STANFORD ONLINE HIGH SCHOOL
UM170

Lattice Point Geometry Portfolio

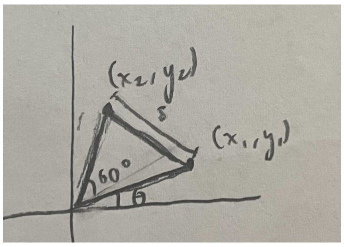
Ryan Lin

Spring 2023

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. It is **not possible** to construct a regular lattice 3-gon. We can show this through a proof by contradiction.
Assume without loss of generality that there is a regular 3-gon with a vertex located at the origin $(0,0)$. This 3-gon has another vertex at some arbitrary point (x_1, y_1). Given this information, as well as the properties of an equilateral 3-gon, let us try to express the location of the last point in terms of x_1 and y_1.
The line segment connecting the points $(0,0)$ and (x_1, y_1) form an angle θ with the x-axis (without loss of generality). We also know that, in a 2D plane, the angle between this line segment and the line segment that connects (0,0) with the other vertex is 60°. See the figure for a visualization:



Let s be the side length of the triangle, where s is equal to $\sqrt{x_1^2 + y_1^2}$. We can then clearly see that

$$x_2 = s \cdot \cos(\theta + 60^\circ)$$
$$y_2 = s \cdot \sin(\theta + 60^\circ)$$

By the sum identities for sin and cos, we then have that

$$x_2 = s \cdot (\cos\theta\cos(60^\circ) - \sin\theta\sin(60^\circ))$$
$$y_2 = s \cdot (\sin\theta\cos(60^\circ) + \cos\theta\sin(60^\circ))$$

Moreover, we know that $\sin\theta = \frac{y_1}{s}$ and $\cos\theta = \frac{x_1}{s}$. Substituting this into the above relations gives that

$$x_2 = s \cdot \left(\frac{x_1}{2s} - \frac{\sqrt{3}y_1}{2s}\right) = \frac{x_1}{2} - \frac{\sqrt{3}y_1}{2}$$
$$y_2 = s \cdot \left(\frac{y_1}{2s} + \frac{\sqrt{3}x_1}{2s}\right) = \frac{y_1}{2} + \frac{\sqrt{3}x_1}{2}$$

Clearly, if x_1 and x_2 are both integers, then the x_2 and y_2 cannot be integers. Therefore, the point (x_2, y_2) cannot be a lattice point, and we have proved that it is impossible to form an equilateral triangle using only lattice points as vertices. Also note that $(x_1, y_1) \neq (0,0)$. If this were not true, then we wouldn't have a triangle.

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**. One example of this is the regular lattice 4-gon formed with vertices (0,0), (1,0), (1,1), and (0,1).

Exercise 3

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

Solution. It is **not possible** to construct a regular lattice pentagon. Let us first assume that it is possible to construct a regular lattice pentagon. This pentagon can be split into five isosceles triangles, which each can be split into two right triangles. For every right triangle, the angle closest to the center of the pentagon is equal to $\frac{\pi}{5}$.

For each triangle, let us calculate the area A_T. The area of the pentagon would then just be $10 \cdot A_T$.

$$A_T = \frac{1}{2} \cdot \frac{s}{2} \cdot h = \frac{1}{2} \cdot \frac{s}{2} \cdot \frac{s}{2 \cdot \tan(\frac{\pi}{5})}$$

$$A_P = 10 \cdot A_T = \frac{5s^2}{4\tan(\frac{\pi}{5})}$$

To continue this proof, we must first show that the area of a lattice triangle must be rational. Suppose there exists a regular lattice triangle ABC with vertices A $(0,0)$, B (x_1, y_1), and C (x_2, y_2). The area of such a triangle can be represented as

$$A_T = \frac{\|\vec{AB} \times \vec{AC}\|}{2} = \frac{1}{2} \cdot (x_1 y_2 - x_2 y_1)$$

Because all the coordinates are rational, we know that the area of a triangle which has all three vertices at lattice points must be rational.

Now let us prove that $\tan(\frac{\pi}{5})$ is irrational. We know that $0 = \tan(\pi)$, and that π can be rewritten as $n \cdot \frac{\pi}{n}$. We can then use the sum identity for tangent repeatedly to arrive at a polynomial with irrational roots. First, let $x = \tan(\frac{\pi}{5})$.

$$0 = \tan(\pi) = \tan(5 \cdot \frac{\pi}{5}) = \tan(\frac{4\pi}{5} + \frac{\pi}{5}) = \frac{\tan(\frac{4\pi}{5}) + \tan(\frac{\pi}{5})}{1 - \tan(\frac{4\pi}{5})\tan(\frac{\pi}{5})}$$

$$\tan(\frac{2\pi}{5}) = \tan(\frac{\pi}{5} + \frac{\pi}{5}) = \frac{\tan(\frac{\pi}{5}) + \tan(\frac{\pi}{5})}{1 - \tan(\frac{\pi}{5})\tan(\frac{\pi}{5})} = \frac{2x}{1 - x^2}$$

$$\tan(\frac{3\pi}{5}) = \tan(\frac{2\pi}{5} + \frac{\pi}{5}) = \frac{\tan(\frac{2\pi}{5}) + \tan(\frac{\pi}{5})}{1 - \tan(\frac{2\pi}{5})\tan(\frac{\pi}{5})} = \frac{3x - x^3}{1 - 3x^2}$$

$$\tan(\frac{4\pi}{5}) = \tan(\frac{3\pi}{5} + \frac{\pi}{5}) = \frac{\tan(\frac{3\pi}{5}) + \tan(\frac{\pi}{5})}{1 - \tan(\frac{3\pi}{5})\tan(\frac{\pi}{5})} = \frac{-4x^3 + 4x}{x^4 - 6x^2 + 1}$$

$$\begin{aligned}
0 &= \frac{\tan(\frac{4\pi}{5}) + \tan(\frac{\pi}{5})}{1 - \tan(\frac{4\pi}{5})\tan(\frac{\pi}{5})} = \frac{\frac{-4x^3+4x}{x^4-6x^2+1} + x}{1 - \frac{-4x^3+4x}{x^4-6x^2+1}x} \\
0 &= \frac{-4x^3 + 4x}{x^4 - 6x^2 + 1} + x \\
&= -4x^3 + 4x + x^5 - 6x^3 + x \\
&= x^5 - 10x^3 + 5x \\
&= x(x^4 - 10x^2 + 5) \\
0 &= x^4 - 10x^2 + 5
\end{aligned}$$

Solving this polynomial, through the quadratic formula for example, yields that

$$x = \sqrt{5 + 2\sqrt{5}}, -\sqrt{5 + 2\sqrt{5}}, \sqrt{5 - 2\sqrt{5}}, -\sqrt{5 - 2\sqrt{5}}$$

Seeing as all these values are irrational, we can conclude that $\tan(\frac{\pi}{5})$ must be irrational.

With that in mind, our formula for A_T presents a contradiction. We know that s^2 will be rational, since s is $\sqrt{a^2 + b^2}$ (if we set one vertex at (0,0) and the other at $(a.b)$) and a and b are both rational. We also know that $\tan(\frac{\pi}{5})$ is irrational. Thus, the overall expression for the area is irrational. This contradiction means we have proved that it is impossible to construct a regular lattice pentagon.

EXERCISE 4

Show that the cosine of each interior and exterior angle of any regular lattice polygon must be rational.

Solution. Let there be two vectors $\mathbf{u} = \langle a, b\rangle$ and $\mathbf{v} = \langle c, d\rangle$. These two vectors represent the two sides of an arbitrary regular lattice polygon and form an angle θ.
From the dot product, we can show that

$$\cos(\theta) = \frac{ac + bd}{\|\mathbf{u}\|\,\|\mathbf{v}\|}$$

We also know, due to the properties of a regular polygon, that $\|\mathbf{u}\| = \|\mathbf{v}\|$. Thus, we can rewrite the above expression like so:

$$\cos(\theta) = \frac{ac + bd}{\|\mathbf{u}\|^2} = \frac{ac + bd}{a^2 + b^2}$$

Because we know that a, b, c, and d are all rational integer values, we know that $\cos(\theta)$ must also be rational. Moreover, we know that $\cos(\theta) = -\cos(\pi - \theta)$ and that the exterior angle is the same as $\pi - \theta$. Thus, we have shown that the cosine of each interior and exterior angle of any regular lattice polygon must be rational.

EXERCISE 5

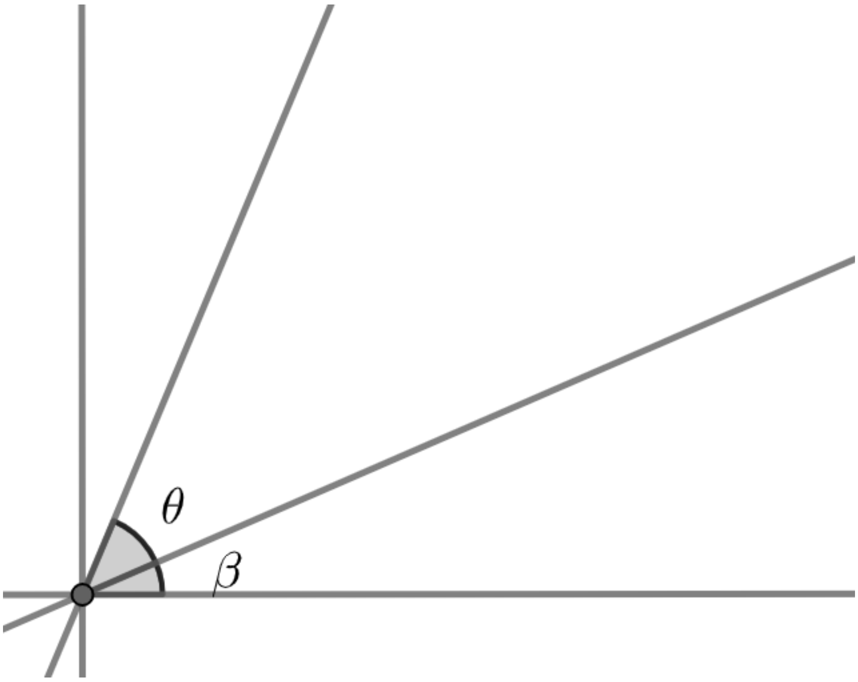
Use Exercise 4 to show that it is not possible to construct a regular lattice octagon (8-gon).

Solution. We know that the interior angles of a hypothetical regular lattice octagon must be 135°(this is fairly easy to prove by dividing the regular octagon into 8 parts. The central angles must be $\frac{360}{8} = 45°$, and thus the base angles must be 67.5°. Adding up two base angles shows that each interior angle is just 135°).
We also know that $\cos(135°) = -\frac{\sqrt{2}}{2}$, which is irrational. From **Exercise 4**, we also know that a regular lattice polygon must have interior angles such that $\cos(\theta)$ is rational. The octagon contradicts this requirement, meaning we have shown that it is impossible 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 $\frac{\pi}{2}$ or an odd integer multiple of $\frac{\pi}{2}$, then the tangent of α is a rational number.

Solution. Let the lattice angle be denoted as θ, and be defined by points $A\ (x_1, y_1)$, $B(0,0)$, and $C(x_2, y_2)$, and let β be the offset of θ from the x-axis (which allows us to generalize this result and make use of a handy trig identity). Let $\alpha = \theta + \beta$.



From this, we can show that

$$\tan(\alpha-\beta)=\tan(\theta)=\frac{\tan\alpha-\tan\beta}{1+\tan\alpha\tan\beta}=\frac{\frac{y_1}{x_1}-\frac{y_2}{x_2}}{1+\frac{y_1y_2}{x_1x_2}}$$

To begin with, we know that the numerator $\frac{y_1}{x_1}-\frac{y_2}{x_2}$ will be rational, since x_1, y_1, x_2, and y_2 are all lattice coordinates. Moreover, we know that the dot product of the vectors which define the angle, $\vec{BA}$ and $\vec{BC}$, is not equal to 0 (since it is given that α is not equal to $\frac{\pi}{2}$ or some odd integer multiple of $\frac{\pi}{2}$). This means that $x_1x_2 \neq -y_1y_2$. Therefore, $\frac{y_1y_2}{x_1x_2} \neq -1$, and the denominator will never be 0. Thus, $\tan(\theta)$ must be rational.

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. From the exercises above, we can make the conjecture that the only regular lattice polygon which can be constructed (in a 2D plane) is the square.
We have shown that we cannot construct a regular lattice polygon for the case of $n=3$. Let us then take the tangent of each angle of the polygon for $n>4$:

$$\tan\theta=\tan\left(\frac{(n-2)\pi}{n}\right)=\tan\left(\pi-\frac{2\pi}{n}\right)=-\tan\left(\frac{2\pi}{n}\right)$$

To be able to represent the angle of the polygon with lattice points, its tangent must be rational (Exercise 6). We know that the above RHS can only be rational when $\frac{2\pi}{n} = \frac{\pi}{4}$. This is only true when $n = 8$. However, from Exercise 5, we know that we cannot construct an octagon. Thus, we can make the conjecture that the only regular lattice polygon which can be constructed in a 2D space is the square.

EXERCISE 8

For which positive integers n is it possible to construct an equilateral (but not necessarily regular) lattice n-gon?

Solution. Suppose that n is odd. By way of contradiction, let us assume that there does exist an equilateral lattice polygon P_n with side lengths of d. Then, let (x_1, y_1) and (x_2, y_2) be two adjacent vertices of P_n. We now have

$$d^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2$$

Because d^2 is the sum of squares of two integers, we must have that

$$d^2 = 0, 1, 2 \mod 4$$

Now let us consider the following cases.

> **Case 1:** Suppose that $d^2 \equiv 1 \mod 4$. We can form a graph G with all lattice points and vertices $(x, y) \in \mathbb{Z}^2$. Let us connect two vertices in this graph with an edge if there is a distance of d between the two lattice points. From this, we can separate two subsets of the vertices: If x and y for (x, y) have the same parity, then put them in subset X. If they have different parity, put them in subset Y. By construction, we have two sets X and Y such that $X \cap Y = \emptyset$. Now let us prove that no edge of G can join two vertices from the same subset. If there was such an edge joining vertices (x_1, y_1) and (x_2, y_2) in X, then x_1 and y_1 would have the same parity, and x_2 and y_2 would also have the same parity. Thus, $x_2 - x_1$ and $y_2 - y_1$ would have the same parity, meaning d^2 would be even. This contradicts our assumption that $d^2 \equiv 1 \mod 4$. Similarly, we can say the same for any two vertices in Y. This means our graph G is bipartite. However, P_n is odd, so G must contain an odd cycle. Bipartite graphs cannot contain odd cycles. This contradiction shows that we cannot have an equilateral lattice polygon.
>
> **Case 2:** Suppose that $d^2 \equiv 2 \mod 4$. Now consider our graph G. Let us again connect two lattice points only if they have a distance d between them. If x and y have the same parity, let us put them in subset X. If they have a different parity, put them in subset Y. By construction, we have two sets X and Y such that $X \cap Y = \emptyset$. We will again show that G is bipartite. Assume there is an edge connecting two vertices (x_1, y_1) and (x_2, y_2) in X. This would mean x_1 and x_2 are both even, implying that $x_1 - x_2$ is also even, meaning
>
> $$(x_1 - x_2)^2 \equiv 0 \mod 4$$

Recall that we have

$$d^2 \equiv (x_2 - x_1)^2 + (y_2 - y_1)^2 \equiv 2 \mod 4$$

This would mean that $(y_2 - y_1)^2 \equiv 2 \mod 4$. However, $(y_2 - y_1)^2 \equiv 0$ or $1 \mod 4$. This contradiction shows that G is bipartite and cannot contain an odd cycle (and therefore we cannot have an equilateral lattice polygon).

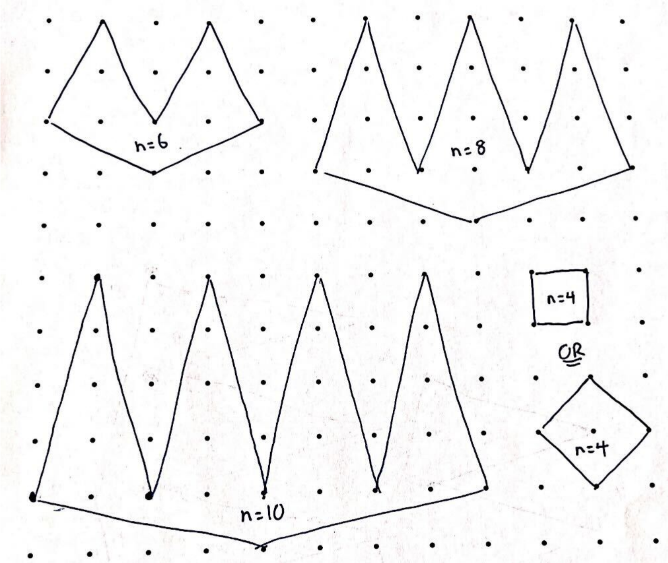
Case 3: Suppose that $d^2 \equiv 0 \mod 4$. This would mean that d^2 is divisible by 4, implying that d must be an even integer. This would also mean that $\frac{1}{2}d$ is an integer, as well. If we translate each of the n vectors of P_n to the origin, and let $(p_i q_i)$ denote the endpoint of the i-th vector, then $p_i, q_i \in \mathbb{Z}$. Because

$$d^2 = p_i^2 + q_i^2 \equiv 0 \mod 4$$

We must have that p and q are both even. Thus, $(p_i/2, q_i/2) \in \mathbb{Z}^2$. From this, we can construct a new smaller equilateral lattice polygon with side lengths of $d_1 = \frac{1}{2}d$. For this new polygon, we either have $d_1^2 \equiv 0, 1$, or $2 \mod 4$. We already proved that the 1 and 2 case are impossible. If $d_1^2 \equiv 0 \mod 4$, then we could again produce a smaller equilateral lattice n-gon with side length $d_2 = \frac{1}{2}d_1 = \frac{1}{4}d$. Continuing this on, we would have infinite polygons with side length $d_k = \frac{1}{2^k}d$. Note that $\lim_{k\to\infty}\left(\frac{1}{2^k}d\right) = 0$. This contradicts the fact that every lattice polygon must have a side length of at least 1. Thus, we have shown that we cannot have an equilateral lattice polygon to begin with.

Because we have obtained contradictions in all possible cases, we have shown that we cannot have an equilateral lattice polygon P_n for an odd n.

We can now show that it is possible to construct an equilateral lattice polygon for even n. Consider the following "comb" construction.



We can easily extend this construction for all even n. Thus, we have proved that we can indeed construct an equilateral lattice polygon for even n.

EXERCISE 9

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. It **is possible** to construct a lattice square whose area is not a perfect square, since it is possible to produce irrational side lengths for a lattice square. Take, for example, the square formed by the points (0,1), (1,0), (2,1), (1,2). The sides of this square are hypotenuses of a 45-45-90 triangle which has base length 1, meaning that the side lengths of the square are $\sqrt{2}$.
Clearly, the area of this square is then $\sqrt{2}^2 = 2$, which is not a perfect square.

EXERCISE 10

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

Solution. It **is not possible** to construct a lattice square whose area is not an integer. Let a lattice square be defined by the points ABCD. Side length AB is defined by the two endpoints (x_a, y_a) and (x_b, y_b). By construction, we know that these coordinates are integers. The side length, by the distance formula, $\sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$. Thus, the area of the square is going to be $\sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}^2 = (x_a - x_b)^2 + (y_a - y_b)^2$, which we know will be an integer value.

