Graphs and Combinatorics (2011) 27:441–450
DOI 10.1007/s00373-011-1015-4

PROCEEDINGS PAPER

Lattice Points on Similar Figures and Conics

Takayasu Kuwata · Hiroshi Maehara

Published online: 17 March 2011

Abstract Let us say that a plane figure F satisfies Steinhaus' condition if for any positive integer n, there exists a figure F_n similar to F which satisfies the condition $|F_n \cap \mathbb{Z}^2| = n$. For example, the circular disc satisfies Steinhaus' condition. We prove that every compact convex region in the plane $\mathbb{R}^2$ satisfies Steinhaus' condition. As for plane curves, it is known that the circle satisfies Steinhaus' condition. We consider Steinhaus' condition for other conics, and present several results.

Keywords Lattice point · Similar figure · Conics

1 Introduction

In 1957, Steinhaus raised the following problem (cf. [5]): Does there exist a circular disc in $\mathbb{R}^2$ which contains exactly n lattice points? Where a lattice point means a point whose coordinates are all intergers. Sierpinski [4] solved the problem affirmatively by showing that the distances from lattice points to $(\sqrt{2},\ 1/3)$ are all distinct. We study similar problems for various plane figures in this paper.

Definition 1 Let F be a plane figure. Let us call the following condition Steinhaus' Condition and denote it by SC.
SC: For any positive integer n, there exists a figure F_n similar to F which satisfies the condition $|F_n \cap \mathbb{Z}^2| = n$.

T. Kuwata (✉) · H. Maehara
Research Institute of Educational Development, Tokai University,
2-28-4 Tomigaya,
Shibuya-ku, Tokyo 151-0063, Japan
e-mail: kuwata@tokai-u.jp

Example 1 Sierpinski's result implies that the circular disc satisfies SC. In fact, for any positive integer n, there is a circular disc whose center is $(\sqrt{2}, 1/3)$ and which contais exactly n lattice points.

We prove the following more general theorem.

Theorem 1 *In the plane* $\mathbb{R}^2$, *every compact convex region* Γ *satisfies SC. Namely, for any positive integer* n, *there exists a figure* Γ_n *similar to* Γ *satisfying* $|\Gamma_n \cap \mathbb{Z}^2| = n$.

What can we say for curves in the plane? It is easy to see that the line does not satisfy SC. The circle satisfies SC as proved by Schinzel in [3] (cf. [2]).

Theorem 2 ([3], [2]) *Let* p *be a prime number such that* $p \equiv 1 \pmod 4$, $p^{n-1} \equiv 1 \pmod 8$. *Then the circle* $(4x-1)^2 + (4y)^2 = p^{n-1}$ *passes through exactly* n *lattice points, for any* $n > 0$. *As a cosequence, the circle satisfies SC.*

How about for other conics? Irreducible conics are classified in similarities by their eccentricities. That is, if two conics have the same eccentricity e, then they are similar in shape. All irreducible conics are classified as follows:

$$\begin{cases} Circle & e = 0: \text{all circles are similar in shape} \\ Ellipse & 0 < e < 1 \\ Parabola & e = 1: \text{all parabolas are similar in shape} \\ Hyperbola & e > 1 \end{cases}$$

We show the follwing result for the parabola.

Theorem 3 *In the plane* $\mathbb{R}^2$, *the parabola does not satisfy SC.*

For ellipses and hyperbolas, the ratio λ = (minor axis)/(major axis) is also an invariant under similarity. For example, the ratio λ of an ellipse $x^2/a^2 + y^2/b^2 = 1$ is equal to $\lambda = \min\{b/a, a/b\}$. The ratios of hyperbolas $x^2/a^2 - y^2/b^2 = 1$, $x^2/a^2 - y^2/b^2 = -1$ are equal to b/a, a/b, respectively.

For ellipses and hyperbolas, we prove the following theorem. A few more results about the number of lattice points on the conics will be given in Sects. 4, 5.

Theorem 4 *Let* λ *be the ratio of an ellipse* (*or a hyperbola*).

(1) *If* λ^2 *is an algebraic number of degree greater than* 2 *or a transcendental real number, then the ellipse* (*or the hyperbola*) *does not satisfy SC.*
(2) *In the case of ellipses,* $\lambda^2 \in \mathbb{Q}$ *implies SC.*

2 Compact convex regions in the plane

For two regions $C, D \subset \mathbb{R}^2$, let us say that D is an *expansion* of C if C is similar to D $(C \sim D)$ and $C \subset \text{Int } D$, where $\text{Int} D$ denotes the set of interior points of D.

