

Circumscribed Circles in Integer Geometry

Oleg Karpenkov^{id} Anna Pratoussevitch^{id}
Rebecca Sheppard^{id}

Received 17 Dec 2024; Accepted 7 May 2025

Abstract:

Integer geometry on a plane deals with objects whose vertices are points in \mathbb{Z}^2 . The congruence relation is provided by all affine transformations preserving the lattice \mathbb{Z}^2 . In this paper we study circumscribed circles in integer geometry. We introduce the notions of integer and rational circumscribed circles of integer sets. We determine the conditions for a finite integer set to admit an integer circumscribed circle and describe the spectra of radii for integer and rational circumscribed circles.

AMS Classification: 52B20, 11H06, 11P21

Key words and phrases: integer geometry, number theory, integer circumscribed circles

Introduction

In this paper we introduce the notion of circumscribed circles in integer geometry and investigate their properties.

The integer distance between two points in the lattice \mathbb{Z}^2 is defined in terms of the number of lattice points on the segment between them; see Section 1.2 for more details. An *integer circle* is the locus of all lattice points at a fixed integer distance from a given lattice point. The properties of integer circles differ substantially from the properties of their Euclidean counterparts. In fact, using the Basel Problem [Ayo74], it can be shown that the density of a unit integer circle in \mathbb{Z}^2 is positive and equal to $6/\pi^2$ (see also [HW08]) Note that the chords of unit integer circles provide a tessellation which is combinatorially equivalent to the Farey tessellation of the hyperbolic plane, while their radial segments correspond to geodesics in the hyperbolic plane (see [Ser, MGO19]).

An *integer circumscribed circle* of a subset of \mathbb{Z}^2 is defined as an integer circle that contains this subset. While in Euclidean geometry every non-degenerate triangle has a unique circumscribed circle, this is no longer the case in integer geometry. In fact, the number of integer circumscribed circles of an integer triangle is infinite.

This paper aims to provide a comprehensive study of circumscribed circles in integer geometry. In Theorem 2.9 we introduce necessary and sufficient conditions for a finite integer set to admit a circumscribed circle. As a special case, we discuss the circumscribed circles of integer quadrangles and their Euclidean counterparts.

While a finite set might not admit an integer circumscribed circle, it will have integer dilates that do. The integer circumscribed circles of the dilates can be interpreted as integer circles with rational centres and radii. We call the set of all such rational radii the *rational spectrum*. In Theorem 3.10 we describe the structure of rational spectra of finite sets.

This paper is organized as follows. In Section 1, we begin with basic definitions of integer

geometry and introduce the notion of an integer circle. In Section 2 we state and prove the conditions under which a finite integer set admits an integer circumscribed circle. We extend the notion of circumscribed circles to the case of rational radii and rational centres and describe the spectra of the radii of such circles in Section 3. In Section 4 we discuss integer and rational circumscribed circles for segments, triangles and quadrangles in more detail.

1 Basic Notions of Integer Geometry

1.1 Objects in Integer Geometry

Consider the plane \mathbb{R}^2 with the fixed basis $(1, 0), (0, 1)$. An *integer point* is a point in \mathbb{R}^2 whose coordinates in this basis are integers, i.e. the set of all integer points is the lattice \mathbb{Z}^2 . An *integer set* is a subset of \mathbb{Z}^2 . An *integer segment* is a segment in \mathbb{R}^2 with endpoints in \mathbb{Z}^2 . An *integer line* is a line in \mathbb{R}^2 that contains at least two integer points. An *integer vector* is a vector in \mathbb{R}^2 with integer endpoints. An *integer polygon* is a polygon in \mathbb{R}^2 whose vertices are integer points.

An *integer affine transformation* is an affine transformations that preserves the integer lattice \mathbb{Z}^2 . We denote the set of all integer affine transformations by $\text{Aff}(2, \mathbb{Z})$. Similar to the Euclidean isometries, $\text{Aff}(2, \mathbb{Z})$ contains *integer translations*, *integer rotations* and *integer symmetries*. They correspond to translations by integer vectors, multiplication by matrices in $\text{SL}(2, \mathbb{Z})$ and multiplication by matrices in $\text{GL}(2, \mathbb{Z}) \setminus \text{SL}(2, \mathbb{Z})$ respectively.

We say that two integer sets are *integer congruent* if there exists an integer affine transformation sending one set to another.

An angle in \mathbb{R}^2 with an integer point as its vertex is called an *integer angle*. An integer angle that contains an integer point other than its vertex on each of its sides is called a *rational integer angle*.

1.2 Some Integer Invariants

Let us recall some basic notions of integer geometry (see [Kar22]). The *integer length* $l\ell(AB)$ of a vector AB in \mathbb{Z}^2 is defined as the number of lattice points that the vector passes through, minus one. Note that the integer length is given by the greatest common divisor of the differences of coordinates. The *integer distance* $ld(A, B)$ between integer points A and B is the integer length of AB . The *integer distance* $ld(O, L)$ between an integer point O and an integer line L is the index of the sub-lattice generated by vectors OV , where V runs through all integer points on the line L .

The *integer area* $ls(ABC)$ of a triangle ABC is the index of the sub-lattice generated by AB and AC in \mathbb{Z}^2 . In fact, the integer area is equal to the absolute value of the determinant $\det(AB, AC)$, and therefore it is twice the Euclidean area of the triangle ABC .

1.3 Integer Circles

We define an *integer circle* with centre $O \in \mathbb{Z}^2$ and radius $r \in \mathbb{Z}$, $r > 0$ as the locus of all points P such that $l\ell(OP) = r$.

Proposition 1.1. *The intersection of an integer line L with an integer circle is either empty, or an infinite periodic subset of integer points on L , or two points.* \square

The *integer radial line* of an integer circle C is an integer line passing through the centre of C . An integer radial line of C intersects C in two points. An *integer tangent line* to an integer circle C of radius r with centre O is an integer line L such that $ld(O, L) = r$.

Remark 1.2. For every pair of integer tangent lines of an integer circle there exists an integer isometry of the circle mapping one integer tangent line to the other.

Remark 1.3. Two integer circles of the same radius are integer congruent. Moreover, one can be mapped to the other by a translation by an integer vector.

