Pries: M405 - Number Theory, Spring 2018

Week 8 Friday: elliptic curves in SAGE.

1. Getting started:
   (a) Method 1: go to http://sagecell.sagemath.org/
   Method 2: (required for bigger jobs) start a free CoCalc account at http://www.sagemath.org/
   (b) Helpful websites: Look at this directory
   http://doc.sagemath.org/html/en/reference/curves/sage/schemes/elliptic_curves/
   especially the extensions constructor.html, ell_point.html, ell_finite_field.html, ell_field.html

2. Adding points:
   (a) E=EllipticCurve([-5,4]); E
   (b) Z=E.plot(thickness=4, rgbcolor=(0.1, 0.7, 0.1)); Z.show(figsize=[4,6]);
   (c) P=E([1,0]); Q=E([0,2]); P+Q;
   (d) Explain the output of [n*P for n in range(10)];
   (e) Explain the output of [n*Q for n in range(10)];
   (f) E.torsion_order();
   (g) E.rank();

3. Consider the point $(3, 8)$ on the elliptic curve $y^2 = x^3 - 43x + 166$. Compute P, $2P$, $4P$, $8P$. Comparing P to $8P$, what can you conclude?

4. Torsion points:

   (a) E = EllipticCurve('11a'); E

   (b) plot(E);

   (c) E.rank();

   (d) E.torsion_order();

   (e) G = E.torsion_subgroup(); G;

   (f) P=G.gen(0); P;

   (g) P+P; or 2*P;

   (h) `[n*P for n in range(5)];`

   (i) G.points();

   (j) Compare E.division_polynomial(a).factor(); for a=2,3,5; What is different about a=5?

5. Let $E : y^2 = x^3 + 17$. Find:

   (a) The rank, generators (E.gens();) of $E(\mathbb{Q})$, the sum of the generators; Hint: E.gens(); E.gens(0)+E.gens(1);

   (b) The integral points of E. S=E.integral_points(); S

   (c) Let $P = (-2, 3, 1)$ and $Q = (2, 5, 1)$ and express all the integral points (x, y) with $y > 0$ as $nP + mQ$ for some n and m.

   (d) The torsion subgroup over $\mathbb{Q}$ and over $\mathbb{Q}[t]/(t^3 + 17)$.
   Useful commands:

   ```
   K.<t>=NumberField(f); EK=E.change\_ring(K);
   ```