# Patterns are Fun: Pick's Theorem, Farey Fractions, and Sums of Two Squares

Evan P. Dummit

Northeastern University

Northeastern Math Club

January 31st, 2025

# Outline of Talk

We will start by looking at lattice polygons: these are polygons in the Cartesian plane whose vertices are at lattice points: points whose coordinates are both integers.

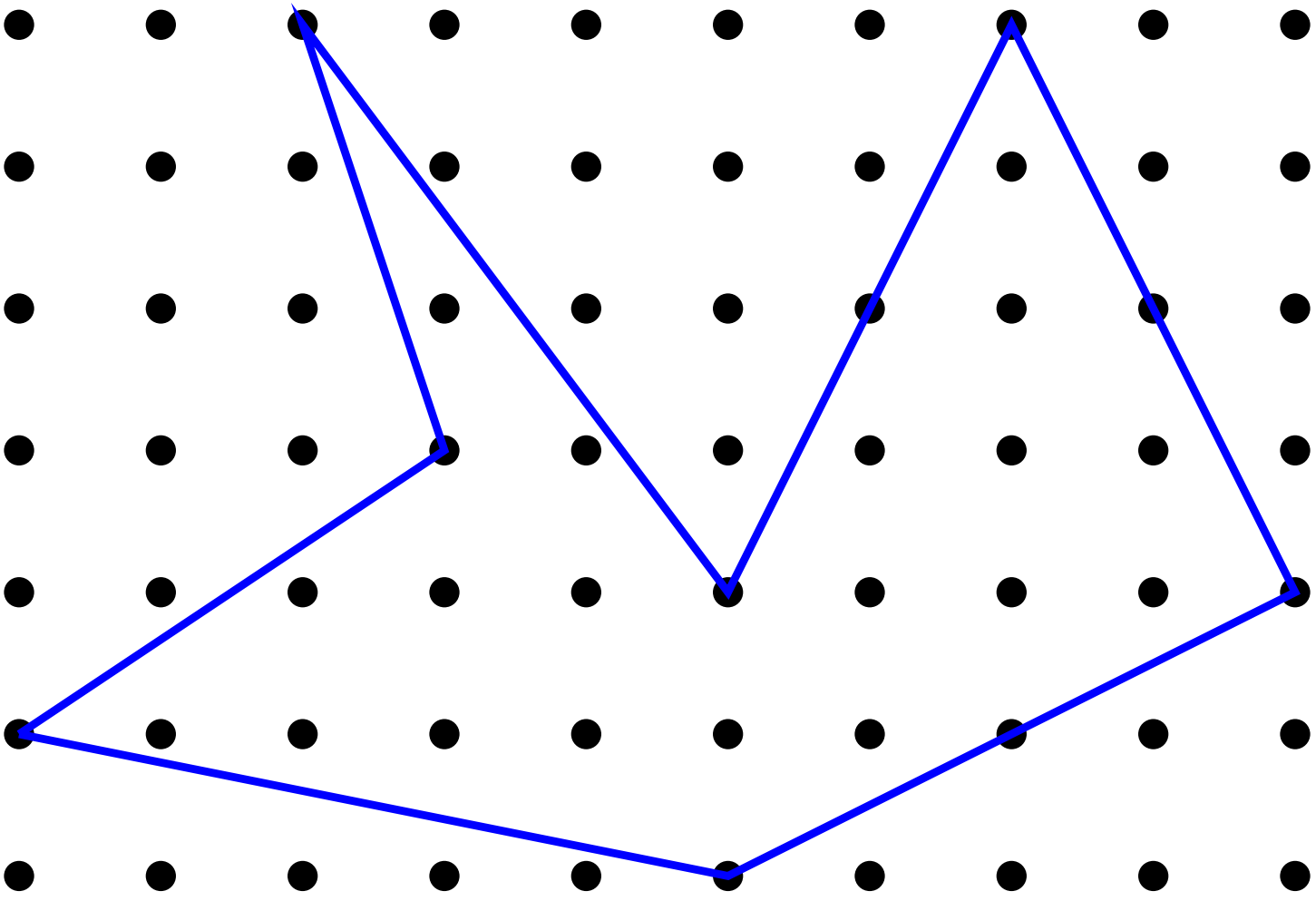
Then we will examine Farey fractions and the Farey sequences: these are lists of fractions arranged in increasing order.

Finally, we will look at sums of two squares.

All of these mathematical problems (one from geometry and two from number theory) turn out to have many interesting patterns associated to them. And perhaps, there just might be a connection or two between them too....

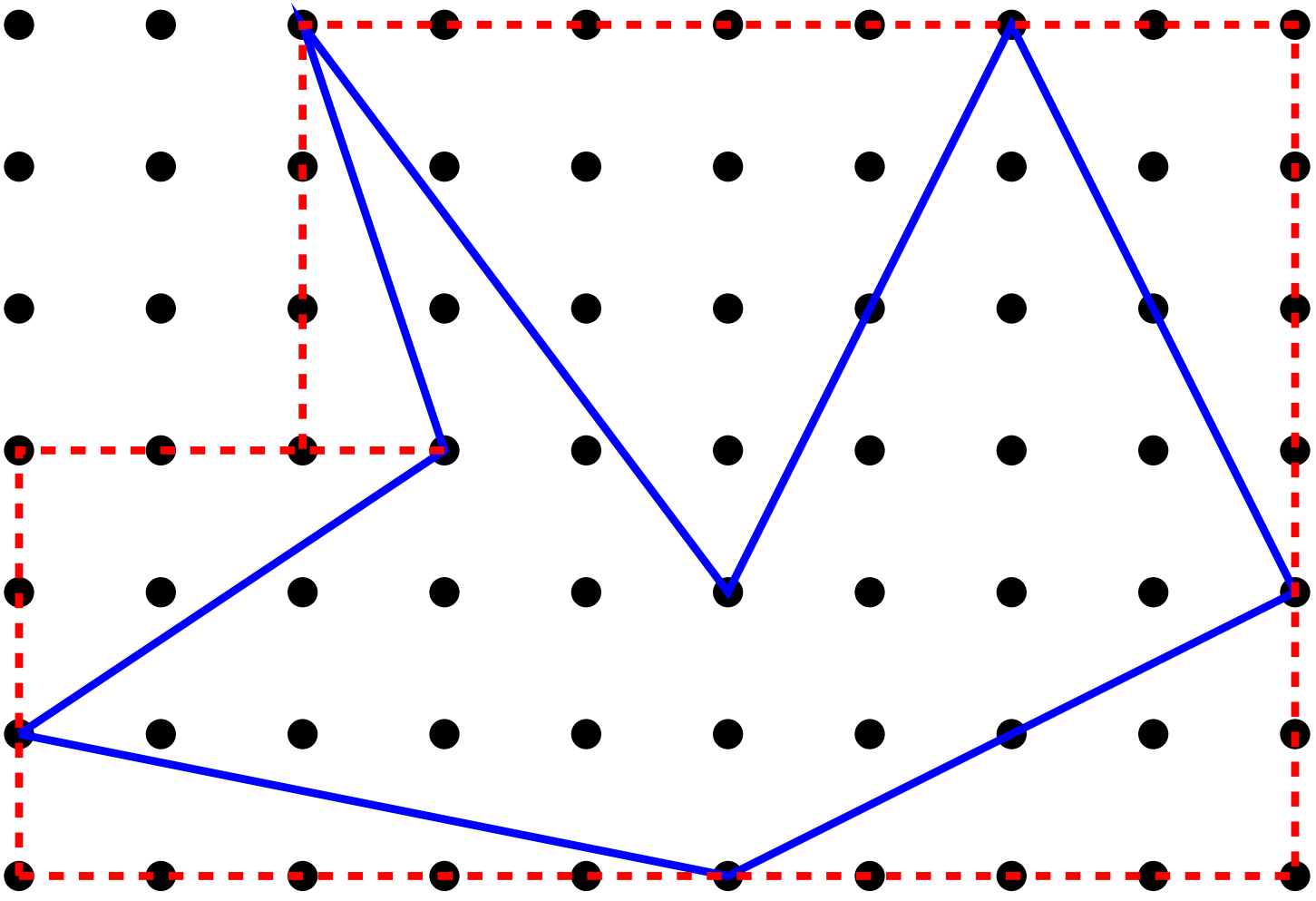
# A Question

What is the area of the lattice polygon pictured below?



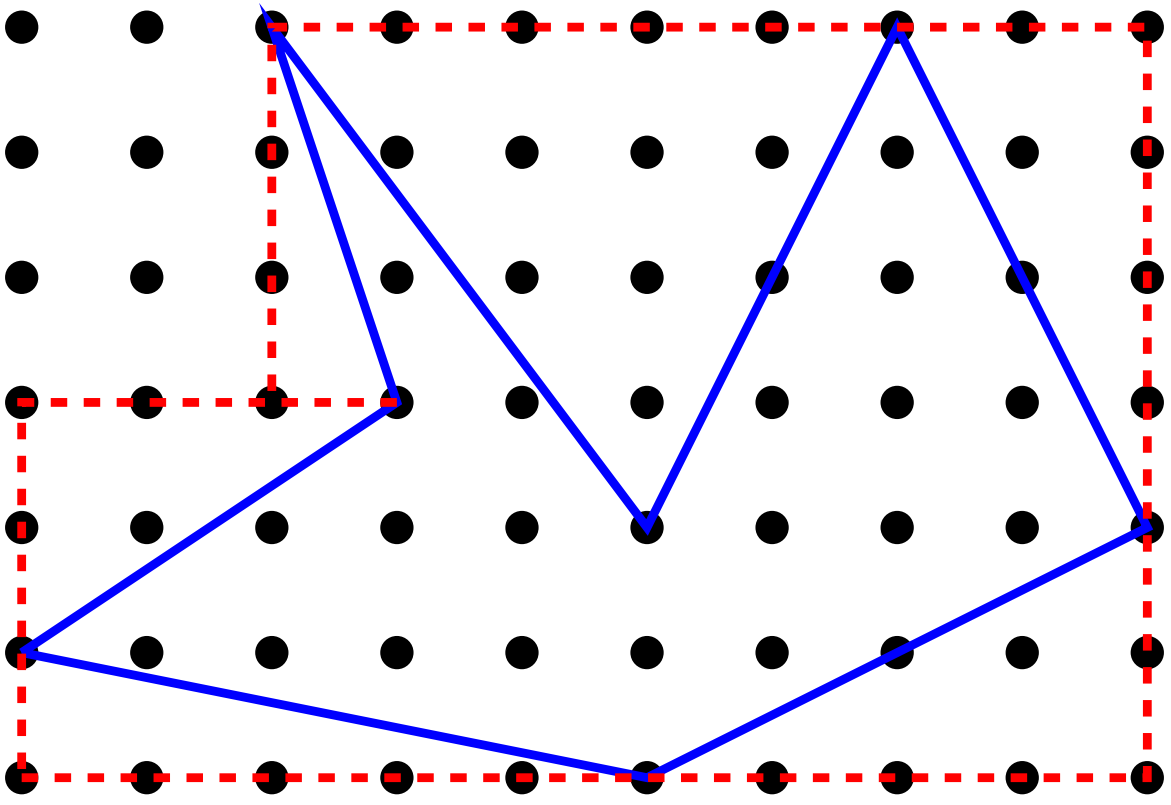
# An Answer, Partway

Let's draw some triangles!