EXERCISE 11

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

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

Solution.

Let us first prove that if there exists non-negative integers a and b such that $n = a^2 + b^2$ then there exists a lattice square with area n. Without loss of generality, let us consider a lattice square with two vertices at (0,0) and (a, b). The other vertices would be located orthogonally with respect to these two vertices, at $(-b, a)$ and $(-b + a, a + b)$. The side lengths of this square would then be the distance between two of the vertices, namely $\sqrt{a^2 + b^2}$. The area, then, is $(\sqrt{a^2 + b^2})^2 = a^2 + b^2 = n$.

Now let us prove the other direction. For squares of area n, we know that $n = \sqrt{n}^2$ where $\sqrt{n}$ is the side length of the square. Substituting our value of $\sqrt{n}$ from above, $n = \sqrt{n}^2 = (\sqrt{a^2 + b^2})^2 = a^2 + b^2$. Moreover, we know it's possible to take the square root of n, since n is an integer (see Exercise 10) and must be positive. Thus, we show that if there exists a lattice square with area n, then there must also exist non-negative integers a and b such that $n = a^2 + b^2$.

This concludes our bidirectional proof.

Exercise 12

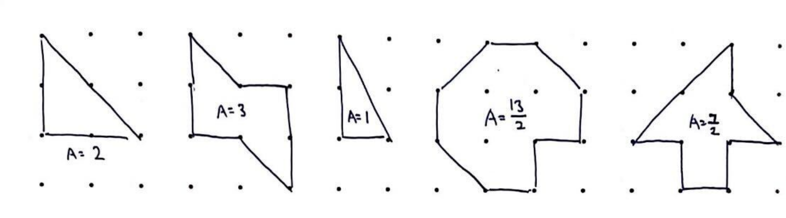
Is it possible to construct a lattice triangle whose area is not an integer? If so, provide an example. If not, prove it.

Solution. It **is possible** to construct a lattice triangle whose area is not an integer. Take, for example, the triangle formed by the points (0,0), (1,0), and (1,1). The area of this triangle is $\frac{1}{2}bh = \frac{1}{2} \cdot 1 \cdot 1 = \frac{1}{2}$, which is not an integer.

Exercise 13

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.

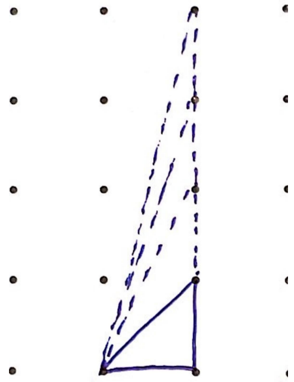


From the examples, it seems that it is possible to achieve all rational areas. Clearly, since we can make triangles of different areas, it is impossible to have all integer areas. Moreover, we can also say that we can form only areas of $\frac{r}{2}$ where r is a positive integer.

Exercise 14

Let T be a lattice triangle with $I(T) = 0$. What are the possible values of $B(T)$? Prove your result.

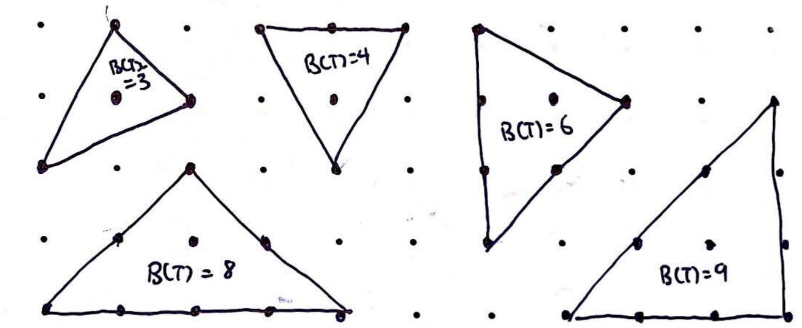
Solution. It is fairly trivial to show that the lower bound of $B(T)$ is 3, since the triangle must at least have its vertices at lattice points. Additionally, we can infinitely extend the height of the triangle to keep increasing the value of $B(T)$. Thus we have the result that for a lattice triangle with $I(T) = 0$, the possible values of $B(T)$ are n where $n \geq 3$. See the diagram for an explanation.



Exercise 15

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.

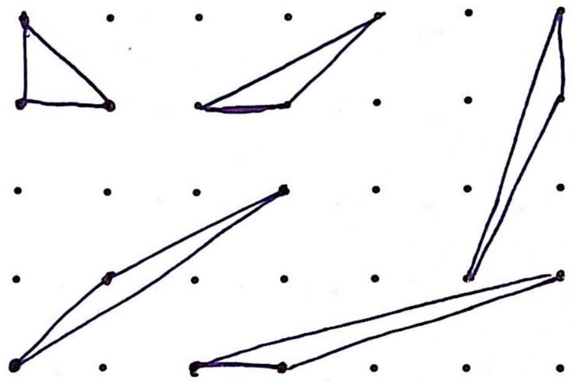
Solution. It seems that the possible values of B for a triangle with $I(T) = 1$ are 3, 4, 6, 8, 9. Clearly, the lower bound is again 3 (or else T would not be a lattice triangle). It seems a bit more difficult to prove the other values, but here are some examples I came up with:



Exercise 16

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.

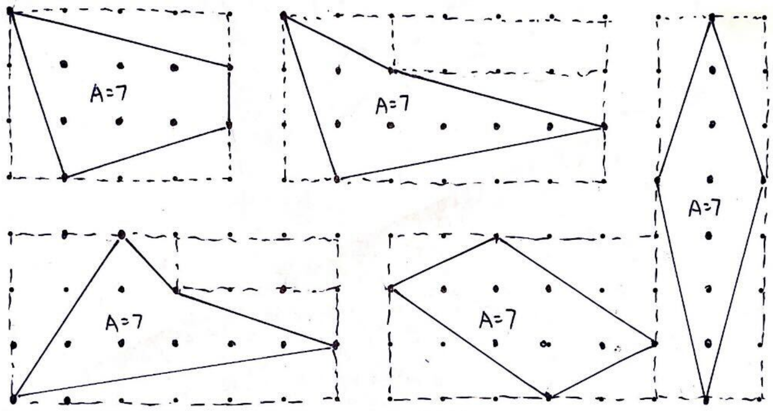
Solution. All primitive lattice triangles must have an area of $\frac{1}{2}$.



Exercise 17

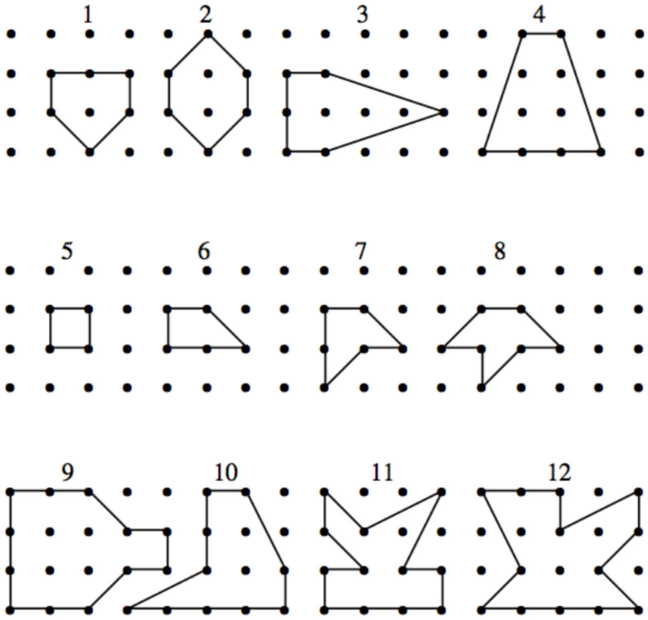
Construct several (at least 5) different polygons that contain 4 boundary lattice points and 6 interior lattice points. Keep in mind that the polygons do not need to be convex! Find the area of each polygon. What do you observe? Make a conjecture based on your observations in this exercise.

Solution. It seems that every one of the polygons has the same area. Thus, we can make the conjecture that perhaps the area of a lattice polygon depends solely on the number of boundary lattice points and interior lattice points.



EXERCISE 18

Find the area of each of the lattice polygons in Figure 1. 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).



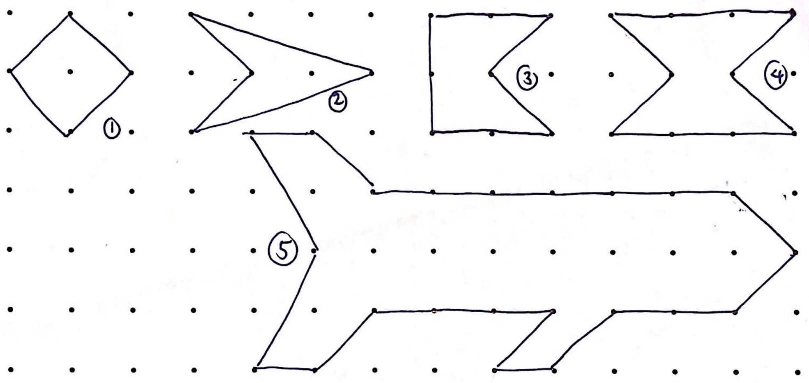
Polygon	Area	I	B
1	3	1	6
2	4	2	6
3	5	3	6
4	6	4	6
5	1	0	4
6	$\frac{3}{2}$	0	5
7	2	0	6
8	$\frac{5}{2}$	0	7
9	9	4	12
10	6	2	10
11	6	1	12
12	$\frac{17}{2}$	3	13
Exercise 19 #1	2	1	4
Exercise 19 #2	2	1	4
Exercise 19 #3	3	0	8
Exercise 19 #4	4	0	10
Exercise 19 #5	19	9	22
Exercise 20	$\frac{11}{2}$	5	3

EXERCISE 19

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 18.

Solution. Here are the polygons I drew out. For the numeric data, please see Exercise 18.



Exercise 20

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 18.

Solution. See Exercise 18.

Exercise 21

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. Whenever B is even, $A(P)$ will be an integer. Whenever B is odd, $A(P)$ will still be a rational number, but will be an odd multiple of $\frac{1}{2}$

Exercise 22

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 I increases by 1 and B stays fixed, the area increases by 1. Thus, we know that I is linearly dependent with A. So, we know our formula will have an I somewhere. Moreover, if B increases by 1 and I stays fixed, then it seems that A increases by $\frac{1}{2}$. Thus, our formula should also include a $\frac{1}{2}B$. However, through trial and error we can see that adding these two terms together yields a value that is always 1 greater than the expected A. We can just correct for this steady-state error and include a -1 in our formula. Thus, our final formula is

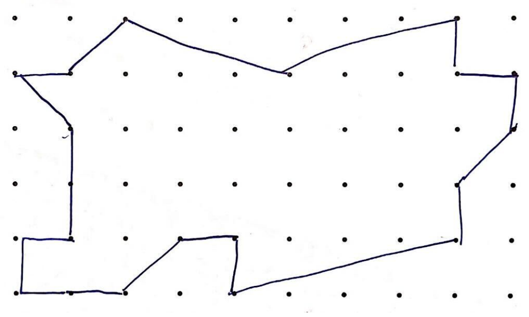
$$A = \frac{1}{2}B + I - 1$$

I suspect that there might be some relationship between the possible area encapsulated by the boundary points, as well as how these boundary points could be folded across the given interior points. This would require more proof, but we may be able to conduct induction from the base case of the smallest possible lattice triangle having an area of $\frac{1}{2}$. Thus, every addition of a new boundary point could introduce a new $\frac{1}{2}$ to the area (?). Every interior point introduces a new unit square to the polygon, but the first interior point will never add a whole square. This is the reason for the -1 in the formula.

EXERCISE 23

Construct your own lattice polygon, and verify that the formula that you conjectured in Exercise 22 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. Below is my hand-crafted artisan polygon:



The area of this polygon is 31. There are 22 interior points and 20 boundary points. We can see that the equality $A = \frac{1}{2}B + I - 1$ holds true, since $31 = \frac{20}{2} + 20 - 1$.

EXERCISE 24

Assuming that your conjecture in Exercise 22 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 the conjecture from Exercise 22 is valid, then the only possible values of the area of a lattice polygon are the multiples of $\frac{1}{2}$ (this is trivial to show, given the formula only includes integers or multiples of $\frac{1}{2}$).
I arrived at this conjecture through analyzing the linear relationships between A, B, and I. It's possible that we can prove this conjecture through analyzing the effects of adding boundary points to the polygon (making use of the property that all primitive lattice triangles have an area of $\frac{1}{2}$), as well as the fact that every additional interior point adds a unit square to the polygon.

EXERCISE 25

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. **No.** Take, for example, the lattice line segment connecting the points $(0,0)$ and $(1,1)$. Clearly, the length of this line segment is irrational ($\sqrt{1^2+1^2}=\sqrt{2}$).

EXERCISE 26

Show that the square of the length of any lattice line segment is an integer.

Solution. The length of any lattice line segment is just the distance between the two endpoints, which can be represented as

$$d^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2$$

Where all x_1, x_2, y_1, and y_2 are integers. Clearly, the square of an integer must also be an integer. Moreover, the sum of two integers is also an integer. Thus, the square of the length of any lattice line segment is an integer.

EXERCISE 27

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. The line L can be represented as $y = mx + b$, where m is rational. Let us denote the lattice point L as (x_1, y_1). Substituting these values in the formula gives $y_1 = m(x_1) + b$ where y_1, x_1, and m are all rational. Now let us solve for the y-intercept, b.

$$b = y_1 - m(x_1)$$

Since all y_1, m, and x_1 are rational, and we know that the products and differences of rational numbers are also rational, we can conclude that the y-intercept of L is also rational.

EXERCISE 28

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. We know that L has a rational slope. Let us denote this to be $\frac{a}{b}$ where a is the change in y for every b-unit change in x. Because the slope is rational, we know that a and b are both integers.

We are also given that there exists a lattice point on L, let us denote this point as (x_1, y_1). Let us keep increasing x by increments of b and y by increments of a. This yields the points $(bk + x_1, ak + y_1)$, where a, b, x_1, y_1, and k are all integers and k is just an index so we can generate scalar multiples of the components of the slope. Continuing this from $k = 1$ to $k =$ inf shows that there are infinitely many lattice points on L (since both $bk + x_1$ and $ak + y_1$ will yield integers).

EXERCISE 29

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. Let us take the line segment connecting $(0, 0)$ and lattice point $p = (m, n)$ such that $\gcd(m, n) = 1$. This line has a slope of $\frac{n}{m}$. Since it is given that $\gcd(m, n) = 1$, then we know that the slope $\frac{n}{m}$ is a fraction that cannot be simplified into an integer.

Now, assume that there does exist a point $(x_1, f(x_1))$ such that $0 < x_1 < m$. If $f(x_1) = \frac{n}{m}x_1$, then $\gcd(nx_1, m) = m$, since it is otherwise impossible for $(x_1, f(x_1))$ to be a lattice point. Because we are given that $\gcd(m, n) = 1$, we can further reduce this to show that $\gcd(nx_1, m) = \gcd(n, m) \cdot \gcd(x_1, m) \Rightarrow \gcd(x_1, m) = m$. However, this violates the condition that $x_1 < m$. Therefore, we can conclude that there are no lattice points strictly between the origin and p on the line segment directly connecting the two points if $\gcd(m, n) = 1$.

EXERCISE 30

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 the lattice point $p = (m, n)$ is on the line L (and p is a visible point), then the equation for L must be $f(x) = \frac{n}{m}x$. We know that the fraction $\frac{n}{m}$ is fully reduced, since p is a visible point and $\gcd(m, n) = 1$.

Any other integer points on the line L must then also satisfy this equation. Let us take any arbitrary lattice point $p_1 = (x_1, f(x_1))$ on line L. Firstly, we know that p_1 cannot be a visible point (since there can only be one visible point, which is (m, n)). From Exercise 29, we also know that $\gcd(x_1, m) = m$, so we can represent x_1 as $x_1 = tm$ where t is some integer > 0. From here,

$$f(x_1) = \frac{n}{m} \cdot tm = tn$$

Thus, we have shown that any lattice point on L is of the form (tm, tn) for some integer t.

Exercise 31

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. Let $p = (m, n)$ be a lattice point such that $\gcd(m, n) = k$. We know then that $\frac{m}{k}, \frac{n}{k} \in \mathbb{N}$, and that $(\frac{m}{k}, \frac{n}{k})$ is a lattice point on the line segment $\mathbf{0}p$. Moreover, we know that $\gcd(\frac{m}{k}, \frac{n}{k}) = 1$, since we divided out all the common factors of m and n. We showed in Exercise 29 that there are no lattice points strictly between the origin and a point like $(\frac{m}{k}, \frac{n}{k})$. Also, in Exercise 30, we showed that all the lattice points on L can be expressed in the form $(t\frac{m}{k}, t\frac{n}{k})$ such that t is some integer (if $(\frac{m}{k}, \frac{n}{k})$ is a visible point on the lattice line L).

Thus, every lattice point on L can be expressed as $(\frac{m}{d}, \frac{n}{d}), (\frac{2m}{d}, \frac{2n}{d}), (\frac{3m}{d}, \frac{3n}{d}), \ldots (\frac{(k-1)m}{k}, \frac{(k-1)n}{k})$, excluding the endpoints. Therefore, there are $k - 1$ (or $\gcd(m, n) - 1$) lattice points on the line segment between the origin and the point (m, n), not including the endpoints.

Exercise 32

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 of the boundary of P is given by

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

Solution. Let $d_i = \gcd(a_{i+1} - a_i, b_{i+1} - b_i)$ for P, as stated in the prompt. Consider a vector connecting the two points p_i and p_{i+1}, which has the components $\langle a_{i+1} - a_i, b_{i+1} - b_i \rangle$. Using the proof from Exercise 31, we show that $\gcd(a_{i+1} - a_i, b_{i+1} - b_i) = d_i - 1$ is the number of lattice points in the vector (excluding the endpoints). Thus, each of the edges have $d_i - 1$ lattice points (this works because we know that $d_n = \gcd(a_1 - a_n, b_1 - b_n))$ for $i = 1$ through $i = n$. We also know that there are n endpoints we have not yet counted. So, the number of lattice points on the boundary of P is given by

$$B(P) = \left(\sum_{i=1}^{n} d_i - 1\right) + n = \sum_{i=1}^{n} d_i$$

EXERCISE 33

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

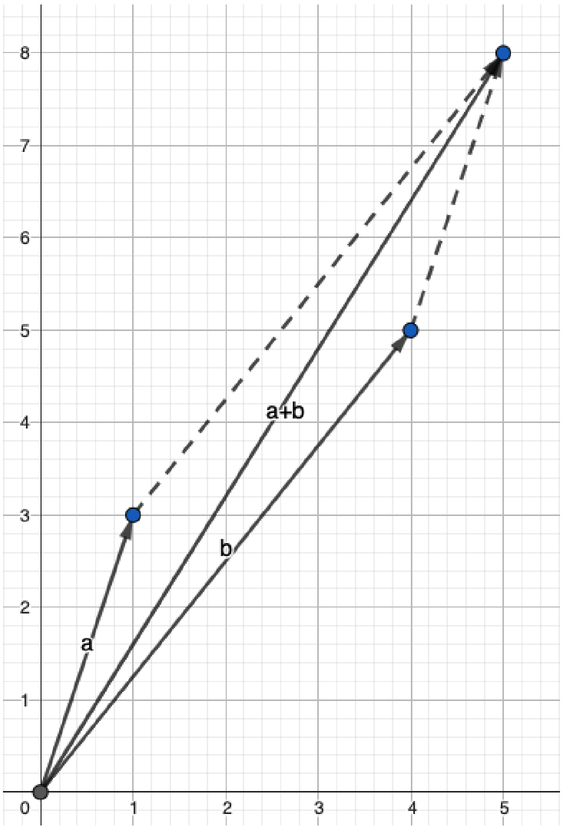
Solution. Let $a = \begin{bmatrix} 4 \\ 3 \\ 2 \\ 1 \end{bmatrix}$, $b = \begin{bmatrix} 7 \\ 2 \\ 6 \\ 5 \end{bmatrix}$. a and b are vectors in $\mathbb{R}^4$ with the sum $a + b = \begin{bmatrix} 11 \\ 5 \\ 8 \\ 6 \end{bmatrix}$.

