CO 480 Lecture 21

Fermat's Last Theorem

July 20th, 2017

July 20th, 1886

Bernhard Riemann died in Selasca, Italy. Most famous for Riemannian space, the Riemann Hypothesis and the Riemann integral, he was a student of Eisenstein, Dirichlet, and Gauss.

History of the Course

- I structured this course to be based around Fermat's Last Theorem
- We started with Diophantine Equations
- We moved to Pell's Equations, talked about roots of single variable polynomial equations
- We also studied such equations modulo p.
- We discussed the revitalization of number theory beginning around the time of Fermat.
- We talked about the cases of Fermat's Last Theorem when $n \in \{3, 4, 5\}$.

The Future of Fermat's Last Theorem

- A early attempt on Fermat's Last Theorem $x^n + y^n = z^n$ involved using the ring of integers of the cyclotomic field $\mathbb{Z}[\zeta_n]$ where ζ_n is a complex root of unity and attempting to factor the equation (due to Lamé and Kummer).

The Future of Fermat's Last Theorem

- A early attempt on Fermat's Last Theorem $x^n + y^n = z^n$ involved using the ring of integers of the cyclotomic field $\mathbb{Z}[\zeta_n]$ where ζ_n is a complex root of unity and attempting to factor the equation (due to Lamé and Kummer).
- The biggest obstacle in this attempt was that $\mathbb{Z}[\zeta_n]$ is not always a unique factorization domain! (In fact erroneous proofs of FLT appeared in the literature which assumed this fact).

The Future of Fermat's Last Theorem

- A early attempt on Fermat's Last Theorem $x^n + y^n = z^n$ involved using the ring of integers of the cyclotomic field $\mathbb{Z}[\zeta_n]$ where ζ_n is a complex root of unity and attempting to factor the equation (due to Lamé and Kummer).
- The biggest obstacle in this attempt was that $\mathbb{Z}[\zeta_n]$ is not always a unique factorization domain! (In fact erroneous proofs of FLT appeared in the literature which assumed this fact).
- Perhaps if we look at rings with unique factorization (or even better - if we look at Euclidean domains) we can extend some of factorization techniques.

Mordell's Conjecture

- In 1922, Mordell made an extremely bold conjecture:

Mordell's Conjecture

- In 1922, Mordell made an extremely bold conjecture:

Mordell's Conjecture

Let C be a non-singular algebraic curve of genus $g > 1$ over $\mathbb{Q}$. Then C has a finite number of rational points.

Mordell's Conjecture

- In 1922, Mordell made an extremely bold conjecture:

Mordell's Conjecture

Let C be a non-singular algebraic curve of genus $g > 1$ over $\mathbb{Q}$. Then C has a finite number of rational points.

- It turns out that for $n > 3$, we see that $x^n + y^n = z^n$ has genus greater than 1.
- In 1983/1984, Gerd Faltings proved this theorem used tools of algebraic geometry, specifically Néron models, to prove this conjecture.

The Modular Method

In the next few slides, we'll outline the elements of a final proof to Fermat's Last Theorem. That is, we will show that there are no solutions to the equation $x^n + y^n = z^n$ in pairwise coprime integers x, y, z and $n \geq 5$.

The Modular Method

In the next few slides, we'll outline the elements of a final proof to Fermat's Last Theorem. That is, we will show that there are no solutions to the equation $x^n + y^n = z^n$ in pairwise coprime integers x, y, z and $n \geq 5$. Without loss of generality, suppose n is prime and $n \geq 5$.

The Modular Method

In the next few slides, we'll outline the elements of a final proof to Fermat's Last Theorem. That is, we will show that there are no solutions to the equation $x^n + y^n = z^n$ in pairwise coprime integers x, y, z and $n \geq 5$. Without loss of generality, suppose n is prime and $n \geq 5$. The techniques here use elliptic curves, modular forms, and a whole lot of machinery.

Definition

An elliptic curve over $\mathbb{Q}$ is any smooth (non-singular) curve (no double roots) satisfying

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Q}$. By clearing denominators and relabeling, we may assume $a_i \in \mathbb{Z}$.

Examples of an Elliptic Curve

- Let's look at examples of elliptic curves. What do they look like on the real plane?
- Let's try to draw $y^2 = x^3 - x$ first by drawing $y = x^3 - x$ and then trying to draw the elliptic curve.

Drawing $y = x^3 - x$

Drawing $y = x^3 - x$

- First, note that $y = x^3 - x = x(x-1)(x+1)$ and so the equation has three zeroes at $x = 0, \pm 1$.

Drawing $y = x^3 - x$

- First, note that $y = x^3 - x = x(x-1)(x+1)$ and so the equation has three zeroes at $x = 0, \pm 1$.
- Now let's break this curve into four intervals and see what happens in each interval $y = x^3 - x = x(x-1)(x+1)$.

Drawing $y = x^3 - x$

- First, note that $y = x^3 - x = x(x-1)(x+1)$ and so the equation has three zeroes at $x = 0, \pm 1$.
- Now let's break this curve into four intervals and see what happens in each interval $y = x^3 - x = x(x-1)(x+1)$.
- Between $-\infty$ and -1, the function is negative.

