Lab 3 – The Congruent Number Problem

By the end of this lab you will show that 5 is a congruent number (see below for the definition) and that it is the smallest one.

Problem 1: The elliptic curve $E : y^2 = x(x+1)(x-1)$ contains points P so that $2P := P + P = \mathcal{O}$. What points are those?

Problem 2: A torsion point on the curve E is a point P so that $nP = \mathcal{O}$ for some $n \in \mathbf{Z}$. Check that you at least got the right number of points in Problem 1 by constructing the elliptic curve E from above and computing the torsion points of E. Type `E.<tab>` and you'll get a list of all possible things that E can do. Find a relevant one in the list and choose that.

Problem 3: An integer n is a congruent number if it's the area of a right triangle with three rational sides. Show that 6 is a congruent number.

Problem 4: An integer n is congruent if and only if there is a nontrivial, nontorsion rational point on the elliptic curve $E_n : y^2 = x(x+n)(x-n)$. To show this, prove the following:

Theorem: For $n > 0$ there is a one-to-one correspondence between the following two sets:

$$\{(a,b,c) : a^2 + b^2 = c^2, ab/2 = n\} \text{ and } \{(x,y) : y^2 = x^3 - n^2 x, y \neq 0\}.$$

The correspondence is given by

$$(a,b,c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) \text{ and } (x,y) \mapsto \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right).$$

Problem 5: Recall that Mordell's theorem (which we have yet to prove) says $E_n(\mathbf{Q}) \cong E_n(\mathbf{Q})_{\mathrm{tor}} \oplus \mathbf{Z}^{r_n}$. Convince yourself that if r_n (called the **(algebraic) rank** of E_n is positive iff n is a congruent number. Show that 1 is not congruent by finding an appropriate command in Sage. Show that 5 and 6 both are.

Problem 6: Find a rational point on E_5 using `E.point_search(10)` (here 10 is some bound; you could make it as big as 20 without Sage crashing) Use what you did in problem 4 to find the actual triangle.

Problem 7: Jerry Tunnell in a beautiful paper from the 1980s gave an easy criterion to determine if n was a congruent number.

Theorem: Let n be a square free positive integer. Set

$$f(n) = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2y^2 + 8z^2 = n\}$$
$$g(n) = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2y^2 + 32z^2 = n\}$$
$$h(n) = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 4y^2 + 8z^2 = n/2\}$$
$$k(n) = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 4y^2 + 32z^2 = n/2\}$$

For odd n, if n is congruent, then $f(n) = 2g(n)$. For even n, if n is congruent, then $h(n) = 2l(n)$. If the conjecture of Birch and Swinnerton-Dyer is true, the converses hold as well. Verify (either by hand or by writing program in Sage) that 5 is the smallest cogruent number.