# Lattice Point Geometry: Pick's Theorem and Minkowski's Theorem

Senior Exercise in Mathematics

Jennifer Garbett
Kenyon College

November 18, 2010

# Contents

# 1 Introduction

Informally, a lattice is a "set of isolated points", one of which is the origin, and this "point set... looks the same no matter from which of its points you observe it" [8]. The study of lattices is interesting on its own and has lead to solutions to problems in other branches of mathematics.

Our main goal here will be to discuss two theorems based in lattice point geometry, Pick's Theorem and Minkowski's Theorem. Both theorems allow us to describe the relationships between the area of a polygon in the plane and the number of lattice points the polygon contains, both extend to higher dimensions, and both have important applications, ranging from solutions to applied problems to proofs of important theorems in number theory.

Let $L$ be a lattice and let $P$ be a polygon in the plane with its vertices at points in $L$. Pick's Theorem allows us to determine the area of $P$ based on the number of lattice points, points in $L$, living inside $P$ and the number of lattice points living on the boundary of $P$. Minkowski's Theorem allows us to go in the other direction. Let $R$ be a region in $\mathbb{R}^2$. Minkowski's Theorem guarantees $R$ contains a lattice point if $R$ satisfies a set of requirements set forth by the theorem.

We will discuss Pick's Theorem and Minkowski's Theorem more after a brief introduction to lattices. We will then give an overview of the steps we will need to take to prove Pick's Theorem and Minkowski's Theorem. We will follow this introductory material with the bulk of the paper, a detailed discussion of the results required to prove Pick's Theorem and Minkowski's Theorem as well as a discussion of the consequences of these two theorems.

Before we get into the details of the main theorems of the paper, we need to address the definition of a lattice in more detail. First, we give a more formal definition of a lattice [8]:

**Definition 1.1.** A set, $L$, of points in $\mathbb{R}^n$ is a *lattice* if it satisfies the following conditions:

1. $L$ is a group under vector addition.
2. Each point in $L$ is the center of a ball that contains no other points of $L$.

What exactly does this formal definition mean geometrically? How does this definition relate to our informal definition? Consider the three graphs in Figure 1.
The two graphs on the left are both graphs of lattices. Both are sets of isolated points, and for both, the points around any particular point look the same as the points around any other point. The graph on the right is not a lattice. We shall discuss the reasons why the set shown in this right-most graph is not a lattice, and in doing so, we will show how the informal definition and the formal definition of a lattice are related.

Let $S$ be the set of points in the graph on the right of Figure 1. We will now give several reasons why $S$ is not a lattice. First, notice the line in $S$. Since $S$ contains this line, $S$ is not a set of isolated points, and $S$ does not satisfy condition two of our formal definition.

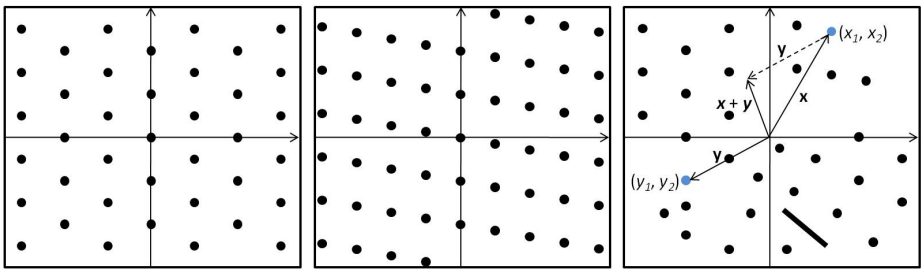


Figure 1: The two sets graphed on the left and in the center are lattices, while the graph on the right is not.

To see why, choose a point on the line. There is no ball centered at this point that contains no other point in $S$.

Next, we'll investigate the relationship between condition 1 of our formal definition and the other part of our informal definition. By the informal definition, if $S$ is a lattice, the set of points around any point in $S$ should look the same as the set of points around any other point in $S$. However, $S$ does not meet this requirement, as the points in $S$ around the point $(x_1, x_2)$ do not look the same as the points in $S$ around the point $(y_1, y_2)$. This violation of the last requirement of our informal definition is also a violation of condition 1 of the formal definition. To see why this is the case, we must investigate condition 1 further.

According to condition 1, to be a lattice, the set $S$ must be a group under vector addition [8], that is, $S$ must satisfy the following conditions [5]:

(a) $S$ is closed under vector addition.

(b) Vector addition is associative in $S$.

(c) $S$ contains an identity element.

(d) $S$ contains an inverse element for each element of $S$.

Let $(x_1, x_2)$ and $(y_1, y_2)$ be points in $S$, and let $\mathbf{x}$ and $\mathbf{y}$ be the vectors which originate at the origin with endpoints at $(x_1, x_2)$ and $(y_1, y_2)$ respectively. Condition (a) requires addition of the vectors $\mathbf{x}$ and $\mathbf{y}$ to yield a vector whose endpoint is in $S$. However, from the graph of the points in $S$ (Figure 1), we see this is not the case. The fact that $S$ is not closed under vector addition is another reason why $S$ is not a lattice. Condition (b) is automatically satisfied since vector addition is always associative. By condition (c), for $S$ to be a lattice, $S$ must contain an identity element, $\mathbf{e}$ such that $\mathbf{e} + \mathbf{v} = \mathbf{v}$ for all vectors $\mathbf{v}$ with endpoints in $S$. However, under vector addition, the zero vector is the identity element. Since $S$ does not contain the origin, $S$ contains no identity element. In general, as stated in the informal definition, a lattice must contain the origin, giving us another reason why $S$ is not a lattice. Condition (d) requires that $S$ contain an inverse element. This

is impossible since $S$ contains no identity element. Had $S$ contained an identity element, the origin, we would need to check whether for every point $p$ in $S$, $-p$ is in $S$. We would need $S$ to satisfy this condition because the inverse of a point $p$ under vector addition is $-p$ since $\mathbf{p} - \mathbf{p} = 0$ where $\mathbf{p}$ is the vector emanating from the origin with endpoint $p$. Since $S$ doesn't contain an inverse for every point in $S$, $S$ violates all of the conditions set out in our formal definition of a lattice other than part (b) of condition one. A set is not a lattice if it violates even one of the conditions or subconditions set forth in our formal definition. Only a set of points that satisfies all of the conditions of our formal definition is a lattice, and the sets plotted in the two graphs on the left of Figure 1 do satisfy all of these conditions and are therefore lattices.

From the definition of a lattice, it is clear that several examples of lattices exist. Here we define a specific type of lattice, the integer lattice:

**Definition 1.2.** A point $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ is an *integer point* if $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. The *integer lattice*, $\mathbb{Z}^n$, is the set of integer points in $\mathbb{R}^n$.

In this paper, much of our discussion will revolve around the two dimensional integer lattice, $\mathbb{Z}^2$.

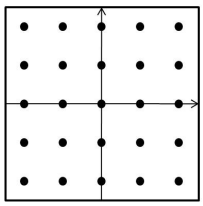

Figure 2: The Integer Lattice, $\mathbb{Z}^2$

Therefore, throughout our discussion, when we refer to a lattice, we mean the integer lattice unless otherwise noted.

Now that we have some basic definitions in hand, we can discuss our main goals for this paper in more depth. First, we'll address Pick's Theorem. Consider a polygon $P$ whose vertices lie at lattice points. As mentioned above, Pick's Theorem allows us to determine the area of $P$ from the number of lattice points on the boundary of $P$, $B(P)$, and the number of lattice points in the interior of $P$, $I(P)$. More specifically, Pick's Theorem states the following,

**Theorem (Pick's Theorem).** *Let $P$ be a polygon in the plane with its vertices at lattice point. Then the area of $P$, $A(P)$, is given by*

$$A(P) = \frac{1}{2}B(P) + I(P) - 1$$

*where $B(P)$ is the number of lattice points on the boundary of $P$ and $I(P)$ is the number of lattice points in the interior of $P$.*

To prove Pick's Theorem, we'll first divide the polygon $P$ into triangles each with area $\frac{1}{2}$; proving that this is possible will complete much of the preliminary work necessary to prove Pick's Theorem. Then, we will introduce some basic definitions and establish a few facts from graph theory. This knowledge of some elementary graph theory will allow us to treat the polygon, $P$, which we divided into triangles of area $\frac{1}{2}$, as a graph. Doing so will allow us to determine how many triangles with area $\frac{1}{2}$ $P$ contains in terms of $B(P)$ and $I(P)$. After we accomplish all of these tasks, we will be able to derive the formula given by Pick's Theorem for the area of $P$.

There are several extensions of Pick's Theorem in the plane. We will discuss a few of these extensions in detail. Those we will discuss in detail include the following. First, we will discuss a version of Pick's Theorem for polygons containing holes (we will see that Pick's Theorem does not apply to polygons containing holes)[9]. Next, we will discuss a version of Pick's Theorem that allows us to determine the number of lattice points in a polygon $kP = \{kx | x \in P\}$, where $P$ is a lattice polygon, for all positive integers $k$ [6]. Finally, we will discuss a version of Pick's Theorem that allows us to find an upper bound for the number of lattice points in a non-polygonal region in $\mathbb{R}^2$ [6]. To discuss this last extension of Pick's Theorem, we will need to discuss convexity in $\mathbb{R}^2$. This discussion of convexity in the plane will lead us to the next major topic of the paper, Minkowski's Theorem.

While our final extension of Pick's Theorem will give us an upper bound on the number of lattice points in a region in $\mathbb{R}^2$, Minkowski's Theorem will allow us to determine whether we are guaranteed to find more than one lattice point in a region in $\mathbb{R}^2$. Minkowski's Theorem is as follows,

**Theorem (Minkowski's Theorem).** *Let $R$ be a bounded, convex region in $\mathbb{R}^2$ having area greater than 4 that is symmetric about the origin. Then $R$ contains an integer point other than the origin.*

We will discuss Minkowski's Theorem and its requirements (convexity, symmetry, etc.) in sections 4 and 5. If Minkowski's Theorem guarantees the existence of a lattice point in a region $R$ besides the origin, then we have a lower bound of two for the number of lattice points in $R$. Thus, both Pick's Theorem and Minkowski's Theorem give us information about regions in the plane based on numbers we can find easily, such as the number of lattice points in the interior of the region, the number of lattice points on the boundary of the region, the area of the region, or the perimeter of the region. We now give a brief overview of Minkowski's Theorem.

We won't need many new results to prove Minkowski's Theorem. First we'll prove Blichfeldt's lemma which guarantees any bounded set in $\mathbb{R}^2$ with area greater than 1 will contain two distinct points whose difference under vector addition is an integer point. We will use this result to show a larger region, a region that satisfies the requirements of Minkowski's Theorem, must contain an integer point.

As we will do for Pick's Theorem, we will also discuss some of the many extensions of Minkowski's Theorem; we'll also discuss a couple of applications of Minkowski's Theorem. First, we will discuss Minkowski's Theorem in lattices other than the integer lattice [2].

Next we'll discuss two applications of Minkwoski's Theorem. As mentioned previously, Minkowski's Theorem can be used in the proofs of some important theorems in number theory. We will discuss and prove one such theorem, the Two Squares Theorem, for a particular case. The Two Squares Theorem tells us which integers can be written as a sum of two squares and which cannot [2]. We will use Minkowski's Theorem to show which primes can be written as a sum of two squares, proving the Two Squares Theorem for prime numbers. Minkowski's Theorem can also be used in solving the Orchard Problem, an applied problem involving a circular orchard of trees planted at lattice points [3]. We will conclude our discussion of Minkowski's Theorem with a proof of an extension of Minkowski's Theorem to regions in $\mathbb{R}^n$ followed by a brief discussion of a few important applications of Minkowski's Theorem in $\mathbb{R}^n$. Throughout the paper, all theorems, definitions, proofs, etc. are adapted from [6] unless otherwise noted.

# 2 Primitive Lattice Triangles

As mentioned above, our proof of Pick's theorem will hinge on the fact that every polygon with its vertices at lattice points can be divided into triangles. Each triangle has all three of its vertices at lattice points and has area $\frac{1}{2}$. Once we complete this section, we will have shown we can divide any polygon $P$, with all of its vertices at lattice points, into triangles all of the same known area, $\frac{1}{2}$.

## 2.1 Triangulation of a Lattice Polygon with Lattice Triangles

Up to now, we've simply said Pick's Theorem will give us a way to determine the area of a polygon with its vertices at lattice points. Before we proceed further, we clarify the specific characteristics a polygon must have for the formula given in Pick's Theorem to determine its area. To use Pick's Theorem to determine the area of a polygon, $P$, $P$ must be a simple lattice polygon.

**Definition 2.1.** A *simple polygon*, $P$, is a polygon whose boundary is a simple closed curve, that is, $P$ contains no holes, and the boundary of $P$ never intersects itself [9]. A *lattice polygon* is a polygon, not necessarily simple, with all its vertices at lattice points. A *simple lattice polygon* is a simple polygon with all its vertices at lattice points.

These definitions give rise to a few issues regarding notation. When we refer to a lattice polygon, we assume it is a simple lattice polygon unless noted otherwise. Also, we refer to a polygon $P$ with $k$ vertices as a $k$-gon,

Our first step towards a proof of Pick's theorem is to show we can dissect any lattice polygon into lattice triangles.

**Definition 2.2.** We call the dissection of a polygon $P$ into triangles a *triangulation* of $P$.

To show we can triangulate any polygon, $P$, even if $P$ is non-simple, we'll first need to show that $P$ must have a diagonal.

**Definition 2.3.** Let $P$ be a polygon which need not be simple. Let $l$ be a line segment contained in $P$ that joins two non-adjacent vertices of $P$. If $l$ does not contain any vertex of $P$ other than the two it connects, then the line segment $l$ is a *diagonal* of $P$.

**Lemma 2.4.** *Every polygon, $P$, where $P$ need not be a simple lattice polygon, has a diagonal.*

*Proof.* Let $P$ be a polygon having $k$ vertices, and graph the polygon $P$ in $\mathbb{R}^2$. Call the vertices of $P$ $(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$. Let $l$ be the line $y = \min\{y_i | 1 \leq i \leq k\}$. Then no vertex of $P$ lies below $l$. Choose a vertex of $P$ that lies on $l$, and call it $A$. Let $B$ and $C$ be the vertices of $P$ adjacent to $A$. We must consider three cases (see Figure 3).

1. Assume the line segment $\overline{BC}$ is a diagonal of $P$. Then $P$ has a diagonal and we're done (see Figure 3).

2. Assume some vertex of $P$ lies on $\overline{BC}$, but no vertex of $P$ lies inside $\triangle ABC$. Choose a vertex of $P$ on $\overline{BC}$ and call it $V$. Then $\overline{AV}$ is a diagonal of $P$ (see Figure 3).

3. Assume some vertex of $P$ lies inside $\triangle ABC$. Choose a vertex of $P$ that lies inside $\triangle ABC$, and call it $V$. Draw a line segment, $s$ with one endpoint at $A$ and the other on $\overline{BC}$ that passes through $V$. If $V$ is the only vertex of $P$ on $s$, then $\overline{AV}$ is a diagonal of $P$. If there is more than one vertex of $P$ on $s$, let $X$ be the one that lies closest to $A$. Then $\overline{AX}$ is a diagonal of $P$ (see Figure 3).

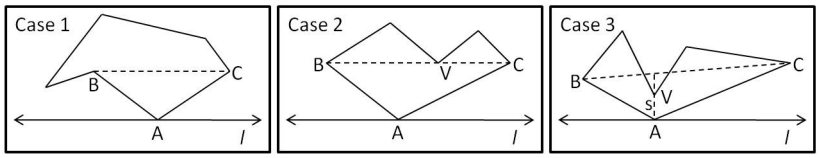


Figure 3: Case 1: $\overline{BC}$ is a diagonal of $P$. Case 2: A vertex of $P$ lies on $\overline{BC}$. Case 3: A vertex of $P$ lies inside $\triangle ABC$

Thus, every polygon, $P$ must have a diagonal.

□

Given this result, proving any polygon, $P$, can be dissected into triangles each of which has vertices that are vertices of $P$ becomes a simple exercise in mathematical induction.

**Theorem 2.5.** *Every $k$-gon, $P_k$, can be dissected into $k-2$ triangles, each of which has vertices that are vertices of $P_k$, by means of nonintersecting diagonals.*

*Proof.* We proceed by complete induction on $k$. Since $P_k$ is not a polygon when $k < 3$, we consider $k \geq 3$. For the base case, assume $k = 3$. Since $P_3$ is a triangle, the theorem is true when $k = 3$. Let $k > 3$ and assume all polygons with $k$ vertices or less satisfy the theorem. We must show a polygon with $k + 1$ vertices satisfies the theorem.

