# Elliptic Curves

Devin Akman

Washington University

February 2024

# What is an Elliptic Curve?

- An elliptic curve is an equation of the form

$$y^2 = x^3 + ax + b.$$

# What is an Elliptic Curve?

- An elliptic curve is an equation of the form

$$y^2 = x^3 + ax + b.$$

- The right-hand side should have three distinct roots.

# What is an Elliptic Curve?

- An elliptic curve is an equation of the form

$$y^2 = x^3 + ax + b.$$

- The right-hand side should have three distinct roots.
- This is equivalent to requiring

$$\Delta := -4a^3 - 27b^2 \neq 0.$$

Washington University in St. Louis

# What is an Elliptic Curve?

- An elliptic curve is an equation of the form

$$y^2 = x^3 + ax + b.$$

- The right-hand side should have three distinct roots.
- This is equivalent to requiring

$$\Delta := -4a^3 - 27b^2 \neq 0.$$

- Why do we care about such equations?

Washington University in St. Louis

# What is an Elliptic Curve?

- An elliptic curve is an equation of the form

$$y^2 = x^3 + ax + b.$$

- The right-hand side should have three distinct roots.
- This is equivalent to requiring

$$\Delta := -4a^3 - 27b^2 \neq 0.$$

- Why do we care about such equations?
- Their solution sets have a special property.

# How Can We Solve the Equation?

- How to solve it over $\mathbb{C}$?

# How Can We Solve the Equation?

- How to solve it over $\mathbb{C}$?
- Easy. We can always take square roots, so there are one or two values of $y$ for every value of $x$:

$$y = \pm\sqrt{x^3 + ax + b}.$$

# How Can We Solve the Equation?

- How to solve it over $\mathbb{C}$?
- Easy. We can always take square roots, so there are one or two values of $y$ for every value of $x$:

$$y = \pm\sqrt{x^3 + ax + b}.$$

- How to solve it over $\mathbb{R}$?

Washington University in St. Louis

# How Can We Solve the Equation?

- How to solve it over $\mathbb{C}$?
- Easy. We can always take square roots, so there are one or two values of $y$ for every value of $x$:

$$y = \pm\sqrt{x^3 + ax + b}.$$

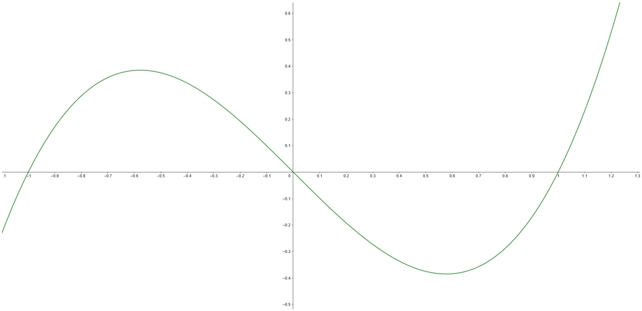
- How to solve it over $\mathbb{R}$?
- The square roots are real numbers iff

$$x^3 + ax + b \geq 0.$$

Washington University in St. Louis

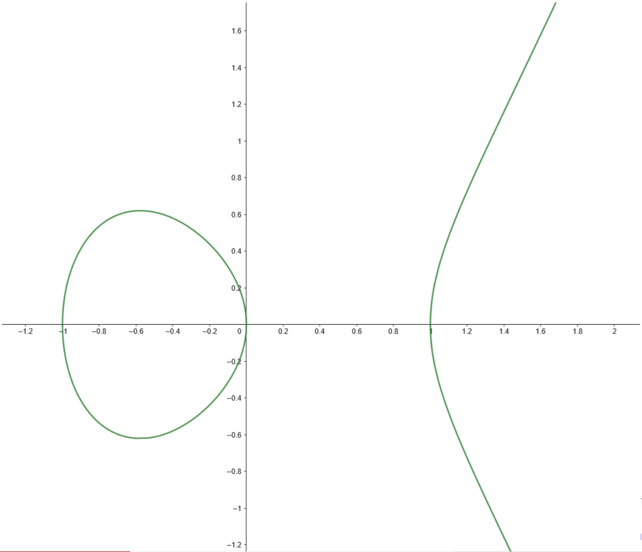
# How Can We Solve the Equation?

