Lattice Point Geometry Ex:1-8

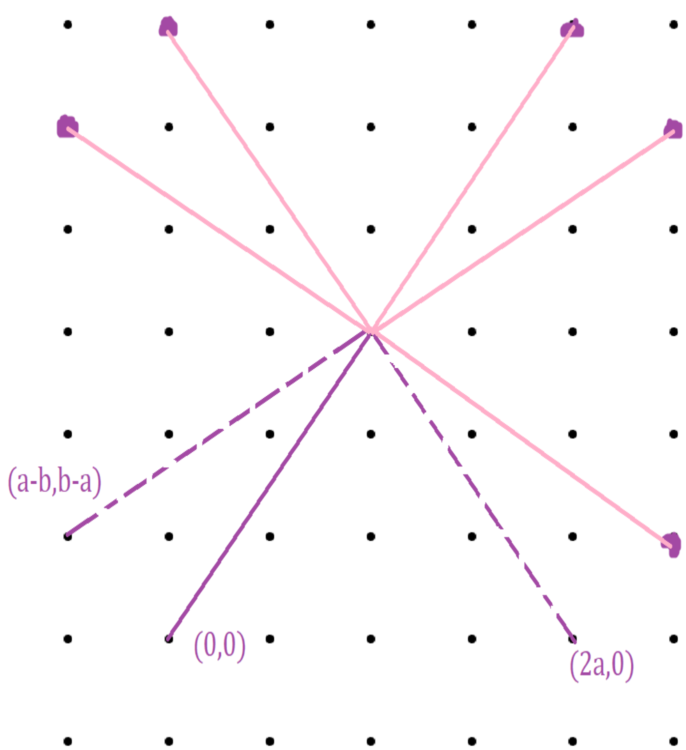
Reed Michael Upson

January 2023

1.

Conjecture. It is not possible to construct a regular lattice triangle.

Proof. Let's show that no regular lattice 3-gon can be constructed by trying to construct one. Let the first vertex of our 3-gon be at $(0,0)$. From there we have to construct one leg, and let's denote that side $L1 : (0,0) \to (a,b)$, where $a, b \in \mathbb{N}^0$. Without loss of generality, we can assume $b \geq a$. We are constructing an equilateral triangle, so the angle between $L1$ and $L2$ must be acute. I.e. $L2 : (a,b) \to (2a,0)$ or $L2 : (a,b) \to (0,0)$ or $L2 : (a,b) \to (a-b, b-a)$, because all other possible sides of equal length necessarily produce an obtuse or right angle. Of course, we must have $L2 : (a,b) \to (2a,0), (a-b, b-a)$ because returning to $(0,0)$ clearly prevents us from building a triangle. Thus, the final leg must be $L3 : (2a,0) \to (0,0)$ or $L3 : (a-b, b-a) \to (0,0)$. The first of these requires $2a = \sqrt{a^2+b^2} \implies b = \sqrt{3}a \notin \mathbb{Q}$ which is incompatible with the assumption $a, b \in \mathbb{N}^0$. Thus, such an arrangement is impossible. The second case implies $\sqrt{a^2+b^2} = \sqrt{(a-b)^2+(b-a)^2} \implies a^2+b^2 = 2(a^2-2ab+b^2)$ which is not true unless $a, b = 0$, in which case the triangle is trivial and nobody likes that!



2.

Conjecture. It is possible to construct a regular lattice square.

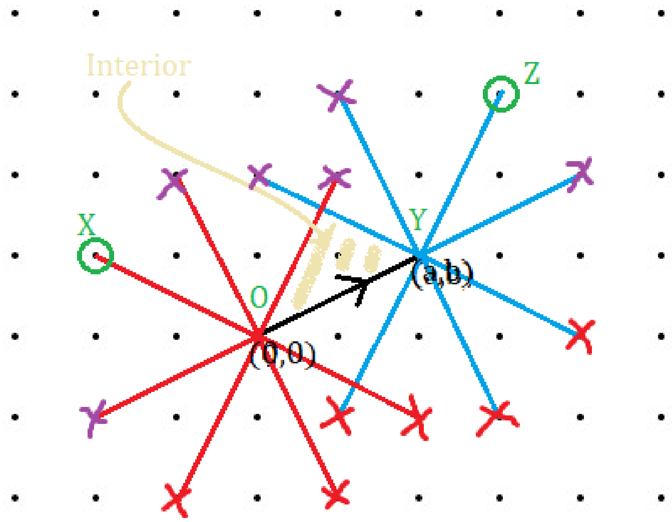
Proof. The square $(0,0) \to (0,1) \to (1,1) \to (1,0) \to (0,0)$ is an example.

3.

Conjecture. It is not possible to construct a regular lattice pentagon.

Proof. Let's try to construct a regular lattice pentagon, and then arrive at a contradiction. We will start by noting three points that must be vertices of the pentagon, and then we will prove that they can't exist together with the equiangular supposition.

Without loss of generality, assume one vertex of the pentagon falls at $(0,0)$, and that one of the two adjacent vertices falls at (a,b) where $a,b \in \mathbb{Z}$. There are 7 vertices we could go to next, but we will reduce this to only 1! Firstly, we are only speaking about simple polygons which have a definite interior and exterior. Let's say (without loss of generality) that we are constructing the pentagon in the positive orientation, so the points to the left of the ray-segment $(0,0) \to (a,b)$, traversed in that order, will be on the interior of the pentagon. This eliminates the vertices $(a-b, b-a), (a+b, b-a)$ and $(2a, 0)$, because we know the regular pentagon to be convex. These eliminations are represented by the red "x"s on the blue lines.



Now, we also know that interior angles of a pentagon are obtuse, but certainly not as great as π in measure, eliminating the vertices $(0, 2b)$ (forming an acute angle), $(a-b, b+a)$ (forming a right angle), and $(2a, 2b)$ (forming an angle of π). These eliminations are represented with purple "x"s on the blue lines. Thus, we are left with the vertex $(a+b, b+a)$. Let's call that vertex Z.

We can make the same observations to select the other vertex adjacent to $(0,0)$, and conclude that it must be at $(-a, b)$. We'll call that vertex X.

Let's label the origin O and the point at (a,b) Y, and the point following that Z, remembering the positive orientation we applied for the purpose of construction. We quite clearly have $m\angle XOY = \pi - 2\arctan\frac{b}{a}$. With a little geometry, we can see that $m\angle OYZ = \frac{3\pi}{2} + 2\arctan\frac{b}{a}$. Thus, if this pentagon has any hope of being equiangular, we need

$$\pi - 2\arctan\frac{b}{a} = \frac{3\pi}{2} + 2\arctan\frac{b}{a}$$

This, of course, implies that $-\frac{\pi}{8} = \arctan\frac{b}{a}$ or $\frac{b}{a} = -\sqrt{\frac{2+\sqrt{2}}{2-\sqrt{2}}}$. We can prove this by simply applying the half angle formula. The right hand side is clearly not rational, so this contradicts the notion that $b, a \in \mathbb{Z}$.

Let's note the implications of what we just proved. We made no mention of the the number of sides, other than to state that the pentagon has obtuse interior angles which is really a special case of the statement that all regular n-gons of $n > 4$ have obtuse interior angles. Thus, our result should hold for all $n > 4$, outlawing all lattice polygons with 5 or more sides.

4.

Conjecture. The cosine of each interior and exterior angle of any regular polygon must be rational.

Proof. Consider two sides of a polygon, and construct them as vectors $\vec{x}$ and $\vec{y}$, where the components $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. We have the dot product $\vec{x} \cdot \vec{y} = x_1y_1 + x_2y_2 = |\vec{x}||\vec{y}|cos\theta$ where θ is the angle between the two vectors and thus the interior angle of the polygon. Because the polygon is regular, we have $|\vec{x}| = |\vec{y}|$ so $|\vec{x}||\vec{y}| = |\vec{x}|^2 = (x_1^2 + x_2^2) \in \mathbb{Z}$ by the closure of $\mathbb{Z}$ under multiplication and addition. Therefore, by those same closure properties,

$$cos\theta = \frac{x_1y_1 + x_2y_2}{|\vec{x}||\vec{y}|} \in \mathbb{Q}$$

as the numerator and denominator are in $\mathbb{Z}$. Because $cos(\theta) = -cos(\pi - \theta)$, the cosines of the exterior angles must also be rational.

5.

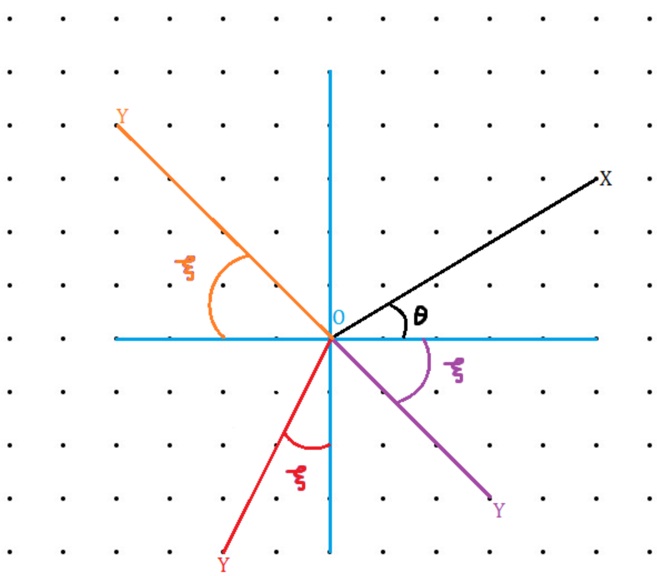
Conjecture. It is not possible to construct a regular lattice octagon.

Proof. The interior angles of the 8-gon are all $\frac{3\pi}{4}$, and $cos(\frac{3\pi}{4}) = \frac{-\sqrt{2}}{2}$. $\frac{-\sqrt{2}}{2} \notin \mathbb{Q}$ so, by the contrapositive of the previous result, no regular 8-gons can be drawn on the lattice.

6.

Conjecture. If α is a lattice angle and if the measure of α is not equal to an integer multiple of $\frac{\pi}{2}$, then $tan(\alpha) \in \mathbb{Q}$.

Proof. Without loss of generality, let's place the vertex of the angle at $(0, 0)$. Let's construct the angle using two points: X at (a, b) and Y at (c, d). Without loss of generality, we can place (a, b) in the first quadrant. I.e. $0 < a, b \in \mathbb{Z}$ (this was stated exactly by Eddy, who gave me this idea). We can call the angle between $\overline{OX}$ and the $x-$axis θ.



We initially have 3 cases, corresponding to the 3 quadrants in which $\overline{OY}$ can fall. Note, however, that the case where Y falls in the 2nd quadrant can be transformed to the case where Y lands in the 4th quadrant by a rotation and reflection (note, reflection represents a simple swap of either a and c or b and d, which we chose arbitrarily). Thus, we end up with two cases, represented above by purple and red lines. Let's introduce the angle ξ for each case.

Case 1: Purple

In the purple case, we have $tan(m\angle XOY) = tan(\theta + \xi) = \frac{tan\theta + tan\xi}{1 - tan\theta tan\xi}$. This is clearly not defined if $\theta + \xi = \frac{\pi}{2}$, so we use that supposition here. Of course, we have

$$tan\theta = \frac{b}{a} \qquad tan\xi = \frac{d}{c}$$

Therefore

$$tan(m\angle XOY) = \frac{\frac{b}{a} + \frac{d}{c}}{1 - \frac{bd}{ca}}$$

which is rational because the rational numbers are closed under addition, multiplication, and division.

Case 2: Red

In the red case, we have $tan(m\angle XOY) = tan(\theta + \frac{\pi}{2} + \xi) = \frac{-1}{tan(\theta+\xi)}$. Again, this is not defined if $\theta + \frac{\pi}{2} + \xi = \pi$, so we use the supposition that $\xi + \theta \neq \frac{\pi}{2}$. We just proved that $tan(\theta + \xi) \in \mathbb{Q}$ so, by the closure of the rational numbers under division, we must have $tan(m\angle XOY) \in \mathbb{Q}$.

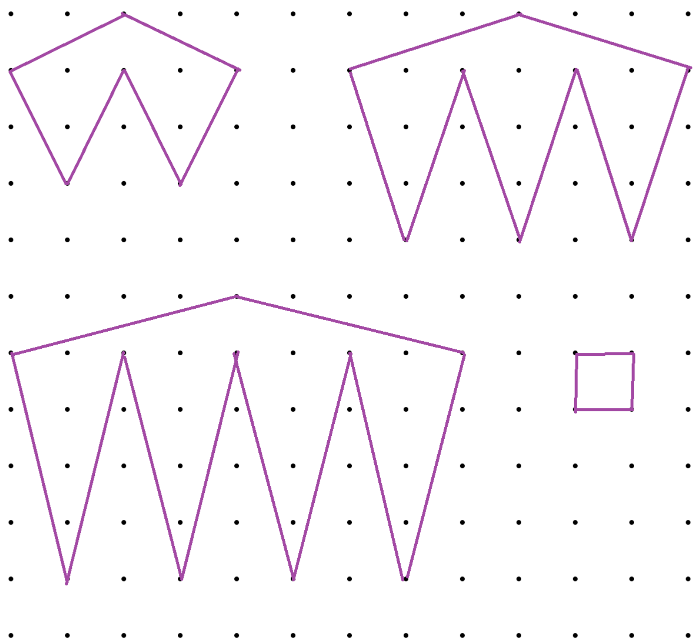
7.

Conjecture. The only possible regular lattice polygon is a square.

See the last paragraph of (3). That taken along with the fact that we can't construct a regular triangle, and that we can construct a square, tells us that the only possible regular lattice polygon is the square. This makes sense, because of the 4-fold reflectional and rotational symmetries of the lattice plane. I would imagine we could get similar results for other latices built out of other symmetries.

8.

I skimped out on this one – here are the constructions (Eddy's combs):



I conjecture that it is possible for even n.

9.

Conjecture. It is possible to construct a square whose area is not a perfect square.

Proof. Just take $(0,0) \to (2,1) \to (1,3) \to (-1,2)$.

10.

Conjecture. The area of all lattice squares is an integer.

Proof. We know that the side length of the square must be of the form $S = \sqrt{a^2+b^2}$ where $a, b \in \mathbb{Z}$, so $A = S^2 = a^2 + b^2 \in \mathbb{Z}$. This follows from the closure of the integers under addition and multiplication.

11.

Conjecture. There exists a lattice square with area $n \in \mathbb{Z}^+$, iff there exist $a, b \in \mathbb{N}^0$ such that

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

Proof. We first prove the direction $\exists\square$ with area $n \implies \exists a, b \in \mathbb{N}^0$ such that $n = a^2 + b^2$. If n represents the area of a lattice square, then $\sqrt{n}$ represents the side length of the square which is necessarily of the form $\sqrt{a^2+b^2}$ (where $a, b \in \mathbb{Z}$). Thus, $n = \sqrt{n} = \sqrt{a^2+b^2}^2 = a^2 + b^2$.

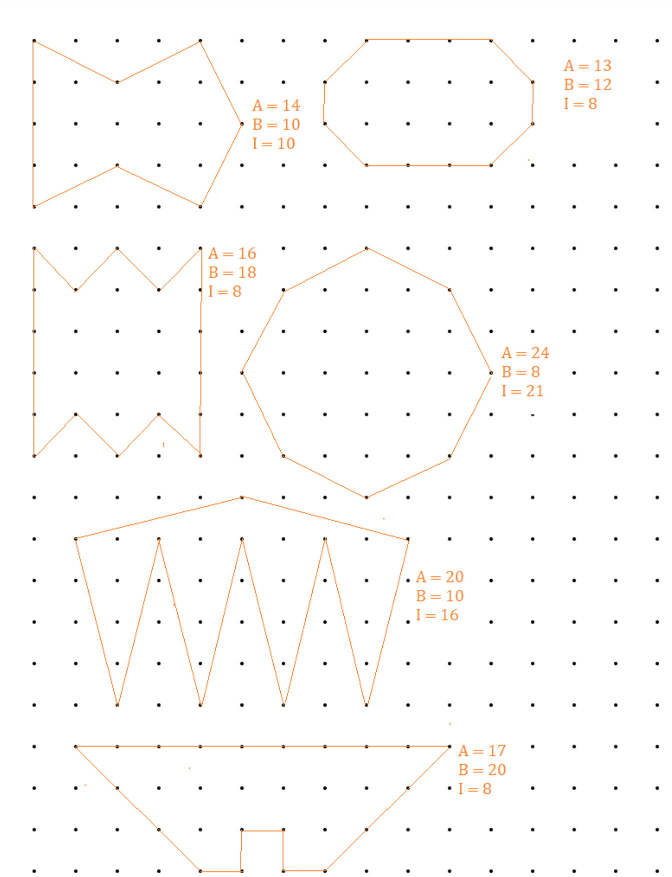
The other direction is $\exists a, b \in \mathbb{N}^0$ such that $a^2 + b^2 = n \implies \exists\square$ with area $n \in \mathbb{N}^0$. If $a^2 + b^2 = n$ then $\sqrt{a^2+b^2} = \sqrt{n}$ which we can take to be the side length of a square with orthogonal lattice steps a, b. By this I mean a square whose sides are constructed by taking a steps in either the x or y directions, and then taking b steps in the other orthogonal direction. This constructs a square of area $a^2 + b^2 = n$, of course!

12.

Conjecture. It is possible to construct a lattice triangle whose area is not an integer.

Proof. Construct $(0, 0) \to (1, 0) \to (1, 1) \to (0, 0)$ which has an area of $\frac{1}{2}$.

13.



All of the areas must be an integer multiple of $\frac{1}{2}$.

14.

Conjecture. For a triangle T such that $I(T) = 0$, $B(T)$ can be any integer greater than or equal to 3.