Drawing $y = x^3 - x$

- First, note that $y = x^3 - x = x(x-1)(x+1)$ and so the equation has three zeroes at $x = 0, \pm 1$.
- Now let's break this curve into four intervals and see what happens in each interval $y = x^3 - x = x(x-1)(x+1)$.
- Between $-\infty$ and -1, the function is negative.
- Between -1 and 0, the function is positive.

Drawing $y = x^3 - x$

- First, note that $y = x^3 - x = x(x-1)(x+1)$ and so the equation has three zeroes at $x = 0, \pm 1$.
- Now let's break this curve into four intervals and see what happens in each interval $y = x^3 - x = x(x-1)(x+1)$.
- Between $-\infty$ and -1, the function is negative.
- Between -1 and 0, the function is positive.
- Between 0 and 1, the function is negative.

Drawing $y = x^3 - x$

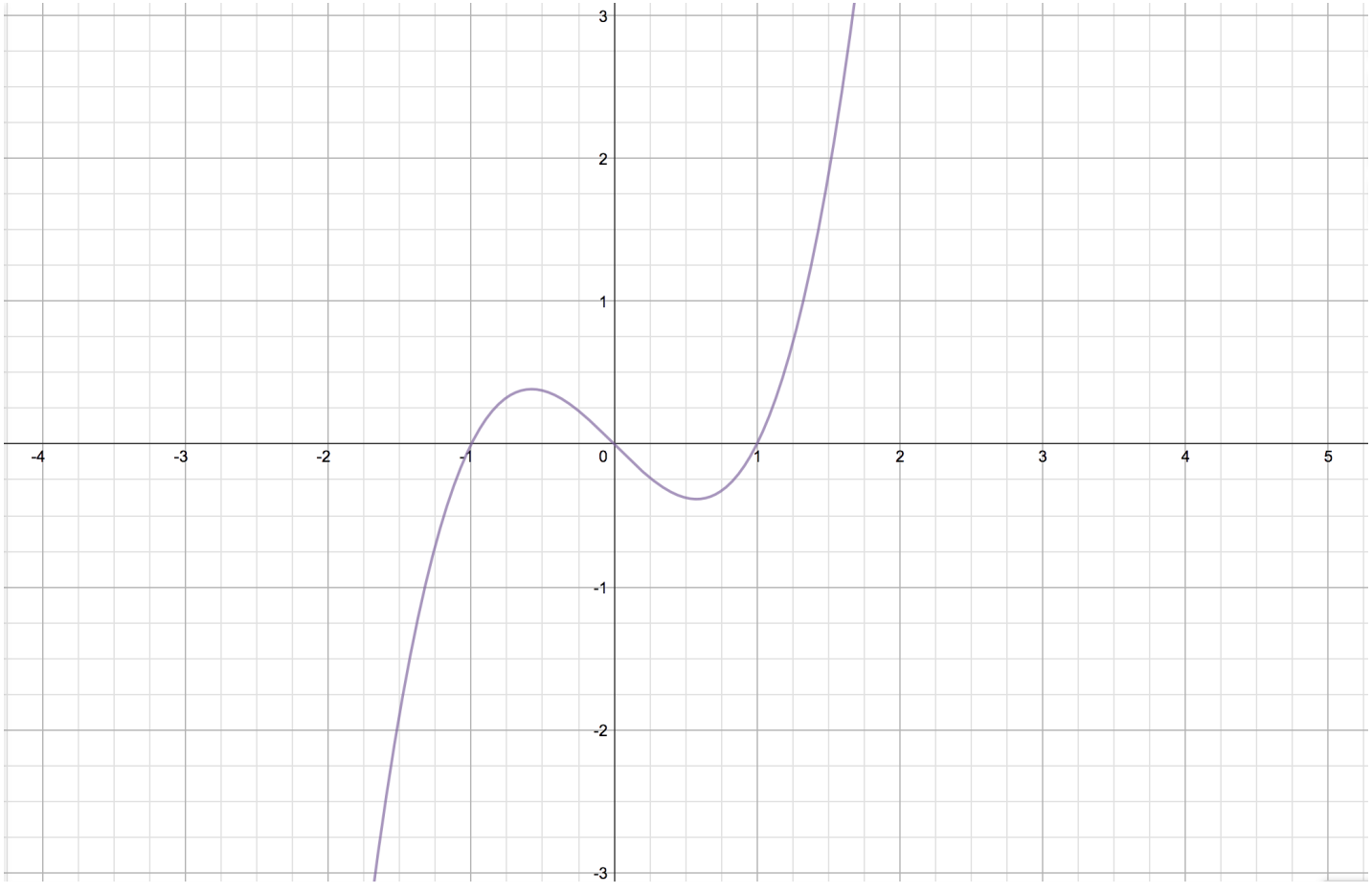
- First, note that $y = x^3 - x = x(x-1)(x+1)$ and so the equation has three zeroes at $x = 0, \pm 1$.
- Now let's break this curve into four intervals and see what happens in each interval $y = x^3 - x = x(x-1)(x+1)$.
- Between $-\infty$ and -1, the function is negative.
- Between -1 and 0, the function is positive.
- Between 0 and 1, the function is negative.
- Between 1 and ∞, the function is positive.

