İTÜ
DERS KATALOG FORMU
(COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Sayılar Teorisi	Number Theory

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	AKTS Kredisi (ECTS Credits)	Ders Uygulaması, Saat/Hafta (Course Implementation, Hours/Week)		
				Ders (Theoretical)	Uygulama (Tutorial)	Laboratuar (Laboratory)
MAT 448 MAT 448E	7,8	3	6	3		

Bölüm / Program (Department/Program)	Matematik Bölümü/ Matematik Mühendisliği Department of Mathematics/ Mathematics Engineering			
Dersin Türü (Course Type)	Seçmeli(Elective)	Dersin Dili (Course Language)	Türkçe/İngilizce (Turkish/English)	
Dersin Önkoşulları (Course Prerequisites)	Yok(None)			

Dersin mesleki bileşene katkısı, % (Course Category by Content, %)	**Temel Bilim (Basic Sciences)**	Temel Mühendislik (Engineering Science)	Mühendislik Tasarım (Engineering Design)	İnsan ve Toplum Bilim (General Education)
	100%		-	-

Dersin İçeriği (Course Description)	Bölünebilme,Euclid algoritması,asal sayılar,kongrüanslar,Çin kalan teoremi,Fermat(küçük teoremi,Euler teoremi, primitif kökler,asal-kuvvet modüllü kongrüanslar,Binom teoremi,cebirsel tamsayılar,kuadratik rezidüler,kuadratik reciprosite,Jakobi ve Legendre sembolleri,Euler fonksiyonu, Möbius fonksiyon,çarpımsal fonksiyonlar,sürekli kesirler,rasyonel yaklaşım,Diophant denklemler,Pell denklemi.
	Divisibility, Euclidean algorithm,prime numbers,congruences,Chinese remainder theorem,Fermat's little theorem,Euler's theorem primitive roots,congruences with prime-power moduli,Binomial theorem,algebraic integers,quadratic residues,quadratic reciprocity,Jacobi and Legendre symbols,Euler's function,Möbius inversion formula,multiplicative functions,continued fractions,rational approximation,Diophantine equations,Pell's equation.
Dersin Amacı	1. Tamsayıların özelliklerinin incelenmesi konusunda bilgilendirmek. 2. Öğrencileri ileri düzey sayılar teorisi ve cebir derslerine hazırlamak. 3. Sayılar teorisinin uygulamalarını (Kriptoloji gibi) sergilemek.
(Course Objectives)	1. To provide an introduction to the study of properties of integers. 2. To prepare students to graduate-level courses in number theory and algebra. 3. To demonstrate applications of number theory (such as public-key cryptography)
Dersin Öğrenme Çıktıları (Course Learning Outcomes)	Beu dersi tamamlayan öğrenci, I. Bölünebilme kavram ve özelliklerini anlar.En büyük ortak bölen ve en küçük ortak kat tanımlarını ve özelliklerini bilir. II. Euclid algoritmasını anlar,lineer diofant denklemleri çözebilir,kongrüans kavramını anlar. III. Bir sayının asal olup olmadığını belirleyebilir.Bir sayıyı asal çarpanlarına ayırabilir. IV. Kongrüanslarla temel işlemler yapabilir,lineer kongrüans denklemlerinin bütün çözümlerini bulabilir. Çinlilerin kalan teoremini uygulayabilir. V. Lineer olmayan kongrüans denklemlerinin çözüm kümelerini belirleyebilir,böyle denklem sistemlerini çözebilir. VI. Kuadratik rezidü ve kuadratik resiprosite kavramlarını anlar,aritmetik fonksiyoanları anlar ve özelliklerini kullanabilir. VII. Rasyonel ve reel sayıların sürekli kesirlerle temsillerini anlar
	Students compteting this course will be able to: I. Understand the concept and properties of divisibility. Know the definitions and properties of greatest common divisor and least common multiple. II. Understand the Euclidean algorithm, can solve the linear diophantine equations and understand the concept of congruence. III. Determine if a number is prime, compute the prime power factorization of a number. IV. Be able to perform basic operations with congruences, compute the set of all solutions to linear congruence. Be able to apply Chinese remainder theorem. V. Describe the set of solutions of non-linear congruence equations and be able to solve systems of such equations. VI. Understand the concepts of quadratic residues and quadratic reciprocity.Understand and use arithmetic functions and their properties. VII. Undertsand the representation of rational and real numbers by continued fractions.

Ders Kitabı (Textbook)	Elemantary Number Theory, William Leveque,Dover Pblications,Inc,NY,1990.		
Diğer Kaynaklar (Other References)	Elemantary Number Theory, Charles Vanden Eyden, McGraw-Hill Elemantary Number Theory, Jones,G. and M. Jones, Springer.		
Ödevler ve Projeler (Homework & Projects			
Laboratuar Uygulamaları (Laboratory Work)			
Bilgisayar Kullanımı (Computer Use)			
Diğer Uygulamalar (Other Activities)			
Başarı Değerlendirme Sistemi (Assessment Criteria)	**Faaliyetler (Activities)**	**Adedi (Quantity)**	**Değerlendirmede Katkısı, % (Effects on Grading, %)**
	Yıl İçi Sınavları (Midterm Exams)	**2**	**50%**
	Kısa Sınavlar (Quizzes)		
	Ödevler (Homeworks)		
	Projeler (Projects)		
	Dönem Ödevi (Term Paper)		
	Laboratuar Uygulaması (Laboratory Work)		
	Diğer Uygulamalar (Other Activities)		
	Final Sınavı (Final Exam)	**1**	**50%**