Proof of Theorem 1. Assume that Γ is a compact convex region and there exists a positive integer m such that $|C \cap \mathbb{Z}^2| \neq m$ for any figure C that is similar to Γ. Let $a = \max\{|C \cap \mathbb{Z}^2| : C \sim \Gamma,\ |C \cap \mathbb{Z}^2| \leq m\}$. Then $a < m$. Let C_0 be a region which satisfies $C_0 \sim \Gamma$ and $|C_0 \cap \mathbb{Z}^2| = a$. Let $b = \min\{|D \cap \mathbb{Z}^2| : D$ is an expansion of $C_0,\ \partial D \cap \mathbb{Z}^2 \neq \emptyset,\ |D \cap \mathbb{Z}^2| \geq m\}$. Then $b > m$. And let D_0 be an expansion of C_0 that satisfies $\partial D_0 \cap \mathbb{Z}^2 \neq \emptyset$ and $|D_0 \cap \mathbb{Z}^2| = b$. Then $|\partial D_0 \cap \mathbb{Z}^2| = b - a \geq 2$ hold. For otherwise, by shrinking D_0, we would get an expansion of C_0 that contains more than a, and less than b lattice points.

Take two points P, Q $\in \partial D_0 \cap \mathbb{Z}^2$. Let L be a supporting line of D_0 at Q.

If P $\notin L$, then by shrinking D_0 suitably with center P, we get an expansion D_0' of C_0 that satisfies $D_0' \subset D_0 - \{\mathrm{Q}\}$. Then $a < |D_0' \cap \mathbb{Z}^2| < b$, which contradicts to the choices of a and b.

If P $\in L$, then by rotating D_0 suitably with center P, we get an expansion D_0' of C_0 that satisfies $D_0' \cap \mathbb{Z}^2 \subset (D_0 - \{\mathrm{Q}\}) \cap \mathbb{Z}^2$. Then $a < |D_0' \cap \mathbb{Z}^2| < b$, which also contradicts to the choices of a and b. □

Remark We conjecture that every region enclosed by a Jordan curve satisfies *SC* in the plane.

3 Parabolas

Proposition 1 *An irreducible conic through* 5 *lattice points is determined uniquely and can be expressed as follows:*

$$a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6 = 0\ (a_1,\ a_2, \ldots, a_6 \in \mathbb{Z}).$$

Proof Note that any 3 points among 5 lattice points are not on a line, because a conic is irreducible.

Let $C : a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6 = 0$ be an irreducible conic which passes through 5 lattice points $\mathrm{P}_i(x_i,\ y_i) \in \mathbb{Z}^2$ $(i = 1,\ 2,\ \ldots,\ 5)$. Then

$$\begin{pmatrix} x_1^2 & x_1y_1 & y_1^2 & x_1 & y_1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_5^2 & x_5y_5 & y_5^2 & x_5 & y_5 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_5 \\ a_6 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \cdots (*)$$

Regard $(*)$ as a linear equation in $a_1,\ a_2, \ldots, a_6$. Since the matrix of coefficients in $(*)$ has a rank less than or equal to 5, it has a solution in $\mathbb{Q}^6$. Multiply by denominators of the solution, we get a solution in $\mathbb{Z}^6$. Since C is irreducible, it does not have a component of a line. So the ratio $a_1 : a_2 : a_3 : a_4 : a_5 : a_6$ in $(*)$ is unique by Bezout's theorem. □

To show Theorem 3, it suffices to prove the following theorem.

Theorem 5 *If a parabola passes through* 5 *lattice points, then it passes through infinitely many lattice points. As a consequence, the parabola does not satisfy SC.*

Proof Let C be a parabola which passes through 5 lattice points. Then C can be expressed by an equation with integer coefficients by Propositin 1.

We may assume that one of 5 lattice points is the origin O by tanslating if necessary. Let O, P_i $(i = 1, 2, 3, 4)$ be 5 lattice points on C. Then we can take a point Q on C such that $\mathrm{OP}_1 \parallel \mathrm{P}_2\mathrm{Q}$. Since the slope of OP_1 is a rational number, Q is a rational point and the midpoints M, N of OP_1, $\mathrm{P}_2\mathrm{Q}$ are also rational points. Then the slope of MN is a ratinal number. Let $b/a (a, b \in \mathbb{Z})$ be the slope of MN. Note that it is equal to the slope of the symmetric axis for C.

