Canad. J. Math. Vol. **61** (6), 2009 pp. 1214–1238

Close Lattice Points on Circles

Javier Cilleruelo and Andrew Granville

Abstract. We classify the sets of four lattice points that all lie on a short arc of a circle that has its center at the origin; specifically on arcs of length $tR^{1/3}$ on a circle of radius R, for any given $t > 0$. In particular we prove that any arc of length $(40 + \frac{40}{3}\sqrt{10})^{1/3}R^{1/3}$ on a circle of radius R, with $R > \sqrt{65}$, contains at most three lattice points, whereas we give an explicit infinite family of 4-tuples of lattice points, $(\nu_{1,n}, \nu_{2,n}, \nu_{3,n}, \nu_{4,n})$, each of which lies on an arc of length $(40 + \frac{40}{3}\sqrt{10})^{1/3}R_n^{1/3} + o(1)$ on a circle of radius R_n.

1 Introduction

How many lattice points $(x, y) \in \mathbb{Z}^2$ can be on a "small" arc of the circle $x^2+y^2 = R^2$? (If there are points with integer coordinates on the circle $x^2 + y^2 = R^2$, then R^2 must be an integer. Henceforth we shall assume this, whether we state it or not.) A. Córdoba and the first author [3] proved that for every $\epsilon > 0$ the number of lattice points on an arc of length $R^{\frac{1}{2}-\epsilon}$ is bounded uniformly in R. More precisely, they proved the following (see also [4, 6]).

Theorem 1.1 *For any integer $k \geq 1$, an arc of length $\sqrt{2}R^{\frac{1}{2}-\frac{1}{4[k/2]+2}}$ on a circle of radius R centered at the origin contains no more than k lattice points.*

This result cannot be improved for $k = 1$, since the circles $x^2 + y^2 = 2n^2 + 2n + 1$ contain two lattice points, $(n, n + 1)$ and $(n + 1, n)$, on an arc of length $\sqrt{2} + o(1)$.

For $k = 2$, Theorem 1.1 was first proved by Schinzel and then used by Zygmund [10] to prove a result about spherical summability of Fourier series in two dimensions. In [2] the first author gave a best possible version of Schinzel's result (which we will prove more easily in Section 2).

Theorem 1.2 *An arc of length $(16R)^{1/3}$on a circle of radius R centered at the origin contains no more than two lattice points.*

This result cannot be improved, since the circles $x^2+y^2 = R_n^2 := 16n^6+4n^4+4n^2+1$ contain three lattice points, $(4n^3-1, 2n^2+2n)$, $(4n^3, 2n^2+1)$, and $(4n^3+1, 2n^2-2n)$, on an arc of length $(16R_n)^{\frac{1}{3}} + o_n(1)$.

Let $[\nu] = (\nu_1, \dots, \nu_k)$ denote a k-tuple of lattice points lying on the same circle of radius $R = R_{[\nu]}$ centered at the origin, and $\mathrm{Arc}[\nu] = \mathrm{Arc}(\nu_1, \dots, \nu_k)$ the length of the shortest arc containing $\nu_1, \dots, \nu_k$.

The next result shows that we cannot improve the constant $(16)^{1/3}$ if we omit the examples above.

Received by the editors January 25, 2007.

The second author was partially supported by an NSERC grant. He would like to thank the first author for his frequent hospitality, as well that of the Universidad Autónoma de Madrid, over the years in which we worked together on this stubborn problem.

AMS subject classification: 11N36.

Theorem 1.3 *The set* $\{\mathrm{Arc}[\nu]R_{[\nu]}^{-1/3}, [\nu] = (\nu_1, \nu_2, \nu_3)\}$ *is dense in* $[(16)^{1/3}, +\infty)$.

Since we have sharp versions of Theorem 1.1 for $k = 1$ and 2, we focus in this paper on giving a sharp version of Theorem 1.1 for $k = 3$. We begin with showing that the exponent given in Theorem 1.1 is best possible for $k = 3$ by exhibiting infinitely many circles $x^2+y^2 = R^2$ with four lattice points in an arc of length $\ll R^{1/3}$. The Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. The circles $x^2 + y^2 = R_n^2 := \frac{5}{2}F_{2n-1}F_{2n+1}F_{2n+3}$ contain the four lattice points $\frac{1}{2}(F_{3n+3}, F_{3n}) + (-1)^n z_j$ for $j = 1, 2, 3, 4$, where

$$z_1 = 2(-F_{n-1}, F_{n+2}), \qquad z_2 = (-F_{n-2}, F_{n+1}),$$
$$z_3 = (F_{n-1}, -F_{n+2}), \qquad z_4 = (F_n, -F_{n+3}).$$

The chord length between z_1 and z_4 is $\sqrt{10F_{2n+3}}$, implying that the arc containing all four lattice points has length

$$2R_n \arcsin\left(\frac{\sqrt{10F_{2n+3}}}{2R_n}\right) = 20^{\frac{1}{3}}\left(\frac{1+\sqrt{5}}{2}\right)R_n^{1/3} + \frac{2\sqrt{5}}{3R_n} + O\left(\frac{1}{R_n^{7/3}}\right).$$

In fact this arc can be shown always to have length $> 20^{\frac{1}{3}}(\frac{1+\sqrt{5}}{2})R_n^{1/3}$. (The reader might like to compare this example with the more easily appreciated example given in Section 10 for the analogous problem involving lattice points on hyperbolae.)

We see here a family $\mathcal{F} = \{[\nu]_n = (\nu_{1,n}, \nu_{2,n}, \nu_{3,n}, \nu_{4,n}),\ n \in \mathbb{N}\}$ of 4-tuples of lattice points, lying on circles centered at the origin, with

$$\mathrm{Arc}[\nu]_n \sim C_{\mathcal{F}} R_n^{1/3}, \quad \text{as } n \to \infty.$$

There are other examples of such families $\mathcal{F}$, which we will describe in detail in Section 3, though there are only finitely many such $\mathcal{F}$ with $C_{\mathcal{F}} \leq t$. The main result of this paper is that any 4-tuple of lattice points that lie on a short arc of a circle, specifically on an arc of length $tR^{1/3}$ on a circle of radius R centered at the origin, either belongs to one of a finite set $\mathcal{F}(t)$ of such families or is one of a finite number of small examples (that is, examples which lie on circles with a bounded radius). We shall show how explicitly to construct the families in $\mathcal{F}(t)$, as well as all the "small examples". These small examples are either so small that the bound $tR^{1/3}$ on the arc length is bigger than the radius R, or they are small members of families $\mathcal{F}$ with $C_{\mathcal{F}}$ a tiny bit bigger than t, or they belong to a class of "degenerate examples" which we will study in detail.

Theorem 1.4 *For any* $t > 0$*, any arc on a circle* $x^2 + y^2 = R^2$ *of length less than* $tR^{1/3}$ *with* $R > 2^{-17}t^{15}$ *contains at most three lattice points, except for those arcs containing* 4*-tuples of lattice points from the families* $\mathcal{F}$*, where* $\mathcal{F} \in \mathcal{F}(t) = \{\mathcal{F},\ C_{\mathcal{F}} \leq t\}$*. The set* $\mathcal{F}(t)$ *is finite.*

Note that although $\mathcal{F}(t)$ is finite, it is also true that $\#\mathcal{F}(t) \to \infty$ as $t \to \infty$.

In contrast to Theorem 1.3, we deduce from Theorem 1.4 the following.

Corollary 1.5 *The set* $\{\mathrm{Arc}[\nu]R_{[\nu]}^{-1/3}, [\nu] = (\nu_1, \nu_2, \nu_3, \nu_4)\}$ *has only finitely many accumulation points in any interval* $[0, t)$*, where* $t \in \mathbb{R}^+$.

We order the families $\mathcal{F}_1, \mathcal{F}_2, \dots$ so that $C_{\mathcal{F}_1} \le C_{\mathcal{F}_2} \le \cdots$. For fixed t we can explicitly determine $\mathcal{F}(t)$ using Algorithm 1, described in Section 8; indeed, in Table 1 there we describe all seven families belonging to $\mathcal{F}(5)$. We found that $C_{\mathcal{F}_1} = (40 + \frac{40}{3}\sqrt{10})^{1/3} = 4.347\cdots$, and then $C_{\mathcal{F}_2} = 20^{\frac{1}{3}}(\frac{1+\sqrt{5}}{2}) = 4.3920\cdots$, where $\mathcal{F}_2$ is the family given above.

Algorithm 2, which is also described in Section 8, gives an effective version of Theorem 1.4 and allow us to describe all 4-tuples of lattice points with $\mathrm{Arc}[\nu] \le tR^{1/3}$. As a consequence we deduce the following result.

Corollary 1.6 *An arc of the circle* $x^2 + y^2 = R^2$ *with* $R > \sqrt{65}$*, of length* $\le (40 + \frac{40}{3}\sqrt{10})^{1/3}R^{1/3}$*, contains at most three lattice points. On the contrary, there are infinitely many circles* $x^2 + y^2 = R_n^2$ *containing four lattice points in arcs of length* $(40 + \frac{40}{3}\sqrt{10})^{1/3}R_n^{1/3} + o(1)$.

As an example of how this corollary may be extended, we also give the following result.

Corollary 1.7 *An arc of the circle* $x^2 + y^2 = R^2$ *with* $R > \sqrt{325}$*, of length* $\le 2(1 + \sqrt{2})R^{1/3}$*, contains at most three lattice points, except for the* 4*-tuples* $(\nu_1, \nu_2, \nu_3, \nu_4)$*, belonging to the families* $\mathcal{F}_i, 1 \le i \le 6$ *described in Table* 1 *of Section* 8.

Let $N_k(t, x)$ be the number of k-tuples of lattice points that lie on an arc of length tR^{e_k} of a circle of radius R centered at the origin, with $R \le x$ and for an appropriate exponent e_k. The only exponents we know are $e_2 = 0, e_3 = e_4 = 1/3$; the rest remain a mystery (see Section 12). It is not difficult to show, via elementary means, that

$$N_2(t, x) = \frac{16}{\pi}xt\log t + O(xt + t^2\log t).$$

For $k = 3$ and 4, the arc is only larger than the circle itself once $x \gg t^{3/2}$. In this, the non-trivial range, we prove the following result.

Theorem 1.8 $x^{2/3}t^2\log t \ll N_3(t, x) \ll x^{2/3}t^2\log^3 t$*, for* $x \gg t^{3/2} \gg 1$*. For each fixed* t *there exists a constant* B_t *such that* $N_4(t, x) \sim B_t \log x$ *as* $x \to \infty$.

We finish this introduction with an overview of the paper. In Section 2 we prove Theorems 1.2 and 1.3 concerning 3-tuples $[\nu]$ of lattice points in short arcs. We return to this theme in Section 9 when we estimate how often short arcs contain 3-tuples of lattice points (Theorem 1.8). In Section 3 we construct the families $\mathcal{F}$ of 4-tuples of lattice points on short arcs that we mentioned above. In Section 5 we study the key invariant $Q_{\mathcal{F}}$ of a family $\mathcal{F}$ of 4-tuples of lattice points. Roughly speaking, the larger $Q_{\mathcal{F}}$ is, the larger $C_{\mathcal{F}}$ is. Section 6 is devoted to classifying the degenerate 4-tuples $[\nu]$ (which are those $[\nu]$ for which $Q_{[\nu]}$ is a square). In Section 7 we study the constant $C_{\mathcal{F}}$ associated with a family $\mathcal{F}$, obtaining an effective version of $\mathrm{Arc}[\nu]_n \sim C_{\mathcal{F}}R_n^{1/3}$. We also prove that if $C_{\mathcal{F}}$ is small, then $\mathcal{F}$ or $\hat{\mathcal{F}}$ contains a small

4-tuple. The results of Sections 5, 6, and 7 are needed to justify the two algorithms that we present in this section: Algorithm 1 determines all families $\mathcal{F}$ with $C_{\mathcal{F}} \le t$, for any $t > 0$, and Algorithm 2 determines all the 4-tuples $[\nu]$ with $\mathrm{Arc}[\nu] < tR_{[\nu]}^{1/3}$. In Section 10 we discuss work in progress on the analogous problem for divisors in short intervals. In Section 11 we discuss related questions and in Section 12 the key open problems that arise after this paper.

2 Three Lattice Points

We give here the proof of several results that were discussed in the introduction. Our new proof of Theorem 1.2 is somewhat simpler than that in [2].

Proof of Theorem 1.2 Suppose that ν_1, ν_2, ν_3 are three lattice points, in order, on a circle of radius R so that

$$|\nu_1 - \nu_2||\nu_2 - \nu_3||\nu_1 - \nu_3| < \mathrm{Arc}(\nu_1, \nu_2)\mathrm{Arc}(\nu_2, \nu_3)\,\mathrm{Arc}(\nu_1, \nu_3) \le \frac{1}{4}\,\mathrm{Arc}(\nu_1, \nu_3)^3.$$

A theorem attributed to Heron of Alexandria states that if Δ is the area of the triangle with sides a, b, c and R is the radius of the circle going through the vertices of the triangle, then $abc = 4\Delta R$. Applying this to the triangle with vertices ν_1, ν_2, ν_3, we have that $|\nu_1 - \nu_2||\nu_2 - \nu_3||\nu_1 - \nu_3| = 4\Delta R$.