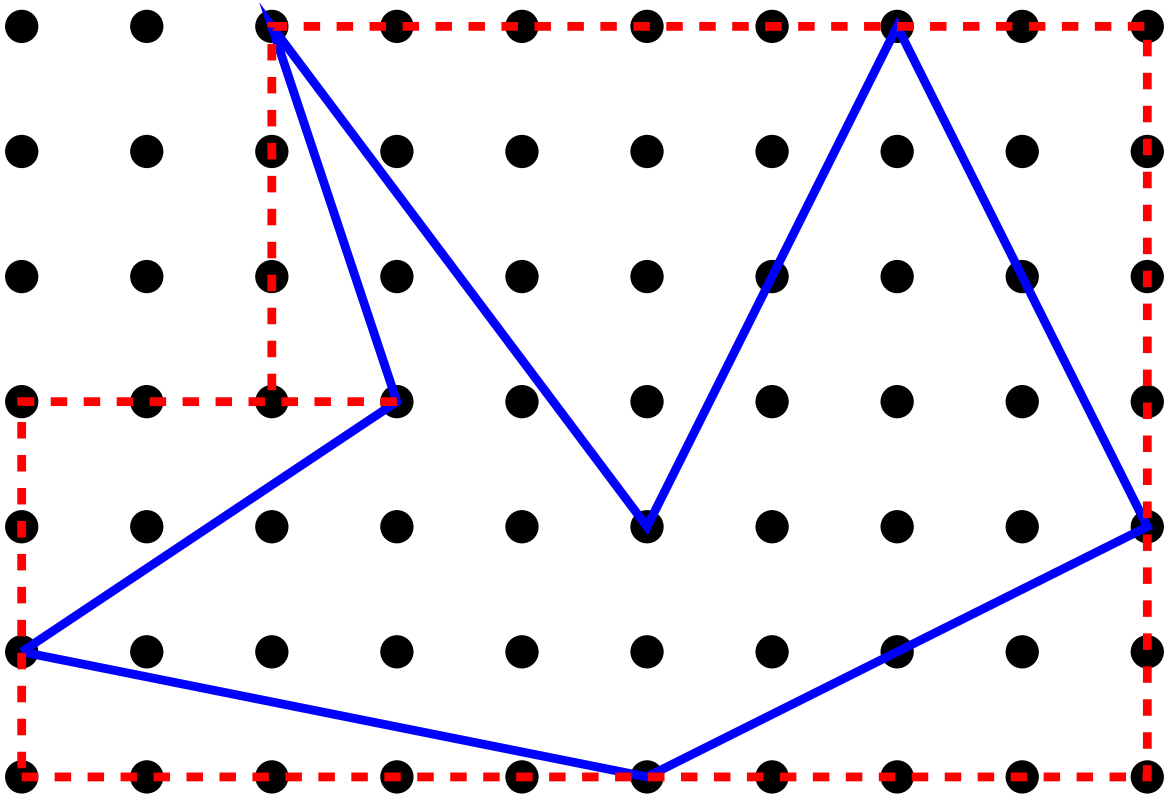
# An Answer, Mostly

The red dotted lines enclose a $9 \times 6$ region, minus a $2 \times 3$ rectangle. Then we have six triangles to subtract, of areas $5/2$, 4, 4, 10, $3/2$, and 3. That leaves (drumroll, please!)...



# An Answer, Completely, For Real This Time, Seriously

... a total area of 23.



# Phew, That Was Easy!

It's not so hard to convince yourself that you can always find the area of any lattice polygon by drawing triangles and rectangles this way. (Though this is harder to prove rigorously than you might think.)

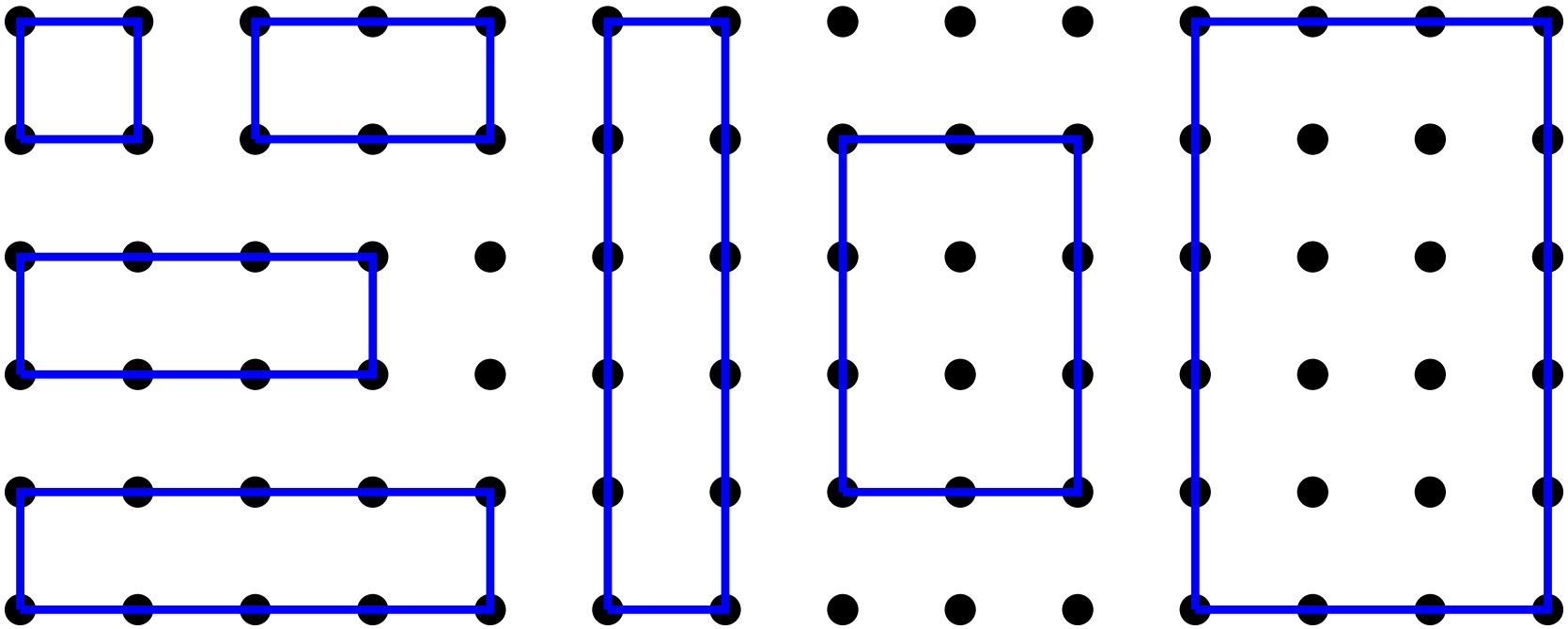
So why are we all here, then? Because, of course, perhaps there's another way to do it. More precisely:

**Boldly Unjustified and Vague Claim**

*There is a way to find the area of any lattice polygon just by counting points inside and on it.*