EXERCISE 34

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

Solution. Let $a = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$, $b = \begin{bmatrix} 4 \\ 5 \end{bmatrix}$. a and b are two unequal vectors in $\mathbb{R}^2$ with the sum $a+b = \begin{bmatrix} 5 \\ 8 \end{bmatrix}$.

We can illustrate the Parallelogram Rule by drawing out vectors a and b, and showing that $a + b$ is just the diagonal of the parallelogram formed by the two vectors.

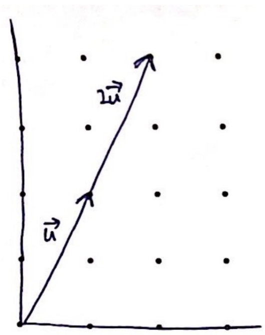


EXERCISE 35

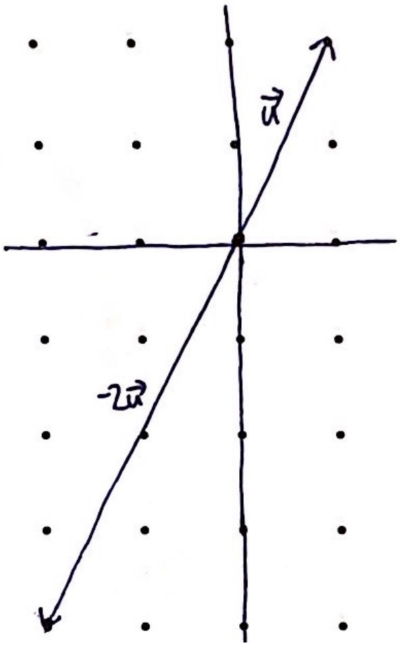
Give an example of a vector **u** in $\mathbb{R}^2$. Compute 2**u**, −2**u**, and $\frac{1}{2}$**u**. Next, draw each of these vectors. What do you observe? What does the set of all scalar multiples of a fixed nonzero vector form?

Solution. Let $\mathbf{u} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$...

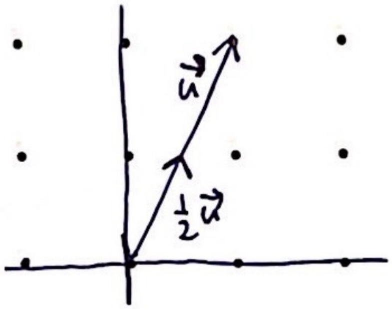
$$2\mathbf{u} = \begin{bmatrix} 2 \\ 4 \end{bmatrix}:$$



$-2\mathbf{u} = \begin{bmatrix} -2 \\ -4 \end{bmatrix}$:



$\frac{1}{2}\mathbf{u} = \begin{bmatrix} -\frac{1}{2} \\ -1 \end{bmatrix}$:



From these, we can observe that scalar multiples of **u** of a fixed nonzero vector form have a slope of $\frac{a}{b}$ (where a and b are the y and x components of **u**) and a length of some scalar multiple of $||\mathbf{u}||$.

Exercise 36

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.

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

Exercise 37

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

Solution.

$$\mathbf{v} = 1\begin{bmatrix} 5 \\ -6 \end{bmatrix} + 3\begin{bmatrix} 1 \\ -2 \end{bmatrix} = \begin{bmatrix} 8 \\ -12 \end{bmatrix}$$

Exercise 38

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

Solution. By Definition 21, we can form a system of linear equations:

$$0 = x\begin{bmatrix} 1 \\ 2 \end{bmatrix} + y\begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$\begin{cases} x+3y=0 \\ 2x+4y=0 \end{cases} \Rightarrow x=y=0.$$

Because the only solution is the trivial solution, these vectors are **linearly independent**.

EXERCISE 39

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

Solution. By Definition 21, we can form a system of linear equations:

$$0 = x\begin{bmatrix} 1 \\ 2 \end{bmatrix} + y\begin{bmatrix} -3 \\ -6 \end{bmatrix}$$

$$\begin{cases} x-3y=0 \\ 2x-6y=0 \end{cases} \Rightarrow x=3y, y\in\mathbb{R}.$$

Because there are infinitely many solutions to this system, the vectors are **linearly dependent**.

EXERCISE 40

(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) **Yes**. We know from Exercise 38 that these two vectors are linearly independent. They can also be written as a linear combination that spans the vector space. As such, we conclude that this set is a basis for $\mathbb{R}^2$.

(b) **No**. We know from Exercise 38 that these two vectors are linearly independent. Let us try to write these vectors as a linear combination to express an arbitrary vector in $\mathbb{Z}^2$:

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

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

This shows that c_1 and c_2 are not necessarily integers for this set, meaning these vectors do not form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$.

We can further demonstrate through the counterexample $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. For this $\begin{bmatrix} x \\ y \end{bmatrix}$, the only possible solution is $c_1 = -\frac{1}{2}, c_2 = \frac{1}{2}$. Clearly, this violates the condition that the scalars c_1 and c_2 must be integers.

EXERCISE 41

Use Definition 25 to show that the matrix

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

is invertible over $\mathbb{R}$.

Solution. Let us calculate the inverse of A by the formula directly.

$$A^{-1} = \frac{1}{11-12} \begin{bmatrix} 11 & -3 \\ -4 & 1 \end{bmatrix} = \begin{bmatrix} -11 & 3 \\ 4 & -1 \end{bmatrix}$$

Now we can show that $AA^{-1} = I$:

$$AA^{-1} = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix} \begin{bmatrix} -11 & 3 \\ 4 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Since both A and A^{-1} have real entries, by Definition 25, we have shown that A is invertible over $\mathbb{R}$.

EXERCISE 42

Use Definition 25 to show that the matrix

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

is invertible over $\mathbb{R}$.

Solution. Let us calculate the inverse of A by the formula directly.

$$A^{-1} = \frac{1}{4-6}\begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

Now we can show that $AA^{-1} = I$:

$$AA^{-1} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Since both A and A^{-1} have real entries, by Definition 25, we have shown that A is invertible over $\mathbb{R}$.

EXERCISE 43

Use Definition 25 to show that the matrix

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

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

Solution. If we try to calculate the inverse of A as we did in previous problems, we can see that a problem arises:

$$A^{-1} = \frac{1}{4-4}\begin{bmatrix} 4 & -2 \\ -2 & 1 \end{bmatrix} = \frac{1}{0}\begin{bmatrix} 4 & -2 \\ -2 & 1 \end{bmatrix}$$

We see that A^{-1} is undefined. Thus, there does not exist a matrix B with real entries such that $AB = I$. By Definition 25, A is then not invertible.

EXERCISE 44

(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 25. Then find the determinant of each of your matrices.

Solution. Let

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 1 & 7 \\ 2 & 5 \end{bmatrix}, C = \begin{bmatrix} 1 & 3 \\ 5 & 7 \end{bmatrix}.$$

Each of these matrices has a corresponding inverse such that $AA^{-1} = I$, $BB^{-1} = I$, $CC^{-1} = I$:

$$A^{-1} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}, B^{-1} = \begin{bmatrix} -\frac{5}{9} & \frac{7}{9} \\ \frac{2}{9} & -\frac{1}{9} \end{bmatrix}, C^{-1} = \begin{bmatrix} -\frac{7}{8} & \frac{3}{8} \\ \frac{5}{8} & -\frac{1}{8} \end{bmatrix}$$

Thus, by Definition 25, each of these matrices are invertible over $\mathbb{R}$.
$\det(A) = (1 \cdot 4) - (2 \cdot 3) = 4 - 6 = -2$
$\det(B) = (1 \cdot 5) - (2 \cdot 7) = 5 - 14 = -9$
$\det(C) = (1 \cdot 7) - (3 \cdot 5) = 7 - 15 = -8$

(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 25. Then find the determinant of each of your matrices.

Solution. Let

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}, B = \begin{bmatrix} 1 & 3 \\ 3 & 9 \end{bmatrix}, C = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}.$$

Each of these matrices does NOT have a corresponding inverse. This is because we run into the same problem as Exercise 43, where it turns out that the inverse is undefined. Thus, there does not exist a matrix with real entries such that the product is the identity (for all three matrices). Therefore, by Definition 25, none of these matrices are invertible.
$\det(A) = (1 \cdot 4) - (2 \cdot 2) = 4 - 4 = 0$
$\det(B) = (1 \cdot 9) - (3 \cdot 3) = 9 - 9 = 0$
$\det(C) = (2 \cdot 6) - (3 \cdot 4) = 12 - 12 = 0$

(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. I conjecture that the determinant of a matrix with real entries that is invertible over $\mathbb{R}$ must be nonzero.

EXERCISE 45

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 $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Show that if $ad - bc = 0$, then A is not invertible.

Solution.

Let us first show that if $ad - bc \neq 0$, then A is invertible and $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. We can see that if $ad - bc \neq 0$, then we can show that $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ will satisfy the condition for invertibility:

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

Since there clearly exists a matrix B such that $AB = I$, then we have shown that A is invertible.

Let us now show that if $ad - bc = 0$, then A is not invertible. We can do so through proof by contradiction. Suppose A is indeed invertible. Then, $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. However, if $ad - bc = 0$, then the inverse is clearly undefined. This contradiction shows that A must be invertible.

EXERCISE 46

Use Definition 27 to show that the matrix

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

is invertible over $\mathbb{Z}$.

Solution. By Definition 27, a matrix A with integer entries is invertible over $\mathbb{Z}$ if there exists a matrix B with integer entries such that $AB = I$. Let us assume the matrix B takes the form

$$B = \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix}$$

The product AB evaluates to

$$AB = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}\begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} b_1 + 3b_2 & b_3 + 3b_4 \\ 4b_1 + 11b_2 & 4b_3 + 11b_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

From this product, we can form a system of equations and solve for the components of B.

$$\begin{cases} b_1 + 3b_2 = 1 \\ 4b_1 + 11b_2 = 0 \\ b_3 + 3b_4 = 0 \\ 4b_3 + 11b_4 = 1 \end{cases}$$

We find that the solution for this system is $b_1 = -11, b_2 = 4, b_3 = 3, b_4 = -1$. Thus,

$$B = \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix} = \begin{bmatrix} -11 & 3 \\ 4 & -1 \end{bmatrix}$$

Because $AB = I$ and B has all integer entries, A must be invertible over $\mathbb{Z}$ by Definition 27.

EXERCISE 47

Use Definition 27 to show that the matrix

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

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

Solution. By Definition 27, a matrix A with integer entries is invertible over $\mathbb{Z}$ if there exists a matrix B with integer entries such that $AB = I$. Let us assume the matrix B takes the form

$$B = \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix}$$

The product AB evaluates to

$$AB = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} b_1 + 2b_2 & b_3 + 2b_4 \\ 3b_1 + 4b_2 & 3b_3 + 4b_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

From this product, we can form a system of equations and solve for the components of B.

$$\begin{cases} b_1 + 2b_2 = 1 \\ 3b_1 + 4b_2 = 0 \\ b_3 + 2b_4 = 0 \\ 3b_3 + 4b_4 = 1 \end{cases}$$

We find that the solution for this system is $b_1 = -2, b_2 = \frac{3}{2}, b_3 = 1, b_4 = -\frac{1}{2}$. Thus,

$$B = \begin{bmatrix} b_1 & b_3 \\ b_2 & b_4 \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

Because B does not have all integer entries, A is not invertible over $\mathbb{Z}$.

EXERCISE 48

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. Let

$$A = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}, B = \begin{bmatrix} 4 & 1 \\ 1 & 0 \end{bmatrix}, C = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$$

(a) We find that the inverse of these matrices are:

$$A^{-1} = \begin{bmatrix} -11 & 3 \\ 4 & -1 \end{bmatrix}, B^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & -4 \end{bmatrix}, C^{-1} = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$$

Clearly, since each of these matrices have inverses that have all integer entries (and the matrices themselves also have all integer entries), they are all invertible over $\mathbb{Z}$ by Definition 27.

(b) $\det(A) = (1 \cdot 11) - (3 \cdot 4) = 11 - 12 = -1$
$\det(B) = (4 \cdot 0) - (1 \cdot 1) = 0 - 1 = -1$
$\det(C) = (2 \cdot 3) - (5 \cdot 1) = 6 - 5 = 1$

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

Exercise 49

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 results holds for more general $n \times n$ matrices with entries in $\mathbb{Z}$.

Solution. For a matrix A to be invertible over $\mathbb{Z}$, it is necessary that $A, A^{-1} \in \mathbb{Z}$ and $AA^{-1} = I$. Let us also make use of the fact that the determinant is multiplicative. Thus, we can also say that

$$\det(A) \cdot \det(A^{-1}) = \det(AA^{-1}) = \det(I) = 1$$
$$\det(A)\det(A^{-1}) = 1$$

From this, we see that

$$\det(A) = \frac{1}{\det(A^{-1})}$$

We know that both $\det(A)$ and $\det(A^{-1})$ must be integer values (since A and A^{-1} have all integer entries). Moreover, the only integers that have a multiplicative inverse that is also integer are ± 1. Thus, a matrix A must have $\det(A) = \pm 1$ for it to be invertible over $\mathbb{Z}$.

Now let us prove the other direction. If $\det(A) = ad - bc = \pm 1$, then

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{\pm 1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

By construction, $a, b, c, d \in \mathbb{Z}$. Dividing by ± 1 still yields integer values, meaning A^{-1} is an inverse matrix with all integer entries and A is invertible over $\mathbb{Z}$. Thus, we conclude that A is invertible over $\mathbb{Z}$ if and only if $\det(A) = \pm 1$.

EXERCISE 50

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

Solution. For a real number x to have a multiplicative inverse in $\mathbb{R}$, it must satisfy the condition $x \cdot \frac{1}{x} = 1$. The only number that does not satisfy this condition is 0, since $\frac{1}{0}$ is undefined. Every other real number's inverse is defined, meaning that all real numbers (other than zero) have a multiplicative inverse in $\mathbb{R}$.

EXERCISE 51

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

Solution. We know that since $\frac{1}{0}$ is undefined, 0 does not have a multiplicative inverse. Let us assume that there exists integers a, b such that $a \neq 0$, $b \neq 0$, and $ab = 1$. Because a and b are nonzero integers, their absolute value must be at least 1. If $|a|$ or $|b|$ are > 1, then it is impossible for $ab = 1$, since $ab = 1 = |ab| = |a||b|$ (an integer >1 multiplied by an integer that is ≥1 must be >1). Thus, the only integers with a multiplicative inverse that is also an integer are {1,-1}.

EXERCISE 52

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. Below are my three bases:

$$\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}, \left\{\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}3\\4\end{bmatrix}\right\}, \left\{\begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}3\\11\end{bmatrix}\right\}$$

(a) We know that a set is a basis of $\mathbb{R}$ if the two vectors are linearly independent and any arbitrary vector in $\mathbb{R}$ can be expressed as a linear combination of the two vectors. The first set is essentially just the identically matrix, which we know to have linearly independent columns. We know from Exercises 38 and 41 that the other two sets are linearly independent. Moreover, we can clearly express any arbitrary vector through a linear combination of the two vectors in each basis (since we are allowed to have non-integer scalar constants in our linear combo).

(b) Let

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}, C = \begin{bmatrix} 1 & 3 \\ 4 & 11 \end{bmatrix}$$

We calculate the determinants to be

$$\det(A) = 1, \det(B) = -2, \det(C) = -1$$

(c) I conjecture that the determinants of all matrices whose columns form a basis in $\mathbb{R}$ must be non-zero. In order for the columns to form a basis in $\mathbb{R}$, these columns have to be invertible. This is because, by definition of a basis, there exists a c_1 and c_2 such that

$$c_1 \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} + c_2 \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and there exists a d_1 and d_2 such that

$$d_1 \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} + d_2 \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

This corresponds to the equation

$$\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix} \begin{bmatrix} c_1 & d_1 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, by definition,

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

is invertible. We know from Exercise 45 that a 2x2 invertible matrix must have a non-zero determinant.

EXERCISE 53

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. Below are my three bases:

$$\left\{\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right\},\left\{\begin{bmatrix}1\\4\end{bmatrix},\begin{bmatrix}3\\11\end{bmatrix}\right\},\left\{\begin{bmatrix}1\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right\}$$

(a) We already know that the first two bases are linearly independent from previous exercises. It is also easy to show that the third basis has linearly independent vectors (since the only solution to the system of equations $x=0, x+y=0$ is the trivial solution). Now let us show that we can express any arbitrary vector $\begin{bmatrix}x\\y\end{bmatrix}$ can be expressed as a linear combination of our basis vectors:

1. $\begin{bmatrix}x\\y\end{bmatrix}=x\begin{bmatrix}1\\0\end{bmatrix}+y\begin{bmatrix}0\\1\end{bmatrix}$
2. $\begin{bmatrix}x\\y\end{bmatrix}=c_1\begin{bmatrix}1\\4\end{bmatrix}+c_2\begin{bmatrix}3\\11\end{bmatrix}=(-11x+3y)\begin{bmatrix}1\\4\end{bmatrix}+(4x-y)\begin{bmatrix}3\\11\end{bmatrix}$
   We also know that x and y are integers by construction, so the second example is indeed a $\mathbb{Z}$-basis of $\mathbb{Z}$.
3. $\begin{bmatrix}x\\y\end{bmatrix}=c_1\begin{bmatrix}1\\0\end{bmatrix}+c_2\begin{bmatrix}1\\1\end{bmatrix}=(x-y)\begin{bmatrix}1\\0\end{bmatrix}+y\begin{bmatrix}1\\1\end{bmatrix}$
   We also know that x and y are integers by construction, so the second example is indeed a $\mathbb{Z}$-basis of $\mathbb{Z}$.

(b) Let

$$A=\begin{bmatrix}1&0\\0&1\end{bmatrix},B=\begin{bmatrix}1&3\\4&11\end{bmatrix},C=\begin{bmatrix}1&1\\0&1\end{bmatrix}$$

We calculate the determinants to be

$$\det(A)=1,\det(B)=-1,\det(C)=1$$

(c) I conjecture that the determinant of a matrix whose columns form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ must be ±1. Let us first prove that a matrix must be invertible over $\mathbb{Z}$ for its columns to form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$. Let the columns of the matrix

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

form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$. We know that we can form any arbitrary vector $\begin{bmatrix}x\\y\end{bmatrix}$ using the columns of our matrix. Using this property of a basis, we can form the following equations:

$$c_1\begin{bmatrix}v_1\\v_2\end{bmatrix}+c_2\begin{bmatrix}w_1\\w_2\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}$$
$$d_1\begin{bmatrix}v_1\\v_2\end{bmatrix}+d_2\begin{bmatrix}w_1\\w_2\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}$$

for some $c_1, c_2, d_1, d_2 \in \mathbb{Z}$. This corresponds to the equation

$$\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix} \begin{bmatrix} c_1 & d_1 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, by definition,

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

is invertible over $\mathbb{Z}$. In Exercise 49, we showed that a matrix invertible over $\mathbb{Z}$ must have a determinant of ± 1. Thus, by showing that a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ must be invertible over $\mathbb{Z}$, we have also shown (by Exercise 49) that the determinant of a matrix whose columns form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ must be ± 1.

