MATH 3094 - Practice Final Exam

YOUR NAME: ____

P1	P2	P3	P4	P5	Extra	Total

Please review the previous practice exams and midterms for practice on material from Chapters 1-4.

Problem 1. Draw the elliptic curve $y^2 = x^3 + 1$ and illustrate addition and doubling of points on the graph, by adding $P = (0, 1)$ and $Q = (2, 3)$, and also $Q + Q = 2Q$.

Solution. *Hint:* $P + Q = (-1, 0)$ *and* $2Q = (0, 1)$.

Problem 2. Let E be the elliptic curve $y^2 = x^3 + 1$ defined over $\mathbb{F}_{11}$.

(1) State Hasse's theorem, and give a bound on the number of points in $E(\mathbb{F}_{11})$ using Hasse's theorem.
(2) Find all the points on $E(\mathbb{F}_{11})$.
(3) Let $P = (5, 4)$. Show that P is on E, and compute $2P$ using the doubling formulas on E.
(4) Let $P = (5, 4)$ and $Q = (7, 5)$. Compute $P + Q$ using the addition formulas on E.

Solution. (1) *By Hasse's theorem, the number of elements in* $E(\mathbb{F}_{11})$ *is less or equal to*

$$p + 1 + 2\sqrt{p} = 11 + 1 + 2\sqrt{11} \approx 18.63\ldots$$

(2) *The points on* E *are* $(0, 1), (0, 10), (2, 3), (2, 8), (5, 4), (5, 7), (7, 5), (7, 6), (9, 2), (9, 9),$ $(10, 0)$, *and the point at infinity* $\mathcal{O} = [0, 1, 0]$.
(3) *Hint:* $2P = (10, 0)$.
(4) *Hint:* $P + Q = (2, 3)$.

Problem 3. Let E be the elliptic curve $y^2 = x^3 + 1$ defined over $\mathbb{F}_{11}$, and let $P = (9, 9)$. The multiples of P are, in order:

$$(9, 9), (2, 3), (5, 7), (0, 1), (7, 5), (10, 0), (7, 6), (0, 10), (5, 4), (2, 8), (9, 2), \mathcal{O} = (0 : 1 : 0)$$

That is, $2P = (2, 3)$, $3P = (5, 7)$, etc.

(1) In Problem 2 you should have proved that $\#E(\mathbb{F}_{11}) = 12$. If $P = (9, 9)$ and Q is an arbitrary point on $E(\mathbb{F}_{11})$, is the ECDLP problem $nP = Q$ solvable?
(2) Find n such that $nP = (5, 4)$.
(3) Find n such that $nP = (7, 6)$.
(4) Use the elliptic collision algorithm to solve $nP = (5, 4)$.

Solution. (1) *In Problem 2 we found that* $E(\mathbb{F}_{11})$ *has* 12 *points, and the multiples of* $(9, 9)$ *go through* 12 *different points. Therefore every point on* E *is a multiple of* $(9, 9)$ *and therefore every ECDLP problem* $nP = Q$ *has a solution.*
(2) *From the list of multiples of* P *that we are provided with, we see that* $9P = (5, 4)$.
(3) *From the list of multiples of* P *that we are provided with, we see that* $7P = (5, 4)$.
(4) *Review the collision algorithm for elliptic curves!*

Problem 4. Let E be the elliptic curve $y^2 = x^3 + 1$ defined over $\mathbb{F}_{11}$, and let $P = (9, 9)$. The multiples of P are, in order:

$$(9,9),(2,3),(5,7),(0,1),(7,5),(10,0),(7,6),(0,10),(5,4),(2,8),(9,2),\mathcal{O} = (0:1:0)$$

That is, $2P = (2,3)$, $3P = (5,7)$, etc.

(1) Alice sets up an Elliptic Diffie–Hellman system with p, E and P as above. She chooses $n_A = 2$ and Bob chooses $n_B = 5$. Compute the secret key (the secret point) that they will share using the Elliptic Diffie–Hellman algorithm.
(2) Eve intercepts a communication between Alice and Bob. Eve knows that Alice set up an Elliptic Diffie–Hellman with p, E, P as above, and intercepts a communication from Alice to Bob ($Q_A = (7,5)$) and a communication from Bob to Alice ($Q_B = (2,8)$). What is the secret that Alice and Bob share?

