ELİPTİK EĞRİLER TEORİSİ ve UYGULAMALARI I

1	Ders Adi:	ELİPTİK EĞRİLER TEORİSİ ve UYGULAMALARI I
2	Ders Kodu:	MAT6111
3	Ders Türü:	Seçmeli
4	Ders Seviyesi	Doktora
5	Dersin Verildiği Yıl:	1
6	Dersin Verildiği Yarıyıl	1
7	Dersin AKTS Kredisi:	5.00
8	Teorik Ders Saati (saat/Hafta)	3.00
9	Uygulama Ders Saati(saat/Hafta)	0.00
10	Laboratuvar Ders Saati (saat/hafta) :	0
11	Dersin Önkoşulu:	yok
12	Dersin Dili:	Türkçe
13	Dersin Veriliş Şekli:	Yüz yüze
14	Dersin Koordinatörü:	Prof. Dr. İSMAİL NACİ CANGÜL
15	Dersi Veren Diğer Öğretim Elemanları:	Prof. Dr. Osman Bizim
16	Koordinatör İletişim Bilgileri:	Uludağ Üniversitesi, Fen-Edebiyat Fakültesi Matematik Bölümü, Görükle Bursa-TÜRKİYE 0 224 294 17 57 / obizim@uludag.edu.tr
17	Dersin WEB adresi:	
18	Dersin Amacı:	Eliptik eğriler, sayılar teorisi, grup ve cisim teorisi, kriptoloji gibi matematiğin önemli teorileri arasındaki ilişkilerin ortaya konulduğu bir derstir. Dersin amacı, öğrencinin tüm bu alanlar arasında bağlantılar kurarak eliptik eğriler teorisine yeni kavramlar ve sonuçlar kazandırmasını sağlamak ve kriptoloji, çarpanlaştırma ve asallık testleri gibi teorinin uygulama alanlarına hazırlık yapmaktır. Böylece öğrencinin lisansüstü özgün çalışma yapabileceği alt yapının oluşturabilmesi hedeflenmektedir.
19	Dersin Mesleki Gelişime Katkısı:	
20	Dersin Öğrenme Kazanımları:	
	1	Eliptik eğriler üzerindeki noktaların grup yapısı, birleşme özelliğinin ispatını öğrenir.
	2	Bir eliptik eğrinin büküm noktaları ve bölüm polinomları kavramları, Weil eşleştirmeleri ve Tate-Licthenbaum eşleştirmeleri öğrenir.
	3	Sonlu cisimler üzerinde tanımlı eliptik eğriler, bu eğriler üzerindeki noktaların sayısı, Hasse teoremi, Frobenius endomorfizmleri, Schoof Algoritması.
	4	Ayrık logaritma problemi, ayrık logaritma da genel hamleler, bebek ve dev adım yöntemleri, Pollard yöntemleri, Pohling-Hellman yöntemini öğrenir.
	5	MOV hamle, Frey-Rück hamlesi ve diğer hamlelerini kullanır.
	6	Q üzerinde tanımlı eliptik eğriler, büküm grupları ve Lutz-Nagell teoremini ve Fermat'ın azalma metodu ve Mordell-Weil teoremini öğrenir.

