Written Assignment 6

MATH2144, Fall 2018

due Wednesday, the 10^{th} of October

Problem 1

This problem is about a special type of curve called an *elliptic curve*. These curves are used extensively in the most secure public protocols of cryptography. The following is a simple but interesting example of one.[1]

Let Γ be the elliptic curve given by

$$y^2 - x \cdot y + 2 \cdot y = x^3 + 2 \cdot x^2.$$

Exercise 1. Find equations of the tangent lines to Γ at the points $(0, 0)$, $(-2, 0)$, $(2, 4)$, $(0, -2)$, $(-2, -4)$, and $(2, -4)$.

Bonus 1. What is special about this curve and these lines, compared (for instance) with some other elliptic curve like

$$y^2 - x \cdot y + 2 \cdot y = x^3 + x^2?$$

[1] I worked out this example from slide 21 of the talk at `https://www.hyperelliptic.org/tanja/conf/summerschool08/slides/Elliptic-curves-over-Q.pdf`, which itself is just Table 3 from page 217 the paper "Universal bounds on the torsion of elliptic curves" by D. S. Kubert from 1976 in the Proceedings of the London Mathematical Society.

Problem 2

This problem is about how logarithms to base e are estimated by most computers.[2]

Definition 1. Two functions f and g are said to *agree to order n at a point a* when $f(a) = g(a)$, $f'(a) = g'(a)$, and so on, up until $f^{(n)}(a) = g^{(n)}(a)$. That is, for all natural numbers m up to and including n, $f^{(m)}(a) = g^{(m)}(a)$.

We begin with the easiest way to approximate fancy functions like ln, using what are called *Taylor approximations.* You may read about these more in section 10.7 of our text if you like.

Exercise 2. Let

$$p(x) = (x-1) - \frac{1}{2}\cdot(x-1)^2 + \frac{1}{3}\cdot(x-1)^3 - \frac{1}{4}\cdot(x-1)^4.$$

Show that p and ln agree up to order 4 at 1.

That is not how the standard `C` software "library" implements ln, though. Instead, let

$$L(w) = \ln\left(\frac{1+w}{1-w}\right).$$

Exercise 3. Show that L and $p_3(w) = 2\cdot(w + w^3/3)$ agree to order 3 at 0.

Exercise 4. Show that L and $p_5(w) = 2\cdot(w + w^3/3 + w^5/5)$ agree to order 5 at 0.

Exercise 5. Let $A(w) = (1+w)/(1-w)$, and let $B(x) = (x-1)/(x+1)$. Show that A and B are inverse functions.

Exercise 6. Plot graphs of L, p_3, and p_5 near 0.

Please plot the graphs over an interval where it is easy to tell where they are similar, and where they are different. For instance, don't plot them over $(-0.5, 0.5)$.)

Exercise 7. Plot graphs of ln, $p_3 \circ B$, and $p_5 \circ B$ near 1.

Please make the plot scaled logarithmically in the x-axis, and as before, pick an interval that makes the differences and similarities clear.

Bonus 2. Explain how the standard `C` library implements ln.[3]

[2] Cf. `http://www.netlib.org/cephes/qlibdoc.html#qlog`. Intel `x86` chips actually have a base-2 logarithm instruction, so for these chips, using the change-of-base formula for logarithms would probably be faster. Other chips abound, though—for instance, in 2010, 95% of smartphones had ARM chips.

[3] Cite any sources you use.