Solution. (1) *The common secret is* $n_A \cdot n_B \cdot P$ *so* $2 \cdot 5 \cdot P = 10P = (2,8)$.
(2) *Since* $n_A \cdot P = Q_A = (7,5)$ *we must have that* $n_A = 5$. *Since* $n_B \cdot P = Q_B = (2,8)$ *we must have* $n_B = 10$. *Thus the common secret is* $n_A n_B P = 50P$. *Since* P *has order* 12, *we have* $50P = 48P + 2P = 2P = (2,3)$.

Problem 5. Explain how Alice could set up an Elliptic Elgamal system using p, P, E as in Problem 4, and give an example of a message being encrypted in this system.

Solution. *Review Elliptic Elgamal.*

Problem 6. Explain how Alice could set up an Elliptic Digital Signature system using p, E as in Problem 4, and give an example of a document being signed in this system.

Solution. *Review Elliptic Digital Signatures.*

Problem 7. Let $N = 143$ and $E : y^2 = x^3 + x - 1$ and $P = (1,1)$. Use Lenstra's algorithm to factor N, using E and P modulo N. (*For this problem, you can use a computer if you want, to practice and to learn how the algorithm works. In the exam, a question of this type would be set up so you don't have to use a computer – a calculator would suffice.*)

Solution. *Here are the coordinates of the multiples of* P *modulo* N*:*

- $P \equiv (1,1) \bmod N$,
- $2P \equiv (2,140) \bmod N$,
- $3(2P) = 6P \equiv (133,56) \bmod N$,
- $4(6P) = 24P \equiv (133,43) \bmod N$,

However, computing $5(24P)$ *fails. Here is why:* $Q = 24P \equiv (133,43) \bmod 143$. *In order to compute* $5Q$ *we need to do* $5Q = 2Q + 3Q$. *First* $2Q \equiv (68,113) \bmod 143$. *And* $3Q = 2Q + Q = (68,113) + (133,43)$. *But to do so, we need to invert* $133 - 68 \equiv 65 \bmod N$, *and it turns out this is impossible because* $\gcd(N,65) = \gcd(143,65) = 13$. *Hence we have found a factor of* N, *namely* 13, *and* $N = 143 = 11 \cdot 13$.

Highlights of Chapter 6.

Chapter 6: Elliptic Curves and Cryptography

1. **Number theory concepts:**
   (a) An *elliptic curve* over a field F (where $F \neq \mathbb{F}_2$) is a curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$, with $A, B \in F$, such that $4A^3 + 27B^2 \neq 0$ in F.
   (b) The geometric secant and tangent method on an elliptic curve E to find a third point R on E from two known points P and Q. Addition of points on the elliptic curve.
   (c) Elliptic curve addition algorithm: let E be given by $y^2 = x^3 + Ax + B$, and let P and Q be points on E.
   - If $P = \mathcal{O}$, then $P \oplus Q = Q$. If $Q = \mathcal{O}$, then $P \oplus Q = P$.
   - If $P = (x_1, y_1)$ and $Q = (x_1, -y_1)$, then $P \oplus Q = \mathcal{O}$, i.e., $Q = -P$.
   - If $P \neq Q$ and $P = (x_1, y_1)$, $Q = (x_2, y_2)$, then define $\lambda = (y_2 - y_1)/(x_2 - x_1)$. Then $P \oplus Q = (x_3, y_3)$, with
   $$x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1.$$
   - If $P = Q = (x_1, y_1)$, then define $\lambda = (3x_1^2 + A)/(2y_1)$. Then $2P = (x_3, y_3)$ where the coordinates x_3, y_3 are defined as above.

