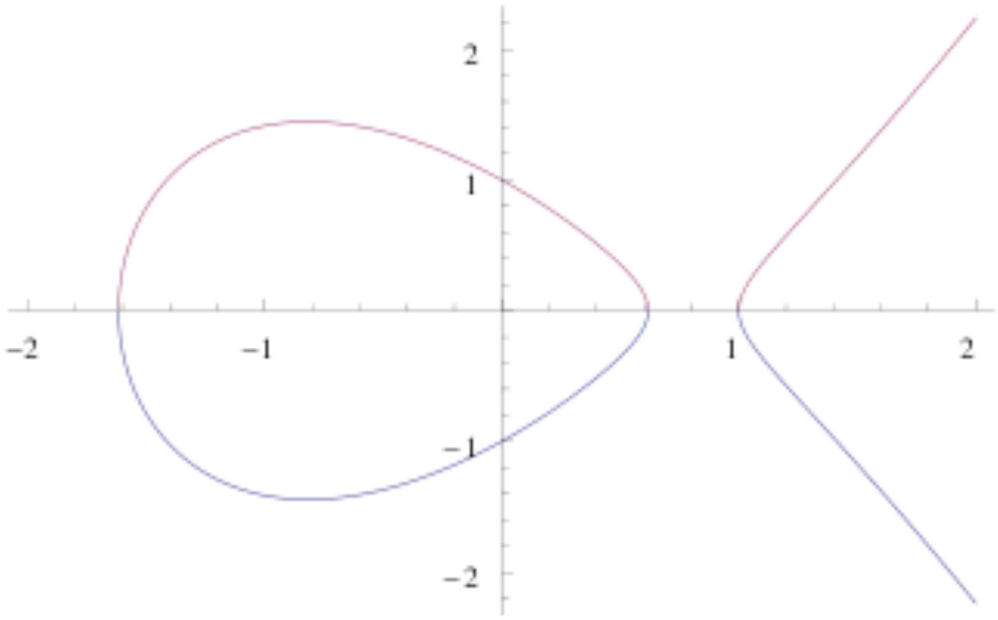
ELLIPTIC CURVES

By Jessica and Sushi

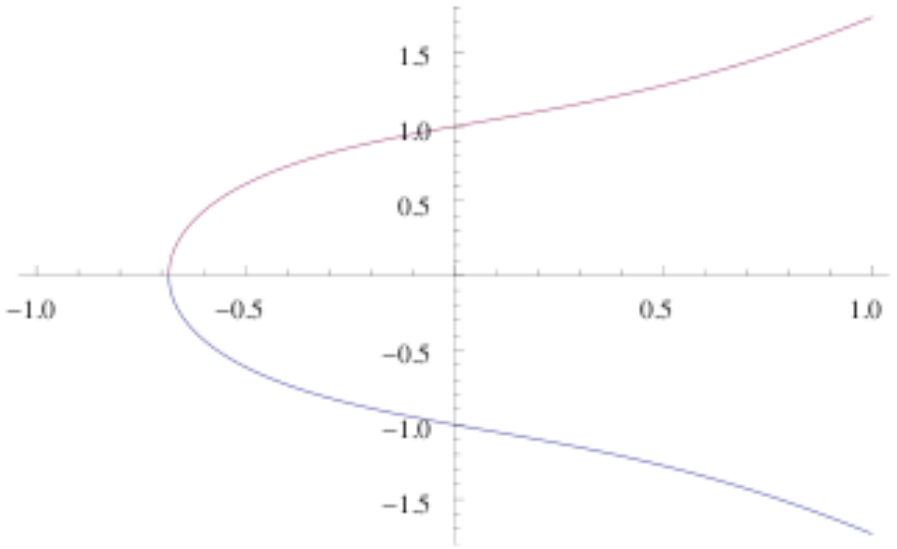
WHAT ARE ELLIPTIC CURVES?!