By Lemma 2.4, $P_{k+1}$ must have a diagonal, $d$. The diagonal $d$ splits $P_{k+1}$ into two smaller polygons, $P_m$ which has $m$ vertices and $P_n$ which has $n$ vertices (see figure 4). Since each of the two smaller polygons, $P_m$ and $P_n$, contains the endpoints of $d$ as two of its vertices, $m+n$ gives us two more than number of vertices of $P_{k+1}$, that is, $m+n=(k+1)+2$. Since $3 \leq m \leq k$ and $3 \leq n \leq k$, by our induction hypothesis, $P_m$ and $P_n$ satisfy the theorem; they can be dissected into $m-2$ and $n-2$ triangles, respectively. Each vertex of each triangle lies at a vertex of $P$. Since the diagonals of $P_m$ must be inside $P_m$, the diagonals of $P_n$ must be inside $P_n$, and $P_m$ and $P_n$ are disjoint and separated by $d$, no diagonal of $P_m$ or $P_n$ intersects $d$. Therefore, the nonintersecting diagonals of $P_m$, the nonintersecting diagonals of $P_n$, and $d$ dissect $P_{k+1}$ into $(m-2)+(n-2)=(m+n)-4=((k+1)+2)-4=(k+1)-2$ triangles as stated in the theorem. Thus, every $k$-gon can be dissected into $k-2$ triangles as stated by the theorem.

□

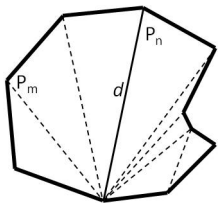


Figure 4: The polygon $P_{k+1}$ is divided by a diagonal, $d$, into two smaller polygons, $P_m$ and $P_n$, each of which can be triangulated (dotted lines) as in the theorem.

We've shown any polygon, $P$, can be triangulated with triangles each of which has vertices that are vertices of $P$. If $P$ is a lattice polygon, all of its vertices are at lattice points. Since we can triangulate $P$ with triangles whose vertices are at vertices of $P$, all of the vertices of the triangles with which we triangulate $P$ are at lattice points. Thus, Corollary **??** follows directly from Theorem 2.5.

**Corollary 2.6.** *Every lattice polygon, $P$ can be dissected into lattice triangles whose vertices are vertices of $P$.*

Corollary 2.6 allows us to triangulate any lattice polygon with lattice triangles. However, to prove Pick's theorem, we'll need a stronger result; as mentioned before, we need to show any lattice polygon can be triangulated with triangles each of which has an area of $\frac{1}{2}$.

## 2.2 Triangulation of a Lattice Polygon with Primitive Lattice Triangles

In this section we will show we can triangulate a lattice polygon with a particular type of triangle, a primitive lattice triangle.

**Definition 2.7.** A *primitive lattice polygon* is a lattice polygon with no lattice points in its interior and with no lattice points on its sides other than its vertices.

In this section, we are concerned with primitive lattice triangles. A primitive lattice triangle is a triangle with no lattice points in its interior and with no lattice points on its sides other than its vertices. We will defer showing the area of a primitive triangle must be $\frac{1}{2}$ to the following sections. Here, we show triangulation with primitive lattice triangles is possible.

**Theorem 2.8.** *Every lattice polygon can be dissected into primitive lattice triangles.*

*Proof.* Let $P$ be a lattice polygon. By Corollary 2.6 we can triangulate $P$ with lattice triangles. Therefore, it is sufficient to show a lattice triangle can be triangulated with primitive lattice triangles. Let $T_r = \triangle ABC$ be a lattice triangle with a finite number, $r \geq 0$, of lattice points in its interior. If $T_r$ is primitive, then we're done. Assume $T_r$ is not primitive. We proceed by complete induction on $r$. We have two base cases.

First, let $r = 0$. Since there are no lattice points inside $T_0$ and $T_0$ is not primitive, there must be at least one lattice point on the boundary of $T_0$. Without loss of generality, assume that this lattice point, or at least one lattice point if there are multiple lattice points on the boundary of $T_0$, lies on $\overline{AB}$. Call the lattice points on $\overline{AB}$ $X_1, X_2, \ldots, X_k$. The line segments $\overline{CX_1}, \overline{CX_2}, \ldots, \overline{CX_k}$ dissect $T_0$ into triangles. Since there are no lattice points inside $T_0$, all of the triangles formed by $\overline{CX_1}, \overline{CX_2}, \ldots, \overline{CX_k}$ are primitive except possibly $\triangle ACX_1$ and $\triangle CBX_k$. Assume there are no lattice points on $\overline{AC}$ and there are no lattice points on $\overline{CB}$. Then $\triangle ACX_1$ and $\triangle CBX_k$ are primitive, and we're done. Assume there are lattice points $Y_1, Y_2, \ldots, Y_m$ on $\overline{AC}$. Since $T_0$ contains no interior lattice points, $\triangle ACX_1$ contains no interior lattice points, and therefore, the line segments $\overline{X_1Y_1}, \overline{X_1Y_2}, \ldots, \overline{X_1Y_m}$ divide $\triangle ACX_1$ into primitive lattice triangles. The same argument holds when there are lattice points on $\overline{CB}$. Thus, $T_0$ can be triangulated with primitive lattice triangles (see Figure 5).

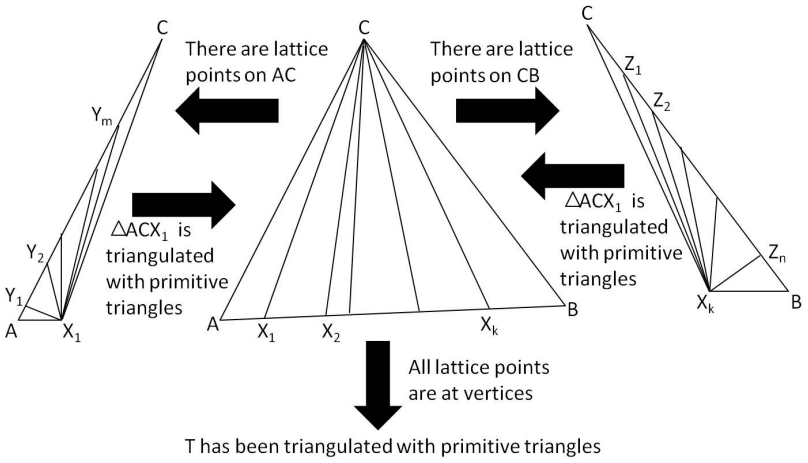


Figure 5: A triangulation of $T_0$ with primitive triangles

Assume $r = 1$. Let $V$ be the interior lattice point of $T_1$. The line segments $\overline{AV}, \overline{BV}$, and $\overline{CV}$ divide $T_1$ into three lattice triangles. For each of triangle, $\triangle AVC$, $\triangle VBC$, and $\triangle ABV$, $r = 0$. We showed above that we can dissect a lattice triangle for which $r = 0$ into primitive lattice triangles. Therefore, $T_1$ can be triangulated with primitive lattice triangles when $r = 1$ (see Figure 6).

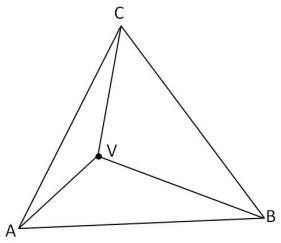


Figure 6: $T_1$

Now, let $r > 1$ and assume $T$ can be triangulated with primitive lattice triangles when the number of lattice points in $T$ is less than or equal to $r$. We must show $T_{r+1}$ can be triangulated with primitive lattice triangles. Choose an interior lattice point of $T_{r+1}$ and call it $V$. The line segments $\overline{AV}, \overline{BV}$, and $\overline{CV}$ dissect $T$ into three lattice triangles, $\triangle AVC, \triangle VBC$, and $\triangle ABV$, each with $r$ or fewer interior lattice points. By our induction hypothesis, $\triangle AVC, \triangle VBC$, and $\triangle ABV$ can be dissected into primitive lattice triangles. Therefore, $T$ can be triangulated by primitive lattice triangles when $T$ contains $r+1$ interior lattice points (see Figure 7). Thus, any lattice triangle $T$ can be triangulated with primitive lattice triangles, and hence, any lattice polygon can be triangulated with primitive lattice triangles.

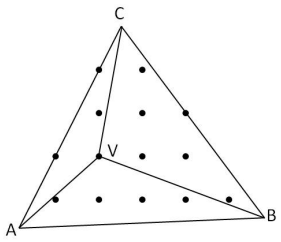


Figure 7: $T_{r+1}$

□

Our next step in preparing to prove Pick's Theorem will be to show the area of any primitive lattice triangle in $\mathbb{Z}^2$ is $\frac{1}{2}$. To show the area of a primitive triangle is $\frac{1}{2}$, we'll need to discuss visible points, plane isometries, and the area of a primitive parallelogram, which we'll do in the next few sections.

## 2.3 Visible Points

We'll begin by discussing visible points. A visible point is the lattice point we would see if we stood at the origin and looked in a particular direction. Visible points will be important in section 2.5 when we utilize certain characteristics of visible points and plane isometries, which are discussed in section 2.4 to show the area of a primitive parallelogram is 1. We define visible point more formally as follows.

**Definition 2.9.** A *lattice line* is a line that passes through at least two lattice points. A *lattice line segment* is a line segment with endpoints at lattice points. Let $l$ be a lattice line through the origin. Then the *visible points* on $l$ are the two non-zero lattice points on $l$ that have minimum positive distance to the origin.

For example, consider the graph in Figure 8. The lattice points $(2, 1)$ and $(-2, -1)$ are visible points on the line $y = \frac{1}{2}x$ since $d((2, 1), (0, 0)) = d((-2, -1), (0, 0)) = \sqrt{5} \leq d((x, y), (0, 0))$ for all other points, $(x, y)$ on the line $y = \frac{1}{2}x$.

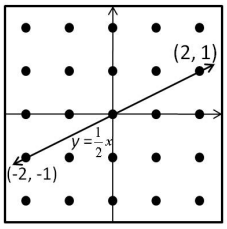


Figure 8: The lattice line $y = \frac{1}{2}x$ and its visible points

As it turns out, for any lattice point $(m, n)$, the value of the greatest common divisor of $m$ and $n$ allows us to determine whether or not $(m, n)$ is a visible point.

**Definition 2.10.** Two non-zero integers $m$ and $n$ are *relatively prime* if the greatest common divisor of $m$ and $n$ ($\gcd(m, n)$)is 1.

We'll need two lemmas to prove the following theorem about the coordinates of a visible lattice point. Both appear in [5]. A proof for the first lemma can be found in [5], and we'll prove the second here.

**Lemma 2.11.** *If $m$ and $n$ are integers, then $\gcd(m, n)$ is a linear combination of $m$ and $n$, that is, we can find integers $s$ and $t$ so that $\gcd(m, n) = sm + tn$.*

**Lemma 2.12.** *Let $k$, $m$, and $n$ be integers. If $n$ and $k$ are relatively prime and if $n|km$, then $n|m$.*

*Proof.* Let $k$, $m$, and $n$ be integers, and assume that $n$ and $k$ are relatively prime, that is, $\gcd(k, n) = 1$. Also assume that $n|km$. Since $n|km$, $km = nd$ for some integer $d$. Since $\gcd(k, n) = 1$, by Lemma 2.11, there are integers $s$ and $t$ such that $1 = sn + tk$. Thus,

$$\begin{aligned} m &= m(sn+tk) \\ &= smn+tkm \\ &= smn+tnd \\ &= n(sm+td). \end{aligned}$$

Since $s$, $m$, $t$, and $d$ are all integers, $sm+td$ is an integer, so $n|m$.

□

**Theorem 2.13.** *A lattice point $p=(m,n)$ is visible if and only if $m$ and $n$ are relatively prime.*

*Proof.* We must show two implications.

($\Longrightarrow$) Let $p=(m,n)$ be a visible point, and let $s$ be a the lattice line segment with endpoints at the origin and $p$. Then there is no lattice point on $s$ other than its endpoints. Assume $m$ and $n$ are not relatively prime, that is, $\gcd(m,n)=k>1$. It follows that $\frac{m}{k}$ and $\frac{n}{k}$ are integers, and since $s$ is a segment of the lattice line $y=\frac{n}{m}x$, the lattice point $(\frac{m}{k},\frac{n}{k})$ lies on $s$. This means the point $(\frac{m}{k},\frac{n}{k})$ lies between the point $p$ and the origin, contradicting the fact that $(m,n)$ is a visible point. Thus, $\gcd(m,n)=1$, and therefore, $m$ and $n$ are relatively prime.

($\Longleftarrow$) Assume $m$ and $n$ are relatively prime, that is, $\gcd(m,n)=1$. Let $s$ be the lattice line segment with endpoints at $(0,0)$ and $p=(m,n)$. Let $q=(m',n')$ be a non-zero lattice point on $s$. To show $p$ is visible, we must show $q=p$. We do so by considering three cases.

1. Assume $m'=0$. Then $s$ must be a vertical line. This means $p=(0,n)$. Since $\gcd(m,n)=1$, $n=1$, and since $q$ is a non-zero lattice point on $s$, $n'=1$. Thus, $q=p$.
2. Assume $n'=0$. Then $s$ must be a horizontal line. This means $p=(m,0)$. Since $\gcd(m,n)=1$, $m=1$, and since $q$ is a non-zero lattice point on $s$, $m'=1$. Thus, $q=p$.
3. Now assume that $m'\neq 0$ and $n'\neq 0$. Since $p$ and $q$ both lie on $s$, the slope of $s$ is $\frac{n}{m}=\frac{n'}{m'}$. Since $\frac{n}{m}=\frac{n'}{m'}$, $mn'=m'n$, and thus, $m|m'n$. By Lemma 2.12, since $m|m'n$ and since $m$ and $n$ are relatively prime, $m|m'$. Similarly, $mn'=m'n \Longrightarrow n|mn'$. Also by Lemma 2.12, $n|n'$. Since $q$ is on the line segment $s$, it must be the case that $|m'|\leq|m|$ and $|n'|\leq|n|$. Therefore, since $m',n'\in\mathbb{Z}$, $m'=m$ and $n'=n$. Thus, $q=p$.

□

This relationship between the greatest common divisor of the coordinates of a point and whether or not the point is a visible point will be necessary in the steps leading up to showing the area of a primitive lattice triangle is $\frac{1}{2}$. As mentioned above, we will combine the result of Theorem 2.13 with characteristics of plane isometries to show the area of a primitive lattice parallelogram is 1.

## 2.4 Plane Isometry

The information about plane isometries presented here is from [5]. An understanding of plane isometries will allow us to employ functions to move lattice polygons within a lattice while ensuring the area of the polygon does not change. This is important since we are interested in the areas of lattice polygons, and it is often easier to calculate the area of a polygon when we know its location in the plane.

**Definition 2.14.** A *plane isometry* is a distance preserving function $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$. That is, for all points $x = (x_1, x_2)$ and $y = (y_1, y_2)$ in $\mathbb{R}^2$, $||\varphi(x) - \varphi(y)|| = ||x - y||$ where $||x - y||$ is the Euclidean distance between the points $x$ and $y$.

We will not prove it here, but it is also the case that plane isometries preserve angles. Since under some plane isometry $\varphi$, the angles of a lattice polygon $P$ will remain the same, and the sides of $P$ will remain the same length, the area of $P$ is preserved under $\varphi$.

Translation and rotation are the two plane isometries we will utilize in this paper. We will need a translation to show the area of a primitive lattice parallelogram is 1 and a rotation to show the area of a primitive lattice triangle is $\frac{1}{2}$. Fortunately, the image of a lattice polygon, $P$, under any translation, $T$, by a lattice point is also a lattice polygon. This is because, as stated in our formal definition of a lattice, a lattice is a group under vector addition. Thus, every lattice is closed under vector addition, and every lattice point i.e. every vertex of $P$ will be mapped to a lattice point under $T$.

## 2.5 Primitive Parallelograms

Now, we can use our result about visible points and the area preserving properties of plane isometries to show the area of a primitive parallelogram is 1. Recall that a primitive polygon is a lattice polygon with no lattice points in its interior and no lattice points on its boundary other than its vertices. Therefore, a primitive parallelogram is simply a parallelogram with no lattice points in its interior and with no lattice points on its boundary other than its vertices. Showing the area of any primitive parallelogram is 1 will bring us one step closer to showing the area of a primitive triangle is $\frac{1}{2}$. The proof that follows is adapted from [1].

