A Smörgåsbord of Arithmetic Geometry

Shishir Agrawal

University of California, Berkeley

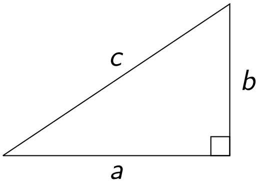
February 2, 2018

Smörgåsbord

Arithmetic geometry is an active area of mathematical research with a rich history. Today, I'd like to give you a taste of the field with a smörgåsbord of motivating examples.

Outline

The Pythagorean theorem



If a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then

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

Pythagorean triples

Are there any right triangles all of whose sides have integer lengths?

Pythagorean triples

Are there any right triangles all of whose sides have integer lengths?

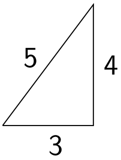
In other words, are there positive integers (a, b, c) satisfying $a^2 + b^2 = c^2$?

Pythagorean triples

Are there any right triangles all of whose sides have integer lengths?

In other words, are there positive integers (a, b, c) satisfying $a^2 + b^2 = c^2$?

Yes! $(3, 4, 5)$ is an example.

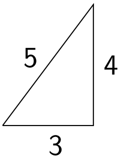


Pythagorean triples

Are there any right triangles all of whose sides have integer lengths?

In other words, are there positive integers (a, b, c) satisfying $a^2 + b^2 = c^2$?

Yes! $(3, 4, 5)$ is an example.



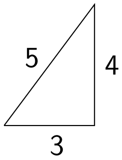
Lists of integers like this are called *Pythagorean triples*.

Pythagorean triples

Are there any right triangles all of whose sides have integer lengths?

In other words, are there positive integers (a, b, c) satisfying $a^2 + b^2 = c^2$?

Yes! $(3, 4, 5)$ is an example.



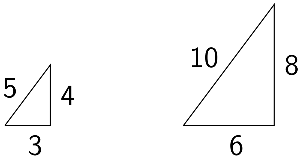
Lists of integers like this are called *Pythagorean triples*.

Are there any other Pythagorean triples?

Yes, we could multiply $(3, 4, 5)$ by 2 to get $(6, 8, 10)$,

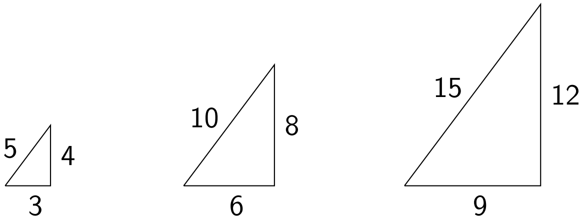
Yes, we could multiply $(3, 4, 5)$ by 2 to get $(6, 8, 10)$, which is also a Pythagorean triple:

$$6^2 + 8^2 = 36 + 64 = 100 = 10^2.$$



Yes, we could multiply $(3, 4, 5)$ by 2 to get $(6, 8, 10)$, which is also a Pythagorean triple:

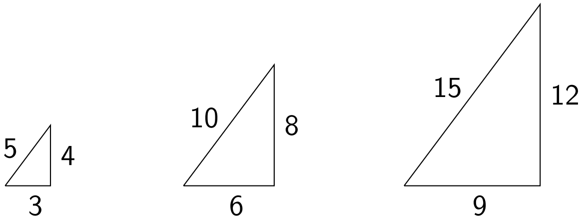
$$6^2 + 8^2 = 36 + 64 = 100 = 10^2.$$



We could also have multiplied by 3, or 4, or...

Yes, we could multiply $(3, 4, 5)$ by 2 to get $(6, 8, 10)$, which is also a Pythagorean triple:

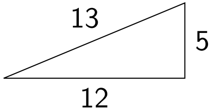
$$6^2 + 8^2 = 36 + 64 = 100 = 10^2.$$



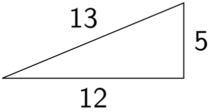
We could also have multiplied by 3, or 4, or...

Are there any other Pythagorean triples?

Sure, there's $(12, 5, 13)$.

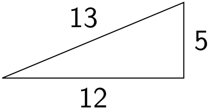


Sure, there's $(12, 5, 13)$.



As before, its integer multiples (like $(24, 10, 26), (36, 15, 39), \ldots$) are also Pythagorean triples.

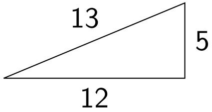
Sure, there's $(12, 5, 13)$.



As before, its integer multiples (like $(24, 10, 26), (36, 15, 39), \ldots$) are also Pythagorean triples.

Are there any others?

Sure, there's $(12, 5, 13)$.

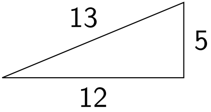


As before, its integer multiples (like $(24, 10, 26), (36, 15, 39)$,...) are also Pythagorean triples.

Are there any others?

Is there a systematic way of finding *all* of the Pythagorean triples?

Sure, there's $(12, 5, 13)$.



As before, its integer multiples (like $(24, 10, 26), (36, 15, 39)$,...) are also Pythagorean triples.

Are there any others?

Is there a systematic way of finding *all* of the Pythagorean triples?

Yes! Let's see how.

Reduced triples

Before proceeding, let's say that a Pythagorean triple (a, b, c) is *reduced* if a, b and c have no common factors.

Reduced triples

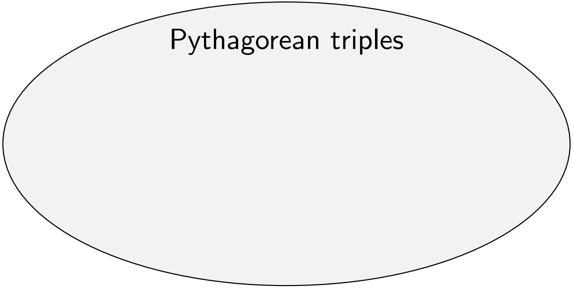
Before proceeding, let's say that a Pythagorean triple (a, b, c) is *reduced* if a, b and c have no common factors.

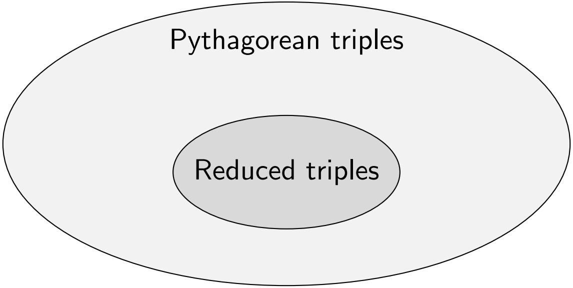
For example, $(3, 4, 5)$ is reduced,

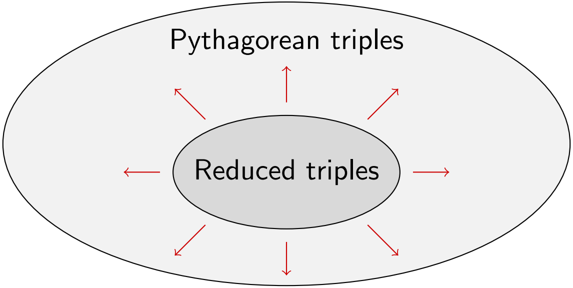
Reduced triples

Before proceeding, let's say that a Pythagorean triple (a, b, c) is *reduced* if a, b and c have no common factors.

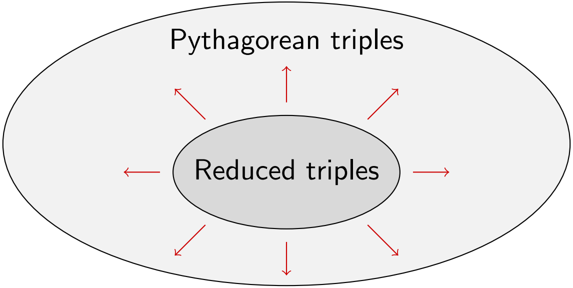
For example, $(3, 4, 5)$ is reduced, but $(6, 8, 10)$ is not since 2 is a common factor of $6, 8$ and 10.


Pythagorean triples


Pythagorean triples
Reduced triples

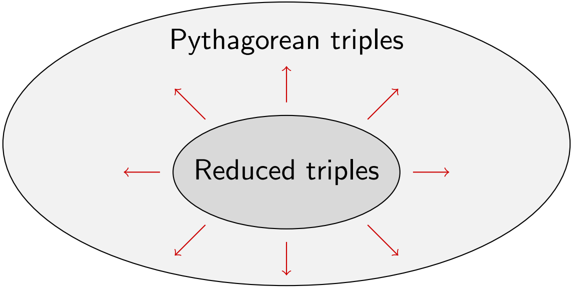


Every Pythagorean triple can be found by scaling up a reduced triple.



Every Pythagorean triple can be found by scaling up a reduced triple.

So, if we can find the reduced triples, we can find the rest.



Every Pythagorean triple can be found by scaling up a reduced triple.

So, if we can find the reduced triples, we can find the rest.

Our goal will be to systematically list the reduced triples.

Rational numbers

A *rational number* is a number that can be written as an integer over another integer.

Rational numbers

A *rational number* is a number that can be written as an integer over another integer.

For example,

$$\frac{1}{3}, \frac{-5}{173}, \text{ and } \frac{4}{1} = 4$$

are all rational numbers.

Rational numbers

A *rational number* is a number that can be written as an integer over another integer.

For example,

$$\frac{1}{3}, \frac{-5}{173}, \text{ and } \frac{4}{1} = 4$$

are all rational numbers.

If I add, subtract, multiply, or divide two rational numbers, the result will still be a rational number.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

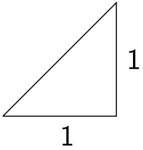
Irrational numbers

Not all numbers are rational.

Irrational numbers

Not all numbers are rational.

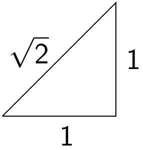
Let's think about the right triangle with leg lengths 1.



Irrational numbers

Not all numbers are rational.

Let's think about the right triangle with leg lengths 1.

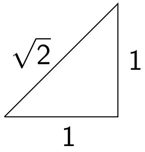


The Pythagorean theorem tells us that the hypotenuse has length $\sqrt{2}$.

Irrational numbers

Not all numbers are rational.

Let's think about the right triangle with leg lengths 1.



The Pythagorean theorem tells us that the hypotenuse has length $\sqrt{2}$.

It has been known for thousands of years that this number is *irrational*. A classical proof by contradiction can be found in Euclid's *Elements*.

Back to finding a systematic way of listing reduced triples...

Back to finding a systematic way of listing reduced triples...

We'll start with a reduced Pythagorean triple (a, b, c).

Back to finding a systematic way of listing reduced triples...

We'll start with a reduced Pythagorean triple (a, b, c).

Let's take the Pythagorean theorem

$$a^2 + b^2 = c^2$$

and divide through by c^2.

Back to finding a systematic way of listing reduced triples...

We'll start with a reduced Pythagorean triple (a, b, c).

Let's take the Pythagorean theorem

$$a^2 + b^2 = c^2$$

and divide through by c^2.

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

Back to finding a systematic way of listing reduced triples...

We'll start with a reduced Pythagorean triple (a, b, c).

Let's take the Pythagorean theorem

$$a^2 + b^2 = c^2$$

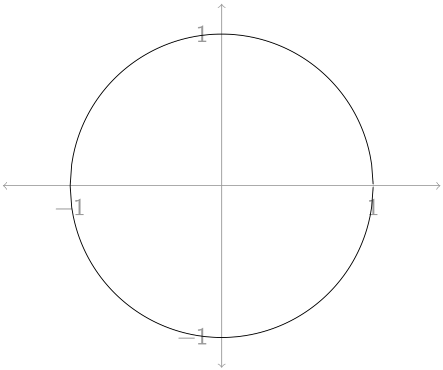
and divide through by c^2.

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

In other words, $x = a/c$ and $y = b/c$ are rational numbers satisfying

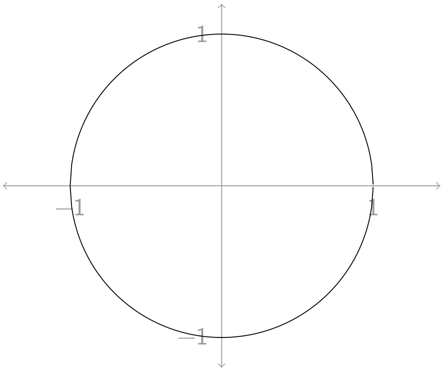
$$x^2 + y^2 = 1.$$

The equation $x^2 + y^2 = 1$ defines a circle of radius 1.



The equation $x^2 + y^2 = 1$ defines a circle of radius 1.

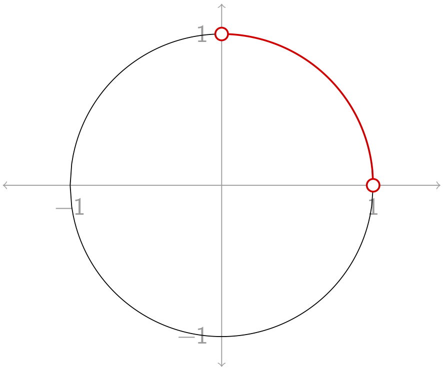
If a, b, c are all positive, so are $x = a/c$ and $y = b/c$...

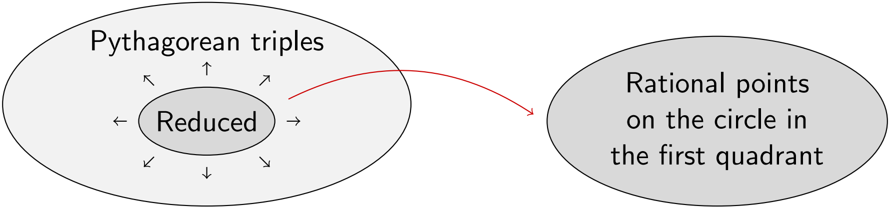


The equation $x^2 + y^2 = 1$ defines a circle of radius 1.

If a, b, c are all positive, so are $x = a/c$ and $y = b/c$...