- If $\Delta > 0$, then the cubic has three distinct real roots:



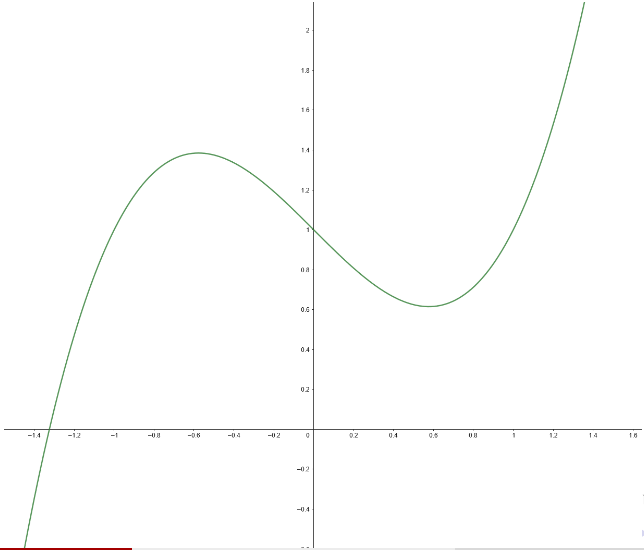
# How Can We Solve the Equation?

- The solution looks like this:



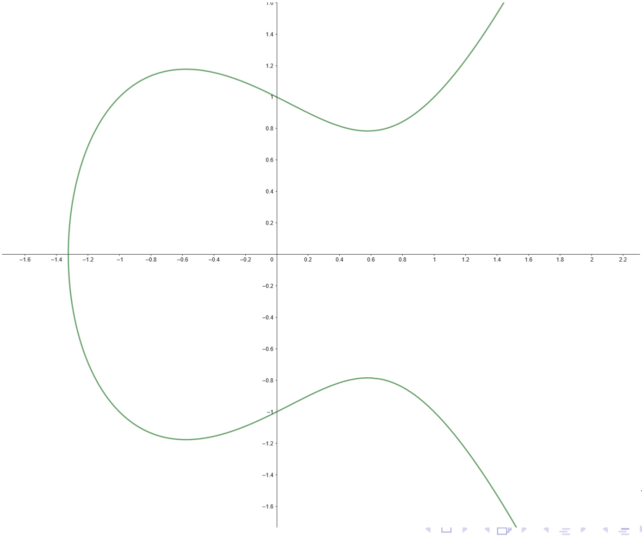
# How Can We Solve the Equation?

- If $\Delta < 0$, then the cubic has one real root:



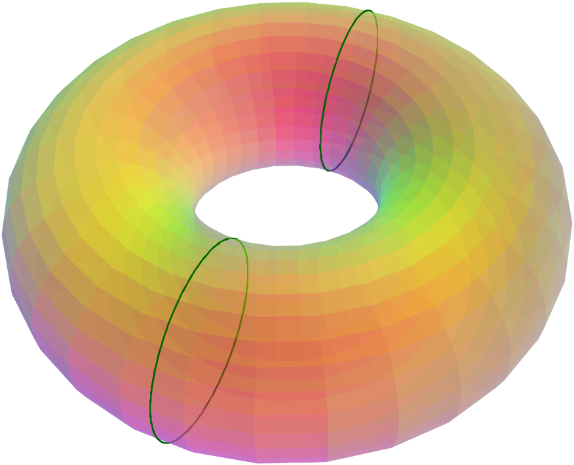
# How Can We Solve the Equation?

- The solution looks like this:



# How Can We Solve the Equation?

- The circles are a slice of the solutions over $\mathbb{C}$.



# How Can We Solve the Equation?

- How to solve it over $\mathbb{Q}$?

