Problem Sheet 2.

1. $y^2 = x^3 + 1$

$P = (2,3)$, $Q = (-1,0)$

$P \oplus Q = (0,-1)$.

(a) Calculate $P \oplus (P \oplus Q)$.

Solution: Let's write R for $P \oplus Q$, so $R = (0,-1)$.

To find $P \oplus R$ first find $\overline{PR}$.

This line has slope $\dfrac{-1-3}{0-2} = 2$

so its eqn is $y = 2x + c$

Plugging in e.g. coords of P we find $c = -1$.

So $\overline{PR}$ is $y = 2x - 1$.

To find $P * R$ we intersect $\overline{PR}$ with C.

Substitute eqn. of $\overline{PR}$ into $y^2 = x^3 + 1$:

get $(2x-1)^2 = x^3 + 1$

Roots of this cubic are x-coords of P, R, and $P * R$

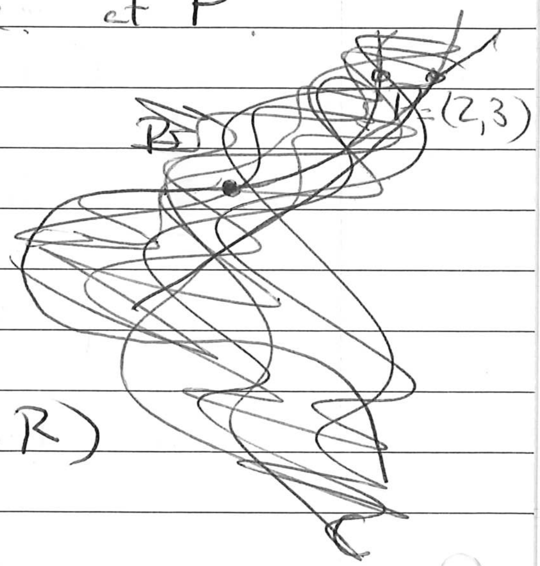
Rearrange to get

$$x^3 - 4x^2 + 4x = 0$$

Roots: $\underset{\uparrow \, R}{x = 0}$, $\underbrace{\overset{P}{x = 2}, \; x = 2}_{\text{double root.}}$

So the line $\overline{PR}$ intersect C with

mult. 2 at $x = 2$, i.e. at P.



So $P * R = P$.

$$= (2, 3)$$

Hence $P \oplus R = O * (P * R)$

$$= (2, -3).$$

So $P \oplus (P \oplus Q) = (2, -3)$.

(b) Eq'n of tangent line at P:

we just saw that $\overline{PR}$ is tangent to C at P, so the tangent line is $\overline{PR}$ with equation $y = 2x - 1$.

Alternatively: tangent line to C at P has slope $m = \left.\frac{3x^2}{2y}\right|_P$

$$= \frac{3(2)^2}{2(3)} = 2.$$

$y^2 = x^3 + 1$

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

So eqn is $y = 2x + c \rightarrow$ as before, plug in coords of P to find $c = -1$.

(c) Find $P \oplus P$: first find $P * P$

Know tangent line at P is the line $\overline{PR}$.

So $P * P = R = (0, -1)$

Hence $P \oplus P = (0, 1)$.

(d) Verify that

$$2P \oplus Q = P \oplus (P \oplus Q)$$

From Part (a) $P \oplus (P \oplus Q) = (2,-3)$

Let's compute $2P \oplus Q$

$$= (P \oplus P) \oplus Q.$$

From (c) we have $P \oplus P = (0,1)$

Know $Q = (-1,0)$

So $\overline{(P \oplus P)Q}$ is the line $y = x+1$.

Substitute into $y^2 = \cancel{}\ x^3 + 1$,

get $(x+1)^2 = x^3 + 1$

$\iff x^3 - x^2 - 2x = 0$.

$\iff x(x-2)(x+1) = 0$

So the point $(P \oplus P) * Q$

has x-coordinate $x = 2$

It also lies on the line $y = x+1$

$$\therefore \quad (P \oplus P) * Q = (2,3)$$

$$\therefore \quad (P \oplus P) \oplus Q = (2,-3)$$

$$= P \oplus (P \oplus Q)$$

(e) $aP \oplus bQ \quad (a, b \in \mathbb{Z})$?

First of all: $Q = (-1,0)$

$$\therefore \quad \mathcal{O} * Q = (-1,0)$$

$$\therefore \quad \mathcal{O} = \underbrace{Q \oplus (\mathcal{O} * Q)}_{\mathcal{O} * Q \text{ is additive inverse of } Q} = Q \oplus Q$$

$$= 2Q$$

[Q is called a "2-torsion" point].

So $-Q = Q$ and in general for any $k \in \mathbb{Z}$, $kQ = \bar{k}Q \quad \bar{k} = k \bmod 2$

We also found that

$$2P \oplus Q = (2,-3) = -P$$

so $3P \oplus Q = \mathcal{O}$.

$3P \oplus Q = \mathcal{O}$

Add Q to both sides:

$3P = Q$

Double both sides:

$6P = 2Q = \mathcal{O}$

(Found $2P = (0,1)$ already)

So $4P = -2P = (0,-1)$

$5P = -P = (2,-3)$.

In general: $kP = \overline{k}P$

where $\overline{k} = k \mod 6$.

So finally: for $a, b \in \mathbb{Z}$,

$aP \oplus bQ = (a+3b)P$

$= \overline{(a+3b)}P$

where $\overline{a+3b} = a+3b \mod 6$.