$$y^2 = ax^3 + bx + c$$

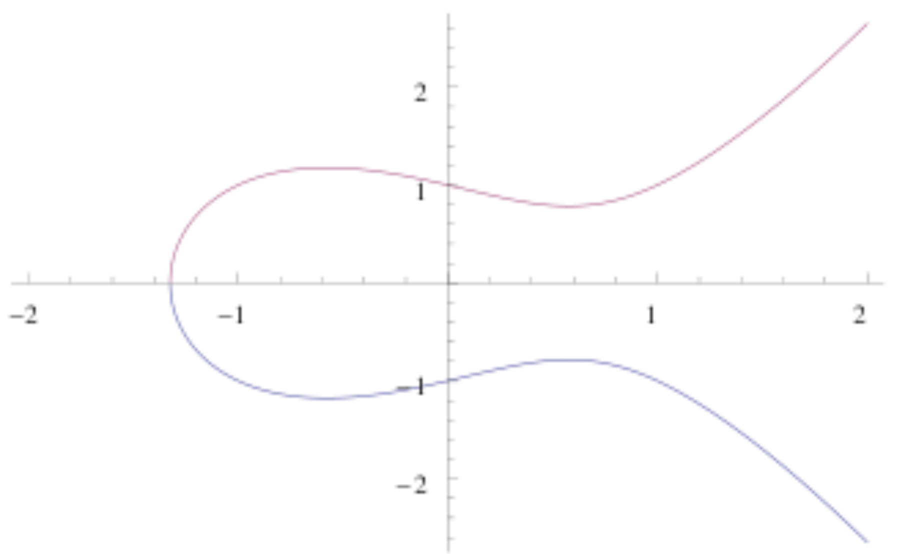
```
Plot[{-(x^3 - 2 x + 1)^.5, (x^3 - 2 x + 1)^.5}, {x, 2, -2}]
```



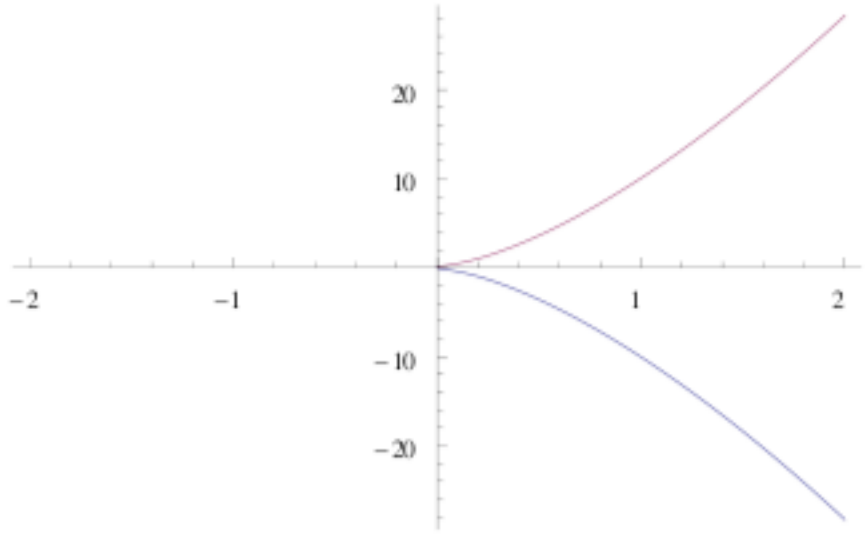
```
Plot[{- (x^3 + x + 1)^.5, (x^3 + x + 1)^.5}, {x, -1, 1}]
```



