Artemis Pados

UM 170 Lattice Point Geometry Exercise Portfolio

Stanford University Online High School

1 Lattice Polygon Investigations

Exercise 1 Is it possible to construct a regular lattice 3-gon (i.e. an equilateral and equiangular lattice triangle)? If so, provide an example. If not, prove it.

Solution We will use proof by contradiction to show that it is not possible to construct a regular lattice 3-gon. Assume that there exists a regular lattice 3-gon, without loss of generality with vertices at points $O = (0,0)$, $A = (x_1, y_1)$, $B = (x_2, y_2)$, for some $\theta \in [0°, 120°)$ as in Fig. 1. Note: You can always translate a triangle such that one vertex is at the origin and the other two are in the first or second quadrant. If the original points are at integer coordinates $(x_1', y_1'), (x_2', y_2')$, and (x_3', y_3'), define $y_0 \triangleq \min\{y_1', y_2', y_3'\}$ and $x_0 \triangleq x_i'$ where x_i' is the x-coordinate of point (x_i', y_0). Then, translate all three vertices $(x_1', y_1'), (x_2', y_2')$, and (x_3', y_3') to new integer points $(x_1' - x_0, y_1' - y_0), (x_2' - x_0, y_2' - y_0)$, and $(x_3' - x_0, y_3' - y_0)$ as in Fig. 1.

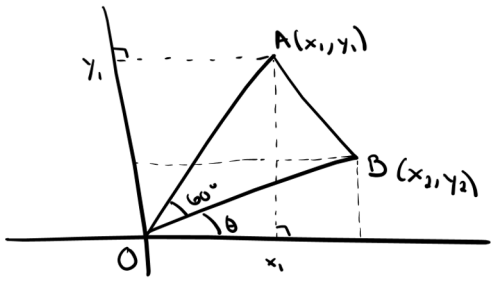


Figure 1: A regular 3-gon.

By the definition of a regular lattice 3-gon, $\angle AOB = 60°$. Then,

$$\tan(60° + \theta) = \frac{y_1}{|x_1|} = \frac{\tan(60°) - \tan\theta}{1 + \tan(60°)\tan\theta} = \frac{\sqrt{3} - \tan\theta}{1 + \sqrt{3}\tan\theta}, \tag{1}$$

which implies that $\frac{\sqrt{3}-\tan\theta}{1+\sqrt{3}\tan\theta}$ is rational. Also, $\tan\theta = \frac{y_2}{|x_2|}$ is rational. Therefore, there exist integers k, l, m, n such that

$$\frac{\sqrt{3} - \tan\theta}{1 + \sqrt{3}\tan\theta} = \frac{k}{l} \text{ and } \tan\theta = \frac{m}{n}. \tag{2}$$

Due to (2), $\sqrt{3} - \frac{m}{n} = \frac{k}{l}(1 + \sqrt{3}(\frac{m}{n})) \implies \sqrt{3} = \frac{\frac{k}{l} + \frac{m}{n}}{1 - \frac{km}{ln}}$ which implies that $\sqrt{3}$ is rational. This is a contradiction (we know that $\sqrt{3}$ is irrational - it is easy to prove).

We conclude that there is no regular lattice 3-gon. □

Exercise 2 Is it possible to construct a regular lattice 4-gon (i.e. a square)? If so, provide an example. If not, prove it.

Solution Yes (easily!). Consider the regular lattice square (0,0), (0,1), (1,1), (1,0). Note: This happens to be a primitive lattice as well (there is no integer in the (0,1) subset of $\mathbb{R}$). □

Exercise 3 Is it possible to construct a regular lattice pentagon (5-gon)? If so, provide an example. If not, prove it.

Solution We will use proof by contradiction to show that it is not possible to construct a regular lattice pentagon.

Assume that there exists a regular lattice 5-gon, without loss of generality with one vertex at $O = (0,0)$ and all

other vertecies in the first and second quadrants, as in Fig. 2. Note: You can always translate a lattice polygon in the first two quadrants with one vertex at the origin following the argument of Exercise 1.

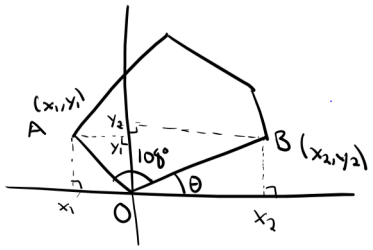


Figure 2: A regular 5-gon.

By the definition of a regular lattice 5-gon, $\angle AOB = 108^\circ$ and $\theta \in [0^\circ, 72^\circ)$. Then,

$$\tan(180^\circ - 108^\circ - \theta) = \frac{y_1}{|x_1|} = \tan(72^\circ - \theta) = \frac{\tan 72^\circ - \tan\theta}{1 + \tan 72^\circ \tan\theta}, \tag{3}$$

which implies that $\frac{\tan 72^\circ - \tan\theta}{1+\tan 72^\circ \tan\theta}$ is rational. Also, $\tan\theta = \frac{y_2}{x_2}$ is rational. Therefore, there exist integers k, l, m, n such that

$$\frac{\tan 72^\circ - \tan\theta}{1 + \tan 72^\circ \tan\theta} = \frac{k}{l} \text{ and } \tan\theta = \frac{m}{n}. \tag{4}$$

Due to (4), $\tan 72^\circ - \frac{m}{n} = \frac{k}{l}(1 + \tan 72^\circ(\frac{m}{n})) \implies \tan 72^\circ = \frac{\frac{k}{l}+\frac{m}{n}}{1-\frac{km}{ln}}$ which implies that $\tan 72^\circ$ is rational. We also know that $\tan 72^\circ = \frac{\sqrt{10+2\sqrt{5}}}{\sqrt{5}-1}$, therefore $\frac{\sqrt{10+2\sqrt{5}}}{\sqrt{5}-1}$ is rational, i.e. there exist integers b and c such that

$$\frac{\sqrt{10+2\sqrt{5}}}{\sqrt{5}-1} = \frac{b}{c}. \tag{5}$$

Squaring both sides of (5) we obtain $\frac{10+2\sqrt{5}}{5+1-2\sqrt{5}} = \frac{b^2}{c^2} \implies \sqrt{5} = \frac{6b^2-10c^2}{2b^2+2c^2}$; hence, $\sqrt{5}$ is rational. This is a contradiction. We know that $\sqrt{5}$ is irrational (it is easy to prove).

We conclude that there is no regular lattice 5-gon. □

Exercise 4 Show that the cosine of each interior and exterior angle of any regular lattice polygon must be rational. Hint: One way to do this is to use vectors and the dot product!

Solution Consider an arbitrary regular lattice polygon with angle $\angle AOB$ on the origin. Note: You can always translate a polygon as in Fig. 3.

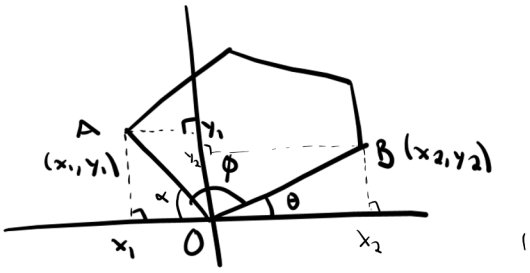


Figure 3: A regular polygon.

Then, $\cos\phi = \cos(180^\circ - (\alpha+\theta)) = -\cos(\alpha+\theta) = -(\cos\alpha\cos\theta - \sin\alpha\sin\theta) = \frac{|x_1|}{|AO|}\frac{x_2}{|BO|} - \frac{y_1}{|AO|}\frac{y_2}{|BO|}$ where $|AO| = |BO|$ denote the common length of a side of the polygon. Therefore, $\cos\phi = \frac{|x_1|x_2 - y_1y_2}{|AO|^2} = \frac{|x_1|x_2 - y_1y_2}{x_1^2+y_1^2}$ which is a rational number. Also, $\cos\phi = -\cos(180^\circ - \phi)$. We conclude that the cosine of each interior and exterior angle of any regular lattice polygon is rational. □

Exercise 5 Use Exercise 4 to show that it is not possible to construct a regular lattice octagon (8-gon).

Solution A regular lattice octagon has interior angles of 135°. Then,

$$\cos 135^\circ = \cos(90^\circ + 45^\circ) = -\cos 45^\circ = -\frac{\sqrt{2}}{2} \text{ irrational.}$$

By Exercise 4, it is not possible to construct a regular lattice octagon. □

Exercise 6 Show that if α is a lattice angle and if the measure of α is not equal to $\pi/2$ or an odd integer multiple of $\pi/2$, then the tangent of α is a rational number.

Solution Consider three arbitrary lattice points A, O, B and the corresponding angle $\angle AOB$. Without loss of generality, O is at the origin and $0^\circ < \angle AOB < 180^\circ$ ($\tan(180^\circ - \phi) = -\tan\phi$). That is, w.l.o.g. points A and B are in the first and second quadrant, as in Fig. 4 for example.

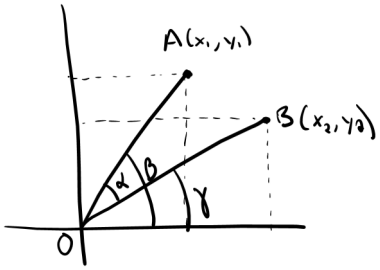


Figure 4: Lattice angle AOB.

By the description of the problem, $\angle AOB \neq \frac{\pi}{2}$ therefore $\tan\angle AOB$ is defined. Following the notation in Fig. 4, $\tan(\angle AOB) = \tan\alpha = \tan(\beta-\gamma) = \frac{\tan\beta - \tan\gamma}{1+\tan\beta\tan\gamma} = \frac{\frac{y_1}{x_1} - \frac{y_2}{x_2}}{1+\frac{y_1y_2}{x_1x_2}}$, where x_1, y_1, x_2, y_2 are integers. Therefore, $\tan\alpha$ is rational. Note: Since $\angle AOB \neq \frac{\pi}{2}$, $\overrightarrow{OA}\cdot\overrightarrow{OB} \neq 0 \implies x_1x_2 + y_1y_2 \neq 0 \implies x_1x_2 \neq -y_1y_2 \implies 1 + \frac{y_1y_2}{x_1x_2} \neq 0$ as needed for the denominator of the final rational expression . □

Exercise 7 Make a conjecture about the positive integers n for which it is possible construct a regular lattice n-gon. Although you do not need to provide a formal proof of your conjecture here, you should provide sufficient justification and reasoning (beyond simply citing the exercises that you have already solved above) to indicate why you believe your conjecture is valid.

Solution Conjecture: The only regular lattice n-gon is the lattice square (i.e., $n = 4$).

In Exercise 1, we saw that there is no regular lattice 3-gon. In Exercise 2, we saw that there exist regular lattice 4-gons. I will support my conjecture through a contradiction argument. Assume that there is $n > 4$ for which a regular lattice n-gon exists. Since the n-gon is regular, each angle of the n-gon is $\phi = \frac{n-2}{n}\pi$ (easy to prove, shown in Discrete Math of Fall Semester). But, ϕ is a lattice angle, therefore $\tan\phi = \tan(\frac{n-2}{n}\pi)$, $n > 4$, is rational by Exercise 6. But, $\tan(\frac{n-2}{n}\pi) = \tan(\pi - \frac{2}{n}\pi) = -\tan(\frac{2}{n}\pi)$, $n > 4$. Without proof, $\tan(\frac{2}{n}\pi)$, $n > 4$, is rational only for $\frac{2}{n}\pi = \frac{\pi}{4} = 8$. Hence, the only other possible case of a regular lattice n-gon (other than 4-gons) is

the 8-gon. But in Exercise 5 we showed that no regular lattice 8-gon exists. This is a contradiction that supports my conjecture. The missing piece to complete the proof is that $\tan(\frac{2}{n}\pi)$, $n > 4$, is rational only for $n = 8$. □

Exercise 8 Is it possible to construct a lattice square whose area is not a perfect square? If so, provide an example. If not, prove it.

Solution Yes, it is possible to construct a lattice square whose area is not a perfect square. Consider the following four lattice points $A = (0, 1), B = (1, 3), C = (3, 1), D = (1, 0)$. It is easy to show that ABCD is a square by seeing that all angles are equal to 90° and all sides are of equal length.

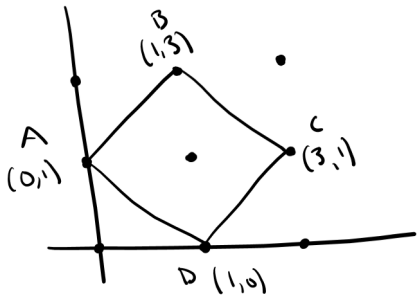


Figure 5: Lattice square ABCD.

In fact, the length of a side is $\sqrt{1^2 + 1^2} = \sqrt{2}$. Therefore, the area of $ABCD = \sqrt{2}^2 = 2$ and 2 is not a perfect square. We conclude that we can construct a lattice square whose area is not a perfect square.

Exercise 9 Is it possible to construct a lattice square whose area is not an integer? If so, provide an example. If not, prove it.

Solution Consider an arbitrary lattice-point line segment AB, without loss of generality in the first quadrant, with end point $A = (a, b)$ and $B = (c, d)$ where $a, b, c, d \in \mathbb{Z}^+$.

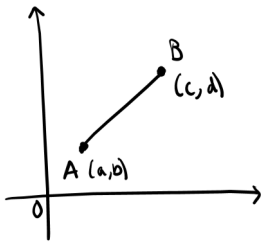


Figure 6: Lattice point line segment AB.

The length of segment AB is $\sqrt{(a-c)^2 + (b-d)^2}$ by the distance formula (Pythagorean Theorem). The radicand is necessarily in $\mathbb{Z}^+$ because $a, b, c, d \in \mathbb{Z}^+$. The area of a square with arbitrary side AB is $\sqrt{(a-c)^2 + (b-d)^2}^2 = (a-c)^2 + (b-d)^2$ which is integer. We conclude that every lattice square has integer area. □

Exercise 10 Show that there exists a lattice square with area n, where n is a positive integer, if and only if there exist non-negative integers a and b such that

$$n = a^2 + b^2.$$

Solution I will prove first the $\Longleftarrow$ direction of the iff statement.

Assume $\exists$ non-negative integers a, b such that $n = a^2 + b^2$. I will show that there exists a lattice square with area n.

Take the lattice points $(a, 0), (0, b), (b, a + b), (a + b, a)$. These define a lattice 4-gon. Each side of the 4-gon has length $l = \sqrt{a^2 + b^2}$ and angle $\angle DAB = 90°$. Therefore, it is a lattice square.

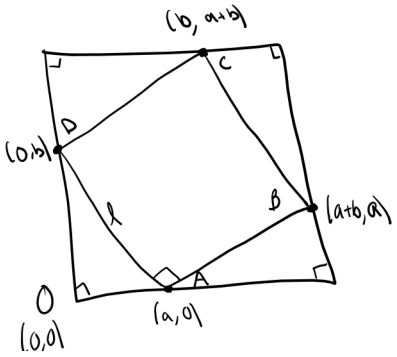


Figure 7: Lattice square ABCD.

The area of the lattice square is $l^2 = a^2 + b^2 = n$.

I will now prove the other direction $\Longrightarrow$ of the iff statement. Assume that there exists a lattice square with area n, where n is a positive integer. I will show that n can be written as $a^2 + b^2$ for some non-negative integers a, b.

If there exists a lattice square with area n integer, then $n = l^2$ for some $l > 0$ where l is the length of the side of the lattice square. You can always translate the lattice square and rename the vertices such that the lattice square takes the form ABCD in Fig. 7. Call the x-coordinate of A a and the y-coordinate of D b. By the right angle triangle $\triangle DOA$, $l^2 = n = a^2 + b^2$. $\square$

Exercise 11 Is it possible to construct a lattice triangle whose area is not an integer? If so, provide an example. If not, prove it.

Solution Consider an *arbitrary* triangle that without loss of generality has one vertex at the origin and the other two vertices $A = (x_1, y_1)$ and $B = (x_2, y_2)$ in the first or second quadrant. Fig. 8 below shows the case where A and B are in the first quadrant. The cases where A and B are both in the second quadrant or one is in the first quadrant and the other is in the second quadrant are treated similarly.

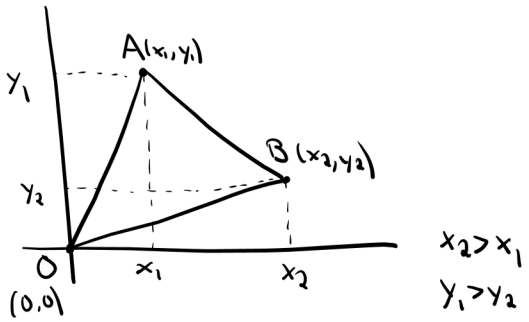


Figure 8: Triangle AOB.

Area of $\triangle AOB = x_2 y_1 - \frac{x_1 y_1}{2} - \frac{x_2 y_2}{2} - \frac{(x_2 - x_1)(y_1 - y_2)}{2} = \frac{x_2 y_1 - x_1 y_2}{2}$, $x_2 > x_1$ and $y_1 > y_2$.

We conclude that the area of $\triangle AOB$ is an integer iff $x_2y_1 - x_1y_2$ is even.

An example of non-integer area: Take $A = (0,1)$ and $B = (1,0)$. The area of this triangle is $\frac{1\cdot 1 - 0\cdot 0}{2} = \frac{1}{2}$ which is non-integer. $\square$

Exercise 12 Construct (at least) 5 lattice polygons with different areas. Keep in mind that the polygons do not need to be convex! Find the area of each polygon. What do you observe? Make a conjecture about the possible values of the area of a lattice polygon based on your computations in this problem. For example, do you think it's possible to achieve all integer areas? All rational areas? All real areas?

Solution

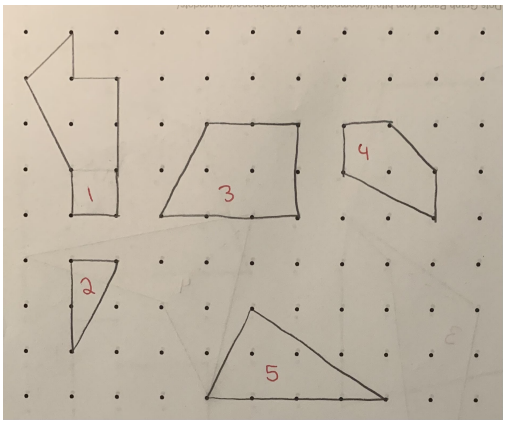


Figure 9: Lattice polygons.

Area of polygon $1 = 3 + 1 + \frac{1}{2} = \frac{9}{2}$
Area of polygon $2 = \frac{2\cdot 1}{2} = 1$
Area of polygon $3 = \frac{(3+2)2}{2} = 5$
Area of polygon $4 = (1 \cdot 1) + \frac{1\cdot 1}{2} + \frac{2\cdot 1}{2} = 1 + \frac{1}{2} + 1 = \frac{5}{2}$
Area of polygon $5 = \frac{4\cdot 2}{2} = 4$
I conjecture that the area of lattice polygons is rational.

Exercise 13 Make a conjecture about the possible values of B (the number of lattice points on the boundary) for a lattice triangle T with $I(T) = 1$. Although you do not need to provide a formal proof of your conjecture here, you should provide sufficient justification and reasoning (beyond simply citing computational work) to indicate why you believe your conjecture is valid.

Solution Without loss of generality, assume that the unique interior lattice point of the lattice triangles in question is at $(1,1)$. (If the lattice interior point were at (x_0, y_0), we would translate all pertinent lattice triangles by $x_0 - 1$ and $y_0 - 1$ so that the interior lattice point in question would end up at $(x_0 - (x_0 - 1), y_0 - (y_0 - 1)) = (1,1)$).

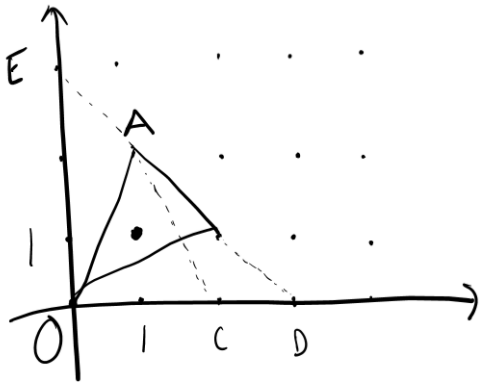


Figure 10: Triangles with one interior lattice point at (1,1).

For $\triangle OAB$, $B(T) = 3$.
For $\triangle OAC$, $B(T) = 4$.
For $\triangle OAD$, $B(T) = 6$.
For $\triangle OED$, $B(T) = 9$.
In all cases, $B(T) = 2 \cdot \text{Area}(T)$ which I claim/conjecture is true for every lattice T with one interior lattice point.
I will conjecture that no lattice triangle with one interior point lattice exists with $\text{Area}(T) > \frac{9}{2}$.
Therefore, I conjecture that $B(T) = 3, 4, 6, 9$ are the only possible values for the boundary lattice points of a lattice triangle with $I(T) = 1$.

Exercise 14 Construct (at least) 5 different non-congruent primitive lattice triangles, and find their area. Make a conjecture about the value of the area of a primitive lattice triangle.

Solution

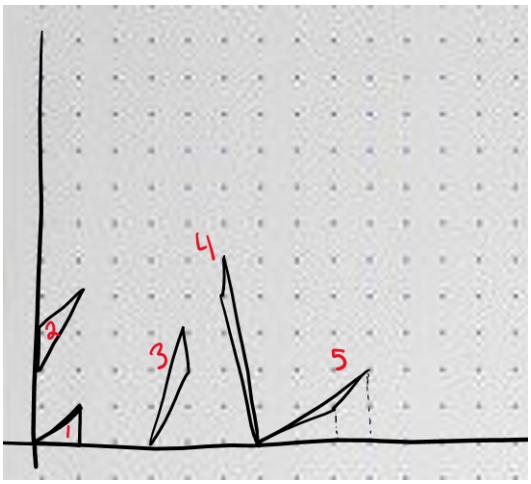


Figure 11: Non-congruent primitive triangles.

Triangles 1, 2, 3, 4, 5 are non-congruent primitive lattice triangles. Their areas are as follows:
Area of $\triangle 1 = \frac{1 \cdot 1}{2} = \frac{1}{2}$
Area of $\triangle 2 = \frac{1 \cdot 1}{2} = \frac{1}{2}$

Area of $\triangle 3 = \frac{1 \cdot 1}{2} = \frac{1}{2}$
Area of $\triangle 4 = \frac{1 \cdot 1}{2} = \frac{1}{2}$
Area of $\triangle 5 = \frac{3 \cdot 2}{2} - \frac{2 \cdot 1}{2} - \frac{(1+2)1}{2} = 3 - 1 - \frac{3}{2} = \frac{1}{2}$
I conjecture that the area of every primitive lattice triangle is 1/2.

Exercise 15 Construct several (at least 5) different polygons that contain 4 boundary lattice points and 6 interior lattice points. Keep in mind that the polygons do not need to be convex! Find the area of each polygon. What do you observe? Make a conjecture based on your observations in this exercise.

Solution

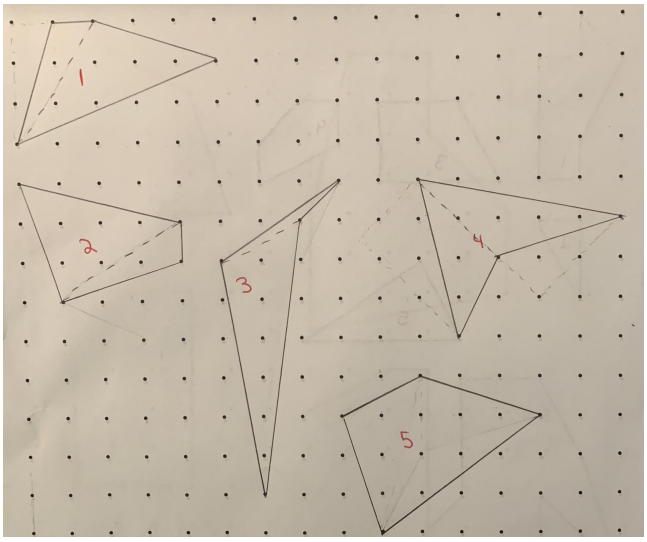


Figure 12: Lattice polygons with 4 boundary lattice points and 6 interior lattice points.

Area of polygon $1 = \frac{1 \cdot 3}{2} + \frac{11}{2} = \frac{14}{2} = 7$
Area of polygon $2 = \frac{1 \cdot 3}{2} + \frac{11}{2} = \frac{14}{2} = 7$
Area of polygon $3 = \frac{1}{2} + \frac{13}{2} = \frac{14}{2} = 7$
Area of polygon $4 = \frac{2\sqrt{2} \cdot \frac{3}{2}\sqrt{2}}{2} + \frac{2\sqrt{2} \cdot 2\sqrt{2}}{2} = 3 + 4 = 7$
Area of polygon $5 = \frac{5 \cdot 1}{2} + \frac{9}{2} = \frac{14}{2} = 7$
All the areas of the polygons I constructed with 4 boundary lattice points and 6 interior lattice points have the same value (7). I conjecture that the area of lattice polygons is dependent only on the number of boundary lattice points and interior lattice points of the polygon. □

Exercise 16 Find the area of each of the lattice polygons in Figure 13. Make a table that contains the following information for each polygon: the area of the polygon, the number of lattice points inside the polygon (I), and the number of lattice points on the boundary of the polygon (B).

Polygon	Area	I	B
1	3	1	6
2	4	2	6
3	5	3	6
4	6	4	6
5	1	0	4
6	$\frac{3}{2}$	0	5
7	2	0	6
8	$\frac{5}{2}$	0	7
9	9	4	12
10	6	2	10
11	6	1	12
12	$\frac{17}{2}$	3	13
Exercise 17 #1	$\frac{39}{2}$	13	15
Exercise 17 #2	$\frac{49}{2}$	19	13
Exercise 17 #3	16	8	18
Exercise 17 #4	$\frac{27}{2}$	8	13
Exercise 17 #5	$\frac{39}{2}$	14	13
Exercise 18	$\frac{11}{2}$	5	3

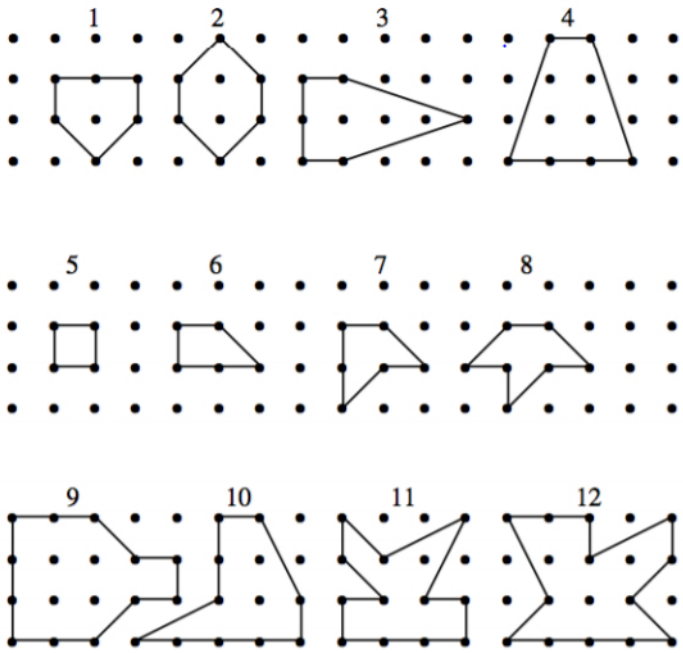


Figure 13: Find A, I, and B for each of these polygons.

Exercise 17 Construct 5 different lattice polygons. To keep this problem interesting, at least 3 of your polygons should be non-convex. All of your polygons should have at least 6 sides, and at least 10 boundary lattice points and at least 8 interior lattice points. For each of these 5 polygons, find the area, the number of lattice points inside the polygon, and the number of lattice points on the boundary of the polygon. Add this information to your table from Exercise 16.

