MATH 343, PROBLEM SET 5

ANDREW J. BLUMBERG

1. Problems

(1) Please write a program which computes the addition law on $E[F_p]$ for an elliptic curve E. Take p and the coefficients of the curve as input on the first line of the input file (tab-delimited, descending order of degree). Take the points to add on the second and third line. Let the “point” X denote the point at infinity.

(2) Please write a program which takes as input p a prime, $m \in \mathbb{F}_p[t]$, $q_1 \in \mathbb{F}_p[t]$, and $q_2 \in \mathbb{F}_p[t]$ and outputs $q_1 q_2 \mod m$ and $q_1 + q_2 \mod m$ (i.e., the computation takes place in the quotient $\mathbb{F}_p[t]/(m)$.

(3) From the text: 3.11, 5.42, 5.43, 6.1, 6.4, 6.6 (use the program above), 6.10, 6.13.