INTRODUCTION TO THE THEORY OF ELLIPTIC CURVES

1	Course Title:	INTRODUCTION TO THE THEORY OF ELLIPTIC CURVES
2	Course Code:	MAT4081
3	Type of Course:	Optional
4	Level of Course:	First Cycle
5	Year of Study:	4
6	Semester:	7
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. OSMAN BİZİM
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 50 / 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 know the basic theory of elliptic curves.
19	Contribution of the Course to Professional Development:	
20	Learning Outcomes:	

	1	Use elliptic curves to solve some problems of mathematics.
	2	Learn the group structure of the points on the elliptic curves.
	3	Learn the j-invariant of an elliptic curve and isomorphisms and endomorphisms of the curves
	4	Learn the singular curves and determine group law of singular curves.
	5	Learn the torsion points of an elliptic curve and learn division polynomials of an elliptic curve.
	6	Learn elliptic curves over finite fields and counts the number of the points on these curves.
	7	Give some results about the numbers of the points of the elliptic curves over finite fields
	8	Learn the elliptic curves over Q and the torsion subgroup and the Lutz-Nagell theorem.
	9	Learn the method of descent of Fermat and the Mordell-Weil theorem.
	10	Learn the elliptic curves over C.

21	Course Content:
	Course Content:

Week	Theoretical	Practice
1	Basic concepts on groups, rings and fields.	
2	Use elliptic curves to solve some problems of mathematics.	
3	The group law on the elliptic curves and proof of associativity.	
4	Other equations for elliptic curves, Legendre equation, cubic equations and quartic equations.	
5	The j-invariant of an elliptic curve and isomorphisms and endomorphisms of the curves.	
6	The singular curves and determining group law of singular curves.	
7	Torsion points of elliptic curves and division polynomials of an elliptic curve.	
8	Elliptic curves over finite fields, counting the number of the points on these curves and the theorem of Hasse.	
9	Determining the group structure of the points on the elliptic curves over finite fields and the group order.	
10	Some family of elliptic curves over finite fields.	
11	The elliptic curves over Q and the torsion subgroup and the Lutz-Nagell theorem.	
12	The method of descent of Fermat and the Mordell-Weil theorem.	
13	The elliptic curves over C.	
14	Overview on Fermat’s last theorem.	

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.
23	Assesment	

TERM LEARNING ACTIVITIES	**NUMBER**	**WEIGHT**
Midterm Exam	1	40.00
Quiz	0	0.00
Home work-project	0	0.00
Final Exam	1	60.00
Total	2	100.00
Contribution of Term (Year) Learning Activities to Success Grade		40.00
Contribution of Final Exam to Success Grade		60.00
Total		100.00
Measurement and Evaluation Techniques Used in the Course		

24	**ECTS / WORK LOAD TABLE**

Activites	Number	Duration (hour)	Total Work Load (hour)
Theoretical	14	3.00	42.00
Practicals/Labs	0	0.00	0.00
Self study and preperation	14	5.00	70.00
Homeworks	0	0.00	0.00
Projects	0	0.00	0.00
Field Studies	0	0.00	0.00
Midterm exams	1	15.00	15.00
Others	14	1.00	14.00
Final Exams	1	9.00	9.00
Total Work Load			150.00
Total work load/ 30 hr			5.00
ECTS Credit of the Course			5.00

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
ÖK8	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK9	5	5	5	5	5	5	5	5	5	5	0	0	0	0	0	0
ÖK10	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**						