Eğri Tabanlı Kriptografiye Matematiksel Bakış

Proje No: 112T011

Sonuç Raporu

Prof. Dr. Ferruh Özbudak
Prof. Dr. Henning Stichtenoth
Doç. Dr. Cem Güneri
Yrd. Doç Dr. Sedat Akleylek
Yrd. Doç. Dr. Alp Bassa
Yrd. Doç. Dr. Ömer Küçüksakallı
Yrd. Doç. Dr. Seher Tutdere

EKİM 2014

Önsöz

Kriptografik uygulamalar gün geçtikçe yaşamtımızın içinde daha önemli bir rol almaktadır. Kriptografik uygulamaların güvenilir ve verimli bir şekilde uygulanabilmesi büyük önem arzetmektedir. Bu raporda, aynı güvenlik seviyesinde diğer uygulamalara göre daha verimli çözümler sunan eliptik eğriler ve bunların bileşenleri hakkında yapılan çalışmalar özetlenmiştir.

112T011 nolu "Eğri Tabanlı Kriptografiye Matematiksel Bakış" başlıklı bu çalışma, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Almanya Federal Eğitim ve Araştırma Bakanlığı (Federal Ministry of Education and Research-BMBF) tarafından İkili İşbirliği Proje Destekleri kapsamında 15.09.2012 - 15.09.2014 tarihleri arasında desteklenmiştir.

Projenin yürütücülüğünü Ferruh Özbudak yapmıştır. Henning Stichtenoth, Cem Güneri, Alp Bassa, Ömer Küçüksakallı, Sedat Akleylek, Seher Tutdere ve Dilek Buyruk araştırmacı, Pınar Çomak ve Murat Demircioğlu ise bursiyer olarak görev almıştır.

İçindekiler

Tablo Listesi

Şekil Listesi

Özet

Eliptik eğri tabanlı kriptografide belirli sayıda noktası olan bir eliptik eğri bulmak önemli bir uygulamadır. Ayrıca, kriptografi ve kodlama teorisindeki uygulamalar için çok rasyonel noktaya sahip eğrilere ihtiyaç duyulduğundan maksimal eğriler ve çok rasyonel noktaya sahip eğrilerin önemi aşikardır. Bunlara ek olarak, bu eğrilerin tanımlandığı yapılar üzerindeki aritmetiğin hızlandırılması güncel bir konudur.

Cebirsel egrilerin kriptografi ve kodlama teorisinde çok önemli uygulamaları vardır. Bu uygulamalarda sonlu cisimlerin çesitli özellikleri ve bazı kombinatorik yöntemler kullanılır. Bu final raporunda, sonlu cisimler üzerindeki cebirsel eğrilerin cinslerini ve rasyonel nokta sayılarını bulma üzerine sonuçlar, mükemmel lineer olmayan fonksiyonların sınıfları ve bunların yarıcisimlerler olan ilişkileri, sonlu cisimler üzerindeki bazı cebirsel eğrilerin $L-$polinomları, Galois halkalarındaki aritmetik işlemleri, cebirsel fonksiyon cisimleri, ikinci dereceden kompleks sayı cisimlerinin dallanmış (ramified) genişlemelerinde minimal polinomlarının katsayıları küçük olan özel elemanlar ve eşleniklerinin hesaplanması, çok boyutlu sanki-devirsel ve konvolusyon kodları, sonlu cisimler üzerinde kuadratik lineer olmayan eşlemeler hakkında proje kapsamında yapılanlar belirtilmiştir.

Anahtar Kelimeler: cebirsel eğriler, kriptografi, kodlama teorisi, sonlu cisimler, Galois halkaları, polinom çarpımı, kuadratik formlar, rasyonel nokta sayıları, kompleks sayı cisimleri, $L-$polinomları, çok boyutlu sanki-devirsel ve konvolusyon kodları, cebirsel fonksiyon cisimleri kuleleri

Abstract

In curve-based cryptography, it's an important issue to find elliptic curves with desired number of points. Since ellliptic curves are needed with so many rational points applications in cryptography and coding theory, finding maximal curves is very important. Moreover, it's an open problem to improve the arithmetic operations over these curves.

Algebraic curves have very important applications in cryptography and coding theory. In these applications, some combinatorial techniques and properties of finite fields are commonly used. In this final report, we discuss the following issues: genus of algebraic curves over finite fields and counting the number of rational points, perfect nonlinear maps and their relations with semifields, $L-$polynomials of some algebraic curves over finite fields, arithmetic operations in Galois rings, algebraic function fields, certain complex multiplication class fields with smaller generators, convolutional codes, quadratic nonlinear maps over finite fields.

Keywords: algebraic curves, cryptography, coding theory, finite fields, Galois rings, polynomial multiplication, quadratic forms, the number of rational points, complex number fields, $L-$polynomials, multidimensional quasi-cyclic and convolutional codes, towers of algebraic function fields

Bölüm 1

Giriş

Eğri tabanlı kriptografi konusu barındırdığı teorik yapılar ve bunların uygulamadaki kullanımlarından dolayı hem matematikçiler hem de mühendisler tarafından büyük ilgi görmektedir. Bu konudaki çalışmaların yeni kriptografik yöntemlerin çıkmasına, varolanların verimli çalışmasına, kriptografik sistemlerde kullanılan yapı taşlarının farklı ifade edilmesine ve disiplinlerarası işbirliğine katkı sağlamak olarak sınıflandırılan konularda yardımcı olduğu bilinmektedir. Bu proje kapsamında, yapılan akademik çalışmalar ikili işbirliği çerçevesinde düşünülmüştür. Bu bağlamda, üç tane çalıştay düzenlenmiştir.

- **Workshop on Mathematical Aspects of Curve-Based Cryptography**, 8-9 Ekim 2012, Ankara: Çalıştayda Türkiye ekibi tarafından 5, Almanya ekibi tarafından 5 adet sunum gerçekleştirilmiştir. Bu çalıştayda sunulan çalışmalar için özetler kitabı hazırlanmıştır. Daha detaylı bilgiler 1. Gelişme Raporu'nda yer almaktadır.

- **Workshop on Algebraic Curves and Cryptography**, 18-19 Temmuz 2013, Oldenburg, Almanya: Çalıştayda 3 davetli konuşmacının yanısıra, Türkiye ekibinden 3 kişi, Almanya ekibinden 6 kişi sunum yapmıştır. Daha detaylı bilgiler 2. Gelişme Raporu'nda yer almaktadır.

- **Workshop on Mathematical Aspects of Curve-Based Cryptography**, 29-30 Mayıs 2014, İstanbul: Çalıştayda 1 davetli konuşmacının yanısıra, Türkiye ekibinden 3 kişi, bu araştırmacıların danışmanlığını yaptığı 2 yüksek lisans ve doktora öğrencisi ve Almanya ekibinden 4 kişi sunum yapmıştır. Proje kapsamına uygun olarak gerçekleştirilen bu çalıştay ile projenin gidişatı ve olası gelecek çalışmalar hakkında fikir alışverişinde bulunulmuştur. Bu çalıştaya dinleyici olarak katılan doktora öğrencileri, güncel gelişmeleri yakından takip etme imkanı bulmakla beraber, bir çok

açık problem hakkında çözüm önerilerini ve tartışmaları görme imkanı bulmuştur. Detaylar için EK1'e bakınız.

Bunların yanısıra, Almanya proje ekibinden araştırmacılar, Türkiye proje ekibindeki araştırmacıların yer aldığı üniversitelere çeşitli ziyaretler gerçekleştirilmiş ve buralarda sunumlar yapmıştır. Benzer olarak, Türkiye proje ekibindeki araştırmacılar Almanya proje ekibine kısa süreli ziyaretler yapmıştır. Yapılan bu ziyaretler ve konuşma içerikleri gelişme raporlarında detaylı olarak sunulmuştur.

İkili işbirliği kapsamında yapılan akademik çalışmalar ile eğri tabanlı kriptografiye farklı bir bakış açısı kazanılmıştır. Bunlar, hem teorik hem de uygulamalı olarak değerlendirilebilecek bir yapıya sahiptir. Yapılan araştırmalar ile elde edilen sonuçlar çeşitli bilimsel toplantılarda sunulmuş ve dergilere değerlendirilmesi amacıyla gönderilmiştir.

Yapılan bu araştırmaların gelişmesinde, yapılan çalıştaylar, ziyaretler ve sunumlardaki fikir alışverişlerinin önemli bir yer tuttuğunu vurgulamakta fayda görmekteyiz. Bu çerçevede, yapılan çalışmalar ve elde edilen sonuçların özetleri şu şekilde belirtilmiştir:

1. Eliptik eğri tabanlı kriptografide belirli sayıda noktası olan bir eliptik eğri bulmak önemli bir uygulamadır. Bunun başarılması için Hilbert sınıf polinomları kullanılabilir. Bu polinomlar ikinci dereceden kompleks sayı cisimlerinin değişmeli genişlemelerinde uygun elemanlar ve eşlenikleri kullanılarak elde edilir. Sınıf polinomu hesaplaması j değişmezi kullanılarak yapılırsa katsayıları oldukça büyük olan polinomlar elde edilir. Diğer taraftan katsayıları j değişmezinin minimal polinomundan çok daha küçük olan çeşitli elemanlar bulunmuştur. Bu proje kapsamında ikinci dereceden kompleks sayı cisimlerinin dallanmış (ramified) genişlemelerinde minimal polinomlarının katsayıları küçük olan özel elemanlar ve eşleniklerinin hesaplaması verilmiştir. Elde edilen minimal polinomlar literatürdeki benzerlerine göre büyük bir iyileşme göstermektedir.

2. En küçük asal sonlu cisim olan $\mathbb{F}_2$ üzerinde tanımlanan potansiyeli iyi olan ikinci dereceli özyineli kuleler üzerine çalışılmıştır. Bu kulelerin hangi tür denklemlerle ifade edilebileceği üzerine çalışılmış ve bu denklemlerin bir sınıflandırması verilmiştir. Daha sonra da elde edilen bu kuleler için β_1 değeri hesaplanmış ve birçok durumda bu değerin sıfır olduğu sonucuna varılmıştır.

3. Catalan sayılarının özellikle kombinatorikte sıkça karşımıza çıkmasından dolayı modüler polinomun bu ifadesinde katsayı olarak bulunan Catalan sayılarının daha derin kombinatorik bir açıklaması olduğu aşikardır. Literatürde yer alan sonuçlar modüler polinomun tanımında bazı kombinatorik öğelerin varlığına işaret

etmektedir. Bu bağlantıyı incelemek modüler polinomun aritmetik özellklerini anlamak için önemli bir adım oluşturacaktır. Proje kapsamında $\Phi_T(X,Y)$ modüler polinomunun katsayılarında karşımıza çıkan Catalan sayılarını kombinatorik yönden açıklamaya çalışılmıştır.

4. Sonlu cisimler üzerindeki cebirsel eğrilerin cinslerini (genus) ve rasyonel nokta sayılarını kesin olarak bulmak zor bir problemdir ve kriptografide önemli bir yere sahiptir. 2'den farklı herhangi bir asal sayının kuvveti olmak üzere $n|m$ şartını sağlayan keyfi h,n,m pozitif tam sayıları ve $\gamma,\alpha \in \mathbb{F}_{q^m}$, $\gamma \neq 0$ elemanları için $y^{q^n}-y=\gamma x^{q^h+1}-\alpha$ eğrisinin bir çok durumdaki $\mathbb{F}_{q^m}$-rasyonel noktalarının sayısı hesaplanmıştır.

5. Mükemmel lineer olmayan fonksiyonlar, kriptografide önemli bir yeri olan bükük (bent) ve düzlemsel (planar) fonksiyonları içeren önemli bir sınıftır. Mükemmel lineer olmayan fonksiyonların hangi sınıflarının genişletilemez (non-extendable) olduğunu incelemek zor bir problemdir. Ayrıca konunun yarıcisimlerle (semifield) doğal ilişkileri vardır. Birçok $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyon sınıfının genişletilemez olduğunu gösterilmiştir.

6. Cebirsel eğrilerin bazı karakteristik özelliklerini hesaplamada kullanılan L-polinomlarını bulmada bir çok önemli sonuç elde edilmiştir.

7. n pozitif bir tamsayı olmak üzere eleman sayısı 4^n olan Galois halkasındaki verimli polinom çarpımı üzerine çalışma yapılmıştır. Sonlu cisimlerdeki polinom çarpımı için kullanılan yöntemler incelenmiş olup, bunların Galois halkasındaki polinom çarpımına uyarlanması yapılmıştır. Galois halkasındaki iki polinomun çarpımı Toeplitz matrisi ve vektör çarpımı şeklinde ifade edilerek alt üssel alan karmaşıklığı elde edilmiştir. Bu çalışma literatürde Galois halkasındaki iki polinomu alt üssel alan karmaşıklığı ile çarpan ilk yöntem olarak göze çarpmaktadır.

8. Sanki-devirsel kodların çok boyutlu benzerlerini tanımlamak ve bir boyutta sanki-devirsel kodlarla konvolusyon kodları arasındaki ilişkinin, çok boyutlu konvolusyon kodları ile çok boyutlu sanki-devirsel kodlar arasında da var olduğu gösterilmiştir.

Proje kapsamındaki çalışmalarımızı ve araştırmalarımızı bu Proje Sonuç Raporu'nda TÜBİTAK'ın "Proje Rapor Yazımında Uyulması Gereken Kurallar" (*https://ardeb-pts.tubitak.gov.tr/mainPage.htm* adresinden temin edilmiştir) belgesinde istenen şekilde düzenledik ve bu raporda yer alacak önemli gördüğümüz sonuçlarımızı

aktarıyoruz. Bu sonuçların bilimsel dergi ve bilimsel toplantılarda yayınlanması ve sunulması ile ilgili referans bilgileri de aşağıda verilmiştir.

"Proje Sonuç Raporu Yazımında Uyulması Gereken Kurallar" belgesi gereğince bu raporun ana metni

1. Giriş
2. Literatür Özeti, Gereç, Yöntem ve Bulgular
3. Tartışma ve Sonuç

bölümlerinden oluşturulmuştur. Proje sonuç raporunun oluşturulmasında bir bütünlük sağlayabilmek için makale yazım formatı baz alınmıştır. Bundan dolayı, Gereç, Yöntem ve Bulgular bölümü içerisinde her bir çalışma için literatür özeti ayrıca verilmiştir. Bu sayede, raporun alt bölümlerinde tutarlılık sağlanması ve konuyla ilgili bir araştırmacının ilgili açıklamalara kolayca ulaşması hedeflenmiştir.

Bu projede elde edilen sonuçlar 8 alt bölümde sunulmuştur. Bu sınıflandırma yapılırken, elde edilen sonuçların birbirleri ile olan ilişkileri gözetilmiş ve bunlar açıkca ifade edilmeye çalışılmıştır. Her bölüm aynı bir makale düzeninde oluşturulmuş ve içerisinde konu hakkında kısa bir giriş, önceki çalışmalar, kullanılan tekniklerin kısa açıklanması ve elde edilen sonuçlar olarak verilmiştir. Bu bölümler sırasıyla şunlardır (bkz. Gereç, Yöntem ve Bulgular Bölümü alt bölümleri):

2.1 Daha Küçük Üreteçler ile Karmaşık Çarpım Sınıf Cisimleri

2.2 $\mathbb{F}_2$ Üzerinde Tanımlanan İkinci Dereceli Özyineli Fonksiyon Cisimleri Kuleleri

2.3 Cebirsel Eğriler, Rasyonel Noktaları, Modüler Polinom ve Uygulamaları

2.4 $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ Eğrisinin $\mathbb{F}_{q^m}$ Üzerindeki Rasyonel Noktaları

2.5 Genişletilemez $\mathbb{F}_q$-kuadratik Mükemmel Lineer Olmayan Fonksiyonlar

2.6 $\mathbb{F}_{q^m}$ Üzerinde $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ Eğrisinin L-polinomları

2.7 Galois Halkalarında Polinom Çarpımı

2.8 Çok Boyutlu Sanki-Devirsel ve Konvolusyon Kodları

Tartışma ve Sonuç bölümünde de her bir alt bölümde edilen sonuçlar hakkında kısa bir açıklama ve gelecek çalışmalar için bilgiler verilmiştir.

Bölüm 2

Literatür Özeti, Gereç, Yöntem ve Bulgular

Bu bölümde, proje kapsamında çalışılan konuların literatürdeki yeri, kullanılan yöntemler ve elde edilen sonuçlara yer verilmiştir. Bu bölüm 8 tane alt bölümden meydana gelmektedir. Her bölüm aynı bir makale düzeninde oluşturulmuş ve içerisinde konu hakkında kısa bir giriş, önceki çalışmalar, kullanılan tekniklerin kısa açıklanması ve elde edilen sonuçlar olarak verilmiştir. Burada yer alanlar aşağıdaki şekilde sınıflandırılmıştır:

2.1 Daha Küçük Üreteçler ile Karmaşık Çarpım Sınıf Cisimleri

2.2 $\mathbb{F}_2$ Üzerinde Tanımlanan İkinci Dereceli Özyineli Fonksiyon Cisimleri Kuleleri

2.3 Cebirsel Eğriler, Rasyonel Noktaları, Modüler Polinom ve Uygulamaları

2.4 $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ Eğrisinin $\mathbb{F}_{q^m}$ Üzerindeki Rasyonel Noktaları

2.5 Genişletilemez $\mathbb{F}_q$-kuadratik Mükemmel Lineer Olmayan Fonksiyonlar

2.6 $\mathbb{F}_{q^m}$ Üzerinde $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ Eğrisinin L-polinomları

2.7 Galois Halkalarında Polinom Çarpımı

2.8 Çok Boyutlu Sanki-Devirsel ve Konvolusyon Kodları

2.1 Daha Küçük Üreteçler ile Karmaşık Çarpım Sınıf Cisimleri

2.1.1 Özet

Hilbert'in 12. problemi sayı cisimlerinin azami değişmeli genişlemelerinin analitik bir fonksiyonun değerleri ile elde edilip edilemeyeceğini sorar. Bu problem Kronecker-Weber teoremindeki üstel $e^{2\pi ix}$ fonksiyonun genelleştirilmiş halini bulmaya denktir. Kompleks kuadratik durumda Hilbert'in 12. problem Kronecker'in gençlik hayali olarak da bilinir (Kronecker's Jugendtraum) ve ispatlanmıştır. Bu soruya ilk ispat Hasse tarafından 1927 yılında verilmiştir (Hasse, 1931). Hasse'nin ispatı 1958 yılında Deuring tarafından komplex çarpım (complex multiplication) teorisi kullanılarak oldukça basitleştirilmiştir (Deuring, 1958). Deuring bu ispatı eliptik eğriler üzerinde noktalar veren Weierstrass $\wp$ fonksiyonu ve Hilbert sınıf cismini üreten j-değişmezi ile elde etmiştir. Bu ispatın daha modern bir versiyonu görmek için (Silverman, 1994)'e bakılabilir.

Shimura'nın karşılıklılık teoremi (Shimura's reciprocity law) kompleks kuadratik sınıf cisim teorisi ile modüler fonksiyonlar teorisi arasında Galois teorisini de kullanarak bir bağlantı kurar (Shimura, 1971). Shimura'nın bu teoremi sayesinde değişmeli genişlemelerdeki elemanların Galois grubun etkisi altındaki karşılıkları bulunabilir. Bunun yanında hesaplamalar 1'in köklerinden gelen değerler yüzünden oldukça karmaşıktır.

Eliptik eğrilerin kompleks çarpım teorisi sonlu cisimler teorisinde ve uygulamalarında önemli bir rol oynar. Örneğin rasyonel noktası sayısı bilinen eliptik eğriler üretmek gibi. Bu komplex çarpım uygulaması en iyi biçimde Hilbert sınıf cismi kullanılarak yapılabilir. Katsayıları j değişmezinin minimal polinomundan çok daha küçük olan çeşitli elemanlar bulunmuştur. Bu çalışmaların detayları için (Gee, 2001), (Enge and Morain, 2009), (Leprévost and Uzunkol, 2011) ve (Uzunkol, 2013)'a bakılabilir. Ayrıca benzer inşaalar asallık ispatı (Atkin and Morain, 1993), (Morain, 2007) ve eşleme tabanlı kriptografide (Blake and Smart, 1999), (Blake and Smart, 2005), (Freeman and Teske, 2010) kullanılmaktadır.

$m \not\equiv 2 \pmod 4$ ve $2 \leq a \leq m-1$ birer doğal sayı olsunlar. Ayrıca $\mathbb{Q}_{(m)}$ rasyonel sayıların ışın sınıf gelişlemesi olsun. Çok iyi bilindiği gibi bu genişleme m'ninci reel siklotimik cisim $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$'dir. Bu genişleme rasyonel sayılara $\psi(1-e^{2\pi iz})$ fonksiyonun $\psi(a/m)$ değerleri eklenerek elde edilebilir. Ayrıca siklotomik birim elemanların aşağıdaki gibi sade bir ifadesi vardır (Washington, 1997):

$$\zeta_m^{(1-a)/2}\frac{1-\zeta_m^a}{1-\zeta_m} = \pm\frac{\sin(\pi a/m)}{\sin(\pi/m)} \in \mathcal{O}^*_{\mathbb{Q}_{(m)}}.$$

Komplex kuadratik durumda da özel birim elemanlar vardır. Bu özel elemanlar eliptik birim elemanlar olarak bilinir. Bu çalışmadaki amacımız sınıf cisimlerini elde etmemizi sağlayan bu elemanların minimal polinomları hesaplamak için bir algoritma vermektir. Bu eliptik birim elemanlar aynı işlevi gören diğer üreteçlere göre oldukça küçük katsayılı minimal polinomlara sahiptir. Ayrıca siklotomik birim elemanlara benzer şekilde Siegel ϕ fonksiyonun basit bir kesiri biçiminde verilebilir.

Ramachandra 1964 yılında Kronecker'in limit formülünü kullanarak çeşitli fonksiyonların değerlerinin çarpımı olacak şekilde ışın sınıf cisimlerinin üreteçlerini elde etmiştir (Ramachandra, 1964). Bu üreteçler çok sayıda çarpan içerdiği için hesaplamalar için uygun değildir. Schertz'in yeni ispatlanan (Jung and Shin, 2011) bir sanısı (Schertz, 1997) aşağıda verilen elemanların $K_{(N)}$'i kompleks kuadratik K üzerinde ürettiğini söyler:

$$\phi(0, 1/N, \tau)^{12N/\gcd(6,N)}$$

Bettner ve Schert çok kısıtlı durumlarda Siegel ϕ fonksiyonunundan oluşan bir çarpımın ışın cisim genişlemesi $K_{(N)}$'de kaldığını göstermişlerdir. Ayrıca bu elemanların $K_{(N)}$'yi ürettiğini de iddia etmişlerdir.