Drawing $y = x^3 - x$

- First, note that $y = x^3 - x = x(x-1)(x+1)$ and so the equation has three zeroes at $x = 0, \pm 1$.
- Now let's break this curve into four intervals and see what happens in each interval $y = x^3 - x = x(x-1)(x+1)$.
- Between $-\infty$ and -1, the function is negative.
- Between -1 and 0, the function is positive.
- Between 0 and 1, the function is negative.
- Between 1 and ∞, the function is positive.
- Lastly, the curve should look smooth with no breaks.

The Cubic Curve $y = x^3 - x$

Here is the picture (Using Desmos.com)



The Elliptic Curve $y^2 = x^3 - x$

- What changes when we make the left hand side y^2 instead of y?

The Elliptic Curve $y^2 = x^3 - x$

- What changes when we make the left hand side y^2 instead of y?
- For almost all values of x, we will get not 1 but 2 output values (the exceptions are the roots).

The Elliptic Curve $y^2 = x^3 - x$

- What changes when we make the left hand side y^2 instead of y?
- For almost all values of x, we will get not 1 but 2 output values (the exceptions are the roots).
- This means that we no longer have a function, rather a curve.

The Elliptic Curve $y^2 = x^3 - x$

- What changes when we make the left hand side y^2 instead of y?
- For almost all values of x, we will get not 1 but 2 output values (the exceptions are the roots).
- This means that we no longer have a function, rather a curve.
- The cubic must be positive to have a real root! So all the areas where the picture is negative are gone.

The Elliptic Curve $y^2 = x^3 - x$

- What changes when we make the left hand side y^2 instead of y?
- For almost all values of x, we will get not 1 but 2 output values (the exceptions are the roots).
- This means that we no longer have a function, rather a curve.
- The cubic must be positive to have a real root! So all the areas where the picture is negative are gone.
- The curve still has no breaks and is symmetric about the x-axis, that is, if I reflect the top half of the picture, it should match the bottom half.

The Elliptic Curve $y^2 = x^3 - x$

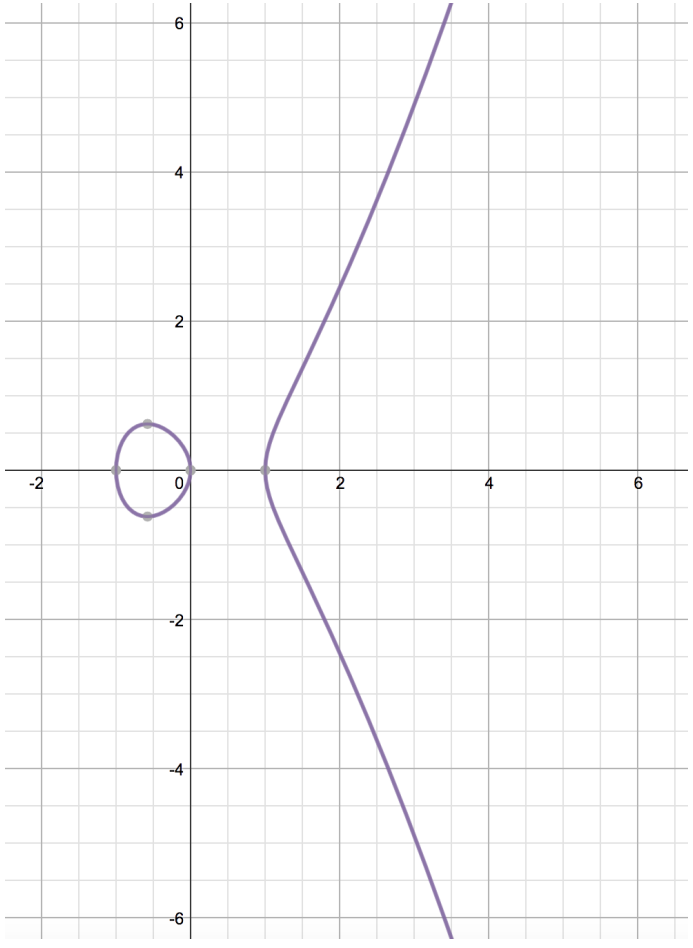
- What changes when we make the left hand side y^2 instead of y?
- For almost all values of x, we will get not 1 but 2 output values (the exceptions are the roots).
- This means that we no longer have a function, rather a curve.
- The cubic must be positive to have a real root! So all the areas where the picture is negative are gone.
- The curve still has no breaks and is symmetric about the x-axis, that is, if I reflect the top half of the picture, it should match the bottom half.
- The function should still be smooth (even at 1).