Figure 1 shows in bold those points of the integer unit circle S_0 centred at the origin O whose coordinates do not exceed 5 in absolute value. The polygon in Figure 1 is called a

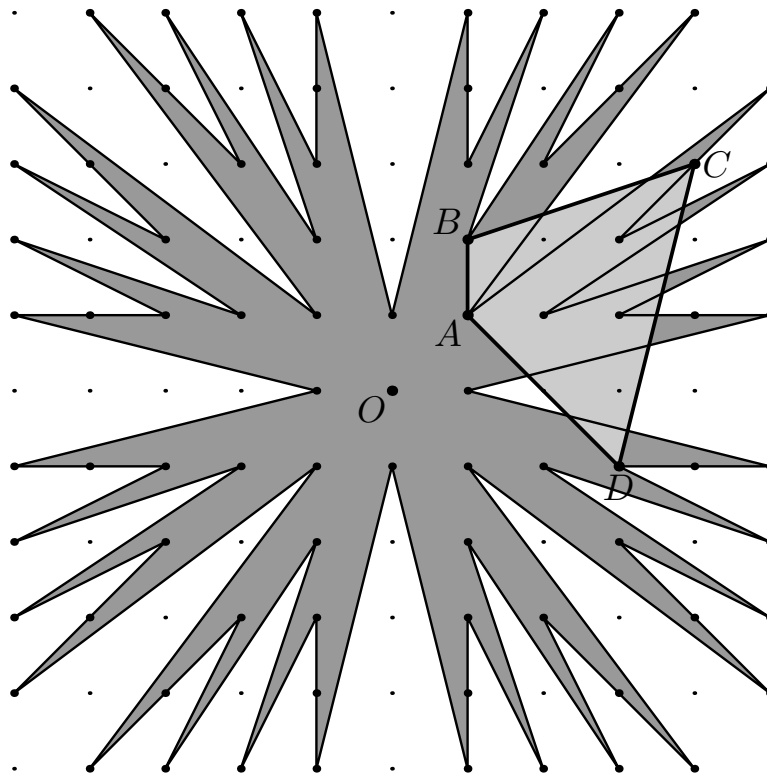


Figure 1: An integer circle circumscribed about an integer quadrangle.

Farey starburst and is obtained by connecting these points by straight segments in the order of increasing argument. The vertices A, B, C, D belong to the integer circle S_0 , hence S_0 is a circumscribed circle of the quadrangle $ABCD$.

Remark 1.4. Consider the integer unit circle S_0 centred at the origin O . Let α be some integer angle and A the point $(1, 0)$. Then it is possible to find infinitely many points B in S_0 such that the angle $\angle AOB$ is integer congruent to α . Note the difference with the Euclidean case, where there are exactly two such points B .

1.4 Integer Trigonometry

Let us discuss basic definitions of integer trigonometry introduced in [Kar09, Kar08] (for the multi-dimensional trigonometry see [BKD23]).

Definition 1.5. Let p, q be co-prime integers with $q \geq p > 0$. The *integer arctangent of q/p* is the angle $\angle AOB$, where

$$A = (1, 0), \quad O = (0, 0), \quad \text{and} \quad B = (p, q).$$

We define *integer sine*, *integer cosine* and *integer tangent* as

$$\text{lsin } \angle AOB = q, \quad \text{lcoss } \angle AOB = p, \quad \text{and} \quad \text{ltan } \angle AOB = q/p.$$

Note that any rational angle is integer congruent to exactly one integer arctangent. So the values of integer trigonometric functions form in fact a complete set of invariants of rational angles up to integer congruence.

The integer sine has a nice geometric definition:

$$\text{lsin } \angle ABC = \frac{\text{ls}(ABC)}{\text{l}\ell(AB)\text{l}\ell(AC)}$$

which directly corresponds to the Euclidean formula for the area of a parallelogram in terms of the sine of its angle. The integer tangent is closely related to the geometry of numbers and their connections to continued fractions [Kar13].

2 Integer Circumscribed Circles

In this section we generalise the notion of a circumscribed circle in the context of integer geometry.

Definition 2.1. An *integer circumscribed circle* of $S \subset \mathbb{Z}^2$ is an integer circle that contains S .

In the Euclidean geometry there exists at most one circumscribed circle for a given set S with $|S| > 2$. This is not the case in integer geometry where a set can have several circumscribed circles. The radius of the circumscribed circle is an important quantity in Euclidean geometry. A suitable replacement for this quantity in integer geometry is the integer circumscribed spectrum.

Definition 2.2. Let S be an integer set. The set of all radii of integer circumscribed circles of S is called the *integer circumscribed spectrum* of S and denoted by $\Lambda_{\mathbb{Z}}(S)$.

Note the following.

Proposition 2.3. Let $a, b \in S$ and let r be the radius of a circumscribed circle of S . Then r divides $\text{ld}(a, b)$.

Proof. Let x be the centre of the circumscribed circle of S . Then

$$a - x \equiv b - x \equiv (0, 0) \pmod{r}.$$

Hence $a - b \equiv (0, 0) \pmod{r}$, and therefore r divides $\text{ld}(a, b)$. □

This proposition implies that the integer spectrum is bounded:

Corollary 2.4. The integer spectrum $\Lambda_{\mathbb{Z}}(S)$ of an integer set S that contains at least 2 points is bounded. □

The first natural question in the study of integer circumscribed circles is whether $\Lambda_{\mathbb{Z}}(S)$ is empty. In this section we will introduce a criterion that answers this question

for a finite set S in terms of projections of S to integer tori as defined below. Later in Subsection 3.2 we will study the structure of $\Lambda_{\mathbb{Z}}(S)$.

Definition 2.5. For an integer $m \geq 2$, let the $(\text{mod } m)$ integer torus be

$$\mathcal{T}_m = \mathbb{Z}^2 / \langle (m, 0), (0, m) \rangle \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

The projection $\pi_m : \mathbb{Z}^2 \rightarrow \mathcal{T}_m$ is given by $(x, y) \rightarrow (x \bmod m, y \bmod m)$.

We say that two integer points v_1 and v_2 in \mathbb{Z}^2 are *equivalent mod m* if $\pi_m(v_1) = \pi_m(v_2)$, denoted by $v_1 \equiv v_2 \bmod m$.

In the statement of the main result of this section we use the following terminology.

Definition 2.6. We say that an integer set S is a *covering set* of \mathcal{T}_m if $\pi_m(S) = \mathcal{T}_m$.

Definition 2.7. We say that an integer set S is *tori-transparent* if for every integer $m \geq 2$ we have that S is not a covering set of \mathcal{T}_m .

Remark 2.8. Note that a covering set of an integer torus \mathcal{T}_t with $t \geq 2$ must consist of at least $|\mathcal{T}_t| = t^2 \geq 4$ points, hence all integer sets S with $|S| \leq 3$ are tori-transparent.