Consider the similarity transformation $\varphi\colon \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} b & -a \\ a & b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. The parabola C is transformed to $C'\colon py = qx^2 + rx\,(p, q, r \in \mathbb{Z})$ by φ and we have infinitely many lattice points $\mathrm{R}_n = (pn(a^2 + b^2), pqn^2(a^2 + b^2)^2 + rn(a^2 + b^2))\ (n \in \mathbb{Z})$ on C'. Then $\varphi^{-1}(\mathrm{R}_n)\ (n \in \mathbb{Z})$ are lattice points on C. Therefore C passes through infinitely many lattice points. □

Example 2 The parabolas $y = \sqrt{2}x^2$, $y = \sqrt{2}(x^2 - 1)$, $(x + \sqrt{2}y)^2 = x + 2y$, and $\{6x + (-3 + \sqrt{15})y\}^2 - 72x + (-24 + 6\sqrt{15})y = 0$ passes through exactly 1, 2, 3, and 4 lattice points, respectively.

4 Ellipses and Hyperbolas

Definition 2 Let us define $\mathcal{R}$ by
$\mathcal{R} := \{|\alpha/\beta|\colon \alpha \text{ and } \beta \text{ are eigenvalues of } \begin{pmatrix} a & h \\ h & b \end{pmatrix} \in GL(2, \mathbb{Q})\}$.
We denote the ellipse and the hyperbola whose ratio of axes is λ by E_λ and H_λ, respectively.

Theorem 6 *If E_λ (or H_λ) passes through 5 lattice points, then $\lambda^2 \in \mathcal{R}$. As a consequence, if $\lambda^2 \notin \mathcal{R}$, then E_λ (or H_λ) does not satisfy SC.*

Proof Let C be an ellipse (or a hyperbola) whose ratio is λ and which passes through 5 lattice points. Applying Proposition 1, C can be expressed as

$$C\colon ax^2 + 2hxy + by^2 + cx + dy + e = 0\ (a, h, b, c, d, e \in \mathbb{Z}).$$

By a suitable rotation, C can be transformed to

$$C'\colon \alpha x^2 + \beta y^2 + px + qy + r = 0,$$

where α, β are eigenvalues of $\begin{pmatrix} a & h \\ h & b \end{pmatrix} \in GL(2, \mathbb{Q})$. Therefore $\lambda^2 = |\alpha/\beta| \in \mathcal{R}$. □

Theorem 7 *If λ is a rational number, then E_λ (or H_λ) satisfies the condition SC.*

Proof The case of the ellipse: suppose $\lambda = b/a \in \mathbb{Q}\,(a, b$ are coprime and a is an odd number). Let p be a prime number such that $p \equiv 1 \pmod 8$. Since $(4x/a - 1)^2 + (4y/b)^2 = p^{n-1}$, $x, y \in \mathbb{Z}$ implies $a|x$ and $b|y$, there exists a bijection between

Table 1 Steinhaus condition for ellipses and hyperbolas

λ	$\lambda \in \mathbb{Q}$	$\begin{cases}\lambda \notin \mathbb{Q}\\ \lambda^2 \in \mathbb{Q}\end{cases}$	$\lambda^2 \in \mathcal{R}\backslash\mathbb{Q}$	$\lambda^2 \notin \mathcal{R}$
E_λ	SC	SC	(1)	not SC
H_λ	SC	(2)	(3)	not SC

$\{(x, y) \in \mathbb{Z}^2 : (4x/a - 1)^2 + (4y/b)^2 = p^{n-1}\}$ and $\{(X, Y) \in \mathbb{Z}^2 : (4X - 1)^2 + (4Y)^2 = p^{n-1}\}$ by $(x, y) \mapsto (X, Y) = (x/a, y/b)$. Then by Theorem 2, the ellipse $(4x/a - 1)^2 + (4y/b)^2 = p^{n-1}$ passes through exactly n lattice points.

