Lattice Points on Algebraic Curves

Thesis Report Submitted in Partial Fulfillment of the Requirement for the Degree of Master of Science in Mathematics

Author: Kim Sokun

Advisor: Takayasu Kuwata

July 01-September 29, 2012
ACKNOWLEDGMENT

In the writing of this thesis, I could reach the step of success depending on the help from my advisor Pro. Takayasu Kuwata, Japan. He always gave me opinion and ideas to think along the way. He introduced me to the excellent books that involved my topic written by THOMAS W. HUNGERFORD, Abstract Algebra An Introduction, RUPP lecture notes, February-March 2012, and other additional material as in the references which are really helps for my thesis.

Special thanks goes to Pro. Michel Jambu (former President of CIMPA) who created and provides funds to sponsor this program, and all professors who gave us very nice lectures at RUPP. The best thanks also goes to my parents, Mr. Kim Ros and Mrs. Khuon Leng, who nursed and supported me.

Finally, I would like to thank H.E Lav Chiv Eav, rector of the Royal University of Phnom Penh (RUPP), Cambodia, for full support in this mathematics program from the beginning to completion.
We 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, proved by Sierpinski. As for plane curves, it is known that the circle satisfies Steinhaus’ condition but doesn’t the parabola. We introduce these and how much is known about ellipses and hyperbolas.

1 Introduction

In 1975, Steinhaus raised the following problem: Does there exist a circular disc in $\mathbb{R}^2$ which contains exactly $n$ lattice points? Where a circular disc is inside of a circle and a lattice point means a point whose coordinates are all integers. Sierpinski solved the problem affirmatively.

**Definition 1.1** 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 $|F_n \cap \mathbb{Z}^2| = n$.

Since all circular disc are similar in shape, the Steinhaus problem can be expressed as whether the circular disc satisfies $SC$ or not. How about algebraic curves in $\mathbb{R}^2$? All lines are similar in shape, and it is easy to see that the line satisfies $SC$ (see Proposition 2.2). 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:

- **Circle** $e = 0$,
- **Ellipses** $0 < e < 1$,
- **Parabola** $e = 1$,
- **Hyperbolas** $1 < e$.

All parabolas are similar in shape. The following theorem is known.
Theorem 1.1 If a parabola passes through five lattice points in $\mathbb{R}^2$, then it contains infinitely many lattice points.

As consequence, the parabola does not satisfy $SC$. Since all circles are similar in shape, the following theorem implies that the circle satisfies $SC$.

Schinzel and Maehara-Matsumoto proved the theorem independently in [1], [3].

Theorem 1.2 For any positive integer $n$, there exists a circle which passes through exactly $n$ lattice points in $\mathbb{R}^2$.

For ellipses and hyperbolas, the lattice point problem is rather complicated. Ellipses and hyperbolas, we use another invariant of similarities. It is the ratio of axis which is defined by $\lambda = (\text{minor axis})/(\text{major axis})$. For example, the ratio $\lambda$ of an ellipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, $(a > 0, b > 0)$ is $\lambda = \min\left\{\frac{b}{a}, \frac{a}{b}\right\}$, the ratio of a hyperbola $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ is $\lambda = \frac{b}{a}$ and the ratio $\lambda$ of a hyperbola $\frac{x^2}{a^2} - \frac{y^2}{b^2} = -1$ is $\lambda = \frac{a}{b}$.

We introduce the following theorem for ellipses and hyperbolas only in the case whose ratios are rational numbers.

Theorem 1.3 For ellipses and hyperbolas with rational ratios of axes, these satisfy $SC$.

This theorem means: Pick any rational number $\lambda$, and fix it. For any positive integer $n$, there exists an ellipse (or a hyperbola) with the ratio $\lambda$ of axis which passes through exactly $n$ lattice points in $\mathbb{R}^2$.

For ellipses and hyperbolas, the lattice points problem has not completed. We write a further direction in the last.
2 Preliminaries

We show the lattice points problems for the circular disc and the line. And we prove a useful lemma for next sections. Sierpinski proved the following proposition, as a consequence the circular disc satisfies \( SC \).