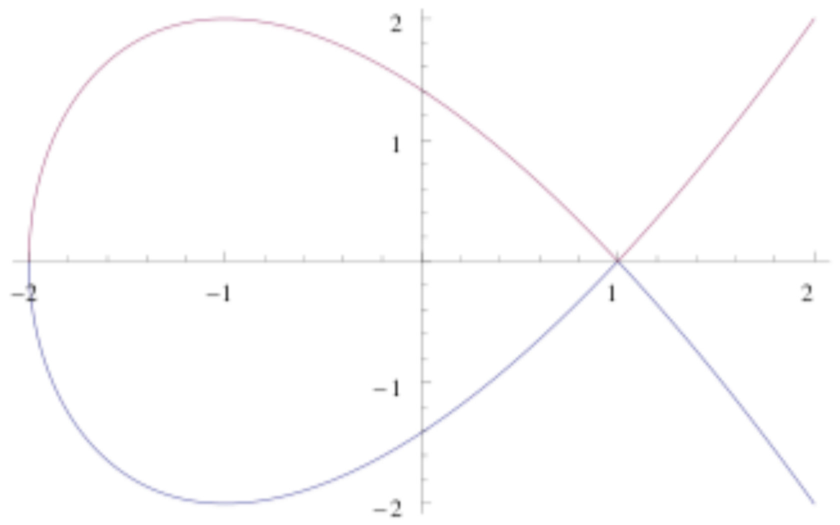

```
Plot[{- (x^3 - x + 1)^.5, (x^3 - x + 1)^.5}, {x, -2, 2}]
```



```
Plot[{-(100 x^3 + x)^.5, (100 x^3 + x)^.5}, {x, -2, 2}]
```

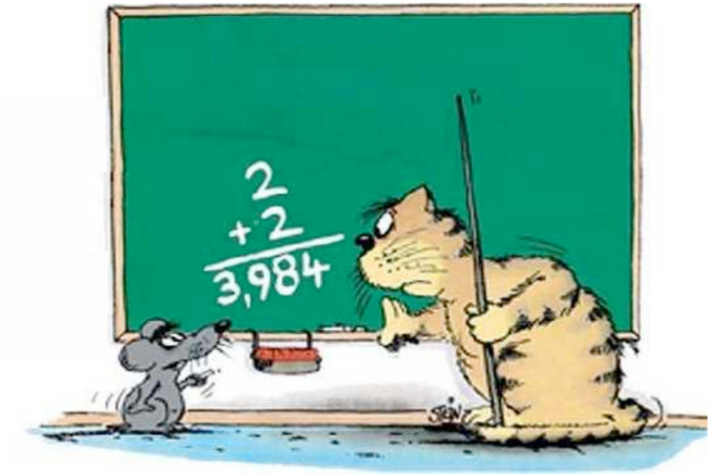


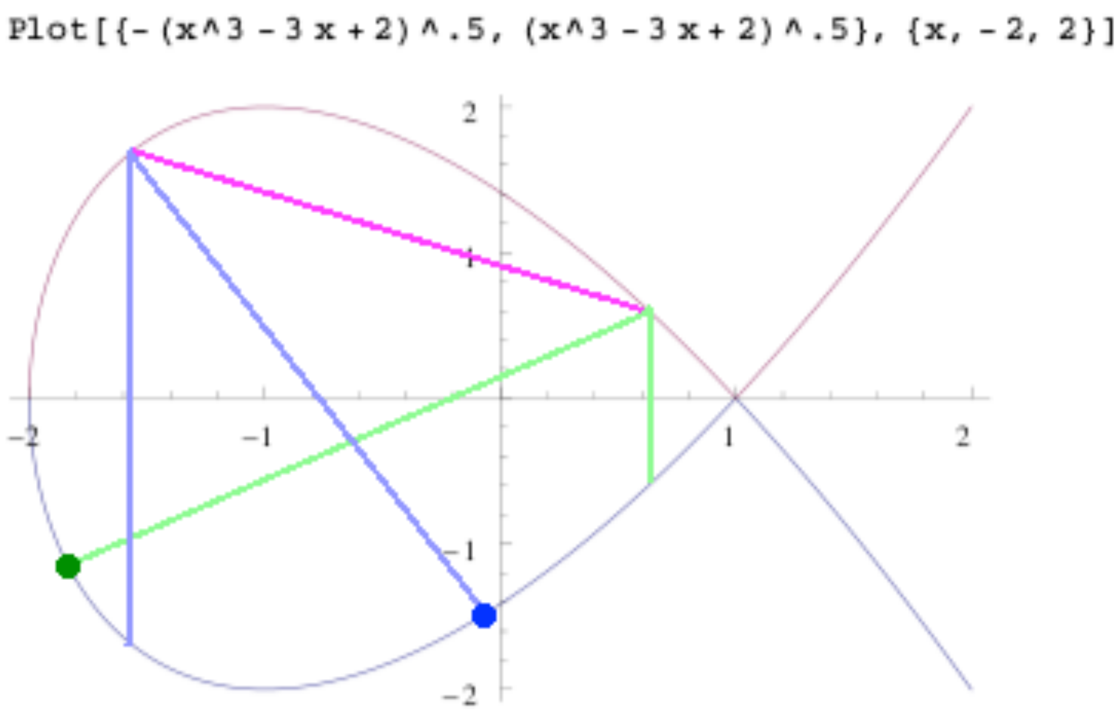

```
Plot[{-(x^3 - 3 x + 2)^.5, (x^3 - 3 x + 2)^.5}, {x, -2, 2}]
```