Proof. We can prove this by constructing a triangle T with $B(T) = n$ for $n \geq 3$. Take the triangle $(0, 0) \to (n - 1, 0) \to (n - 1, 1) \to (0, 0)$. The triangle can't contain any lattice points because $\forall \ (x, y) \in T$ (where T is the open set of points that lie inside the triangle as defined by its edges), $0 < y < 1$ so $y \notin \mathbb{Z}$. The boundary clearly includes n points ($n - 1$ on the bottom edge and then one on the top corner), and n can be chosen arbitrarily.

15.

Conjecture. For a triangle with $I(T) = 1$ we can have $B(T) \in \{3, 4, 6, 8, 9\}$

See the proof in Ex85!

16.

The area of all of these lattice triangles is $\frac{1}{2}$. This is clear for the triangles which have base and height equal to 1. For the other triangles, we can use the cross-product area relation. That is, $\binom{a}{b} \times \binom{c}{d} = 2A$.

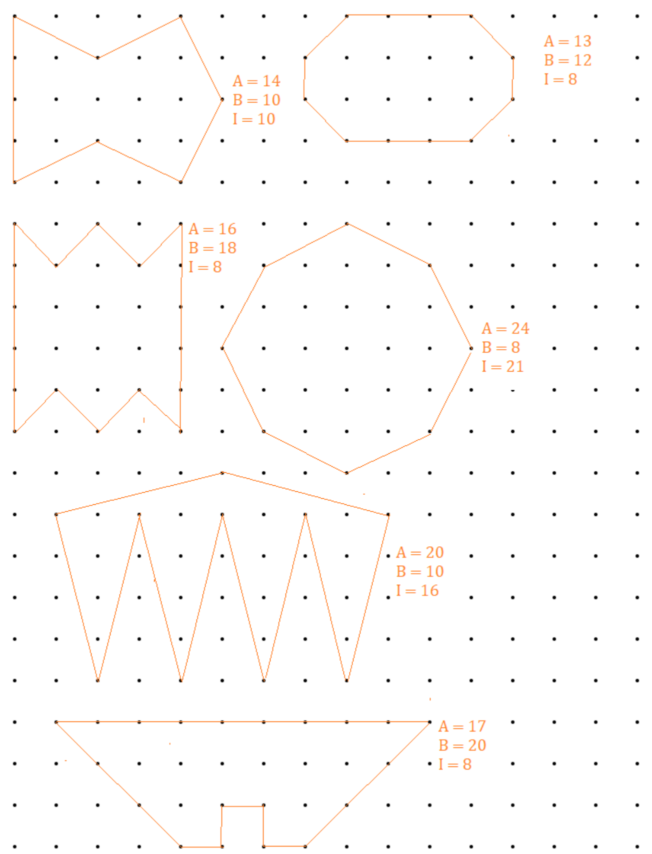
17.

I conjecture Pick's theorem (see Ex22, Ex67).

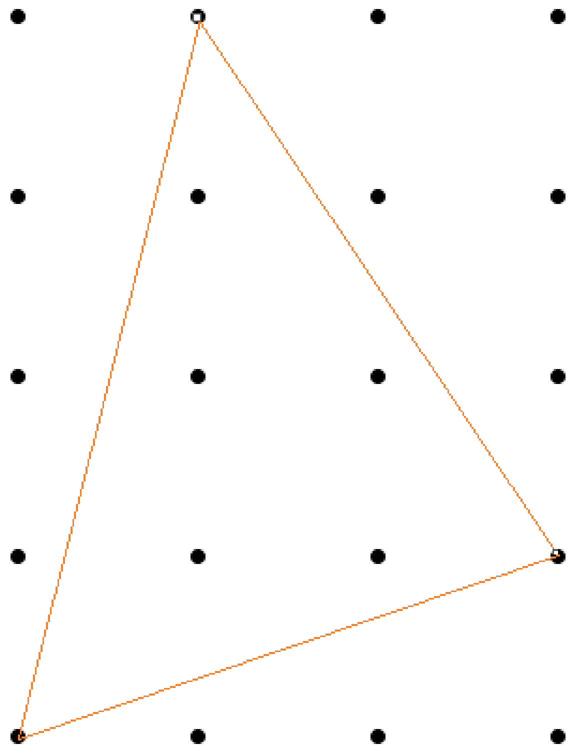
18.

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

19.


A = 14
B = 10
I = 10
A = 13
B = 12
I = 8
A = 16
B = 18
I = 8
A = 24
B = 8
I = 21
A = 20
B = 10
I = 16
A = 17
B = 20
I = 8

20.



$$B(T) = 3 \qquad I(T) = 5$$

$$A(T) = \frac{1}{2}|\begin{pmatrix}3\\1\end{pmatrix} \times \begin{pmatrix}1\\4\end{pmatrix}| = \frac{11}{2}$$

21.

Conjecture. For a lattice pentagon P, if $B(P) \in \{\text{even}\}$ then $A(P) \in \mathbb{N}$. Otherwise, $A(P) = \frac{n}{2}$ for some $n \in \mathbb{N}$.

Proof. This follows directly from Pick's theorem, see Ex22 or Ex67 (I proved those before this one).

22.

Conjecture. The area, number of interior points, and the number of boundary points in a lattice polygon follow the relationship: $A = I + \frac{B}{2} - 1$. This is, of course, Pick's theorem.

Proof. *Note that we must assume some things that will be proven later in the exercises.*

[For now] Let's assume we can triangulate any lattice polygon into primitive triangles. Lets consider the triangulation of a polygon P into primitive triangles t_i, of which there are v. Now let's construct a graph in the following way:

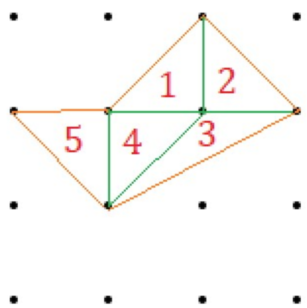
Each t_i in our triangulation maps to a vertex in our graph. The border between t_i and t_j in P maps to an edge between the vertices t_i and t_j in our graph.

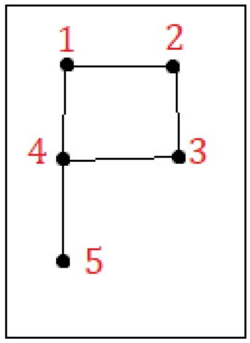
Using Ex58, we know that the area of a primitive triangle is always $\frac{1}{2}$, we can rewrite the area of P to be $A = \frac{1}{2}v$.

Now, let's think about the number of faces in our graph. A cycle is sufficient to form a face, and every interior vertex necessarily forms a cycle because at least three primitive triangles share that point. There is an additional face, which is the external face, so the number of faces is given by $f = I + 1$.

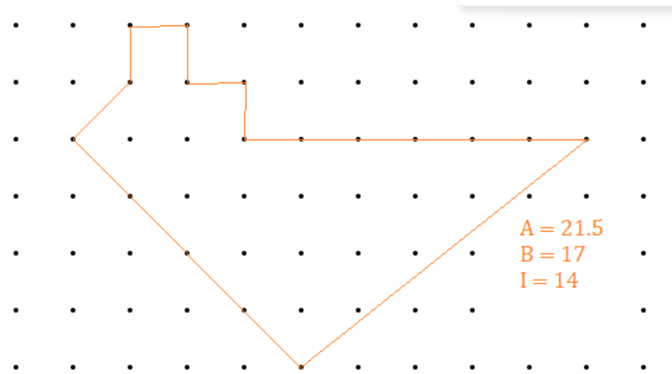
Now, edges. Each t_i has three faces, but B total faces border the exterior of the polygon rather than any other t_i. Each interior face is shared by two t_i, so the number of edges is given by $e = \frac{3v-B}{2}$.

Combining these three results, we have $2A - \frac{6A-B}{2} + I + 1 \Longrightarrow A = I + \frac{B}{2} - 1$, completing the proof [for the most part]! Below is an example of one of these graphs:





23.



In fact, $21.5 = 14 + \frac{17}{2} - 1$, so Pick's theorem holds here.

24.

Conjecture. We can only construct lattice polygons with area which is an integer multiple of $\frac{1}{2}$.

Proof. Take Pick's formula: $A = I + \frac{B}{2} - 1$. We must have $2A = (2I + B - 2) \in \mathbb{Z}$ so $\exists k \in \mathbb{Z}$ such that $A = k\frac{1}{2}$, completing the proof.

25.

Conjecture. There exist lattice line segments with irrational length.

Proof. Example: $(0,0) \longrightarrow (1,1)$ has a length of $\sqrt{2} \notin \mathbb{Q}$.

26.

Conjecture. The square of the length of any lattice line segment is an integer.

Proof. Without loss of generality we can set one end of the lattice line segment at $(0,0)$. The other end of this line segment falls at (a,b). Thus, by the Pythagorean theorem, the length of the line segment is $\sqrt{a^2+b^2}$. Thus, the square of the length of the general line segment is $(a^2+b^2) \in \mathbb{Z}$, the latter statement coming from the closure of the integers under multiplication and addition.

27.

Conjecture. A line with rational slope which passes through at least one lattice point has a rational y-intercept.

Proof. We know we can define the the line L as the set of points (x,y) which satisfy $y = mx + b$ for some slope m and some y-intercept b. If m is rational, then $\exists p, q \in \mathbb{Z}$ such that $m = \frac{p}{q}$. Note $q \neq 0$ because the slope would be undefined then.

Let's name one of the lattice points lying on L (x_0, y_0). Of course, $x_0, y_0 \in \mathbb{Z}$ by the definition of the lattice plane. Thus, we can write the equation

$$y_0 = \frac{p}{q} \cdot x_0 + b$$

or

$$b = (y_0 - \frac{p}{q} x_0) \in \mathbb{Q}$$

The rationality is the product of the closure of the rational numbers under addition and multiplication.

28.

Conjecture. If L is a line with rational slope in the plane and a lattice point lies on that line, then an infinite number of lattice points must lie on the line.

Proof. We can define $L = \{(x, y) : y = mx + b\}$ for some $m, b \in \mathbb{Q}$ (from the previous result). We know that there is at least one lattice point on the line, so let's call that (x_0, y_0) allowing us to write

$$y_0 = \frac{p}{q} x_0 + b$$

where $m = \frac{p}{q}$ for $p, q \in \mathbb{Z}$. We can construct an infinite number of points that also lie in L. Namely the points $P_n = (x_0 + nq, y_0 + np)$ where $n \in \mathbb{Z}$. We can prove this by plugging the points P_n into the condition for L:

$$y_0 + np = \frac{p}{q}(x_0 + nq) + b = \frac{p}{q} x_0 + np + b$$

subtracting off np we get the true statement for our initial point

$$y_0 = \frac{p}{q} x_0 + b$$

Thus, because n can take on an infinite number of values, there are an infinite number of lattice points on the line.

29.

Conjecture. If $P = (m, n)$ is a lattice point on the plane with $gcd(m, n) = 1$, then there are no lattice points strictly between $(0, 0)$ and p lying on the line segment $(0, 0) \to p$. (Note, this is actually a bijection and the other direction is part of the next proof)

Proof. Consider the line containing the origin and point (m, n). Its slope is $\frac{n}{m}$ so we can represent this line with the equation $y = \frac{n}{m} x$. Let's assume (for the purpose of contradiction) that there exists some point on that line (α, β) where $\alpha < m$ and $\beta < n$. Because (α, β) lies on the line segment, the following statement must hold true:

$$\beta = \frac{n\alpha}{m}$$

Because $\beta \in \mathbb{Z}$, we necessarily have $m | (n\alpha)$ but $m \nmid n$ so $m | \alpha$. We arrive at a contradiction because we supposed $m > \alpha$ and so $m \nmid \alpha$.

30.

Conjecture. 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 $t \in \mathbb{Z}$.

Proof. Firstly, let's show that if p is visible from the origin, then $gcd(m, n) = 1$. Assume some point (m, n) is visible from the origin and that $gcd(m, n) > 1$, an equivalent statement to $gcd(m, n) \neq 1$ as $0 < gcd(m, n) \in \mathbb{Z}$. Therefore, $\exists 1 < k \in \mathbb{N}$ such that $k|m$ and $k|n$. Let's call $\frac{m}{k} = \alpha$ and $\frac{n}{k} = \beta$. We have

$$L = \{(x, y) : y = \frac{n}{m} x\}$$

so $(\alpha, \beta) \in L$. Because $k > 1$, $\alpha < m$ and $\beta < n$ so (α, β) necessarily lies on the segment of L between $(0, 0)$ and p, violating our visibility condition for p. Thus, by way of a contradiction, we know that the visibility of p implies $gcd(m, n) = 1$. This taken together with the result from the previous exercise shows that the visibility of p is equivalent to the statement $gcd(m, n) = 1$. I.e. we know that $gcd(m, n) = 1$ because we are given p is visible.

As stated before, we have

$$L = \{(x, y) : y = \frac{n}{m}x\}$$

so we must have any point on L satisfy

$$my = nx$$

Clearly $n|nx \implies n|my \implies n|y$ by the gcd condition. Similarly, $m|my \implies m|nx \implies m|x$. Thus, we can write

$$x = t_1 m \quad y = t_2 n \quad \text{for } t_{1,2} \in \mathbb{Z}$$

But we need (x, y) to satisfy

$$my = nx$$

or

$$mt_2 n = nt_1 m \implies t_1 = t_2 = t$$

Thus $(x, y) = (tm, tn)$, completing our proof!

Note.

The following two proofs are identical in structure to those that Devi presented in class – so I would like to thank her for these ideas!

31.

Conjecture. If $n, m \in \mathbb{Z}^+$ there are exactly $gcd(m, n) - 1$ lattice points on the line segment between the origin and the point (m, n), not including endpoints.

Proof. Let (α, β) be the visible point on the line in question. By the nature of the line, there is only one visible point lying along it in the given direction. By the converse of 29 (which we proved in 30), we have $gcd(\alpha, \beta) = 1$. Thus, we know $\exists t \in \mathbb{Z}$ such that $(m, n) = (t\alpha, t\beta)$. Of course, $t|m$ and $t|n$. Now lets assume that $t < k \ \forall k$ such that $k|m, n$. Call $\frac{m}{k} = \gamma$ and $\frac{n}{k} = \delta$. Because $k > t$, $\gamma < \alpha$ and $\delta < \beta$. Of course, $(x, y) = (\gamma, \delta)$ satisfy the equation $y = \frac{n}{m}x$. But this contradicts the visibility of (α, β), meaning $t = gcd(m, n)$ by way of contradiction. Note that all lattice points on the given line segment must be of the form $(\tau\alpha, \tau\beta)$ per 30, so $\exists t$ points between (α, β) and (m, n) inclusive. Subtracting off the endpoint, $\exists t - 1$ points between $(0, 0)$ and (m, n) exclusive, completing the proof!

32.

Conjecture. If P is a lattice $n - gon$ with vertices

$$p_0 = (0, 0) \quad p_1 = (a_1, b_1) \quad p_2 = (a_2, b_2) \ \cdots \ p_n = (a_n, b_n)$$

then

$$B(P) = \sum_{i=1}^{n} gcd(a_{i+1 \mod n+1} - a_i, b_{i+1 \mod n+1} - b_i)$$

Proof. Let's imagine translating the n-gon n different times so that at time i the vertex p_i is at the origin. I.e. make the translation that takes $p_i \mapsto (0, 0)$ and thus $p_{i+1} \mapsto (a_{i+1 \mod n+1} - a_i, b_{i+1 \mod n+1} - b_i)$. By 31, there exists $gcd(a_{i+1 \mod n+1} - a_i, b_{i+1 \mod n+1} - b_i) - 1$ points on that segment, and so $gcd(a_{i+1} - a_i, b_{i+1 \mod n+1} - b_i)$ points excluding p_i. We know we have to do this n times to count up all of the boundary points, so

$$B(P) = \sum_{i=1}^{n} gcd(a_{i+1 \mod n+1} - a_i, b_{i+1 \mod n+1} - b_i)$$

33.

Take

$$\vec{u} = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} \qquad \vec{v} = \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix}$$

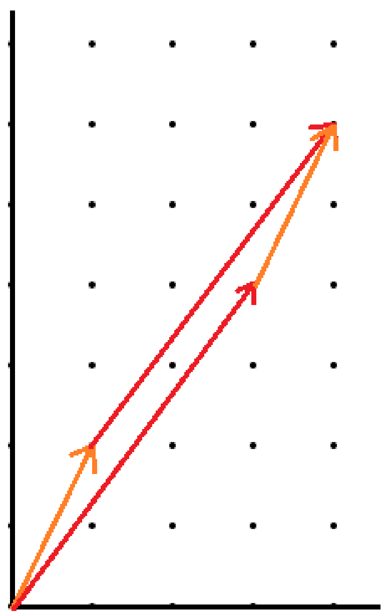
$$\vec{u} + \vec{v} = \begin{bmatrix} 6 \\ 8 \\ 10 \\ 12 \end{bmatrix}$$

34.

Take

$$\vec{u} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \qquad \vec{v} = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

$$\vec{u} + \vec{v} = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$$



35.

Take $\vec{u} = 5\hat{\imath} + 4\hat{\jmath}$. $2\vec{u} = 10\hat{\imath} + 8\hat{\jmath} = -2\vec{u}$. All scalar multiples of $\vec{u}$ lie on the span of $\vec{u}$ (on the same line).

36.

$$\frac{1}{2}\begin{pmatrix} -2 \\ 5 \end{pmatrix} + 3\begin{pmatrix} 4 \\ 1 \end{pmatrix} - 2\begin{pmatrix} \frac{3}{4} \\ 8 \end{pmatrix} = \begin{pmatrix} 9.5 \\ -10.5 \end{pmatrix}$$

37.

$$\begin{pmatrix} 8 \\ -12 \end{pmatrix} = 2\begin{pmatrix} 2 \\ -3 \end{pmatrix} + \begin{pmatrix} 4 \\ -6 \end{pmatrix}$$

38.