**Proposition 2.1** The distances from lattice points to \( (\sqrt{2}, \frac{1}{3}) \) are all distinct.

Proof: We know \( A(\sqrt{2}, \frac{1}{3}) \) is not a lattice point and the coordinate of \( x = \sqrt{2} \) is irrational number. Let \( P_1(x_1, y_1) \) and \( P_2(x_2, y_2) \) be two different lattice points where \( x_1, x_2, y_1, y_2 \in \mathbb{Z} \). Suppose \( AP_1 = AP_2 \) holds. Then \((x_1 - \sqrt{2})^2 + (y_1 - \frac{1}{3})^2 = (x_2 - \sqrt{2})^2 + (y_2 - \frac{1}{3})^2 \) holds. \((x_1^2 - x_2^2) + (y_1^2 - y_2^2) - 2\sqrt{2}(x_1 - x_2) - \frac{2}{3}(y_1 - y_2) = 0 \). Since \( \sqrt{2} \) is irrational number, then \( x_1 = x_2 \) and \( y_1 = y_2 \). So, \( (x_1, x_2) = (y_1, y_2) \). Therefore the distances from lattice points to \( (\sqrt{2}, \frac{1}{3}) \) are all distinct.

As a consequence, the circular disc satisfies \( SC \).

All lines are similar in shape. The following proposition holds.

**Proposition 2.2** If a line passes through two lattice points in \( \mathbb{R}^2 \), then it contains infinitely many lattice points. As a consequence, the line does not satisfy \( SC \).

Proof: Suppose that a line \( L \) passes through 2 lattice points \( P_1(x_1, y_1) \) and \( P_2(x_2, y_2) \) where \( x_1, x_2, y_1, y_2 \in \mathbb{Z} \). Let \( P_n \) be a point defined by \( \overrightarrow{OP}_n = \overrightarrow{OP}_1 + n\overrightarrow{P_1P_2} = \left( x \begin{array}{c} x - x_1 \end{array}, y \begin{array}{c} y - y_1 \end{array} \right) \) \((n \in \mathbb{Z})\)

Then \( P_n \) is a lattice point on the line \( L \). Hence there are infinitely lattice points on line \( (L) \). ■

Remark: We may assume \( a, b, c \in \mathbb{Z} \)

The following lemma is used in the next section.

**Lemma 2.3** An irreducible conic through five lattice points can be express as: \( a_1x^2 + a_2y^2 + a_3xy + a_4x + a_5y + a_6 = 0 \), \((a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{Z})\)
Proof: Let $C$ be an irreducible conic, then $f(x, y)$ is irreducible in $\mathbb{R}[x, y]$. Suppose $C$ passes through 5 lattice points. Let $(x_1, y_1), (x_2, y_2), \ldots, (x_5, y_5) \in (C \cap \mathbb{Z}^2)$ be such lattice points.

Then the system of equations \( A \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \) holds, where

\[
A = \begin{pmatrix} x_1^2 & y_1^2 & x_1y_1 & x_1 & y_1 & 1 \\ x_2^2 & y_2^2 & x_2y_2 & x_2 & y_2 & 1 \\ x_3^2 & y_3^2 & x_3y_3 & x_3 & y_3 & 1 \\ x_4^2 & y_4^2 & x_4y_4 & x_4 & y_4 & 1 \\ x_5^2 & y_5^2 & x_5y_5 & x_5 & y_5 & 1 \end{pmatrix} \in M_{5, 6}(\mathbb{Q}).
\]

Since the number of the rows of $A$ is 5, then $\text{rank } A \leq 5$. Therefore $(\ast)$ has nontrivial solution in $\mathbb{Q}^6$. So we may assume $a_1, a_2, \ldots, a_6 \in \mathbb{Z}$.

3 Parabola

All parabolas are similar in shape. Theorem 1.1 state that the parabola does not satisfy $SC$.