Solution

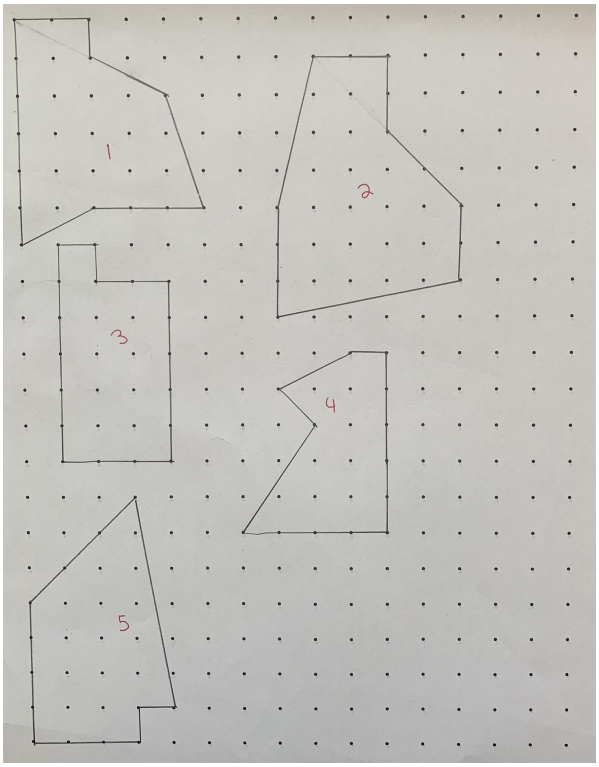


Figure 14: Lattice polygons with at least 6 sides, 10 boundary lattice points and 8 interior lattice points.

Exercise 18 Let P be the triangle with vertices $(0,0)$, $(3,1)$, and $(1,4)$. Find the area of P, the number of lattice points inside the polygon, and the number of lattice points on the boundary of the polygon. Add this information to your table from Exercise 16.

Solution

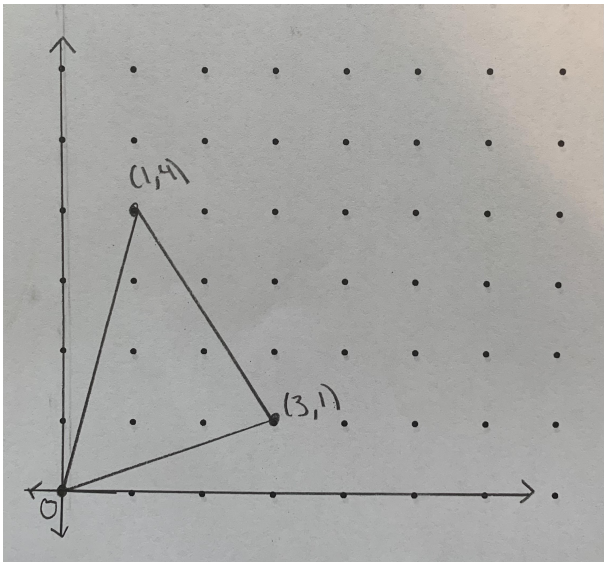


Figure 15: Triangle P.

Exercise 19 Based on your work so far, make a conjecture about the *area* of a lattice pentagon in the case when B (the number of lattice points on the boundary) is even and in the case when B is odd.

Solution I conjecture that the area of a lattice pentagon with even number of boundary lattice points is integer. I conjecture that with odd number of boundary lattice points, the area of a lattice pentagon is a multiple of $\frac{1}{2}$.

Exercise 20 Based on your work so far, conjecture a formula that relates the area of a lattice polygon to the number of lattice points inside the polygon and the number of lattice points on the boundary of the polygon. Explain how you obtained your conjecture, and why you think it makes sense (including a proof or partial proof if you have ideas). Although you do not need to provide a formal proof here, you should provide sufficient justification and reasoning to indicate why you believe your conjecture is valid. Please do not try to find the formula online or in another reference–it's so much more fun and interesting if you discover the formula on your own! If you're not sure where to start, start with thinking about a linear relationship. If I increases by 1 and B stays fixed, what happens to the area? Similarly, if B increases by 1 and I stays fixed, what happens to the area? Use these observations to try to find an equation that relates A, B, and I.

Solution If you take an arbitrary lattice polygon and keep the number on interior lattice points constant and increase the number of boundary lattice points by 1, the area increases by $\frac{1}{2}$. If you keep the number of boundary lattice points constant and increase the number on interior lattice points by 1, the area increases by 1 also. By testing with multiple of the examples we have gathered, you can see that the formula Area$= I + \frac{B}{2}$ is still off by a constant of -1. Therefore, I conjecture that the area of a lattice polygon P is $A(P) = I(P) + \frac{B(P)}{2} - 1$.

Exercise 21 Construct your own lattice polygon, and verify that the formula that you conjectured in Exercise 20 is satisfied. Your polygon should be at least somewhat interesting–for example, make it non-convex, and have at least 10 boundary lattice points and at least 8 interior lattice points.

Solution

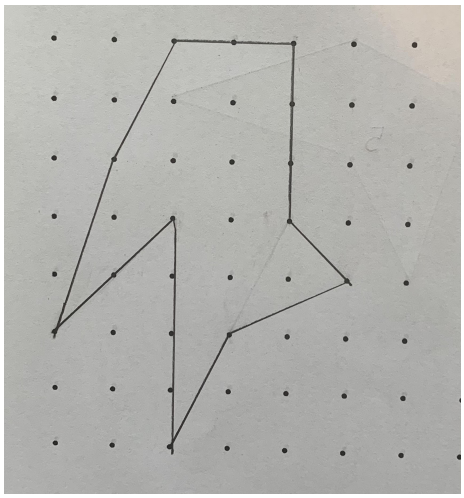


Figure 16: Lattice polygon P with 8 interior lattice points and 16 boundary lattice points.

The polygon P I constructed in Fig. 16 has $I(P) = 8$ and $B(P) = 16$. Therefore, by my conjecture in Exercise 20 $A(P) = 8 + \frac{16}{2} - 1 = 15$, which is accurate for this polygon. □

Exercise 22 Assuming that your conjecture in Exercise 20 is valid, make a conjecture about the possible values of the area of a lattice polygon. Can you construct a lattice polygon with area 5/2, for example? How about 5/3? Which real numbers are possible? Explain how you obtained your conjecture, and why you think it makes sense

(including a proof or partial proof if you have ideas). Although you do not need to provide a formal proof here, you should provide sufficient justification and reasoning to indicate why you believe your conjecture is valid.

Solution Assuming that my conjecture from Exercise 20 is correct, that is $A(P) = I(P) + \frac{B(P)}{2} - 1$, then it follows that $A(P)$ is a multiple of $\frac{1}{2}$ since $I(P),\ B(P) \in \mathbb{Z}^+$. $\square$

---

2 Basic Properties of Lattice Points in the Plane

Exercise 23 Does every lattice line segment have rational length? If so, prove it. If not, provide an example of a lattice line segment with non-rational length.

Solution Consider an arbitrary lattice line segment. Without loss of generality we can translate the segment such that one end is at the origin $O = (0, 0)$ and the other end $A = (x_1, y_1)$ is in the first or second quadrant. Fig. 17 shows the case where $x_1 > 0$, i.e. A is in the first quadrant. The case where $x_1 < 0$ (A is in the second quadrant) is treated similarly.

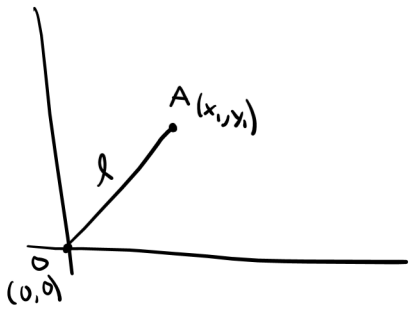


Figure 17: Line segment OA.

The length l is such that $l^2 = x_1^2 + y_1^2 \implies l = \sqrt{x_1^2 + y_1^2}$. Take $x_1 = 1$ and $y_1 = 1$. Then, $l = \sqrt{2}$ which is irrational.

We conclude that there is a lattice line segment that does not have rational length. □

Exercise 24 Make and prove a conjecture about the square of the length of any lattice line segment.

Solution By Exercise 23, $l^2 = x_1^2 + y_1^2$; x_1, y_1 are integers, therefore $l^2 \in \mathbb{Z}^+$. We conclude that the square of the length of any lattice line segment is integer. □

Exercise 25 Let L be a line with rational slope in the plane. Show that if there is a lattice point on L, then the y-intercept of L is rational.

Solution Consider an arbitrary line L with rational slope in the plane

$$f(x) = \frac{k}{l}x + b,\ k \in \mathbb{Z},\ l \in \mathbb{Z} - \{0\},\ b \in \mathbb{R}.$$

If there exists a lattice point on L, say $(m, f(m))$ where $m, f(m) \in \mathbb{Z}$, then $f(m) = \frac{k}{l}m + b \implies b = f(m) - \frac{km}{l} = \frac{lf(m) - km}{l}$, i.e. b is rational. □

Exercise 26 Let L be a line with rational slope in the plane. Show that if there is one lattice point on L, then there are infinitely many lattice points on L.

Solution Consider an arbitrary line L with rational slope in the plane

$$f(x) = \frac{k}{l}x + b,\ k \in \mathbb{Z},\ l \in \mathbb{Z} - \{0\},$$

and a lattice point $(m, f(m))$ on the line, i.e.

$$f(m) = \frac{k}{l}m + b$$

(by Exercise 25, b is rational). Consider the integer points $x = m+p\cdot l$, $p \in \mathbb{Z}$. Then, $f(m+p\cdot l) = \frac{k}{l}(m+pl)+b = \frac{k}{l}m + b + \frac{k}{l}pl = f(m) + pk$ which is integer.

We conclude that if L is a line with rational slope $f(x) = \frac{k}{l}x+b$ and goes through one lattice point $(m, f(m))$, then there are infinitely many lattice points $(m+pl, f(m+pl))$, $p \in \mathbb{Z}$, on L. □

Exercise 27 Let $p = (m, n)$ be a lattice point in the plane with $\gcd(m, n) = 1$. Show that there are no lattice points strictly between the origin $\mathbf{0} = (0, 0)$ and p on the line segment $\mathbf{0}p$. (Recall that the *greatest common divisor* of two integers a and b, denoted $\gcd(a, b)$ is largest integer d that is a divisor of both a and b.)

Solution Consider a lattice point $P = (m, n)$ with $\gcd(m, n) = 1$. Without loss of generality, $m, n \in \mathbb{Z}^+$ (if m or n or both are in $\mathbb{Z}^-$ the same arguments follow).

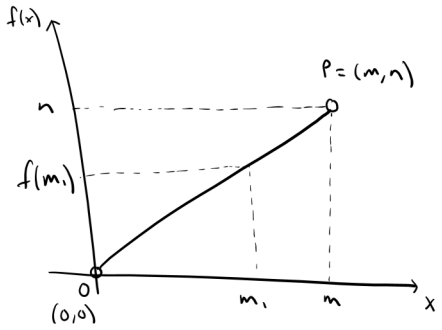


Figure 18: Lattice point P=(m, n) and line segment OP.

The line segment OP is

$$f(x) = \frac{n}{m}x,\ x \in (0, m).$$

I will show by contradiction that there are no lattice points on the line segment OP for $x \in (0, m)$.

Assume that there is $m_1 \in \mathbb{Z}^+$, $0 < m_1 < m$ such that $f(m_1) = \frac{n}{m}m_1 \in \mathbb{Z}^+$ (see Fig. 18). Then, $\frac{nm_1}{m} \in \mathbb{Z}^+$ implies that

$$gcd(nm_1, m) = m. \tag{6}$$

But, gcd is a multiplicative function in the sense that

$$gcd(nm_1, m) = gcd(n, m) \cdot gcd(m_1, m). \tag{7}$$

By (6) and (7), $gcd(m_1, m) = m$. This is a contradiction (impossible) because $m_1 < m$.

We conclude that there are no lattice points on OP if $P = (m, n)$ with $gcd(m, n) = 1$. □

Definition 1 A lattice point $p = (m, n)$ is **visible from the origin** or **visible** if there are no lattice points strictly between the origin $\mathbf{0} = (0, 0)$ and p on the line segment $\mathbf{0}p$.

Exercise 28 Show that if $p = (m, n)$ is a visible point on the lattice line L through the origin $(0, 0)$, then any lattice point on L is of the form (tm, tn) for some integer t.

Solution If $p = (m, n)$, $m, n \neq 0$, is a lattice point visible from the origin $O = (0, 0)$, then $gcd(m, n) = 1$. Otherwise, $(\frac{m}{gcd(m,n)}, \frac{n}{gcd(m,n)})$ is a lattice point on OP with $\frac{m}{gcd(m,n)} < m$ (contradiction).

Consider the line L through O and P defined by $f(x) = \frac{n}{m}x$. If $(q, f(q))$ is any lattice point on L, $f(q) = \frac{n}{m}q = \frac{nq}{m}$, $\in \mathbb{Z} \implies gcd(nq, m) = m \implies gcd(n, m) \cdot gcd(q, m) = m \implies gcd(q, m) = m \implies q = km$ and $f(q) = \frac{n}{m}k \cdot m = kn$, $k \in \mathbb{Z}$. □

Exercise 29 Let m and n be nonnegative integers. Show that there are exactly $\gcd(m,n)-1$ lattice points on the line segment between the origin and the point (m,n), not including the endpoints.

Solution Consider the line segment from $(0,0)$ to (m,n) where (m,n) is a lattice point,

$$y = \frac{n}{m}x,\ x \in (0,m).$$

Then,

$$y = \frac{n_1 gcd(n,m)}{m_1 gcd(n,m)}x,\ x \in (0,m).$$

For y to be in $\mathbb{Z}$, x must be a multiple of m_1 and $x \in (0,m) \implies 0 < x = k \cdot m_1 < m \implies 0 < x = k \cdot m_1 < gcd(n,m)m_1 \implies k = 1,2,...,gcd(n,m)-1$.

We conclude that there are $gcd(n,m)-1$ lattice points on the line segment from $(0,0)$ to (m,n) excluding the end points. □

Exercise 30 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

$$d_i = \gcd(a_{i+1}-a_i, b_{i+1}-b_i)$$

for $i = 1,2,\ldots,n-1$ and let

$$d_n = \gcd(a_1-a_n, b_1-b_n).$$

Show that the number of lattice points on the boundary of P is given by

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

Solution

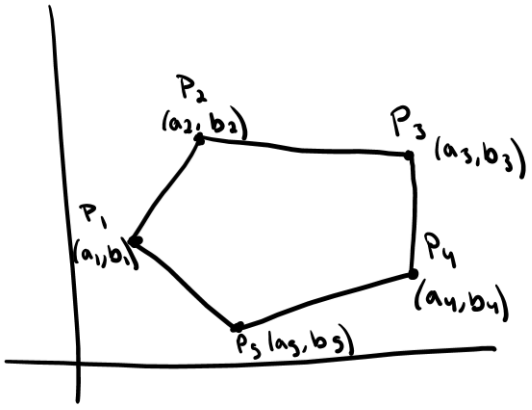


Figure 19: A lattice pentagon example (n=5).

For i=1, 2, ..., n-1, translate the lattice line segment P_iP_{i+1} to the origin to create the corresponding segment OP_{i+1}', $O=(0,0)$ and $P_{i+1}' = (a_{i+1}-a_i, b_{i+1}-b_i)$. By the symmetry of the lattice plane, the number of lattice points on P_iP_{i+1} excluding P_i and P_{i+1} is equal to the number of lattice points on OP_{i+1}' excluding O and P_{i+1} which, by Exercise 29, is equal to $gcd(a_{i+1}-a_i, b_{i+1}-b_i)-1 \triangleq d_i$, i=1, 2, ..., n-1. Finally, translate P_1P_n to OP_1', $O=(0,0)$ and $P_1' = (a_1-a_n, b_1-b_n)$. The number of lattice points on OP_1' excluding O and P_1' is equal to the number of lattice points on P_1P_n excluding P_1 and P_n which is equal to $gcd(a_1-a_n, b_1-b_n)-1 \triangleq d_n$.

Therefore, the number of lattice points on the boundary of P,

$$B(P) = \sum_{i=1}^{n} [gcd(a_{i+1} - a_i, b_{i+1} - b_i) - 1] + gcd(a_1 - a_n, b_1 - b_n) - 1 + n = \sum_{i=1}^{n} d_i. \square$$

3 The Algebraic Structure of the Lattice $\mathbb{Z}^2$

In this section, we will use linear algebra to explore the algebraic properties of the integer lattice $\mathbb{Z}^2$. It will be useful to regard an integer point (a, b) also as an integer-valued vector from the origin $(0, 0)$ to the point (a, b).

Definition 2 Matrix. A **matrix** is a rectangular array of real numbers. An $m \times n$ matrix has m rows and n columns. The entry (number) in the ith row and jth column of a matrix A is denoted by a_{ij} and is called the (i, j)-entry of A. Each column of A is a list of m real numbers.

For example,

$$A = \begin{bmatrix} -2 & 5 & 4 \\ 3.2 & \pi & 0 \\ 13 & 105 & -1 \\ \frac{3}{4} & 7 & 24 \end{bmatrix}$$

is a 4×3 matrix. The $(3, 2)$ entry of A is 105.

- The **zero matrix** is defined to be a matrix of all zeros.
- The diagonal entries in an $m \times n$ matrix $A = [a_{ij}]$ are $a_{11},\ a_{22}, \ldots$, and they form the **main diagonal** of A.
- A **diagonal matrix** is a square matrix whose non-diagonal entries are zero.
- The $n \times n$ **identity matrix** is the diagonal matrix with ones on the main diagonal and zeros elsewhere.
- Two matrices are **equal** if they have the same size and if their corresponding entries are equal.

Definition 3 Vector. A matrix with only one column is called a **column vector**, or simply a **vector**.

- The set $\mathbb{R}^2$ is the set of all vectors with 2 entries, and we can visualize vectors in $\mathbb{R}^2$ using ordered pairs. For example, the vector $\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ is a vector in $\mathbb{R}^2$. To visualize this vector, we draw an arrow from $(0, 0)$ to $(3, 4)$, with the arrow "pointing" at the point $(3, 4)$.
- Similarly, $\mathbb{R}^3$ is the set of all vectors with 3 entries, and we can visualize vectors in $\mathbb{R}^3$ as ordered 3-tuples of points in 3-dimensional space. The vector $\begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix}$ is an example of a vector in $\mathbb{R}^3$.
- More generally, $\mathbb{R}^n$ is the set of all vectors with n entries. Of course, it is more difficult to visualize vectors in $\mathbb{R}^n$ if $n > 3$. However, from a mathematical point of view, it still makes sense to think about vectors in $\mathbb{R}^n$. The vector $\begin{bmatrix} 3 \\ -2 \\ 4 \\ 1 \\ 7 \end{bmatrix}$ is an example of a vector in $\mathbb{R}^5$.
- We say that 2 vectors are **equal** if and only if all of their corresponding entries are equal.
- In $\mathbb{R}^n$, the zero vector is the vector with all zero entries, and it is denoted by $\mathbf{0}$.
- To add 2 vectors, simply add their corresponding entries. We can only add two vectors if they have the same number of entries. So, for example, we can't add a vector in $\mathbb{R}^2$ and a vector in $\mathbb{R}^3$.

Exercise 31 Give two examples of vectors in $\mathbb{R}^4$, and find their sum.

Solution Consider the two vectors in $\mathbb{R}^4$, $\mathbf{a} = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}$ and $\mathbf{b} = \begin{bmatrix} 0.1 \\ 0.2 \\ 0.3 \\ 0.4 \end{bmatrix}$. Then, $\mathbf{a} + \mathbf{b} = \begin{bmatrix} 1.1 \\ 2.2 \\ 3.3 \\ 4.4 \end{bmatrix}$. □

- **Parallelogram Rule for Addition of Vectors in $\mathbb{R}^2$**: If $\mathbf{u}$ and $\mathbf{v}$ are vectors in $\mathbb{R}^2$, represented as points in the plane, then $\mathbf{u}+\mathbf{v}$ is the vector that corresponds to the fourth vertex of the parallelogram whose other vertices are $\mathbf{0}$, $\mathbf{u}$, and $\mathbf{v}$.

  Exercise 32 Choose 2 (unequal) vectors in $\mathbb{R}^2$, and illustrate the Parallelogram Rule for your vectors.

  Solution Consider the two (unequal) vectors in $\mathbb{R}^2$, $\mathbf{a} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\mathbf{b} = \begin{bmatrix} 0 \\ 2 \end{bmatrix}$. The sum of the two vectors $\mathbf{a} + \mathbf{b} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ is shown below using the Parallelogram Rule for Addition of Vectors in $\mathbb{R}^2$.

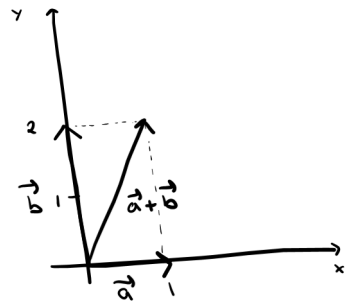


Figure 20: Vector a+b using Parallelogram Rule.

  □

- To multiply a vector by a scalar (real number), just multiply each entry of the vector by the scalar.

  Exercise 33 Give an example of a vector $\mathbf{u}$ in $\mathbb{R}^2$. Compute $2\mathbf{u}$, $-2\mathbf{u}$, and $\frac{1}{2}\mathbf{u}$. Next, draw each of these vectors. What do you observe? What does the set of all scalar multiples of a fixed nonzero vector form?

  Solution Consider the vector $\mathbf{u} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ in $\mathbb{R}^2$.

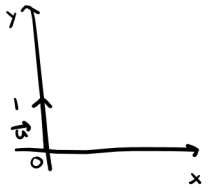


Figure 21: Vector $\mathbf{u}$.

  Then, $2\mathbf{u} = \begin{bmatrix} 0 \\ 2 \end{bmatrix}$ shown in Fig. 22.

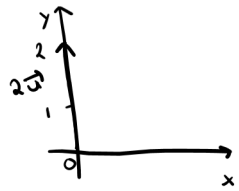


Figure 22: Vector 2**u**.

Vector $-2\mathbf{u} = \begin{bmatrix} 0 \\ -2 \end{bmatrix}$ is shown in Fig. 23.

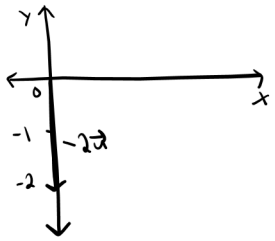


Figure 23: Vector -2**u**.

Finally, vector $\frac{1}{2}\mathbf{u} = \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix}$ is shown in Fig. 24.

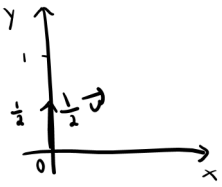


Figure 24: Vector 1/2**u**.

The set of all scalar multiples of a fixed nonzero vector $\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$, $u_1 \neq 0$ defines a line through the origin with slope $\frac{u_2}{u_1}$ (in our special example of $u_1 = 0$ the line is x=0). □

Definition 4 Integer Lattice. Let $n \geq 1$ be a positive integer. The **lattice** $\mathbb{Z}^n$ is the set of all vectors

$$\mathbf{v} = \langle a_1, a_2, \ldots, a_n \rangle$$

such that

$$a_1,\ a_2, \ldots, a_n \in \mathbb{Z}.$$

We will primarily be interested in working with the lattice $\mathbb{Z}^2$, though in future work you may consider how the properties that we study here extend to higher dimensions. We define addition and scalar multiplication as usual for vectors, but in this case, scalar multiplication means multiplication of a vector *by an integer*, i.e. the scalars are integers (not all real numbers):

- If $\mathbf{v} = \langle a, b\rangle$ and $\mathbf{w} = \langle c, d\rangle$ are two vectors in $\mathbb{Z}^2$, then

$$\mathbf{v} + \mathbf{w} = \langle a + c, b + d\rangle .$$

- If $\mathbf{v} = \langle a, b\rangle$ is a vector in $\mathbb{Z}^2$ and m is an *integer*, then

$$m\mathbf{v} = \langle ma, mb\rangle .$$

It is straightforward to check that the following rules are satisfied for all vectors $\mathbf{v}$ and $\mathbf{w}$ in $\mathbb{Z}^2$ and all integers m and n:

(i) $1\mathbf{v} = \mathbf{v}$

(ii) $(mn)\mathbf{v} = m(n\mathbf{v})$

(iii) $(m + n)\mathbf{v} = m\mathbf{v} + n\mathbf{v}$

(iv) $m(\mathbf{v} + \mathbf{w}) = m\mathbf{v} + m\mathbf{w}$

Observe that these rules are the same as those for a vector space! The difference here is that the scalars must be in $\mathbb{Z}$ (not the more general $\mathbb{R}$). The lattice $\mathbb{Z}^2$ is an example of what is called a $\mathbb{Z}-$*module*. Modules are studied in more detail in advanced abstract algebra, and have a broad range of important applications.

Definition 5 Linear Combinations in $\mathbb{R}^2$. Given vectors $\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_p}$ in $\mathbb{R}^2$ and *real numbers* $c_1,\ c_2, \ldots, c_p$, the vector $\mathbf{y} \in \mathbb{R}^2$ defined by

$$\mathbf{y} = c_1\mathbf{v_1} + c_2\mathbf{v_2} + \cdots c_p\mathbf{v_p}$$

is called a **linear combination** of the vectors $\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_p}$.

Exercise 34 Find $\frac{1}{2}\begin{bmatrix} -2 \\ 5 \end{bmatrix} + 3\begin{bmatrix} 4 \\ 1 \end{bmatrix} - 2\begin{bmatrix} \frac{3}{4} \\ 8 \end{bmatrix}$. This is an example of a linear combination of 3 vectors in $\mathbb{R}^2$.

Solution $\frac{1}{2}\begin{bmatrix} -2 \\ 5 \end{bmatrix} + 3\begin{bmatrix} 4 \\ 1 \end{bmatrix} - 2\begin{bmatrix} \frac{3}{4} \\ 8 \end{bmatrix} = \begin{bmatrix} -1 \\ \frac{5}{2} \end{bmatrix} + \begin{bmatrix} 12 \\ 3 \end{bmatrix} - \begin{bmatrix} \frac{3}{2} \\ 16 \end{bmatrix} = \begin{bmatrix} \frac{19}{2} \\ -\frac{21}{2} \end{bmatrix}$. □

Definition 6 $\mathbb{Z}^2$-Linear Combinations in $\mathbb{Z}^2$. Given vectors $\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_p}$ in $\mathbb{Z}^2$ and *integers* $c_1,\ c_2, \ldots, c_p$, the vector $\mathbf{y} \in \mathbb{Z}^2$ defined by

$$\mathbf{y} = c_1\mathbf{v_1} + c_2\mathbf{v_2} + \cdots c_p\mathbf{v_p}$$

is called a **$\mathbb{Z}$-linear combination** of the vectors $\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_p}$.

Exercise 35 Express $\mathbf{v} = \begin{bmatrix} 8 \\ -12 \end{bmatrix}$ as a $\mathbb{Z}$-linear combination of 2 vectors in $\mathbb{Z}^2$.

Solution $\mathbf{v} = \begin{bmatrix} 8 \\ -12 \end{bmatrix} = 2\begin{bmatrix} 4 \\ -1 \end{bmatrix} + 1\begin{bmatrix} 0 \\ -10 \end{bmatrix}$. □

Definition 7 Linear Independence in $\mathbb{R}^2$. A set of vectors $\mathbf{v_1}, \ldots, \mathbf{v_p}$ in $\mathbb{R}^2$ is **linearly independent** if the vector equation

$$x_1\mathbf{v_1} + x_2\mathbf{v_2} + \cdots + x_p\mathbf{v_p} = \mathbf{0},$$

where

$$x_1,\ x_2, \ldots, x_p \in \mathbb{R}$$

has only the trivial solution

$$x_1 = x_2 = \cdots = x_p = 0.$$

If a non-trivial solution exists, i.e. if there exist *real numbers* $c_1,\ c_2,\ \ldots, c_p$ not all zero such that

$$c_1\mathbf{v_1} + c_2\mathbf{v_2} + \cdots + c_p\mathbf{v_p} = \mathbf{0},$$

then we say that the set of vectors is **linearly dependent**.

Exercise 36 Are the vectors $\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ linearly independent or dependent?

Solution Consider the vector equation $x_1 \begin{bmatrix} 1 \\ 2 \end{bmatrix} + x_2 \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \mathbf{0}$, which implies

$$\begin{cases} x_1 + 3x_2 = 0 \\ 2x_1 + 4x_2 = 0 \end{cases} \implies \begin{cases} x_1 = 0 \\ x_2 = 0 \end{cases}.$$

By definition, the vectors $\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ are linearly independent in $\mathbb{R}^2$ (in $\mathbb{Z}^2$ as well since they have integer coordinates). □

Exercise 37 Are the vectors $\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} -3 \\ -6 \end{bmatrix}$ linearly independent or dependent?