The case of the hyperbola: suppose $\lambda = b/a \in \mathbb{Q}$ (a, b are coprime). Let p be a prime number such that $p \equiv 1 \pmod{6ab}$. Note that such prime numbers exist infinitely, by Dirichlet's Theorem. The condition $(3ax+1)^2 - (3by)^2 = p^{n-1}$ $(x, y \in \mathbb{Z})$ implies

$$6ax + 2 = p^k + p^{n-1-k} \quad \text{and} \quad 6by = p^k - p^{n-1-k}\ (0 \le k < n).$$

Therefore the hyperbola $(3ax+1)^2 - (3by)^2 = p^{n-1}$ passes through exactly n lattice points. □

For ellipses, the following stronger result holds.

Theorem 8 *If $\lambda^2 \in \mathbb{Q}$, then E_λ satisfies SC.*

To prove this theorem, we use the following result by E.Bannai and T.Miezaki [1]. If $(a, b), (c, d) \in \mathbb{R}^2$ $(ad - bc \neq 0)$, then $\{m(a, b) + n(c, d) \mid m, n \in \mathbb{Z}\}$ is called the lattice spanned by $(a, b), (c, d)$. An *integral lattice* means that the inner product of any two vectors in the lattice is an integer.

Theorem 9 ([1]) *In any integral lattice, there exists a circle that passes through exactly n points of the lattice for every positive integer n.*

Proof of Theorem 8. Let λ be a positive number that satisfies $\lambda^2 \in \mathbb{Q}$. Let $\lambda^2 = b/a$ (a, b are coprime), i.e., $\lambda = \sqrt{b/a} = \sqrt{ab}/a$. Then the lattice $\Lambda[(a, 0), (0, \sqrt{ab})]$ is an integral lattice, where the notation $\Lambda[(a, 0), (0, \sqrt{ab})]$ means the lattice spanned by $(a, 0), (0, \sqrt{ab})$. Applying Theorem 9, there exists a circle $\Gamma : (x - p)^2 + (y - q)^2 = r^2$ that passes through exactly n points of $\Lambda[(a, 0), (0, \sqrt{ab})]$ for any positive integer n. By the affine transformation $(x, y) \mapsto (X, Y) = (x/a, y/\sqrt{ab})$, Γ is transformed to $\Gamma' : (aX - p)^2 + (\sqrt{ab}Y - q)^2 = r^2$, and $\Lambda[(a, 0), (0, \sqrt{ab})]$ is transformed to $\mathbb{Z}^2$, bijectively. Therefore Γ' passes through exactly n points of $\mathbb{Z}^2$, that is, $|\Gamma' \cap \mathbb{Z}^2| = n$. Since Γ' is an ellipse whose ratio is λ, E_λ satisfies SC. □

Let us summarize these results in the following table.
The cases (1), (2), (3) are not decided yet, which will be considered in some extent in the following section.

5 Examples and Problems

Definition 3 For a plane figure F, let us call the set

$$\mathcal{S}(F) := \{|F' \cap \mathbb{Z}^2| \in \mathbb{N} \cup \{\infty\} : F' \sim F \text{ in } \mathbb{R}^2,\ F' \cap \mathbb{Z}^2 \neq \emptyset\}$$

the size-set of F.

Remark A figure F satisfies SC if and only if $\mathbb{N} \subset \mathcal{S}(F)$.

Example 3 (1) $\mathcal{S}(\text{line}) = \{1, \infty\}$.
(2) $\mathcal{S}(\text{circle}) = \mathbb{N}$ by Theorem 2.
(3) $\mathcal{S}(\text{parabola}) = \{1, 2, 3, 4, \infty\}$ by Theorem 5 and Example 2.

Theorem 10 *If $\lambda^2 = \alpha/\beta \in \mathcal{R}\backslash\mathbb{Q}$ and $\sqrt{\alpha\beta} \notin \mathbb{Q}$, then $\mathcal{S}(E_\lambda)$ is an infinite set. Here λ, α, β, and $\mathcal{R}$ are as in* Definition 2.