Proof of Theorem 1.1:
Let $P_1, P_2, \ldots, P_5 \in C$. $C : a_1x^2 + a_2y^2 + a_3xy + a_4x + a_5y + a_6 = 0$, $a_1, a_2, \ldots, a_6 \in \mathbb{Z}$. We may assume one of the five lattice points is the origin.

Suppose $P_5 = O$ then $C$ become $a_1x^2 + a_2y^2 + a_3xy + a_4x + a_5y = 0$, $a_1, a_2, \ldots, a_5 \in \mathbb{Z}$

$a_1(x + a_2y)^2 + a_3x + a_4y = 0$

Let $M, N$ be midpoints of $OP_1, P_2Q$ respectively, where $Q$ is the point on $C$ which satisfies $P_2Q \parallel OP_1$. Then $M, N \in \mathbb{Q}^2$ and there exist $a, b \in \mathbb{Z}$ which satisfy $\begin{pmatrix} a \\ b \end{pmatrix} \parallel \overrightarrow{MN}$.

Let: $\varphi : \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} b & -a \\ a & b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. 

5
Then: \( \varphi^{-1}: \begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{a^2 + b^2} \begin{pmatrix} b & a \\ -a & b \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \).
The symmetric of \( \varphi(C) \) is parallel to \( Y \) axis and so \( \varphi(C) \) can be expressed as \( Y = \tilde{p} X^2 + \tilde{q} X, \) \((\tilde{p}, \tilde{q} \in Q)\). This equation can be written by \( \varphi(C) : pY = qX^2 + rX, \) \((p, q, r \in \mathbb{Z})\).

Choose \( R_n \in \varphi(C) \) which satisfies: \( R_n((a^2 + b^2)p_n, q(a^2 + b^2)p_n^2 + r(a^2 + b^2)n) \).

There are infinitely many lattice points \( R_n \) on \( \varphi(C) \) such that \( \varphi^{-1}(R_n) \in C \cap \mathbb{Z}^2 \).

\( X = (a^2 + b^2)X_0; Y = (a^2 + b^2)Y_0, \) \((X_0, Y_0 \in \mathbb{Z})\) then \( \varphi(C) : p(a^2 + b^2)Y_0 = q(a^2 + b^2)X_0^2 + r(a^2 + b^2)X_0 \) \( pY_0 = q(a^2 + b^2)X_0^2 + rX_0. \) Let \( X_0 = pm, (n \in \mathbb{Z}) \) then \( Y_0 = q(a^2 + b^2)p_n^2 + rn \).

\( \varphi(R_n) = ((a^2 + b^2), (a^2 + b^2)[q(a^2 + b^2)]p_n^2 + rn) \) Since \((a, b, p, q, r \in \mathbb{Z})\) then \( \varphi(R_n) \in C \cap \mathbb{Z}^2 \). Let compute \( \varphi^{-1}(R_n) \).

\[
x = \frac{1}{a^2 + b^2} \left[ b(a^2 + b^2)p_n + a(a^2 + b^2)(q(a^2 + b^2))p_n^2 + rn \right]
\]

\[
y = \frac{1}{a^2 + b^2} \left[ (-a)(a^2 + b^2)p_n + b(a^2 + b^2)(q(a^2 + b^2))p_n^2 + rn \right]
\]

Since \((a, b, p, q, r \in \mathbb{Z})\) then \( x, y \in \mathbb{Z} \).

\[
\therefore \varphi^{-1}(R_n) = \left( bp_n + a[q(a^2 + b^2)p_n^2 + rn], (-a)pn + b[q(a^2 + b^2)p_n^2 + rn] \right) \in C \cap \mathbb{Z}^2.
\]

This theorem implies that the parabola does not satisfies \( SC \). Does there exist a parabola which passes through exactly \( n \) lattice points, for \( n = 1, 2, 3, 4 \) respectively? We answer for the question in the following example.

