CLOSE LATTICE POINTS ON CIRCLES

JAVIER CILLOREUO AND ANDREW GRANVILLE

Abstract. We classify the sets of four lattice points that all lie on a short arc of a circle which 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, \((\nu_1, n, \nu_3, n, \nu_4, n)\), each of which lies on an arc of length \( (40 + \frac{40}{3}\sqrt{10})^{1/3} R^{1/3} n + o(1) \) on a circle of radius \( R_n \).

1. Introduction

How many lattice points can be on a “small” arc of the circle \( x^2 + y^2 = R^2 \)? \(^1\) A. Córdoba and the first author [2] proved that for every \( \epsilon > 0 \) the number of lattice points on an arc of length \( R^{1/2} - \epsilon \) is bounded uniformly in \( R \). More precisely they proved (see also [3] and [4]):

**Theorem 1.1.** For any integer \( k \geq 1 \), an arc of length \( \sqrt{2}R^{1/2} - \frac{1}{4\sqrt{2}R^{1/2}} \) 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 \( \sqrt{2} + o(1) \).

Theorem 1.1 for \( k = 2 \) was first proved by Schinzel, and then used by Zygmund [5] to prove a result about spherical summability of Fourier series in two dimensions. In [1] 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 \( (16R_n)^{1/3} + o_n(1) \).

\(^1\)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.
Let \([\nu] = (\nu_1, \ldots, \nu_k)\) denote a \(k\)-tuple of lattice points lying on the same circle of radius \(R = R_0[\nu]\) centered at the origin, and \(\text{Arc}(\nu) = \text{Arc}(\nu_1, \ldots, \nu_k)\) the length of the shortest arc containing \(\nu_1, \ldots, \nu_k\).

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

**Theorem 1.3.** The set \(\{\text{Arc}(\nu)R_0^{-1/3}, [\nu] = (\nu_1, \nu_2, \nu_3)\}\) 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 by 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
\[
\begin{align*}
    z_1 &= 2(-F_{n-1}, F_{n+2}), \quad z_2 = (-F_{n-2}, F_{n+1}), \quad z_3 = (F_{n-1}, -F_{n+2}), \quad z_4 = (F_n, -F_{n+3}).
\end{align*}
\]

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

In fact the arc length can be shown to be \(> 20^{1/3} \left( \frac{1 + \sqrt{5}}{2} \right) R_n^{1/3}\).

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
\[
\text{Arc}([\nu]_n) \sim C_{\mathcal{F}} R_n^{1/3} \text{ as } n \to \infty.
\]

The main result of this paper is that 4-tuples of lattice points which lie on a short arc of a circle centered at the origin, belong to such a family, and that \(\mathcal{F}(t) = \{\mathcal{F}, \ C_{\mathcal{F}} \leq t\}\) is a finite set for any given \(t\) (which is rather different from the \(k = 2\) case, as given in Theorem 1.3).

**Theorem 1.4.** For any \(t > 0\) any arc on the circle \(x^2 + y^2 = R^2\), of length less than \(tR_n^{1/3}\) with \(R > 2^{-18} t^{15}\), contains at most three lattice points except for the families \(\mathcal{F} \in \mathcal{F}(t)\).

Therefore, in contrast to Theorem 1.3, we deduce the following.

**Corollary 1.** The set \(\{\text{Arc}(\nu)R_0^{-1/3}, [\nu] = (\nu_1, \nu_2, \nu_3, \nu_4)\}\) has only finitely many accumulation points in any interval \((0, t)\), where \(t \in \mathbb{R}^+\).

We order the families \(\mathcal{F}_1, \mathcal{F}_2, \ldots\) so that \(C_{\mathcal{F}_1} \leq C_{\mathcal{F}_2} \leq \ldots\). For fixed \(t\) we can explicitly determine \(\mathcal{F}(t)\) (as described in section 8); indeed, in the table there we describe all seven families belonging to \(\mathcal{F}(5)\). We found that \(C_{\mathcal{F}_1} = (40 + \frac{40}{\sqrt{10}})\) and then \(C_{\mathcal{F}_2} = 20^{1/3} \left( \frac{1 + \sqrt{5}}{2} \right)\) where \(\mathcal{F}_2\) is the family given above. We deduce the following.
Corollary 2. An arc of the circle $x^2 + y^2 = R^2$, with $R > \sqrt{65}$, of length $< (40 + \frac{40}{3}\sqrt{10})^{1/3}$ contains at most three lattice points.

Note that $16^{1/3} = 2.5198 \ldots < (40 + \frac{40}{3}\sqrt{10})^{1/3} = 4.347 \ldots < 20^{1/3} \left(1 + \frac{\sqrt{5}}{2}\right) = 4.3920 \ldots$

The coordinates of the 4-tuples in each family $\mathcal{F}$ grow exponentially. This implies that for each fixed $t > 0$ there exists a constant $\beta_t$ (which will be described in section 9) such that there are $\sim \beta_t \log x$ 4-tuples of lattice points which lie on an arc of length $tR^{1/3}$ of a circle of radius $R$ centered at the origin, where $R \leq x$.