Lemma 1 *Let $d \in \mathbb{N}$ such that $\sqrt{d} \notin \mathbb{Q}$. Then for any positive integers k, n with $k\pi > n\sqrt{d}$, the equation $x^2 + dy^2 = (k^2 + d)^n$ has at least $n + 1$ integer solutions (x, y).*

Proof Let $w = k + \sqrt{-d} \in \mathbb{Z}[\sqrt{-d}]$. Then $w\overline{w} = k^2 + d$. Let $z_s := x_s + y_s\sqrt{-d} = w^s\overline{w}^{n-s}$ $(s = 0, 1, 2, \dots, n)$. Then (x_s, y_s) $(s = 0, 1, 2, \dots, n)$ are integer solutins of the given equation. Let $\theta = \operatorname{Arg} w$. Since $k\pi > n\sqrt{d}$, we have $0 < \theta < \tan\theta = \sqrt{d}/k < \pi/n$. Hence $\operatorname{Arg} z_s = (2s - n)\theta$ $(s = 0, 1, 2, \dots, n)$ are all distinct, and the solutions (x_s, y_s) $(s = 0, 1, 2, \dots, n)$ are all distinct. □

Proof of Theorem 10. Let λ be a real number with $\lambda^2 \in \mathcal{R}\backslash\mathbb{Q}$. Then there exist $a, b, h \in \mathbb{Z}$ such that $\lambda^2 = \alpha/\beta$, where α, β are the eigenvalues of $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$. Let k, n be integers with $k\pi > n\sqrt{d}$. By Lemma 1, the ellipse $C : dX^2 + Y^2 = (k^2 + d)^n$ passes through at least $n + 1$ lattice points. Let $d = ab - h^2$. We consider the transformation $(X, Y) \mapsto (x, y)$ by $X = ax + hy$, $Y = dy$. The ellipse C is transformed to C': $d(ax + hy)^2 + (dy)^2 = (k^2 + d)^n$ and C' passes through at least $n+1$ points of $(\frac{1}{ad}\mathbb{Z})^2$. Moreover, the transformation $(x, y) \mapsto (u, v) = (adx, ady)$ sends C' to C'': $au^2 + 2huv + bv^2 = ad(k^2 + d)^n$. Then C'' passes through at least $n + 1$ lattice points. The ratio of the ellipse C'' is equal to λ. Let N_1 be the number of lattice points on C''. Then $N_1 \geq n + 1$ holds.

Next, regard N_1 as new n and repeat the same process. We will get a new ellipse C'' whose ratio of axes is λ and the ellipse passes through $N_2 > N_1$ lattice points. This process can be repeated infinitely, and $N_1, N_2, \dots \in \mathcal{S}(E_\lambda)$. Hence $\mathcal{S}(E_\lambda)$ is an infinite set. □

Problem 1 Does $\lambda^2 \in \mathcal{R}\backslash\mathbb{Q}$ imply that $\mathcal{S}(E_\lambda)$ is an infinite set?

Proposition 2 *If $\lambda^2 \notin \mathbb{Q}$, then $\mathcal{S}(E_\lambda)$ and $\mathcal{S}(H_\lambda)$ contains* $\{1, 2, 3, 4\}$.

Proof Let μ be an irrational number such that μ, λ^2 are algebraically independent over $\mathbb{Q}$. Then $\pm\lambda^2 x^2 + y^2 + \mu x = 0$, $\pm\lambda^2(x^2 - 1) + y^2 + \mu y = 0$, $\pm\lambda^2(x^2 - x) + y^2 + x - 1 = 0$, and $\pm\lambda^2(x^2 - 1) + y^2 - 1 = 0$ passes through exactly 1, 2, 3, and 4 lattice points, respectively. □

Theorem 11 *If* $\lambda \notin \mathbb{Q}$ *and* $\lambda^2 \in \mathbb{Q}$, *then* $\mathcal{S}(H_\lambda)$ *contains* $\{1, 2, 3, 4\}$.

Proof Hyperbolas $\lambda^2 x^2 - y^2 + \sqrt{2}y = 0$, $\lambda^2(x^2 - 1) - y^2 + \sqrt{2}y = 0$ pass through exactly 1, 2 lattice points, respectively.

Let $H_\lambda : ax^2 + 2hxy + by^2 + cx + dy = 0$. Then eigenvalues α, β of $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$ induces $\lambda^2 = -\alpha/\beta$. Since $\lambda^2 \in \mathbb{Q}$, let $\alpha = ms$, $\beta = ns$ $(s > 0)$, where $m, n \in \mathbb{Z}$ are coprime and $mn < 0$, $m + n \neq 0$. Then $a + b = \alpha + \beta = (m + n)s$, $ab - h^2 = \alpha\beta = mns^2$. We choose $t \in \mathbb{Q}$ such that

$$a = t(m + n)s, \quad b = (1 - t)(m + n)s, \quad h^2 = As^2 > 0, \quad \text{and} \quad \sqrt{A} \notin \mathbb{Q} \cdots (*),$$

where $A := t(1 - t)(m + n)^2 - mn$.

