Due Aug 18, 2025

MATH 173B: Cryptology II
Homework 2: Lenstra's Algorithm

Instructions: Please answer the following questions carefully. Show all your work to receive full credit. Write your answers clearly and justify each step.

1 Problem 1 (20pts)

Suppose E_1 and E_2 are elliptic curves, and let $f : E_1 \to E_2$ be a function satisfying

$$f(P + Q) = f(P) + f(Q)$$

for all points $P, Q \in E_1$.

(a) Prove that $f(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ denotes the identity element (point at infinity) on the elliptic curves.

(b) Prove that if n is a non-negative solution to the discrete logarithm problem for points $P, Q \in E_1$ (i.e., $Q = nP$), then n is also a solution to the discrete log problem for the points $f(P), f(Q) \in E_2$ (i.e., $f(Q) = nf(P)$).

2 Problem 2 (80pts)

Use Lenstra's elliptic curve factorization algorithm as outlined in Section 6.6 to factor each of the integers N using the given elliptic curve E and point P. For Step 3 in the algorithm, use the upper bound $j = 1000$.

(a) $N = 589, \quad E : Y^2 = X^3 + 4X + 9, \quad P = (2, 5)$.

(b) $N = 26167, \quad E : Y^2 = X^3 + 4X + 128, \quad P = (2, 12)$.