Now we are ready to write down the existence criterion.

Theorem 2.9. Consider a finite integer set $S \subset \mathbb{Z}^2$. Then the following three statements are equivalent:

(i) There exists an integer circumscribed circle of S , i.e.

$$\Lambda_{\mathbb{Z}}(S) \neq \emptyset.$$

(ii) There exists an integer unit circumscribed circle of S , i.e.

$$1 \in \Lambda_{\mathbb{Z}}(S).$$

(iii) The set S is tori-transparent.

We start the proof with the following four lemmas.

Lemma 2.10. *Let $v_1, v_2 \in \mathbb{Z}^2$. Consider two integers d and m such that d is a divisor of m . Then $\pi_m(v_1) = \pi_m(v_2)$ implies $\pi_d(v_1) = \pi_d(v_2)$.*

Proof. If $\pi_m(v_1) = \pi_m(v_2)$, then $v_1 - v_2 \equiv 0 \pmod{m}$ and hence $v_1 - v_2 \equiv 0 \pmod{d}$, since d is a divisor of m . Therefore $\pi_d(v_1) = \pi_d(v_2)$. \square

Lemma 2.11. *Let S be any subset of \mathbb{Z}^2 . If S is a covering set of \mathcal{T}_m then it is a covering set of \mathcal{T}_p for any prime divisor p of m .*

Proof. The set S is a covering set of \mathcal{T}_m , hence for each $v \in \mathbb{Z}^2$ there exists some $s \in S$ such that $\pi_m(v) = \pi_m(s)$. By Lemma 2.10, $\pi_p(v) = \pi_p(s)$. Hence, S is a covering set of \mathcal{T}_p . \square

Lemma 2.12. *For any integer set S the following statements are equivalent:*

- (i) *The set S is tori-transparent.*
- (ii) *The set S is not a covering set of any torus \mathcal{T}_p for prime p .*

Proof. **(i) \Rightarrow (ii)** If the set S is tori-transparent then S is not a covering set of any torus \mathcal{T}_m for integer $m \geq 2$, hence S is not a covering set of any torus \mathcal{T}_p for prime p .

(ii) \Rightarrow (i) Consider any integer $m \geq 2$ and let p be a prime divisor of m . By assumption, S is not a covering set of \mathcal{T}_p . Hence, by Lemma 2.11, S is not a covering set of \mathcal{T}_m . \square

Lemma 2.13. *Consider a finite, tori-transparent integer set S . Then for any finite subset M of \mathbb{Z} there exists a point $v \in \mathbb{Z}^2$ such that $\pi_m(v) \notin \pi_m(S)$ for all $m \in M$.*

Proof. Let $\{p_1, \dots, p_n\}$ be the set of all prime divisors of all elements in M . By Lemma 2.11 for every $i = 1, \dots, n$ the set S is not a covering set of \mathcal{T}_{p_i} . Hence for every $i = 1, \dots, n$ there exists a point $v_i \in \mathbb{Z}^2$ such that for any $s \in S$ we have

$$v_i \not\equiv s \pmod{p_i}.$$

Then by the Chinese Remainder Theorem (applied coordinate-wise) there exists a point v such that for every $i = 1, \dots, n$ it holds:

$$v \equiv v_i \pmod{p_i}.$$

Hence for every $i = 1, \dots, n$ we have

$$\pi_{p_i}(v) = \pi_{p_i}(v_i) \notin \pi_{p_i}(S).$$

Therefore, by Lemma 2.11 $\pi_{p_i}(v) \notin \pi_m(S)$ for all $m \in M$. □

Proof of Theorem 2.9 (iii) \Rightarrow (ii). The existence of a circumscribed circle and the property of being a covering set of integer tori \mathcal{T}_m are invariant under translation by integer vectors. Thus we can assume that the set S is contained in the positive quadrant of \mathbb{Z}^2 . Choose N satisfying the following two conditions:

- S is completely contained in the box $[1, N] \times [1, N]$;
- the number of elements in S does not exceed N .

Consider $Z = \{1, 2, \dots, N\} = [1, N] \cap \mathbb{Z}$. By Lemma 2.13 there exists (a, b) such that $\pi_m(a, b)$ is not in $\pi_m(S)$ for all $m \in Z$.

Set $\beta = b + N!$.

Let p_1, \dots, p_k be all prime numbers in the segment $[N + 1, \beta]$. Now note that the size of the set S is $|S| \leq N < p_i$. Hence the set of first co-ordinates of points in S has fewer than p_i elements. Therefore, for any $i = 1, \dots, k$ we can choose c_i such that c_i is not equal modulo p_i to the first coordinate of any point in S .

By Chinese Remainder Theorem there exists a solution α of the following system of equations:

$$\begin{cases} \alpha \equiv a \pmod{N!} \\ \alpha \equiv c_i \pmod{p_i} \end{cases}$$

Then we will show that the point (α, β) has the property that $\pi_m(\alpha, \beta) \notin \pi_m(S)$ for every integer m , and therefore (α, β) belongs to the unit integer circle with centre at (x, y) for every $(x, y) \in S$.

- If $m \leq N$ then $\pi_m(\alpha, \beta) = \pi_m(a, b) \notin \pi_m(S)$.
- If $m \in [N + 1, \beta]$ and m is a prime, say $m = p_i$, then $\alpha \equiv c_i \pmod{p_i}$ and hence is not equal to the first coordinate of any point in S modulo p_i (by the above). Therefore $\pi_m(\alpha, \beta) \notin \pi_m(S)$.
- If $m \in [N + 1, \beta]$ and m is not a prime then $\pi_m(\alpha, \beta) \notin \pi_m(S)$ by Lemma 2.12 and by the cases considered above.
- If $m > \beta$ then the second co-ordinate of any point in S is in the interval $[1, N]$ while $\beta > N! > N$. Hence the difference of the second coordinates is contained in $[\beta - N, \beta - 1] \subset [1, m - 1]$ and is therefore not equal to zero modulo m . Thus $\pi_m(\alpha, \beta) \notin \pi_m(S)$. \square

Proof of Theorem 2.9 (ii) \Rightarrow (i). This is straightforward. \square

Proof of Theorem 2.9 (i) \Rightarrow (iii). Assume that there exists a circumscribed circle of S of some radius r centred at O . Suppose that S is a covering set of \mathcal{T}_m for some integer $m \geq 2$. Let p be a prime divisor of m . Lemma 2.11 implies that S is a covering set of \mathcal{T}_p .

