MA 842: Explicit methods for elliptic and hyperelliptic curves

Spring 2017

Problem Set 4

Due: March 3, 2017

---

(1) Let $C/\mathbb{Q}$ be a hyperelliptic curve given by $y^2 = f(x)$. Let $P = (a, 0) \in C(\mathbb{Q})$. The usual choice of uniformizer at P is $y(t) = t$. Write a function in Sage that takes as input C, P and uses this uniformizer to compute the corresponding $x(t)$.

(2) Let $C : y^2 = x(x-1)(x-2)(x-5)(x-6)$. Compute $(x(t), y(t))$ at $P_0 = (0, 0)$ and at $P_1 = (1, 0)$.

(3) Let $C/\mathbb{Q}_p$ be a hyperelliptic curve given by $y^2 = f(x)$, with $f(x) \in \mathbb{Z}_p[x]$. Consider the mod p reduction $C_p : y^2 = \overline{f}(x)$ over $\mathbb{F}_p$, where $\overline{f}$ denotes the reduction of f at p. If $Q \in C_p(\mathbb{F}_p)$ is a smooth point, show that there are points $P \in C(\mathbb{Q}_p)$ such that $\overline{P} = Q$.

(4) For a smooth projective absolutely irreducible curve C of genus g over a finite field F with q elements, we have the Hasse-Weil bound

$$|\#C(F) - (q+1)| \leq 2g\sqrt{q}.$$

   (a) Is the upper bound of $\#C(F) \leq (q+1) + 2g\sqrt{q}$ ever sharp? If so, give an example.

   (b) Are there improvements to the upper bound? Read and write up what you find.