MATH 343, PROBLEM SET 7

ANDREW J. BLUMBERG

1. Problems

(1) Please write a program which computes the Weil pairing on an elliptic curve E. The first line of the input should be the coefficients of the curve E, the second line m, and the third and fourth lines a pair of m-torsion points P and Q.
(2) Please write out a complete formal specification of the block chain protocol, based on the original bitcoin paper. (The answer here should be phrased akin to the way we presented the El gamal protocol in class.)
(3) Explain (in detail) how an adversary with over 50% of the computing power in a block chain protocol could seize control.
(4) From the text: 6.32, 6.33.