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 [1].

Proof of Theorem 1.2. Suppose that $\nu_1, \nu_2, \nu_3$ are three lattice points, in order, on a circle of radius $R$ so that

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

A theorem attributed to Heron of Alexandria states that if $\Delta$ 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 $\nu_1, \nu_2, \nu_3$ 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 $\geq 1/2$ so, a priori, $\Delta \geq 1/2$. However, we can do better than this: Since $\nu_1, \nu_2, \nu_3$ lie on the same circle, an easy parity argument implies that the co-ordinates of two of these lattice points, say $\nu_i \neq \nu_j$, have the same parity, and so $\frac{1}{2}(\nu_i + \nu_j)$ is also an integer lattice point. Therefore the triangle $\nu_1, \nu_2, \nu_3$ is the disjoint union of two triangles with integer coordinates, which implies that $\Delta \geq 1$. The result follows. \qed

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.

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

Proof of Theorem 1.3. Let $C \geq (16)^{1/3}$ and $\alpha$ satisfying $(1 + \alpha) \left(\frac{4}{\alpha + \alpha^2}\right)^{1/3} = C$. 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 $\mu_j = n_j + im_j, \ j = 1, 2, 3$ and consider

$$v_1 = \mu_1 \overline{\mu}_2 \mu_3, \quad v_2 = i\overline{\mu}_1 \mu_2 \overline{\mu}_3, \quad v_3 = \overline{\mu}_1 \mu_2 \mu_3.$$ 

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

$$R^{1/3} = |v_j|^{1/3} \sim ((\alpha + \alpha^2) / \sqrt{2})^{1/3} m_1.$$
Now $|\nu_3 - \nu_1| R^{-1/3} = |\mu_3||\mu_3 \tau_2 - \tau_1 \mu_2| R^{-1/3} = 2|\mu_3| R^{-1/3} \sim (1 + \alpha) \left( \frac{4}{\alpha + \alpha^2} \right)^{1/3} = C$, and similarly both $|\nu_3 - \nu_2| R^{-1/3} \sim \left( \frac{4}{\alpha + \alpha^2} \right)^{1/3}$ and $|\nu_2 - \nu_1| R^{-1/3} \sim \alpha \left( \frac{4}{\alpha + \alpha^2} \right)^{1/3}$. □

3. THE CONSTRUCTION OF THE FAMILIES OF 4-TUPLES OF LATTICE POINTS

If $g = \gcd(\nu_1, \ldots, \nu_k)$ then $\frac{\text{Arc}[\nu]}{R} = \frac{\text{Arc}[\nu/g]}{R/g}$ so that $\text{Arc}[\nu] = |g| \text{Arc}[\nu/g]$. Therefore $C_{\mathcal{F}([\nu])} = |g|^{2/3} C_{\mathcal{F}([\nu]/g)}$ when $k = 4$, so we can reduce our study to primitive 4-tuples of lattice points where $[\nu]$ is primitive if $\gcd(\nu_1, \nu_2, \nu_3, \nu_4) = 1$.

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

$$\sigma[\nu] := \nu_1 + \nu_2 + \nu_3 + \nu_4 \neq 0$$

Note that if $\sigma = 0$ then the $\nu_i$ cannot all lie on the same half circle, so that $\text{Arc}[\nu] \geq \pi R$.

Next define

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

Let $\Psi[\nu] := \text{Arg}(\sigma[\nu] \omega_{[\nu]})$, so that $-1 < \tan(\Psi[\nu]) \leq 1$ and $\cos(\Psi) > 0$. As $\Psi[\nu] = -\Psi[\nu]$ we can replace $\nu$ with $\overline{\nu}$ if necessary, to guarantee that $0 \leq \Psi[\nu] \leq \pi/4$.

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 4). If $Q[\nu]$ is a square then $[\nu]$ is degenerate, a simple case that we will examine in section 5. 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

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

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

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

$$\omega_1 = \left( \frac{\nu_1 \nu_2 \nu_3 \nu_4}{R} \right)^{1/4}, \quad \omega_2 = \left( \frac{\nu_1 \nu_2 \nu_3 \nu_4}{R} \right)^{1/4}, \quad \text{and} \quad \omega_3 = \left( \frac{\nu_1 \nu_2 \nu_3 \nu_4}{R} \right)^{1/4}.$$

For each integer $n$ we define

$$\omega_{1,n} = \alpha^n \frac{\omega_1 + \overline{\omega_1}}{2}, \quad \omega_{2,n} = \beta^n \frac{\omega_2 - \overline{\omega_2}}{2}, \quad \text{and} \quad \omega_{3,n} = \beta^n \frac{\omega_3 - \overline{\omega_3}}{2}, \quad i = 1, 2, 3,$$