**Example 3.1** The parabolas \( y = \sqrt{2}x^2, \) \( y = \sqrt{2}(x^2 - x) \) \( (x + \sqrt{2}y)^2 = x + 2y \) and \( [x + (\sqrt{2} - \frac{1}{2})y]^2 = 2x + \frac{5 - 2\sqrt{2}}{2}y \) pass through exactly 1, 2, 3 and 4 lattice points, respectively.

For example, \((x + \sqrt{2}y)^2 = x + 2y \) pass through exactly 3 lattice points \((0, 0), (0, 1) \) and \((1, 0)\). Because \((x + \sqrt{2}y)^2 = x + 2y \) can be express as \( x(x - 1) + 2y(y - 1) + 2\sqrt{2}xy = 0. \) \( 2\sqrt{2} \) is a irrational number then to make expression \( 2\sqrt{2}xy \) equal to zero, \( x \) or \( y \) must be equal to zero or both \( x \) and \( y \) equal to zero. Again, to make \( x(x - 1) \) and \( 2y(y - 1) \) equal to zero \( x, y \) can be equal to 0 or 1. So the possible way to make this expression equal to zero is \( x, y \) must be equal to 0 or 1. The pair of 0 and 1 is \((0, 1) \) and \((1, 0)\). Therefore there is no other lattice points than \((0, 0) \) \( (0, 1) \) \( (1, 0)\).
on \((x + \sqrt{2}y)^2 = x + 2y\). ■

4 Circle

All circles are similar in shape. Theorem 1.2 states that the circle satisfies \(SC\). We first need to prove the following lemma.

**Lemma 4.1** For any nonnegative integer \(k\), the number of integral solutions \((X,Y)\) of the equation

\[
x^2 + y^2 = 5^k
\]

is equal to \(4(k + 1)\).

Proof of Lemma 4.1: Let count instead the number of gaussian integers \(z \in \mathbb{Z}[i]\) which satisfies \(|z|^2 = 5^k\). We assume that \(z \in \mathbb{Z}[i]\) satisfies \(5^k = |z|^2\). If \(k \geq 1\) then since \((1 + 2i)(1 - 2i) = 5\) divides \(z\overline{z} = 5^k\) and since \(1 + 2i, 1 - 2i\) are primes then \(z\) is divisible by \(1 + 2i\) or \(1 - 2i\). So we can write \(z\) as:

\[
z = u(1 + 2i)^s(1 - 2i)^{k-s}
\]

where \(0 \leq s \leq k\) and \(u \in \{\pm 1, \pm i\}\). Since \(\frac{\text{arg}(1+2i)}{\pi}\) is irrational, by varying \(s\) and \(u\) in the expression (2), then we obtain exactly \(4(k+1)\) distinct solution \(z \in \mathbb{Z}[i]\), of the equation \(|z|^2 = 5^k\). ■

Now we prove the following theorem for \(n \geq 0\), there is a circle that passes through exactly \(n\) lattice points in \(\mathbb{R}^2\).

**Proof of Theorem 1.2:** First, in the even case \(n = 2(k+1)\). Consider the circle represented by the equation:

\[
(2x - 1)^2 + (2y)^2 = 5^k
\]

The number of integral solution (3) is equal to the number of integral solution \((X,Y)\) of (1) in which \(X\) is odd. Since such solutions comprise half the solutions of (1), equation (3) has \(2(k+1) = n\) solutions. Hence the circle represented by (3) passes through exactly \(n\) lattice points.

