MAC260 Elliptic Curves

Week 4 Problem Class

2.
$$f(x) = x^3 + ax + b$$

We defined $\Delta = -4a^3 - 27b^2$

Suppose f has roots x_0, x_1, x_2

(a) Write a and b in terms of x_0, x_1, x_2.

Solution:
$$f = (x - x_0)(x - x_1)(x - x_2)$$

Multiplying out: coefficient of x equals
$$x_0 x_1 + x_0 x_2 + x_1 x_2$$

So $a = x_0 x_1 + x_0 x_2 + x_1 x_2$

$$\left(= \sigma_2(x_0, x_1, x_2) \right).$$

Also, constant term in f equals

$-x_0 x_1 x_2$, so $b = -x_0 x_1 x_2$

$$\left(= -\sigma_3(x_0, x_1, x_2) \right).$$

What is $x_0 + x_1 + x_2$? $= 0$: $\to$ coeff of x^2

(b) Show

$$\Delta = (x_0 - x_1)^2 (x_0 - x_2)^2 (x_1 - x_2)^2$$

Solution: Know $x_2 = -x_0 - x_1$

So $a = x_0 x_1 + x_0 x_2 + x_1 x_2$

$= x_0 x_1 + x_0(-x_0 - x_1) + x_1(-x_0 - x_1)$

$= -x_0^2 - x_1^2 - x_0 x_1$

$b = -x_0 x_1 x_2$

$= -x_0 x_1 (-x_0 - x_1)$

$= x_0^2 x_1 + x_0 x_1^2$

So $\Delta = -4a^3 - 27b^2$

$= -4(-x_0^2 - x_1^2 - x_0 x_1)^3 -$

$27(x_0^2 x_1 + x_0 x_1^2)^2$ (*)

On the other hand:

$(x_0 - x_1)^2 (x_0 - x_2)^2 (x_1 - x_2)^2$

$= (x_0 - x_1)^2 (2x_0 + x_1)^2 (x_0 + 2x_1)^2$ (**)

Both expressions are homog. of degree 6 in x_0, x_1, and symmetric.

So it's enough to show that coefficients of

$$x_0^6, \quad x_0^5 x_1, \quad x_0^4 x_1^2, \quad x_0^3 x_1^3$$

agree in the 2 expressions.

<u>Remark:</u> this gives another proof that $\Delta = 0$

$\Leftrightarrow$ two roots are the same.

<u>Q3:</u> $y^2 = x^3 + 73$

$P = (2, 9)$.

<u>Formulae from lectures:</u> Say $P = (x_0, y_0)$

Then $2P = (x_1, -y_1)$

where $x_1 = (m')^2 - 2x_0$

where $m' = \left(\frac{3x^2}{2y}\right)\Big|_{(x_0, y_0)}$,

$y_1 = y_0 + m'(x_1 - x_0)$.

So:

$$m' = \frac{3(2)^2}{2\cdot 9} = 2/3$$

$$\therefore \quad x_1 = (2/3)^2 - 2\cdot 2$$

$$= 4/9 - 4 = -32/9.$$

$$y_1 = 9 + 2/3(-32/9 - 2)$$

$$= 9 + 2/3(-50/9)$$

$$= 9 - 100/27 = 143/27$$

So $2P = \left(-32/9, -143/27\right)$

$3P = 2P \oplus P$

Formula: if $P = (x_0, y_0)$
$2P = (x_1, y_1)$ $\quad (x_0 \neq x_1)$

Then let $m = \dfrac{y_1 - y_0}{x_1 - x_0}$ $\quad x_0 = 2 \quad x_1 = -32/9$
$y_0 = 9, \; y_1 = \dfrac{-143}{27}$

Then let $x_2 = m^2 - x_0 - x_1$
$y_2 = y_0 + m(x_2 - x_0)$

Then $3P = (x_2, -y_2)$
$= \left(5111/625, -\dfrac{389106}{15625}\right).$

4. $C_t : Y^2 Z = tX^3 - XZ^2 - Z^3$

(a) Find t s.t. C_t not elliptic curve.

- If $t=0$, RHS not cubic in X

$\therefore$ not an elliptic curve.

So suppose $t \neq 0$.

Dehomogenise to get

$$y^2 = tx^3 - x - 1.$$

Convert to Weierstrass form: put $x = x'/t$, $y = y'/t$

to get $(y')^2 = (x')^3 - tx' - t^2$

Write as $y^2 = x^3 - tx - t^2$.

Weierstrass form: discriminant is

$$\Delta = -4a^3 - 27b^2 \quad \begin{pmatrix} a = -t \\ b = -t^2 \end{pmatrix}$$
$$= 4t^3 - 27t^4$$

$t \neq 0$: $\Delta = 0 \iff t = 4/27$.

So ~~t~~ ~~is~~ C_t is not an elliptic curve $\iff$ $t = 0$ or $t = 4/27$.