It should be noted that any triangle with integer vertices has area $\ge 1/2$ so, *a priori*, $\Delta \ge 1/2$. However, we can do better than this: since ν_1, ν_2, ν_3 lie on the same circle, an easy parity argument implies that the coordinates of two of these lattice points, say $\nu_i \ne \nu_j$, have the same parity, and so $\frac{1}{2}(\nu_i + \nu_j)$ is also an integer lattice point. Therefore the triangle ν_1, ν_2, ν_3 is the disjoint union of two triangles with integer coordinates, which implies that $\Delta \ge 1$. The result follows.[1] ∎

Henceforth we identify the lattice point $(x, y) \in \mathbb{Z}^2$ with the Gaussian integer $x + iy$.

Proof of Theorem 1.3 Let $C \ge (16)^{1/3}$ and let α satisfy $(1 + \alpha)(\frac{4}{\alpha+\alpha^2})^{1/3} = C$. Take p and q to be distinct large primes for which $n_2 \sim \alpha n_1$ where $n_1 = 2p$ and $n_2 = q$. Now take m_1 to be an odd integer and m_2 to be an even integer much larger than n_1 and n_2, such that $m_1 n_2 - m_2 n_1 = \pm 1$. Finally take $n_3 = \frac{1}{2}(n_1 + n_2 + m_1 + m_2)$ and $m_3 = \frac{1}{2}(n_1 + n_2 - m_1 - m_2)$. We write $\mu_j := n_j + i m_j,\ j = 1, 2, 3$ and consider

$$\nu_1 = \mu_1 \overline{\mu}_2 \mu_3 \quad \nu_2 = i\overline{\mu}_1 \overline{\mu}_2 \overline{\mu}_3, \quad \nu_3 = \overline{\mu}_1 \mu_2 \mu_3.$$

Notice that $|\mu_1| \sim m_1,\ |\mu_2| \sim m_1 \alpha$ and $|\mu_3| \sim m_1(1 + \alpha)/\sqrt{2}$, so that

$$R^{1/3} = |\nu_j|^{1/3} \sim ((\alpha + \alpha^2)/\sqrt{2})^{1/3} m_1.$$

Now $|\nu_3 - \nu_1| R^{-1/3} = |\mu_3||\mu_1 \overline{\mu}_2 - \overline{\mu}_1 \mu_2| R^{-1/3} = 2|\mu_3| R^{-1/3} \sim (1+\alpha)(\frac{4}{\alpha+\alpha^2})^{1/3} = C$, and similarly both $|\nu_3 - \nu_2| R^{-1/3} \sim (\frac{4}{\alpha+\alpha^2})^{1/3}$ and $|\nu_2 - \nu_1| R^{-1/3} \sim \alpha(\frac{4}{\alpha+\alpha^2})^{1/3}$. ∎

[1] The second author posed a weak version of Theorem 1.2 as problem A5 on the 2000 Putnam examination; about 45 contestants had the wherewithal to provide a solution somewhat like that above.

3 The Construction of the Families of 4-Tuples of Lattice Points

Given a given 4-tuple $[\nu]$ of lattice points in a short arc we will construct a family $\mathcal{F}$ of such 4-tuples, containing $[\nu]$, by giving an explicit expression for all elements of $\mathcal{F}$ in terms of powers of certain algebraic numbers (and they can also be described in terms of a certain second-order linear recurrence sequence). In each such family we will discover a canonical initial 4-tuple, and each such family will have an explicitly described "dual" family.

Before proceeding, we note that one can find many other 4-tuples from trivial operations applied to a given 4-tuple, so we wish to restrict our attention to a single element of such an "equivalence class". Indeed, if $\mathbf{g} = \gcd(\nu_1, \nu_2, \nu_3, \nu_4)$, then $\frac{\mathrm{Arc}[\nu]}{R} = \frac{\mathrm{Arc}[\nu/\mathbf{g}]}{R/|\mathbf{g}|}$, so that $\mathrm{Arc}[\nu] = |\mathbf{g}|\,\mathrm{Arc}[\nu/\mathbf{g}]$, and we can reduce our study to primitive 4-tuples of lattice points, where $[\nu]$ is *primitive* if $\gcd(\nu_1, \nu_2, \nu_3, \nu_4) = 1$. One can also obtain further (ordered) 4-tuples of lattice points by re-ordering the lattice points, and by the natural symmetries in the plane (taking conjugates, and by multiplying through by a fourth root of unity). We will take just one element of each such "equivalence class" of 4-tuples.

We therefore consider primitive 4-tuples of lattice points $[\nu] = (\nu_1, \nu_2, \nu_3, \nu_4)$ that all lie on the same circle centered at the origin, say $x^2 + y^2 = R^2$, and we assume that

$$\sigma := \nu_1 + \nu_2 + \nu_3 + \nu_4 \neq 0.$$

(Note that if $\sigma = 0$, then the ν_i cannot all lie on the same half circle, and hence $\mathrm{Arc}[\nu] \geq \pi R$; we shall have more to say about this case at the start of Section 6.) Next define

$$\omega_{[\nu]} = \left(\frac{\nu_1\nu_2\nu_3\nu_4}{|\nu_1\nu_2\nu_3\nu_4|}\right)^{\frac{1}{4}} = \frac{(\nu_1\nu_2\nu_3\nu_4)^{1/4}}{R} \text{ so that } -\pi/4 < \mathrm{Arg}(\sigma_{[\nu]}\overline{\omega_{[\nu]}}) \leq \pi/4.$$

Let $\Psi_{[\nu]} := \mathrm{Arg}(\sigma_{[\nu]}\overline{\omega_{[\nu]}})$, so that $-1 < \tan(\Psi_{[\nu]}) \leq 1$ and $\cos(\Psi_{[\nu]}) > 0$.

Let $Q = Q_{[\nu]}$ be the smallest positive integer for which $\sqrt{Q}\omega^2 \in \mathbb{Z}[i]$ (we will prove that Q exists in Section 5). If $Q_{[\nu]}$ is a square, then $[\nu]$ is *degenerate*, a simple case that we will examine in Section 6. Typically $Q_{[\nu]}$ is not a square, that is, $[\nu]$ is non-degenerate, in which case we select the smallest possible positive integers p and q for which[2]

$$p^2 - q^2 Q = \epsilon = \pm 1,$$

and we write $\alpha := p + q\sqrt{Q}$ and $\beta := p - q\sqrt{Q}$.

For a given $[\nu]$, we define the complex numbers[3]

$$\omega_1 = \frac{(\nu_1\overline{\nu}_2\overline{\nu}_3\nu_4)^{1/4}}{R}, \quad \omega_2 = \frac{(\overline{\nu}_1\nu_2\overline{\nu}_3\nu_4)^{1/4}}{R}, \quad \text{and} \quad \omega_3 = \frac{(\overline{\nu}_1\overline{\nu}_2\nu_3\nu_4)^{1/4}}{R}.$$

---

[2] But see Remark 3.1

[3] There is some ambiguity here, in that these quantities are well defined only up to a fourth root of unity. Our protocol is to make a choice for the value of each $\nu_j^{1/4}/R$ (out of the four possibilities) so as to validate the choice of fourth root of unity in the definition of $\omega = \omega_{[\nu]}$, and then to use this same value for $\nu_j^{1/4}/R$ consistently throughout these definitions.

For each integer n we define

$$\omega_{i,n} = \alpha^n \frac{\omega_i + \overline{\omega_i}}{2} + \beta^n \frac{\omega_i - \overline{\omega_i}}{2}, \quad i = 1, 2, 3. \tag{3.1}$$

and then a sequence of 4-tuples of lattice points $\{[\nu]_n = (\nu_{1,n}, \nu_{2,n}, \nu_{3,n}, \nu_{4,n}), n \in \mathbb{Z}\}$ by

$$\begin{aligned} \nu_{1,n} &= R\omega\omega_{1,n}\overline{\omega}_{2,n}\overline{\omega}_{3,n}, \\ \nu_{2,n} &= R\omega\overline{\omega}_{1,n}\omega_{2,n}\overline{\omega}_{3,n}, \\ \nu_{3,n} &= R\omega\overline{\omega}_{1,n}\overline{\omega}_{2,n}\omega_{3,n}, \\ \nu_{4,n} &= R\omega\omega_{1,n}\omega_{2,n}\omega_{3,n}. \end{aligned} \tag{3.2}$$

We immediately deduce that the lattice points $\nu_{j,n}$, $j = 1, 2, 3, 4$ all lie on the same circle, and that $\omega^4_{[\nu]_n} = \omega^4$. Multiplying out the terms in this definition we obtain

$$\begin{aligned} \nu_{j,n} = \alpha^{3n} \frac{\sigma + \omega^2\overline{\sigma}}{8} &+ (\epsilon\alpha)^n \Big(\frac{\nu_j - \omega^2\overline{\nu_j}}{2} - \frac{\sigma - \omega^2\overline{\sigma}}{8} \Big) \\ &+ \beta^{3n} \frac{\sigma - \omega^2\overline{\sigma}}{8} + (\epsilon\beta)^n \Big(\frac{\nu_j + \omega^2\overline{\nu_j}}{2} - \frac{\sigma + \omega^2\overline{\sigma}}{8} \Big), \end{aligned} \tag{3.3}$$

so that

$$\begin{aligned} \nu_{j,n}\overline{\omega} = \frac{\alpha^{3n}}{4} \operatorname{Re}(\sigma\overline{\omega}) &+ i(\epsilon\alpha)^n \Big(\operatorname{Im}(\nu_j\overline{\omega}) - \frac{\operatorname{Im}(\sigma\overline{\omega})}{4} \Big) \\ &+ i\frac{\beta^{3n}}{4} \operatorname{Im}(\sigma\overline{\omega}) + (\epsilon\beta)^n \Big(\operatorname{Re}(\nu_j\overline{\omega}) - \frac{\operatorname{Re}(\sigma\overline{\omega})}{4} \Big) \end{aligned} \tag{3.4}$$

for $j = 1, 2, 3, 4$. We deduce that $\nu_{j,n} = \omega R_n + O(R_n^{1/3})$ as $\alpha > 1 > |\beta|$, and that

$$\sigma_n := \sum_{j=1}^{4} \nu_{j,n} = \alpha^{3n} \frac{\sigma + \omega^2\overline{\sigma}}{2} + \beta^{3n} \frac{\sigma - \omega^2\overline{\sigma}}{2} = \omega\big(\alpha^{3n} \operatorname{Re}(\sigma\overline{\omega}) + i\beta^{3n} \operatorname{Im}(\sigma\overline{\omega}) \big).$$

Now

$$|\tan(\operatorname{Arg}(\sigma_n\overline{\omega}))| = \Big|\frac{\beta^{3n} \operatorname{Im}(\sigma\overline{\omega})}{\alpha^{3n} \operatorname{Re}(\sigma\overline{\omega})}\Big| = |\beta^{6n} \tan \Psi_{[\nu]}| < 1,$$

as $|\beta| < 1$ if $n \geq 0$, and also $\cos(\operatorname{Arg}(\sigma_n\overline{\omega})) > 0$, as $\alpha > 0$ and $\operatorname{Re}(\sigma\overline{\omega}) > 0$, which implies that $\omega_{[\nu]_n} = \omega$ (since we already know that $\omega^4_{[\nu]_n} = \omega^4$). In other words, ω is an invariant of the family, and so $Q = Q_{\mathcal{F}}$ is also.

With a formula like (3.3) it is evident that one can express the $\nu_{j,n}$ in terms of a recurrence. For $n \geq 0$ we have

$$\nu_{j,n+1} = pq\big(qQ\sigma_n + p\sqrt{Q}\omega^2\overline{\sigma_n} \big) + \epsilon\big(p\nu_{j,n} - q\sqrt{Q}\omega^2\overline{\nu_{j,n}} \big). \tag{3.5}$$

We deduce that each $\nu_{j,n}$ is in $\mathbb{Z}[i]$ by induction on $n \geq 0$, since $\sqrt{Q}\omega^2 \in \mathbb{Z}[i]$. This completes the proof that each $[\nu]_n$ with $n \geq 0$ gives rise to a 4-tuple of lattice points on a circle centered at the origin.