**Proposition 2.15.** *A primitive parallelogram has area 1.*

*Proof.* Let $P$ be a primitive parallelogram. Since translation is a plane isometry, we can translate $P$ to any part of the plane without changing its area. Therefore, we can assume under under an appropriate translation $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, the lower left vertex of $P$ lies at

the origin, the lower right and upper left vertices of $P$ lie at $A = (m, n)$ and $B = (i, j)$ respectively, and the upper right vertex of $P$ lies at the point $A + B = (m + i, n + j)$ (see Figure 9).

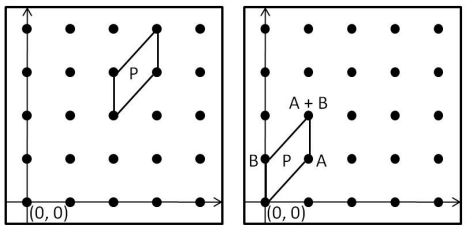


Figure 9: Left: A graph of a primitive parallelogram, $P$. Right: The image of $P$ after its lower left vertex has been translated to the origin by the function $\varphi$.

Since lattices are closed under vector addition, the non-lattice points on the lattice line segment with endpoints $\varphi^{-1}((0, 0))$ and $\varphi^{-1}(A)$ all map to non-lattice points. Therefore, since $P$ is primitive, there are no lattice points on the lattice line segment between the origin and $A$. This means $A$ is a visible point, and by Proposition 2.13, $m$ and $n$ are relatively prime, and $\gcd(m, n) = 1$. By Lemma 2.11, there are integers $p$ and $q$ that satisfy the equation $mp + nq = 1$. Choose such integers $p$ and $q$.

Consider the matrix

$$M = \begin{bmatrix} p & q \\ -n & m \end{bmatrix}.$$

Note that $M$ has integer entries. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear transformation given by $T(\mathbf{x}) = M\mathbf{x}$ for all vectors $\mathbf{x}$ each emanating from the origin with an integer point as its endpoint. Since $\det(M) = 1$, the image of $P$ under $T$ has the same area as $P$. This means we can determine the area of $P$ by determining the area of the image of $P$ under $T$. The bottom left vertex of $T(P)$ is the origin, the top left vertex is $(pi + qj, -ni + mj)$, the bottom right vertex is $(1, 0)$, and the top right vertex is $(pi + qj + 1, -ni + mj)$ (see Figure 10). Let $u = pi + qj$ and let $v = -ni + mj$. Then the vertices of $T(P)$ are $T((0, 0)) = (0, 0), T(B) = (u, v), T(A) = (1, 0)$, and $T(A + B) = (u + 1, v)$ (Figure 10). If $v = 0$, then four vertices of $T(P)$ are collinear and $T(P)$ is not a parallelogram, so we can assume $|v| \geq 1$.

Assume $|v| > 1$, and assume $v$ is positive. Then two sides of $T(P)$ both pass through the line $y = 1$ at non-lattice points, $p_1$ and $p_2$, that are 1 unit apart ($p_1$ and $p_2$ are marked with red arrows in Figure 11). The points $p_1$ and $p_2$ both lie on the lattice line $y = 1$, and each lattice point on the line $y = 1$ is a distance of 1 from each of the two neighboring lattice points on the line $y = 1$. Since $p_1$ and $p_2$ are not lattice points, but the distance between $p_1$ and $p_2$ is 1, there must be a lattice point on the line $y = 1$ between $p_1$ and $p_2$. As shown in Figure 11, this means the polygon $T(P)$ has an interior lattice point. This interior lattice point contradicts the fact that $T(P)$ is a primitive lattice parallelogram. A

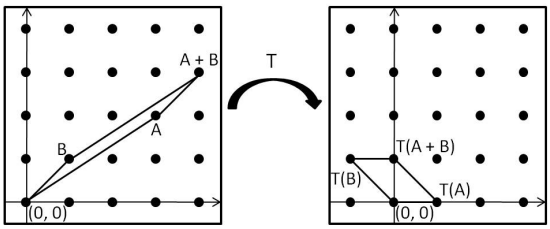


Figure 10: A parallelogram (left) and its image under the linear transformation $T$ (right).

similar argument holds true when $|v| > 1$ and $v$ is negative except the points $p_1$ and $p_2$ and the interior lattice point lie on the line $y = -1$. Thus, $v = 1$.

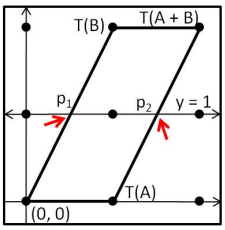


Figure 11: An example of the polygon $T(P)$ when $|v| > 1$ and $v$ is positive. Since two sides pass through the line $y = 1$ at the points $p_1$ and $p_2$ (marked with red arrows), and the points $p_1$ and $p_2$ are a distance of 1 unit apart, $T(P)$ has an interior lattice point.

Thus, the base of $T(P)$ has length 1 and the height is 1. Therefore, the area of $T(P)$ is 1. Since $P$ and $T(P)$ have the same area, the area of $P$ is 1.

□

In order to show the area of a primitive lattice triangle is $\frac{1}{2}$, we'll need the following theorem which determines whether a lattice parallelogram is primitive by whether or not the vectors spanning it are a basis for $\mathbb{Z}^2$. Spanning and linear independence are the same in $\mathbb{Z}^2$ as they are in $\mathbb{R}^2$ except in $\mathbb{Z}^2$, for a set of vectors to be linearly independent, the vectors must have only integer components, and for a set of vectors, $\mathbf{v}$ and $\mathbf{w}$, to span $\mathbb{Z}^2$, there must exist integers $m$ and $n$ for each $\mathbf{u} \in \mathbb{Z}^2$ such that $\mathbf{u} = m\mathbf{v} + n\mathbf{w}$.

**Definition 2.16.** Let $\mathbf{v}$ and $\mathbf{w}$ be vectors in $\mathbb{Z}^2$. The *lattice parallelogram spanned by* $\mathbf{v}$ *and* $\mathbf{w}$ is the set of vectors, $\mathbf{u} \in \mathbb{R}^2$ for which $\mathbf{u} = a\mathbf{v} + b\mathbf{w}$ for $a, b \in \mathbb{R}^2$ such that $0 \leq a \leq 1$ and $0 \leq b \leq 1$.

**Proposition 2.17.** *The lattice parallelogram $P$ spanned by linearly independent vectors $\boldsymbol{v}$ and $\boldsymbol{w}$ in $\mathbb{Z}^2$ is primitive if and only if $\{\boldsymbol{v}, \boldsymbol{w}\}$ is a basis for $\mathbb{Z}^2$.*

*Proof.* Let $\mathbf{v}$ and $\mathbf{w}$ be linearly independent vectors in $\mathbb{Z}^2$. We must show two implications.

($\Longrightarrow$) Let $P$ be the primitive parallelogram spanned by $\mathbf{v}$ and $\mathbf{w}$. Since $\mathbf{v}$ and $\mathbf{w}$ are linearly independent, they form a basis for $\mathbb{R}^2$ over $\mathbb{R}$. Let $\mathbf{u} \in \mathbb{Z}^2$. Then $\mathbf{u}$ can be written as a linear combination of $\mathbf{v}$ and $\mathbf{w}$. Choose $a, b \in \mathbb{R}$ such that $\mathbf{u} = a\mathbf{v} + b\mathbf{w}$. We show $\mathbf{v}$ and $\mathbf{w}$ span $\mathbb{Z}^2$ by showing that $a$ and $b$ must be integers. Let $a = \lfloor a \rfloor + a'$, let $b = \lfloor b \rfloor + b'$, and note that $0 \leq a' < 1$ and $0 \leq b' < 1$. Let $\mathbf{u}_0 \in \mathbb{R}^2$ and let $\mathbf{u}_0 = a'\mathbf{v} + b'\mathbf{w}$. Then $\mathbf{u}_0 = \mathbf{u} - \lfloor a \rfloor \mathbf{v} - \lfloor b \rfloor \mathbf{w}$. Since $\mathbf{u}, \mathbf{v}$, and $\mathbf{w} \in \mathbb{Z}^2$ and $\lfloor a \rfloor, \lfloor b \rfloor \in \mathbb{Z}$, $\mathbf{u}_0 \in \mathbb{Z}^2$. We know $a' < 1$, $b' < 1$, and $\mathbf{v}$ and $\mathbf{w}$ span $P$. Therefore, $\mathbf{u}_0$ is in $P$. However, $P$ is primitive, so $\mathbf{u}_0$ must be a vertex of $P$. Since $a' \neq 1$ and $b' \neq 1$, $\mathbf{u}_0 = (0, 0)$. It follows that $a' = b' = 0$ since $\mathbf{u}_0 = a'\mathbf{v} + b'\mathbf{w}$, $\mathbf{v} \neq 0$, and $\mathbf{u} \neq 0$. This means $a$ and $b$ are integers, and therefore, $\mathbf{v}$ and $\mathbf{w}$ span $\mathbb{Z}^2$. Thus, since $\mathbf{v}$ and $\mathbf{w}$ are linearly independent, $\{\mathbf{v}, \mathbf{w}\}$ is a basis for $\mathbb{Z}^2$.

($\Longleftarrow$) Let $\{\mathbf{v}, \mathbf{w}\}$ be a basis for $\mathbb{Z}^2$. Then for any vector $\mathbf{u} \in \mathbb{Z}^2$, $\mathbf{u} = m\mathbf{v} + n\mathbf{w}$ for some integers $m$ and $n$. Let $P$ be the parallelogram spanned by $\mathbf{v}$ and $\mathbf{w}$. Assume $\mathbf{u} \in \mathbb{Z}^2$ is in $P$. We must show $\mathbf{u}$ is a vertex of $P$. Since $P$ is spanned by $\mathbf{v}$ and $\mathbf{w}$, we can write $\mathbf{u} = a\mathbf{v} + b\mathbf{w}$ where $a, b \in \mathbb{R}, 0 \leq a \leq 1$, and $0 \leq b \leq 1$. This means $m$ and $n$ must each be 0 or 1. Thus, $\mathbf{u}$ is a vertex of $P$, and $P$ is primitive.

□

## 2.6 The Area of a Primitive Lattice Triangle

Now, we use the facts about plane isometry and visible points, together with our results about primitive parallelograms to prove the area of a primitive lattice triangle is $\frac{1}{2}$. We'll need to know the sides of a primitive lattice triangle form a bas is of $\mathbb{Z}^2$. The following lemma shows this is the case.

**Lemma 2.18.** *If the vectors $\boldsymbol{v}$ and $\boldsymbol{w}$ correspond to adjacent sides of a primitive lattice triangle $T$, then $\boldsymbol{v}$ and $\boldsymbol{w}$ form a basis of $\mathbb{Z}^2$.*

*Proof.* Let $\mathbf{v}$ and $\mathbf{w}$ be vectors corresponding to adjacent sides of the primitive lattice triangle, $T = \triangle ABC$. Let $P$ be the primitive parallelogram spanned by $\mathbf{v}$ and $\mathbf{w}$, and let $T^C$ be the complement of $T$ in $P$. Let $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ be the rotation by $\pi$ about the midpoint of the line segment $\overline{BC}$ (see Figure 12). Since $\rho$ is a plane isometry, it preserves distance and angles. Therefore, $\rho(T) = T^C$ and $\rho(T^C) = T$. Let $X$ be a lattice point on the boundary but not at a vertex of $T^C$ or in the interior of $T^C$. Then since $\rho(T^C) = T$, $\rho(X)$ is a lattice point on the boundary of $T$ but not at a vertex of $T$ or $\rho(X)$ is a lattice point in the interior of $T$. Since $T$ is primitive, this is not possible. Therefore, there are no lattice points in the interior of $T^C$ and there are no lattice points on the boundary of $T^C$ other than the vertices of $T^C$. Thus, $P$ is primitive, and by Proposition 2.17, $\{\mathbf{v}, \mathbf{w}\}$ is a basis for $\mathbb{Z}^2$.

□

Now we can combine the fact that the area of a primitive lattice parallelogram is 1 and the facts we've just shown relating bases and primitive lattice parallelograms to show the area of a primitive triangle is $\frac{1}{2}$.

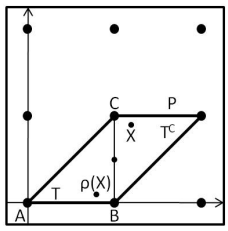


Figure 12: The parallelogram $P$ is the union of the primitive lattice triangle $T = \triangle ABC$ and the lattice triangle $T^C$. The plane isometry $\rho$ is a rotation by $\pi$ about the midpoint of the line segment $\overline{BC}$.

**Theorem 2.19.** *A primitive triangle $T$ has area $\frac{1}{2}$.*

*Proof.* Let $T$ be a primitive lattice triangle, and let $\mathbf{v}$ and $\mathbf{w}$ be vectors corresponding to adjacent sides of $T$. By Lemma 2.18, $\{\mathbf{v}, \mathbf{w}\}$ is a basis for $\mathbb{Z}^2$. By Proposition 2.17, $\mathbf{v}$ and $\mathbf{w}$ span a primitive parallelogram $P$, and by Proposition 2.15, the area of $P$ is 1. Since $T$ has the same base and height as $P$, $T$ has area $\frac{1}{2}$.

□

# 3 Pick's Theorem

Now that we've shown the area of a primitive lattice triangle is $\frac{1}{2}$, we're very close to being able to prove Pick's Theorem. There are many different proofs of Pick's theorem. The one we provide here utilizes some basic graph theory, so we'll begin with some definitions of the terms we'll need to use. These terms and the lemmas we'll present next will allow us to think of the triangulation of a lattice polygon, $P$, with primitive lattice triangles as a graph.

## 3.1 Basic Definitions From Graph Theory

**Definition 3.1.** A *graph*, denoted by $G = (V, E)$, consists of a finite nonempty set, $V$ of points called *vertices* and a finite set, $E$ of unordered pairs of distinct elements of $V$, called *edges*.

For a graph $G = (V, E)$, the elements of $E$ are of the form $\{u, v\}$, where $u \neq v$ and $u$ and $v$ are the endpoints of an edge in $G$. Note that $u, v \in V$. Consider the graph, in Figure 13. This is a graph with 14 vertices, $v_1, v_2, \ldots, v_{14}$ and 20 edges. A few of these edges, which are elements of the set $E$, are $\{v_1, v_2\}, \{v_{11}, v_{12}\}$, and $\{v_8, v_9\}$. We will use the graph in Figure 13, which we'll call $G_0 = (V_0, E_0)$, to illustrate each of the definitions to follow.

**Definition 3.2.** A graph $G' = (V', E')$ is a *subgraph* of a graph $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$.

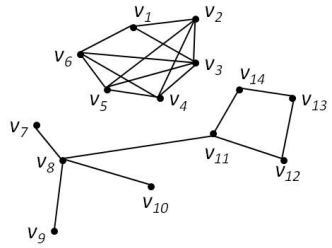


Figure 13: The graph $G_0 = \{V_0, E_0\}$

The graph $G_1 = (V_1, E_1)$ where $V_1 = \{v_7, v_8, v_9, v_{10}, v_{11}\}$ and $E_1 = \{\{v_7, v_8\}, \{v_8, v_9\}, \{v_8, v_{10}\}, \{v_8, v_{11}\}\}$, is a subgraph of $G_0$.

**Definition 3.3.** Let $u$ and $v$ be vertices of a graph, $G$. Then a *path of length $n$ from $u$ to $v$* is a sequence of $n$ distinct edges on the graph that connect $u$ to $v$. We denote a path by its vertex sequence.

In the graph $G_0$, one possible path of length 3 from $v_8$ to $v_{13}$ is $v_8, v_{11}, v_{12}, v_{13}$. Another is $v_8, v_{11}, v_{14}, v_{13}$.

**Definition 3.4.** A path is a *circuit* if the last vertex in the vertex sequence of the path is the same as the first vertex. That is, a circuit is a path from a vertex to itself.

In the graph $G_0$, the path $v_1, v_2, v_3, v_4, v_5, v_6, v_1$ is a circuit.

**Definition 3.5.** If there is a path between every pair of distinct vertices of $G$, then we say $G$ is *connected*.

The graph $G_0$ is not connected because there is no path between $v_7$ and $v_5$. Note that there are also several other "missing" paths that keep $G_0$ from being connected. However, the subgraph of $G_0$, $G_2 = \{V_2, E_2\}$ where $V_2 = \{v_3, v_4, v_5\}$ and $E_2 = \{\{v_3, v_4\}, \{v_4, v_5\}, \{v_3, v_5\}\}$ is connected.