Bu çalışmada ortaya konan üreteçlerin önemli bir avantajı çok basit bir Siegel ϕ fonksiyonu kesiri olarak üretilmesidir. Bunun sayesinde yukarıdaki ifadede görülen $12N/\mathrm{OBEB}(6, N)$ büyüklüğündeki bir kuvvetten kurtulabiliyoruz. Bir diğer avantaj hiçbir kısıtlayıcı durum koymayıp herhangi bir $\mathfrak{f}$ modulusu için üreteçlerimizi elde edebilmemizdir. Yaptığımız çalışma uluslararası saygın bir dergiye gonderilmiş olup arxiv.org'ta 1307.6273 numarasıyla da bulunabilir.

2.1.2 Giriş

Shimura'nin Karşılıklılık Teoremi

K diskriminantı d_K olan kompleks kuadratik bir sayı cismi olsun. Bu sayı cisminin tamsayılar halkasını $\mathcal{O}_K$ ile gösterelim. Bu çalışmamızdaki sonuçları $\mathcal{O}_K$'nın azami alt halkası için formüle edeceğiz. Çalışmalarımız daha sade ifade edebilmek için bu halkayı $\mathcal{O}$ ile göstereceğiz.

Bu bölümde Shimura'nin karşılıklılık teoremini Gee ve Stevenhagen'in ele aldığı biçimde özetleyeceğiz (Gee, 2001), (Stevenhagen, 2001). Aksi söylenmediği sürece bu bölümdeki tanımlara ve sonuçlara (Lang, 1987), (Stark, 1980) ve (Shimura, 1971) referanslarından ulaşılabilir. Bunun yanında Siegel ϕ fonksiyonun tanımını ve sağladığı dönüşüm formüllerini özetleyeceğiz. Bu formüllerin detaylı bir şekilde ele alınışını görmek için (Stark, 1980)'a bakılabilir.

Verilen bir kompleks kuadratik sayı cismi için $\mathrm{Cl}(K)$ ideal sınıf grubu ve H de Hilbert sınıf cismi olsun. $[\cdot, K]$ ile sonlu $K-$idèl grubu üzerindeki Artin eşlemesini gösterelim. Bu durumda sınıf cismi teorisinin temel teoremi aşağıdaki tam dizi ile özetlenebilir:

$$1 \longrightarrow K^* \longrightarrow \widehat{K^*} \xrightarrow{[\cdot,K]} \mathrm{Gal}(K^{ab}/K) \longrightarrow 1. \tag{2.1}$$

Birim elemanlar grubu yarı Artin eşlemesi altında $\mathrm{Gal}(K^{ab}/K)$ Galois grubunun ters görüntüsüdür.

$$\widehat{\mathcal{O}^*} = \left(\lim_{\leftarrow N}(\mathcal{O}/N\mathcal{O})\right)^* = (\mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^* \subseteq \widehat{K^*}$$

Sınıf cisim teorisi kullanarak aşağıdaki tam diziyi elde ederiz:

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \widehat{\mathcal{O}^*} \xrightarrow{[\cdot,K]} \mathrm{Gal}(K^{ab}/H) \longrightarrow 1. \tag{2.2}$$

$\tau \in K$ üst yarı düzlemde minimal polinomu $Ax^2 + Bx + C$ olan bir eleman olsun. Ayrıca $B^2 - 4AC = d_K$ olsun. Klasik j fonksiyonu $\Gamma := \mathrm{SL}(2, \mathbb{Z})$ grubunun etkisi altında değişmezdir ve kompleks çarpım teorisi $j(\tau)$ değerinin Hilbert sınıf cismi için K üzerinde bir üreteç olduğunu söyler.

Dallanmış değişmeli genişlemeleri üretmek için modüler fonksiyonları kullabiliriz. Düzeyi N olan bir modüler bir fonksiyon Γ'nın $\Gamma(N) = \ker[\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})]$ kongrüans altgrubunun etkisi altında değişmez kalan meromorfik fonksiyon olarak tanımlanır. Ayrıca q açılımı her boynuzda $\mathbb{Q}(\zeta_N)$'den katsayılara sahipse bu modüler fonksiyona aritmetik denir. Düzeyi N olan bütün aritmetik modüler fonksiyonları içeren cismi $\mathcal{F}_N$ ile gösterilir. Örneğin $\mathcal{F}_1 = \mathbb{Q}(j)$ olur.

Kompleks çarpım teorisinin bir sonucu olarak her bir $g \in \mathcal{F}_N$ modüler fonksiyonu için $g(\tau)$ değeri $K_{(N)}$ sayı cismi içinde kalır. Bunun bir ispatı için (Gee, 2001, p. 41)'ye bakılabilir.

Düzeyi N olan bütün modüler fonksiyonları içeren $\mathcal{F}_N$ cismi $\mathcal{F}_1$'nin bir Galois genişlemesidir. Karşılık gelen Galois grubu ise aşağıdaki gibidir:

$$\begin{aligned}\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) &\cong \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \rtimes (\mathbb{Z}/N\mathbb{Z})^* \\ &\cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm I_2.\end{aligned}$$

Galois grubunun $\mathcal{F}_N$ üzerindeki etkisi kolayca açıklanabilir. Eğer $A \in \Gamma$ ise

$$f(z) \circ A = f(Az)$$

olur. Ayrıca N ile aralarında asal bir d tamsayısı için $A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]$ ise

$$f(z) \circ A = \left(\sum_{n=n_0}^{\infty} \alpha_n q_N^n \right) \circ A = \sum_{n=n_0}^{\infty} \alpha_n^{\sigma} q_N^n$$

olur. Burada σ eşlemesi $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ genişlemesinin $\zeta_N^{\sigma} = \zeta_N^d$ şeklinde verilen otomorfizmasıdır.

Bütün düzeydeki modüler fonksiyonları bir arada ele almak için idèlik formülasyonu ele alabiliriz. Gee aşağıdaki gibi bir tam diziden yola çıkılabileceğini söyler (Gee, 2001, p. 10):

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1(\zeta_N)) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow \det & & \downarrow & & \\
1 & \longrightarrow & 1 & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathcal{F}_1(\zeta_N)/\mathcal{F}_1) & \longrightarrow & 1.
\end{array} \tag{2.3}$$

Bütün aritmetik modüler fonksiyonları içeren cismi $\mathcal{F} = \cup_{N \geq 1} \mathcal{F}_N$ şeklinde gösterelim. Bu cismin Galois grubunu projektif limit alarak oluşturabiliriz:

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}(2, \widehat{\mathbb{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1. \tag{2.4}$$

Stevenhagen'in verdiği Shimura'nın karşılıklılık teoremini açık versiyounu kullanarak daha önce verdiğimiz tam diziler, (2.2) ve (2.4), arasında aşağıdaki gibi bir bağlantı elde ederiz:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \prod_p{}' \mathcal{O}_p^* & \longrightarrow & \mathrm{Gal}(K^{ab}/H) & \longrightarrow & 1 \\
 & & & & \downarrow h_\tau & & & & \\
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}(2, \widehat{\mathbb{Z}}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) & \longrightarrow & 1.
\end{array} \tag{2.5}$$

Burada $h_\tau : \prod_p{}' \mathcal{O}_p^* \to \mathrm{GL}(2, \widehat{\mathbb{Z}})$ olup $x \in \prod_p{}' \mathcal{O}_p^*$ idèlini uygun bir matrisin devriğine götürür. Aşağıdaki (2.5) denkleminde bahsi geçen h_τ eşlemesinin nasıl hesaplanacağı verilmiştir:

$$h_\tau : \ x = sA\tau + t \mapsto \left[\begin{smallmatrix} t - Bs & -Cs \\ sA & t \end{smallmatrix}\right]. \tag{2.6}$$

Karşılıklılık eşlemesini kullanarak $\widehat{\mathcal{O}^*}$ grubunun $\mathcal{F}$ üzerindeki etkisini aşağıdaki gibi elde ederiz (Stevenhagen, 2001, p. 165):

$$(g(\tau))^{[x^{-1}, K]} = (g^{h_\tau(x)})(\tau).$$

Stevenhagen karşılıklılık kuralını sonlu grupların tam dizileri haline indirgemiştir (Stevenhagen, 2001, p. 167),

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & (\mathcal{O}/N\mathcal{O})^* & \longrightarrow & \mathrm{Gal}(K_{(N)}/H) & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle h_{\tau,N}} & & & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) & \longrightarrow & 1. \end{array}$$

Bu eşleme altında $(\mathcal{O}/N\mathcal{O})^*$ grubunun $h_{\tau,N}$ altındaki görüntüsü $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ grubunun karşılık gelen alt grubudur.

$$\mathcal{W}_{N,\tau} = \left\{ \left[\begin{smallmatrix} t-Bs & -Cs \\ sA & t \end{smallmatrix} \right] \in \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z}) : \ s,t \in \mathbb{Z}/N\mathbb{Z} \right\}. \tag{2.7}$$

$\mathrm{Cl}(d_K)$ indirgenmiş ikili kuadratik formlardan oluşan grup olsun. Formların oluşturduğu grup $\mathrm{Cl}(d_K)$ ile ideallerin oluşturduğu sınıf grubu birbiriyle eş yapılıdır (Cox, 1989, p. 50). Bu eş yapılar arasındaki eşleme $Q = [a,b,c]$ kuadratik formunu $\tau_Q = (-b+\sqrt{dk})/2a$ tarafında üretilen kesirsel ideale gönderilerek elde edilir. Gee aşağıdaki teoremi ispatlamıştır (Gee, 2001, Chapter 1):

Teorem 2.1.1. *$Q = [a,b,c]$ formu diskriminnantı d_K olan indirgenmiş ikili bir formve $\tau_Q = (-b+\sqrt{dk})/2a$ olsun. u_Q elemanı $u_Q = (u_p)_p \in \prod_p \mathrm{GL}(2,\mathbb{Z}_p)$ çarpımıyla verilsin ve bu çarpımdaki her bir terim aşağıdaki gibi tanımlansın*

- $d_K \equiv 0 \bmod 4$ *için:*

$$u_p = \begin{cases} \left[\begin{smallmatrix} a & b/2 \\ 0 & 1 \end{smallmatrix} \right] & \text{eğer } p \not| a, \\ \left[\begin{smallmatrix} -b/2 & -c \\ 1 & 0 \end{smallmatrix} \right] & \text{eğer } p|a \text{ ve } p \not| c, \\ \left[\begin{smallmatrix} -a-b/2 & -c-b/2 \\ 1 & -1 \end{smallmatrix} \right] & \text{eğer } p|a \text{ ve } p|c, \end{cases}$$

- $d_K \equiv 1 \bmod 4$ *için:*

$$u_p = \begin{cases} \left[\begin{smallmatrix} a & (b-1)/2 \\ 0 & 1 \end{smallmatrix} \right] & \text{eğer } p \not| a, \\ \left[\begin{smallmatrix} -(b+1)/2 & -c \\ 1 & 0 \end{smallmatrix} \right] & \text{eğer } p|a \text{ ve } p \not| c, \\ \left[\begin{smallmatrix} -a-(b+1)/2 & -c-(1-b)/2 \\ 1 & -1 \end{smallmatrix} \right] & \text{eğer } p|a \text{ ve } p|c. \end{cases}$$

$g \in \mathcal{F}$ modüler bir fonksiyon ise

$$g(\tau)^{[x_Q^{-1},K]} = g^{u_Q}(\tau_Q)$$

olur. Burada g fonksyionu τ değerinde tanımlı ve sonludur. Ayrıca $x_Q = (x_p)_p$ ve

$$x_p = \begin{cases} a & \text{eğer } p \not| a, \\ a\tau_Q & \text{eğer } p|a \text{ ve } p \not| c, \\ a(\tau_Q - 1) & \text{eğer } p|a \text{ ve } p|c. \end{cases}$$

Jung, Koo ve Shin'in 2011 yıllı makalesinde aşağıdaki teorem ispatlanmıştır (Jung and Shin, 2011, p. 418–420):

Teorem 2.1.2. *Diyelim ki $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ ve $N > 0$. O zaman aşağıdaki gibi birebir ve örten bir Ψ eşlemesi vardır:*

$$\Psi : \mathcal{W}_{N,\tau}/\{\pm I_2\} \times \mathrm{Cl}(d_K) \longrightarrow \mathrm{Gal}(K_{(N)}/K)$$

$$(\alpha, Q) \longmapsto (g(\tau) \mapsto g^{\alpha \cdot u_Q}(\tau_Q))_{g \in \mathcal{F}_{N,\tau}}$$

Siegel ϕ Fonksiyonu İçin Dönüşüm Formülleri

Stark Siegel ϕ fonksiyonunu kompleks kuadratik sayılarda hesaplayarak $K_{\mathfrak{f}}$ ışın sınıf cisminde elemanlar elde eder. Üst yarı düzlemde verilen $z \in \mathfrak{h}$ ve $u, v \in \frac{\mathbb{F}_2[x]}{\langle x^7+1 \rangle}$ için $\gamma = uz + v$ olsun. Siegel ϕ fonksiyonu sonsuz bir çarpım biçiminde tanımlanır:

$$\phi(u, v, z) = -ie^{\frac{\pi i z}{6}} e^{\pi i u \gamma}(e^{\pi i \gamma} - e^{-\pi i \gamma}) \prod_{n=1}^{\infty}(1 - e^{2\pi i(nz+\gamma)})(1 - e^{2\pi i(nz-\gamma)}).$$

Önerme 2.1.3. *Siegel ϕ fonksiyonu aşağıdaki dönüşüm özelliklerini sağlar:*

1. $\phi(u, v+1, z) = -e^{\pi i u}\phi(u, v, z)$
2. $\phi(u+1, v, z) = -e^{-\pi i v}\phi(u, v, z)$
3. $\phi(u, v, z+1) = e^{\pi i/6}\phi(u, u+v, z)$
4. $\phi(u, v, -1/z) = e^{-\pi i/2}\phi(v, -u, z)$

İspat. Bu özellikler Kronecker'in ikinci limit formülünün sonuçlarıdır ve ispatları için (Stark, 1980, p. 207-208) referansına bakılabilir. □

Aralarında asal $N > 1, s, t$ tamsayılarını düşünelim. Ayrıca $u = s/N, v = t/N$ ve $M = 12N^2$ olsun. O zaman Siegel ϕ fonksiyonu $\phi(u, v, z)$ düzeyi M olan bir modüler fonksiyon verir (Stark, 1980, p. 208). Şimdi bu fonksiyonlar üzerinde bazı temel matrislerin etkisini incelyeceğiz. İlk olarak $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ ve $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ elemanları tarafından üretilen

$\mathrm{SL}(2,\mathbb{Z})$ grubunu ele alalım. Bu gruptan $T \mapsto e^{\pi i/6}$ ve $S \mapsto e^{-\pi i/2}$ olacak şekilde $\omega : \mathrm{SL}_2(\mathbb{Z}) \to \langle\zeta_{12}\rangle$ çarpımsal bir homomorfizma elde ederiz. Bu eşleme Önerme 2.1.3 ile uyumludur ve determinantı 1 olan tamsayı girdili bir A matrisi için aşağıdaki eşitlik sağlanır:

$$\phi(u,v,z)\circ A = \phi(u,v,Az) = \omega(A)\phi((u,v)A,z)$$

Özel olarak $S^2 = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ ve bunun sonucunda

$$\phi(u,v,z) = -\phi(-u,-v,z)$$

olur. Genel olarak ise $\omega(A)$ değerini hesaplamak için A'yı S ve T cinsinden çarpanlarına ayırmaya gerek yoktur. Verilen bir $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma$ matrisi için, aşağıdaki fonksiyonları tanımlayalım:

$$\begin{aligned} p_3(A) &= ac(b^2+1) + bd(a^2+1) \\ p_4(A) &= (b^2 - a + 2)c + (a^2 - b + 2)d + ad. \end{aligned}$$

Herglotz (Herglotz, 1921) aşağıdaki formülü ispatlamıştır:

$$\omega(A) = \zeta_4^{p_4(A)}\zeta_3^{-p_3(A)}. \tag{2.8}$$

Bir sonraki adım olarak $\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]$ biçimindeki matrislerin etkisini ele alalım. $\phi(u,v,z)$ fonksiyonunun katsayıları $\mathbb{Q}(\zeta_M)$ cisminde yer alır ve $\sigma : \zeta_M \mapsto \zeta_M^d$ otomorfizmasının ϕ üzerindeki etkisi v değerinin d ile çarpılmasıyla elde edilir. Sonuç olarak aşağıdaki eşitliği elde ederiz:

$$\phi(u,v,z)\circ \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right] = \phi(u,vd,z)(-1)^{(d-1)/2}.$$

Ayrıca $\left[\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ matrisinin etkisi de aşağıdaki gibi kolayca elde edilebilir:

$$\begin{aligned} \phi(u,v,z)\circ \left[\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right] &= \phi(u,v,z)\circ \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \\ &= -i\phi(v,-u,z)\circ \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \\ &= -i\phi(v,-ud,z)\circ \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \\ &= -\phi(-ud,-v,z) \\ &= \phi(ud,v,z). \end{aligned} \tag{2.9}$$

Eliptik Birim Elemanlar

K kompleks kuadratik bir sayı cismi ve $\mathfrak{f} \subset \mathcal{O}_K$ bu cismin has bir ideali olsun. Bu bölümde Siegel ϕ fonksiyonun değerlerinin kesiri biçiminde verilen bazı özel elemanların

bütün eşleniklerini hesaplamak için bir algoritma vereceğiz. Bu eliptik birim elemanlar Stark'ın $\mathfrak{f} = \mathfrak{p}^s$ için olan temel sonucunun genelleştirilmiş halidir. Burada $\mathfrak{p}$ derecesi bir olan ve normu $6d_K$'yi bölmeyen K'nın asal bir idealidir (Stark, 1980, p. 229).

Verilen bir $\mathfrak{f} \neq (1)$ ideali için f bu idealdeki en küçük pozitif tamsayı olsun. Işın sınıfı grubundaki her $\mathfrak{c}$ sınıfı için $\mathfrak{f}$'ye asal ve bütün $\mathfrak{a} \in \mathfrak{c}$ için $\mathfrak{ab}$ temel ideal olacak şekilde bir $\mathfrak{b}$ ideali seçelim. Ayrıca $\mathcal{O}$'daki bir α elemanı için $\mathfrak{ab} = (\alpha)$ olduğunu varsayalım. Bunun yanısıra $\mathfrak{bf} = [\omega_1, \omega_2]$ ve $\tau = \omega_1/\omega_2 \in \mathfrak{h}$ olsun. Bu durumda aşağıdaki elemanlar sadece ve sadece $\mathfrak{c}$ sınıfına bağlı olacaktır (Stark, 1980, Lemma 7)

$$E(\mathfrak{c}) = \phi(u, v, \tau)^{12f} \in K_{\mathfrak{f}} \tag{2.10}$$

Kompleks kuadratik τ değeri bir kesirsel ideale denk gelir ve bir indirgenmiş kuadratik form Q için τ değeri τ_Q değerine dönüştürülebilir. O yüzden genelliği kaybetmeden $\tau = \tau_Q$ olduğunu varsayabiliriz.

Diyelim ki $\mathfrak{p} \subset \mathcal{O}_K$ birinci dereceden $\mathfrak{c}$ sınıfında olan bir asal ideal olsun. Ayrıca bu idealin normunun p olduğunu ve $12f$'yi bölmediğini varsayalım. Stark $E(\mathfrak{c})/E(1)^p$ kesrinin $K_{\mathfrak{f}}$ ışın sınıf cismindeki bir elemanın $12f$'ninci bir kuvveti olduğunu göstermiştir. Eğer $K_{\mathfrak{f}}$ cismi 1'in tam olarak W tane kökünü içeriyorsa, o zaman $W|12f$ ve $E(\mathfrak{c})^W$ bir cebirsel tamsayının $12f$'ninci kuvveti olur (Stark, 1980, Lemma 9).

$\mathrm{Gal}(K_{\mathfrak{f}}/K)$ Galois grubunun $\mathfrak{c}$ sınıfına karşılık gelen elemanı $\sigma_{\mathfrak{c}}$ olsun. Bu elemanın 1'in kökleri üzerindeki etkisi şöyledir: $\zeta_W^{\sigma_{\mathfrak{c}}} = \zeta_W^{d_{\mathfrak{c}}}$. Burada $d_{\mathfrak{c}} \equiv |p| \bmod W$ biçiminde elde edilir. $e_{\mathfrak{c}}$ tamsayısını $e_{\mathfrak{c}} = W/(W, d_{\mathfrak{c}} - 1)$ biçiminde tanımlayalım. Stark'ın sonuçlarından yola çıkarak aşağıdaki elemanı elde edebiliriz:

$$\left(\frac{E(\mathfrak{c})}{E(1)}\right)^{e_{\mathfrak{c}}}. \tag{2.11}$$

Bu elemanın normu 1 olmasının yanı sıra, cebirsel bir tamsayının $12f$'ninci kuvvetidir (Stark, 1980, Theorem 1). Bir diğer deyişle bu basit kesir bize bir eliptik birim eleman verir.

Hilbert sınıf cismine indirgenişi $\mathfrak{f}$'yi içerecek şekilde bir $\mathfrak{c}_0$ ideal sınıfı seçebiliriz. Bu durumda seçeceğimiz $\mathfrak{b}$ idealinin temel olması $\mathfrak{ab}$ idealinin temel olmasına bağlı olacaktır. Bundan yola çıkarak öyle $u_1, v_1 \in (1/f)\mathbb{Z}$ seçebiliriz ki, aşağıdaki eşitlik sağlanır:

$$E(\mathfrak{c}_0) = \phi(u_1, v_1, \tau_1)^{12f}. \tag{2.12}$$

Eğer $\mathfrak{f} = (N)$ olursa, bu durumda $\mathfrak{b} = 1$ seçebilir ve (2.12) denkleminde $[u_1, v_1] = [0, 1/N]$ çiftiyle işlemlerimize başlayabiliriz. Genel durumda $[u_1, v_1]$ çifti $\mathfrak{f}$'ye asal uygun

bir $\mathfrak{b}$ ideali bulunarak hesaplanabilir.

Stark'ın karşılıklılık teoremini kullanarak (Stark, 1980, p. 223),

$$\sigma_{\mathfrak{c}}(E(\mathfrak{c}_0)) = E(\mathfrak{c}\mathfrak{c}_0) = \phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_{\mathfrak{c}})^{12f}$$

elde ederiz. Burada $u_{\mathfrak{c}}, v_{\mathfrak{c}} \in (1/f)\mathbb{Z}$ ve $\tau_{\mathfrak{c}} = \tau_Q$ olur. Ayrıca $\mathfrak{c}$ sınıfının Hilbert cismine indirgenişi ve Q kuadratik formu aynı sınıfa denk gelir.