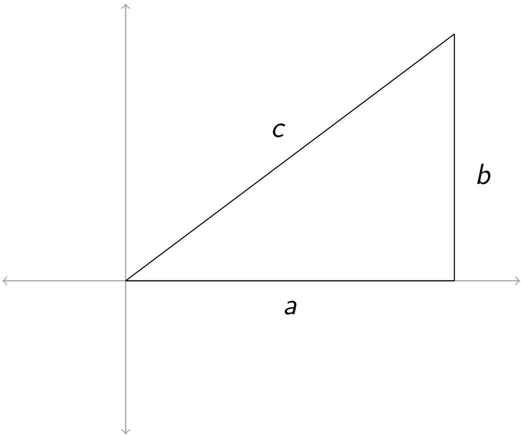
...so (x, y) is a *rational point* on the circle in the first quadrant.



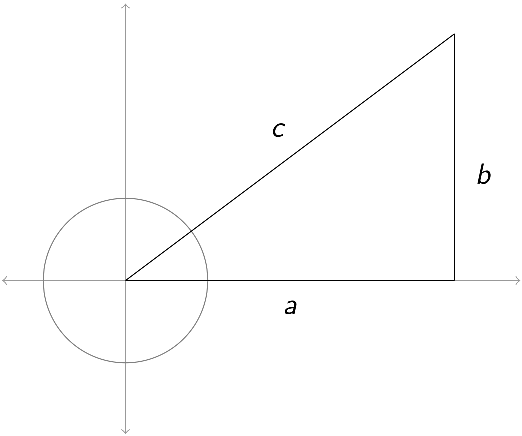


We started with a reduced Pythagorean triple and found a rational point on the circle $x^2 + y^2 = 1$ inside the first quadrant.

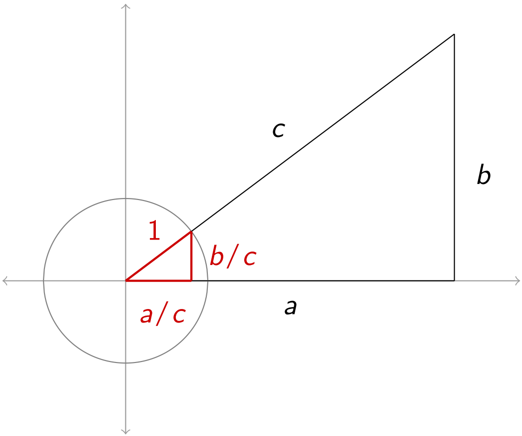
Geometrically, here's what we did.



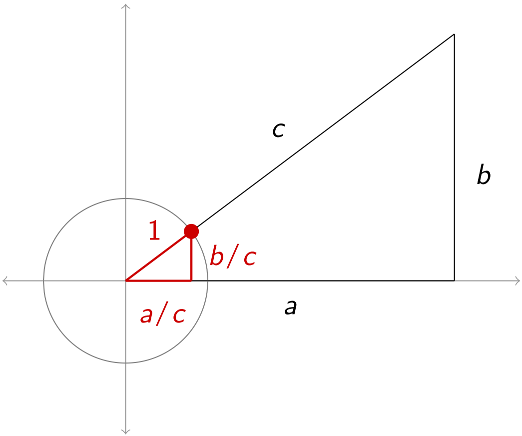
Geometrically, here's what we did.

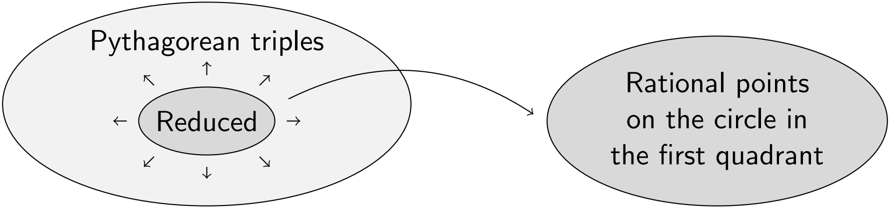


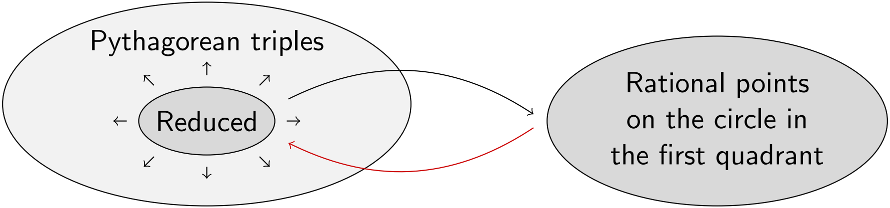
Geometrically, here's what we did.



Geometrically, here's what we did.




Pythagorean triples
Reduced
Rational points
on the circle in
the first quadrant



We can also go the other way: given any rational point on the circle $x^2 + y^2 = 1$ in the first quadrant, we can get a reduced Pythagorean triple.

Let's see how!

Least common denominator

The *least common denominator* of two fractions is the smallest number that is a multiple of both of the denominators.

Least common denominator

The *least common denominator* of two fractions is the smallest number that is a multiple of both of the denominators.

It's the smallest denominator that makes it easy to add the fractions.

Least common denominator

The *least common denominator* of two fractions is the smallest number that is a multiple of both of the denominators.

It's the smallest denominator that makes it easy to add the fractions.

For example,

$$\frac{1}{4} + \frac{5}{6} = \frac{3}{12} + \frac{10}{12} = \frac{13}{12},$$

and the least common denominator of $1/4$ and $5/6$ is 12.

Suppose x and y are positive rational numbers such that

$$x^2 + y^2 = 1.$$

Suppose x and y are positive rational numbers such that

$$x^2 + y^2 = 1.$$

We write them over the least common denominator as $x = a/c$ and $y = b/c$,

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1,$$

Suppose x and y are positive rational numbers such that

$$x^2 + y^2 = 1.$$

We write them over the least common denominator as $x = a/c$ and $y = b/c$,

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1,$$

and then clear denominators:

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

Suppose x and y are positive rational numbers such that

$$x^2 + y^2 = 1.$$

We write them over the least common denominator as $x = a/c$ and $y = b/c$,

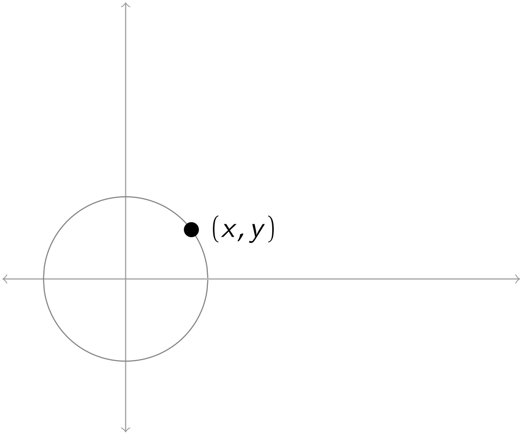
$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1,$$

and then clear denominators:

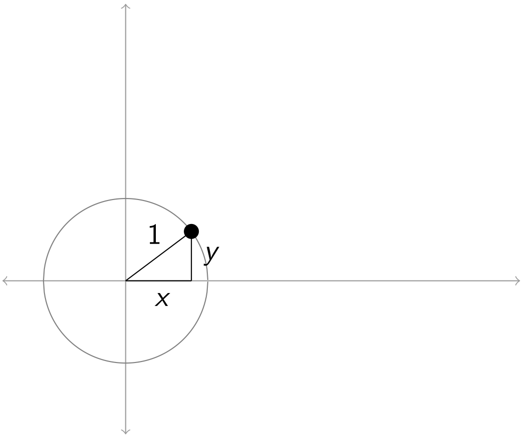
$$a^2 + b^2 = c^2.$$

Since c is the least common denominator, (a, b, c) is a reduced Pythagorean triple.

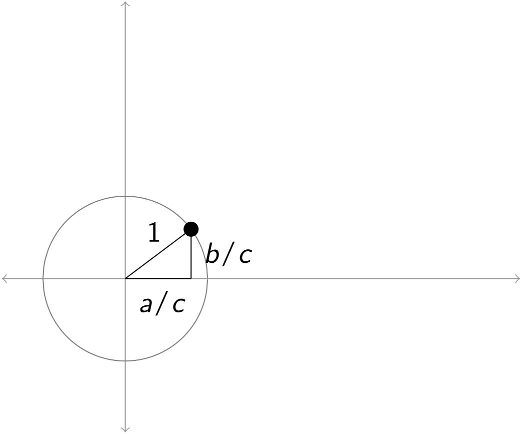
Geometrically, here's what we did!



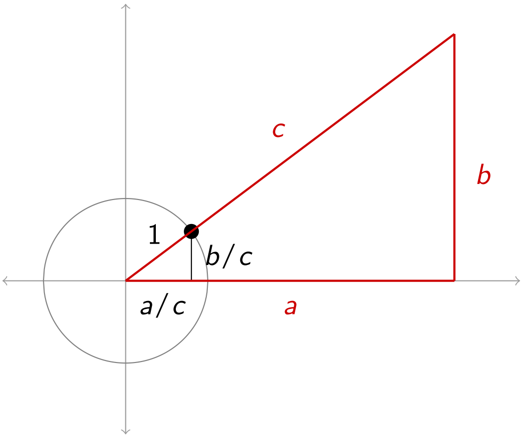
Geometrically, here's what we did!

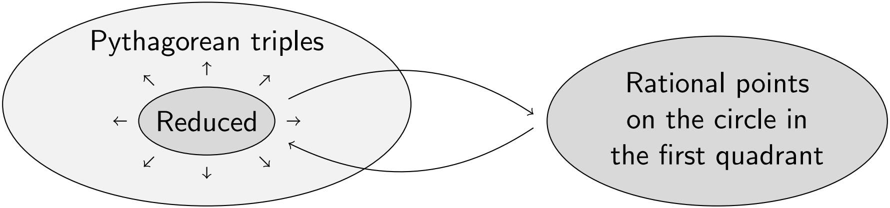


Geometrically, here's what we did!

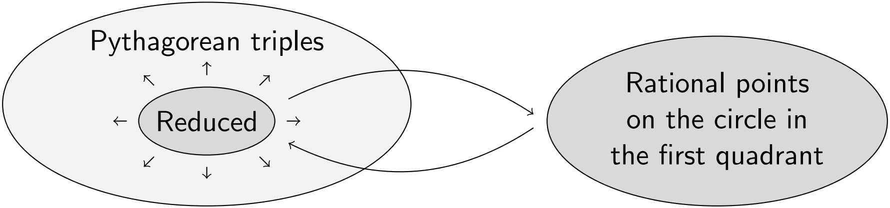


Geometrically, here's what we did!



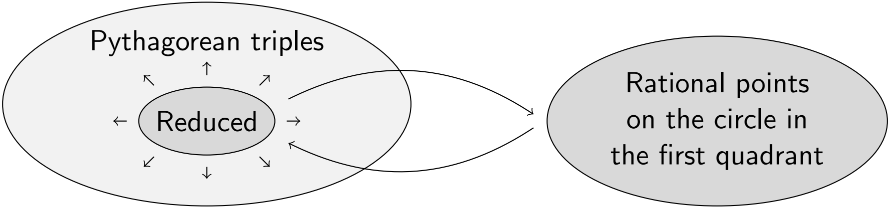


So, finding reduced Pythagorean triples is the same as finding rational points on the circle $x^2 + y^2 = 1$ inside the first quadrant.



So, finding reduced Pythagorean triples is the same as finding rational points on the circle $x^2 + y^2 = 1$ inside the first quadrant.

Is there a systematic way to list these rational points?

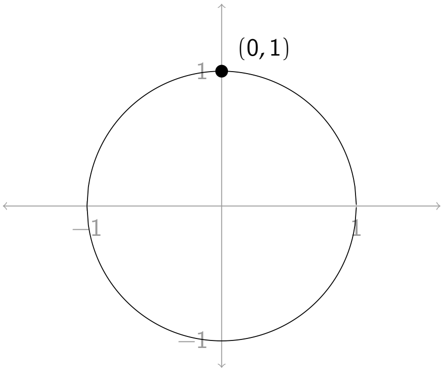


So, finding reduced Pythagorean triples is the same as finding rational points on the circle $x^2 + y^2 = 1$ inside the first quadrant.

Is there a systematic way to list these rational points?

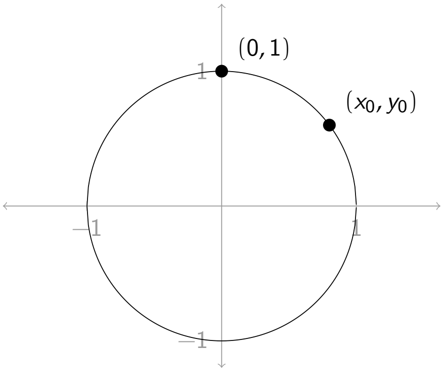
Let's see!

The point $(0, 1)$ is on the circle.



The point $(0, 1)$ is on the circle.

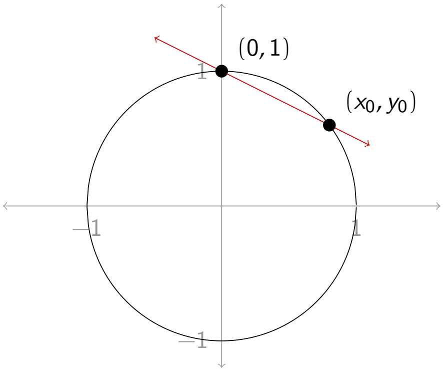
Let's say that (x_0, y_0) is another rational point on the circle.



The point $(0,1)$ is on the circle.

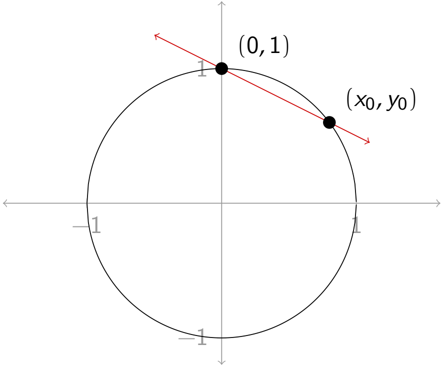
Let's say that (x_0, y_0) is another rational point on the circle.

Draw a line through $(0,1)$ and (x_0, y_0).