ADDING POINTS!

- Adding points is not the same addition as 1+1=2.
- The addition of points is the production of a third point using two already known points
- Properties of addition
  - Closure
  - Associativity
  - Existence of inverse
  - Existence of identity
  - Commutativity



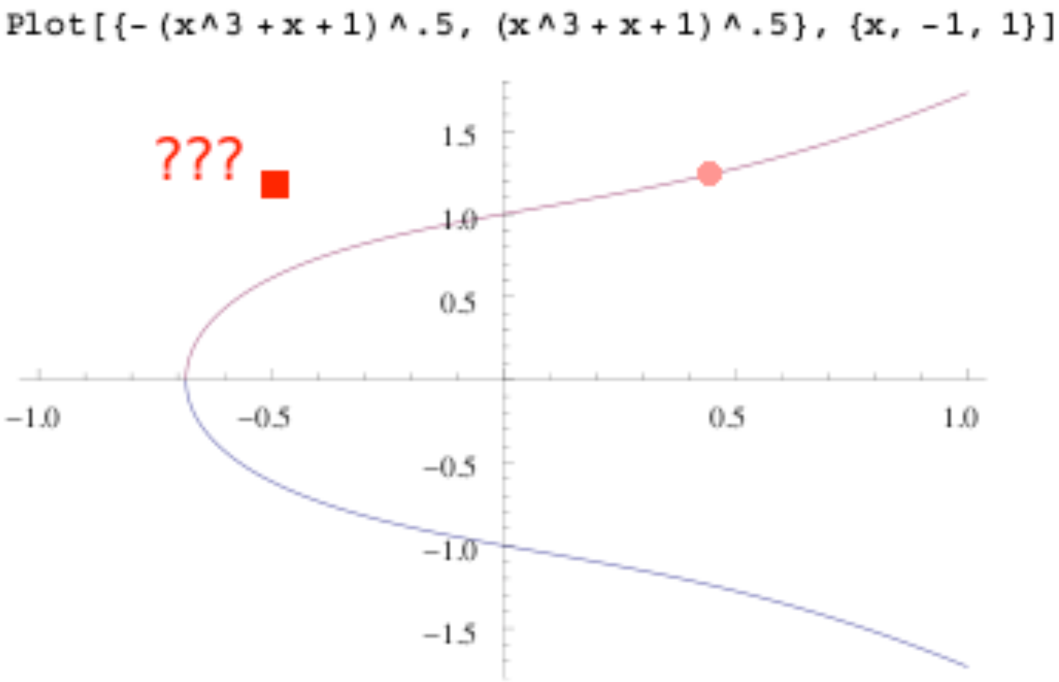


) 1

Angle bisector method –

- Reflect one of the points across the x-axis
- Connect the 3 points together
- Draw and extend the line that bisects the angle formed by the 3 points

This method did not work because it was not commutative or associative. Which of the 2 points



) 2

Rotation method –

- Rotate the point through an arbitrary angle.