Bu noktadan itibaren sadelik için $\tau_{\mathfrak{c}} = \tau_1$ durumuna yoğunlaşacağız. Ayrıca minimal polinomları ufak elemanlar elde edebilmek amacıyla $e_{\mathfrak{c}} = 1$ olduğunu varsayacağız. Bazı karşılaştırmalar için Örnek 2.1.7'e bakılabilir.

$\tau_{\mathfrak{c}} = \tau_1$ ve $e_{\mathfrak{c}} = 1$ şartları ancak ve ancak $\mathfrak{c}$ sınıfının temel ideallerden oluşması ve $\sigma_{\mathfrak{c}}$ otomorfizmasının 1'nin kökleri üzerindeki etkisinin bayağı olması durumunda mümkündür. Böyle bir $\mathfrak{c} \neq 1$ sınıfı ancak ve ancak $K_{\mathfrak{f}} \neq H(\zeta_W)$ olması durumunda mümkündür.

Eğer $K_{\mathfrak{f}} = H(\zeta_W)$ olursa, bu durumda ışın sınıf cismi $K_{\mathfrak{f}}$ Hilbert sınıf cismini üreten elemanların yanında siklotomik elemanları da kullanılarak elde edilebilir. Bu yüzden bu noktadan sonra $K_{\mathfrak{f}} \neq H(\zeta_W)$ şartı herhangi bir sınırlama getirmeyecektir.

Verilen $\mathfrak{f}$ modulusuna göre aldığımız $\mathfrak{c}$ ideal sınıfı $\tau_{\mathfrak{c}} = \tau_1$ ve $e_{\mathfrak{c}} = 1$ şartlarını sağlasın. Verilen $[u_1, v_1]$ çiftinden yola çıkarak $[u_{\mathfrak{c}}, v_{\mathfrak{c}}]$ çiftini hesaplamak istiyoruz. Işın sayı cismindeki 1'in kökleri sayısı olan W, $12f$'yi tam böler. Bu yüzden $\ell = 12f/W$ pozitif bir tamsayı olacaktır. $E(1)^W$ cebirsel bir elemanın $12f$'ninci kuvveti olduğu için, aşağıdaki ifadeyi elde ederiz:

$$G(1) := \sqrt[\ell]{E(1)} = \phi(u_1, v_1, \tau_1)^W \cdot \zeta_\ell^* \in K_{\mathfrak{f}}.$$

Daha önceden tanımladığımız gibi $M = 12f^2$ olsun. Öyle bir $\alpha \in \mathcal{W}_{M,\tau_1}$ elemanı bulabiliriz ki $K_{\mathfrak{f}}$'ye indirgenişi $\sigma_{\mathfrak{c}}$ otomorfizmasına denk gelir ve $K_{\mathfrak{f}}(\zeta_\ell)/K_{\mathfrak{f}}$ genişlemesinde aşikar bir şekilde etki eder. Diyelim ki $\widehat{\alpha} = \alpha - 1$ elemanı $\mathbb{Z}[G]$ grup halkasında bir eleman olsun. Burada $G = \mathcal{W}_{M,\tau_1}/\{\pm I_2\}$ ve aşağıdali eşitlik elde edilir:

$$G(1)^{\widehat{\alpha}} = \left[\frac{\phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_{\mathfrak{c}})}{\phi(u_1, v_1, \tau_1)}\right]^W \in K_{\mathfrak{f}}.$$

Kolayca görülebilir ki $[u_{\mathfrak{c}}, v_{\mathfrak{c}}] = [u_1, v_1] \cdot \alpha$ ve $\tau_{\mathfrak{c}} = \tau_1$ olur. Ayrıca $e_{\mathfrak{c}} = 1$ şartı yukarıdaki kesrin (2.11) denkleminden dolayı $K_{\mathfrak{f}}$'deki bir elemanın W'ninci bir kuvveti olmasını gerektirir. Işın sınıf cismi $K_{\mathfrak{f}}$'deki 1'in sadece W kökü olduğu için, aşağıdaki gibi bir eleman tanımlayabiliriz:

$$\epsilon(\mathfrak{c}) := \frac{\phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_1)}{\phi(u_1, v_1, \tau_1)} \in K_{\mathfrak{f}}.$$

Bu ifade 1'in W'ninci bir köküyle çarpımına kadar iyi tanımladır ve bir eliptik birim eleman verir. Bu noktada Stark'ın karşılıklılık teoremini kullanarak da benzer bir sonuç elde edebilirdik (Küçüksakallı, 2011). Ancak idèlik yorumlama konuyu daha iyi kavramımızı ve daha rahat işlem yapmamızı sağlamaktadır.

2.1.3 Sonuçlar

Algoritma

Şimdiki amacımız $\epsilon(\mathfrak{c})^\sigma$ eliptik birim elemanlarını $\mathrm{Gal}(K_\mathfrak{f}/K)$ Galois grubundaki bütün σ'lar için hesaplamaktır. İlk olarak

$$(\beta, Q) \in \mathcal{W}_{M,\tau_1} \times \mathrm{Cl}(d_K)$$

biçiminde bir çift buluruz. Bu çiftin $K_\mathfrak{f}$ ışın sayı cismine indirgenişi σ'ya denk gelir. Çin kalan teoremini kullnarak $u_Q \bmod M$ matrisi hesaplanabilir (Gee, 2001, p. 46). Teorem 2.1.1 ve Teorem 2.1.2'i kullanarak $\beta \cdot u_Q \in \mathrm{GL}(2, \mathbb{Z}/M\mathbb{Z})$ matrisininin Siegel ϕ fonksiyonu üzerindeki etkisi açık bir biçimde elde edilebilir. Sonuç olarak

$$\phi(u, v, \tau_1)^{(\beta,Q)} = \phi([u, v] \cdot \beta \cdot u_Q, \tau_Q) \cdot \zeta_Q$$

eşitliğini elde ederiz. Buradaki 1'in kökü olan ζ_Q sadece Q'ya bağlıdır, u'ya veya v'ye değil. $\tau_\mathfrak{c} = \tau_1$ şartı pay ve paydadaki ζ_Q terimlerini sadeleştirir ve hesaplamalarda büyük kolaylık sağlar. Sonuç olarak aşağıdaki formülü elde ederiz:

$$\epsilon(\mathfrak{c})^\sigma = \frac{\phi([u_\mathfrak{c}, v_\mathfrak{c}] \cdot \beta \cdot u_Q, \tau_Q)}{\phi([u_1, v_1] \cdot \beta \cdot u_Q, \tau_Q)}. \tag{2.13}$$

Diğer durumlarda da benzer ama karmaşık hesaplamalar yapılması mümkündür. Bunun için Örnek 2.1.7'e bakılabilir. Aşağıdaki algoritma yukarıda açıkladığımız teorinin bir özetidir ve (2.13) denklemindeki gibi elde edilebilir.

Algoritma I: $\epsilon(\mathfrak{c})$ ve eşleniklerinin hesaplanması

Girdi: Diskriminant d_K ve K'nin bir modulusu $\mathfrak{f}$.
Çıktı: $\epsilon(\mathfrak{c})$ ve eşleniklerinin eksiksiz bir kümesi.

1. W'yi hesapla ve $K_\mathfrak{f} = H(\zeta_W)$ olup olmadığını kontrol et.

- Eğer cevap EVETse, yaz: `Hilbert sınıf üreteçlerini ve siklotomik elemanları kullan.` ve sonuç olarak 0 ver.
- Eğer cevap HAYIRsa, $\mathfrak{c} \neq 1, e_{\mathfrak{c}} = 1$ ve $\tau_{\mathfrak{c}} = \tau_1$ şartlarını sağlayan bir $\mathfrak{c}$ sınıfı bul. Bir sonraki adıma geç

2. $[u_1, v_1]$ çiftini hesapla. Bir sonraki adıma geç
3. $\widehat{\alpha}$ matrisini üret ve $[u_{\mathfrak{c}}, v_{\mathfrak{c}}]$ çiftini hesapla. Bir sonraki adıma geç
4. $\mathrm{Cl}(d_K)$ sınıf gurunundaki elemanlara denk gelen bütün indirgenmiş ikili kuadratik formları
$$[Q_1, \ldots, Q_m]$$
şeklinde listele. Bunlara karşılık gelen $\mathcal{W}_{M,\tau_1}/\{\pm I_2\}$ grubundaki matrisleri
$$[\beta_1, \ldots, \beta_n]$$
şeklinde listele. Bir sonraki adıma geç
5. $[u_{Q_1}, \ldots, u_{Q_m}]$ ve $[\tau_{Q_1}, \ldots, \tau_{Q_m}]$ listelerini elde et. Bir sonraki adıma geç
6. $1 \leq i \leq n$ ve $1 \leq j \leq m$ için aşağıdaki eeliptik birim elemanları hesapla
$$\epsilon(i,j) = \frac{\phi([u_{\mathfrak{c}}, v_{\mathfrak{c}}] \cdot \beta_i \cdot u_{Q_j}, \tau_{Q_j})}{\phi([u_1, v_1] \cdot \beta_i \cdot u_{Q_j}, \tau_{Q_j})}.$$
7. ϵ matrisini sonuç olarak ver.

Bu algoritmayı PARI/GP (PAR, 2014) programında yazdık ve elde ettiğimiz sonuçları daha önce verilmiş olan üreteçlerle kıyasladık. Geliştirdiğimiz teori aşağıdaki teoremle özetlenebilir:

Teorem 2.1.4. *K kompleks kuadratik bir sayı cismi ve $\mathfrak{f}$ bu cismin birden farklı bir ideali olsun. Bu idealin içindeki en küçük pozitif tamsayı f olsun. $K_{\mathfrak{f}} \neq H(\zeta_W)$ şartı sağlansın ve $\mathfrak{c} \neq 1$ sınıfı temel ideallerden oluşan ve $\sigma_{\mathfrak{c}}$ otomorfizması 1'in kökleri üzerinde aşikar bir şekilde etki eden bir sınıf olsun. O zaman $u_{\mathfrak{c}}, v_{\mathfrak{c}}, u_1, v_1 \in \frac{1}{f}\mathbb{Z}$ sayılarını hesaplayan öyle bir algoritma vardır ki*
$$\epsilon(\mathfrak{c}) = \frac{\phi(u_{\mathfrak{c}}, v_{\mathfrak{c}}, \tau_1)}{\phi(u_1, v_1, \tau_1)} \in K_{\mathfrak{f}}.$$
eliptik bir eleman olur. Ayrıca bu algoritma bu eliptik birim elemanın bütün eşleniklerini eksiksiz bir biçimde elde etmemizi sağlar.

Bütün hesaplamalarımızda $\epsilon(\mathfrak{c})$ birim elemanı $K_{\mathfrak{f}}$ sayı cisminin K üzerinde bir üreteci olarak ortaya çıktı. Ayrıca (Jung and Shin, 2011, Lemma 3.3)'nın ispatı da bu tür elemanların $K_{\mathfrak{f}}/K$ genişlemesini üretebileceğini tahmin etmemizi sağlıyor. Bu yüzden aşağıdaki savı öne sürüyoruz.

Varsayım 2.1.5. Teorem 2.1.4'in şartları sağlansın. O zaman $K_{\mathfrak{f}}/K$ cisim genişlemesi eliptik birim eleman $\epsilon(\mathfrak{c})$ tarafından üretilir.

Aşağıdaki eksonuç Algoritma-I ile hemen elde edilir.

Ek Sonuç 2.1.6. *Teorem 2.1.4'in şartları sağlansın ve Sav 2.1.5 doğru olsun. O zaman $\epsilon(\mathfrak{c})$ üretecinin K üzerindeki minimla polinomu $h(x) \in \mathcal{O}[x]$'i hesaplayan bir algoritma vardır.*

Varsayalım $h_{\mathfrak{c}}(x)$ ve $h_{\phi}(x)$ polinomları sırasıyla $\epsilon(\mathfrak{c})$ ve (Jung and Shin, 2011)'daki

$$\phi(0, 1/N, \tau_1)^{12N/(6,N)}$$

elemanların $\mathbb{Q}$ üzerindeki minimal polinomları olsun. Ayrıca $\gamma_{\mathfrak{c}}$ ve γ_{ϕ} değerleri de bu polinomların katsayılarının azami mutlak değerinin logaritması olsun. Deneysel olarak $\gamma_{\mathfrak{c}}$ ve γ_{ϕ} karşılaştırdığımızda yeterince büyük N değerleri için

$$r(N) := \frac{\gamma_{\phi}}{\gamma_{\mathfrak{c}}} \approx \frac{12N}{\mathrm{OBEB}(6, N)}$$

kadar iyileşme elde etmeyi bekleriz. Bu iyileşme aşağıda verilen örneklerde daha açık bir biçimde görülebilir.

Örnekler

Örnek 2.1.7. *$K = \mathbb{Q}(\sqrt{-91})$ ve $\mathfrak{f} = (5)$ olsun. Form sınıf grubu aşağıdaki gibidir:*

$$Cl(d_K) = \{[1, 1, 23], [5, 3, 5]\}.$$

Ayrıca $\mathcal{W}$ matris grubu aşağıdaki gibi elde edilir

$$\mathcal{W}_{5,\tau_1}/\{\pm I_2\} = \left\{ \begin{array}{l} \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & -23 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -23 \\ 1 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 & -23 \\ 1 & 3 \end{smallmatrix}\right], \\ \left[\begin{smallmatrix} -2 & -46 \\ 2 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -46 \\ 2 & 2 \end{smallmatrix}\right] \end{array} \right\}.$$

Bu iki kümeyi elde etmek ile ışın sınıf grubundaki sınıfları listelemek ile eş değerde olduğu Teorem 2.1.2'den de görülebilir.$[u_1, v_1] = [0, 1/5]$ olarak seçelim. Eğer $(5, a, b) = 1$ ise $\phi(a/5, b/5, z)$ fonksiyonu $M = 12 \cdot 5^2$ düzeyinde modüler bir fonksiyondur. Işın sınıf cismi

$K_{(5)}$'teki 1'in köklerinin sayısı ise $W = 10$ olarak bulunur. Bundan dolayı $\ell = 12 \cdot 5/10 = 6$ olur.

1. Kısım: $\mathfrak{c}_1$ sınıfı $\left(\left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right], [5,3,5]\right)$ çiftine karşılık gelsin. Eğer $Q = [5,3,5]$ ise $u_Q \equiv \left[\begin{smallmatrix} 293 & 169 \\ 276 & 49 \end{smallmatrix}\right] \bmod M$ olarak buluruz. $\alpha = \left[\begin{smallmatrix} 9 & -46 \\ 2 & 11 \end{smallmatrix}\right]$ matrisi $\mathcal{W}_{M,\tau_1}$ grubunun $\left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right]$'e 5 modunda denk olan bir elemanıdır. Ayrıca $\alpha \cdot u_Q$ çarpımının determinantı ℓ modundan 1'e denktir. $\det(\alpha \cdot u_Q) \equiv 3 \bmod W$ olduğunu kolayca hesaplarız ve sonuç olarak $e_{\mathfrak{c}_1} = 5$ olduğunu elde ederiz. Bunun ardından $[0, 1/5] \cdot \alpha \cdot u_Q$ hesabı bize aşağıdaki değerleri verir:

$$\epsilon(\mathfrak{c}_1) = \left[\frac{\phi\left(\frac{3622}{5}, \frac{877}{5}, \tau_Q\right) \cdot \zeta_Q}{\phi\left(0, \frac{1}{5}, \tau_1\right)}\right]^5 \in K_{(5)}.$$

Burada ζ_Q, 1'in onikinci bir köküdür ve sadece Q'ya bağlıdır. Değeri u_Q matrisinin ϕ üzerindeki etkisine bakılarak tam olarak bulunabilir. Bunu yapmak için u_Q matrisini S, T ve $\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]$ cinsinden çarpanlarına ayırmak gerekir. Diğer taraftan bu adım $\mathfrak{c}$'yi aşağıdaki gibi seçmemiz halinde gerekli olmayacaktır.

2. Kısım: $\mathfrak{c}_2$ sınıfı $\left(\left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right], [1,1,23]\right)$ çiftine karşılık gelsin. $u_Q \equiv \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \bmod M$ buluruz. $\alpha = \left[\begin{smallmatrix} -1 & -46 \\ 2 & 1 \end{smallmatrix}\right]$ olur ve bu matrisin determinantı ℓ modundan 1'e denktir. Ayrıca $\det(\alpha \cdot u_Q) = 1$ olur ve buradan $e_{\mathfrak{c}_2} = 1$ elde ederiz. Bunun ardından $[0, 1/5] \cdot \alpha \cdot u_Q$ çarpımını hesaplayarak aşağıdaki değerleri elde ederiz:

$$\epsilon(\mathfrak{c}_2) = \frac{\phi\left(\frac{2}{5}, \frac{1}{5}, \tau_1\right)}{\phi\left(0, \frac{1}{5}, \tau_1\right)} \in K_{(5)}.$$

$h_1(x)$ ve $h_2(x)$ polinomları sırasıyla $\epsilon(\mathfrak{c}_1)$ ve $\epsilon(\mathfrak{c}_2)$ elemanlarının $\mathbb{Q}$ üzerindeki minimal polinomları olsun. $h_1(x)$ polinomunun katsayılarının mutlak değerleri $h_2(x)$ polinomunun katsayılarının mutlak değerlerine nazaran daha büyüktür. Bir karşılaştırma yapmak için c_1 ve c_2 sayıları sırasıyla bu polinomların mutlak değeri en büyük katsayıları olsun:

$$c_1 = 140393060269843208789297210092029 46,$$

$$c_2 = 910425.$$

Daha önceden de tahmin edebileceğimiz gibi ikinci kısımdaki örnekte beşinci dereceden bir iyileşme söz konusudur: $\log(c_1)/\log(c_2) \approx 5.73015$.

Örnek 2.1.8. $\mathfrak{f}$ birinci dereceden asal ideallerin çarpımı şeklinde yazılabilen $(\mathfrak{f}, 6\bar{\mathfrak{f}}) = 1$ şartını sağlayan bir ideal olsun. Çin kalan teoremi sayesinde öyle bir t_1 tamsayısı vardır ki $\tau_1 \equiv t_1 \bmod \bar{\mathfrak{f}}$ şartını sağlar. Bu durumda $\bar{\mathfrak{f}} = (f, \tau_1 + t_1)$ olur. Bir $\mathfrak{a} \in \mathfrak{c}_0$ ideali için temel ideal $(\tau_1 + t_1)$'ni $(\tau_1 + t_1) = \bar{\mathfrak{f}}\mathfrak{a}$ şeklinde yazalım. $\mathfrak{b} = \bar{\mathfrak{f}}$ şeklinde bir seçim yaparak, $E(\mathfrak{c}_0) = \phi(1/f, t_1/f, \tau_1)^{12f} \in K_{\mathfrak{f}}$ ifadesini elde ederiz. Sonuç olarak $[u_1, v_1] = [1/f, t_1/f]$

olur.

Bu durumda $K_{\mathfrak{f}} \cap K_{\bar{\mathfrak{f}}} = H$ *şartı sağlanır ve buradan* $K_{\mathfrak{f}}$ *cismindeki* 1*'in köklerininin hepsinin* H*'de olduğunu görürüz.* $\mathfrak{c} \neq 1$ *temel ideallerden oluşan bir sınıf olsun.* $\sigma_{\mathfrak{c}}$ *otomorfizmasının* $K_{\mathfrak{f}}$ *cismindeki* 1*'in kökleri üzerindeki etkisi aşikar olacaktır.* $M = 12f^2$ *olsun. Verilen bir* $\sigma \in Gal(K_{\mathfrak{f}}/H)$ *için* $\alpha_a = \left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right] \in \mathcal{W}_{M,\tau_1}$ *şeklinde bir matris bulabiliriz. Bu matrise karşılık gelen etki* $K_{\mathfrak{f}}$ *üzerinde* σ*'nın etkisine denk olacaktır. Daha önce de belirttiğimiz gibi* $\ell = 12f/W$ *olsun. Genelliği kaybetmeden* $\det(\alpha_a) = a^2 \equiv 1 \pmod{\ell}$ *olduğunu varsayalım. O zaman* $\epsilon(\mathfrak{c})$ *eliptik birim elemanın herhangi bir eşleniği aşağıdaki formül ile bulunabilir:*

$$\epsilon(\mathfrak{c})^{(\beta,Q)} = \frac{\phi([\frac{1}{f}, \frac{t_1}{f}] \cdot \alpha_a \cdot \alpha_b \cdot u_Q, \tau_Q)}{\phi([\frac{1}{f}, \frac{t_1}{f}] \cdot \alpha_b \cdot u_Q, \tau_Q)} = \frac{\phi([\frac{ab}{f}, \frac{abt_1}{f}] \cdot u_Q, \tau_Q)}{\phi([\frac{b}{f}, \frac{bt_1}{f}] \cdot u_Q, \tau_Q)}.$$

Burada (α_b, Q) *çifti* $b \in (\mathbb{Z}/M\mathbb{Z})^*$ *ve* $Q \in Cl(d_K)$ *şartlarını sağlar.*

Örnek 2.1.9. *Bu örnekte elde ettiğimiz elemanlar ile (Jung and Shin, 2011, Example 3.8) örneğinde verilen elemanları kıyaslıyoruz.* $K = \mathbb{Q}(\sqrt{-10})$ *ve* $\mathfrak{f} = (6)$ *olsun. Bu durumda* $K_{\mathfrak{f}}$ *cismindeki* 1*'in kökleri sayısı* $W = 24$ *olarak bulunur. Ayrıca* $\mathcal{W}$ *grubu aşağıdaki gibidir:*

$$\mathcal{W}_{6,\tau_1}/\{\pm I_2\} = \left\{ \begin{array}{l} \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & -10 \\ 1 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 3 & -10 \\ 1 & 3 \end{smallmatrix}\right], \left[\begin{smallmatrix} 5 & -10 \\ 1 & 5 \end{smallmatrix}\right], \\ \left[\begin{smallmatrix} 1 & -20 \\ 2 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 3 & -20 \\ 2 & 3 \end{smallmatrix}\right], \left[\begin{smallmatrix} 5 & -20 \\ 2 & 5 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & -30 \\ 3 & 1 \end{smallmatrix}\right] \end{array} \right\}.$$

Sekiz tane temel ideal sınıfı arasında sadece ikisi, 1 *ve* $2\sqrt{-10} + 3$*'e karşılık gelen, öyle matrislere sahiplerdir ki determinantları* 24 *modunda* 1*'e denk olsun. Daha önce de belirttiğimiz gibi* $\ell = 12 \cdot f/24 = 3$ *olsun. Sonuç olarak* $\alpha = \left[\begin{smallmatrix} 3 & -20 \\ 2 & 3 \end{smallmatrix}\right] \in \mathcal{W}_{M,\tau_1}$ *matrisini kullanmalıyız. Burada* $M = 12 \cdot 6^2$ *olur.* α *matrisinin determinantı* ℓ *modunda* 1*'e denktir. Böylelikle aşağıdaki eliptik birim elemanı elde ederiz:*

$$\epsilon(\mathfrak{c}) = \frac{\phi(\frac{2}{6}, \frac{3}{6}, \tau_1)}{\phi(0, \frac{1}{6}, \tau_1)}$$

Bu eliptik birim eleman $K_{(6)}$ *cisminde yer alır.* $\epsilon(\mathfrak{c})$ *birim elemanını* $\zeta_{12}^5 \in K_{(6)}$ *ile çarparak gerçel bir sayı elde ederiz ve bu elemanın minimal polinomu aşağıdaki gibidir:*

$$\begin{aligned} \min(\epsilon(\mathfrak{c})\zeta_{12}^5, K) = \; & x^{16} + 8x^{15} - 18x^{14} - 68x^{13} + 50x^{12} \\ & +108x^{11} - 44x^{10} - 28x^9 + 63x^8 \\ & -28x^7 - 44x^6 + 108x^5 + 50x^4 - 68x^3 \\ & -18x^2 + 8x + 1. \end{aligned}$$

Bu polinom Jung, Koo ve Shin tarafından bulunan aşağıdaki polinoma göre daha küçük

katsayılara sahiptir (Jung and Shin, 2011):

$$\begin{aligned}\min\left(\phi^{12}\left(0,\frac{1}{6},\tau_1\right),K\right) = \; & x^{16}+20560x^{15}-1252488x^{14}-829016560x^{13}\\ & -8751987701092x^{12}+217535583987600x^{11}\\ & +1812625206211110344x^{10}+43806873084101200x^{9}\\ & -27861628000497273 0x^{8}+139245187265282800x^{7}\\ & -8883048242697656x^{6}+352945014869040x^{5}\\ & +23618989732508x^{4}-1848032773840x^{3}\\ & +49965941112x^{2}-425670800x+1.\end{aligned}$$

Bir önceki örneğe benzer şekilde, polinomların mutlak değeri en büyük olan katsayılarını c_1 *ve* c_2 *ve olarak belirleyelim:*

$$c_1 = 278616280004972730,$$

$$c_2 = 108.$$

Bu hesaplamadan oldukça iyi bir iyileşmenin olduğunu görürüz: $\log(c_1)/\log(c_2) \approx 8.57913$.

