TEST 2

JASON MEDCOFF

1. Consider the curve $Y^2 = X^3 - 2X + 4$ and the points $P = (0, 2)$, $Q = (3, -5)$. Compute, by hand, $P \oplus Q$.

Solution. First, we obtain the equation of the line passing through P and Q as $y = -\frac{7}{3}x + 2$. Next, we want the intersections of this line with the curve, so set

$$\Big(-\frac{7}{3}x + 2\Big)^2 = x^3 - 2x + 4$$
$$0 = x^3 - \frac{49}{9}x^2 + \frac{22}{3}x$$

Clearly, $x = 0$ is a solution, so we divide by x.

$$0 = x^2 - \frac{49}{9}x + \frac{22}{3}$$

As we already know from point Q, $x = 3$ is also a solution so we use polynomial long division to obtain $x = \frac{22}{9}$. Then from the equation of the curve,

$$y^2 = (\frac{22}{9})^3 - 2(\frac{22}{9}) + 4$$

and we have that

$$y = \pm\sqrt{\frac{10000}{729}} = \pm\frac{100}{27}.$$

Plugging our $x = \frac{22}{9}$ into the line equation, we have the negative value, so the positive value gives the correct y for the new point. So the result of $P \oplus Q$ is $(\frac{22}{9}, \frac{100}{27})$.

2. Consider the cubic polynomial

$$x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$$

and show that $4a^3 + 27b^2 = 0$ if and only if two or more of e_1, e_2, e_3 are the same.

Solution. Recall from elementary algebra that the discriminant is a function of a polynomial's coefficients, that gives interesting properties of the polynomial. Namely the discriminant equals zero if and only if the polynomial has a multiple root. So, we will begin by finding the discriminant of the given polynomial.

If we expand $(x - e_1)(x - e_2)(x - e_3)$, we have

$$x^3 - x^2(e_1 + e_2 + e_3) + x(e_1e_2 + e_1e_3 + e_2e_3) - (e_1e_2e_3)$$

but clearly it must be that $(e_1 + e_2 + e_3) = 0$. Then make the substitution $e_3 = -e_1 - e_2$. Then we obtain

$$x^3 + x(-e_1^2 - e_1e_2 - e_2^2) + (e_1^2e_2 + e_1e_2^2) \tag{1}$$

and it is plainly clear how a and b are expressed in terms of the roots.

The discriminant for a cubic with roots e_1, e_2, e_3 is given by

$$\Delta_f := \prod_{i \neq j}(e_i - e_j) = (e_1 - e_2)(e_2 - e_1)(e_3 - e_2)(e_2 - e_3)(e_1 - e_3)(e_3 - e_1)$$

and since $e_3 = -e_1 - e_2$, we can make the substitution

$$\Delta_f = (e_1 - e_2)(e_2 - e_1)((-e_1 - e_2) - e_2)(e_2 - (-e_1 - e_2))(e_1 - (-e_1 - e_2))((-e_1 - e_2) - e_1).$$

Expanding yields

$$\Delta_f = -4e_1^6 - 12e_1^5 e_2 + 3e_1^4 e_2^2 + 26e_1^3 e_2^3 + 3e_1^2 e_2^4 - 12e_1 e_2^5 - 4e_2^6. \tag{2}$$

If we take $4a^3 + 27b^2$ and make the substitution for a and b shown in equation (1) in terms of the roots, we have

$$\begin{aligned} 4p^3 + 27q^2 &= 4(-e_1^2 - e_1 e_2 - e_2^2)^3 + 27(e_1^2 e_2 + e_1 e_2^2)^2 \\ &= -4e_1^6 - 12e_1^5 e_2 + 3e_1^4 e_2^2 + 26e_1^3 e_2^3 + 3e_1^2 e_2^4 - 12e_1 e_2^5 - 4e_2^6 \end{aligned}$$

which is precisely equation (2). Thus $4a^3+27b^2$ is the discriminant and it follows that $4a^3+27b^2 = 0$ if and only if two or more of e_1, e_2, e_3 are the same.