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

$$\nu_{1,n} = R \omega_1 \omega_{1,n} \overline{\omega}_{2,n} \overline{\omega}_{3,n},$$

$$\nu_{2,n} = R \omega_2 \overline{\omega}_{1,n} \omega_{2,n} \overline{\omega}_{3,n},$$

$$\nu_{3,n} = R \omega_3 \overline{\omega}_{1,n} \overline{\omega}_{2,n} \omega_{3,n},$$

$$\nu_{4,n} = R \omega_4 \omega_{1,n} \omega_{2,n} \omega_{3,n}. $$

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

\[
\nu_{j,n} = \alpha^{3n} \sigma + \omega^2 \frac{\alpha^n}{2} + (\epsilon \alpha)^n \left( \frac{\nu_j - \omega^2 \pi}{2} - \frac{\sigma - \omega^2 \pi}{2} \right) + \beta^{3n} \sigma - \omega^2 \frac{\beta^n}{2} + (\epsilon \beta)^n \left( \frac{\nu_j + \omega^2 \pi}{2} - \frac{\sigma + \omega^2 \pi}{2} \right)
\]

so that

\[
\nu_{j,n} \omega = \frac{\alpha^{3n}}{4} \operatorname{Re}(\sigma \omega) + i (\epsilon \alpha)^n \left( \operatorname{Im}(\nu_j \omega) - \operatorname{Im}(\sigma \omega) \right) + i \frac{\beta^n}{2} \operatorname{Im}(\sigma \omega) + (\epsilon \beta)^n \left( \operatorname{Re}(\nu_j \omega) - \operatorname{Re}(\sigma \omega) \right)
\]

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

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

Now $|\tan(\arg(\sigma_n \omega))| = |\frac{\beta^n \operatorname{Im}(\sigma \omega)}{\alpha^n \operatorname{Re}(\sigma \omega)}| = |\beta^n \tan \Psi_{[\nu]|} < 1$ as $|\beta| < 1$ if $n \geq 0$, and also $\cos(\arg(\sigma_n \omega)) > 0$ as $\alpha > 0$ and $\operatorname{Re}(\sigma \omega) > 0$, which implies that $\omega_{|\nu|} = \omega$ (since we already know that $\omega^4 = \omega^4$). In other words, $\omega$ is an invariant of the family. To ensure that $0 \leq \Psi_{[\nu]|} < \pi/4$, we replace $[\nu]_n$ by $[\nu]_n$ if $\beta^n < 0$, that is if $\epsilon = -1$ and $n$ is odd.

Using (3.3) one can show that the 4-tuples $[\nu]_n$ satisfy the recurrence

\[
\nu_{j,n+1} = p q \sigma n + p \sqrt{Q} \omega^2 \sigma n + (p v_{j,n} - q \sqrt{Q} \omega^2 v_{j,n} \epsilon)
\]

We deduce that each $\nu_{j,n} \in \mathbb{Z}[i]$ 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.

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

\[
\mathcal{F}([\nu]) = \{ (\nu_{1,n}, \nu_{2,n}, \nu_{3,n}, \nu_{4,n}), \ n \geq 0 \}.
\]

We extend this definition to any $[\nu]$ by defining $\mathcal{F}([\nu]) = \mathcal{F}([\nu]_{n_0})$ for $[\nu] \in \mathcal{F}([\nu]_{n_0})$. If $[\nu]$ is an initial 4-tuple then $[\nu]_{-1}$ is an initial 4-tuple of a different family, the dual family, which we denote by $\breve{\mathcal{F}} := \mathcal{F}([\nu]_{-1})$.

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

\[
\max_{1 \leq j < k \leq 4} \left| \frac{\operatorname{Im}(\nu_j - \nu_k \omega)}{\alpha^n} \right| \sim \frac{\alpha}{4} R_n^{1/3},
\]

so that

\[
\operatorname{Arc}([\nu]_n) \sim C_{\mathcal{F}} R_n^{1/3} \quad \text{as } n \to \infty.
\]
Similarly

\[ C_{\mathcal{F}}(\nu) = \max_{1 \leq j < k \leq 4} \frac{|2 \text{Re}((\nu_j - \nu_k)\sigma\omega)|}{|2 \text{Im}(\sigma\omega)|^{1/3}}, \]

and note that \( C_{\mathcal{F}}(\nu) = C_{\mathcal{F}}(i\nu) \).

4. Properties of \( Q \)

**Lemma 4.1.** There exists a positive integer \( Q \), not divisible by 4, for which \( \sqrt{Q} \omega^2 \in \mathbb{Z}[i] \). In fact if odd prime \( p \) divides \( Q \) then \( p \equiv 1 \pmod{4} \). Moreover \( Q/(2, Q) \) divides \( R^2 \).