Örnek 2.1.10. $K = \mathbb{Q}(\sqrt{-11})$ *ve* $\mathfrak{f} = (9)$ *olsun. Bu örnekte Algoritma-I ile elde ettiğimiz polinom ile Bettner ve Schertz tarafından verilen bir* $\Theta \in K_{\mathfrak{f}}$ *elemanının minimal polinomunu kıyaslayacağız (Bettner and Schertz, 2001, Example 3).*

$$\begin{aligned}\min(\Theta,K) = \; & x^{18}+9x^{17}+36x^{16}+(-8\tau_1+91)x^{15}\\ & +(-78\tau_1+150)x^{14}+(-294\tau_1+45)x^{13}\\ & +(-492\tau_1-479)x^{12}+(-120\tau_1-1020)x^{11}\\ & +(816\tau_1-327)x^{10}+(1068\tau_1+1469)x^{9}\\ & +(-18\tau_1+1707)x^{8}+(-882\tau_1-357)x^{7}\\ & +(-288\tau_1-1523)x^{6}+(516\tau_1-345)x^{5}\\ & +(390\tau_1+540)x^{4}+(2\tau_1+219)x^{3}\\ & +(-6\tau_1-15)x^{2}+(6\tau_1+15)x+1.\end{aligned}$$

Diğer taraftan $\epsilon(\mathfrak{c}) = \phi(7/3,-2/9,\tau_1)/\phi(0,1/9,\tau_1)$ *eliptik birim elemanının minimal*

polinomu aşağıdaki gibidir:

$$\begin{aligned}\min(\epsilon(\mathfrak{c}), K) = \; & x^{18} + 3x^{17} + (-6\tau_1 + 3)x^{16} + (5\tau_1 - 4)x^{15} \\ & +(-6\tau_1 + 18)x^{14} + (3\tau_1 - 3)x^{13} \\ & +(-12\tau_1 + 40)x^{12} + (-6\tau_1 + 6)x^{11} \\ & +(-15\tau_1 + 63)x^{10} - 2x^9 + (15\tau_1 + 78)x^8 \\ & +(6\tau_1 + 12)x^7 + (12\tau_1 + 52)x^6 + (-3\tau_1 - 6)x^5 \\ & +(6\tau_1 + 24)x^4 + (-5\tau_1 - 9)x^3 + (6\tau_1 + 9)x^2 \\ & +3x + 1.\end{aligned}$$

Daha önceki örneklere benzer şekilde c_Θ *ve* $c_{\epsilon(\mathfrak{c})}$ *sırasıyla yukarıdaki polinomların katsayılarının en büyük mutlak değerli olana olsun. Buradan* $\log(c_\Theta)/\log(c_{\epsilon(\mathfrak{c})}) \approx 1.76212$ *buluruz. Algoritma-I tarafından üretilen elemanların minimal polinomunda ufak da olsa bir iyilişme görülmektedir. Ama bu ufak iyileşme elde ettiğimiz yegane avantaj değildir. Bu iyileşmenin yanı sıra Algoritma-I* $\mathfrak{f}$ *modulusu üzerinde hiçbir kısıtlama getirmez. Diğer taraftan Bettner ve Schertz tarafından verilen metod sadece özel ve çok kısıtlı durumlarda uygulanabilir.*

Olası Uygulamalar

Bu bölümde verdiğimiz algoritmanının olası uygulamalarını ve hesaplamaların nasıl daha genel hale getirebileceğimiz listeleyeceğiz.

İlk olarak, Algoritma-I tarafından verilen $\epsilon(\mathfrak{c})$ elemanların $K_\mathfrak{f}$ cismini K üzerinde üretip üretmediğini araştırmak ilginç bir problem olabilir. Ayrıca bu birim elemanların, Hilbert sınıf cisminden gelen birim elemanlarla beraber $U(\mathcal{O}_{K_\mathfrak{f}})$ birim eleman grubunun sonlu indisli bir alt grubunu oluşturup oluşturmadığını bulmak önemli bir uygulama olacaktır.

İkinci olarak Klebel'in (Klebel, 1996) sonuçlarından yola çıkarak elde ettiğimiz elemanlardan kuvvetsel bir baz bulmanın mümkün olup olmaycaığını araştırmak istiyoruz. Böyle bir bazın bulunması halinde bazı Diophantine denklemlerini çözmek mümkün olacaktır (Gaal, 2002).

Bir diğer araştırma konusu olarak bulduğumuz algoritmayı kompleks çarpım teorisinin diğer durumlarına genelleştirmeyi düşünüyoruz (Küçüksakallı, 2013). Bu sayede herhangi bir halka sınıf cismini (ring class field) K üzerinde üretmek mümkün olabilecektir.

Son olarak elde ettiğimiz bu eliptik birim elemanlarının Hilbert sınıf cismine indirgenmiş normlarının oluşturduğu çarpımsal birim eleman grububu incelemek ilginç olabilir. Bu sayede çeşitli Hilbert sınıf üreteçleri elde etmek mümkün olacaktır. Bu tür üreteçlerin kompleks çarpım teorisinin uygulamalarının içinde yeri büyüktür. Örnek vermek gerekirse bu tür elemanlar asallık ispatlama, grup ve eşleme tabanlı kriptografide

kullanılabilir. Bu konuların detayları için (Atkin and Morain, 1993), (Morain, 2007), (Blake and Smart, 1999), (Blake and Smart, 2005) veya (Freeman and Teske, 2010) referanslarına bakılabilir.

2.2 $\mathbb{F}_2$ Üzerinde Tanımlanan İkinci Dereceli Özyineli Fonksiyon Cisimleri Kuleleri

2.2.1 Giriş

Sonlu cisimler üzerinde tanımlanan özyineli cebirsel fonksiyon cisimleri kuleleri ilk olarak 1995 yılında A. Garcia ve H. Stichtenoth tarafından (Garcia and Stichtenoth, 1995) makalesinde sunulmuştur. Literatürde herhangi bir sonlu cisim $\mathbb{F}_q$ üzerinde birçok özyineli cebirsel fonksiyon cisimleri kuleleri örnekleri bulunmaktadır, örneğin bkz. (Bassa, 2006), (Beelen and Stichtenoth, 2004), (Beelen and Stichtenoth, 2006), (Garcia and Stichtenoth, 1996), (Hess and Tutdere, 2013) vs. Diyelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ herhangi bir sonlu $\mathbb{F}_q$ cismi üzerinde tanımlanan ikinci dereceden özyineli bir cebirsel fonksiyon cisimleri kulesi. Yani; $\mathcal{F}$ kulesi $\mathbb{F}_q$ üzerinde tanımlanan öyle bir özyineli kule ki bütün $n \geq 1$ için $[F_n : F_{n-1}] = 2$ dir. Herhangi bir $r \geq 1$ tam sayısı için $B_r(F_n)$ ve $g(F_n)$, $F_n/\mathbb{F}_2$ nin sırasıyla r mertebeli yerlerin sayısı ve cinsi olmak üzere $\beta_r(\mathcal{F}) := \lim_{n\to\infty} B_r(F_n)/g(F_n)$ olsun. En az bir r için $\beta_r(\mathcal{F}) > 0$ olan kulelere *potansiyeli iyi* olan kuleler diyeceğiz. Literatürde, potansiyeli iyi olan birçok kule örneği bulunmaktadır, örneğin bkz.(Bassa and Stichtenoth, 2012), (Garcia and Stichtenoth, 1995), (Hess and Tutdere, 2013) vs.. Kodlama teorisi ve kriptografi gibi alanlardaki öneminden dolayı özellikle $r = 1$ durumu birçok araştırmacı tarafından çalışılmıştır.

Sonlu cisim $\mathbb{F}_q$ öyle ki $q = p^k$, burada p asal ve $k \geq 2$, ise literatürde $\beta_1(\mathcal{F}) > 0$ olan birçok kule örnekleri mevcuttur, örneğin bkz. (Garcia and Stichtenoth, 1995), (Garcia and Stichtenoth, 1996). Bu kulelere özel olarak *asimptotik olarak iyi* olan kuleler denilmektedir. Ancak, $q = p$ olduğu durumlarda asal sonlu cisim $\mathbb{F}_p$ üzerinde özyineli asimptotik olarak iyi olan özyineli cebirsel fonksiyon cisimleri kulelerin varlığı henüz bilinmemektedir. Bu proje kapsamında yapılan çalıştaylarda bu problem üzerine bazı tartışmalarda bulunduk. Daha sonra bu problemin $p = 2$ durumunu ele aldık. Özel olarak ikinci dereceden olan kuleler üzerinde çalıştık.

Öncelikle en küçük asal sonlu cisim olan $\mathbb{F}_2$ üzerinde tanımlanan potansiyeli iyi olan ikinci dereceli özyineli kuleler üzerine çalıştık. Bu kulelerin hangi tür denklemlerle ifade edilebileceği üzerine çalıştık ve bu denklemlerin bir sınıflandırmasını verdik. Daha sonra da elde ettiğimiz bu kuleler için β_1 değerini hesapladık ve birçok durumda bu değerin sıfır

olduğu sonucuna vardık.

2.2.2 Genel Bilgiler

Cebirsel Fonksiyon Cisimleri

Bu bölümde kısaca cebirsel fonksiyon cisimlerini tanıtacağız. Bu bölüm boyunca K ile herhangi bir cismi göstereceğiz.

Tanım 2.2.1. Diyelim ki F, K cisminin bir genişlemesidir. K üzerinde aşkın olan herhangi bir $x \in F$ elemanı için eğer F, $K(x)$ cisminin sonlu bir cebirsel genişlemesi ise F/K ya K üzerinde *tek değişkenli cebirsel fonksiyon cismi* denir.

Kolaylık olsun diye F/K ya bir fonksiyon cismi diyeceğiz. Diyelim ki

$$\tilde{K} := \{z \in F | z,\ K \text{ üzerinde cebirsel}\}.$$

Bu durumda $K \subseteq \tilde{K} \subseteq F$ olduğu açıktır. $\tilde{K}$ kümesine F/K *nın sabitlerinin cismi* denir. $\tilde{K} = K$ olduğunda K, F nin içinde cebirsel olarak kapalıdır ya da K, F/K nın *tüm sabitlerinin cismidir* denir.

Açıklama 2.2.2. K üzerinde aşkın olan F nin elemanları şu şekilde karakterize edilebilir: $z \in F$ elemanı K üzerinde aşkındır ancak ve ancak F, $K(z)$ nin sonlu bir genişlemesidir.

Örnek 2.2.3. *En basit cebirsel fonksiyon cisim örneği rasyonel fonksiyon cismidir. Eğer K üzerinde aşkın olan bazı $x \in F$ için $F = K(x)$ ise F/K ya rasyonel fonksiyon cismi denir.*

Şimdi de cebirsel fonksiyon cisimleri için önemli olan *yer* kavramını tanıtacağız. Bunun için öncelikle şu tanıma ihtiyacımız var.

Tanım 2.2.4. Bir fonksiyon cisminin *değerlendirme halkası* $\mathcal{O} \subseteq F$ aşağıdaki koşulları sağlayan bir halkadır:

(i) $K \subsetneq \mathcal{O} \subsetneq F$,

(ii) her $z \in \mathcal{O}$ için $z \in \mathcal{O}$ ya da $z^{-1} \in O$ dir.

Örneğin; rasyonel fonksiyon cismi $K(x)/K$ için bir değerlendirme halkası şu şekilde verilebilir: verilen ayrışmaz bir monik $p(x) \in K[X]$ polinomu için diyelim ki

$$\mathcal{O}_{p(x)} := \{\frac{f(x)}{g(x)} \in K(x) |\ f(x), g(x) \in K[x] \text{ ve } p(x) \nmid g(x)\}.$$

Bu durumda $\mathcal{O}_{p(x)}$, $K(x)/K$ nin bir değerlendirme halkası olur.

Önerme 2.2.5. *Diyelim ki $\mathcal{O}$, F/K fonksiyon cisminin bir değerlendirme halkasıdır. Bu durumda aşağıdakiler olur:*

(i) O bir lokal halkadır. Yani; $\mathcal{O}$ halkasının sadace bir $P = \mathcal{O} \setminus \mathcal{O}^*$ maksimal ideali vardır. Burada $\mathcal{O}^* = \{z \in \mathcal{O} |$ bazı $w \in \mathcal{O}$ için $zw = 1$ dir$\}$.

(ii) $x \in F$ olsun. O zaman $x \in P$ ancak ve ancak $x^{-1} \notin P$ dir.

(iii) F/K nın tüm sabitlerinin cismi olan $\tilde{K}$ için $\tilde{K} \subseteq \mathcal{O}$ ve $\tilde{K} \cap P = \{0\}$ dır.

Tanım 2.2.6. Bir fonksiyon cismi F/K nın herhangi bir değerlendirme halkasının P maksimal idealine F/K nın bir *yeri* denir.

Bir fonksiyon cisminin yerleri ve değerlendirme halkaları ayrık değerlendirme denilen bazı gönderimlerle de tanımlanabilir.

Tanım 2.2.7. Aşağıdaki koşulları sağlayan herhangi bir $v : F \to \mathbb{Z} \cup \{\infty\}$ gönderimine F/K fonksiyon cisminin bir *ayrık değerlendirmesi* denir:

(1) $v(x) = \infty \Longleftrightarrow x = 0$.

(2) Bütün $x, y \in F$ için $v(xy) = v(x) + v(y)$ olur.

(3) Bütün $x, y \in F$ için $v(x + y) \geq min\{v(x), v(y)\}$ dir.

(4) Öyle bir $z \in F$ vardır ki $v(z) = 1$ dir.

(5) Bütün $0 \neq a \in K$ için $v(a) = 0$ dir.

Tanım 2.2.7 kullanılarak bir fonksiyon cisminin bir yeri P ve değerlendirme halkası $\mathcal{O}_P$ şu şekilde tanımlanabilir:

Önerme 2.2.8. *Diyelim ki F/K bir fonksiyon cismidir ve v_P de F/K nın ayrık bir değerlendirmesidir. Diyelim ki*

$$\mathcal{O}_P := \{z \in F |\ v_P(z) \geq 0\} \text{ ve } P := \{z \in F |\ v_P(z) > 0\}.$$

O zaman $\mathcal{O}_P$, F/K nın bir değerlendirma halkasıdır ve P de $\mathcal{O}_P$ nin maksimal ideali, yani F/K nin bir yeridir. Diğer taraftan F/K nın her bir P yeri bir ayrık değerlendirme tanımlar. Yani; F/K nın ayrık değerlendirmeleri ile yerleri arasında birebir eşleme vardır.

Herhangi bir lokal $\mathcal{O}_P$ halkası ve onun maksimal ideali P için $\mathcal{O}_P/P$ bölümünün bir cisim olduğunu hatırlayalım.

Tanım 2.2.9. Diyelim ki $\mathcal{O}_P$, F/K fonksiyon cisminin bir değerlendirme halkası ve P de $\mathcal{O}_P$ nin maksimal ideali olan F/K nın bir yeridir.

(a) $F_P := \mathcal{O}_P/P$ cismine P nin *kalan sınıf cismi* denir.

(b) $F_P \supseteq K$ cisim genişlemesinin derecesine P *nin derecesi* denir ve $\deg P$ ile gösterilir. Derecesi bir olan yerlere *rasyonel yer* denir. F/K nın her bir P yeri için eğer $0 \neq x \in P$ ise $\deg P \leq [F : K(x)] < \infty$ dir.

Bölüm 2.2.3 de fonksiyon cisimlerinin yerlerinin sayısının ve cinsinin hesaplanması üzerindeki çalışmalarımızın detayları verilmektedir. Bir fonksiyon cisminin cinsi için burada sadace aşağıdaki tanımın verilmesini yeterli buluyoruz. Bir fonksiyon cisminin cinsinin tam tanımı için daha fazla kavramların tanımlanması gerekiyor. Bunun için bkz. (Stichtenoth, 2009a).

Tanım 2.2.10. Herhangi bir F/K fonksiyon cisminin *cinsi* F/K ya özgü olan negatif olmayan bir tam sayıdır. Her fonksiyon cisminin sadace bir cins değeri vardır.

Cebirsel Fonksiyon Cisimleri Kuleleri

Diyelim ki $\mathbb{F}_q$, q tane elemanı olan bir sonlu cisim. Burada $q = p^k$, p bir asal sayı ve $k \in \mathbb{N}$. Bu bölüm boyunca $F/\mathbb{F}_q$ ile tüm sabitlerinin cismi $\mathbb{F}_q$ olan cebirsel fonksiyon cisimlerini ele alacağız. Sırasıyla, $g(F)$, $B_r(F)$ $(r \in \mathbb{N})$ ve $\mathbb{P}(F)$ ile $F/\mathbb{F}_q$ nin cinsi, derecesi r olan yerlerin sayısı ve bütün yerlerin oluşturduğu kümeyi göstereceğiz.

Tanım 2.2.11. Sonsuz bir $F_n/\mathbb{F}_q$ fonksiyon cisimleri dizisi $\mathcal{F} = (F_n)_{n\geq 0}$ eğer aşağıdaki koşulları sağlıyorsa bu diziye *kule* denir:

(i) $F_0 \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \ldots$,

(ii) bütün F_{n+1}/F_n genişlemeleri sonlu ve ayrışabilir,

(iii) $n \to \infty$ iken $g(F_n) \to \infty$.

Tanım 2.2.12. Diyelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanan bir kule ve $r \in \mathbb{N}$. Reel değerleri olan

$$\nu_r(\mathcal{F}) = \lim_{n\to\infty} \frac{B_r(F_n)}{[F_n : F_0]}, \quad \beta_r(\mathcal{F}) = \lim_{n\to\infty} \frac{B_r(F_n)}{g(F_n)} \text{ ve } \gamma(\mathcal{F}) = \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F_0]}$$

limitlerine sırasıyla $\mathcal{F}/\mathbb{F}_q$ nın *genel değişmezleri* ve *cinsi* denir.

Herhangi bir sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanan bütün $\mathcal{F}$ fonksiyon cisimleri kuleleri ve $r \geq 1$ için $\beta_r(\mathcal{F}) = \nu_r(\mathcal{F})/\gamma(\mathcal{F})$ olduğu tanımdan açıktır.

Tanım 2.2.13. Herhangi bir $\mathcal{F}/\mathbb{F}_q$ fonksiyon cisimleri kulesi için eğer en az bir $r \geq 1$ için $\beta_r(\mathcal{F}) > 0$ ise $\mathcal{F}/\mathbb{F}_q$ kulesine *potansiyeli iyi* olan kule denir.

Şimdi de ikinci dereceli özyineli kuleleri tanıyalım.

Tanım 2.2.14. Diyelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanan bir kule ve $f(X, Y) \in \mathbb{F}_q(X, Y)$ sabit olmayan bir rasyonel fonksiyon.

(a) Farzedelim ki öyle $x_n \in F_n$ ($n \geq 0$ için) elemanları vardır ki aşağıdaki olur:

$$F_{n+1} = F_n(x_{n+1}) \text{ öyle ki bütün } n \geq 0 \text{ için } f(x_n, x_{n+1}) = 0.$$

O zaman $\mathcal{F}$ kulesi *özyineli olarak* sonlu cisim $\mathbb{F}_q$ üzerinde $f(X, Y) = 0$ denklemi ile tanımlanır denir.

(b) Eğer bütün $n \geq 0$ için $[F_{n+1} : F_n] = 2$ ise $\mathcal{F}/\mathbb{F}_q$ kulesine *ikinci dereceli* kule denir.

(c) Diyelim ki $F := \mathbb{F}_q(x, y)$ öyle ki x ve y elemanları $f(x, y) = 0$ denklemini sağlasın. O zaman $F/\mathbb{F}_q$ fonksiyon cismine $\mathcal{F}/\mathbb{F}_q$ kulesinin *temel fonksiyon cismi* denir ($F \cong F_1$ olduğu açıktır).

(d) $f(Y, X) = 0$ denklemi tarafından $\mathbb{F}_q$ üzerinde özyineli olarak taımlanan $\mathcal{G}/\mathbb{F}_q$ kulesine $\mathcal{F}/\mathbb{F}_q$ kulesinin *eşlek (dual)* kulesi denir.