Choose $t = 1$, then $H_\lambda : (m + n)(x^2 - x + y) + 2\sqrt{-mn}(xy - 2y) = 0$ passes through exactly 3 lattice points $(0, 0)$, $(1, 0)$, $(2, -2)$.

Choose $t \in \mathbb{Q}$ which satisfies $(*)$, then $H_\lambda : (m + n)\{tx^2 + (1 - t)y^2 - (1 - t)(x + 1) - t(y + 1)\} + 2\sqrt{A}xy = 0$ passes through exactly 4 rational points $(0, -1)$, $\left(0, \frac{1}{1-t}\right)$, $(-1, 0)$, $\left(\frac{1}{t}, 0\right)$. Let $t = P/Q$ $(P, Q \in \mathbb{Z}, P \neq Q)$. Then $1 - t = (Q - P)/Q$. By the similarity transformation $\varphi : (x, y) \mapsto (X, Y) = (P(Q - P)x, P(Q - P)y)$, $\varphi(H_\lambda)$ passes through exactly 4 lattice points $(0, -P(Q - P))$, $(0, PQ)$, $(-P(Q - P), 0)$, $(Q(Q - P), 0)$. □

Remark There exists $t \in \mathbb{Q}$ such that $(*)$ holds. Let $t = 1/k(m + n)$. Then $A = -\frac{1}{k^2}(km - 1)(kn - 1)$. Assume that $m > 0$, $n < 0$, $m + n > 0$. If $k > 2$, then $km - 1 > -kn + 1$. We choose k such that $p := km - 1$ is a prime number. Then $p^2 \not| (km - 1)(kn - 1)$. Hence $\sqrt{A} \notin \mathbb{Q}$.

Corollary 1 *Both* $\mathcal{S}(E_\lambda)$ *and* $\mathcal{S}(H_\lambda)$ *contain* $\{1, 2, 3, 4\}$, *for every* λ. □

Theorem 12 *Suppose that* $a, b, c, d \in \mathbb{Z}$ *satisfy* $ad - bc \neq 0$. *Let* $T = a^2 + b^2 + c^2 + d^2$, $D = (ad - bc)^2$. *If* $\lambda > 0$ *and* $\lambda^2 = \frac{T^2 - 2D - T\sqrt{T^2 - 4D}}{2D}$, *then* $\mathcal{S}(E_\lambda) = \mathbb{N}$ *holds.*

Proof The linear map $f : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ transforms $\mathbb{Z}^2$ to $\Lambda[(a, b), (c, d)]$, bijectively. Since $\Lambda[(a, b), (c, d)]$ is an integral lattice, there exists a circle $C : (X - p)^2 + (Y - q)^2 = r^2$ which passes through exactly n points of the lattice for any $n \in \mathbb{N}$, by Theorem 9. Then $f^{-1}(C) : (ax + cy - p)^2 + (bx + dy - q)^2 = r^2$ is an ellipse which passes through exactly n points of $\mathbb{Z}^2$. The terms of degree 2 of the equation is $(a^2 + b^2)x^2 + 2(ac + bd)xy + (c^2 + d^2)y^2$, and therefore the square of the ratio of the ellipse $f^{-1}(C)$ is equal to $\frac{T^2 - 2D - T\sqrt{T^2 - 4D}}{2D}$. □

Corollary 2 *There exists a* $\lambda > 0$ *such that* $\lambda^2 \in \mathcal{R}\backslash\mathbb{Q}$ *and* $\mathcal{S}(E_\lambda) = \mathbb{N}$.

Proposition 3 (*cf.*[6]) *If positive integer* d *satisfies* $\sqrt{d} \notin \mathbb{Q}$, *then Pell equation* $x^2 - dy^2 = 1$ *has infinitely many integer solutions.* □

Theorem 13 *Let* $\lambda \in \mathbb{Q}$, $\lambda > 0$. *If* $\lambda = 1$, *then* $\infty \in \mathcal{S}(H_\lambda)$. *Otherwise,* $\infty \notin \mathcal{S}(H_\lambda)$.

Proof Since Pell equation $X^2 - 2Y^2 = 1$ has infinitely many integral solutions, so does $(x+y)^2 - 2y^2 = 1$. This equation expresses a hyperbola whose ratio of axes is equal to $\lambda = 1$.

