MA 842: Explicit methods for elliptic and hyperelliptic curves
Spring 2017
Problem Set 2
Due: February 8, 2017

---

(1) Let E_1 and E_2 be isogenous elliptic curves over a finite field $\mathbb{F}_q$ of characteristic p.
   (a) Prove that $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.
   (b) Prove that $E_1(\mathbb{F}_q)$ is not necessarily isomorphic to $E_2(\mathbb{F}_q)$ by giving an explicit example.

(2) Let E be an elliptic curve over $\mathbb{Q}$. Prove that any elliptic curve $E'/\mathbb{Q}$ that is (rationally) isogenous to E has the same rank.

(3) Let E_1 and E_2 be isogenous elliptic curves over a field k that is not finite. Suppose $\#E_1(k)$ and $\#E_2(k)$ are finite. Is it true that $\#E_1(k) = \#E_2(k)$?

(4) Use LMFDB (`www.lmfdb.org`) to find an example of an elliptic curve over $\mathbb{Q}$ that admits a rational 3-isogeny but that does not have rational 3-torsion.

(5) Let $a, b \in \mathbb{Z}$. Show that all elliptic curves of the form $y^2 + axy + by = x^3$ have a rational 3-torsion point.

(6) Read about division polynomials associated to elliptic curves and describe how they can be used to compute torsion.

(7) Consider $E : y^2 = x^3 + 41x$ over $\mathbb{Q}$. Compute $E(\mathbb{Q})$.