This line has equation

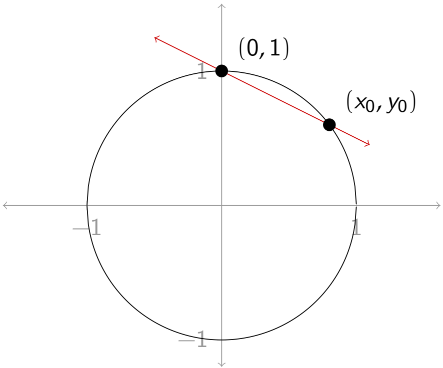
$$y = \underbrace{\left(\frac{y_0 - 1}{x_0}\right)}_{r} x + 1.$$



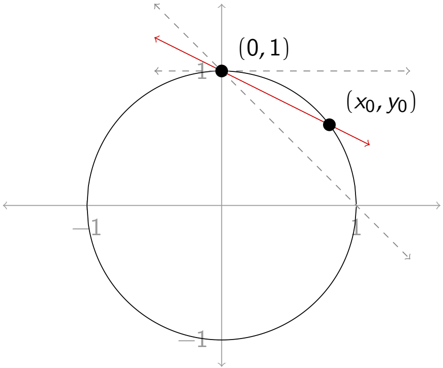
This line has equation

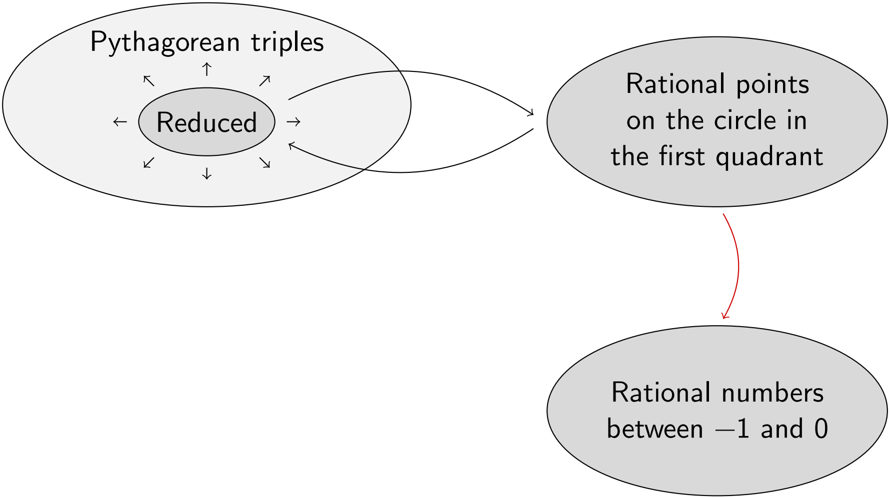
$$y = \underbrace{\left(\frac{y_0 - 1}{x_0}\right)}_{r} x + 1.$$

Notice that the slope r is a rational number.

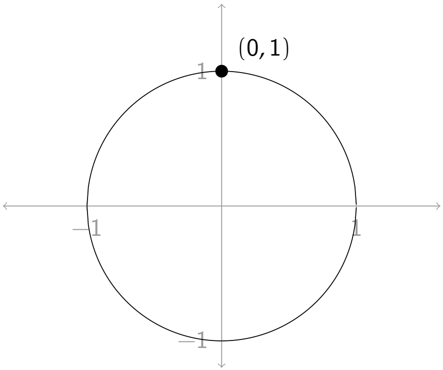


If (x_0, y_0) is in the first quadrant, the slope r is between -1 and 0.



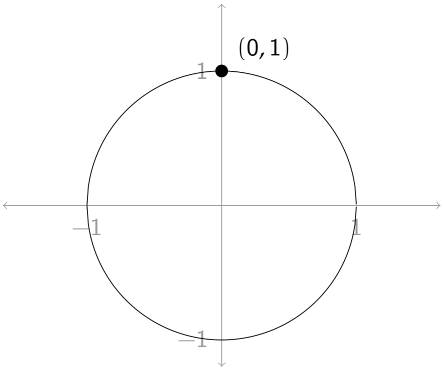

Pythagorean triples
Reduced
Rational points
on the circle in
the first quadrant
Rational numbers
between −1 and 0

Can we go the other way?



Can we go the other way?

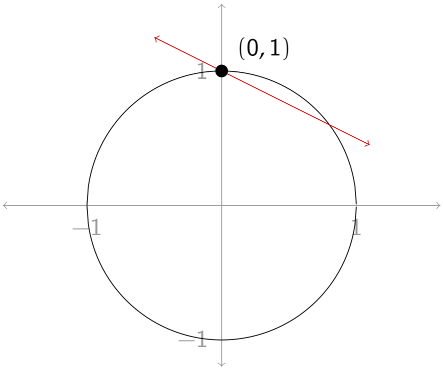
Suppose we start with an arbitrary rational slope r between -1 and 0...



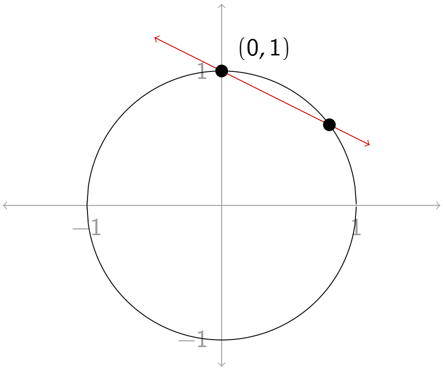
Can we go the other way?

Suppose we start with an arbitrary rational slope r between -1 and 0...

... and we draw the line of slope r passing through $(0, 1)$.

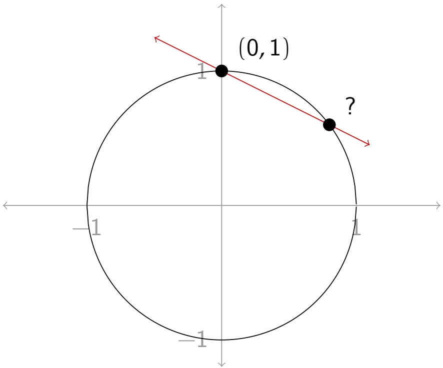


This line will intersect the circle in another point inside the first quadrant.



This line will intersect the circle in another point inside the first quadrant.

Will that point have rational coordinates?



Let's find the coordinates of the point of intersection.

Let's find the coordinates of the point of intersection.

In other words, we want to solve the following system of equations.

$$\begin{cases} x^2 + y^2 = 1 \\ y = rx + 1 \end{cases}$$

Let's find the coordinates of the point of intersection.

In other words, we want to solve the following system of equations.

$$\begin{cases} x^2 + y^2 = 1 \\ y = rx + 1 \end{cases}$$

Substituting $y = rx + 1$ into $x^2 + y^2 = 1$, we find

$$x^2 + (rx + 1)^2 = 1.$$

The equation $x^2 + (rx + 1)^2 = 1$...

The equation $x^2 + (rx + 1)^2 = 1$...

- is quadratic, so it has two roots,

The equation $x^2 + (rx + 1)^2 = 1$...

- is quadratic, so it has two roots,
- has rational coefficients,

The equation $x^2 + (rx + 1)^2 = 1$...

- is quadratic, so it has two roots,
- has rational coefficients,
- and has the *rational* number $x = 0$ as a root.

The equation $x^2 + (rx + 1)^2 = 1$...

- is quadratic, so it has two roots,
- has rational coefficients,
- and has the *rational* number $x = 0$ as a root.

Fact

If we have a polynomial with rational coefficients and we know that all but possibly one of its roots are rational, then the last root must be rational too.

The equation $x^2 + (rx+1)^2 = 1\ldots$

- is quadratic, so it has two roots,
- has rational coefficients,
- and has the *rational* number $x = 0$ as a root.

Fact

If we have a polynomial with rational coefficients and we know that all but possibly one of its roots are rational, then the last root must be rational too.

This means that the second root of $x^2 + (rx+1)^2 = 1$ is also rational.

The equation $x^2 + (rx + 1)^2 = 1$...

- is quadratic, so it has two roots,
- has rational coefficients,
- and has the *rational* number $x = 0$ as a root.

Fact

If we have a polynomial with rational coefficients and we know that all but possibly one of its roots are rational, then the last root must be rational too.

This means that the second root of $x^2 + (rx + 1)^2 = 1$ is also rational.

Since $y = rx + 1$, we know that y is rational when x is rational.

The equation $x^2 + (rx+1)^2 = 1$...

- is quadratic, so it has two roots,
- has rational coefficients,
- and has the *rational* number $x = 0$ as a root.

Fact

If we have a polynomial with rational coefficients and we know that all but possibly one of its roots are rational, then the last root must be rational too.

This means that the second root of $x^2 + (rx+1)^2 = 1$ is also rational.

Since $y = rx + 1$, we know that y is rational when x is rational.

So the second point of intersection is a rational point!

We can find the coordinates of the second point of intersection explicitly.

$$x^2 + (rx + 1)^2 = 1$$

We can find the coordinates of the second point of intersection explicitly.

$$
\begin{aligned}
x^2 + (rx + 1)^2 &= 1 \\
x^2 + (r^2x^2 + 2rx + 1) &= 1
\end{aligned}
$$

We can find the coordinates of the second point of intersection explicitly.

$$
\begin{aligned}
x^2 + (rx+1)^2 &= 1 \\
x^2 + (r^2x^2 + 2rx + 1) &= 1 \\
(1+r^2)x^2 + 2rx &= 0
\end{aligned}
$$

We can find the coordinates of the second point of intersection explicitly.

$$\begin{aligned} x^2 + (rx+1)^2 &= 1 \\ x^2 + (r^2x^2 + 2rx + 1) &= 1 \\ (1+r^2)x^2 + 2rx &= 0 \\ x((1+r^2)x + 2r) &= 0 \end{aligned}$$

We can find the coordinates of the second point of intersection explicitly.

$$
\begin{aligned}
x^2 + (rx + 1)^2 &= 1 \\
x^2 + (r^2x^2 + 2rx + 1) &= 1 \\
(1 + r^2)x^2 + 2rx &= 0 \\
x((1 + r^2)x + 2r) &= 0 \\
x &= \begin{cases} 0 \\ \dfrac{-2r}{1 + r^2} \end{cases}
\end{aligned}
$$

We can find the coordinates of the second point of intersection explicitly.

$$\begin{aligned} x^2 + (rx+1)^2 &= 1 \\ x^2 + (r^2x^2 + 2rx + 1) &= 1 \\ (1+r^2)x^2 + 2rx &= 0 \\ x((1+r^2)x + 2r) &= 0 \\ x &= \begin{cases} 0 \\ \dfrac{-2r}{1+r^2} \end{cases} \end{aligned}$$

Note that $x = 0$ corresponds to the point $(0, 1)$, so we want $x = \dfrac{-2r}{1+r^2}$.

Plugging in $x = \dfrac{-2r}{1+r^2}$, we have

$$y = rx + 1$$

Plugging in $x = \dfrac{-2r}{1+r^2}$, we have

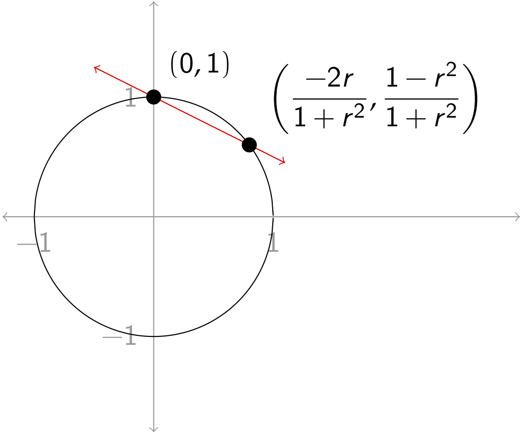
$$\begin{aligned} y &= rx + 1 \\ &= r\left(\frac{-2r}{1+r^2}\right) + 1 \end{aligned}$$

Plugging in $x = \dfrac{-2r}{1+r^2}$, we have

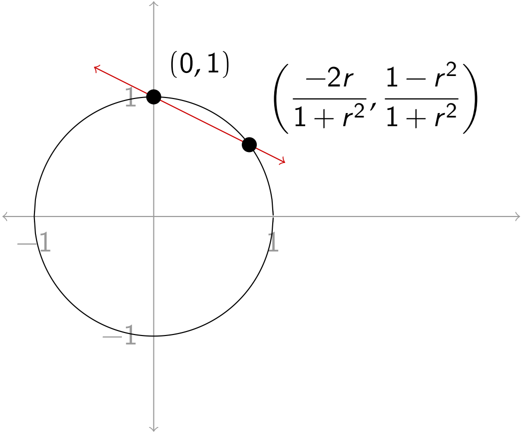
$$\begin{aligned} y &= rx + 1 \\ &= r\left(\frac{-2r}{1+r^2}\right) + 1 \\ &= \frac{-2r^2}{1+r^2} + \frac{1+r^2}{1+r^2} \end{aligned}$$

Plugging in $x = \dfrac{-2r}{1+r^2}$, we have

$$\begin{aligned} y &= rx + 1 \\ &= r\left(\frac{-2r}{1+r^2}\right) + 1 \\ &= \frac{-2r^2}{1+r^2} + \frac{1+r^2}{1+r^2} \\ &= \frac{1-r^2}{1+r^2} \end{aligned}$$

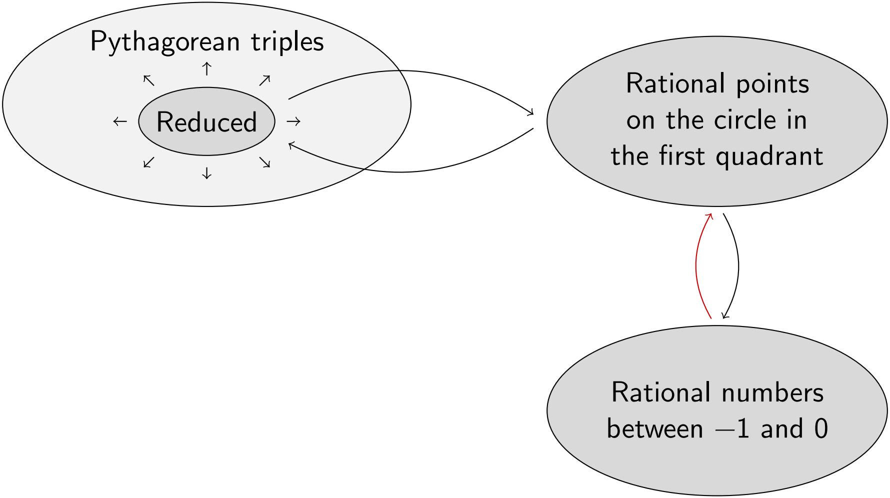


$(0, 1)$
$\left(\frac{-2r}{1+r^2}, \frac{1-r^2}{1+r^2}\right)$
1
-1
1
-1



Since r is rational, the second point of intersection is too!