# How Can We Solve the Equation?

- How to solve it over $\mathbb{Q}$?
- Much more difficult! Still an active research area.

# How Can We Solve the Equation?

- How to solve it over $\mathbb{Q}$?
- Much more difficult! Still an active research area.
- Can you find solutions to

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

that are integers or rational numbers?

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.
- Let $-R$ be the reflection of $R$ across the $x$-axis (also a point on $E$!).

Washington University in St. Louis

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.
- Let $-R$ be the reflection of $R$ across the $x$-axis (also a point on $E$!).
- $P + Q = -R$.

Washington University in St. Louis

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.
- Let $-R$ be the reflection of $R$ across the $x$-axis (also a point on $E$!).
- $P + Q = -R$.
- The solutions form an *abelian group*.

Washington University in St. Louis

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.
- Let $-R$ be the reflection of $R$ across the $x$-axis (also a point on $E$!).
- $P + Q = -R$.
- The solutions form an *abelian group*.
- Things to ponder:

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.
- Let $-R$ be the reflection of $R$ across the $x$-axis (also a point on $E$!).
- $P + Q = -R$.
- The solutions form an *abelian group*.
- Things to ponder:
  - What if $Q = P$?

Washington University in St. Louis

# Special Property of Solutions

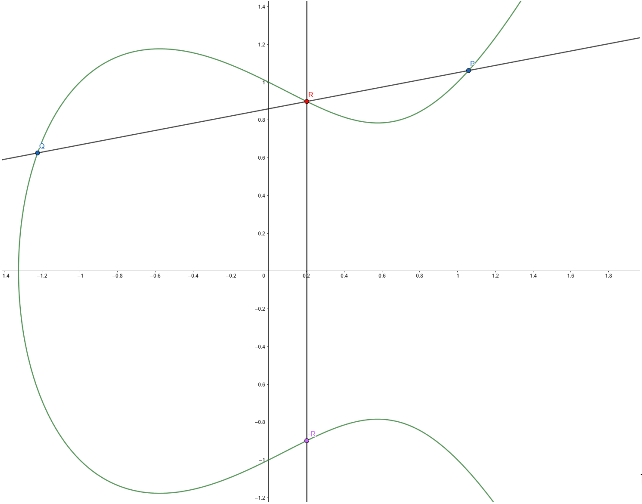
- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.
- Let $-R$ be the reflection of $R$ across the $x$-axis (also a point on $E$!).
- $P + Q = -R$.
- The solutions form an *abelian group*.
- Things to ponder:
  - What if $Q = P$?
  - What if $Q = -P$?

Washington University in St. Louis

# Special Property of Solutions

- Two solutions (over any field!) can be added to get a third one.
- Let $P$ and $Q$ be two points on an elliptic curve $E$.
- The secant line $\overline{PQ}$ intersects $E$ at a third point $R$.
- Let $-R$ be the reflection of $R$ across the $x$-axis (also a point on $E$!).
- $P + Q = -R$.
- The solutions form an *abelian group*.
- Things to ponder:
  - What if $Q = P$?
  - What if $Q = -P$?
  - What is the identity element?

- Example:



# Special Property of Solutions

- Use this addition law to generate more solutions from the ones you've already found.

# Special Property of Solutions

- Use this addition law to generate more solutions from the ones you've already found.
- Strategy:

# Special Property of Solutions

- Use this addition law to generate more solutions from the ones you've already found.
- Strategy:
  - Find an equation for the line between two points.

# Special Property of Solutions

- Use this addition law to generate more solutions from the ones you've already found.
- Strategy:
  - Find an equation for the line between two points.
  - Substitute $y = mx + b$ into the equation for the curve.

Washington University in St. Louis

# Special Property of Solutions

- Use this addition law to generate more solutions from the ones you've already found.
- Strategy:
  - Find an equation for the line between two points.
  - Substitute $y = mx + b$ into the equation for the curve.
  - Use the fact that you already know two out of three solutions of the resulting cubic.

