Senior Math Circles - Elliptic Curves - Problem Set - November 4, 2015

(i) Draw the elliptic curves $y^2 = x^3 - 4x$ and $y^2 = x^3 - 9x$. For a challenge, try to draw $y^2 = x^3 + 1$. Check your answer on a computer!, specifically around x=0.

(ii) Show that the elliptic curve defined by $y^2 = x^3 + 7$ has no integer solution when x is even. Challenge: Prove true for x odd as well showing that this equation has no integer solutions.

(iii) 1. Let $y^2 = x^3 + Ax + B$ be an elliptic curve and $P = (x, y)$ a point on the elliptic curve. Recall that the slope of the tangent line at the point P is given by $m = \frac{3x^2+A}{2y}$. Show that the x-coordinate of $P + P$ is given by

$$\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}.$$

Justify to yourself that when $A = -N^2$ and $B = 0$, the formula becomes:

$$\frac{x^4 - 2N^2x^2 + N^4}{4(x^3 - N^2x)}.$$

2. Show that the x-coordinate of a point $P = (x, y)$ (different from $(0, 0), (\pm N, 0)$) on the elliptic curve $y^2 = x^3 - N^2x$ with N squarefree satisfies
   i. x is the square of a rational number
   ii. x has an even denominator (when in lowest terms)
   iii. x has a numerator that shares no common factor with N (when in lowest terms)

(iv) (Borrowed from Silverman-Tate Rational Points on Elliptic Curves exercise 1.18) Consider the elliptic curve $y^2 = x^3 + 17$. By trial and error one can find several small solution to this equation, such as

$$P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 23).$$

(It may be easier to do this exercise if you use a math software. I recommend trying SAGE online via Sage Math Cloud. Do searches for these and Sage + Elliptic Curves for help with the syntax.)

1. Compute the values of $-(P_1 + P_1) = -2P_1$, $P_1 - P_3$ and $P_3 - 2P_1$. Do these values look familiar?
2. Compute $P_6 = -P1 + 2P_3$ and $P_7 = 3P_1 - P_3$.
3. Notice that the points $P_1, P_2, P_3, P_4, P_5, P_6, P_7$ all have integer coordinates. There is exactly one more rational point on the curve which has integer coordinates and $y > 0$. Find that point. (Hint: Try subtracting the two points from the previous exercise).
4. Very Difficult Challenge: Can you prove that these are the only rational points with integer coordinates?

(v) (Borrowed from Silverman-Tate Rational Points on Elliptic Curves exercise 1.20) Compute $2P$, $4P$, $8P$ for the point $P = (3, 8)$ on the elliptic curve $y^2 = x^3 - 43x + 166$. Compare P and $8P$. What do you notice?