NMMB430 - DÚ 3

Jan Oupický

1

We will proceed by calculating $[2]P, [2]P + [2]P = [4]P$ (doubling) and finally $[4]P + P = [5]P$ (addition).

$[2]P$:

$$\gamma_1 = 20, \gamma_2 = 5, \gamma_3 = 8$$
$$\implies [2]P = (20 : 5 : 8)$$

$[4]P$:

$$\gamma_1 = 18, \gamma_2 = 4, \gamma_3 = 4$$
$$\implies [4]P = (18 : 4 : 4)$$

$[4]P + P$:

$$U = 0, W = 0, V = 26$$
$$\implies [5]P = (0 : -4 : 4)$$

Since $4^{-1} = 8$ we get that $[5]P = (0 : -4 : 4) = (0 : -1 : 1)$ i.e. $[5]P = (0, -1) = (0, 30)$ in affine coordinates.