**Proof.** Let \( \gamma_i \) be the exact power of prime ideal \( p \) of norm \( p \) which divides \( \nu_i \), \( i = 1, 2, 3, 4 \), 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 \( p^{\gamma_1} \) is the exact power of \( p \) dividing \( R^2 \), so that \( \gamma_1 - \gamma_i \) is the exact power of prime ideal \( \mathfrak{p} \) which divides \( \nu_i \). Therefore if \( \gamma = \gamma_1 - \gamma_2 - \gamma_3 - \gamma_4 \) then the exact powers of \( \mathfrak{p} \) and \( \mathfrak{P} \) dividing \( \omega^4 \) are given by \((\mathfrak{P}/\mathfrak{p})^\gamma \) which equals \((\mathfrak{P}^2/\mathfrak{p})^\gamma \) if \( \gamma \geq 0 \), and equals \((\mathfrak{P}^2/\mathfrak{p})^{-\gamma} \) if \( \gamma < 0 \). We see that if \( Q_1 \) is the product of these \( p^{\gamma_i} \) 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 \( Q_1 \) divides \( R^2 \). \qed

**Lemma 4.2.** Let \( \mathfrak{p} \) be a prime ideal in \( \mathbb{Z}[i] \). If \([\nu] = (\nu_1, \nu_2, \nu_3, \nu_4) \) is primitive and \( \mathfrak{p}^\alpha \) divides \( \sqrt{Q} \omega^2 \), then \( \mathfrak{p}^\alpha \) 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 \( \mathfrak{p} \) which divides \( \sqrt{Q} \omega^2 \) is \( \mathfrak{p}^{\max\{0, -\gamma\}} \), and \( \max\{0, -\gamma\} = \max\{0, \gamma_3 - (\gamma_1 - \gamma_2)\} \leq \gamma_3 \), so the result follows. \qed

For given odd integer \( n \) we define

\[ r(n) := \min_{(r_1, r_3) = 1, \ i \neq j} \max_{1 \leq i \leq 4} r_i \]

and then let \( r(2^k n) = r(n) \).

**Lemma 4.3.** If \([\nu] \in \mathcal{F} \) and \( Q = Q(\mathcal{F}) \) we have \( \text{Arc}[\nu] \geq (16r(Q))^{1/3} R^{1/3} \).

**Proof.** Suppose that \([\nu]\) is primitive. Let \( g_i = \gcd(\nu_j : j \neq i) \) for \( i = 1, 2, 3, 4 \). By the previous lemma we know that \( \sqrt{Q} \omega^2 \) divides \( g_1 g_2 g_3 g_4 \), so that \( Q \) divides \( |g_1|^2 |g_2|^2 |g_3|^2 |g_4|^2 \). Therefore there exists some \( j \) for which \( |g_j|^2 \geq r(Q) \). Suppose that \( j = 4 \) here and let \( g = g_4 \). Let \( \nu_i = g \sigma \tau \) for \( i = 1, 2, 3 \) then \( \text{Arc}(\nu_i) \geq \text{Arc}[\nu_1, \nu_2, \nu_3] = \text{Arc}(g \tau) = |g| \text{Arc}(\tau) \geq |g|(16R(\tau))^{1/3} = |g|^{2/3}(16R)^{1/3} \) by Theorem 1.2, as \( R(\tau) = R/|g| \). The result follows.

One can immediately deduce the result for imprimitive \([\nu]\). \qed

We deduce the following result from Lemma 4.3 and (3.5).

**Corollary 3.** If \( \mathcal{F} \) is a non-degenerate family then \( C_{\mathcal{F}} \geq (16r(Q))^{1/3} \).
5. Degenerate 4-tuples

If $Q$ is a square then $\alpha = \beta = 1$ so that $\nu_{j,n} = \nu_j$ for all $n$ and $j$, which is why this is the "degenerate" case.

**Lemma 5.1.** If $Q_{[\nu]}$ is a square then $\text{Arc}([\nu]) > 2R^{1/2}/Q^{1/8}$.

*Proof.* In the argument of Lemma 4.1 we see that if $Q$ is a square then each $\gamma$ 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 $(\ell_{\nu_1})(\ell_{\nu_2})(\ell_{\nu_3})(\ell_{\nu_4}) = \ell^4 R^4 \omega^4 = \pm |\ell|^4 R^4/Q = \pm Q R^4$. If $\pm = +$ then let $[\nu'] = \ell [\nu]$; if $\pm = -$ let $[\nu'] = (1 + i \ell) [\nu]$. Either way we have $(\omega')^4 = 1$, so that $Q' = 1$.

Now $R^2 \geq 5$ else there are exactly four lattice points on our circle so that $\sigma_{[\nu]} = 0$. We may assume that $\text{Arc}([\nu']) < \frac{2}{5} R'$, else $\text{Arc}([\nu]) \geq 2(R')^{1/2}$ as $R' \geq \sqrt{5}$. Therefore, using the obvious symmetries (that is, multiplying $[\nu']$ through by a unit or replacing it with $[\nu']$), we can 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 $\text{Arc}[\nu'] > 2y_4 = 2\sqrt{R^2 - x_4^2} \geq 2\sqrt{R^2 - (x_3 - 1)^2} \geq 2\sqrt{R^2 - (R' - 1)^2} = 2\sqrt{2R' - 1} > 2^{5/4}(R')^{1/2}$ as $R' \geq \sqrt{5}$. Therefore from the remarks at the beginning of section 3 we have

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

□

**Corollary 4.** If $\text{Arc}[\nu] < t R^{1/3}$ and $[\nu]$ is degenerate then $R \leq t^{15}/2^{18}$.

*Proof.* $\text{Arc}[\nu] > \max\{2R^{1/2}/Q^{1/8}, (16r(Q)R)^{1/3}\}$ by Lemmas 4.3 and 5.1. Therefore $\text{Arc}[\nu] > 2^{6/5}R^{2/5}$ as $r(Q) \geq Q^{1/4}$ and the result follows.