**Definition 3.6.** A connected graph that has no circuits is called a *tree*.

The subgraph of $G_0$, $G_3 = \{V_3, E_3\}$, where $V_3 = \{v_7, v_8, v_9, v_{10}, v_{11}\}$ and $E_3 = \{\{v_7, v_8\}, \{v_8, v_9\}, \{v_8, v_{10}\}, \{v_8, v_{11}\}\}$ is a tree. However, the subgraph of $G_0$, $G_4 = \{V_4, E_4\}$ where $V_4 = \{v_{11}, v_{12}, v_{13}, v_{14}\}$ and $E_4 = \{\{v_{11}, v_{12}\}, \{v_{12}, v_{13}\}, \{v_{13}, v_{14}\}, \{v_{14}, v_{11}\}\}$ is not a tree because the path $v_{11}, v_{12}, v_{13}, v_{14}, v_{11}$ is a circuit.

**Definition 3.7.** If a graph $G$ can be drawn in the plane in such a way that no two edges cross, then $G$ is *planar*.

The subgraph of $G_0$, $G_3$ as defined above is planar, but the subgraph of $G_0$, $G_5 = \{V_5, E_5\}$ where $V_5 = \{v_2, v_3, v_4, v_5\}$ and $E_5 = \{\{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_5, v_2\}, \{v_2, v_4\}, \{v_3, v_5\}\}$ is not planar.

**Definition 3.8.** The regions bounded by the edges in the circuits of a planar graph, $G$, and the unbounded region around $G$ are called *faces*.

Let $G_6 = \{V_6, E_6\}$ be the subgraph of $G_0$ where $V_6 = \{v_1, v_2, v_3, v_4, v_5, v_6\}$ and $E_6 = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_6, v_1\}, \{v_1, v_3\}, \{v_3, v_5\}\}$. The faces of $G_6$ are numbered in Figure 14. The unbounded region outside of $G_6$ is also a face. The specific number assigned to a particular face has no significance. The numbers are simply a way to differentiate between faces.

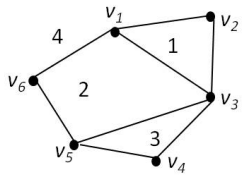


Figure 14: The graph $G_6$ with its faces numbered

## 3.2 Proving Pick's Theorem

We'll need to prove three lemmas which use the definitions from graph theory given above to prove Pick's Theorem. The first guarantees a unique path between distinct vertices of a graph when the graph is a tree. The second gives us a relationship between the number of edges and the number of vertices in a graph that is a tree. The third, attributed to Euler, gives a relationship between the number of vertices, $v$, the number of edges, $e$, and the number of faces, $f$, of a planar graph by the formula $\chi = v - e + f = 2$ where $\chi$ is called the Euler characteristic. The first two lemmas will allow us to prove the third, Euler's formula. Euler's formula will allow us to determine the number primitive triangles needed to triangulate a polygon, $P$, in terms of the number of lattice points in the interior of $P$ and the number of lattice points on the boundary of $P$. Since we know each primitive lattice triangle has area equal to $\frac{1}{2}$, we can determine the area of $P$ in terms of the number of lattice points in the interior of $P$ and the number of lattice points on the boundary of $P$, as stated in Pick's Theorem.

**Lemma 3.9.** *If a graph, $G$, is a tree, then there is a unique path between any two vertices of $G$.*

*Proof.* Let $G$ be a graph that is a tree, and let $u$ and $w$ be vertices of $G$. Assume there are two paths, $u = v_0, v_1, \ldots, v_{n-1}, v_n = w$ and $u = v'_0, v'_1, \ldots, v'_{m-1}, v'_m = w$ connecting $u$ and $w$. Since $G$ is a tree it has no circuits. Since a path must be a sequence of distinct edges, no two vertices in a particular path are the same. Choose $j > 0$ so that $j$ is the first index for which $v'_j = v_k$ for some $k$ where $0 < k \leq n$. Since $v'_m = w = v_n$, such a $j$ must

exist. The path $u, v_1, v_2, \ldots, v_k, v'_{j-1}, \ldots, v'_2, v'_1, u$ is a circuit in $G$. Since $G$ is a tree, this is a contradiction. Thus, there is a unique path between any two vertices in $G$.

□

**Lemma 3.10.** *If a graph, $G$, is a tree with $v$ vertices and $e$ edges, then $e = v - 1$.*

*Proof.* Let $G = \{V, E\}$ be a graph that is a tree, and let $u$ be a vertex in $G$. By Lemma 3.9, for each vertex, $w \in V \setminus \{u\}$, there is a unique path from $u$ to $w$. For each vertex $w \in V \setminus \{u\}$, associate the last edge in the unique path from $u$ to $w$ with $w$. Note that every edge in $G$ is the last edge in the unique path from $u$ to $w$ for some vertex $w \in V \setminus \{u\}$. Since $G$ is a tree, there is a one to one correspondence between $V \setminus \{u\}$ and $E$. This means that $V \setminus \{u\}$ and $E$ have the same number of elements. Thus, $e = v - 1$.

□

**Lemma 3.11.** *(Euler) If $G$ is a connected, planar graph with $v$ vertices, $e$ edges, and $f$ faces, then $v - e + f = 2$.*

*Proof.* Let $G$ be a connected, planar graph with $v$ vertices, $e$ edges, and $f$ faces. We proceed by induction on $e$. For the base case, let $e = 0$. Since $G$ is connected, $v = 1$ and $f = 1$. Thus, $v - e + f = 1 - 0 + 1 = 2$.

Let $e > 0$ and assume Euler's formula holds for all connected planar graphs with $e - 1$ edges. We must show $v - e + f = 2$.

Assume $G$ does not contain a circuit. Then $G$ is a tree. Thus, $f = 1$, and by Lemma 3.10, $e = v - 1$. Thus, $v - e + f = v - (v - 1) + 1 = v - v + 1 + 1 = 2$.

Assume $G$ contains a circuit, $C$. Choose some edge of $C$ and call it $g$. Let $G' = G \setminus \{g\} = (V, E \setminus \{g\})$ be a subgraph of $G$. Since $G$ is connected, and $G'$ is only missing an edge that was part of a circuit, $G'$ is connected. Since $G$ is planer, and since removing an edge won't cause two edges to cross each other, $G'$ is planar. Removing $g$ from $G$ causes the face contained inside the circuit of $G$ to combine with the face outside the circuit, meaning $G'$ has one less face than $G$, that is, $G'$ has $f - 1$ faces. Since we only removed an edge from $G$, $G$ has $e - 1$ edges and $v$ vertices (see Figure 15). By the induction hypothesis, $v - (e - 1) + (f - 1) = 2 \implies v - e + 1 + f - 1 = 2 \implies v - e + f = 2$.

□

Now, we're ready to combine our graph theory definitions and results with our results regarding the area of a primitive lattice triangle and the triangulation of a polygon by primitive lattice triangles to prove Pick's Theorem.

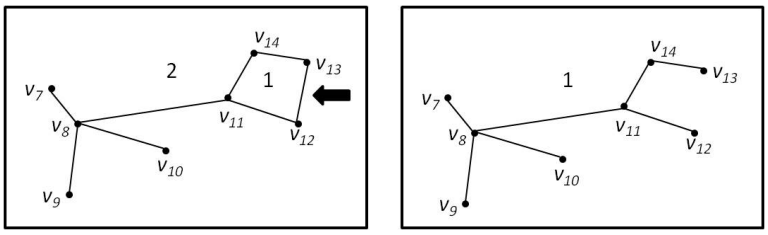


Figure 15: Left: The connected, planar, graph $G_7$ which is a subgraph of the graph $G_0$ shown in Figure 13. The faces of $G_7$ are numbered. We will remove the edge $\{v_{12}, v_{13}\}$ which is indicated by the arrow to obtain the subgraph of $G_7$, $G_7'$. Right: The graph $G_7'$ is connected and planar, and $G_7'$ has one fewer region and one fewer edge, but the same number of vertices as $G_7$.

**Theorem 3.12 (Pick's Theorem).** *Let $P$ be a polygon in the plane with its vertices at lattice points. Then the area of $P$, $A(P)$, is given by*

$$A(P) = \frac{1}{2}B(P) + I(P) - 1.$$

*where $B(P)$ is the number of lattice points on the boundary of $P$ and $I(P)$ is the number of lattice points in the interior of $P$.*

*Proof.* Let $P$ be a lattice polygon with $B(P)$ lattice points on its boundary and $I(P)$ lattice points in its interior. By Theorem 2.8, we can dissect $P$ into primitive lattice triangles. Note that the sides of the triangles do not intersect and since the triangles are primitive, each lattice point in $P$ is a vertex of a triangle. This means the graph, $G$, whose vertices are the lattice points in $P$ and whose edges are the sides of the primitive triangles that triangulate $P$ is planar and connected.

Let $f$ be the number of faces in $G$, let $e$ be the number of edges in $G$, and let $v$ be the number of vertices in $G$. Then there are $f-1$ primitive triangles in $P$. The other face in $G$ is the unbounded space outside $P$. By Theorem 2.19, the area of a primitive triangle is $\frac{1}{2}$, so, since $P$ contains $f-1$ primitive triangles,

$$A(P) = \frac{1}{2}(f-1). \tag{1}$$

Now let's consider the number of edges in $G$. Each of the $e_i$ edges in $G$ living inside the polygon $P$ is shared as a side of two primitive lattice triangles. Each of the $e_b$ edges living on the boundary of the polygon $P$ is a side of one primitive triangle. Since the edges in $G$ are the lattice line segments that form the sides of the primitive triangles in $P$, $e_i + e_b = e \implies e_i = e - e_b$.

Since $f-1$ primitive triangles triangulate $P$, the number of sides of primitive triangles in $P$ is given as follows,

$$3(f-1) = 2e_i + e_b = 2(e - e_b) + e_b = 2e - 2e_b + e_b = 2e - e_b.$$

Solving for $f$ gives,

$$f = 2(e - f) - e_b + 3. \tag{2}$$

By Lemma 3.11, $v - e + f = 2 \Longrightarrow e = v + f - 2$. Substituting this into equation (2), we get

$$f = 2(v - 2) - e_b + 3. \tag{3}$$

Since we can associate each of the $e_b$ edges of $G$ lying on the boundary of $P$ with one lattice point on the boundary of $P$, and this accounts for all lattice points on the boundary of $P$, there are $e_b$ lattice points on the boundary of $P$, so $B(P) = e_b$. As mentioned above, the vertices of $G$ are the interior and boundary lattice points of $P$. Therefore, $v = B(P)+I(P)$. Substituting this, $e_b = B(P)$, and equation (3) into equation (1) gives

$$\begin{aligned} A(P) &= \frac{1}{2}(f-1) \\ &= \frac{1}{2}(2(v-2) - e_b + 2) \\ &= \frac{1}{2}(2((B(P) + I(P)) - 2) - B(P) + 2) \\ &= \frac{1}{2}B(P) + I(P) - 1. \end{aligned}$$

□

Let's look at a couple of examples of how we can find the area of a lattice polygon using Pick's theorem. First consider the polygon on the left in Figure 16. Call this polygon $P_1$. There are 13 lattice points on the boundary of $P_1$, so $B(P) = 13$. Since $P_1$ has 3 interior lattice points, $I(P) = 3$. Thus, by Pick's Theorem, $A(P_1) = \frac{1}{2} \cdot 13 + 3 - 1 = 8\frac{1}{2}$.

We can check the area given by Pick's Theorem by counting the primitive parallelogram (primitive squares) and primitive triangles in $P_1$. These primitive polygons are shown with dotted lines in Figure 16. The polygon $P_1$ contains 7 primitive lattice squares and 3 primitive lattice triangles. Since by Proposition 2.15, the area of a primitive latticeparallelogram, and therefore a primitive lattice square, is 1 and since by Theorem 2.19, the area of a primitive lattice triangle is $\frac{1}{2}$, $A(P_1) = 7(1) + 3(\frac{1}{2}) = 8\frac{1}{2}$.

Now consider the polygon on the right in figure 16. Call this polygon $P_2$. Since $P_2$ has 7 lattice points on its boundary and 6 interior lattice points, $B(P) = 7$ and $I(P) = 6$. Therefore, by Pick's Theorem, $A(P_2) = \frac{1}{2} \cdot 7 + 7 - 1 = 9\frac{1}{2}$.

The areas of $P_1$ and $P_2$ are both multiples of $\frac{1}{2}$. Since for any lattice polygon, $P$, Pick's Theorem tells us $A(P) = \frac{1}{2}B(P) + I(P) - 1$ where $B(P)$ and $I(P)$ are integers, the area of a lattice polygon $P$ will always be a multiple of $\frac{1}{2}$.

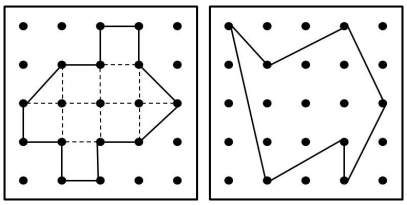

Figure 16: Lattice polygons for which we can use Pick's Theorem to calculate area. A dissection of the polygon on the left into primitive lattice squares and primitive lattice triangles is shown with dotted lines.

## 3.3 Beyond Pick's Theorem

There are many extensions of Pick's Theorem. Two extensions of Pick's Theorem we will discuss here are a version of Pick's theorem for non-simple polygons and a version of Pick's theorem for polygons $kP = \{kx | x \in P\}$ for some positive integer $k$ and some lattice polygon $P$. Later, once we've discussed convexity, we will discuss a version of Pick's theorem for convex regions in $\mathbb{R}^2$.

### 3.3.1 Pick's Theorem for Non-Simple Polygons

Up until now we've dealt only with simple lattice polygons. However, there is actually a relatively simple extension of Pick's theorem for non-simple lattice polygons. This discussion of Pick's theorem for non-simple lattice polygons is adapted from [9].

As mentioned earlier, a non-simple lattice polygon is a lattice polygon having holes or a boundary crossing itself. Two non-simple lattice polygons are pictured in Figure 17. The first is not simple because it contains 1 hole. The second is not simple because its boundary intersects itself. We can't use our current version of Pick's theorem to calculate the areas of these polygons. To see this, first consider the non-simple polygon on the left in Figure 17. For this polygon, $P_3$, $B(P_3) = 12$ and $I(P_3) = 4$. If we use Pick's theorem to get an area, we get $A(P_3) = \frac{1}{2} \cdot 12 + 4 - 1 = 9$. However, $P_3$ is made up of 5 primitive lattice parallelograms and 10 primitive lattice triangles as shown by the dotted lines in Figure 17. Since by Proposition 2.15 the area of a primitive lattice parallelogram is 1 and by Theorem 2.19, the area of a primitive lattice triangle is $\frac{1}{2}$, $A(P_3) = 1(5) + \frac{1}{2}(10) = 10$. Pick's theorem did not give us the correct area.

Similarly, the polygon on the right in Figure 17, which we'll call $P_4$, has 6 lattice points on its boundary, so $B(P_4) = 6$, and 4 interior lattice points, so $I(P_4) = 4$. By Pick's theorem, the area of $P_4$ would be $\frac{1}{2} \cdot 6 + 4 - 1 = 6$. However, as shown in by the dotted lines in Figure 17, $P_4$ is composed of 11 primitive lattice triangles. Since by Theorem 2.19, the area of a primitive lattice triangle is $\frac{1}{2}$, $A(P_4) = \frac{1}{2} \cdot 11 = 5\frac{1}{2}$. Again, Pick's theorem does not give us the correct area.

We now present a generalization of Pick's theorem which will allow us to determine the area of a non-simple polygon. In our proof of Theorem 2.8 which guarantees any lattice

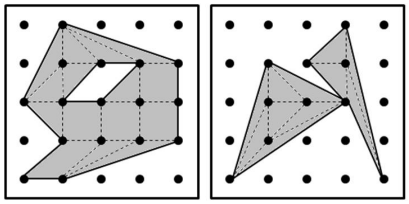

Figure 17: The regions that are shaded grey are Non-Simple polygons. The dotted lines show the division of these on-simple polygons into primitive lattice parallelograms and primitive lattice triangles.

polygon $P$ can be triangulated with primitive lattice triangles, the lattice polygon, $P$, did not need to be simple. Therefore, Theorem 2.8 applies to non-simple polygons; we can triangulate non-simple polygons with primitive lattice triangles. Now we prove a version of Pick's theorem for non-simple polygons. The proof given here is a combination of the proofs given in [6] and [9]. In this proof, as in the proof presented for Pick's Theorem in section 3.2, we define a graph from the the triangulation of the polygon, $P$. The proof of Pick's Theorem for non-simple polygons differs from Pick's Theorem only because we must account for holes to prove Pick's Theorem for non-simple polygons. In this section, a lattice polygon is not automatically assumed to be simple.

