MATH 314 Spring 2018 - Class Notes

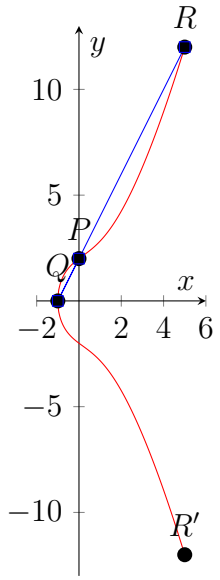
12/05/2018

Scribe: Kyle Clabough

Summary: This class we began working with elliptic curves and introduced to the Mordell Weil Theorem.

Notes:

$y^2 = x^3 + ax + b$
$P = (x_1, y_1)$
$Q = (x_2, y_2)$
$R = (x_3, y_3)$
$R' = P + Q$



To do addition using points on an elliptic curve, We need equations to find the coordinates of the point we get by adding P and Q.

$$P = (x_1, y_2), Q = (x_2, y_2)$$

We first need to find the slope, m, of the line connecting P and Q

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

the line has the equation: $y = m * x + c$
(x_3, y_3) needs to satisfy both $y = m * x + c$ and $y^2 = x^3 + a * x + b$
so, x_3 must satisfy:

$$(mx_3 + c)^2 = (x_3)^3 + ax_3 + b$$

$$(mx + c)^2 = (x)^3 + ax + b$$

$$m^2x^2 + 2mcx + c^x = (x)^3 + ax + b$$

$$0 = x^3 - m^2x^2 + (a - 2cm)x + b - c^2$$

$$0 =)(x - x_1)(x - x_2)(x - x_3)$$

now match up the coefficients of x^2

$$-m^2 = -x_1 - x_2 - x_3$$

$$m^2 = x_1 + x_2 + x_3$$

This gives us the equation:

$$x_3 = m^2 - x_1 - x_2$$

for the x-coordinate for R

Plug this into the equation for the line $y_3 = y_1 - m(x_1 - x_3)$

$$R = (x_3, y_3)$$

$$R' = (x_3, -y_3) = P + Q$$

$$P(x_1, y_1)$$

$$Q(x_2, y_2)$$

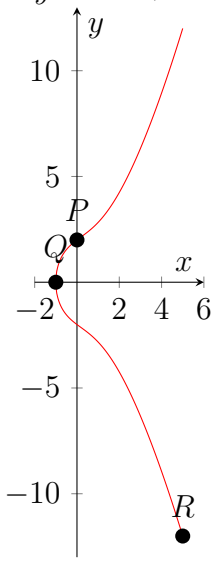
$$R' = P + Q = (x_3, y_3)$$

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

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

Ex: $y^2 = x^3 + 3x + 4$



$$P = (-1, 0)$$

$$Q = (0, 2)$$

what is $P + Q$?

$$m = \frac{2 - 0}{0 - (-1)}$$

$$m = \frac{2}{1} = 2$$

$$x_3 = m^2 - x_1 - x_2$$

$$x_3 = 2^2 - (-1) - 0$$

$$x_3 = 4 + 1$$

$$x_3 = 5$$

$$y_3 = 2(-1 - 5) - 0$$

$$y_3 = -12$$

$$R = (5, -12)$$

This doesn't work if $x_1 = x_2$. So, We add a new point to our curve, ∞

If Q and Q' have the same x-coordinate then we define $Q + Q' = \infty$

What if we add ∞ to another point on the curve?

$P + \infty = P$ for every P

To add $Q + Q$, we define the tangent line to, the curve at Q and use that line instead.

If $P \neq Q$, then $P + P$ and

$$m = \frac{3x_1 + b}{2y_1}$$

Let's compute:

$$Q + Q$$

$$(0, 2) + (0, 2)$$

$$m = \frac{3(0) + 3}{2 * 2}$$

$$\frac{3}{4}$$

$$x_3 = (\frac{3}{4})^2 - 0 - 0 = \frac{9}{16}$$

$$y_3 = \frac{3}{4}(0 - \frac{9}{16}) - 2$$

$$y_3 = \frac{-27}{64} - 2 = \frac{-155}{64}$$

$$R = (\frac{9}{16}, \frac{-155}{64})$$

Mordell Weil Theorem

Take all points on an Elliptic Curve, over rationals, there is a finite list of points on the curve that we can write andy point as a sum of those points