Let $p = 10103$ We will consider the elliptic curves $E_C : y^2 = x^3 + x + C$ over the field $\mathbf{F}_p$.

1 In this part, we consider the curve $E_1 : y^2 = x^3 + x + 1$.

(A) Determine $|E_1(\mathbf{F}_p)|$ by using either Baby-Step-Giant-step of Schoof's algorithm.

(B) Find a point P of order as large as possible. on $E_1(\mathbf{F}_p)$.

(C) Find a point Q so that the x-coordinate of Q is as small as possible with $x > 100$.

(D) Use Baby-step-giant-step, a Pollard method (kangaroos) to solve the discrete logarithm problem. $Q = kP$. Reminder: Your explanation should be complete enough that it is possible to re-create your work.

(E) Use Pohlig-Hellman to solve the discrete logarithm problem $Q = kP$.

(F) Select a point P and a secret value integer a. Compute aP. Select a secret integer b and compute bP.

(G) Given P, aP and bP, show how to compute abP without knowing beforehand either a or b.

2 (A) Find the smallest positive integer C so that $E_C : y^2 = x^3 + x + C$ is an elliptic curve so that $|E(\mathbf{F}_p)|$ is prime. (B) Find a point P of order as large as possible. on $E_1(\mathbf{F}_p)$.

(C) Find a point Q so that the x-coordinate of Q is as small as possible with $x > 100$.

(D) Use Baby-step-giant-step, or a Pollard method (kangaroos) to solve the discrete logarithm problem. $Q = kP$.

(E) Show an example of an implementation of a Diffie-Hellman key exchange on this curve over this field.

(F) Show an example of an implementation of the Digital Signature Algorithm on the curve over this field.

3 Let $q = 1001003$.

(A) Find the smallest positive integer C so that $E_C : y^2 = x^3 + x + C$ is an elliptic curve so that $|E(\mathbf{F}_q)|$ is prime. (B) Find a point P of order as large as possible. on $E_1(\mathbf{F}_q)$.

(C) Find a point Q so that the x-coordinate of Q is as small as possible with $x > 100$.

(D) Use Baby-step-giant-step, or a Pollard method (kangaroos) to solve the discrete logarithm problem. $Q = kP$.