The Elliptic Curve $y^2 = x^3 - x$

Here is the picture (All graphs courtesy of Desmos.com)

The Elliptic Curve $y^2 = x^3 - x$

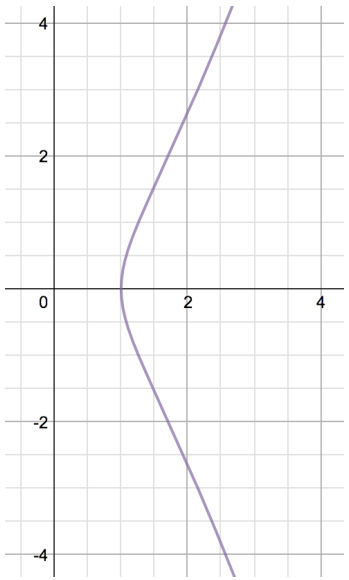
Here is the picture (All graphs courtesy of Desmos.com)



Notice that the curve has two connected components!

Connected Components

Note: In general, not all elliptic curves have two components. Some have one like $y^2 = x^3 - 1$:



However, the elliptic curves associated to the Congruent Number Problem always have two connect components.

Points on an elliptic curve

- Elliptic curves have infinitely many real points.

Points on an elliptic curve

- Elliptic curves have infinitely many real points.
- As an example, $y^2 = x^3 - x$ has infinitely many real points by noticing that the cubic on the right is always positive when $x > 1$ and hence we can find a y value by taking the square root.
- So if we take $x = 2$, then we see that $y^2 = 2^3 - 2 = 6$ and so the point $P = (2, \sqrt{6})$ and $Q = (2, -\sqrt{6})$ are on the curve.

Points on an elliptic curve

- From the perspective of Diophantine equations, it is interesting to ask: How many integer points are on elliptic curves?
- For the example $y^2 = x^3 - x$, it turns out that $(\pm 1, 0)$ and $(0, 0)$ are the only integer points, though this is hardly obvious.

Points on an elliptic curve

- From the perspective of Diophantine equations, it is interesting to ask: How many integer points are on elliptic curves?
- For the example $y^2 = x^3 - x$, it turns out that $(\pm 1, 0)$ and $(0, 0)$ are the only integer points, though this is hardly obvious.
- How many rational points are on elliptic curves?
- Above, the only rational points are also the integral ones.

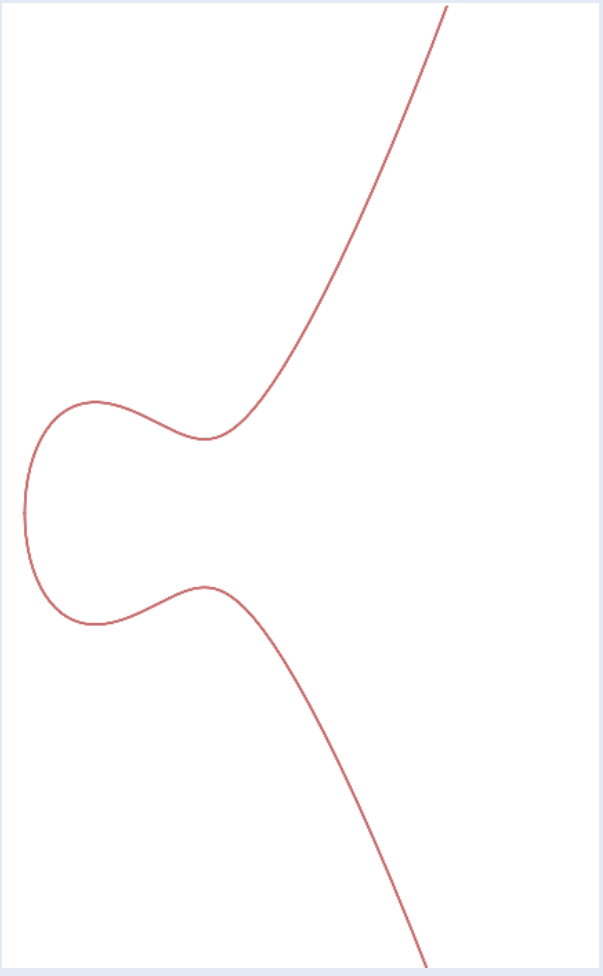
Points on an elliptic curve

- From the perspective of Diophantine equations, it is interesting to ask: How many integer points are on elliptic curves?
- For the example $y^2 = x^3 - x$, it turns out that $(\pm 1, 0)$ and $(0, 0)$ are the only integer points, though this is hardly obvious.
- How many rational points are on elliptic curves?
- Above, the only rational points are also the integral ones.
- More on this later.