We can re-express (3.5) in the more friendly looking form

$$\nu_{j,n} = aG_{3n} + bG_{3n+1} + \epsilon^n \left(a_j G_n + b_j G_{n+1}\right) \quad \text{for all } n \geq 0, \tag{3.6}$$

with $b = \sigma/4$, $a = q\sqrt{Q}\omega^2\overline{b} - pb$, and $b_j = b - \nu_j$, $a_j = q\sqrt{Q}\omega^2\overline{b}_j + pb_j$ for each j, where the recurrence sequence $\{G_n : n \geq 0\}$ is defined by

$$G_0 = 0, \quad G_1 = 1, \quad \text{and} \quad G_n = 2pG_{n-1} - \epsilon G_{n-2} \quad \text{for all } n \geq 2. \tag{3.7}$$

Remark 3.1 This formula can be used to show that one can obtain Gaussian integers $\nu_{j,n}$ even when $p, q \in \mathbb{Z} + \frac{1}{2}$ (instead of in $\mathbb{Z}$); we take these semi-integer values for $p = p_{[\nu]}, q = q_{[\nu]}$ whenever possible. For example, if

$$[\nu] = (1 - 2i, 2 - i, 2 + i, -1 + 2i),$$

then $Q = 5$ and we can take $p = q = 1/2$ (as we now verify). The sequence G_n in (3.7) is the Fibonacci sequence F_n, and we have

$$\begin{aligned} a_1 &= -1 + i, & b_1 &= 2i, \\ a_2 &= 1 + i, & b_2 &= -1 + i, \\ a_3 &= 2, & b_3 &= -1 - i, \\ a_4 &= -2 - 2i, & b_4 &= 2 - 2i, \end{aligned}$$

so that (3.6) gives

$$\nu_{j,n} = \frac{1+i}{2} F_{3n} + F_{3n+1} + a_j F_n + b_j F_{n+1}.$$

Hence $\nu_{j,n}$ is always a Gaussian integer, since F_{3n} is always an even rational integer (and we obtain the example given in the introduction).

What about $n < 0$? The above proof is easily modified to work for all negative n *except* the requirement that $|\beta^{6n} \tan \Psi_{[\nu]}| < 1$. Thus we select n_0 to be the smallest integer for which $|\beta^{6n} \tan \Psi_{[\nu]}| < 1$, let $[\nu'] := [\nu]_{n_0}$ be this *initial 4-tuple*, and then define the family

$$\mathcal{F}([\nu]) = \{[\nu']_n = (\nu'_{1,n}, \nu'_{2,n}, \nu'_{3,n}, \nu'_{4,n}),\ n \geq 0\}, \tag{3.8}$$

where the $\nu'_{j,n}$ are defined as in (3.2). Note that $[\nu']$ is an invariant of the family $\mathcal{F}$, as is $Q_{\mathcal{F}} := Q_{[\nu]}$ and hence $\alpha, \beta, p, q, \ldots$ above.

Remark 3.2 There is an irritating ambiguity in the definition of $[\nu]_n$, in that it may stem from a chosen $[\nu]$, or from $[\nu']$ as above. These two possibilities differ only by the translation $n \to n - n_0$ of the parameter n, and we hope that which one is being used is clear from the context.

If $[\nu]_0$ is an initial 4-tuple, then $[\nu]_{-1}$ is an initial 4-tuple of a different family, the *dual family*, which we denote by $\hat{\mathcal{F}} := \mathcal{F}([\nu]_{-1}$.

3.1 The Main Constant $C_{\mathcal{F}}$

By (3.4) we see that $R_n \sim (\alpha^{3n}/4)\,\mathrm{Re}(\sigma\overline{\omega})$ and $|\nu_{j,n} - \nu_{k,n}| \sim \alpha^n |\,\mathrm{Im}((\nu_j - \nu_k)\overline{\omega}|$, as $\alpha > 1 > |\beta|$, from which we deduce that

$$\mathrm{Arc}[\nu]_n \sim R_n^{1/3} \max_{1\le j<k\le 4} \frac{|2\,\mathrm{Im}((\nu_j - \nu_k)\overline{\omega}|}{|2\,\mathrm{Re}(\sigma\overline{\omega})|^{1/3}}$$

as $n \to \infty$. The constant multiplying $R_n^{1/3}$ is evidently an invariant of the family $\mathcal{F}$ and does not depend on the choice of $[\nu] \in \mathcal{F}$. Hence we can define

$$C_{\mathcal{F}} := \lim_{n\to\infty} \frac{\mathrm{Arc}[\nu]_n}{R_n^{1/3}} = \max_{1\le j<k\le 4} \frac{|2\,\mathrm{Im}((\nu_j - \nu_k)\overline{\omega}|}{|2\,\mathrm{Re}(\sigma\overline{\omega})|^{1/3}}, \tag{3.9}$$

for any $[\nu] \in \mathcal{F}$. Similarly, it can be checked that

$$C_{\hat{\mathcal{F}}} = \lim_{n\to-\infty} \frac{\mathrm{Arc}[\nu]_n}{R_n^{1/3}} = \max_{1\le j<k\le 4} \frac{|2\,\mathrm{Re}((\nu_j - \nu_k)\overline{\omega}|}{|2\,\mathrm{Im}(\sigma\overline{\omega})|^{1/3}},$$

for any $[\nu] \in \mathcal{F}$ (indeed that $C_{\hat{\mathcal{F}}}([\nu]) = C_{\mathcal{F}}(i[\nu])$). An alternative and useful expression for $C_{\mathcal{F}}$, which can be deduced directly from (3.3), is

$$C_{\mathcal{F}} = \max_{1\le j<k\le 4} \frac{|\sqrt{Q}(\nu_j - \nu_k) - \sqrt{Q}\omega^2(\overline{\nu}_j - \overline{\nu}_k)|}{Q^{1/3}|\sqrt{Q}\sigma + \sqrt{Q}\omega^2\overline{\sigma}|^{1/3}}$$

and similarly

$$C_{\hat{\mathcal{F}}} = \max_{1\le j<k\le 4} \frac{|\sqrt{Q}(\nu_j - \nu_k) + \sqrt{Q}\omega^2(\overline{\nu}_j - \overline{\nu}_k)|}{Q^{1/3}|\sqrt{Q}\sigma - \sqrt{Q}\omega^2\overline{\sigma}|^{1/3}}.$$

We will prove Theorem 1.4 by using the construction in this section. The idea is that *every* 4-tuple of lattice points leads to a family of 4-tuples of lattice points as described above. A few of the 4-tuples are degenerate and are easily classified and determined (as in Section 6 and then Algorithm 2, step 2). If we want to find all families $\mathcal{F}$ which contain 4-tuples $[\nu]$ with $\mathrm{Arc}[\nu] < tR^{1/3}$, then, as one might expect from (3.9)), one only needs to consider families $\mathcal{F}$ with $C_{\mathcal{F}}$ no bigger than a few percent larger than t. In fact if $C_{\mathcal{F}} \le t$, then $\mathrm{Arc}[\nu] < tR^{1/3}$ for every $[\nu]$ in those families except perhaps when $R_{[\nu]}$ is smaller than an explicitly given bound; and if $C_{\mathcal{F}} > t$, then one can only possibly have $\mathrm{Arc}[\nu] < tR^{1/3}$ for $[\nu]$ in those families if $R_{[\nu]}$ is smaller than an explicitly given bound (see Theorem 7.3). Finally one can compute each of the finitely many $[\nu]$ with $R_{[\nu]}$ smaller than that bound to determine whether they satisfy $\mathrm{Arc}[\nu] < tR^{1/3}$.

4 Summary of Notation

- $\nu, \nu_1, \ldots$ denote lattice points or gaussian integers, depending on the context.
- $[\nu] = (\nu_1, \ldots, \nu_k)$ denotes a k-tuple of lattice points (gaussian integers), all on the circle of radius $R_{[\nu]}$ centered at the origin. Typically $k = 4$.
- $\sigma = \sigma_{[\nu]} = \nu_1 + \nu_2 + \nu_3 + \nu_4$.
- We say that $[\nu]$ is *primitive* if $\gcd(\nu_1, \ldots, \nu_k) = 1$.
- $\mathrm{Arc}[\nu]$ denotes the length of the shortest arc containing $\nu_1, \ldots, \nu_k$.
- $\mathcal{F}$ denotes a family $\mathcal{F} = \{[\nu]_n = (\nu_{1,n}, \nu_{2,n}, \nu_{3,n}, \nu_{4,n}),\ n \geq 0\}$, as described in (3.8). The 4-tuple $[\nu]_0$ is the *initial 4-tuple* of the family.
- $\mathcal{F}([\nu])$ is the family $\mathcal{F}$ that contains $[\nu]$.
- $\hat{\mathcal{F}}$ is the dual family of $\mathcal{F}$.
- $R_n = R_{[\nu]_n}$ when the family is given, but see Remark 3.2.
- $\sigma_n = \sigma_{[\nu]_n}$ when the family is given, but see Remark 3.2.
- $C_{\mathcal{F}}$ is the constant $\lim_{n\to\infty} \mathrm{Arc}[\nu]_n R_n^{-1/3}$.
- $\omega_{[\nu]} = (\nu_1\nu_2\nu_3\nu_4)^{1/4} R_{[\nu]}^{-1}$ such that $-\pi/4 < \mathrm{Arg}(\sigma_{[\nu]}\overline{\omega_{[\nu]}}) \leq \pi/4$, which is an invariant of the family, so can be written as $\omega_{\mathcal{F}}$.
- $\Psi_{[\nu]} := \mathrm{Arg}(\sigma_{[\nu]}\overline{\omega_{[\nu]}})$.
- $Q_{[\nu]}$ is the smallest positive integer for which $\sqrt{Q_{[\nu]}}\omega_{[\nu]}^2 \in \mathbb{Z}[i]$, which is an invariant of the family, so can be written as $Q_{\mathcal{F}}$.
- $p = p_{[\nu]} = p_{\mathcal{F}}, q = q_{[\nu]} = q_{\mathcal{F}}$ are the smallest positive integers such that $p^2 - q^2 Q = \epsilon = \pm 1$.
- $\alpha = \alpha_{[\nu]} = \alpha_{\mathcal{F}} = p + q\sqrt{Q}$ and $\beta = \beta_{[\nu]} = \beta_{\mathcal{F}} = p - q\sqrt{Q}$.

5 Properties of Q

In this section we suppose that $[\nu]$ is given and will determine properties of $Q = Q_{[\nu]} = Q_{\mathcal{F}}, R = R_{[\nu]}, C = C_{[\nu]} = C_{\mathcal{F}}$.

Lemma 5.1 *There exists a positive integer Q, not divisible by* 4*, for which*

$$\sqrt{Q}\omega^2 \in \mathbb{Z}[i].$$

In fact, if an odd prime p divides Q, then $p \equiv 1 \pmod 4$. *Moreover* $Q/(2, Q)$ *divides* R^2.

Proof Let γ_i be the exact power of a prime ideal $\mathbf{p}$ of norm p which divides ν_i, $i = 1, 2, 3, 4$, say with $\gamma_1 \geq \gamma_2 \geq \gamma_3 \geq \gamma_4$. Since $[\nu]$ is primitive, we know that $p \neq 2$, $\gamma_4 = 0$, and p^{γ_1} is the exact power of p dividing R^2, so that $\gamma_1 - \gamma_i$ is the exact power of that prime ideal $\overline{\mathbf{p}}$ that divides ν_i. Therefore if $\gamma = \gamma_1 - \gamma_2 - \gamma_3 - \gamma_4$, then the exact powers of $\mathbf{p}$ and $\overline{\mathbf{p}}$ dividing ω^4 are given by $(\overline{\mathbf{p}}/\mathbf{p})^{\gamma}$, which equals $(\overline{\mathbf{p}}^2/p)^{\gamma}$ if $\gamma > 0$, and equals $(\mathbf{p}^2/p)^{-\gamma}$ if $\gamma < 0$. We see that if Q_1 is the product of these $p^{|\gamma|}$, then $Q_1\omega^4 \in u\mathbb{Z}[i]^2$ for some unit u, since all ideals of $\mathbb{Z}[i]$ are principal. Taking square roots, we see that we can take $Q = Q_1$ if $u = \pm 1$, and $Q = 2Q_1$ if $u = \pm i$, so that Q is not divisible by 4, and all of its prime factors are norms of elements of $\mathbb{Z}[i]$ and are thus not $\equiv 3 \pmod 4$.

Finally note that $|\gamma| = |\gamma_1 - \gamma_2 - \gamma_3| \leq \gamma_1$, so that $Q_1 = Q/(2, Q)$ divides R^2. ∎

Lemma 5.2 *Let* $\mathbf{p}$ *be a prime ideal in* $\mathbb{Z}[i]$, $|\mathbf{p}|^2 \neq 2$. *If* $[\nu] = (\nu_1, \nu_2, \nu_3, \nu_4)$ *is primitive and* $\mathbf{p}^\alpha$ *divides* $\sqrt{Q}\omega^2$, *then* $\mathbf{p}^\alpha$ *divides exactly three of* $\{\nu_1, \nu_2, \nu_3, \nu_4\}$.