On the one hand there exists $s_1 \in S$ such that $\pi_p(s_1) = \pi_p(O)$. Therefore, p divides r .

On the other hand there exists $s_2 \in S$ such that $\pi_p(s_2) \neq \pi_p(O)$. Therefore, p does not divide $l\ell(s_2, O) = r$.

This is a contradiction. Hence S is tori-transparent. \square

Remark 2.14. The finiteness of the set S is crucial in Theorem 2.9. For instance, the set

$$S = \{0, 6\} \times \mathbb{Z}$$

is an example of an infinite set, for which Theorem 2.9 does not hold.

Indeed, for every m , the set S is not a covering set of \mathcal{T}_m as $[1, 0]_m \notin \pi_m(S)$ for $m \neq 5$ and $[2, 0]_m \notin \pi_m(S)$ for $m = 5$. Assume that there exists a circle through all points of S with centre (x, y) . The point (x, y) is at integer distance one from all points of $\{0\} \times \mathbb{Z}$,

hence $\gcd(x, y - n) = 1$ for all $n \in \mathbb{Z}$ and therefore $x = \pm 1$. Similarly, (x, y) is at integer distance one from all points of $\{6\} \times \mathbb{Z}$, hence $\gcd(x - 6, y - n) = 1$ for all $n \in \mathbb{Z}$ and therefore $x - 6 = \pm 1$. We arrive at a contradiction.

Finally let us say a few words about the $\text{Aff}(2, \mathbb{Z})$ -invariance of the property of being a covering set of a torus.

Proposition 2.15. *Let S be an integer set and m an integer number. The property of S to be a covering set of \mathcal{T}_m is preserved under $\text{Aff}(2, \mathbb{Z})$.*

Proof. Any element of $\text{Aff}(2, \mathbb{Z})$ can be written as a map $v \mapsto Av + b$ for some matrix $A \in \text{GL}(2, \mathbb{Z})$ and vector $b \in \mathbb{Z}^2$. Note that the equation $v_1 \equiv v_2 \pmod{m}$ (coordinate-wise) is equivalent to the equation $Av_1 + b \equiv Av_2 + b \pmod{m}$. So the number of points in the image under the projection π_m is preserved under $\text{Aff}(2, \mathbb{Z})$. \square

Corollary 2.16. *The property of a finite set to be tori-transparent is invariant under $\text{Aff}(2, \mathbb{Z})$.* \square

Definition 2.17. Let S be an integer set and k a positive integer. We say that S is *shift-divisible* by k if there exists an integer point x and an integer set \hat{S} such that

$$S = x + k\hat{S}.$$

We then say that $\hat{S} \approx S/k$. Note that S is shift-divisible by k if and only if any two points in S are equivalent modulo k . Note that the set \hat{S} is uniquely defined up to a translation by an integer vector. We define S/k as the equivalence class of \hat{S} under translations by integer vectors. The property of an integer set to be a covering set of \mathcal{T}_m is preserved under translations by integer vectors, hence we can say that S/k is a covering set of \mathcal{T}_m or is *tori-transparent* if the set \hat{S} has this property.

Proposition 2.18. *Let S be a finite integer set and a, b integers. If S is shift-divisible by a and b then S is shift-divisible by $\text{lcm}(a, b)$.*

Proof. If S is shift-divisible by a and b then any two points in S are equivalent modulo a and modulo b and therefore equivalent modulo $\text{lcm}(a, b)$. Hence S is shift-divisible by $\text{lcm}(a, b)$. \square

Proposition 2.19. *Let S be a finite integer set and r an integer. Then S has a circumscribed circle of radius r if and only if S is shift-divisible by r and S/r is tori-transparent.*

Proof. Suppose that the set S has a circumscribed circle C of radius r with centre x . Then $S - x \subset r\mathbb{Z}^2$ and $\hat{S} = (S - x)/r$ is an integer set such that $S = x + r\hat{S}$, i.e. S is shift-divisible by r and $S/r \approx \hat{S}$. Moreover, $\hat{C} = (C - x)/r$ is a unit integer circumscribed circle of \hat{S} , hence $1 \in \Lambda_{\mathbb{Z}}(\hat{S})$. Theorem 2.9 implies that S/r is tori-transparent.

Now suppose that S is shift-divisible by r and S/r is tori-transparent, i.e. there exists an integer point x and an integer tori-transparent set \hat{S} such that $S = x + r\hat{S}$. By Theorem 2.9, the set \hat{S} admits a unit integer circumscribed circle \hat{C} . Then $C = x + r\hat{C}$ is an integer circumscribed circle of S of radius r . \square

Proposition 2.20. *Let S be a finite integer set and a, b integers. If $a, b \in \Lambda_{\mathbb{Z}}(S)$ then $\text{lcm}(a, b) \in \Lambda_{\mathbb{Z}}(S)$.*

Proof. If $a, b \in \Lambda_{\mathbb{Z}}(S)$ then Proposition 2.19 implies that S is shift-divisible by a and b and $S/a, S/b$ are tori-transparent. Proposition 2.18 implies that S is shift-divisible by $\text{lcm}(a, b)$. Let $\hat{S} = S/(\text{lcm}(a, b))$. Let $d = \gcd(a, b)$, $\hat{a} = a/d$ and $\hat{b} = b/d$, so that $\gcd(\hat{a}, \hat{b}) = 1$ and $\text{lcm}(a, b) = d\hat{a}\hat{b}$. The set

$$\hat{a}\hat{S} = \hat{a}(S/(d\hat{a}\hat{b})) = S/(d\hat{b}) = S/b$$

is tori-transparent, hence \hat{S} is not a covering set of \mathcal{T}_m for all m co-prime with \hat{a} . Similarly, the set

$$\hat{b}\hat{S} = \hat{b}(S/(d\hat{a}\hat{b})) = S/(d\hat{a}) = S/a$$

is tori-transparent, hence \hat{S} is not a covering set of \mathcal{T}_m for all m co-prime with \hat{b} . The integers \hat{a} and \hat{b} are co-prime, hence every integer m is co-prime with at least one of \hat{a} and \hat{b} . Therefore \hat{S} is not a covering set of any \mathcal{T}_m for $m \geq 2$, i.e. $\hat{S} = S/(\text{lcm}(a, b))$ is tori-transparent. Proposition 2.19 implies that $\text{lcm}(a, b) \in \Lambda_{\mathbb{Z}}(S)$. \square

3 Rational Circumscribed Circles

Some sets do not have integer circumscribed circles. However we can extend the definition of integer circumscribed circles to circles with rational radii. We will see that every finite set has at least one rational circumscribed circle.

