d_1)}{d_1}+O(N).$$

The last sum equals $\sum_{d|b_j}\frac{\mu(d)}{d}=\frac{\phi(b_j)}{b_j}$, which when multiplied by the preceding product becomes $\prod_{p|b_j}(1+\frac{1}{p})^{-1}$. In addition, by the same argument as in the proof of Lemma 3.10,

$$\prod_{p|Q_{N,\mathbf{b}}}\left(1-\frac{1}{p^2}\right)^{-1} = \prod_{(\frac{p}{P_{\mathbf{p}}})=-1}\left(1-\frac{1}{p^2}\right)^{-1}+O\left(\frac{1}{\sqrt{\log N}}\right).$$

We therefore see that we have established the proposition with

$$\kappa_{\mathbf{a},\mathbf{b}} = \frac{6}{\pi^2}\frac{c_{P_{\mathbf{b}}}h(-P_{\mathbf{b}})}{\sqrt{2}(P_{\mathbf{b}}-1)}\prod_{(\frac{p}{P_{\mathbf{p}}})=-1}\left(1-\frac{1}{p^2}\right)^{-1}\sum_{j=1}^{k}a_j\prod_{p|b_j}\left(1+\frac{1}{p}\right)^{-1}$$
$$= \frac{e^{\gamma/2}3\sqrt{2}}{\pi^{5/2}}\frac{h(-P_{\mathbf{b}})^{1/2}}{P^{1/4}\sqrt{P_{\mathbf{b}}-1}}\prod_{(\frac{p}{P_{\mathbf{p}}})=-1}\left(1-\frac{1}{p^2}\right)^{-1/2}\sum_{j=1}^{k}a_j\prod_{p|b_j}\left(1+\frac{1}{p}\right)^{-1} \tag{3.4}$$

by the definition (3.2) of c_P. □

Remark. The condition that all of the a_j are positive is used here only to ensure that this last line is non-zero. In the case where the a_j may be arbitrary, and thus where the innermost sum in equation (3.4) may equal 0, it is possible that modifying $Q_{N,\boldsymbol{b}}$ and the above argument could prove the totient independence for any coefficients; however, we succeeded in getting this to work only when $k\le 3$.

It is interesting to note that the methods of [2], which handle primitive points in planar convex regions that have nowhere-vanishing Gaussian curvature, are quite different from the present methods and they involve the analysis of zeta functions.

Acknowledgments. The first author was partially supported by ERC Advanced Research Grant no 267165 (DISCONV) and by Hungarian National Science Grant K 111827. The second author was supported in part by a Natural Sciences and Engineering Research Council of Canada Discovery Grant. The fourth author was partially supported by ICERM, the Institute for Computational and Experimental Research in Mathematics, Brown University, and would like to thank the warm hospitality of the first author and the Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences.

References

[1] Tom M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer–Verlag 1976.

[2] Roger C. Baker, *Primitive lattice points in planar domains*, Acta Arith. 142 (2010), no. 3, 267–302.

[3] Harold Davenport, *Multiplicative number theory, Third Edition*, Graduate Texts in Mathematics 74, Springer–Verlag, New York, 2000.

[4] Paul Erdős and Harold N. Shapiro, *On the changes of sign of a certain error function*, Canadian J. Math. 3 (1951), 375–385.

[5] Godfrey Harold Hardy and Edward Maitland Wright, *An Introduction to the Theory of Numbers* (5th ed.), The Clarendon Press Oxford University Press, 1979.

[6] Graham J. O. Jameson, *The Prime Number Theorem*, London Mathematical Society, Student Texts 53. Cambridge University Press, 2003.

[7] Evangelos Kranakis and Michel Pocchiola, *Counting problems relating to a theorem of Dirichlet*, Computational Geometry, theory and applications 4 (1994), 309–325.

[8] Nhat Le Quang and Sinai Robins, *Solid angle sums for real dilations of rational polygons*, preprint.

[9] Franz Mertens, *Über einige asymptotische Gesetze der Zahlentheorie*, J. Reine Angew. Math. 77 (1874), 289–338.

[10] Hugh L. Montgomery, *Fluctuations in the mean of Euler's phi function*, Proc. Indian Acad. Sci. (Math. Sci.), vol. 97 (1987), 1–3, 239–245.

[11] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[12] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, Inc., New York (1991).

[13] Maria Nosarzewska, *Evaluation de la difference entre l'aire d'une region plane convexe et le nombre des points aux coordonnes entieres couverts par elle*, Colloq. Math. 1 (1948), 305–311.

[14] Subbayya Sivasankaranarayana Pillai and Sarvadaman Chowla, *On the error terms in some asymptotic formulae in the theory of numbers (1)*, J. London Math. Soc. 5 (1930), no. 2, 95–101.

[15] Joseph Ludwig Raabe, *Zurückführung einiger Summen und bestimmten Integrale auf die Jacob Bernoullische Function*, J. Reine Angew. Math. 42 (1851), 348–376.

[16] Claude Ambrose Rogers, *Existence theorems in the geometry of numbers*, Ann. of Math. 48 (1947), 994–1002.

[17] Arnold Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Mathematische Forschungsberichte, XV. VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.

Rényi Institute of Mathematics, Hungarian Academy of Sciences,
H-1364 Budapest, Pf. 127, Hungary and
Department of Mathematics, University College London,
Gower Street, London, WC1E 6BT, England
E-mail address: barany@renyi.hu

Department of Mathematics, University of British Columbia
Room 121, 1984 Mathematics Road, Vancouver, BC, Canada V6T 1Z2
E-mail address: gerg@math.ubc.ca

E-mail address: naslund.eric@gmail.com

Sinai Robins, Instituto de Mathematica e Estatistica, Universidade de São Paulo,
05508-090 São Paulo, Brazil
E-mail address: srobins@ime.usp.br