Group Law of an Elliptic Curve

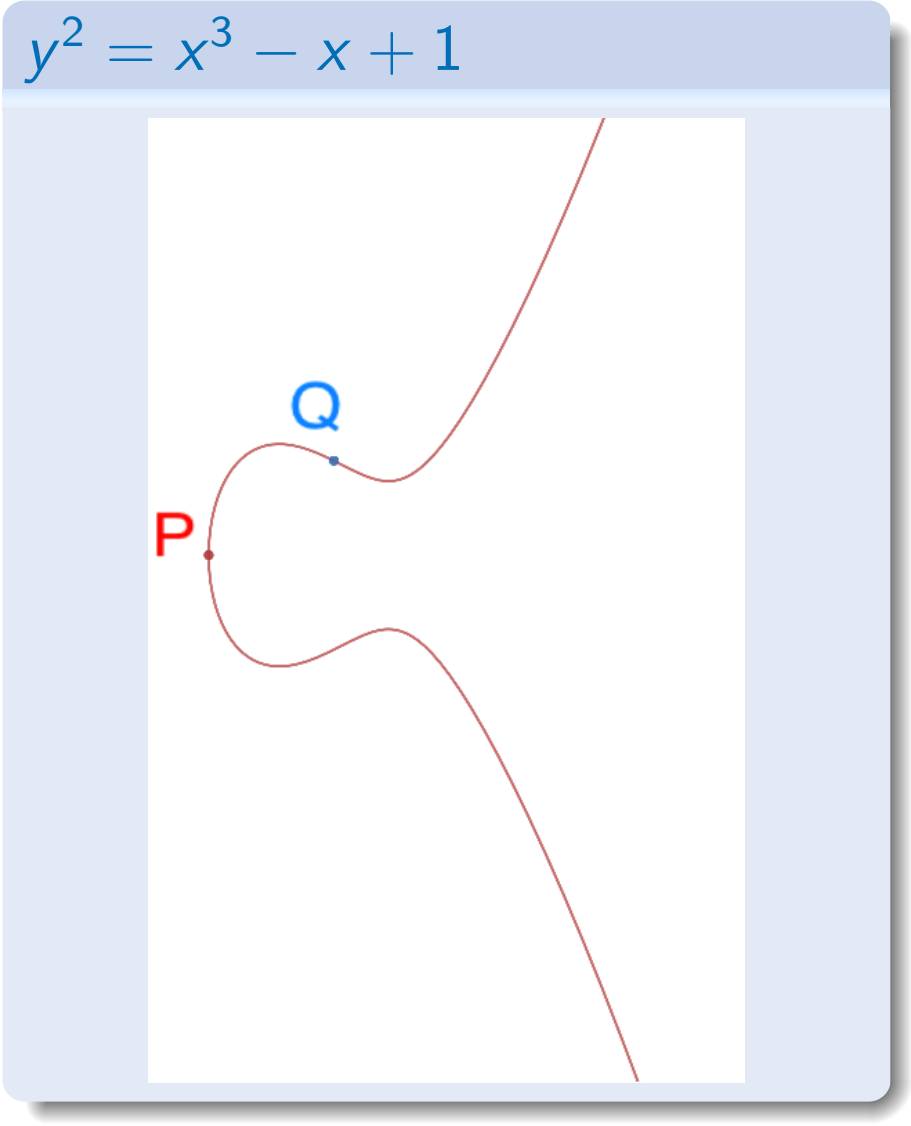
- With an elliptic curve, we can actually describe a way to, given two rational points P and Q, create a third rational point R.
- Let's begin with the elliptic curve $y^2 = x^3 - x + 1$ for illustrative purposes.

$y^2 = x^3 - x + 1$



Group Law of an Elliptic Curve

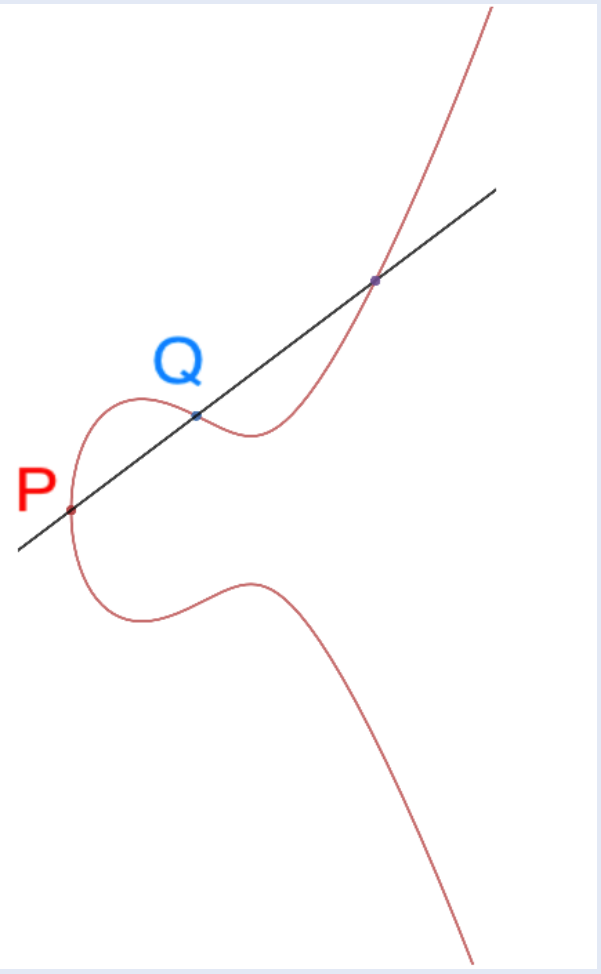
- Let's take the points $P = (-1.324, 0)$ and $Q = (0, 1)$ (correct to three decimal places).



Group Law of an Elliptic Curve

- Draw the line between P and Q. It intersects the curve in a third point as shown in the picture at coordinates $(1.895, 2.43)$.