What we've discovered!



Listing the rational numbers

We can systematically list off the rational numbers between -1 and 0 as follows:

$$-\frac{1}{2}$$

Listing the rational numbers

We can systematically list off the rational numbers between -1 and 0 as follows:

$$-\frac{1}{2} \quad -\frac{1}{3}$$

Listing the rational numbers

We can systematically list off the rational numbers between -1 and 0 as follows:

$$-\frac{1}{2} \quad -\frac{1}{3} \quad -\frac{2}{3}$$

Listing the rational numbers

We can systematically list off the rational numbers between -1 and 0 as follows:

$$-\frac{1}{2} \quad -\frac{1}{3} \quad -\frac{2}{3} \quad -\frac{1}{4}$$

Listing the rational numbers

We can systematically list off the rational numbers between -1 and 0 as follows:

$$-\frac{1}{2} \quad -\frac{1}{3} \quad -\frac{2}{3} \quad -\frac{1}{4} \quad \cancel{-\frac{2}{4}}$$

Listing the rational numbers

We can systematically list off the rational numbers between -1 and 0 as follows:

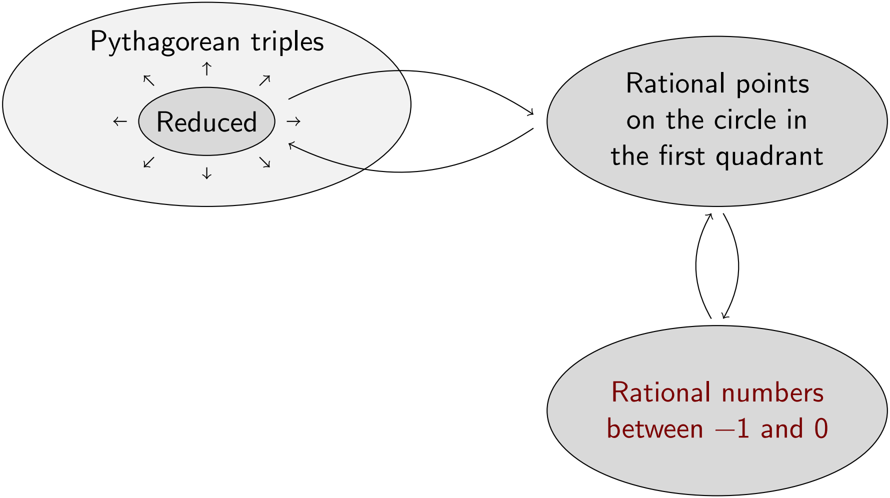
$$-\frac{1}{2} \quad -\frac{1}{3} \quad -\frac{2}{3} \quad -\frac{1}{4} \quad \cancel{-\frac{2}{4}} \quad -\frac{3}{4}$$

Listing the rational numbers

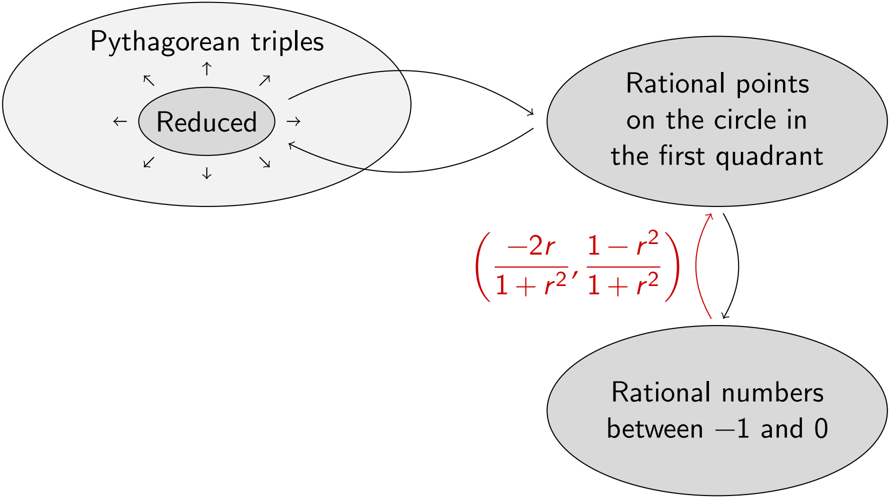
We can systematically list off the rational numbers between -1 and 0 as follows:

$$-\frac{1}{2} \quad -\frac{1}{3} \quad -\frac{2}{3} \quad -\frac{1}{4} \quad \cancel{-\frac{2}{4}} \quad -\frac{3}{4} \quad -\frac{1}{5} \quad -\frac{2}{5} \quad -\frac{3}{5} \quad \cdots$$

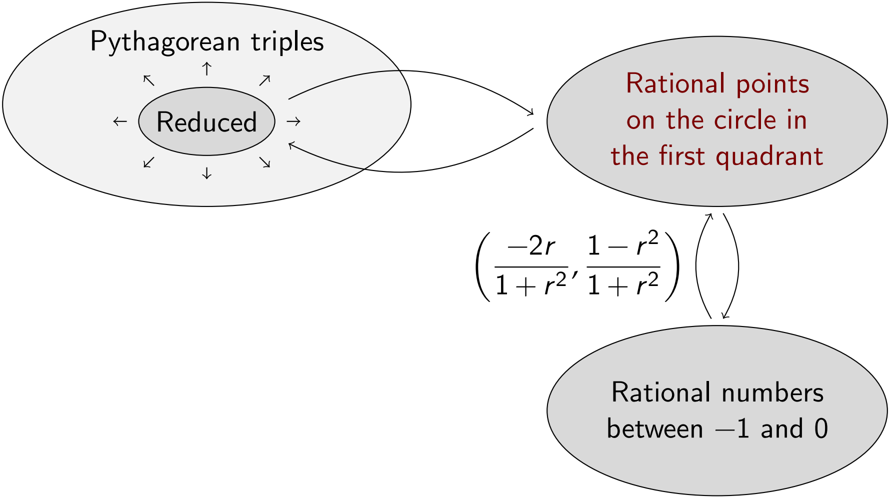
Generating the Pythagorean triples



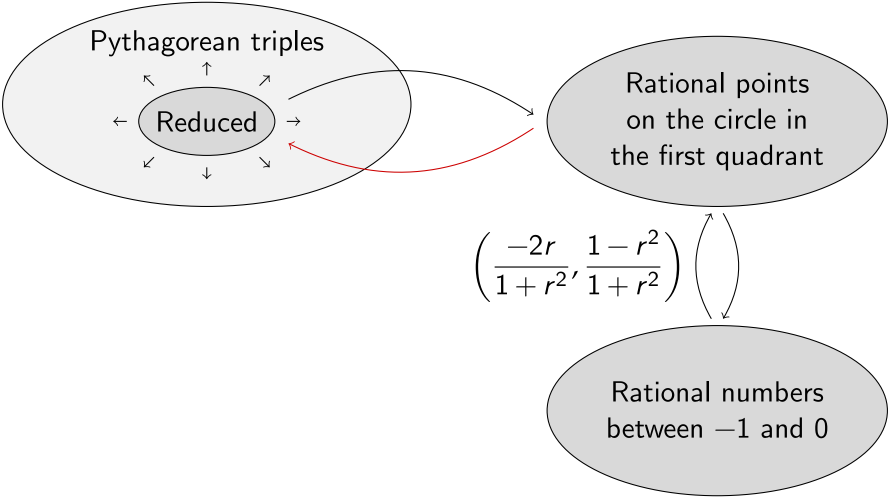
Generating the Pythagorean triples



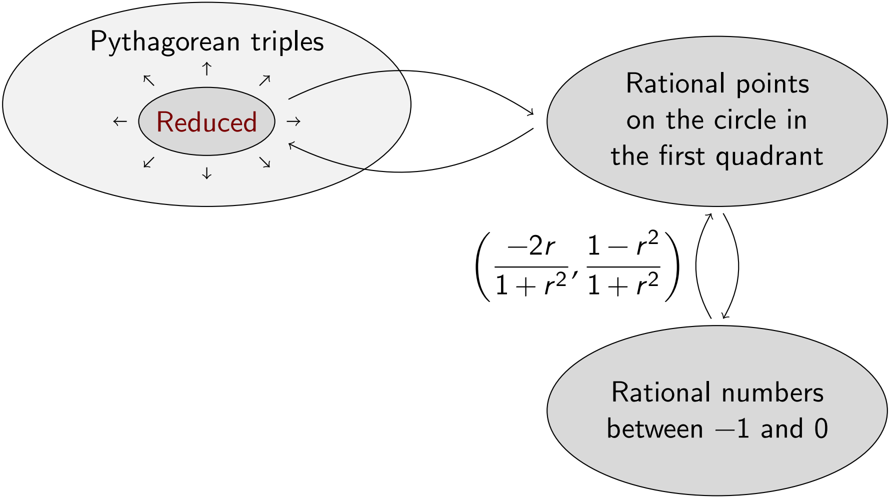
Generating the Pythagorean triples



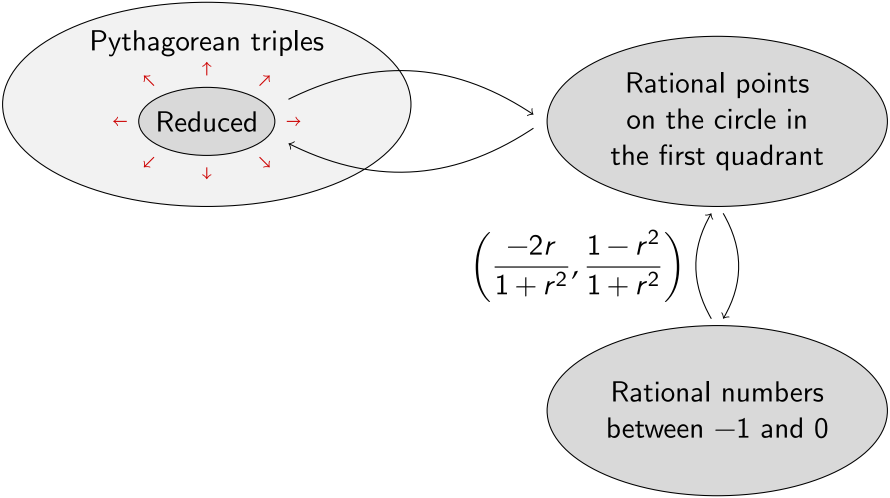
Generating the Pythagorean triples



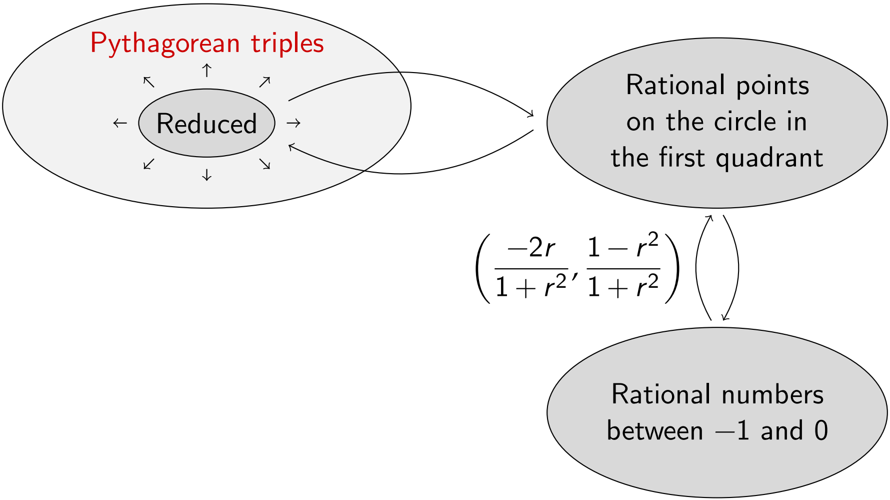
Generating the Pythagorean triples



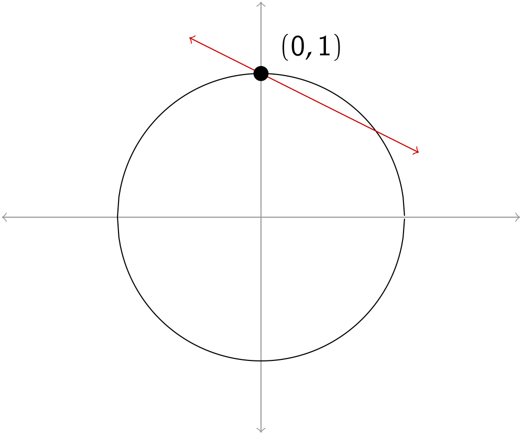
Generating the Pythagorean triples



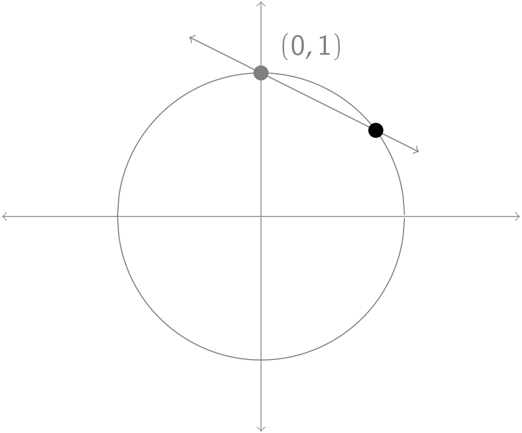
Generating the Pythagorean triples



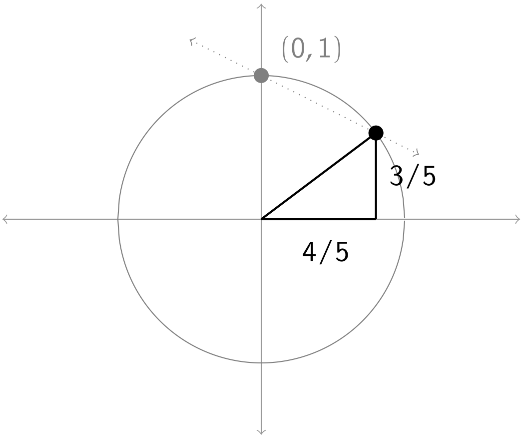
$$r = -\frac{1}{2}$$



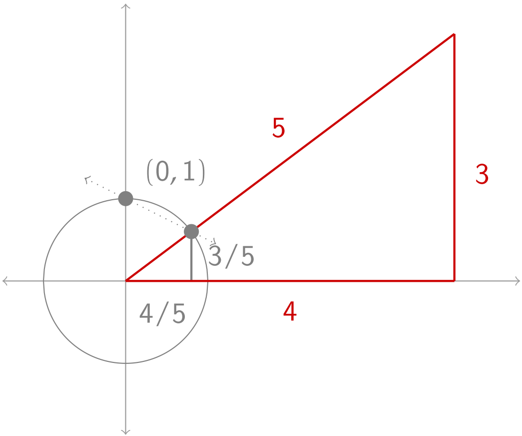
$$r = -\frac{1}{2} \quad \rightsquigarrow \quad \left(\frac{1}{5/4}, \frac{3/4}{5/4}\right)$$



$$r = -\frac{1}{2} \quad \rightsquigarrow \quad \left(\frac{1}{5/4}, \frac{3/4}{5/4}\right) \quad = \left(\frac{4}{5}, \frac{3}{5}\right)$$



$$r = -\frac{1}{2} \quad \rightsquigarrow \quad \left(\frac{1}{5/4}, \frac{3/4}{5/4}\right) = \left(\frac{4}{5}, \frac{3}{5}\right) \quad \rightsquigarrow \quad (4, 3, 5)$$



Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$				

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$		

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$
$-2/3$				

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$
$-2/3$	$\rightsquigarrow$	$(12/13, 5/13)$	$\rightsquigarrow$	$(12, 5, 13)$

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$
$-2/3$	$\rightsquigarrow$	$(12/13, 5/13)$	$\rightsquigarrow$	$(12, 5, 13)$
$-1/4$				

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$
$-2/3$	$\rightsquigarrow$	$(12/13, 5/13)$	$\rightsquigarrow$	$(12, 5, 13)$
$-1/4$	$\rightsquigarrow$	$(8/17, 15/17)$	$\rightsquigarrow$	$(8, 15, 17)$

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$
$-2/3$	$\rightsquigarrow$	$(12/13, 5/13)$	$\rightsquigarrow$	$(12, 5, 13)$
$-1/4$	$\rightsquigarrow$	$(8/17, 15/17)$	$\rightsquigarrow$	$(8, 15, 17)$
$-2/4$				

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$
$-2/3$	$\rightsquigarrow$	$(12/13, 5/13)$	$\rightsquigarrow$	$(12, 5, 13)$
$-1/4$	$\rightsquigarrow$	$(8/17, 15/17)$	$\rightsquigarrow$	$(8, 15, 17)$
$\cancel{-2/4}$				

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\rightsquigarrow$	$(4/5, 3/5)$	$\rightsquigarrow$	$(4, 3, 5)$
$-1/3$	$\rightsquigarrow$	$(3/5, 4/5)$	$\rightsquigarrow$	$(3, 4, 5)$
$-2/3$	$\rightsquigarrow$	$(12/13, 5/13)$	$\rightsquigarrow$	$(12, 5, 13)$
$-1/4$	$\rightsquigarrow$	$(8/17, 15/17)$	$\rightsquigarrow$	$(8, 15, 17)$
$\cancel{-2/4}$				
$-3/4$	$\rightsquigarrow$	$(24/25, 7/25)$	$\rightsquigarrow$	$(24, 7, 25)$

Rational Slope		Rational Point		Reduced Triple
$-1/2$	$\leadsto$	$(4/5, 3/5)$	$\leadsto$	$(4, 3, 5)$
$-1/3$	$\leadsto$	$(3/5, 4/5)$	$\leadsto$	$(3, 4, 5)$
$-2/3$	$\leadsto$	$(12/13, 5/13)$	$\leadsto$	$(12, 5, 13)$
$-1/4$	$\leadsto$	$(8/17, 15/17)$	$\leadsto$	$(8, 15, 17)$
$\cancel{-2/4}$				
$-3/4$	$\leadsto$	$(24/25, 7/25)$	$\leadsto$	$(24, 7, 25)$
$\vdots$		$\vdots$		$\vdots$

We probably could have found those ones just messing around on a calculator, but we can also use this method to generate enormous Pythagorean triples.

We probably could have found those ones just messing around on a calculator, but we can also use this method to generate enormous Pythagorean triples.

For example, starting with $r = -13711/31161$ (which is a rational number between -1 and 0),

We probably could have found those ones just messing around on a calculator, but we can also use this method to generate enormous Pythagorean triples.

For example, starting with $r = -13711/31161$ (which is a rational number between -1 and 0), we get the Pythagorean triple

$$(472\,248\,471, 391\,508\,200, 579\,499\,721)$$

which you might not have known about.

Food for thought

When I wanted to find a really big Pythagorean triple, I chose the really crazy-looking fraction $r = -13711/31161$ instead of something like $r = -5/6$. Why might crazy-looking fractions give us big Pythagorean triples?

Outline

1. Pythagorean triples
2. The Hardy-Ramanujan number
3. Fermat's last theorem
4. What is arithmetic geometry?

Hardy and Ramanujan

Around 1919, G. H. Hardy visited Srinivas Ramanujan when he was sick. Hardy mentioned that he had ridden in taxicab number 1729 on his way over, and that he thought it was "rather a dull number."

Hardy and Ramanujan

Around 1919, G. H. Hardy visited Srinivas Ramanujan when he was sick. Hardy mentioned that he had ridden in taxicab number 1729 on his way over, and that he thought it was "rather a dull number."

Ramanujan immediately responded, "No, Hardy! It is a very interesting number. It is the smallest number expressible as the sum of two cubes in two different ways."

Hardy and Ramanujan

Around 1919, G. H. Hardy visited Srinivas Ramanujan when he was sick. Hardy mentioned that he had ridden in taxicab number 1729 on his way over, and that he thought it was “rather a dull number.”

Ramanujan immediately responded, “No, Hardy! It is a very interesting number. It is the smallest number expressible as the sum of two cubes in two different ways.”

And indeed, $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

1729 as a sum of cubes

Ramanujan was talking about writing 1729 as the sum of cubes of two positive integers.

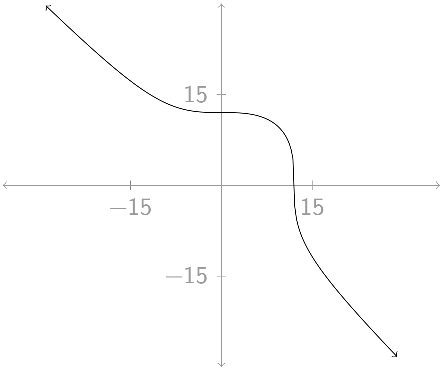
1729 as a sum of cubes

Ramanujan was talking about writing 1729 as the sum of cubes of two positive integers.

Let's think about the related problem of writing 1729 as the sum of cubes of two *rational* numbers.

In other words, we want to think about rational points on the *elliptic curve*

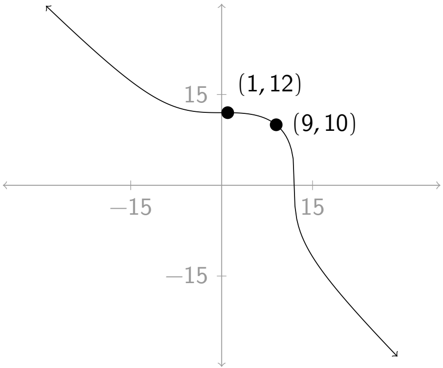
$$x^3 + y^3 = 1729.$$



In other words, we want to think about rational points on the *elliptic curve*

$$x^3 + y^3 = 1729.$$

Ramanujan gave us two rational points on this elliptic curve.

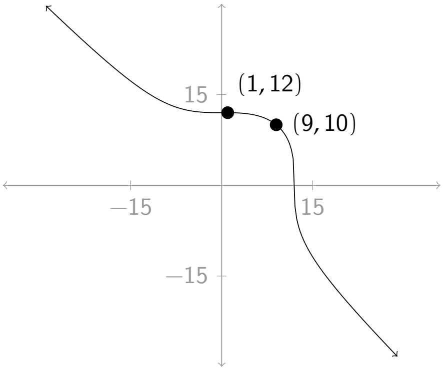


In other words, we want to think about rational points on the *elliptic curve*

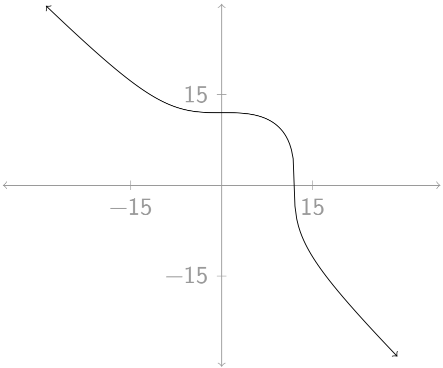
$$x^3 + y^3 = 1729.$$

Ramanujan gave us two rational points on this elliptic curve.

Is there a systematic way of producing all of the rational points?

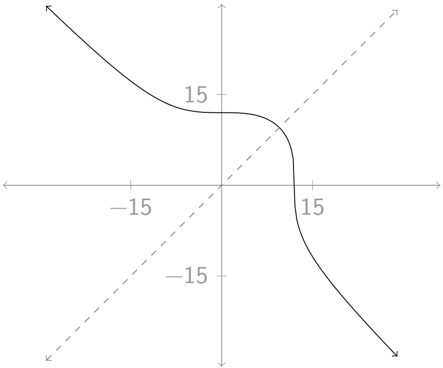


We have one really easy way of finding new rational points.



We have one really easy way of finding new rational points.

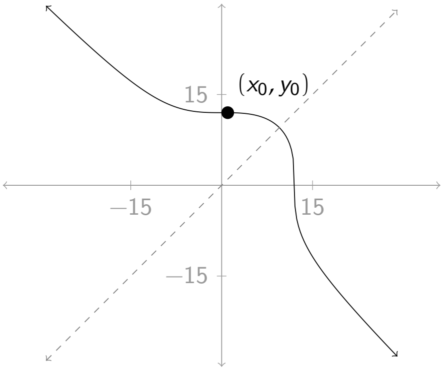
Our curve is symmetric about $y = x$.



We have one really easy way of finding new rational points.

Our curve is symmetric about $y = x$.

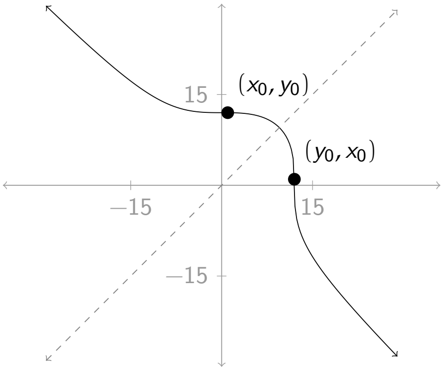
So, if $P = (x_0, y_0)$ is a rational point,



We have one really easy way of finding new rational points.

Our curve is symmetric about $y = x$.

So, if $P = (x_0, y_0)$ is a rational point, so is its reflection across this line.

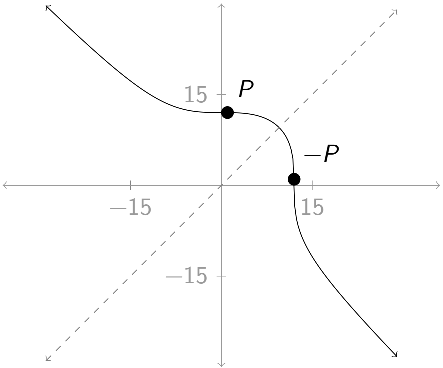


We have one really easy way of finding new rational points.

Our curve is symmetric about $y = x$.

So, if $P = (x_0, y_0)$ is a rational point, so is its reflection across this line.

Let's call this reflected point $-P$.



However, reflecting points across $y = x$ by itself doesn't get us very far.

However, reflecting points across $y = x$ by itself doesn't get us very far.

What else could we try?

However, reflecting points across $y = x$ by itself doesn't get us very far.

What else could we try?

Previously our strategy for finding rational points was to first find one rational point and then to draw lines of rational slope through that point.

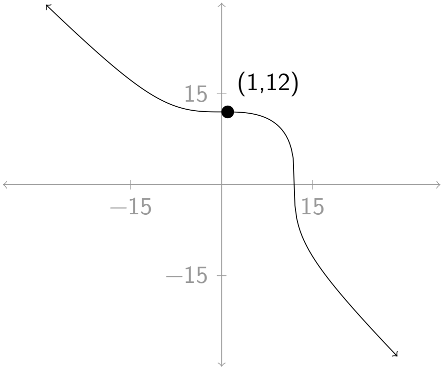
However, reflecting points across $y = x$ by itself doesn't get us very far.

What else could we try?

Previously our strategy for finding rational points was to first find one rational point and then to draw lines of rational slope through that point.

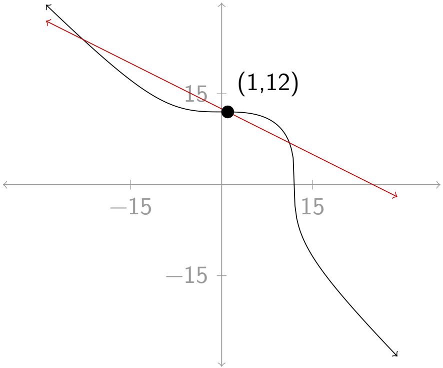
Let's try it!

Let's take the point $(1, 12)$...



Let's take the point $(1, 12)$...

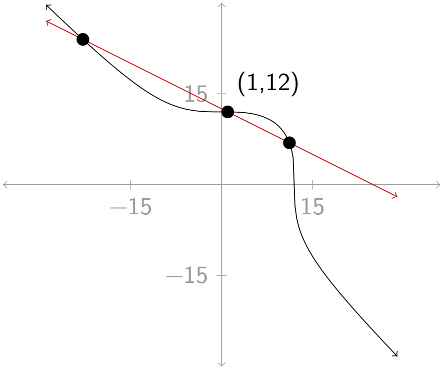
... and draw the line of slope $-1/2$ through it.