Using the definition of linear independence, we can try to solve for c_1 and c_2 in the equations

$$c_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + c_2 \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \vec{0}$$

$$c_1 + 3c_2 = 0$$

$$2c_1 + 4c_2 = 0$$

-2 times the first equation plus the second equation gives:

$$-2c_2 = 0 \Longrightarrow c_2 = 0 \Longrightarrow c_1 = 0$$

so, by the definition given for linear independence, these vectors are linearly independent.

39.

The given vectors are clearly not linearly independent, because

$$c_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + c_2 \begin{pmatrix} -3 \\ -6 \end{pmatrix} = k \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

for some k, so we can't produce vectors off the span of $\binom{1}{2}$. Also, purely by the definition, there are clearly an infinite c_1, c_2 that zero the equation. An example is $c_1 = 3, c_2 = 1$.

40.

a.

Yes, $\{\binom{1}{2}, \binom{3}{4}\}$ is a basis. Per 38, $\{\binom{1}{2}, \binom{3}{4}\}$ is a linearly independent set, and we can write the two equations

$$c_1 + 3c_2 = a$$

$$2c_1 + 4c_2 = b$$

which has the solution

$$c_1 = -2a + \frac{3}{2}b \qquad c_2 = a - \frac{1}{2}b$$

these satisfy the conditions for a basis.

b.

This isn't a $\mathbb{Z}$-basis because, for example, take $(a, b) = (1, 1)$ which produces $c_1 = -\frac{1}{2}$ and $c_2 = \frac{1}{2}$ which cannot form a $\mathbb{Z}$-linear combination.

41.

Take $\begin{bmatrix} -11 & 3 \\ 4 & -1 \end{bmatrix}$. Clearly

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

42.

Take $A^{-1} = -\frac{1}{2} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix}$. We have

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

43.

Th general result for any 2×2 matrix is given in problem 45 (which I did before this one), so let's use that formula to show that

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

has no inverse.

Clearly, the determinant is $det(A) = 4 - 4 = 0$, so $\frac{1}{det(A)}$ is undefined, and so too is the inverse. Note, we could have done the special case for A if we just took a, b, c, d to be their values given in A and applied the same technique as showed in 45.

44.

a.

Take

$$A_1 = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad A_2 = \begin{bmatrix} 5 & 7 \\ 6 & 8 \end{bmatrix} \quad \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{2}{3} & 1 \end{bmatrix}$$

The inverses are

$$A_1^{-1} = -\frac{1}{2} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} \quad A_2^{-1} = -\frac{1}{2} \begin{bmatrix} 8 & -7 \\ -6 & 5 \end{bmatrix} \quad A_3^{-1} = -\frac{1}{6} \begin{bmatrix} 1 & -1 \\ \frac{-2}{3} & \frac{1}{2} \end{bmatrix}$$

These inverses exist (verify them!), so the given matrices must be invertible in $\mathbb{R}^2$.

b.

Take the matricies

$$B_1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \quad B_2 = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \quad B_3 = \begin{bmatrix} \pi & \pi e \\ \phi & \phi e \end{bmatrix}$$

Again, I will just use the result given in 45 (which I proved before doing this problem) and cite the fact that the determinant of each of these matrices is 0 so that formula produces an undefined inverse.

c.

Again, as we saw from 45, we need $det(A) \neq 0$ for there to be an inverse of A.

45.

Conjecture. Take $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. If $ad - bc = det(A) \neq 0$ then A is invertible and $A^{-1} = \frac{1}{det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Proof 1. Let

$$B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

and let's find $\alpha, \beta, \gamma, \delta$ such that $AB = I$ or

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, we have the four equations

$$a\alpha + b\gamma = c\beta + d\delta = 1 \qquad a\beta + b\gamma = c\alpha + d\gamma = 0$$

We can pop this system into a matrix and row-reduce:

$$\begin{bmatrix} a & 0 & b & 0 & 1 \\ 0 & c & 0 & d & 1 \\ c & 0 & d & 0 & 0 \\ 0 & a & 0 & b & 0 \end{bmatrix}$$

$$cR_1 - aR_3 \to R_1 \qquad cR_4 - aR_2 \to R_4$$

$$\begin{bmatrix} 0 & 0 & cb-ad & 0 & c \\ 0 & c & 0 & d & 1 \\ c & 0 & d & 0 & 0 \\ 0 & 0 & 0 & bc-ad & -a \end{bmatrix}$$

$$dR_1 + (ad-cb)R_3 \to R_3 \qquad (ad-bc)R_2 + dR_4 \to R_2$$

$$R_3 = \frac{R_3}{c} \qquad R2 = \frac{R_2}{c}$$

$$\begin{bmatrix} 0 & 0 & cb-ad & 0 & c \\ 0 & ad-bc & 0 & 0 & -b \\ ad-bc & 0 & 0 & 0 & d \\ 0 & 0 & 0 & bc-ad & -a \end{bmatrix}$$

$$R_3 \leftrightarrow R_1$$

$$\begin{bmatrix} ad-bc & 0 & 0 & 0 & d \\ 0 & ad-bc & 0 & 0 & -b \\ 0 & 0 & ad-bc & 0 & -c \\ 0 & 0 & 0 & ad-bc & a \end{bmatrix}$$

$$R_{1,2,3,4} \cdot \frac{1}{ad-bc}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \frac{d}{ad-bc} \\ 0 & 1 & 0 & 0 & \frac{b}{bc-ad} \\ 0 & 0 & 1 & 0 & \frac{c}{bc-ad} \\ 0 & 0 & 0 & 1 & \frac{a}{ad-bc} \end{bmatrix}$$

so $\alpha = \frac{d}{ad-bc}$, $\beta = \frac{b}{bc-ad}$, $\gamma = \frac{c}{bc-ad}$, and $\delta = \frac{a}{ad-bc}$.

Thus we have

$$B = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = A^{-1}$$

Clearly, A^{-1} does not exist if $det(A) = 0$.

46.

We can simply find the inverse of A, and note that it has integer entries!

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

We have

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

which satisfies the definition for invertibility.

47.

Let's try to construct an inverse (which we know to be *the* inverse in $\mathbb{R}^2$) using the formula found in exercise 45. That is

$$\left[A^{-1} = \tfrac{-1}{2} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} \right]$$

This clearly does not have integer entries, so we know A is not invertible in $\mathbb{Z}^2$.

48.

Let's examine

$$A_1 = \begin{bmatrix} 1 & 3 \\ 1 & 4 \end{bmatrix} \qquad A_2 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \qquad A_3 = \begin{bmatrix} 6 & 7 \\ 1 & 1 \end{bmatrix}$$

a.

We will show that these are invertible over $\mathbb{Z}$ by verifying inverses with integer entries.

$$A_1^{-1} = \begin{bmatrix} 4 & -3 \\ -1 & 1 \end{bmatrix} \qquad A_1A_1^{-1} = \begin{bmatrix} 1 & 3 \\ 1 & 4 \end{bmatrix}\begin{bmatrix} 4 & -3 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$A_2^{-1} = \begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix} \qquad A_2A_2^{-1} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$A_3^{-1} = \begin{bmatrix} 6 & 7 \\ 1 & 1 \end{bmatrix} \qquad A_3A_3^{-1} = \begin{bmatrix} 6 & 7 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 6 & 7 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

b.

A few very simple computations yield $det(A_1) = 1$ and $det(A_2) = det(A_3) = -1$.

d.

I conjecture (I know, in fact, but that proof is later) that for a matrix A to be invertible over $\mathbb{Z}$, we must have $det(A) = \pm 1$.

49.

Conjecture. If A is a 2×2 matrix with entries in $\mathbb{Z}$, then A is invertible over $\mathbb{Z}$ if and only if $det(A) = \pm 1$.

Proof. We must prove two directions. The first being

$$det(A) = \pm 1 \Longrightarrow \exists A^{-1} \in M_{2\times 2}(\mathbb{Z})$$

The second direction being

$$\exists A^{-1} \in M_{2\times 2}(\mathbb{Z}) \Longrightarrow det(A) = \pm 1$$

Let's start with the first direction. Ex45 shows that if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Thus, if $det(A) = \pm 1$, A^{-1} is clearly well defined, and so exists.

Now for the reverse direction. This follows the logic given in Ryan's presentation. If A is invertible, then A^{-1} exists and is equal to

$$\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

by EX45. If A is $\mathbb{Z}$ invertible, then we know $a, b, c, d \in \mathbb{Z}$ by definition. Thus, $det(A^{-1}) \in \mathbb{Z}$.

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

Proof of lemma. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Thus, $det(A) = ad - bc \in \mathbb{Z}$. By $Ex45$ $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ so $det(A^{-1}) = \frac{ad-bc}{(ad-bc)^2} = \frac{1}{ad-bc} = \frac{1}{det(A)}$. This completes the proof of the lemma!

Where were we... Oh yes, if $det(A^{-1}) \in \mathbb{Z}$ (it is, from invertibility) then $\frac{1}{det(A)} \in \mathbb{Z}$. If $\det A \in \mathbb{Z}$ then $det(A) = \pm 1$ because ± 1 are the only integers whose inverses are also integers! This completes the proof.

50.

Conjecture. $\forall k \in \mathbb{R}\ \exists n \in \mathbb{R}$ such that $k \cdot n = 1$.

Proof. Take $n = \frac{1}{k}$. We know $n \in \mathbb{R}$ because of the closure of the real numbers under division.

51.

Conjecture. ± 1 are the only integers that have a multiplicative inverse in the integers.

Proof. We can first show that ± 1 do have multiplicative inverses in $\mathbb{Z}$. Clearly $-1 \cdot -1 = 1$ and $1 \cdot 1 = 1$. Now take some $k \in \mathbb{Z}/\{\pm 1\}$. Because $\mathbb{Z} \subset \mathbb{R}$, if k any multiplicative inverse of k in $\mathbb{Z}$ must also be a multiplicative inverse of k in $\mathbb{R}$. We know that there exists a unique multiplicative inverse for k in $\mathbb{R}$, $\frac{1}{k}$, so the only possible multiplicative inverse for k in $\mathbb{Z}$ is also $\frac{1}{k}$. Because $0, 1 \neq k \in \mathbb{Z}$ we have $|k| > 1$ and so $|\frac{1}{k}| < 1$ which directly implies that $\frac{1}{k} \notin \mathbb{Z}$. This completes the proof.

52.

Let's use the bases

$$\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\} \quad \{\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\3\end{pmatrix}\} \quad \{\begin{pmatrix}1\\7\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}\}$$

a.

We will show that these are bases for $\mathbb{R}^2$ by finding a $c_1, c_2 \in \mathbb{R}$ such that the equation $c_1\vec{v} + c_2\vec{u} = \vec{\alpha}$ has a distinct solution. The first set is trivial:)

$$c_1 = a \qquad c_2 = b$$

For the second set we have

$$c_1 + c_2 = a \qquad 2c_1 + 3c_2 = b$$

which has the solution

$$c_1 = 3a - b \qquad c_2 = b - 2a$$

For the third set we have

$$c_1 + c_2 = a \qquad 7c_1 + 2c_2 = b$$

which has the solution

$$c_1 = \frac{b - 2a}{5} \qquad c_2 = \frac{7a - b}{5}$$

In all of these cases, we found the solutions algebraically – in a reversible manner – so the solutions are unique.

b.

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

$$det(\begin{bmatrix}1 & 1\\2 & 3\end{bmatrix}) = 1$$

$$det(\begin{bmatrix}1 & 7\\1 & 2\end{bmatrix}) = -5$$

We should have $det(A) \neq 0$ where A is the matrix in question.

c.

Conjecture. If $\{\vec{v}, \vec{w}\}$ forms a basis for $\mathbb{R}^2$, then the determinant of the matrix $[\vec{v} \quad \vec{w}]$ must not be equal to 0.

Proof. If $\{\vec{v}, \vec{w}\}$ forms a basis for $\mathbb{R}^2$ then $\exists c_1, c_2, c_3, c_4 \in \mathbb{R}$ such that

$$c_1\vec{v} + c_2\vec{w} = \begin{pmatrix}1\\0\end{pmatrix}$$

and

$$c_3\vec{v} + c_4\vec{w} = \begin{pmatrix}0\\1\end{pmatrix}$$

These two vector equations correspond exactly to the matrix multiplication

$$\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix} \begin{bmatrix} c_1 & c_3 \\ c_2 & c_4 \end{bmatrix} = I$$

Thus, the matrix $A = \begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix}$ is invertible (its inverse is the coefficient matrix above) and by Ex. 45 $det(A) \neq 0$ to guarantee the existence of that inverse.

53.

Let's take the sets

$$\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\} \quad \{\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}\} \quad \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}\}$$

a.

We will show (in the exact same way as the previous problem) that these are $\mathbb{Z}-$bases by finding a c_1, c_2 such that the equation $c_1\vec{v} + c_2\vec{u} = \vec{\alpha}$ has a distinct solution. The first set is trivial:)

$$c_1 = a \qquad c_2 = b$$

For the second set we have

$$c_1 + c_2 = a \qquad 2c_1 + 3c_2 = b$$

which has the solution

$$c_1 = 3a - b \qquad c_2 = b - 2a$$

For the third set we have

$$c_1 + c_2 = a \qquad c_1 + 2c_2 = b$$

which has the solution

$$c_1 = 2a - b \qquad c_2 = b - a$$

In all of these cases, we found the solutions algebraically – in a reversible manner – so the solutions are unique.

b.

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

$$det(\begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}) = 1$$

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

I suspect the determinants have to be ± 1. All of these values are 1, and if we just switch the columns we get a determinant of -1.

c.

Conjecture. The determinant of a matrix whose columns form a $\mathbb{Z}-$basis for $\mathbb{Z}^2$ is ± 1.

Proof. If $\{\vec{v}, \vec{w}\}$ form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$ then $\exists c_1, c_2, c_3, c_4 \in \mathbb{Z}$ such that

$$c_2\vec{v} + c_2\vec{w} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and

$$c_3\vec{v} + c_4\vec{w} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

These two vector equations are precisely the matrix equation

$$\begin{bmatrix} v_1 & w_1 \\ v_2 & w_2 \end{bmatrix} \begin{bmatrix} c_1 & c_3 \\ c_2 & c_4 \end{bmatrix} = I$$

Thus $A = [\vec{v} \quad \vec{w}]$ is $\mathbb{Z}$ invertible. By Ex. 48, we must have $det(A) = \pm 1$.

54.

a.

We know that the area of the parallelogram spanned by two vectors $\vec{u}, \vec{v}$ is just $|det([\vec{u} \quad \vec{v}])|$, so we have, by part b of the previous problem, that all of the areas of the parallelograms given in 53 are 1.

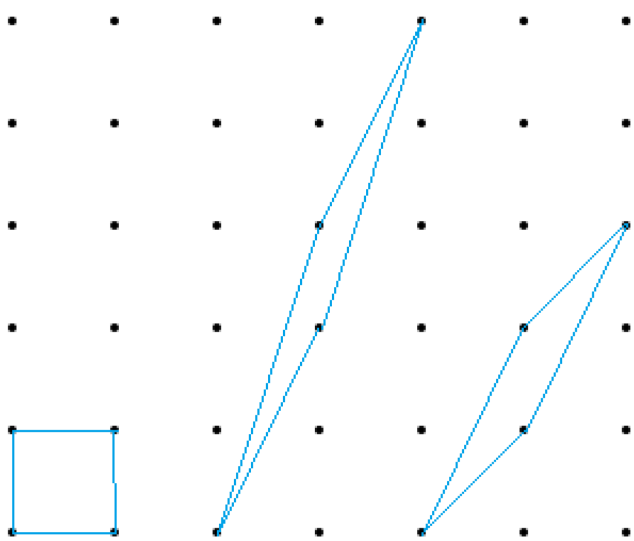
b.

Let's consider the linear transformation that takes $\binom{1}{0} \mapsto \vec{v}$ and $\binom{0}{1} \mapsto \vec{w}$. In matrix form, that is

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

It follows directly from part c of the previous problem that the area of the corresponding parallelogram (the image of the lattice square under the transformation) is 1.

55.



a.

There are always 4 boundary points and 0 interior points.

b.

Conjecture. If $P(\vec{v}, \vec{w})$ is the parallelogram spanned by $\vec{v}$ and $\vec{w}$ where $\{\vec{v}, \vec{w}\}$ forms a $\mathbb{Z}$-basis for $\mathbb{Z}^2$, then $I(P) = 0$ and $B(P) = 4$

Proof. Without loss of generality, place one corner of the parallelogram at the origin (this is implicitly assumed in the definition given in the course reader). $\{\vec{v}, \vec{w}\}$ being a $\mathbb{Z}$ basis implies that the corners of P adjacent to the origin are visible from the origin and that the far corner is visible from the two origin-adjacent corners (just translate by $-\vec{v}$ or $-\vec{w}$, so that we can use the same visibility result). Thus $B(P) = 4$. [this next part uses logic which Eddy used in one of his presentations] Now assume there exists a point $\alpha = (a, b)$ for $a, b \in \mathbb{Z}$ (which we will sometimes refer to by the vector α) that lies inside the parallelogram. Because $\{\vec{v}, \vec{w}\}$ is a $\mathbb{Z}-$basis, there must exist $c_1, c_2 \in \mathbb{Z}$ such that $c_1\vec{v} + c_2\vec{w} = \vec{\alpha}$. But, because $\alpha \in P(\vec{v}, \vec{w})$ we have $0 < c_1, c_2 < 1$ by the definition of P, so $c_1, c_2 \notin \mathbb{Z}$ bringing us to a contradiction. Thus, $I(P) = 0$.