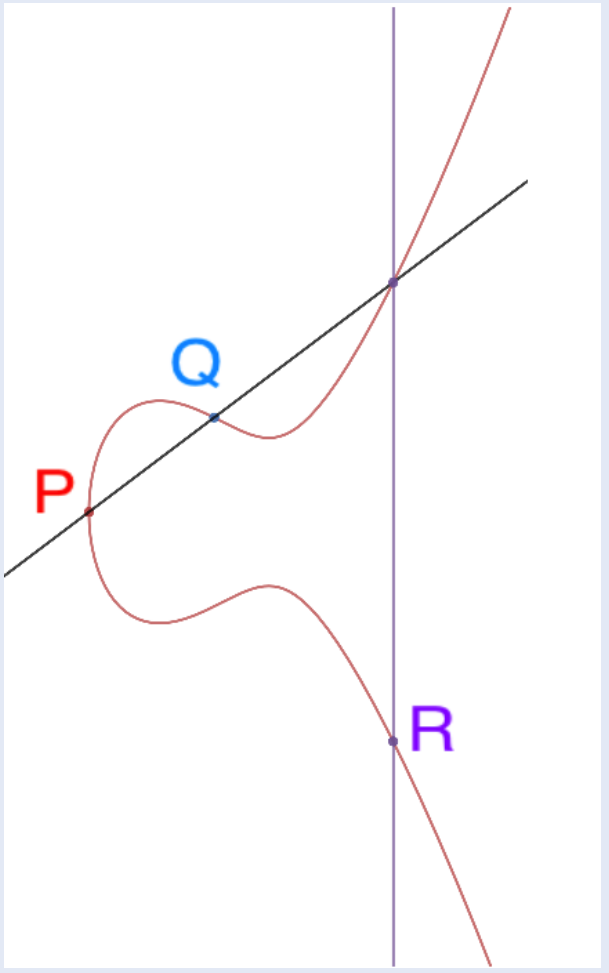
$y^2 = x^3 - x + 1$



Group Law of an Elliptic Curve

- Draw the vertical line through the point which must intersect the curve in a third point, in our case, $R = (1.895, -2.43)$ (this is the same as reflecting about the x-axis).
- Define $P + Q = R$ for points on an elliptic curve (note that this isn't just adding the coordinates!)

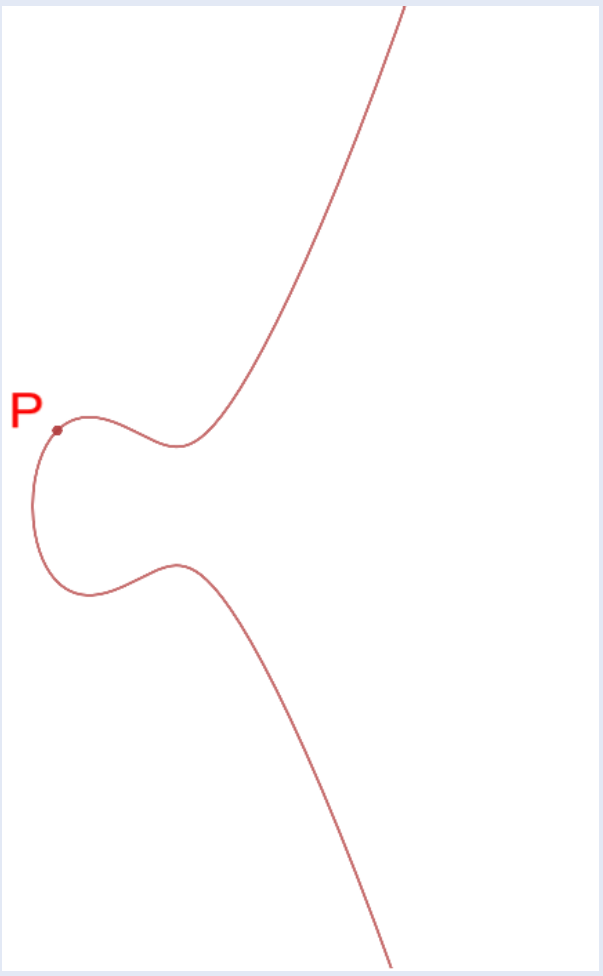
$y^2 = x^3 - x + 1$



Group Law of an Elliptic Curve

- If $P = Q$, then we can still add points.
- Here, we use the tangent line to find a third point of intersection.
- To the right, we start with the point $P = (-1, 1)$ on the same elliptic curve.