Solution Consider the vector equation $x_1 \begin{bmatrix} 1 \\ 2 \end{bmatrix} + x_2 \begin{bmatrix} -3 \\ -6 \end{bmatrix} = \mathbf{0}$ which implies

$$\begin{cases} x_1 - 3x_2 = 0 \\ 2x_1 - 6x_2 = 0 \end{cases} \implies x_1 = 3x_2\ \forall\ x_2 \in \mathbb{R} \text{ (infinitely many solutions other than the trivial} x_1 = 0, x_2 = 0).$$

Therefore, vectors $\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} -3 \\ -6 \end{bmatrix}$ are linearly dependent in $\mathbb{R}^2$ (in $\mathbb{Z}^2$ as well since $x_2 = 1, x_1 = 3$ is an integer non-trivial solution for example). □

Definition 8 Linear Independence in $\mathbb{Z}^2$. A set of vectors $\mathbf{v_1}, \ldots, \mathbf{v_p}$ in $\mathbb{Z}^2$ is **linearly $\mathbb{Z}$-independent** if the vector equation

$$x_1\mathbf{v_1} + x_2\mathbf{v_2} + \cdots + x_p\mathbf{v_p} = \mathbf{0},$$

where

$$x_1,\ x_2, \ldots, x_p \in \mathbb{Z}$$

has only the trivial solution

$$x_1 = x_2 = \cdots = x_p = 0.$$

If a non-trivial solution exists, i.e. if there exist *integers* $c_1,\ c_2,\ \ldots, c_p$ not all zero such that

$$c_1\mathbf{v_1} + c_2\mathbf{v_2} + \cdots + c_p\mathbf{v_p} = \mathbf{0},$$

then we say that the set of vectors is **linearly $\mathbb{Z}$-dependent**.

Definition 9 Basis for $\mathbb{R}^2$. A basis for $\mathbb{R}^2$ is a set

$$\{\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_k}\}$$

of linearly independent vectors in $\mathbb{R}^2$ with the property that every vector in $\mathbb{R}^2$ can be expressed as a linear combination of the basis vectors $\{\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_k}\}$.

Definition 10 $\mathbb{Z}$-Basis for $\mathbb{Z}^2$. A $\mathbb{Z}-$**basis** for $\mathbb{Z}^2$ is a set

$$\{\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_k}\}$$

of linearly $\mathbb{Z}$-independent vectors in $\mathbb{Z}^2$ with the property that every vector in $\mathbb{Z}^2$ can be expressed as a $\mathbb{Z}-$ linear combination of the basis vectors $\{\mathbf{v_1},\ \mathbf{v_2}, \ldots, \mathbf{v_k}\}$.

Exercise 38 (a) Is the set

$$\{\begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \begin{bmatrix} 3 \\ 4 \end{bmatrix}\}$$

a basis for $\mathbb{R}^2$? Prove your result.

(b) Is the set

$$\{\begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \begin{bmatrix} 3 \\ 4 \end{bmatrix}\}$$

a $\mathbb{Z}$-basis for $\mathbb{Z}^2$? Prove your result.

With appropriate modification so that the scalars are *integers* rather than real numbers, many of the important geometric and algebraic results that you learned (or will learn) about vector space bases for $\mathbb{R}^2$ (or, more generally, $\mathbb{R}^n$) hold for $\mathbb{Z}^2$ (or, more generally, $\mathbb{Z}^n$).

Solution

(a) Consider an arbitrary $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$. If it can be described by $\{\begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \begin{bmatrix} 3 \\ 4 \end{bmatrix}\}$, then there exist $c_1, c_2 \in \mathbb{R}$ such that

$$\begin{bmatrix} x \\ y \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 2 \end{bmatrix} + c_2 \begin{bmatrix} 3 \\ 4 \end{bmatrix} \implies$$

$$\begin{cases} x = c_1 + 3c_2 \\ y = 2c_1 + 4c_2 \end{cases} \implies \begin{cases} c_1 = \frac{y-4x+2y}{2} \\ c_2 = \frac{2x-y}{2} \end{cases} .$$

We conclude that for any given $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$ there exist c_1, c_2 ($c_1 = \frac{y-4x+2y}{2}, c_2 = \frac{2x-y}{2}$) for which $\begin{bmatrix} x \\ y \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 2 \end{bmatrix} + c_2 \begin{bmatrix} 3 \\ 4 \end{bmatrix}$. Therefore, the set $\{\begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \begin{bmatrix} 3 \\ 4 \end{bmatrix}\}$ is a basis for $\mathbb{R}^2$.

<u>*Note* :</u> Also, $\begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ are linearly independent, i.e. if $c_1 \begin{bmatrix} 1 \\ 2 \end{bmatrix} + c_2 \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, then

$$\begin{cases} c_1 + 3c_2 = 0 \\ 2c_1 + 4c_2 = 0 \end{cases} \implies \begin{cases} c_1 = 0 \\ c_2 = 0 \end{cases} . \quad \square$$

(b) $\begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \begin{bmatrix} 3 \\ 4 \end{bmatrix} \in \mathbb{Z}^2$ are linearly independent by the note in Part (a). By Part (a) again, an arbitrary $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Z}^2$ can be described as

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{y-4x+2y}{2} \begin{bmatrix} 1 \\ 2 \end{bmatrix} + \frac{2x-y}{2} \begin{bmatrix} 3 \\ 4 \end{bmatrix}.$$

But, $\frac{y-4x+2y}{2}, \frac{2x-y}{2}$ are not necessarily integers for integer x and y. For example, for $x = 1, y = 1, c_1 = \frac{y-4x+2y}{2} = -\frac{1}{2}$. Therefore, $\{\begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \begin{bmatrix} 3 \\ 4 \end{bmatrix}\}$ is not a $\mathbb{Z}$-basis for $\mathbb{Z}^2$. $\square$

Definition 11 A matrix A with real entries is said to be **invertible over** $\mathbb{R}$, or **invertible** if there exists a matrix B with real entries such that $AB = I$, where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is the standard 2×2 identity matrix).

Exercise 39 Use Definition 11 to show that the matrix

$$A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$$

is invertible over $\mathbb{R}$.

Solution For matrix $A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$ to be invertible over $\mathbb{R}$ there must be a matrix B such that $AB = I_2$. Consider matrix $B = \begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix}$. $AB = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix} \begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix A is invertible over $\mathbb{R}$. $\square$

Exercise 40 Use Definition 11 to show that the matrix

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

is invertible over $\mathbb{R}$.

Solution For matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ to be invertible over $\mathbb{R}$ there must be a matrix B such that $AB = I_2$. Consider matrix $B = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{3} \end{bmatrix}$. $AB = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix A is invertible over $\mathbb{R}$. $\square$

Exercise 41 Use Definition 11 to show that the matrix

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$$

is *not* invertible over $\mathbb{R}$.

Solution I will prove that A is not invertible over $\mathbb{R}$ by contradiction. Assume that $A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is invertible over $\mathbb{R}$. Then, there exists $B = \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix}$ in $\mathbb{R}^{2x2}$ such that $AB = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \implies$

$$b_1 + 2b_3 = 1 \tag{8}$$

$$b_2 + 2b_4 = 0 \tag{9}$$

$$2b_1 + 4b_3 = 0 \tag{10}$$

$$2b_2 + 4b_4 = 1 \tag{11}$$

By (9), $b_2 + 2b_4 = 0$. By (11), $2(b_2 + 2b_4) = 1$. This is a contradiction, therefore, the matrix $A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is not invertible over $\mathbb{R}$. $\square$

Definition 12 The **determinant** of a 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, denoted $\det(A)$, is given by

$$\det(A) = ad - bc.$$

Exercise 42 (a) Construct (at least) 3 different (non-identity) matrices with real entries that are invertible over $\mathbb{R}$. Show that each of your matrices is invertible over $\mathbb{R}$ using Definition 11. Then find the determinant of each of your matrices.

(b) Construct (at least) 3 different matrices with real entries that are *not* invertible over $\mathbb{R}$. Show that each of your matrices is not invertible over $\mathbb{R}$ using Definition 11. Then find the determinant of each of your matrices.

(c) Performing additional computations if necessary, make a conjecture about the determinant of a matrix with real entries that is invertible over $\mathbb{R}$.

Solution

(a) Consider matrix $A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$. For A to be invertible over $\mathbb{R}$ there must be a matrix B such that $AB = I_2$. Consider matrix $B = \begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix}$; $AB = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}\begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix A is invertible over $\mathbb{R}$ and $det(A) = 1 \cdot 11 - 3 \cdot 4 = -1$.

Consider matrix $C = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. For C to be invertible over $\mathbb{R}$ there must be a matrix D such that $CD = I_2$. Consider matrix $D = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{3} \end{bmatrix}$; $CD = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix C is invertible over $\mathbb{R}$ and $det(C) = 2 \cdot 10 - 5 \cdot 5 = -5$.

Consider matrix $E = \begin{bmatrix} 5 & 10 \\ 2 & 5 \end{bmatrix}$. For E to be invertible over $\mathbb{R}$ there must be a matrix F such that $EF = I_2$. Consider matrix $F = \begin{bmatrix} 1 & -2 \\ -\frac{2}{5} & 1 \end{bmatrix}$; $EF = \begin{bmatrix} 5 & 10 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 1 & -2 \\ -\frac{2}{5} & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix E is invertible over $\mathbb{R}$ and $det(E) = 2 \cdot 10 - 5 \cdot 5 = -5$.

(b) Consider the matrix $G = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$. I will show that G is not invertible over $\mathbb{R}$ by contradiction. Assume $G = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is invertible over $\mathbb{R}$. Then, there exists $H = \begin{bmatrix} h_1 & h_3 \\ h_2 & h_4 \end{bmatrix}$ in $\mathbb{R}^{2x2}$ such that $GH = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \implies$

$$h_1 + 2h_3 = 1 \tag{12}$$

$$h_2 + 2h_4 = 0 \tag{13}$$

$$2h_1 + 4h_3 = 0 \tag{14}$$

$$2h_2 + 4h_4 = 1 \tag{15}$$

By (30), $h_2 + 2h_4 = 0$. By (15), $2(h_2 + 2h_4) = 1$. This is a contradiction, therefore the matrix $G = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is not invertible over $\mathbb{R}$.

The determinant of G is $det(G) = 1 \cdot 4 - 2 \cdot 2 = 0$.

Consider the matrix $J = \begin{bmatrix} 2 & 3 \\ 2 & 3 \end{bmatrix}$. I will show that J is not invertible over $\mathbb{R}$ by contradiction. Assume $J = \begin{bmatrix} 2 & 3 \\ 2 & 3 \end{bmatrix}$ is invertible over $\mathbb{R}$. Then, there exists $K = \begin{bmatrix} k_1 & k_3 \\ k_2 & k_4 \end{bmatrix}$ in $\mathbb{R}^{2x2}$ such that $JK = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \implies$

$$2k_1 + 2k_3 = 1 \tag{16}$$
$$2k_2 + 2k_4 = 0 \tag{17}$$
$$3k_1 + 3k_3 = 0 \tag{18}$$
$$3k_2 + 3k_4 = 1 \tag{19}$$

By (17), $2k_2 + 2k_4 = 0 \implies k_2 + k_4 = 0$. By (19), $3k_2 + 3k_4 = 1 \implies k_2 + k_4 = \frac{1}{3}$. This is a contradiction, therefore the matrix $J = \begin{bmatrix} 2 & 3 \\ 2 & 3 \end{bmatrix}$ is not invertible over $\mathbb{R}$.

The determinant of J is $det(J) = 2 \cdot 3 - 3 \cdot 2 = 0$.

Consider the matrix $L = \begin{bmatrix} -2 & 4 \\ -6 & 12 \end{bmatrix}$. I will show that L is not invertible over $\mathbb{R}$ by contradiction. Assume $L = \begin{bmatrix} -2 & 4 \\ -6 & 12 \end{bmatrix}$ is invertible over $\mathbb{R}$. Then, there exists $M = \begin{bmatrix} m_1 & m_3 \\ m_2 & m_4 \end{bmatrix}$ in $\mathbb{R}^{2x2}$ such that $LM = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \implies$

$$-2m_1 - 6m_3 = 1 \tag{20}$$
$$-2m_2 - 6m_4 = 0 \tag{21}$$
$$4m_1 + 12m_3 = 0 \tag{22}$$
$$4m_2 + 12m_4 = 1 \tag{23}$$

By (21), $-2m_2 - 6m_4 = 0 \implies m_2 + 3m_4 = 0$. By (23), $4m_2 + 12m_4 = 1 \implies m_2 + 3m_4 = \frac{1}{4}$. This is a contradiction, therefore the matrix $L = \begin{bmatrix} -2 & 4 \\ -6 & 12 \end{bmatrix}$ is not invertible over $\mathbb{R}$.

The determinant of L is $det(L) = -2 \cdot 12 - 4 \cdot -6 = 0$.

(c) I conjecture that the determinant of a matrix with real entries that is invertible over $\mathbb{R}$ is $\neq 0$. $\square$

Exercise 43 Inverses of 2×2 Matrices. Consider the 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Show that if $ad - bc \neq 0$, then A is invertible and $A^{-1} = \dfrac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Show that if $ad - bc = 0$, then A is not invertible.

Solution Assume first that $ad - bc \neq 0$. Consider the matrix $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Then,

$$AA^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} ad - bc & -ab + ab \\ cd - cd & -bc + ab \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We conclude that if $ad - bc \neq 0$, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse and the inverse is $A^{-1} = \dfrac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Assume now that $ad - bc = 0$. I will show by contradiction that in this case $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is not invertible.

Assume that $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible. Therefore, there exists matrix $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $AB = I_2 \implies$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \implies \begin{cases} aw + by = 1 \\ ax + bz = 0 \\ cw + dy = 0 \\ cx + dz = 1 \end{cases} \implies$$

$$adw + bdy = d \tag{24}$$
$$adx + bdz = 0 \tag{25}$$
$$bcw + bdy = 0 \tag{26}$$
$$bcx + bdz = b \tag{27}$$

By substituting (25) from (27) and using $ad - bc = 0$ or $ad = bc$, we obtain

$$b = 0.$$

Similarly, by substituting (26) from (24) and using $ad = bc$, we obtain

$$d = 0.$$

Then,

$$aw = 1 \tag{28}$$
$$ax = 0 \tag{29}$$
$$cw = 0 \tag{30}$$
$$cx = 1 \tag{31}$$

By (28), $a \neq 0$ and $w = \frac{1}{a}$. By (30), $cw = c\frac{1}{a} = 0 \implies c = 0$. By (31), $c \neq 0$ which is a contradiction.

Therefore, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is not invertible.

We conclude that $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible iff $ad - bc \neq 0$. □

Definition 13 A matrix A with integer entries is said to be **invertible over** $\mathbb{Z}$, or **$\mathbb{Z}$-invertible** if there exists a matrix B with *integer* entries such that $AB = I$ (where I is the standard 2×2 identity matrix).

Exercise 44 Use Definition 13 to show that the matrix

$$A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$$

is invertible over $\mathbb{Z}$.

Solution For matrix $A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$ to be invertible over $\mathbb{Z}$ there must be a matrix B with integer entries such that $AB = I_2$. Consider matrix $B = \begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix}$. $AB = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}\begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix A is invertible over $\mathbb{Z}$. □

Exercise 45 Use Definition 13 to show that the matrix

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

is *not* invertible over $\mathbb{Z}$.

Solution I will prove that $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is not invertible over $\mathbb{Z}$ by contradiction. Assume $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is invertible over $\mathbb{Z}$. Then, there exists $B = \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix}$ isuch that $b_1, b_2, b_3, b_4 \in \mathbb{Z}$ and $AB = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix} = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

$$AB = I_2 \implies \begin{cases} b_1 + 2b_2 = 1 \\ b_3 + 2b_4 = 0 \\ 3b_1 + 4b_2 = 0 \\ 3b_3 + 4b_4 = 1 \end{cases} \implies \begin{cases} b_1 = -2 \\ b_2 = \frac{3}{2} \\ b_3 = \frac{1}{2} \\ b_4 = -\frac{1}{8} \end{cases}.$$

and $b_2, b_3, b_4 \notin \mathbb{Z}$, which is a contradiction. Therefore, the matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is not invertible over $\mathbb{Z}$. □

Exercise 46 Construct (at least) 3 different (non-identity) matrices with integer entries that are invertible over $\mathbb{Z}$.

(a) Show that each of your matrices is invertible over $\mathbb{Z}$.

(b) Find the determinant of each of your matrices. What do you observe?

(c) Performing additional computations if necessary, make a conjecture about the determinant of a matrix with integer entries that is invertible over $\mathbb{Z}$.

Solution Consider the three matrices with integer entries $A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$, and $C = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$.

(a) For matrix $A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$ to be invertible over $\mathbb{Z}$ there must be a matrix D with integer entries such that $AD = I_2$. Consider matrix $D = \begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix}$. $AD = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix} \begin{bmatrix} -11 & 3 \\ -4 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix A is invertible over $\mathbb{Z}$.

For matrix $B = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$ to be invertible over $\mathbb{Z}$ there must be a matrix E with integer entries such that $BE = I_2$. Consider matrix $E = \begin{bmatrix} -5 & 2 \\ 3 & -1 \end{bmatrix}$. $BE = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} -5 & 2 \\ 3 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix B is invertible over $\mathbb{Z}$.

For matrix $C = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$ to be invertible over $\mathbb{Z}$ there must be a matrix F with integer entries such that $CF = I_2$. Consider matrix $F = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix}$. $CF = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$. Therefore, matrix C is invertible over $\mathbb{Z}$.

(b) $det(A) = 1 \cdot 11 - 3 \cdot 4 = -1$.
$det(B) = 1 \cdot 5 - 2 \cdot 3 = -1$.
$det(C) = 2 \cdot 5 - 3 \cdot 3 = 1$.
I observe that the determinant of the matrices invertible over $\mathbb{Z}$ is ± 1.

(c) I conjecture that the determinant of a matrix with integer entries that is invertible over $\mathbb{Z}$ is ± 1. □

Exercise 47 Let A be a 2×2 matrix with entries in $\mathbb{Z}$. Show that A is invertible over $\mathbb{Z}$ if and only if $\det(A) = \pm 1$. Note that you only need to prove this result here for 2×2 matrices, but the same result holds for more general $n \times n$ matrices with entries in $\mathbb{Z}$. (You are of course welcome to prove the more general result here if you wish.)

Solution Consider an arbitrary matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $\mathbb{Z}^{2x2}$ (i.e,. $a, b, c, d \in \mathbb{Z}$). Assume $ad - bc \neq 0$. Then, A^{-1} exists in $\mathbb{R}^{2x2}$ and $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

If $det(A) = ad - bc = \pm 1$, then $A^{-1} = \begin{bmatrix} \pm d & \mp b \\ \mp c & \pm a \end{bmatrix} \in \mathbb{Z}^{2x2}$. Therefore, we proved that if $det(A_{2x2}) = \pm 1$, then A is invertible over $\mathbb{Z}$.

If $A^{-1} \in \mathbb{Z}$ (i.e., A is invertible over $\mathbb{Z}$), $det(A^{-1}) = det(\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}) = \frac{da}{(ad-bc)^2} - \frac{bc}{(ad-bc)^2} = \frac{1}{da-bc} \in \mathbb{Z} \implies da - bc = \pm 1 \implies det(A) = \pm 1$. Therefore, if a matrix A is invertible over $\mathbb{Z}$, then $det(A) = \pm 1$.

After having proved both directions of the statement, we conclude that A is invertible over $\mathbb{Z}$ if and only if $det(A) = \pm 1$. □

Definition 14 Multiplicative Inverse The **multiplicative inverse** of a real number x is the real number y such that

$$x \cdot y = 1.$$

Exercise 48 Which real numbers have a multiplicative inverse in $\mathbb{R}$? Prove your statement.

Solution Consider any $x \in \mathbb{R} - \{0\}$. Then, $\frac{1}{x}$ is also in $\mathbb{R}$ and $x \cdot \frac{1}{x} = 1$. We know that there is no number by which 0 can be multiplied to obtain 1. Therefore, every real number other than 0 has a multiplicative inverse in $\mathbb{R}$, namely $\frac{1}{x}$. □

Exercise 49 Which *integers* have a multiplicative inverse that is *also an integer*? Prove your statement.

Solution In Exercise 48 we proved that every real number x has a multiplicative inverse $\frac{1}{x}$ (except for 0 which does not have a multiplicative inverse). Therefore, for x and $\frac{1}{x}$ to be both be integer, x can only be 1 or -1. Therefore, 1 and -1 are the only integers that have multiplicative inverses that are also integers. □

Observe that Exercise 42 implies that a matrix A with entries in $\mathbb{R}$ is invertible over $\mathbb{R}$ if and only if $\det(A)$ has a multiplicative inverse in $\mathbb{R}$. In Exercises 47 and 49, we showed that a matrix A with entries in $\mathbb{Z}$ is invertible over $\mathbb{Z}$ if and only if $\det(A)$ has a multiplicative inverse that is also an integer. This provides a beautiful connection between invertibility of a matrix with entries in a given space and invertibility of the determinant of the matrix in that space.

Exercise 50 Construct 3 different examples of bases $\{\mathbf{v} = \langle v_1, v_2 \rangle, \ \mathbf{w} = \langle w_1, w_2 \rangle\}$ of $\mathbb{R}^2$. Note that your bases do not need to be $\mathbb{Z}$-bases!

(a) Show that each of your examples is actually a basis of $\mathbb{R}^2$.

(b) For each basis, compute the determinant of the matrix

$$\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}.$$

What do you observe?

(c) Doing more computations if necessary, state and prove a conjecture about the determinant of a matrix whose columns form a basis for $\mathbb{R}^2$.

Solution Here are three different bases of $\mathbb{R}^2$.

$$\mathbf{a} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ \mathbf{b} = \begin{bmatrix} 0 \\ 1 \end{bmatrix};$$

$$\mathbf{c} = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ \mathbf{d} = \begin{bmatrix} 1 \\ 1 \end{bmatrix};$$
$$\mathbf{e} = \begin{bmatrix} 5 \\ 1 \end{bmatrix},\ \mathbf{f} = \begin{bmatrix} 2 \\ 2 \end{bmatrix}.$$

(a) i) $\mathbf{a},\ \mathbf{b}$ are linearly independent because if

$$x_1\mathbf{a} + x_2\mathbf{b} = \mathbf{0} \implies$$
$$\begin{bmatrix} x_1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies$$
$$x_1 = 0 \text{ and } x_2 = 0.$$

Consider an arbitrary vector $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$. Then, $\begin{bmatrix} x \\ y \end{bmatrix} = x\begin{bmatrix} 1 \\ 0 \end{bmatrix} + y\begin{bmatrix} 0 \\ 1 \end{bmatrix} = x\mathbf{a} + y\mathbf{b}$. We conclude that $\mathbf{a},\ \mathbf{b}$ is a basis of $\mathbb{R}^2$.

ii) $\mathbf{c},\ \mathbf{d}$ are linearly independent because if

$$x_1\mathbf{c} + x_2\mathbf{d} = \mathbf{0} \implies$$
$$\begin{bmatrix} x_1 \\ 0 \end{bmatrix} + \begin{bmatrix} x_2 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies$$
$$x_2 = 0 \text{ and } x_1 + x_2 = 0 \implies x_1 = 0.$$

Consider an arbitrary vector $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$. Then, $\begin{bmatrix} x \\ y \end{bmatrix} = s\begin{bmatrix} 1 \\ 0 \end{bmatrix} + t\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} s+t \\ t \end{bmatrix} \implies t = y$ and $s = x - y$. Therefore, any $\begin{bmatrix} x \\ y \end{bmatrix}$ in $\mathbb{R}^2$ can be written as $\begin{bmatrix} x \\ y \end{bmatrix} = (x-y)\begin{bmatrix} 1 \\ 0 \end{bmatrix} + y\begin{bmatrix} 1 \\ 1 \end{bmatrix}$. We conclude that $\mathbf{c},\ \mathbf{d}$ is a basis of $\mathbb{R}^2$.

iii) $\mathbf{e},\ \mathbf{f}$ are linearly independent because if

$$x_1\mathbf{e} + x_2\mathbf{f} = \mathbf{0} \implies$$
$$\begin{bmatrix} sx_1 \\ x_1 \end{bmatrix} + \begin{bmatrix} 2x_2 \\ 2x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies$$
$$\begin{cases} x_1 = -2x_2 \\ -10x_2 + 2x_2 = 0 \end{cases} \implies \begin{cases} x_1 = 0 \\ x_2 = 0 \end{cases}.$$

Consider an arbitrary vector $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$. Then, $\begin{bmatrix} x \\ y \end{bmatrix} = s\begin{bmatrix} 5 \\ 1 \end{bmatrix} + t\begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 5s+2t \\ 5+2t \end{bmatrix} \implies \begin{cases} 5+2t = y \\ 5s+2t = x \end{cases} \implies$ $\begin{cases} s = \frac{2y-2x}{-8} \\ t = \frac{x-5y}{-8} \end{cases}$. Therefore, any $\begin{bmatrix} x \\ y \end{bmatrix}$ in $\mathbb{R}^2$ can be written as $\begin{bmatrix} x \\ y \end{bmatrix} = \frac{2y-x}{-8}\begin{bmatrix} 5 \\ 1 \end{bmatrix} + \frac{x-5y}{-8}\begin{bmatrix} 2 \\ 2 \end{bmatrix}$. We conclude that $\mathbf{e},\ \mathbf{f}$ is a basis of $\mathbb{R}^2$.

(b) $det([\mathbf{a}\ \mathbf{b}]) = det(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) = 1.$

$det([\mathbf{c}\ \mathbf{d}]) = det(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}) = 1.$

$det([\mathbf{e}\ \mathbf{f}]) = det(\begin{bmatrix} 5 & 2 \\ 1 & 2 \end{bmatrix}) = -8.$

I observe that the determinant is non-zero for all bases.

(c) I conjecture that the columns of a matrix in $\mathbb{R}^{2x2}$ form a basis of $\mathbb{R}^2$ iff the determinant of the matrix is non-zero. □

Exercise 51 Construct 3 different examples of $\mathbb{Z}$-bases $\{\mathbf{v} = \langle v_1, v_2\rangle\,,\ \mathbf{w} = \langle w_1, w_2\rangle\}$ of $\mathbb{Z}^2$.

(a) Show that each of your examples is actually a $\mathbb{Z}-$basis of $\mathbb{Z}^2$.

(b) For each basis, compute the determinant of the matrix

$$\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}.$$

What do you observe?

(c) Doing more computations if necessary, state and prove a conjecture about the determinant of a matrix whose columns form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$.

Solution Consider the following suggested $\mathbb{Z}$ bases of $\mathbb{Z}^2$:

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w}_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix};$$

$$\mathbf{v}_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w}_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix};$$

$$\mathbf{v}_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \mathbf{w}_3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

(a) $\mathbf{v}_1, \mathbf{w}_1$ are linearly independent in $\mathbb{Z}$ because there are no k_1, k_2 in $\mathbb{Z} - \{0\}$ such that $k_1\mathbf{v}_1 + k_2\mathbf{w}_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.
Indeed, $k_1\mathbf{v}_1 + k_2\mathbf{w}_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies \begin{bmatrix} k_1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ k_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, i.e. $\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.
Every $\begin{bmatrix} x \\ y \end{bmatrix}$ in $\mathbb{Z}^2$ can be written as $\begin{bmatrix} x \\ y \end{bmatrix} = x\mathbf{v}_1 + y\mathbf{w}_1$. Therefore, $\mathbf{v_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w_1} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are a $\mathbb{Z}$-basis of $\mathbb{Z}^2$.

$\mathbf{v}_2, \mathbf{w}_2$ are linearly independent in $\mathbb{Z}$ because there are no k_1, k_2 in $\mathbb{Z} - \{0\}$ such that $k_1\mathbf{v}_2 + k_2\mathbf{w}_2 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.
Indeed, $k_1\mathbf{v}_2 + k_2\mathbf{w}_2 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies \begin{bmatrix} k_1 \\ 0 \end{bmatrix} + \begin{bmatrix} k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies \begin{cases} k_1 + k_2 = 0 \\ k_2 = 0 \end{cases} \implies \begin{cases} k_1 = 0 \\ k_2 = 0 \end{cases}$.
Every $\begin{bmatrix} x \\ y \end{bmatrix}$ in $\mathbb{Z}^2$ can be written as $\begin{bmatrix} x \\ y \end{bmatrix} = (x-y)\mathbf{v}_2 + y\mathbf{w}_2$. Therefore, $\mathbf{v_2} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w_2} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ are a $\mathbb{Z}$-basis of $\mathbb{Z}^2$.