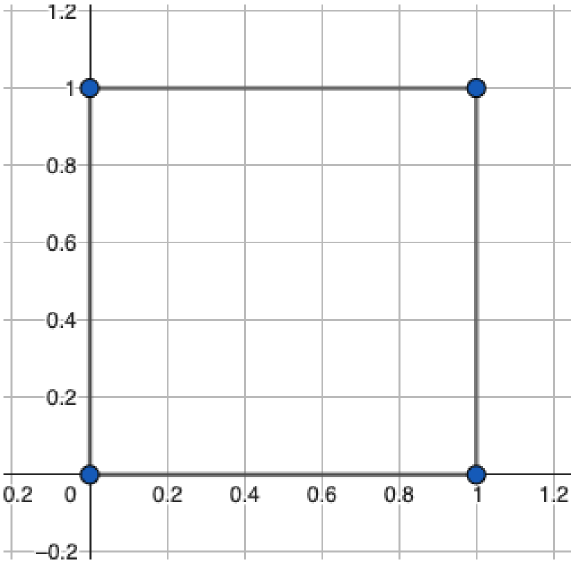
EXERCISE 54

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

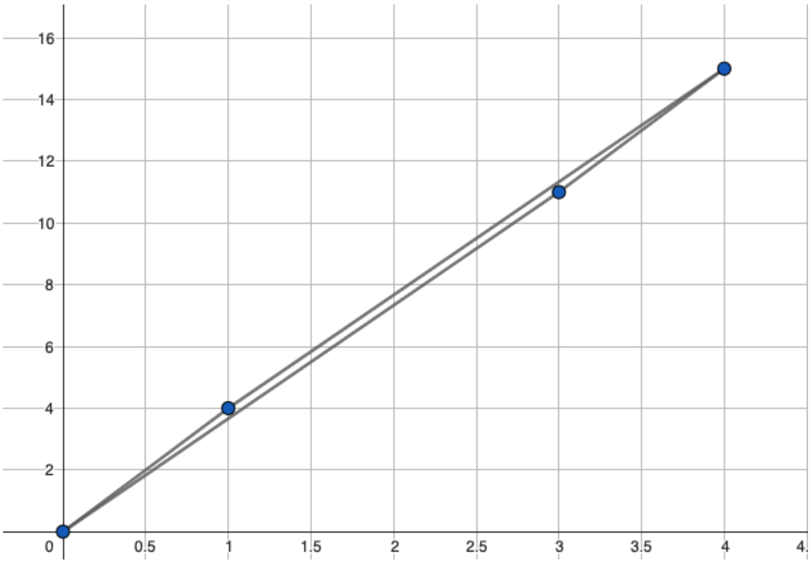
(a) Find the area of the parallelogram spanned by each of the $\mathbb{Z}-$bases for $\mathbb{Z}^2$ that you constructed in Exercise 53.

(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 $\mathbb{Z}^2$.

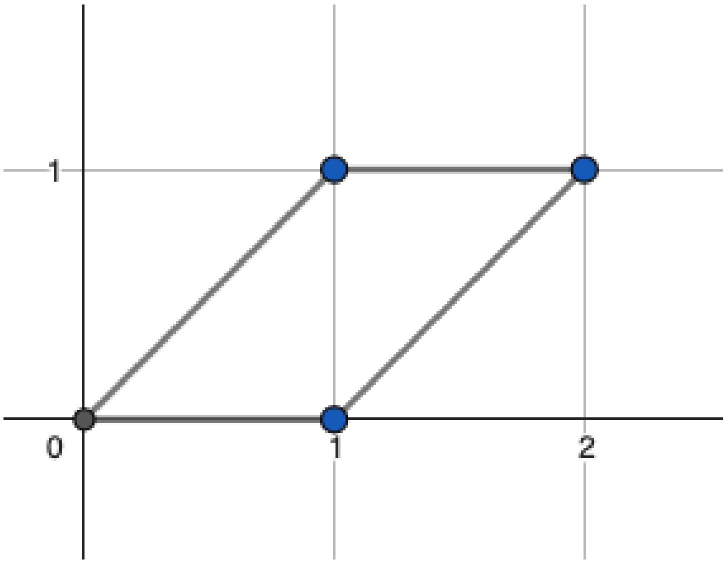
Solution.



The parallelogram formed by the basis vectors $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$



The parallelogram formed by the basis vectors $\begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}3\\11\end{bmatrix}$



The parallelogram formed by the basis vectors $\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}$

(a) There are various ways to find the area of these parallelograms, such as taking the determinant or breaking up the area of the encompassing rectangle into rectangles and triangles to find the area of the parallelogram. My personal calculation used the former, and yielded that the area of each of these parallelograms is 1.

(b) I conjecture that the area of every lattice parallelogram $P(\mathbf{v},\mathbf{w})$ where vectors $\mathbf{v},\mathbf{w}$ form a basis of $\mathbb{Z}^2$ is 1. We know the area is equal to $\left|\det\left(\begin{bmatrix}v_1 & w_1\\ v_2 & w_2\end{bmatrix}\right)\right|$ and that the determinant of any matrix whose columns form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ is 1.

EXERCISE 55

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

(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. See Exercise 54 for the sketched out parallelograms.

(a) We can see that there are four lattice points on the sides of the parallelogram (if we count the vertices) and zero lattice points in the interior.

(b) I conjecture that any vector lattice parallelogram with vectors that form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$, $B(P) = 4$ and $I(P) = 0$.

Suppose there exists a vector with endpoints at the origin and a non-vertex lattice point such that $\mathbf{u} \in P(\mathbf{v},\mathbf{w})$. We know that $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$, so they must also be linearly independent. Because they are linearly independent, we can represent $\mathbf{u}$ as some linear combination, say

$$c_1\mathbf{v} + c_2\mathbf{w}$$

where $c_1, c_2 \in \mathbb{Z}$. Moreover, since we know that $\mathbf{u} \in P(\mathbf{v},\mathbf{w})$,

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

where $a, b \in \mathbb{R}$ and $0 < a, b < 1$ (since $\mathbf{u}$ cannot possibly be outside our parallelogram). Subtracting these two equations yields

$$\vec{0} = (c_1 - a)\mathbf{v} + (c_2 - b)\mathbf{w}$$

Because we know that both $\mathbf{v}$ and $\mathbf{w}$ are linearly independent, we also know that the only solution that can allow the linear combination of these two vectors to be equal to $\vec{0}$ is the trivial solution. Thus, $c_1 - a = c_2 - b = 0$ and $c_1 = a$, $c_2 = b$. This yields a contradiction, since c_1 and c_2 are integers but $0 < a, b < 1$. This means there does not exist a vector with endpoints at the origin and a non-vertex lattice point in $P(\mathbf{v},\mathbf{w})$. By extension, there are no lattice points in $P(\mathbf{v},\mathbf{w})$ that are not the vertices. This means that the only lattice points are the four vertices, which are boundary points, and no interior points.

EXERCISE 56

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. Firstly, because $\mathbf{v}, \mathbf{w}$ form a valid parallelogram, they must be linearly independent in $\mathbb{R}^2$ (and also non-co-linear by extension).

Let us now take an arbitrary vector $\mathbf{u} \in \mathbb{Z}^2$. Because it has been established that $\mathbf{v}, \mathbf{w}$ form a basis for $\mathbb{R}^2$, we can express $\mathbf{u}$ as some linear combination $\mathbf{u} = c_1\mathbf{v} + c_2\mathbf{w}$. To prove that $\mathbf{v}, \mathbf{w}$ form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$, we must show that $c_1, c_2 \in \mathbb{Z}$.

Let us take the vector $\mathbf{u}'$ such that $\mathbf{u}' = (c_1 - \lfloor c_1 \rfloor)\mathbf{v} + (c_2 - \lfloor c_2 \rfloor)\mathbf{w})$. We know that $0 \leq c_1 - \lfloor c_1 \rfloor, c_2 - \lfloor c_2 \rfloor < 1$. We can also express $\mathbf{u}'$ in the form

$$\mathbf{u}' = \mathbf{u} - \lfloor c_1 \rfloor \mathbf{v} - \lfloor c_2 \rfloor \mathbf{w}$$

We know that $\mathbf{u}, \mathbf{v}, \mathbf{w}, \lfloor c_1 \rfloor, \lfloor c_2 \rfloor \in \mathbb{Z}$. Thus, $\mathbf{u}'$ is just a difference of integers and is in $\mathbb{Z}$. We know that $\mathbf{u}'$ is also in the parallelogram because it is a linear combination of $\mathbf{v}, \mathbf{w}$ with constants less than one and greater than or equal to zero. However, we showed in Exercise 55 that the only lattice points within a primitive lattice polygon must be one of its vertices. Considering the bounds we set earlier, $0 \leq c_1 - \lfloor c_1 \rfloor, c_2 - \lfloor c_2 \rfloor < 1$, $\mathbf{u}'$ must be the zero vector. Therefore, $c_1 = \lfloor c_1 \rfloor, c_2 = \lfloor c_2 \rfloor$. This means that $c_1, c_2 \in \mathbb{Z}$ and that we have shown $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$.

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 57

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. Let us denote the primitive triangle T, which is made up of the vectors $\mathbf{v}$ and $\mathbf{w}$, which form its adjacent sides. The line segment connecting the tips of these two vectors makes up the final side of the triangle. Because T is a primitive triangle, we know that this line segment does not contain any lattice points (aside from its endpoints).
Let the lattice parallelogram $P(\mathbf{v}, \mathbf{w})$ be spanned by $\mathbf{v}$ and $\mathbf{w}$, and consist of the two triangles T' and T where T' is just a reflection of triangle T. More specifically, T' is simply just a rotation of T by 180 degrees about the line segment connecting the endpoints of $\mathbf{v}$ and $\mathbf{w}$.
We know none of the sides of T' contain any boundary points, since none of the sides of T have boundary points either. Because T' was constructed through a rotation, any interior lattice point (x, y) in T' must reflect onto the area of T. This interior lattice point is not a vertex,

so a contradiction arises (since T is primitive and, by definition, does not have any interior lattice points). From this contradiction, we know that $P(\mathbf{v},\mathbf{w})$ has no interior lattice points. Therefore, since it has 4 boundary lattice points and 0 interior lattice points, $P(\mathbf{v},\mathbf{w})$ is primitive. By Theorem 1, we know that the vectors which make up a primitive parallelogram $P(\mathbf{v},\mathbf{w})$ form a $\mathbb{Z}$-basis of $\mathbb{Z}^2$. Thus, the vectors $\mathbf{v}$ and $\mathbf{w}$ form a $\mathbb{Z}$-basis of $\mathbb{Z}^2$.

EXERCISE 58

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

Solution. We know from Exercise 57 that the vectors which form the adjacent edges of a primitive lattice triangle T also form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$. By Theorem 1, we know that the vectors $\mathbf{v}$ and $\mathbf{w}$ also span a primitive parallelogram. From Exercise 52, we found that the area of a primitive lattice parallelogram $P(\mathbf{v},\mathbf{w})$ is 1. By construction, T has half the area of P. Therefore, T has an area of $\frac{1}{2}$.

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 59

Prove Theorem 3.

Solution. We can dissect any convex n-gon into $n-2$ triangles bu selecting any vertex v, and forming a triangulation with all other non-adjacent vertices. For vertex v_1, that means there are $n-3$ possible non-intersecting diagonals we can draw (these diagonals will not intersect because the n-gon is convex). Let the adjacent vertices of v_1 be denoted as v_2 and v_n. Each diagonal that connects v_1 with $v_3, v_4, ..., v_{n-1}$ forms a triangle. Thus, there are $n-3$ triangles in this triangulation. However, the final diagonal (v_1 and v_{n-1}) actually forms an additional triangle with the sides $v_1 \to v_n$, $v_1 \to v_{n-1}$, and $v_n \to v_{n-1}$. Thus, there are $n-2$ triangles in this triangulation. With this, we have shown that every convex n-gon can be dissected into $n-2$ triangles.

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 60

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

Solution. Let us approach this problem through proof by induction. Firstly, let us define P as some polygon with n sides and vertices.

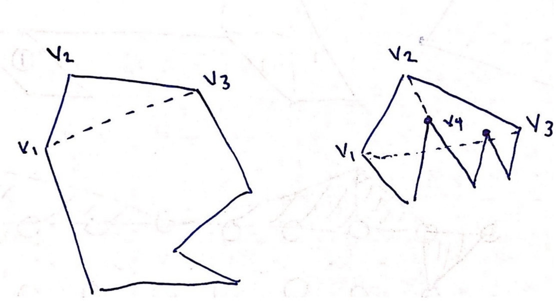
Base Case: For $n = 3$, clearly P is a triangle and it can be dissected into $n-2 = 3-2 = 1$ triangle.

Inductive Step: Our inductive hypothesis is that any polygon P_n with n sides can be dissected into $n-2$ triangles by means of nonintersecting diagonals. To prove that this holds true for P_{n+1} requires us to first show that every polygon P has a diagonal.

Assume $n \geq 4$ (since we have already proven the case of $n = 3$). Let us take the arbitrary adjacent vertices v_1, v_2, and v_3 (the vertices are joined such that v_1 connects to v_2 and v_2 connects to v_3. If we take the segment $\overline{v_1 v_3}$, there are several possible cases:

1) If $\overline{v_1 v_3}$ lies completely within the polygon, then it is by definition a diagonal of P.

2) If $\overline{v_1 v_3}$ is outside the polygon, then that means there must lie some vertex v_4 such that v_4 lies within the area bounded by v_1, v_2, v_3 (in the event that more than one vertex lies within this area, let us just take v_4 to be the vertex closest to v_2, in terms of Euclidean distance). The line segment $\overline{v_2 v_4}$ is then a diagonal of P by definition, since it is completely within P.



Thus, we have shown that every polygon P has a diagonal.

For a polygon with $n+1$ vertices, we can then claim that it must have some diagonal d. This diagonal splits P_{n+1} into two different polygons, P_a and P_b. By definition, the diagonal d splits P_{n+1} by connecting two previously non-connected vertices. That means, there is at least one vertex (other than the two endpoints of d) in each of the polygons P_a and P_b. This vertex can be found by using the original edges and vertices of P_{n+1}. Thus, $x, y \geq 3$.

By our inductive hypothesis, we can dissect P_a and P_b into $a-2$ and $b-2$ triangles respectively. Thus, we have shown that there are

$$(a-2)+(b-2)=(a+b)-4$$

triangles in P_{n+1}. Recall that both P_a and P_b share only the endpoints of d as vertices. Thus, if we try to represent $n+1$ in terms of a and b, adding a and b would result in two of their vertices being over-counted. This means that $a+b=(n+1)+2$. Substituting this relation into our above expression gives

$$a+b-4=n+1+2-4=(n+1)-2$$

Thus, we have shown that every n-gon can be dissected into $n-2$ triangles with non-intersecting diagonals.

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

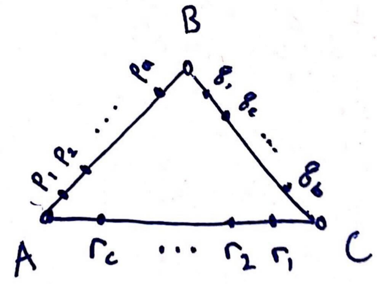
Every lattice triangle can be dissected into primitive lattice triangles.

EXERCISE 61

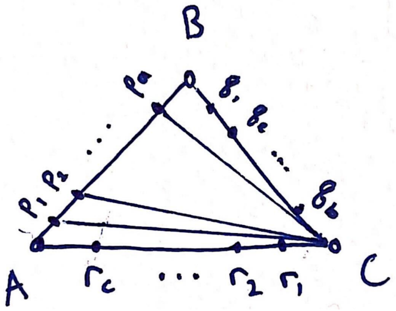
Prove Lemma 1. Hint: induction on the number of interior lattice points in the lattice triangle.

Solution. We can go about this problem through proof by induction on the number of interior lattice points in the lattice triangle.

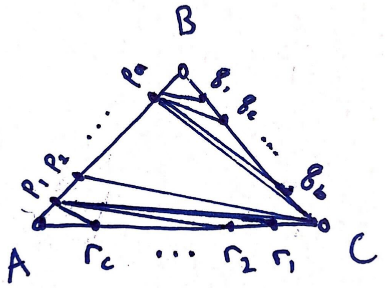
Base Case: Let T be a lattice triangle with no interior points. Let A, B, and C be the vertices of T, and let $p_1, p_2, p_3, ..., p_a$ and $q_1, q_2, ..., q_b$, and r_1, r_2, r_c denote the arbitrary non-vertex boundary points on each side of T.



If we pick any vertex of T, say C, and draw lines to all the boundary points on the opposite side, we produce a set of primitive lattice triangles (and the edges are still just normal lattice triangles).



From here, we still have to dissect the triangles formed by A, p_1, C and p_a, B, C. This can be done by connecting p_1 to all r_1 through r_c, and connecting p_a to all q_1 through q_b like so:



Clearly, since all these triangles have 3 boundary points and no interior points (T had no interior points by construction), they are all primitive. This concludes our proof for the base case.

Inductive Step: Suppose every triangle with $\leq k$ lattice points in its interior can be dissected into primitive lattice triangles. Let T be a triangle with $k+1$ interior points. Selecting an interior lattice point and connective it to each of the vertices ensures that we have dissected T into 3 lattice triangles with $\leq k$ interior points. By our inductive hypothesis, we know that each of these triangles can be separately dissected into primitive lattice triangles. Then, by extension, we have shown that T itself can be dissected into primitive lattice triangles as well.

THEOREM 5

Every lattice polygon can be dissected into primitive lattice triangles.

EXERCISE 62

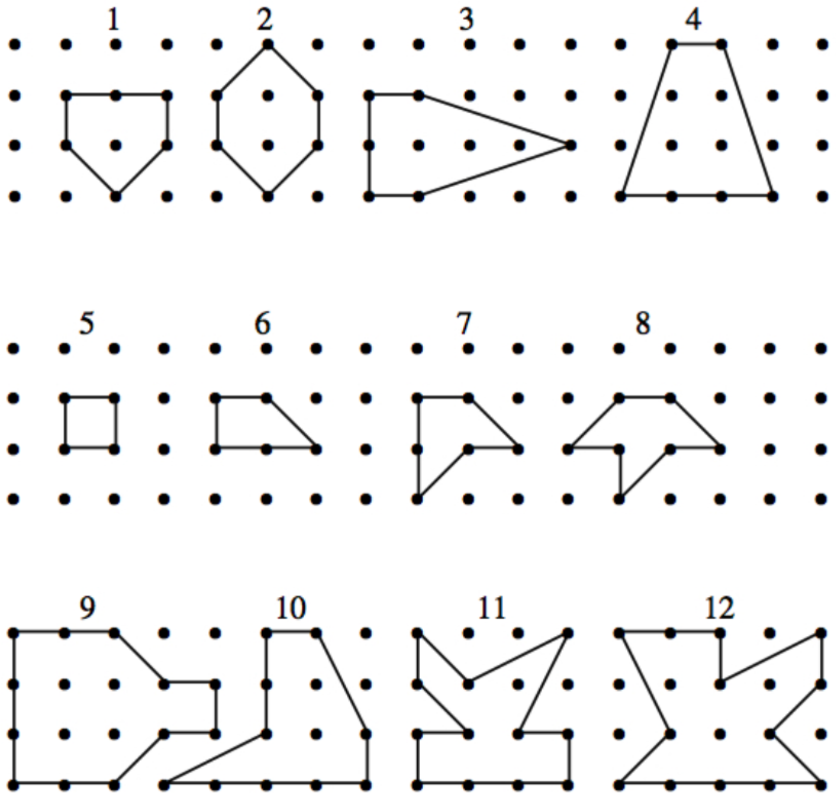
Prove Theorem 5.