**Theorem 3.13.** *Let $P$ be a lattice polygon, simple or not, with $m$ holes. Then we can triangulate $P$ with primitive lattice triangles. We can also construct a graph $G$ with the lattice points in the interior of $P$ and the lattice points on the boundary of $P$ as vertices and with the sides of the primitive lattice triangles that triangulate $P$ as edges. The area of $P$, $A(P)$, is given by*

$$A(P) = v - \frac{1}{2}e_b + m - 1$$

*where $v$ is the number of vertices in the graph $G$ and $e_b$ is the number of edges in $G$ that lie on the boundary of $P$.*

*Proof.* Let $P$ be a polygon, not necessarily simple, with $m$ holes, $m \geq 0$. By Theorem 2.8, we can dissect $P$ into primitive lattice triangles. Since the sides of these triangles do not intersect and since the triangles are primitive, each vertex in $P$ is a vertex of a primitive lattice triangle. This means $G$ is planar and connected.

Let $f$ be the number of faces of $G$, let $e$ be the number of edges of $G$, and let $v$ be the number of vertices of $G$. Then there are $f - 1 - m$ primitive triangles in $P$. The other $1 + m$ faces are the $m$ holes in $P$ and the unbounded space outside $P$. By Theorem 2.19, the area of a primitive triangle is $\frac{1}{2}$, so

$$A(P) = \frac{1}{2}(f - 1 - m) \tag{4}$$

As in our proof of Pick's theorem, $e_i + e_b = e \implies e_i = e - e_b$ where $e$ is the total number of edges in $G$, $e_i$ is the number of edges in $G$ that lie in the interior of $P$, and $e_b$ is the number of edges in $G$ that lie on the boundary of $P$. Since $f - 1 - m$ primitive triangles triangulate $P$,

$$3(f - 1 - m) = 2e_i + e_b = 2e - e_b. \tag{5}$$

Solving for $f$ yields

$$f = 2(e - f) - e_b + 3(m + 1). \tag{6}$$

Since $G$ is connected and planar, by Lemma 3.11, $v - e + f = 2 \implies e = v + f - 2$. Substituting this into equation (6), we get

$$f = 2(v - 2) - e_b + 3(m + 1). \tag{7}$$

Finally, substituting equation (7) into equation (4) gives us

$$A(P) = v - \frac{1}{2}e_b + m - 1. \tag{8}$$

□

With this extension of Pick's theorem, we can now find the areas of the non-simple polygons in Figure 3.13 without dissecting the polygons into primitive lattice triangles and primitive lattice parallelograms. The polygon $P_3$ has 16 lattice points on its boundary and in its interior, so $v = 16$, 12 edges on its boundary, so $e_b = 12$, and 1 hole, so $m = 1$. Therefore, by Theorem 3.13, $A(P_3) = 16 - \frac{1}{2} \cdot 12 + 1 - 1 = 10$, which is the correct area.

The polygon $P_4$ has 10 lattice points on its boundary and in its interior, so $v = 10$, 7 edges on its boundary, so $e_b = 7$, and 0 holes, so $m = 0$. Thus, by Theorem 3.13, $A(P_4) = 10 - \frac{1}{2} \cdot 7 + 0 - 1 = 5\frac{1}{2}$. Once again, the area given by our generalization of Pick's theorem is the same as the area given by dissecting $P_4$ into primitive polygons.

Note that we did not express the area of $P$ in terms of $B(P)$ and $I(P)$ for the version of Pick's theorem for non-simple polygons like we did for Pick's theorem. This is because for some non-simple polygons, the equation $e_b = B(P)$ is not true. For example, consider the non-simple polygon, $P_5$ in Figure 18. The polygon $P_5$ has 14 edges on its boundary, but it has 13 lattice points on its boundary, so $e_b = 14 \neq 13 = B(P_5)$.

The area of a simple polygon, $P$, as given by Pick's theorem is $A(P) = \frac{1}{2}B(P) + I(P) - 1$. However, if we don't set $e_b = B(P)$ and $v = B(P) + I(P)$, then the area given by Pick's theorem is $v - \frac{1}{2}e_b - 1$. From this, we see the only differences between the version of Pick's theorem for non-simple polygons and Pick's theorem are first, for a non-simple polygon, we cannot write the area in terms of the numbers of boundary and interior lattice points in $P$ and second, for the generalization of Pick's theorem to non-simple polygons, we must factor in the number of holes in $P$.

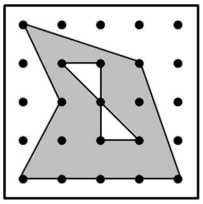

Figure 18: The grey shaded region is a non-simple polygon.

### 3.3.2 Pick's Theorem for Polygons $kP$

From this point on, we will use Pick's Theorem in a slightly different way. Rather than using Pick's Theorem to determine the area of a lattice polygon based on the number of lattice points the polygon contains in its interior and on its boundary, we'll now use Pick's Theorem to determine the total number of boundary and interior lattice points contained in a lattice polygon based on the area of the polygon. To find the formula for this total number of lattice points in a lattice polygon, let $P$ be a lattice polygon with $B(P)$ boundary lattice points and $I(P)$ interior lattice points. Let $L(P)$ be the total number of lattice points living inside and on the boundary of $P$, that is,

$$L(P) = B(P) + I(P) \Longrightarrow B(P) = L(P) - I(P) \tag{9}$$

Pick's Theorem gives $A(P) = \frac{1}{2}B(P) + I(P) - 1$. Substituting equation (9) for $B(P)$ and solving for $L(P)$ gives

$$L(P) = A(P) + \frac{1}{2}B(P) + 1.$$

Why do we know want to find $L(P)$ rather than $A(P)$? The main reason is the last two extensions of Pick's Theorem we present involve finding $L(P)$ based on $A(P)$, and other extensions of Pick's Theorem appearing in the literature involve $L(P)$ rather than $A(P)$. [1] Also, if we think about Pick's Theorem as a way to determine the number of interior and boundary lattice points in a polygon based on the polygon's area, the similarities between Pick's Theorem and Minkowski's Theorem become more obvious. Each theorem tells us something about the number of lattice points in a region based mainly on the region's area.

From here on, we will again assume lattice polygons are simple. Consider two polygons, $P_1$ and $P_2$, which are related in such a way that $P_2 = \{nx | x \in P_1\}$ for some positive integer $n$. Fix such an $n$. How would we find $L(P_1)$ and $L(P_2)$? If we were to use only the results we have so far, we would need to apply Pick's Theorem to $P_1$ and then we would have to apply Pick's Theorem to $P_2$. Hpwever, we need not use Pick's Theorem twice, because

[1] In fact, the extension of Pick's Theorem to $\mathbb{R}^n$, Ehrharts's Theorem, which we will not discuss here involves finding $L(P)$ for a convex region in $\mathbb{R}^n$ rather than finding an area. See [6] for a discussion of Ehrhart's Theorem.

there is an extension of Pick's Theorem that gives a formula for $L(kP)$, where $P$ is a lattice polygon, and $kP = \{kx | x \in P\}$ for any positive integer $k$. We'll call This formula Pick's Theorem for polygons $kP$. To prove it, we'll need a few lemmas.

The first two lemmas require a return to visible points. We will determine the coordinates of lattice points on a line $l$ in terms of the visible points on $l$ and we will use this result to determine the number of lattice points on a line between a lattice point and the origin. Since we can translate any lattice polygon so one of its vertices lies at the origin while ensuring lattice points remain lattice points and non-lattice points remain non-lattice point, the edges of the polygon adjacent to the vertex that is mapped to the origin become lattice line segments from a lattice point to the origin. The results we've mentioned here and we'll prove next, will allow us to determine the number of lattice points on the boundary of a polygon based on the number of lattice points on each edge of the polygon.

Recall that a visible point is the point on a particular line through the origin lying closest to the origin.

**Lemma 3.14.** *If $p = (m, n)$ is a visible point on the lattice line $l$, then the lattice points on $l$ are each of the form $tp$ for some integer $t$.*

*Proof.* Let $p = (j, k)$ be a visible point on the lattice line $l$. Let $q = (m, n)$ be a lattice point on $l$ that is distinct from $p$. Since $l$ passes through $q = (m, n)$ and $(0, 0)$, the equation for $l$ is $y = \frac{n}{m}x$. Since $q$ is not visible, by Theorem 2.13, $m$ and $n$ are not relatively prime, that is, $\gcd(m, n) = d > 1$ for some integer $d$. It follows that $\frac{m}{d}$ and $\frac{n}{d}$ are integers and $(\frac{m}{d}, \frac{n}{d})$ is therefore a lattice point. Since the point $(\frac{m}{d}, \frac{n}{d})$ satisfies $y = \frac{n}{m}x$, $(\frac{m}{d}, \frac{n}{d})$ is on $l$. Since $d = \gcd(m, n)$, $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$. Therefore, by Theorem 2.13, $(\frac{m}{d}, \frac{n}{d})$ is visible. This means $(\frac{m}{d}, \frac{n}{d}) = \pm p$. Thus, $q = \pm dp$.

□

**Lemma 3.15.** *Let $m$ and $n$ be nonnegative integers. There are exactly $\gcd(m, n) - 1$ lattice points on the lattice line segment between the origin and the point $(m, n)$ not including the endpoints.*

*Proof.* Let $(m, n)$ be a lattice point, and let $l$ be the lattice line segment with endpoints $(0, 0)$ and $(m, n)$. Let $\gcd(m, n) = d$. Then $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$, and by Theorem 2.13, $(\frac{m}{d}, \frac{n}{d})$ is visible. By Lemma 3.14, the lattice points on $l$ other than $(0, 0)$ and $(m, n)$ must be $(\frac{m}{d}, \frac{n}{d}), (\frac{2m}{d}, \frac{2n}{d}), (\frac{3m}{d}, \frac{3n}{d}), \ldots, (\frac{(d-1)m}{d}, \frac{(d-1)n}{d})$. Thus, there are $d-1$ points on $l$ not including its endpoints.

□

In the following lemma, we'll use the results we just proved about visible points to give a formula for the number of points on the boundary of a lattice polygon $P$.

**Lemma 3.16.** *Let $P$ be a lattice $n$-gon with vertices $p_1 = (a_1, b_1), p_2 = (a_2, b_2), \ldots, p_n = (a_n, b_n)$. If $d_i = \gcd(a_{i+1} - a_i, b_{i+1} - b_i)$, then the number of lattice points on the boundary of $P$, $B(P)$, is*

$$B(P) = \sum_{i=1}^{n} d_i.$$

*Proof.* Let $P$ be a lattice $n$-gon with vertices $p_1 = (a_1, b_1), p_2 = (a_2, b_2), \ldots, p_n = (a_n, b_n)$. Let $\gcd(a_{i+1} - a_i, b_{i+1} - b_i) = d_i$, $1 \leq i < n$ and let $\gcd(a_1 - a_i, b_1 - b_i) = d_i$ when $i = n$. Since translation is a plane isometry, and a lattice must be closed under vector addition, distance and the number of lattice points on a lattice line are preserved under translation. Therefore, we can translate each side of $P$ with endpoints $p_i$ and $p_{i+1}$ by a lattice point, $p_i$, so one of its endpoints, $p_i = (a_i, b_i)$ lies at the origin. After this translation, the other endpoint, $p_{i+1} = (a_{i+1}, b_{i+1})$ lies at the point $(a_{i+1} - a_i, b_{i+1} - b_i)$. Note that we can map the side with endpoints $p_n$ and $p_1$ to the line segment with endpoints at the origin and $(a_1 - a_n, b_1 - b_n)$. Since $\gcd(a_{i+1} - a_i, b_{i+1} - b_i) = d_i$ when $1 \leq i < n$ and $\gcd(a_1 - a_n, b_1 - b_n) = d_i$, by Lemma 3.15, there are $d_i - 1$ lattice points on the side of $P$ with endpoints $p_i$ and $p_{i+1}$ (or with endpoints $p_n$ and $p_1$) not including $p_i$ and $p_{i+1}$ (or $p_n$ and $p_1$). Since $d_i - 1$ gives the number of lattice points on the side of $P$ with $p_i$ and $p_{i+1}$ as endpoints for every $i < n$, and $d_i - 1$ gives the number of lattice points on the side of $P$ with $p_n$ and $p_1$ as endpoints for $i = n$, we know the number of lattice points that are not vertices on each side of $P$. Therefore, the number of lattice points on the boundary of $P$ not counting the vertices of $P$, is

$$\sum_{i=1}^{n} (d_i - 1).$$

Thus, adding in the vertices of $P$ gives

$$\begin{aligned} B(P) &= n + \sum_{i=1}^{n} (d_i - 1) \\ &= n + (d_1 - 1) + (d_2 - 1) + \cdots + (d_n - 1) \\ &= n + d_1 + d_2 + \cdots + d_n - n \\ &= d_1 + d_2 + \cdots + d_n \\ &= \sum_{i=1}^{n} d_i. \end{aligned}$$

□

The last thing we need in order to prove our generalization of Pick's theorem for polygons $kP$ is the fact that multiplication of every point in a polygon by some integer $k$ changes the lengths of the sides of the polygon by a factor of $k$ and changes the area of the polygon by a factor of $k^2$. This can be shown with some simple linear algebra. Let $M : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear transformation given by $M\mathbf{x} = k\mathbf{x}$ where $\mathbf{x}$ is a vector in $\mathbb{R}^2$ emanating from the origin with its endpoint at a lattice point and $M$ is the matrix

$$M = \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}.$$

Under $M$, the vector $\mathbf{v} = \langle x, y \rangle$ is mapped to the vector $k\mathbf{v} = \langle kx, ky \rangle = k\langle x, y \rangle$ so the length of the vector $\mathbf{v}$ is changed by a factor of $k$. Since $\det(M) = k^2$, the area of the image under $M$ of any closed, bounded region, $R$, in $\mathbb{R}^2$ is different from the area of $R$ by a factor of $k^2$. Now we can find a formula for the number of lattice points in a polygon $kP$. Note that the are of $R$ will still change by a factor of $k^2$ even if $k$ is a positive real number that is not an integer. We assume $k$ is an integer here, becasue we will need this condition in the next theorem so we can talk about the greatest common divisor of an integer multiplied by $k$. However, we will need to consider changes in area when $k$ is not an integer later when we prove Minkowski's Theorem.

**Theorem 3.17.** *Let $P$ be a polygon, let $k$ be a positive integer, and define $kP = \{kx | x \in P\}$. Then the number of boundary and interior lattice points in $kP$, $L(kP)$, is*

$$L(kP) = A(P)k^2 + \frac{1}{2}B(P)k + 1$$

*where $B(P)$ and $A(P)$ are defined as for Pick's Theorem.*

*Proof.* Let $P$ be an $n$-gon, let $k$ be a positive integer, and define $kP = \{kx | x \in P\}$. Equation (**??**) gives us

$$L(kP) = A(kP) + \frac{1}{2}B(kP) + 1.$$

Lemma 3.16 and the fact that $\gcd(ka, kb) = k\gcd(a, b)$ give us that

$$\begin{aligned} B(kP) &= \sum_{i=1}^{n} d_i \\ &= \sum_{i=1}^{n} \gcd(k(a_{i+1} - a_i), k(b_{i+1} - b_i)) \\ &= k\sum_{i=1}^{n} \gcd(a_{i+1} - a_i, b_{i+1} - b_i) \\ &= B(P)k. \end{aligned}$$

As we discussed above, multiplication of every point in $P$ by $k$ changes the area of $P$ by a factor of $k^2$, so $A(kP) = A(P)k^2$. Thus,

$$L(kP) = A(P)k^2 + \frac{1}{2}B(P)k + 1.$$

□

This generalization of Pick's theorem to polygons $kP$ allows us to determine the number of lattice points in a polygon $kP$ in terms of the area of $P$ and the number of lattice points on the boundary of $P$.

As mentioned above, there are many other extensions of Pick's Theorem not discussed in this paper. There are more extensions of Pick's Theorem than would realistically fit into a paper of this size.

While this is the end of our discussion on Pick's theorem specifically, we will return to Pick's theorem briefly after we discuss convex regions in $\mathbb{R}^2$ in order to discuss one more extension of Pick's theorem, this one to convex regions in $\mathbb{R}^2$. This last extension of Pick's Theorem will lead us to Minkowski's Theorem.