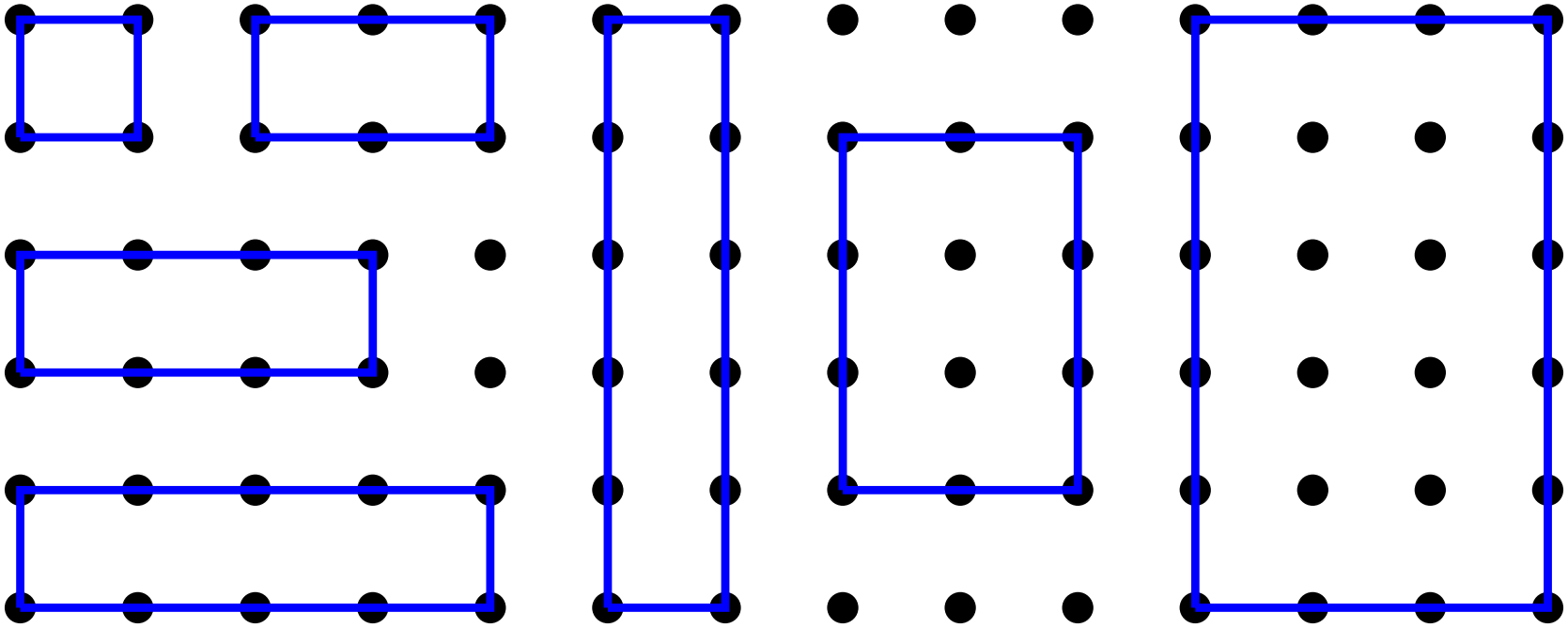
# More Specificity

Let's try to extract a more precise statement from some examples.



# More Specificity

Let's try to extract a more precise statement from some examples.



The areas are 1, 2, 3, 4, 5, 6, and 15. The rectangles respectively pass through 4, 6, 8, 10, 12, 10, and 16 points.

# Data Tabulation

Let's collect our data so far:

| Rectangle Area | Number of Points |
|---|---|
| 1 | 4 |
| 2 | 6 |
| 3 | 8 |
| 4 | 10 |
| 5 | 12 |
| 6 | 10 |
| 15 | 16 |

# Data Tabulation

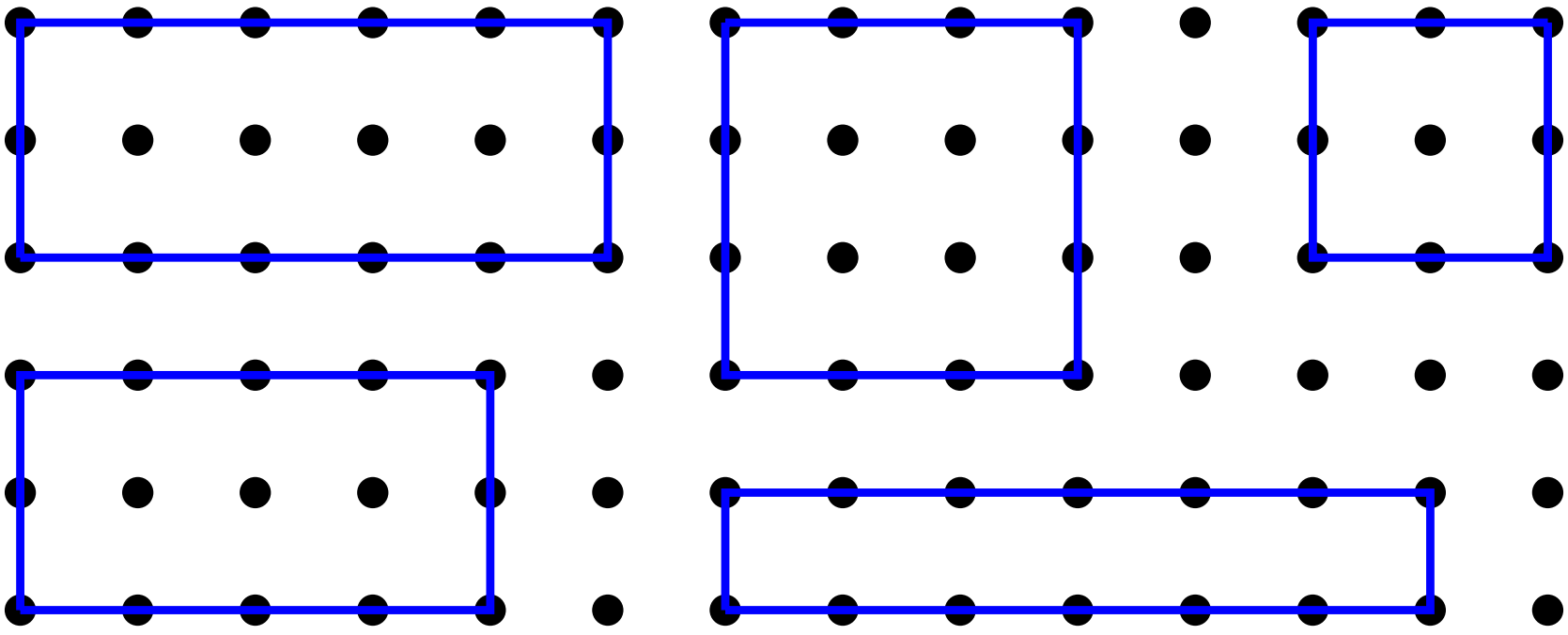
Let's collect our data so far:

| Rectangle Area | Number of Points |
|---|---|
| 1 | 4 |
| 2 | 6 |
| 3 | 8 |
| 4 | 10 |
| 5 | 12 |
| 6 | 10 |
| 15 | 16 |

For the first few entries, the relationship seems linear: the number of points is twice the area plus 2. But it breaks down for the last two rectangles. This shouldn't be surprising, since the number of points being counted is just the perimeter, and that doesn't scale the same as the area will: we're ignoring all of the points inside the rectangle.

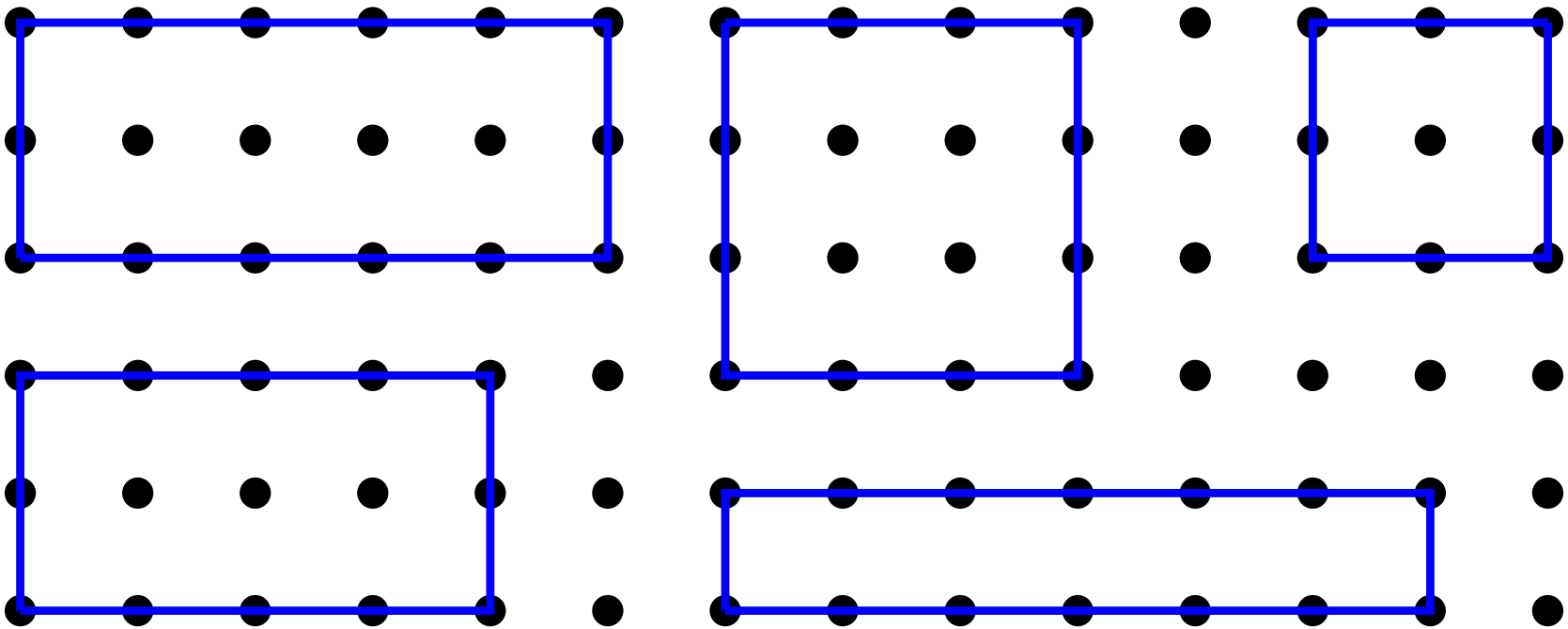
# More Examples

So let's count interior points as well!



# More Examples

So let's count interior points as well!



These rectangles have areas 10, 9, 4, 8, and 6. They pass through 14, 12, 8, 12, and 14 points respectively, and contain 4, 4, 1, 3, and 0 points in their interiors.