Proof In the notation of the proof of the previous lemma one finds that the exact power of $\mathbf{p}$ which divides $\sqrt{Q}\omega^2$ is $\mathbf{p}^{\max\{0,-\gamma\}}$, and

$$\max\{0, -\gamma\} = \max\{0, \gamma_3 - (\gamma_1 - \gamma_2)\} \leq \gamma_3,$$

so the result follows. ■

Lemma 5.3 *If* $[\nu]$ *is a primitive* 4*-tuple we have* $\mathrm{Arc}[\nu] > (16\, r(Q))^{1/3} R^{1/3}$ *where*

$$r(Q) := \min_{\substack{r_1 r_2 r_3 r_4 = Q/(2,Q) \\ (r_i, r_j)=1,\ i \neq j}} \max_{1 \leq i \leq 4} r_i. \tag{5.1}$$

Proof Let $\mathbf{g}_i = \gcd(\nu_j : j \neq i)$ for $i = 1, 2, 3, 4$. If $p \neq \pm 1 \pm i$, then by the previous lemma we know that any prime ideal power $\mathbf{p}^\alpha$ dividing $\sqrt{Q}\omega^2$ divides one of the $\mathbf{g}_i$. Therefore $\sqrt{Q}\omega^2$ divides $(1+i)\mathbf{g}_1\mathbf{g}_2\mathbf{g}_3\mathbf{g}_4$, so that $Q/(2, Q)$ divides $|\mathbf{g}_1|^2|\mathbf{g}_2|^2|\mathbf{g}_3|^2|\mathbf{g}_4|^2$. Therefore, as $[\nu]$ is primitive, so that $(|\mathbf{g}_i|^2, |\mathbf{g}_j|^2) = 1$, $i \neq j$, there exists some j for which $|\mathbf{g}_j|^2 \geq r(Q)$. Suppose that $j = 4$ here and let $\mathbf{g} = \mathbf{g}_4$. Let $\nu_i = \mathbf{g}\tau_i$ for $i = 1, 2, 3$. Then

$$\begin{aligned} \mathrm{Arc}[\nu] &\geq \mathrm{Arc}[\nu_1, \nu_2, \nu_3] = \mathrm{Arc}(\mathbf{g}[\tau]) = |\mathbf{g}|\, \mathrm{Arc}([\tau]) \geq |\mathbf{g}|(16 R_{[\tau]})^{1/3} \\ &= |\mathbf{g}|^{2/3}(16 R_{[\nu]})^{1/3} \end{aligned}$$

by Theorem 1.2, as $R_{[\nu]} = |\mathbf{g}| R_{[\tau]}$. The result follows. ■

We deduce the following result from Lemma 5.3 and (3.9).

Corollary 5.4 *If* $\mathcal{F}$ *is a non-degenerate family, then* $C_{\mathcal{F}} \geq (16 r(Q_{\mathcal{F}}))^{1/3}$.

6 Degenerate 4-Tuples

In this section we shall assume that we are given a degenerate $[\nu]$, that is, a $[\nu]$ for which $Q_{[\nu]}$ is a square. One can verify that, in this case, $\alpha = \beta = 1$, so that $\nu_{j,n} = \nu_j$ for all n and j, and thus the (purportedly infinite) sequence of 4-tuples of lattice points degenerates into a single example.

In Section 2 we noted that if $\sigma = 0$, then the ν_i cannot all lie on the same half circle, implying that $\mathrm{Arc}[\nu] \geq \pi R$; now we will show that if $[\nu]$ is also primitive, then it is degenerate. Since $\nu_1 + \nu_2 = (-\nu_3) + (-\nu_4)$ where $|\nu_1| = |\nu_2| = |-\nu_3| = |-\nu_4|$, we either have $\nu_1 + \nu_2 = 0$ (in which case $\nu_3 + \nu_4 = 0$), or that the non-zero sum of two vectors, ν_1 and ν_2, of the same length equals the sum of two other vectors, $-\nu_3$ and $-\nu_4$, of the same length, and it is then easy to show that those two sets of two vectors must be identical. Thus, by re-ordering the indices if necessary, we have $\nu_1 + \nu_2 = \nu_3 + \nu_4 = 0$. But $(\nu_1, \nu_3) = 1$ since $[\nu]$ is primitive and hence $\nu_3 = u\overline{\nu}_1$ where $u = 1, -1, i$ or $-i$. Therefore $\nu_1\nu_2\nu_3\nu_4 = (\nu_1\nu_3)^2 = u^2 R^4$ so that $\omega_{[\nu]}^2 = \pm u$ and therefore $Q_{[\nu]} = 1$.

Lemma 6.1 *If $Q_{[\nu]}$ is a square, then* $\mathrm{Arc}[\nu] > 2R^{1/2}/Q_{[\nu]}^{1/8}$.

Proof The argument of Lemma 5.1 implies that if Q is a square, then Q is odd, each γ must be even, and $u = \pm 1$. Therefore there exists $\ell \in \mathbb{Z}[i]$ for which $Q\omega^4 = \pm\ell^4$, so that $|\ell| = Q^{1/4}$. We deduce that $(\bar{\ell}\nu_1)(\bar{\ell}\nu_2)(\bar{\ell}\nu_3)(\bar{\ell}\nu_4) = \bar{\ell}^4 R^4\omega^4 = \pm|\ell|^8 R^4/Q = \pm QR^4$. Let $[\nu'] = \ell'[\nu]$ where $\ell' = \bar{\ell}$ if $\pm$ is $+$ and $\ell' = (1+i)\bar{\ell}$ if $\pm$ is $-$. Writing $\omega' = \omega_{[\nu']}$, $Q' = Q_{[\nu']}$, and $R' = R_{[\nu']}$, we have $(\omega')^4 = 1$, so that $Q' = 1$.

If $R' < \sqrt{5}$, then there are exactly four lattice points on our circle, so that $\sigma_{[\nu']} = 0$. Hence $\sigma_{[\nu]} = \sigma_{[\nu']}/\ell' = 0$ and therefore $\mathrm{Arc}[\nu] \geq \pi R$, as noted at the beginning of the Section 3.

We now prove that if $R' \geq \sqrt{5}$, then $\mathrm{Arc}[\nu'] \geq 2^{5/4}(R')^{1/2}$. We may assume that $\mathrm{Arc}[\nu'] < \frac{\pi}{2}R'$, else this is immediate. Using the obvious symmetries (that is, multiplying $[\nu']$ through by a unit or replacing it with $[\overline{\nu'}]$), we may assume that $-\pi/2 < \varphi_1 < \varphi_2 < \varphi_3 < \varphi_4 < \pi/2$, where $\nu_j' = R'e^{i\varphi_j} = x_j + iy_j,\ j = 1,2,3,4$, and we already know that $\varphi_1 + \varphi_2 + \varphi_3 + \varphi_4 = 0$. Thus $\varphi_1 < 0 < \varphi_4$, and suppose that $|\varphi_1| \geq \varphi_4$. This implies that $\varphi_3 > 0$, so that $y_3 > 0$ and $x_3 > x_4$, and thus

$$\begin{aligned}\mathrm{Arc}[\nu'] > 2y_4 = 2\sqrt{R'^2 - x_4^2} &\geq 2\sqrt{R'^2 - (x_3 - 1)^2} \\ &\geq 2\sqrt{R'^2 - (R'-1)^2} = 2\sqrt{2R'-1} > 2^{5/4}(R')^{1/2},\end{aligned}$$

as $R' \geq \sqrt{5}$. Therefore, from the remarks at the beginning of Section 3 we have

$$\mathrm{Arc}[\nu] = \frac{\mathrm{Arc}[\nu']}{|\ell'|} > \frac{2^{5/4}(R')^{1/2}}{|\ell'|} = \frac{2^{5/4}R^{1/2}}{|\ell'|^{1/2}} \geq \frac{2^{5/4}R^{1/2}}{(\sqrt{2}|\ell|)^{1/2}} \geq \frac{2R^{1/2}}{Q^{1/8}}. \qquad \blacksquare$$

Corollary 6.2 *If* $\mathrm{Arc}[\nu] < tR^{1/3}$ *and* $[\nu]$ *is primitive and degenerate, then* $R \leq t^{15}2^{-17}$.

Proof If $Q_{[\nu]}$ is a square, then $\mathrm{Arc}[\nu] > \max\{2R^{1/2}/Q^{1/8}, (16r(Q)R)^{1/3}\}$ by Lemmas 5.3 and 6.1. From (5.1) we see that $r(Q) \geq (Q/2)^{1/4}$. Therefore $\mathrm{Arc}[\nu] > 2^{23/20}R^{2/5}$, so $R < t^{15}2^{-69/4} < t^{15}2^{-17}$ and the result follows. $\blacksquare$

7 The Constant $C_{\mathcal{F}}$ Associated with a Family $\mathcal{F}$

We begin this section by noting, without proof, two technical trigonometric lemmas that will be useful below.

Lemma 7.1 *If* $-\pi/2 \leq x_1 < \cdots < x_n \leq \pi/2$, *then*

$$\max_{1\leq i<j\leq n} |\sin(x_i) - \sin(x_j)| = |\sin(x_1) - \sin(x_n)|.$$

Lemma 7.2 *If* $|x| \leq \pi/4$, *then*

(i) $|\sin x| < 1.0106|x| \cdot |\cos x|^{1/3}$,
(ii) $|\sin x| < |x| \cdot |\frac{\cos x + \cos y}{2}|^{1/3}$ *whenever* $|y| \leq |x| - 0.137|x|^3$,

(iii) $|\sin x||\cos x|^{1/3} \geq \max(2|x|/\pi, |x| - |x|^3/3)$.

The following is the main result in this section.

Theorem 7.3 *If* $\text{Arc}[\nu] < \frac{\pi}{2} R_{[\nu]}$ *where* $[\nu]$ *is primitive and non-degenerate, then*

(i) $\text{Arc}[\nu] > 0.9895 C_{\mathcal{F}} R_{[\nu]}^{1/3}$,

(ii) $\text{Arc}[\nu] > C_{\mathcal{F}} R_{[\nu]}^{1/3}$ *for* $R_{[\nu]} > 0.08 C_{\mathcal{F}}^{15/4}$,

(iii) $\text{Arc}[\nu] \leq C_{\mathcal{F}} R_{[\nu]}^{1/3} \left(1 + \frac{\pi^3}{96} \frac{C_{\mathcal{F}}^2}{R_{[\nu]}^{2/3}}\right)$.

Proof Write $\nu_j \overline{\omega} = Re^{i\varphi_j}$, $j = 1, 2, 3, 4$, with $\varphi_1 < \varphi_2 < \varphi_3 < \varphi_4 \leq \varphi_1 + \pi/2$, so that $\text{Arc}[\nu] = (\varphi_4 - \varphi_1)R$, and note that $\varphi_1 + \varphi_2 + \varphi_3 + \varphi_4 = 0$ by the definition of ω. Therefore,

$$C_{\mathcal{F}([\nu])} = \frac{2R^{2/3}|\operatorname{Im}((\nu_1 - \nu_4)\overline{\omega}|}{(2\operatorname{Re}(\sigma\overline{\omega}))^{1/3}} = \frac{2R^{2/3}|\sin(\varphi_1) - \sin(\varphi_4)|}{|2(\cos(\varphi_1) + \cos(\varphi_2) + \cos(\varphi_3) + \cos(\varphi_4))|^{1/3}}.$$

Now $\sin(\varphi_1) - \sin(\varphi_4) = 2\sin(\frac{\varphi_1 - \varphi_4}{2})\cos(\frac{\varphi_1 + \varphi_4}{2})$, and

$$\begin{aligned}&\cos(\varphi_1) + \cos(\varphi_2) + \cos(\varphi_3) + \cos(\varphi_4)\\&\qquad = 2\left(\cos\left(\frac{\varphi_1 - \varphi_4}{2}\right) + \cos\left(\frac{\varphi_2 - \varphi_3}{2}\right)\right)\cos\left(\frac{\varphi_1 + \varphi_4}{2}\right),\end{aligned}$$

since $\frac{\varphi_2 + \varphi_3}{2} = -\frac{\varphi_1 + \varphi_4}{2}$, and therefore

$$C_{\mathcal{F}} = \frac{2R^{2/3}|\sin(\frac{\varphi_1 - \varphi_4}{2})||\cos(\frac{\varphi_1 + \varphi_4}{2})|^{2/3}}{|\frac{1}{2}(\cos(\frac{\varphi_1 - \varphi_4}{2}) + \cos(\frac{\varphi_2 - \varphi_3}{2}))|^{1/3}} \leq \frac{2R^{2/3}|\sin(\frac{\varphi_1 - \varphi_4}{2})|}{|\cos(\frac{\varphi_1 - \varphi_4}{2})|^{1/3}}, \tag{7.1}$$

since $0 \leq \cos(\frac{\varphi_4 - \varphi_1}{2}) \leq \cos(\frac{\varphi_3 - \varphi_2}{2})$, as $0 \leq \varphi_3 - \varphi_2 \leq \varphi_4 - \varphi_1 \leq \pi/2$. By Lemma 7.2 we deduce that $C_{\mathcal{F}} < 1.0106(\varphi_4 - \varphi_1)R^{2/3} = 1.0106 R^{-1/3}\,\text{Arc}[\nu]$, and part (i) follows.