56.

Conjecture. If $P(\vec{v}, \vec{w})$ is a primitive lattice parallelogram, then $\{\vec{v}, \vec{w}\}$ must be a $\mathbb{Z}$-basis for $\mathbb{Z}^2$.

Proof. Because $\vec{v}$ and $\vec{w}$ form a nontrivial lattice parallelogram, they must span $\mathbb{R}^2$, For that same reason, they must be linearly independent. Thus, $\{\vec{v}, \vec{w}\}$ is a basis for $\mathbb{R}^2$. As a result, we can write any point $\vec{\alpha} \in \mathbb{Z}^2 \subset \mathbb{R}^2$ as

$$\vec{\alpha} = c_1\vec{v} + c_2\vec{w}$$

Now suppose that $\exists\vec{\alpha} \in \mathbb{Z}^2$ such that, in the expression above, $c_{1,2} \notin \mathbb{Z}$. I.e., assume that $\{\vec{v}, \vec{w}\}$ does not form a $\mathbb{Z}$ basis for $\mathbb{Z}^2$.

Now perform the transformation T defined by the vector $\vec{\tau} = -\lfloor c_1 \rfloor\vec{v} - \lfloor c_2 \rfloor\vec{w}$. This transformation is a translation that performs the following to the arbitrary vector $\vec{\gamma}$:

$$T : \vec{\gamma} \mapsto \vec{\gamma} + \vec{\tau}$$

Because $\lfloor c_{1,2} \rfloor \in \mathbb{Z}$, the image of any lattice point under T must also be a lattice point. Now we consider $T(\vec{\alpha})$.

$$T : \vec{\alpha} \mapsto \vec{\alpha} + \vec{\tau} = (c_1 - \lfloor c_1 \rfloor)\vec{v} + (c_2 - \lfloor c_2 \rfloor)\vec{w}$$

Because we already noted that $c_{1,2} \notin \mathbb{Z}$, we have

$$0 < (c_1 - \lfloor c_1 \rfloor), (c_2 - \lfloor c_2 \rfloor) < 1$$

By the definition of $P(\vec{v}, \vec{w})$, $T(\alpha)$ must lie inside of $P(\vec{v}, \vec{w})$, contradicting the notion that $P(\vec{v}, \vec{w})$ is primitive. As a result, our assumption can't hold and $\{\vec{v}, \vec{w}\}$ must be a $\mathbb{Z}$ -basis for $\mathbb{Z}^2$.

Note, this argument was given by Ryan in class, so thanks to him for the initial idea to use the floor function!

57.

Conjecture. If vectors $\vec{v}$ and $\vec{w}$ form adjacent sides of the primitive lattice triangles T, then $\{\vec{v}, \vec{w}\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}^2$.

Proof. Consider the two transformations

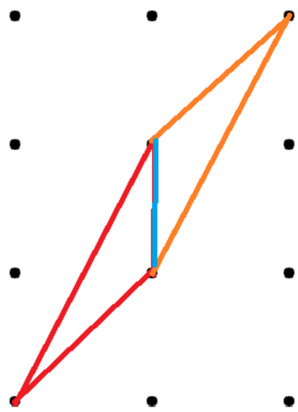
$$R(\vec{\gamma}) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \vec{\gamma} \text{ and } A(\vec{\gamma}) = \vec{\gamma} + \vec{v} + \vec{w}$$

which rotate a vector $\vec{\gamma}$ by π radians and translate it by $\vec{v} + \vec{w}$ respectively. (Yes, we could have said $R : \vec{\gamma} \mapsto -\vec{\gamma}$, but the intuition for rotation seems nicer).

A note on notation: we will use $R(T)$ and $A(T)$ to denote the lattice triangle that results after each of these transformations is performed on the component vectors of T.

The lattice plane has π rotational symmetry, so $R(T)$ will not include any lattice points. Likewise, the lattice plane is symmetric under integer translations, so $A(T)$ is still primitive. As a result, the successive transformations preserve the primitiveness of the lattice triangle.

We note that the four vectors must connect to the image of their partner($-\vec{v} + \vec{v} + \vec{w} = \vec{w}$ and $-\vec{w} + \vec{v} + \vec{w} = \vec{v}$). Thus, $T \cup R(A(T))$ is a primitive lattice parallelogram. A diagram is shown below.



From Ex56, $\{\vec{v}, \vec{w}\}$ must be a $\mathbb{Z}$-basis for $\mathbb{Z}^2$.

58.

Conjecture. The area of a primitive lattice triangle is $\frac{1}{2}$.

Proof. From Ex57 we have that the two vectors, call them $\vec{v}, \vec{w}$, spanning adjacent edges of the lattice triangle must form a $\mathbb{Z}$-basis for $\mathbb{Z}^2$. As a general property of determinants, we know $|det(\vec{v} \;\; \vec{w})|$ is the area of the primitive lattice parallelogram spanned by $\vec{v}$ and $\vec{w}$. From Ex53.c. we have that the determinant of the matrix $(\vec{v} \;\; \vec{w})$ is ± 1.

Thus, the area of the primitive lattice parallelogram spanned by $\vec{v}$ and $\vec{w}$ is 1. As a result, the area of the *triangle* spanned by $\vec{v}$ and $\vec{w}$ must be $\frac{1}{2}$. We justify this by noting that drawing the diagonal from $\vec{v}$ to $\vec{w}$ in the primitive lattice parallelogram spanned by $\vec{v}$ and $\vec{w}$ uniquely produces the primitive lattice triangle spanned by $\vec{v}$ and $\vec{w}$.

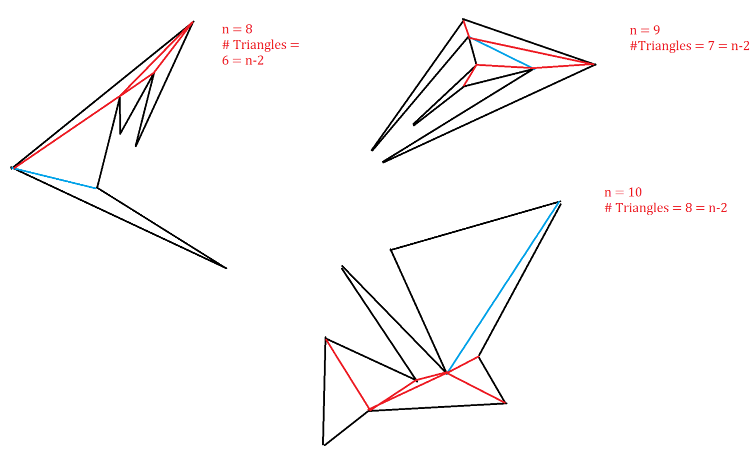
59.

Conjecture. Every convex n-gon can be dissected into $n-2$ triangles by means of non-intersecting diagonals.

Proof. Label the n vertices $v_1, \cdots, v_n$. Draw the dissection $\overline{v_1 v_i}$ for $i \in \{3, \cdots, n-1\}$. Clearly, this will dissect the polygon into triangles. We clearly draw $n-3$ diagonals, and that must produce $n-3+1 = n-2$ triangles (one for each diagonal plus the residual triangle produced by the last diagonal). We only drew diagonals from vertices, so the triangles must have vertices that are polygon vertices.

60.

I have thought of two ways to approach this problem, neither of which I have had time to execute on, so below are the examples to fulfill option 1. The blue diagonal is the first one, showing existence, and the remaining diagonals create the triangles.



My two ideas are: **1.** Let P be a path whose constituent points fall inside or on an edge of any given polygon. By the definition of a Jordan polygon, such a P must exist. By the well ordering axiom (I think), there must be a P with minimal length. Let's call this $\tilde{P}$. Note that, using the Euclidean metric, the shortest distance between two points is a line segment. Thus, if we have a minimal path P between the points v_1 and v_2 which must contain some point α falling between v_1 and v_2 then $P = \overline{v_1\alpha} \cup \overline{\alpha v_2}$. Note that this holds in general for n constraints, α_1 through α_n in that order, i.e.

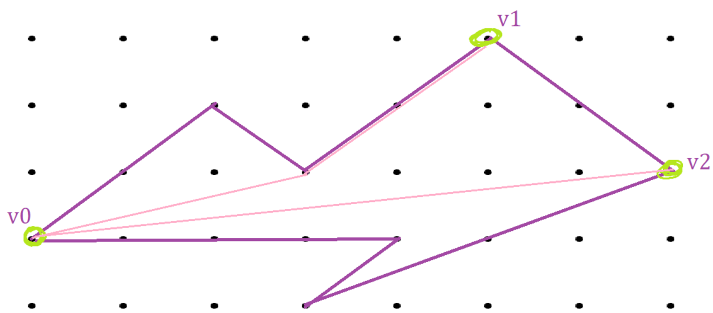
$$P = \bigcup_{i=1}^{n-1} \overline{\alpha_i \alpha_{i+1}}$$

where α_i and α_n are taken to be the endpoints themselves.

Here we need only prove that for a Jordan polygon there must exist some pair of vertices such that the minimal distance between them is not just the distance around the edges.

To do that we will start with two cases:

Case 1. The polygon has an odd number of sides. Pick any vertex of the polygon and call it v_0. Now pick the two vertices the largest number of sides away from v_0. Call them v_1 and v_2. We know that v_1 and v_2 are adjacent and that the number of sides between v_0 and v_1 or v_2 is $\lfloor \frac{n}{2} \rfloor$. Now, draw the shortest constrained path, as previously proven to exist, between v_0 and v_1, as well as between v_0 and v_2. You can think of this as looping a string around v_0 and $v_{1,2}$ and then pulling it taught. Or don't image it this way... the intuition might overlook some important nuance to the mathematics. That idea is shown in the diagram below – the pink path is that shortest constrained path.



Either some subset of one of those shortest constrained paths lies fully within the interior of the polygon or it doesn't – it isn't too hard to see that is exhaustive. If they do, we have our diagonal because we defined $\tilde{P}$ to only be constrained by vertex points. If they lie entirely on the edges of the polygon, we have to use the following bit of logic.

We start with a defined interior and exterior of our polygon. Note that, if neither shortest path between v_0 and $v_{1,2}$ has any portion lying completely within the interior of the polygon, then every angle of that polygon is necessarily $\geq \pi$. If there were any angle less than π, there would be a portion of the path lying in the interior of the polygon. Now, if we add an extra bit to our path between v_1 and v_2 (a path that necessarily lies only along a side of the polygon), we have a closed curve with all angles $\geq \pi$. We now take the complement of the set we considered to be the interior of the polygon initially. Now the new interior of the polygon has interior angles that are the complement of the previous interior angles. I.e. all interior angles of the "new" polygon (really just a new way of looking at the old one) are $\leq \pi$. Thus, the polygon is convex and we can use Ex59 to triangulate it!

Case 2: The polygon has an even number of sides. Repeat the exact same process as in case 1 but define v_1 as the point $\frac{n}{2}$ sides away from v_0 and define v_2 as the point $\frac{n}{2} - 1$ edges away but such that the path from v_0 to v_1 does not overlap the path from v_0 to v_2. A diagram is below:

2. This thought is less formal and is likely difficult to formalize in general. That is, we leverage the Riemann mapping theorem. Let P be the open set defined by the given polygon, and let U be the unit disc in the complex plane. By the

Riemann mapping theorem, there exists a bijective holomorphic map between P and U. Denote the transformation $S : U \mapsto P$ (which I believe is a form of the Schwartz Christoffel transformation). Let $\{u_1, \cdots, u_n\}$ be the images of the polygon vertices $\{v_1, \cdots, v_n\}$ under S^{-1}. If we can find some subset of the $\{u_i, u_j\}$ such that $\overline{u_i u_j} \longrightarrow^{S^{-1}} \overline{v_i v_j}$ such that $\overline{v_i v_j}$ is a line, we have the initial result that we need to proceed.

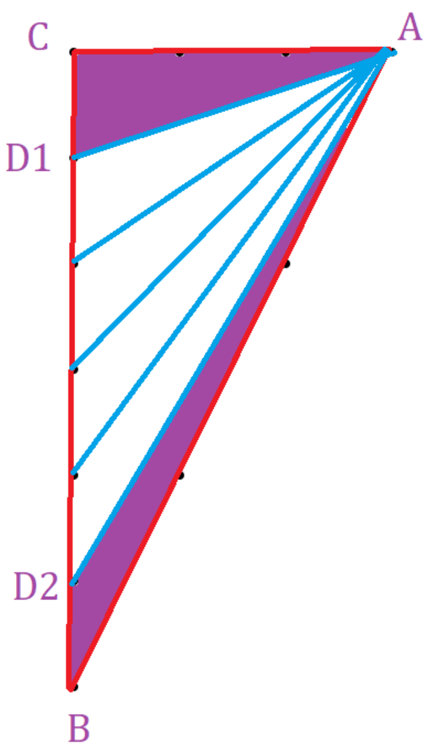
Note. The graph construction used below (used in the course reader) is different from the one I used in Ex22, but I believe both work!

61.

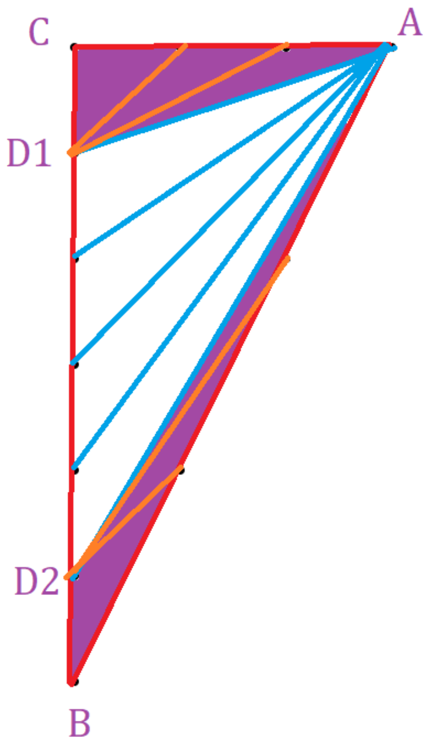
Conjecture. Every lattice triangle can be dissected into primitive lattice triangles.

Proof. We will prove this by induction on the number of interior points of the triangles.

Base Case: $I = 0$. In the case of a triangle with no interior points, we can begin by dissecting it into lesser triangles by drawing lines from one vertex to every boundary point on the opposite side. See the diagram below:

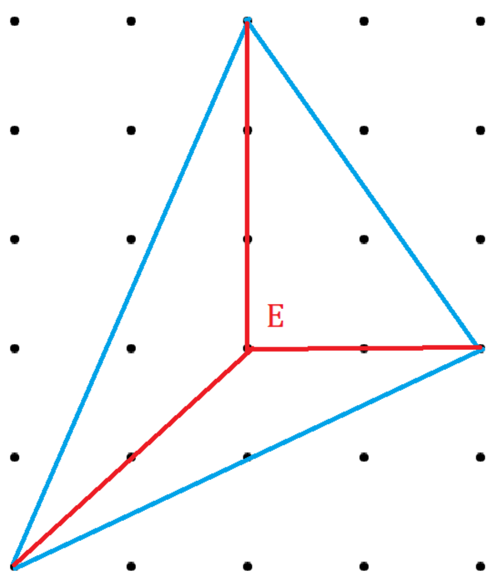


In this case we drew lines between vertex A and all lattice points lying along $\overline{CB}$. Note that all but two of these lesser triangles *must* be primitive. There are no interior points, no boundary points on the edges completely contained within the larger triangle, and no boundary points on the side opposite A (by the definition of our dissection). The other two triangles, shaded in purple, are not necessarily primitive, but we can dissect them in the following way.



Draw lines between boundary points D_1 and all boundary points lying along $\overline{AB}$, and do the same for D_2 and the points lying along $\overline{AC}$ (shown above in orange). These new triangles also *must* be primitive because we know there to be no lattice points on the lines $\overline{AD_1}$ and $\overline{AD_2}$, there to be no lattice points on the lines between $D_{1,2}$ and any boundary point of the original triangle, and there to be no boundary points *not now a vertex of a lesser triangle* on the edges $\overline{AB}$ and $\overline{AC}$. Finally note that all of this labeling was arbitrary and without loss of generality, so we can apply this argument to *any* lattice triangle. That finishes the proof of the base case.

Inductive Step.
Assume that a lattice triangle T with $I(T) \leq k$ can be dissected into primitive lattice triangles. Consider a lattice triangle with $k+1$ interior points. Choose one of the $k+1$ interior points, E, and draw the three line segments from that interior point to each of the vertices of the triangle.



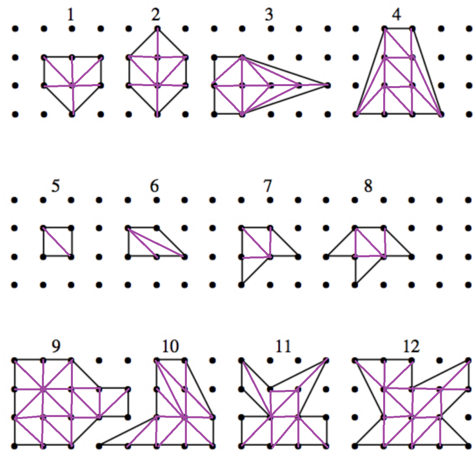
This trisects T into three smaller triangles with necessarily $\leq k$ interior points. We justify this by noting that one of the $k+1$ interior points of T is counted only as a boundary point in the new resulting lesser triangles. These lesser triangles, by the inductive hypothesis, can be dissected into primitive lattice triangles, and so T can be dissected into primitive lattice triangles. This completes the inductive step and the proof!