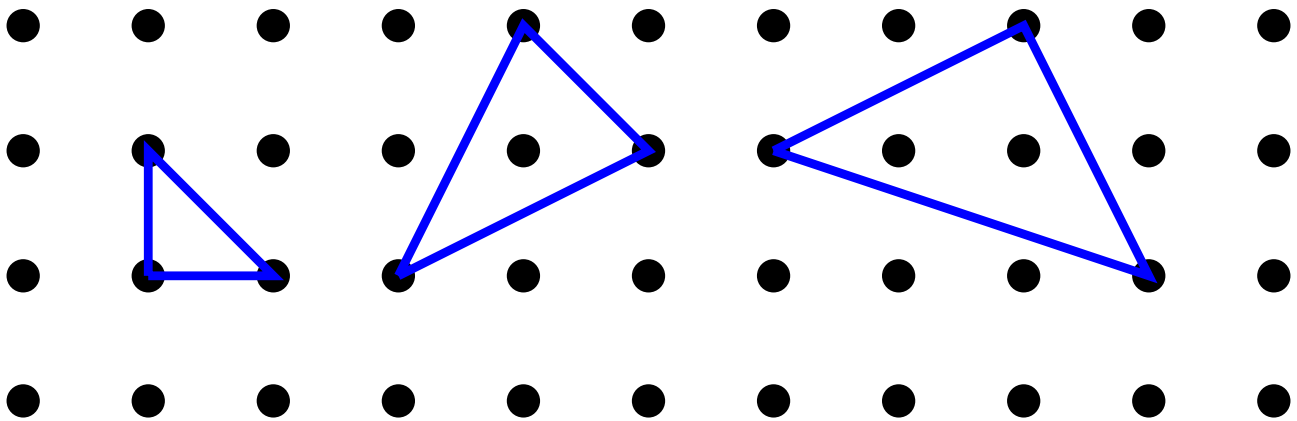
# The Inside ~~Scoop~~ Count

Let's tabulate both boundary points and interior points:

| Rectangle Area | Boundary Points | Interior Points |
|---|---|---|
| 1 | 4 | 0 |
| 2 | 6 | 0 |
| 3 | 8 | 0 |
| 4 | 8 | 1 |
| 4 | 10 | 0 |
| 5 | 12 | 0 |
| 6 | 10 | 2 |
| 6 | 14 | 0 |
| 8 | 12 | 3 |
| 9 | 12 | 4 |
| 10 | 14 | 4 |
| 15 | 16 | 8 |

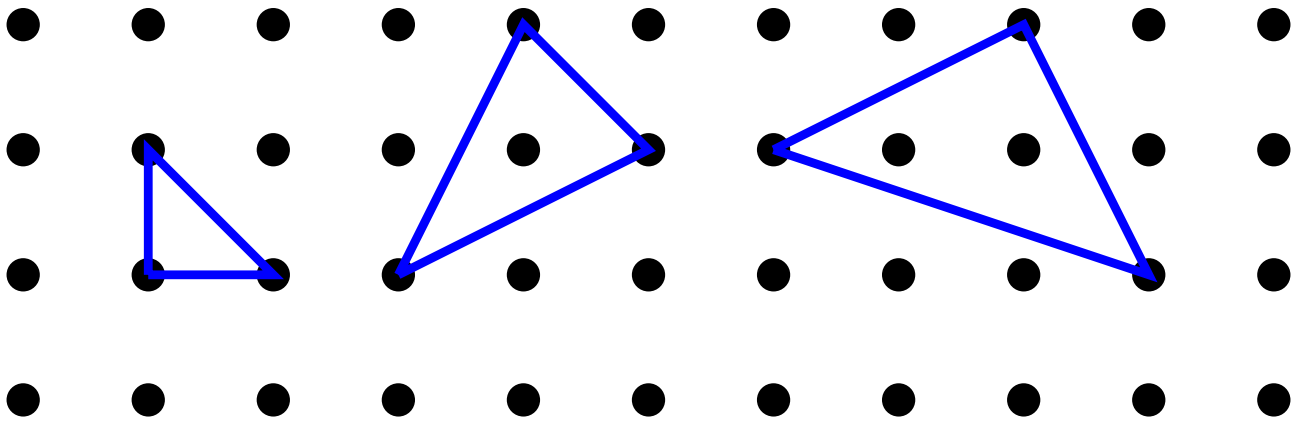
# Yet More Examples

Let's do more examples, just to be sure, with some non-rectangles this time.



# Yet More Examples

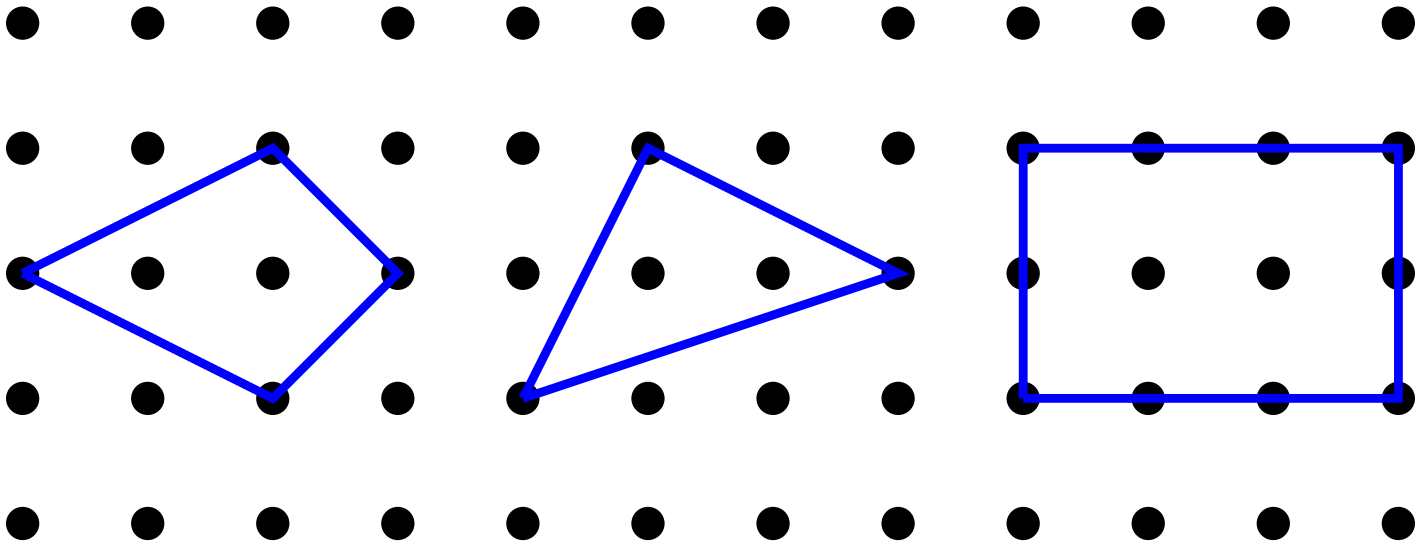
Let's do more examples, just to be sure, with some non-rectangles this time.



Triangle 1 has area 1/2 and 3 boundary and 0 interior points.
Triangle 2 has area 3/2 and 3 boundary and 1 interior point.
Triangle 3 has area 5/2 and 3 boundary and 2 interior points.

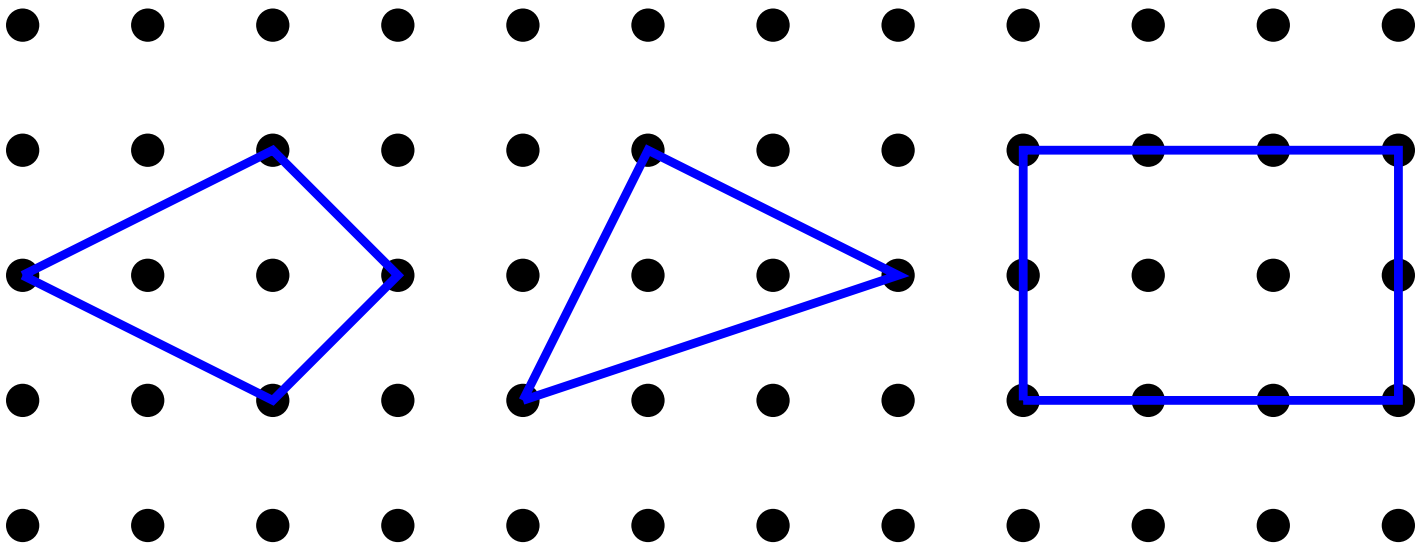
# Even Yet More Examples

Here's a few more shapes.



# Even Yet More Examples

Here's a few more shapes.



The kite has area 3, and 4 boundary and 2 interior points.
The triangle has area 5/2, and 3 boundary and 2 interior points.
The rectangle has area 6, and 8 boundary and 2 interior points.

# Much Data, Very Want, Such Pattern

Here's some relevant snippets of the data table:

| Polygon Area | Boundary Points | Interior Points |
|---|---|---|
| 1 | 4 | 0 |
| 2 | 6 | 0 |
| 3 | 8 | 0 |
| 4 | 10 | 0 |
| 1/2 | 3 | 0 |
| 3/2 | 3 | 1 |
| 5/2 | 3 | 2 |
| 5/2 | 3 | 2 |
| 3 | 4 | 2 |
| 6 | 8 | 2 |

Any patterns yet?

# A Theorem

It looks like there might be a linear relationship between the area, the number of boundary points, and the number of interior points.