$\mathbf{v}_3, \mathbf{w}_3$ are linearly independent in $\mathbb{Z}$ because there are no k_1, k_2 in $\mathbb{Z} - \{0\}$ such that $k_1\mathbf{v}_3 + k_2\mathbf{w}_3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.
Indeed, $k_1\mathbf{v}_3 + k_2\mathbf{w}_3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies \begin{bmatrix} k_1 \\ k_1 \end{bmatrix} + \begin{bmatrix} 2k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ i.e. $\begin{cases} k_1 + 2k_2 = 0 \\ k_1 + k_2 = 0 \end{cases} \implies \begin{cases} k_1 = 0 \\ k_2 = 0 \end{cases}$.
Every $\begin{bmatrix} x \\ y \end{bmatrix}$ in $\mathbb{Z}^2$ can be written as $\begin{bmatrix} x \\ y \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} + c_2 \begin{bmatrix} 2 \\ 1 \end{bmatrix} \implies \begin{cases} c_1 + 2c_2 = x \\ c_1 + c_2 = y \end{cases} \implies \begin{cases} c_2 = x - y \\ c_1 = -x + 2y \end{cases}$
with $c_1 = -x + 2y$ and $c_2 = x - y$ integers. Therefore, $\mathbf{v}_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \mathbf{w}_3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$ are a $\mathbb{Z}$-basis of $\mathbb{Z}^2$.

(b) $det(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) = 1.$
$det(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}) = 1.$

$det(\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}) = -1$.

So far, I observe that $det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}) = \pm 1$.

(c) I conjecture that the determinant of a matrix $\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}$ whose columns form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ is ± 1.

Assume that the columns of $\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}$ form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ and $det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix})$=0. If the columns of $\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}$ are a basis for $\mathbb{Z}^2$, then for any $x, y \in \mathbb{Z}$ we can write $\begin{bmatrix} x \\ y \end{bmatrix} = c_1 \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} + c_2 \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$ with $c_1, c_2 \in \mathbb{Z}$. Consider an arbitrary $x \neq 0$. Then, $v_1 \neq 0$ or $w_1 \neq 0$ (or both). Say $v_1 \neq 0$ (the case $v_1 = 0$ and $w_1 \neq 0$ is treated similarly). Then,

$$c_1 = \frac{x - w_1 c_2}{v_1}. \tag{32}$$

Consider an arbitrary $y \neq 0$. Then, $v_2 \neq 0$ or $w_2 \neq 0$ (or both). Say $w_2 \neq 0$ (the case $w_2 = 0$ and $v_2 \neq 0$ is treated similarly). Then,

$$c_2 = \frac{y - v_2 c_1}{w_2}. \tag{33}$$

By (32) and (33),

$$c_1 = \frac{x - w_1 \frac{y - v_2 c_1}{w_2}}{v_1} \implies \frac{x w_2 - w_1 y + w_1 v_2 c_1}{v_1 w_2}.$$

Because $det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}) = 0 \implies w_1 v_2 = v_1 w_2 \implies$

$$c_1 = \frac{x w_2 - w_1 y}{v_1 w_2} + c_1 \implies \frac{x w_2 - w_1 y}{v_1 w_2} = 0 \implies x w_2 - w_1 y = 0$$

for any $x,\ y \in \mathbb{Z} - \{0\}$. This is a contradiction. Therefore, $det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}) \neq 0$. Since $det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}) \neq 0$, $\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}$ is invertible over $\mathbb{R}$. Therefore,

$$\begin{cases} c_1 v_1 + c_2 w_2 = x \\ c_1 v_2 + c_2 w_2 = y \end{cases} \implies \begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \implies \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}^{-1} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Let $\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then, $\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$. Since $c_1, c_2 \in \mathbb{Z}$ for any $x, y \in \mathbb{Z}$, $ax + by$ and $cx + dy$ are in $\mathbb{Z}$ for any $x, y \in \mathbb{Z}$. Then, a, b, c, d must be $\in \mathbb{Z}$. Therefore, $\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}$ is ivertible over $\mathbb{Z}$ and by Exercise 47 $det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}) = \pm 1$. □

Geometric properties of a $\mathbb{Z}$-basis. Next, we will consider the geometric properties of a set of two vectors that form a basis of $\mathbb{Z}^2$. First, recall the vector definition of a parallelogram:

Definition 15 The parallelogram $P(\mathbf{v}, \mathbf{w})$ spanned by two vectors $\mathbf{v}$ and $\mathbf{w}$ in $\mathbb{R}^2$ is defined as follows:

$$P(\mathbf{v}, \mathbf{w}) = \{a\mathbf{v} + b\mathbf{w} \text{ such that } 0 \leq a \leq 1 \text{ and } 0 \leq b \leq 1\}.$$

Exercise 52 Sketch the parallelogram spanned by each of the $\mathbb{Z}-$bases for $\mathbb{Z}^2$ that you constructed in Exercise 51.

(a) Find the area of the parallelogram spanned by each of the $\mathbb{Z}-$bases for $\mathbb{Z}^2$ that you constructed in Exercise 51.

(b) State and prove a conjecture about the area of a lattice parallelogram $P(\mathbf{v}, \mathbf{w})$, where $\mathbf{v}$ and $\mathbf{w}$ form a basis of $\mathbb{Z}^2$.

Solution Consider the following suggested $\mathbb{Z}$ bases of $\mathbb{Z}^2$ from Exercise 51.

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w}_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\mathbf{v}_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w}_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\mathbf{v}_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \mathbf{w}_3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

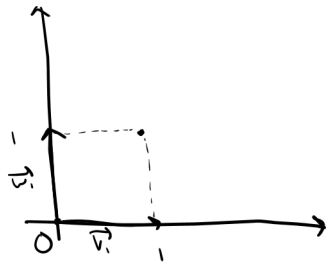


Figure 25: P($\mathbf{v}_1,\ \mathbf{w}_1$).

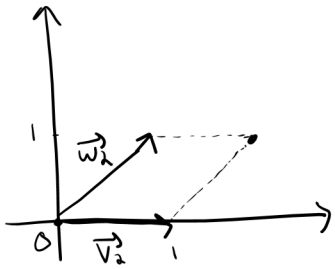


Figure 26: P($\mathbf{v}_2,\ \mathbf{w}_2$).

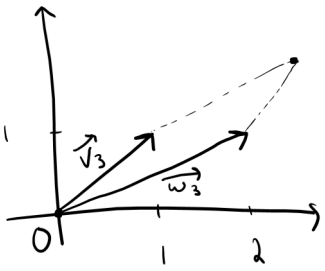


Figure 27: P($\mathbf{v}_3,\ \mathbf{w}_3$).

(a) Consider an arbitrary parallelogram $P(\mathbf{v}, \mathbf{w})$, $\mathbf{v},\ \mathbf{w} \in \mathbb{R}^2$, without loss of generality in the first quadrant as for example in Fig. (28) below.

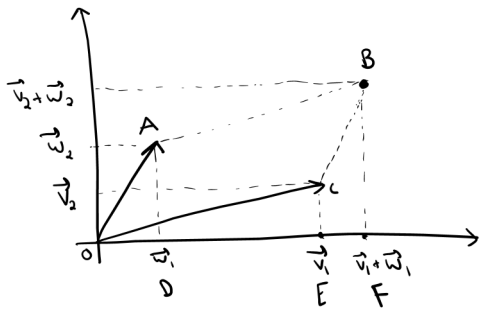


Figure 28: Arbitrary Parallelogram.

$OABC = P(\mathbf{v}, \mathbf{w}),\ \mathbf{v},\ \mathbf{w} \in \mathbb{R}^2$. Then, $Area(OABC) = Area(ABFD) + Area(OAD) - Area(OCE) - Area(CEFB) = \frac{((\mathbf{v}_2+\mathbf{w}_2)+\mathbf{w}_2)\mathbf{v}_1}{2} + \frac{\mathbf{w}_2\mathbf{w}_1}{2} - \frac{\mathbf{v}_2\mathbf{v}_1}{2} - \frac{((\mathbf{v}_2+\mathbf{w}_2)+\mathbf{v}_2)\mathbf{w}_1}{2} = \mathbf{v}_1\mathbf{w}_2 - \mathbf{v}_2\mathbf{w}_1 = |det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix})|$. Therefore, the area of all parallelograms spanned by each of the $\mathbb{Z}$-bases for $\mathbb{Z}^2$ in Exercise 51 is 1.

(b) Conjecture: The area of every lattice parallelogram $P(\mathbf{v}, \mathbf{w})$ where $\mathbf{v},\ \mathbf{w}$ form a basis of $\mathbb{Z}^2$ is 1. Proof: Every parallelogram $P(\mathbf{v}, \mathbf{w})$ has area equal to $|det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix})|$. Since, $\mathbf{v},\ \mathbf{w}$ form a basis of $\mathbb{Z}^2$, $|det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix})| = 1$ by Exercise 51 (c). The proof is complete. □

Exercise 53 Sketch the parallelogram spanned by each of the $\mathbb{Z}-$bases for $\mathbb{Z}^2$ that you constructed in Exercise 51.

(a) How many lattice points are on the sides of the parallelogram? How many lattice points are in the interior?

(b) Doing more computations if necessary, make and prove a conjecture about the number of lattice points on the sides and in the interior of a lattice parallelogram $P(\mathbf{v}, \mathbf{w})$, where $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}-$basis for $\mathbb{Z}^2$.

Solution Consider the following suggested $\mathbb{Z}$ bases of $\mathbb{Z}^2$ from Exercise 51.

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w}_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\mathbf{v}_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{w}_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$
$$\mathbf{v}_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \mathbf{w}_3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

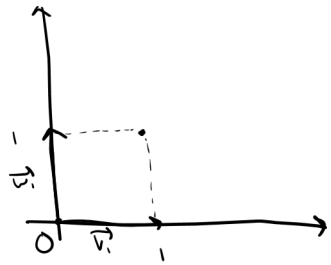


Figure 29: P($\mathbf{v}_1,\ \mathbf{w}_1$).

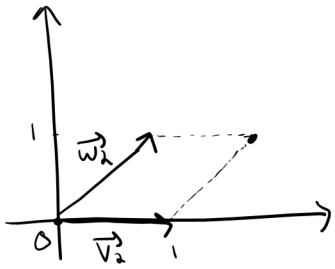


Figure 30: P($\mathbf{v}_2,\ \mathbf{w}_2$).

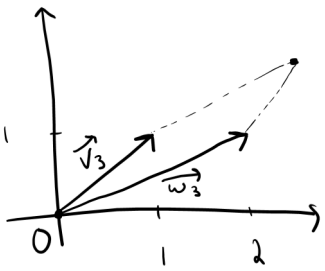


Figure 31: P($\mathbf{v}_3,\ \mathbf{w}_3$).

(a) There are no lattice points on the sides of the parallelogram other than the four vertices. There are no lattice points in their interior.

(b) Conjecture: Consider any lattice parallelogram $P(\mathbf{v}, \mathbf{w})$ where $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}-$basis for $\mathbb{Z}^2$. Then, there are no lattice points on the sides and in the interior of $P(\mathbf{v}, \mathbf{w})$ other than the four vertices.

Proof: I will prove by contradiction that if $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}-$basis for $\mathbb{Z}^2$ in the lattice parallelogram $P(\mathbf{v},\mathbf{w})$, then there are no lattice points on the sides or the interior besides the vertices.

Assume that there is a lattice point $\mathbf{p}$. Then, because $\mathbf{p} \in P(\mathbf{v},\mathbf{w})$ and is not a vertex

$$\mathbf{p} = a\mathbf{v} + b\mathbf{w} \text{ for some } 0 < a < 1,\ 0 < b < 1. \tag{34}$$

But, $\mathbf{v}$ and $\mathbf{w}$ are a $\mathbb{Z}$-basis for $\mathbb{Z}^2 \implies$ there exists $c_1,\ c_2 \in \mathbb{Z}$ such that

$$\mathbf{p} = c_1\mathbf{v} + c_2\mathbf{w}. \tag{35}$$

By (34) and (35),

$$(c_1 - a)\mathbf{v} + (c_2 - b)\mathbf{w} = \mathbf{0} \implies \begin{cases} (c_1 - a)v_1 + (c_2 - b)w_1 = 0 \\ (c_1 - a)v_2 + (c_2 - b)w_2 = 0 \end{cases} \implies \begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix} \begin{bmatrix} c_1 - a \\ c_2 - b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\implies \begin{bmatrix} c_1 - a \\ c_2 - b \end{bmatrix} = \begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$\implies a$ is an integer in (0,1), b is an integer in (0,1). This is a contradiction.

Note: $\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}$ is invertible since it is a $\mathbb{Z}$-basis and therefore has a determinant of ± 1. $\square$

Exercise 54 Suppose that the parallelogram $P(\mathbf{v},\mathbf{w})$, where $\mathbf{v},\ \mathbf{w} \in \mathbb{Z}^2$, is a primitive lattice parallelogram. Show that $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}-$basis for $\mathbb{Z}^2$.

Solution Since $P(\mathbf{v},\mathbf{w})$, $\mathbf{v},\ \mathbf{w} \in \mathbb{Z}^2$ is a parallelogram, $\mathbf{v}$, $\mathbf{w}$ are linearly independent in $\mathbb{R}^2$. (If $\mathbf{v}$ and $\mathbf{w}$ were linearly dependent in $\mathbb{R}^2$, there would have been $k_1, k_2 \in \mathbb{R} - \{0\}$ such that $k_1\mathbf{v} + k_2\mathbf{w} = \mathbf{0} \implies \mathbf{v} = -\frac{k_2}{k_1}\mathbf{w} \implies$ $\mathbf{v},\ \mathbf{w}$ collinear $\implies P(\mathbf{v},\mathbf{w})$ is not a parallelogram, which is a contradiction). Since $\mathbf{v},\ \mathbf{w}$ linearly independent in $\mathbb{R}^2$, there are no $k_1,\ k_2 \in \mathbb{R} - \{0\}$ such that $k_1\mathbf{v} + k_2\mathbf{w} = \mathbf{0}$. Therefore, there are no $k_1,\ k_2 \in \mathbb{Z} - \{0\}$ such that $k_1\mathbf{v} + k_2\mathbf{w} = \mathbf{0}$. Therefore, $\mathbf{v},\ \mathbf{w}$ are linearly independed in $\mathbb{Z}^2$.

Take an arbitrary $\mathbf{u} \in \mathbb{Z}^2$. Because $\mathbf{v}$, $\mathbf{w}$ linearly independent in $\mathbb{R}^2$ there exist $a,\ b \in \mathbb{R}$ such that

$$\mathbf{u} = a\mathbf{v} + b\mathbf{w}. \tag{36}$$

I will show that $a,\ b$ are in fact in $\mathbb{Z}$ therefore, $\mathbf{v}$, $\mathbf{w}$ are a $\mathbb{Z}$-basis of $\mathbb{Z}^2$.

Let $\lfloor a \rfloor$ be the largest integer less than or equal to a. Let $\lfloor b \rfloor$ be the largest integer less than or equal to b. Then,

$$a = \lfloor a \rfloor + x,\ x \in [0, 1)$$
$$b = \lfloor b \rfloor + y,\ y \in [0, 1).$$

By (36), $\mathbf{u} = \lfloor a \rfloor\mathbf{v} + x\mathbf{v} + \lfloor b \rfloor\mathbf{w} + y\mathbf{w} \implies x\mathbf{v} + y\mathbf{w} = \mathbf{u} - \lfloor a \rfloor\mathbf{v} - \lfloor b \rfloor\mathbf{w}$ in $\mathbb{Z}^2$ and in $P(\mathbf{v},\mathbf{w})$ because $x \in [0, 1)$ and $y \in [0, 1)$. But, $P(\mathbf{v},\mathbf{w})$ is primitive which implies $x = 0,\ y = 0$ and $a, b \in \mathbb{Z}$. $\square$

Exercises 53 and 54 combine to give us the following theorem:

Theorem 1 Let $\mathbf{v}$ and $\mathbf{w}$ be vectors in $\mathbb{Z}^2$. The parallelogram $P(\mathbf{v},\mathbf{w})$ spanned by $\mathbf{v}$ and $\mathbf{w}$ is primitive if and only if $\{\mathbf{v},\mathbf{w}\}$ is a $\mathbb{Z}-$basis for $\mathbb{Z}^2$.

Exercise 55 Let T be a primitive lattice triangle. If $\mathbf{v}$ and $\mathbf{w}$ are vectors corresponding to adjacent sides of T, show that $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}-$basis of $\mathbb{Z}^2$.

Solution Consider the primitive lattice triangle OAB formed by $\mathbf{v}$ and $\mathbf{w}$ in Fig. 32.

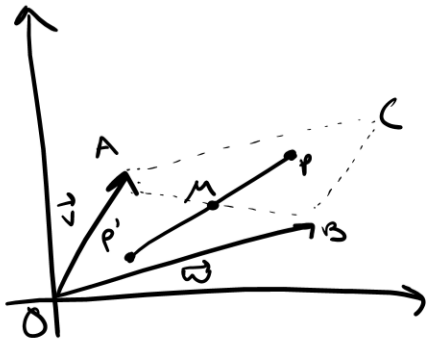


Figure 32: Primitive lattice triangle OAB.

Consider next the lattice parallelogram $OACB$ defined by $P(v,w) = \{a\mathbf{v} + b\mathbf{w} : \ 0 \leq a \leq 1, \ 0 \leq b \leq 1\}$.

Assume that there is a lattice point in the interior of $\triangle ACB$, say P. Say M is the midpoint of AB (diagonal of $ACBO$). Then, P' on the line defined by MP with $length(P'M) = length(MP)$ is in the interior of $\triangle OAB$ and is a lattice point by the rotational symmetry of the lattice plane by 180°. This is a contradiction because $\triangle OAB$ is lattice primitive. We conclude that $P(v,w)$ is primitive.

Then, by Theorem 1 above, $\{\mathbf{v}, \ \mathbf{w}\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}^2$. □

Exercise 56 Prove that the area of a primitive lattice triangle is equal to $\frac{1}{2}$.

Solution

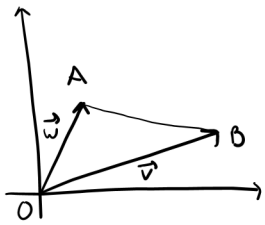


Figure 33: Primitive lattice triangle OAB.

Consider an arbitrary primitive lattice triangle OAB formed by vectors $\mathbf{v}$ and $\mathbf{w}$ as in Fig. (33).

Because OAB is primitive, by Exercise 55 $\mathbf{v}$ and $\mathbf{w}$ are a $\mathbb{Z}$-basis of $\mathbb{Z}^2$.

Consider the parallelogram $P(\mathbf{v},\mathbf{w})$. Area of $(P(\mathbf{v},\mathbf{w}))$= 2∗Area$(OAB)$ which by Exercise 52

$$= |det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix})| \tag{37}$$

But, $\mathbf{v}, \ \mathbf{w}$ are a $\mathbb{Z}$-basis for $\mathbb{Z}^2 \implies$

$$|det(\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix})| = 1 \tag{38}$$

By (37) and (38), Area$(OAB) = \frac{\text{Area}(P(\mathbf{v},\mathbf{w}))}{2} = \frac{1}{2}$. □

4 Pick's Theorem

Pick's Theorem was published in 1899 by Georg Alexander Pick, an Austrian mathematician born in Vienna in 1859. Pick published his first mathematical paper when he was only 17 years old, and went on to publish over 70 papers on a wide range of topics including linear algebra, calculus, and geometry. He was the head of the committee at the University of Prague which appointed Albert Einstein to his position of chair of mathematical physics in 1911, and was in fact a driving force behind the appointment. Tragically, Pick was sent to the Theresienstadt concentration camp in 1942, and died there 2 weeks after his arrival. Pick's Theorem is a beautiful result on determining the area of a lattice polygon. Although the result was published in 1899, it was not popularized until Dyonizy Steinhaus included it in his 1969 text *Mathematical Snapshots*.

Theorem 2 Pick's Theorem. Let P be a lattice polygon in $\mathbb{R}^2$. Suppose that there are $B(P)$ lattice points on the boundary of P and $I(P)$ lattice points in the interior of P. Then the area $A(P)$ is given by:

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

4.1 Proof of Pick's Theorem using Graph Theory

We will need a few classic dissection theorems to prove Pick's Theorem using graph theory.

Theorem 3 Every convex n-gon can be dissected into $n-2$ triangles by means of nonintersecting diagonals. The vertices of the triangles in this dissection by diagonals are vertices of the original polygon.

Exercise 57 Prove Theorem 3.

Solution Consider an arbitrary convex n-gon (a polygon with n vertices and n edges). Pick one vertex and draw lines to every non-adjacent vertex. Evidently, these lines are non-intersecting and form a triangulation of the convex n-gon into $n-2$ triangles. We can formally prove this by considering the triangulated n-gon as a planar graph (since no edges intersect using this method of triangulation) and using Euler's formula for planar graphs. Euler's formula states that $f = 2 + e - v$ for planar graphs with f regions, e edges, and v vertices. The n-gon triangulated with this method has n vertices and $n + n - 3 = 2n - 3$ edges. Therefore, by Euler's formula, the triangulated n-gon has $f = 2 + 2n - 3 - n = n - 1$ regions. This include the exterior region so the triangulated n-gon has $n - 1 - 1 = n - 2$ interior regions, i.e. interior triangles. □

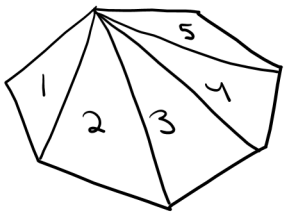


Figure 34: 7-gon triangulation example into n-2=7-2=5 triangles.

It turns out that the statement of Theorem 3 is true even if the polygon is not convex! The proof is much more technical, but it's an interesting and beautiful result to work through!

Theorem 4 Every n-gon can be dissected into $n-2$ triangles by means of nonintersecting diagonals. The vertices of the triangles in this dissection by diagonals are vertices of the original polygon.

Exercise 58 Prove Theorem 4. Hint: induction on n, the number of vertices of the polygon.

Solution Per instructions by the teacher, I will not attempt to prove Theorem 4, but instead I give below three demonstrations of triangulation of non-convex n-gons.

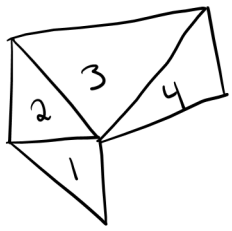


Figure 35: Triangulation of a non-convex 5-gon.

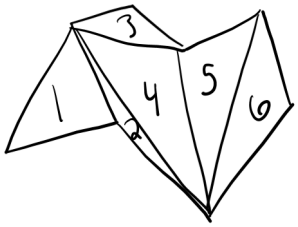


Figure 36: Triangulation of a non-convex 8-gon.

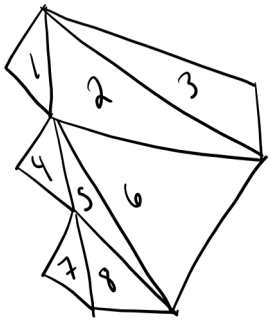


Figure 37: Triangulation of a non-convex 10-gon.

Observe that Theorem 4 implies that every lattice polygon P can be dissected into lattice triangles whose vertices are vertices of P. Since the vertices of P are lattice points (by definition of lattice polygon), Theorem 4 therefore implies that every lattice polygon P can be dissected into *lattice triangles* whose vertices are vertices of P. Next, although we will lose the property that all the vertices of the triangles in the triangulation are vertices of P, we will consider a "finer" dissection of a lattice polygon into lattice triangles.

Lemma 1 Every lattice triangle can be dissected into primitive lattice triangles.

Exercise 59 Prove Lemma 1. Hint: induction on the number of interior lattice points in the lattice triangle.

Solution I will prove that every lattice triangle can be dissected into primitive lattice triangles by induction on the number of interior lattice points in the lattice triangle.

Case $p = 0$ lattice points on the interior: Consider an arbitrary nonprimitive triangle ABC with $p = 0$ lattice points on the interior.

Since $p = 0$ and ABC is not primitive, there are one or more boundary lattice points on ABC (that is, lattice points on the sides of ABC other than the vertices).

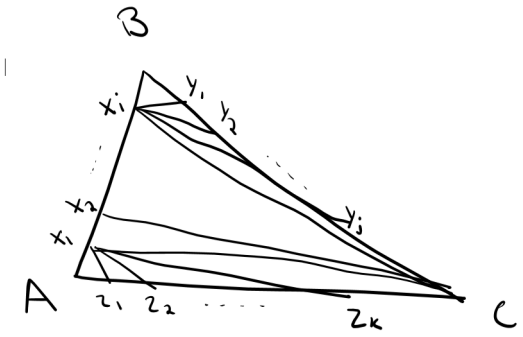


Figure 38: ABC with boundary lattice points and p=0.

Say $X_1, X_2, ..., X_i$ are boundary lattice points on AB, $Y_1, Y_2, ..., Y_j$ are boundary lattice points on BC, and $Z_1, Z_2, ..., Z_k$ are boundary lattice points on AC as in Fig. (38).

Draw lines $CX_1, CX_2, ..., CX_i$; $X_iY_1, X_iY_2, ..., X_iY_j$; $X_1Z_1, X_1Z_2, ..., X_1Z_k$.

ABC has been dissected into primitive lattice triangles. We conclude that for the the case $p = 0$ lattice points in the interior of a lattice triangle we can always dissect the lattice triangle into primitive lattice triangles.

Assume now without loss of generality due to the study above that ABC is a lattice triangle with no boundary lattice points and $p = 1$ lattice points in the interior as in Fig. (39).

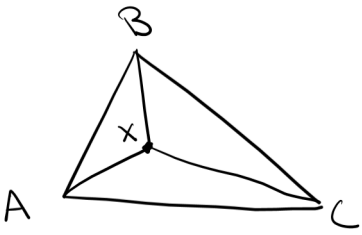


Figure 39: ABC with no boundary lattice points and p=1.

Draw AX, BX, CX and we have dissected ABC into three primitive lattice triangles ABX, BCX, ACX.

Now assume that we can dissect any lattice triangle ABC with $1 < p \leq n$, $W_1, W_2, ..., W_n$ interior lattice points into primitive triangles.

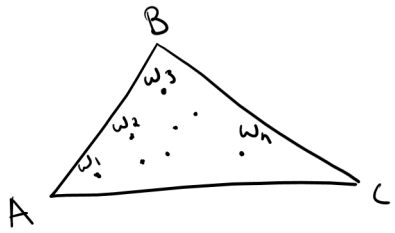


Figure 40: ABC with $1 < p \leq n$ interior lattice points.

Consider a lattice triangle with $p = n + 1$ interior lattice points $W_1, W_2, ..., W_n, W_{n+1}$.

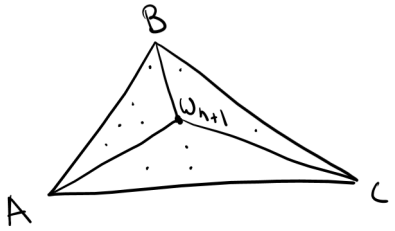


Figure 41: ABC with $p = n + 1$ interior lattice points.

Draw $AW_{n+1}, BW_{n+1}, CW_{n+1}$. $ABW_{n+1}, BCW_{n+1}, ACW_{n+1}$ are all lattice triangles with less than or equal to n interior lattice points each. Therefore, they can all be dissected into primitive lattice triangles one by one.

We conclude that any lattice triangle ABC with $n + 1$ interior lattice points can be dissected.

Finally, we conclude by inductive argument that every lattice triangle can be dissected into primitive lattice triangles. □

Theorem 5 Every lattice polygon can be dissected into primitive lattice triangles.

Exercise 60 Prove Theorem 5.

Solution By Theorem 4, we can triangulate any lattice n-gon into lattice triangles. By Lemma 1, every lattice triangle can be dissected into primitive lattice triangles. Therefore, every lattice polygon can be dissected into primitive lattice triangles. □

Exercise 61 Dissect the twelve lattice polygons in Figure 42 into primitive lattice triangles. Note: you do not need to reproduce these drawings when you turn in your portfolio, but you will need the dissections when you complete Exercise 62.

