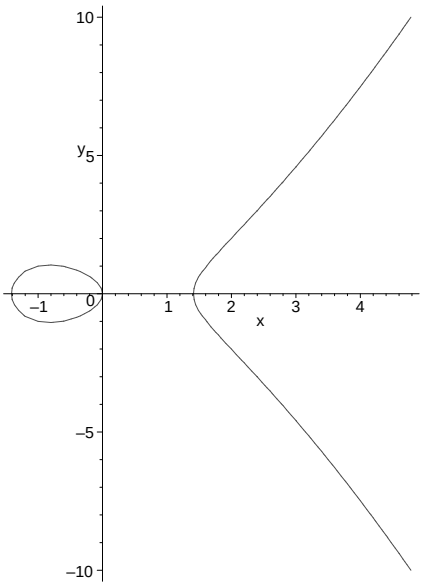
These homework problems are meant to expand your understanding of what goes on during class. Any you turn in will be graded and returned to you. Answers may or may not be posted on the web, depending on demand.

1. Here is a graph of the elliptic curve $y^2 = x^3 - 2x$. Notice that $a = -2$ and $b = 0$, so $4a^3 + 27b^2 = 108 \neq 0$. (That is, our elliptic curve is non-singular.)




   Let $P = (-1, 1)$, $Q = (2, 2)$, and $R = (2, -2)$ be points on this curve.

   (a) Compute $P + Q$.

   (b) Compute $(P + Q) + R$.

   (c) Compute $Q + R$.

   (d) Compute $P + (Q + R)$.

   This demonstrates that the elliptic curve is associative. That is, one *always* has $(P + Q) + R = P + (Q + R)$, for any points $P$, $Q$, and $R$.

2. Consider the elliptic curve $y^2 = x^3 - 2x$ (the same one as in the previous problem), now modulo 5. (Note that $4a^3 + 27b^2 = 108 \equiv 3 \not\equiv 0 \bmod 5$.)

   (a) Write down all the points on this curve. Don't forget $\mathcal{O}$, the identity!

   (b) Find all points $P$ for which $P + P = \mathcal{O}$. That is, find all points that are there own inverses.

   (c) Find the inverses of all other points on this curve.

3. One thing we didn't cover in class is that the various elliptic curve expressions, from

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

to

$$y^2 = x^3 + Ax^2 + Bx + C \tag{2}$$

and finally

$$y^2 = x^3 + ax + b, \tag{3}$$

may be obtained by changing variables. This question is essentially algebra, walking through these changes.

(a) Show that if we change $y$ to $y - \frac{a_1}{2}x - \frac{a_3}{2}$, the expression (1) changes to equation (2). (Here we leave $x$ unchanged.)

(b) Show that if we change $x$ to $(x - 3A)/9$ and $y$ to $y/27$, the expression (2) changes to equation (3).

This means that, in a sense, the two expressions (1) and (3) represent the same object. (Compare this notion with the discussion in problem 3 of homework 6. We've just transformed one expression into the other.)