If $(\varphi_4 - \varphi_1) - (\varphi_3 - \varphi_2) \geq 0.137(\varphi_4 - \varphi_1)^3$, then

$$C_{\mathcal{F}} < (\varphi_4 - \varphi_1)R^{2/3} = R^{-1/3}\,\text{Arc}[\nu]$$

by Lemma 7.2(ii), and the result follows. Otherwise $(\varphi_4 - \varphi_3) + (\varphi_2 - \varphi_1) < 0.137(\varphi_4 - \varphi_1)^3$, and suppose, for example, that $\varphi_2 - \varphi_1 < \frac{0.137}{2}(\varphi_4 - \varphi_1)^3$. Applying the argument in the proof of Theorem 1.2 to the triangle formed by ν_1, ν_2, ν_4, we obtain

$$\begin{aligned}2R \leq 4\Delta R &= |\nu_1 - \nu_2||\nu_1 - \nu_4||\nu_2 - \nu_4|\\&\leq \text{Arc}(\nu_1, \nu_2)\text{Arc}(\nu_1, \nu_4)\text{Arc}(\nu_2, \nu_4)\\&= (\varphi_2 - \varphi_1)(\varphi_4 - \varphi_1)(\varphi_4 - \varphi_2)R^3\\&< 0.0685(\varphi_4 - \varphi_1)^5 R^3 = 0.0685 R^{-2}\,\text{Arc}^5[\nu],\end{aligned}$$

so that $\mathrm{Arc}[\nu] > 1.963667195R^{3/5} > C_{\mathcal{F}}R^{1/3}$ for $R > 0.08C_{[\nu]}^{15/4}$, and part (ii) follows.

Let us suppose that $\varphi_4 - \varphi_1 = 4\lambda$ so that $\pi/2 \geq 4\lambda \geq 0$. Therefore,

$$0 = \varphi_1 + \varphi_2 + \varphi_3 + \varphi_4 = 4\varphi_1 + m\lambda$$

for some $m, 4 \leq m \leq 12$, so that $\varphi_1 + \varphi_4 = 2\varphi_1 + 4\lambda = (4 - m/2)\lambda$ and therefore $|(\varphi_1 + \varphi_4)/2| \leq \lambda$. We therefore deduce that

$$\begin{aligned} \left|\cos\left(\frac{\varphi_1 + \varphi_4}{2}\right)\right| &\geq |\cos\lambda| \geq \cos^2\lambda = (1 + \cos 2\lambda)/2 \\ &\geq \left|\frac{1}{2}\left(\cos\left(\frac{\varphi_1 - \varphi_4}{2}\right) + \cos\left(\frac{\varphi_2 - \varphi_3}{2}\right)\right)\right|. \end{aligned}$$

Therefore (7.1) implies that

$$C_{\mathcal{F}} \geq 2R^{2/3}\left|\sin\left(\frac{\varphi_1 - \varphi_4}{2}\right)\right| \left|\cos\left(\frac{\varphi_1 - \varphi_4}{2}\right)\right|^{1/3}.$$

Applying Lemma 7.2(iii) yields $C_{\mathcal{F}} \geq R^{2/3}\frac{2}{\pi}|\varphi_1 - \varphi_4| = R^{-1/3}\frac{2}{\pi}\,\mathrm{Arc}[\nu]$, so that

$$\mathrm{Arc}[\nu] < (\pi/2)C_{\mathcal{F}}R^{1/3},$$

and also that

$$C_{\mathcal{F}} \geq 2R^{2/3}\left(\frac{\varphi_1 - \varphi_4}{2} - \frac{(\varphi_1 - \varphi_4)^3}{24}\right) = \frac{\mathrm{Arc}[\nu]}{R^{1/3}} - \frac{\mathrm{Arc}^3[\nu]}{12R^{7/3}} \geq \frac{\mathrm{Arc}[\nu]}{R^{1/3}} - \frac{\pi^3}{96}\frac{C_{\mathcal{F}}^3}{R^{4/3}},$$

which implies part (iii). ∎

Lemma 7.4 *Given $[\nu] \in \mathcal{F}$, there exists $[\nu]_n$ (as defined in (3.2)) such that $R^2_{[\nu]_n} \leq C^3_{\mathcal{F}}p^3$. In other words, for any family $\mathcal{F}$, there exists $[\nu] \in \mathcal{F} \cup \hat{\mathcal{F}}$ such that $R^2_{[\nu]_n} \leq C^3_{\mathcal{F}}p^3$.*

Proof Fix $\delta > 0$, and select m such that $\mathrm{Arc}([\nu]_m) \leq (1+\delta)C_{\mathcal{F}}R^{1/3}$, which is possible by (3.9). For convenience we replace $[\nu]$ by $[\nu]_m$. By (3.1) we have, using the arithmetic-geometric mean inequality,

$$\begin{aligned} R^2_{[\nu]_n}/R^2_{[\nu]} &= \prod_{i=1}^{3}\left(\alpha^{2n}\left|\frac{\omega_i + \overline{\omega_i}}{2}\right|^2 + \beta^{2n}\left|\frac{\omega_i - \overline{\omega_i}}{2}\right|^2\right) \\ &\leq \left(\frac{\alpha^{2n}\sum_{i=1}^{3}\left|\frac{\omega_i+\overline{\omega_i}}{2}\right|^2 + \beta^{2n}\sum_{i=1}^{3}\left|\frac{\omega_i-\overline{\omega_i}}{2}\right|^2}{3}\right)^3 \\ &\leq \left(\alpha^{2n} + \beta^{2n}(1+\delta)^2\frac{C_{\mathcal{F}}^2}{8R^{4/3}}\right)^3. \end{aligned}$$

To obtain this last inequality we first note that each $|\frac{\omega_i+\overline{\omega_i}}{2}| \le 1$ and that, if we write each $\nu_j = Re^{i\varphi_j}$ where $\varphi_1 \le \varphi_2 \le \varphi_3 \le \varphi_4 < \varphi_1 + \pi/2$, then

$$\begin{aligned} 2|\omega_1 - \overline{\omega_1}| &= 4\left|\sin\left(\frac{\varphi_1 - \varphi_2 - \varphi_3 + \varphi_4}{4}\right)\right| \\ &\le |\varphi_1 - \varphi_2 - \varphi_3 + \varphi_4| = |(\varphi_4 - \varphi_1) - (\varphi_3 - \varphi_1) - (\varphi_2 - \varphi_1)| \\ &\le |\varphi_4 - \varphi_1|, \end{aligned}$$

and similarly, $2\,|\omega_2 - \overline{\omega_2}| \le |\varphi_4 - \varphi_1|$ and $|\omega_3 - \overline{\omega_3}| \le |\varphi_4 - \varphi_1|$, so that

$$\frac{1}{3}\sum_{i=1}^{3}\left|\frac{\omega_i - \overline{\omega_i}}{2}\right|^2 \le \frac{(\varphi_4 - \varphi_1)^2}{8} = \frac{\text{Arc}[\nu]^2}{8R^2} \le (1+\delta)^2\frac{C_{\mathcal{F}}^2}{8R^{4/3}}.$$

Now let n be the integer closest to $\frac{\log((1+\delta)^2 C_{\mathcal{F}}^2/(8R^{4/3}))}{4\log\alpha}$; in fact, suppose that this equals $n - \gamma$ with $|\gamma| \le 1/2$. Then

$$R_{[\nu]_n}^2 \le R^2\left((1+\delta)\frac{C_{\mathcal{F}}}{8^{1/2}R^{2/3}}(\alpha^{2\gamma} + |\beta|^{2\gamma})\right)^3 \le \frac{(1+\delta)^3 C_{\mathcal{F}}^3(\alpha + |\beta|)^3}{8^{3/2}}.$$

Now $\alpha + |\beta| = 2p$ if $\epsilon = 1$, and $\alpha + |\beta| = 2q\sqrt{Q}$ if $\epsilon = -1$. In the latter case we have $q\sqrt{Q} = p + 1/(p + q\sqrt{Q}) \le 2^{1/2}p$ (which is attained when $Q = 2$). We obtain our result by an appropriate choice of δ, since $R_{[\nu]_n}^2$ is an integer. Finally note that $[\nu]_n \in \mathcal{F} \cup \hat{\mathcal{F}}$. ■

8 Our Algorithms

Algorithm 1 This algorithm calculates, for a given $t > 0$, all the families $\mathcal{F} \in \mathcal{F}(t) = \{\mathcal{F},\, C_{\mathcal{F}} \le t\}$.

Step 1: Finding admissible Q**.** We determine all the non-square values of $Q \not\equiv 0 \pmod 4$, whose prime factors are 2 or are $\equiv 1 \pmod 4$, which can be written as the product of four co-prime integers all of which are $\le t^3/16$ (by Corollary 5.4).

Step 2: Finding possible families. For each Q in Step 1 we consider all the non-degenerate 4-tuples $[\nu]$ such that $Q_{[\nu]} = Q$ and $R_{[\nu]}^2 \le t^3 p^3$, where $p = p(Q)$ is defined in Section 3. (Recall that if $C_{\mathcal{F}} \le t$, then $\mathcal{F}$ or $\hat{\mathcal{F}}$ contains at least one of such 4-tuple, by Lemma 7.4.)

Step 3: Computing the constants $C_{\mathcal{F}}$**.** Use (3.9) to compute the constants $C_{\mathcal{F}}$ and $C_{\hat{\mathcal{F}}}$ for the families $\mathcal{F} = \mathcal{F}([\nu])$ obtained in Step 2. Finally we save those with $C_{\mathcal{F}} \le t$.

As an example we apply Algorithm 1 to calculate $\mathcal{F}(5) = \{\mathcal{F}, C_{\mathcal{F}} \le 5\}$. In Step 1 we see that $5^3/16 < 8$ and so the possible values of the four (pairwise co-prime) factors of Q are $1, 2$, and 5, so that $Q = 2, 5$, or 10.

In Step 2, noting that $p(2) = 1$, $p(5) = 2$, and $p(10) = 3$, we consider those $[\nu]$ for which $Q_{[\nu]} = 2, 5$, or 10, with $R_{[\nu]}^2 \le (5)^3, (10)^3$, or $(15)^3$, respectively. Then in

Step 3 we found seven families (which we describe in Table 1), with constants

$$C_{\mathcal{F}_1} = 2\Big(\frac{5}{3}(3+\sqrt{10})\Big)^{\frac{1}{3}} < C_{\mathcal{F}_2} = \Big(20\Big)^{\frac{1}{3}}\Big(\frac{1+\sqrt{5}}{2}\Big) < C_{\mathcal{F}_3} = 4\Big(\frac{1}{7}(5+4\sqrt{2})\Big)^{\frac{1}{3}}$$
$$< C_{\mathcal{F}_4} = \Big(\frac{10}{3}(14+5\sqrt{10})\Big)^{\frac{1}{3}} < C_{\mathcal{F}_5} = 3\sqrt{2}\Big(\frac{2}{7}(5+3\sqrt{2})\Big)^{\frac{1}{3}}$$
$$< C_{\mathcal{F}_6} = 10^{\frac{1}{3}}\Big(\frac{1+\sqrt{5}}{2}\Big)^{\frac{5}{3}} < C_{\mathcal{F}_7} = 2(1+\sqrt{2}) < 5.$$

One can show that $\mathcal{F}_8 := \hat{\mathcal{F}}_6 = \mathcal{F}(2+i, -1-2i, -2-i, -1+2i)$ where $C_{\hat{\mathcal{F}}_6} = 5.490599585\cdots$ is the family $\mathcal{F}$ that gives the next smallest constant $C_{\mathcal{F}}$.

Theorem 8.1 *If* $\mathrm{Arc}[\nu] < tR^{1/3}$, *where* $[\nu]$ *is primitive and non-degenerate, then either* $\mathrm{Arc}[\nu] \geq \frac{\pi}{2}R$ *with* $R \leq (2t/\pi)^{3/2}$, *or* $[\nu] \in \mathcal{F}$ *for some* $\mathcal{F} \in \mathcal{F}(t)$, *or* $[\nu] \in \mathcal{F}$ *for some* $\mathcal{F} \in \mathcal{F}(1.01062t)$ *with* $R \leq 0.084t^{15/4}$.

Proof If $\mathrm{Arc}[\nu] \geq \frac{\pi}{2}R$, then $\frac{\pi}{2}R < tR^{1/3}$ and the first option follows. If $C_{\mathcal{F}} \leq t$, then the second option follows. Finally suppose that $\mathrm{Arc}[\nu] < \frac{\pi}{2}R$ and $C_{\mathcal{F}} > t$. Then $tR^{1/3} > \mathrm{Arc}[\nu] > 0.9895C_{[\nu]}R^{1/3}$ by Theorem 7.3(i), so that $C_{\mathcal{F}} \leq 1.01062t$, that is, $\mathcal{F}_{[\nu]} \in \mathcal{F}(1.01062t)$. But then $R \leq 0.084t^{15/4}$, else

$$R > 0.084t^{15/4} > (0.08)(1.01062t)^{15/4} \geq 0.08C_{\mathcal{F}}^{15/4}$$

implying that $\mathrm{Arc}[\nu] > C_{\mathcal{F}}R^{1/3} \geq tR^{1/3}$ by Theorem 7.3(ii). ■

Proof of Theorem 1.4 We have that $\max\{2^{-17}t^{15}, 0.084t^{15/4}, (2t/\pi)^{3/2}\}$ is equal to $2^{-17}t^{15}$ for $t \geq 2.2871\ldots$, and is less than 1.87 for smaller t. The result then follows from Theorem 8.1 and Corollary 6.2.

For any given t, there are only a finite number of possible values of Q, and so only a finite number of possible values of p, and hence by Lemma 7.4 every family in $\mathcal{F}(t)$ contains a 4-tuple ν such that $R_{[\nu]}$ is bounded by a quantity which depends only on t. Therefore there are only finitely many such ν, and so there are only finitely many families in $\mathcal{F}(t)$. ■

Algorithm 2 This algorithm determines, for a given $t > 0$, all primitive 4-tuples $[\nu]$ of lattice points for which $\mathrm{Arc}[\nu] \leq tR_{[\nu]}^{1/3}$.