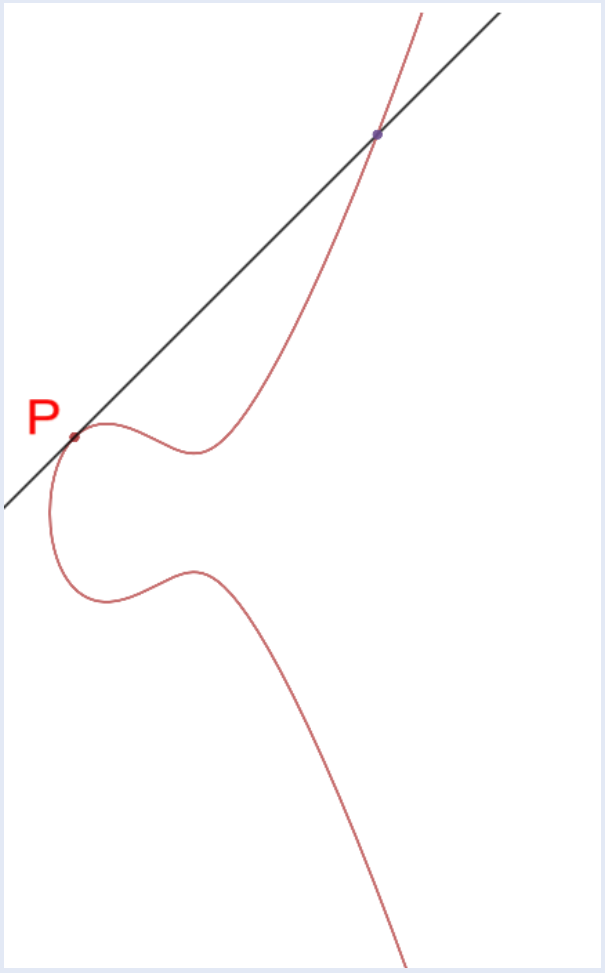
$y^2 = x^3 - x + 1$



Group Law of an Elliptic Curve

- Using calculus, we can calculate the tangent line at P to be $y = x + 2$.
- This intersects the elliptic curve at the point $(3, 5)$.

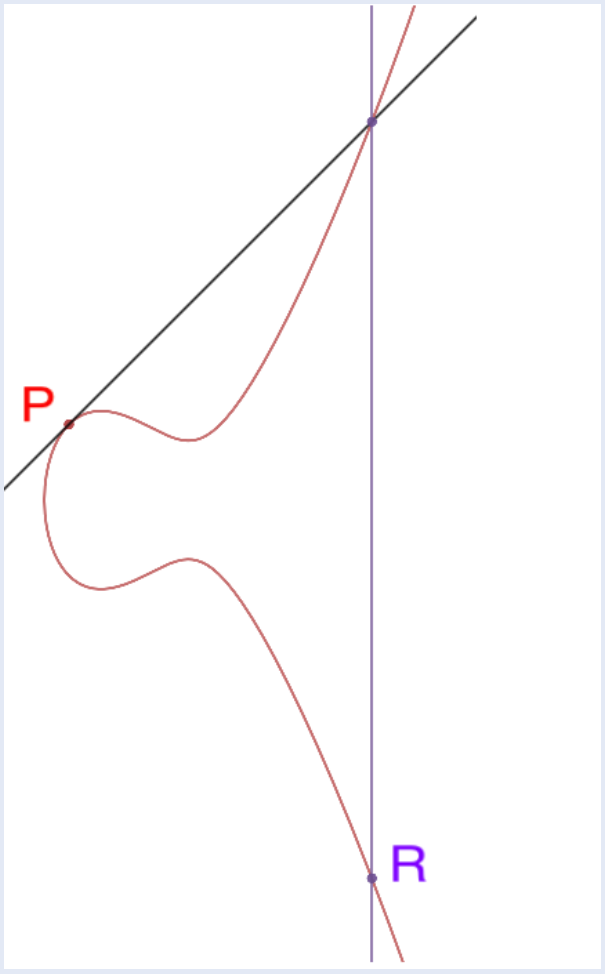
$y^2 = x^3 - x + 1$



Group Law of an Elliptic Curve

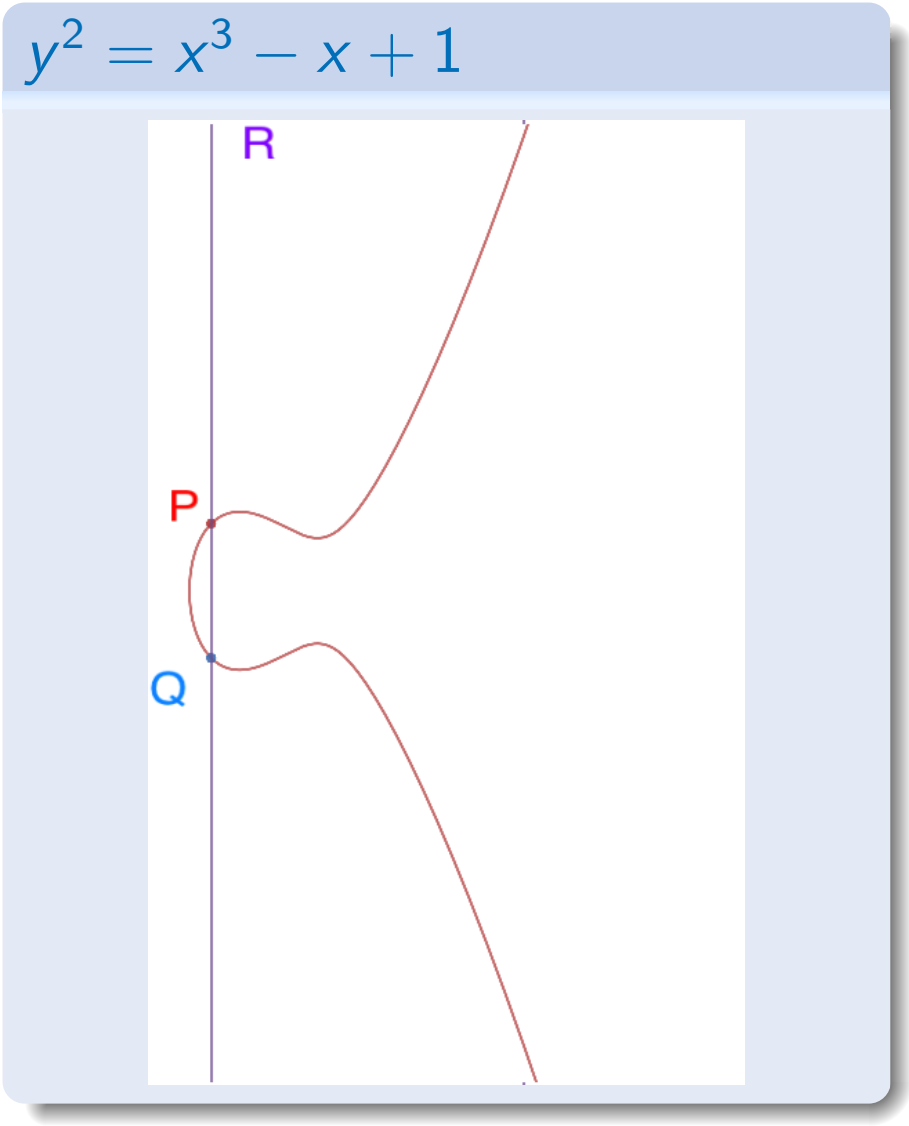
- Reflecting as before gives us that $2P = P + P = (3, -5)$.

