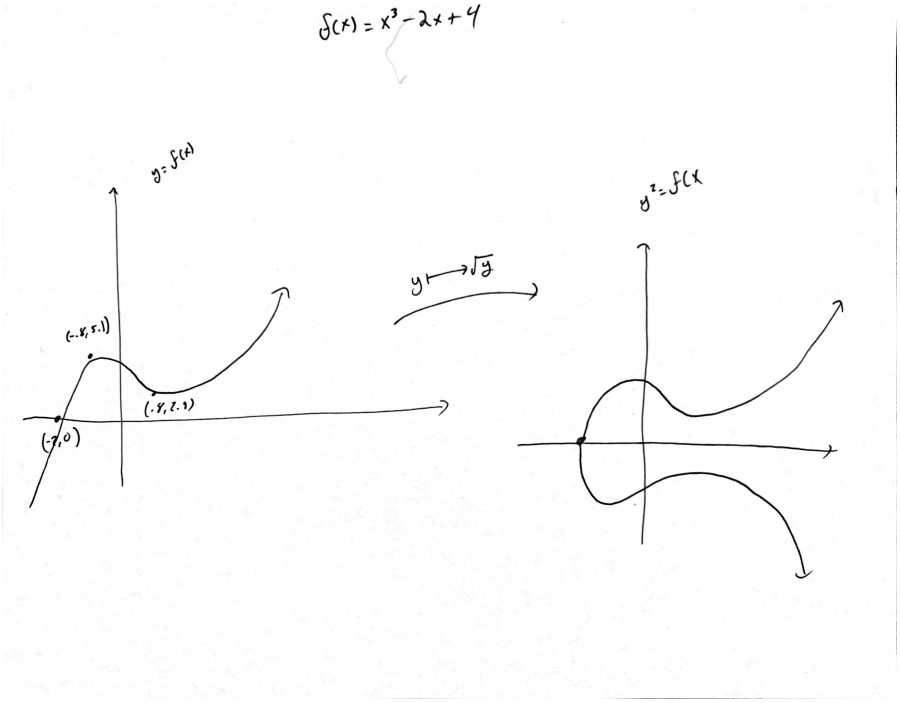
Homework 10 Written Solutions

Written Part

3. Graph the following curves over $\mathbb{R}$ in the following steps. Since each is of the form $y^2 = f(x)$ first draw a graph of $y = f(x)$ by finding its roots and critical points. Then deduce the shape of $y^2 = f(x)$ by taking square roots of the y coordinates (when you can). Which of them are elliptic curves?

   (a) $y^2 = x^3 - 2x + 4$

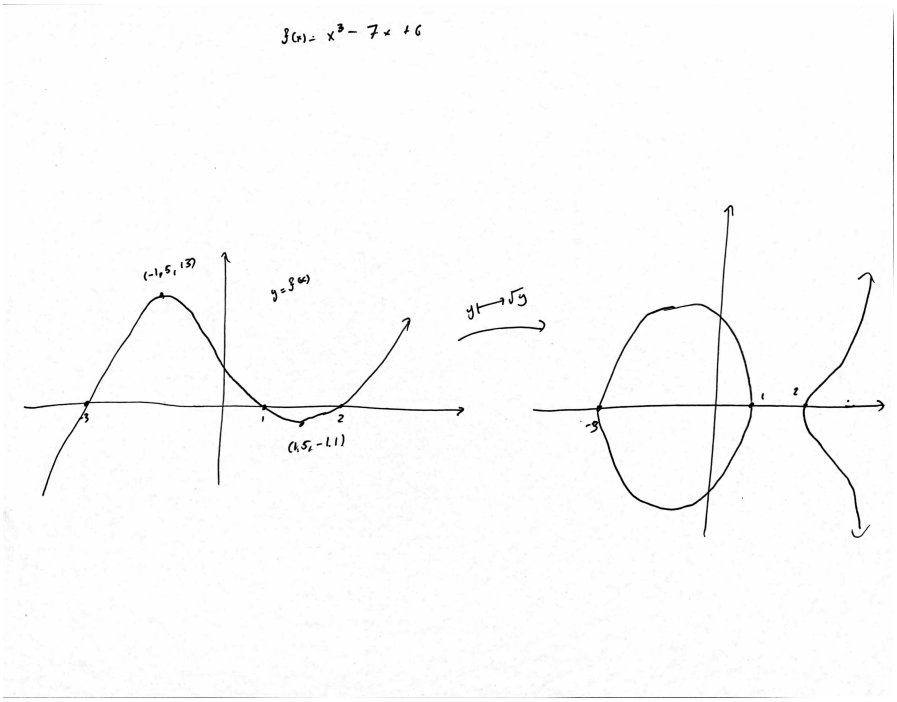
   Proof. Observe that $x^3 - 2x + 4 = (x+2)(x^2 - 2x + 2)$ so it has a single root $x = -2$. Further, $f'(x) = 3x^2 - 2$. Setting this equal to 0 gives critical points at the x-coordinates $x = \pm\sqrt{2/3} \approx \pm.8$. The associated y values are $f(-\sqrt{2/3}) \approx 5.1$ and $f(\sqrt{2/3} \approx 2.9$. Therefore the graphs of $y = f(x)$ and $y^2 = f(x)$ are:



   □

   (b) $y^2 = x^3 - 7x + 6$

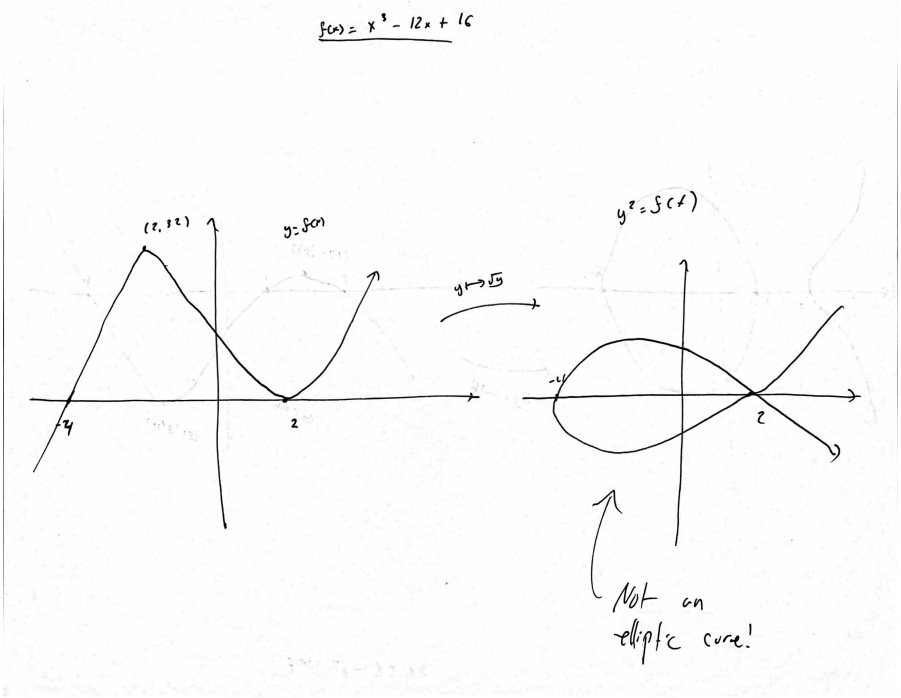
   Proof. $x^3 - 7x + 6 = (x+3)(x-1)(x-2)$ so that it has 3 roots at $x = -3, 1, 2$. Further, $f'(x) = 3x^2 - 7$, giving critical points at $x = \pm\sqrt{7/3} \approx \pm 1.5$. The y values are $f(-\sqrt{7/3}) \approx 13.1$ and $f(\sqrt{7/3}) \approx -1.1$. The graphs of $y = f(x)$ and $y^2 = f(x)$ are:



□

(c) $y^2 = x^3 - 12x + 16$

Proof. $x^3 - 12x + 16 = (x+4)(x-2)^2$, so that it has a root at 4 and a double root at 2. $f'(x) = 3x^2 - 12$ giving critical points at $x = \pm 2$. The associated y coordinates are $f(-2) = 32$ and $f(2) = 0$. The graphs of $y = f(x)$ and $y^2 = f(x)$ are therefore:



□

4. Consider the elliptic curve E over $\mathbb{R}$ given by the equation $y^2 = x^3 - 2x + 4$. Let $P = (0, 2)$ and $Q = (3, -5)$. Compute the following *by hand*, explaining the geometry behind each step.

   (a) Show $P, Q \in E$.

   Proof. Since $0^3 - 2 \cdot 0 + 4 = 4 = 2^2$, we confirm $P \in E$. Since $3^3 + 2 \cdot 3 + 4 = 27 - 6 + 4 = 25 = (-5)^2$, we confirm $Q \in E$. □

   (b) Compute $P \oplus Q$.

   Proof. We first compute the line between P and Q. The slope is $\frac{-5-2}{3-0} = -7/3$. Since P lies on it, the y intercept is 2. Therefore the line is $y = -\frac{7}{3}x + 2$. We intersect this with the elliptic curve. We do this algebraically by plugging it into the equation for $y^2 = \left(\frac{7}{3}x + 2\right)^2 = \frac{49}{9}x^2 - \frac{28}{3}x + 4$. Setting this equal to $x^3 - 2x + 4$ gives the following.

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

   where on the right side we use that the x-coordinates of P and Q are solutions. In particular, $-3 - \lambda = -\frac{49}{9}$ so that $\lambda = \frac{22}{9}$. This gives the x coordinate of $P \oplus Q$, to compute the y-coordinate we plug into the equation for a line to get:

$$y = -\frac{7}{3}\frac{22}{9} + 2 = -\frac{154}{27} + \frac{54}{27} = \frac{100}{27},$$

   and invert to get $P \oplus Q = \left(\frac{22}{9}, -\frac{100}{27}\right)$. □

   (c) Compute $P \oplus P$.

   Proof. We first compute the tangent line to P. We do this with implicit differentiation, noting that $2yy' = 3x^2 - 2$ so that $y' = \frac{3x^2-2}{2y}$. Plugging in the point $P = (0, 2)$ gives a slope of $-1/2$. Since it contains P we get the line $y = -\frac{1}{2}x + 2$. Now we intersect this with the elliptic curve, first by squaring to get $\frac{1}{4}x^2 - 2x + 4$. Setting this equal to the righthand side of the equation of the elliptic curve gives:

$$x^3 - \frac{1}{4}x^2 = x^2(x - \lambda),$$

   since we know the lines are tangent at P so that the x-coordinate 0 is a double root. In particular, we se that the x-coordinate of the third intersection point is $\lambda = 1/4$. Plugging back into the line we get:

$$y = -\frac{1}{2}\frac{1}{4} + 2 = \frac{15}{8},$$

   so that the point on the curve is $P \oplus P = \left(\frac{1}{4}, \frac{-15}{8}\right)$. □

   (d) Compute $P \oplus P \oplus P$.

Proof. We would like to add P and $2P$ (the latter computed in part (c) above). As usual, we begin by computing the slope, which is $\frac{-15/8-2}{1/4} = -31/2$. This gives the line $y = -\frac{31}{2}x + 2$. Squaring gives $\frac{961}{2}x^2 - 62x + 4$. Intersecting this with the curve again gives:

$$x^3 - \frac{961}{4}x^2 + 60x = x(x - \frac{1}{4})(x - \lambda),$$

where we know the x-coordinates of P and $2P$ are already roots. Therefore we may compute $\lambda + 1/4 = \frac{961}{4}$ so that $\lambda = 960/4 = 240$. Then the y coordinate is computed as:

$$y = -\frac{31}{2}240 + 2 = -3718,$$

so that $P \oplus P \oplus P = P \oplus 2P = (240, 3718)$. □

Recall that a curve given by an equation $y^2 = x^3 + ax + b$ is an elliptic curve if and only if the value $\Delta_E = 4a^3 + 27b^2 \neq 0$. This has to do with the right side of the equation having double roots, leading to nonuniqueness of tangent lines after taking square roots (cf. the graphs in question 3). Let's make this more precise.