Özyineli kulelelerin değişmezleri (Hasegawa, 2007), (Hess and Tutdere, 2013), (Lebacque, 2007) ve (Tutdere, 2009a) gibi birçok yerde çalışılmıştır. Sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanan özyineli kulelerin değişmezleri için aşağıdaki sınır iyi bilinmektedir, örneğin bkz. (Tsfasman, 1992, Corollary 1):

Teorem 2.2.15 (Generalized Drinfeld-Vladut Bound). *Diyelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanan özyineli bir kule. O zaman bütün $r \in \mathbb{N}$ için*

$$\beta_r(\mathcal{F}) \leq (q^{r/2} - 1)/r \quad \textit{olur.}$$

Özellikle, $r = 1$ durumu oldukça birçok araştırmacı tarafından çalışılmıştır, örneğin bkz. (Bassa and Stichtenoth, 2012), (Garcia and Stichtenoth, 1995), (Garcia and Stichtenoth, 1996) vs. Ayrıca, herhangi bir $\mathcal{F}/\mathbb{F}_q$ için $\beta_1(\mathcal{F}) \leq A(q)$, burada $A(q)$ bilinen Ihara sabitidir. Bu yüzden, $r = 1$ durumu kriptografi ve kodlama teorisi gibi alanlarda kullanılmaktadır. Literatürde $q = p^k$, burada p asal ve $k \geq 2$ iken β_1 değişmezi pozitif olan özyineli bir çok kule mevcuttur, örneğin bkz. (Bassa and Stichtenoth, 2012). Ancak, $q = p$ asal iken $\mathbb{F}_q$ üzerinde tanımlanan β_1 değişmezi pozitif olan özyineli kulelerin

varlığı henüz bilinmemektedir. Bu problem özyineli cebirsel fonksiyon cisimleri kuleleri alanındaki en önemli ve zor problemlerden biridir.

A. Garcia, H. Stichtenoth ve M. Thomas (Garcia and Stichtenoth, 1997) asal olmayan sonlu cisimler üzerinde tanımlanan Kummer türü özyineli ve β_1 değişmezi pozitif olan kulelerin inşasıyla ilgili bir metod sunmuşlardır. Jr. H. W. Lenstra, (Lenstra, 2002) makalesinde bu metodun asal cisimler üzerinde çalışmadığını göstermiştir. Yani; bu metodla asal cisimler üzerinde tanımlanan özyineli fonksiyon cisimleri kulelerinin β_1 değişmezi sıfırdır.

Bu proje kapsamında, en küçük asal cisim olan $\mathbb{F}_2$ üzerinde ikinci dereceli özyineli kuleleri tanımlayan $f(X,Y) \in \mathbb{F}_2(X,Y)$ rasyonel fonksiyonları inceledik. Sonuç olarak potansiyeli iyi olan yani en az bir $r \geq 1$ için β_r değişmezi pozitif olan $\mathbb{F}_2$ üzerinde ikinci dereceli özyineli kuleler tanımlayan bütün $f(X,Y) \in \mathbb{F}_2(X,Y)$ rasyonel fonksiyonların bir sınıflandırmasını elde ettik. Ayrıca, elde ettiğimiz her rasyonel fonksiyonun tanımladığı kulenin β_1 değişmezini inceledik ve bu sınıftaki kulelerin neredeyse hepsinin β_1 değişmezinin sıfır olduğu sonucuna vardık.

2.2.3 Gereç, Yöntem ve Sonuçlar

Bu bölümde sonlu cisimler üzerinde potansiyeli iyi olan özyineli kuleleri tanımlayan $f(X,Y) \in F_q(X,Y)$ rasyonel fonksiyonları inceleyeceğiz. Esas olarak; sonlu asal cisimler üzerinde tanımlanan potansiyeli iyi olan özyineli fonksiyon cisimleri kuleleri problemi ile ilgili çalışmalarımızı sunacağız. Daha özel olarak; $\mathbb{F}_2$ üzerinde tanımlanan ikinci dereceli özyineli ve potansiyeli iyi olan kuleleri tanımlayan $f(X,Y) \in \mathbb{F}_2(X,Y)$ rasyonel fonksiyonların bir sınıflandırmasını vereceğiz. Ayrıca, bu kulelerin β_1 değişmezlerini inceleyeceğiz. Bu bölümdeki sonuçlar (Stichtenoth and Tutdere, 2014) ve bu proje kapsamında 29-30 Mayıs 2014 te İstanbul'da yapılan "Mathematical Aspects of Curve Based Cryptography" başlıklı çalıştayda sunulmuştur.

Bu bölümde $\mathbb{F}_q$ ile q elemanlı sonlu bir cisim ve $\mathcal{F} = (F_n)_{n\geq 0}$ ile de $\mathbb{F}_q$ üzerinde tanımlanan özyineli bir fonksiyon cisimleri kulesi gösterilecektir. Bu bölümde kullanılan temel kavramların tanımları Bölüm 2.2.2'de verilmiştir. Bu bölüm boyunca $\mathcal{F}/\mathbb{F}_q$ ile özyineli bir cebirsel fonksiyon cisimleri kulesini göstereceğiz. Yani; $\mathcal{F}/\mathbb{F}_q$ kulesi bir $f(X,Y) = 0$ denklemi tarafından özyineli olarak sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanabilir. Bu konu üzerindeki çalışmamlarımız sonucunda elde ettiğimiz ana sonucumuz aşağıdaki teoremde verilmiştir.

Teorem 2.2.16. *Farzedelim ki $\mathcal{F}/\mathbb{F}_2$ ikinci dereceli özyineli potansiyeli iyi olan bir kule. O zaman $\mathcal{F}/\mathbb{F}_q$ kulesinin temel foksiyon cismi F/F_2 eliptik bir fonksiyon cismidir öyle ki $B_1(F) \in \{2,3,4,5\}$ ve izomorfizma ve eşleniğe kadar aşağıdakiler olur:*

(a) $B_1(F) = 2$ *ise* $\mathcal{F}/\mathbb{F}_2$ *yi tanımlayan sadace bir denklem vardır ve* $\beta_3(\mathcal{F}) = \frac{1}{2}$ *ve bütün* $r \neq 3$ *için* $\beta_r(\mathcal{F}) = 0$.

(b) $B_1(F) = 3$ *ise* $\mathcal{F}/\mathbb{F}_2$ *yi tanımlayan sadace üç denklem vardır ve* $\beta_1(\mathcal{F}) = 0$.

(c) $B_1(F) = 4$ *ise* $\mathcal{F}/\mathbb{F}_2$ *yi tanımlayan sadace altı denklem vardır ve* $\beta_1(\mathcal{F}) = 0$.

(d) $B_1(F) = 5$ *ise* $\mathcal{F}/\mathbb{F}_2$ *yi tanımlayan sadace dört denklem vardır.*

Şimdi de bu teoremin kanıtı için kullandığımız bazı metod ve sonuçları vereceğiz. Öncelikle, diyelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanan bir kule ve $\mathcal{G} = (G_n)_{n\geq 0}$ kulesi de $\mathcal{F}$ kulesinin eşlek kulesi olsun. Bu durumda tanım gereği bütün $n \geq 0$ için $F_n \cong G_n$ olduğu için bütün $r \geq 1$ için

$$\nu_r(\mathcal{F}) = \nu_r(\mathcal{G}), \quad \gamma(\mathcal{F}) = \gamma(\mathcal{G}), \quad \text{ve bu yüzden} \quad \beta_r(\mathcal{F}) = \beta_r(\mathcal{G}) \quad \text{olur.}$$

Şimdi de diyelim ki $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{F}_q)$ (yani; $a, b, c, d \in \mathbb{F}_q$ ve $ad \neq bc$) ve u, $\mathbb{F}_q$ cisminin bir genişlemesinde yer alan $cu + d \neq 0$ koşulunu sağlayan bir eleman olsun. Diyelim ki

$$A \cdot u := \frac{au + b}{cu + d}.$$

$\mathcal{F}/\mathbb{F}_q$, $f(X) = g(Y)$, burada $f(T), g(T) \in \mathbb{F}_q(T)$, denklemi tarafından özyineli olarak tanımlanabilen bir kule olsun. (Beelen and Stichtenoth, 2006) makalesinde şunun kanıtı verilmiştir: herhangi bir $A \in GL(2, \mathbb{F}_q)$ için $f(A \cdot X) = g(A \cdot Y)$ denklemi de özyineli olarak $\mathcal{F}$ kulesini tanımlar. Açıklama 2.2.17 de bu sonucun daha geniş bir genellemesini vereceğiz. Bu genellemenin kanıtı da (Beelen and Stichtenoth, 2006) makalesinde verilen kanıta benzer şekilde yapılabilir.

Açıklama 2.2.17. $\mathcal{F}/\mathbb{F}_q$, $f(X, Y) = 0$ denklemi tarfından tanımlanan bir kule olsun. Herhangi bir $A \in GL(2, \mathbb{F}_2)$ için $f(A \cdot X, A \cdot Y) = 0$ denklemi de $\mathcal{F}/\mathbb{F}_q$ kulesini tanımlar. Ayrıca, $f_1(X, Y)$, $f_2(X, Y) \in \mathbb{F}_2[X, Y]$ aralarında asal polinomlar olmak üzere $f(X, Y) = \frac{f_1(X,Y)}{f_2(X,Y)} = 0$ ve $f_1(X, Y) = 0$ denklemleri özyineli olarak $\mathbb{F}_q$ üzerinde aynı kuleyi tanımlarlar.

Lemma 2.2.18. *Diyelim ki* $\mathcal{F} = (F_n)_{n\geq 0}$ *sonlu cisim* $\mathbb{F}_q$ *üzerinde* $f(X, Y) = 0$ *denklemiyle tanımlanan bir kule öyle ki bazı* $k \geq 1$ *için* $g(F_{k-1}) = 0$ *ve* $g(F_k) \geq 1$. *Diyelim ki bütün* $i \geq 0$ *için* $G_i := F_{i+k-1}$. *O zaman* $G_i/\mathbb{F}_q$ *cebirsel fonksiyon cisimleri dizisi* $\mathcal{G} := (G_i)_{i\geq 0}$ *temel fonksiyon cismi rasyonel olmayan özyineli bir kuledir.*

Açıklama 2.2.19. Lemma 2.2.18 den dolayı temel fonksiyon cisminin cinsi bir ve birden büyük olan $\mathcal{F}/\mathbb{F}_q$ kulelerini ele almak yeterlidir.

Herhangi bir $f(X,Y) \in \mathbb{F}_q(X,Y)$ rasyonel fonksiyonu $f_1(X,Y), f_2(X,Y) \in \mathbb{F}_q[X,Y]$ birer polinom ve $f_2(X,Y) \neq 0$ olmak üzere $f(X,Y) = f_1(X,Y)/f_2(X,Y)$ biçiminde yazılabileceğini biliyoruz. Farzedelim ki $f_1(X,Y)$ ve $f_2(X,Y)$ polinomları aralarında asal. O zaman $T = X$ ya da $T = Y$ için $\deg_T f(X,Y) := \max\{\deg_T f_1(X,Y), \deg_T f_2(X,Y)\}$ değerlerine sırasıyla $f(X,Y)$ fonksiyonun X ya da Y değişkenine göre derecesi diyeceğiz.

Lemma 2.2.20. *Farzedelim ki $\mathcal{F}/\mathbb{F}_q$, $\deg_X f(X,Y) \neq \deg_Y f(X,Y)$ olmak üzere $f(X,Y) = 0$ denklemi tarafından tanımlanan bir kuledir. O zaman bütün $r \geq 1$ için $\beta_r(\mathcal{F}) = 0$ olur.*

Şimdi $\mathcal{F}$ kulesini bir $f(X,Y) = 0$ denklemi tarafından $\mathbb{F}_2$ üzerinde tanımlanan ikinci dereceli potansiyeli iyi olan bir kule olduğunu varsayalım. Lemma 2.2.20 den dolayı $\deg_X f(X,Y) = \deg_Y f(X,Y)$=2 olur. Başka bir deyişle, $\mathcal{F}/\mathbb{F}_2$ kulesinin temel fonksiyon cismi $F/\mathbb{F}_2$ için $f(x,y) = 0$ olmak üzere $F = \mathbb{F}_2(x,y)$ öyle ki $[F : \mathbb{F}_2(x)] = [F : \mathbb{F}_2(y)] = 2$ dir. Riemann'nın Eşitsizliği (Riemann's Inequality) (Stichtenoth, 2009a, Corollary 3.11.4) sonucundan $F/\mathbb{F}_2$ fonksiyon cisminin cinsi $g \leq 1$ olur. Ayrıca, Hasse-Weil sınırını (Stichtenoth, 2009a, Theorem 5.2.3) kullanarak $g = 1$ iken $1 \leq B_1(F) \leq 5$ sonucunu elde ederiz, yani bu durumda $F/\mathbb{F}_2$ eliptik bir fonksiyon cismidir.

Önerme 2.2.21. *$\mathbb{F}_2$ üzerindeki izomorfizmaya kadar her $n \in \{1,2,3,4,5\}$ için $B_1(F) = n$ olan $\mathbb{F}_2$ üzerinde sadace bir $F := \mathbb{F}_2(x,y)$ eliptik fonksiyon cismi vardır. Bu fonksiyon cisimleri açık olarak aşağıdaki gibi ifade edilebilir:*

(i) $B_1(F) = 1$ *ve* $y^2 + y = x^3 + x + 1$,

(ii) $B_1(F) = 2$ *ve* $y^2 + y = (x^2 + x + 1)/x$,

(iii) $B_1(F) = 3$ *ve* $y^2x + yx^2 + 1 = 0$,

(iv) $B_1(F) = 4$ *ve* $y^2 + y = x/(x^2 + x + 1)$,

(v) $B_1(F) = 5$ *ve* $y^2x + y = x^2 + 1$.

Buraya kadar verdiğimiz lemma ve açıklamları kullanarak şu sonuca vardık:

Teorem 2.2.22. *Farzedelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ potansiyeli iyi olan ikinci dereceli $f(X,Y) = 0$ denklemi tarafından $\mathbb{F}_2$ üzerinde tanımlanan özyineli bir kule. O zaman aşağıdakiler olur:*

(a) $\mathcal{G}/\mathbb{F}_2$, $\mathcal{F}/\mathbb{F}_2$ kulesinin eşleniği ise bütün $r \geq 1$ için $\beta_r(\mathcal{F}) = \beta_r(\mathcal{G})$.

(b) Herhangi bir $A \in GL(2,\mathbb{F}_2)$ için $f(A\cdot X, A\cdot Y) = 0$ denklemi de $\mathcal{F}$ kulesini tanımlar.

(c) $\deg_X f(X,Y) = \deg_Y f(X,Y) = 2$ *dir.*

(d) Genelliği kaybetmeksizin $F_1/\mathbb{F}_2$, $B_1(F_1) \in \{1,2,3,4,5\}$ *olan bir eliptik fonksiyon cismidir.*

(e) $f(X,Y) \neq f(Y,X)$.

İspat. Burda (a)-(d) daha önce verdiğimiz lemma ve açıklamaların sonucudur. (e) de (Garcia and Stichtenoth, 2000, Lemma 2.7) de verilmiştir. □

Şimdi farzedelim ki $\mathcal{F} = (F_n)_{n\geq 0}$, sonlu cisim $\mathbb{F}_2$ üzerinde $f(X,Y) = 0$ denklemiyle tanımlanan ikinci dereceli özyineli bir kule ve $F_1/\mathbb{F}_2$ de $\mathcal{F}/\mathbb{F}_2$ nin temel fonksiyon cismidir. Kolaylık olsun diye diyelim ki $F := F_1$. Teorem 2.2.22(d) den genelliği kaybetmeksizin bazı $x, y \in F$ öyle ki $f(x,y) = 0$ için $F = \mathbb{F}_2(x,y)$ dir ve $F/\mathbb{F}_2$, bazı $n \in \{2,3,4,5\}$ için $B_1(F) = n$ olan bir eliptik fonksiyon cismidir. Önerme 2.2.21 den F/F_2 nin izomorfizmaya kadar n tane rasyonel yeri olan tek bir eliptik fonksiyon cismi olduğunu biliyoruz. Ayrıca, $F/\mathbb{F}_2$ aşağıdaki kümede yer alan denklemler tarafından da ifade edilebildiğini biliyoruz.

$$S_n := \{f(A \cdot X, B \cdot Y) = 0 \mid A, B \in GL(2,\mathbb{F}_2)\}.$$

Teorem 2.2.22(b) den herhangi $A, B \in GL(2,\mathbb{F}_2)$ ve $f(X,Y) \in \mathbb{F}_2(X,Y)$ için $f(A \cdot X, B \cdot Y) = 0$ ve $f(X, A^{-1} \cdot (B \cdot Y)) = 0$ denklemleri $\mathbb{F}_2$ üzerinde aynı fonksiyon cisimleri dizisi tanımlarlar. Bu yüzden, her $f(X,Y) \in \mathbb{F}_2(X,Y)$ için $f(X, A \cdot Y) = 0$, burada $A \in GL(2,\mathbb{F}_2)$, öyle ki $f(x,y) = 0$ ve aşağıdaki koşulu sağlayan denklemleri incelemek yeterlidir:

$$\deg_X f(X,Y) = [F : \mathbb{F}_2(x)] = [F : \mathbb{F}_2(y)] = \deg_Y f(X,Y) = 2.$$

Şimdi sırasıyla her $n \in \{1,2,3,4,5\}$ için elde ettiğimiz sonuçları sunacağız.

Önerme 2.2.23. *Sonlu cisim* $\mathbb{F}_2$ *üzerinde potansiyeli iyi olan ikinci dereceli özyineli ve temel fonksiyon cismi* $F/\mathbb{F}_2$ *için* $B_1(F) = g(F) = 1$ *olan bir* $\mathcal{F}/\mathbb{F}_2$ *kulesi tanımlayacak herhangi bir* $f(X,Y) = 0$ *denklemi yoktur.*

Bu bölümün geri kalan kısmında aşağıdaki kavramı sık sık kullanacağız:

Tanım 2.2.24. Diyelim ki F bir cisim ve farzedelim ki $\mathbb{F}_2(x)$, F nin bir altcismi öyle ki $[F : \mathbb{F}_2(x)] = 2$ dir. O zaman $\mathbb{F}_2(x)$, F cisminin *derecesi iki olan bir alt cismidir* diyeceğiz.

Teorem 2.2.25. *Farzedelim ki* $\mathcal{F}/\mathbb{F}_2$ *potansiyeli iyi olan ikinci dereceli özyineli ve temel fonksiyon cismi* $F/\mathbb{F}_2$ *için* $B_1(F) = 2$ *olan bir kule. O zaman eşlenik ve izomorfizmaya*

kadar $\mathcal{F}/\mathbb{F}_2$ aşağıdaki denklemle tanımlanabilir:

$$Y^2 + Y = \frac{X^2 + X + 1}{X}. \tag{2.1}$$

Ayrıca, $\beta_3(\mathcal{F}) = \frac{1}{2}$ ve bütün $r \neq 3$ için $\beta_r(\mathcal{F}) = 0$ dir.

Teorem 2.2.25 nin ispatı için aşağıdaki lemmayı kullandık.

Lemma 2.2.26. *Diyelim ki $F/\mathbb{F}_2$ bir eliptik fonksiyon cismi öyle ki $B_1(F) = 2$. O zaman F cisminin derecesi iki olan sadace iki farklı altcismi $\mathbb{F}_2(x)$ ve $\mathbb{F}_2(y)$ vardır ve aşağıdaki durum sağlanır:*

$$y^2 + y = \frac{x^2 + x + 1}{x}. \tag{2.2}$$

Şimdi de temel fonksiyon cismi $F/\mathbb{F}_2$ nin üç tane rasyonel yeri olduğu durum için elde ettiğimiz sonucu vereceğiz:

Teorem 2.2.27. *Farzedelim ki $\mathcal{F}/\mathbb{F}_2$ potansiyeli iyi olan ikinci dereceli özyineli ve temel fonksiyon cismi $F/\mathbb{F}_2$ için $B_1(F) = 3$ olan bir kule. O zaman eşlenik ve izomorfizmaya kadar $\mathcal{F}/\mathbb{F}_2$ aşağıdaki denklemlerden biriyle tanımlanabilir:*

(1) $Y^2X + X + YX^2 + X^2 + 1 = 0$,

(2) $YX^2 + Y^2 + X = 0$,

(3) $X^2Y^2 + X^2Y + XY^2 + X + Y^2 = 0$.

Teorem 2.2.27 nin kanıtı için şu lemmayı kullandık:

Lemma 2.2.28. *Diyelim ki $F/\mathbb{F}_2$ bir eliptik fonksiyon cismi öyle ki $B_1(F) = 3$. O zaman F cisminin derecesi iki olan sadace üç farklı altcismi $\mathbb{F}_2(x)$, $\mathbb{F}_2(y)$ ve $\mathbb{F}_2(z)$ öyle ki $z := \frac{x^2+x+1}{xy+x}$ vardır ve x, y, z aşağıdaki denklemleri sağlarlar:*

(a) $y^2x + yx^2 + 1 = 0$,

(b) $y^2 + zy^2 + yz^2 + y + 1 = 0$,

(c) $x^2 + zx^2 + xz^2 + x + 1 = 0$.

Ek Sonuç 2.2.29. *Farzedelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ kulesi $\mathbb{F}_2$ üzerinde tanımlanan ikinci dereceli özyineli bir kule öyle ki $\mathcal{F}/\mathbb{F}_2$ nin temel fonksiyon cismi $F_1/\mathbb{F}_2$ için $B_1(F_1) = 3$. O zaman $\beta_1(\mathcal{F}) = 0$ olur.*

Şimdi de temel fonksiyon cismi $F/\mathbb{F}_2$ nin dört tane rasyonel yeri olduğu durum için elde ettiğimiz sonucu vereceğiz.

Teorem 2.2.30. *Farzedelim ki $\mathcal{F}/\mathbb{F}_2$ potansiyeli iyi olan ikinci dereceli özyineli ve temel fonksiyon cismi $F/\mathbb{F}_2$ için $B_1(F) = 4$ olan bir kule. O zaman eşlenik ve izomorfizmaya kadar $\mathcal{F}/\mathbb{F}_2$ aşağıdaki denklemlerden biriyle tanımlanabilir:*

(1) $(Y^2 + Y)(X^2 + X + 1) + X = 0$, *(4)* $X^2Y^2 + X^2Y + XY + X + Y$,

(2) $XY^2 + XY + X^2 + 1 = 0$, *(5)* $X^2Y + XY + X^2 + Y^2 + Y = 0$,

(3) $X^2Y^2 + X^2Y + XY + Y + 1 = 0$, *(6)* $X^2Y + XY + X + Y^2 + Y = 0$.

Teorem 2.2.30 ün kanıtı için şu lemmayı kullandık:

Lemma 2.2.31. *Diyelim ki $F/\mathbb{F}_2$ bir eliptik fonksiyon cismi öyle ki $B_1(F) = 4$. O zaman F cisminin derecesi iki olan sadace dört farklı altcismi $\mathbb{F}_2(x)$, $\mathbb{F}_2(y)$, $\mathbb{F}_2(z)$ ve $\mathbb{F}_2(t)$ öyle ki*

$$z = \frac{1}{y(x^2 + x + 1) + x + 1} \quad ve \quad t = \frac{1}{y(x^2 + x + 1) + x^2 + 1}.$$

Ayrıca, x, y, z, t aşağıdaki denklemleri sağlarlar:

(a) $(y^2 + y)(x^2 + x + 1) = x$, *(d)* $x^2t + xt^2 + xt+ = t + 1$,

(b) $z(t^2 + t) = z^2 + 1$, *(e)* $y^2z^2 + y^2z + y^2 + yz = z^2 + z$,

(c) $x^2z^2 + x^2z + xz = z + 1$, *(f)* $y^2t^2 + y^2t + y^2 + yt^2 + yt = t + 1$.