3.1 Definition of a Rational Circumscribed Circle

Definition 3.1. We call a fraction $\frac{p}{q}$ *irreducible* if $\gcd(p, q) = 1$.

Definition 3.2. Consider an integer set S and let p and q be two integers. We say that S has a *rational circumscribed circle* of radius $\frac{p}{q}$ if the set qS has a circumscribed circle of radius p .

Definition 3.3. The *rational circumscribed spectrum* $\Lambda_{\mathbb{Q}}(S)$ of an integer set S is the set of all rational values $\frac{p}{q}$ such that S admits a rational circumscribed circle of radius $\frac{p}{q}$.

Remark 3.4. Since every integer circle is also a rational circle, we have

$$\Lambda_{\mathbb{Z}}(S) \subset \Lambda_{\mathbb{Q}}(S).$$

Proposition 3.5. Let S be an integer set. If $\frac{p}{q}$ is an irreducible fraction in $\Lambda_{\mathbb{Q}}(S)$ and $a, b \in S$ then p divides $\text{ld}(a, b)$.

Proof. By definition, $\frac{p}{q} \in \Lambda_{\mathbb{Q}}(S)$ implies $p \in \Lambda_{\mathbb{Z}}(qS)$, i.e. the set qS has an integer circumscribed circle of radius p . Proposition 2.3 implies that p is a divisor of $\text{ld}(qa, qb) = q \cdot \text{ld}(a, b)$ for any $a, b \in S$. As p and q are co-prime, it follows that p is a divisor of $\text{ld}(a, b)$. \square

This proposition implies that the rational spectrum is bounded.

Corollary 3.6. Let S be an integer set, $|S| \geq 2$. Then the rational spectrum $\Lambda_{\mathbb{Q}}(S)$ of S and the set of numerators of irreducible fractions in $\Lambda_{\mathbb{Q}}(S)$ are bounded. \square

Proposition 3.7. Let S be a finite integer set. If $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ are two irreducible fractions in $\Lambda_{\mathbb{Q}}(S)$ then

$$\frac{\text{lcm}(p_1 q_2, p_2 q_1)}{q_1 q_2} = \frac{\text{lcm}(p_1, p_2)}{\gcd(q_1, q_2)} \in \Lambda_{\mathbb{Q}}(S).$$

Proof. If $\frac{p_1}{q_1} \in \Lambda_{\mathbb{Q}}(S)$ then $p_1 \in \Lambda_{\mathbb{Z}}(q_1 S)$, hence $p_1 q_2 \in \Lambda_{\mathbb{Z}}(q_1 q_2 S)$. Similarly, $p_2 q_1 \in \Lambda_{\mathbb{Z}}(q_1 q_2 S)$.

Proposition 2.20 implies $\text{lcm}(p_1 q_2, p_2 q_1) \in \Lambda_{\mathbb{Z}}(q_1 q_2 S)$, hence

$$\frac{\text{lcm}(p_1 q_2, p_2 q_1)}{q_1 q_2} \in \Lambda_{\mathbb{Q}}(S).$$

Finally, we will use the following identity known in elementary number theory

$$\frac{\text{lcm}(p_1 q_2, p_2 q_1)}{q_1 q_2} = \frac{\text{lcm}(p_1, p_2)}{\text{gcd}(q_1, q_2)}. \quad \square$$

3.2 Structure of Rational Spectra

Proposition 3.8. *Let S be a finite integer set. If $\frac{p}{q}$ and $\frac{p'}{q'}$ are two irreducible fractions in $\Lambda_{\mathbb{Q}}(S)$ and $\max(\Lambda_{\mathbb{Q}}(S)) = \frac{p}{q}$, then $p' \mid p$ and $q \mid q'$.*

Proof. By Proposition 3.7, the number

$$\frac{\text{lcm}(p, p')}{\text{gcd}(q, q')}$$

is in $\Lambda_{\mathbb{Q}}(S)$, hence

$$\frac{\text{lcm}(p, p')}{\text{gcd}(q, q')} \leq \max(\Lambda_{\mathbb{Q}}(S)) = \frac{p}{q}.$$

Note that $\text{lcm}(p, p') \geq p$ and $\text{gcd}(q, q') \leq q$, hence the inequality above can only hold if

$$\text{lcm}(p, p') = p, \quad \text{gcd}(q, q') = q.$$

Therefore $p' \mid p$ and $q \mid q'$. \square

Corollary 3.9. *Let S be a finite integer set. If $\frac{p}{q}$ is an irreducible fraction in $\Lambda_{\mathbb{Q}}(S)$ and $\max(\Lambda_{\mathbb{Q}}(S)) = \frac{p}{q}$, then p is the largest possible numerator and q is the smallest possible denominator of an irreducible fraction in $\Lambda_{\mathbb{Q}}(S)$.*

Theorem 3.10. *Let S be a finite integer set. Let $\{t_1, \dots, t_n\}$ be the set of all primes t such that S is a covering set of \mathcal{T}_t . Let $\tau = \prod_{i=1}^n t_i$. Then there exists $p \in \mathbb{Z}_+$ such that*

$$\Lambda_{\mathbb{Q}}(S) = \left\{ \frac{1}{c} \cdot \frac{p}{\tau} \mid c \in \mathbb{Z}_+ \right\}.$$

In fact, $p = \max(\Lambda_{\mathbb{Z}}(\tau S))$, $p/\tau = \max(\Lambda_{\mathbb{Q}}(S))$, and the greatest common divisor of all integer distances between pairs of points in S is a multiple of p .

If S is tori-transparent then $\tau = 1$,

$$\Lambda_{\mathbb{Q}}(S) = \left\{ \frac{p}{c} \mid c \in \mathbb{Z}_+ \right\}$$

and $p = \max(\Lambda_{\mathbb{Z}}(S)) = \max(\Lambda_{\mathbb{Q}}(S))$.

Proof. Let $\frac{p}{q}$ be an irreducible fraction such that $\max(\Lambda_{\mathbb{Q}}(S)) = \frac{p}{q}$.