□

6. The constant $C_F$ associated to a family $\mathcal{F}$

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

**Lemma 6.1.** If $-\pi/2 \leq x_1 < \cdots < x_n \leq \pi/2$ then

$$(6.1) \max_{1 \leq i < j \leq n} |\sin(x_i) - \sin(x_j)| = |\sin(x_1) - \sin(x_n)|$$

.

**Lemma 6.2.** If $|x| \leq \pi/4$, then $|\sin x| < 1.0106|x| \cdot |\cos x|^{1/3}$.

**Lemma 6.3.** If $|x| \leq \pi/4$ and $|y| \leq |x| - 0.137|x|^3$, then $|\sin x| < |x| \cdot \frac{\cos x + \cos y}{2} |1/3|.$

The following is the main result in the section.
Theorem 6.1. If \( \text{Arc}[\nu] < \frac{\pi}{2} R[\nu] \) where \([\nu]\) is 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 \( R_{[\nu]} > 0.08 C_\mathcal{F}^{15/4} \).

Proof. Write \( \nu \omega = Re^{i\phi_j}, j = 1, 2, 3, 4 \), with \( \phi_1 < \phi_2 < \phi_3 < \phi_4 \leq \phi_1 + \pi/2 \) so that \( \text{Arc}[\nu] = (\phi_4 - \phi_1)R \) and note that \( \phi_1 \pm \phi_2 \pm \phi_3 \pm \phi_4 = 0 \) by the definition of \( \omega \). Therefore

\[
C_{\mathcal{F}}(\nu) = \frac{2R^{2/3} |\text{Im}((\nu_1 - \nu_4)\omega)|}{(2\text{Re}(\sigma \omega))^{1/3}} = \frac{2R^{2/3} |\sin(\phi_1) - \sin(\phi_4)|}{|2(\cos(\phi_1) + \cos(\phi_2) + \cos(\phi_3) + \cos(\phi_4))|^{1/3}}.
\]

Now \( \sin(\phi_1) - \sin(\phi_4) = 2\sin(\frac{\phi_1 - \phi_4}{2}) \cos(\frac{\phi_1 + \phi_4}{2}) \) and

\[
\text{cos}(\phi_1) + \text{cos}(\phi_2) + \text{cos}(\phi_3) + \text{cos}(\phi_4) = 2(\cos(\frac{\phi_1 - \phi_4}{2}) + \cos(\frac{\phi_2 - \phi_3}{2})) \cos(\frac{\phi_1 + \phi_4}{2}) \text{ since } \frac{\phi_1 - \phi_4}{2} = \frac{-\phi_4 + \phi_1}{2} \text{, and therefore}
\]

\[
C_{\mathcal{F}} = \frac{2R^{2/3} |\sin(\frac{\phi_1 - \phi_4}{2})| |\cos(\frac{\phi_1 + \phi_4}{2})|^{2/3}}{|\frac{1}{2}(\cos(\frac{\phi_1 - \phi_4}{2}) + \cos(\frac{\phi_2 - \phi_3}{2}))|^{1/3}} \leq \frac{2R^{2/3} |\sin(\frac{\phi_1 - \phi_4}{2})|}{|\cos(\frac{\phi_1 - \phi_4}{2})|^{1/3}}
\]

since \( 0 \leq \cos(\frac{\phi_2 - \phi_4}{2}) \leq \cos(\frac{\phi_2 - \phi_3}{2}) \), so that \( 0 \leq \phi_3 - \phi_2 \leq \phi_4 - \phi_1 \leq \pi/2 \). By Lemma 6.2 we deduce that \( C_{\mathcal{F}} < 1.0106(\phi_4 - \phi_1)R^{2/3} = 1.0106R^{-1/3}\text{Arc}[\nu] \) and part (i) follows.

If \( (\phi_4 - \phi_1) - (\phi_3 - \phi_2) \geq 0.137(\phi_4 - \phi_1)^2 \), then \( C_{\mathcal{F}} < (\phi_4 - \phi_1)R^{2/3} = R^{-1/3}\text{Arc}(\nu) \) by Lemma 6.3, and the result follows. Otherwise \( (\phi_4 - \phi_3) + (\phi_2 - \phi_1) < 0.137(\phi_4 - \phi_1)^2 \) and suppose, for example, that \( \phi_2 - \phi_1 < \frac{0.137}{2} (\phi_4 - \phi_1)^2 \). Applying the argument in the proof of Theorem 1.2 to the triangle formed by \( \nu_1, \nu_2, \nu_4 \) we obtain

\[
2R \leq 4\Delta R = |\nu_1 - \nu_2||\nu_1 - \nu_4||\nu_2 - \nu_4| \leq \text{Arc}(\nu_1, \nu_2)\text{Arc}(\nu_1, \nu_4)\text{Arc}(\nu_2, \nu_4) = (\phi_2 - \phi_1)(\phi_4 - \phi_1)(\phi_4 - \phi_2)R^3 < 0.0685(\phi_4 - \phi_1)^5 R^3 = 0.0685 R^{-2} \text{Arc}[\nu],
\]

so that \( \text{Arc}[\nu] > 1.963667195R^{3/5} > C_{\mathcal{F}} R^{1/3} \) for \( R > 0.08 C_\mathcal{F}^{15/4} \).