It's not hard to identify the coefficients, and the end result is the content of Pick's Theorem:

**Theorem (Pick's Theorem)**

*If $R$ is a lattice polygon in the plane, then the area of $R$ is given by the formula* $\boxed{A = I + \frac{1}{2}B - 1}$, *where $I$ is the number of lattice points in the interior of $R$ and $B$ is the number of lattice points on the boundary of $R$.*

# Strategy for Pick's Theorem

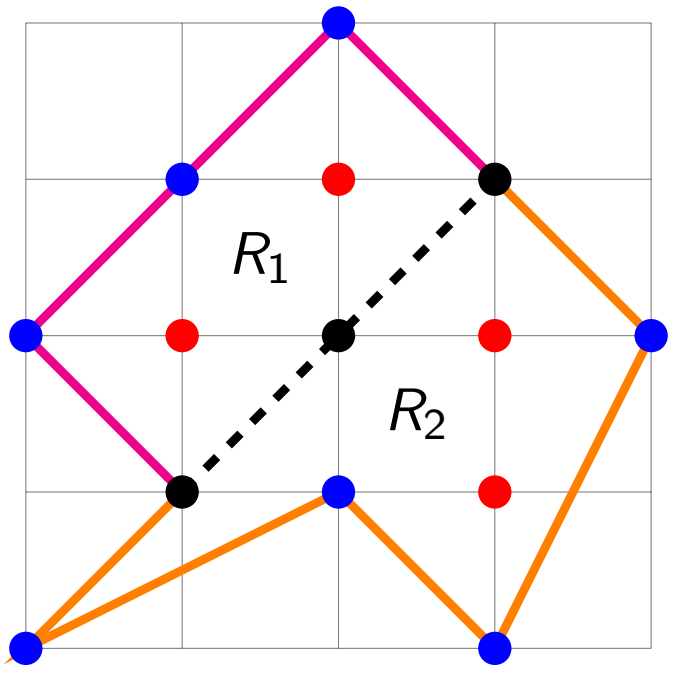
There are a number of approaches to proving Pick's Theorem. Here is our strategy:

- First, we show that if Pick's Theorem is true for two regions $R_1$ and $R_2$ that border each other along an edge (but don't overlap), then it is also true for the union $R_1 \cup R_2$.
- Second, we show that if Pick's Theorem is true for the regions $R_1$ and the union $R_1 \cup R_2$, then it is also true for $R_2$.
- Third, we will show that Pick's Theorem holds for an increasingly general collection of shapes, ending in general lattice polygons.

Steps 1 and 2 allow us to glue regions together, and to take regions apart. Step 3 allows us to apply these operations to any polygons we can show Pick's Theorem holds for. By gluing appropriately, we conclude that Pick's Theorem holds for every polygon.

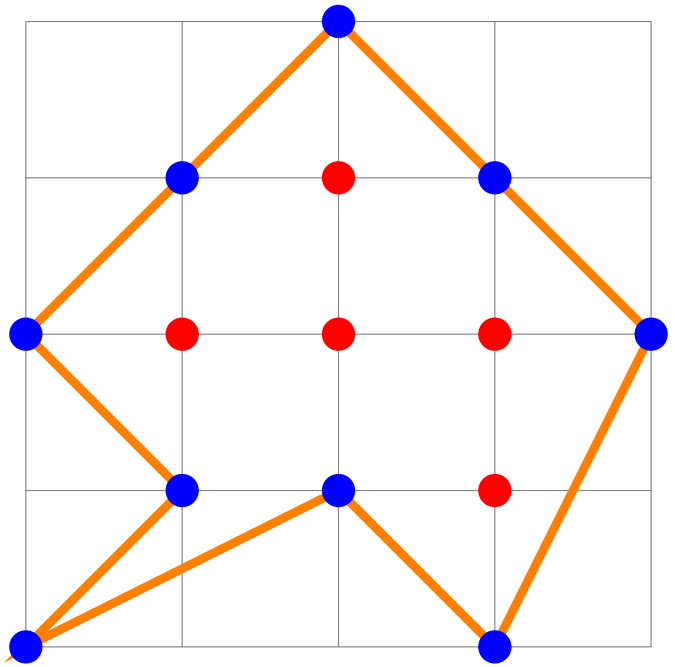
# Proof of Pick's Theorem: Step 1.1

So first suppose we have two regions $R_1$ and $R_2$ that border each other along an edge, like the example shown:



# Proof of Pick's Theorem: Step 1.2

When we glue the regions together, all the interior points of each region will remain interior points. The boundary points not on the common border also remain boundary points. The boundary points inside each border will become interior points, except for the two at the end (which stay boundary points). Or, just look below:



# Proof of Pick's Theorem: Step 1.3

The only points that change status are the boundary points on the border. Each of the 1/2 contributions to the area (from $R_1$ and $R_2$ separately) as boundary points becomes a 1 contribution to the area in the combined region... and those two boundary points at the end of the border cancel the extra $-1$ term that comes from adding the area formulas.

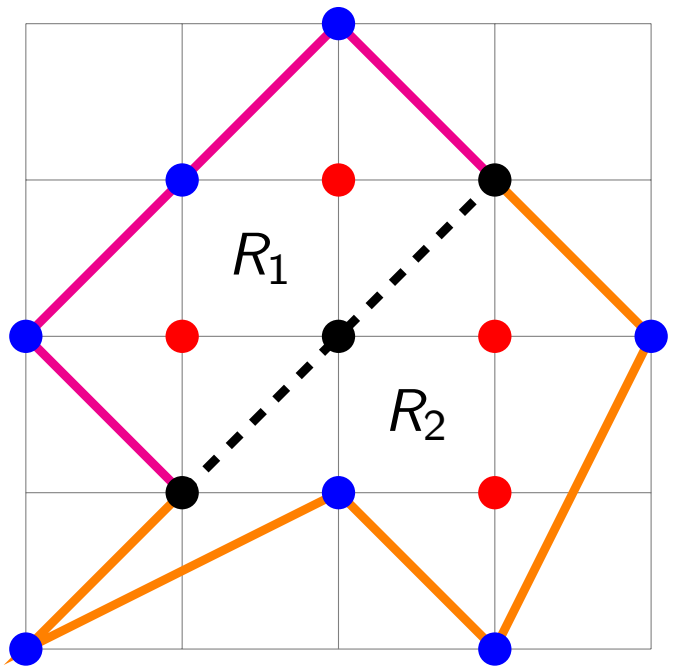
Or if you don't believe that, here's the algebra:

- If there are $I_i$ interior and $B_i$ boundary points of $R_i$ for $i = 1, 2$, and $N$ of the boundary points are common to both regions, then by the above analysis, $R_1 \cup R_2$ has $I = I_1 + I_2 + N - 2$ interior points and $B = B_1 + B_2 - 2N$ boundary points.
- Since $A_1 = I_1 + \frac{1}{2}B_1 - 1$ and $A_2 = I_2 + \frac{1}{2}B_2 - 1$, we have

$$A_1 + A_2 = (I_1 + I_2 + N) + \frac{1}{2}(B_1 + B_2 + 2N) - 1 = I + \frac{1}{2}B - 1.$$

# Proof of Pick's Theorem: Step 2

Now that we've shown that gluing regions together works correctly, we can just run our argument in reverse to see that subtracting one region from a union will also work correctly. (If you like, you can work out the counting parts yourself.)



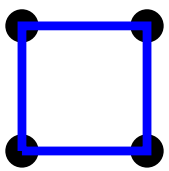
# Proof of Pick's Theorem: Step 3.1

Now we show that Pick's Theorem holds for more and more interesting regions.

# Proof of Pick's Theorem: Step 3.1

Now we show that Pick's Theorem holds for more and more interesting regions.

Region #1:

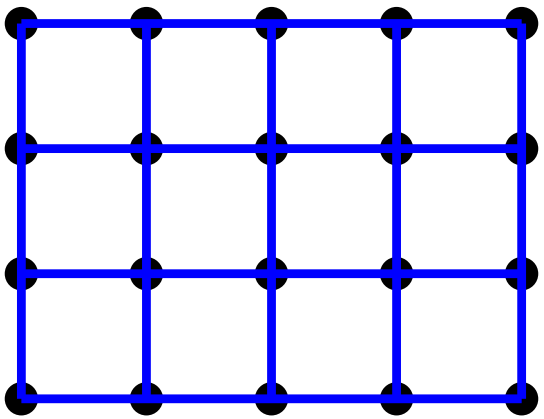


Area 1, 4 boundary points, 0 interior points.

Pick's Theorem says $A = \frac{4}{2} + 0 - 1 = 1$ ✓

# Proof of Pick's Theorem: Step 3.2

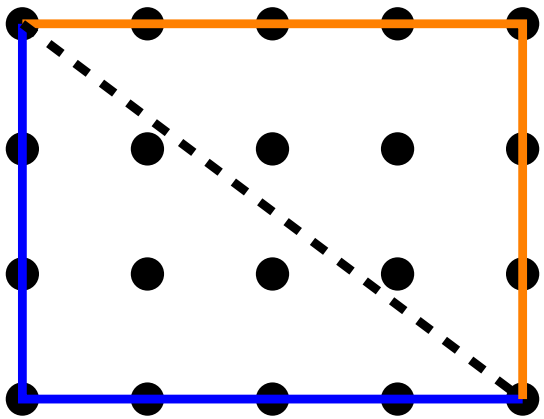
Region #2: (a general $m \times n$ rectangle, use your imagination!)



This rectangle is obtained by gluing together individual $1 \times 1$ rectangles. So since Pick's Theorem works for $1 \times 1$ rectangles, it works for rectangles of any size.

# Proof of Pick's Theorem: Step 3.3: Are We Done Yet?

Region #3: (a general $m \times n$ right triangle, use your imagination!)