1. We will show that q is a divisor of τ : We know that S and hence τS is not a covering set of \mathcal{T}_t for any prime $t \notin \{t_1, \dots, t_n\}$. For $i = 1, \dots, n$, the set $t_i S$ and hence τS is not a covering set of \mathcal{T}_{t_i} . In summary, the set τS is not a covering set of \mathcal{T}_t for every prime t , i.e. τS is tori-transparent. Theorem 2.9 implies $1 \in \Lambda_{\mathbb{Z}}(\tau S)$ and hence $\frac{1}{\tau} \in \Lambda_{\mathbb{Q}}(S)$. Proposition 3.8 implies $q \mid \tau$.
2. We will now show that $q = \tau$: We have shown that q is a divisor of τ . Suppose that $q \neq \tau$ then q is the product of some but not all of t_1, \dots, t_n . We can assume without loss of generality that t_1 is not a divisor of q . We know that S is a covering set of \mathcal{T}_{t_1} and $\gcd(t_1, q) = 1$, hence qS is also a covering set of \mathcal{T}_{t_1} and therefore not tori-transparent. Theorem 2.9 implies that $\Lambda_{\mathbb{Z}}(qS) = \emptyset$. On the other hand, we know that $\frac{p}{q} \in \Lambda_{\mathbb{Q}}(S)$, hence $p \in \Lambda_{\mathbb{Z}}(qS)$ in contradiction to $\Lambda_{\mathbb{Z}}(qS) = \emptyset$. Hence $q = \tau$.

3. We will next show that

$$\Lambda_{\mathbb{Q}}(S) \subset \left\{ \frac{1}{c} \cdot \frac{p}{\tau} \mid c \in \mathbb{Z}_+ \right\} :$$

Consider an irreducible fraction $\frac{p'}{q'}$ in $\Lambda_{\mathbb{Q}}(S)$. We know that the irreducible fraction $\frac{p}{q} = \frac{p}{\tau}$ is the maximum of $\Lambda_{\mathbb{Q}}(S)$. Proposition 3.8 implies that $p' \mid p$ and $\tau \mid q'$, hence there exists $c \in \mathbb{Z}_+$ such that

$$\frac{p'}{q'} = \frac{1}{c} \cdot \frac{p}{\tau}.$$

4. We will now show that

$$\left\{ \frac{1}{c} \cdot \frac{p}{\tau} \mid c \in \mathbb{Z}_+ \right\} \subset \Lambda_{\mathbb{Q}}(S) :$$

Let $c \in \mathbb{Z}_+$. We know that $\frac{p}{\tau} \in \Lambda_{\mathbb{Q}}(S)$, hence $p \in \Lambda_{\mathbb{Z}}(\tau S)$ and therefore $\Lambda_{\mathbb{Z}}(\tau S) \neq \emptyset$. Theorem 2.9 implies that the set τS is tori-transparent. It follows that the set $c(\tau S)$ is also tori-transparent. Theorem 2.9 implies that $1 \in \Lambda_{\mathbb{Q}}(c\tau S)$ and therefore $\frac{1}{c} \in \Lambda_{\mathbb{Q}}(\tau S)$. We know that $p, \frac{1}{c} \in \Lambda_{\mathbb{Q}}(\tau S)$, hence $\frac{p}{c} \in \Lambda_{\mathbb{Q}}(\tau S)$ according to Proposition 3.7. Therefore $\frac{p}{c\tau} \in \Lambda_{\mathbb{Q}}(S)$.

5. Finally, we will show that the greatest common divisor of all integer distances between pairs of points in S is a multiple of p : We know that $\frac{p}{q} = \frac{p}{\tau} \in \Lambda_{\mathbb{Q}}(S)$, hence $p \in \Lambda_{\mathbb{Z}}(\tau S)$ and therefore τS has a circumscribed circle of radius p . It follows that the integer distance between any two points in τS is a multiple of p . We know that $\gcd(p, \tau) = \gcd(p, q) = 1$, hence the integer distance between any two points in S is a multiple of p . \square

Remark 3.11. Let S be a finite integer set. Then

$$\Lambda_{\mathbb{Z}}(S) = \Lambda_{\mathbb{Q}}(S) \cap \mathbb{Z}.$$

In the case $\Lambda_{\mathbb{Z}}(S) \neq \emptyset$, we additionally get the equality

$$\max(\Lambda_{\mathbb{Z}}(S)) = \max(\Lambda_{\mathbb{Q}}(S)).$$

Remark 3.12. There is a similarity between the expression for the rational circumscribed spectrum in Theorem 3.10 and some formulas for coefficients of Ehrhart polynomials, see for example [BR15].

Note that while Theorem 3.10 states that the greatest common divisor of all integer distances between pairs of points in S is a multiple of p , it is not necessarily equal to p as can be seen in the following example:

Example 3.13. Consider the set

$$S = \{(0, 0), (2, 0), (0, 2), (2, 2)\}.$$

On the one hand, the set S is tori-transparent, so Theorem 3.10 implies that there exists a divisor p of all integer distances between pairs of points in S such that

$$\Lambda_{\mathbb{Q}}(S) = \left\{ \frac{p}{c} \mid c \in \mathbb{Z}_+ \right\}.$$

The greatest common divisor of all integer distances between points in S is $g = 2$, hence either $p = 1$ and $\Lambda_{\mathbb{Z}}(S) = \{1\}$ or $p = g = 2$ and $\Lambda_{\mathbb{Z}}(S) = \{1, 2\}$. On the other hand, we have $S = 2\hat{S}$, where

$$\hat{S} = \{(0, 0), (1, 0), (0, 1), (1, 1)\}.$$

Now \hat{S} is a covering set of \mathcal{T}_2 , hence Theorem 2.9 implies $1 \notin \Lambda_{\mathbb{Z}}(\hat{S})$ and therefore $2 \notin \Lambda_{\mathbb{Z}}(S)$. Thus $p = 1 \neq g$.

To give a more precise description of circumscribed spectra, we will need the following definition:

Definition 3.14. An integer set S is called *primitive* if it is not shift-divisible by k for any integer $k > 1$.

Remark 3.15. Note that a set is primitive if and only if the greatest common divisor of the distances between all pairs of its points equals to one.