		7	Cantor algoritması, Zeta fonksiyonları, Fermat'ın son teoremi ve bu teoremin Wiles tarafından verilen ispatını öğrenir.
		8	
		9	
		10	
21	Dersin İçeriği:		
Hafta	**DERS İÇERİKLERİ**		
	Teorik		**Uygulama**
1	Eliptik eğriler ile ilgili temel kavramlar, Eliptik eğriler üzerindeki noktaların grup yapısı, birleşme özelliğinin ispatı.		
2	Diğer eliptik eğri denklemleri, Legendre denklemi, kübik ve quartik denklemler. Bir eliptik eğrinin j-invaryantı, iki eliptik eğrinin izomorfizmi ve endomorfizmi.		
3	Bir eliptik eğrinin büküm noktaları ve bölüm polinomları kavramları, Weil eşleştirmeleri ve Tate-Licthenbaum eşleştirmeleri.		
4	Sonlu cisimler üzerinde tanımlı eliptik eğriler, bu eğriler üzerindeki noktaların sayısı, Hasse teoremi, Frobenius endomorfizmleri, Schoof Algoritması.		
5	Sonlu cisimler üzerinde tanımlı bazı eliptik eğri aileleri, singüler ve süper singüler eğriler.		
6	Ayrık logaritma problemi, ayrık logaritma da genel hamleler, bebek ve dev adım yöntemleri, Pollard yöntemleri, Pohling-Hellman yöntemi.		
7	MOV hamle, Frey-Rück hamlesi ve diğer hamleler.		
8	Eliptik eğri kriptolojisinde temel kavramlar, Diffie-Hellman anahtar değişimi, Massey-Omura kriptosu.		
9	ElGamal kriptosu ve dijital imzaları, dijital imza algoritması.		
10	Q üzerinde tanımlı eliptik eğriler, büküm grupları ve Lutz-Nagell teoremi, Fermat'ın azalma metodu ve Mordell- Weil teoremi		
11	2-Selmer grupları, Shafarevich-Tate grupları, aşikar olmayan Shafarevich-Tate grupları, Galois kohomolojisi.		
12	C üzerinde tanımlı eliptik eğriler, çifte periyodik fonksiyonlar, tor ve eliptik eğriler, periyotların hesaplanması, aritmetik ve geometrik ortalamalar.		
13	Bölüm polinomları ve torsiyon alt gruplar, Doud yöntemi, kompleks çarpım ve nümerik örnekler, j-invaryantın tamlığı.		
14	Hipereliptik eğriler, Cantor algoritması, Zeta fonksiyonları, Fermat'ın son teoremi ve bu teoremin Wiles tarafından verilen ispatına bir bakış.		
22	Ders Kitabı, Referanslar ve/veya Diğer Kaynaklar:		[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	Değerlendirme	
YARIYIL İÇİ ÇALIŞMALARI	**SAYISI**	**KATKI YÜZDESİ**
Ara Sınav	0	0.00
Kısa Sınav	0	0.00
Ödev, Performans	0	0.00
Yıl Sonu Sınavı	1	100.00
Toplam	1	100.00
Yıl içi çalışmalarının Başarıya Oranı		0.00
Finalin Başarıya Oranı		100.00
Toplam		100.00
Kullanılan Ölçme ve Değerlendirme Yaklaşımları		

24 AKTS / İŞ YÜKÜ TABLOSU

ETKİNLİK	SAYISI	Süresi (Saat)	Toplam İş Yükü (Saat)
Teorik Dersler	14	3.00	42.00
Uygulamalı Dersler	0	0.00	0.00
Sınıf Dışı Ders Çalışma Süresi (Ön çalışma, pekiştirme)	14	5.00	70.00
Ödevler, Performanslar	0	0.00	0.00
Projeler	0	0.00	0.00
Arazi Çalışmaları	0	0.00	0.00
Arasınavlar	0	0.00	0.00
Diğer	14	5.00	70.00
Yarıyıl Sonu Sınavı	1	13.00	13.00
Toplam İş Yükü			195.00
Toplam İş Yükü / 30 saat			6.50
Dersin AKTS Kredisi			5.00

25 PROGRAM YETERLİLİKLERİ İLE DERS ÖĞRETİM KAZANIMLARI İLİŞKİSİ TABLOSU

	PY1	PY2	PY3	PY4	PY5	PY6	PY7	PY8	PY9	PY10	PY11	PY12	PY13	PY14	PY15	PY16
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

ÖK: Öğrenme kazanımlar PY: Program yeterlilikleri

Katkı Düzeyi:	1 çok düşük	2 Düşük	3 Orta	4 Yüksek	5 Çok Yüksek