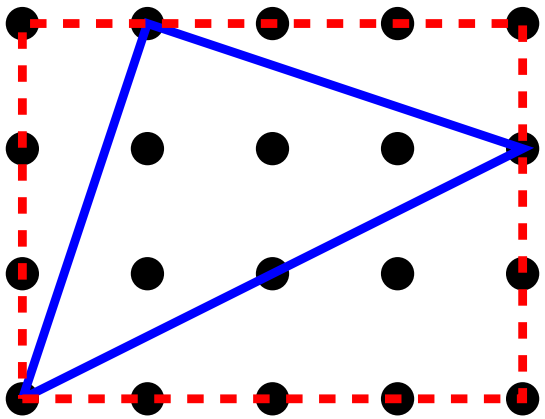


If we glue together two of these right triangles, then we obtain an $m \times n$ rectangle, for which we have just shown Pick's Theorem holds. If Pick's Theorem were wrong for the right triangle[1] (say it is off by an error $E$ from the right area) then gluing together the two congruent triangles would give an area that is off by $2E$. But we know that the area works out correctly, so $E = 0$.

[1] Not to be confused with Pick's Theorem being right for the wrong triangle!

# Proof of Pick's Theorem: Step 3.4: Apparently Not!

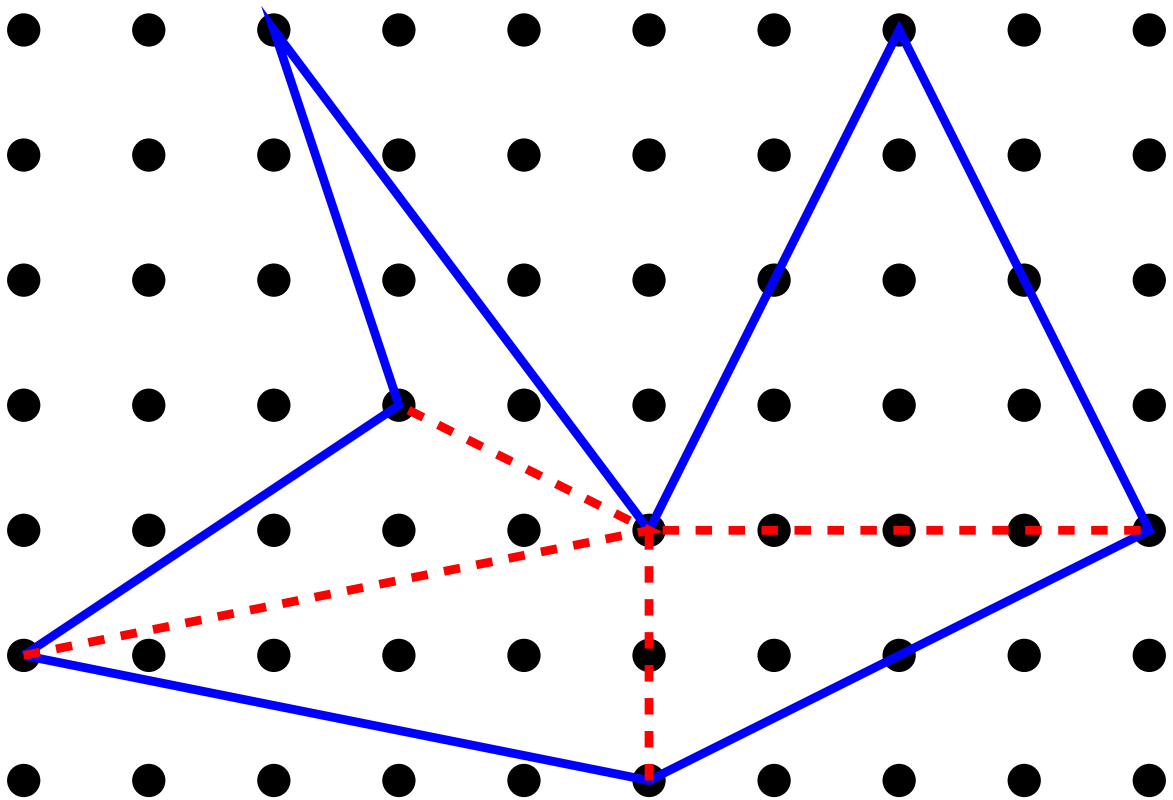
Region #4: (a general triangle, use your imagination!)



By drawing right triangles around a general triangle, we can form a rectangle. Since Pick's Theorem holds for rectangles and right triangles, by our removing result, it also holds for general triangles.

# Proof of Pick's Theorem: Step 3.5: We're Done Now!

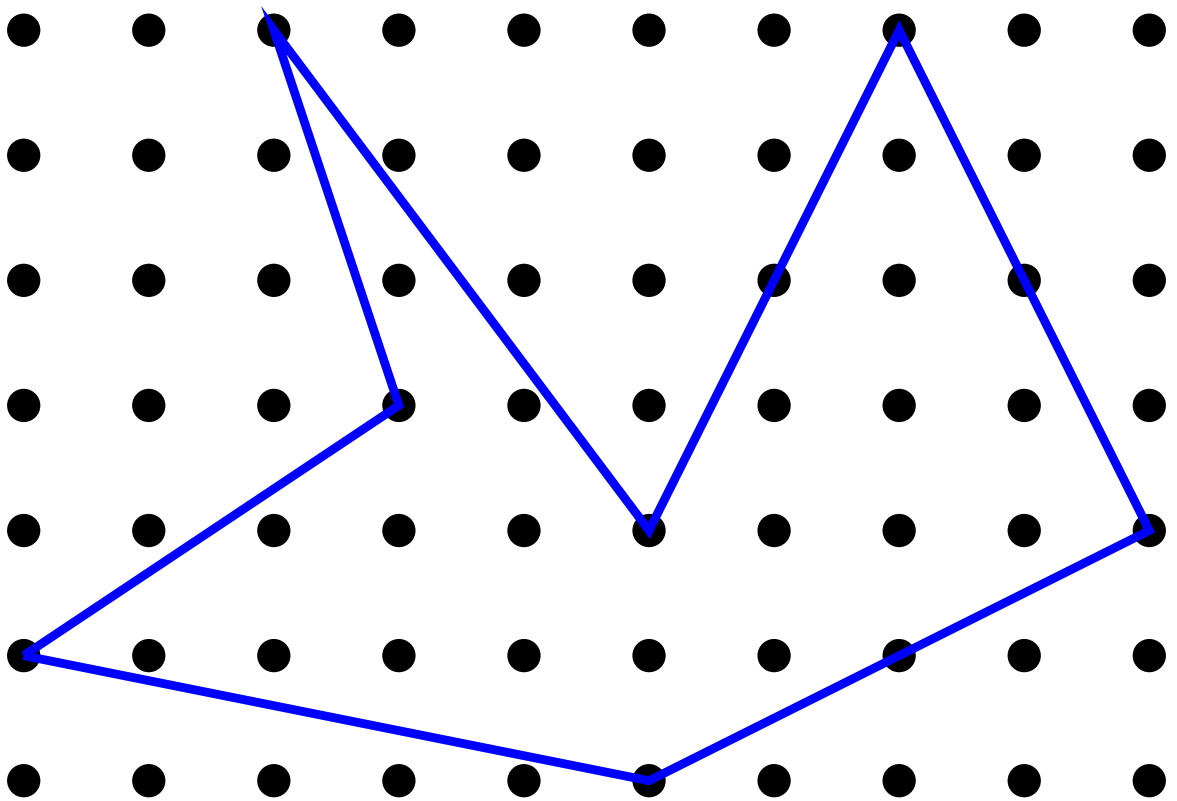
Region #5: (a general polygon, use your imagination!)



We may construct any polygon by adding and subtracting triangular regions from rectangular ones. This completes our proof.

# Give Pick's A Chance!

Let's confirm it really does work for this polygon we saw before:



There are 19 interior points and 10 boundary points. So Pick's Theorem says the area is $A = \frac{10}{2} + 19 - 1 = 23$ ✓

# Warning: Jarring Transition Ahead

So far, we have learned about the values of looking for patterns, making conjectures, and then testing and refining them.

... well, that's usually how I usually describe this procedure when I explain Pick's theorem to elementary school students, anyway.

# Warning: Jarring Transition Ahead

So far, we have learned about the values of looking for patterns, making conjectures, and then testing and refining them.

... well, that's usually how I usually describe this procedure when I explain Pick's theorem to elementary school students, anyway.

But it's also great advice at all levels of mathematics! Working out a bunch of examples and then making wild conjectures based on the examples and your own intuition can get you pretty far on actual research problems. (Or perhaps less excitingly, but more relevant to you, on your homework problems in upper-level math courses.)

Now let's look for some patterns in number theory.

# Farey Sequences, I

**Definition**

The Farey sequence of level $n$ consists of the rational numbers between 0 and 1 inclusive, whose denominators are at most $n$, arranged in increasing order.

# Farey Sequences, I

**Definition**

The Farey sequence of level $n$ consists of the rational numbers between 0 and 1 inclusive, whose denominators are at most $n$, arranged in increasing order.

Here are the first few Farey sequences:

- Level 1: $\frac{0}{1}, \frac{1}{1}$.
- Level 2: $\frac{0}{1}, \frac{1}{2}, \frac{1}{1}$.
- Level 3: $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$.
- Level 4: $\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$.

# Farey Sequences, II

To get the $(n+1)$st Farey sequence from the $n$th one, we just need to insert the fractions with denominator $n+1$ in the proper locations (and of course, make sure we don't try to include non-reduced terms!).

# Farey Sequences, II

To get the $(n+1)$st Farey sequence from the $n$th one, we just need to insert the fractions with denominator $n+1$ in the proper locations (and of course, make sure we don't try to include non-reduced terms!). Here are a few more:

- Level 5: $\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$.
- Level 6: $\frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1}$.
- Level 7:

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

What patterns do you notice?

# Farey Sequences, III

Let me draw your attention to the "new" terms (highlighted in color): try comparing them to the terms on either side.

- Here's 3 sets: $\frac{1}{2}, \frac{3}{5}, \frac{2}{3}$ $\quad$ $\frac{0}{1}, \frac{1}{7}, \frac{1}{6}$ $\quad$ $\frac{2}{5}, \frac{3}{7}, \frac{1}{2}$.