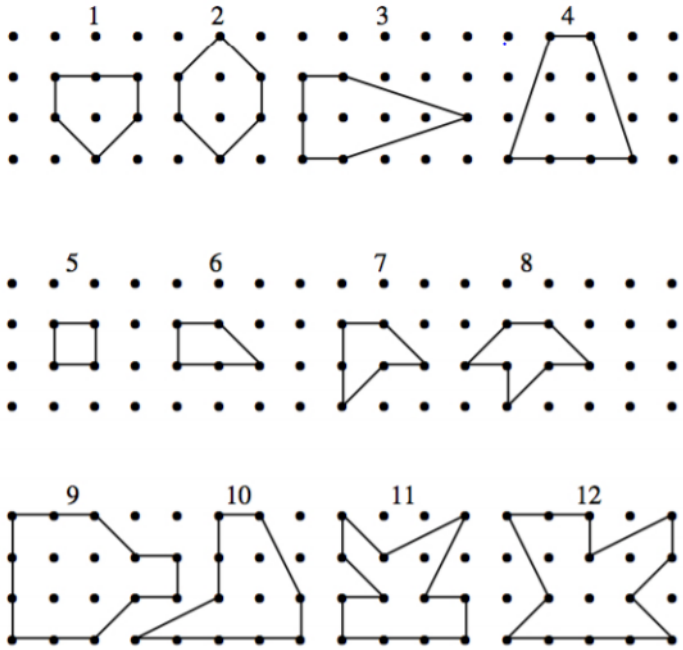


Figure 42: Dissect these lattice polygons into primitive lattice triangles.

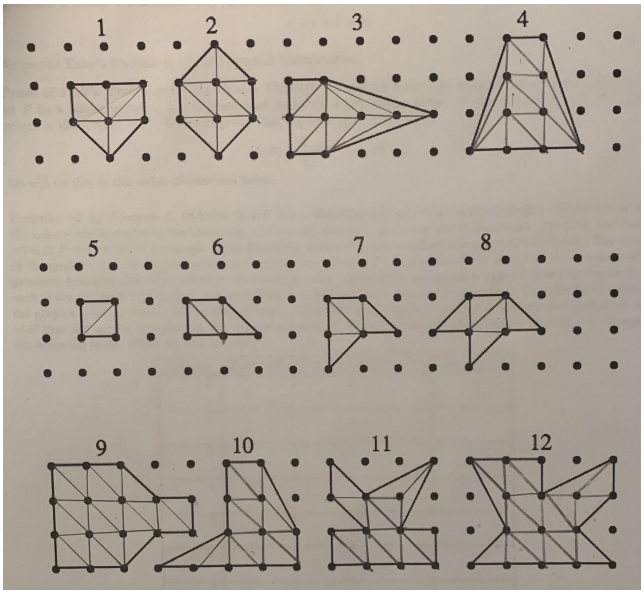


Figure 43: Dissected lattice polygons into primitive lattice triangles.

In this section, we will prove Pick's Theorem using graph theory. Before we get started, we need to recall few definitions from our study of graph theory.

Definition 16 A *graph* $G = (V, E)$ consists of a nonempty, finite set V of *vertices* and a finite set E of unordered pairs of distinct elements of V called *edges*. If $\{u, v\}$ is an edge e of G, the edge e is said to connect u and v, and

the vertices u and v are the endpoints of the edge e.

Definition 17 Planar Graph. A graph is said to be *planar* if it can be **drawn in such a way** that no two edges cross (i.e. pairs of edges only intersect at vertices). A planar graph splits the plane into regions or faces, including one unbounded region "outside" the graph. Given a planar representation of a graph G, a *region* or *face* is a maximal section of the plane in which any two points can be joined by a curve that does not intersect any part of G. For example, the graph in Figure **??** contains 5 regions.

Theorem 6 Euler's Formula: If G is a connected, planar graph with v vertices, e edges, and f regions, then:

$$v - e + f = 2.$$

We proved Euler's Formula in UM160 Discrete Mathematics.

Proof of Pick's Theorem Using Graph Theory. We will use Euler's formula to prove Pick's Theorem. We let P be a lattice polygon, and suppose that there are $B(P)$ lattice points on the sides of P and $I(P)$ lattice points in the interior of P. We must prove that the area $A(P)$ is given by

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

We will do this in the series of exercises below.

Exercise 62 By Theorem 5, we know that P has a dissection into primitive lattice triangles. Observe that since the sides of the triangles in the dissection of P do not intersect, and since the triangles are primitive, each lattice point in P is a vertex of a triangle. This dissection makes P a connected planar graph G as follows. The vertices of the graph G are the lattice points in P and on the sides of P. The edges of the graph G are the sides of the primitive triangles that triangulate P. Demonstrate this construction using the polygons shown in Figure 42. For each of the polygons in Figure 42, use your dissection into primitive lattice triangles from Exercise 61 to construct the graph G. Let e_i denote the number of edges of G *inside* the polygon P and let e_b denote the number of edges of G that are on the *boundary* of the original polygon P. Finally, compute the quantity $2v - e_b - 1$. Complete the following table. What do you observe?

Polygon	Area of P	f = # of regions of G	$2v - e_b - 1$
1	3	7	7
2	4	9	9
3	5	11	11
4	6	13	13
5	1	3	3
6	$\frac{3}{2}$	4	4
7	2	5	5
8	$\frac{5}{2}$	6	6
9	9	19	19
10	6	13	13
11	6	13	13
12	$\frac{17}{2}$	18	18

I observe that the number of regions of G is equal to the quantity $2v - e_b - 1$. □

For the next series of exercises, let G denote the connected planar graph that results from dissecting a lattice polygon P into primitive lattice triangles. Let f denote the number of regions in G, let e be the number of edges in G, and let v be the number of vertices in G.

Exercise 63 Use Exercise 56 to state and prove an equation that relates the area of P to f.

Solution Consider an arbitrary lattice polygon P. From Theorem 5 we know that every lattice polygon can be dissected into primitive lattice triangles. From Exercise 56 we know that the area of every primitive lattice triangle is $\frac{1}{2}$. Therefore, the area of a given polygon P is equal to the number of primitive lattice triangles in which it is dissected times $\frac{1}{2}$.

The dissected form of the polygon is a planar graph (no two edges cross) if you take the vertices of the triangles to be the vertices of the planar graph and the sides of the triangles to be the edges. The number of faces of the planar graph is then the number of primitive lattice triangles plus 1. We conclude that the area of a lattice polygon

$$P = (f - 1) \cdot \frac{1}{2} \tag{39}$$

where f is the number of faces of the planar graph created by dissecting P into primitive triangles.

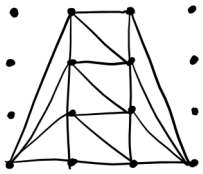


Figure 44: An illustration of a dissected lattice 4-gon into primitive lattice triangles.

Exercise 64 The next step in the proof of Pick's Theorem is to compute e and relate it to f. Let e_i denote the number of edges of G *inside* the polygon P and let e_b denote the number of edges of G that are on the *boundary* of the original polygon P. Show that

$$f = 2v - e_b - 1.$$

Solution By Euler's formula, $v - e_i - e_b + f = 2 \implies f = e_i + e_b - v + 2$. Since $f - 1$ is the total number of primitive lattice triangles (created by dissecting P by Theorem 5), $3(f-1)$ is the number of sides of the primitive lattice triangles. But, $3(f-1) = e_b + 2e_i$ because each of the interior edges e_i borders two interior triangles, while each of the boundary edges e_b borders only one triangular. So,

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

Because $e_b + e_i = e$,

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

by Euler's formula. Therefore,

$$3(f-1) = 2(f+v-2) - e_b \implies$$
$$f = 2v - e_b - 1. \quad \square$$

Exercise 65 Finally, show that

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

This concludes the proof of Pick's Theorem!

Solution By Theorem 5, any lattice polygon can be split into $f-1$ primitive lattice triangles, each with area $\frac{1}{2}$. Thus, $A(P) = \frac{1}{2}(f-1)$. From Exercise 64, $f = 2v - e_b - 1$; so ,

$$A(P) = \frac{1}{2}(2v - e_b - 1 - 1) = v - \frac{1}{2}e_b - 1. \tag{40}$$

Every graph vertex is either an interior point or a boundary point of the lattice polygon; so, $v = I(P) + B(P)$. Further, in any lattice polygon $e_b = B(P)$. By making these two substitutions into (40), we obtain

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

concluding the proof of Pick's Theorem. $\square$
We will provide two additional proofs of Pick's Theorem. The next proof is fairly short, but does require a number of new ideas. The final proof is a proof by induction.

4.2 Proof of Pick's Theorem by Additivity

Let P be a lattice polygon in the plane. We will need the following definitions:

Definition 18 For each $p \in \mathbb{Z}^2$, we define $a_p(P)$, called *the measure of the internal angle of P at p*, as follows:

- If p is a vertex of P, then $a_p(P)$ is the measure of the interior angle of the polygon at p.
- If p is on a side of P, but is not a vertex of P, then $a_p(P) = \pi$.
- If p is in the interior of P, then $a_p(P) = 2\pi$.
- For all other lattice points $p \in \mathbb{Z}^2$, we set $a_p(P) = 0$.

Definition 19 The *lattice weight* of P at p is defined as

$$w_p = \frac{1}{2\pi} a_p(P).$$

Definition 20 The *total weight* of P is

$$W(P) = \sum_{p \in \mathbb{Z}^2} w_p(P).$$

Exercise 66 Why is $W(P)$ finite?

Definition 21 Let P be a lattice polygon, and let Q be a lattice polygon whose intersection with P is a portion s' of a side s of P. Then the *join*, or *sum*, of P and Q, denoted $P + Q$, is the lattice polygon obtained by gluing P and Q along s'. The vertices, boundary lattice points, and interior lattice points of P and of Q that do not lie on s' become vertices, boundary lattice points, and interior lattice points, respectively, of $P + Q$, as described in the following way. Let p' be a lattice point on s'.

- If p' is a vertex of P but not a vertex of Q, then p' is a vertex of $P + Q$:
- If p' is a vertex of P and a vertex of Q, and if the interior angles of P and Q at p' are not supplementary, then p' is also a vertex of $P + Q$:
- If p' is a vertex of P and a vertex of Q, and if the interior angles of P at p' and Q are supplementary, then p' is a lattice point on a side of $P + Q$, but is not a vertex of $P + Q$:
- Similar statements hold if the initial hypothesis is that p' is a vertex of Q.
- If p' is a lattice point on s' that is not a vertex of P or Q, then p' is an interior point of $P + Q$.

Exercise 67 Construct a lattice polygon P and a lattice polygon Q whose intersection with P is a portion s' of a side s of P. Then construct the join $P + Q$ using Definition 21.

Lemma 2 Let P be a lattice polygon, and let Q be a lattice polygon whose intersection with P is a portion s' of a side s of P. Then

$$W(P + Q) = W(P) + W(Q).$$

Lemma 2 says that W is **additive**. Observe that area is also clearly additive: if P is a lattice polygon and Q is a lattice polygon whose intersection with P is a portion s' of a side s of P, then $A(P + Q) = A(P) + A(Q)$. These additivity properties will be useful when we prove Pick's Theorem.

Lemma 3 Let P be a lattice polygon. Then

$$W(P) = A(P),$$

where $W(P)$ is the total weight of P and $A(P)$ is its area.

Proof: We will prove this lemma in a series of exercises. We will use the additivity of $W(P)$ and $A(P)$ to prove equality by triangulating P. We begin by first considering two special cases.

Exercise 68 *Case 1.* Suppose that R is a lattice rectangle of length r and width s with horizontal and vertical sides.

(a) How many lattice points does R have on its sides? How many of these are vertices?

(b) How many interior lattice points does R have?

(c) Compute $W(R)$ and $A(R)$ and show that they are equal.

Exercise 69 *Case 2.* Suppose that T is a lattice right triangle with horizontal and vertical legs of length r and s, respectively. Show that $W(T) = A(T)$. Hint: consider the triangle T' obtained by rotating T by π around the midpoint of the hypotenuse of T. Together T and T' form a rectangle. Explain why $W(T) = W(T')$ and $A(T) = A(T')$ and use Case 1.

Now suppose that T is an arbitrary lattice triangle. We can embed T into the smallest possible lattice rectangle R with horizontal and vertical sides. There are two cases to consider in this scenario:

- If all of the interior angles of T measure at most $\pi/2$, then R is the union of T and three Case 2 lattice triangles.
- If T has an interior angle measuring more than $\pi/2$, then R is the union of T, a Case 1 lattice rectangle, and three Case 2 lattice triangles.

Exercise 70 Show that $W(T) = A(T)$ in both of the cases described above.

Finally, if P is an arbitrary lattice n-gon, then by Theorem 4, P can be dissected into lattice triangles. Thus, by additivity, $W(P) = A(P)$. To finish the proof of Pick's Theorem, we will show that

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

Once we have proven this equality, Pick's Theorem will follow from Lemma 3.

Exercise 71 Let P be a lattice n-gon. Let $B(P)$ denote the number of lattice points on the sides (boundary) of P, and let $I(P)$ denote the number of interior lattice points of P.

(a) How many vertices does n have?

(b) How many lattice points does P have on its sides that are *not* vertices?

(c) What is the sum of the interior angles of P?

(d) Use (a)-(c) to show that the sum of w_p as p ranges over all points on the sides (boundary) of P is

$$\frac{1}{2}B(P) - 1.$$

(e) Show that the sum of w_p as p ranges over all the lattice points in the interior of P is $I(P)$.

(f) Conclude that

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

Since $A(P) = W(P)$ by Lemma 3, Exercise 71 implies that

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

as needed. This concludes the proof of Pick's Theorem!

4.3 Proof of Pick's Theorem by Induction

In this series of exercises, we will prove Pick's Theorem using induction on the number of sides of the polygon.

Exercise 72 Consider an $m \times n$ lattice-aligned rectangle:

Show that Pick's Theorem holds for a lattice-aligned rectangle.

Exercise 73 Prove that Pick's Theorem holds for a lattice-aligned right triangle with legs of lengths m and n.

Exercise 74 The next step is to show that Pick's Theorem holds for arbitrary lattice triangles. If T is an arbitrary lattice triangle, draw right triangles A, B, C to form a rectangle R, as shown below.

Use the results of the previous exercises to show that Pick's theorem holds for an arbitrary lattice triangle T.

So far, we've shown that Pick's Theorem is true for every polygon with 3 sides. To complete the proof that Pick's Theorem is true for any polygon, we'll use induction on the number of sides of the polygon. The base case is $n = 3$ sides, and we've already shown that Pick's Theorem holds for $n = 3$. For the inductive step, assume that Pick's Theorem holds for $n = 3, 4, \ldots, k-1$ sides. We must now prove that Pick's Theorem holds for $n = k$ sides to complete the induction.

Exercise 75 Suppose that P is a polygon with k sides ($k > 3$). Show that P must have an *interior diagonal* that will split P into 2 smaller polygons. Here's an example. OW is the interior diagonal for this example.

Once we have shown that we can always split a polygon P with k sides into 2 smaller polygons P_1 and P_2 (each with fewer than k sides), the final step is to show that if 2 polygons satisfy Pick's Theorem, then the polygon formed by *attaching* the 2 will also satisfy Pick's Theorem. Since the smaller polygons satisfy Pick's Theorem by the inductive hypothesis, we have

$$A(P) = A(P_1) + A(P_2) = I_1 + \frac{B_1}{2} - 1 + I_2 + \frac{B_2}{2} - 1.$$

Exercise 76 Finally, find a relationship between I and I_1, I_2 and between B and B_1, B_2 to conclude that

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

This concludes the proof of Pick's Theorem!

5 Applications of Pick's Theorem

Exercise 77 Use Pick's Theorem to prove that it is not possible to construct an equilateral lattice triangle.

Solution Assume that there exists an equilateral lattice triangle with side length l and height h as in Fig. 45.

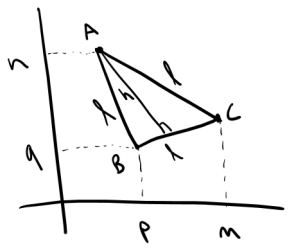


Figure 45: An assumed equilateral lattice triangle.

By the Pythagorean Theorem, $l^2 = h^2 + (\frac{l}{2})^2 \implies h^2 = l^2 - \frac{l^2}{4} = \frac{3l^2}{4} \implies h = \frac{\sqrt{3}l}{2}$. Then,

$$Area(\triangle ABC) = \frac{l \cdot h}{2} = \frac{l^2\sqrt{3}}{4}. \tag{41}$$

Also,

$$l^2 = (n-q)^2 + (m-p)^2 \in \mathbb{Z}^+. \tag{42}$$

By (41) and (42), Area($\triangle$ ABC) is irrational. However, by Pick's Theorem, $Area(\triangle ABC) = I(\triangle ABC) + \frac{B(\triangle ABC)}{2} - 1$ which is rational.

We reach a contradiction, hence it is not possible to construct an equilateral lattice triangle. $\square$

Exercise 78 Use Pick's Theorem to show that the area of a primitive lattice triangle is equal to 1/2. (Of course, we used this fact in our proof of Pick's Theorem, so it was necessary to have an independent derivation of this.)

Solution By Pick's Theorem the area of a primitive lattice triangle ABC is Area($\triangle$ ABC)= $I(\triangle ABC) + \frac{B(\triangle ABC)}{2} - 1 = 0 + \frac{3}{2} - 1 = \frac{1}{2}$. $\square$

Exercise 79 Use Pick's Theorem to show that if it is possible to construct a regular lattice n-gon, then $\tan\left(\frac{\pi}{n}\right)$ is rational.

Note: If you are interested in exploring this result further, please let me know! It is an interesting (and challenging) problem to classify those integers n for which $\tan\left(\frac{\pi}{n}\right)$ is rational. You can also prove that the statement above is actually and if and only if statement.

Solution

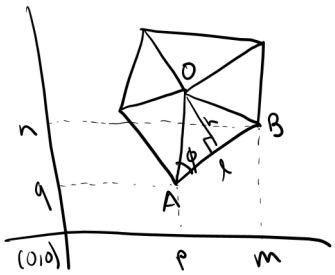


Figure 46: Hypothetical regular lattice n-gon with side length l.

Assume that there exists a regular lattice n-gon as in Fig. 46. Each angle of the polygon has value $\frac{(n-2)\pi}{n}$. If O is the center of the regular n-gon, the n-gon can be divided into n equal-area triangles of the form of the triangle OAB in Fig.46 where

$$\phi = \frac{(n-2)\pi}{2n}. \tag{43}$$

Then,

$$Area(n-gon) = n \cdot Area(3-gon) = n\frac{l \cdot h}{2}. \tag{44}$$

Also,

$$\tan\phi = \frac{h}{\frac{l}{2}} \implies h = \tan\phi \cdot \frac{l}{2}. \tag{45}$$

By (44) and (45),

$$Area(n-gon) = \frac{n \cdot l \cdot \tan\phi \cdot \frac{l}{2}}{2} = \frac{n \cdot \tan\phi \cdot l^2}{4}. \tag{46}$$

By Pick's Theorem,

$$Area(n-gon) = I(P) + \frac{B(P)}{2} - 1 \text{ and rational.} \tag{47}$$

By (46) and (47), $\frac{n\cdot\tan\phi\cdot l^2}{4}$ is rational. But, $l^2 = (m-p)^2 + (n-q)^2$ is in $\mathbb{Z}^+$, therefore $\tan\phi$ must be rational. But, $\tan\phi = \tan\frac{(n-2)\pi}{2n} = \tan(\frac{\pi}{2} - \frac{\pi}{n}) = \frac{1}{\tan(\frac{\pi}{n})}$.

We conclude that $\tan(\frac{\pi}{n})$ must be rational if a regular lattice n-gon exists. □

Exercise 80 Show that if P is a convex lattice pentagon, then the area of P must be greater than or equal to 5/2. Is this bound strict? In other words, is it possible to construct a convex lattice pentagon with area equal to 5/2?

Solution Consider an arbitrary convex lattice pentagon with set of vertices $V = \{v_1 = (m_1, n_1), v_2 = (m_2, n_2), ..., v_s = (m_s, n_s)\}$.

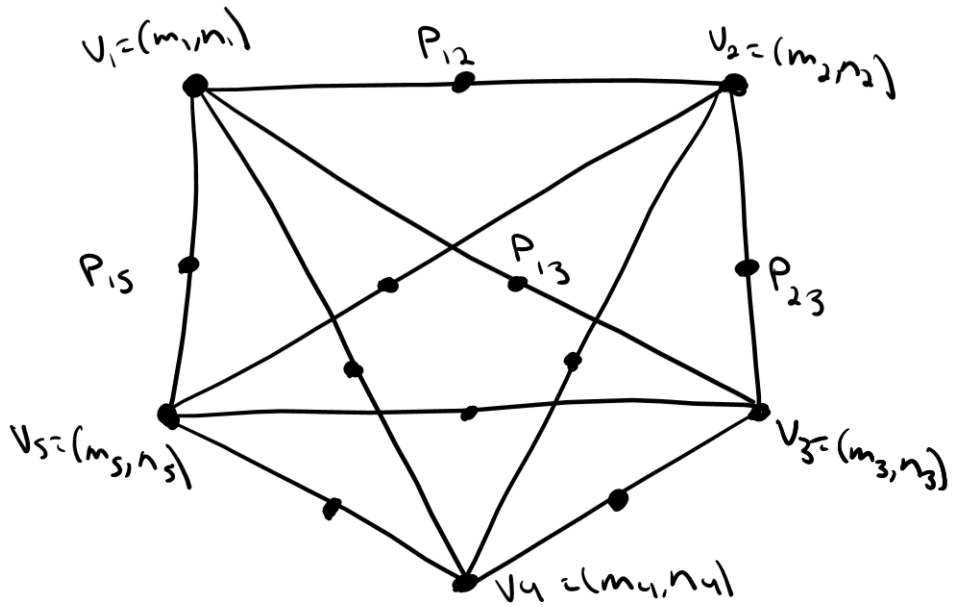


Figure 47: Convex lattice pentagon P with midpoints $p_{ij},\ i \neq j \in \{1, ..., 5\}$.

Consider the midpoint p_{ij} between any two points $v_i,\ v_j \in V$. Then,

$$p_{ij} = (\frac{m_i + m_j}{2}, \frac{n_i + n_j}{2}).$$

There are $\binom{5}{2} = 10$ such midpoints. At least one of them is lattice. Indeed, at least one pair of points in set V has the same even/odd parity because there are 4 possibilities (ee, eo, oe, oo) and 5 points (pigeonhole principle).

If the lattice midpoint is not between adjacent vertices, then the lattice point is in the interior of P because P is convex. In that case,

$$I(P) \geq 1. \tag{48}$$

By Pick's Theorem,

$$Area(P) = \frac{B(P)}{2} + I(P) - 1. \tag{49}$$

By (48) and (49),

$$Area(P) \geq \frac{5}{2} + 1 - 1 = \frac{5}{2}. \tag{50}$$

If the lattice point is $p_{i,i+1}$ between adjacent vertices $v_i,\ v_i + 1,\ i \in \{1, 2, 3, 4\}$, then at least two of the five points $p_{i,i+1},\ i \in \{1, 2, 3, 4\}$, and $v_j,\ j \in \{1, 2, 3, 4, 5\}$ and $j \neq i$, have the same parity and therefore a lattice midpoint either on the boundary or in the interior of the pentagon. As a lower bound on the area of P, the boundary point is worst case scenario and gives

$$B(P) \geq 5 + 1 + 1 = 7. \tag{51}$$

By (49) (Pick's Theorem) and (51), again

$$Area(P) \geq \frac{7}{2} + 0 - 1 = \frac{5}{2}. \tag{52}$$

The lower bound in (52) is tight (attainable). Consider the lattice pentagon in Fig. 48 with Area$= \frac{5}{2} + 1 - 1 = \frac{5}{2}$. □

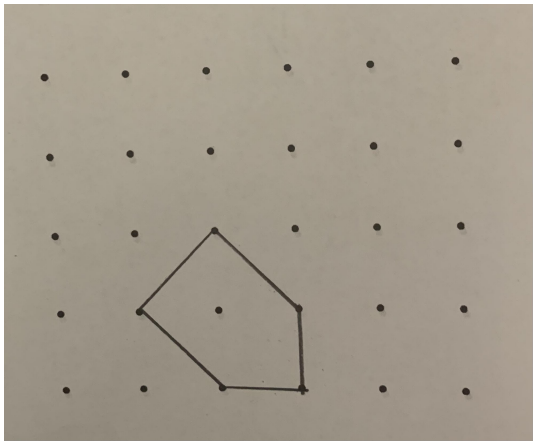


Figure 48: Lattice pentagon with area $\frac{5}{2}$.

Exercise 81 Let A denote the point $(n, 0)$ and let B denote the point $(0, n)$. There are $n-1$ lattice points, each of the form $(i, n-i)$, for $i = 1, 2, 3, \ldots, n-1$, between A and B. Connect each one of them with the origin $O(0, 0)$. The lines divide $\triangle OAB$ into n small triangles. It is clear that the 2 triangles next to the axes (i.e. the triangle adjacent to the x-axis and the triangle adjacent to the y-axis) contain no lattice points in their interior. Prove that if n is prime, then each of the remaining triangles contains exactly the same number of interior lattice points. Find an expression (in terms of n) for the number of interior lattice points in each of these triangles.

Solution

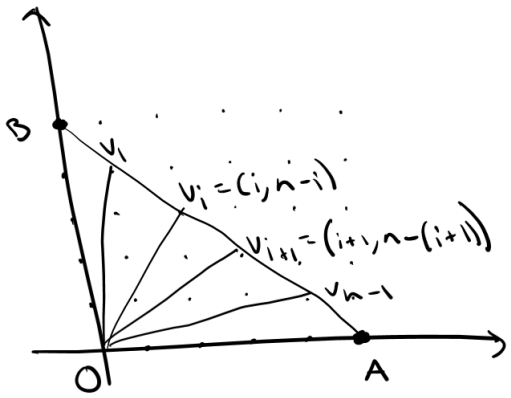


Figure 49: Exercise 81 with n=5 (prime) and general interior triangle OV_iV_{i+1}.

Consider a general interior (non-primitive) triangle OV_iV_{i+1} created by the described process.

$$Area(\triangle OV_iV_{i+1}) = \frac{|det(\begin{bmatrix} i & i+1 \\ n-i & n-i-1 \end{bmatrix})|}{2} = \frac{|i(n-i-1)-(n-i)(i+1)|}{2} = \frac{n}{2} \tag{53}$$

same for each of the interior triangles. Regarding boundary lattice points on $\triangle OV_iV_{i+1}$, there is no boundary point on V_iV_{i+1} because $V_i = (i, n-1)$ and $V_{i+1} = (i+1, n-(i+1))$.The number of boundary points on OV_i excluding O and V_i is $gcd(i, n-i) - 1$ (Ex. 29). Say $gcd(i, n-i) = k$. Then, $\frac{i}{k}$ integer and $\frac{n-i}{k} = \frac{n}{k} - \frac{i}{k}$ integer; $\frac{n}{k}$ minus an integer is an integer means that $\frac{n}{k}$ is an integer. But n is prime $\implies k = 1$, i.e. $gcd(i, n-i) = 1$.

Therefore, the number of boundary points on OV_i excluding O and V_i is zero. Similarly, the same holds true for OV_{i+1}.

We conclude that the boundary lattice points of $\triangle OV_iV_{i+1}$ is

$$B(\triangle OV_iV_{i+1}) = 3. \tag{54}$$

By Pick's Theorem, (53), and (54), $\frac{n}{2} = \frac{3}{2} + I(\triangle OV_iV_{i+1}) - 1 \implies I(\triangle OV_iV_{i+1}) = \frac{n}{2} - \frac{1}{2} = \frac{n-1}{2}$. $\square$

Exercise 82 Let n be an integer greater than or equal to 3. Prove that there is a set of n points in the plane such that the distance between any 2 points is irrational and each set of three points determines a non-degenerate triangle with rational area.