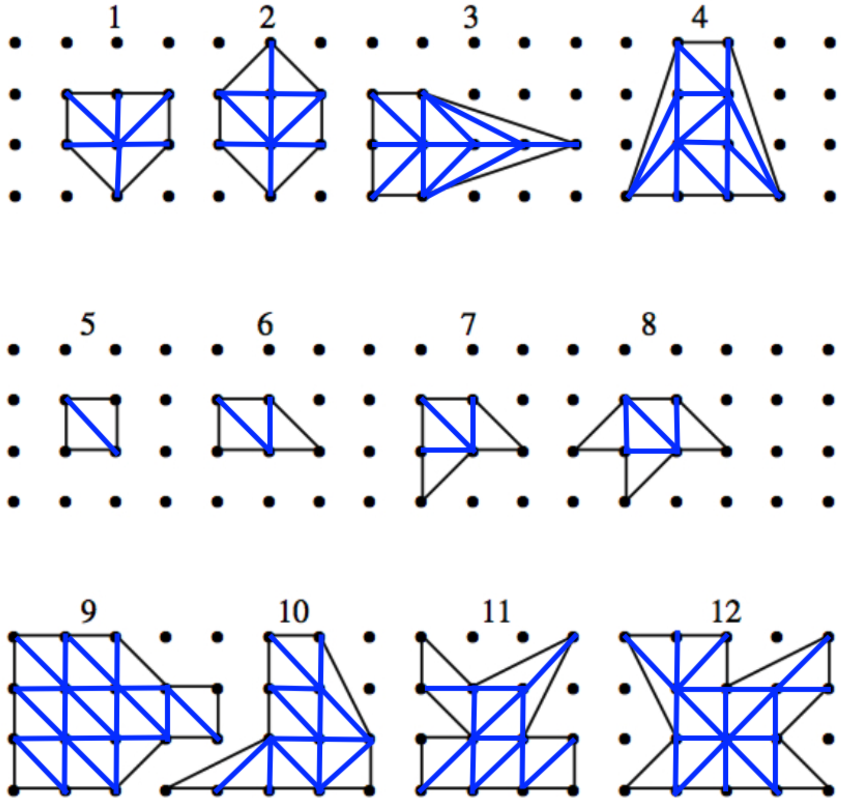
Solution. We know from Exercise 60 that every n-gon can be dissected into $n-2$ triangles by means of non-intersecting diagonals. Every lattice polygon is an n-gon itself. Thus, every lattice n-gon can be dissected into $n-2$ triangles by means of non-intersecting diagonals. Each vertex of the n-gon is a lattice point. Because the diagonals were created using the vertices, each of the generated triangles must also be a lattice triangle.

We know from Exercise 61 that every lattice triangle can be dissected into primitive lattice triangles. Thus, we can dissect every lattice triangle on the lattice n-gon that was generated using the theorem proved in Exercise 60 into primitive lattice triangles. This shows that every lattice polygon can be dissected into primitive lattice triangles.

EXERCISE 63

Dissect the twelve lattice polygons in Figure 2 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 64.





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 30

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 31 Planar Graph.

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 3 contains 5 regions.

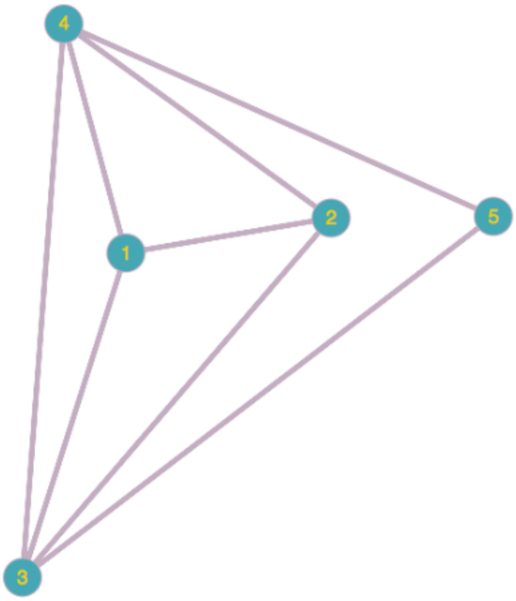


Figure 3: An example of a planar graph with 5 regions.

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 64

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 2. For each of the polygons in Figure 2, use your dissection into primitive lattice triangles from Exercise 63 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?

Solution.

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

We can observe that f is equal to $2v - e_b - 1$.

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 65

Use Exercise 58 to state and prove an equation that relates the area of P to f.

Solution. We know from Exercise 58 that the area of every primitive lattice triangle is going to be $\frac{1}{2}$. We know from Theorem 5 that every lattice polygon can be dissected into primitive lattice triangles. Thus, the area of a lattice polygon P can be represented as

$$A(P) = \frac{1}{2} \cdot m$$

Where m is the number of primitive lattice triangles in P. If we represent P as a graph, the number of regions of the graph G is one more than the number of primitive lattice triangles. Thus, $m = f - 1$. If we substitute this back into our above formula for $A(P)$,

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

EXERCISE 66

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. We know that there are $f - 1$ primitive triangles in P. Thus, there are a total of $3(f - 1)$ sides of these triangles.

Each of the e_i interior edges in G borders two interior triangles. Each of the outer e_b edges borders one triangle. Thus,

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

If we apply Euler's formula to this relation, (and using the fact that $e_i + e_b = e$) we obtain:

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

Thus, we obtain that

$$\begin{aligned} 3(f - 1) &= 2(f + v - 2) - e_b \\ f &= 2v - 4 + 3 - e_b \\ f &= 2v - e_b - 1 \end{aligned}$$

EXERCISE 67

Finally, show that

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

This concludes the proof of Pick's Theorem!

Solution. Let us substitute the expression for f from Exercise 66 into the formula we obtained in Exercise 65 to obtain the following:

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

We also know that $v = I(P) + B(P)$ and $B(P) = e_b$, so:

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

Thus, we have proved Pick's Theorem.

EXERCISE 79

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

Solution. The known formula for the area of an equilateral triangle T is

$$A(T) = \frac{\sqrt{3}}{2}s^2$$

Where s is the side length of a triangle. Because we know that s^2 must be positive and rational (side length cannot be imaginary) and $\sqrt{3}$ is irrational, we know that the equilateral triangle always has an irrational area.

We know from Pick's Theorem that the area of any lattice polygon (and by extension any lattice triangle)

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

This is always rational, as $I(T)$ and $B(T)$ must be counting numbers. This is a contradiction. Thus, it is impossible to construct an equilateral lattice triangle.

EXERCISE 80

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. Using Pick's Theorem, and the fact that a primitive lattice triangle T has $B(T) = 3$ and $I(T) = 0$

$$A(T) = \frac{3}{2} - 0 - 1 = \frac{1}{2}$$

EXERCISE 81

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.

Solution. Recall that Pick's Theorem states the area $A(P)$ of any lattice polygon P is

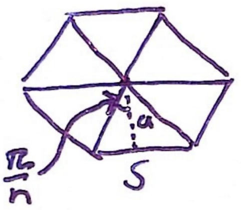
$$A(P) = \frac{1}{2}B(P) + I(P) - 1$$

where $B(P)$ is the number of boundary lattice points on P and $I(P)$ is the number of interior lattice points in P. Given that $B(P)$ and $I(P)$ are counting numbers, it follows that $A(P)$ will always be rational (more specifically, a multiple of $\frac{1}{2}$).

Let P be some regular lattice n-gon. By the above reasoning, $A(P)$ will be rational. Let us calculate the area of P a different way. We can start by examining the properties of s, the side length of P. We can find s by taking the distance between two vertices (x_1, y_1) and (x_2, y_2) where all the coordinates are integers (since the vertices are lattice points by construction).

$$s = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

We can see that s turns out to be the square root of some integer. Thus, s^2 will turn out to be some integer. This will be important later.



Example of the dissection for $n = 6$

Suppose we dissect P into n triangles by connecting the central point with the vertices of the n-gon. In each triangle, the angle corresponding to the central point has a value of $\frac{2\pi}{n}$. To find the area of this triangle, we can multiply the base and the height (a.k.a. the apothem). Note that angle formed by the apothem and the outer edge of triangle is $\frac{1}{2}\frac{2\pi}{n} = \frac{\pi}{n}$. Thus, the apothem can be found like so

$$a = \frac{\frac{s}{2}}{\tan(\frac{\pi}{n})} = \frac{s}{2\tan(\frac{\pi}{n})}$$

Finally, the area of P can be represented as n times the area of each triangle:

$$A(P) = n \cdot \frac{1}{2} \cdot s \cdot \frac{s}{2\tan(\frac{\pi}{n})} = \frac{s^2 n}{4\tan(\frac{\pi}{n})}$$

Recall also that $A(P) = \frac{1}{2}B(P) + I(P) - 1$. This gives way to the following equality:

$$\frac{1}{2}B(P) + I(P) - 1 = \frac{s^2 n}{4\tan(\frac{\pi}{n})}$$

We found that s^2 is positive and rational. n must also be positive and rational, since it's a counting number. We know that the LHS is rational. Thus, $\tan(\frac{\pi}{n})$ must also be rational (since the product of a rational and an irrational cannot possibly be rational).

EXERCISE 82

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. By Pick's Theorem, the area of the convex pentagon is $A(P) = \frac{B(P)}{2} + I(P) - 1$ where $B(P) \geq 5$. The area $A(P)$ will be $\geq \frac{5}{2}$ if $B(P) \geq 7$ or $I(P) \geq 1$.

Let us prove that $I(P) \geq 1$ through midpoints. The midpoint $M_{i,j}$ of two vertices (x_i, y_i) and (x_j, y_j) is

$$M_{i,j} = \left(\frac{x_i + x_j}{2}, \frac{y_i + y_j}{2}\right)$$

This midpoint will be a lattice point if $x_i + x_j$ and $y_i + y_j$ are even. This occurs when x_i has the same parity as x_j (and y_i has the same parity as y_j). Thus, there are 2^2 possible parity choices: (even, even), (even, odd), (odd, even), and (odd, odd). There are 5 vertices to choose from. Then, by the PHP, there must be at least two vertices which have the same parity. Thus, we can claim that the midpoint of two vertices v_1 and v_2 must be a lattice point M.

This midpoint M could be either between two adjacent vertices or two non-adjacent vertices.

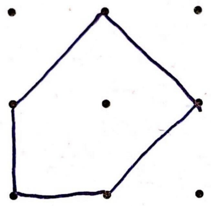
> *Case 1:* In the case that v_1 and v_2 are non-adjacent vertices, this means their midpoint lies within P (since P is convex). Because M is a lattice point that lies within the pentagon, it is an interior lattice point. Then, by Pick's Theorem,
>
> $$A(P) \geq \frac{5}{2} + 1 - 1 \geq \frac{5}{2}$$
>
> *Case 2:* In the case that v_1 and v_2 are adjacent vertices, the midpoint M is a boundary lattice point (since P is convex, M must lie on the segment $\overline{v_1 v_2}$). Let us then form a new pentagon P' with the vertices v_1, v_3, v_4, v_5, M. From here, we can repeat the argument that there must exist a midpoint between two vertices of P' that is a lattice point.

This new midpoint, M' must either be an interior lattice point of the original pentagon P or another unique boundary point of P (because we used M as one of the vertices in P', it is impossible for $M = M'$).

If M' is an interior lattice point: $I(P) \geq 1 \Rightarrow A(P) \geq \frac{6}{2} + 1 - 1 \geq \frac{6}{2}$

If M' is a boundary lattice point: $B(P) \geq 5 + 2 = 7 \Rightarrow A(P) \geq \frac{7}{2} + 0 - 1 \geq \frac{5}{2}$

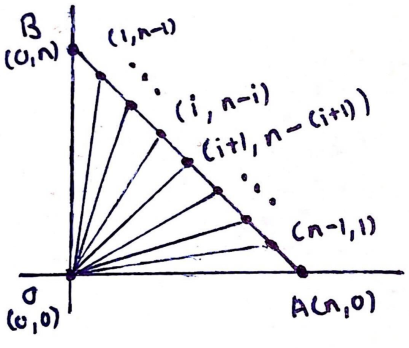
Thus, we have proven that the area of P must be greater than or equal to $\frac{5}{2}$. It is indeed possible to construct a convex lattice pentagon with an area equal to $5/2$. See the example below.



Exercise 83

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.



Firstly, note that $\gcd(i, n-i) = 1$. This is because if $\gcd(i, n-i) = d \neq 1$, the sum $i+n-i$ would be divisible by $d \neq 1$. This implies that $n|d$, which is a contradiction (since n is prime). Now, we can use Exercise 29 to claim that there are no lattice points that lie on the line between $(0,0)$ and $(i, n-i)$. This means that each triangle on the inside of ΔOAB has only 3 boundary points.

Now, we must find the area of each of the small triangles. Let v_i be the vector from $(0,0)$ to $(i, n-i)$. Thus, the area of a triangle $\Delta Ov_{i-1}v_i$ is

$$A(\Delta Ov_{i-1}v_i) = \frac{||v_{i-1} \times v_i||}{2} = \frac{1}{2}|(i-1(n-i)) - (i(n-i+1))| = \frac{n}{2}$$

Therefore, every one of the small triangles has the same area. Now, let us apply Pick's Theorem. We know that each of the areas of the triangles is the same. We also know that each of the "middle" triangles has $B(P) = 3$. The only other variable in Pick's Theorem is $I(P)$. Thus, $I(P)$ must also remain constant across all the middle triangles. To derive an expression for the number of interior lattice points, we can just solve for $I(P)$ in Pick's Theorem:

$$I(\Delta Ov_{i-1}v_i) = A(\Delta Ov_{i-1}v_i) - \frac{1}{2}B(\Delta Ov_{i-1}v_i) + 1 = \frac{n}{2} - \frac{3}{2} + \frac{2}{2} = \frac{n-1}{2}$$

EXERCISE 84

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. Let us take the set of lattice points that lie on the parabola $y = x^2$ in the domain $x \geq 0$. We know that none of these points are co-linear to each other. Thus, any three points in the set can form a non-degenerate triangle. By Pick's Theorem, the area of this arbitrary triangle will be rational. The distance between the two points (a, a^2) and (b, b^2) can be found through the distance formula

$$\begin{aligned} d &= \sqrt{(a-b)^2 + (a^2-b^2)^2} \\ &= \sqrt{(a-b)^2 + ((a+b)(a-b))^2} \\ &= (a-b)\sqrt{1+(a+b)^2} \end{aligned}$$

Note that $(a+b)^2$ must be a perfect square, as a and b are integers. Thus, we know that $\sqrt{1+(a+b)^2}$ cannot possibly be a perfect square, as no perfect squares have a difference of 1. The only exception to this case is when $(a+b)^2 = 0$. This only occurs when $a = -b$, which is impossible because we are working in the domain $x \geq 0$. Therefore, the set of lattice points that lie on the parabola $y = x^2, x \geq 0$ form a set of infinitely many points $(n \geq 3)$ such that the distance between any two points is irrational and each set of three points determines a non-degenerate triangle with rational area.

EXERCISE 85

Show that if T is a lattice triangle with $I(T) = 1$, then $B(T) = 3, 4, 6, 8,$ or 9.

Solution. Let T be a lattice triangle such that $I(T) = 1$ and (without loss of generality) be determined by the vertices $(0,0)$, (a_1, a_2), and (b_1, b_2). By Pick's Theorem, the area of such a triangle is

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

Let a, b, c be defined as the gcd of the differences in each coordinate:

$$\begin{aligned} a &= gcd(a_1 - 0, a_2 - 0) = gcd(a_1, a_2) \\ b &= gcd(b_1 - 0, b_2 - 0) = gcd(b_1, b_2) \\ c &= gcd(a_1 - b_1, a_2 - b_2) \end{aligned}$$

By Exercise 32, we have

$$B(T) = a + b + c$$

Now, let us first prove that ab, ac, and bc are divisors of $B(T)$. We can do so by first computing the area of T in two different ways. Firstly, we have by Pick's Theorem that

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

Next, we can represent $A(T)$ through the cross product:

$$A(T) = \frac{1}{2}|a_1b_2 - a_2b_1|$$

Let us now rewrite the expression for $A(T)$ with the cross product as

$$\begin{aligned} A(T) &= \frac{1}{2}|a_1b_2 - a_2b_1| \\ &= \frac{1}{2}(ab)\left|\frac{a_1b_2}{ab} - \frac{a_2b_1}{ab}\right| \\ &= \frac{1}{2}(ab)k = \frac{1}{2}B(T) \end{aligned}$$

for some integer k. We know the term $\left|\frac{a_1b_2}{ab} - \frac{a_2b_1}{ab}\right|$ will be an integer because a and b are the gcd's of (a_1, a_2) and (b_1, b_2) respectively. Thus, we have shown that $ab|B(T)$. We can use analogous arguments to show that $ac|B(T)$ and $bc|B(T)$. This also implies that $a|B(T)$, $b|B(T)$, and $c|B(T)$.

Recall that $B(T) = a + b + c$. W.l.o.g, assume $a \geq b \geq c$. We know that

$$a \geq \frac{1}{3}B(T)$$

because a, b, c add up to $B(T)$ and a is the largest of them. If $a < \frac{1}{3}B(T)$, it would be impossible for a, b, c to add up to $B(T)$. Moreover, we know that $a|B(T)$, which implies there is some integer k such that $a = \frac{B(T)}{k}$. However, because $a \geq \frac{1}{3}B(T)$, the only possible values of a are:

$$a = \frac{B(T)}{3} \text{ or } \frac{B(T)}{2} \text{ or } \frac{B(T)}{1}$$

It is impossible for $a = \frac{B(T)}{1}$, as that would imply $b = c = 0$ (which is impossible because b and c are gcd's). Thus, we have

$$a = \frac{1}{2}B(T) \text{ or } \frac{1}{3}B(T)$$

Let us split up these two possible cases.

