



ANAHTAR KELİMELER

- ✓ Birim Çember
- ✓ Edwards eğrisi
- ✓ Eliptik eğri
- ✓ Geometrik dizi
- ✓ Huff eğrisi
- ✓ Rasyonel nokta
- ✓ Rasyonel dizi

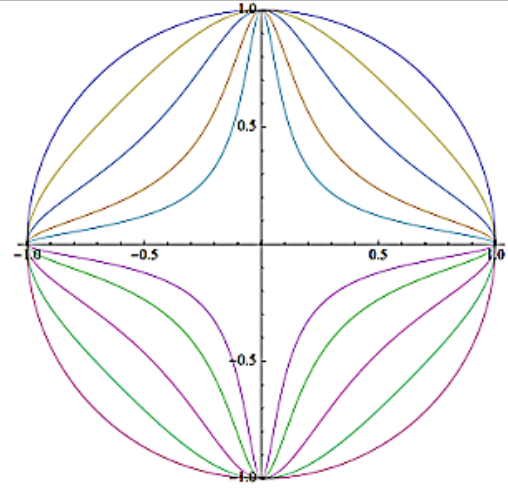
İLETİŞİM

E-POSTA:
gamzesavascelik@gmail.com

TEZ DANIŞMANI

TELEFON:
678-555-0103

E-POSTA:
gsoydan@uludag.edu.tr



CEBİRSEL EĞRİLER ÜZERİNDEKİ RASYONEL DİZİLER

Gamze SAVAŞ ÇELİK

0000-0002-6609-1713

BURSA ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
DOKTORA PROGRAMI

DANIŞMAN

PROF. DR.Gökhan SOYDAN
0000-0002-6321-4132
BURSA ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
BURSA – TÜRKİYE



TEZ ÖZETİ

Bu çalışmada bazı düzlem cebirsel eğriler üzerindeki maksimum uzunluklu rasyonel dizilerin bulunması amaçlanmıştır. Bu amaca ulaşmak için eliptik eğriler, eliptik eğrilerin farklı modelleri ve birim çember üzerindeki rasyonel noktaların x-bileşenlerin oluşturduğu rasyonel diziler incelenmiştir.

Weierstrass formunda eliptik eğriler üzerindeki rasyonel noktaların apsilerinin ardışık küpler olduğu 5-uzunluklu dizilerin varlığı gösterildi. Ayrıca bu dizileri bulunduran eliptik eğrilerin sonsuz çoklukta olduğu ispatlandı. Ardından Edwards eğrisi, (twisted) bükülmüş Edwards eğrisi, Huff eğrisi ve Genel Huff eğrisi üzerinde bulunan maksimum uzunluklu dizileri ile ilgili sonuçlar verildi. Son olarak rasyonel noktaların Birim çember üzerinde 3-uzunluklu geometrik dizisi oluşturduğu gösterildi.

TEZ SONUÇLARININ UYGULAMA ALANLARI

Eliptik eğriler kriptografide kriptografik sistemleri oluşturmak için kullanılır. Kriptografik uygulamalar hızlı ve hassas aritmetiğe ihtiyaç duyar. Ayrıca, eliptik eğrilerle aritmetik işlem maliyetleri, asimetrik ailesinin diğer üyelerine göre daha düşük olduğundan eliptik eğri grupları kullanılır. Örneğin; bükülmüş Edwards eğrilerin kriptografik uygulamaları hesaplamalar açısından daha hızlı olduğundan Edwards eğrilerine göre daha avantajlıdır.

YAYINLAR

Savaş Çelik, G., Soydan, G. 2018. Elliptic curves containing sequences of consecutive cubes. Rocky Mountain J. Math., 48: 2163–2174.

Savaş Çelik, G., Sadek, M., Soydan, G. 2019. Rational sequences on different models of elliptic curves. Glasnik Math., 54: 53–64.

Savaş Çelik, G., Sadek, M., Soydan, G. 2021. Rational Points in Geometric Progression on the Unit Circle. Publ. Math. Debrecen, 98/3-4: 513–520.