Step 1: Small 4-tuples. We examine each $[\nu]$ satisfying $R_{[\nu]} \leq (2t/\pi)^{3/2}$, to test whether $\mathrm{Arc}[\nu] \leq tR_{[\nu]}^{1/3}$ (as demanded by Theorem 8.1).

Step 2: Finding admissible Q. We determine all positive integers $Q \not\equiv 0 \pmod 4$, whose prime factors are 2 or are $\equiv 1 \pmod 4$, which can be written as the product of four co-prime integers, all of which are $\leq t^3/16$ (by Lemma 5.3).

Step 3: Degenerate 4-tuples. By Lemma 6.1 we examine, for each such Q that is a square, all $[\nu]$ with $Q_{[\nu]} = Q$ and $R_{[\nu]} \leq (t/2)^6 Q^{3/4}$.

Step 4: Families with $t \leq C_{\mathcal{F}} < 1.01062t$. We examine all $[\nu] \in \mathcal{F}$ such that $R_{[\nu]} \leq 0.084t^{15/4}$, to test whether $\mathrm{Arc}[\nu] \leq tR_{[\nu]}^{1/3}$ (by the last part of Theorem 8.1).

	$\hat{\mathcal{F}}$	$[\nu]_0$	$[\nu]_1$	$[\nu]_2$	$[\nu]_3$	$[\nu]_4$
$\mathcal{F}_1$		(1,-2)	(190,155)	(46561,33448)	(10882804,7844567)	(2546700757,1835553826)
4.347370624$\cdots$	$\mathcal{F}_4$	(2,1)	(197,146)	(46520,33505)	(10883057,7844216)	(2546699198,1835555989)
$\sqrt{Q}\omega^2 = 1+3i$		(1,2)	(202,139)	(46489,33548)	(10883248,7843951)	(2546698021,1835557622)
$\alpha = 3+\sqrt{10}$		(-1,2)	(206,133)	(46463,33584)	(10883408,7843729)	(2546697035,1835558990)
$\mathcal{F}_2$		(1,-2)	(3,4)	(18,-1)	(70,25)	(308,59)
4.392019964$\cdots$	$\mathcal{F}_2$	(2,-1)	(4,3)	(18,1)	(71,22)	(307,64)
$\sqrt{Q}\omega^2 = 2+i$		(2,1)	(5,0)	(17,6)	(73,14)	(304,77)
$\alpha = (1+\sqrt{5})/2$		(-1,2)	(4,-3)	(15,10)	(74,7)	(301,88)
$\mathcal{F}_3$		(8,-1)	(91,48)	(1342,531)	(18739,7822)	(264028,109219)
4.601544787$\cdots$	$\mathcal{F}_5$	(8,1)	(93,44)	(1338,541)	(18749,7798)	(264004,109277)
$\sqrt{Q}\omega^2 = 1+i$		(7,4)	(96,37)	(1331,558)	(18766,7757)	(263963,109376)
$\alpha = 1+\sqrt{2}$		(4,7)	(99,28)	(1322,579)	(18787,7706)	(263912,109499)
$\mathcal{F}_4$		(37,16)	(7516,5483)	(1766281,1272658)	(413271130,297871475)	(96707495041,69702803308)
4.631841066$\cdots$	$\mathcal{F}_1$	(35,20)	(7532,5461)	(1766183,1272794)	(413271734,297870637)	(96707491319,69702808472)
$\sqrt{Q}\omega^2 = 1+3i$		(29,28)	(7568,5411)	(1765961,1273102)	(413273102,297868739)	(96707482889,69702820168)
$\alpha = 3+\sqrt{10}$		(28,29)	(7573,5404)	(1765930,1273145)	(413273293,297868474)	(96707481712,69702821801)
$\mathcal{F}_5$		(1,-2)	(6,7)	(113,36)	(1528,659)	(21653,8906)
4.65445600$\cdots$	$\mathcal{F}_3$	(2,-1)	(7,6)	(112,39)	(1531,652)	(21646,8923)
$\sqrt{Q}\omega^2 = 1+i$		(2,1)	(9,2)	(108,49)	(1541,628)	(21622,8981)
$\alpha = 1+\sqrt{2}$		(-2,1)	(9,-2)	(104,57)	(1549,608)	(21602,9029)
$\mathcal{F}_6$		(16,13)	(774,1307)	(60800,98145)	(4613294,7465447)	(350706224,567450437)
4.804476431$\cdots$	$\mathcal{F}_8$	(13,16)	(789,1298)	(60737,98184)	(4613561,7465282)	(350705093,567451136)
$\sqrt{Q}\omega^2 = -1+2i$		(8,19)	(810,1285)	(60648,98239)	(4613938,7465049)	(350703496,567452123)
$\alpha = 2+\sqrt{5}$		(5,20)	(821,1278)	(60601,98268)	(4614137,7464926)	(350702653,567452644)
$\mathcal{F}_7$		(-2,1)	(9,8)	(48,149)	(869,2018)	(11762,28589)
4.828427124$\cdots$	$\mathcal{F}_7$	(-1,2)	(8,9)	(51,148)	(862,2021)	(11779,28582)
$\sqrt{Q}\omega^2 = -1+i$		(2,1)	(1,12)	(68,141)	(821,2038)	(11878,28541)
$\alpha = 1+\sqrt{2}$		(2,-1)	(-1,12)	(72,139)	(811,2042)	(11902,28531)

Table 1: All families $\mathcal{F}$ with $C_{\mathcal{F}} \leq 5$.

Step 5: Families with $C_{\mathcal{F}} < t$. We examine each $[\nu] \in \mathcal{F}$ such that

$$R_{[\nu]} \leq \left(\frac{C_{\mathcal{F}}^3}{t - C_{\mathcal{F}}} \frac{\pi^3}{96} \right)^{3/2},$$

to test whether $\text{Arc}[\nu] \leq t R_{[\nu]}^{1/3}$. (For, if $R_{[\nu]} > \left(\frac{C_{\mathcal{F}}^3}{t - C_{\mathcal{F}}} \frac{\pi^3}{96} \right)^{3/2}$, then $\text{Arc}[\nu] \leq t R_{[\nu]}^{1/3}$, by Theorem 7.3(iii).)

Proof of Corollary 1.7 Write $t = 2(1+\sqrt{2}) = 4.8284271 \cdots < 5$. To begin with, we determine all such $[\nu]$ for which $R_{[\nu]}^2 \leq (2t_0/\pi)^3 < (10/\pi)^3 < 33$; these all happen to be degenerate examples (see the table below). In Step 2 we see that $5^3/16 < 8$, and so the possible values of the four (pairwise co-prime) factors of Q are $1, 2$, and 5, so that $Q = 1, 2, 5$, or 10. In Step 3 we look for degenerate 4-tuples on circles of radius $\leq (5/2)^6 Q^{3/4}$ for $Q = 1, 2, 5$, and 10, finding the examples listed in Table 2, as well as examples equivalent to these via multiplication by $1, -1, i$, or $-i$, or via complex conjugation. Thus, if $[\nu]$ is degenerate and $R_{[\nu]} > \sqrt{325}$, then $\text{Arc}[\nu] > t R_{[\nu]}^{1/3}$.

R^2	$[\nu]$	$\text{Arc}[\nu] R^{-1/3}$
5	$1+2i, 2+i, 2-i, 1-2i$	**3.7863** $\cdots$
65	$7+4i, 8+i, 8-i, 7-4i$	**4.1746** $\cdots$
5	$2+i, 2-i, 1-2i, -1-2i$	**4.2716** $\cdots$
25	$5i, 3+4i, 4+3i, 5$	**4.5930** $\cdots$
13	$2+3i, 3+2i, 3-2i, 2-3i$	**4.6217** $\cdots$
125	$10+5i, 11+2i, 11-2i, 10-5i$	**4.6364** $\cdots$
325	$17+6i, 18+i, 18-i, 17-6i$	**4.6655** $\cdots$
85	$2+9i, 6+7i, 7+6i, 9+2i$	**4.9836** $\cdots$
533	$22+7i, 23+2i, 23-2i, 22-7i$	**4.9953** $\cdots$

Table 2: Degenerate 4-tuples $[\nu]$ with $\text{Arc}[\nu] < 5 R_{[\nu]}^{1/3}$.

In Step 4, the family $\mathcal{F}_7$ is the only family satisfying $t \leq C_{\mathcal{F}} \leq t \cdot 1.01062$, and we check that $\text{Arc}[\nu] > t R_{[\nu]}^{1/3}$ for all $[\nu] \in \mathcal{F}_7$ with $R_{[\nu]} \leq 0.084 t^{15/4}$. For Step 5, a simple calculation reveals that $\text{Arc}[\nu] \leq t R_{[\nu]}^{1/3}$ for all $[\nu]_n \in \mathcal{F}_m, 1 \leq m \leq 6$, with

$$R_{[\nu]} \leq \left(\frac{C_{\mathcal{F}_m}^3}{t - C_{\mathcal{F}_m}} \frac{\pi^3}{96} \right)^3,$$

except the initial 4-tuples $[\nu]_0$ in $\mathcal{F}_1, \mathcal{F}_2$ and $\mathcal{F}_5$. ■

Proof of Corollary 1.6 Most of the work has been done in the proof above. Now $t = \left(40 + \frac{40}{3}\sqrt{10}\right)^{1/3} = 4.347370 \cdots$. The family $\mathcal{F}_1$ is the only family satisfying $t \leq C_{\mathcal{F}} \leq t \cdot 1.01062$, and we check that $\text{Arc}[\nu] > t R_{[\nu]}^{1/3}$ for all $[\nu] \in \mathcal{F}_1$ with $R_{[\nu]} \leq 0.08 t^{15/4} = 19.7897 \cdots$. Step 4 is vacuous because $\mathcal{F}_1$ is the first family. We are therefore left only with a subset of the degenerate cases given above, namely the top three cases, each of which have $R \leq \sqrt{65}$. ■

9 Asymptotic Estimates for $N_k(t,x),\ k=3,4$

9.1 Counting 4-Tuples

The proof of Theorem 1.8 for 4-tuples Fix t. We wish to determine the number of 4-tuples of lattice points that lie on an arc of length $tR^{1/3}$ of a circle of radius R centered at the origin, where $R \le x$. First we deal only with primitive 4-tuples. Since there are only a bounded number of degenerate $[\nu]$ with $\mathrm{Arc}[\nu] < tR^{1/3}$ by Corollary 6.2, this reduces to determining the number of primitive 4-tuples in each family $\mathcal{F}$ with $C_{\mathcal{F}} < t$. For a given family $\mathcal{F}$ we have $R_n \sim \alpha^{3n}|\,\mathrm{Re}(\sigma\overline{\omega})|/4$ by (3.4), so the number with $R_n \le x$ is $\log x/3\log\alpha + O(1)$. Now each such 4-tuple is one of an equivalence class of 8 examples (as we have discussed). Therefore there are a total of $\sim \beta_t \log x$ primitive 4-tuples of lattice points which lie on an arc of length $tR^{1/3}$ on a circle of radius $R \le x$ centered at the origin, where

$$\beta_t = \frac{8}{3}\sum_{\mathcal{F}:C_{\mathcal{F}}<t} \frac{1}{\log \alpha_{\mathcal{F}}} = \frac{8}{3}\sum_{\alpha} \frac{|\mathcal{F}_\alpha(t)|}{\log\alpha},$$

with $\mathcal{F}_\alpha(t) = \{\mathcal{F}, \alpha_{\mathcal{F}} = \alpha, C_{\mathcal{F}} < t\}$. Rather like in the prime number theorem, if we count each primitive 4-tuple $[\nu]$ with weight $\log\alpha = \log\alpha_{[\nu]}$, then we have

$$\sum_{\substack{\text{primitive } [\nu] \\ \mathrm{Arc}[\nu]<tR^{1/3} \\ R_{[\nu]}<x}} \log\alpha_{[\nu]} \sim \frac{8}{3}\#\{\mathcal{F} : C_{\mathcal{F}} < t\}\log x.$$

Write $N_4(t,x) = \#\{[\nu] : \mathrm{Arc}[\nu] < tR_{[\nu]}^{1/3}, R_{[\nu]} \le x\}$ and, for $g \in \mathbb{Z}[i]$,

$$N_4(t,x,g) = \#\big\{\, [\nu] = (\nu_1,\nu_2,\nu_3,\nu_4) : \gcd(\nu_1,\nu_2,\nu_3,\nu_4) = g,\ \mathrm{Arc}[\nu] < tR^{1/3},\ R_{[\nu]} \le x \big\}.$$

We proved above that $N_4(t,x,1) \sim \beta_t \log x$ for fixed t as $x \to \infty$. To estimate $N(t,x)$ we use the formula $\mathrm{Arc}[\nu] = |g|\,\mathrm{Arc}[\nu/g]$ to obtain

$$\begin{aligned} N_4(t,x) &= \sum_g N_4(t,x,g) \\ &= \sum_g N_4(t|g|^{-2/3}, x|g|^{-1}, 1) \sim \sum_g \beta_{t|g|^{-2/3}} \log(x|g|^{-1}) \sim B_t \log x, \end{aligned}$$

as $x \to \infty$, where

$$B_t = \frac{8}{3}\sum_\alpha \frac{1}{\log\alpha}\sum_g |\mathcal{F}_\alpha(t|g|^{-2/3})|,$$

and the sums are over all $g = a + bi,\ 0 \le b < a$ for which $|g| \le (t/C_{\mathcal{F}_1})^{3/2}$. ■

By Theorem 1.4 and the fact that $\mathcal{F}(t)$ is finite, we know that B_t is a piecewise constant function. We conjecture that $B_t \asymp t^3 \log^6 t$ and, more generally, that

$$N_4(t,x) \asymp \min\{x^2, t^3\}(\log(\min\{x^2, t^3\}))^6 \log x$$

for all $t > \left(40 + \frac{40}{3}\sqrt{10}\right)^{1/3}$. One can prove the slightly stronger estimate $N_4(t,x) \sim c_4 x^2 \log^7 x$ for $x \leq (t/(2\pi))^{3/2}$ for some constant $c_4 > 0$ by a simple counting argument (the analogous argument for N_3 is given at the beginning of the next section).