> *Case 1:* If $a = \frac{1}{3}B(T)$, we know that $b + c = \frac{2}{3}B(T)$. However, we know that $b|B(T)$. Thus, the only possible value of b is $\frac{1}{3}B(T)$. (Any number smaller than $\frac{1}{3}B(T)$ would force b to be less than c. This is impossible because $a \geq b \geq c$. Also, $b \geq \frac{B(T)}{2}$ would force $b > a$, which is impossible.) The corresponding possible value of c is then $\frac{B(T)}{3}$.
>
> *Case 2:* If $a = \frac{1}{2}B(T)$, we know that $b + c = \frac{1}{2}B(T)$. However, we know that $b|B(T)$. Thus, the only possible values of b are $\frac{B(T)}{3}$ and $\frac{B(T)}{4}$. (Any number smaller than $\frac{B(T)}{4}$ would force b to be less than c. This is impossible because $a \geq b \geq c$. Also, $b \geq \frac{B(T)}{2}$ would force $c \leq 0$, which is impossible.) This means the corresponding possible values of c are $\frac{B(T)}{4}$ and $\frac{B(T)}{6}$

This shows that the only posible values of (a, b, c) are

$$(a,b,c) = \left(\frac{1}{2}B(T), \frac{1}{3}B(T), \frac{1}{6}B(T)\right)$$
$$(a,b,c) = \left(\frac{1}{2}B(T), \frac{1}{4}B(T), \frac{1}{4}B(T)\right)$$
$$(a,b,c) = \left(\frac{1}{3}B(T), \frac{1}{3}B(T), \frac{1}{3}B(T)\right)$$

Because we have $ab|B(T)$, we know that $\frac{1}{6}(B(T))^2$, $\frac{1}{8}(B(T))^2$, and $\frac{1}{9}(B(T))^2$ must divide $B(T)$. Therefore, $B(T)$ must divide 6, 8, or 9.

$B|6 \Rightarrow B = 1, 2, 3$ or $6 \Rightarrow B = 3$ or 6 (Because a triangle cannot have < 3 boundary points)

$B|8 \Rightarrow B = 1, 2, 4$ or $8 \Rightarrow B = 4$ or 8 (Because a triangle cannot have < 3 boundary points)

$B|9 \Rightarrow B = 1, 3$ or $9 \Rightarrow B = 3$ or 9 (Because a triangle cannot have < 3 boundary points)

Thus, the possible values of $B(T)$ are $3, 4, 6, 8$, or 9.

Definition 36 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.

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

EXERCISE 86

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 87

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

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

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

Solution.

(a) Let $\frac{a}{b}$ be an arbitrary fraction such that $\frac{a}{b} \in F_k$. To prove this statement, we must show also that $\frac{a}{b} \in F_n$. The fact that $\frac{a}{b} \in F_k$ implies several things, namely:

$$gcd(a,b) = 1$$
$$0 \le \frac{a}{b} \le 1$$
$$b \le k$$

We also know that $k \le n$. Thus, $b \le n$. This implies that $\frac{a}{b} \in F_n$ as well.

(b) Let $\frac{a}{b}$ be an arbitrary fraction such that $\frac{a}{b} \in F_n$. First, let us prove that $1 - \frac{a}{b}$ is also an element of F_n. Because $\frac{a}{b} \in F_n$, we know that $b \le n$, $gcd(a,b) = 1$, and $0 \le \frac{a}{b} \le 1$. For $1 - \frac{a}{b} = \frac{b-a}{b}$, we already know that the denominator b is less than or equal to n. It is also trivial to prove that $0 \le \frac{b-a}{b} \le 1$, since we know that $\frac{b}{b} = 1$ and $0 \le a \le b$. Moreover, we know that $gcd(b-a,b) = 1$, since if there was a divisor d such that $d|b-a, b$, there would exist integers s and t such that

$$\begin{aligned} ds = b-a,\ dt = b \\ ds = dt - a \\ a = ds - dt = d(t-s) \Rightarrow d|a \end{aligned}$$

Thus, $d|a$ and $d|b$. Since we know that $\frac{a}{b} \in F_n$, we know that $d = 1$ (since $gcd(a,b) = 1$). Thus, $gcd(b-a,b) = 1$.

These fractions will always pair with each other, since $\frac{a}{b} \in F_n$ and $1 - \frac{a}{b} \in F_n$, unless we have $\frac{a}{b} = 1 - \frac{a}{b}$. Only one fraction, $\frac{1}{2}$, is included in this edge case. Because every element pairs with a distinct fraction besides one, $|F_n|$ must be odd.

Exercise 88

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

Solution. Let $\frac{a}{b}$ be an arbitrary fraction such that $\frac{a}{b} \in F_n$ and $\frac{a}{b} \notin F_{n-1}$. Because of this, we know that $b = n$. Moreover, for $\frac{a}{b} \in F_n$, it must hold true that $gcd(a,b) = gcd(a,n) = 1$. The number of elements in F_n, then is defined by the number of integers a such that $1 \le a \le n$ and $gcd(a,n) = 1$. By definition, this is equal to $\phi(n)$.

Exercise 89

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) We can see that $\frac{1+1}{5+3} = \frac{1}{4}$.

(b) Indeed, we can find other Farey sequences that exhibit this property. Take, for example F_2. Here, we see that $\frac{0+1}{1+1} = \frac{1}{2}$. We observe that for all Farey sequences, $\frac{p_1+p_3}{q_1+q_3} = \frac{p_2}{q_2}$.

EXERCISE 90

(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 $p_2 q_1 - p_1 q_2$.

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

(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 $p_2 q_1 - p_1 q_2$. We will use Pick's Theorem to prove this conjecture!

Solution.

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

(b) Let us take the fractions $\frac{4}{7}$ and $\frac{3}{5}$. Here, we can see that $7 \cdot 3 - 5 \cdot 4 = 1$.

(c) Let us take the fractions $\frac{1}{3}$ and $\frac{2}{5}$. Here, we can see that $2 \cdot 3 - 1 \cdot 5 = 1$.

(d) I conjecture that for any two successive terms $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ in F_n, it will hold that

$$p_2 q_1 - p_1 q_2 = 1$$

EXERCISE 91

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 $p_2 q_1 - p_1 q_2 = 1$. 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

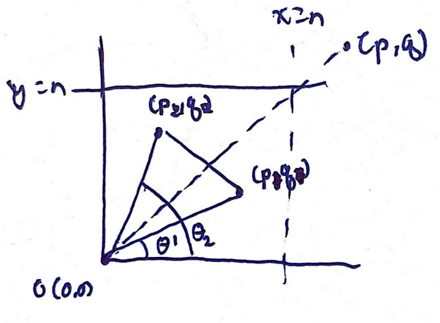
$$A(T) = \frac{1}{2}\left(p_2 q_1 - p_1 q_2\right).$$

(e) Conclude that

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

Solution.

(a) Let the angle between (p_1, q_1) and the x-axis be θ_1. Let the angle between (p_2, q_2) and the x-axis be θ_2. Let (p, q) be a lattice point such that $\tan(\theta) = q/p$ where $\theta_1 < \theta < \theta_2$ (assuming $\theta_1 < \theta_2$ - if this does not hold true, then just swap everything w.l.o.g).



Let us first remind ourselves that we are only working in the first quadrant. This implies that $0 \leq \theta_1 < \theta < \theta_2 \leq \frac{\pi}{2}$. We know that tan is strictly increasing in this domain, so it must also be true that:

$$\begin{aligned}\tan(\theta_1) < \tan(\theta) < \tan(\theta_2) &\Rightarrow \frac{q_1}{p_1} < \frac{q}{p} < \frac{q_2}{p_2}\\ &\Rightarrow \frac{p_1}{q_1} > \frac{q}{p} < \frac{q_2}{p_2}\end{aligned}$$

However, it is impossible for $\frac{p}{q}$ to be between two consecutive terms of F_n unless $\frac{p}{q}$ is not in F_n. Because of this, we know that (p, q) must lie outside the bounds $y = n$, $x = n$, $y = 0$, $x = 0$. Therefore, (p, q) cannot possibly be within the triangle T. Thus, $I(T) = 0$.

(b) Let $A = (p_1, q_1)$ and $B = (p_2, q_2)$. Applying the same logic from part (a), it is impossible for there to be a boundary point on $\overline{AB}$ (since any lattice point located between these two points' angles must lie outside of our domain). We also know that $\gcd(p_1, q_1) = 1$ and $\gcd(p_2, q_2) = 1$ because the numerator and denominator of the fractions in F_n must be relatively prime. Thus, both are visible lattice points and there are no boundary points along $\overline{OA}$ or $\overline{OB}$. Therefore, $B(T) = 3$.

(c) By Pick's Theorem,

$$A(T) = \frac{1}{2}B(T) + I(T) - 1 = \frac{3}{2} - 1 = \frac{1}{2}$$

(d) The triangle T forms half of a lattice parallelogram. We know that the area of the parallelogram is equal to the determinant of the two vectors formed by two non-parallel edges. The determinant of this parallelogram in particular is $(p_2q_1 - p_1q_2)$. Because $A(T)$ is half of the area of the parallelogram,

$$A(T) = \frac{1}{2}(p_2q_1 - p_1q_2)$$

(e) Let us equate the two areas we found in parts (c) and (d):

$$A(T) = \frac{1}{2} = \frac{1}{2}(p_2q_1 - p_1q_2) \Rightarrow 1 = (p_2q_1 - p_1q_2)$$

Exercise 92

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

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

Solution. If $0 < \frac{a}{b} < \frac{c}{d} < 1$, we can conclude that $ad < bc$. Adding ab to both sides of this inequality yields

$$\begin{gathered} ad + ab < bc + ab \\ a(b+d) < b(a+c) \\ \frac{a}{b} < \frac{a+c}{b+d} \end{gathered}$$

On the other hand, if we add cd to the original inequality, we have

$$\begin{gathered} ad + cd < bc + cd \\ d(a+c) < c(b+d) \\ \frac{d}{c} < \frac{b+d}{a+c} \\ \frac{a+c}{b+d} < \frac{c}{d} \end{gathered}$$

Note that none of these denominators will be undefined, since a, b, c, and d are all greater than 0. Putting this all together, we have proved that if $0 < \frac{a}{b} < \frac{c}{d} < 1$, then

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

EXERCISE 93

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

Solution. Let $\vec{v}$ and $\vec{w}$ be two vectors that connect from the origin to $(a,b),(c,d)$, respectively. From this construction, there exists a parallelogram P such that its vertices are defined by the points $(0,0),(a,b),(c,d),(a+c,b+d)$.

In Exercise 91, we found that the determinant of two consecutive terms of F_n (namely p_1/q_1 and p_2/q_2) have a determinant of 1. Thus,

$$A(P) = det\left(\begin{bmatrix} a & c \\ b & d \end{bmatrix}\right)$$

We know that $B(P) \geq 4$, since P is a non-degenerative parallelogram. By Pick's Theorem,

$$\begin{aligned} A(P) &= \frac{1}{2}B(P) + I(P) - 1 \\ 1 &= \frac{1}{2} \cdot 4 + I(P) - 1 \\ I(P) + 1 &= 1 \\ I(P) &= 0 \end{aligned}$$

Thus, we know that P is primitive. Because P is primitive, we know that the vertex $(a+c, b+d)$ must be a visible point. By Exercise 29, the GCD of a visible point is 1. Thus, we have proven that $\gcd(a+c, b+d) = 1$.

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 94

Use Algorithm 1 to compute F_8 using F_7.

Solution. We know that

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

By Algorithm 1, we have

$$F_8 = \{0/1, 1/8, 1/7, 1/6, 1/5, 1/4, 2/7, 1/3, 3/8, 2/5, 3/7, 1/2, 4/7, 3/5, 5/8, 2/3, 5/7, 3/4, 4/5, 5/6, 6/7, 7/8, 1/1\}$$

EXERCISE 95

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. Let us first express the fraction $\frac{61}{79}$ as $\frac{a+c}{b+d}$. From this, we know that

$$a+c=61$$
$$b+d=79$$

We also know from Exercise 91 that the determinant of adjacent elements in the Farey Sequence is 1. Thus, we have

$$61b-79a=1$$
$$79c-61d=1$$

We are then left with four equations for four variables. Solving for each of these variables yields that we have one free variable, $d=t$. We also obtain the relations

$$a=\frac{48181-61d}{79}, b+d=79, c=\frac{61}{79}d+\frac{1}{79}$$

We know from the first relation that $4818 \equiv -1 \equiv 61d \mod 79$, since a is an integer. We also know that $d \leq 78$ because $b \geq 1$. A bit of trial and error yields

$$a=44, b=57, c=17, d=22$$
$$\frac{a}{b}=\frac{44}{57}, \frac{c}{d}=\frac{17}{22}$$

EXERCISE 96

Let b_j be the ordered denominators of F_n. Find, with proof, each of the following sums.

(a) $\sum\limits_{j=1}^{|F_n|-1} \frac{b_j}{b_{j+1}}$

(b) $\sum\limits_{j=1}^{|F_n|-1} \frac{1}{b_j b_{j+1}}$

Solution.

(a) Let there be three consecutive fractions $a_1/b_1, a_2/b_2, a_3/b_3$ where a_2/b_2 is a newly introduced element of F_n. Originally, the terms generated by the terms a_1/b_1 and a_3/b_3 in our summation would be

$$\frac{b_1}{b_3}$$

However, with the addition of a_2/b_2, we have

$$\frac{b_1}{b_2} + \frac{b_2}{b_3}$$

Recall that the a_2/b_2 is the mediant fraction of a_1/b_1 and a_3/b_3. Thus, $b_2 = b_1 + b_3$. If we try to use this property to define a mapping from the terms of the summation for F_{n-1} to F_n, we obtain no useful mapping:

$$\begin{aligned}\frac{b_1}{b_3} &\Rightarrow \frac{b_1}{b_2} + \frac{b_2}{b_3}\\ &= \frac{b_1}{b_1+b_3} + \frac{b_1+b_3}{b_3}\\ &= 1 + \frac{b_1}{b_1+b_3} + \frac{b_1}{b_3}\end{aligned}$$

Regardless of how we reduce this final expression, we cannot express it purely in terms of $\frac{b_1}{b_3}$. However, note that we we add the reciprocals of these fractions together, a mapping can be formed:

$$\begin{aligned}\frac{b_1}{b_3} + \frac{b_3}{b_1} &\Rightarrow \frac{b_1}{b_2} + \frac{b_2}{b_1} + \frac{b_2}{b_3} + \frac{b_3}{b_2}\\ &= \frac{b_1}{b_1+b_3} + \frac{b_1+b_3}{b_1} + \frac{b_1+b_3}{b_3} + \frac{b_3}{b_1+b_3}\\ &= \frac{b_1}{b_1+b_3} + 1 + \frac{b_3}{b_1} + 1 + \frac{b_1}{b_3} + \frac{b_3}{b_1+b_3}\\ &= \frac{b_1+b_3}{b_1+b_3} + 2 + \frac{b_1}{b_3} + \frac{b_3}{b_1}\\ &= \frac{b_1}{b_3} + \frac{b_3}{b_1} + 3\end{aligned}$$

Now that we have a mapping between the terms of our summation as n increases, we must modify our original summation to fit this mapping. Recall that instead of b_1/b_3, we added b_3/b_1 as well to generate our mapping. Thus, our new summation is just

$$S_n = \sum_{j=1}^{|F_n|-1} \left(\frac{b_j}{b_{j+1}} + \frac{b_{j+1}}{b_j}\right)$$

Note that this is also equivalent to 2 times our original summation. This is because

$$\sum_{j=1}^{|F_n|-1} \frac{b_j}{b_{j+1}} = \sum_{j=1}^{|F_n|-1} \frac{b_{j+1}}{b_j}$$

due to the symmetry of the denominators in the Farey sequence. This fact will become useful later. Our mapping dictates that every new term in our sequence will add 3 to our total summation. By Exercise 88, we showed that the number of new elements introduced from F_{n-1} to F_n is $\varphi(n)$ where φ is the Euler function. Thus, $S_{n+1} = S_n + 3\varphi(n+1)$. Recall that S_n is 2 times our desired summation. So, let us try to express this summation relation in closed form and divide it by 2 to obtain our desired result. Generalizing the result from Exercise 88 and using the fact that $|F_1| = 2$, we find that $|F_n| = 2 + \sum_{k=2}^{n} \varphi(k)$. We can apply this closed form to our expression for S_{n+1} and use the fact that $S_1 = 1/1 + 1/1 = 2$ to see that

$$S_n = 2 + 3\sum_{k=2}^{n} \varphi(k) = 2 + 3(|F_n| - 2) = 3|F_n| + 2 - 6 = 3|F_n| - 4$$

Dividing this by two yields our desired expression

$$\sum_{j=1}^{|F_n|-1} \frac{b_j}{b_{j+1}} = \frac{3|F_n| - 4}{2}$$

(b) Recall from Exercise 91 that for two consecutive fractions a_j/b_j and a_{j+1}/b_{j+1}, the following holds true

$$a_{j+1}b_j - a_j b_{j+1} = 1$$

From this, we can show that

$$\frac{a_{j+1}}{b_{j+1}} - \frac{a_j}{b_j} = \frac{a_{j+1}b_j - a_j b_{j+1}}{b_j b_{j+1}} = \frac{1}{b_j b_{j+1}}$$

Note that the RHS is the expression in our desired summation. Thus,

$$\sum_{j=1}^{|F_n|-1} \frac{1}{b_j b_{j+1}} = \sum_{j=1}^{|F_n|-1} \left(\frac{a_{j+1}}{b_{j+1}} - \frac{a_j}{b_j} \right)$$

If we expand this summation,

$$\sum_{j=1}^{|F_n|-1} \left(\frac{a_{j+1}}{b_{j+1}} - \frac{a_j}{b_j} \right) = \frac{a_2}{b_2} - \frac{a_1}{b_1} + \frac{a_3}{b_3} - \frac{a_2}{b_2} + \cdots + \frac{a_{|F_n|}}{b_{|F_n|}} - \frac{a_{|F_n|-1}}{b_{|F_n|-1}}$$

Note that all terms cancel except for $\frac{a_1}{b_1}$ and $\frac{a_{|F_n|}}{b_{|F_n|}}$. We know that $\frac{a_1}{b_1} = 0/1 = 0$ and $\frac{a_{|F_n|}}{b_{|F_n|}} = 1/1 = 1$. Thus, we can conclude that

$$\sum_{j=1}^{|F_n|-1} \frac{1}{b_j b_{j+1}} = 1$$

EXERCISE 97

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

Solution. We know from Exercise 92 that $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$. Moreover, we know from Exercise 93 that $gcd(a+c, b+d) = 1$. This means that $\frac{a+c}{b+d}$ is fully reduced. Thus, the sum of $b+d$ cannot possibly be less than or equal to n (otherwise $\frac{a+c}{b+d}$ would lie between a/b and c/d, and this would contradict the assumption that the two fractions are consecutive terms of F_n).

EXERCISE 98

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

Solution. Because the denominators of all the terms of the Farey sequence must be $\leq n$, the only case in which $b+d$ can be equal to $2n$ is if both b and d equal n (in other words, $b = d = n$). We know from Exercise 91e, we know that $bc - ad = 1$. Substituting $b = d$, then we have

$$\begin{aligned} bc - ab &= 1 \\ b(c-a) &= 1 \end{aligned}$$

Because a, b, c, d must all be integers, we must have $b = d = c - a = 1$. Note that either one of c or a must be 1, and the other must be equal to 0, since they are both integers which cannot be greater than their denominators b and d and must also have a difference of 1. Assuming a/b and c/d are consecutive fractions, $a = 0, b = c = d = 1$. This implies that $0/1$ and $1/1$ are consecutive. However, for $n > 1$, we know this is not the case. Therefore, it is impossible for $b+d > 2n$.

EXERCISE 99

Dirichlet's Theorem on Rational Approximations The terms of the Farey sequence F_n partition the interval $[0,1]$ into sub-intervals 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

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

Show that if α is a real number in $[0,1]$ and if n is a positive integer, then there is a rational number a/b with $0 < k \leq n$ such that

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

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

Solution. For F_n, let there exist two consecutive fractions a/b and c/d such that $a \in \left[\frac{a}{b}, \frac{c}{d}\right]$. We know from Exercise 88 that $bc - ad = 1$. Let us now consider the following cases: 1) if α is greater than the mediant and 2) if α is less than the mediant.