Washington University in St. Louis

# Special Property of Solutions

- Use this addition law to generate more solutions from the ones you've already found.
- Strategy:
  - Find an equation for the line between two points.
  - Substitute $y = mx + b$ into the equation for the curve.
  - Use the fact that you already know two out of three solutions of the resulting cubic.
  - Polynomial long division or Vieta's formulas may help.

Washington University in St. Louis

# A General Formula for Adding Points

- We'll derive a general addition formula.

# A General Formula for Adding Points

- We'll derive a general addition formula.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.

# A General Formula for Adding Points

- We'll derive a general addition formula.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.
- The slope of the line between them is

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

# A General Formula for Adding Points

- We'll derive a general addition formula.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.
- The slope of the line between them is

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

- If $x_2 = x_1$ and $y_2 = -y_1$, then $P + Q = \infty$.

Washington University in St. Louis

# A General Formula for Adding Points

- We'll derive a general addition formula.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.
- The slope of the line between them is

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

- If $x_2 = x_1$ and $y_2 = -y_1$, then $P + Q = \infty$.
- We'll handle the case $P = Q$ later.

# A General Formula for Adding Points

- The equation of the line $\overline{PQ}$ is

$$y = m(x - x_1) + y_1.$$

Washington University in St. Louis

# A General Formula for Adding Points

- The equation of the line $\overline{PQ}$ is

$$y = m(x - x_1) + y_1.$$

- Substitute:

$$x^3 - x + 1 - [m(x - x_1) + y_1]^2 = 0$$

# A General Formula for Adding Points

- The equation of the line $\overline{PQ}$ is

$$y = m(x - x_1) + y_1.$$

- Substitute:

$$x^3 - x + 1 - [m(x - x_1) + y_1]^2 = 0$$

- The coefficient of $x^2$ is

$$-m^2 = -(x_1 + x_2 + x_3) \implies x_3 = m^2 - (x_1 + x_2).$$

Washington University in St. Louis

# A General Formula for Adding Points

- Plug $x_3$ back into the equation of the line:

$$-y_3 = m(x_3 - x_1) + y_1 \implies y_3 = m(x_1 - x_3) - y_1.$$

# A General Formula for Adding Points

- Plug $x_3$ back into the equation of the line:

$$-y_3 = m(x_3 - x_1) + y_1 \implies y_3 = m(x_1 - x_3) - y_1.$$

- The final formula is $P + Q = (x_3, y_3)$, where

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$
$$x_3 = m^2 - (x_1 + x_2)$$
$$y_3 = m(x_1 - x_3) - y_1.$$

Washington University in St. Louis

# A General Formula for Adding Points

- When $P = Q$, the only change we have to make is using the tangent line instead of the secant line.

# A General Formula for Adding Points

- When $P = Q$, the only change we have to make is using the tangent line instead of the secant line.
- Implicit differentiation gives us

$$2yy' = 3x^2 - 1 \implies y' = \frac{3x^2 - 1}{2y} \implies m = \frac{3x_1^2 - 1}{2y_1}.$$

Washington University in St. Louis

# A General Formula for Adding Points

- When $P = Q$, the only change we have to make is using the tangent line instead of the secant line.
- Implicit differentiation gives us

$$2yy' = 3x^2 - 1 \implies y' = \frac{3x^2 - 1}{2y} \implies m = \frac{3x_1^2 - 1}{2y_1}.$$

- This formula doesn't work at $y_1 = 0$.

Washington University in St. Louis

# A General Formula for Adding Points

- When $P = Q$, the only change we have to make is using the tangent line instead of the secant line.
- Implicit differentiation gives us

$$2yy' = 3x^2 - 1 \implies y' = \frac{3x^2 - 1}{2y} \implies m = \frac{3x_1^2 - 1}{2y_1}.$$

- This formula doesn't work at $y_1 = 0$.
- Why not? If $P = (x_1, 0)$, then what is $2P$?