5. Let $f(x) = x^3 + ax + b$ be a cubic equation, which factors over $\mathbb{C}$ as $(x - e_1)(x - e_2)(x - e_3)$. Show that $4a^3 + 27b^2 \neq 0$ if and only if the e_i are all distinct.

Proof. One can show this directly with a lot of tedious and painful algebraic manipulations, but it takes pages and is not particularly illuminating (at least not to me). Instead we will deduce the result from the following observation from calculus.

Proposition 1. *Let $p(x)$ be a polynomial. x_0 is a double root of $p(x)$ if and only if $p(x_0) = 0$ and $p'(x_0) = 0$.*

Proof. I won't require you to prove this fact since it was established calc 1, but I'll include a proof for the curious. Suppose x_0 is a double root. In particular, this means that $p(x)$ factors as $(x - x_0)^2 q(x)$ for some polynomial $q(x)$. Therefore $p'(x) = 2(x - x_0)q(x) + (x - x_0)^2 q'(x)$ so that x_0 is a root. Conversely, suppose x_0 is a root of $p(x)$ and $p'(x)$. Then we see that $p(x)$ factors as $(x - x_0)q(x)$ for some polynomial $q(x)$, and so $p'(x) = q(x) + (x - x_0)q'(x)$. Evaluating at x_0 and using that it is a root of $p'(x)$ shows that $q(x_0) = 0$, so that $q(x)$ factors as $(x - x_0)r(x)$ for some polynomial $r(x)$. In particular, we have shown that $p(x) = (x - x_0)^2 r(x)$ and therefore x_0 is a double root. This completes the proof of the proposition. □

With this in hand, we can prove the without several pages of calculations. Indeed, the proposition shows that $f(x)$ has a double root e if and only if $f(e) = f'(e) = 0$. Since $f'(e) = 0$, we deduce that $3e^2 + a = 0$ so that $a = -3e^2$. Since $f(e) = 0$ we therefore deduce that $e^3 + ae + b = e^3 - 3e^3 + b = b - 2e^3 = 0$ so that $b = 2e^3$. Then we compute:

$$\Delta = 4a^3 + 27b^2 = 4(-3e^2)^3 + 27(2e^3)^2 = -108e^6 + 108e^6 = 0.$$

Conversely, let $\Delta = 4a^3 + 27b^2 = 0$. We want to show that f and f' have a shared root, but this process will involve dividing by a, so let's first consider the case where $a = 0$. Then since $\Delta = 0$ we also have $b = 0$ and $f(x) = x^3$, and 0 is a double (indeed even a triple) root.

Now suppose $a \neq 0$. Notice $f'(x) = 3x^2 + a$ has roots $e = \pm\sqrt{-a/3}$. Since $\Delta = 0$ we can solve for:

$$\frac{-a}{3} = \frac{9b^2}{4a^2}.$$

Therefore we can solve for

$$e = \pm\sqrt{\frac{-a}{3}} = \pm\sqrt{\frac{9b^2}{4a^2}} = \pm\frac{3b}{2a}.$$

We will show that $e = -3b/2a$ is also a root of f. Indeed:

$$f(e) = \left(\frac{-3b}{2a}\right)^3 + a\cdot\frac{-3b}{2a} + b = \frac{-27b^3}{8a^3} - \frac{3b}{2} + b = \frac{-27b^3 - 3b * 4a^3 + b * 8a^3}{8a^3} = \frac{b(4a^3 - 27b^2)}{8a^3} = 0,$$

where in the last step again we use that $\Delta = 0$. Therefore we see that f and f' share a root, so that by the proposition, it is a double root, completing the proof. □