Ek Sonuç 2.2.32. *Farzedelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ kulesi $\mathbb{F}_2$ üzerinde tanımlanan ikinci dereceli özyineli bir kule öyle ki $\mathcal{F}/\mathbb{F}_2$ nin temel fonksiyon cismi $F_1/\mathbb{F}_2$ için $B_1(F_1) = 4$. O zaman $\beta_1(\mathcal{F}) = 0$ olur.*

Şimdi de temel fonksiyon cismi $F/\mathbb{F}_2$ nin beş tane rasyonel yeri olduğu durum için elde ettiğimiz sonucu vereceğiz.

Teorem 2.2.33. *Farzedelim ki $\mathcal{F}/\mathbb{F}_2$ potansiyeli iyi olan ikinci dereceli özyineli ve temel fonksiyon cismi $F/\mathbb{F}_2$ için $B_1(F) = 5$ olan bir kuledir. O zaman eşlenik ve izomorfizmaya kadar $\mathcal{F}/\mathbb{F}_2$ aşağıdaki denklemlerden biriyle tanımlanabilir:*

(1) $Y^2X + Y + X^2 + 1 = 0$, *(3)* $X^2Y^2 + XY^2 + X + Y = 0$,

(2) $X^2 + XY^2 + X + Y = 0$, *(4)* $X^2Y^2 + X^2 + XY^2 + Y + 1 = 0$.

Teorem 2.2.33 in kanıtı için aşağıdaki lemmayı kullandık.

Lemma 2.2.34. *Diyelim ki $F/\mathbb{F}_2$ bir eliptik fonksiyon cismi öyle ki $B_1(F) = 5$. O zaman F cisminin derecesi iki olan sadace beş farklı altcismi $\mathbb{F}_2(x)$, $\mathbb{F}_2(y)$, $\mathbb{F}_2(z)$ ve $\mathbb{F}_2(t)$ öyle ki $\mathbb{F}_2(x), \mathbb{F}_2(y), \mathbb{F}_2(z), \mathbb{F}_2(t)$ ve $\mathbb{F}_2(w)$ öyle ki*

$$z = \frac{xy + x + 1}{x^2}, \quad t = \frac{x}{xy + 1}, \quad ve \quad w = \frac{y + 1}{x}.$$

Ayrıca, x, y, z, t, ve w aşağıdaki denkemleri sağlarlar:

(a) $uv^2 + v = u^2 + 1$ *for* $(u, v) \in \{(x, y), (w, y)\}$,

(b) $u^2v^2 + u = v + 1$ *for* $(u, v) \in \{(x, z), (x, w)\}$,

(c) $u^2v^2 + u = v^2 + v$ *for* $(u, v) \in \{(x, t), (z, t), (t, w)\}$,

(d) $y^2z^2 + z^2 + zy^2 = y$,

(e) $y^2t^2 + y^2t + y = t^2 + 1$,

(f) $z^2w^2 + z^2 + z = w^2 + w$.

Açıklama 2.2.35. Teorem 2.2.33(1) de verilen denklemin tanımladığı $\mathcal{F}$ kulesi (Tutdere, 2009b) de $\mathbb{F}_2$ üzerinde incelenmiştir. Ancak, bu kulenin β_1 değeri tam olarak hesaplanamamıştır. Ancak, bu değerin hesaplanabilmesi için gerekli olan kuledeki fonksiyon cisimlerin yer sayısı ve cinsi için bazı sınırlar (Tutdere, 2009b) de verilmiştir. Bu kulenin β_1 değerini hesaplayabilmek için çalışmalarımız devam etmektedir.

İspat. [Teorem 2.2.16 in Kanıtı] Önerme 2.2.23, Teoremler 2.2.25, 2.2.27, 2.2.30, 2.2.33, Ek sonuçlar 2.2.29 ve 2.2.32 kullanarak Teorem 2.2.16 elde edilir. □

2.3 Cebirsel Eğriler, Rasyonel Noktaları, Modüler Polinom ve Uygulamaları

Bu alt bölümde cebirsel eğriler, rasyonel noktaları, modüler polinom ve uygulamaları hakkında proje kapsmında bilgi verilecektir.

2.3.1 Giriş

Polinom denklemlerinin çözümü matematik tarihinde her zaman önemli bir yer tutmuştur. En genel haliyle bir K cismi üzerinde tanımlanan r adet n değişkenli polinom

$$f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$$

verilmiş olsun. Bu polinomlar yardımı ile oluşturulan

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= 0 \\ f_2(x_1, x_2, \ldots, x_n) &= 0 \\ &\ldots \\ f_r(x_1, x_2, \ldots, x_n) &= 0 \end{aligned}$$

polinom sisteminin çözümleri ile ilgileniyoruz. K cisminin $\mathbb{Q}, \mathbb{Q}_p$, bir sayı cismi veya bir $\mathbb{F}_q$ sonlu cismi gibi sayı kuramı açısından ilginç bir cisim olmasının aritmetik önemi bulumaktadır. Diğer yandan ilgili soruların K cisminin bir sonlu cisim olması durumunda cevaplandırılmasının uygulamalar açısından ayrı bir önemi vardır. Verilen bir sıralı $(a_1, a_2, \ldots, a_n) \in K^n$ için $x_1, x_2, \ldots, x_n$ değişkenlerinin yerine sırasıyla $a_1, a_2, \ldots, a_2$ değerlerini koyduğumuzda yukarıdaki denklemlerin herbiri sağlanıyorsa, bu sıralıya bu denklem sisteminin bir çözümü diyeceğiz. Genellikle a_i değerlerinin K cismin genişlemesi olan bir L cisminden geldiğini varsayacağız. Çoğu durumda L cismi olarak K cisminin bir cebirsel kapanışını alacağız. Böylelikle yukarıdaki denklem sisteminin çözümleri L^n uzayının bir altkümesini oluşturacak. Bu şekilde tanımlanan altkümeye bir *cebirsel varyete* diyeceğiz. Varyetenin geomterisini inceleyerek polinom denklemlerinin çözümleri hakkında önemli sonuçlar elde edilebilir.

Verilen bir $(a_1, a_2, \ldots, a_n)$ çözümü için a_i değerlerinin herbiri K cismi içinde yer alıyorsa, bu çözüme rasyonel çözüm, varyete üzerindeki ilgili noktaya da *rasyonel nokta* diyeceğiz. Sayılar kuramındaki neredeyse her soru uygun varyetelerin rasyonel noktaları hakkında sorulara indirgenebilir.

Polinom denkleminin tanımladığı varyetenin tek boyutlu olması durumunun ayrı bir önemi olmasından bu durum geçmişte ayrıntılı bir şekilde incelenmiştir. Bu durumda varyeteye *cebirsel eğri* adı verilir. Cebirsel eğrilerin daha yüksek boyutlu varyetelerle kıyasla daha iyi anlaşılmış olmasına rağmen bu durumda da hala cevaplanmayı bekleyen önemli problemler fazlasıyla mevcuttur. Bundan böyle cebirsel eğriler ile ilgileneceğiz. Yukarıda verilen tanımdan biraz ayrılarak, teknik bir farklılık olarak bu eğrilere sonsuzdaki sonlu adet noktalarını da ekleyerek elde edilen projektif (izdüşümsel) eğriler ile uğraşacağız. Bu eğrilerin indirgenemez olduğunu ve ayrıca tekil noktası olmadığını varsayacağız. Her eğri için tekil noktası olmayan projektif bir model bulunabileceğinden bu ciddi bir sınırlama oluşturmamaktadır. (Hirschfeld and Torres, 2008; Niederreiter and Xing, 2001; Stichtenoth, 2009b; Villa Salvador, 2006) kaynaklarında cebirsel eğrilerin teorisi ile ilgili

daha detaylı bilgi bulunabilir.

Bundan sonra K cisminin q elemana sahip $\mathbb{F}_q$ sonlu cismi olduğunu varsayacağız. $\mathcal{C}$ eğrisi $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı bir cebirsel eğri olsun (projektif, indirgenemez ve tekil noktası olmayan). Bu şekilde verilen bir eğriye cins adını verdiğimiz ve $g(\mathcal{C})$ ile göstereceğimiz bir negatif olmayan tamsayı değişmezi eşlenebilir. Bu değişmez eğrinin geomterisi hakkında önemli bilgi ihtiva eder. Eğrinin rasyonel noktaları $\mathbb{F}_q^n$ sonlu kümesinin bir altkümesini oluşturduğundan sonlu sayıdadır. Bunların sayısının incelenmesi sayılar kuramının tarihsel gelişimi boyunca sıklıkla araştırılmış bir konudur. Bu yönde elde edilen en önemli sonuçlardan biri yirminci yüzyılın ilk yarısında ispatlanan Hasse–Weil Teoremi'dir. Verilen bir eğrinin birçok aritmetik özelliği bu eğriye eşlenen bir zeta fonksiyonu $\zeta(s)$ yardımı ile tutulabilir. Hasse–Weil Teoremi ise bu zeta fonksiyonunun bütün köklerinin $\Re s = 1/2$ doğrusu üzerinde olduğunu ifade eder (bkz. (Hasse, 1933; Weil, 1948)). Diğer bir deyişle cebirsel eğrilere eşlenen zeta fonksionları için Riemann hipotezinin bir ispatını verir. Bunun eğrinin aritmetiği ile ilgili önemli sonuçları vardır: rasyonel noktalarının sayısını $N(\mathcal{C})$ ile gösterirsek Hasse–Weil üst sınırı olarak bilinen şu eşitlik sağlanır:

$$N(\mathcal{C}) \leq q + 1 + 2 \cdot g(\mathcal{C})\sqrt{q}.$$

Bu sonuçtan sonra sonlu cisimler üzerinde tanımlı cebirsel eğrilerin rasyonel noktaların sayısı ile ilgili birçok sonuç elde edilmiş olmakla birlikte hala anlaşılmayan birçok nokta ve cevaplanamayan birçok soru vardır. Bu eşitliği sağlayan eğrilere *maksimal eğri* adı verilir. Özellikle kriptoloji ve kodlama teorisindeki uygulamalar için çok rasyonel noktaya sahip eğrilere ihtiyaç duyulduğundan maksimal eğriler ve çok rasyonel noktaya sahip eğrilerin önemi aşikardır. Verilen bir cinse sahip bir sonlu cisim üzerinde tanımlı bilinen en çok rasyonel noktaya sahip eğrilerin listesi van der Geer–van der Vlugt tarafından sistematik olarak tablolarda toplanmaya başlanmıştır (bkz. (Geer and Vlugt, 2000)). Bu listelerin en güncel hali (mp, 2014) sayfasında bulunabilir. çok rasyonel noktaya sahip eğrilerin kripoloji ve kodlama teorisindeki farlı uygulamaları için bkz. (Chen and Cramer, 2006; Ishai and Sahai, 2009; Niederreiter and Xing, 2001; **?**; Tsfasman and Vladut, 1991; Tsfasman and Nogin, 2007; Tsfasman and Zink, 1982). Bu eğriler aynı zamanda hızlı çarpma algoritmaları elde etmek için kullanılmaktadır, bkz. (Chudnovsky and Chudnovsky, 1988; Shparlinski and Vladut, 1991).

1980 yılında Ihara'nın yüksek cinse sahip maksimal eğrinin var olamayacağını göstermesi ile birlikte yüksek cinse sahip eğriler için uygun alternatif sınırlar ile ilgili araştırmalar hız kazandı. Verilen bir $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı yüksek cinse sahip eğrilerin nokta sayısını daha iyi anlamak için Ihara sabiti olarak bilinen şu şekildeki

sabitler incelenmeye başladı:

$$A(q) := \limsup_{g(\mathcal{C})\to\infty} \frac{N(\mathcal{C})}{g(\mathcal{C})}$$

Ihara sabiti bize yüksek cinsten bir eğrinin cinsine oranla en fazla ne kadar rasyonel noktaya sahip olabileceğini söyler. Hasse–Weil üst sınırı bize $A(q) \leq 2\sqrt{q}$ eşitsiliğini verse de $A(q)$'nun gerçek değeri bundan daha küçük olmak zorundadır (yüksek cinste maksimal eğriler olmadığından). Drinfeld–Vladut (bkz. (Vladuts and Drinfeld, 1983)) Ihara sabiti için şu eşitsizliği elde etmişlerdir:

$$A(q) \leq \sqrt{q} - 1.$$

Günümüzde de Ihara sabiti için bilinen en iyi üst sınır budur.

2.3.2 Yöntem ve Sonuçlar

Alt sınırlar elde etmek için ise cinsleri artan ve herbiri çok rasyonel noktaya sahip olan eğri dizileri inşa etmek gerekmektedir. Diğer bir deyişle, her biri aynı $\mathbb{F}_q$ sonlu cismi üzerinde tanımlanmış ve doğal sayılar tarafından endeklenmiş bir dizi $(\mathcal{C}_i)_{i\geq 1}$. Verilen böyle bir $\mathcal{F}$ dizisi için dizinin limiti şu şekilde tanımlanır:

$$\lambda(\mathcal{F}) = \lim_i \frac{N(C_i)}{g(C_i)}.$$

Bu şekildeki her $\mathcal{F}$ dizi için

$$0 \leq \lambda(\mathcal{F}) \leq A(q) \leq \sqrt{q} - 1$$

eşitliği sağlanacağından yüksek limite sahip $\mathcal{F}$ dizilerinden doğrudan Ihara sabiti için altlimitler elde edeceğimiz aşikardır.

Bu dizilerin inşası için farklı yöntemler kullanılmıştır. Serre sınıf cisim kuleleri yardımı ile her $\mathbb{F}_q$ için

$$A(q) > 0$$

olduğunu göstermiştir. Ihara q'nun bir tam kare olması durumu için çok daha güçlü olan

$$A(q) \geq \sqrt{q} - 1$$

eşitliğinin sağlanması gerektiği göstermiştir (bkz. (Ihara, 1982)). Drinfeld–Vladut üst sınırı ile karşılaştırıldığında bu şekildeki sonlu cisimler için Ihara sabitinin değerinin $\sqrt{q} - 1$ olduğu hemen görünür. Ihara sabitinin tam değerinin bilindiği tek sonlu cisimler eleman

sayısı bir tam kare olanlardır. Bu ispatın arkasında yatan ana fikir şu şekildedir: Eliptik eğriler $4a^3 + 27b^2 \neq 0$ olmak üzere

$$y^2 - (x^3 + a \cdot x + b)$$

polinomu ile tanimlanan eğrilerdir. İki eliptik eğrinin ne zaman izomorf olacağı doğal bir şekilde tanımlanabilir. Eliptik eğrilerin izomorfizma sınıfları ise yine başka eğriler yardımı ile parametrize edilebilir. Bu eğrilere *modüler eğri* adı verilir. Modüler eğrilerin üzerindeki herbir nokta bir eliptil eğri izomorfizma sınıına tekabül eder. Pozitif karakteristikte eliptik eğriler endomorfizma halkalarının özelliğine bağlı olarak *adi* ve *süpersingüler* olmak üzere iki gruba ayrılabilirler. Süpersingüler eliptik eğriler her zaman eğrinin tanımlı olduğu cismin asal cisminin ikinci dereceden bir genişlemesi üzerinde tanımlanabilir. Diğer bir değişle, karakteristik p'de bir süpersingüler eğri $\mathbb{F}_{p^2}$ cismi üzerinde tanımlanabilir. Bu modüler eğrinin üzerinde bulunan ve süpersingüler bir eliptik eğri izomorfizma sınıfına denk gelen noktalar da bu sebepten dolayı modüler eğrinin üzerinde $\mathbb{F}_{p^2}$-rasyonel noktalar verir. Sadece izomorfizmsa sınıf yerine daha kapsamlı bir denklik kullanarak ise bu şekilde üzerinde çok sayıda $\mathbb{F}_{p^2}$-rasyonel nokta olan yüksek cinse sahip eğriler elde etmek mümkün. Bu eğrilerin $\mathbb{F}_{p^2}$-rasyonel noktalarının cinslerine orani ise $\sqrt{p^2} - 1 = p - 1$ değerine yakınsamakta. Bu da bize yukarıda belirtilen sonucu verir.

p bir asal sayı olmak üzere $q = p^3$ olacak şekildeki sonlu cisimler için ise Zink ((Zink, 1985)) Shimura yüzeylerinin indirgenmesi ile elde ettiği eğri dizilerin yardımı ile

$$A(p^3) \geq \frac{2(p^2 - 1)}{p + 2}$$

olduğunu göstermiştir. Bu sonucun bütün kübik sonlu cisimler için genelleştirilmiş hali Bezerra–Garcia–Stichtenoth tarafından verilmiştir (bkz. (Bezerra and Stichtenoth, 2005)).

Son olarak Bassa–Beelen–Garcia–Stichtenoth (bkz. (Bassa, 2006)) $k \geq 1$ olmak üzere $q = p^{2k+1}$ şeklindeki sonlu cisimler için

$$A(p^{2k+1}) \geq \frac{2}{\frac{1}{p^k - 1} + \frac{1}{p^{k+1} - 1}}$$

eşitsizliğini göstermişlerdir. Bu sonuç Drinfeld modüler varyeteler üzerinde bulunan bazı özel eğriler kullanılarak elde edilmiştir. Biraz detay vermek gerekirse; klasik durumda, yukarıda bahsi geçen eliptik eğriler karmaşık sayı düzlemindeki mertebesi 2 olan ızgaralara (latislere) denk gelir. Pozitif karakteristikte süpersingüler eliptik eğrilerin $\mathbb{F}_{p^2}$ üzerinde tanımlanabiliyor olmasının ve böylelikle modüler eğriler üzerinde $\mathbb{F}_{p^2}$-rasyonel nokta

vermesinin sebebi temelde ızgaraların mertebesinin 2 olmasından kaynaklanmaktadır. Karmaşık düzlemde daha yüksek mertebeden izgaralar olmadığından bu yaklaşım kare sonsuz cisimler dışında sonuç vermemektedir. Fakat eliptik eğri yerine onların karakteristik p analojisini oluşturan Drinfeld modülleri ve bunları parametrize eden Drinfeld Modüler varyetelere baktığımızda durum farklıdır (Drinfeld modülleri ve Drinfeld modüler eğriler için bkz (Gekeler, 1986; Goss, 1997; Thakur, 2004)): bu durumda $\mathbb{C}$ karmaşık sayıları yerine pozitif karakteristikte bunun analogu olan $\mathbb{C}_\infty$ cismi kullanılır, ki bu cisim her mertebeden izgaralar içerir. Belirli bir r mertebesinden ızgaralara denk gelen Drinfeld modüllerinden süper singüler olanlar bu sefer $\mathbb{F}_q^r$ cismi üzerinde tanımlanabilir ve bunları parametrize eden uzay üzerinde $\mathbb{F}_q^r$-rasyonel noktalar verir. Daha yüksek mertebeden izgaralar için daha büyük bir serbestlik derecesi olmasından dolayı bunları parametrize eden geometrik objeler daha yüksek boyuttandır (mertebe r izgaralar için boyutu $r-1$ dir). Bu varyeteler üzerinde süpersingüler Drinfel modüllerinin izomorfizma sınıflarına denk gelen noktalardan geçen eğriler bularak yukarıdaki eşitsizliği ispatlamak mümkün oluyor. Elde edilen bu eğrilerin rasyonel noktalarının sayısını elde edilmesinin kolay olmasına karşın bu eğrilerin cinslerini hesaplamak kolay değildir. Bu pozitif karakteristikte vahşi (wild) dallanmanın varlığından kaynaklanmaktadır. Bu nedenle çok rasyonel noktaya sahip bu eğrileri elde ederken aynı zamanda cinsleri de kolay hesaplanacak eğriler elde etmek gerekmektedir. En iyi durumda bu eğrilerin denklemleri özyinelemeli olarak verilir: bu durumda söz konusu eğriler yukarıdaki gibi farklı $f_1(x_1,\ldots,x_n), f_2(x_1,\ldots,x_n),\ldots,f_r(x_1,\ldots,x_n)$ polinomları yardımı ile verilmek yerine tek bir polinomda değişkenlerin kaydırılması ile elde edilir: bir $F(U,V)\in K[U,V]$ iki değişkenli polinomu verilmiş olsun. $\mathcal{F}=(\mathcal{C}_i)_{i\geq 1}$ dizisindeki $\mathcal{C}_n$ eğrisi

$$F(x_1,x_2)=0, F(x_2,x_3)=0,\ldots,F(x_{n-1},x_n)=0$$

denklemleri yardımı ile verilmiş ise $\mathcal{F}$ eğri dizisine $F(U,V)$ denklemi yardımı ile özyinelemeli olarak tanımlanmış denir. Burada dikkat edilecek husus, $\mathcal{C}_{n+1}$ eğrisinin $\mathcal{C}_n$ eğrisine $F(x_n,x_{n+1})=0$ eşitliğini sağlayan bir x_{n+1} değişkeni eklemek ile elde ediliyor olması. x_{n+1} değişkeninin sağlaması gerektiği tek koşulun son değişken olan x_n ile ilgili olmasi bu dizideki eğrilerin cinslerinin hesaplanmasını oldukca kolaylaştırmaktadır. Fakat çoğu durumda eğrilerin denklemleri özyinelemeli denklemler ile verilememektedir. Bu şekilde verilen eğri dizileri elde etmek için söz konusu eğriler üzerinde ciddi sınırlamalar koymak gerekmektedir. Örneğin mertebe 2 durumunda modüler eğrilerin seviyeleri sabit tutulan bir indirgenemezin kuvvetleri olarak seçildiğinde özyinelemeli bir şekilde tanımlanmış eğri dizileri elde edilir. Bu durumda eğrileri tanımlayan $F(U,V)$ polinomu modüler polinom $\Phi_n(X,Y)$ tarafından verilmektedir. Pozitif karakteristikte

modüler polinom ile ilgili elde edilen bazı son sonuçlar (Bassa and Beelen, 2011, 2012) kaynaklarında bulunabilir. Fakat modüler polinomlar ile ilgili halen birçok açık soru bulunmaktadır. (Bassa and Beelen, 2012) makalesinde seviyesi T olan modüler polinom $\Phi_T(X,Y)$ için

$$\Phi_T(X,Y) = (X+Y+T(T^{q-1}-1)^{q+1})^{q+1} - XY^q - X^qY$$

$$+(XY)^q(T^{1-q}-1) + XY(T^{q-1}-1)^{q^2}$$

$$-T^{1-q}XY\sum_{i=0}^{\lfloor\frac{q-1}{2}\rfloor} C_i \cdot (XY - T^q(X+Y+T(T^{q-1}-1)^{q+1}))^{q-1-2i}(XYT^{q^2+1})^i$$

ifadesinin doğru olduğu ispatlanmıştır. Burada geçen C_i sabitleri

$$C_i := \frac{1}{i+1}\binom{2i}{i} = \binom{2i}{i} - \binom{2i}{i-1}$$

ifadesi ile tanımlanan Catalan sayılarını göstermekte. Modüler polinom için verilen bu ifadenin doğrulu j-değişmezinin özellikleri kullanılarak bazı sadeleştirmeler yardımı ile gösterilebiliyor olsa da modüler polinomu veren ifadenin içinde Catalan sayılarının neden karşımıza çıktığının herhangi bir açıklaması bulunmamaktadır. Catalan sayılarının özellikle kombinatorikte sıkça karşımıza çıkmasından dolayı modüler polinomun bu ifadesinde katsayı olarak bulunan Catalan sayılarının daha derin kombinatorik bir açıklaması olduğu aşikardır. (El-Guindy and Papanikolas, 2013; El-Guindy, 2013) çalışmalarında elde edilen sonuçlar da modüler polinomun tanımında bazı kombinatorik öğelerin varlığına işaret etmektedir. Bu bağlantıyı incelemek modüler polinomun aritmetik özellklerini anlamak için önemli bir adım oluşturacaktır. Proje kapsamında $\Phi_T(X,Y)$ modüler polinomunun katsayılarında karşımıza çıkan Catalan sayılarını kombinatorik yönden açıklamaya çalışmak yönünde girişimlerde bulunulmuş olsa da bu yönde tatmin edici bir cevap bulunulamamıştır. Benzer şekilde daha yüksek mertebeden Drinfeld modülleri için mertebe 2 durumundaki modüler polinoma benzer özelliklere sahip yapılar elde etmek yine başka sonlu cisimler üzerinde özyinelemeli bir şekilde tanımlı ve rasyonel noktalarının cinslerine oranının iyi davranış sergilediği eğri dizileri elde etmek için önemli bir adım oluşturacaktır. Çok daha zor ve kapsamlı olan bu soru üzerinde yürütülen çalışmalar ne yazık ki herhangi bir sonuç vermemiştir. Fakat yapılan çalışmalar bu problemlerin daha iyi anlaşılmasına ve bu konuda ileride de çalışmalara devam edilecek üniversitelerarası ve uluslararası ortak çalışmalara sebebiyet vermiş olması açısından çok faydalı olmuştur. Bu alandaki çalışmalara gelecekte de devam edilmesi öngörülmektedir. Oluşan bilgi birikimi ile beraber gelecekteki ortak çalışmaların sonucunda tatmin edici

sonuçlar elde edileneceği umulmaktadır.