Washington University in St. Louis

# Solutions over $\mathbb{Q}$ and Finite Fields

- For this curve, it turns out that adding the point $(1, 1)$ to itself forever generates half of all rational solutions.

# Solutions over $\mathbb{Q}$ and Finite Fields

- For this curve, it turns out that adding the point $(1,1)$ to itself forever generates half of all rational solutions.
- The other half is their negatives.

# Solutions over $\mathbb{Q}$ and Finite Fields

- For this curve, it turns out that adding the point $(1, 1)$ to itself forever generates half of all rational solutions.
- The other half is their negatives.
- The abelian group of rational points is $\mathbb{Z}$ with $(1, \pm 1)$ as generators.

# Solutions over $\mathbb{Q}$ and Finite Fields

- For this curve, it turns out that adding the point $(1, 1)$ to itself forever generates half of all rational solutions.
- The other half is their negatives.
- The abelian group of rational points is $\mathbb{Z}$ with $(1, \pm 1)$ as generators.
- Other curves may have more complicated groups of rational points (or no rational points at all!).

# Solutions over $\mathbb{Q}$ and Finite Fields

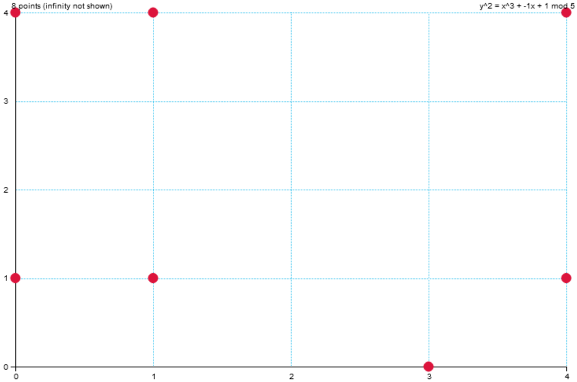
- For this curve, it turns out that adding the point $(1,1)$ to itself forever generates half of all rational solutions.
- The other half is their negatives.
- The abelian group of rational points is $\mathbb{Z}$ with $(1,\pm 1)$ as generators.
- Other curves may have more complicated groups of rational points (or no rational points at all!).
- Easier exercise: find all solutions to

$$y^2 \equiv x^3 - x + 1 \pmod 5.$$

Washington University in St. Louis

# Solutions over $\mathbb{Q}$ and Finite Fields

- Our curve looks like this over $\mathbb{F}_5$:



# Applications

- Computers can find points on elliptic curves over finite fields and add them quickly.

# Applications

- Computers can find points on elliptic curves over finite fields and add them quickly.
- This addition appears "random," which cryptographers like.

# Applications

- Computers can find points on elliptic curves over finite fields and add them quickly.
- This addition appears "random," which cryptographers like.
- Elliptic curve cryptography (ECC) is a faster replacement for RSA.

# Applications

- Computers can find points on elliptic curves over finite fields and add them quickly.
- This addition appears "random," which cryptographers like.
- Elliptic curve cryptography (ECC) is a faster replacement for RSA.
- It kicks in each time you go online or make a credit card purchase.

# Applications

- Computers can find points on elliptic curves over finite fields and add them quickly.
- This addition appears "random," which cryptographers like.
- Elliptic curve cryptography (ECC) is a faster replacement for RSA.
- It kicks in each time you go online or make a credit card purchase.
- Elliptic curves were a crucial ingredient in Andrew Wiles' proof of Fermat's Last Theorem (FLT).

# Applications

- Computers can find points on elliptic curves over finite fields and add them quickly.
- This addition appears "random," which cryptographers like.
- Elliptic curve cryptography (ECC) is a faster replacement for RSA.
- It kicks in each time you go online or make a credit card purchase.
- Elliptic curves were a crucial ingredient in Andrew Wiles' proof of Fermat's Last Theorem (FLT).
- FLT says there are no integer solutions to the equation

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

where $n > 2$ and $a, b, c$ are all nonzero.

Washington University in St. Louis