

THEORY OF ELLIPTIC CURVES AND ITS APPLICATIONS I

1	Course Title:	THEORY OF ELLIPTIC CURVES AND ITS APPLICATIONS I
2	Course Code:	MAT6111
3	Type of Course:	Optional
4	Level of Course:	Third Cycle
5	Year of Study:	1
6	Semester:	1
7	ECTS Credits Allocated:	5.00
8	Theoretical (hour/week):	3.00
9	Practice (hour/week):	0.00
10	Laboratory (hour/week):	0
11	Prerequisites:	none
12	Language:	Turkish
13	Mode of Delivery:	Face to face
14	Course Coordinator:	Prof. Dr. İSMAIL NACİ CANGÜL
15	Course Lecturers:	Prof. Dr. Osman Bizim
16	Contact information of the Course Coordinator:	Uludağ Üniversitesi, Fen-Edebiyat Fakültesi Matematik Bölümü, Görükle Bursa-TÜRKİYE 0 224 294 17 57 / obizim@uludag.edu.tr
17	Website:	
18	Objective of the Course:	The theory of elliptic curves brings important areas of mathematics such as abstract algebra, number theory and related fields. The aim of this course is to make the students get all connections among all these areas. The goal is to teach the elementary theory of elliptic curves. So students can bring new ideas the theory of elliptic curves and have the ability conduct original research and independent publication.
19	Contribution of the Course to Professional Development:	
20	Learning Outcomes:	
	1	Learn the group structure of the points on the elliptic curves and the proof of associativity.
	2	Learn division polynomials and torsion points of the elliptic curves and Weil pairing and Tate-Lichtenbaum pairing.
	3	Learn elliptic curves over finite fields and counts the number of the points on these curves, the theorem of Hasse, Frobenius endomorphism and Schoof's algorithm.
	4	Learn the discrete logarithm problem, general attacks on discrete logs, baby step, giant step, Pollard's method, the Pohling-Hellman method.
	5	Learn MOV attack, Frey-Rück attack and other attacks.
	6	Learn the elliptic curves over \mathbb{Q} and the torsion subgroup and the Lutz-Nagell theorem, the method of descent, the Mordell-Weil theorem.
	7	Learn the elliptic curves over \mathbb{C} , doubly periodic functions, tori are elliptic curves, the arithmetic and geometric mean. Cantor's algorithm, zeta functions, Fermat's last theorem, sketch of Wiles's proof.

		8	
		9	
		10	
21	Course Content:		
	Course Content:		
Week	Theoretical	Practice	
1	Basic concepts of elliptic curves, the group law on the elliptic curves and proof of associativity.		
2	Other equations for elliptic curves, Legendre equation, cubic equations and quartic equations. The j-invariant of an elliptic curve and isomorphisms and endomorphisms of the curves.		
3	Torsion points of elliptic curves and division polynomials of an elliptic curve. Weil paring, Tate-Lichtenbaum pairing.		
4	Elliptic curves over finite fields, counting the number of the points on these curves and the theorem of Hasse, The frobenius endomorphism, Schoof's Algorithm.		
5	Determining the group structure of the points on the elliptic curves over finite fields and the group order. Some family of elliptic curves over finite fields, singular and supersingular curves.		
Activites		Number	Duration (hour)
			Total Work Load (hour)
Theoretical	method.	14	3.00
			42.00
Practicals/Labs		0	0.00
			0.00
Self study and preparation	The basic concepts in the elliptic curve	14	5.00
			70.00
Homeworks		0	0.00
			0.00
Projects	modular encryption.	0	0.00
			0.00
Field Studies	ElGamal public key encryption and the digital	0	0.00
			0.00
Midterm Exams	The elliptic curves over Q and the torsion subgroups and the Lutz-Nagell theorem, the	0	0.00
			0.00
Others		14	5.00
			70.00
Final Exams	theorem.	1	13.00
			13.00
Total Work Load			195.00
Total work load/30 hr			6.50
ECTS Credit of the Course			5.00
	functions, tori are elliptic curves, the arithmetic and geometric mean.		
13	Division polynomials and the torsion subgroups, Douud's method, complex multiplication and numerical examples, the integrality of j-invariants.		
14	Hyperelliptic curves, Cantor's algorithm, zeta functions, Fermat's last theorem, sketch of Wiles's proof.		
22	Textbooks, References and/or Other Materials:	[1] Rational Points on Elliptic Curves, J. H. Silverman ve J. Tate, [2]The Arithmetic of Elliptic Curves, J. H. Silverman, [3]Elliptic Curves, L. C. Washington. [4] Introduction to Elliptic Curves and Modular Forms, N. Koblitz.	

23	Assesment	
TERM LEARNING ACTIVITIES	NUMBE R	WEIGHT
Midterm Exam	0	0.00
Quiz	0	0.00
Home work-project	0	0.00
Final Exam	1	100.00
Total	1	100.00
Contribution of Term (Year) Learning Activities to Success Grade		0.00
Contribution of Final Exam to Success Grade		100.00
Total		100.00
Measurement and Evaluation Techniques Used in the Course		

24	ECTS / WORK LOAD TABLE
-----------	-------------------------------

25	CONTRIBUTION OF LEARNING OUTCOMES TO PROGRAMME QUALIFICATIONS															
	PQ1	PQ2	PQ3	PQ4	PQ5	PQ6	PQ7	PQ8	PQ9	PQ10	PQ11	PQ12	PQ13	PQ14	PQ15	PQ16
ÖK1	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK2	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK3	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK4	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK5	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK6	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK7	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
LO: Learning Objectives PQ: Program Qualifications																
Contribution Level:	1 very low		2 low		3 Medium		4 High		5 Very High							