1) In the case that $\alpha \le \frac{a+c}{b+d}$, we have

$$\begin{aligned}
\alpha - \frac{a}{b} &\le \frac{a+c}{b+d} - \frac{a}{b} \\
\alpha - \frac{a}{b} &\le \frac{(a+c)b - a(b+d)}{b(b+d)} \\
\alpha - \frac{a}{b} &\le \frac{ab+bc-ab-ad}{b(b+d)} \\
\alpha - \frac{a}{b} &\le \frac{bc-ad}{b(b+d)} \\
\alpha - \frac{a}{b} &\le \frac{1}{b(b+d)} \le \frac{1}{b(n+1)}
\end{aligned}$$

since by Exercise 97, we know that $b+d > n$. Moreover, we know that $0 < b \le n$. Thus, this shows that $\frac{a}{b}$ is a good rational approximation for α if it is less than or equal to the mediant fraction.

2) In the case that $\alpha \ge \frac{a+c}{b+d}$, we have

$$\begin{aligned}
\frac{c}{d} - \alpha &\le \frac{c}{d} - \frac{a+c}{b+d} \\
\frac{c}{d} - \alpha &\le \frac{1}{d(b+d)} \le \frac{1}{d(n+1)}
\end{aligned}$$

since by Exercise 97, we know that $b+d > n$. Moreover, we know that $0 < d \le n$. Thus, this shows that $\frac{c}{d}$ is a good rational approximation for α if it is greater than or equal to the mediant fraction.

Combining these two cases together, we have shown that one of $\frac{a}{b}$ or $\frac{c}{d}$ can approximate α.

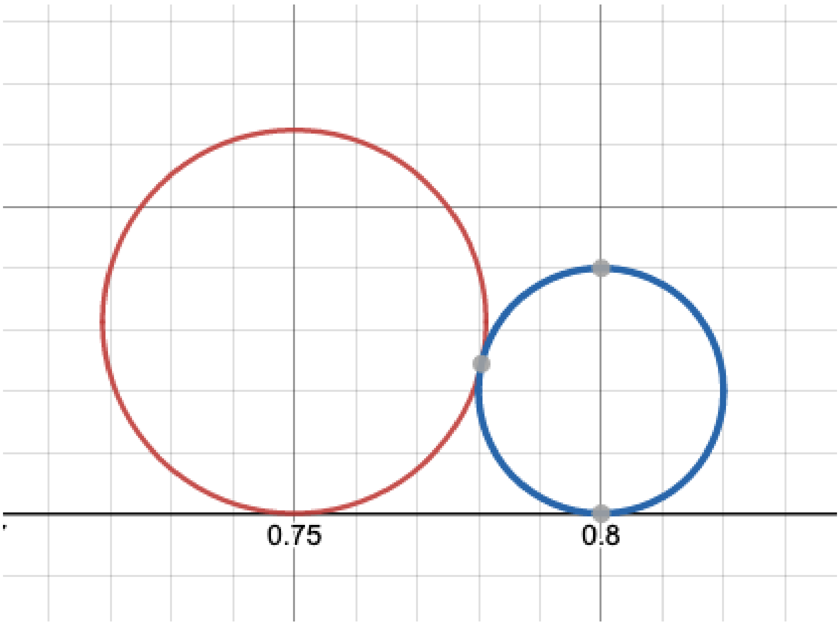
DEFINITION 38 FORD CIRCLE

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

EXERCISE 100

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. We can observe that these two circles are tangent at exactly one point.

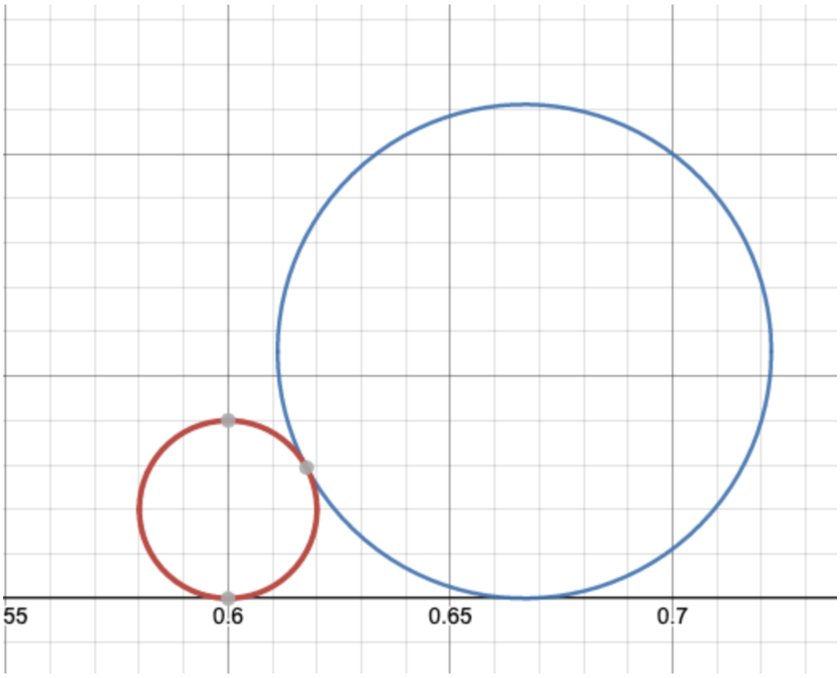


There is an interesting and beautiful connection between Farey sequences and Ford circles, which we will explore in the next set of exercises. There is also a nice connection between group actions of $SL_2(\mathbb{Z})$ to properties of Ford circles and Farey sequences, which I encourage you to explore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

EXERCISE 101

Choose two fractions $\frac{a}{b}$ and $\frac{d}{c}$ (other than $3/4$ and $4/5$) 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?

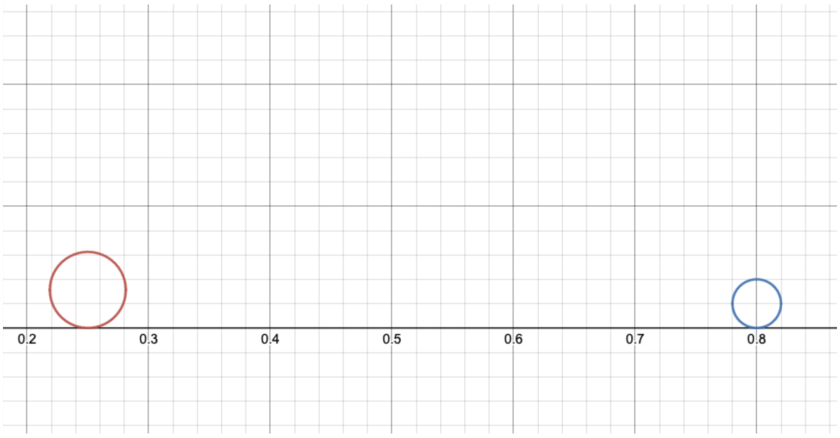
Solution. I chose to graph $C(3,5)$ and $C(2,3)$. These two Ford circles represent $3/5$ and $2/3$. Again, we note that these Ford circles are tangent at exactly one point.



EXERCISE 102

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. I chose to graph $C(1,4)$ and $C(4,5)$. These two Ford circles represent $1/4$ and $4/5$. This time, note that these Ford circles do not intersect at any point.



Exercise 103

Repeat Exercises 101 and 102 for several additional pairs of fractions in F6, keeping track of what you observe about the circles in the cases where the fractions are adjacent and are not adjacent.

Solution. (I did not include images of these graphs so that I didn't use unnecessary space) It seems that the Ford circles from consecutive Farey Sequence elements are always tangent at exactly one point. In addition, it also seems that the Ford circles constructed from non-consecutive terms in the Farey sequence are non-intersecting/wholly external.

Exercise 104

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

Solution. Consider the line segment which connects the centers of the representative Ford circles of two distinct fractions. If the length of this line segment were to be less than the sum of the two radii, then the circles would either be intersecting or completely enclosed within one another. Thus, to show that these two circles are either tangent at exactly one point or wholly external, we must show that the length of this line segment is greater than or equal to the sum of the two radii.

Let us take the representative Ford circles of two distinct fractions, $C(x_1, y_1)$ and $C(x_2, y_2)$. By definition, the centers of these two circles are $\left(\frac{x_1}{y_1}, \frac{1}{2y_1^2}\right)$ and $\left(\frac{x_2}{y_2}, \frac{1}{2y_2^2}\right)$, respectively. The distance between these centers can be represented as

$$d = \sqrt{\left(\frac{x_2}{y_2} - \frac{x_1}{y_1}\right)^2 - \left(\frac{1}{2y_2^2} - \frac{1}{2y_1^2}\right)^2}$$

Recall that the radii of the circles $C(x_1, y_1)$ and $C(x_2, y_2)$ are $\frac{1}{2y_1^2}$ and $\frac{1}{2y_2^2}$, respectively. We must show that $d \geq \frac{1}{2y_1^2} + \frac{1}{2y_2^2}$. If we square both sides of our equation, this inequality is introduced fairly naturally

$$\begin{aligned} d^2 = \left(\frac{x_2}{y_2} - \frac{x_1}{y_1}\right)^2 - \left(\frac{1}{2y_2^2} - \frac{1}{2y_1^2}\right)^2 &\geq \left(\frac{1}{2y_1^2} + \frac{1}{2y_2^2}\right)^2 \\ \left(\frac{x_2}{y_2} - \frac{x_1}{y_1}\right)^2 &\geq \frac{1}{y_1^2 y_2^2} \\ \frac{(x_2 y_1 - x_1 y_2)^2}{y_1^2 y_2^2} - \frac{1}{y_1^2 y_2^2} &\geq 0 \end{aligned}$$

Note that $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Thus, $(x_2 y_1 - x_1 y_2)^2$ must also be an integer ≥ 0. Moreover, note that if $(x_2 y_1 - x_1 y_2)^2 = 0$, that would imply that $\frac{x_1}{y_1} = \frac{x^2}{y_2}$, which is impossible since the two fractions are defined to be distinct. Thus, $(x_2y_1 - x_1y_2)^2 \geq 1$. Thus, it follows that

$$d \geq \frac{1}{2y_1^2} + \frac{1}{2y_2^2}$$

With this, we have proved that the distance between the centers of two distinct Ford circles are greater than or equal to the sum of their radii. We can then conclude that any two Ford circles must be either tangent at one point or wholly external.

EXERCISE 105

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. From Exercise 104, we know that two Ford circles $C(x_1, y_1)$ and $C(x_2, y_2)$, we have

$$\frac{(x_2y_1 - x_1y_2)^2}{y_1^2y_2^2} - \frac{1}{y_1^2y_2^2} \geq 0$$

This inequality represents the distance between the two circles in comparison with the sum of the two radii (after a bit of algebraic manipulation, of course). From exercise 91, we found that the determinant of two adjacent fractions in F_n is 1. If we substitute $x_2y_1 - x_1y_2 = 1$, we have

$$\frac{(x_2y_1 - x_1y_2)^2}{y_1^2y_2^2} - \frac{1}{y_1^2y_2^2} = \frac{1}{y_1^2y_2^2} - \frac{1}{y_1^2y_2^2} = 0$$

What this means is that the distance d is exactly equivalent to the sum of the two radii. Therefore, the representative Ford circles of two distinct fractions that are adjacent in some Farey sequence F_n must be tangent at one point.

EXERCISE 106

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. We know from Exercise 92 that for a mediant fraction $\frac{a+c}{b+d}$, the following property holds true:

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

Because of this, we also know that these three fractions are consecutive in F_{b+d}. Thus, by Exercise 105, we know that $C(a + c, b + d)$ is tangent to both $C(a, b)$ and $C(c, d)$. The radius of each Ford circle $C(p, q)$ is $\frac{1}{2q^2}$ by definition. Thus, the largest circle between $C(a, b)$ and $C(c, d)$ must have the smallest possible q. This circle is $C(a + c, b + d)$, as $b + d$ is the smallest possible q that would still allow a circle to be tangent to both $C(a, b)$ and $C(c, d)$.

EXERCISE 107

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

Solution. Let there be two distinct lattice points (a, b) and (c, d). For these points to be equidistant from the point $(\sqrt{2}, 1/3)$,

$$\begin{aligned}(a-\sqrt{2})^2+(b-\frac{1}{3})^2 &= (c-\sqrt{2})^2+(d-\frac{1}{3})^2\\ a^2-2\sqrt{2}a+2+b^2-\frac{2}{3}b+\frac{1}{9} &= c^2-2\sqrt{2}c+2+d^2-\frac{2}{3}d+\frac{1}{9}\\ a^2+b^2-c^2-d^2-\frac{2}{3}b+\frac{2}{3}d &= 2\sqrt{2}(a-c)\end{aligned}$$

Indeed, because both (a, b) and (c, d) are lattice points, we know that $a, b, c, d \in \mathbb{Z}$. As a result, we can claim that the LHS of the above equation must be rational. However, the RHS is a product of an integer and a simplified square root (namely $2\sqrt{2}$). Thus, the RHS must be irrational unless $a-c=0$. This would imply that $b^2-d^2=\frac{2}{3}b-\frac{2}{3}d \Rightarrow (b+d)(b-d)=\frac{2}{3}(b-d) \Rightarrow b+d=\frac{2}{3}$. This is impossible because $b, d \in \mathbb{Z}$ and the sum of two integers must also be an integer. Therefore, it is impossible for the above equation to hold. These contradictions show that no two lattice points can be equidistant from the point $(\sqrt{2}, 1/3)$.

EXERCISE 108

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. Let us first take a circle centered at the point $(\sqrt{2}, \frac{1}{3})$. In Exercise 107, we found that no two lattice points are the same distance from $(\sqrt{2}, \frac{1}{3})$. By extension, no two lattice points can both be on the edge of a circle centered at $(\sqrt{2}, \frac{1}{3})$ because all points of a circle are equidistant from its center. Let p_0 be the closest lattice point to $(\sqrt{2}, \frac{1}{3})$. If we expand the radius of the circle until the next closest point, p_1, is on the edge of the circle, we are guaranteed to have a circle with one interior lattice point. We can continue this for $p_2, p_3, p_4, ..., p_{n+1}$ to generate circles with n interior points, as we will never encounter two lattice points with the same distance from the center point (and therefore are only ever adding one lattice point per expansion). Therefore, we have proven that for every natural number n, there exists a plane in the circle with exactly n lattice points in its interior.

EXERCISE 109

Show that the result of Exercise 107 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. If we want two lattice points (x,y) and (a,b) to be equidistant from the point $(\sqrt{e},1/f)$, then we have (by the Distance Formula),

$$\begin{aligned}(x-\sqrt{e})^2+(y-\frac{1}{f})^2 &= (a-\sqrt{e})^2+(b-\frac{1}{f})^2\\ x^2-2\sqrt{e}x+e+y^2-\frac{2}{f}y+\frac{1}{f^2} &= a^2-2\sqrt{e}a+e+b^2-\frac{2}{f}b+\frac{1}{f^2}\\ x^2+y^2-a^2-b^2-\frac{2}{f}y+\frac{2}{f}b &= 2\sqrt{e}(x-a).\end{aligned}$$

Note that after some manipulation, we know that the LHS is a summation of only rational values. This is because $x,y,a,b,f\in\mathbb{Z}$. On the other hand, the RHS is the product of the difference of two integers as well as a square-free square root. For these two sides to be equal to each other, $2\sqrt{e}(x-a)$ must be a rational number. However, the only way this is possible is if $x-a=0\Rightarrow x=a$. This would then imply that

$$\begin{aligned}y^2-b^2 &= \frac{2}{f}y-\frac{2}{f}b\\ (y-b)(y+b) &= \frac{2}{f}(y-b)\\ y+b &= \frac{2}{f}\end{aligned}$$

Because $y,b\in\mathbb{Z}$, the sum of the two cannot possibly be a fraction (Note that if $y-b=0$, this would mean that (x,y) and (a,b) are not distinct points - this is impossible by construction). Therefore, no two lattice points can be equidistant from a point of the form $(\sqrt{e},1/f)$.

DEFINITION 39

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

DEFINITION 40

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

EXERCISE 110

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

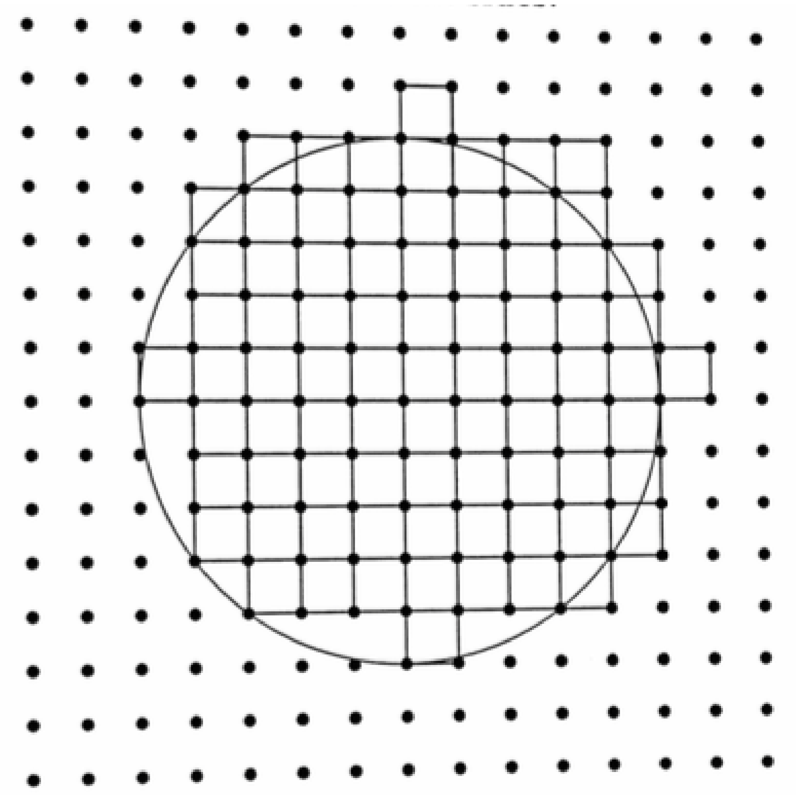
Solution. This is a rather trivial problem, so I will omit the diagram

$L(5)=21$

$L(7)=21$

$L(10) = 37$

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



EXERCISE 111

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

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

Solution. Let us first multiply both sides by n to eliminate the fractions. this yields

$$|L(n)| - \pi n| \le A(n)$$

We know that the radius of the circle is $\sqrt{n}$ (and thus the area is πn). The LHS can then be interpreted as the difference between all lattice squares within the circle and cut by the edge of the circle minus the area of the circle itself. In other words, it is the area of the lattice squares that are outside the circle (or less).