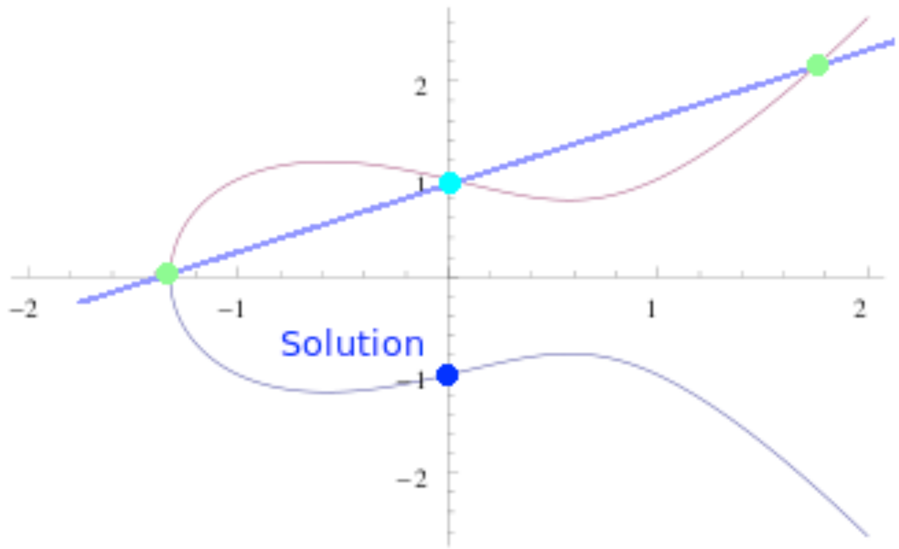
Rotation and flip across the y-axis violated closure, since the point no longer lies on the curve.

Special Case: Flipping

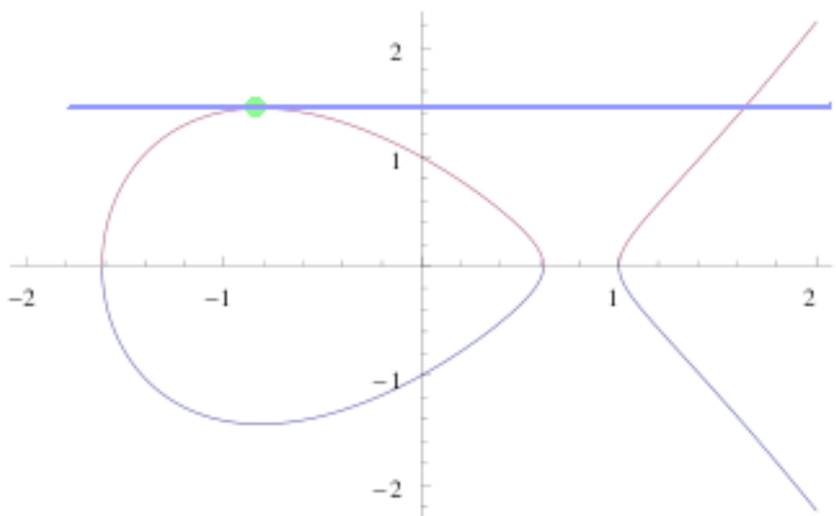
CORRECT SOLUTION!

- Given two points, connect them and extend the line. The solution point is the third point the line intersects on the elliptic curve reflected across the x-axis.
- Special Cases:
  - For lines that are tangent to the curve, the points where the lines are tangent to the curve count as two points.
  - If the 2 points have the same x values, then a vertical line is formed. Because the 2 points are inverses, the solution is the identity.

```
Plot[{- (x^3 - x + 1) ^ .5, (x^3 - x + 1) ^ .5}, {x, -2, 2}]
```




```
Plot[{- (x^3 - 2 x + 1) ^ .5, (x^3 - 2 x + 1) ^ .5}, {x, 2, -2}]
```



ALGEBRAIC FORM OF ADDITION

$$y^2 = ax^3 + bx + c$$

$$(x_1, y_1) \star (x_2, y_2) = (x_3, y_3)$$

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) = \frac{y_2 - y_1}{x_2 - x_1}x + \frac{y_2 - y_1}{x_2 - x_1}x_1 + y_1$$

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1}$$

$$\beta = \frac{y_2 - y_1}{x_2 - x_1}x_1 + y_1$$

$$y = (\alpha x + \beta)$$

$$(\alpha x + \beta)^2 = ax^3 + bx + c$$

$$\alpha^2 x^2 + 2\alpha\beta x + \beta^2 = ax^3 + bx + c$$

$$0 = ax^3 - \alpha^2 x^2 + (b - 2\alpha\beta)x + c - \beta^2$$

Using Vieta's Formula:

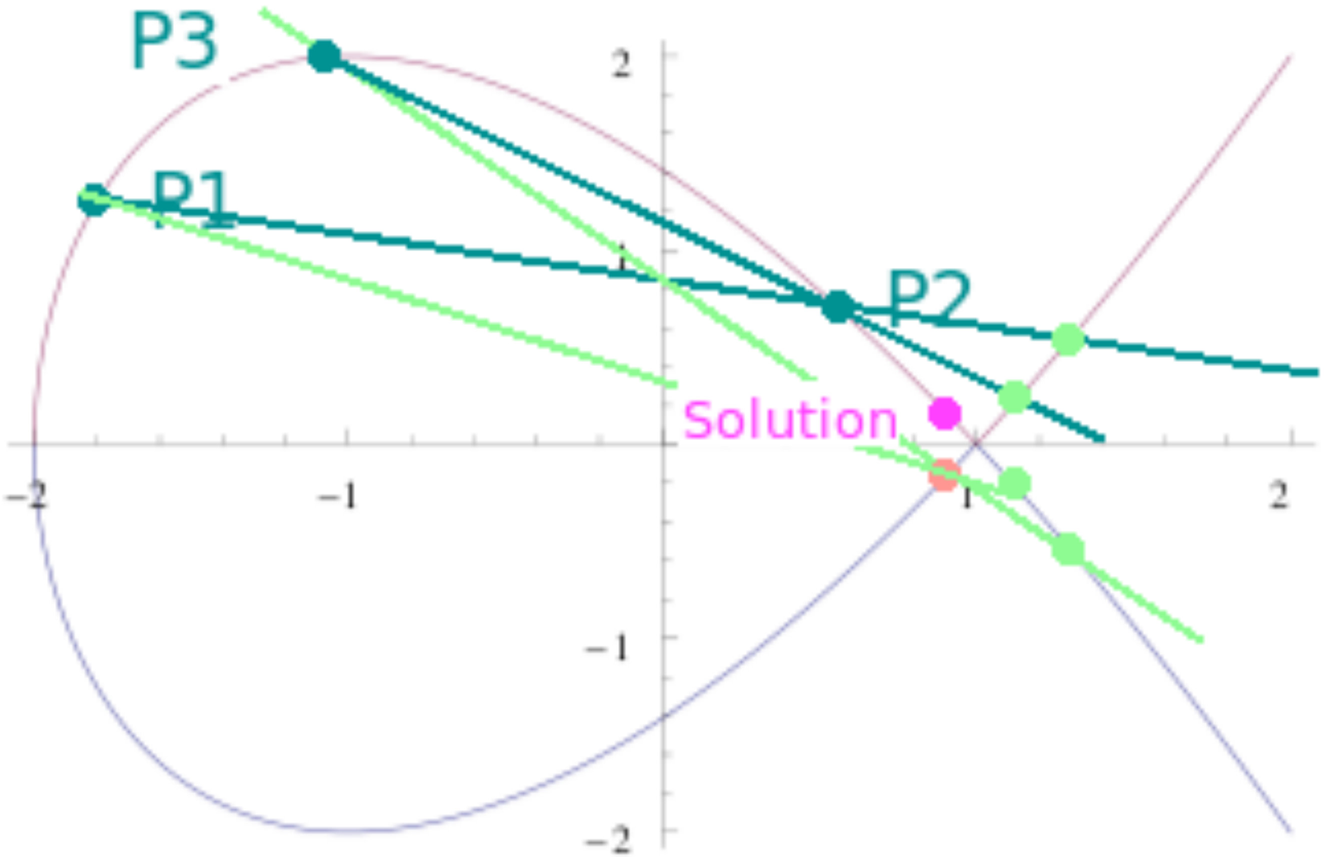
$$x_1 + x_2 + x_3 = -\frac{-\alpha^2}{a} = \frac{\alpha^2}{a}$$

$$x_3 = \frac{\alpha^2}{a} - (x_1 + x_2)$$

$$y_3 = \alpha((x_1 + x_2) - \frac{\alpha^2}{a}) - \beta$$

ASSOCIATIVITY

Plot[{-(x^3 - 3 x + 2)^.5, (x^3 - 3 x + 2)^.5}, {x, -2, 2}]



CLOSURE

Closure:

Given 2 points (x_1, y_1) and (x_2, y_2) on an elliptic curve, the line connecting them intersects the curve at a third point (x_3, y_3). This is because $y \to \infty$ as $x \to \infty$ and the graph has a curvature, so the straight line can't be parallel to it, so it must intersect.