# 4 Convex Regions in $\mathbb{R}^2$

We will now discuss convex regions in $\mathbb{R}^2$. This discussion will be important in extending Pick's theorem to convex regions in $\mathbb{R}^2$. We will also need the condition of convexity in Minkowski's theorem. First, we'll begin the formal definition of convexity. The definition we give here is for $\mathbb{R}^n$, but our immediate discussion involving it will be in $\mathbb{R}^2$. We will need this definition in $\mathbb{R}^n$ later when we discuss Minkowski's Theorem in $\mathbb{R}^n$ in section 6.

**Definition 4.1.** Let $R \subseteq \mathbb{R}^n$. Then $R$ is *convex* if for all points $x$ and $y$ in $R$, the line segment joining $x$ and $y$ is contained in $R$. The *convex hull* of $R$ is the intersection of all of the convex sets that contain $R$.

Note that the intersection of a collection of convex sets is convex, and therefore, the convex hull of a set is convex.

We can determine an upper bound on the number of lattice points in a bounded, closed, convex region, $R$, in $\mathbb{R}^2$ by using an extension of Pick's Theorem that is attributed to Ehrhart. We're able to determine this upper bound because $R$ is convex. Theorem 4.2, which we will state but not prove, states that for any bounded, closed, convex region, $C$, in $\mathbb{R}^2$, we can construct a lattice polygon, $H$, which is the convex hull of the lattice points living on the boundary and in the interior of $C$. Theorem 4.2 also gives $A(H) \leq A(C)$ and $p(H) \leq p(C)$ where $p(H)$ denotes the perimenter of $H$. This means we can construct such a polygonal region, $P$ in our bounded, closed, and convex region $R$ (see Figure 19). Pick's Theorem allows us to determine the number of lattice points in $P$ if we know the area of $P$ and the number of lattice points on the boundary of $P$. Since we $R$ and $P$ have the same number of lattice points, this gives us $L(R)$. However, it's quite possible that we may only know information about $R$. Theorem 4.3 gives us an upper bound on $L(R)$ based only on the area and perimeter of $R$. In proving Theorem 4.3, we we rely on the results from Theorem 4.2: $P$ must exist, $A(P) \leq A(R)$, and $p(P) \leq p(R)$.

**Theorem 4.2.** *Let $R$ be a bounded, closed, convex set in $\mathbb{R}^2$ that contains three noncollinear in teger points. Then the convex hull of the set of all integer points in $R$ is a convex lattice polygon, $P$, which contains the same number of integer points as $R$. Furthermore, $A(P) \leq A(R)$ and $p(P) \leq p(R)$.*

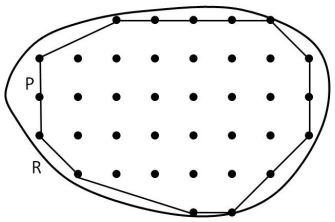


Figure 19: The convex polygon, $P$, is a convex lattice polygon that contains the same number of lattice points as the convex region $R$.

**Theorem 4.3.** *Let $R$ be a bounded, convex region in $\mathbb{R}^2$. Then*

$$L(R) \leq A(R) + \frac{1}{2}p(R) + 1.$$

*Proof.* Let $R$ be a bounded, convex region in $\mathbb{R}^2$.

First assume the integer points in $R$ are collinear. Since the area and perimeter of $R$ must be nonnegative, $A(R) + \frac{1}{2}p(R) + 1 \geq 1$. Clearly, $L(R) \leq A(R) + \frac{1}{2}p(R) + 1$ when $L(R) \leq 1$. Assume $L(R) \geq 2$. Let $G$ be the connected planar graph with the integer points $p_1, p_2, \ldots, p_{L(R)}$ in $R$ as vertices; label these vertices in order starting at the left-most end of the line of integer points (Figure 20). The edges of $G$ are $(p_1, p_2), (p_2, p_3), \ldots, (p_{L(R)-1}, p_{L(R)})$; these are the line segments that connect $p_1, p_2, \ldots, p_{L(R)}$. Then by lemma 3.10, the number of edges in $G$ is $L(R) - 1$ (see Figure 20, left). Imagine stretching a rubber band around this line of integer points (see Figure 20, right). The rubber band's length is the "perimeter" of the line segment connecting the left-most integer point, $p_1$ to the right-most integer point $p_{L(R)}$. Since $R$ is convex, this "perimeter", which is $2(L(R) - 1)$, is clearly less than or equal to the perimeter of $R$. Thus, $L(R) = 2 \cdot \frac{1}{2}(L(R) - 1) + 1 \leq \frac{1}{2}p(R) + 1 \leq A(R) + \frac{1}{2}p(R) + 1$.

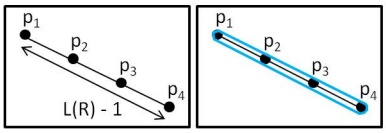


Figure 20: Left: The collinear points inside $R$ and the edges between them Right: The blue outline shows the "perimeter" of the line that connects the left-most integer point in $R$ to the right-most integer point in $R$.

Now assume that the integer points in $R$ are not collinear, and let $C$ be the convex hull of the set of integer points in $R$. By Theorem 4.2, $C$ is a convex polygon with $p(C) \leq p(R)$ and $A(C) \leq A(R)$. By Pick's Theorem (Theorem 3.12), $L(C) = A(C) + \frac{1}{2}B(C) + 1$. Since $C$ has $B(C)$ lattice points on its boundary, it has $B(C)$ line segments connecting these boundary lattice points. Since each of these line segments must have length at least 1, $B(C) \leq p(C) \leq p(R)$. Thus, $L(R) = L(C) = A(C) + \frac{1}{2}B(C) + 1 \leq A(R) + \frac{1}{2}p(R) + 1$.

□

Now we can use this extension of Pick's theorem to convex regions in $\mathbb{R}^2$ to get an upper bound on the number of lattice points in a bounded, convex region in $\mathbb{R}^2$. For example, consider the bounded, convex regions, $R_1$ and $R_2$ in figure 21.

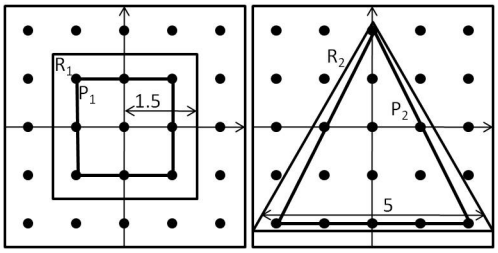


Figure 21: The convex, bounded regions $R_1$ and $R_2$ and the convex hulls of their integer points, $P_1$ and $P_2$, respectively

The square region, $R_1$ has area $A(R_1) = (3)^2 = 9$ and perimeter $p(R_1) = (3)(4) = 12$. By our generalization of Pick's theorem to convex regions in $\mathbb{R}^2$, Theorem 4.3, $L(R_1) \leq 9 + \frac{1}{2}(12) + 1 = 16$. Since $R_1$ contains 9 lattice points, our upper bound is correct. The equiangular triangle, $R_2$ has area $A(R_2) = \frac{1}{2}(5)(\frac{5}{2}\sqrt{3}) = \frac{25}{4}\sqrt{3} \approx 10.83$ and perimeter $p(R_2) = (4)(3) = 12$. By our generalization of Pick's theorem to convex regions in $\mathbb{R}^2$, $L(R_2) \leq 10.83 + \frac{1}{2}(12) + 1 = 17.83$. Since $R_2$ contains 13 lattice points, our upper bound is correct. Notice that our upper bound is quite a bit higher than the actual number of lattice points. We'll investigate this a little more in the next section.

# 5 Minkowski's Theorem

Now we will prove Minkowski's theorem and then give a few extensions and applications. Minkowski's theorem gives us the conditions that must be satisfied to guarantee that a convex, bounded region $R$ in $\mathbb{R}^2$ that is symmetric about the origin contains a lattice point other than the origin. Though Minkowski first developed this theorem for the cases where $R$ is a box or a ball, he then generalized it to the case when $R$ is any convex, bounded region in $\mathbb{R}^2$ that is symmetric about the origin [8].

The upper bound on the number of lattice points in a convex region, $R$, in $\mathbb{R}^2$ given by Ehrhart's extension of Pick's theorem to convex regions in $\mathbb{R}^2$ must always be at least 1. This is because the area and perimeter of $R$ must be nonnegative which implies $L(R) = A(R) + \frac{1}{2}p(R) + 1 \geq 1$. However, there are convex regions in $\mathbb{R}^2$ with only 1 lattice point, and there are convex regions in $\mathbb{R}^2$ with no lattice points. Also, the upper bound for $L(R)$ can be quite a bit larger than the actual value of $L(R)$, as we saw in the regions in Figure 21, even when $L(R)$ is only 1. Here, we're interested in when we can guarantee that $L(R) > 1$.

Consider the two convex regions in $\mathbb{R}^2$, $R_1$ and $R_2$, pictured in Figure 22. For the larger circle, which has radius $\frac{5}{4}$, Ehrhart's extension of Pick's theorem to convex regions in $\mathbb{R}^2$

yields $L(R_1) \leq A(R_1) + \frac{1}{2}p(R_1) + 1 = \frac{25}{16}\pi + \frac{1}{2} \cdot \frac{5}{2}\pi + 1 = \frac{45}{16}\pi + 1 \approx 9.84$. This means there are 9 or fewer lattice points in $R_1$. Similarly, the same extension of Pick's theorem yields $L(R_2) \leq A(R_2) + \frac{1}{2}p(R_2) + 1 = \frac{49}{64}\pi + \frac{1}{2} \cdot \frac{7}{4}\pi + 1 = \frac{105}{64}\pi + 1 \approx 6.15$. This means that there are 6 or fewer lattice points in $R_2$. However, we can see from Figure 22 that there are 5 lattice points in $R_1$, so $L(P) = 5$ and that there are no lattice points other than the origin in $R_2$, so $L(P) = 1$. In both cases, the actual value of $L(R)$ is quite a bit smaller than our upper bound. How can we gain more information about the actual number of lattice points in a convex region in $\mathbb{R}^2$? More specifically, can we at least determine when $L(R)$ will be at least 1 based on a minimum amount of information?

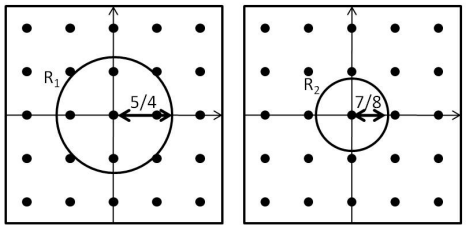


Figure 22: Two convex regions in $\mathbb{R}^2$

Minkowski's Theorem gives us a simple way to determine whether a given convex region in $\mathbb{R}^2$ that is symmetric about the origin, as are $R_1$ and $R_2$, is guaranteed to contain a lattice point other than the origin. This is very useful in proving theorems involving a situation where we need to be sure that there is at least one lattice point in a convex planar region, but we don't know everything about the region. We'll give two examples of this usefulness of Minkowski's Theorem in section 5.3 when we discuss the Two Squares Theorem and an applied problem, the Orchard Problem. We'll begin our discussion of Minkowski's Theorem with a definition and a few notes on notation. As with our definition for convexity, this definition is for $\mathbb{R}^n$, but we will use it in $\mathbb{R}^2$ now and in $\mathbb{R}^n$ later.

**Definition 5.1.** A set, $R$ in $\mathbb{R}^n$ is *symmetric about the origin* if whenever the point $(x_1, x_2, \ldots, x_n)$ is in $R$, the point $(-x_1, -x_2, \ldots, -x_n)$ is also in $R$.

Minkowski's theorem will only apply to regions that are symmetric about the origin. However, since translation is a plane isometry, we can translate any region that is symmetric about some other lattice point to the origin while leaving its area and the number of lattice points it contains unchanged. This allows us to apply Minkowski's theorem to regions that are symmetric about other lattice points.

Our proof of Minkowski's theorem will rely on translations of points in $\mathbb{R}^2$, so we will define our notation for these translations here. Let $R$ be a set in $\mathbb{R}^2$, and let $p$ be a point in $\mathbb{R}^2$. We denote the image of the set $R$ under the translation that takes the origin to $p$ by $R + p$. Taking $p$ to the origin is denoted by $R - p$. Now we are ready to prove Minkowski's Theorem.

## 5.1 Proving Minkowski's Theorem

There are many proofs of Minkowski's theorem. The one we give here, like many others, relies on Blichfeldt's lemma, which we prove now.

**Lemma 5.2.** *(Blichfeldt) If $R$ is a bounded set in $\mathbb{R}^2$ with area greater than 1, then $R$ contains two distinct points $(x_1, y_1)$ and $(x_1, y_2)$ such that the point $(x_2 - x_1, y_2 - y_1)$ is an integer point in $\mathbb{R}^2$.*

*Proof.* Let $R$ be a bounded set in $\mathbb{R}^2$ with area greater than 1. Let $S$ be the half-open unit square. That is, let $S = \{(x, y) | 0 \leq x < 1 \text{ and } 0 \leq y < 1\}$ (see Figure 23, left). For each point, $z \in \mathbb{Z}^2$, let $S_z = S + z$ be the translation of $S$ along the lattice line segment $l_z$, with endpoints $(0, 0)$ and $z$. Note that $z$ is the only integer point in $S_z$. Let $R_z = R \cap S_z$. Since $R$ is bounded, there are finitely many points $z \in \mathbb{R}^2$ for which $R_z$ is non-empty. This means $R$ is the disjoint union of finitely many of the sets $R_z$. Let $R_z - z$ be the translation of $R_z$ along the lattice line segment $l_z$. Note that $R_z - z$ is in $S$ for every $z$. Since translation is a plane isometry, it preserves area, so $A(R_z - z) = A(R_z)$. Thus,

$$\sum_{z \in \mathbb{Z}^2} A(R_z - z) = \sum_{z \in \mathbb{Z}^2} A(R_z) = A(\cup_z R_z) = A(R) > 1.$$

We can imagine stacking the sets $R_z - z$ on top of each other in the square $S$. Since $\sum_{z \in \mathbb{Z}^2} A(R_z - z) > 1$, $A(S) = 1$, and all of the sets $R_z - z$ lie in $S$, there are integer points $v$ and $w$ such that $(R_v - v) \cap (R_w - w) \neq \emptyset$. Let $r \in (R_v - v) \cap (R_w - w)$. Then there are points $r_v \in R_v$ and $r_w \in R_w$ such that $r = r_v - v = r_w - w$. Note that $r_v, r_w \in R$ and $v$ and $w$ are integer points. Since $r_v - v = r_w - w \Longrightarrow r_v - r_w = v - w$, there are two distinct points in $R$, $r_v$ and $r_w$, such that $r_v - r_w$ is an integer point.

□

Now we can prove Minkowski's Theorem. To determine whether a convex planar region, $R$, that is symmetric about the origin contains a lattice point, we simply apply Blichfeldt's Lemma to a smaller region (with area greater than 1) contained in $R$ to find an integer point that is the difference under vector addition of two points in the smaller region. Once we show this integer point is in $R$, we're done. The proof goes as follows.

**Theorem 5.3 (Minkowski's Theorem).** *Let $R$ be a bounded, convex region in $\mathbb{R}^2$ that is symmetric about the origin and having area greater than 4. Then $R$ contains an integer point other than the origin.*

*Proof.* Let $R$ be a bounded, convex region in $\mathbb{R}^2$ that is symmetric about the origin and has area greater than 4. Consider the region $R' = \{\frac{1}{2}x | x \in R\}$ (see Figure 23, right). Note that $A(R') = \frac{1}{4}A(R) > 1$ (see section 3.3.2). Since $R'$ is just a smaller version of $R$, it is convex, closed, and symmetric about the origin. By Lemma 5.2, since $A(R') > 1$, there are points $x'$ and $y'$ in $R'$ such that $x' - y'$ is a nonzero integer point. Since $x', y' \in R'$ and $R' = \{\frac{1}{2}x | x \in R\}$, $2x', 2y' \in R$. Since $R$ is symmetric about the origin, $-2y' \in R$. The fact that $R$ is convex ensures that every point on the line segment between $2x'$ and $-2y'$ is in

$R$. Therefore, $\frac{1}{2}(2x') + (1 - \frac{1}{2})(-2y') = x' - y'$ is in $R$. Since $x' - y'$ is a non-zero integer point, it satisfies the theorem.