Next, in the odd case \(n = 2l + 1\). Let \(k = 2l\) then since \(5^k = 25^l \equiv 1(\text{mod8})\), any integral solutions \((X,Y)\) of (1) must satisfy either \(X \equiv \pm 1, Y \equiv 0(\text{mod4})\) or \(X \equiv 0, Y \equiv \pm 1(\text{mod4})\).
Now we consider the circle represented by the equation:

\[(4x - 1)^2 + (4y)^2 = 5^k\]  \hspace{1cm} (4)

The number of integral solutions of (4) is equal to the number of integral solutions \((X,Y)\) of (1) such that

\[X \equiv -1(\text{mod} 4).\]  \hspace{1cm} (5)

If \((X,Y) = (A, B)\) is an integral solutions of (1) with \(A \neq 0, B \neq 0\), then \((\pm A, \pm B), (\pm B, \pm A)\) are eight distinct solutions of (1) and just two of them satisfy (5). Otherwise, in the four solutions \((0, \pm 5^l), (\pm 5^l, 0)\) of (1), just \((-5^l, 0)\) satisfy (5). So the number of those integral solutions \((X,Y)\) of (1) that satisfies (5) is equal to:

\[
\frac{4(k+1)-4}{4} + 1 = k + 1
\]

**Example 4.1** Circle \((2x - 1)^2 + (2y)^2 = 1\) passes through exactly 2 lattice points \((0, 0)\) and \((1, 0)\).

Circle \((4x - 1)^2 + (4y)^2 = 5^2\) passes through exactly 3 lattice points \((-1, 0), (1,1)\) and \((1,-1)\).

Circle \((2x - 1)^2 + (2y)^2 = 5\) passes through exactly 4 lattice points \((0,1), (0,-1), (1,1)\) and \((1,-1)\).

Therefore the circle (4) passes through exactly \(k + 1 = n\) lattice points. ■

Remark: \(\mathbb{Z}[i]\) is a unique factorization domain. So the expression (2) is unique up to units. And the set of units in \(\mathbb{Z}[i]\) is equal to \(\{\pm 1, \pm i\}\). It is denoted by \(U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}\).

\section{Ellipses and hyperbolas}

For ellipses and hyperbolas, the ratio \(\lambda = (\text{minor axis})/(\text{major axis})\) is also an invariant under similarity. We denote the ellipse and the hyperbola whose ratio of axes is \(\lambda\) by \(E_\lambda\) and \(H_\lambda\), respectively.
Proof of Theorem 1.3

The case of the ellipse: Suppose $\lambda = \frac{b}{a} \in Q$ ($a, b$ are coprime and $a$ is an odd number). Let $p$ be a prime number such that $p \equiv 1(\text{mod}8)$. Then $(\frac{4x}{a} - 1)^2 + (\frac{4y}{b})^2 = p^{n-1}, x, y \in \mathbb{Z}$ implies $a|x$ and $b|y$.

Let $A := \{(x, y) \in \mathbb{Z}^2 | (\frac{4x}{a} - 1)^2 + (\frac{4y}{b})^2 = p^{n-1}\}$ and $B := \{(X, Y) \in \mathbb{Z}^2 | (4X - 1)^2 + (4Y)^2 = p^{n-1}\}$. Then the map $\Phi := A \rightarrow B$ defined by $(x, y) \mapsto (X, Y) = (\frac{x}{a}, \frac{y}{b})$ is bijective. Since $|B| = n$ holds, we get $|A| = n$. Therefore $E_\lambda$ satisfies $SC$.

The case of hyperbolas: let $\lambda = \frac{b}{a} \in \mathbb{Q}$ ($a, b$ are coprime). Suppose $p$ is a prime number such that $p \equiv 1(\text{mod}6ab)$. Then hyperbola $(3ax + 1)^2 - (3by)^2 = p^{n-1}$ passes through exactly $n$ lattice points. Therefore $H_\lambda$ satisfies $SC$. ■

Let $\mathcal{R} := \{|\frac{\alpha}{\beta}| \alpha$ and $\beta$ are eigenvalues of $\begin{pmatrix} a & h \\ h & b \end{pmatrix} \in GL(2, \mathbb{Q})\}$. It is known that $E_\lambda$ (or $H_\lambda$) with $\lambda^2 \notin \mathcal{R}$ does not satisfy $SC$ (cf.[2]). And the case of $E_\lambda$ (or $H_\lambda$) with $\lambda^2 \in \mathbb{R} \setminus \mathbb{Q}$ is open.
Reference