2.4 $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ Eğrisinin $\mathbb{F}_{q^m}$ Üzerindeki Rasyonel Noktaları

Bu çalışmada q, 2'den farklı herhangi bir asal sayının kuvveti olmak üzere $n|m$ şartını sağlayan keyfi h, n, m pozitif tam sayıları ve $\gamma, \alpha \in \mathbb{F}_{q^m}$, $\gamma \neq 0$ elemanları için $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ eğrisinin bir çok durumdaki $\mathbb{F}_{q^m}$-rasyonel noktalarının sayısı hesaplanmıştır.

Sonlu cisimler üzerindeki cebirsel eğriler matematiğin önemli araştırma konularından biridir. Bu eğrilerin kodlama teorisi, kriptografi ve yarı-rastgele nokta kümeleri (quasi-random point sets) gibi pek çok alanda uygulamaları vardır (Niederreiter and Xing, 2001, 2009; Stichtenoth, 2000; Tsfasman et al., 2007). Burada kısaca cebirsel eğri dediğimiz yapı daha geniş olarak açıklandığında aslında singüler noktası olmayan (smooth), geometrik indirgenemez (geometrically irreducible) ve projektif (projective) eğridir.

Sonlu cisimler üzerindeki cebirsel eğrilerin önemli parametreleri arasında cins ve rasyonel nokta sayıları vardır. Bazı durumlarda cinsleri hesaplanabilir ve rasyonel nokta sayılarını hesaplamak zor olabilir. Sonlu cisim üzerindeki bir eğri $\mathcal{X}$, onun cinsi $g(\mathcal{X})$ ve rasyonel nokta sayısı $N(\mathcal{X})$ olsun. Bu eğri q elemanlıbir sonlu cisim üzerinde tanımlanmış ve bu cisim üzerinde kesinlikle indirgenemez (absolutely irreducible) olsun. Bu aslında bu eğrinin her pozitif n sayısı için q^n elemanlı bir sonlu cisim altında da indirgenemez olduğu anlamındadır. Karakteristiği pozitif olan cisimler üzerinde Riemann Hipotezi olarak adlandırılan Hasse-Weil eşitsizliği aşağıdaki çok ilginç sonucu vermektedir:

$$q + 1 - 2g(\mathcal{X})\sqrt{q} \leq N(\mathcal{X}) \leq q + 1 + 2g(\mathcal{X})\sqrt{q} \tag{2.1}$$

Dikkat edilirse burada $\mathcal{X}$ eğrisinin yalnızca 2 parametresi, $g(\mathcal{X})$ ve $N(\mathcal{X})$, kullanılmıştır. Yukarıdaki (2.1) denkleminde üst sınırı sağlayan eğriler vardır ve maksimal eğriler diye adlandırılır. Yine (2.1) denkleminde alt sınırı sağlayan eğriler vardır ve minimal eğriler diye adlandırılır. Tüm maksimal ve minimal eğrilerin bulunması ve sınıflandırılması önemli bir açık problemdir.

Eliptik eğriler cinsi 1 olan eğriler demektir. Eliptik eğriler için rasyonel noktaların neler olabileceği çözülmüş ve çözümü oldukça derin olan bir sonuçtur.

Diyelim ki E eleman sayısı p^n olan bir cismin üzerinde tanımlanmış, kesinlikle indirgenemez ve cinsi 1 olan bir eğri olsun. Bu eliptik eğrinin rasyonel nokta sayısı $N(\mathrm{E}) = p^n + 1 - 6$ olsun. Yani b sayısı bize bir bakıma rasyonel nokta sayısını bir önceki

formül ile versin. O zaman b sayısı, $-2p^{\frac{n}{2}} \leq b \leq 2p^{\frac{n}{2}}$ aralığında aşağıdaki özelliklerden birini sağlıyorsa, $N(\mathrm{E}) = p^n + 1 - 6$ değerini alan bir eliptik eğri E vardır. Aksi halde yoktur:

1. $\gcd(b, p) = 1$.
2. n çift ve $b \in \{-2p^{\frac{n}{2}}, 2p^{\frac{n}{2}}\}$. Bu durumda E eğrisi maksimal/minimal eğri olur.
3. n çift ve $p \equiv 1 \pmod 3$ ve $b = \pm p^{\frac{n+1}{2}}$.
4. n tek, $p \in \{2, 3\}$ ve $b = \pm p^{\frac{n+1}{2}}$.
5. n tek ve $b = 0$.
6. n çift, $p \equiv 1 \pmod 4$ ve $b = 0$.

Bu tür bir sonuç cinsi 2 veya daha büyük olan eğriler için bilinmemektedir (ve büyük olasılıkla çok zordur). Ancak bazı eğri sınıfları için rasyonel nokta sayısı ve cins tam olarak hesaplanabilir. Projemizin 3. gelişme raporunda sunulan çalışmamızda rasyonel nokta sayısı ve cinsi tam olarak hesaplanabilen bir eğri sınıfı çalışılmıştır. Ayrıca bu eğri sınıfı daha önce çalışılan bir eğri sınıfının bir güncellemesidir. Literatürde verilen sonuçlar geliştirilmiş ve hesaplanmış, bazı durumlarda hesaplamalar tamamlanmıştır. Sonuçlarımız bu yeni durumların çok daha komplike olduğunu göstermektedir (Özbudak and Saygı, 2014).

Diyelim ki p tek bir asal sayı olsun. Yine e ve m pozitif sayılar, $q = p^e$, $\mathbb{F}_q$ ve $\mathbb{F}_{q^m}$ eleman sayısı q ve q^m olan sonlu cisimler olsun. Ayr?ca n pozitif sayısı m pozitif sayısını bölsün. İz (trace) fonksiyonu şu şekilde tanımlanır:

$$\begin{aligned} \mathrm{Tr}_{q^m/q^n} : &\mathbb{F}_{q^m} \to \mathbb{F}_{q^n} \\ &x \longmapsto x + x^{q^m} + x^{q^{2m}} + ... + x^{q^{m(n-1)}} \end{aligned}$$

Bizim çalışacağımız cebirsel eğri Artin-Schreier türünde şu şekilde ifade edilir:

$$\mathcal{X} : y^{q^n} - y = \gamma x^{q^{h+1}} - \alpha$$

öyle ki h negatif olmayan bir tam sayı, $\gamma \in \mathbb{F}_{q^m}^*$ ve $\alpha \in \mathbb{F}_{q^m}$. Burada $\mathcal{X}$ eğrisi $\mathbb{F}_{q^m}$ üzerinde kesinlikle indirgenemezdir. Yine bu eğrinin cinsi $g(\mathcal{X})$ şudur:

$$g(\mathcal{X}) = \frac{(q^n - 1)q^h}{2}$$

Yani cinsi oldukça yüksek olabilen bir eğridir.

Bu eğrinin rasyonel nokta sayısı $N(\mathcal{X})$ hem δ ve α'ya hem de n, m ve h sayılarının asal çarpanlarına bağlıdır. Bu asal çarpanlara bağlı olarak $s, t \geq 0$ tam sayılarını ve r, m_1, h_1 pozitif tam sayılarını şu şekilde tanımlayalım:

$$m = 2^s r m_1, \quad h = 2^t r h_1$$

öyle ki obeb(m_1, h_1) =obeb$(2, rm_1h_1) = 1$. Ayrıca $u \geq 0$ tam sayısını ve ρ, n_1, m_2 pozitif sayısını şu şekilde tanımlayalım:

$$m = 2^u \rho n_1, \quad m_1 = n_1 m_2$$

öyle ki obeb$(2, \rho n_1) = 1$, $\rho | r$ ve $n_1 | m_1$. Son olarak da

$$A = \mathrm{Tr}_{q^m/q^n}(\alpha)$$

olsun.

$\mathcal{X}$ eğrisinde sonsuzda 1 rasyonel nokta vardır. Diğer rasyonel noktaların sayısı için Hilbert'in 90 numaralı teoremini kullanarak:

$$N(\mathcal{X}) = 1 + q^n N(m, n)$$

öyle ki

$$N(m, n) = \left| \left\{ x \in \mathbb{F}_{q^m} : \mathrm{Tr}_{q^m/q^n} \left(\gamma x^{q^h+1} - \alpha \right) = 0 \right\} \right|$$

denklemini elde ederiz. Yani $\mathcal{X}$ eğrisinin rasyonel nokta sayısını bulmak bir bakıma $N(m, n)$ ile ifade edilen kümenin eleman sayısını bulmak anlamındadır.

Hipotezimizde $n | m$ olduğu için $n \leq s$ şeklindedir. Bu makalede $N(m, n)$ ve ilgili $\mathcal{X}$ eğrisinin rasyonel nokta sayısı:

- $s \leq t$ olduğunda Teorem 2.4.1'de tamamen,
- $s \geq t + 1$ ve $u \leq t$ olduğunda Teorem 2.4.2'de tamamen,
- $t + 1 \leq u \leq s$ ve $A = 0$ olduğunda ise Teorem 2.4.3'te

bulunmuştur. Geriye $t + 1 \leq u \leq s$ ve $A \neq 0$ durumu kalmıştır ve daha zor olduğu düşünülmektedir. Literatürde bu soru $n = 1, s \geq t + 1$ ve $\alpha = 0$ için Klapper tarafından çözülmüştür (Klapper, 1997). Bu bizim verdiğimiz Teorem 2.4.2'nin özel bir alt haline denk gelmektedir.

Teorem 2.4.1. *Diyelim ki $s \leq t$, η ve η' $\mathbb{F}_q$ ve $\mathbb{F}_{q^m}$ sonlu cisimlerinin çarpımsal kuadratik karakterleri (multiplicative quadratic characters) olsun. O zaman şu sonuçlar vardır:*

- *Eğer m/n çift sayı ve $A = 0$ ise;*

$$N(m,n) = \begin{cases} q^{m-n} - (q^n - 1)q^{m/2-n} & \text{eğer } \eta\left((-1)^{m/2} - n\right)\eta'(\gamma) = 1 \text{ ise;} \\ q^{m-n} + (q^n - 1)q^{m/2-n} & \text{eğer } \eta\left((-1)^{m/2} - n\right)\eta'(\gamma) = -1 \text{ ise.} \end{cases}$$

- *Eğer m/n çift sayı ve $A \neq 0$ ise;*

$$N(m,n) = \begin{cases} q^{m-n} + q^{m/2-n} & \text{eğer } \eta\left((-1)^{m/2} - n\right)\eta'(\gamma) = 1 \text{ ise;} \\ q^{m-n} - q^{m/2-n} & \text{eğer } \eta\left((-1)^{m/2} - n\right)\eta'(\gamma) = -1 \text{ ise.} \end{cases}$$

- *Eğer m/n tek sayı ve $A = 0$ ise;*

$$N(m,n) = q^{m-n}$$

- *Eğer m/n tek sayı, $A \neq 0$ ve n çift sayı ise;*

$$N(m,n) = \begin{cases} q^{m-n} + q^{m-n/2} & \text{eğer } (u_1,u_2) \in \{(1,1),(-1,-1)\} \text{ ise;} \\ q^{m-n} - q^{m-n/2} & \text{eğer } (u_1,u_2) \in \{(1,-1),(-1,1)\} \text{ ise.} \end{cases}$$

Burada u_1, u_2, aşağıdaki denklemlerle verilen, $\{-1,1\}$ kümesinin elemanlarıdır:

$$u_1 = \eta\left((-1)^{m/2}\right)\eta'(\gamma) \text{ ve } u_2 = \eta\left((-1)^{n/2}\right)\eta'(A)$$

- *Eğer m/n tek sayı, $A = 0$ ve n tek sayı ise;*

$$N(m,n) = \begin{cases} q^{m-n} + q^{m-n/2} & \text{eğer } (u_1,u_2) \in \{(1,1),(-1,-1)\} \text{ ise;} \\ q^{m-n} - q^{m-n/2} & \text{eğer } (u_1,u_2) \in \{(1,-1),(-1,1)\} \text{ ise.} \end{cases}$$

Burada u_1, u_2, aşağıdaki denklemlerle verilen, $\{-1,1\}$ kümesinin elemanlarıdır:

$$u_1 = \eta\left((-1)^{(m-1)/2}\right)\eta'(\gamma) \text{ ve } u_2 = \eta\left((-1)^{(n-1)/2}\right)\eta'(A)$$

Teorem 2.4.2. *Diyelim ki $s \geq t+1$ ve $u \leq t$ olsun. ω, $\mathbb{F}_{q^m} \setminus \{0\}$ çarpımsal grubunun bir üreteci ve a, $\gamma = \omega^a$ ve $0 \leq a < q^m - 1$ şartlarını sağlayan bir tam sayı olsun. O zaman:*

- *$s = t+1$, $q_1 = q^{2^t r}$ iken:*

Eğer $a \not\equiv m_1 \frac{q_1+1}{2} \pmod{(q_1+1)}$ *ise;*

$$N(m,n) = \begin{cases} q^{m-n} + q^{m/2-n} & \text{eğer } A \neq 0 \text{ ise;} \\ q^{m-n} - (q^n - 1)\, q^{m/2-n} & \text{eğer } A = 0 \text{ ise.} \end{cases}$$

Eğer $a \equiv m_1 \frac{q_1+1}{2} \pmod{q_1+1}$ *ise* $k = 2^{t+1}r$ *olmak üzere;*

$$N(m,n) = \begin{cases} q^{m-n} - q^{(m+k)/2-n} & \text{eğer } A \neq 0 \text{ ise;} \\ q^{m-n} + (q^n - 1)\, q^{(m+k)/2-n} & \text{eğer } A = 0 \text{ ise.} \end{cases}$$

- $s \geq t+2$, $q_1 = q^{2^t r}$ *iken:*
  Eğer $a \not\equiv 0 \pmod{(q_1+1)}$ *ise;*

$$N(m,n) = \begin{cases} q^{m-n} - q^{m/2-n} & \text{eğer } A \neq 0 \text{ ise;} \\ q^{m-n} + (q^n - 1)\, q^{m/2-n} & \text{eğer } A = 0 \text{ ise.} \end{cases}$$

  Eğer $a \equiv 0 \pmod{q_1+1}$ *ise* $k = 2^{t+1}r$ *olmak üzere;*

$$N(m,n) = \begin{cases} q^{m-n} + q^{(m+k)/2-n} & \text{eğer } A \neq 0 \text{ ise;} \\ q^{m-n} - (q^n - 1)\, q^{(m+k)/2-n} & \text{eğer } A = 0 \text{ ise.} \end{cases}$$

Son olarak bu çalışmanın ana teoremi $n > 1$ *için aşağıda verilmiştir:*

Teorem 2.4.3. *Diyelim ki* $t+1 \leq u \leq s$ *ve* $A = 0$. ω, $\mathbb{F}_{q^m} \setminus \{0\}$ *çarpımsal grubunun bir üreteci ve* a, $\gamma = \omega^a$ *ve* $0 \leq a < q^m - 1$ *şartlarını sağlayan bir tam sayı olsun. O zaman:*

- $s = t+1$, $B_1 = \text{obeb}\left(m_2, q^{2^t\rho} + 1\right)$ *iken:*
  Eğer $a \equiv n_1 m_2 \frac{q^{2^t r}+1}{2} \pmod{\left(\frac{q^{2^t r}+1}{q^{2^t\rho}+1} B_1\right)}$ *ise;*

$$N(m,n) = q^{m-n} - (q^n - 1)\, q^{m/2-n} + B_1 \frac{q^n - 1}{q^{2^t\rho} + 1} \left(q^{m/2+2^t r-n} + q^{m/2-n}\right).$$

  Eğer $a \not\equiv n_1 m_2 \frac{q^{2^t r}+1}{2} \pmod{\left(\frac{q^{2^t r}+1}{q^{2^t\rho}+1} B_1\right)}$ *ise;*

$$N(m,n) = q^{m-n} - (q^n - 1)\, q^{m/2-n}.$$

- $s \geq t+2$, $B_1 = \text{obeb}\left(2^{s-u} m_2, q^{2^t\rho} + 1\right)$ *iken:*
  Eğer $a \equiv 0 \pmod{\left(\frac{q^{2^t r}+1}{q^{2^t\rho}+1} B_1\right)}$ *ise;*

$$N(m,n) = q^{m-n} + (q^n - 1)\, q^{m/2-n} - B_1 \frac{q^n - 1}{q^{2^t\rho} + 1} \left(q^{m/2+2^t r-n} + q^{m/2-n}\right).$$

Eğer $a \not\equiv 0 \mod \left(\frac{q^{2^t r}+1}{q^{2^t \rho}+1} B_1\right)$ *ise;*

$$N(m,n) = q^{m-n} + (q^n - 1)\, q^{m/2-n}.$$

2.5 Genişletilemez $\mathbb{F}_q$-kuadratik Mükemmel Lineer Olmayan Fonksiyonlar

2.5.1 Giriş

Genişletilemez $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyonları (ki tanımını aşağıda veriyoruz) karakterize etmek zor bir problemdir. Ayrıca bu fonksiyonların yarıcisimlerle (semifield) doğal bağlantıları vardır. Dolayısıyla uygulama alanı da geniştir. (Özbudak and Pott, 2015) çalışmamızda birçok $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyon sınıfının genişletilemez olduğunu gösterdik. Ayrıca yarıcisimlerle olan bazı doğal ilişkileri örnekleriyle belirttik. Konuya ilişkin birçok açık problemi açıkladık.

Diyelim ki q tek bir asalın kuvveti olsun. $\mathbb{F}_q$ da q elemanlı sonlu cisim olsun. Yine n bir pozitif sayı olsun. $\mathbb{F}_{q^n}$ üzerindeki bir $\mathbb{F}_q$*-kuadratik form* f şu şekilde ifade edilir:

$$f(x) = \mathrm{Tr}(a_0 x^2 + a_1 x^{q+1} + ... + a_{\frac{n}{2}} x^{\frac{n}{2}+1})$$

Burada Tr ifadesi $\mathbb{F}_{q^n}$'den $\mathbb{F}_q$'ya olan iz fonksiyonunu, yani

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}} = x + x^{q^m} + x^{2q^m} + ... + x^{q^{(n/m-1)m}}$$

belirtir. Bu f'e ayrıca $\mathbb{F}_{q^n}$'den $\mathbb{F}_q$'ya $\mathbb{F}_q$*-kuadratik fonksiyonu* da diyoruz.

Dembowski-Ostrom polinomu ile $\mathbb{F}_{q^n}$'den $\mathbb{F}_{q^n}$'e giden $\mathbb{F}_q$-kuadratik fonksiyonları anlarız ki şöyle ifade edilir:

$$F(x) = \sum_{i,j=0}^{n-1} a_{i,j} x^{q^i+q^j}$$

öyle ki $a_{i,j} \in \mathbb{F}_{q^n}$.

Eğer $\{e_1, e_2, ..., e_n\}$ bir $\mathbb{F}_q$-lineer baz ve $\{e_1^*, e_2^*, ..., e_n^*\}$ buna karşılık gelen iz-dik (trace-orthogonal) bir baz ise

$$F(x) = \sum_{i=1}^{n} f_i(x) e_i$$

ve

$$f_i(x) = \mathrm{Tr}(e_i^* \sum_{i_1,i_2=0}^{n-1} a_{i_1,i_2} x^{q^{i_1}+q^{i_2}})$$

olarak bulunur. Burada $1 \leq i \leq n$ için f_i, $\mathbb{F}_{q^n}$'den $\mathbb{F}_q$'ya giden bir $\mathbb{F}_q$-kuadratik fonksiyon (ya da aynı anlamda $\mathbb{F}_{q^n}$ üzerinde bir $\mathbb{F}_q$-kuadratik form)dur.

Dolayısıyla, bazı açık yazmadan, $\mathbb{F}_{q^n}$'den $\mathbb{F}_{q^n}$'e giden bir Dembowski-Ostrom polinomunu, hiçbir genellikten feragat etmeden

$$F(x) = \begin{bmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{bmatrix}$$

matris formu ile ifade edebiliriz. Burada $f_1, ..., f_n$'ler $\mathbb{F}_{q^n}$ üzerinde birer $\mathbb{F}_q$-kuadratik formdur.