\[
\square
\]

7. Classification

Theorem 7.1. If \( \text{Arc}[\nu] < t R_{[\nu]}^{1/3} \) where \([\nu]\) is non-degenerate, then either \( \text{Arc}[\nu] \geq \frac{\pi}{2} R[\nu] \) with \( R \leq (2t/\pi)^{3/2} \), or \([\nu] \in \mathcal{F}, \) for some \( \mathcal{F} \in \mathcal{F}(1.01062t) \) with \( R \leq 0.084 t^{15/4} \), or \([\nu] \in \mathcal{F} \) for some \( \mathcal{F} \in \mathcal{F}(t) \).

Proof. If \( \text{Arc}[\nu] \geq \frac{\pi}{2} R \) then \( \frac{\pi}{2} R < t R_{[\nu]}^{1/3} \) and the first option follows. If \( C_{\mathcal{F}} < t \) then the second option follows. Finally suppose that \( \text{Arc}[\nu] < \frac{\pi}{2} R[\nu] \) and \( C_{\mathcal{F}} \geq t \). Then \( t R_{[\nu]}^{1/3} > \text{Arc}[\nu] > 0.9895 C_{[\nu]} R_{[\nu]}^{1/3} \) by Theorem 6.1 i), so that \( C_{\mathcal{F}} \leq 1.01062t \), that is \( [\nu] \in \mathcal{F}(1.01062t) \). But then \( R \leq 0.084 t^{15/4} \) else \( R > 0.084 t^{15/4} > (0.08)(1.01062t)^{15/4} \geq 0.08 C_{\mathcal{F}}^{15/4} \) implying that \( \text{Arc}(\nu) \) \( C_{\mathcal{F}} R_{[\nu]}^{1/3} \geq t R_{[\nu]}^{1/3} \) by Theorem 6.1 ii). \( \square \)

Proof of Theorem 1.4. \( \max\{2^{-18} t^{15}, 0.084 t^{15/4}, (2t/\pi)^{3/2}\} = 2^{-18} t^{15} \) for \( t \geq 2.432362919 \ldots \), and is \( < 2.4 \) for smaller \( t \). The result then follows from Theorem 7.1 and Corollary 4, and by verifying that the 4-tuples of lattice points on the circles of radius \( \leq \sqrt{3} \) satisfy our bound. \( \square \)

Lemma 7.1. Given \([\nu] \in \mathcal{F} \) there exists \([\nu]_n \) such that \( R_{[\nu]}^2 \leq C_\mathcal{F}^3 p(Q)^3 \).
Proof. Fix \( \delta > 0 \), and select \( m \) such that \( \text{Arc}([\nu]_m) \leq (1 + \delta)C_\mathcal{F}R^{1/3} \), which is possible by (3.5). For convenience we replace \([\nu]\) by \([\nu]_m\). By (3.1) we have, using the arithmetic-geometric mean inequality,

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

To obtain this last inequality we first note that each \( \left| \frac{\omega_i + \overline{\omega_i}}{2} \right| \leq 1 \) and that, if we write each \( \nu_j = R e^{i \varphi_j} \) where \( \varphi_1 \leq \varphi_2 \leq \varphi_3 \leq \varphi_4 < \varphi_1 + \pi/2 \) then \( 2 \left| \frac{\omega_1 - \overline{\omega_1}}{2} \right| = 4 \left| \sin \left( \frac{\varphi_1 - \varphi_2 - \varphi_3 + \varphi_4}{4} \right) \right| \leq |\varphi_1 - \varphi_2 - \varphi_3 + \varphi_4| = |(\varphi_4 - \varphi_1) - (\varphi_3 - \varphi_1) - (\varphi_2 - \varphi_1)| \leq |\varphi_4 - \varphi_1| \) and, similarly, \( 2 \left| \frac{\omega_2 - \overline{\omega_2}}{2} \right| \leq |\varphi_4 - \varphi_1| \) and \( |\varphi_3 - \overline{\varphi_3}| \leq |\varphi_4 - \varphi_1| \), so that

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

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 \( |\gamma| \leq 1/2 \). Then

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

Now \( \alpha + |\beta| = 2p \) if \( \epsilon = 1 \), and \( \alpha + |\beta| = 2q \sqrt{Q} \) if \( \epsilon = -1 \). In the latter case we have \( q \sqrt{Q} = p + 1/(p + q \sqrt{Q}) \leq 2^{1/2} p \) (which is attained when \( Q = 2 \)). We obtain our result by an appropriate choice of \( \delta \), since \( R^2_{[\nu]_m} \) is an integer. \( \Box \)

8. Our algorithm

Fix \( t > 0 \) and suppose that we wish to determine all primitive 4-tuples \([\nu]\) of lattice points for which \( \text{Arc}([\nu]) \leq tR^{1/3}_{[\nu]} \).