   (d) If E is an elliptic curve over $\mathbb{F}_p$, with p prime, then
   $$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 \equiv x^3 + Ax + B \bmod p\} \cup \{\mathcal{O}\}.$$
   (e) Hasse's theorem: if E is an elliptic curve over $\mathbb{F}_p$, then
   $$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

2. **Cryptography:**
   (a) The Elliptic Curve Discrete Logarithm Problem (ECDLP): given an elliptic curve E over $\mathbb{F}_p$ and points P and Q on E, find a number n such that $nP = Q$, where $nP = P \oplus \cdots \oplus P$ is the sum of n copies of P using the elliptic curve addition algorithm.
   (b) The double-and-add algorithm to compute a multiple of a point on an elliptic curve.
   (c) Collision algorithm to find a solution to an ECDLP problem: to solve $Q = nP$, find lists:
   - List 1: $k_1P, k_2P, \ldots, k_rP$, where $k_1, \ldots, k_r$ are distinct integers.
   - List 2: $k_1'P + Q, k_2'P + Q, \ldots, k_r'P + Q$, where $k_1', \ldots, k_r'$ are distinct integers.

   If $k_uP = k_v'P + Q$, then $Q = (k_u - k_v')P$. One needs about $r \approx 3\sqrt{p}$ to have a "very good chance" of finding a collision.
   (d) Elliptic Diffie-Hellman Key Exchange:
   - A trusted party chooses a large prime p, an elliptic curve E over $\mathbb{F}_p$, and a points P in $E(\mathbb{F}_p)$.
   - Alice chooses a secret integer n_A, Bob chooses a secret integer n_B.
   - Alice computes $Q_A = n_A \cdot P$ and sends it to Bob. Bob computes $Q_B = n_B \cdot P$ and sends it to Alice.
   - Alice computes the secret shared point $n_A \cdot Q_B$. Bob computes the secret shared point $n_B \cdot Q_A$. We have $n_An_BP = n_AQ_B = n_BQ_A$.

   (e) Elliptic Elgamal cryptosystem:
   - A trusted party chooses a large prime p, an elliptic curve E over $\mathbb{F}_p$, and a points P in $E(\mathbb{F}_p)$.

- Alice chooses a private key n_A. Computes $Q_A = n_A \cdot P$ in $E(\mathbb{F}_p)$. Publishes Q_A.
- Bob chooses plaintext $M \in E(\mathbb{F}_p)$, chooses a random element k, and computes $C_1 = kP$ and $C_2 = M + kQ_A$. Sends the ciphertext (C_1, C_2) to Alice.
- Alice computes the plaintext $M = C_2 - n_A C_1 \in E(\mathbb{F}_p)$.

(f) Elliptic Curve Digital Signatures:

- A trusted party chooses a large prime p, an elliptic curve E over $\mathbb{F}_p$, and a points G in $E(\mathbb{F}_p)$ of large prime order q.
- Sam chooses a secret signing key $1 < s < q - 1$. Computes $V = sG$ in $E(\mathbb{F}_p)$, and publishes V.
- Sam chooses a document $d \bmod q$, chooses a random element $e \bmod q$, computes eG in $E(\mathbb{F}_p)$, and a signature $(s_1, s_2) = (x(eG) \bmod q, (d + s \cdot s_1)e^{-1} \bmod q)$. Publish $(d, (s_1, s_2))$.
- Victor computes $v_1 \equiv ds_2^{-1} \bmod q$ and $v_2 \equiv s_1 s_2^{-1} \bmod q$. Then verifies that

$$x(v_1 G + v_2 V) \bmod q = s_1.$$

(g) Lenstra's Factorization Algorithm:

i. Input: N to be factored.
ii. Choose random A, a, and $b \bmod N$.
iii. Set $P = (a, b)$ and $B \equiv b^2 - a^3 - Aa \bmod N$, and $E : y^2 = x^3 + Ax + B \bmod N$.
iv. Loop $j = 2, 3, 4, \ldots$
    A. Set $Q \equiv j \cdot P \bmod N$ and set $P = Q$.
    B. If computing $j \cdot P$ in Step 4 fails, we have found a divisor $d > 1$ of N.
        - If $d < N$, then success, return d.
        - If $d = 1$, then go to step 1.
    C. If computing $j \cdot P$ is successful, then increase j by 1, and return to Step A.