Let's take the point $(1, 12)$...

... and draw the line of slope $-1/2$ through it.

It intersects the curve in *two* other points,

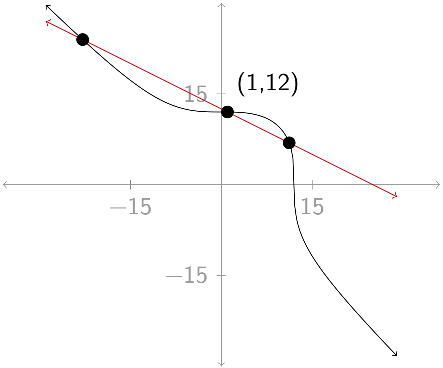


Let's take the point $(1, 12)$...

... and draw the line of slope $-1/2$ through it.

It intersects the curve in *two* other points, whose x-coordinates are

$$\frac{1}{7}\left(-41 \pm \sqrt{3558}\right),$$



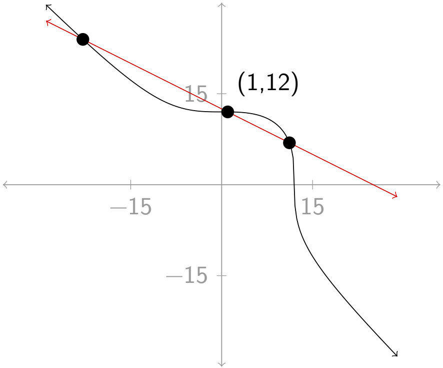
Let's take the point $(1, 12)$...

... and draw the line of slope $-1/2$ through it.

It intersects the curve in *two* other points, whose x-coordinates are

$$\frac{1}{7}\left(-41 \pm \sqrt{3558}\right),$$

and these are *not* rational numbers.



Let's take the point $(1, 12)$...

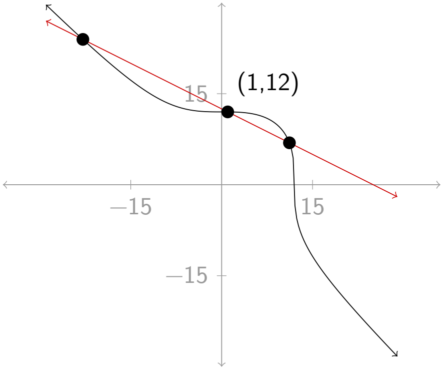
... and draw the line of slope $-1/2$ through it.

It intersects the curve in *two* other points, whose x-coordinates are

$$\frac{1}{7}\left(-41 \pm \sqrt{3558}\right),$$

and these are *not* rational numbers.

What went wrong?



The line with rational slope r through the point $(1, 12)$ has equation

$$y = r(x - 1) + 12.$$

The line with rational slope r through the point $(1, 12)$ has equation

$$y = r(x - 1) + 12.$$

We substitute this into $x^3 + y^3 = 1729$ to get

$$x^3 + (r(x - 1) + 12)^3 = 1729.$$

The line with rational slope r through the point $(1, 12)$ has equation

$$y = r(x - 1) + 12.$$

We substitute this into $x^3 + y^3 = 1729$ to get

$$x^3 + (r(x - 1) + 12)^3 = 1729.$$

Notice that...

The line with rational slope r through the point $(1, 12)$ has equation

$$y = r(x-1) + 12.$$

We substitute this into $x^3 + y^3 = 1729$ to get

$$x^3 + (r(x-1) + 12)^3 = 1729.$$

Notice that...

- this equation is (usually) cubic, so it (usually) has 3 roots, and

The line with rational slope r through the point $(1, 12)$ has equation

$$y = r(x - 1) + 12.$$

We substitute this into $x^3 + y^3 = 1729$ to get

$$x^3 + (r(x - 1) + 12)^3 = 1729.$$

Notice that...

- this equation is (usually) cubic, so it (usually) has 3 roots, and
- it has rational coefficients,

The line with rational slope r through the point $(1, 12)$ has equation

$$y = r(x - 1) + 12.$$

We substitute this into $x^3 + y^3 = 1729$ to get

$$x^3 + (r(x - 1) + 12)^3 = 1729.$$

Notice that...

- this equation is (usually) cubic, so it (usually) has 3 roots, and
- it has rational coefficients,
- but we only know for sure that it has *one* rational root: namely, $x = 1$.

The line with rational slope r through the point $(1, 12)$ has equation

$$y = r(x - 1) + 12.$$

We substitute this into $x^3 + y^3 = 1729$ to get

$$x^3 + (r(x - 1) + 12)^3 = 1729.$$

Notice that...

- this equation is (usually) cubic, so it (usually) has 3 roots, and
- it has rational coefficients,
- but we only know for sure that it has *one* rational root: namely, $x = 1$.

The fact about polynomials with rational coefficients that we used earlier doesn't apply anymore.

However, if we knew that the cubic equation had *two* rational roots, then that fact *would* guarantee us another rational root.

However, if we knew that the cubic equation had *two* rational roots, then that fact *would* guarantee us another rational root.

This gives us an idea!

However, if we knew that the cubic equation had *two* rational roots, then that fact *would* guarantee us another rational root.

This gives us an idea!

Let's insist that the line through $(1, 12)$ also pass through *another* rational point on the curve.

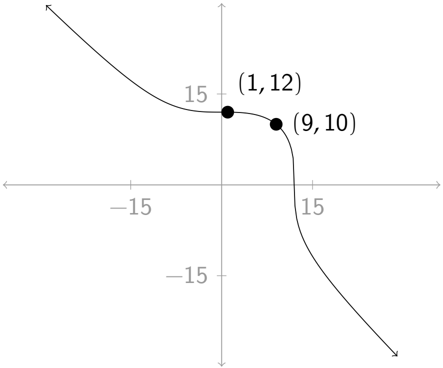
However, if we knew that the cubic equation had *two* rational roots, then that fact *would* guarantee us another rational root.

This gives us an idea!

Let's insist that the line through $(1, 12)$ also pass through *another* rational point on the curve.

Thankfully, Ramanujan gave us another point: namely, $(9, 10)$.

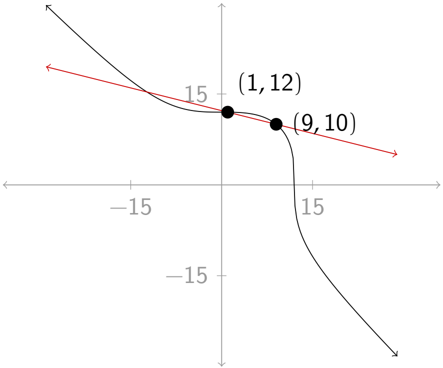
We have the two rational points $(1, 12)$ and $(9, 10)$.



We have the two rational points $(1, 12)$ and $(9, 10)$.

Draw the line that passes through them:

$$y = \frac{-x}{4} + \frac{49}{4}.$$

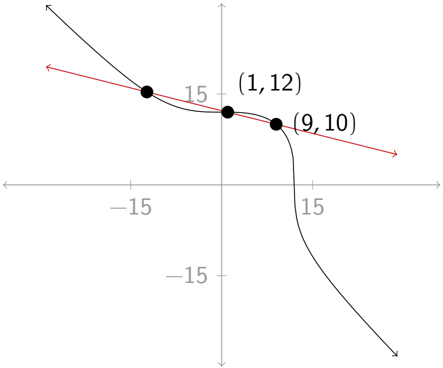


We have the two rational points $(1, 12)$ and $(9, 10)$.

Draw the line that passes through them:

$$y = \frac{-x}{4} + \frac{49}{4}.$$

It intersects the curve in another point,



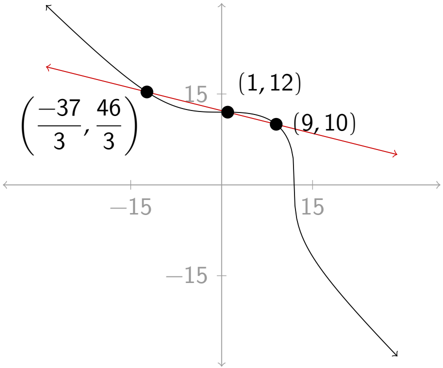
We have the two rational points $(1, 12)$ and $(9, 10)$.

Draw the line that passes through them:

$$y = \frac{-x}{4} + \frac{49}{4}.$$

It intersects the curve in another point, whose coordinates are

$$\left(\frac{-37}{3}, \frac{46}{3}\right).$$



We have the two rational points $(1, 12)$ and $(9, 10)$.

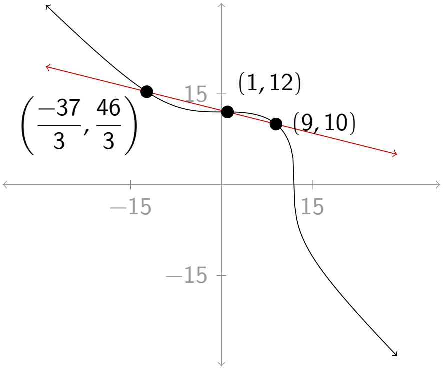
Draw the line that passes through them:

$$y = \frac{-x}{4} + \frac{49}{4}.$$

It intersects the curve in another point, whose coordinates are

$$\left(\frac{-37}{3}, \frac{46}{3}\right).$$

This is a rational point!



So we've discovered another way of writing 1729 as a sum of two rational cubes:

$$\left(\frac{-37}{3}\right)^3 + \left(\frac{46}{3}\right)^3 = 1729.$$

Drawing secants

We can generalize what we've observed.

Drawing secants

We can generalize what we've observed.

Given two different rational points P and Q on the curve $x^3 + y^3 = 1729$,

Drawing secants

We can generalize what we've observed.

Given two different rational points P and Q on the curve $x^3 + y^3 = 1729$, the line that goes through them will (usually) intersect the curve in another point, and this point must be rational.

Drawing secants

We can generalize what we've observed.

Given two different rational points P and Q on the curve $x^3 + y^3 = 1729$, the line that goes through them will (usually) intersect the curve in another point, and this point must be rational.

Our argument that the third point of intersection must be rational was kind of abstract, but it is possible to write down its coordinates explicitly in terms of the coordinates of P and Q. Try it at home!

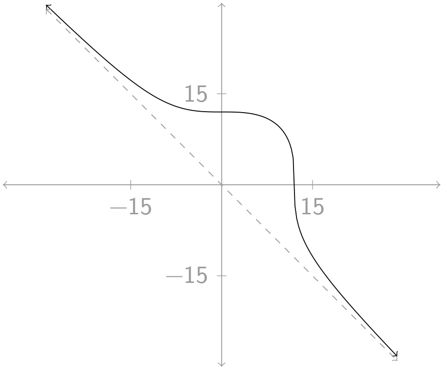
Snag

Why the “usually”?

Snag

Why the "usually"?

Notice that that $y = -x$ is a slant asymptote for the curve.

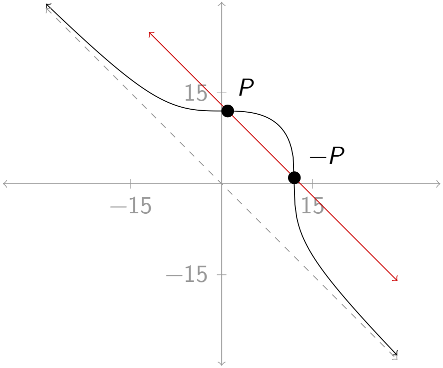


Snag

Why the "usually"?

Notice that that $y = -x$ is a slant asymptote for the curve.

When we draw the line through P and $-P$, it has slope -1, so it and the curve are asymptotically parallel.



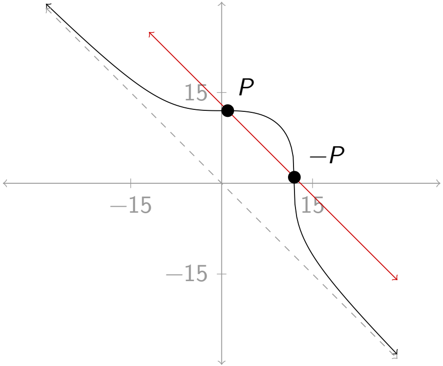
Snag

Why the “usually”?

Notice that that $y = -x$ is a slant asymptote for the curve.

When we draw the line through P and $-P$, it has slope -1, so it and the curve are asymptotically parallel.

So there is no third point of intersection!



Fiat O!

We "solve" this problem by conjuring up a new rational point on the curve, called "the point at infinity" and denoted O.

Fiat O!

We "solve" this problem by conjuring up a new rational point on the curve, called "the point at infinity" and denoted O.

We declare O to be a point of intersection of our curve with any line that is asymptotically parallel to it (that is, has slope -1).

Fiat O!

We “solve” this problem by conjuring up a new rational point on the curve, called “the point at infinity” and denoted O.

We declare O to be a point of intersection of our curve with any line that is asymptotically parallel to it (that is, has slope -1).

Now every line passing through two distinct rational points P and Q on the curve intersects the curve in a third rational point.

Fiat O!

We “solve” this problem by conjuring up a new rational point on the curve, called “the point at infinity” and denoted O.

We declare O to be a point of intersection of our curve with any line that is asymptotically parallel to it (that is, has slope -1).

Now every line passing through two distinct rational points P and Q on the curve intersects the curve in a third rational point.

Problem “solved”!

Wait, what...?

I thought parallel lines never intersected!

Wait, what...?

I thought parallel lines never intersected!

These railroad tracks are parallel and they never *actually* intersect, but it *looks* like they meet up at a point off “at infinity” on the horizon.

Wait, what...?

I thought parallel lines never intersected!

These railroad tracks are parallel and they never *actually* intersect, but it *looks* like they meet up at a point off "at infinity" on the horizon.

This idea is the starting point for *projective geometry*.

“Adding” points

Addition of numbers is a nice way of taking two numbers and producing a third number.

"Adding" points

Addition of numbers is a nice way of taking two numbers and producing a third number.

We can define a similar "addition" on the set of rational points of our elliptic curve (including the point at infinity O).

“Adding” points

Addition of numbers is a nice way of taking two numbers and producing a third number.

We can define a similar “addition” on the set of rational points of our elliptic curve (including the point at infinity O).