Reflect (x_3, y_3) over x-axis to obtain final point. Because on the elliptic curve, there is x-axis symmetry, so there is closure (2 points map to 3rd point)

EXISTENCE OF IDENTITY

Given (x_1, y_2) and $(x_1, y_2) = (x_1, \infty)$

Line: $x - x_1 = \frac{x_2 - x_1}{y_2 - y_1}(y - y_1)$

$x = \frac{x_2 - x_1}{y_2 - y_1} y + x_1$

$x = \frac{0}{\infty - y_1} y + \frac{0}{\infty - y_1} y_1 + x_1$

Note: $\frac{0}{\infty - y_1} = 0$

$x = x_1$ and $y = -y_1$

Thus, since the third point of intersection is $(x, -y_1)$, the solution is (x, y_1), which is what we started with. Therefore ∞ is the identity.

The reason we must reflect the point by the x-axis is so we have an identity.

EXISTENCE OF INVERSE

Given two points (x_1, y_1) and (x_2, y_2) so that $x_1 = x_2$ and $y_2 = -y_1$

Then, $y_3 = \alpha(x_1 + x_2 - \frac{\alpha^2}{a}) - \beta$

$\alpha = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-2y_2}{0} \to \infty$

Since ∞ is the identity,(x_1, y_1) and (x_2, y_2) are inverses.

COMMUTATIVITY

$x_3 = \frac{\alpha^2}{a} - (x_1 + x_2)$

$\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ is the same no matter which order the 2 points are imputed, since it's the same line.

The order of $(x_1 + x_2)$ does not matter since adding is commutative.

Thus, x_3 is the same even if x_1 and x_2 are flipped.

$y_3 = \alpha((x_1 + x_2) - \frac{\alpha^2}{a}) - \beta$

As above, α and $x_1 + x_2$ are commutative. β is also commutative b/c the line remains the same regardless of the order of the 2 points.

Thus, y_3 is the same if (x_1, y_1) and (x_2, y_2) are switched.

Therefore, $\star$ is commutative.

A Brief Review of Groups

- **Groups**: sets with the following properties
  - Closure
  - Associative
  - Identity
  - Inverse
- Abelian Group: a group that is commutative

A Brief Introduction to Rings and Fields

- **Rings:** sets with the following properties
  - Abelian under "addition"
  - Not groups under "multiplication": have all properties except inverse
  - Distributive property
  - Ex: **Z ={…−4,−3,−2,−1,0,1,2,3,4,…}**
- **Fields:** sets with the following properties
  - Group under addition
  - Isn't group under multiplication but would be if 0 were removed (because 0 has no inverse)
  - Distributive
  - Ex: **Q, Fp**

Cryptography

Group of points $E(\mathbf{F}_p)$

over finite field Fp

on elliptic curve

$$Q = \underbrace{P+P+P+P+P+.....+P}_{\substack{\text{adding same point P} \\ \text{to itself "n" times}}} = nP$$

Cryptography

- **Public key**: can be seen by everyone
  - large prime p (for $\mathbf{F}_p$)
  - equation for elliptic curve E over $\mathbf{F}_p$
  - coordinates of point P in E($\mathbf{F}_p$)

- **Private key:** can only been seen the senders of the message (Alice and Bob)

Private Key

Alice	Bob
Picks a secret integer n_a	Picks a secret integer n_b
Calculates $n_aP = Q_a$	Calculates $n_bP = Q_b$

Alice sends Q_a to Bob.

Bob sends Q_b to Alice.

Private Key

Alice	Bob
Calculates n_aQ_b	Calculates n_bQ_a

SHARED SECRET KEY

$$n_aQ_b = n_a(n_bP) = (n_aP)n_b = Q_an_b$$

THE END