Step 0. Determine all such \([\nu]\) for which \( \text{Arc}([\nu]) \geq \frac{2}{3} R_{[\nu]} \), so that \( R_{[\nu]} \leq (2t/\pi)^{3/2} \).

Step 1. We determine all positive integers \( Q \not\equiv 0 \) (mod 4), whose prime factors are 2 or are \( \equiv 1 \) (mod 4), which can be written as the product of four coprime integers all of which are \( \leq t^3/16 \) (by Lemmas 4.1 and 4.3).

Step 2. By Lemma 5.1 we examine, for each such square \( Q \), all circles of radius \( R \leq t^6 Q^{3/4} \), and find all of the degenerate examples. By Theorem 7.1 we find all \([\nu]\), with \( t < C_\mathcal{F}([\nu]) \leq 1.01062 t \) and \( R_{[\nu]} \leq 0.084 t^{15/4} \).

Step 3. For each such non-square \( Q \), consider all circles \( x^2 + y^2 = R^2 \), with \( R^2 \equiv 0 \) (mod \( Q_1 \)), where \( Q_1 = Q/(2, Q) \), such that \( R^2 \leq t^3 p(Q)^3 \) (by Lemma 7.1).

Step 4. Consider all \([\nu]\) in each circle obtained in step 2, and compute the constants \( C_{\mathcal{F}[\nu]} \).
For example, suppose that we wish to determine all primitive 4-tuples \([\nu]\) of lattice points for which \(\text{Arc}(\nu) \leq 5R_{[\nu]}^{1/3}\). To begin with we determine all such \([\nu]\) for which \(\text{Arc}(\nu) \geq \frac{\pi}{2}R_{[\nu]}\), so that \(R_{[\nu]}^2 \leq \left(\frac{10}{\pi}\right)^3 < 33\); these all happen to be degenerate examples (see the table below). In step 1 we see that \(5^3/16 < 8\) and so the possible values of the four (pairwise coprime) factors of \(Q\) are 1, 2 and 5, so that \(Q = 1, 2, 5\) or 10. In step 2 we take \(Q = 1\) and look for degenerate examples on circles of radius \(\leq 5^0\), finding

\[
\begin{array}{|c|c|c|}
\hline
R^2 & [\nu] & \text{Arc}(\nu)R^{-1/3} \\
\hline
5 & 1 + 2i, 2 + i, 2 - i, 1 - 2i & 3.7863\ldots \\
65 & 7 + 4i, 8 + i, 8 - i, 7 - 4i & 4.1746\ldots \\
5 & 2 + i, 2 - i, 1 - 2i, -1 - 2i & 4.2716\ldots \\
25 & 5i, 3 + 4i, 4 + 3i, 5 & 4.5930\ldots \\
13 & 2 + 3i, 3 + 2i, 3 - 2i, 2 - 3i & 4.6217\ldots \\
125 & 10 + 5i, 11 + 2i, 11 - 2i, 10 - 5i & 4.6364\ldots \\
325 & 17 + 6i, 18 + i, 18 - i, 17 - 6i & 4.6655\ldots \\
85 & 2 + 9i, 6 + 7i, 7 + 6i, 9 + 2i & 4.9836\ldots \\
533 & 22 + 7i, 23 + 2i, 23 - 2i, 22 - 7i & 4.9953\ldots \\
\hline
\end{array}
\]

as well as examples equivalent to these via multiplication by 1, \(-1, i\) or \(-i\), or via complex conjugation. Also we look for \([\nu]\), with \(5 < C_{\mathcal{F}([\nu])} \leq 5.0531\) and \(R_{[\nu]}^2 < 1239\): we do have an example, \([\nu] = (31 + 12i, 32 + 9i, 33 + 4i, 33 - 4i)\) with \(R_{[\nu]}^2 = 1105\) and \(C_{\mathcal{F}([\nu])} = 5.0403\ldots\), but \(\text{Arc}(\nu)R^{-1/3} = 5.0653\ldots\).

