

Mahindra University Hyderabad École Centrale School of Engineering Spring Semester Regular Examinations, June-2023

Program: B. Tech. Branch: Computation & Mathematics Year: II Semester: II Subject: Number Theory & Cryptography (MA 2209)

Date: 06/06/2023

Start Time: 10:00 AM

Time Duration: 3 Hours

Max. Marks: 100

Instructions:

- 1. There are 6 questions. All of which are compulsory. The credit for each question is mentioned at the end of the question.
- 2. Justify your answer wherever required.
- 3. All notations are standard and same as used in the lectures.

 (a) Compute -7503 (mod 81.) [3] (b) Compute (3,5) + (3,5) in the elliptic curve x³ + x + 6 over Z₁1. [5] (c) Evaluate the Jacobi symbol (4317/7563). [4] (d) Evaluate the discrete logarithm log₂(11) for the prime 19. [4] (e) Find all primitive roots modulo 7. [4] 2. Let E be the elliptic curve y² = x³ + x + 1 over Z₅. (a) Determine all the points in E. [7] (b) Show that E is cyclic. [7] (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z*_p. Show that α is a primitive element modulo p if and only if α* p ≠ 1 mod p for all primes q such that q divides p − 1. [8] 		
 (b) Compute (3,5) + (3,5) in the elliptic curve x³ + x + 6 over Z₁₁. [5] (c) Evaluate the Jacobi symbol (4317/7563). [4] (d) Eyaluate the discrete logarithm log₂(11) for the prime 19. [4] (e) Find all primitive roots modulo 7. [4] 2. Let E be the elliptic curve y² = x³ + x + 1 over Z₅. [7] (a) Determine all the points in E. [7] (b) Show that E is cyclic. [7] (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z⁵. Show that α is a primitive element modulo p if and only if α 1 mod p for all primes q such that q divides n. 1 		[3]
 (c) Evaluate the Jacobi symbol (4317/7563). [4] (d) Evaluate the discrete logarithm log₂(11) for the prime 19. [4] (e) Find all primitive roots modulo 7. [4] 2. Let E be the elliptic curve y² = x³ + x + 1 over Z₅. [7] (a) Determine all the points in E. [7] (b) Show that E is cyclic. [7] (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z⁵. Show that α is a primitive element modulo p if and only if α p-1/q ≠ 1 mod p for all primes q such that q divides n = 1 	(b) Compute $(3,5) + (3,5)$ in the elliptic curve $x^3 + x + 6$ over \mathbb{Z}_{11} .	
 (d) Evaluate the discrete logarithm log₂(11) for the prime 19. [4] (e) Find all primitive roots modulo 7. [4] 2. Let E be the elliptic curve y² = x³ + x + 1 over Z₅. (a) Determine all the points in E. [7] (b) Show that E is cyclic. [7] (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z⁺p. Show that α is a primitive element modulo p if and only if α p-1/q ≠ 1 mod p for all primes q such that q divides x = 1 	(c) Evaluate the Jacobi gumb at (4317)	[0]
 (e) Find all primitive roots modulo 7. [4] 2. Let E be the elliptic curve y² = x³ + x + 1 over Z₅. (a) Determine all the points in E. [7] (b) Show that E is cyclic. [7] (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z⁺_p. Show that α is a primitive element modulo p if and only if α p-1/q ≠ 1 mod p for all primes q such that q divides n = 1. 	$\frac{7563}{7563}$	[4]
 (e) Find all primitive roots modulo 7. [4] 2. Let E be the elliptic curve y² = x³ + x + 1 over Z₅. (a) Determine all the points in E. [7] (b) Show that E is cyclic. [7] (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z⁺_p. Show that α is a primitive element modulo p if and only if α p-1/q ≠ 1 mod p for all primes q such that q divides n = 1. 	(d) Eyaluate the discrete logarithm $\log_2(11)$ for the prime 19.	. [4]
 2. Let E be the elliptic curve y² = x³ + x + 1 over Z₅. (a) Determine all the points in E. (b) Show that E is cyclic. (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. (d) 3. a. Suppose that p is an odd prime and α ∈ Z*_p. Show that α is a primitive element modulo p if and only if α = 1 mod p for all primes q such that q divides n = 1. 	(e) Find all primitive roots modulo 7.	
 (a) Determine all the points in E. (b) Show that E is cyclic. (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. (d) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. (e) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. (f) A = (1,2) and (1,2) and		[4]
 (a) Determine all the points in E. (b) Show that E is cyclic. (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. (d) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. (e) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. (f) A = (1,2) and (1,2) and	2. Let E be the elliptic curve $y^2 = x^3 + x + 1$ over \mathbb{Z}_5 .	
 (b) Show that E is cyclic. [7] (c) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z_p*. Show that α is a primitive element modulo p if and only if α = 1 mod p for all primes q such that q divides n = 1. 		
 (x) Let P = (0,1), Q = (4,2). Given that P, Q ∈ E, find 2P. Does there exists a positive integer n such that nQ = P? If it exists, find such an n. [6] 3. a. Suppose that p is an odd prime and α ∈ Z_p*. Show that α is a primitive element modulo p if and only if α = 1 mod p for all primes q such that q divides n = 1. 		[7]
3. a. Suppose that p is an odd prime and $\alpha \in \mathbb{Z}_p^*$. Show that α is a primitive element modulo p if and only if $\alpha^{\frac{p-1}{q}} \neq 1 \mod p$ for all primes q such that q divides $p = 1$.	(c) Let $P = (0, 1) O = (4, 2) O(1)$	[7]
3. a. Suppose that p is an odd prime and $\alpha \in \mathbb{Z}_p^*$. Show that α is a primitive element modulo p if and only if $\alpha^{\frac{p-1}{q}} \neq 1 \mod p$ for all primes q such that q divides $p = 1$.	integer n such that $nQ = P$? If it exists a point $Q \in E$, find $Q \in P$. Does there exists a point $Q \in P$?	ositive
and p for all primes q such that q divides q	n in the exists, find such an n .	[6]
	3. a. Suppose that p is an odd prime and $\alpha \in \mathbb{Z}_p^*$. Show that α is a primitive element p if and only if $\alpha^{\frac{p-1}{q}} \neq 1 \mod p$ for all primes q such that q divides $p-1$.	

43 = 12- 11-12-13)-131

- b. Using the above statement prove that 2 is a primitive element modulo 101.
- 4. For n = pq, where p and q are distinct odd primes, define

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1,q-1)}.$$

Suppose that we modify the RSA cryptosystem by requiring that $ab \equiv 1 \pmod{\lambda(n)}$ where a and b are decryption and encryption exponents respectively.

- a. Prove that encryption and decryption are still inverse operations in this modified cryptosystem. [10]
- b. If p = 43, q = 67, and b = 5, compute the decryption exponent a in this modified cryptosystem. [5]
- 5. a. Suppose Allice is using ElGamal Signature scheme with p=47, primitive root $\alpha=5$ and private key a=8.
 - (i) If Alice uses the secret random number k = 9 to sign the message x = 38. Compute her signature for her.
 - (ii) Suppose Bob receives the message x=45 with signature $(\gamma, \delta)=(11,7)$. Help him to verify the signature.
 - b. Suppose Allice is using ElGamal Signature scheme with p=23. She sends Bob the message x=16 with signature $(\gamma,\delta)=(9,0)$. Help Oscar to find the private key a. [7]
 - 6. Given that 5 is a primitive root of \mathbb{Z}_{43} , solve the DLP $5^x \equiv 13 \pmod{43}$ using Shank's Algorithm.