□

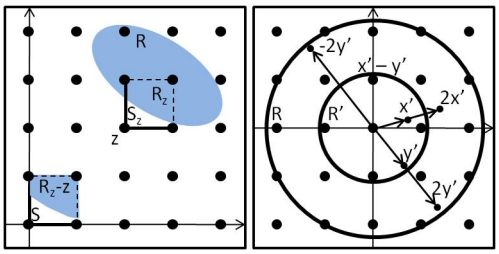


Figure 23: Left: The regions and points defined in Blichfeldt's Lemma Right: The regions and points defined in Minkowski's Theorem

With Minkowski's theorem in hand, we can now determine whether or not a convex region in $\mathbb{R}^2$ that is symmetric about a lattice point contains a lattice point other than its center. For example, we can apply Minkowski's theorem to the two regions, $R_1$ and $R_2$, in Figure 22. For the larger region, $A(R_1) = \frac{25}{16}\pi \approx 4.91 > 4$. Since $R_1$ is bounded, convex, and symmetric about the origin, and $A(R_1) > 4$, by Minkowski's theorem, $R_1$ contains a lattice point other than the origin. On the other hand, $A(R_2) = \frac{49}{64}\pi \approx 2.41 < 4$. Since $A(R_2) < 4$ we are not guaranteed that $R_2$ contains a lattice point other than the origin, and in fact, $R_2$ does not contain a lattice point other than the origin.

## 5.2 Minkowski's Theorem in an Arbitrary Lattice

As with Pick's Theorem, there are many extensions of Minkowski's theorem. Here, we will concern ourselves with a discussion of Minkowski's Theorem in an arbitrary lattice rather than restricting ourselves to $\mathbb{Z}^2$. This discussion arises from the discussion presented in [2].

Recall that a set of points, $L$, in $\mathbb{R}^2$ is a lattice if $L$ is a group under vector addition, and each point in $L$ is the center of a ball that contains no other points of $L$ [8]. We've been dealing exclusively with the lattice $\mathbb{Z}^2$, but there are other lattices. Here we will consider these other lattices. Examples of lattices other than $\mathbb{Z}^2$ include those in the left and middle pictures in Figure 1. Another example appears on the right hand side of Figure 24. Notice that connecting neighboring lattice points in $\mathbb{Z}^2$ results in tiling the plane with squares, each with area 1. This tiling is shown with dashed lines in Figure 24. If we connect neighboring lattice points in the lattice, $L$, shown with dashed lines in Figure 24 on the right, we get a tiling of the plane with parallelograms. Let $d$ be the area of each parallelogram. To guarantee a convex, bounded region, $R$, in $\mathbb{R}^2$ that is centered at a lattice point in some lattice $L$ contains a lattice point other than its center, the area of $R$ must be greater than $4d$. Since $d = 1$ in $\mathbb{Z}^2$, this is simply a generalization of Minkowski's Theorem.

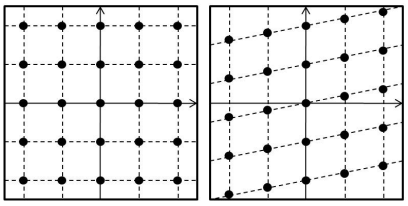

Figure 24: Left: The lattice $\mathbb{Z}^2$ Right: An arbitrary lattice. The dashed lines show how the lattices can be divided into parallelograms to tile the plane.

We will now prove Minkowski's theorem for an arbitrary lattice. The proof will combine the proof for Minkowski's theorem for an arbitrary lattice in [2], the proof for Minkowski's theorem in [6], and my own work.

**Theorem 5.4.** *Let $L$ be a lattice in $\mathbb{R}^2$ where the parallelograms formed by connecting neighboring lattice points each have area $d$. If $R$ is a convex, centrally symmetric region centered at a lattice point and having area greater than $4d$, then $R$ contains a lattice point in its interior other than its center.*

*Proof.* Let $L$ be a lattice in $\mathbb{R}^2$ with parallelogram area $d$. Let $R$ be a convex, bounded region in $\mathbb{R}^2$ with area greater than $4d$ centered at the lattice point $X$. Consider the primitive lattice parallelogram $XABC$, and choose every second lattice line that is parallel to either $\overline{XA}$ or $\overline{XC}$ (see Figure 25). These lines give a tiling of the plane with parallelograms $P_1, P_2, \ldots$ each with area $4d$. If for all $i \in \mathbb{N}$, there is no vertex of $P_i$ at the origin, translate every point in $\mathbb{R}^2$ so that for some $i \in \mathbb{N}$, some vertex of $P_i$ lies at the origin. From now on, we consider the image of this translation. However, we will call the images of the points and regions we've named by their original names. This translation does not affect the area of $R$ or the number or configuration of lattice points in $R$. The set of vertices of $P_1, P_2, \ldots$ is a lattice, which we'll call $M$. Note that $X$ is a lattice point in $M$.

Choose $i \in \mathbb{N}$ such that $P_i \cap R = \emptyset$, and let $P_i = P = DEFG$. For each lattice point, $p$ in $M$, let $P_p = P + p$ be the translation of $P$ along the lattice line segment $l_p$ with endpoints $D$ and $p$. Let $R_p = R \cap P_p$. Since $R$ is bounded, there are finitely many points $p \in M$ for which $R_p$ is non-empty. This means that $R$ is the disjoint union of finitely many of the sets $R_p$. Let $R_p - p$ be the translation of $R_p$ along the lattice line segment $l_p$. Note that $R_p - p$ lies in $P$ (see Figure 26).

Since translation is a plane isometry, it preserves area, so $A(R_p - p) = A(R_p)$. This means

$$\sum_{p \in M} A(R_p - p) = \sum_{p \in M} A(R_p) = A(\cup_{p \in M}(R_p)) = A(R) > 4d.$$

We can imagine stacking the regions $R_p - p$ on top of each other in the parallelogram $P$. Since $\sum_{p \in M} A(R_p - p) > 4d$, $A(P) = 4d$, and all of the sets $R_p - p$ lie in $P$, there are lattice points $v$ and $w$ in $M$ such that $(R_v - v) \cap (R_w - w) \neq \emptyset$. Let $r$ be a point in $(R_v - v) \cap (R_w - w)$.

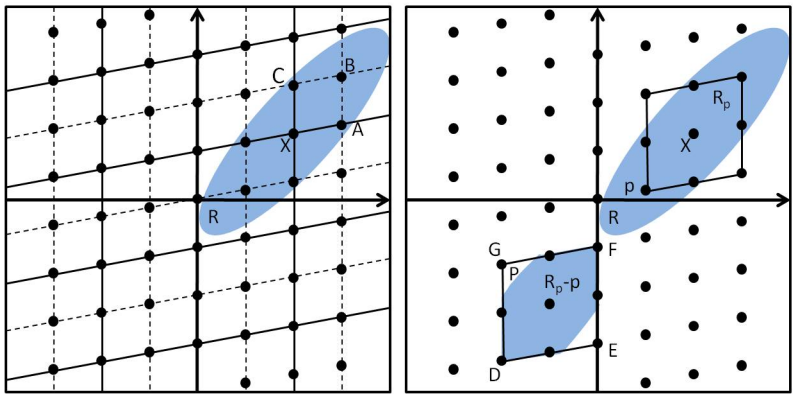


Figure 25: Left: The bounded, convex region, $R$ which is symmetric about a lattice point $X$ (shown in blue) and the parallelogram $XABC$. The tiling of the plane with parallelograms of area $4d$ is shown with solid lines. The primitive lattice parallelograms determined by the lattice $L$ are shown with dashed lines. Right: The blue regions inside of the parallelograms are $R_p$ and $R_p - p$.

Then there are points $r_v \in R_v$ and $r_w \in R_w$ such that $r = r_v - v = r_w - w$. Note that $r_v, r_w \in R$, $v$ is a lattice point in $M$, and $w$ is a lattice point in $M$, and by the definition of a lattice, $v - w$ is a lattice point in $M$. Since $r = r_v - v = r_w - w \implies r_v - r_w = v - w$, $r_v - r_w$ is also a lattice point in $M$.

Let $l$ be the line passing through $X$ that is perpendicular to the line that passes through $r_v$ and $X$. Reflect $r_v$ in $l$ and call the image of $r_v$ under this reflection $r_x$. Since $R$ is symmetric about $X$, and we reflected in a line that passes through $X$, $r_x \in R$. The midpoint of the line segment with endpoints $r_x$ and $r_v$ is $X$. Let $Y$ be the midpoint of the line segment with endpoints $r_x$ and $r_w$. Since $Y$ is on a line segment between points in $R$ and $R$ is convex, $Y \in R$ (see Figure 26.

Since $X$ is the midpoint of the line segment $\overline{r_v r_x}$, $X = \frac{1}{2}r_v + \frac{1}{2}r_x$. Since $Y$ is the midpoint of the line segment $\overline{r_w r_x}$, $Y = \frac{1}{2}r_w + \frac{1}{2}r_x$. Solving both equations for $\frac{1}{2}r_x$ gives $\frac{1}{2}r_x = X - \frac{1}{2}r_v$ and $\frac{1}{2}r_x = Y - \frac{1}{2}r_w$. Setting these equations equal gives $X - \frac{1}{2}r_v = Y - \frac{1}{2}r_w$, and simplification yields

$$r_v - r_w = 2(X - Y). \tag{10}$$

This means $2(X - Y)$ is a lattice point in $M$. Expanding $2(X - Y)$ gives us $r_v - r_w = 2(X - Y) = 2X - 2Y = (X + X) - (Y + Y)$. Since $X$ is a lattice point in $M$, $X + X$ is a lattice point in $M$.

Next we show $Y+Y$ must be a lattice point in $M$. To do so, assume the contrary: assume $Y+Y$ is not a lattice point in $M$. Then since $X+X$ is a lattice point in $M$, $(X+X)-(Y+Y)$ cannot be a lattice point in $M$. Since we know $(X + X) - (Y + Y) = 2(X - Y)$ is a lattice point, this is a contradiction, so $Y + Y$ must be a lattice point in $M$.

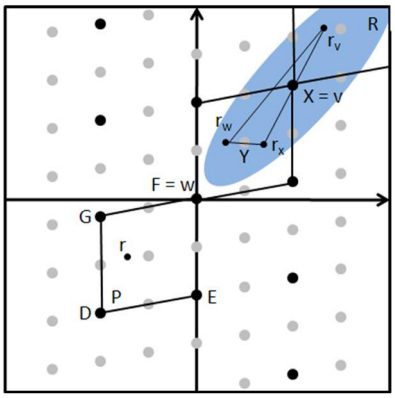


Figure 26: The points in the lattice $M$ are in black. All of the lattice points shown are in $L$.

Since $Y + Y = 2Y$ is a lattice point in $M$, it follows that $Y$ is a lattice point in $L$. Since $r_v$ and $r_w$ are distinct points, $X$ is the midpoint between $r_v$ and another point, $r_x$, and $Y$ is a midpoint between $r_w$ and another point, $r_x$, $X$ and $Y$ are distinct points. Therefore, $Y$ is a lattice point in $L$ other than $X$ that lies in the region $R$.

□

Minkowski's Theorem holds when the area of the our region of interest is greater than $4d$. What happens when the area of the region is equal to $4d$? Though we will not prove it here, we state the following corollary which tells us what happens when the area is $4d$. A proof can be found in [2].

**Corollary 5.5.** *Let $L$ be a lattice in $\mathbb{R}^2$ where the parallelograms formed by connecting neighboring lattice points each have area $d$. If $R$ is a convex, centrally symmetric region centered at a lattice point and having area equal to $4d$, then $R$ contains a lattice point other than its center on its boundary or in its interior.*

## 5.3 Applications of Minkowski's Theorem

Minkowski's theorem is useful in that it offers an easy way to determine whether a given convex, bounded region in $\mathbb{R}^2$ that is symmetric about a lattice point is guaranteed to contain a lattice point other than its center. Here, we will discuss two specific uses of Minkowski's theorem. The first is a proof of the Two Squares Theorem for prime numbers that uses Minkowski's theorem. The Two Squares Theorem for prime numbers allows us to determine whether a given prime number can be written as the sum of two squares. The second use of Minkowski's theorem we will discuss is in a solution to the Orchard Problem. This applied problem requires us to determine the maximum radius for trees, all of which have the same radius, planted at lattice points in a circular orchard such that a person standing at the origin cannot see out of the orchard no matter which direction he looks.

### 5.3.1 The Two Squares Theorem

Minkowski's theorem can be used in proving the two squares theorem. More specifically, Minkowski's Theorem is used to show which primes can be written as the sum of two squares. We will only prove a version of the two squares theorem which shows which primes can be written as the sum of two squares here. A proof of the two squares theorem for all positive integers can be found in [6]. The following discussion of the two squares theorem for prime numbers has been adapted from [2].

Before we can prove the two squares theorem for primes, we must find a way to generate sets of points that is a lattice. Let $\alpha$ and $\beta$ be real numbers such that $\alpha \neq 0$. Then for each ordered pair of integers, $(u, v)$, let $x_{(u,v)} = \alpha u + \beta v$ and let $y_{(u,v)} = v$. Then the set of points

$$L = \{\cup_{(u,v)}(x_{(u,v)}, y_{(u,v)})\} \tag{11}$$

is a lattice.

To see intuitively why $L$ must be a lattice, first let $\alpha = 1$ and let $\beta = 0$. Then the lattice $L_1$ is made up of the points in $\{\cup_{(u,v)}(u, v)\}$. Since $u$ and $v$ are both integers, $L_1$ is the integer lattice. Now let $\alpha = 2$ and let $\beta = 2$. The lattice we generate with these values, $L_2 = \{\cup_{(u,v)}(x_{(u,v)}, y_{(u,v)})\} = \{\cup_{(u,v)}(2u + 2v, v)\}$ is shown in Figure 27. As another example, let $\alpha = 3$ and let $\beta = 1$. The lattice $L_3$ generated by these values for $\alpha$ and $\beta$ is given by $L_3 = \{\cup_{(u,v)}(3u + v, v)\}$ and is shown in figure 27. Though we won't show it here, the set of points $\{\cup_{(u,v)}(\alpha u + \beta v, v)\}$ is a lattice for any values of $\alpha$ and $\beta$ we choose as long as $\alpha \neq 0$.

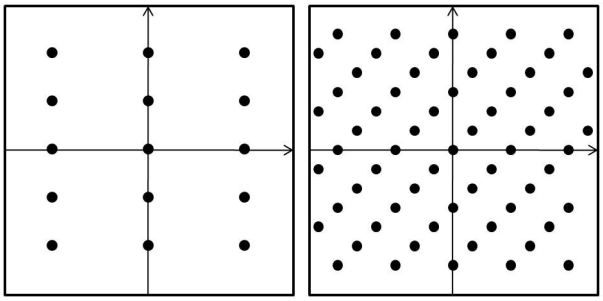

Figure 27: Left: The lattice $L_2$ which is generated by equation (11) where $\alpha = 2$ and $\beta = 2$. Right: The lattice $L_3$ which is generated by equation (11) where $\alpha = 3$ and $\beta = 1$.

The points $(0, 0)$, $(\alpha, 0)$, $(\beta, 1)$, and $(\alpha+\beta, 1)$ are the vertices of a primitive parallelogram that defines $L$. This means the area of this primitive parallelogram is $\alpha \cdot 1 = \alpha = d$.

Here we state two lemmas which we'll need to prove the two squares theorem for primes. We'll prove the first lemma here. A proof of the second can be found in [2].

**Lemma 5.6.** *The square of an even number is divisible by* 4. *The number preceding the square of an odd number has remainder* 1 *upon division by* 4.

*Proof.* Let $n$ be an even number. Then for some integer $k$, $n = 2k$. This means $n^2 = (2k)^2 = 4k^2$. Thus, $n^2$ is divisible by 4.

Let $n$ be an odd number. Then the number preceding the square of $n$ is $n^2 - 1 = (n+1)(n-1)$. Since $n$ is odd, $n+1$ and $n-1$ are both even, and therefore $(n+1)(n-1)$ is divisible by 4.

□

**Lemma 5.7.** *Let $p$ be a prime of the form $4k+1$. Then there exists an integer $c$ for which $c^2 + 1 \equiv 0 (mod\ p)$.*

**Theorem 5.8.** *Let $p$ be a prime number. If $p = 2$ or $p$ is of the form $4k+1$, then $p$ can be written as the sum of the squares of two positive integers. If $p$ is of the form $4k+3$, then $p$ cannot be written as the sum of squares of two positive integers.*

*Proof.* Let $p$ be a prime number such that $p = 2$ or $p = 4k+1$ for some integer $k$. By Lemma 5.7, there is an integer, $a$, for which $a^2+1$ is divisible by $p$. Note that when $p = 2$, such an $a$ exists as well, since $(1)^2 + 1 = 2$ is divisible by 2. Fix $a$ such that $a^2 + 1$ is divisible by $p$.