62.

Conjecture. Every lattice polygon can be dissected into primitive lattice triangles.

Proof. By Ex60 we know any lattice polygon can be dissected into lattice triangles. By Ex61 we know that every lattice triangle can be dissected into primitive lattice triangles. Taking these two statements together, we must have that every lattice polygon can be dissected into primitive lattice triangles.

63.



64.

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

Something's afoot! We have if Area of P $= \frac{k}{2}$ for some k, then $\#$ of regions of $G = k + 1 = 2v - e_b - 1$.

65.

Conjecture. In the graph deconstruction of a lattice polygon P, the number of faces in the graph, f, are related to the area of P by $f = 2A + 1$.

Proof. By Ex58, the area of each lattice triangle is $\frac{1}{2}$. Each lattice triangle defines one face of G, but there is one additional face (the outside), so $f = \#$ of PLTs $+ 1$. But, since P is fully triangulated, $\#$ triangles $= 2A$ where A is the area of P. Thus, $f = 2A + 1$.

66.

Note: This solution is essentially identical to Tarun's, I think it is likely the simplest!

Conjecture. In the graph deconstruction of P, let e_i denote the number of edges of the graph deconstruction inside the polygon. Let e_b denote the number of edges in the graph deconstruction that lie on the boundary of P. We must have $f = 2v - e_b - 1$

Proof. We start by counting the number of edges. There are three edges to each triangle face (that is to each face not the outside face). Thus, we can start with $e = 3(f-1)$ but we have to note that we are double counting each edge, and that we end up neglecting the boundary edges if we simply divide that by two, so we must really have $e = \frac{3(f-1)+e_b}{2}$. Applying Euler's formula for planar graphs (and the graph is planar) we have:

$$v - \frac{3(f-1)+e_b}{2} + f = 2 \Longrightarrow 2v - 3f + 3 - e_b + 2f = 4 \Longrightarrow 2v - f - e_b = 1 \Longrightarrow f = 2v - e_b - 1$$

That completes the proof!

67.

Conjecture. Pick's theorem.

Proof. By Ex66 we have $f = 2v - e_b - 1 = 2I + 2B - e_b - 1 = 2A + 1$ where the second equality is by Ex65. There is clearly a one-to-one correspondence between boundary edges and boundary lattice points, so we have $e_b = B$. Thus, $2A = 2I + B - 2$ or $A = I + \frac{B}{2} - 1$ which is Pick's theorem!

68.

Conjecture. $W(P)$ is finite.

Proof. $W(P) = \sum_{p\in\mathbb{Z}^2} w_p(P)$ must be finite because there are a finite number (namely $B(P)+I(P)$) of $p \in \mathbb{Z}^2$ for whom $a_p(P)$ is nonzero. Thus, there are a finite number of $p \in \mathbb{Z}^2$ such that $w_p(P)$ is nonzero. A sum of finitely many nonzero quantities is finite (just take the bound $2\pi(B(P) + I(P))$).

79.

Conjecture. (same as Ex1) It is not possible to construct a regular lattice triangle.

Proof. Assume it is possible to construct an equilateral lattice triangle. Say the triangle has side length d. The area is therefore $\frac{\sqrt{3}d^2}{4}$. By Pick's theorem, we know

$$\frac{\sqrt{3}d}{4} = I(P) + \frac{B(P)}{2} - 1$$

or

$$\sqrt{3}d^2 = 4I(P) + 2B(P) - 4$$

We must have $d = \sqrt{a^2+b^2}$ for $a, b \in \mathbb{Z}$, so $d^2 \in \mathbb{Z}$. Therefore $\sqrt{3}d^2 \notin \mathbb{Z}$. We do have, however, that $(4I(P)+2B(P)-4) \in \mathbb{Z}$ because $I, B \in \mathbb{Z}$. Thus, we have a contradiction, and so we cannot construct an equilateral lattice triangle.

80.

Conjecture. The area of a primitive lattice triangle is $\frac{1}{2}$.

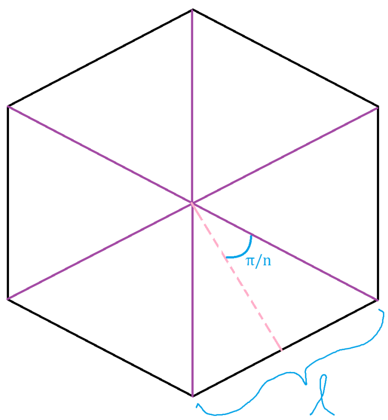
Proof. We will use Pick's theorem this time. I am not sure this is actually a valid method of proof, unless we can guarantee that there exists a proof of Pick's theorem that does not use the notion that the area of a primitive lattice triangle is $\frac{1}{2}$. That being said, here goes:

If P is a primitive lattice triangle than $B(P) = 3$ and $I(P) = 0$. Thus, $A = I(P) + \frac{B(P)}{2} - 1 = \frac{3}{2} - 1 = \frac{1}{2}$. Hooray!

81.

Conjecture. If there exists a regular lattice n-gon, then $tan(\frac{\pi}{n}) \in \mathbb{Q}$.

Proof. Refer to the following diagram:



We can find the area of the regular polygon by first finding the area of the component triangle subdivisions. Let's call the altitude of those triangles h, so we can find h via the tangent function:

$$h = \frac{l}{2tan\frac{\pi}{n}}$$

Thus, the area of the triangles A_t is

$$A_t = \frac{l^2}{4tan\frac{\pi}{n}}$$

Clearly, the area of the entire polygon is

$$A(P) = nA_t = \frac{nl^2}{4tan\frac{\pi}{n}}$$

So

$$tan\frac{\pi}{n} = \frac{nl^2}{4A}$$

If P is a lattice polygon, then we apply Pick's theorem to get

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

with the usual meanings for I and B. Clearly, I, B, and n are rational, as well as all of the constants. Note that by Ex26 l^2 is also rational. Thus, by the closure of $\mathbb{Q}$ under addition and multiplication, $tan\frac{\pi}{n} \in \mathbb{Q}$. This completes the proof!

82.

Conjecture. If P is a convex lattice pentagon, then the area of P must be greater than or equal to $\frac{5}{2}$. This bound is strict.

Proof. Let's consider the five vertices of the pentagon $\mod 2$. That is, for every vertex $v_i = (a_i, b_i)$, we consider $v_i \mod 2 = (a_i \mod 2, b_i \mod 2)$. We have two congruence classes for each co-ordinate, so four cases total. Namely:

$$(1,0); (1,1); (0,0); (0,1)$$

Note that these cases are exhaustive. There are five vertices so, by the pigeonhole principle, there are at least two vertices in the pentagon within the same class. This means that both the x co-ordinate and the y co-ordinate have the same parity for each. Without loss of generality, label these two vertices v_1 and v_2.

We have two cases.
Case 1: v_1 and v_2 are not adjacent.

Because each cross-vertex co-ordinate pair has the same parity, we must have

$$2|(a_2 - a_1) \text{ and } 2|(b_2 - b_1)$$

Thus, $gcd(a_2 - a_1, b_2 - b_1) \geq 2$ so by Ex31 there is at least one lattice point lying strictly between v_1 and v_2 on the line segment between them. This is an interior point because v_1 and v_2 are non-adjacent and the pentagon is assumed convex. By Pick's theorem, we must have

$$A \geq 1 + \frac{5}{2} - 1 = \frac{5}{2}$$

because we know $B(P) \geq 5$

Case 2: v_1 and v_2 are adjacent.

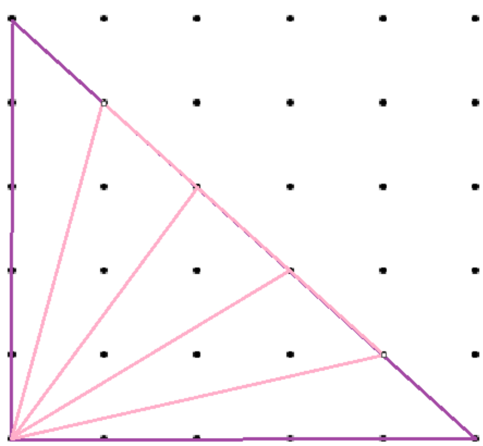
By the same logic as in case 1, there is a lattice point lying on the side of the pentagon between v_1 and v_2. Call that point v_6. Now repeat either case 1 or case 2 for the pentagon $v_2, \cdots, v_6$. Thus, there is either another boundary point or another interior point. Either way, by Pick's theorem again, $A \geq \frac{5}{2}$. This completes the proof!

83.

Conjecture. Let A denote the point $(n, 0)$ and let B denote the point $(0, n)$. Connect each lattice point along the side opposite the origin to the origin. If n is prime than each of the central triangles (pink) contains exactly the same number of lattice points. The number of such interior lattice points is given by

$$\#\text{of interior lattice points} = \frac{n-1}{2}$$

Proof. For the following proof, we will rely on the diagram below:



Let n be a prime number. Let's find $d = gcd(i, n-i)$. Because $d = gcd(i, n-i)$, $d|i$ and $d|(n-i)$ so d divides any linear combination of $n-i$ and i. In particular, $d|(n-i+i) \quad \therefore d|n$. By $d|(n-i)$ we know $d < n$ because $i > 0$, so we have $d = 1$ from the primality of n. As a result, all of the lattice points along the diagonal opposite the origin are visible from the origin (Ex29). Looking at any of the inner sub-triangles (the ones in pink) we note that there are no boundary points between the vertices on the side opposite the origin and there are no boundary points on the other two sides because of the result we just proved. Thus, we have that for all interior sub-triangles T_i, $B(T_i) = 3 = B$.

Now note that these triangles all have the same base and same height, and so they must have the same area. That area is just the area of the larger triangle over n, or $\frac{n}{2}$. So we know that $A(T_i) = \frac{n}{2} = A$. Now we apply Pick's theorem:

$$A = \frac{n}{2} = I + \frac{B}{2} - 1 = I + \frac{3}{2} - 1 = I + \frac{1}{2}$$

thus

$$I = \frac{n-1}{2}$$

This completes the proof.

Note: This is essentially Ethan's argument from in class, so thank you to him for presenting and giving this proof!

84.

Conjecture. If n is an integer greater than or equal to 3 then there exists a set of n points in the plane such that the distance between any two points is irrational but the area of a non-degenerate triangle formed by any three is rational.

Proof. We will prove this by constructing such a set (many sets, actually). Let's first construct

$$\mathcal{S} = \{(x, x^{2k}) : 0 < x \in \mathbb{Z}\} \text{ for each } 0 < k \in \mathbb{Z}$$

Now let's choose our sets $\mathcal{T} = \{(x_1, x_1^{2k}), (x_2, x_2^{2k}), \cdots, (x_n, x_n^{2k})\} \subset \mathcal{S}$. Let d be the distance between points (x_1, x_1^{2k}) and (x_2, x_2^{2k}). Clearly, we have

$$d = \sqrt{(x_2 - x_1)^2 + (x_2^{2k} - x_1^{2k})^2}$$

We can factor

$$(x_2^{2k} - x_1^{2k}) = (x_2 - x_1) \sum_{j=0}^{2k-1} x_2^{2k-j-1} x_1^j$$

For the sake of notation, let $A = \sum_{j=0}^{2k-1} x_2^{2k-j-1} x_1^j$. Thus,

$$d = \sqrt{(x_2 - x_1)^2 + (x_1 - x_2)^2 A^2} = |x_2 - x_1|\sqrt{1 + A^2}$$

Note that, by the closure of the integers under multiplication and addition, $A \in \mathbb{Z}$. Thus, $A^2 + 1$ is necessarily not a square number because the next square number greater than A^2 would be $(A+1)^2$, and if $A = 1$ then $A^2 + 1 = 2$ is not a square number. Finally, we note that $A \neq 0$ because we took $x_i > 0$ to be part of our definition of $\mathcal{S}$. Thus, $d = |x_2 - x_1|\sqrt{1 + A^2}$ is an irrational number, satisfying the irrational separation condition.

Now, note that the triangle formed by any 3-subset of $\mathcal{T}$ is necessarily non-degenerate because $\frac{d}{dx} x^{2k}|_{x_0=0} > 0 \quad \forall x_0 > 0, \forall 0 < k \in \mathbb{Z}$, i.e. there are no three points which are co-linear on the curve because x^{2k} is always increasing.

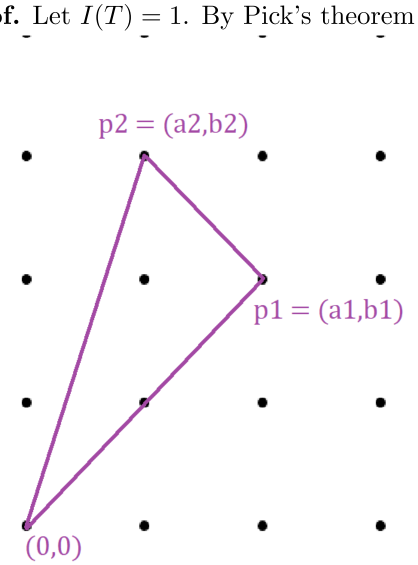
Finally, note that since $\mathcal{S}$ is defined as a set of integer tuples, all points in $\mathcal{T}$ must lie in $\mathbb{Z}^2$. By Pick's theorem (or the fact that we can dissect a lattice triangle into primitive lattice triangles that have area $\frac{1}{2}$), the triangle must have rational area. This completes the proof!

Note: This was entirely inspired by Sterling's beautiful solution with parabolas. I just extended it in a minor way. Also, I noticed upon finishing this that it can be further generalized *either* to any curve of the form x^k where k need not be even *or* $x \in R/\{0\}$ but not both. I am not entirely sure that this works yet, and I have some other things to do tonight, so I leave this modification for future Reed Michael.

85.

Conjecture. For a triangle T with $I(T) = 1$ we must have $B(T) \in \{3, 4, 6, 8, 9\}$.

Proof. Let $I(T) = 1$. By Pick's theorem $A = \frac{B}{2}$ or $B = 2A$.



Using the determinant area result, we can write the area as

$$A = \frac{1}{2}|det \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}| = \frac{1}{2}|det \begin{bmatrix} -a_1 & a_2 - a_1 \\ -b_1 & b_2 - b_1 \end{bmatrix}| = \frac{1}{2}|det \begin{bmatrix} -a_2 & a_1 - a_2 \\ -b_2 & b_1 - b_2 \end{bmatrix}|$$

$$\therefore B = |a_1 b_2 - a_2 b_1| = |b_1(a_2 - a_1) - a_1(b_2 - b_1)| = |b_2(a_1 - a_2) - a_2(b_1 - b_2)| \tag{1}$$

Now let's use Ex31 to note that the number of points on the sides, call those α, β, γ, can be written in terms of the *gcd*s of the co-ordinates of the vertices.

$$\alpha = gcd(a_1, b_1) \qquad \beta = gcd(a_2, b_2) \qquad \gamma = gcd(a_2 - a_1, b_2 - b_1)$$

By Ex32 we have $B = \alpha + \beta + \gamma$. Now note that since $\alpha | a_1, b_1$ and $\beta | a_2, b_2$ then $\alpha\beta | B$ by the first equality in 1. For the same reason, we must have $\alpha\gamma | B$ and $\gamma\beta | B$.

Without loss of generality, let $\alpha \geq \beta \geq \gamma$. Thus, $\alpha \geq \frac{B}{3}$. Also $\alpha\beta | B \implies \alpha, \beta | B$ and $\alpha\gamma | B \implies \gamma | B$. As a result, we must have $\alpha \in \{B, \frac{B}{2}, \frac{B}{3}\}$. If $\alpha = B$ then $\beta, \gamma = 0$ but $\beta | B$ and $\gamma | B$ so $\beta, \gamma \neq 0 \implies \alpha \in \{\frac{B}{2}, \frac{B}{3}\}$.

Now we have two cases.
Case 1. $\alpha = \frac{B}{2}$:
We must have $\beta + \gamma = \frac{B}{2}$. But $\beta | B$ so $\exists 0 < k \in \mathbb{Z}$ such that $\beta k = B$ which implies $\beta = \frac{B}{k}$. We know $k \neq 1$ because $\alpha \geq \beta$. We know $k \neq 2$ because we already showed $\gamma \neq 0$. If $k = 3$ then $\beta = \frac{B}{3}$ and $\gamma = \frac{B}{6}$. If $k = 4$ then $\beta = \frac{B}{3}$ and $\gamma = \frac{B}{4}$. We know that $k \leq 4$ because if $k > 4$ then $\gamma > \beta$ which contradicts the initial inequality we set up.

Case 2. $\alpha = \frac{B}{3}$:
We must have $\beta + \gamma = \frac{2B}{3}$. Again, $\exists 0 < k \in \mathbb{N}$ such that $\beta = \frac{B}{k}$. The assumption $\beta \leq \alpha$ implies $k \geq 3$. $k = 3$ makes $\beta = \frac{B}{3}$ and $\gamma = \frac{B}{3}$. We know that this is the only possible sub-case because if $k > 3$ then $\gamma > \beta$.

Our options are:

$$(\alpha, \beta, \gamma) = (\frac{B}{2}, \frac{B}{3}, \frac{B}{6}), (\frac{B}{2}, \frac{B}{4}, \frac{B}{4}), (\frac{B}{3}, \frac{B}{3}, \frac{B}{3})$$

We have

$$\alpha\beta | B \implies (\frac{B^2}{6} | B) \vee (\frac{B^2}{8} | B) \vee (\frac{B^2}{9} | B)$$

$$\therefore \exists l \in \mathbb{Z} : (\frac{B^2 l}{6} = B) \vee (\frac{B^2 l}{8} = B) \vee (\frac{B^2 l}{9} = B)$$

This implies

$$(Bl = 6) \vee (Bl = 8) \vee (Bl = 9)$$

so

$$(B | 6) \vee (B | 8) \vee (B | 9)$$

as a result

$$B \in \{1, 2, 3, 6\} \cup \{1, 2, 4, 8\} \cup \{1, 3, 9\} = \{1, 2, 3, 4, 6, 8, 9\}$$

But $B \geq 3$ so $B \in \{3, 4, 6, 8, 9\}$
This completes the proof!