# Farey Sequences, III

Let me draw your attention to the "new" terms (highlighted in color): try comparing them to the terms on either side.

- Here's 3 sets: $\frac{1}{2}, \frac{3}{5}, \frac{2}{3}$ $\quad$ $\frac{0}{1}, \frac{1}{7}, \frac{1}{6}$ $\quad$ $\frac{2}{5}, \frac{3}{7}, \frac{1}{2}$.
- Notice that the denominators surrounding each new term always seem to sum to the denominator of the new term. And in fact, the same property also holds for the numerators!
- This suggests that if $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive terms in a Farey sequence, then the mediant $\frac{a+c}{b+d}$ (sometimes called the "baseball average") is always in lowest terms, and will be the next term that appears between $\frac{a}{b}$ and $\frac{c}{d}$.

# Farey Sequences, IV

For example, if you track the fractions $\frac{1}{2}$ and $\frac{2}{3}$, you'll see that the first term that is put between them is in fact the mediant $\frac{3}{5}$:

- Level 3: $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$.
- Level 4: $\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$.
- Level 5: $\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$.

# Farey Sequences, V

We can also look at differences of consecutive terms:

- Here's 4 pairs: $\frac{1}{3}, \frac{2}{5}$ $\frac{1}{6}, \frac{1}{5}$ $\frac{2}{7}, \frac{1}{3}$ $\frac{5}{6}, \frac{6}{7}$.

# Farey Sequences, V

We can also look at differences of consecutive terms:

- Here's 4 pairs: $\frac{1}{3}, \frac{2}{5} \qquad \frac{1}{6}, \frac{1}{5} \qquad \frac{2}{7}, \frac{1}{3} \qquad \frac{5}{6}, \frac{6}{7}$.
- We have $\frac{2}{5} - \frac{1}{3} = \frac{1}{15}$, and $\frac{1}{5} - \frac{1}{6} = \frac{1}{30}$, and $\frac{2}{7} - \frac{1}{5} = \frac{1}{35}$, and $\frac{6}{7} - \frac{5}{6} = \frac{1}{42}$.
- Note in each case that the difference $\frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}$ always seems to have numerator 1.
- This suggests that the value $bc - ad$ for consecutive terms $\frac{a}{b}$ and $\frac{c}{d}$ is always equal to 1.

# Farey Sequences, VI

In fact, both of these observations are true in general!

**Theorem (Properties of Farey Sequences)**

*Suppose that* $\frac{a}{b}$ *and* $\frac{c}{d}$ *are consecutive terms in a Farey sequence. Then*

1. *The value* $bc - ad$ *is equal to 1.*
2. *The mediant* $\frac{a+c}{b+d}$ *is always in lowest terms, and will be the next term that appears between* $\frac{a}{b}$ *and* $\frac{c}{d}$ *in a Farey sequence.*

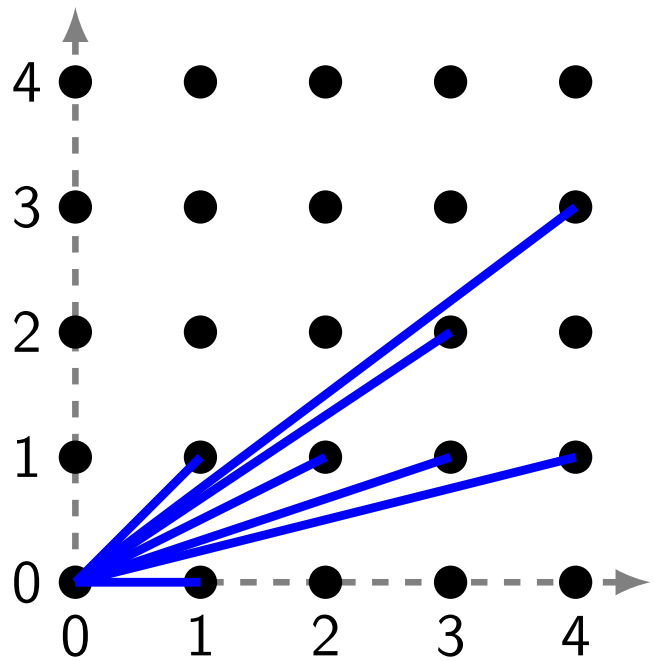
Let's prove these properties of Farey sequences.

# Farey Sequences, VII: The Force of geometry Awakens

A very simple but very useful idea is that we can interpret the Farey fraction $\frac{a}{b}$ as the slope of the line segment from the origin $(0, 0)$ to the point $(b, a)$.

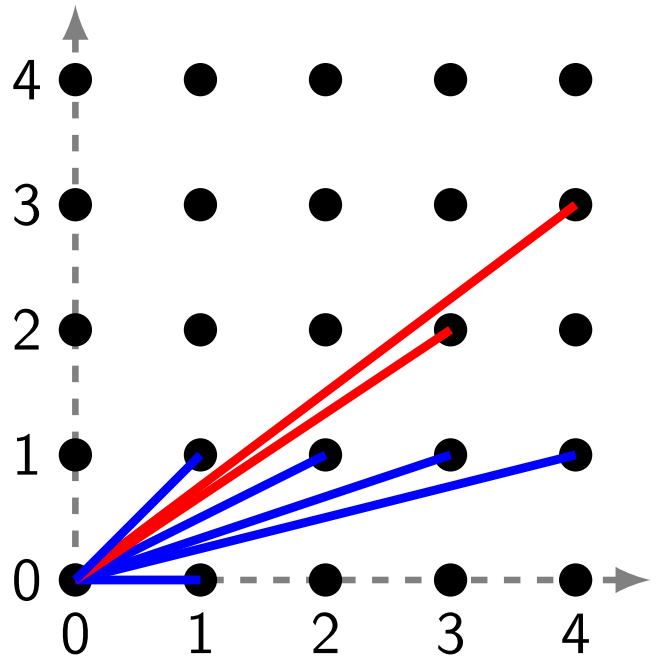
# Farey Sequences, VII: The Force of geometry Awakens

A very simple but very useful idea is that we can interpret the Farey fraction $\frac{a}{b}$ as the slope of the line segment from the origin $(0,0)$ to the point $(b,a)$. Here are the resulting line segments for the Farey sequence $\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$ of level 4:



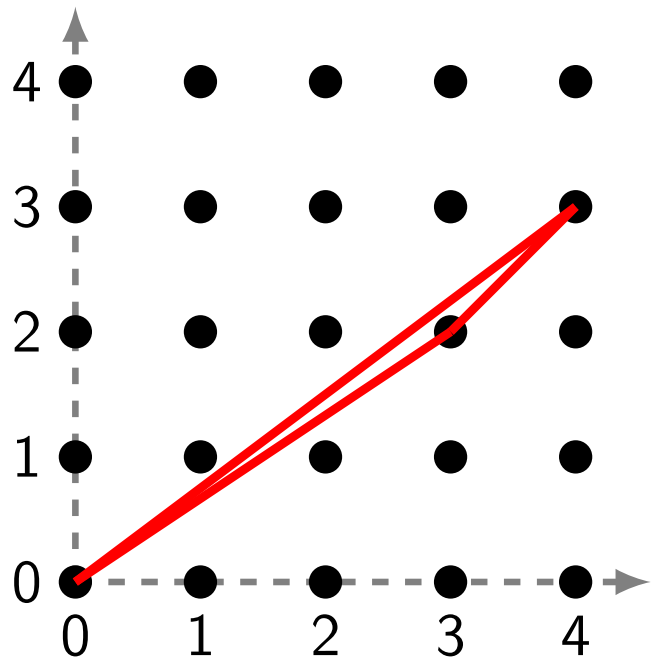
# Farey Sequences, VIII

Let's look at the two segments corresponding to two consecutive Farey fractions (in the diagram below, they are $\frac{2}{3}$ and $\frac{3}{4}$):



# Farey Sequences, IX: Pick The Right Idea

Now, if $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive Farey fractions, notice that these three points $(0,0)$, $(b,a)$, and $(d,c)$ form a triangle.



# Farey Sequences, IX: Pick's The Right Idea!

Let's compute the area of this triangle in two ways:

- If we just draw right triangles and subtract (or alternatively, we could use the "shoelace formula", or use the formula for the area of a triangle in terms of the cross product), we can see that the area of the triangle is $\frac{1}{2}(bc - ad)$.
- But we can also use (drumroll)...

# Farey Sequences, IX: Pick's The Right Idea!

Let's compute the area of this triangle in two ways:

- If we just draw right triangles and subtract (or alternatively, we could use the "shoelace formula", or use the formula for the area of a triangle in terms of the cross product), we can see that the area of the triangle is $\frac{1}{2}(bc - ad)$.
- But we can also use (drumroll)... Pick's Theorem! We just need to count interior and boundary points.
- From the picture on the previous slide, it seems very clear that there will be 3 boundary points and 0 interior points.
- If this is true, then the triangle's area is $A = \frac{3}{2} + 0 - 1 = \frac{1}{2}$.
- This means $\frac{1}{2} = \frac{1}{2}(bc - ad)$, and so $bc - ad = 1$ as claimed!

# Farey Sequences, XI: Wait, Where Did X Go?

Let's show that this triangle does indeed have 3 boundary points and 0 interior points:

- For boundary points, there are obviously the 3 vertices.
- Since $a/b$ is in lowest terms, there are no other boundary points on the segment from $(0,0)$ to $(b,a)$.
- Similarly, there are no extra points on the segment from $(0,0)$ to $(d,c)$.
- If there was an interior point or a boundary point on the segment from $(b,a)$ to $(d,c)$, say $(x,y)$, the slope of the line segment from $(0,0)$ to $(x,y)$ would be between $\frac{a}{b}$ and $\frac{c}{d}$. But this can't happen because $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive Farey fractions!
- We conclude that this triangle has 3 boundary points and 0 interior points, and so the result works out as claimed.

# Farey Sequences, XII: But Wait, There's More!

We now want to show the other part of the Theorem: so suppose that $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive, and that $\frac{e}{f}$ is the first term that appears between them.