Solution Consider the set of points (i, i^2), $i \in \mathbb{Z}^+$. Degenerate triangles are those with all three vertices on a line. All the points in the set (i, i^2) lie on the parabola $y = x^2$ and no three points on a parabola lie on the same line. Therefore, any set of 3 points in the set (i, i^2) $(i \in \mathbb{Z}^+)$ forms a non-degenerate lattice triangle. By Pick's Theorem, this triangle has rational area.

Now, assume for a proof by contradiction that the distance between two points in the set, say (w, w^2) and (v, v^2) with $w < v$ is rational. Set $D = (v - w)^2 + (v^2 - w^2)^2$. Then, $D \in \mathbb{Z}^+$ and D is the square of the distance between (w, w^2) and (v, v^2) (see Fig. 50). If D is not a perfect square, then $\sqrt{D}$ which is the distance is irrational. Thus, D is a perfect square and the distance is an integer. So far, we have that $\sqrt{D} = \sqrt{(v - w)^2 + (v^2 - w^2)^2} = (v - w)\sqrt{1 + (v + w)^2}$ is an integer. Therefore, $\sqrt{1 + (v + w)^2}$ must be a perfect square. So, $1 + (w + v)^2 = d^2$ for some $d \in \mathbb{Z}^+ \implies w + v = 0$; but, $1 \leq w < v \leq n \implies w + v > 2$. This is a contradiction. We conclude that there are no two points in the set (i, i^2), $(i \in \mathbb{Z}^+)$ with rational distance.

In summary, we conclude that the distance between any two points in the set of n points $(1, 1), (2, 4), (3,), ..., (n, n^2)$ is irrational and each subset of three points in $(1, 1), (2, 4), (3,), ..., (n, n^2)$ determines a non-degenerate triangle with rational area. $\square$

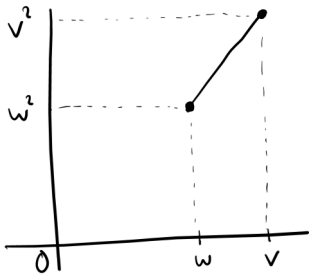


Figure 50: Lattice points (w, w^2), (v, v^2) with distance $\sqrt{(v - w)^2 + (v^2 - w^2)^2}$.

5.1 Farey Sequences

Next, we will consider an interesting application of Pick's Theorem to Farey sequences!

Definition 22 Farey Sequence. The **Farey sequence of order** n, denoted F_n is the sequence of completely reduced fractions between 0 and 1 which, in lowest terms, have denominators less than or equal to n, arranged in order of increasing size.

The first five Farey sequences are shown below.

$$\begin{aligned} F_1 &= \{0/1, 1/1\} \\ F_2 &= \{0/1, 1/2, 1/1\} \\ F_3 &= \{0/1, 1/3, 1/2, 2/3, 1/1\} \\ F_4 &= \{0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1\} \\ F_5 &= \{0/1, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 1/1\} \end{aligned}$$

Exercise 83 Find F_6 and F_7.

Solution
$F_6 = \{0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1\}$.
□
$F_7 = \{0/1, 1/7, 1/6, 1/5, 1/4, 2/7, 1/3, 2/5, 3/7, 1/2, 4/7, 3/5, 2/3, 5/7, 3/4, 4/5, 5/6, 6/7, 1/1\}$.
□

Exercise 84 Properties of Farey Sequences. Prove each of the following statements.

(a) F_n contains F_k for all $k \leq n$.

(b) Let $|F_n|$ denote the number of fractions in F_n. For $n > 1$, $|F_n|$ is odd.

Solution

(a) Consider the Farey Sequence F_n for some $n \geq 1$ and all Farey sequences F_k for $1 \leq k \leq n$. Trivially, F_n contains (is) $F_{k=n}$. Consider next the Farey sequences F_k, $1 \leq k < n$. Say $\frac{a}{b},\ a,\ b \in \mathbb{Z}^+,\ a \leq b$ belong to an F_k sequence, $1 \leq k < n$. Then, $b \leq k < n$, $\frac{a}{b} \in [0, 1]$ and $\frac{a}{b}$ is fully reduced since $\frac{a}{b} \in F_k$. By definition, $\frac{a}{b} \in F_n$. We proved that $\bigcup_{k=1}^{n} F_k \subseteq F_n$. By the way also, $F_n \subseteq \bigcup_{k=1}^{n} F_k$, so $F_n = \bigcup_{k=1}^{n} F_k$. □

(b) Consider an arbitrary Farey sequence $F_n,\ n > 1$. Then, $\frac{0}{1} \in F_n$ and $\frac{1}{1} \in F_n$ ($\frac{0}{1} \in F_1,\ \frac{1}{1} \in F_1$ and $F_1 \subseteq F_n$ by part (a)). Say $\frac{a}{b}$ is an arbitrary element of F_n other than $\frac{0}{1},\ \frac{1}{1}$ above. Then, $a < b < n$ and $gcd(a, b) = 1$ (meaning irreducible). If $\frac{a}{b} \in F_n$, then $1 - \frac{a}{b} = \frac{b-a}{b} \in F_n$ because $b < n$, $\frac{b-a}{b} \in (0, 1)$, and $gcd(b - a, b) = 1$.

Note: $gcd(a, b) = gcd(-a, b) = gcd(-a + b, b) = 1$ and $\frac{b-a}{b} \neq \frac{a}{b}$ if $a \neq b - a$ or $2a \neq b$ or $\frac{a}{b} \neq \frac{1}{2}$.

We conclude that all elements of F_n come in pairs $(\frac{0}{1}, \frac{1}{1})$, $(\frac{a}{b}, \frac{b-a}{a})$, except for $\frac{1}{2}$ which is in F_n for every $n \geq 2$. Therefore, $|F_n|$ is odd for $n \geq 2$. □

Definition 23 Euler's phi function or Euler's totient function. Let $\phi(n)$ denote the number of positive integers less than or equal to n that are relatively prime to n, i.e. the number of integers d such that

$$1 \leq d \leq n \text{ and } \gcd(d, n) = 1.$$

For example,

$$\phi(9) = 6$$

because the six integers 1, 2, 4, 5, 7, 8 are relatively prime to 9, but 3, 6, and 9 are not. As another example,

$$\phi(10) = 4$$

because the four integers 1, 3, 7, 9 are relatively prime to 10, but 2, 4, 5, 6, 8, 10 are not.

Exercise 85 Show that $|F_n| = |F_{n-1}| + \phi(n)$.

Solution By Exercise 84(a), F_n contains F_{n-1}. Therefore, $|F_n|$ equals $|F_{n-1}|$ plus the total number of ratios $\frac{d}{n}$ such that $1 \leq d \leq n$ and $gcd(d,n) = 1$. By definition, this number is Euler's phi function. We conclude $|F_n| = |F_{n-1}| + \phi(n)$. □

Recursively speaking, the size of any Farey F_n is the size of the previous Farey sequence F_{n-1} plus some number of new fractions with denominator n, call them $\frac{a}{n}$. $\frac{a}{n}$ will be added if and only if $gcd(a,n) = 1$, meaning that it is irreducible and therefore not already in the sequence. By definition, there are $\phi(n)$ integers a, $1 \leq a \leq n$ such that $gcd(a,n) = 1$.

Exercise 86 The Mediant Property. Unfortunately, addition of fractions is not as easy as we would like it to be. For example,

$$\frac{1}{5} + \frac{1}{3} \neq \frac{1+1}{5+3} = \frac{1}{4}.$$

(a) Looking at the Farey sequences F_4 and F_5, how does 1/4 relate to 1/5 and 1/3?

(b) Can you find other Farey sequences in which you observe this phenomena? In particular, choose a Farey sequence F_n and choose 3 consecutive terms of F_n, say $p_1/q_1, p_2/q_2, p_3/q_3$. Compute

$$\frac{p_1 + p_3}{q_1 + q_3}.$$

What do you observe?

Solution

(a) In Farey F_5, $\frac{1}{5}$, $\frac{1}{4}$, $\frac{1}{3}$ are consecutive fractions in this order. I observe that $\frac{1+1}{5+3} = \frac{1}{4}$.

(b) Consider Farey F_3. $\frac{1}{3}$, $\frac{1}{2}$, $\frac{2}{3}$ are consecutive fractions in this order and $\frac{1+2}{3+3} = \frac{1}{2}$.
For 3 consecutive terms $p_1/q_1, p_2/q_2, p_3/q_3$ in some F_n, I conjecture that $\frac{p_1+p_3}{q_1+q_3} = \frac{p_2}{q_2}$. □

Exercise 87 (a) The fractions $\frac{2}{5}$ and $\frac{3}{7}$ are adjacent terms of the Farey sequence F_7. Compute $5 \cdot 3 - 2 \cdot 7$.

(b) Choose two other adjacent terms $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ of F_7 and compute $p_2q_1 - p_1q_2$.

(c) Choose two adjacent terms $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ of F_5 and compute $p_2q_1 - p_1q_2$.

(d) Suppose that $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ are two successive terms of a Farey sequence F_n. Make a conjecture about the value of $p_2q_1 - p_1q_2$. We will use Pick's Theorem to prove this conjecture!

Solution

(a) $5 \cdot 3 - 2 \cdot 7 = 15 - 14 = 1$.

(b) $\frac{1}{6}$, $\frac{1}{5}$ are adjacent in F_7; $1 \cdot 6 - 1 \cdot 5 = 1$.

(c) $\frac{1}{3}$, $\frac{2}{5}$ are adjacent in F_5; $2 \cdot 3 - 1 \cdot 5 = 1$.

(d) For $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$ being successive terms in some F_n, I conjecture that $p_2q_1 - p_1q_2 = 1$. □

Exercise 88 Suppose that p_1/q_1 and p_2/q_2 are two successive terms of F_n. In this problem, we will use Pick's Theorem to prove that $p_2q_1 - p_1q_2 = 1$. Let T be the triangle with vertices $(0,0)$, (p_1,q_1), and (p_2,q_2).

(a) Show that T has no lattice points in its interior, i.e. $I(T) = 0$.

(b) Show that the only boundary points of T are the vertices of the triangle, i.e. $B(T) = 3$.

(c) Conclude, using Pick's Theorem, that

$$A(T) = \frac{1}{2}.$$

(d) Use geometry to show that

$$A(T) = \frac{1}{2}\left(p_2 q_1 - p_1 q_2\right).$$

(e) Conclude that

$$p_2 q_1 - p_1 q_2 = 1.$$

Solution

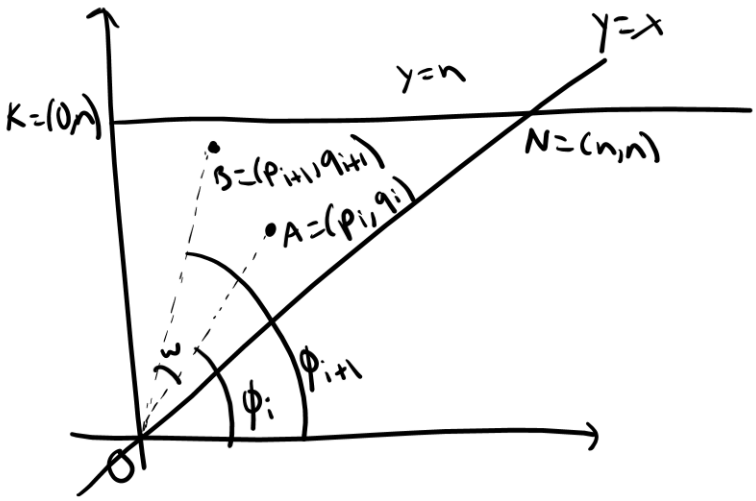


Figure 51: Triangle OAB.

(a) All visible lattice points in triangle OKN pictured above are elements of F_n, say $\frac{p_i}{q_i}$. Define $\phi_i = cot^{-1}\frac{p_i}{q_i}$. The elements in F_n are ordered in increasing value of ϕ_i, $\phi_i \in [45°,\ 90°]$. Take two successive elements $\frac{p_i}{q_i} < \frac{p_{i+1}}{q_{i+1}}$ in F_n. Because $\frac{p_i}{q_i}$ and $\frac{p_{i+1}}{q_{i+1}}$ are successive there is no visible point within $\omega = \phi_{i+1} - \phi_i$. Therefore there is no visible point within the angle ω and below the $y = n$ horizontal. We conclude that OAB has no lattice points in its interior.

(b) Similarly, because A and B have $gcd = 1$, they are visible. By part (a), because there is no visible point within the angle ω and below the $y = n$ horizontal there are no lattice points on AB. We conclude that $A,\ B$ are the only points together with O that are lattice points on the boundary of T. That is, $B(T) = 3$.

(c) By Pick's Theorem, $A(T) = I(T) + \frac{1}{2}B(T) - 1 = 0 + \frac{1}{2}\cdot 3 - 1 = \frac{1}{2}$.

(d) Consider without loss of generality the triangle below with vertices $O = (0,0)$, $A = (p_1, q_1)$, and $B = (p_2, q_2)$.

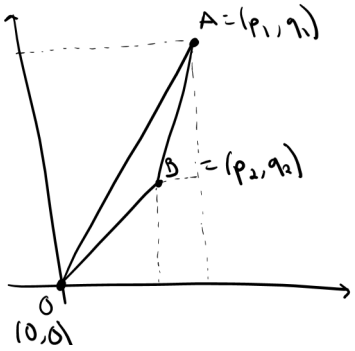


Figure 52: Triangle OAB.

The area of this triangle is $A = p_1q_1 - \frac{1}{2}p_1q_1 - (p_1 - p_2)q_2 - \frac{1}{2}p_2q_2 - \frac{1}{2}(p_1 - p_2)(q_1 - q_2) = \frac{1}{2}p_2q_1 - \frac{1}{2}p_1q_2 = \frac{1}{2}(p_2q_1 - q_2p_1)$.

(e) Since $\frac{1}{2}(p_2q_1 - q_2p_1) = A(T) = \frac{1}{2}$, we conclude that $(p_2q_1 - q_2p_1) = 1$.

Finally, we will think about how to use the mediant property to develop an algorithm for computing F_n. In particular, we wish to answer the following question: How do we go from the $(n-1)$-st Farey sequence to the n-th Farey sequence?

Exercise 89 Prove that if $0 < \dfrac{a}{b} < \dfrac{c}{d} < 1$, then

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}.$$

Solution For the sake of generality, I will prove this for $a,\ b,\ c,\ d \in \mathbb{R}^+$ (not only $a, b, c, d \in \mathbb{N}^+$). It is given that $\frac{a}{b} < \frac{c}{d} \implies a < \frac{bc}{d} \implies$

$$ad < bc. \tag{55}$$

Adding ab to both sides of (55) we obtain,

$$ad + ab < bc + ab \implies a(b+d) < b(a+c) \implies$$

$$\frac{a}{b} < \frac{a+c}{b+d}, \tag{56}$$

since $b > 0$ and $b + d > 0$. Adding cd to both sides of (55) we obtain,

$$ad + cd < bc + cd \implies d(a+c) < c(b+d) \implies$$

$$\frac{a+c}{b+d} < \frac{c}{d}, \tag{57}$$

since $d > 0$ and $b + d > 0$. Combining (56) and (57), we obtain $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$. □

Exercise 90 Prove that if a/b and c/d are adjacent in some F_n, then $\gcd(a + c, b + d) = 1$.

Solution

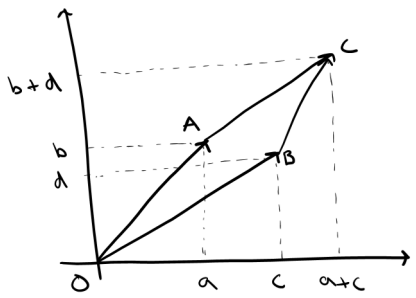


Figure 53: Primitive triangle OAB formed by consecutive terms $\frac{a}{b}$, $\frac{c}{d}$ in Farey F_n and primitive parallelogram OACB.

Consider the vectors $\vec{OA}$ and $\vec{OB}$ in Fig. 53 where $A = (a, b)$ and $B = (c, d)$. By Exercise 88 (e), $|det(\begin{bmatrix} a & c \\ b & d \end{bmatrix})| = |ad - cb| = 1$, therefore $\vec{OA}$ and $\vec{OB}$ are a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ (Exercise 51). By Exercise 53, the parallelogram $OABC$ with $C = (a + c, b + d)$ is primitive. Therefore, C is visible $\implies \gcd(a + c, b + d) = 1$. □

We thus have the following algorithm for computing F_n using F_{n-1}:

Algorithm 1 How to Compute F_n Using F_{n-1}.

1. Copy F_{n-1} in order.
2. Insert the **mediant fraction** $\dfrac{a+c}{b+d}$ between $\dfrac{a}{b}$ and $\dfrac{c}{d}$ if $b + d \leq n$. (If $b + d > n$, the mediant $\dfrac{a+c}{b+d}$ will appear in a later sequence).

Exercise 91 Use Algorithm 1 to compute F_8 using F_7.

Solution $F_7 = \{0/1, 1/7, 1/6, 1/5, 1/4, 2/7, 1/3, 2/5, 3/7, 1/2, 4/7, 3/5, 2/3, 5/7, 3/4, 4/5, 5/6, 6/7, 1/1\}$.
By executing step 2 of the algorithm, we see that four mediant fractions will need to be computed and inserted into F_7 to create F_8: The mediant fraction between $\frac{0}{1}$ and $\frac{1}{7}$ equals $\frac{1}{8}$; the mediant fraction between $\frac{1}{3}$ and $\frac{2}{5}$ equals $\frac{3}{8}$; the mediant fraction between $\frac{3}{5}$ and $\frac{2}{3}$ equals $\frac{5}{8}$; the mediant fraction between $\frac{6}{7}$ and $\frac{1}{1}$ equals $\frac{7}{8}$. Therefore, $F_7 = \{0/1, 1/8, 1/7, 1/6, 1/5, 1/4, 2/7, 1/3, 3/8, 2/5, 3/7, 1/2, 4/7, 3/5, 5/8, 2/3, 5/7, 3/4, 4/5, 5/6, 6/7, 7/8, 1/1\}$.
□

Exercise 92 Without listing out all of the fractions in F_{100}, find the fraction $\dfrac{a}{b}$ immediately before and the fraction $\dfrac{c}{d}$ immediately after $\dfrac{61}{79}$ in F_{100}.

Solution Since $\frac{61}{79}$ is between terms $\frac{a}{b}$ and $\frac{c}{d}$ in F_{100} and by Exercise 90 we know that $gcd(a + c, b + d) = 1$, $\frac{61}{79} = \frac{a+c}{b+d} \implies a + c = 61,\ b + d = 79$. From Exercise 88 we know that $p_2q_1 - p_1q_2 = 1$ for adjacent terms $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$. So, for the two pairs of adjacent terms $(\frac{a}{b}, \frac{61}{79})$ and $(\frac{61}{79}, \frac{c}{d})$,

$$61b - 79a = 1 \tag{58}$$

$$79c - 61d = 1. \tag{59}$$

There is no clear solution for this set of equations. We can convert the equations, however, into congruences with modulus 61 to find possibilities for the integers a, b, c, d.

$$-18a \equiv 1 \text{mod } 61$$

$$18c \equiv 1 \text{mod } 61$$

$$18c - 18a \equiv 2 \text{mod } 61$$

$$18(c-a) \equiv 2 \equiv 61 \cdot 10 + 2 \equiv 612 \text{mod } 61$$

$$c - a \equiv 34 \text{mod } 61$$

$$c - a = 34 + 61t, \ t \in \mathbb{Z}.$$

We know that $a+c = 61$ and that a and c are positive, thus $c < 61$. Without loss of generality, $2c = 61+34+61t = 34 + 61t$. It is evident that t must equal 0, implying then that $c = 17$. As a result, $a = 44$. By (58) and (59), $b = 57$ and $d = 22$. Therefore, the three consecutive terms in Farey $F_1 00$ are $\frac{44}{57}, \ \frac{61}{79}, \ \frac{17}{22}$. $\square$

The next series of exercises illustrates how terms of Farey sequences can be used to provide rational approximations for real numbers.

Exercise 93 Show that if a/b and c/d are consecutive terms of F_n, then $b + d > n$.

Solution I will prove this by contradiction. Suppose that $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive fraction in F_n. By Exercise 89, $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$. By Exercise 90, $gcd(a + c, b + d) = 1$, so $\frac{a+c}{b+d}$ is in lowest terms. Thus, if $b + d \leq n$, then $\frac{a+c}{b+d} \in F_n$ and is in between $\frac{a}{c}$ and $\frac{c}{d}$. But, $\frac{a}{b}, \ \frac{c}{d}$ are consecutive, so this is a contradiction. Therefore, $b + d > n$. $\square$

Exercise 94 Show that if a/b and c/d are consecutive terms of F_n and if $n > 1$, then $b + d < 2n$.

Solution Let $n > 1$ and $\frac{a}{b}, \ \frac{c}{d}$ be consecutive fractions of F_n. It is enough to show that $b \neq d$ because $b, d \leq n$ (by definition of F_n). We know that $bc - ad = 1$ by Exercise 88. If $b = d$, then $bc - ad = 1 \implies bc - ab = 1 \implies b(c - a) = 1 \implies b = 1, \ d = 1, \ c - a = 1$. Thus, $\frac{a}{b}, \ \frac{c}{d}$ are $\frac{a}{1}, \ \frac{c}{1}$. Then, $c = 1$ and $a = 0$. The fractions are thus $\frac{0}{1}, \ \frac{1}{1}$, but they are not consecutive for $n > 1$. Thus, $b \neq d$. So, $b + d < 2n$ $(b, d \leq n)$. $\square$

Exercise 95 Dirichlet's Theorem on Rational Approximations The terms of the Farey sequence F_n partition the interval $[0, 1]$ into subintervals of length at most $1/n$. If α is any real number in $[0, 1]$, then there are consecutive terms a/b and c/d of F_n such that

$$\alpha \in [\frac{a}{b}, \frac{c}{d}].$$

Show that if α is a real number in $[0, 1]$ and if n is a positive integer, then there is a rational number h/k in F_n such that

$$\left| \alpha - \frac{h}{k} \right| \leq \frac{1}{k(n+1)}.$$

This exercise demonstrates that one of a/b or c/d provides a good **rational** approximation to the real number α.

Solution Let n be a positive integer and $0 \leq \alpha \leq 1$. There exist two consecutive fractions, $\frac{h}{k}$ and $\frac{h'}{k'}$ in F_n such that $\alpha \in [\frac{h}{k}, \frac{h'}{k'}]$. By Exercise 88, $h'k - hk' = 1$. Now, we consider two cases:

Case 1: $\alpha \leq \frac{h+h'}{k+k'}$.
Then, $\alpha - \frac{h}{k} \leq \frac{h+h'}{k+k'} - \frac{h}{k} = \frac{(h+h')k - h(k+k')}{k(k+k')} = \frac{hk+h'k-hk-hk'}{k(k+k')} = \frac{h'k-hk'}{k(k+k')} \implies$
$\alpha - \frac{h}{k} \leq \frac{1}{k(k+k')} \leq \frac{1}{k(n+1)}$ since $k + k' \geq n + 1$.

So, Case 1 gives $\frac{h}{k}$ (the lesser fraction) as the desired approximation for α since α is less that or equal to the mediant fraction.

Case 2: $\alpha > \frac{h+h'}{k+k'}$.
Then, $\frac{h'}{k'} - \alpha < \frac{h'}{k'} - \frac{h+h'}{k+k'} \implies$
$\frac{h'}{k'} - \alpha < \frac{1}{k'(k+k')} < \frac{1}{k'(n+1)}$ since $k + k' \geq n + 1$.
So, Case 2 gives $\frac{h'}{k'}$ (the greater fraction) as the desired approximation for α since α is greater that or equal to the mediant fraction.

So, either $\frac{h}{k}$ or $\frac{h'}{k'}$ approximates α as required. □

Exercise 96 Illustrate Exercise 95 for $\alpha = \dfrac{\sqrt{2}}{2}$ and $n = 10$.

Solution There exist consecutive $\frac{h}{k}$ and $\frac{h'}{k'} \in F_{10}$ such that $\alpha = \frac{\sqrt{2}}{2} \in [\frac{h}{k}, \frac{h'}{k'}]$.
For reference, $F_{10} = \{0/1, 1/10, 1/9, 1/8, 1/7, 1/6, 1/5, 2/9, 1/4, 2/7, 3/10, 1/3, 3/8, 2/5, 3/7, 4/9, 1/2, 5/9, 4/7, 3/5, 5/8, 2/3, 7/10, 5/7, 3/4, 7/9, 4/5, 5/6, 6/7, 7/8, 8/9, 9/10, 1/1\}$.
$\alpha = \frac{\sqrt{2}}{2}$ falls between the consecutive fractions of F_{10}, $\frac{7}{10}$ and $\frac{5}{7}$. So, let $\frac{h}{k} = \frac{7}{10}$ and $\frac{h'}{k'} = \frac{5}{7}$. We have to test and see which case this example falls in. The mediant fraction $\frac{h+h'}{k+k'} = \frac{7+5}{10+7} = \frac{12}{17}$ is less than $\frac{\sqrt{2}}{2}$ so we fall in Case 2 from Exercise 95. Therefore, $\frac{h'}{k'} = \frac{5}{7}$ is the desired approximation for $\frac{\sqrt{2}}{2}$. □

Check with Dirichlet's Theorem: $|\alpha - \frac{h'}{k'}| \leq \frac{1}{k(n+1)} \implies |\frac{\sqrt{2}}{2} - \frac{5}{7}| \leq \frac{1}{7(10+1)} \implies |\frac{7\sqrt{2}-10}{14}| \leq \frac{1}{77}$ which hold true.

5.2 Ford Circles

Definition 24 Ford Circle. For every rational number p/q in lowest terms, the **Ford circle** $C(p, q)$ is the circle with center $(\dfrac{p}{q}, \dfrac{1}{2q^2})$ and radius $\dfrac{1}{2q^2}$. This means that $C(p, q)$ is the circle tangent to the x-axis at $x = p/q$ with radius $\dfrac{1}{2q^2}$. Observe that every small interval of the x-axis contains points of tangency of infinitely many Ford circles. Several examples are shown below.

Exercise 97 Graph $C(3, 4)$ and $C(4, 5)$ clearly on the same set of axes. I recommend that you use a graphing software package to do this. What do you observe about these two circles?

Solution C(3,4): $(x - \frac{3}{4})^2 + (y - \frac{1}{2\cdot 4^2})^2 = (\frac{1}{2\cdot 4^2})^2$; C(4,5): $(x - \frac{4}{5})^2 + (y - \frac{1}{2\cdot 5^2})^2 = (\frac{1}{2\cdot 5^2})^2$.

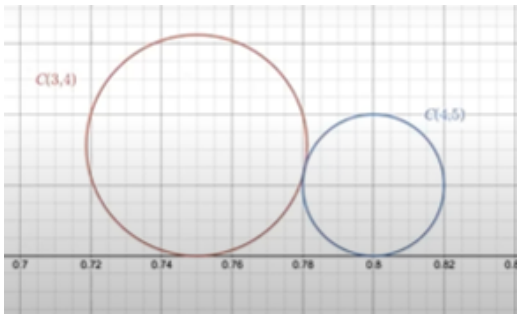
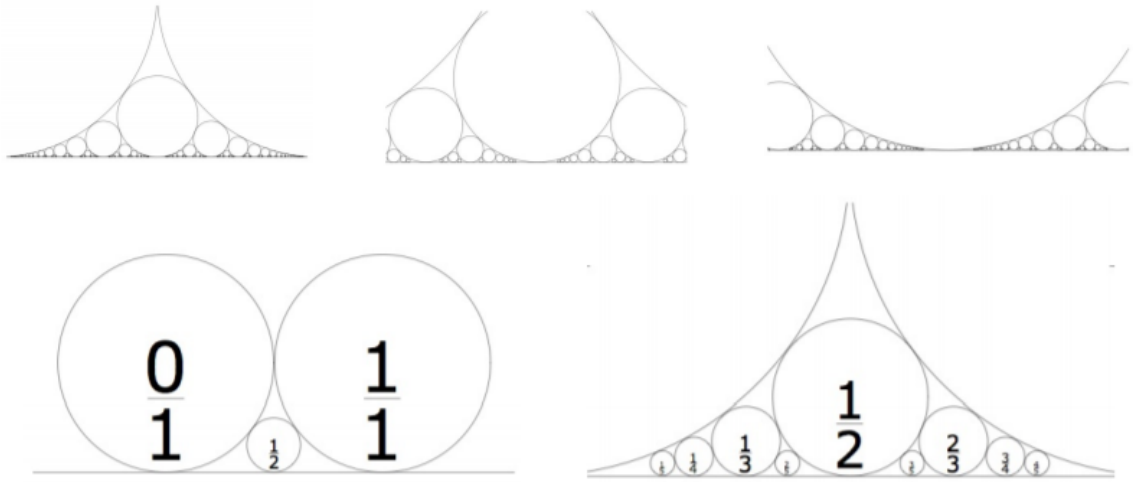


Figure 54: Ford circles C(3,4) and C(4,5).

