MATH 178 Homework #12

Tamir Enkhjargal

May 2019

Elliptic Curve Cryptography

1.

Our EC is $y^2 = x^3 + 17$. This means $a_1 = 0,\ a_3 = 0,\ a_2 = 0,\ a_4 = 0,\ a_6 = 17$.

Add $[-2, 3]$ to $[2, -5]$ in the EC.

$$m = \frac{(-5) - 3}{2 - (-2)} = -2 \tag{1}$$

$$y = ax + b \to 3 = -2x + b \to y = -2x - 1 \tag{2}$$

$$\text{Solve for } y^2 = x^3 + 17 \text{ and } y = -2x - 1 \tag{3}$$

$$0 = (x + 2)(x - 2)(x - 4) \tag{4}$$

$$y = -2(4) - 1 \to y = -9 \tag{5}$$

Therefore, $[-2, 3] + [2, -5] + [4, -9] = 0$.

$[-2, 3] + [2, -5] = -[4, -9]$. $y^2 = 4^3 + 17 = 81,\ y = -9, 9$.

$[-2, 3] + [2, -5] = [4, 9]$

Using the equation, $\lambda = \frac{-5-3}{2-(-2)} = -2$. $\nu = \frac{3*2-(-5*-2)}{2-(-2)} = -1$.

$x_3 = (-2)^2 - (-2) - 2 = 4$. $y_3 = -(-2)4 - (-1) = 9$

$[-2, 3] + [2, -5] = [4, 9]$

2.

To double the point $[-2, 3]$, begin with implicit differentiation.

$$y^2 = x^3 + 17 \tag{1}$$

$$\frac{d}{dx}(y^2) = \frac{d}{dx}(x^3 + 17) \tag{2}$$

$$2y\frac{dy}{dx} = 3x^2 \tag{3}$$

$$\frac{dy}{dx} = \frac{3x^2}{2y} \tag{4}$$

At the point $[-2, 3]$, the slope becomes $\frac{3*4}{2*3} = 2$. Finding the line, $y = 2x + 7$.

Solving the equations, $y = 2x + 7$ and $y^2 = x^3 + 17$, $0 = (x + 2)^2(x - 8)$. $x = 8,\ y = 2 * 8 + 7 = 23$. Therefore $2[-2, 3] + [8, 23] = 0$. $-[8, 23] = [8, -23]$.

$2[-2, 3] = [8, -23]$

3.

```
e=[0,0,0,0,17]

q=[-2,3]

r=[2,5

2q=ellpow(e,q,2)=[8,-23]

q+r=elladd(e,q,r)=[1/4,-33/8]

3q=ellpow(e,q,3)=[19/25,522/125]

4q=ellpow(e,q,4)=[752/529,-54239/12167]

2r=ellpow(e,r,2)=[-64/25,59/125]

q-r=ellsub(e,q,r)=[4,9]

2q-r=ellsub(e,q2,r)=[-1,-4]

3q-r=ellsub(e,q3,r)=[52,375]

4q-r=ellsub(e,q4,r)=[-206/81,541/729]

2q-2r=ellsub(e,q2,r2)=[-8/9,109/27]
```