# Eliptic Curves Continued 12/5

Kayla Jurew

December 13, 2023

Last class we were working on the following example: Eliptic curve: $y^2 = x^3 + 2x + 4$ with the two points $p(0,2)$ and q(-1,1)

To add P+Q we do the following:

$$Since$$

P $\neq Q$ we use the slope formula: $s = y_2 - y_1/(x_2 - x_1)$

$$s = 1 - 2/-1 - 0$$

$$= -1/1$$
$$= 1$$

The formula to find our $x_3$ is: s$^2 - x_1 - x_2$

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

The formula to find our $y_3$ is: $s(x_1 - x_3) - y_1$

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

$$-4$$

$$P + Q = (2, -4)$$

In the next example, if we want to do $(P+Q)+P$ we have the points $(1,-4)+(0,2)$ Step 1 is to find the slope using the regular slope formula since

$$P \neq Q$$

$$s = (-4 - 2)/(2 - 0) = -6/2 = -3$$

$$x_3 = (-3)^2 - 2 - 0 = 7$$

$$y_3 =_3 (2 - 7) - (-4)$$

$$= 15 + 4 = 19$$

$$(x_3, y_3) = (7, -4)$$

Then we add this new P to our original P to complete the formula:

$$(7, -4) + (1, -4) : P \neq P$$

$$s = (-4 - (-4))/(1 - 7) = -8/ - 6 = -4/3$$
$$x_4 = (-4/3)^2 - 7 - (-4) = (16/9) - 3 = (-11/9)$$
$$y_4 = -4/3(7 - (-11/9)) - (-4) = -4/3(188/36) = -4/3(47/9) = (-188/27)$$
$$(x_4, y_4) = ((11/9), (-188/27))$$

For cryptography, we do all the same arithmetic mod $p$ Hasse's Theorem: if $E$ is any elliptic curve (mod $p$) the number of points on E (#E) is between p+1-2 $\sqrt{p} < \#E < p + 1 + 2\sqrt{p}$