We’ll call this set E.

“Adding” points

Addition of numbers is a nice way of taking two numbers and producing a third number.

We can define a similar “addition” on the set of rational points of our elliptic curve (including the point at infinity O).

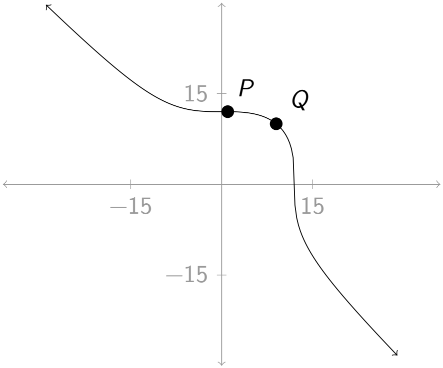
We’ll call this set E.

For the experts...

We are going to turn E into an abelian group with identity element O.

Addition on E

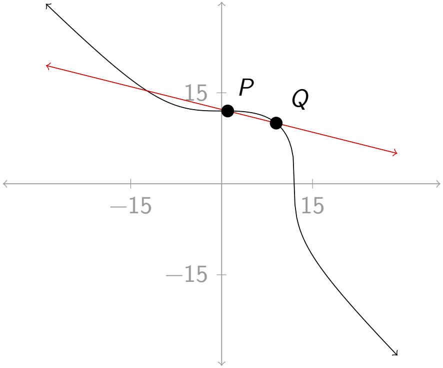
Start with any two distinct points P and Q.



Addition on E

Start with any two distinct points P and Q.

Consider the line passing through them.

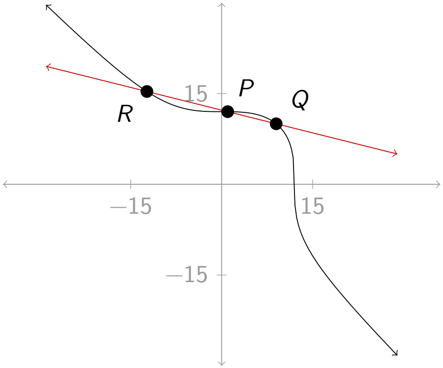


Addition on E

Start with any two distinct points P and Q.

Consider the line passing through them.

Let R be the third point at which E intersects this line.



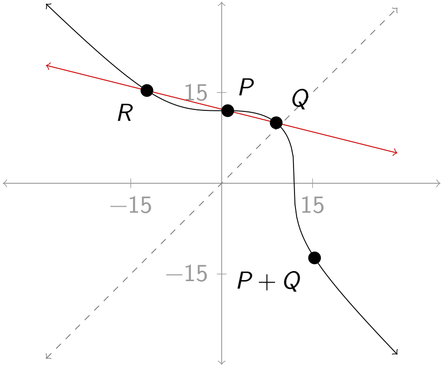
Addition on E

Start with any two distinct points P and Q.

Consider the line passing through them.

Let R be the third point at which E intersects this line.

Then define $P + Q$ to be the reflection of R across the line $y = x$.



Generating the rational points

Let's start with the two rational points $R = (1, 12)$ and $S = (9, 10)$,

Generating the rational points

Let's start with the two rational points $R = (1, 12)$ and $S = (9, 10)$, and iterate the following operations to generate more rational points on the curve $x^3 + y^3 = 1729$.

Generating the rational points

Let's start with the two rational points $R = (1, 12)$ and $S = (9, 10)$, and iterate the following operations to generate more rational points on the curve $x^3 + y^3 = 1729$.

- Take a rational point P on the curve that we've already generated, and generate $-P$.

Generating the rational points

Let's start with the two rational points $R = (1, 12)$ and $S = (9, 10)$, and iterate the following operations to generate more rational points on the curve $x^3 + y^3 = 1729$.

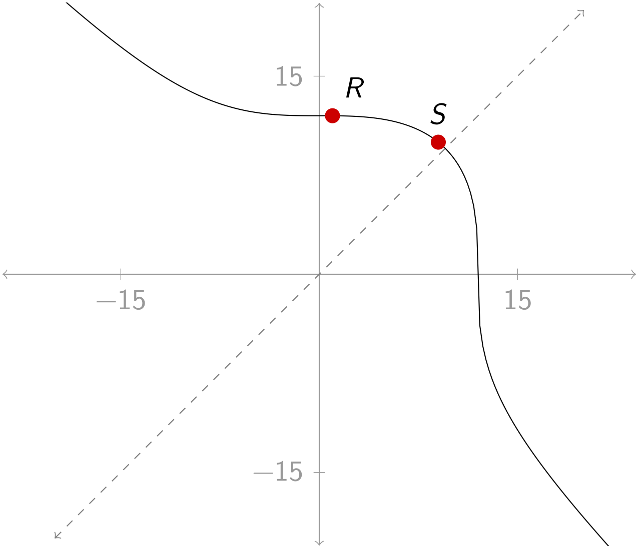
- Take a rational point P on the curve that we've already generated, and generate $-P$.
- Take two distinct rational points P and Q on the curve that we've already generated, and generate $P + Q$.

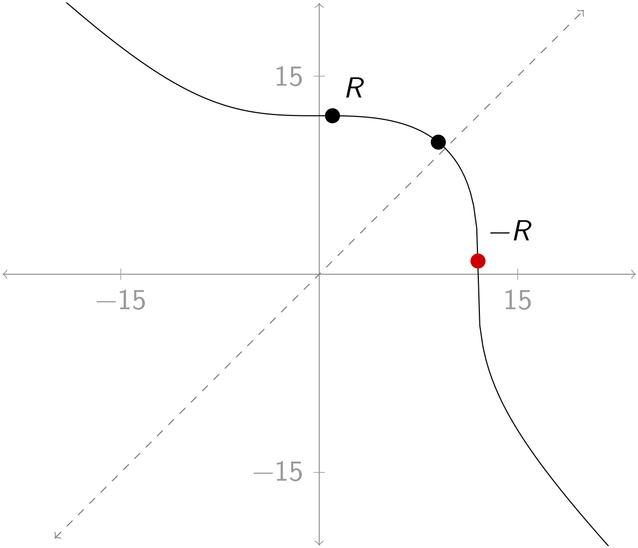
Generating the rational points

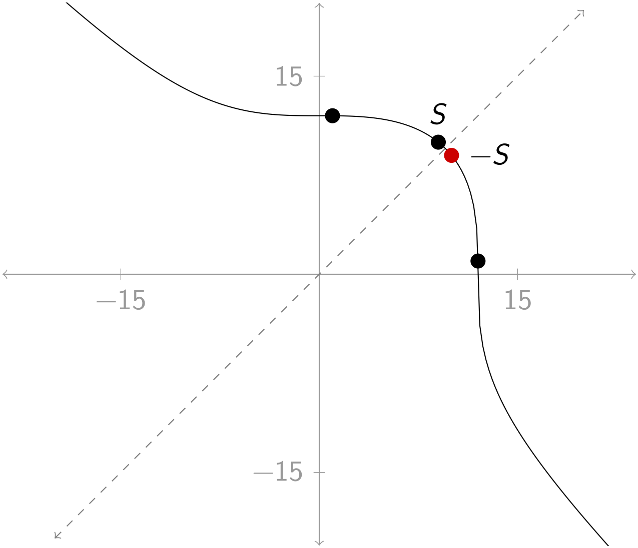
Let's start with the two rational points $R = (1, 12)$ and $S = (9, 10)$, and iterate the following operations to generate more rational points on the curve $x^3 + y^3 = 1729$.

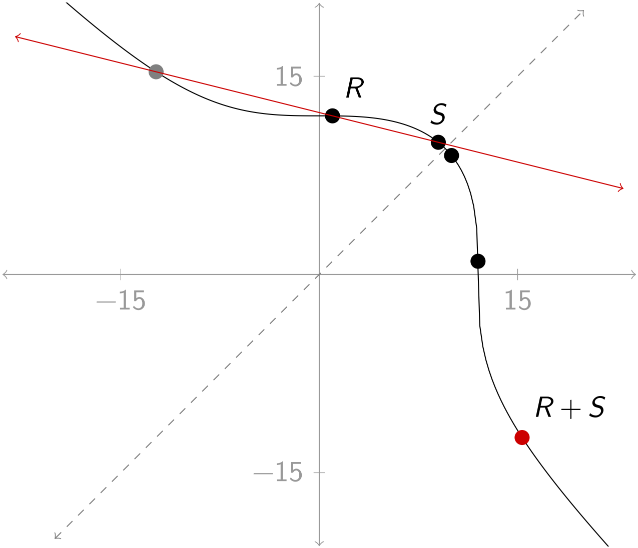
- Take a rational point P on the curve that we've already generated, and generate $-P$.
- Take two distinct rational points P and Q on the curve that we've already generated, and generate $P + Q$.

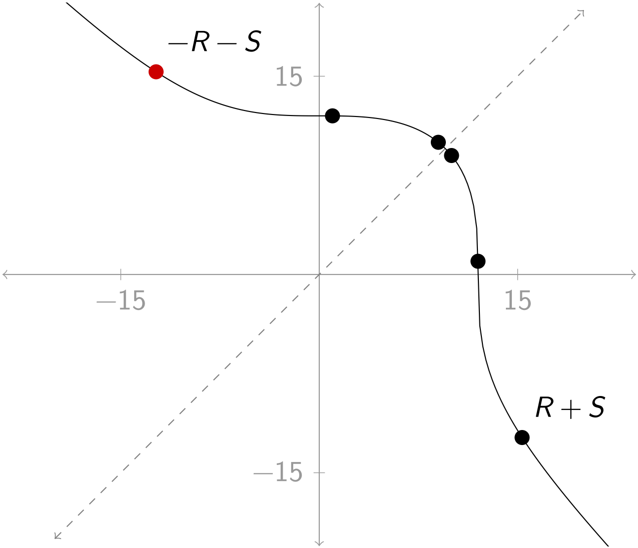
Do we generate all of the rational points on the curve this way?


15
R
S
−15
15
−15

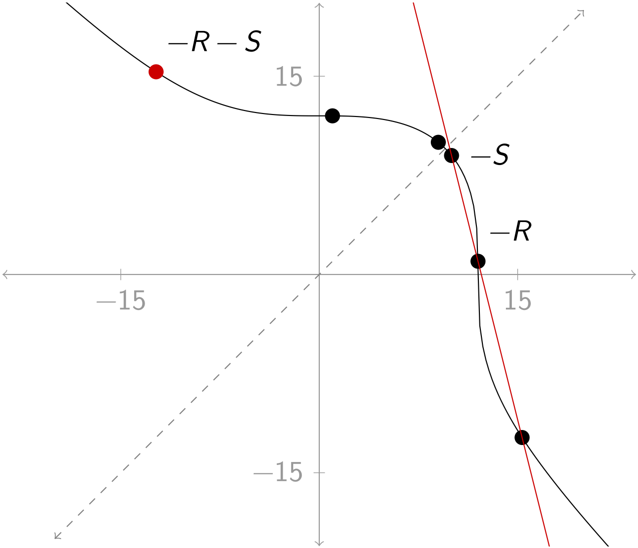

15
R
$-R$
-15
15
-15


15
−15
15
−15
S
−S

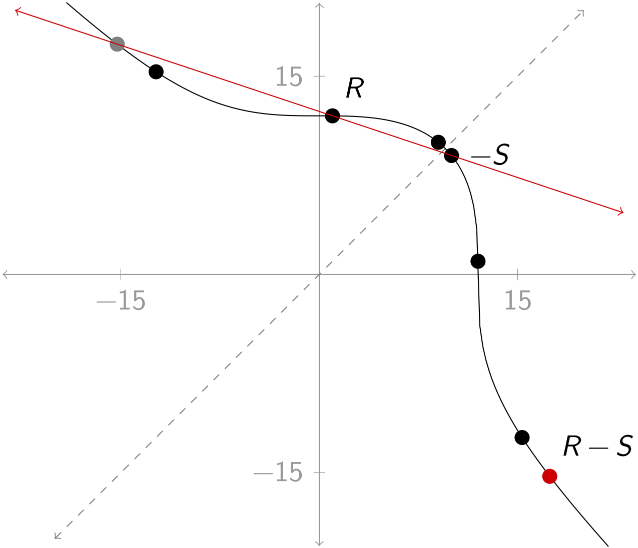

15
R
S
-15
15
$R+S$
-15

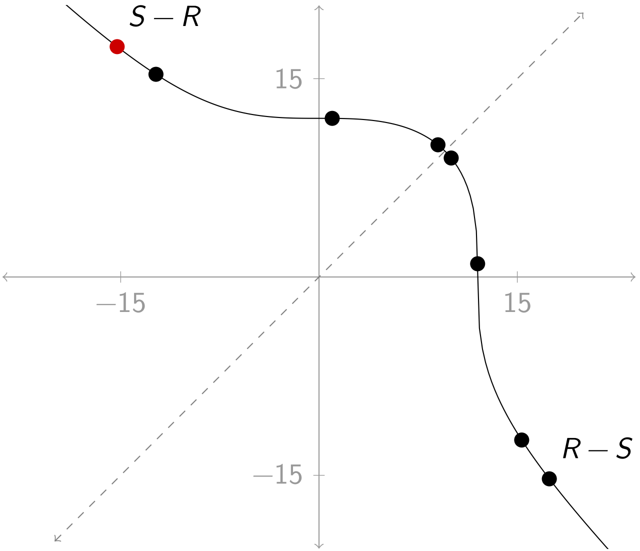


$-R-S$
15
-15
15
$R+S$
-15



$-R-S$
15
$-S$
$-R$
-15
15
-15


15
R
$-S$
-15
15
$R-S$
-15


S − R
15
−15
15
−15
R − S

Let's take a step back...

There could be (and in fact, there are) an infinite number of rational points on our elliptic curve.

Let's take a step back...

There could be (and in fact, there are) an infinite number of rational points on our elliptic curve.

Do we have any reason to think that we could generate *all* of them starting with only *two*?

Let's take a step back...

There could be (and in fact, there are) an infinite number of rational points on our elliptic curve.

Do we have any reason to think that we could generate *all* of them starting with only *two*?

A hallmark of 20th century arithmetic geometry is the *Mordell-Weil theorem*, which tells us that there is *some* finite set of rational points that will generate the rest.

Let's take a step back...