- By the result we just proved, since $\frac{a}{b}$ and $\frac{e}{f}$ are consecutive, we know $be - af = 1$.
- Likewise, since $\frac{e}{f}$ and $\frac{c}{d}$ are consecutive, we know $cf - de = 1$.
- This is a system of two linear equations in the two variables $e$ and $f$. Solving it (row-reduce if you like!) yields the unique solution $e = \frac{a+c}{bc-ad}$ and $f = \frac{b+d}{bc-ad}$ after a bit of algebra.
- But $bc - ad = 1$, so in fact $e = a + c$ and $f = b + d$.

# Farey Sequences, XIII: Approximately Interesting

We can use these results about Farey sequences to establish a simple but very useful result about rational approximations:

**Proposition (Rational Approximation)**

*Suppose $\alpha$ is a real number. Then for any $N \geq 1$ there is a rational number $r/s$ such that $\left|\alpha - \frac{r}{s}\right| \leq \frac{1}{s(N+1)}$ and whose denominator $s$ is at most $N$.*

To prove this, first note that we can assume $\alpha$ lies in the interval $[0, 1]$ by subtracting off the integer part. Then if we write out the Farey sequence of level $N$, we see that $\alpha$ necessarily lands between two consecutive terms $a/b$ and $c/d$ in the Farey sequence. We can then compare $\alpha$ to the next term $(a+c)/(b+d)$ that appears between $a/b$ and $c/d$ in a later sequence.

# Farey Sequences, XIV: Approximately Interesting Proof

Here's the details (after assuming $\alpha \in [0,1]$):

- Consider the Farey sequence of level $N$ and let $\frac{a}{b}$ and $\frac{c}{d}$ be two consecutive terms with $\frac{a}{b} \le \alpha \le \frac{c}{d}$. Note $b+d \ge N+1$.
- Then $\alpha$ either lies in $\left[\frac{a}{b}, \frac{a+c}{b+d}\right]$ or in $\left[\frac{a+c}{b+d}, \frac{c}{d}\right]$.
- In the first case,
$$\left|\alpha - \frac{a}{b}\right| \le \left|\frac{a}{b} - \frac{a+c}{b+d}\right| = \frac{|ad-bc|}{b(b+d)} \le \frac{1}{b(N+1)}.$$
- In the second case,
$$\left|\alpha - \frac{c}{d}\right| \le \left|\frac{c}{d} - \frac{a+c}{b+d}\right| = \frac{|bc-ad|}{d(b+d)} \le \frac{1}{d(N+1)}.$$
- So in either case, we get an $\frac{r}{s}$ with $\left|\alpha - \frac{r}{s}\right| \le \frac{1}{s(N+1)}$.

# Warning: Jarring Transition Ahead, II

So, once again, we have seen the value of looking for patterns, making conjectures, and then connecting them to other results.

So now let's jump into looking at a third question, regarding sums of two squares.

# Sums of Two Squares, I

A very classical problem in number theory is to characterize the positive integers that can be written as the sum of two squares: i.e., find all $n = a^2 + b^2$ where $a$ and $b$ are integers.

- We can start making a list using the first few squares (0, 1, 4, 9, 16, 25, 36, 49, 64, 81, ...).
- So: which integers less than 40 are the sum of two squares?

# Sums of Two Squares, II

The first few sums of two squares are 0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, 65, 68, 72, 73, 74, ....

There are many patterns to be found on this list. Here are a few:

# Sums of Two Squares, II

The first few sums of two squares are 0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, 65, 68, 72, 73, 74, ....

There are many patterns to be found on this list. Here are a few:

- The list is closed under multiplication.
- There are never more than 3 consecutive terms. (There can be 3 in a row, such as 0-1-2, 8-9-10, 16-17-18, 72-73-74, ....)
- More generally, none of the numbers on the list is congruent to 3 modulo 4.

# Sums of Two Squares, III

We can in fact establish all of these things:

**Proposition (Properties of Sums of Two Squares)**

*Suppose that $S$ is the set of integers that are sums of two squares. Then the following hold:*

1. *$S$ is closed under multiplication.*
2. *No element of $S$ is congruent to 3 modulo 4, and therefore $S$ never contains more than 3 consecutive integers.*

# Sums of Two Squares, III

We can in fact establish all of these things:

**Proposition (Properties of Sums of Two Squares)**

*Suppose that $S$ is the set of integers that are sums of two squares. Then the following hold:*

1. *$S$ is closed under multiplication.*
2. *No element of $S$ is congruent to 3 modulo 4, and therefore $S$ never contains more than 3 consecutive integers.*

The proofs are not so hard:

- For the first, we can use the identity $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$, which was known to Diophantus.
- For the second, we can simply observe that any square is either 0 or 1 modulo 4, so the sum of two squares must be 0, 1, or 2 modulo 4.

# Sums of Two Squares, IV

Since there seems to be some amount of multiplicative structure to the sums of two squares, perhaps we should restrict attention to the primes.

- From the proposition, we know that primes congruent to 3 modulo 4 cannot be the sum of two squares.
- The remaining primes are 2 and the 1 mod 4 primes: 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, ....
- Which of these are sums of two squares?

# Sums of Two Squares, IV

Since there seems to be some amount of multiplicative structure to the sums of two squares, perhaps we should restrict attention to the primes.

- From the proposition, we know that primes congruent to 3 modulo 4 cannot be the sum of two squares.
- The remaining primes are 2 and the 1 mod 4 primes: 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, ....
- Which of these are sums of two squares?

It seems like... all of them!

# Sums of Two Squares, V

In fact, this is a famous theorem of Fermat, which he remarked upon in a letter to Mersenne dated December 25, 1640.

**Theorem (Fermat's Christmas Theorem)**

*If $p$ is a prime, then $p$ is a sum of two squares if and only if $p = 2$ or $p \equiv 1$ (mod 4).*

As noted on the last slide, it is clearly necessary that $p = 2$ or $p \equiv 1 \pmod 4$. And since 2 is a sum of two squares, we just need to show that if $p \equiv 1 \pmod 4$, then $p$ is the sum of two squares.

# Sums of Two Squares, V

In fact, this is a famous theorem of Fermat, which he remarked upon in a letter to Mersenne dated December 25, 1640.

**Theorem (Fermat's Christmas Theorem)**

*If $p$ is a prime, then $p$ is a sum of two squares if and only if $p = 2$ or $p \equiv 1$ (mod 4).*

As noted on the last slide, it is clearly necessary that $p = 2$ or $p \equiv 1 \pmod 4$. And since 2 is a sum of two squares, we just need to show that if $p \equiv 1 \pmod 4$, then $p$ is the sum of two squares.

To prove Fermat's theorem we will first establish a lemma:

**Lemma**

*If $p \equiv 1$ (mod 4) is a prime, then there exists an integer $A$ such that $A^2 \equiv -1$ (mod $p$).*

# Sums of Two Squares, VI

Proof:

- Suppose $p \equiv 1 \pmod 4$ is prime and group the $p-1$ nonzero residue classes modulo $p$ into sets $\{a, -a, a^{-1}, -a^{-1}\}$.
- It is easy to see that this is a well-defined equivalence relation, so we obtain a partition of the residue classes.
- Consider the sizes of the possible sets. If all four elements are different, the size is 4. Otherwise some elements are equal.
- We cannot have $a \equiv -a$, but $a \equiv a^{-1}$ is equivalent to $a^2 \equiv 1$ with solutions $a \equiv \pm 1 \pmod p$, and $a \equiv -a^{-1}$ is equivalent to $a^2 \equiv -1 \pmod p$.
- So all of the sets have size 4, except for the one set $\{1, -1\}$ and possibly another $\{A, -A\}$ where $A^2 \equiv -1 \pmod p$.
- But because $p-1$ is a multiple of 4, we must actually have a set $\{A, -A\}$, so there is a solution to $A^2 \equiv -1 \pmod{\text{p}}$.

# Sums of Two Squares, VII

I'll also mention that there are a lot of other ways to prove the lemma, such as the following:

- Use Wilson's theorem that $(p-1)! \equiv -1 \pmod{p}$ to show that $A = [(p-1)/2]!$ has $A^2 \equiv -1 \pmod{p}$.
- Show that the group of units modulo $p$ is cyclic of order $p-1$, and deduce that it has an element of order 4 since 4 divides $p-1$.
- Observe that if $a$ is any nonsquare residue class modulo $p$, then $a^{(p-1)/2} \equiv -1 \pmod{p}$, and so $A = a^{(p-1)/4}$ necessarily has square $-1 \pmod{p}$.

# Sums of Two Squares, VIII

Now we can finish off Fermat's Christmas theorem with a little bit of help from Farey, as follows:

- Suppose $p \equiv 1 \pmod 4$ is prime and let $N = \lfloor \sqrt{p} \rfloor$ be the greatest integer less than $\sqrt{p}$ and let $A$ be a solution to $A^2 \equiv -1 \pmod p$.
- By our Farey approximation theorem, there exists a rational $\frac{r}{s}$ such that $\left| \frac{A}{p} - \frac{r}{s} \right| \leq \frac{1}{s(N+1)}$, where $s \leq N < \sqrt{p}$.
- With $t = As - rp$, we have $|t| = |As - rp| \leq \frac{p}{N+1} < \sqrt{p}$.
- Thus, $0 < s^2 + t^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$.
- But $s^2 + t^2 = s^2 + (As - rp)^2 \equiv s^2(1 + A^2) \equiv 0 \pmod p$.
- So $s^2 + t^2$ is an integer between 0 and $2p$ that is divisible by $p$, so it equals $p$. Thus, $p$ is the sum of two squares!

# Thanks!

Thanks to Zack Eisbach, Toby Busick-Warner, and the other math club organizers for providing me the opportunity to speak here today! Although I usually give research-centered talks in the math club, I thought it would be nice to lead a more relaxed tour through some nice gems from elementary mathematics.

I hope you enjoyed it, and I'd like to thank you for attending! Enjoy your weekend!