Elliptic Curves - List 4

Task 1 (7 pts) Implement the elliptic curve group operation in the standard projective coordinates: addition of two different points, and doubling a point. Keep an eye on the border cases: if the point is the zero at infinity point, or if you add two points and actually the points are the same so you should double it.

Task 2 (13 pts) Use your implementation of the projective coordinates in the Pollard-ρ method to solve the instances of DLP from List 2. Measure execution times for both the *projective coordinates* version of the Pollard-ρ method and the *affine coordinates* one. Show the execution times for both DLP instances (i.e., four result to present).