I observe visually that these two circles are tangent at one point. □



There is an interesting and beautiful connection between Farey sequences and Ford circles, which we will explore in the next set of exercises. There is also a nice connection between group actions of $SL_2(\mathbb{Z})$ to properties of Ford circles and Farey sequences, which I encourage you to explore in more detail if you have had some advanced abstract algebra.

Exercise 98 Choose two fractions a/b and c/d that are adjacent in F_6, and clearly graph $C(a,b)$ and $C(c,d)$ on the same set of axes. I recommend that you use a graphing software package to do this. What do you observe about the two circles?

Solution For reference, $F_6 = \{0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1\}$.
I consider the adjacent fractions $\frac{3}{5}$, $\frac{2}{3}$ and graph C(3,5) and C(2,3). Again, these circles (from consecutive fractions) are tangent at one point.
C(3,5): $(x-\frac{3}{5})^2 + (y-\frac{1}{2\cdot 5^2})^2 = (\frac{1}{2\cdot 5^2})^2$.
C(2,3): $(x-\frac{2}{3})^2 + (y-\frac{1}{2\cdot 3^2})^2 = (\frac{1}{2\cdot 3^2})^2$. □

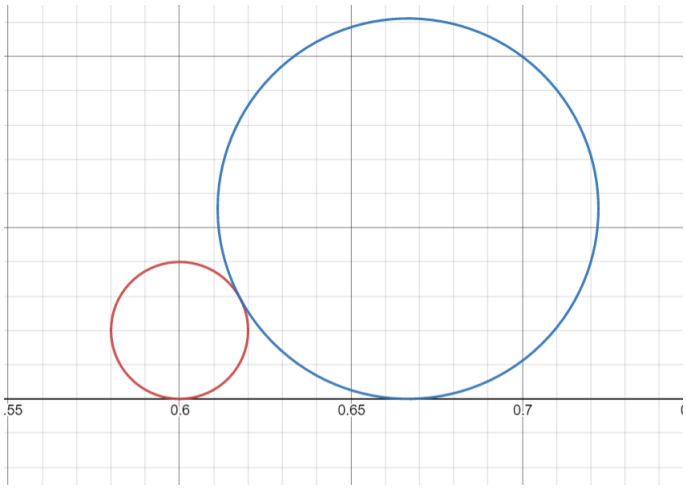


Figure 55: Ford circles C(3,5) and C(2,3).

Exercise 99 Next, choose two fractions a/b and c/d that are *not* adjacent in F_6, and clearly graph $C(a,b)$ and $C(c,d)$ on the same set of axes. I recommend that you use a graphing software package to do this. What do you observe about the two circles?

Solution For reference, $F_6 = \{0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1\}$.
I consider the non-adjacent fractions $\frac{3}{5}$ and $\frac{5}{6}$ and graph C(3,5) and C(5,6):
C(3,5): $(x-\frac{3}{5})^2 + (y-\frac{1}{2\cdot 5^2})^2 = (\frac{1}{2\cdot 5^2})^2$,
C(5,6): $(x-\frac{5}{6})^2 + (y-\frac{1}{2\cdot 6^2})^2 = (\frac{1}{2\cdot 6^2})^2$.

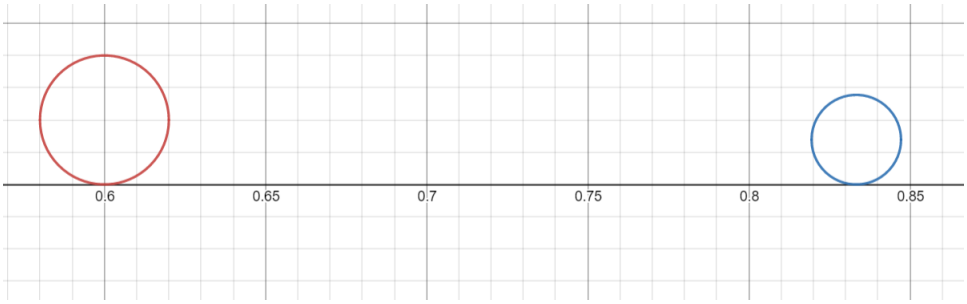


Figure 56: Ford circles C(3,5) and C(5,6).

I observe that that these Ford circles from non-consecutive Farey fractions do not intersect at all. □

Exercise 100 Repeat Exercises 98 and 99 for several additional pairs of fractions in F_6, keeping track of what you observe about the circles in the cases where the fractions are adjacent and are not adjacent.

Solution For reference, $F_6 = \{0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1\}$.
Consider the Ford circles C(1,6) and C(1,5) created from consecutive Farey fractions.
C(1,6): $(x-\frac{1}{6})^2 + (y-\frac{1}{2\cdot 6^2})^2 = (\frac{1}{2\cdot 6^2})^2$,
C(1,5): $(x-\frac{1}{5})^2 + (y-\frac{1}{2\cdot 5^2})^2 = (\frac{1}{2\cdot 5^2})^2$.

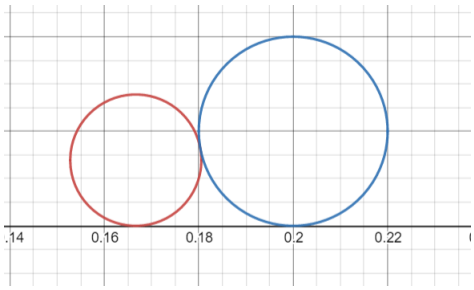


Figure 57: Ford circles C(1,6) and C(1,5).

Consider the Ford circles C(1,6) and C(1,3) created from non-consecutive Farey fractions.
C(1,6): $(x-\frac{1}{6})^2 + (y-\frac{1}{2\cdot 6^2})^2 = (\frac{1}{2\cdot 6^2})^2$
C(1,3): $(x-\frac{1}{3})^2 + (y-\frac{1}{2\cdot 3^2})^2 = (\frac{1}{2\cdot 3^2})^2$

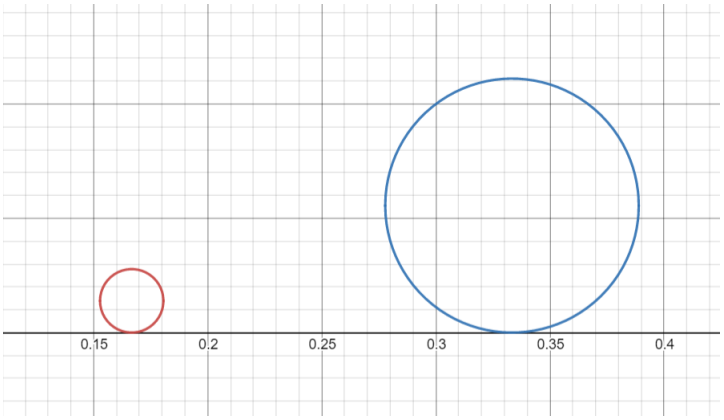


Figure 58: Ford circles C(1,6) and C(1,3).

The Ford circles created from consecutive Farey fractions are tangent at one point and the Ford circles created from non-consecutive Farey fractions do not intersect at all.

Exercise 101 Prove that the representative Ford circles of two distinct fractions are either tangent at one point or wholly external.

Solution Consider two distinct circles in a plane. These circles may have (1) one circle completely inside the other, (2) they can be internally tangent, (3) partially intersecting, (4) externally tangent, or (5) wholly external. We must prove that if two circles are representative Ford circles they are either externally tangent or wholly external (that is, they fall in either Case 4 or 5).

Consider the line segment joining the centers of the two Ford circles. In Cases 4 and 5, the length of this segment is greater than or equal to the sum of the radii of the circles. In Cases 1, 2, and 3 however, the length of this segment is less than the sum of the radii of the circles. Therefore, it suffices to prove that the length of the segment connecting the centers of two Ford circles is greater than or equal to the sum of the radii. Then, the two circles are either tangent at one point or wholly external.

Consider two Ford circles $C(p,q)$ and $C(r,s)$ with centers at $(\frac{p}{q}, \frac{1}{2q^2})$ and $(\frac{r}{s}, \frac{1}{2s^2})$, respectively. Then, the radius of $C(p,q)$ is $r_1 = \frac{1}{2q^2}$ and the radius of $C(r,s)$ is $r_2 = \frac{1}{2s^2}$. Then, the distance between their centers is $D = \sqrt{(\frac{p}{q} - \frac{r}{s})^2 + (\frac{1}{2q^2} - \frac{1}{2s^2})^2} \implies D^2 = (\frac{ps-qr}{qs})^2 + (\frac{1}{2q^2} - \frac{1}{2s^2})^2 = \frac{1}{4q^2} + \frac{2(ps-qr)^2-1}{2q^2s^2} + \frac{1}{4s^4}$. Note that $(ps-qr)^2 \geq 0$ and $ps-qr$ is integer. If $(ps-qr)^2 = 0 \implies \frac{p}{q} = \frac{r}{s}$ which is not possible since the circles are distinct. So, $(ps-qr)^2 \geq 1$. Then, $D^2 \geq \frac{1}{4q^2} + \frac{2\cdot 1-1}{2q^2s^2} + \frac{1}{4s^4} = (\frac{1}{2q^2} + \frac{1}{2s^2})^2 \implies D \geq (\frac{1}{2q^2} + \frac{1}{2s^2})$. Therefore, we conclude that the distance between the centers of the two circles is greater than or equal to the sum of the radii of the circles. Hence, any two Ford circles are either tangent at one point or wholly external. □

Exercise 102 Show that the representative Ford circles of two distinct fractions are tangent at one point precisely when the fractions are adjacent in some Farey sequence F_n.

Solution First, I will show that if the fractions are adjacent in some Farey F_n, then the Ford circles are tangent at one point. As seen in Exercise 101, the square distance between the centers of two Ford circles is $D^2 = \frac{1}{4q^2} + \frac{2(ps-qr)^2-1}{2q^2s^2} + \frac{1}{4s^4}$. By Exercise 88, for adjacent fractions $ps-qr = 1$. Therefore, $D^2 = \frac{1}{4q^2} + \frac{2(ps-qr)^2-1}{2q^2s^2} + \frac{1}{4s^4} \implies D = \frac{1}{2q^2} + \frac{1}{2s^2} \implies$ the Ford circles are tangent at one point.

Next, I will show that if the Ford circles are tangent at one external point, the fractions are adjacent in some Farey sequence F_n. I will prove this by contradiction. Assume that $C(p,q)$ and $C(r,s)$ are Ford circles tangent at one external point and without loss of generality $\frac{p}{q} < \frac{r}{s}$. Since the circles are tangent at one external point, $qr-ps = 1$ by Exercise 101. Assume that there exists a lowest-terms fraction $\frac{l}{m}$ such that $\frac{p}{q} < \frac{l}{m} < \frac{r}{s}$ and $\frac{p}{q}$, $\frac{l}{m}$

are consecutive franction in a Farey F_n. By Bezout's identity, if $gcd(a,b) = 1$, then integer solutions (x, y) to the equation $ax + by = 1$ are of the form $(x_0 - kb, y_0 + ka)$ where k is an integer and (x_0, y_0) is a particular solution to the equation. Here, we have $qr - ps = 1$ and $\frac{p}{q}$ and $\frac{l}{m}$ are consecutive terms in some F_n. By Exercise 88, we have $ql - pm = 1$ and since $gcd(p, q) = 1$, Bezout's identity is applicable. Using $(a, b) = (p, q)$ and $(x_0, y_0) = (-s, r)$, we obtain $(-m, l) = (-s - kq, r + kp)$. Therefore, $l = kp + r$ and $m = kq + s$ for some integer k. Using the condition that $\frac{l}{m} < \frac{r}{s}$, $ls < rm \implies kps + rs < kqr + rs \implies kps < kqr \implies 0 < k(qr - ps) \implies 0 < k$. We know also that since $\frac{l}{m}$ is between $\frac{p}{q}$ and $\frac{r}{s}$ in some F_n, m must be less than or equal to $max(q, s)$. We construct two cases:

Case 1, $s < q$: $m \leq q \implies kq + s \leq q \implies kq \leq q - s \implies k \leq \frac{q-s}{q} < 1 \implies k \leq 0$. Contradiction.

Case 2, $q \leq s$: $m \leq s \implies kq + s \leq s \implies kq \leq 0 \implies k \leq 0$. Contradiction.

Therefore, if two Ford circles are tangent at one external point, their fractions are adjacent in some Farey sequence F_n. □

Exercise 103 Suppose that $C(a, b)$ and $C(c, d)$ are tangent Ford circles. Prove that $C(a + c, b + d)$ is the unique circle tangent to the real line and to both of the circles $C(a, b)$ and $C(c, d)$, i.e. $C(a+c, b+d)$, the circle associated with the mediant fraction, is the largest circle between $C(a, b)$ and $C(c, d)$.

Solution Since $C(a, b)$, $C(c, d)$ are tangent Ford circles, by Exercise 102 $\frac{a}{b}$ and $\frac{c}{d}$ are adjacent terms in some Farey F_n.

By Exercises 89 and 90 (see also Algorithm 1), $\frac{a+c}{b+d}$ is the unique reduced ratio for which $\frac{a}{b}$, $\frac{a+c}{b+d}$, $\frac{c}{d}$ are successive terms in some Farey F_k, $k > n$.

Therefore, $C(a + c, b + d)$ is the unique Ford circle tangent to Ford circles $C(a, b)$ and $C(c, d)$ and - of course - to the real line as a Ford circle. □

6 Lattice Points In and On a Circle

Exercise 104 Prove that no two lattice points are the same distance from the point $(\sqrt{2}, 1/3)$.

Solution I will prove this by contradiction. Assume that (x, y) and (a, b) are distinct lattice points equidistant from $(\sqrt{2}, \frac{1}{3})$. By the Distance Formula, $(x-\sqrt{2})^2+(y-\frac{1}{3})^2 = (a-\sqrt{2})^2+(b-\frac{1}{3})^2 \implies x^2-2\sqrt{2}x+2+y^2-\frac{2}{3}y+\frac{1}{9} = a^2-2\sqrt{2}a+2+b^2-\frac{2}{3}b+\frac{1}{9} \implies x^2+y^2-a^2-b^2-\frac{2}{3}y+\frac{2}{3}b = 2\sqrt{2}x-2\sqrt{2}a = (x-a)2\sqrt{2}$. It is clear that $x^2+y^2-a^2-b^2-\frac{2}{3}y+\frac{2}{3}b$ is rational since $x, y, a, b \in \mathbb{Z}$, so any solution for (x, y, a, b) must make $(x-a)2\sqrt{2}$ a rational quantity. This is possible only when $x = a$ (because any integer multiple of $2\sqrt{2}$ beside 0 leads to an irrational quantity). Going back now to the original equation with $x = a$, $y^2-b^2 = \frac{2}{3}y-\frac{2}{3}b \implies (y-b)(y+b) = \frac{2}{3}(y-b) \implies y+b = \frac{2}{3}$ because $y-b \neq$ ($x = a$ and $(x, y), (a, b)$ are distinct). Since y, b are integers, this equation has no solutions and we have reached a contradiction. Therefore, each lattice point has a unique distance from $(\sqrt{2}, \frac{1}{3})$. □

Exercise 105 Prove that for every natural number n, there exists in the plane a circle with exactly n lattice points in its interior. Hint: order the lattice points according to their distance from the point $(\sqrt{2}, 1/3)$.

Solution

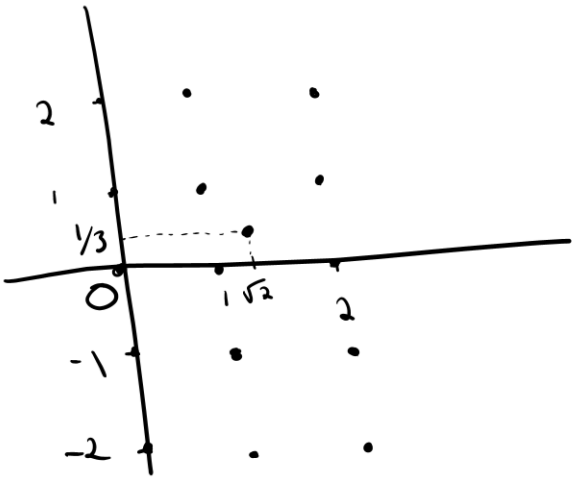


Figure 59: Lattice grid and point $(\sqrt{2}, \frac{1}{3})$.

Consider all lattice point (k, l) where $k, l \in \mathbb{Z}$. By Exercise 104, each lattice point (a, b) has distinct distance from point $(\sqrt{2}, \frac{1}{3})$,

$$D_{(a,b)} = (a-\sqrt{2})^2 + (b-\frac{1}{3})^2, \quad a, b \in \mathbb{Z}. \tag{60}$$

By inspection, $D_{(a,b)}$ becomes minimum over $a, b \in \mathbb{Z}$ for $a = 1,\ b = 0$, i.e. $(1, 0)$ is the lattice point closest to $(\sqrt{2}, 1/3)$:

$$D_{(1,0)} = (1-\sqrt{2})^2 + \frac{1}{9} = 1+2-2\sqrt{2}+\frac{1}{9} = \frac{28}{9}-2\sqrt{2}. \tag{61}$$

Consider the circle with center $(\sqrt{2}, \frac{1}{3})$ and radius $0 < r_0 \leq D_{(1,0)} \triangleq p_0$. The circle has zero lattice point in its interior. Order lattice points $p = (a, b)$ according to their distance from $(\sqrt{2}, \frac{1}{3})$, $D_{(a,b)}$ in (60): $p_0, p_1, p_2, ..., p_k$. The circle with center $(\sqrt{2}, \frac{1}{3})$ and radius p_k has exactly k lattice points in its interior, $p_0, p_1, p_2, ..., p_{k-1}$. □

Exercise 106 Show that the result of Exercise 104 holds if the point $(\sqrt{2}, 1/3)$ is replaced with any point of the form $(\sqrt{e}, 1/f)$, where e and f are positive integers with $e > 1$ and square-free and $f > 2$.

Solution I will prove this by contradiction. Suppose there are two lattice points A and B which are equidistant from the point $C = (\sqrt{e}, \frac{1}{f})$, where e, f are positive integers and $e > 1$ and square-free and $f > 2$. Consider the line segment AB which must have a rational slope. Let $y = mx + b$ be the perpendicular bisector of AB. Since $-\frac{1}{m}$ is equal to the slope of AB, m is rational. Let M be the midpoint of AB with coordinates (M_x, M_y). M_x, M_y are rational because A, B are lattice points. Further, M lies on $y = mx + b$, so $M_y = m \cdot M_x + b$. Thus, b is rational. In addition, C must lie on $y = mx + b$, so $\frac{1}{f} = m \cdot \sqrt{e} + b \implies \sqrt{e} = \frac{\frac{1}{f} - b}{m}$. Thus, $\sqrt{e}$ is also rational. This is a contradiction because it would mean that e is not square-free. Therefore, no two lattice points are equidistant from any point of the form $(\sqrt{e}, \frac{1}{f})$ where e, f are positive integers and $e > 1$. □

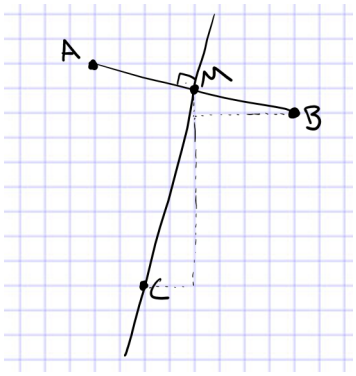


Figure 60: Line segment AB and its perpendicular bisector.

Definition 25 Let $C(\sqrt{n})$ denote the circle with center $(0, 0)$ and radius $\sqrt{n}$.

Definition 26 Let $L(n)$ be the number of lattice points in the interior and on the boundary of the circle $C(\sqrt{n})$.

Exercise 107 Find $L(5)$, $L(7)$, and $L(10)$.

Solution

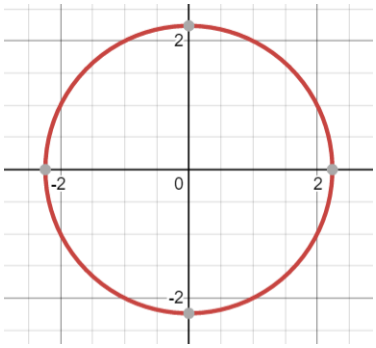


Figure 61: $C(\sqrt{5})$.

$L(5) = 21$

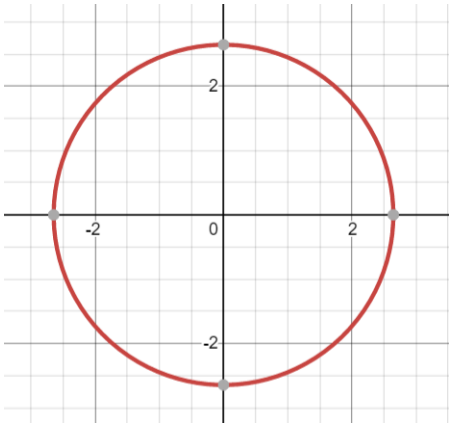


Figure 62: $C(\sqrt{7})$.

$L(7) = 21$

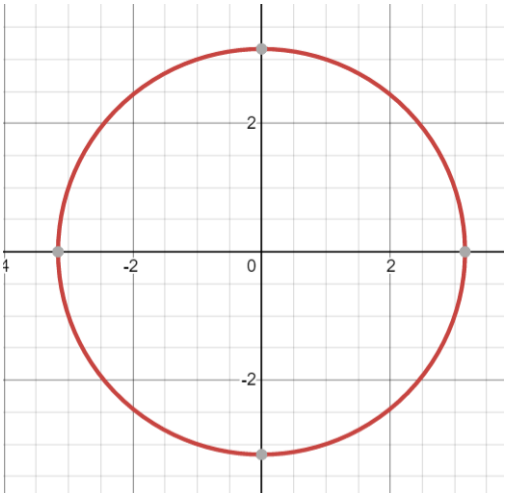
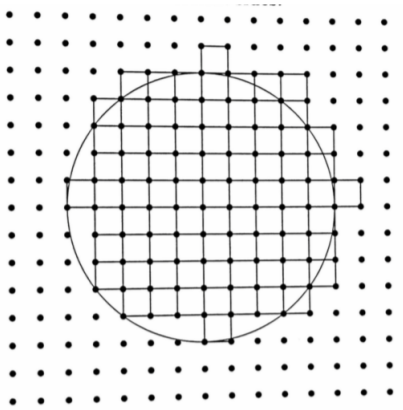


Figure 63: $C(\sqrt{10})$.

$L(10) = 37$

We may regard the lattice $\mathbb{Z}^2$ as being generated by unit squares with horizontal and vertical edges, as shown below.



Exercise 108 Let $A(n)$ denote the area of all of the unit lattice squares with horizontal and vertical sides that are cut by the boundary of the circle. Show that

$$\left|\frac{L(n)}{n} - \pi\right| \leq \frac{A(n)}{n}.$$

Solution To show that $\left|\frac{L(n)}{n} - \pi\right| \leq \frac{A(n)}{n}$, it is equivalent to show that $|L(n) - \pi n| \leq A(n)$. $L(n)$ is the number of lattice points in the interior and on the boundary of the circle $C(\sqrt{n})$. We can create a one-to-one mapping between the unit squares and the number of lattice points such that $L(n)$ can more easily be thought of as the area of the region covered by all of the unit squares with, say, lower left corner inside or on the boundary of circle $C(\sqrt{n})$. An example of this can be seen in the figure above. Since, the radius of circle $C(\sqrt{n})$ is $\sqrt{n}$, the area of the circle is $\pi\sqrt{n}^2 = \pi n$. Therefore, the small difference in area between the circle and the region of unit squares with lower left corner in or on the circle is less the the area of all of the unit lattice squares with horizontal and vertical sides that are cut by the boundary of the circle. Therefore, $\left|\frac{L(n)}{n} - \pi\right| \leq \frac{A(n)}{n}$ holds. □

Exercise 109 All of the squares that are cut by the boundary of the circle are contained in an annulus of width $2\sqrt{2}$ (since the maximum distance between any two points of a unit square is $\sqrt{2}$. Show that the area $R(n)$ of this annulus is

$$R(n) = 4\sqrt{2n}\pi.$$

Solution The area of the annulus is $R(n) = \pi(\sqrt{n}+\sqrt{2})^2 - \pi(\sqrt{n}-\sqrt{2})^2 = \pi(n+2+2\sqrt{n}\sqrt{2}) - \pi(n+2-2\sqrt{n}\sqrt{2}) = 4\sqrt{2n}\pi$. □

Exercise 110 Show that

$$\left|\frac{L(n)}{n} - \pi\right| \leq \frac{4\sqrt{2}\pi}{\sqrt{n}}.$$

Solution We know that $A(n) \leq R(n)$ since $R(n)$ is the maximum possible area that the squares cut by the circle boundary can take up. By Exercise 108 and 109, $\left|\frac{L(n)}{n} - \pi\right| \leq \frac{A(n)}{n} \implies \left|\frac{L(n)}{n} - \pi\right| \leq \frac{R(n)}{n} = \frac{4\sqrt{2n}\pi}{n} = \frac{4\sqrt{2}\pi}{\sqrt{n}}$. □

Exercise 111 Show that

$$\lim_{n\to\infty} \frac{L(n)}{n} = \pi.$$

Solution By Exercise 110, we know that $\left|\frac{L(n)}{n} - \pi\right| \leq \frac{4\sqrt{2}\pi}{\sqrt{n}} \implies -\frac{4\sqrt{2}\pi}{\sqrt{n}} \leq \frac{L(n)}{n} - \pi \leq \frac{4\sqrt{2}\pi}{\sqrt{n}}$. We know also that

$$\lim_{n\to\infty} -\frac{4\sqrt{2}\pi}{\sqrt{n}} = 0$$

and

$$\lim_{n\to\infty} \frac{4\sqrt{2}\pi}{\sqrt{n}} = 0.$$

Therefore, by the Squeezing Theorem,

$$\lim_{n\to\infty} \frac{L(n)}{n} - \pi = 0 \implies \lim_{n\to\infty} \frac{L(n)}{n} = \pi.$$

□

Gauss used this result to approximate π. The table below illustrates some of the values that Gauss found empirically for $L(n)$ and the corresponding approximations of π.

$\sqrt{n}$	$L(n)$	π
10	317	3.17
20	1257	3.1425
30	2821	3.1344
100	31417	3.1417
200	125629	3.1407
300	282697	3.1411

7 Extensions of Pick's Theorem

There are many extensions of Pick's Theorem, leading to areas of current research on open problems in mathematics (including the Riemann Hypothesis).

Exercise 112 This problem is an introduction to how Pick's Theorem generalizes in higher dimensions. First, we'll rewrite Pick's Theorem as follows. Let P be a lattice polygon, and let $L(P)$ denote the total number of lattice points in the interior and on the sides of P, so

$$L(P) = B(P) + I(P).$$

Then Pick's Theorem can be restated as follows:

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

This generalization of Pick's Theorem describes how $L(P)$ changes as the polygon undergoes dilation by a positive integer. For each positive integer n, we define the lattice polygon nP as

$$nP = \{nx \mid x \in P\}.$$

Prove that

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

Solution By Pick's Theorem, $L(nP) = A(nP) + \frac{1}{2}B(nP) + 1$. Therefore, to prove that $L(nP) = A(P)n^2 + \frac{1}{2}B(P)n + 1$, it suffices to show that $A(nP) = n^2A(P)$ and $B(nP) = nB(P)$.

Let T be a triangle with vertices $(0,0)$, (a,b), and (c,d). $A(T) = \frac{1}{2} \cdot |det(\begin{bmatrix} a & b \\ c & d \end{bmatrix})| = \frac{1}{2}|ad - bc|$. Consider $A(nT)$ now. The vertices of this triangle are by definition $(0,0)$, (na, nb), and (nc, nd). $A(nT) = \frac{1}{2} \cdot |det(\begin{bmatrix} na & nb \\ nc & nd \end{bmatrix})| = \frac{1}{2}|n^2ad - n^2bc| = \frac{1}{2}n^2|ad - bc| = n^2A(T)$. So, for arbitrary $A(nT) = n^2A(T)$. We know that we can dissect any polygon into triangles, so this result for triangles applies to polygons overall. So, it holds that $A(nP) = n^2A(P)$.