Consider the lattice $L$ where the lattice points $(x, y)$, satisfy $x = pu + av$ and $y = v$ for $u, v \in \mathbb{Z}$. Let $d$ be the area of each of the parallelograms that determine $L$. From the discussion above concerning area of the primitive parallelogram that determines a lattice, $L$, $d = p$. Since $x^2 + y^2 = p(pu^2 + 2auv) + (a^2+1)v^2$ and $(a^2+1)$ is divisible by $p$, $x^2 + y^2$ is divisible by $p$.

Consider the circle, $C$, that is centered at the origin with radius $2\sqrt{\frac{d}{\pi}}$. Since $A(C) = 4d$, by Corollary 5.5, there must be a lattice point, $(x, y)$ in the interior or on the boundary of $C$ that is not the origin. Fix such a lattice point, and call it $(x, y)$. Since $(x, y)$ is either on the boundary of $C$ or in the interior of $C$, $(x, y)$ must satisfy $x^2 + y^2 \leq \frac{4d}{\pi} = \frac{4p}{\pi} < 2p$. Since $(x, y)$ is not the origin, $x^2 + y^2$ must be positive. Since $x^2 + y^2$ is divisible by $p$ and is less than $2p$, it must be the case that $x^2 + y^2 = p$. Thus, since $x$ and $y$ are integers, $p$ can be written as the sum of two squares.

For the second part of the theorem, let $p$ be a prime number so that $p = 4k+3$ for some integer $k$. By Lemma 5.6, the square of an even number, $n$ is divisible by 4, that is, $n^2 \equiv 0 (\text{mod } 4)$. Also by Lemma 5.6, the number preceding the square of an odd number, $m$ is divisible by 4, that is, $m^2 \equiv 1 (\text{mod } 4)$. This means that for a sum of two squares, $s$, $s \equiv 0 (\text{mod } 4)$ when $s$ is the sum of squares of two even integers, $s \equiv 1 (\text{mod } 4)$ when $s$ is the sum of squares of an even integer and an odd integer, or $s \equiv 2 \ (\text{mod } 4)$ when $s$ is the sum of squares of two odd integers. However, it is never the case that $s \equiv 3 \ (\text{mod } 4)$. Thus, $p$ is not a sum of two squares.

□

We can actually use the Two Squares Theorem to gain more information about the integer lattice, $\mathbb{Z}^2$. The only numbers that can be equal to the area of a lattice square in $\mathbb{Z}^2$ are integers that can be written as the sum of two squares of positive integers.

### 5.3.2 The Orchard Problem

Now we will examine an entirely different application of Minkowski's theorem, the Orchard Problem. To discuss the Orchard Problem, we will return to working in the integer lattice. Our discussion of the Orchard Problem and its solution has been adapted from [3].

The orchard problem, as stated in [3], asks us to consider a circular orchard with radius fifty feet that has its center at the origin. A tree is planted at each lattice point that lies in the orchard. Assuming all trees have the same radius, we must show a person standing at the origin cannot see out of the orchard no matter which direction he or she looks when the trees have radius greater than $\frac{1}{50}$ units.

Though there are several solutions to this problem, one relatively simple solution involves the application of Minkowski's theorem, and this is the solution we will present here.

Consider the circular orchard with radius 50 units centered at the origin. Let the line segment $\overline{AB}$ which passes through the origin be some diameter of the orchard (see Figure 28). Let the radius of a tree, $r$, be greater than $\frac{1}{50}$. We must have $r < \frac{1}{2}$ since the trees would grow into each other if $r$ were any bigger than $\frac{1}{2}$. Choose $p$ so $\frac{1}{50} < p < r$, and draw a line segment, $l_1$, of length $2p$ which has its midpoint at $A$ and which lies tangent to the orchard. Let $C$ and $D$ be the endpoints of $l_1$. Also draw a line segment, $l_2$, of length $2p$ which has its midpoint at $B$. Let $E$ and $F$ be the endpoints of $l_2$ (see figure 28).

The rectangle $CDEF$ is bounded, convex, symmetric about the origin, and has length equal to the length of the line segment $\overline{AB}$, which is 100, and width equal to the length of $\overline{CD}$ (or $\overline{EF}$), which is $2p$. Since $p > \frac{1}{50}$, $A(CDEF) = (100)(2p) = 200p > (200)\frac{1}{50} = 4$. Therefore, by Minkowski's theorem, the rectangle $CDEF$ contains some lattice point $T$ other than the origin. Like all of the trees planted in the orchard, the tree at the lattice point $T$ has radius $r$. Since $r > p$, the tree planted at $T$ must cross the line $\overline{AB}$. By symmetry, the point $-T$ is also in $CDEF$, and as with the tree planted at $T$, the tree planted at the point $-T$ must also cross the line $\overline{AB}$. Therefore, as long as $T$ does not lie outside the orchard, since we chose the diameter $\overline{AB}$ arbitrarily, no matter which way we look from the origin, our view is blocked by a tree crossing $\overline{AB}$ (see Figure 28).

Now we only need to show $T$ lies inside the orchard. We do so by assuming the opposite and finding a contradiction. Assume $T$ lies outside of the orchard (but inside the rectangle $CDEF$). The furthest point from the origin living in the rectangle $CDEF$ lies at a vertex of $CDEF$. The distance from any vertex of $CDEF$ to the origin is $\sqrt{50^2 + p^2}$ , so the distance from $T$ to the origin, $d(T, \mathbf{0})$ must be less than $d(C, \mathbf{0}) = \sqrt{50^2 + p^2}$ where $d(X, Y)$ denotes the Euclidian distance between the points $X$ and $Y$ in $\mathbb{R}^2$ and $\mathbf{0}$ is the origin. Since $p < 1$, $d(T, \mathbf{0}) \leq d(C, \mathbf{0}) < \sqrt{2501}$. Since $T$ is outside the orchard but inside the rectangle $CDEF$, $50 < d(T, \mathbf{0}) < \sqrt{2501} \implies 2500 < (d(T, \mathbf{0}))^2 < 2501$. Since $T$ is some lattice point, $(x, y)$, $(d(T, \mathbf{0}))^2 = x^2 + y^2$. Since $(x, y)$ is a lattice point, $x$ and $y$ are integers, and therefore $(d(T, \mathbf{0}))^2$ is an integer. However, since $2500 < (d(T, \mathbf{0}))^2 < 2501$, $(d(T, \mathbf{0}))^2$ is not an integer. Thus, we have a contradiction, and $T$ must lie inside the orchard. Hence, we've shown when $r > \frac{1}{50}$, a person standing at the origin cannot see out of the orchard no matter in which direction he or she looks.

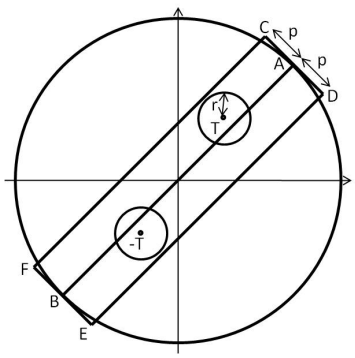


Figure 28: Our view from the origin along some diagonal $\overline{AB}$ is always blocked in both directions by trees planted at the lattice points $T$ and $-T$. Note that the size of the rectangle $CDEF$ is exaggerated in this figure.

# 6 Minkowski's Theorem in $\mathbb{R}^n$

As with Pick's theorem, we can extend Minkowski's Theorem to bounded, convex regions in $\mathbb{R}^n$. However, unlike Pick's Theorem, Minkowski's Theorem generalizes to $\mathbb{R}^n$ quite easily. We first prove a version of Blichfeldt's Lemma for convex, bounded regions in $\mathbb{R}^n$, and then we proceed to prove Minkowski's Theorem for convex, bounded regions in $\mathbb{R}^n$. The proof of Blichfeldt's Lemma and that of Minkowski's theorem in $\mathbb{R}^n$ are more difficult to visualize. However, the proofs are very close to those of Blichfeldt's Lemma and Minkowski's Theorem in $\mathbb{R}^2$, so the pictures that go along with the proofs of Blichfeldt's Lemma and Minkowski's Theorem in $\mathbb{R}^2$ can be used to get some idea of what's happening geometrically in $\mathbb{R}^n$.

## 6.1 Proving Minkowski's Theorem in $\mathbb{R}^n$

The proofs that follow are my own, though they are extensively based on the proofs of the analogues of these theorems in $\mathbb{R}^2$ given in [6]. Throughout, let $V(X)$ denote the n-dimensional volume of the region $X$.

**Lemma 6.1.** *Let $R$ be a bounded set in $\mathbb{R}^n$ with volume greater than 1. Then $R$ contains two distinct points $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ such that the point $(y_1 - x_1, y_2 - x_2, \ldots, y_n - x_n)$ is an integer point in $\mathbb{R}^n$.*

*Proof.* Let $R$ be a bounded set in $\mathbb{R}^n$ with volume greater than 1. Let $C$ be the half-open unit hypercube. That is, let $C = \{(x_1, x_2, \ldots, x_n) | 0 \leq x_1 < 1, \leq x_2 < 1, \ldots, 0 \leq x_n < 1\}$. For each point, $z \in \mathbb{Z}^n$, let $C_z = C + z$ be the translation of $C$ along the lattice line segment $l_z$, with endpoints $(0, 0)$ and $z$. Note that $z$ is the only integer point in $C_z$. Let $R_z = R \cap C_z$. Since $R$ is bounded, there are finitely many of the sets $R_z$. Let $R_z - z$ be the translation of $R_z$ along the lattice line segment $l_z$. Note that $R_z - z$ is in $C$. Since translation is a plane isometry, it preserves area, so $V(R_z - z) = V(R_z)$. It follows that

$$\sum_{z\in\mathbb{Z}^n} V(R_z - z) = \sum_{z\in\mathbb{Z}^n} V(R_z) = V(\cup_{z\in\mathbb{Z}^n}(R_z)) = V(R) > 1.$$

We can imagine placing all of the sets $R_z - z$ together in $C$. Since $\sum_{z\in\mathbb{Z}^n} V(R_z - z) > 1$, $V(C) = 1$, and all of the sets $R_z - z$ are in $C$, there are integer points $v$ and $w$ such that $(R_v - v) \cap (R_w - w) \neq \emptyset$. Let $r \in (R_v - v) \cap (R_w - w)$. Then there are points $r_v \in R_v$ and $r_w \in R_w$ such that $r = r_v - v = r_w - w$. Note that $r_v, r_w \in R$ and $v$ and $w$ are integer points. Since $r_v - v = r_w - w \Longrightarrow r_v - r_w = v - w$, there are two distinct points in $R$, $r_v$ and $r_w$, such that $r_v - r_w$ is an integer point.

□

We will need one additional fact to prove Minkowski's Theorem in $\mathbb{R}^n$. Recall that when length in a region, $R$, in $\mathbb{R}^2$ is changed by a factor of $k$, the area of $R$ is changed by a factor of $k^2$ where $k$ is a positive real number. Similarly, when length in a region, $R$ in $\mathbb{R}^n$ is changed by a factor of $k$, the volume of $R$ is changed by a factor of $k^n$. As with the case in two dimensions, this can be shown using linear algebra. Let $M : \mathbb{R}^n \to \mathbb{R}^n$ be the linear transformation given by $M\mathbf{x} = n\mathbf{x}$ where $\mathbf{x}$ is a vector in $\mathbb{R}^n$ emanating from the origin with endpoint at a lattice point and $M$ is the $n \times n$ matrix

$$M = \begin{bmatrix} k & 0 & \dots & 0 \\ 0 & k & \dots & 0 \\ \dots & & & \dots \\ 0 & 0 & \dots & k \end{bmatrix}.$$

Under $M$, the vector $\mathbf{v} = \langle x_1, x_2, \dots, x_n\rangle$ is mapped to the vector $k\mathbf{v} = \langle kx_1, kx_2, \dots, kx_n\rangle = k\langle x_1, x_2, \dots, x_n\rangle$ which results in the length of the vector $\mathbf{v}$ changing by a factor of $k$. Since $\det(M) = k^n$, the volume of the image of any bounded region, $R$, in $\mathbb{R}^n$ is different from the volume of $R$ by a factor of $k^n$.

**Theorem 6.2.** *If $R$ is a bounded, convex region in $\mathbb{R}^n$ having volume greater than $2^n$ and is symmetric about the origin, then $R$ contains an integer point other than the origin.*

*Proof.* Let $R$ be a bounded, convex region in $\mathbb{R}^n$ that is symmetric about the origin and has volume greater than $2^n$. Consider the region $R' = \{\frac{1}{2}x | x \in R\}$. Note that $V(R') = \frac{1}{2^n}V(R) > 1$. Since $R'$ is just a smaller version of $R$, it is convex, closed, and symmetric about the origin. It follows that since $V(R') > 1$, by Lemma 6.1, there are points $x'$ and $y'$ in $R'$ such that $x' - y'$ is a nonzero integer point. Since $x', y' \in R'$ and $R' = \{\frac{1}{2}x | x \in R\}$, $2x', 2y' \in R$. Since $R$ is symmetric about the origin, $-2y' \in R$. The fact that $R$ is convex ensures that every point on the line segment between $2x'$ and $-2y'$ is in $R$. Therefore, $\frac{1}{2}(2x') + (1 - \frac{1}{2})(-2y') = x' - y'$ is in $R$. Since $x' - y'$ is a non-zero integer point, it satisfies the theorem.

□

Though we will not pursue it here, it is possible to prove Minkowski's theorem for an arbitrary lattice in $\mathbb{R}^n$. Those interested in the proof should see [8].

### 6.2 Applications of Minkowski's Theorem in $\mathbb{R}^n$

As with Minkowski's theorem in $\mathbb{R}^2$, there are many applications of Minkowski's theorem in $\mathbb{R}^n$. Though we won't elaborate on any of these applications here, we will list a few of them.

First, there are many fundamental facts in algebraic number theory which can be proved using Minkowski's theorem in $\mathbb{R}^n$ [7]. There are also some more elementary results in number theory that can be obtained using Minkowski's lattice point theorem in $\mathbb{R}^n$. These include the Four Squares Theorem, which states that every natural number can be written as the sum of four squares of nonnegative integers, and a theorem from Legendre that gives the conditions under which the equation $ax^2+by^2+cz^2=0$, where $a, b$, and $c$ are relatively prime, square-free integers which do not all have the same sign, has non-trivial solutions [7].

# 7 Conclusions

We've employed some basic facts and definitions about lattices to investigate two theorems, Pick's Theorem and Minkowski's Theorem. Both Pick's theorem and Minkowski's Theorem have a very wide range of extensions and applications reaching far beyond anything we've discussed here. While at first glance, the two theorems seem to address entirely different questions, Pick's theorem involves finding the area of lattice polygons, while Minkowski's Theorem involves determining when a convex region in $\mathbb{R}^2$ centered at a lattice point contains a lattice point other than its center, we find through examining extensions of both theorems that they are more closely related than they seem at first. In the end, both give us information about the number of lattice points in a particular region, and both have applications to other branches of mathematics.

# 8 Acknowledgements

I would like to thank my advisors Professor Marie Snipes and Professor Judy Holdener for answering all of my questions regarding the subject matter of this paper and for offering helpful feedback on preliminary drafts. I would also like to thank Professor Holdener for her help in choosing a topic for the paper and Yinan Yu for reading and commenting on a draft of the paper.

# References

[1] Bridger, Mark, Andrei Zelevinsky. "Visibles Revisited." *The College Mathematics Journal.* 36 (2005), 289-300.

[2] Erdos, Paul, Janos Suranyi. *Topics in the Theory of Numbers.* Translated by Bary Guiduli. New York: Springer, 2003.

[3] Honsberger, Ross. "The Orchard Problem." *Biscuits of Number Theory*. Edited by Arthur Benjamin and Ezra Brown. Washington, D.C.: Mathematical Association of America, 2009.

[4] Poole, David. *Linear Algebra: A Modern Introduction*. Australia: Brooks/Cole-Thomson Learning, 2006.

[5] Rotman, Joseph J. *A First Course in Abstract Algebra*. Upper Saddle River, N.J.: Prentice Hall, 2006.

[6] Sally, Judith D., and Paul Sally. *Roots to Research: A Vertical Development of Mathematical Problems*. Providence, RI: American Mathematical Society, 2007.

[7] Scharlau, Winfried, Hans Opolka. *From Fermat to Minkowski: Lectures on the Theory of Numbers and Its Historical Development*. New York: Springer-Verlag, 1985.

[8] Stein, Sherman K., and Sandor Szabo. *Algebra and Tiling: Homomorphisms in the Service of Geometry*. Washington D.C.: Mathematical Association of America, 1994.

[9] Varberg, Dale E. "Pick's Theorem Revisited." *American Mathematical Monthly*. 92 (1985), 584-587.