Math 445 — Problem Set #7
Due: Tuesday, November 14 by 7 pm, on Canvas

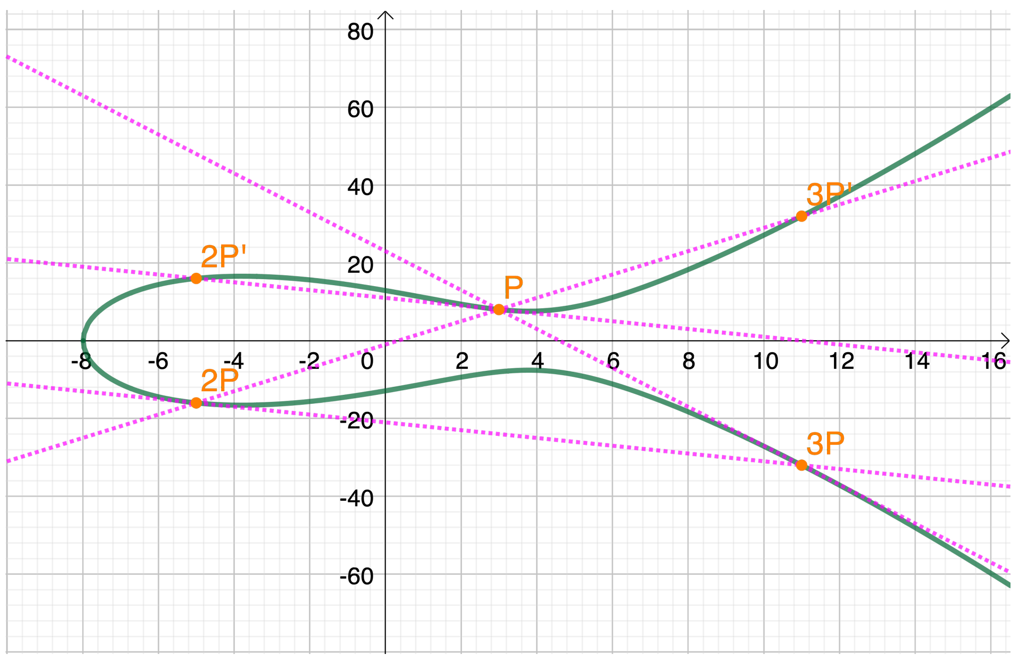
Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. If you do work with others, I ask that you write something along the top like "I collaborated with Steven Smale on problems 1 and 3". If you use a reference, indicate so clearly in your solutions. In short, be intellectually honest at all times. Please write neatly, using complete sentences and correct punctuation. Label the problems clearly.

(1) Let E be a real elliptic curve. Recall that a point $P \in \overline{E}$ has order 2 if and only if P has a vertical tangent line. Prove[1] that every point of order 2 in $\overline{E}$ is a point on the x-axis, and that $\overline{E}$ has at most three points of order 2.

Using implicit differentiation, we have $2y\frac{dy}{dx} = 3x^2 + a$, so $\frac{dy}{dx} = \frac{3x^2+a}{2y}$. Then a vertical tangent line occurs if and only if $y = 0$, i.e., for a point on the x-axis.

To find such points, we solve $0 = x^3 + ax + b$, which has at most three solutions.

(2) Find all powers $P, 2P, 3P, \ldots$ of the point $P = (3, 8)$ in $E : y^2 = x^3 - 43x + 166$. You can, and may want to, use a computer graphing system to start by computing small powers.



We play the usual game to find powers of a point, and eventually determine that $4P = 3P^\vee$. This means that $7P = \infty$, so P has order 7. The powers of P are $(3, 8)$, $(-5, -16)$, $(11, -32)$, $(11, 32)$, $(-5, 16)$, $(3, -8)$, ∞, and repeat like so.

[1] Use calculus.

(3) In this problem, we will prove that the elliptic curve $E : y^2 = x^3 + 7$ has no integer solutions.
  (a) Suppose that (a, b) is an integer solution. Show that a must be odd.
  (b) Show that $b^2 + 1 = (a + 2)((a - 1)^2 + 3)$.
  (c) Show that there exists a prime $q \equiv 3 \pmod 4$ that divides the integer in (b), and obtain a contradiction.

(a) We consider the equation modulo 4. If a is even, then $a^3 \equiv 0 \pmod 4$, so $a^3 + 7 \equiv 3 \pmod 4$. Then $b^2 \equiv 3 \pmod 4$ has no solution. We must have that a is odd.
(b) Straightforward.
(c) If a is odd, then $((a - 1)^2 + 3) \equiv 3 \pmod 4$. Thus, it is divisible by some prime $q \equiv 3 \pmod 4$. Then $b^2 + 1 \equiv 0 \pmod q$, so -1 is a quadratic residue modulo q. But then, by quadratic reciprocity, this contradicts that $q \equiv 3 \pmod 4$.