$y^2 = x^3 - x + 1$



Group Law of an Elliptic Curve

- What about if the line between P and Q is vertical?
- We define a "point at infinity" and call it $R = \mathcal{O}$. This point intersects all vertical lines.
- In this case, we also call $Q = -P$ (this is the reflection of P about the x-axis).
- Thus $P - P = P + Q = R = \mathcal{O}$



The Modular Method

Associated to each elliptic curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a number N called the conductor and another number Δ called the discriminant (much like the discriminant of a quadratic or a cubic). These values tell you when the curve is also defined over $\mathbb{F}_p$.

The Modular Method

Associated to each elliptic curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a number N called the conductor and another number Δ called the discriminant (much like the discriminant of a quadratic or a cubic). These values tell you when the curve is also defined over $\mathbb{F}_p$. For example, $y^2 = x^3 + x^2 + 4x + 4$ has conductor $N = 20 = 2^2 \cdot 5$. This elliptic curve is defined in all $\mathbb{F}_p$ where $p \neq 2, 5$. Reducing the curve modulo 5 for example gives

$$y^2 = x^3 + x^2 + 4x + 4 \equiv x^3 + x^2 - x - 1 \equiv (x+1)^2(x-1) \mod 5$$

which has a double root and hence is not smooth.
Also, special values called the Trace of Frobenius given by

$$a_p(E) = p + 1 - \#E(\mathbb{F}_p)$$

Now For Something Completely Different...

Let $\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$.

Definition

A modular form of weight k for $\mathrm{SL}(2,\mathbb{Z})$ is a complex valued function on the upper half plane $\mathbb{H}$ to the upper half plane satisfying three properties

- The function f is a holomorphic function on $\mathbb{H}$.
- For any $z \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, we have

$$f(\gamma z) = (cz + d)^k f(z)$$

  where $\gamma z = \frac{az+b}{cz+d}$.
- The function f is holomorphic at infinity (that is, it has a well defined Fourier Transformation)

Examples

Explicit examples of Modular forms are difficult - such functions are very complicated.

Eisenstein Series

The Eisenstein series:

$$E_k(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m+nz)^k}.$$

Is a weight k modular form over $\mathrm{SL}(2,\mathbb{Z})$ for all even $k > 2$.

Frey Curves

- A Frey curve is an elliptic curve associated to a solution to a Diophantine equation (with a few additional properties).
- Let (a, b, c) be an integer solution to $x^p + y^p = z^p$. Consider

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

This is an elliptic curve with conductor $2\mathrm{rad}_2(abc)$ (all non-two primes dividing abc) and [minimal] discriminant $2^{-8}(abc)^{2p}$.

Finishing Up

- Wiles (et al.) showed that newforms are a generalization of elliptic curves. The conductor of an elliptic curve corresponds to something called the level of a modular form.

Finishing Up

- Wiles (et al.) showed that newforms are a generalization of elliptic curves. The conductor of an elliptic curve corresponds to something called the level of a modular form.
- Ribet showed that newforms with [minimal] discriminants that have very high prime powers in their exponents can be associated to newforms with lower levels.

Finishing Up

- Wiles (et al.) showed that newforms are a generalization of elliptic curves. The conductor of an elliptic curve corresponds to something called the level of a modular form.
- Ribet showed that newforms with [minimal] discriminants that have very high prime powers in their exponents can be associated to newforms with lower levels.
- The smallest level for a newform is $N = 11$.
- In this case, one can associate a newform at level 2 to this elliptic curve which by the above doesn't exist.