İçerik

Ders Kodu	Dersin Adı	Yarıyıl	Teori	Uygulama	Lab	Kredisi	AKTS
MAT364	Sayılar Kuramına Giriş	6	3	0	0	3	5

Ön Koşul	
Derse Kabul Koşulları	

Dersin Dili	İngilizce
Türü	Seçmeli
Dersin Düzeyi	Lisans
Dersin Amacı	Bu dersin nihai amacı, karakterler ve Gauss toplamlarını kullanarak kuadratik karşılıklılık yasasını ispatlamaktır.
İçerik	Ders, alanın temel kavramlarını ve başlıca araçlarını kapsar; teori ile uygulamayı, yönlendirilmiş örnekler ve kademeli olarak zorlaşan alıştırmalar aracılığıyla ilişkilendirir.
Kaynaklar	William Stein, Elementary Number Theory: Primes, Congruences, and Secrets, https://wstein.org/ent/ent.pdf Kenneth Ireland & Michael Rosen, A Classical Introduction to Modern Number Theory Ivan Niven, Herbert Zuckerman, Hugh Montgomery, An Introduction to the Theory of Numbers

Teori Konu Başlıkları

Hafta	Konu Başlıkları
1	Kongrüanslar; mod n aritmetiği; yol gösterici örnekler ve kestirimler
2	Öklid algoritması ve Bézout özdeşliği. EBOB; modüler tersler; lineer kongrüanslar.
3	Asal sayılar ve tekil çarpanlara ayrışma. Temel lemmalar; kongrüenslere uygulamalar.
4	$(\mathbb{Z}/n\mathbb{Z})^\times$ grubu. Euler'in φ fonksiyonu; Euler teoremi; bir elemanın mertebesi.
5	Kuadratik kalıntılar: keşif. Bir asal modunda kareler; sayma; ilk kalıntı tabloları.
6	Legendre sembolü ve Euler ölçütü. Tanım; çarpımsallık; hızlı hesaplamalar.
7	Ek yasalar. $\left(\frac{-1}{p}\right)$ (mod 4) ve $\left(\frac{2}{p}\right)$ (mod 8); yönlendirmeli ispatlar.
8	Çarpımsal karakterler $(\mathbb{Z}/p\mathbb{Z})^\times$ karakterleri; ortogonallik; kuadratik karakter.
9	Toplamsal karakterler ve birim kökleri. p modunda üstel toplamlar; temel özdeşlikler.
10	Gauss toplamları I. Tanım $\tau(\chi)$; bükme (twisting) özdeşlikleri; mutlak değer ve örnekler.
11	Gauss toplamları II. Kuadratik Gauss toplamının değerlendirilmesi; işaretin $p \bmod 4$ ile belirlenmesi.
12	Kuadratik karşılıklılık. Gauss toplamları ve karakterlerle ispat; adımların sentezi.
13	Jacobi sembolü ve etkin hesaplama. Bileşik paydalara genelleme; dikkat noktaları ve örnekler.
14	Uygulamalar & projeler. $x^2\equiv a \pmod p$ denkliğinin çözülebilirliğine karar verme; mini-projeler ve final portfolyoları.