DERS PLANI

Hafta	Konular	Ders Çıktısı
1	Bölünebilme, Bölenler, Bölme Algoritması, En Büyük Ortak Bölen, Aralarında Asal Sayılar	I
2	En Küçük Ortak Kat, Euclid Algoritması	II
3	Lineer Diofant Denklemler, Kongrüanslar	II
4	Asal Sayılar, Asal Çarpanlara Ayırma, Aritmetiğin Temel Teoremi, Asal Sayıların Dağılımı	III
5	Ara Sınav I	II,III
6	Kongrüanslar, Lineer Kongrüanslar, Lineer Kongrüans Sistemler-Çinlilerin Kalan Teoremi	IV
7	Fermat ve Euler Teoremlaeri	IV
8	Polinom Kongrüanslar, Asal Kuvvet Modüllü Kongrüanslar, Primitif Kökler	V
9	Kuadratik Residüler (Legendre sembolü), Kuadratik reciprocite	VI
10	Ara Sınav II	IV,V,VI
11	Asal Kuvvet Modüllü Kuadratik Residüler. Herhangi Modüllü Kuadratik Residüler.	VI
12	Aritmetik Fonksiyonlar. Euler Phi Fonksiyonu, Möbiüs Fonksiyonu, Dirichlet Çarpımı	VI
13	SonluSürekli Kesirler, Sonsuz Sürekli Kesirler, Rasyonel Yaklaşım.	VII
14	Diofant Denklemleri, Pell Denklemi	VI

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Divisibility,Divisors,Division Algorithm,The Greatest Common Divisor and Least Common Multiple	I
2	Euclidean Algorithm, Relatively Prime Numbers	II
3	Linear Diophanetine Equation, Conguences	II
4	Prime Numbers,Prime Factorisation,The Fundamental Theorem of Arithmetic,Distribution of Primes	III
5	Midterm I	II,III
6	Congruences,Linear Congruences,Systems of Linear Congruences-Chinese Remainder Theorem	IV
7	The Teorems of Fermat and Euler	IV
8	Polynomail Congruences, Congruences with prime-power Moduli,Primitive Roots	V
9	Quadratic Residues,(Legendre Symbol), Quadratic Reciprocity	VI
10	Midterm II	IV,V,VI
11	Quadratic Residues for prime-power Moduli, Quadratic Residues for arbitrary Moduli	VI
12	Arithmetic Functions, Euler Phi Function, Möbius Function, Dirichlet Product	VI
13	Finite continued fractions, Infinite continued fractions, Rational Approximations	VII
14	Diophhantine equations, Pell equation	VI

Dersin Matematik Mühendisliği Programıyla İlişkisi

	Programın mezununa kazandıracağı bilgi ve beceriler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
a	Matematik ile ilgili kavramları ve kavramlar arası ilişkileri anlayabilme; kuramsal ve uygulamalı bilgilere sahip olabilme			X
b	Matematik bilgilerini diğer disiplinlere uygulayabilme	X		
c	Bilim ve mühendisliğe ait problemleri tanımlama, modelleme ve çözümleyebilme	X		
d	Çok disiplinli gruplarda çalışabilme ve/veya liderlik yapabilme			
e	Problem çözmek için algoritma ve bilgisayar programı yazma, kullanma ve sayısal çözümleri görselleştirebilme		X	
f	Mesleki ve etik sorumluluk anlayışına sahip olabilme,		X	
g	Türkçe ve/veya İngilizce etkin yazılı ve sözlü iletişim kurabilme,		X	
h	Matematiksel düşünme ve ispat tekniklerini öğrenme ve uygulayabilme			X
i	Hayat boyu öğrenimin önemini kavrama ve uygulayabilme		X	
j	Matematiğin güncel ve çağdaş konularını araştırabilme		X	
k	Matematik ile ilgili ileri düzeydeki bir çalışmayı bağımsız olarak yürütebilme		X	
l	Alanı ile ilgili konularda düşüncelerini ve sorunlara ilişkin çözüm önerilerini yazılı ve sözlü olarak aktarabilme		X	

1: Az Katkı, 2. Kısmi Katkı, 3. Tam Katkı

Relationship between the Course and the Mathematics Engineering Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
a	An ability to understand the concepts of mathematics and the relationships between these concepts; an ability to acquire theoretical and practical knowledge			X
b	An ability to apply knowledge of mathematics to other disciplines	X		
c	An ability to identify, formulate and solve science and engineering problems	X		
d	An ability to function in and/or develop leadership in multi-disciplinary teams.			
e	An ability to write and use algorithms and computer programs to solve problems; an ability to visualize numerical solutions		X	
f	An understanding of professional and ethical responsibility		X	
g	An ability to communicate effectively in written and oral Turkish and/or English.		X	
h	An ability to learn and apply mathematical thinking and proof techniques			X
i	A recognition of the need for, and an ability to engage in, life-long learning		X	
j	An ability to research current and contemporary issues in mathematics		X	
k	An ability to conduct an independent study in advanced mathematics		X	
l	An ability to effectively communicate ideas and solutions proposals related to the field, both orally and in writing		X	

1: Little Contribution, 2. Partial Contribution, 3. Full Contribution

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
Department of Mathematics	2013	