Problem 1. ***Week 1 - 9.)***

Let $E : y^2 = x^3 + Ax + B$.

(a) Find a polynomial in x *whose roots are the* x*-coordinates of the point* $P = (x, y)$ *satisfying* $3P = \infty$ *(Hint. The relation* $3P = \infty$ *can also be written* $2P = -P$*.)*

(b) For the particular curve $E : y^2 = x^3 + 1$*, solve the equation from part (a) to find all points of* E *satisfying* $3P = \infty$*.*
Note that you will need to use complex numbers.

Solution.
The obvious idea following the hint is to express $2P$ using the duplication formula and express it in the equation $2P = -P$.

(a) Points P x-coordinate is calculated as following: $\left(\frac{3x_P^2+A}{2y_P}\right)^2 - 2x_P$. We know that point $-P$ is just a reflection against x-axis, namely $-P = (x_P, -y_P)$. That gives us something to work with:

$$\left(\frac{3x_P^2 + A}{2y_P}\right)^2 - 2x_P = x_P$$

.

$$\frac{9x_P^4 + 6Ax_P^2 + A^2}{4y_P^2} = 3x_P$$

. Assuming that $y_P \neq 0$, we get

$$9x_P^4 + 6x_P^2 A + A^2 = 12x_P y_P^2$$

Considering the fact that P is a point on an elliptic curve, we know that $y_P^2 = x_P^3 + Ax_P + B$.
That gives us:

$$9x_P^4 + 6Ax_P^2 + A^2 = 12x_P(x_P^3 + Ax_P + B)$$
$$9x_P^4 + 6Ax_P^2 + A^2 = 12(x_P^4 + Ax_P^2 + Bx_P)$$
$$-3x_P^4 - 6Ax_P^2 - 12Bx_P + A^2 = 0$$

or if we multiply by -1 to have a bit more positive parameters :)

$$3x_P^4 + 6Ax_P^2 + 12Bx_P - A^2 = 0$$

.

This polynomial $f(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$ is the one whose roots satisfy the $3P = \infty$.

(b) Given $y^2 = x^3 + 1$, we see that $A = 0, B = 1$. That simplifies our polynomial into

$$f(x) = 3x^4 + 12x$$

. Starting our hunt for zeroes, we can clearly divide the whole equation by 3, and perform some minor grouping

$$x(x^3 + 4) = 0$$

Obviously,

$$x_1 = 0$$

is one solution and gives us the first two points such that $3P = \infty$, point $P_1 = (0, 1)$, and $P_2 = (0, -1)$.
Equation $x^3 = -4$ has three distinct roots (the real and two complex). Real one is

$$x_2 = -\sqrt[3]{4}$$

while the complex ones can be written like

$$x_{3,4} = \sqrt[3]{4}\left(\frac{1}{2} \pm \frac{\sqrt{3}}{2}i\right)$$

.

All these values give us two values for y, since from $x^3 + 4 = 0$, we can figure out that $x^3 + 1 = -3$, which means that our y values are $\pm\sqrt{3}$. This adds up six more points, namely:

$$P_{3,4} = \left(-\sqrt[3]{4}, \pm\sqrt{3}i\right), P_{5,6} = \left(\sqrt[3]{4}\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right), \pm\sqrt{3}i\right), P_{7,8} = \left(\sqrt[3]{4}\left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right), \pm\sqrt{3}i\right)$$

The last remaining point is the 'point at infinity', which we can mark by index P_9. $\square$

Problem 2. ***Week 2 - 7.)***

Let $E/\mathbb{Q}$ be an elliptic curve. Prove that $E(\mathbb{Q})_{tors}$ is finite.

Solution. Let $E : y^2 = x^3 + Ax + B$ be some elliptic curve over $\mathbb{Q}$.
From the Nagell-Lutz theorem, we know that if a point $P \in E(\mathbb{Q})_{tors}$ then two things are known about its coordinates:

1.) $x, y \in \mathbb{Z}$

2.) If $y \neq 0$, then $y^2 | \Delta$, where $\Delta = 4A^3 + 27B^2$.

As Δ is some element of $\mathbb{Z}$ it can have a finite set of divisors. Even more precisely, by the fundamental theorem of arithmetic, we can write $\Delta = \prod_i p_i^{q_i}$, where $p_i \in \mathbb{P}$, $\mathbb{P}$ being the set of all prime numbers, and $q_i \in \mathbb{N}_{\nvdash}$. The exact count of options that y^2 can be is $\prod_i \left\lceil \frac{q_i}{2} \right\rceil$ (each p_i can be $0, 2, .., \left\lfloor \frac{q_i}{2} \right\rfloor$, and independently we can choose exponents for other primes.). That means that the set of y coordinates is finite. Each of the values of y can give no more than 3 different values for x since our elliptic curve becomes just a simple cubic equation. This implies that whole $E/\mathbb{Q}$ cannot be infinite. $\square$