By Exercises 29 and 30, there are $gcd(a,b) - 1$ lattice points on the segment connecting $(0,0)$ and (a,b). Since $gcd(na, nb) = n \cdot gcd(a,b)$, there are $n \cdot gcd(a,b) - 1$ lattice points on the segments connecting $(0,0)$ and (na, nb). Since we can translate every line segment to the origin, by applying this result to each of the polygon edges and adding back in the endpoints we obtain $B(nP) = nB(P)$. □

Exercise 113 Let P be the triangle with vertices $(0,0)$, $(3,1)$, and $(1,4)$.

(a) Sketch P and $5P$ (using the definition for nP provided in Exercise 112.

(b) Compute $L(5P)$ directly using your sketch from part (a).

(c) Compute $L(5P)$ using the result in Exercise 112, and verify that you obtain the same result as in part (b).

Solution

(a) .

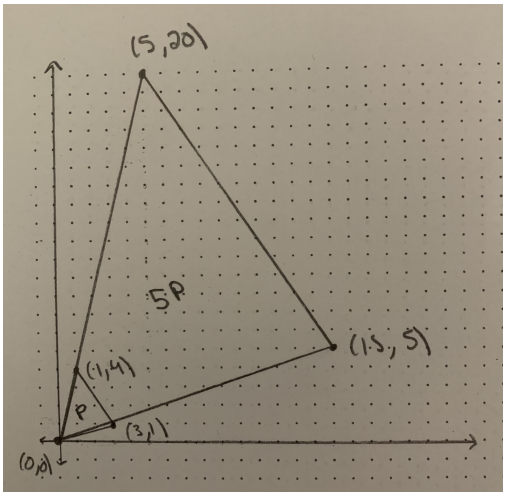


Figure 64: Traingle P and $5P$.

(b) $L(5P) = B(P) + I(P) = 15 + 131 = 146$.

(c) $L(5P) = A(5P) + \frac{1}{2}B(5P) + 1 = 137.5 + \frac{1}{2} \cdot 15 + 1 = 146$.

Definition 27 Let $R \subseteq \mathbb{R}^n$. R is *convex* if for all points x and y in R, the line segment joining x and y is contained in R.

Definition 28 Let $R \subseteq \mathbb{R}^n$. The *convex hull* of R is the intersection of all of the convex sets that contain R. Alternatively, the convex hull of R is the smallest convex set that contains R.

To prove Minkowski's Theorem, we will need the following result, which we will state but not prove.

Theorem 7 Let R be a bounded, closed, convex set in $\mathbb{R}^2$ that contains three non-collinear lattice points. Then the convex hull of the set of all lattice points in R is a lattice polygon P that contains the same number of lattice points as R. Moreover,

$$A(P) \leq A(R) \text{ and } p(P) \leq p(R),$$

where $p(X)$ denotes the perimeter of X.

Exercise 114 Illustrate Theorem 7 for the following regions:

(a) A square with sides of length 3 whose center is the point $(0, 0)$.

(b) An equilateral triangle with vertices $(0, 3)$, $(-2.5, 3 - \frac{5\sqrt{3}}{2})$ and $(2.5, 3 - \frac{5\sqrt{3}}{2})$. Note: this is an equilateral triangle with base 5.

(c) A circle with center $(0, 0)$ and radius $5/4$.

(d) A circle with center $(0, 0)$ and radius $7/8$.

Solution

(a) .

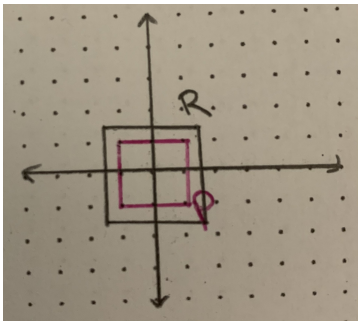


Figure 65: Square with side length 3 and its convex hull.

$L(P) = L(R) = 9$
$A(P) = 4 \leq A(R) = 9$
$p(P) = 8 \leq p(R) = 12$

(b) .

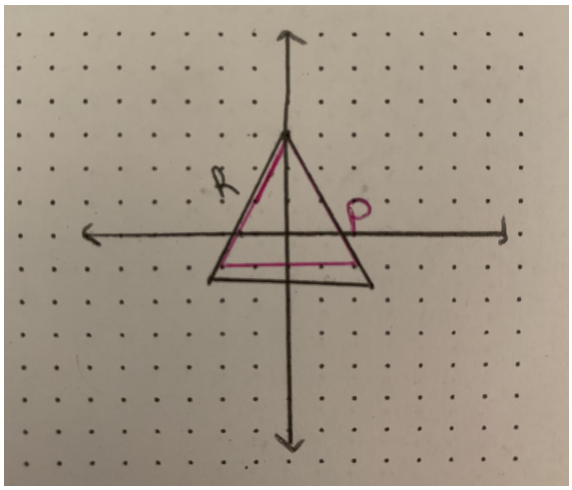


Figure 66: Equilateral triangle and its convex hull.

$L(P) = L(R) = 13$
$A(P) = 8 \leq A(R) \approx 10.8$
$p(P) \approx 12.9 \leq p(R) = 15$

(c) .

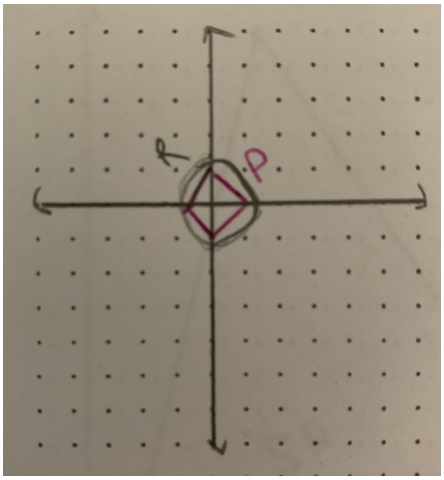


Figure 67: Circle with radius $\frac{5}{4}$ and its convex hull.

$L(P) = L(R) = 5$
$A(P) = 8 \leq A(R) \approx 4.9$
$p(P) \approx 5.7 \leq p(R) \approx 7.9$

(d) A circle with center at $(0, 0)$ and radius $\frac{7}{8}$ is not applicable to Theorem 7 because it only contains 1 lattice point.

The next exercise, a theorem of Ehrhart, generalizes Pick's Theorem to bounded, convex regions in the plane.

Exercise 115 Let R be a bounded, convex region in $\mathbb{R}^2$. Let $L(R)$ denote the total number of lattice points in the interior and boundary of R (i.e. $L(R) = B(R) + I(R)$). Use Pick's Theorem to prove that

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

Solution Consider the lattice polygon P that forms the convex hull P of the region R. By definition, P contains the same number of lattice points as R. Thus $L(R) = L(P)$ and as a result $L(R) = B(P) + I(P)$. Hence, we need to show that $B(P) + I(P) \leq A(R) + \frac{1}{2}p(R) + 1 \iff B(P) + I(P) - 1 \leq A(R) + \frac{1}{2}p(R) \iff \frac{1}{2}B(P) + I(P) - 1 \leq A(R) + \frac{1}{2}p(R) + \frac{1}{2}B(P)$. Using Pick's Theorem for substitution on the left hand side, this is equivalent to showing that

$$A(P) \leq A(R) + \frac{1}{2}p(R) - \frac{1}{2}B(P). \tag{62}$$

By Theorem 7, $A(P) \leq A(R)$. For (62) to hold, we need only to show that $\frac{1}{2}p(R) - \frac{1}{2}B(P) \geq 0 \iff \frac{1}{2}B(P) \leq \frac{1}{2}p(R) \iff B(P) \leq p(R)$.

We also know from Theorem 7 that $p(P) \leq p(R)$. Consider first $p(P)$, the perimeter of the convex lattice polygon P that forms the hull of R. In a lattice polygon, P in this case, adjacent boundary lattice points have a distance between them of at least 1 (the minimum distance possible distance between two lattice points). Thus, the perimeter of a lattice polygon must be greater than or equal to the number of boundary lattice points. That is, $p(P) \geq B(P)$. Since $p(R) \geq p(P)$, we can conclude that $p(R) \geq B(P)$. □

Exercise 116 Illustrate Exercise 115 for the same regions as in Exercise 114.

Solution

(a) .

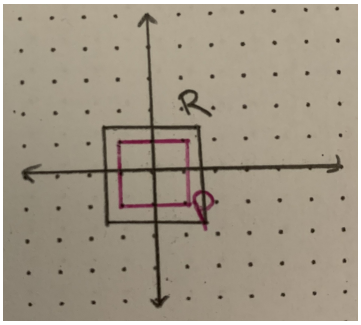


Figure 68: Square with side length 3 and its convex hull.

$L(P) = 9,\ A(P) = 4,\ p(P) = 8$
$L(P) \leq A(P) + \frac{1}{2}p(P) + 1 \implies 9 \leq 4 + \frac{1}{2} \cdot 8 + 1 \implies 9 \leq 9$

(b) .

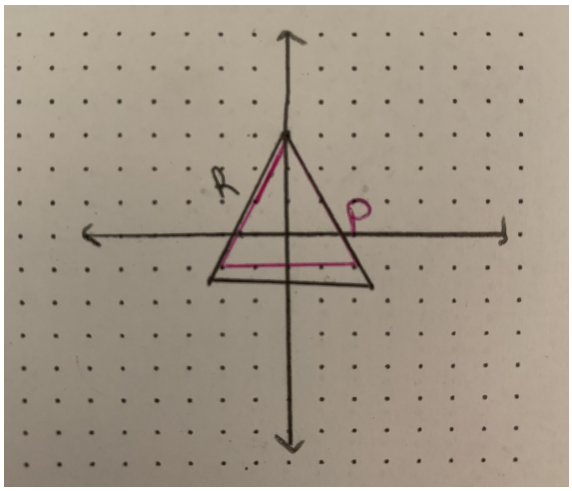


Figure 69: Equilateral triangle and its convex hull.

$L(P) = 13,\ A(P) = 8,\ p(P) \approx 12.9$
$L(P) \leq A(P) + \frac{1}{2}p(P) + 1 \implies 13 \leq 8 + \frac{1}{2} \cdot 12.9 + 1 \implies 13 \leq 15.45$

(c) .

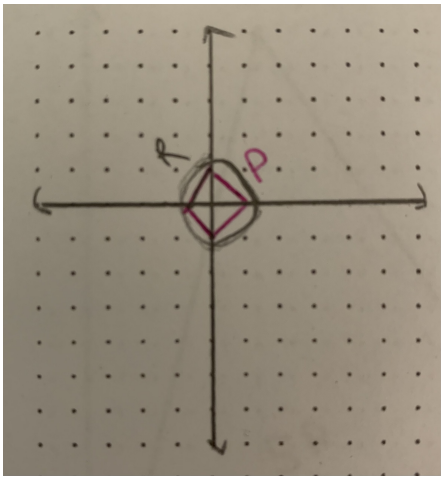


Figure 70: Circle with radius $\frac{5}{4}$ and its convex hull.

$L(P) = 5,\ A(P) = 2,\ p(P) \approx 5.7$
$L(P) \leq A(P) + \frac{1}{2}p(P) + 1 \implies 5 \leq 2 + \frac{1}{2} \cdot 5.7 + 1 \implies 5 \leq 5.85$

(d) We cannot create a convex region from a circle with center at $(0, 0)$ and radius $\frac{7}{8}$ because the circle is not applicable to Theorem 7 since it only contains 1 lattice point.

Theorem 8 Blichfeldt's Theorem. Let R be a bounded set in $\mathbb{R}^2$ with area greater than 1. Then R must contain two distinct points (x_1, y_1) and (x_2, y_2) such that the point $(x_2 - x_1, y_2 - y_1)$ is an integer point (not necessarily in R).

We will prove Blichfeldt's Theorem in a series of exericses. The key idea in this problem is to show that there must exist two distinct points (x_1, y_1) and (x_2, y_2) in R such that x_1 and x_2 have the same *decimal part* (so that $x_1 - x_2 \in \mathbb{Z}$) and y_1 and y_2 have the same decimal part. The important intuition here is to think about how R "compares" to the unit square. To do this, we will introduce some notation.

- Let S denote the unit square, i.e.
$$S = \{(x, y) \text{ such that} 0 \leq x < 1 \text{ and } 0 \leq y < 1\} = [0, 1) \times [0, 1).$$
- For integers i and j, let
$$I_{i,j} = [i, i + 1) \times [j, j + 1).$$
- Let
$$R_{i,j} = I_{i,j} \cap R,$$
i.e. $R_{i,j}$ is the portion of R that lies in the unit interval $[i, i + 1) \times [j, j + 1)$.
- Let
$$T_{i,j} = R_{i,j} - (i, j).$$
This translates each $R_{i,j}$ to the unit square S.

Make sure that you completely understand all of the definitions above before you move on to the next exercise!

Exercise 117 Show that there must exist i, j and m, n such that
$$T_{i,j} \cap T_{m,n} \neq \emptyset$$
and $i \neq m$ or $j \neq n$.

Solution Since R is bounded in $\mathbb{R}^2$, there are finitely many sets $T_{i,j}$. Order the sets $T_{i,j}$ in an arbitrary way and denote them by $T_1, T_2, ..., T_k$. I will prove the suggested result by contradiction. Suppose that $T_a \cap T_b = \emptyset$ whenever $a \neq b$ for all $a, b \leq k$.

Consider T_1. T_1 is a subset of the unit square, so $T_1 \subseteq S$. T_2 is also a subset of the unit square, but cannot include any point in T_1. So, $T_2 \subseteq S \setminus T_1$. By similar reasoning, $T_n \subseteq S \setminus (T_1 \cup T_2 \cup ... \cup T_{n-1})$ for $n = 2, 3, ..., k$.

Now, let $|X|$ denote the area of the region defined by the set X. Then,

$$\begin{aligned} |R| &= |T_1| + |T_2| + ... + |T_{k-1}| + |T_k| \\ &\leq |T_1| + |T_2| + ... + |T_{k-1}| + |S \setminus (T_1 \cup T_2 \cup ... \cup T_{n-1})| \\ &= |T_1| + |T_2| + ... + |T_{k-1}| + |S| - (|T_1| + |T_2| + ... + |T_{n-1}|) \\ &= |S| = 1. \end{aligned} \tag{63}$$

Note: $|T_1|+|T_2|+...+|T_{k-1}|+|S\setminus(T_1\cup T_2\cup...\cup T_{n-1})| = |T_1|+|T_2|+...+|T_{k-1}|+|S|-(|T_1|+|T_2|+...+|T_{n-1}|$ holds true due to the disjointedness of $T_1, T_2, ..., T_{k-1}$.

The finding in (63) is a contradiction as the area of R is strictly greater than 1 by the assumption of Blichfeldt's Theorem. Thus, there must exist i, j and m, n in $\mathbb{Z}$ where $i \neq m$ or $j \neq n$ such that

$$T_{i,j} \cap T_{m,n} \neq \emptyset.$$

□

Exercise 118 Complete the proof of Blichfeldt's Theorem.

Solution Let R be a bounded set in $\mathbb{R}^2$ with area greater than 1. By Exercise 117, there exist $T_{i,j}$ and $T_{m,n}$ satisfying $T_{i,j} \cap T_{m,n} \neq \emptyset$ with $i \neq m$ or $j \neq n$. Let (x, y) be an arbitrary point in the non-empty set $T_{i,j} \cap T_{m,n}$. By construction, we know that $(x + i, y + j) \in R_{i,j}$ and $(x + m, y + n) \in R_{m,n}$. Let $(x_1, y_1) = (x + i, y + j)$ and $(x_2, y_2) = (x + m, y + n)$. Since both $R_{i,j}$ and $R_{m,n}$ are subsets of R, we know that $(x_1, y_1), (x_2, y_2) \in R$. All that is left to show is that $(x_2 - x_1, y_2 - y_1)$ is an integer point. By construction $(x_2 - x_1, y_2 - y_1) = ((x + m) - (x + i), (y + n) - (y + j)) = (m - i, n - j)$ which is a lattice point since $i, j, m, n \in \mathbb{Z}$. □

Definition 29 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.

Theorem 9 Minkowski's Theorem Let R be a bounded, convex region in $\mathbb{R}^2$ that is symmetric about the origin and has area greater than 4. Then R contains a lattice point other than the origin.

Exercise 119 Illustrate Minkowski's Theorem for the following regions:

(a) A circle with center $(0, 0)$ and radius $5/4$.

(b) A circle with center $(0, 0)$ and radius $7/8$.

Solution

(a) A circle with radius $\frac{5}{4}$ has area of about 4.9 and contains 5 lattice points including $(0, 0)$.

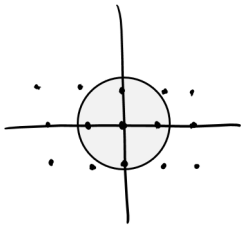


Figure 71: Circle with center $(0, 0)$ and radius $\frac{5}{4}$.

(b) A circle with with radius $\frac{7}{8}$ has an area of about 2.4, so Minkowski's Theorem is not applicable. □

We will now prove Minkowski's Theorem in a series of exercises.

Exercise 120 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

$$R' = \{\frac{1}{2}x \text{ such that } x \in R\}.$$

Since R' is just a smaller version of R, it is clear that R' is convex and symmetric about the origin. Show that there are points x' and y' in R' such that $x' - y'$ is a nonzero lattice point.

Solution Let $[R]$ denote the area of region R. Since R' is scaled down by a factor of 2 from R, we have that $[R'] = \frac{[R]}{4}$. Since, $[R] > 4$, this implies that $[R'] > 1$. At this point, since R is a bounded region, the existence of point x' and y' is guaranteed by Blichfeldt's Theorem from Exercise 118. □

Exercise 121 Let x' and y' be as in Exercise 120. Show that $x' - y'$ is in R. Hint: express $x' - y'$ as a linear combination of points that you know are in R.

Solution For any two points x and y in R, R is defined to be convex if every point on the segment connecting x and y is in R. Since we proved that x', y' are in R', by definition of R' it follows that $2x'$ and $2y'$ are in R. Since R is symmetric, we also have that $-2x'$ and $-2y'$ are in R. Let $x' = (a, b)$ and $y' = (c, d)$.

Case 1: x' and y' are collinear on the ray originating from the origin. In this case, we could write y' as (ka, kb) with both x' and y' falling on the line $y = \frac{b}{a}x$. Assume without loss of generality that y' is further from the origin than x' (this implies that $|k| > 1$). Note that $x' - y' = ((1-k)a, (1-k)b)$ which still falls on the same line. Since we know that $2y' = (2ka, 2kb)$ is in R, then due to the convexity of R, any point on this line with an x-coordinate in the interval $[-2k, 2k]$ must be inside R. In our case, the x-coordinate of $x' - y'$ is $1 - k$. Since $|k| > 1$, it necessarily follows that $|1 - k| < 2k$. Therefore, $x' - y'$ is a nonzero lattice point inside of R, proving Minkowski's Theorem for Case 1.

Case 2: x' and y' are not collinear. In this case, the 4 points form a parallelogram: $(-2a, -2b)$, $(-2c, -2d)$, $(2a, 2b)$, $(2c, 2d)$ (possibly in a different order). Consider a liner transformation defined by the matrix $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$. M is defined since $ad - bc \neq 0$, due to the constraint of the case (since x' and y' are not collinear, they are independent vectors, so their determinant is non-zero). This linear transformation would bring our parallelogram to the square centered at the origin with side length 4 and it would bring $x' - y'$ to the point $(1, 1)$. The transformed version of R is still convex, so every point inside the square uniquely maps to a point in R. Since $(1, -1)$ is obviously inside the square, $x' - y'$ is in R.
Taking cases 1 and 2 together, this concludes the proof of Minkowski's Theorem!

---

8 Challenge Problems

1. Prove that it is possible to construct a regular lattice $n-$gon if and only if $n = 4$. Hint: By Pick's Theorem, the area of any lattice polygon is rational. Use geometry to show that the area of a regular lattice $n-$gon with sides of length b is
$$A = \frac{nb^2}{4\tan\left(\frac{\pi}{n}\right)}.$$
Thus, to show that it is impossible to construct a regular n-gon if $n \neq 4$, it's sufficient to show that the quantity $\tan\left(\frac{\pi}{n}\right)$ is irrational. One way to do this is with the Rational Root Theorem.

2. **Pick's Theorem for Non-Simple Polygons** In the following figure, there are 5 examples of polygons with holes. Polygons A, B, C have one hole, and polygons D and E have 2 holes. Find the area of each of these polygons. Make a table that contains the following information for each polygon: I, B, area, number of holes. Doing more examples if necessary, modify Pick's Theorem to conjecture and prove a formula that works for polygons with holes.

pickholes.jpg

3. For which positive integers n is it possible to construct an *equilateral* (but not necessarily regular) lattice n-gon?

4. **Browkin's Theorem.** Prove that for every natural number n, there exists in the plane a square with exactly n interior lattice points.

5. **Schnizel's Theorem.** Show that for every positive integer n, there is a circle in the plane that has exactly n lattice points on its boundary.
Hint: Consider separately the cases n even and n odd. Here's a hint for the n even case. Show that if $n = 2k$, then the circle with center $\left(\frac{1}{2}, 0\right)$ and radius $\frac{1}{2} \cdot 5^{(k-1)/2}$ contains exactly n boundary lattice points. Then try to do something similar for n odd.

6. Prove that for every natural number n, there exists in the plane a square with exactly n boundary lattice points.

7. **Browkin's Theorem.** Prove that for every natural number n, there exists in the plane a square with exactly n interior lattice points.

8. Browkin's Theorem is actually valid for triangles, pentagons, ellipses, and other figures. In fact, it can be proved that, for every nonempty plane bounded convex figure C, and for every natural number n, there exists in the plane a figure with the shape of C which contains exactly n interior lattice points.

9. **Kulikowski's Theorem.** Prove that for every natural number n, there exists in 3-dimensional space a sphere that contains exactly n boundary lattice points on its surface.

10. Prove that for every natural number n, there exists in 3-dimensional space a sphere that contains exactly n interior lattice points.
Hint: order the lattice points (x, y, z) by showing that no two are the same distance from the point $(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

11. Let $(a, b) \in \mathbb{R}^2$. Suppose that for every positive integer n, there is a circle with center (a, b) containing exactly n lattice points. Show that at least one of a or b is irrational.

12. Let $V_{C(\sqrt{n})}$ be the number of visible lattice points in and on $C(\sqrt{n})$, the circle with center $(0,0)$ and radius $\sqrt{n}$. Find a formula for
$$\frac{V_{C(\sqrt{n})}(n)}{L(n)},$$
and determine the limit
$$\lim_{n\to\infty} \frac{V_{C(\sqrt{n})}(n)}{L(n)}.$$

13. *The distribution of visible lattice points in the plane is* $6/\pi^2$. Consider the square region $S(t)$ in the plane defined by the inequalities
$$|x| \le t \text{ and } |y| \le t,$$
where t is a positive real number. Let $N(t)$ denote the number of lattice points in this square, and let $V(t)$ denote the number of lattice points in the square that are *visible* from the origin. Show that
$$\lim_{t\to\infty} \frac{V(t)}{N(t)} = \frac{6}{\pi^2}.$$
Since the visible points are precisely those lattice points with relatively prime coordinates, this result can be interpreted as saying that the probability that two randomly picked integers are relatively prime is $\dfrac{6}{\pi^2}$.

14. Show that
$$|F_n| \sim \frac{3n^2}{\pi^2} \text{ as } n \to \infty.$$

15. Recall that the Fibonacci sequence is given by
$$\{\phi_m\} 1, 1, 2, 3, 5, 8, 13, \cdots,$$
where each term ϕ_m in the sequence is given by the sum of the previous two terms, i.e.
$$\phi_m = \phi_{m-1} + \phi_{m-2}.$$
Define the sequence of Fibonacci fractions as
$$\frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{3}{8}, \ldots, \frac{\phi_m}{\phi_{m+2}}, \frac{\phi_{m+1}}{\phi_{m+3}}, \ldots.$$
Prove that any two neighboring fractions in the sequence of Fibonacci fractions are adjacent in a Farey sequence F_n.

16. Let a/b and a'/b' be the fractions immediately to the left and the right of the fraction $1/2$ in the Farey sequence of order n. Prove that b is the greatest odd integer less than or equal to n. Next, by experimenting with various choices of n, make and prove a conjecture about the value of $a + a'$.

17. Let a/b and a'/b' run through all pairs of adjacent fractions in the Farey sequence of order $n > 1$. Make and prove a conjecture about the values of
$$\min\left(\frac{a'}{b'} - \frac{a}{b}\right) \text{ and } \max\left(\frac{a'}{b'} - \frac{a}{b}\right).$$

18. Consider the fractions from $0/1$ to $1/1$ inclusive in the Farey sequence of order n. Reading from left to right, let the denominators of these fractions be $b_1, b_2, \ldots, b_k$ so that $b_1 = b_k = 1$. By experimenting with various values of n, make and prove a conjecture about the value of $\displaystyle\sum_{j=1}^{k-1} \frac{1}{b_j b_{j+1}}$.

19. **The Orchard Problem** A circular forest has center at the origin and diameter 27 yards. The trees in the first have diameter 0.15 yards and grow at every lattice point except the origin, where you are standing. Use Minkowski's Theorem to show that you cannot see out of the forest.

20. (Unsolved problem.)

    (a) Consider the following generalization of Farey sequences (due to K. Mahler, A generalization of Farey sequences, *Journal of Number Theory*, **3**(1971) 364–370). The Farey sequence of order n may be regarded as the positive real roots of linear equations whose coefficients are relatively prime and do not exceed n. For $n \in \mathbb{N}$, list the coefficients a, b of the linear equations

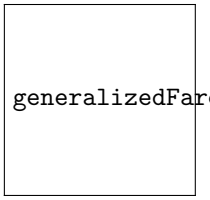
    $$ax + b = 0, \quad a \geq 0, \quad \gcd(a, b) = 1, \quad \max\{a, |b|\} \leq n,$$

    which have positive real roots, in order of the size of the roots. Observe that this procedure produces the Farey sequence of order n. We have proved that the determinant formed from any two consecutive rows of this list is equal to 1. Do this for $n = 5$ to make sure that you understand how the list is formed, and how the *determinants* are computed.

    (b) Next, generalize the above to quadratic equations. List the coefficients a, b, c of the quadratic equations

    $$ax^2 + bx + c = 0, \quad a \geq 0, \quad \gcd(a, b, c) = 1, \quad \max\{a, |b|, |c|\} \leq n,$$

    which have positive real roots, in order of the size of the roots. Next, compute the determinant formed from any **three** consecutive rows. An example of this generalized Farey sequence for $n = 3$ is shown below.

    It appears that the determinant formed from any three consecutive rows is always equal to 0 or ± 1. Can you verify this for $n = 4$? This conjecture has been verified for $n \leq 5$.

    (c) However, it turns out that this conjecture is actually false when $n = 7$. Can you find a counterexample?

    (d) In 1980, Lewis Low (L. Low, Some lattice point problems, *Bulletin of the Australian Mathematical Society*, **21**(1980) 303–305) proved that the absolute value of the determinant is always less than or equal to n. It remains an unsolved problem to make and prove a statement that reduces this bound.

    (e) Studying fourth-order determinants (i.e. determinants formed by four consecutive rows for cubic equations) is also an open question.

9 Topics for Further Research

If you are interested in studying the mathematics of lattice point geometry in more detail, the following are some areas for further research:

- Investigate the relationship between Farey sequences and the Riemann hypothesis. In particular, find and explore the equivalent statement to the Riemann hypothesis using the Farey sequence.
- Investigate the relationship between Pick's Theorem and Euler characteristic.
- Investigate Ehrhart polynomials and the generalization of Pick's Theorem to higher dimensions.
- Investigate the extension of Minkowski's Theorem to an arbitrary lattice.
- Investigate the extension of Minkowski's Theorem to $\mathbb{R}^n$ for $n \geq 3$.
- Investigate the connection between group actions of the group $SL_2(\mathbb{Z})$, Mobius transformations on the plane, and Ford circles and Farey sequences.
- Investigate the Stern-Brocot tree, its connection with Farey sequences, and its application to clock-making.