Theorem 3.16. Let S be a finite integer set. Let x be an integer point, g an integer and \hat{S} a primitive set such that $S = x + g\hat{S}$. Let $\{t_1, \dots, t_n\}$ be the set of all primes t such that \hat{S} is a covering set of \mathcal{T}_t . Let $\tau = \prod_{i=1}^n t_i$. Then the rational circumscribed spectrum of S is

$$\Lambda_{\mathbb{Q}}(S) = \left\{ \frac{1}{c} \cdot \frac{g}{\tau} \mid c \in \mathbb{Z}_+ \right\}.$$

If \hat{S} is tori-transparent then $\tau = 1$ and

$$\Lambda_{\mathbb{Q}}(S) = \left\{ \frac{g}{c} \mid c \in \mathbb{Z}_+ \right\}.$$

Proof. Theorem 3.10 implies that there exists $p \in \mathbb{Z}_+$ such that

$$\Lambda_{\mathbb{Q}}(\hat{S}) = \left\{ \frac{1}{c} \cdot \frac{p}{\tau} \mid c \in \mathbb{Z}_+ \right\},$$

and that p is a divisor of all integer distances between pairs of points in \hat{S} . The set \hat{S} is primitive, hence the greatest common divisor of all integer distances between pairs of points in \hat{S} is equal to 1 and therefore $p = 1$. It follows that

$$\Lambda_{\mathbb{Q}}(\hat{S}) = \left\{ \frac{1}{c} \cdot \frac{1}{\tau} \mid c \in \mathbb{Z}_+ \right\}$$

and therefore

$$\Lambda_{\mathbb{Q}}(S) = \Lambda_{\mathbb{Q}}(g\hat{S}) = g \cdot \Lambda_{\mathbb{Q}}(\hat{S}) = \left\{ \frac{1}{c} \cdot \frac{g}{\tau} \mid c \in \mathbb{Z}_+ \right\}. \quad \square$$

Definition 3.17. The *primorial* $d\#$ of $d \in \mathbb{Z}_+$ is defined as the product of all prime numbers smaller or equal to d .

Proposition 3.18. Let S be a finite integer set and $k = |S|$ then

$$\frac{1}{[\sqrt{k}]\#} \in \Lambda_{\mathbb{Q}}(S).$$

Proof. Let $k = |S|$. Theorem 3.10 implies that $\frac{1}{n\tau} \in \Lambda_{\mathbb{Q}}(S)$ for every $n \in \mathbb{Z}_+$, where $\tau = \prod_{i=1}^n t_i$ and $\{t_1, \dots, t_n\}$ is the set of all primes t such that S is a covering set of \mathcal{T}_t . Note that if S is a covering set of an integer torus \mathcal{T}_t then $t^2 = |\mathcal{T}_t| \leq |S| = k$ and therefore $t \leq \sqrt{k}$. It follows that $\{t_1, \dots, t_n\}$ is a subset of the set of all primes smaller or equal to \sqrt{k} , hence τ is a divisor of $[\sqrt{k}]\#$, i.e. $[\sqrt{k}]\# = n\tau$ for some $n \in \mathbb{Z}_+$. Therefore

$$\frac{1}{[\sqrt{k}]\#} = \frac{1}{n\tau} \in \Lambda_{\mathbb{Q}}(S). \quad \square$$

Example 3.19. Let $a, b \geq 2$ be integers. The circumscribed spectra of the integer set

$$G_{a,b} = \{1, \dots, a\} \times \{1, \dots, b\}$$

are given by

$$\Lambda_{\mathbb{Z}}(G_{a,b}) = \emptyset, \quad \Lambda_{\mathbb{Q}}(G_{a,b}) = \left\{ \frac{1}{c} \cdot \frac{1}{(\min(a,b))\#} \mid c \in \mathbb{Z}_+ \right\}.$$

To prove this, note that $G_{a,b}$ is a primitive set. Theorem 3.16 implies that

$$\Lambda_{\mathbb{Q}}(G_{a,b}) = \left\{ \frac{1}{c} \cdot \frac{1}{\tau} \mid c \in \mathbb{Z}_+ \right\},$$

where $\{t_1, \dots, t_n\}$ is the set of all primes t such that $G_{a,b}$ is a covering set of \mathcal{T}_t and $\tau = \prod_{i=1}^n t_i$. The set $G_{a,b}$ is a covering set for an integer torus \mathcal{T}_t if and only if $2 \leq t \leq \min(a, b)$. Hence the set $\{t_1, \dots, t_n\}$ consists of all primes smaller or equal to $\min(a, b)$ and therefore $\tau = (\min(a, b))\#$. Finally, $\Lambda_{\mathbb{Z}}(S) = \Lambda_{\mathbb{Q}}(S) \cap \mathbb{Z} = \emptyset$.

4 Circumscribed Circles of Polygons

We define an *integer circumscribed circle of a polygon P* as the integer circumscribed circle of the set of vertices of P in the sense of Definition 2.1. Note that an integer circle is an integer circumscribed circle of P if and only if all vertices of P are on the circle (see Figure 1). We define a *rational circumscribed circle of a polygon P* as the rational circumscribed circle of the set of vertices of P in the sense of Definition 3.2.

In this section we summarise the implications of the results of Theorem 3.16 for integer and rational circumscribed circles of polygons.

4.1 Circumscribed Circles of Segments and Triangles

An integer segment or triangle always admits a unit integer circumscribed circle.

Proposition 4.1. *Let S be an integer segment or triangle. Let g be the greatest common divisor of all integer distances between pairs of vertices of S . Then the integer circumscribed spectrum $\Lambda_{\mathbb{Z}}(S)$ consists of all positive divisors of g and*

$$\Lambda_{\mathbb{Q}}(S) = \left\{ \frac{g}{c} \mid c \in \mathbb{Z}_+ \right\}.$$

In particular if S is a primitive segment or triangle then

$$\Lambda_{\mathbb{Z}}(S) = \{1\}, \quad \Lambda_{\mathbb{Q}}(S) = \left\{ \frac{1}{c} \mid c \in \mathbb{Z}_+ \right\}.$$

Proof. There exist an integer point x and a primitive polygon \hat{S} such that $S = x + g\hat{S}$. The set of vertices of \hat{S} consists of at most three points and therefore is tori-transparent.

Theorem 3.16 implies that

$$\Lambda_{\mathbb{Q}}(S) = \left\{ \frac{g}{c} \mid c \in \mathbb{Z}_+ \right\}.$$

It follows that $\Lambda_{\mathbb{Z}}(S) = \Lambda_{\mathbb{Q}}(S) \cap \mathbb{Z}$ consists of all positive divisors of g . □

We obtain the following corollary:

Corollary 4.2. *If an integer set S has a integer circumscribed circle of radius r then the integer distance between any two points of S is a multiple of r .*

Proof. Consider $A, B \in S$. Any integer circumscribed circle of S is in particular an integer circumscribed circle of the segment AB , hence the integer length of the segment AB is divisible by r . □

Let us recall the Euclidean Extended Sine Rule: for a triangle ABC we have

$$\frac{|AB|}{\sin \angle BCA} = \frac{|BC|}{\sin \angle CAB} = \frac{|CA|}{\sin \angle ABC} = 2R,$$

where R is the radius of the circumscribed circle.

