MA 842: Explicit methods for elliptic and hyperelliptic curves
Spring 2017
Problem Set 1
Due: February 1, 2017

The formal group of an elliptic curve, torsion, and reduction

(1) Let p be a prime and let $E : y^2 = x^3 + Ax + B$ be an elliptic curve, with $A, B \in \mathbb{Z}_p$. Write $z = -\frac{x}{y}$ and $w = -\frac{1}{y}$. Using the relationship $w = f(z, w) = z^3 + Aw^2z + Bw^3$, express w as an element of $\mathbb{Z}[A, B][[z]]$ and show that it is the unique power series satisfying $w(z) = f(z, w(z))$.

(2) Let $\mathfrak{m} = p\mathbb{Z}_p$. Write x, y as Laurent series in z and show that if $z \in \mathfrak{m}$, then $(x(z), y(z))$ converges to a point of $E(\mathbb{Q}_p)$. Conclude that we have an injection $\mathfrak{m} \hookrightarrow E(\mathbb{Q}_p)$. We will let $\widehat{E}(\mathfrak{m})$ denote the image of $\mathfrak{m}$ under the above map.

(3) Now for $z_1, z_2 \in \mathfrak{m}$, consider the addition $(z_1, w_1) + (z_2, w_2)$. Show that the z-coordinate of $(z_1, w_1) + (z_2, w_2)$ is given by $F(z_1, z_2)$, where

$$F(z_1, z_2) = z_1 + z_2 + (\text{terms of degree } \geq 2) \in \mathbb{Z}[A, B][[z_1, z_2]].$$

($F(z_1, z_2)$ is an example of a *formal group*.)

(4) Let E_p denote the reduction of E mod p. Let $E_{p,ns}(\mathbb{F}_p)$ denote the group of nonsingular points in $E_p(\mathbb{F}_p)$, and let $E_0(\mathbb{Q}_p)$ denote the set

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \widetilde{P} \in E_{p,ns}(\mathbb{F}_p)\}.$$

Prove that the reduction map

$$\begin{aligned} E_0(\mathbb{Q}_p) &\to E_{p,ns}(\mathbb{F}_p) \\ P &\mapsto \widetilde{P}, \end{aligned}$$

is a homomorphism.

(5) Let $E_1(\mathbb{Q}_p)$ denote the kernel of the reduction map from $E_0(\mathbb{Q}_p)$ to $E_{p,ns}(\mathbb{F}_p)$; that is,

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \widetilde{P} = \mathcal{O}\}.$$

Show that $E_1(\mathbb{Q}_p) \cong \widehat{E}(\mathfrak{m})$.

(6) Prove that $E_1(\mathbb{Q}_p)$ has trivial torsion. (Hint: use properties of formal groups[1] for the case of m-torsion where $gcd(m, p) = 1$.)

(7) Show that when E_p is nonsingular, $E_{tors}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $E_p(\mathbb{F}_p)$. Conclude that when $E : y^2 = x^3 + Ax + B, A, B \in \mathbb{Z}$ is an elliptic curve and p is a prime of good reduction, that $\#E_{tors}(\mathbb{Q}) | \#E_p(\mathbb{F}_p)$.

Getting started with Sage and Magma

(1) Create an account on SageMathCloud (SMC).

---

[1] e.g., see Silverman's *Arithmetic of Elliptic Curves*, Chapter 4

(2) Create a Sage worksheet to carry out the following computation:
Let $E/\mathbb{Q}$ be an elliptic curve, and for all good primes p, consider the reductions E_p of E mod p. Let $N_p = \#E_p(\mathbb{F}_p)$. Use Sage to graph

$$\log\left(\prod_{p\leq X}\frac{N_p}{p}\right)$$

for the following:
   (a) The elliptic curves $y^2 = x^3 + 1$, $y^2 = x^3 - x$.
   (b) The elliptic curves $y^2 = x^3 + 2$, $y^2 = x^3 - 2x$.
   (c) The elliptic curves $y^2 = x^3 + 17$, $y^2 = x^3 + 14x$.
   (d) The elliptic curves $y^2 = x^3 - 174$, $y^2 = x^3 - 82x$.

(3) Add me as a collaborator to your SMC project and send me a link to the worksheet.

(4) Ask Tim Kohl for an account on `linear.bu.edu`.

(5) Use Magma to compute the rank of the elliptic curve

$$y^2 + xy + y = x^3 - x^2 - 1608154463x + 25555312501831.$$

(You may assume GRH.)

(6) Read about why GRH is useful for this computation and write up a short explanation.