Next, suppose that $\lambda > 0, \lambda \neq 1$ and that H_λ passes through at least 5 lattice points. Then H_λ can be expressed as $H_\lambda : ax^2 + 2hxy + by^2 + 2fx + 2gy + c = 0$, where $a, h, b, f, g, c \in \mathbb{Z}$, by Proposition 1. Let α, β be roots of the characteristic equation of $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$. By a suitable rotation φ, H_λ is transformed to $\varphi(H_\lambda) : \alpha x^2 + \beta y^2 + \gamma x + \delta y + \epsilon = 0$ with $\lambda^2 = -\alpha/\beta$. Since $\lambda \neq 1, a + b \neq 0$ and $\lambda^2 \in \mathbb{Q}$, it follows that $\alpha, \beta \in \mathbb{Q}$. So we can choose integral eigenvectors $\begin{pmatrix} p \\ q \end{pmatrix}, \begin{pmatrix} -q \\ p \end{pmatrix}$ of $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$. Define a linear map $\varphi : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p & -q \\ q & p \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$. Then $\varphi(H_\lambda)$ can be expressed as $(mx - l)^2 - (ny - k)^2 = r\,(m, n, l, k, r \in \mathbb{Z}, r \neq 0)$. Hence $(mx - l + ny - k)(mx - l - ny + k) = r$. Since $r \neq 0$, both factors of the left hand side must be divisors of r. Therefore $\varphi(H_\lambda)$ cannot pass through infinitely many lattice points. Since $\varphi(\mathbb{Z}^2) \subset \mathbb{Z}^2$, we can deduce that $\infty \notin \mathcal{S}(H_\lambda)$. □

To see whether $\infty \in \mathcal{S}(H_\lambda)$ holds or not for $\lambda \notin \mathbb{Q}$, the following lemma is useful.

Lemma 2 *If* $ax^2 - by^2 = c\,(a, b \in \mathbb{N}, \sqrt{ab} \notin \mathbb{Q}, c \in \mathbb{Z})$ *has at least one integer solution, then it has infinitely many integer solutions.*

Proof Let $(x_0, y_0) \in \mathbb{Z}^2$ be an integer solution of the equation. Namely, $(ax_0)^2 - aby_0^2 = ac$. Since $\sqrt{ab} \notin \mathbb{Q}$, Pell equation $x^2 - aby^2 = 1$ has infinitely many integer solutions (cf. [6]). Let $(x_i, y_i) \in \mathbb{Z}^2\,(i = 1, 2, 3, \ldots)$ be the infinitely many solutions. Then $N((ax_0 + \sqrt{ab}y_0)(x_i + \sqrt{ab}y_i)) = ac$, (that is, $a(x_0x_i + by_0y_i)^2 - ab(x_0y_i + y_0x_i)^2 = ac$ holds for every integer i), where $N(\alpha)$ denotes the *norm* of $\alpha \in \mathbb{Z}[\sqrt{ab}]$. Therefore $(ax_0x_i + aby_0y_i, ax_0y_i + y_0x_i) \in \mathbb{Z}^2\,(i = 1, 2, 3, \ldots)$ are infinitely many integer solutions of $ax^2 - by^2 = c$. □

Corollary 3 *If* $\lambda \notin \mathbb{Q}$ *and* $\lambda^2 \in \mathbb{Q}$, *then* $\infty \in \mathcal{S}(H_\lambda)$ *holds.*

Proof Suppose $\lambda \notin \mathbb{Q}$ and $\lambda^2 \in \mathbb{Q}$. Let $\lambda^2 = m/n$. Since $nx^2 - my^2 = n$ has an integer solution $(x, y) = (1, 0)$, by applying Lemma 2, we get $\infty \in \mathcal{S}(H_\lambda)$. □

Theorem 14 *If* $\lambda^2 = \alpha/\beta \in \mathcal{R}\backslash\mathbb{Q}$ *and* $\sqrt{\alpha\beta} \notin \mathbb{Q}$, *then* $\infty \in \mathcal{S}(H_\lambda)$ *holds. Here* λ, α, β, *and* $\mathcal{R}$ *are as in* Definition 3.

