Math 445/845. Exam #2

(1) Definitions/Theorem statements

(a) Define the **norm function** on $\mathbb{Z}[\sqrt{D}]$ for some positive integer D that is not a perfect square.

(b) Define a **triangular number**.

(c) State **Lagrange's theorem** (about elements of groups).

(d) State the **Dirichlet's approximation theorem**.

(2) Computations.

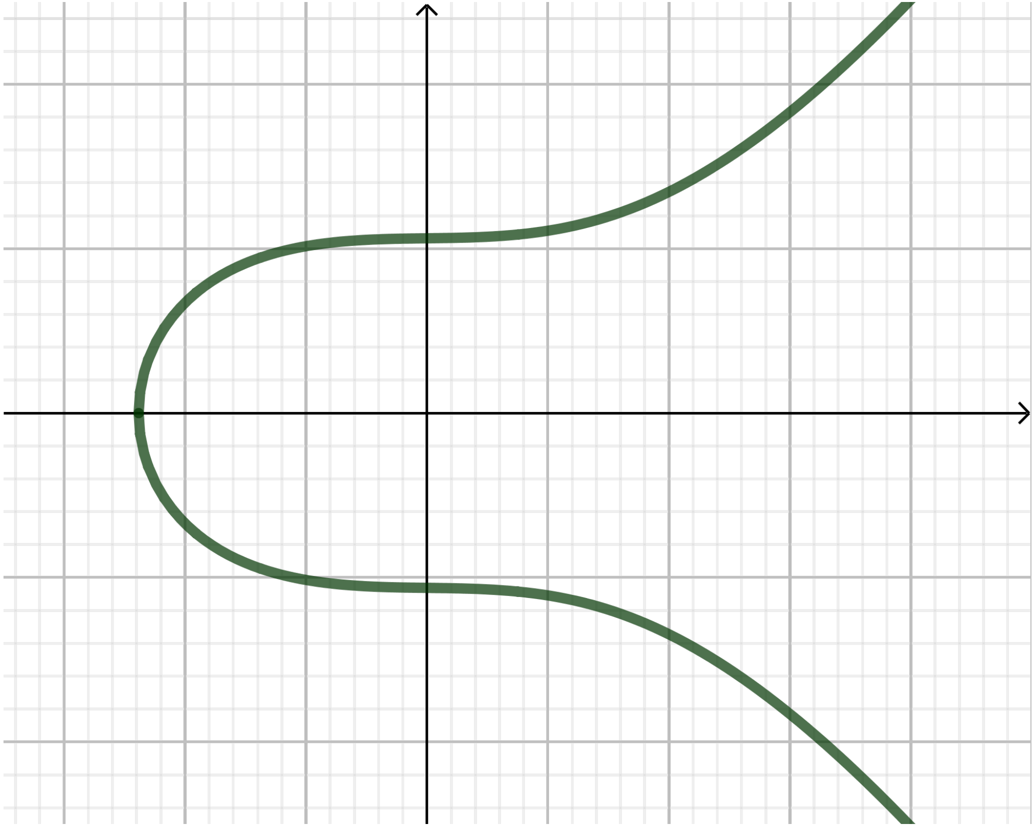
(a) (i) Compute the first two partial quotients (after the integer part) of $\sqrt{11}$.

(ii) Use your calculation from part (a) to give a rational approximation of $\sqrt{11}$. Using results from this class (and not using the decimal expansion from a calculator), what can you say about the accuracy of your approximation?

(b) Give an expression for the general integer solution of $x^2 - 11y^2 = 1$.

(c) The equation $y^2 = x^3 + 44x + 25$ defines an elliptic curve. Two rational solutions to the equation are $(0, 5)$ and $(2, 11)$. Their reflections over the x-axis are also solutions. Use the group law to find another rational solution besides these four.

(d) The picture below is part of the graph of an elliptic curve. Mark all points of order at most 4 in the depicted portion of the graph, and explain each.



(3) Proofs.

(a) Consider the equation

$$x^2 - Dy^2 = 2 \tag{†}$$

where D is some positive integer that is not a perfect square.

(i) Show that if the equation (†) has an integer solution $(x, y) = (a_0, b_0)$, then (†) has infinitely many integer solutions $(x, y) = (a, b)$.

(ii) Show that for $D = 83$, the equation (†) has no solution.

(b) Let $\overline{E}_p$ be an elliptic curve over $\mathbb{Z}_p$ given by the equation $y^2 = x^3 + [a]x + [b]$, where $p \geq 5$ is a prime. Suppose that $[c] \in \mathbb{Z}_p$ is a root of the polynomial $x^3 + [a]x + [b] = 0$.

(i) Show that there exists a point of order 2 in $\overline{E}_p$.

(ii) Use the group structure to show that the equation $y^2 = x^3 + [a]x + [b]$ has an odd number of solutions in $\mathbb{Z}_p \times \mathbb{Z}_p$.

Bonus: Show that for $\varphi = \dfrac{1+\sqrt{5}}{2}$ there do *not* exist infintiely rational numbers $\dfrac{p}{q}$ such that $\left|\varphi - \dfrac{p}{q}\right| < \dfrac{1}{q^3}$.