As was shown in [Kar08], the first two of these equalities hold in lattice geometry:

$$\frac{\ell(AB)}{\ell \sin \angle BCA} = \frac{\ell(BC)}{\ell \sin \angle CAB} = \frac{\ell(CA)}{\ell \sin \angle ABC}.$$

Proposition 4.1 tells us that there is no natural generalisation for the last equality. Indeed, the circumscribed spectrum depends entirely on the integer length of the edges of the triangle and does not depend on the angles.

For instance consider two triangles, one with vertices $(0, 0), (1, 0), (0, 1)$ and another with vertices $(0, 0), (1, 2), (2, 1)$. For both triangles, all edges are of unit integer length. The sets of integer sines of the angles of these triangles are distinct, for the first triangle all integer sines are equal to 1 while for the second triangle all integer sines of the angles are equal to 3. Nevertheless the circumscribed spectra for both triangles coincide.

4.2 Circumscribed Circles of Quadrangles

We have seen that every triangle has an integer circumscribed circle, however this is no longer true for quadrangles as the following example shows.

Definition 4.3. An integer polygon P is *empty* if the only lattice points contained in P are the vertices.

Proposition 4.4. *An empty integer strictly convex quadrilateral does not have a integer circumscribed circle.*

Proof. Note that every empty integer strictly convex quadrilateral is integer congruent to the coordinate square S_1 with vertices $(0, 0)$, $(1, 0)$, $(1, 1)$ and $(0, 1)$. The square S_1 is a covering set of \mathcal{T}_2 , hence it is not tori-transparent. Theorem 2.9 implies that S_1 does not admit integer circumscribed circles of any radius. \square

However some quadrangles have integer circumscribed circles.

Example 4.5. The quadrilateral with vertices $A = (0, 0)$, $B = (1, 0)$, $C = (0, 1)$ and $D = (2, 2)$ has a unit circumscribed circle centred at $(1, 1)$.

The situation is similar to the Euclidean geometry, where a quadrangle has a circumscribed circle if and only if its opposite angles add up to π . The lattice version of this rule is as follows:

Proposition 4.6. *An integer quadrangle has an integer circumscribed circle if and only if the set of its vertices is not a covering set of \mathcal{T}_2 .*

Proof. Theorem 2.9 implies that a quadrangle admits an integer circumscribed circle if and only if its set of vertices V is tori-transparent, i.e. is not a covering set of any integer torus \mathcal{T}_t for $t \geq 2$. The set V cannot be a covering set of \mathcal{T}_t for $t > 2$ since $|V| = 4 < t^2 = |\mathcal{T}_t|$. Hence the set V is tori-transparent if and only if it is not a covering set of \mathcal{T}_2 . \square

Remark 4.7. The conditions for a quadrangle to admit a circumscribed circle can be stated in terms of the parity of the six integer distances between its pairs of vertices as follows: An integer quadrangle admits an integer circumscribed circle if and only if at least one of the integer distances between its vertices is even.

On the other hand, the existence of an integer circumscribed circle is not determined solely by the integer angles of the integer quadrangle. For example, the angles of the quadrangles with vertices $A(0,0)$, $B(0,1)$, $C(1,1)$, $D(1,0)$ and $P(-1,0)$, $Q(-1,1)$, $R(0,1)$, $S(1,0)$ are congruent to each other, however the latter one admits a circumscribed circle, for example one centred at the origin $O(0,0)$, while the former one does not.



4.3 Circumscribed Circles of General Polygons

In fact, the argument used in the proof of Proposition 4.6 holds for all n -gons with $n \leq 8$:

Proposition 4.8. *An integer n -gon with $n \leq 8$ has an integer circumscribed circle if and only if the set of its vertices is not a covering set of \mathcal{T}_2 .* \square

In general, the following statement holds:

Proposition 4.9. *An integer n -gon admits an integer circumscribed circle if and only if its vertices are not a covering set of \mathcal{T}_t for every $t \leq \sqrt{n}$.* \square

Acknowledgements

Grant support for R.S.: This work was supported by a Vacation Bursary of the London Mathematical Society.

We would like to thank the anonymous referee for their helpful suggestions.

References

- [Ayo74] R. Ayoub. Euler and the zeta function. *The American Mathematical Monthly*, 81:1067–1086, 1974. 18
- [BKD23] J. Blackman, O. Karpenkov, and J. Dolan. Multidimensional integer trigonometry. *Commun. Math.*, 31(2):1–26, 2023. 22
- [BR15] M. Beck and S. Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2015. Integer-point enumeration in polyhedra, With illustrations by David Austin. 33
- [HW08] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles. 18
- [Kar08] O. Karpenkov. Elementary notions of lattice trigonometry. *Mathematica Scandinavica*, 102:161–205, 2008. 22, 37
- [Kar09] O. Karpenkov. On irrational lattice angles. *Funct. Anal. Other Math.*, 2(2-4):221–239, 2009. 22
- [Kar13] O. Karpenkov. *Geometry of Continued Fractions*. Springer Nature, 2013. 22
- [Kar22] O. Karpenkov. *Geometry of Continued Fractions*. Springer Nature, 2 edition, 2022. 20
- [MGO19] S. Morier-Genoud and V. Ovsienko. Farey boat: continued fractions and triangulations, modular group and polygon dissections. *Jahresber. Dtsch. Math.-Ver.*, 121(2):91–136, 2019. 18
- [Ser] C. Series, Continued fractions and hyperbolic geometry, LMS Summer School, Notes, 2015.
<http://homepages.warwick.ac.uk/~masbb/HypGeomandCntdFractions-2.pdf>. 18

AUTHORS

Oleg Karpenkov

Department of Mathematical Sciences

University of Liverpool

Liverpool L69 7ZL, United Kingdom

email: karpenk@liverpool.ac.uk

Anna Pratoussevitch

Department of Mathematical Sciences

University of Liverpool

Liverpool L69 7ZL, United Kingdom

email: annap@liverpool.ac.uk

Rebecca Sheppard

Department of Mathematical Sciences

University of Liverpool

Liverpool L69 7ZL, United Kingdom

email: rshepp@liverpool.ac.uk