There could be (and in fact, there are) an infinite number of rational points on our elliptic curve.

Do we have any reason to think that we could generate *all* of them starting with only *two*?

A hallmark of 20th century arithmetic geometry is the *Mordell-Weil theorem*, which tells us that there is *some* finite set of rational points that will generate the rest.

For the experts...

The Mordell-Weil theorem says that E is a *finitely generated* abelian group.

But how many points?

But we still don't know that *two* points is enough. Maybe we would need a trillion points to get the job done...

But how many points?

But we still don't know that *two* points is enough. Maybe we would need a trillion points to get the job done...

Using some advanced techniques, we can prove that two points is enough.

But how many points?

But we still don't know that *two* points is enough. Maybe we would need a trillion points to get the job done...

Using some advanced techniques, we can prove that two points is enough.

For the experts...

- By "reducing modulo various primes," we learn that E is torsion-free.

But how many points?

But we still don't know that *two* points is enough. Maybe we would need a trillion points to get the job done...

Using some advanced techniques, we can prove that two points is enough.

For the experts...

- By "reducing modulo various primes," we learn that E is torsion-free.
- By using "3-descent," we learn that E has rank at most 2.

Do Ramanujan's points work?

So we've learned that *some* pair of points can in fact generate all of the others, but not just any pair will do.

Do Ramanujan's points work?

So we've learned that *some* pair of points can in fact generate all of the others, but not just any pair will do.

Do Ramanujan's points R and S actually generate all of the others?

Do Ramanujan's points work?

So we've learned that *some* pair of points can in fact generate all of the others, but not just any pair will do.

Do Ramanujan's points R and S actually generate all of the others?

In general, finding rational points that generate all the rest is very difficult.

Do Ramanujan's points work?

So we've learned that *some* pair of points can in fact generate all of the others, but not just any pair will do.

Do Ramanujan's points R and S actually generate all of the others?

In general, finding rational points that generate all the rest is very difficult.

Fortunately, we have computers!

`mwrank`

J. E. Cremona has written a package called `mwrank` for the mathematical programming language Sage which can *sometimes* find rational points that *provably* generate the other rational points on an elliptic curve.

`mwrank`

J. E. Cremona has written a package called `mwrank` for the mathematical programming language Sage which can *sometimes* find rational points that *provably* generate the other rational points on an elliptic curve.

When we ask `mwrank` to find generators for E, it returns Ramanujan's points $R = (1, 12)$ and $S = (9, 10)$. Just as important, `mwrank` returns a guarantee that these points are *provably* generators.

`mwrank`

J. E. Cremona has written a package called `mwrank` for the mathematical programming language Sage which can *sometimes* find rational points that *provably* generate the other rational points on an elliptic curve.

When we ask `mwrank` to find generators for E, it returns Ramanujan's points $R = (1, 12)$ and $S = (9, 10)$. Just as important, `mwrank` returns a guarantee that these points are *provably* generators.

Ramanujan's points *do* generate all of the others!

Food for thought

- We defined $P+Q$ when P and Q are different. What should $P+P$ be? (Hint: $P+P=(P+Q)+(P-Q)$.)

Food for thought

- We defined $P+Q$ when P and Q are different. What should $P+P$ be? (Hint: $P+P=(P+Q)+(P-Q)$.)
- Once you've worked out the answer to the previous question, explain why there is no $P \in E$ such that $P+P=O$.

Outline

1. Pythagorean triples
2. The Hardy-Ramanujan number
3. Fermat's last theorem
4. What is arithmetic geometry?

Fermat's last theorem

In 1637, Pierre de Fermat wrote in the margin of a copy of Diophantus' *Arithmetica* that there were no nonzero integer solutions to the equation

$$a^n + b^n = c^n$$

for any exponent $n \geq 3$.

Fermat's last theorem

In 1637, Pierre de Fermat wrote in the margin of a copy of Diophantus' *Arithmetica* that there were no nonzero integer solutions to the equation

$$a^n + b^n = c^n$$

for any exponent $n \geq 3$.

He claimed, "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

Fermat's last theorem

In 1637, Pierre de Fermat wrote in the margin of a copy of Diophantus' *Arithmetica* that there were no nonzero integer solutions to the equation

$$a^n + b^n = c^n$$

for any exponent $n \geq 3$.

He claimed, "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

No proof by Fermat has ever been found.

Fermat's last theorem

In 1637, Pierre de Fermat wrote in the margin of a copy of Diophantus' *Arithmetica* that there were no nonzero integer solutions to the equation

$$a^n + b^n = c^n$$

for any exponent $n \geq 3$.

He claimed, "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

No proof by Fermat has ever been found.

He did, however, prove this for the exponent $n = 4$.

Let's make this easier...

One way that mathematicians approach problems is by proving that they can get away with solving a smaller problem.

Let's make this easier...

One way that mathematicians approach problems is by proving that they can get away with solving a smaller problem.

Reduction

If there is a counterexample to Fermat's last theorem for any exponent, then there must be a counterexample for some *prime* exponent.

Let's make this easier...

One way that mathematicians approach problems is by proving that they can get away with solving a smaller problem.

Reduction

If there is a counterexample to Fermat's last theorem for any exponent, then there must be a counterexample for some *prime* exponent.

Let's see why!

Suppose that we have a counterexample (a, b, c) to Fermat's last theorem for some exponent $n \geq 3$.

Suppose that we have a counterexample (a, b, c) to Fermat's last theorem for some exponent $n \geq 3$. In other words, we have

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

Suppose that we have a counterexample (a, b, c) to Fermat's last theorem for some exponent $n \geq 3$. In other words, we have

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

Let's write $n = mp$ where p is the *largest* prime dividing n.

Suppose that we have a counterexample (a, b, c) to Fermat's last theorem for some exponent $n \geq 3$. In other words, we have

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

Let's write $n = mp$ where p is the *largest* prime dividing n.

Let's first think about what happens when $p \neq 2$.

Suppose that we have a counterexample (a, b, c) to Fermat's last theorem for some exponent $n \geq 3$. In other words, we have

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

Let's write $n = mp$ where p is the *largest* prime dividing n.

Let's first think about what happens when $p \neq 2$. We can rewrite our equation as

$$(a^m)^p + (b^m)^p = (c^m)^p.$$

Suppose that we have a counterexample (a, b, c) to Fermat's last theorem for some exponent $n \geq 3$. In other words, we have

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

Let's write $n = mp$ where p is the *largest* prime dividing n.

Let's first think about what happens when $p \neq 2$. We can rewrite our equation as

$$(a^m)^p + (b^m)^p = (c^m)^p.$$

This gives us a counterexample (a^m, b^m, c^m) to Fermat's last theorem with prime exponent p.

What about $p = 2$?

The case $p = 2$ is a just slightly trickier.

What about $p = 2$?

The case $p = 2$ is a just slightly trickier.

Remember that we saw that $a^2 + b^2 = c^2$ has infinitely many solutions.

What about $p = 2$?

The case $p = 2$ is a just slightly trickier.

Remember that we saw that $a^2 + b^2 = c^2$ has infinitely many solutions.

I'll let you think about how to deal with this case. (Hint: Remember that Fermat proved the case $n = 4$.)

Century of stagnation

For over a hundred years after Fermat's death in 1665, there was no definitive progress on Fermat's last theorem.

Century of stagnation

For over a hundred years after Fermat's death in 1665, there was no definitive progress on Fermat's last theorem.

Then, in 1770, Leonhard Euler published a proof of Fermat's last theorem with exponent $p = 3$.

Legendre and Dirichlet

Half a century later, in 1825, Adrien-Marie Legendre and Johann Peter Gustav Lejeune Dirichlet independently published proofs for $p = 5$.

Lamé

In 1839, Gabriel Lamé proved the case $p = 7$.

Lamé

In 1839, Gabriel Lamé proved the case $p = 7$.

Around 1850, he announced that he had a proof for arbitrary primes $p \geq 3$.

Lamé

In 1839, Gabriel Lamé proved the case $p = 7$.

Around 1850, he announced that he had a proof for arbitrary primes $p \geq 3$.

But his proof was incorrect.

Lamé

In 1839, Gabriel Lamé proved the case $p = 7$.

Around 1850, he announced that he had a proof for arbitrary primes $p \geq 3$.

But his proof was incorrect.

Lamé was not the only one: over the centuries, thousands of incorrect proofs of Fermat's last theorem have been proposed.

Kummer and the regular primes

Soon after Lamé's incorrect proof, Ernst Kummer adapted Lamé's strategy to give a correct proof for all *regular* primes.

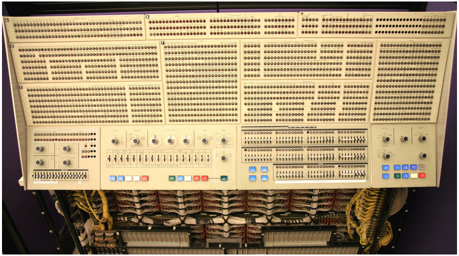
Kummer and the regular primes

Soon after Lamé's incorrect proof, Ernst Kummer adapted Lamé's strategy to give a correct proof for all *regular* primes.

Most primes are regular: the smallest few irregular primes are

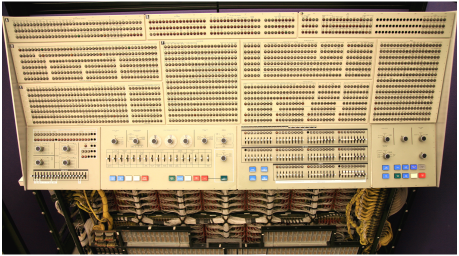
$$37, 59, 67, 101, 103, 131, \ldots .$$

Computational studies



In the latter half of the 1900s, computational methods were used to verify Fermat's last theorem for larger and larger irregular primes.

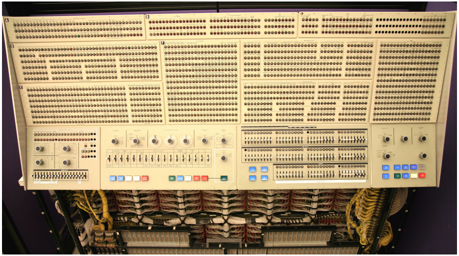
Computational studies



In the latter half of the 1900s, computational methods were used to verify Fermat's last theorem for larger and larger irregular primes.

- By 1954, it had been verified for all primes up to 2521...

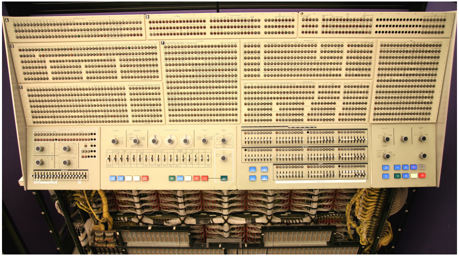
Computational studies



In the latter half of the 1900s, computational methods were used to verify Fermat's last theorem for larger and larger irregular primes.

- By 1954, it had been verified for all primes up to 2521...
- By 1978, all primes up to 124 991...

Computational studies



In the latter half of the 1900s, computational methods were used to verify Fermat's last theorem for larger and larger irregular primes.

- By 1954, it had been verified for all primes up to 2521...
- By 1978, all primes up to 124 991...
- And by 1993, all primes up to 4 000 000.

Enter arithmetic geometry.

Serre and Ribet

In 1985-86, Jean-Pierre Serre and Ken Ribet proved that, if (a, b, c) were a counterexample to Fermat's last theorem for some prime exponent $p \geq 5$, the elliptic curve

$$y^2 = x(x - a^p)(x + b^p)$$

would have some *very* strange properties...

Serre and Ribet

In 1985-86, Jean-Pierre Serre and Ken Ribet proved that, if (a, b, c) were a counterexample to Fermat's last theorem for some prime exponent $p \geq 5$, the elliptic curve

$$y^2 = x(x - a^p)(x + b^p)$$

would have some *very* strange properties...

Properties so strange, in fact, that it had been conjectured a few decades earlier that no elliptic curve could have those properties!

Wiles

In 1995, Andrew Wiles proved that the elliptic curve

$$y^2 = x(x - a^p)(y + b^p)$$

was not as strange as it would have to be for (a, b, c) to be a counterexample to Fermat's last theorem with prime exponent $p \geq 5$.

Wiles

In 1995, Andrew Wiles proved that the elliptic curve

$$y^2 = x(x - a^p)(y + b^p)$$

was not as strange as it would have to be for (a, b, c) to be a counterexample to Fermat's last theorem with prime exponent $p \geq 5$.

This completed the proof of Fermat's last theorem, a full 358 years after Fermat wrote that little note in the margin.

Outline

What is arithmetic geometry?

A geometric object defined by polynomial equations is called a *variety*.

What is arithmetic geometry?

A geometric object defined by polynomial equations is called a *variety*.

We have just met the following examples of varieties.

What is arithmetic geometry?

A geometric object defined by polynomial equations is called a *variety*.

We have just met the following examples of varieties.

- The circle $x^2 + y^2 = 1$

What is arithmetic geometry?

A geometric object defined by polynomial equations is called a *variety*.

We have just met the following examples of varieties.

- The circle $x^2 + y^2 = 1$
- The elliptic curve $x^3 + y^3 = 1729$

What is arithmetic geometry?

A geometric object defined by polynomial equations is called a *variety*.

We have just met the following examples of varieties.

- The circle $x^2 + y^2 = 1$
- The elliptic curve $x^3 + y^3 = 1729$
- The elliptic curve $y^2 = x(x - a^p)(x + b^p)$

What is arithmetic geometry?

A geometric object defined by polynomial equations is called a *variety*.

We have just met the following examples of varieties.

- The circle $x^2 + y^2 = 1$
- The elliptic curve $x^3 + y^3 = 1729$
- The elliptic curve $y^2 = x(x - a^p)(x + b^p)$

The geometry of all of these varieties was linked to certain number theoretic problems.

What is arithmetic geometry?

A geometric object defined by polynomial equations is called a *variety*.

We have just met the following examples of varieties.

- The circle $x^2 + y^2 = 1$
- The elliptic curve $x^3 + y^3 = 1729$
- The elliptic curve $y^2 = x(x - a^p)(x + b^p)$

The geometry of all of these varieties was linked to certain number theoretic problems.

The study of these kinds of relationships is *arithmetic geometry*.

Thank You!

Questions?