9.2 Counting 3-Tuples

Writing $N_3(t,x) = \#\{\text{3-tuples } [\nu] : |\nu| \leq x, \text{ and } \operatorname{Arc}[\nu] < t|\nu|^{1/3}\}$, we conjecture that

$$N_3(t,x) \asymp x^{2/3} \min\{x^2, t^3\}^{2/3}(\log(\min\{x^2, t^3\}))^3 \tag{9.1}$$

for all $t > 16^{1/3}$. We can prove a slightly stronger result when $x \leq (t/(2\pi))^{3/2}$, since in this range all the 3-tuples with $|\nu| \leq x$ are counted in $N_3(t,x)$, so that

$$N_3(t,x) = \sum_{n \leq x^2} \binom{r(n)}{3} = \frac{1}{6} \sum_{n \leq x^2} r^3(n) + O(r^2(n)) \sim c_3 x^2 \log^3 x,$$

for some constant $c_3 > 0$, via the usual counting argument using contour integration. The conjecture in (9.1) is equivalent to $N_3(t,x) \asymp x^{2/3} t^2 \log^3 t$ for $x \geq (t/(2\pi))^{3/2}$; we now prove a weak version of this estimate.

The proof of Theorem 1.8 for 3-tuples Defining

$$N_3(t,x,g) = \#\{[\nu] = (\nu_1,\nu_2,\nu_3) : \gcd(\nu_1,\nu_2,\nu_3) = g, |\nu| \leq x, \operatorname{Arc}[\nu] < t|\nu|^{1/3}\},$$

we have

$$N_3(t,x) = \sum_{|g| \leq t^{3/2}} N_3(t,x,g) = \sum_{|g| \leq t^{3/2}} N_3(t|g|^{-2/3}, x|g|^{-1}, 1),$$

so to prove the theorem it suffices to obtain upper and lower bounds for primitive 3-tuples (that is, the case $g = 1$), which we will do in Lemmas 9.4 and 9.5 below.

First we introduce some lemmas and notation. For any $l \in \mathbb{Z}[i]$ let φ_l be the argument of l, and then $\mathbb{Z}_0[i] = \{l \in \mathbb{Z}[i] : 0 \leq \varphi_l \leq \pi/2\}$ with $\mathbb{Z}_0^{\nu}[i]$ the set of visible lattice points in $\mathbb{Z}_0[i]$ (that is, the numbers $a + bi \in \mathbb{Z}[i]$ with $(a,b) = 1$ and $a \geq b \geq 0$).

Lemma 9.1 *For any 3-tuple $[\nu]$ there exists a unique $g \in \mathbb{Z}_0[i]$, $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3 \in \mathbb{Z}_0^{\nu}[i]$, $(\mathbf{p}_i, \mathbf{p}_j) = 1$, and $t_1, t_2, t_3 \in \{0,1,2,3\}$ such that*

$$\nu_1 = i^{t_1} g \mathbf{p}_1 \mathbf{p}_2 \overline{\mathbf{p}}_3, \quad \nu_2 = i^{t_2} g \mathbf{p}_1 \overline{\mathbf{p}}_2 \mathbf{p}_3, \quad \nu_3 = i^{t_3} g \overline{\mathbf{p}}_1 \mathbf{p}_2 \mathbf{p}_3.$$

Proof The values $g = (\nu_1, \nu_2, \nu_3)$, $\mathbf{p}_1 = (\nu_1/g, \nu_2/g, \overline{\nu_3/g})$, $\mathbf{p}_2 = (\nu_1/g, \overline{\nu_2/g}, \nu_3/g)$, $\mathbf{p}_3 = (\overline{\nu_1/g}, \ \nu_2/g, \nu_3/g)$ are the only ones satisfying the conditions. ∎

Lemma 9.2 *If* $\mathrm{Arc}[\nu] < s|\nu|^{1/3}$ *and* $t_1 = t_2 = t_3$, *then* $|\varphi_{\mathbf{p}_i} - \varphi_{\mathbf{p}_j}| < (s/2)|\nu|^{-2/3}$ *for* $i \neq j$.

Proof Notice that $\varphi_{\mathbf{p}_2} - \varphi_{\mathbf{p}_3} = \frac{1}{2}(\varphi_{\nu_1} - \varphi_{\nu_2}) \leq \frac{s}{2}|\nu|^{-2/3}$; the same argument works for the other differences. ∎

Lemma 9.3 *There are at most* $4w^2\epsilon + 1$ *visible lattice points in the angular sector* $|z| \leq w$, $|\varphi_z - \alpha| \leq \epsilon$.

Proof Let $P_1, \ldots, P_n$ denote the visible lattice points in the sector ordered according to increasing argument. Each of the triangles (O, P_i, P_{i+1}), $i = 1, \ldots, n-1$ are inside the angular sector, each has area $\geq 1/2$, and they are disjoint, so that

$$(n-1) \cdot \frac{1}{2} \leq \text{Area of the angular sector} = 2\epsilon w^2$$ ∎

Lemma 9.4 *If* $y > s^{3/2}$, *then* $N_3(s, y, 1) \ll y^{2/3} s^2 \log^2 s$.

Proof We will count 3-tuples $[\nu]$ with $|\nu| \leq y$, $\mathrm{Arc}[\nu] < s|\nu|^{1/3}$, and

$$g = \gcd(\nu_1, \nu_2, \nu_3) = 1,$$

and restrict our attention, in the notation of Lemma 9.1, to the case where $t_1 = t_2 = t_3$ (the other cases following by analogous arguments), and $|\mathbf{p}_1| \leq |\mathbf{p}_2| \leq |\mathbf{p}_3|$ (the other cases following by re-arrangement of the ν_i). If $2^{j_i} \leq |\mathbf{p}_i| < 2^{j_i+1}$ for $i = 1, 2, 3$, then $j_1 \leq j_2 \leq j_3$, and the condition $|\nu| \leq y$ implies that

$$j := j_1 + j_2 + j_3 \leq \log_2 y.$$

Now

$$2^{j_3} \leq |\mathbf{p}_3| \leq |\nu_2 - \nu_3| \leq \mathrm{Arc}[\nu] \leq s|\nu|^{1/3} = s|\mathbf{p}_1\mathbf{p}_2\mathbf{p}_3|^{1/3} \leq (2s)2^{j/3},$$

so that $j_3 \leq \log_2(2s) + j/3$, and, similarly, $j_1, j_2 \leq \log_2(2s) + j/3$. Together these imply that

$$-2\log_2(2s) \leq j_i - j/3 \leq \log_2(2s) \text{ for } i = 1, 2, 3. \tag{9.2}$$

The condition $\mathrm{Arc}[\nu] < s|\nu|^{1/3}$ implies that $|\varphi_{\mathbf{p}_i} - \varphi_{\mathbf{p}_1}| < s2^{-1-2j/3}$ for $i = 2, 3$ by Lemma 9.2, and therefore p_i is a visible lattice point in the angular sector $|z| \leq 2^{j_i+1}, |\varphi_{\mathbf{p}_i} - \varphi_{\mathbf{p}_1}| < s2^{-2j/3}$. There are $\ll 2^{2j_i} \cdot s2^{-2j/3}$ such lattice points by Lemma 9.3, since

$$1 \leq 2^{2j_2}2^{-j}2^{j_3} \leq 2^{2j_2}2^{-j}(2s)2^{j/3} \leq (2s)2^{2j_2}2^{-2j/3} \leq (2s)2^{2j_3}2^{-2j/3}.$$

There are $\ll 2^{2j_1}$ lattice points π with $|\mathbf{p}_i| < 2^{j_1+1}$, and hence the total number of such triples $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ is $\ll s^2 2^{2j/3}$.

Now, for a given j, there are $\ll (\log s)^2$ triples of integers j_1, j_2, j_3 by (9.2), and so our count of lattice points is

$$\ll \sum_{j \le \log_2 y} s^2 2^{2j/3} (\log s)^2 \ll y^{2/3} s^2 (\log s)^2,$$

as required. ■

We now prove bounds in the other direction.

Lemma 9.5 *We have $N_3(s, y, 1) \gg y^{2/3} s^2$ for s sufficiently large.*

Proof We construct examples in Lemma 9.1 with $g = 1$ and each $t_i = 0$, so we want $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3 \in \mathbb{Z}_0^v[i]$ with each $|\mathbf{p}_i| \le y^{1/3}$, as well as $(\mathbf{p}_i, \mathbf{p}_j) = 1$ and $|\varphi_{\mathbf{p}_i} - \varphi_{\mathbf{p}_j}| < (s/2) y^{-2/3}$ for $i \ne j$. Consider the lattice points $\mathbf{p} = a + bi \in \mathbb{Z}_0^v[i]$ with $a + b$ odd, $|\mathbf{p}| \le y^{1/3}$, and divide the circle of radius $y^{1/3}$ into angular sectors of width $(s/2) y^{-2/3}$, which we will denote $S_1, \ldots, S_k$, with $k \asymp [4\pi y^{2/3}/s]$. Note that $(\mathbf{p}, \overline{\mathbf{p}}) = 1$, as $\mathbf{p}$ is visible and $a + b$ is odd. There are $\sim (1/2\pi) y^{2/3}$ such lattice points, and so an average of $\sim s/8\pi^2$ per sector. We can thus prove that if $s \ge 25\pi^2$, then there are $\gg ks^3 \gg y^{2/3} s^2$ triples $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3 \in \mathbb{Z}_0^v[i]$ with each $|\mathbf{p}_i| \le y^{1/3}$ and $|\varphi_{\mathbf{p}_i} - \varphi_{\mathbf{p}_j}| < (s/2) y^{-2/3}$ for $i \ne j$; however we do not necessarily have $(\mathbf{p}_i, \mathbf{p}_j) = 1$ for each $i \ne j$. Forcing this to happen complicates our argument.

We modify the above construction by considering only those $\mathbf{p} = a + bi \in \mathbb{Z}_0^v[i]$ with $a+b$ odd and $|\mathbf{p}| \le y^{1/3}$ that have no divisor $g \in \mathbb{Z}[i]$ for which $1 < |g| \le B$, for some large fixed B to be chosen later. Sieve methods yield that there are $\asymp y^{2/3}/\log B$ such lattice points. Thus if $(\mathbf{p}_i, \mathbf{p}_j) = g \ne 1$, then $|g| > B$. Now this implies that $\mathbf{p}_i/g, \mathbf{p}_j/g$ are distinct visible lattice points lying in an angular sector of angular width $(s/2) y^{-2/3}$ with $|z| \le y^{1/3}/|g|$. There are $\le 1 + 2(s/2) y^{-2/3} (y^{1/3}/|g|)^2 = 1 + s/|g|^2$ such points by Lemma 9.3, and thus no such pair if $|g|^2 > s$, and at most $k(1 + s/|g|^2)(s/|g|^2)/2 \le ks^2/|g|^4$ such pairs otherwise. Therefore the total number of pairs of such lattice points $\mathbf{p}_i, \mathbf{p}_j$ with $|(\mathbf{p}_i, \mathbf{p}_j)| > B$ is at most

$$\sum_{g:\ B < |g| \le \sqrt{|s|}} \frac{ks^2}{|g|^4} \le \frac{8ks^2}{B^2} \le \frac{101 y^{2/3} s}{B^2}.$$

To complete our proof we translate this into a graph theory problem. Let G_i denote a graph whose vertices are the $\mathbf{p} = a + bi \in \mathbb{Z}_0^v[i]$ with $a + b$ odd and $|\mathbf{p}| \le y^{1/3}$ that have no divisor $g \in \mathbb{Z}[i]$ for which $1 < |g| \le B$, and where $\mathbf{p} \in S_i$. Two vertices in G_i have an edge between them if the corresponding $\mathbf{p}$ have no common factor. Then $N_3(s, y, 1)$ is at least the total number of triangles in all of the graphs G_i. Let n_i be the number of vertices in G_i, and let e_i be the number of edges in the complement of G_i, that is, the number of pairs of $\mathbf{p}$ in this sector that have a common factor. Then

$$n := n_1 + \cdots + n_k \asymp y^{2/3}/\log B, \quad k \asymp y^{2/3}/s, \quad e := e_1 + \cdots + e_k \ll y^{2/3} s/B^2.$$

Our result follows from the next lemma by taking B and then s sufficiently large.