Note that $A(n)$ represents the area of all the unit lattice squares with horizontal and vertical sides cut by the boundary of the circle. This would encompass the area of the lattice squares within and outside the boundary of the circle. Clearly this number is greater than the area of the squares that lie solely outside of the circle. Therefore, we have shown that

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

Exercise 112

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. We know that the area of the annulus will be

$$R(n) = \pi(\sqrt{n}+\sqrt{2})^2 - \pi(\sqrt{n}-\sqrt{2})^2$$

Some manipulation yields that

$$\pi(\sqrt{n}+\sqrt{2})^2 - \pi(\sqrt{n}-\sqrt{2})^2 = \pi(n+2+2\sqrt{n}\sqrt{2}) - \pi(n+2-2\sqrt{n}\sqrt{2}) = 4\sqrt{2n}\pi = R(n)$$

Exercise 113

Show that

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

Solution. Because the maximum distance between any two points of a unit square is $\sqrt{2}$, we know that $R(n)$ must be the maximum possible area of all the squares cut by the arbitrary circle. This would imply that

$$A(n) \leq R(n)$$

We know from Exercise 111 that

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

From this, we can show that

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

We also know from Exercise 112 that

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

Putting this all together, we have shown that

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

EXERCISE 114

Show that

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

Solution. We know from Exercise 113 that

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

From this, we know that

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

Indeed, we also know that

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

By the Squeeze Theorem, we have

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

EXERCISE 115

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. To prove that

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

we must show that $A(nP) = n^2 A(P)$ and $B(nP) = nB(P)$. We found in Exercise 60 that every polygon can be dissected into triangles. Thus, it would be sufficient to prove that $A(nT) = n^2 A(T)$ and $B(nT) = nB(T)$.

A(P): w.l.o.g. Let T be a triangle with vertices at $(0,0),(a,b),(c,d)$. Thus, we have

$$A(T) = \frac{1}{2}\cdot|det(\begin{bmatrix} a & b \\ c & d \end{bmatrix})| = \frac{1}{2}|ad - bc|$$

$$A(nT) = \frac{1}{2}\cdot|det(\begin{bmatrix} na & nb \\ nc & nd \end{bmatrix})| = \frac{1}{2}|n^2 ad - n^2 bc| = \frac{1}{2}n^2|ad - bc| = n^2 A(T)$$

Therefore, we have shown that $A(nT) = n^2 A(T) \Rightarrow A(nP) = n^2 A(P)$.

B(P): Recall in Exercise 31, we showed that there are $gcd(a,b) - 1$ lattice points that lie upon the line segment connecting two lattice points $(0,0)$ and (a,b). Because we know that $gcd(na,nb) = n \cdot gcd(a,b)$, there will be $n \cdot gcd(a,b) - 1$ lattice points on the line segments connecting $(0,0)$ and (na,nb). Therefore, we can see that $B(nP) = nB(P)$.

EXERCISE 116

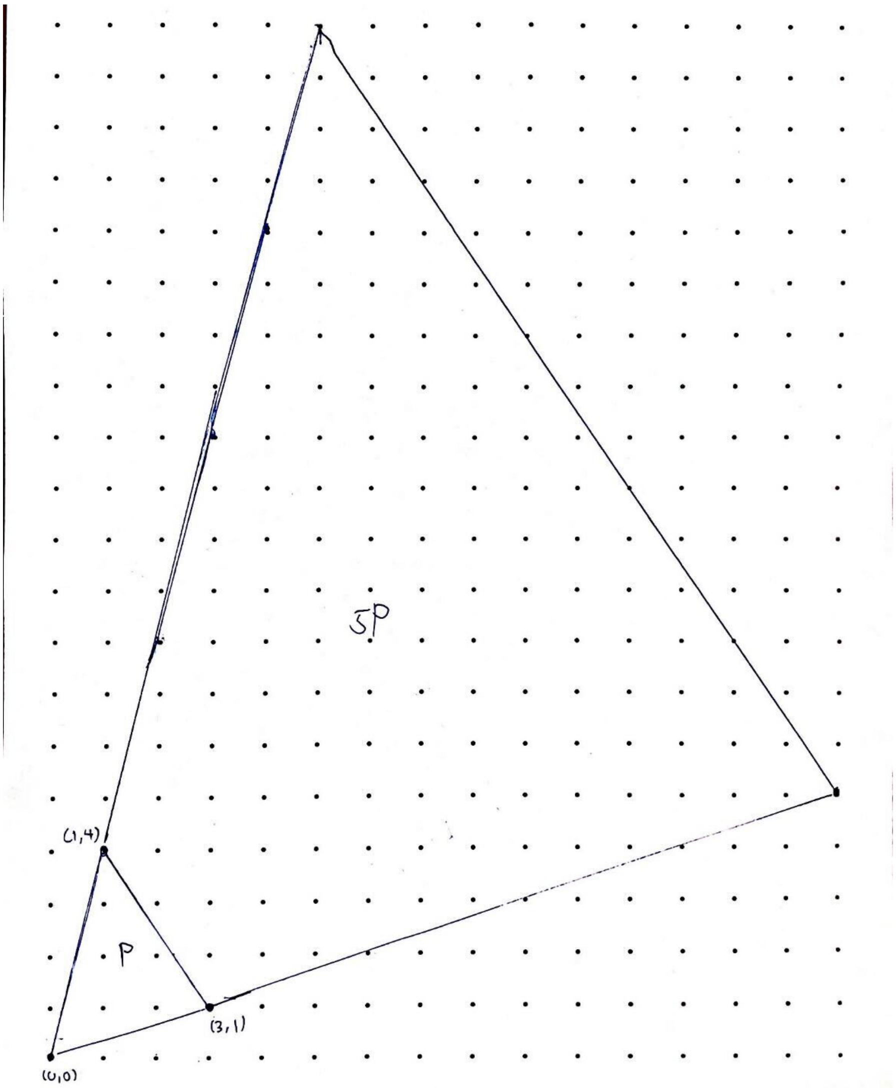
Let P be the triangle with vertices $(0,0)$, $(3,1)$, and $(1,4)$.

(a) Sketch P and $5P$ using the definition for nP provided in Exercise 115.

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

(c) Compute $L(5P)$ using the result in Exercise 115, and verify that you obtain the same result as in part (b).

Solution.

(a) 

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

(c) $L(5P) = A(5P) + \frac{1}{2}B(5P) + 1 = 137.5 + 7.5 + 1 = 146$

DEFINITION 41

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

DEFINITION 42

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.
Theorem 7 is demonstrated in Figure 4.

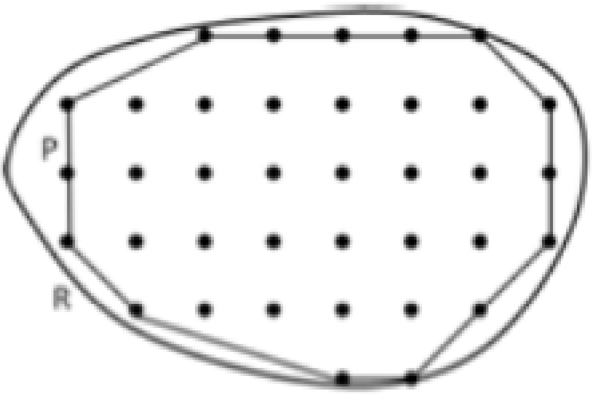


Figure 4: The convex polygon P is a convex lattice polygon that contains the same number of lattice points as the convex region R.

EXERCISE 117

Illustrate Theorem 7 for the following regions:

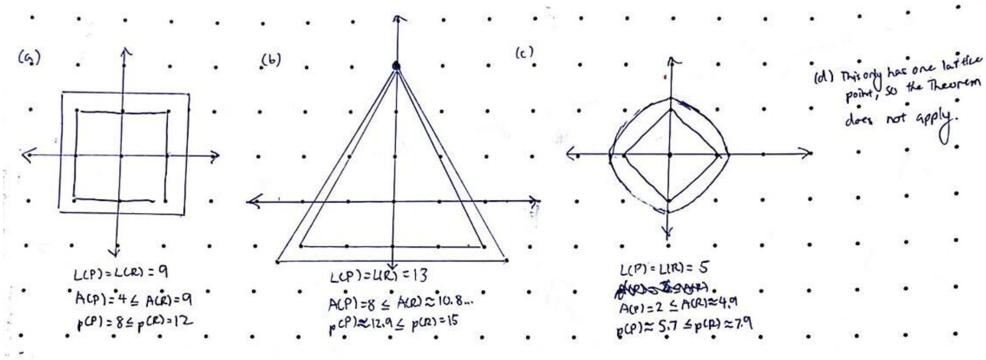
(a) A square with sides of length 3 whose center is at the point $(0,0)$.

(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 $\frac{5}{4}$.

(d) A circle with center $(0,0)$ and radius $\frac{7}{8}$.

Solution.



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

EXERCISE 118

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. By Theorem 7, we know that P will contain the same number of lattice points as R. This means that $L(R) = L(P)$. Recall that Pick's Theorem states

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

Substituting this into our desired inequality, we have

$$L(R) = A(P) + \frac{1}{2}B(P) + 1 \leq A(R) + \frac{1}{2}p(R) + 1$$

Indeed, by Theorem 7, we have $A(P) \leq A(R)$ and we know that $1 = 1$. Thus, we must prove that $B(P) \leq p(R)$. Recall that P is the convex hull of the set of lattice points in P where $L(P) \geq 3$. Thus, the boundary of P must lie within the boundary of R. Because the side length between two lattice points is ≥ 1, we necessarily have that $B(P) \leq p(P) \leq p(R)$ (the last portion of the inequality is true by Theorem 7). Therefore, we have shown that

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

EXERCISE 119

Use Exercise 118 for the same regions as in Exercise 117.

Solution. Refer to the Exercise 117 for the figures.

(a) $9 \leq 9 + \frac{1}{2} \cdot 12 + 1 = 16$

(b) $13 \leq 10.8 + \frac{1}{2} \cdot 15 + 1 = 19.3$

(c) $5 \leq 4.9 + \frac{1}{2} \cdot 7.9 + 1 = 9.85$

(d) $1 \leq 2.4 + \frac{1}{2} \cdot 5.5 + 1 = 7.6$

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 exercises. 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.**

$$S = \{(x, y) \textbf{ such that} 0 \leq x < 1 \textbf{ and } 0 \leq y < 1\} = [0, 1) \times [0, 1).$$

- **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.

EXERCISE 120

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. We can interpret $T_{i,j}$ and $T_{m,n}$ as the translation of $R_{i,j}$ and $R_{m,n}$ to within the unit square. We essentially want to prove that the intersection between the two is not empty.

Because it is given that $A(R) > 1$, it must be true that there is some $R_{i,j}$ and $R_{m,n}$ such that the union of the two is also greater than 1 (since the area of R is just the sum of all $R_{i,j}$). The translation of the two, $T_{i,j}$ and $T_{m,n}$, must then also have some intersection (otherwise we would have $T_{i,j} \cap T_{m,n} = \emptyset$ would imply that $R_{i,j} \cup R_{m,n} = T_{i,j} \cup T_{m,n} > 1$, which is impossible since both Ts are in the unit square that has an area of 1). Therefore, there must exist i, j and m, n such that

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

and $i \neq m$ or $j \neq n$.

EXERCISE 121

Complete the proof of Blichfeldt's Theorem.

Solution. From Exercise 120, we know that there must exist some $T_{i,j}$ and $T_{m,n}$ such that $T_{i,j} \cap T_{m,n} \neq \emptyset$. Let (α, β) be some arbitrary point in the set $T_{i,j} \cap T_{m,n}$. By definition, we have that $(\alpha, \beta) \in R_{i,j} - (i, j)$ and $(\alpha, \beta) \in R_{m,n} - (m, n)$.

For the sake of matching the notation, let there exist some (x_1, y_1) and (x_2, y_2) such that $(\alpha, \beta) = (x_1, y_1) - (i, j) \in R_{i,j}$ and $(\alpha, \beta) = (x_2, y_2) - (m, n) \in R_{m,n}$. Because both $R_{i,j}$ and $R_{m,n}$ are subsets of R, these two points are also within R. Moreover, we have that

$$(x_2 - x_1, y_2 - y_1) = ((\alpha + m) - (\alpha + i), (\beta + n) - (\beta + j)) = (m - i, n - j) \in \mathbb{Z}^2$$

because $i, j, m, n \in \mathbb{Z}$. Therefore, $(x_2 - x_1, y_2 - y_1)$ is a lattice point and we have proven Blichfeldt's Theorem.

DEFINITION 43

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.

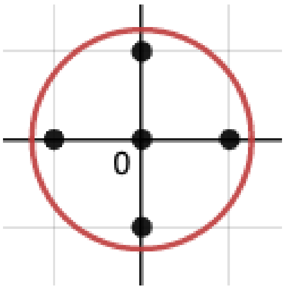
Exercise 122

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) Such a circle would have an area of $A = \pi\left(\frac{5}{4}\right) \approx 4.9$ and contain 5 lattice points.



(b) Note that such a circle would have an area of $A = \pi\left(\frac{7}{8}\right) \approx 2.4$, and thus has too small of an area to apply Minkowski's Theorem.

We will now prove Minkowski's Theorem in a series of exercises.

Exercise 123

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. We know that the area of R' will be $1/4$ of the area of R. It is also given that $A(R) > 4$. Therefore, we have $A(R') > 1$. By Blichtfeldt's Theorem, we can then claim that there exists points $x' = (x_1, y_1)$ and $y' = (x_2, y_2)$ such that

$$x' - y' = (x_2 - x_1, y_2 - y_1)$$

is a nonzero lattice point (we know that it's nonzero because otherwise we have $x' = y'$, which can't be true because Blichtfeldt's Theorem claims there must be two distinct points in R' which have our desired property).

EXERCISE 124

Let x' and y' be as in Exercise 123. Show that $x' - y'$ is in R. Hint: express $x' - y'$ as a linear combination of points that you know are in R.

Solution. Recall that by Blichtfeldt's Theorem, we know that x' and y' are contained within R'. We also know that R' is simply a convex symmetric region that is equivalent to region R scaled down by a factor of 2. Thus, it must follow that

$$2x' = (2x_1, 2y_1) \in R \text{ and } 2y' = (2x_2, 2y_2) \in R$$

Because R is symmetric about the origin, we know that $-2x'$ and $-2y'$ must also be in R as well. Now let us try to express $x' - y'$ as a linear combination of points we know are in R.

> **Case 1:** If x' and y' are non-collinear points. By the symmetry of R' we know that $2x', 2y', -2x', -2y'$ form a parallelogram. We can write this as a linear combination:
>
> $$\frac{1}{2}(2x') + \frac{1}{2}(-2y') = x' - y' \in R$$
>
> We know this because we found earlier that $2x', 2y', -2x', -2y' \in R$.
>
> **Case 2:** If x' and y' are collinear points, they cannot form a parallelogram as in Case 1. Because they are collinear, we can redefine $y' = (tx_1, ty_1)$ where t is just some number. Thus, we can also rewrite $2y' = (2tx_1, 2ty_1)$ wher $|t| > 1$. Without loss of generality, also assume that y' is the one farthest from the origin (between x' and y').
>
> Recall that we know $2y'$ and $-2y'$ are in R. Because R is convex, any point within the interval of these two must also be in R (in other words, any multiple of x' with coefficients between $[-2t, 2t]$ must be in R). We can now rewrite
>
> $$x' - y' = (x_1 - tx_1, y_1 - ty_1) = ((1-t)x_1, (1-t)y_1)$$
>
> Note that $-2t < 1 - t < 2t$ for $|t| > 1$. We already knew from Exercise 123 that $x' - y'$ was a lattice point. Thus, we have shown that $x' - y'$ is a nonzero lattice point in R.

EXERCISE 125

Minkowski's Theorem and Sums of Squares Let p be a prime number. If

$$p = 2 \text{ or } p = 4k + 1$$

for some integer k, show p can be written as the sum of the squares of two positive integers. Hints: you may use the number theoretic fact that if p is a prime such that $p \equiv 1 \mod 4$, then there exists an integer q such that

$$q^2 \equiv -1 \mod p$$

Consider the general lattice Λ defined by

$$\mathbf{v_1}\begin{bmatrix}1\\q\end{bmatrix}, \mathbf{v_2} = \begin{bmatrix}0\\p\end{bmatrix}$$

where $q^2 \equiv 1 \mod p$.

Solution. First consider the general lattice Λ as in the hint. We know that

$$\Lambda = \left\langle \begin{bmatrix}1\\q\end{bmatrix}, \begin{bmatrix}0\\p\end{bmatrix} \right\rangle, \dim(\Lambda) = 2, \det(\Lambda) = p$$

Now consider a circle C centered at $(0,0)$ with a radius of $r = \frac{3\sqrt{p}}{\sqrt{2\pi}}$. The area of this circle is $A(C) = \pi r^2 = \frac{9}{4}p > 4p$. Indeed, this circle and the general lattice Λ fit Minkowski's Theorem, as C has an area of greater than 4. Then, by Minkowski's Theorem, there must exist some non-zero lattice point in C

$$a\begin{bmatrix}1\\q\end{bmatrix} + b\begin{bmatrix}0\\p\end{bmatrix} = \begin{bmatrix}a\\aq+bo\end{bmatrix}$$

Recall that we defined q in the hint to satisfy $q^2 \equiv -1 \mod p$. We know by construction that

$$a^2 + (aq+bp)^2 \leq r^2 = \frac{9}{2\pi}p$$
$$a^2 + a^2q^2 + 2aqbp + b^2p^2 \leq r^2 = \frac{9}{2\pi}p$$
$$a^2(1+q^2) + b^2p^2 + 2aqbp \leq r^2 = \frac{9}{2\pi}p$$

Indeed, all these terms are divisible by p and the LHS must also be an integer (as we started with a lattice point). However, note that p's coefficient on the RHS is not an integer ($\approx 1.2p$). Thus, the only way for this inequality to hold true is if LHS= p (we know it's not 0 because we started with a non-zero lattice point). Note that a and $aq+bp$ are both integers. Thus, we have

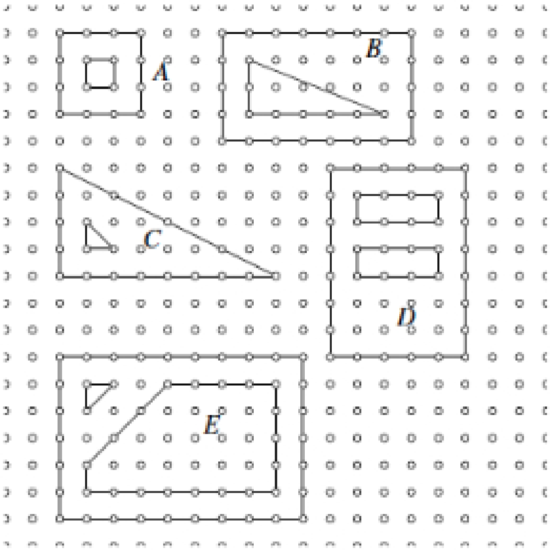
$$a^2 + (aq+bp)^2 = p$$

meaning we have shown that p can be written as the sum of the squares of two positive integers.

This concludes the proof of Minkowski's Theorem!

Challenge Problem 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.



Solution. Let us first write the area of a polygon with holes as

$$A = A_P - \sum_{h=1}^{n} A_h$$

where A_P is the outermost polygon and A_h represents the area of one of the "holes" in the polygon. Recall from Pick's Theorem that $A(P) = I(P) + \frac{1}{2}B(P) - 1$. If we substitute this into our above expression for A, we get

$$\begin{aligned} A &= A_P - \sum_{h=1}^{n} A_h \\ &= I_P + \frac{B_P}{2} - 1 - \sum_{h=1}^{n}(I_h + \frac{B_h}{2} - 1) \\ &= I_P + \frac{B_p}{2} - 1 + n - \sum_{h=1}^{n}(I_h + \frac{B_h}{2}) \end{aligned}$$

Now note that

$$I = I_P - \sum_{h=1}^{n}(I_h + B_h)$$

and

$$B = B_P + \sum_{h=1}^{n} B_h$$

Thus, we can rewrite our formula for A again as

$$A = I + \frac{1}{2}B - 1 + n$$

where n represents the number of holes in P.