86.

By simply adding the fully reduced fractions with denominators 6 and 7 and then ordering them properly, we get

$$F_6 = \{\frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{8}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1}\}$$

$$F_7 = \{\frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{8}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}\}$$

87.

a.

Conjecture. F_n contains F_k for all $k \leq n$.

Proof. Note that if we have $a \in F_k$ then a is a completely reduced fraction with denominator less than or equal to $k+1$ and so satisfies the supposition for F_{k+1}. Thus, $a \in F_{k+1}$. As a result, we must have

$$F_k \subseteq F_{k+1}$$

Telescoping this out implies

$$F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n \subseteq F_{n+1}$$

This completes the proof.

b.

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

Proof. Let's prove this by induction.

Base Case: n = 2

We have $F_2 = \{\frac{0}{1}, \frac{1}{2}, \frac{1}{1}\}$. Thus, $|F_2| = 3$ which is odd.

Induction Step: Assume $|F_n|$ is odd

We will first prove two very short lemmas.

Lemma 1. If $\frac{k}{n} \in F_n$ for $k \in \mathbb{Z}$, $0 \leq k \leq n$ then $\frac{n-k}{n} \in F_n$.

Proof. If $\frac{k}{n} \in F_n$ then $gcd(k, n) = 1$. Let $d = gcd(n-k, n)$. We have $d|(n-k)$ and $d|n$ so $d|(n-(n-k))$ or $d|k$. Thus, $d = 1$. As a result, we know that $\frac{n-k}{n}$ is in lowest terms. Because $n \leq n$, we know that $\frac{n-k}{n} \in F_n$.

Lemma 2. $\frac{k}{n} \notin F_{n-1}$ and $\frac{n-k}{n} \notin F_{n-1}$.

Proof. Per the proof of the previous lemma, $\frac{k}{n}, \frac{n-k}{n}$ are in lowest terms, but $n > n-1$ so neither satisfy the supposition to be in F_{n-1}.

We can't add any higher denominator therm to the sequence, so this taken with lemma 2 says new additions always come in pairs. Thus, if $|F_n|$ is odd, then $|F_{n+1}|$ must also be odd.

88.

Conjecture. $|F_n| = |F_{n-1}| + \phi(n)$ where $\phi(n)$ is Euler's totient function.

Proof.

Let's imagine constructing F_n starting with F_{n-1}. Note that, per Ex87.a,

$$F_n = F_{n-1} \cup S$$

where

$$S = \{\frac{k}{n} : 0 \leq k \leq n\}$$

Note that for all k such that $gcd(k, n) > 1$, $\frac{k}{n}$ reduces to some fraction $\frac{\alpha}{\beta} \in F_{n-1}$, because $\beta \leq n-1$. Thus, the union really only contributes the terms such that $gcd(k, n) = 1$, not including $k = n$ because that case reduces to the term $\frac{1}{1}$. By the definition of Euler's totient function, there are $\phi(n)$ such new elements. Thus,

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

by the principle of inclusion-exclusion.

89.

a.

For F_4, we have $\frac{1}{4}$ before $\frac{1}{3}$ and after $\frac{0}{1}$. Interestingly, the mediant of $\frac{0}{1}$ and $\frac{1}{3}$ is $\frac{1}{4}$.

For F_5 we have $\frac{1}{4}$ between $\frac{1}{3}$ and $\frac{1}{5}$. Again, $\frac{1}{4}$ is the mediant of those two fractions.

b.

For F_6 we have the sub-sequence $\frac{1}{2}, \frac{3}{5}, \frac{2}{3}$. Clearly $\frac{3}{5} = \frac{1+2}{2+3}$ is the mediant of $\frac{1}{2}$ and $\frac{2}{3}$.

90.

a.

$5 \cdot 3 - 2 \cdot 7 = 1$

b.

Let's choose $\frac{1}{6}, \frac{1}{5}$. We have

$$6 \cdot 1 - 5 \cdot 1 = 1$$

c.

Let's choose $\frac{2}{5}, \frac{1}{2}$. We have

$$1 \cdot 5 - 2 \cdot 2 = 1$$

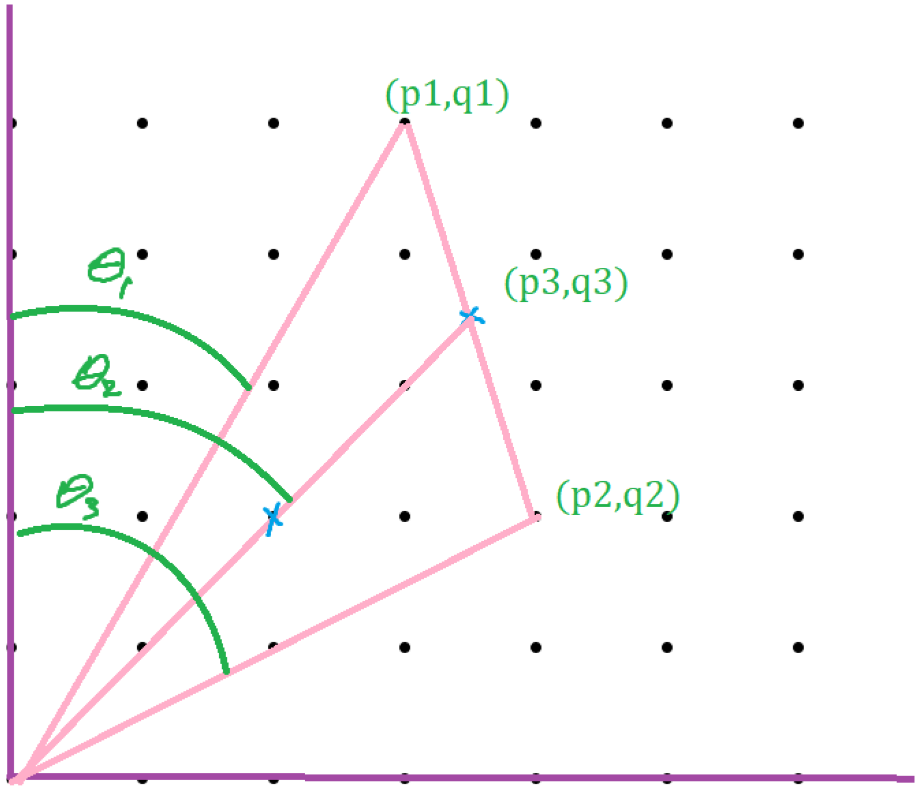
d.

I conjecture that, given two sucessive terms: $\frac{p_1}{q_1}, \frac{p_2}{q_2}$, in the Farey sequence F_n, $p_2q_1 - p_1q_2 = 1$

91.

Conjecture. Suppose that $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ are two successive terms of a Farey sequence F_n. $p_2q_1 - p_1q_2 = 1$.

Proof. We will refer to the following diagram in this proof:



a.

Assume there exist lattice points interior to the triangle in question. At least one such point will be visible from the origin. Call one such visible point (p_3, q_3). Because (p_3, q_3) is visible, $gcd(p_3, q_3) = 1$, so $\frac{p_3}{q_3}$ is in lowest terms. Also, necessarily, $q_3 < max(q_2, q_1) \leq n$. thus, $\frac{p_3}{q_3} \in F_n$. But $\theta_1 < \theta_2 < \theta_3$. Since tangent is monotonic increasing on $(0, \frac{\pi}{2})$, this implies that $tan(\theta_1) < tan(\theta_2) < tan(\theta_3)$. Thus,

$$\frac{p_2}{q_2} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

which violates the notion that $\frac{p_2}{q_2}$ and $\frac{p_1}{q_1}$ are consecutive terms.

b.

Because we already know $gcd(p_1, q_1) = gcd(p_2, q_2)$, Ex31 tells us that there are no boundary lattice points on the sides of the triangle adjacent to the origin (besides the vertices). Assume there exists a boundary point (p_3, q_3) on the side opposite the origin. We use the *exact* same argument as in section a. to conclude that no such point can exist.

c.

We have just shown in parts a. and b. that the triangle defined by $(0, 0), (p_1, q_1),$ and (p_2, q_2) is primitive. By Pick's theorem we have

$$A = 0 + \frac{3}{2} - 1 = \frac{1}{2}$$

d.

We can use the determinant area relation to note that the area must be

$$A = \frac{1}{2}|det(\begin{bmatrix} p_1 & p_2 \\ q_1 & q_2 \end{bmatrix})| = \frac{1}{2}|p_1 q_2 - p_2 q_1| = \frac{1}{2}(p_2 q_1 - p_1 q_2)$$

The last equality is due to the fact that $\frac{p_2}{q_2} > \frac{p_1}{q_1}$.

e.

We set the results of parts d. and c. equal to yield

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

This completes the proof!

92.

Conjecture. If $0 < \frac{a}{b} < \frac{c}{d} < 1$ then

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

Proof. We will first prove the right inequality:

$$\frac{a}{b} < \frac{c}{d} \Longrightarrow a < \frac{cb}{d} \Longrightarrow \frac{cb}{d} + c > a + c \Longrightarrow a + c < \frac{c}{d}(b+d) \Longrightarrow \frac{a+c}{b+d} < \frac{c}{d}$$

Now for the left hand inequality:

$$\frac{a}{b} < \frac{c}{d} \Longrightarrow \frac{ad}{b} < c \Longrightarrow a + \frac{ad}{b} < c + a \Longrightarrow \frac{a}{b}(b+d) < a + c \Longrightarrow \frac{a}{b} < \frac{a+c}{bd}$$

93.

Conjecture. If $\frac{a}{b}, \frac{c}{d}$ are adjacent terms in F_n then $gcd(a+c, b+d) = 1$.
Proof. Please note, this is almost exactly Ryan's proof – because his proof is very nice, and I am lazy. I did go about proving that the parallelogram is primitive in a different way, but that hardly matters.

Let's construct the lattice parallelogram defined by the vectors

$$\vec{v_1} = \begin{pmatrix} a \\ b \end{pmatrix} \quad \vec{v_2} = \begin{pmatrix} c \\ d \end{pmatrix}$$

By the cross-product area relationship, the area of that parallelogram is

$$|\vec{v_1} \times \vec{v_2}| = \left| \begin{vmatrix} a & c \\ b & d \end{vmatrix} \right| = |ad - bc| = 1$$

the last part by Ex91. We also know that since $\frac{a}{b}$ and $\frac{c}{d}$ are in F_n, $gcd(a,b) = 1 = gcd(c,d)$. Thus, the endpoints of $\vec{v}_{1,2}$ are visible from the origin. We can translate the vectors from the other two sides (just copies of $\vec{v}_{1,2}$) to the origin to see that there are no extra edge points on them either. Thus, there are four boundary points. By Pick's theorem,

$$1 = \frac{4}{2} + I - 1 \Longrightarrow I = 0$$

Thus, there are no points between the origin and the far point of the parallelogram, $(a+c, b+d)$. By Ex31, we must have $gcd(a+c, b+d) = 1$.

Note: I am worried about one thing here. We used the fact that a parallelogram with area 1 has only 4 boundary points and no interior points (or rather that a triangle of area $\frac{1}{2}$ has only 3 boundary points and no interior points) to prove Pick's theorem, so I am worried that using Pick's theorem here to verify that isn't *completely* valid. That being said, we have other proofs of Pick's theorem, and the precursors to Pick's theorem also provide valid proof so I am not put off in the slightest by the result, just the citation of Pick's theorem.

94.

We know

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

so we can follow the algorithm to add $\frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \frac{7}{8}$.

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

95.

We can use Ex91 once on each side of $\frac{a}{b} < \frac{61}{79} < \frac{c}{d}$ we have that $61b - 79a = 1$ and $79c - 61d = 1$. By Ex92 we have the two equations $a + c = 61$ and $b + d = 79$. We know that $a + b, c + d$ equal the numerator and the denominator of the fraction exactly because (over complicated but more intuitive argument incoming) because per Ryan's approach to Ex93 we know that the vectors $\binom{a}{b}, \binom{c}{d}$ are a $\mathbb{Z}-$ basis for $\mathbb{Z}^2$ – and so uniquely describes the vector $\binom{61}{79}$.

Anyway, we have four equations and four unknowns:

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

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

Choose your method for solving these. The result is:

$$b = \frac{79a + 1}{61} \quad c = 61 - a \quad d = \frac{4818 - 79a}{61}$$

Now we will take Tarun's modular arithmetic approach to find the free variable a.

$$61b - 79a \equiv 1 \mod 61 \implies -18a \equiv 1 \mod 61 \implies 18a \equiv 60 \mod 61$$

$gcd(6, 61) = 1$ so we know

$$3a \equiv 10 \mod 61$$

We have $3^{-1} \equiv 41 \mod 61$ so $a \equiv 410 \mod 61 \equiv 44$. As Tarun pointed out, we can't have $a > 100$, so $a = 44$. Plugging this back in for the previous equations we get

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

96.

a.

Conjecture. Let $\frac{a_j}{b_j}$ be the fractions that make up the Farey sequence F_n.

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

Proof. This proof is essentially identical to Ryan's. In our proof of Ex87.b. we showed that if $\frac{a_j}{b_j} \in F_n$ then $\frac{n-a_j}{b_j} \in F_n$ (Lemma 1). A direct result of that is

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

so

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

For ease of notation we will say

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

Now let $\frac{a_k}{b_k}\in F_{n+1}$ be a new element. We have $b_k=b_{k-1}+b_{k+1}$ by Ex92 and Ex93. The terms in S_{n+1} involving the new b_k are

$$\frac{b_{k-1}}{b_k}+\frac{b_k}{b_{k+1}}$$

The corresponding terms in $2S_{n+1}$ are therefore

$$\frac{b_{k-1}}{b_k}+\frac{b_k}{b_{k-1}}+\frac{b_k}{b_{k+1}}+\frac{b_{k+1}}{b_k}=\frac{b_{k-1}}{b_{k-1}+b_{k+1}}+\frac{b_{k-1}+b_{k+1}}{b_{k-1}}+\frac{b_{k-1}+b_{k+1}}{b_{k+1}}+\frac{b_{k+1}}{b_{k-1}+b_{k+1}}=3+\frac{b_{k-1}}{b_{k+1}}+\frac{b_{k+1}}{b_{k-1}}$$

The last two terms are carried over from $2S_n$ so we see that ever new term from F_{n+1} adds 3 to the sum $2S_{n+1}$. Ex88 says that $F_{n+1}|=|F_n|+\phi(n+1)$ so $2S_{n+1}=2S_n+2\phi(n+1)$. By induction we see that we must have

$$2S_n=2+3\sum_{j=2}^{n}\phi(j)$$

noting that $2S_1=2$, and that is the first term of our sum. (If $n=1$ we define the right hand sum to be 0). Again, by Ex88, we note that

$$|F_n|=2+\sum_{j=2}^{n}\phi(j)$$

so

$$2S_n=2+3(|F_n|-2)=3|F_n|-4$$

or

$$S_n=\frac{3|F_n|-4}{2}$$

b.

Conjecture.

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

Proof.

Firstly, note that by Ex91.e. we know that $a_{j+1}b_j-a_jb_{j+1}=1$ where $\frac{a_i}{b_i}\in F_n$. Thus

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

But this is just the sum of the consecutive differences between successive terms of F_n, so er must have

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

97.

Conjecture. If $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive terms of F_n, then $b+d>n$.

Proof. Assume $b+d \leq n$. By Ex93 we must have $gcd(a+c, b+d)=1$ which, when taken with Algorithm 1 implies $\frac{a+c}{b+d} \in F_n$, and lies between $\frac{a}{b}$ and $\frac{c}{d}$ which violates the adjacency condition. Thus, we must have $b+d>n$.

98.

Conjecture. If $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive terms of F_n and $n>1$, ten $b+d<2n$.

Proof. Assume for the sake of contradiction that $b+d \geq 2n$. It follows that at least one of b or d is greater than or equal to n. Because $\frac{a}{b}, \frac{c}{d} \in F_n$, we know $b, d \leq n$ so it follows that either b or d is equal to n. Because $b+d \geq 2n$ (per our assumption), we must have $b=d=n$. By Ex91.c. we have

$$cb-ad=1=n(c-a)$$

which implies

$$c-a=\frac{1}{n}$$

The left hand side is an integer, where the right hand side is an integer only when $n=1$, which is assumed false in the problem statement. Thus, our assumption that $b+d \geq 2n$ cannot hold and we must have $b+d<2n$.

99.

Conjecture. If $\alpha \in \mathbb{R}$ where $\alpha \in [\frac{a}{b}, \frac{c}{d}]$ and $\frac{a}{b}, \frac{c}{c} \in F_n$ then one of $\frac{a}{b}$ or $\frac{c}{d}$ is a *good* rational approximation for α. I.e.