Proof Let $H_\lambda : ax^2 + 2hxy + by^2 + px + qy + r = 0$ with $\lambda^2 \in \mathcal{R}\backslash\mathbb{Q}$. Let α, β be eigenvalues of $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$. Then $\lambda^2 = -\alpha/\beta$, and $\alpha\beta = ab - h^2 < 0$. Let

Table 2 The size-set of ellipses and hyperbolas

λ	$\lambda \in \mathbb{Q}$	$\begin{cases}\lambda \notin \mathbb{Q}\\ \lambda^2 \in \mathbb{Q}\end{cases}$	$\lambda^2 \in \mathcal{R}\backslash\mathbb{Q}$	$\lambda^2 \notin \mathcal{R}$
$\mathcal{S}(E_\lambda)$	$\mathbb{N}$	$\mathbb{N}$	(1)	$\{1, 2, 3, 4\}$
$\mathcal{S}(H_\lambda)$	$\begin{cases}\mathbb{N} & (\lambda \neq 1)\\ \mathbb{N} \cup \{\infty\} & (\lambda = 1)\end{cases}$	(2)	(3)	$\{1, 2, 3, 4\}$

$d = -(ab - h^2)$. Applying Lemma 2, the hyperbola $C : -dX^2 + Y^2 = -d + k^2$ passes through infinitely many lattice points. By the transformation $(X, Y) \mapsto (x, y)$: $X = ax + hy$, $Y = dy$, C is transformed to C': $-d(ax + hy)^2 + (dy)^2 = -d + k^2$ and C' passes through infinitely many points of $\left(\frac{1}{ad}\mathbb{Z}\right)^2$. Moreover, the trasformation $(x, y) \mapsto (u, v) = (adx, ady)$ sends C' to C'': $au^2 + 2huv + bv^2 = ad(-d + k^2)$. And C'' passes through infinitely many lattice points. The ratio of axes of the hyperbola C'' is equal to λ and $\infty \in \mathcal{S}(H_\lambda)$. □

Problem 2 Does $\lambda^2 \in \mathcal{R}\backslash\mathbb{Q}$ imply $\infty \in \mathcal{S}(H_\lambda)$?

Theorem 15 *Let* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be a unimodular matrix. Let* λ *be a positive number which satisfies* $\lambda^2 = \frac{s^2+2-s\sqrt{s^2+4}}{2}$ $(s = a^2 - b^2 + c^2 - d^2)$. *Then* $\mathbb{N} \subset \mathcal{S}(H_\lambda)$ *holds.*

Proof By the linear map $f : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$, $\mathbb{Z}^2$ is tranformed to $\mathbb{Z}^2$, bijectively. The hyperbola $C : (X + 1/3)^2 - Y^2 = 7^{n-1}/9$ passes through exactly n points of the lattice for any $n \in \mathbb{N}$, by the proof of Theorem 7. Then $f^{-1}(C)$: $(ax + cy + 1/3)^2 - (bx + dy)^2 = 7^{n-1}/9$ is a hyperbola and the square of the ratio of $f^{-1}(C)$ is equal to $\frac{s^2+2-s\sqrt{s^2+4}}{2}$ $(s = a^2 - b^2 + c^2 - d^2)$. □

Let us summarize the results in Sects. 4 and 5 as follows.

Remark (1), (2), (3) are not decided yet. (1) and (3) contain $\{1, 2, 3, 4\}$. (2) contains $\{1, 2, 3, 4, \infty\}$. We conjecture that $\mathcal{S}(E_\lambda) = \mathbb{N}$ in case (1). *(cf.* Theorem 10, Theorem 12).

Problem 3 Complete the above table by determining (1), (2), (3).

Acknowledgments We thank János Pach for valuable discussions. We would also like to express our gratitude to the referees for pointing out some mistakes.

References

1. Bannai, E., Miezaki, T.: On a property of 2-dimensional integral Euclidean lattices (2011, preprint)
2. Maehara, H., Matsumoto, M.: Is there a circle that passes through a given number of lattice points? Eur. J. Combin. **19**(5), 591–592 (1998)
3. Schinzel, A.: Sur l'existence d'un cercle passant par un nombre donne de points aux coordonnees entieres. Enseignement Math. (2) **4**, 71–72 (1958)

4. Sierpinski, W.: Sur quelques problemes concernant les points aux coordonnees entieres. Enseignement Math. (2) **4**, 25–31 (1958)
5. Steinhaus, H.: One Hundred Problems in Elementary Mathematics. Dover Publications, Inc., New York (1964)
6. Steuding, J.: Diophantine Analysis. Chapman & Hall/CRC, London (2005)