Lemma 9.6 *Fix $\epsilon > 0$. There exist constants $c, C > 0$ such that for any integers n, e, k satisfying $n \geq Ck$ and $e \leq cn^2/k$, if G_i is a graph created by deleting e_i edges from the complete graph on $n_i \geq 3$ vertices, for $i = 1, 2, \ldots k$, then there are $\geq (1/4 - \epsilon)n^3/k^2$ triangles in the set of graphs $G_1, \ldots, G_k$, where $n := n_1 + \cdots + n_k$ and $e := e_1 + \cdots + e_k$.*

Proof A graph G_i with $n_i^2/4 + m_i$ edges contains $\gg m_i n_i$ distinct triangles. Hence the total number of triangles in $G_1, \ldots, G_k$ is

$$\gg \sum_{i=1}^{k} n_i \max\left\{0, \frac{n_i^2 - 2n_i}{4} - e_i\right\}. \tag{9.3}$$

We shall suppose that for given n, e, k we have the choice of non-negative real numbers e_i and $n_1 \geq n_2 \geq \cdots \geq n_k \geq 3$ that minimizes the right side of (9.3). This is evidently minimized by taking $e_i = e_{i,0} := \frac{n_i(n_i-2)}{4}$ for $i = 1, 2, \ldots, \ell - 1$, with $0 \leq e_\ell \leq e_{\ell,0}$, and $e_i = 0$ for $i > \ell$. Now, for fixed $e - e_\ell = \sum_{1 \leq i < \ell} \frac{n_i(n_i-2)}{4}$, we wish to maximize $\sum_{1 \leq i < \ell} n_i$ (so as to minimize $\sum_{i > \ell} n_i$), and thus we take them all to be equal. If $n_\ell > n_k$ with $e_\ell < e_{\ell,0}$, then we get a contradiction of minimality by taking $n_1' = n_1 - \delta$, $n_k' = n_k + \delta$ for some very small $\delta > 0$. Thus we have $n_1 = \cdots = n_{\ell-1} = r$, say, and $n_\ell = \cdots = n_k = s$, say, with $r \geq s \geq 3$. Moreover we have $0 < e - (\ell - 1)\frac{r(r-2)}{4} \leq \frac{s(s-2)}{4}$ and $r(\ell - 1) + s(k - \ell + 1) = n$, and the right side of (9.3) equals $(k + 1 - \ell)\frac{s^2(s-2)}{4} - e_\ell s$.

This is now a classical optimization problem. If we take $\ell - 1 = \lambda k$ for $0 \leq \lambda \leq 1$ and $r = \rho n/k, s = \sigma n/k$, then $\rho\lambda + \sigma(1 - \lambda) = 1$, so that $\rho \geq 1 \geq \sigma \geq 0$. Solving, we find that $\sigma = (1 - \rho\lambda)/(1 - \lambda)$. Now

$$e = \frac{r(r + O(1))}{4}(\ell + O(1)) = \lambda\rho^2 n^2/4k\{1 + O(1/r + 1/\ell)\},$$

so that $\lambda \leq 4c/\rho^2\{1 + O(1/r + 1/\ell)\}$, and so $\sigma > 1 - O(c)$. The quantity to be minimized is

$$\geq (1 - \lambda)ks^3/4\{1 + O(1/s)\} = (1 - O(c))\sigma^3 n^3/4k^2 \geq (1 - O(c))n^3/4k^2.$$

implying the desired result. ■

Remark 9.7 By slightly modifying this proof, one can show that if $n \geq (2 + \epsilon)k$ and $e < (1/4 - \epsilon)n(n - 2k)/k$, then there are $\gg_\epsilon n^3/k^2$ triangles. Evidently the restrictions in the hypothesis of Lemma 9.6 cannot be much improved since $n \geq 3k$, and since there is a triangle-free set of k graphs with $e > n^2/4k$ (by making each G_i a complete bipartite graph with about $n/2k$ vertices in each class).

10 Close Divisors

In a forthcoming paper [5], we will deal with the analogous problem for close divisors $d_1, \ldots, d_k$ of a rational integer N. The quantity $\omega = (d_1 \cdots d_k)^{1/k}/N^{1/2}$ shows where the lattice points $(d_i, N/d_i)$ are located on the hyperbola $xy = N$. Since each N/d_i

is also a divisor of N, we study only the k-tuples of *large* divisors, that is, those with $\omega \geq 1$. We can give a lower bound for $L(d_1, \ldots, d_k) = \max_{i \neq j} |d_i - d_j|$, analogous to Theorem 1.1.

$$L(d_1, \ldots, d_k) \geq N^{1/4-1/(8[(k-1)/2]+4)}. \tag{10.1}$$

The analysis of the cases $k = 2, 3$ is similarly straightforward, and one can obtain the sharp estimates:

$$L(d_1, d_2) \geq 2, \qquad L(d_1, d_2, d_3) \geq 2^{2/3} N^{1/6},$$

and that $\{L(d_1, d_2, d_3) N^{-1/6}\}$ is dense in $[2^{2/3}, \infty)$.

The case $k = 4$ again requires more delicate arguments, as we found in this article for the analogous problem for lattice points on circles. For the problem of close divisors, (10.1) yields $L(d_1, \ldots, d_4) \geq N^{1/6}$, and the exponent "1/6" cannot be increased, as we see from the following example. The integers $N_n = 2p_n p_{n+1} p_{n+2} q_n q_{n+1} q_{n+2}$, have divisors

$$d_{1,n} = 2q_n p_{n+1} q_{n+2},\ d_{2,n} = 2q_n q_{n+1} p_{n+2},\ d_{3,n} = p_n p_{n+1} p_{n+2},\ d_{4,n} = 2p_n q_{n+1} q_{n+2},$$

where (p_n, q_n) denote the solutions of the Pell equation $x^2 - 2y^2 = \pm 1$. In fact

$$\lim_{n \to \infty} L(d_{1,n}, d_{2,n}, d_{3,n}, d_{4,n}) N_n^{-1/6} = 2^{7/12} + 2^{13/12} = 3.6172 \cdots .$$

This is not the only family with this kind of property. As in this paper, we can classify all the "close" 4-tuples $[d] = (d_1, d_2, d_3, d_4)$ of divisors of integers N into families $\mathcal{F}$ such that

$$\lim L(d_{1,n}, d_{2,n}, d_{3,n}, d_{4,n}) N_n^{-1/6} = C_{\mathcal{F}}.$$

One can determine a formula similar to (3.6) to describe each family. We are then able to deduce the following theorem (analogous to Corollary 1.6 herein).

Theorem 10.1 *For any* large 4*-tuple of divisors* d_1, d_2, d_3, d_4 *of* N *we have*

$$L(d_1, d_2, d_3, d_4) > 2\left(\frac{3}{2}\right)^{1/12} \left(\frac{8 + 3\sqrt{6}}{5}\right)^{1/3} N^{1/6},$$

whenever $N > N_0$. *On the contrary there exist infinitely many* large 4*-tuples of divisors* $d_{1,n}, d_{2,n}, d_{3,n}, d_{4,n}$ *of* N_n *with*

$$\lim_{n \to \infty} \frac{L(d_{1,n}, d_{2,n}, d_{3,n}, d_{4,n})}{N_n^{1/6}} = 2\left(\frac{3}{2}\right)^{1/12} \left(\frac{8 + 3\sqrt{6}}{5}\right)^{1/3} = 3.006555939 \cdots .$$

Although the ideas and techniques used in [5] are similar to those used in this paper, there are sufficient differences that it seems necessary to write a different paper.

We do not know if the exponent in (10.1) is sharp for $k \geq 5$, just as we do not know if the exponent in Theorem 1.1 is sharp for $k \geq 5$.

11 Other Related Questions

Herein we have studied very precise questions on close lattice points on a circle, and in [5] we develop a similar study of close lattice points on a hyperbola. Presumably it should be possible to generalize these results to close lattice points on all other curves of degree two in the plane, and perhaps to curves of higher degree. In this case one knows that there are very few points, after Mumford's theorem and Faltings' theorem, and those that there are should presumably be very sparse, but such questions appear, for now, to lie deep. There is an important school of research that attempts to obtain bounds that are within a small factor of best possible, which makes these bounds very applicable. As in proofs of Theorem 1.1, the key articles by Bombieri and Pila [1], Heath-Brown [9], and then Elkies [7], all use combinatorial arguments and linear algebra; these have the severe limitation that they are unlikely to give bounds for typical curves that are much better then what is obtained for the lattice-point rich, rational curve, $y = x^d$. Quite recently, Ellenberg and Venkatesh [8] have incorporated true arithmetic-geometric techniques into these arguments, so as to distinguish between rational and non-rational curves, and thus they get bounds of a strength that had previously seemed inaccessible.

One can also ask about analogous questions in higher dimensions, for instance, how close can one pack k lattice points on a sphere in $\mathbb{R}^3$? One has to be a little careful as Heath-Brown showed us: select an integer r which has many representations as the sum of two squares; for example, if r is the product of ℓ distinct primes that are $\equiv 1 \pmod 4$, then r has 2^ℓ such representations. Now let N be an arbitrarily large integer and consider the set of representations of $n = N^2 + r$ as the sum of three squares. Evidently we have $\geq 2^\ell$ such representations in an interval whose size, which depends only on ℓ, is independent of n. Note though that these lattice points all lie on the hyperplane $x = N$, so we can better formulate our question by asking: *How close can one pack k lattice points on a sphere in* $\mathbb{R}^3$*, no four of which belong to the same hyperplane*?

12 Open Problems

We finish this article with two open problems.

Problem 1 *Do there exist infinitely many circles* $x^2 + y^2 = R_n^2$ *with* five *lattice points on an arc of length* $\ll R_n^{2/5}$*?*

We doubt it. From Theorem 1.1 we know that an arc of length $R^{2/5}$ contains, at most, four lattice points, and our guess is that the exponent $2/5$ can be increased, perhaps to as much as $1/2$.

Problem 2 *Is there a uniform bound for the number of lattice points on an arc of length* $\ll R^{1/2}$*?*

Theorem 1.1 gives the upper bound $\ll \log R$ for the number of lattice points on an arc of length $R^{1/2}$, and we would like to see this significantly improved. Indeed this provokes the following (see also [4]).

Conjecture 12.1 *For every $\epsilon > 0$ there exists a constant B_ϵ such that there are no more than B_ϵ lattice points on an arc of length $R^{1-\epsilon}$ of a circle of radius R that is centered at the origin.*

Fix m. Let a be a large integer. Let $\{\sigma_\ell : j = 1, 2, \ldots, \binom{2m}{m}\}$ be the set of functions $\sigma_\ell \colon \{1, \ldots 2m\} \to \{-1, 1\}$ for which $\sum_{j=1}^{2m} \sigma_\ell(j) = 0$. Now define

$$v_\ell := \prod_{j=1}^{2m} (a + j + i\sigma_\ell(j)).$$

Obviously $v_\ell = \prod_{j=1}^{2m}(a + j)(1 + O(m^2/a^2))$, so that $|v_i - v_j| \ll_m |v_i|^{1-1/m}$. In other words, we have constructed $\binom{2m}{m}$ lattice points in an arc of length $O(r^{1-1/m})$ on a circle of radius r. Thus, if Conjecture 12.1 is true, then B_ϵ would have to be at least $e^{C/\epsilon}$ for some constant $C > 0$.

References

[1] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals.* Duke Math. J. **59**(1989), 337–357.

[2] J. Cilleruelo, *Arcs containing no three lattice points.* Acta Arithmetica **59**(1991), 87–90.

[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 sumset of squares.* In: Additive Combinatorics, CRM Proc. Lecture Notes 43, American Mathematical Society, Providence, RI, 2007, pp. 241–262.

[5] ———, *Close divisors.* In preparation. www.dms.umontreal.ca/~andrew/preprints.html

[6] J. Cilleruelo and G. Tenenbaum, *An overlapping theorem with applications.* Publicacions Mathematiques, **51**(2007), 107–118.

[7] N. D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction.* In: Algorithmic Number Theory, Lecture Notes in Comput. Sci. 1838 Springer-Verlag, New York 2000, pp. 33–63.

[8] J. Ellenberg and A. Venkatesh, *On uniform bounds for rational points on nonrational curves.* Int. Math. Res. Not. **35**(2005), 2163–2181.

[9] R. Heath-Brown, *The density of rational points on curves and surfaces.* Ann. of Math. **155**(2002), 553–595.

[10] A. Zygmund, *A Cantor-Lebesgue theorem for double trigonometric series.* Studia Matematica **43**(1972), 173–178.

Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, Spain
e-mail: franciscojavier.cilleruelo@uam.es

Départment de Mathématiques et Statistique, Université de Montréal, CP 6128 succ Centre-Ville, Montréal, QC H3C 3J7
e-mail: andrew@dms.umontreal.ca