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

where $|\alpha-\frac{h}{k}|=min\{|\alpha-\frac{a}{b}|, |\alpha-\frac{c}{d}|\}$

Proof. The best rational approximation for some $\alpha \in \mathbb{R}$ where $\alpha \in [0,1]$ with denominator $\leq n$ must appear in F_n because F_n contains *all* fractions in $[0,1]$ with denominator $\leq n$. Let $\alpha \in [\frac{a}{b}, \frac{c}{d}]$ where $\frac{a}{b}, \frac{c}{d} \in F_n$. We know the rational approximation we are looking for is either $\frac{a}{b}$ or $\frac{c}{d}$. Let's call the closest of the two $\frac{h}{k}$. We know that

$$|\alpha-\frac{h}{k}| \leq \frac{1}{2}(\frac{c}{d}-\frac{a}{b})=\frac{cb-ad}{2db}$$

By Ex91.c. we have $cb-ad=1$ so

$$|\alpha-\frac{h}{k}| \leq \frac{1}{2db}$$

By Ex97 we have $b+d>n$ which implies $max\{b,d\}>\frac{n}{2}$ or $max\{b,d\} \geq \frac{n+1}{2}$. We will call $max\{b,d\}=f$ and $min\{b,d\}=g$. As a result, we must have

$$\frac{1}{2db}=\frac{1}{2fg} \leq \frac{1}{g(n+1)}$$

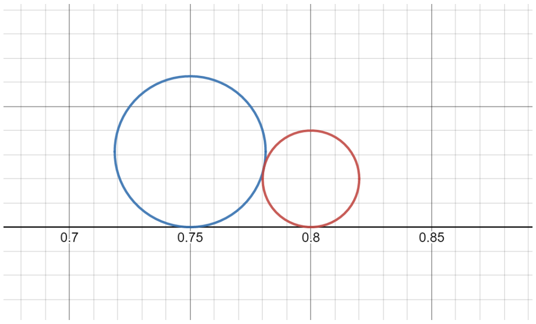
or

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

But $f \geq k$ because $k \in \{b,d\}$ and $f=max\{b,d\}$. So we must have

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

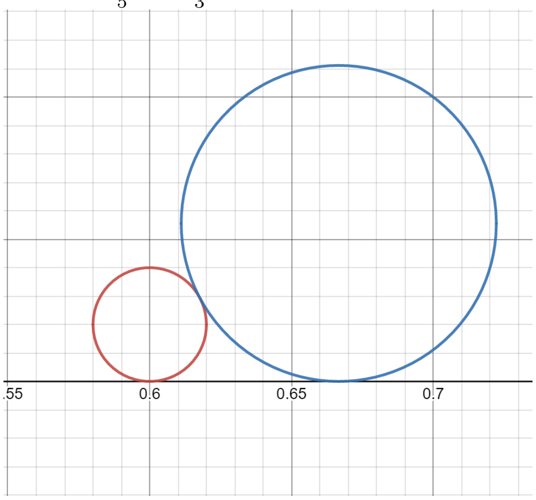
100.



I notice that they are tangent at one point!

101.

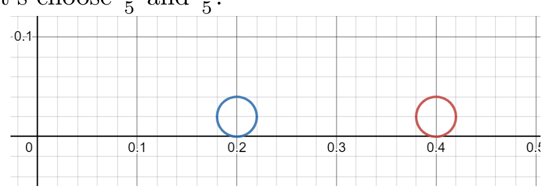
Let's choose $\frac{3}{5}$ and $\frac{2}{3}$.



$C(2,3)$ is in blue and $C(5,3)$ is in red. Again, they are tangent at one point!

102.

Let's choose $\frac{2}{5}$ and $\frac{1}{5}$.

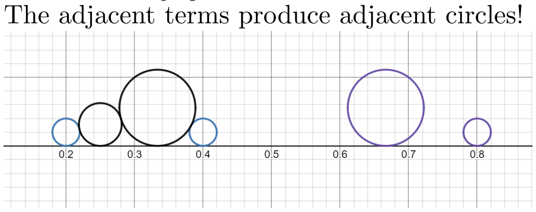


I notice that they are not tangent to one another.

103.

The below image represents three pairs chosen from F_6. Black corresponds to $\{\frac{1}{4}, \frac{1}{3}\}$. Blue corresponds to $\{\frac{2}{5}, \frac{1}{5}\}$. Purple corresponds to $\{\frac{4}{5}, \frac{2}{3}\}$.

The adjacent terms produce adjacent circles!



104. + 105.

This is exactly Eddy's approach, so thank you to him for illustrating it in class!

Let $\frac{p}{q}, \frac{m}{n}$ be adjacent terms in some Farey sequence. By Ex91.e., we must have

$$pn - qm = 1$$

We can square this and divide by q^2n^2 to get

$$(\frac{pn - qm}{qn})^2 = \frac{1}{q^2n^2}$$

Note, however, (thanks to Eddy – I struggled to find this on my own) that

$$\frac{1}{q^2n^2} = (\frac{1}{2q^2} + \frac{1}{2n^2})^2 - (\frac{1}{2q^2} - \frac{1}{2n^2})^2$$

so we have

$$(\frac{1}{2q^2} + \frac{1}{2n^2})^2 - (\frac{1}{2q^2} - \frac{1}{2n^2})^2 = (\frac{p}{q} - \frac{m}{n})^2$$

or

$$(\frac{1}{2q^2} + \frac{1}{2n^2})^2 = (\frac{p}{q} - \frac{m}{n})^2 + (\frac{1}{2q^2} - \frac{1}{2n^2})^2$$

Both sides of this are clearly the distance between two tangent Ford circles, the left hand side being the sum of their radii (hence the tangency) and the right hand side coming from the Euclidean distance formula. Thus, if we have such adjacent terms in a Farey sequence we know that the corresponding Ford circles are tangent. We can see that if we reverse the above calculation we get the other direction.

104.
How do we know the circles never intersect beyond the point of tangency? We can do the same thing backwards but assume

$$(\frac{1}{2q^2} + \frac{1}{2n^2})^2 > (\frac{p}{q} - \frac{m}{n})^2 + (\frac{1}{2q^2} - \frac{1}{2n^2})^2$$

Following the same operations, we arrive at

$$\frac{1}{q^2n^2} > (\frac{pn - qm}{q^2n^2})$$

which can only be true if $pn - qm = 0$ supposing $p, q, m, n \in \mathbb{Z}$, which they are. This is, of course, the trivial case where the two fractions are not distinct.

Note: I am not exactly sure whether "precisely when" implies a bijection. I think it does, but I haven't come up with a proof for:

$$\text{Ford circles are tangent} \implies \text{fractions are adjacent in some } F_n$$

I think that the bijection should be true, but I have been really short on time this week so I (shamefully and regrettably) took Eddy's proof and ran with it after only a day of playing with the problem myself.

106.

Conjecture. If $C(a, b)$ and $C(c, d)$ are tangent Ford circles then $C(a + c, b + d)$ is the unique circle tangent to the real line and to both of the circles $C(a, b)$ and $C(c, d)$.

Proof. We know that $\frac{a}{b}$ and $\frac{c}{d}$ are adjacent fractions in F_n so, by Ex92 and Ex93, there exists some k such that $\frac{a+c}{b+d}$ is adjacent to $\frac{a}{b}$ and $\frac{c}{d}$ in F_k. By Ex97 $b + d > n$ so $\frac{a+c}{b+d}$ will be in some *future* Farey sequence. By Ex105, $C(a + c, b + d)$ is tangent to both $C(a, b)$ and $C(b, d)$.

107.

Take Ex109 and substitute $2 \to e$ and $3 \to f$. Clearly this is a special case.

108.

Per the hint, let's order the points by their distance away from the point $(\sqrt{2}, \frac{1}{3})$. By Ex107 we know that there is a single proper ordering, as no two points are equidistant from $(\sqrt{2}, \frac{1}{3})$. Let that ordering be

$$(\sqrt{2}, \frac{1}{3}), p_2, p_3, \cdots$$

Now, let's construct a circle which contains exactly n points in its interior. Let that circle be the one centered at $(\sqrt{2}, 3)$ and with a radius

$$\frac{d(p_n) + d(p_{n+1})}{2}$$

where $d(p_i)$ is the Euclidean distance between $(\sqrt{2}, \frac{1}{3})$ and p_i. We know that

$$d(p_n) < \frac{d(p_n) + d(p_{n+1})}{2} < d(p_{n+1})$$

by our ordering. Thus, the circle contains exactly the n points $\{(\sqrt{2}, \frac{1}{3}), p_2, \cdots, p_n\}$.

109.

Let's consider the points (x_0, y_0), (x_1, y_1) and assume they are equidistant from the point $(\sqrt{e}, \frac{1}{f})$.

$$(x_0 - \sqrt{e})^2 + (y_0 - \frac{1}{f})^2 = (x_1 - \sqrt{e})^2 + (y_1 - \frac{1}{f})^2$$

Expand that out and combine like terms to get

$$x_0^2 - x_1^2 + y_0^2 - y_1^2 + 2y_1\frac{1}{f} - 2y_0\frac{1}{f} = 2\sqrt{e}(x_0 - x_1)$$

Clearly, the left hand side is in $\mathbb{Q}$ and the right hand side is not, unless $x_0 = x_1$ in which case

$$y_0^2 - y_1^2 = \frac{2}{f}(y_0 - y_1)$$

so

$$y_0 + y_1 = \frac{1}{f}$$

The left hand side is clearly an integer, and the right hand side is not. Thus, this case can't exist. If $y_0 = y_1$ then we have

$$x_0^2 - x_1^2 = 2\sqrt{e}(x_0 - x_1) = (x_0 - x_1)(x_0 + x_1)$$

which implies

$$2\sqrt{e} = x_0 + x_1$$

which is another contradiction as the LHS must be irrational and the RHS rational.

110.

$$L(5) = 21 \qquad L(7) = 21 \qquad L(10) = 37$$

111.

Conjecture. Let $A(n)$ denote the area of the unit lattice squares which is cut by the boundary of the circle $C(\sqrt{n})$.

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

Proof. The area of the squares cut by $C(\sqrt{n})$ is the area of all squares with points on the boundary of $C(\sqrt{n})$ together with the area of all squares who lie partially inside circle and are "fragmented" into two regions by the circle. We know that

$$\left|L(n) - \pi\right|$$

is the area of all squares with lower left hand point on the boundary of $C(\sqrt{n})$ together with the outer fragmented region of any squares cut. Because the area of the square fragments is less than the total area of the collection of whole squares, we must have

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

112.

Conjecture. The area of the annulus enclosing the squares cut by $C(\sqrt{n})$ has area $R(n) = 4\pi\sqrt{2n}$.

Proof. This annulus has thickness $2\sqrt{2}$ so the area must be

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

113.

Conjecture.

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

Proof. Note that proving the conjecture is equivalent to proving

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

We note that $|L(n) - n\pi|$ is the difference between the area of all squares in or on the circle and the area of the circle $C(\sqrt{n})$. I.e., $|L(n) - n\pi|$ is some subset of the area of the squares cut by the circle which in turn is a subset of the annulus that fully contains those squares. By Ex112, we must have

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

This is a necessary and sufficient condition to prove the conjecture.

114.

Conjecture.

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

Proof.
Let $0 < \epsilon \in \mathbb{R}$, $\delta = \frac{32\pi^2}{\epsilon^2}$. Therefore, for $n > \delta$ we have

$$n > \frac{32\pi^2}{\epsilon^2} \implies \epsilon > \frac{4\sqrt{2}\pi}{\sqrt{n}}$$

By Ex113 we have

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

so $\forall 0 < \epsilon \in \mathbb{R} \quad \exists \delta$ such that $n > \delta \Longrightarrow \epsilon > \left|\frac{L(n)}{n} - \pi\right|$. This is, of course, the $\epsilon - \delta$ definition of the limit

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

115.

Conjecture. If $L(P)$ denotes the number of lattice points inside or on the boundary of a lattice polygon P and nP denotes the polygon defined by the points

$nP = \{nx | x \in P\}$

then $L(nP) = A(P)n^2 + \frac{1}{2}B(P)n + 1$. Note that we can rephrase Pick's theorem as:

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

Proof. We can prove this in two parts.

Part 1: $A(nP) = n^2 A(P)$. Note the shoelace theorem which states

$$A(P) = \frac{1}{2}|\sum_{i=1}^{n}(x_{i+1} + x_i)(y_{i+1} - y_i)|$$

where (x_i, y_i) are the coordinates of the ith vertex of an oriented n-gon. Applying the scaling we get

$$A(nP) = \frac{1}{2}|\sum_{i=1}^{n}(nx_{i+1} + nx_i)(ny_{i+1} - ny_i)| = \frac{n^2}{2}|\sum_{i=1}^{n}(x_{i+1} + x_i)(y_{i+1} - y_i)| = n^2 A(P)$$

Part 1, generalized. Note that this actually holds true for any region R in $\mathbb{R}^2$. We can write

$$A(nR) = \int\int_{nR} dx' dy'$$

where $x' = nx$, $y' = ny$. We have

$$\frac{dx'}{dx} = n \qquad \frac{dy'}{dy} = n$$

so

$$A(nR) = \int\int_{R} n^2 dx dy = n^2 A(R)$$

Part 2:

First we will prove the following lemma:

Lemma. $gcd(na, nb) = ngcd(a, b)$.

Proof of lemma. We know $n|na, nb$ so $n|gcd(na, nb)$. Also $gcd(a, b)|na, nb$ so $gcd(a, b)|gcd(na, nb)$. Because $gcd(a, b) \leq a, b$ we know $ngcd(a, b) \leq na, nb$. There can be no greater common divisors of na, nb because $gcd(a, b)$ is a product of *all* common factors of a and b and n clearly contains all factors of n. Thus, there are no additional factors that could be multiplied into $ngcd(a, b)$ to make a greater divisor. We could also prove this using the Euclidean algorithm.

Now we apply the result of Ex30, namely that

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

where $d_i = gcd(x_{i+1} - x_i, y_{i+1} - y_i)$ and $d_n = gcd(x_1 - x_n, y_1 - y_n)$. Now consider $B(nP)$ where

$$d_i = gcd(n(x_{i+1} - x_i), n(y_{i+1} - y_i)) = ngcd(x_{i+1} - x_i, y_{i+1} - y_i)$$

$$d_n = gcd(n(x_1 - x_n), n(y_1 - y_n)) = ngcd(x_1 - x_n, y_1 - y_n)$$

where the right most equalities comes from the above lemma. Thus, we have

$$B(nP) = \sum_{i=1}^{k} nd_i = nB(P)$$

Now we combine these and note that

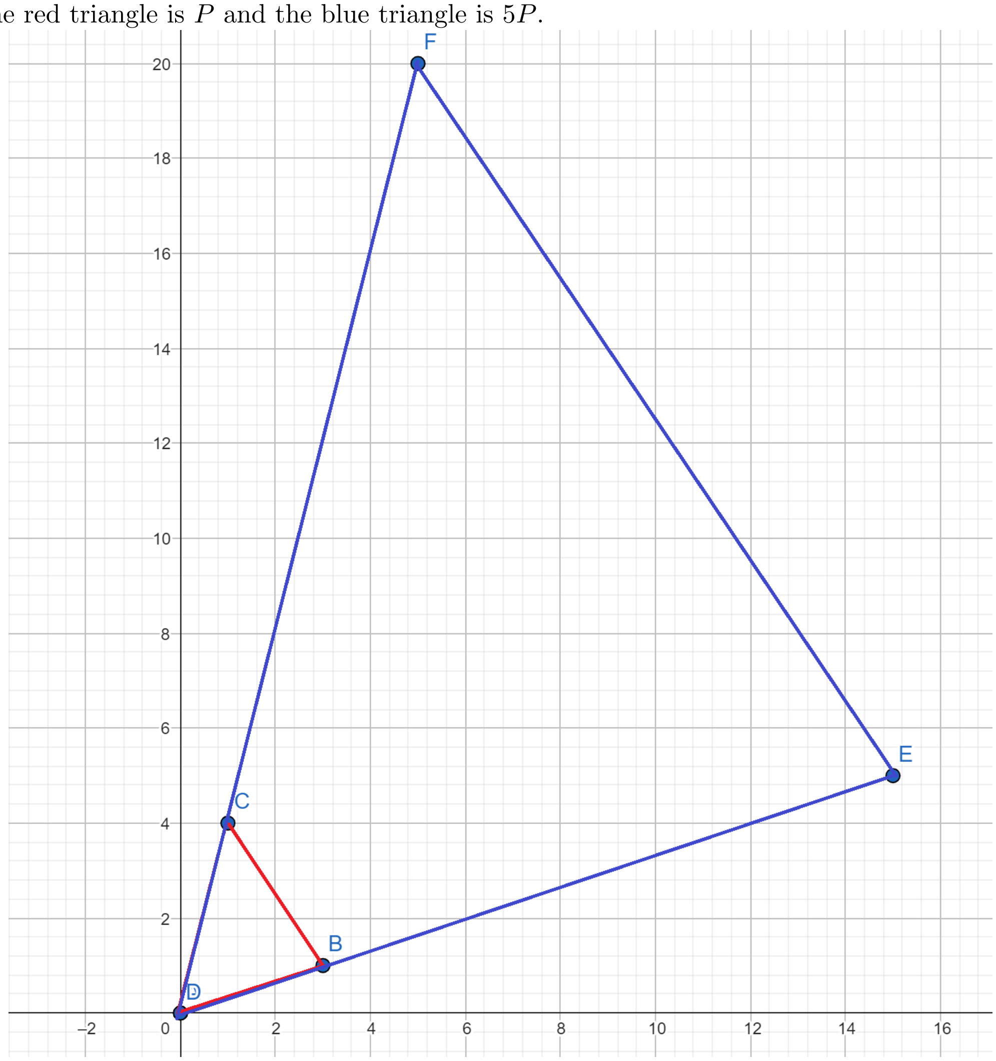
$$L(nP) = A(nP) + \frac{1}{2}B(nP) + 1 = n^2A(P) + \frac{1}{2}nB(P) + 1$$

completing the proof!

116.

a.

The red triangle is P and the blue triangle is $5P$.



b.

I count $L(P) = 8$ and $L(5P) = 146$

c.