In step 3, noting that \(p(2) = 1, p(5) = 2\) and \(p(10) = 3\) we consider those radii \(R\) for which \(R^2\) is divisible by 1, 5 or 5 respectively, while being \(\leq 5^3, 10^3\) or \(15^3\), respectively. Then in step 4 we found seven families (which we describe on the table overleaf), with constants

\[
C_{\mathcal{F}_1} = 2 \left(\frac{5}{3}(3 + \sqrt{10})\right)^{\frac{1}{3}} < C_{\mathcal{F}_2} = (20)^{\frac{1}{3}} \left(\frac{1 + \sqrt{5}}{2}\right)^{\frac{1}{3}} < C_{\mathcal{F}_5} = 4 \left(\frac{1}{4}(5 + 4\sqrt{2})\right)^{\frac{1}{3}} < C_{\mathcal{F}_6} = (\frac{1}{5}(14 + 5\sqrt{9})\right)^{\frac{1}{3}} < C_{\mathcal{F}_7} = (2 + \sqrt{2})^2 < C_{\mathcal{F}_{10}} = \frac{3+2\sqrt{3}}{\sqrt{3}} \left(\frac{1+\sqrt{3}}{2}\right)^{\frac{1}{3}}.
\]

A simple calculation then reveals that \(\text{Arc}(\nu) \leq 5R_{[\nu]}^{1/3}\) for all \([\nu]_n \in \mathcal{F}_m : 1 \leq m \leq 9\), except the initial 4-tuples \([\nu]_0\) in \(\mathcal{F}_1, \mathcal{F}_3, \mathcal{F}_7\) and \(\mathcal{F}_9\).

**Proof of Corollary 2.** By Theorem 6.1(i) we see that \(\text{Arc}(\nu) \geq C_{\mathcal{F}_1}R_{[\nu]}^{1/3}\) if \([\nu] \in \mathcal{F}_m : 2 \leq m \leq 9\) since \(C_{\mathcal{F}_1} < 0.9895C_{\mathcal{F}_2}\). By Theorem 2 we see that \(\text{Arc}(\nu) \geq C_{\mathcal{F}_1}R_{[\nu]}^{1/3}\) for \([\nu] \in \mathcal{F}_1\) if \(R_{[\nu]} > 19.7897\ldots\), which is the case for all \([\nu] \in \mathcal{F}_1\) except the initial 4-tuple, but in that case \(\text{Arc}(\nu) \approx 3.7320\ldots R_{[\nu]}^{1/3}\). We are therefore left only with a subset of the degenerate cases given above, namely the top three cases, which each have \(R \leq \sqrt{65}\). \(\square\)
Here $\mathcal{F}_8 = \mathcal{F}(1 + 2i, -2-i, 2+i, 1-2i)$. In fact we have somewhat abused notation here, by merging three different families from the description of section 3, into one, namely $\mathcal{F}_2$. This is valid since our new family $\mathcal{F}_2$ is obtained by taking $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$ in (3.3) rather than $2 + \sqrt{5} = \frac{(1+\sqrt{5})^3}{2}$, $2 - \sqrt{5}$, respectively, and the values there all remain integral in this case. Note that this is not so if we try to do the same thing with $\mathcal{F}_6$.

9. Asymptotics

Fix $t$. We wish to determine the number of 4-tuples of lattice points which lie on an arc of length $tR^{1/3}$ of a circle of radius $R$ centered at the origin, where $R \leq x$. Since there only a bounded number of degenerate $[v]$ with $\text{Arc}[v] < tR^{1/3}$ by Corollary 4, this reduces to determining the number of 4-tuples in each family $\mathcal{F}$ with $C_{\mathcal{F}} < t$. For a given family $\mathcal{F}$ we have $R_n \sim \alpha^{3n} |\text{Re}(\sigma|\omega)|/4$ by (3.4) so the number with $R_n \leq x$ 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 $\sim \beta t \log x$ 4-tuples of lattice points which lie on an arc of length $tR^{1/3}$.
$tR^{1/3}$ on a circle of radius $R \leq x$ centered at the origin, where

$$\beta_t = \frac{8}{3} \sum_{\mathcal{F}: C_{\mathcal{F}} < t} \frac{1}{\log \alpha_{Q} (\mathcal{F})} = \frac{8}{3} \sum_{Q} \frac{|\mathcal{F}_Q (t)|}{\epsilon_Q}$$

with $\epsilon_Q = \log (p + q \sqrt{Q})$ and $\mathcal{F}_Q (t) = \{\mathcal{F}, \ Q(\mathcal{F}) = Q, \ C_{\mathcal{F}} < t\}$. Rather like in the prime number theorem, if we count each 4-tuple $[\nu]$ with weight $\log \alpha = \epsilon_{\nu}$ then we have

$$\sum_{[\nu] < x} \epsilon_{\nu} \sim \frac{8}{3} \sum_{[\nu]} \# \{\mathcal{F} : C_{\mathcal{F}} < t\} \log x.$$ 

10. 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 [3]):

**Conjecture 1.** For every $\epsilon > 0$ there exists a constant $B_\epsilon$, such that there are no more than $B_\epsilon$ 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 $\sigma_\ell : \{1, \ldots, 2m\} \rightarrow \{-1, 1\}$ 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 $|v_\ell - v_j| \ll_m |v_i|^{1-1/m}$; 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 1 is true then $B_\epsilon$ would have to be at least $e^{C/\epsilon}$ for some constant $C > 0$.

**References**

Departamento de Matemáticas. Universidad Autónoma de Madrid. 28049 Madrid
E-mail address: franciscojavier.cilleruelo@uam.es

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