We know $A(P) = \frac{11}{2}$ and $B(p) = 3$
so

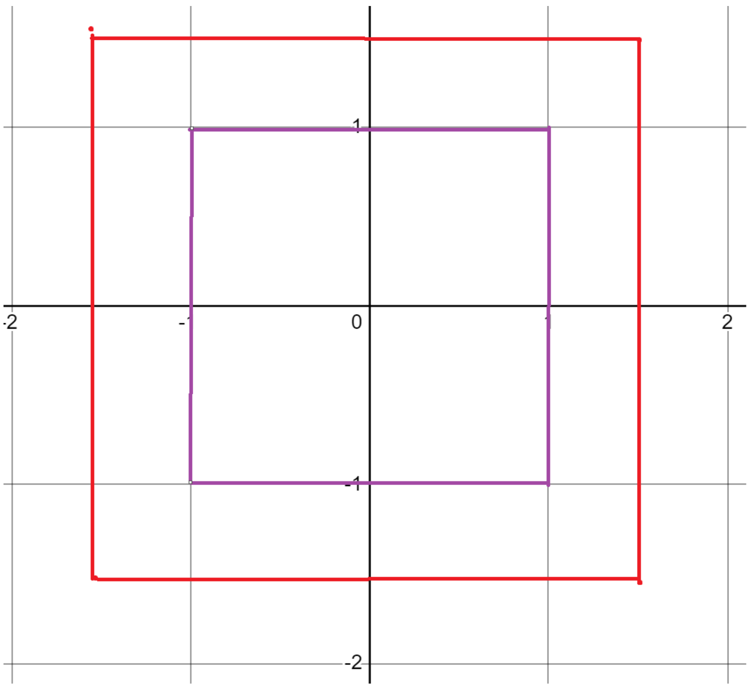
$$L(5P) = \frac{11}{2} \cdot 25 + \frac{3}{2} \cdot 5 + 1 = 146$$

[CHECK THIS]

117.

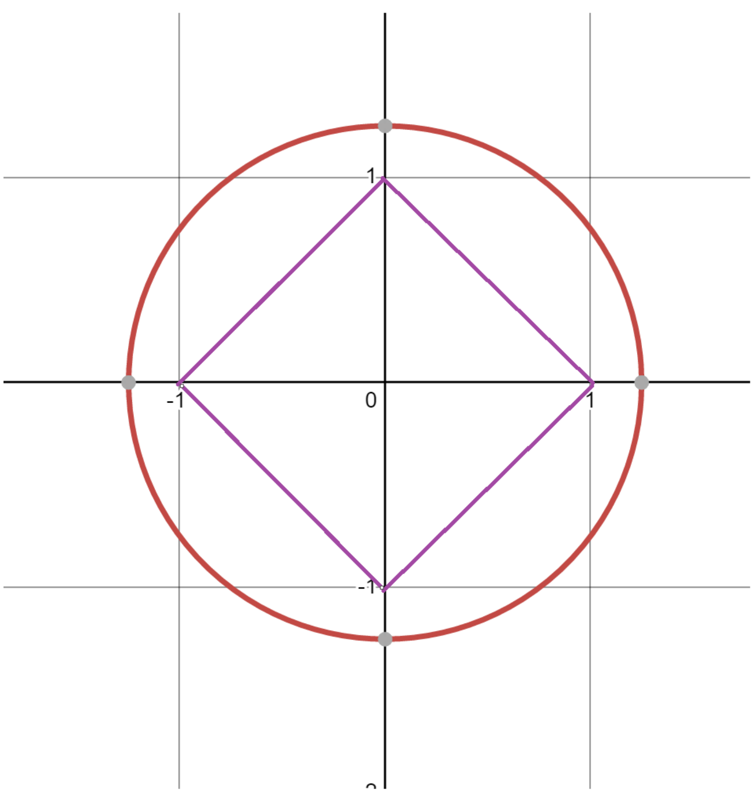
The red outline represents the reigon in question and the purple represents its convex hull.

a.



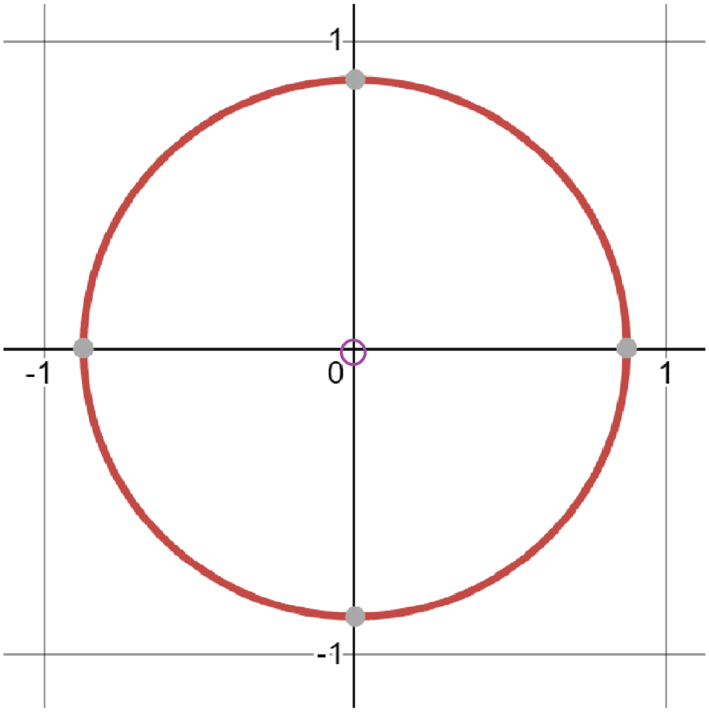
Clearly $L(R) = L(P) = 9$. Also $A(P) = 4 \leq A(R) = 9$. Likewise $p(P) = 8 \leq p(R) = 12$.

b.



Clearly $L(R) = L(P) = 5$. Also $A(P) = 2 \leq A(R) = \frac{\pi \cdot 25}{16}$. Likewise $p(P) = 4\sqrt{2} \leq p(R) = \pi \cdot \frac{5}{2}$.

c.



Here P is the degenerate polygon with one vertex. Clearly $L(R) = L(P) = 1$. Also $A(P) = 0 \leq A(R) = \frac{\pi \cdot 49}{64}$. Likewise $p(P) = 0\sqrt{2} \leq p(R) = \pi \cdot \frac{7}{4}$.

118.

Conjecture. 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. We have

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

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

Proof. Let's use the modified version of Pick's theorem:

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

where we make P the convex hull of R. because the least distance between two lattice points in $\mathbb{Z}^2$ is 1 unit, we must have

$$p(P) \geq B(p)$$

Therefore

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

But Theorem 7 states

$$L(P) = L(R)$$

so, really,

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

Again, by Theorem 7, $A(P) \leq A(R)$ and $p(P) \leq p(R)$ so

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

119.

a.

$$L(R) = 9 \leq A(R) + \frac{1}{2}p(R) + 1 = 17$$

b.

$$L(R) = 5 \leq A(R) + \frac{1}{2}p(R) + 1 \approx 9.84$$

c.

$$L(R) = 1 \leq A(R) + \frac{1}{2}p(R) + 1 \approx 6.15$$

120.

Conjecture. $\exists i, j, m, n \in \mathbb{Z}$ such that $T_{i,j} \cap T_{m,n} \neq \emptyset$.

Proof.

Assume there is no overlap between any $T_{i,j}$. That is, assume

$$\forall i, j, m, n \in \mathbb{Z} \qquad T_{i,j} \cap T_{m,n} = \emptyset$$

By PIE, the area of the region $\bigcup_{i,j} T_{i,j}$ is equal to the area of $\bigcup_{i,j} R_{i,j}$ (no double counting, by the assumption). For ease of notation, we denote this

$$A(\bigcup_{i,j} T_{i,j}) = A(\bigcup_{i,j} R_{i,j})$$

But we must note that (through PIE)

$$A(\bigcup_{i,j} R_{i,j}) = A(R)$$

because

$$0 \leq A(\bigcap_{i,j} R_{i,j}) \leq A(\bigcap_{i,j} I_{i,j}) = 0$$

the rightmost equality coming from the fact that the $I_{i,j}$ intersect only on their boundaries. Thus,

$$A(\bigcup_{i,j} T_{i,j}) = A(R)$$

where $A(R) > 1$. The contradiction arises when we note that

$$\bigcup_{i,j} T_{i,j} \subseteq S$$

and $A(S) = 1$, so $A(\bigcup_{i,j} T_{i,j}) \leq 1$. Thus, $\exists i, j, m, n \in \mathbb{Z}$ such that

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

121.

Conjecture. Blichfeldt's Theorem

Proof. Per Ex120 there exist $i, j, m, n \in \mathbb{Z}$ such that $T_{i,j} \cap T_{m,n} \neq \emptyset$. Thus, there exist at least two points in R, call them $(x_0, y_0), (x_1, y_1)$ such that $(x_0, y_0) - (i, j) = (\alpha, \beta) = (x_1, y_1) - (m, n)$ where $0 \leq \alpha, \beta < 1$. As $i, j, m, n \in \mathbb{Z}$, this implies that $(x_0, y_0), (x_1, y_1)$ share the same decimal parts for their x and y components respectively. We know that

$$(x_0, y_0) = (i, j) + (\alpha, \beta)$$

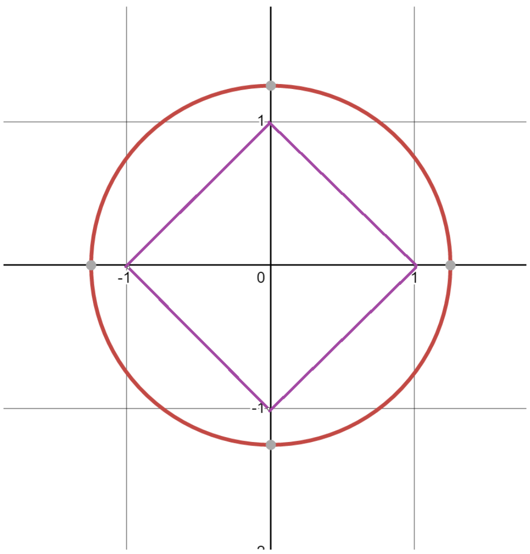
and

$$(x_1, y_1) = (m, n) + (\alpha, \beta)$$

so $(x_0, y_0) - (x_1, y_1) = (x_0 - x_1, y_0 - y_1) = (i - m, j - n) \in \mathbb{Z}^2$ by the closure of the integers under addition. This completes the proof.

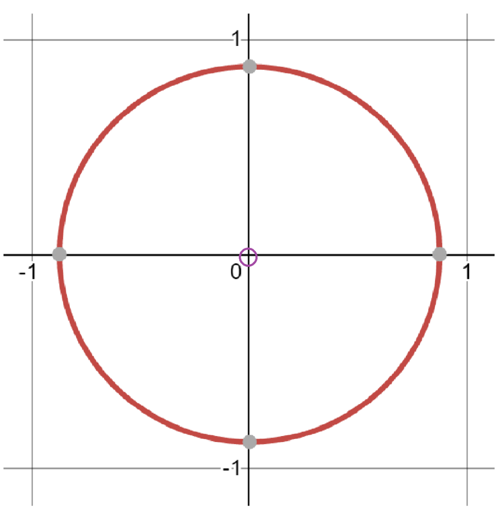
122.

a.



The given circle is a bounded, convex region which is symmetric about the origin and has an area $\frac{25\pi}{16} > 4$. We see that is contains four lattice points which are not the origin.

b.



The circle has area $\frac{49\pi}{64} \approx 2.4 < 4$ so we can't apply Minkowski's theorem! (And that's a good thing because we see there is no point other than the origin!)

123.

Conjecture. 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

$$\frac{1}{2}R = \{\frac{1}{2}x : x \in R\}$$

There exist points $x', y' \in R$ such that $0 \neq x' - y' \in \mathbb{Z}^2$.

Proof. This is a rather simple application of Blichfeldt's theorem. First, by the generalization of part 1 in Ex115 we note that – since $A(R) > 4$, $A(R') > 1$ so we can apply Blichfeldt's theorem. By Blichfeldt's theorem there exist $x', y' \in R'$ such that $x' - y' \in \mathbb{Z}^2$. If we had $x' - y' = 0$, the points couldn't be distinct. This completes the proof.

124.

Conjecture. Let R be a convex region in $\mathbb{R}^2$ which is symmetric about the origin. Let x', y' be points in $R' = \frac{1}{2}R$ such that $0 \neq x' - y' \in \mathbb{Z}^2$ (proved possible in Ex123). Then $x' - y' \in R$.

Proof. From the definition of R' there exist $x, y \in R$ such that

$$x' = \frac{1}{2}x \quad y' = \frac{1}{2}y$$

Therefore

$$x' - y' = \frac{1}{2}(x - y)$$

Because R is symmetric about the origin, we also have $-x, -y \in R$. The line connecting x and $-y$ is parameterized by

$$r(t) = (x + y)t - y$$

and so

$$r(\frac{1}{2}) = \frac{1}{2}(x - y)$$

so $\frac{1}{2}(x - y)$ lies on the line connecting x and $-y$. We know that $\frac{1}{2}(x - y)$ is between x and $-y$ on this line because $0 < t = \frac{1}{2} < 1$. Thus, because R is convex, $\frac{1}{2}(x - y) = x' - y' \in R$. This completes the proof of Minkowski's theorem!

Discussion of problem 119

This is only a quick thought, but it might be interesting to look at what geometries arise from the generalized Farey sequences. I like to look at the Farey sequences visually and think about how the consecutive terms really somehow map their fractions to a vector in $\mathbb{Z}^2$. This makes me think that the generalized form is really more natural, because all of the maths we are doing on Farey sequences really only deals separately with the numerator and denominator, and so we have essentially – by way of the mediant – sidestepped the "fractiony" bit and are really just using the fractions as stand ins for vectors. In fact, the only "important fractiony quality" of the Farey sequence terms is that, by way of the ordering condition for real numbers, they allow us to order vectors in a way which we would be otherwise unable. When we consider the more vector-oriented picture we can notice all sorts of things like that there is a bijection between adjacent terms and primitive triangles and, of course, the Farey sunburst. An extension of the Farey sunburst would really interest me because in $\mathbb{R}^2$ it has no interior points other than the origin which limits its area by Minkowski's theorem, but the fact that the determinants need not be ± 1 in higher dimensions tells me there are probably interior points to the higher dimensional sunburst diagrams, and I wonder if those points are forced because of something special about $\mathbb{R}^3$ and the volume of the shape. Thus, it seems like there could be some really interesting conjectures about higher order determinants (four and beyond) as I wonder if $\mathbb{R}^3$, odd dimensions, or dimensions with other properties are special. I.e. I am curious whether there are any dimensions which preserve what we see in $\mathbb{R}^2$. Note that when I say "dimension" here, I am referring to the order of the generating polynomial, and so the number of coefficients.

Thanks for a great course – I look forward to thinking about more of these concepts over the summer!

$tan\frac{\pi}{5}$ is irrational

Conjecture. $tan\frac{\pi}{5}$ is irrational.

Proof. The idea here is to first illustrate that if $tan\frac{\pi}{5}$ is rational then the real and imaginary parts of a non-trivial 10th root of unity must be rational. Then we prove that if a 10th root of unity other than 1 has rational real and imaginary parts then all 10th roots of unity have rational real and imaginary parts. We then show how this implies we can construct a regular lattice 10−gon which, in turn, implies we can construct a regular lattice pentagon which we proved impossible in Ex3. In other words, a classic proof by contradiction. On with the proof!

Consider the 10th roots of unity:

$$\{z_k = e^{\frac{k\pi i}{5}} : k \in \mathbb{Z}\}$$

The complex exponential form clearly reveals that the angle between the real axis and the ray pointing through the $k = 1$ 10th root of unity is $\frac{\pi}{5}$. Thus, $tan\frac{\pi}{5} = \frac{Im(z_1)}{Re(z_1)}$. We will assume $tan\frac{\pi}{5} \in \mathbb{Q}$ so, by the closure of $\mathbb{Q}$ under division, we know that $Re(z_1), Im(z_1) \in \mathbb{Q}$. Note, however, that we can write any z_k as

$$z_1^k = (Re(z_1) + iIm(z_1))^k$$

But, by the closure of the rational numbers under multiplication, we know every term in the expansion of $(Re(z_1) + iIm(z_1))^k$ will be rational. By the closure of the rational numbers under addition, we know that $Re(z_k), Im(z_k) \in \mathbb{Q}$ because we are simply combining the real and imaginary terms in the aforementioned expansion. Thus, we have the result that if $tan\frac{\pi}{5} \in \mathbb{Q}$ then $Re(z_k), Im(z_k) \in \mathbb{Q}$ for all 10th roots of unity z_k.

Thus, the regular decagon created in the complex plane by the 10th roots of unity has all of its vertices at rational co-ordinates. Map that decagon to $\mathbb{R}^2$ in the usual way: $z \in \mathbb{C} \mapsto (Re(z), Im(z)) \in \mathbb{R}^2$. Label all of the vertices of the decagon $\{(x_1, y_1), \cdots, (x_10, y_10)\}$ where – as we showed – $x_j, y_j \in \mathbb{Q}$. Because all of the points are rational $\exists M \in \mathbb{Z}$ such that $Mx_j, My_j \in \mathbb{Z}$. Scale the decagon by M. That is, take $(x_j, y_j) \mapsto (Mx_j, My_j)$. Now we necessarily have a lattice decagon, albeit an arbitrarily large one. Now create the lattice pentagon

$$(x_1, y_1) \to (x_3, y_3) \to (x_5, y_5) \to (x_7, y_7) \to (x_9, y_9) \to (x_1, y_1)$$

So we have a contradiction because, in this way, we have created a lattice pentagon whose existence is forbidden by the results of Ex3.