Buraya kadar (n, n) ve $(n, 1)$ $\mathbb{F}_q$-kuadratik fonksiyonlarını açıkladık. Benzer şekilde $1 \leq r \leq n$ için $\mathbb{F}_{q^n}$'den $\mathbb{F}_{q^r}$'e giden herhangi bir $\mathbb{F}_q$-kuadratik fonksiyonu

$$F(x) = \begin{bmatrix} f_1(x) \\ \vdots \\ f_r(x) \end{bmatrix}$$

ile ifade edilir, öyle ki $f_1, ..., f_r$ fonksiyonları $\mathbb{F}_{q^n}$ üzerinde $\mathbb{F}_q$-kuadratik formlardır.

Tanım 2.5.1. $1 \leq r \leq n$ pozitif tam sayılar olsun. Diyelim ki $\begin{bmatrix} f_1 \\ \vdots \\ f_r \end{bmatrix}$ ve $\begin{bmatrix} g_1 \\ \vdots \\ g_r \end{bmatrix}$ $\mathbb{F}_{q^n}$'den $\mathbb{F}_q^r$'ye giden $\mathbb{F}_q$-kuadratik fonksiyonlar olsun. Aşağıdaki şart olursa biz bu iki (n, r) fonksiyona denk diyoruz:

Toplamsal permütasyon polinomu ($\mathbb{F}_q$-linearized permutation polynomial) olan $L(x) \in \mathbb{F}_{q^n}[x]$ ve içeriği $\mathbb{F}_q$'dan olan $r \times r$ tersi olan (nonsingular) $[a_{ij}]_{r \times r}$ matrisi vardır öyle ki

$$[a_{ij}] \begin{bmatrix} f_1(L(x)) \\ \vdots \\ f_r(L(x)) \end{bmatrix} = \begin{bmatrix} g_1(x) \\ \vdots \\ g_r(x) \end{bmatrix}$$

her $x \in \mathbb{F}_{q^n}$ için doğrudur.

Bu denklik tanımı ile Genişletilmiş Afin Denkliği (Extended Affine Equivalence) ve Carlet-Charpin-Zinoviev Denkliği (Carlet et al., 1998) bu durumda aynı olmaktadır (bakınız (Özbudak and Pott, 2014)).

Tanım 2.5.2. $1 \leq r \leq n$ tamsayı olsunlar. F de $\mathbb{F}_{q^n}$'den $\mathbb{F}_q^r$'a bir $\mathbb{F}_q$-kuadratik fonksiyon

olsun. Her $a \in \mathbb{F}_{q^n}^*$ için $\mathbb{F}_{q^n}$'den $\mathbb{F}_q^r$'a aşağıdaki şekilde bir $D_{F,a}$ fonksiyonu tanımlayalım:

$$D_{F,a}(x) = F(x+a) - F(x) - F(a).$$

Eğer her $a \in \mathbb{F}_{q^n}^*$ için $D_{F,a}$ eşit ağırlıklı ise, yani her $b \in \mathbb{F}_q^r$ için

$$\{x \in \mathbb{F}_{q^n} : D_{F,a}(x) = b\}$$

kümesinin q^{n-r} tane elemanı var ise, biz F'e (n,r)-*bükük (bent)* fonksiyon diyoruz.

Eğer $n = r$ ise bu tür (n,n)-bükük fonksiyonlara direk geometrik anlamlarından dolayı *düzlemsel (planar)* fonksiyonlar da denir. Literatürde kısaca bükük denen fonksiyonlar aslında $(n,1)$-bükük fonksiyonlardır.

Dikkat edilirse biz yalnızca $\mathbb{F}_q$-kuadratik (n,r)-bükük fonksiyonları düşündüğümüz için bizim denklik tanımı tam olarak yeterlidir. Tüm olası (n,r)-bükük fonksiyonları düşünmek daha genel bir sorudur. Özellikle $r > \frac{n}{2}$ için yalnızca $\mathbb{F}_q$-kuadratik (n,n)-bükük fonksiyonları çalışmak bile çok zordur. Örneğin (n,n)-bükük fonksiyonlardan $\mathbb{F}_q$-kuadratik olanları yukarıdaki denklik tanımına göre tüm sınıflara ayırmak yalnızca $n \leq 3$ için çözülebilmiştir. Bu bağlamda (n,r)-bükük $\mathbb{F}_q$-kuadratik fonksiyonları düşünmek önemlidir.

Tanım 2.5.3. $1 \leq r \leq n-1$ tam sayı olsun. Yine F de (n,r)-bükük $\mathbb{F}_q$-kuadratik bir fonksiyon olsun. Bu durumda eğer $\mathbb{F}_{q^n}$ üzerinde $\mathbb{F}_q$-kuadratik form olan f varsa ve $\begin{bmatrix} F(x) \\ f(x) \end{bmatrix}$ bir $(n,r+1)$-bükük veriyorsa, biz F fonksiyonuna *genişletilebilir (extendable)* diyoruz. Aksi halde F fonksiyonuna *genişletilemez (non-extendable)* diyoruz.

2.5.2 Yöntem ve Sonuçlar

Bu proje kapsamında yapılan (Özbudak and Pott, 2015) makalesindeki sonuçlarımızdan bazıları bu problem ile ilgilidir:

Önerme 2.5.4. *$n \geq 2$ bir tamsayı ve $F : \mathbb{F}_{q^n} \to \mathbb{F}_q$ bir $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan ($\mathbb{F}_q$-quadratic perfect nonlinear) fonksiyon olsun. O zaman F genişletilebilirdir.*

Ek Sonuç 2.5.5. *F fonksiyonu $\mathbb{F}_{q^3}$'ten $\mathbb{F}_{q^2}$'ye bir $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyon olsun. O zaman F genişletilebilirdir.*

Örnek 2.5.6. *$q = 3$ ve $n = 4$ olsun. $\mathbb{F}_{3^4}$'ten $\mathbb{F}_{3^4}$'e denkliğe göre birbirinden farklı tam olarak 2 tane $\mathbb{F}_q$-kuadratik düzlemsel fonksiyon vardır. Bunlar*

$$x \mapsto x^4 + x^{10} - x^{36} \text{ ve } x \mapsto x^2.$$

Bilgisayar ile, tüm $\mathbb{F}_3$-kuadratik (q^4, q^2)-bükük fonksiyonların genişletilebilir olduğunu doğruladık.

Örnek 2.5.7. *$q = 3$ and $n = 5$ olsun. $\mathbb{F}_{3^5}$'ten $\mathbb{F}_{3^5}$'e denkliğe göre birbirinden farklı tam olarak 7 tane $\mathbb{F}_q$-kuadratik düzlemsel fonksiyon ($\mathbb{F}_q$-quadratic planar map) vardır. Bunlar*

- $x \mapsto x^2$,
- $x \mapsto x^{q+1}$,
- $x \mapsto x^{q^2+1}$,
- $x \mapsto x^{10} + x^6 - x^2$,
- $x \mapsto x^{10} - x^6 - x^2$,
- $x \mapsto x^{90} + x^2$,
- $x \mapsto -(x^3 - x) + D(x^3 - x) + \frac{1}{2}x^2$ *ile* $D(x) = -x^{36} + x^{28} + x^{12} + x^4$.

Bilgisayar ile, tüm $\mathbb{F}_3$-kuadratik (q^5, q^2)-bükük fonksiyonların genişletilebilir olduğunu doğruladık.

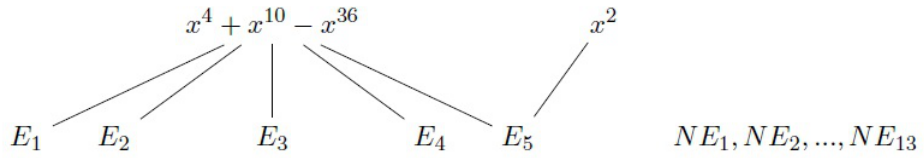
Örnek 2.5.8. *$q = 3$ ve $n = 4$ olsun. Hatırlayalım ki, denkliğe göre $\mathbb{F}_{q^4}$'ten $\mathbb{F}_{q^4}$'ye tam olarak iki tane $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyon vardı ve bunlar x^2 ile $x^4 + x^{10} - x^{36}$ polinomları idi. Ayrıca $\mathbb{F}_{q^4}$'ten $\mathbb{F}_{q^2}$'ye tüm $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyonlar genişletilebilirdi. Aslında denkliğe göre tam olarak 7 tane $\mathbb{F}_{q^4}$'ten $\mathbb{F}_{q^2}$'ye $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyon vardır.*

Öte yandan, $\mathbb{F}_{q^4}$'ten $\mathbb{F}_{q^3}$'e genişletilemez $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyonlar da vardır. $\mathbb{F}_{q^4}$'ten $\mathbb{F}_{q^3}$'e $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyonlar denkliğe göre tam olarak 18 tanedir. Sadece 5 tanesi genişletilebilirdir. Bunları E_1, E_2, E_3, E_4 ve E_5 ile belirterek aşağıdaki gibi tanımlayalım. Sadece E_5 hem x^2'ye hem de $x^4+x^{10}-x^{36}$'ye genişletilebilir. Diğerleri ise sadece $x^4+x^{10}-x^{36}$'ye genişletilebilir. Kalan 13 tane $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyonlar ise genişletilemez. Bunları $NE_1, NE_2, ..., NE_{13}$ ile belirterek aşağıda verdik.

Şimdi bu fonksiyonları açık olarak verelim. w, $\mathbb{F}_{q^4}$'ün $w^4+2w^3+2 = 0$ şartını sağlayan bir ilkel elemanı (primitive element) olsun. $E_1, E_2, E_3, E_4, E_5 : \mathbb{F}_{q^4} \to \mathbb{F}_q^3$ fonksiyonları aşağıdaki gibi verilsin.

$$E_1(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^2x^{10} + w^5x^4) \end{bmatrix}, \; E_2(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^2x^2) \end{bmatrix}, \; E_3(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^8x^2) \end{bmatrix},$$

$$E_4(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(w^{13}x^{10}) \\ \mathrm{Tr}(w^5x^4) \end{bmatrix},\ E_5(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^4) \\ \mathrm{Tr}(w^2x^4) \end{bmatrix}.$$



Şekil 2.1: Matris yapısı

Bunlar genişletilebilir fonksiyonlardır.

$NE_1, NE_2, ..., NE_{13} : \mathbb{F}_{q^4} \to \mathbb{F}_{q^3}$ *fonksiyonları da aşağıdaki gibi verilsin.*

$$NE_1(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(wx^4) \end{bmatrix},\ NE_2(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^5x^4) \end{bmatrix},\ NE_3(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^7x^4) \end{bmatrix},$$

$$NE_4(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^3x^{10} + w^8x^4 + wx^2) \end{bmatrix},\ NE_5(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^3x^{10} + w^{25}x^4 + wx^2) \end{bmatrix},$$

$$NE_6(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^3x^{10} + wx^4 + w^2x^2) \end{bmatrix},\ NE_7(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^{30}x^4 + w^6x^2) \end{bmatrix},$$

$$NE_8(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^{15}x^2) \end{bmatrix},\ NE_9(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^{10}) \\ \mathrm{Tr}(w^4x^4 + w^{15}x^2) \end{bmatrix},$$

$$NE_{10}(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(w^{13}x^{10}) \\ \mathrm{Tr}(wx^4) \end{bmatrix},\ NE_{11}(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^4) \\ \mathrm{Tr}(w^2x^{10} + wx^2) \end{bmatrix},$$

$$NE_{12}(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^4) \\ \mathrm{Tr}(w^{14}x^{10} + w^8x^4 + wx^2) \end{bmatrix},\ NE_{13}(x) = \begin{bmatrix} \mathrm{Tr}(x^2) \\ \mathrm{Tr}(wx^4) \\ \mathrm{Tr}(w^4x^{10} + w^8x^4 + w^2x^2) \end{bmatrix}.$$

Bunlar da genişletilemez fonksiyonlardır.

Projemizin 3. Gelişme Raporunda belirttiğimiz bu projenin çıktılarından olan (Özbudak and Pott, 2015) makalemizin bir diğer sonucunu da şimdi özetliyoruz.

$F(x) = \begin{bmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{bmatrix}$ fonksiyonu $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ arasında bir $\mathbb{F}_q$-kuadratik fonksiyondur. Ayrıca F'in (n,n)-bükük olması, her $1 \leq j \leq n$ için $f_j : \mathbb{F}_{q^n} \to \mathbb{F}_q$ fonksiyonunun dejenere olmayan $\mathbb{F}_q$-kuadratik form verdiğini belirtir. Kuadratik form teorisinden bildiğimiz gibi, karakteristik tek olduğu için, dejenere olmayan $\mathbb{F}_q$-kuadratik formlarla ters çevrilebilir (non-singular, invertible) $n \times n$ simetrik matrislerin ($\mathbb{F}_q$ üzerinde) baz seçmeyle verilen doğal bir ilişkisi vardır.

F fonksiyonu ile değişmeli ön yarıcisimlerin (presemifield) de doğal bir ilişkisi vardır (bakınız (Coulter, 2008)). Ancak değişmeli ön yarıcisimler ile simetrik matrisler arasında doğal bir ilişki direk olarak yoktur. Aslında ön yarıcisimlerle matrisler arasında doğal bir ilişki vardır ancak bu ilişki simetrik matrisler özeline inersek ancak simplektik ön yarıcisimlerle vardır (bakınız (Ball and Brown, 2004)). Acaba bizim kuadratik (n,n)-bükük fonksiyonların koordinat fonksiyonları f_i'leri incelerken doğal olarak karşılaştığımız ters çevrilebilir simetrik matrislerin bu çerçevede yeri nedir diye kendimize sorabiliriz.

Bunun cevabını biz (Özbudak and Pott, 2015) makalesinde Knuth'un kübik dizisini (Knuth's cubical array) (Knuth, 1965) kullanarak veriyoruz. Herhangi bir ön yarıcisim eğer $\mathbb{F}_q$ üzerinde verilirse ve $\{e_1, ..., e_n\}$ kümesi $\mathbb{F}_q$ üzerinde bir baz ise her $1 \leq i, j \leq n$ için

$$e_i \circ e_j = \sum_{n}^{k=1} a_{ijk} e_k$$

şeklinde $a_{ijk} \in \mathbb{F}_q$ katsayılarını bulalım. Burada $\circ$ ön yarıcisim çarpma işlemidir. Dikkat edersek

$$(a_{ijk})_{1 \leq i,j,k \leq n}$$

bir küp oluşturur ve q^3 elemanı vardır.

Bizim özel durumumuzda $\mathbb{F}_{q^n}$ toplamsal olarak yarıcisim ile aynıdır ve yeni çarpma işlemi

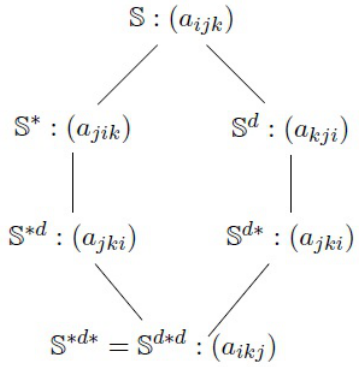
$$x \circ y = F(x+y) - F(x) - F(y)$$

olarak verilir. Dikkat edilirse $\circ$ işleminin bizim özel durumumuzda değişme özelliği vardır. Yine $\{e_1, ..., e_n\}$ bazı seçilerek elde edilen (a_{ijk}) Knuth'un kübik dizisinde bizim yukarda bahsettiğimiz simetrik $n \times n$ matrisleri de her $1 \leq k \leq n$ için k'yi de k_0 olarak sabitleyince elde edilen $(a_{ijk_0})_{1 \leq i,j \leq n}$ matrisleridir.

Bu matrislerin gerçekten de simplektik ön yarıcisimlerle şöyle bir ilişkisi vardır. Knuth'un kübik dizisini kullanarak aslında direk ön yarıcisim kurulabilir. Dolayısıyla

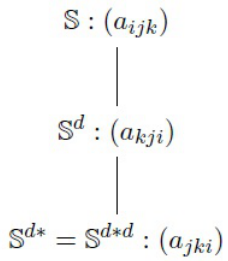
(a_{ijk}) kübik dizisi üzerinde indisleri permütasyonla yer değiştirerek 6 taneye kadar hatta izotopik ön yarıcisim bulabiliriz. Bu çok ilginçtir çünkü izotopik olmayan yarıcisim bulmak genelde çok zordur ve en büyük açık problemlerden biridir. Burada hemen cebirdeki izomorfik kavramının burada uygun olmadığını (daha doğrusu bir bakıma çok daha kolay olduğunu) belirtelim ve detaylar için (Özbudak and Pott, 2015) makalemizdeki referanslara okuyucuyu yönlendirelim.

Knuth'un kübik dizisi ile elde edilen 2 temel operasyon şudur: (12) permütasyonu ile $\mathbb{S}$ yarıcisminden ters $\mathbb{S}^*$ yarıcismini ve (13) permütasyonu ile dual $\mathbb{S}^d$ yarıcismini elde ederiz. Bu bağlamda Şekil 2.2'deki 6 adet yarıcisim çıkar ki bunların bazen birbirlerine izotopik olma durumu vardır. Ancak bizim durumumuzda başladığımız $\mathbb{S}$ zaten değişmeli yarıcisim



Şekil 2.2: İzotopik olma durumları

olduğundan Şekil 2.2 yalnızca Şekil 2.3'e dönüşür.



Şekil 2.3: Değişmeli yarıcisim

Ayrıca $\mathbb{S}$ değişmeli olmadığından $\mathbb{S}^{d*}$ simplektik bir yarıcısimdir. Bu da doğal olarak $\mathbb{S}^{d*}$'a karşılık gelen Knuth'un kübik dizisi $(b_{ijk})_{1\leq i,j,k\leq n}$ ise her $1 \leq j \leq n$ için $j = j_0$ sabitlenince elde edilen $n \times n$ bir $(b_{ij_0k})_{1\leq i,k\leq n}$ matrislerinin simetrik olduğu anlamına gelir. Knuth'un kübik permütasyonları üzerindeki permütasyonları düşünerek (Özbudak and Pott, 2015) makalesinde biz (a_{ijk_0}) simetrik matrislerinin tam olarak (a_{ij_0k}) matrisleriyle denk düştüğünü gösterdik. Daha açık olarak, F olarak (n,n)-bükük $\mathbb{F}_q$-kuadratik fonksiyonun koordinat fonksiyonu olan $f_j : \mathbb{F}_{q^n} \to \mathbb{F}_q$ olan $\mathbb{F}_q$-kuadratik bükük fonksiyonların verdiği simetrik matrisler, F'ten elde edilen $\mathbb{S}$ değişmeli yarıcisminin

değil $\mathbb{S}$'ten elde edilen $\mathbb{S}^{d*}$ simplektik yarıcisminin Knuth kübik dizisinin orta indislerini sabitleyerek elde ettiğimiz simetrik matrislerdir.

Burada yarıcisim ve ön yarıcisim arasında bir fark gözetmedik. Çünkü bunlar izotopik olarak birbirlerine denktir (bakınız (Özbudak and Pott, 2015) bölüm 5).

2.6 $\mathbb{F}_{q^m}$ Üzerinde $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ Eğrisinin L-polinomları

2.6.1 Giriş

Bu bölümde, karakteristiği tek olan sonlu cisimler üzerinde tanımlanan özel bir sınıftaki cebirsel eğrilerin L-polinomlarını dikkate alıyoruz. Sonlu cisimler üzerindeki cebirsel eğrilerin kodlama teorisinde, kriptografide, yarı rastgele sayılar teorisinde ve bağlantılı alanlarda (Niederreiter and Xing, 2001, 2009; Stichtenoth, 2000; Tsfasman and Vladut, 1991) çeşitli uygulamaları vardır. Bu uygulamalar için bir eğrinin rasyonel noktalarının sayısını bilmek önemlidir. Bu bölüm boyunca eğri derken karakteri tek olan bir sonlu cisim üzerinde tanımlı düzgün (smooth), geometrik olarak indirgenemez izdüşümsel eğriyi kastediyor olacağız.

Bir eğrinin rasyonel noktalarının sayısı ile ilgili sonraki adım doğal olarak L-polinomlarıdır (bakınız Kısım 2.6.2). Bu polinom, sonlu cismin tüm genişlemeleri üzerindeki rasyonel nokta sayılarının bilgisini içerir. Eğrilerin L-polinomlarını hesaplamak algoritmik sayılar teorisi ve kriptografi ile bağlantılı zor bir problemdir (Kasami, 1974; Laudera and Wan, 2002).

Bir eğrinin L-polinomu ayrıca o eğrinin Jacobian değişmezi hakkında da bilgi taşır. Bir eğrinin Jacobian değişmezi, g eğrinin cinsini (genus) göstermek üzere g boyutlu bir abelyan değişkendir. Başka bir ifadeyle, L-polinomu Jacobian değişmezi üzerinde tanımlı Frobenius aksiyonunun karakteristik polinomu olarak düşünülebilir (Tate, 1966).

2.6.2 Genel Bilgiler

$\mathbb{F}_q$ ifadesi q elemanlı bir sonlu cismi göstersin. $\mathbb{F}_q$ üzerinde tanımlı tek değişkenli rasyonel fonksiyonların bir sonlu genişlemesi fonksiyon cismi olarak isimlendirilir ve $\mathcal{K}$ ile gösterilir, yani fonksiyon cismi rasyonel fonksiyonlar cismi $\mathbb{F}_q(x)$'nın bir sonlu genişlemesidir. Bundan dolayı, indirgenemez bir $r(T) = r_0(x) + r_1(x)T + \cdots + r_{n-1}(x)T^{n-1} + T^n \in \mathbb{F}_q(x)[T]$ polinomunun kökü y olmak üzere $\mathcal{K} = \mathbb{F}_q(x, y)$'dir. Ortak payda ile çarparak bir $h(x, y) = y^n + y^{n-1}h_{n-1}(x) + \cdots + h_1(x)y + h_0(x) \in \mathbb{F}_q[x, y]$ indirgenemez polinomunu elde ederiz. Aslında bu tümüyle indirgenemezdir (absolutely

irreducible), yani $\overline{\mathbb{F}_q}[x,y]$ üzerinde indirgenemezdir (bundan dolayı da geometrik olarak indirgenemezdir). $\mathbb{F}_q$ üzerinde bir fonksiyon cismi $\mathcal{K}$'nın bir değer halkası (valuation ring) $\mathcal{O}$, $\mathbb{F}_q \subset \mathcal{O} \subset \mathcal{K}$ ve herhangi bir $z \in \mathcal{K}$ için $z \in \mathcal{O}$ veya $z^{-1} \in \mathcal{O}$ olacak şekilde tanımlanır. $\mathbb{F}_q$ üzerinde bir fonksiyon cismi $\mathcal{K}$'nın bir yeri $\mathcal{P}$, $\mathcal{K}$'nın bir değer halkası olan $\mathcal{O}$'nun maksimal ideali şeklinde tanımlanır. $\mathbb{P}_\mathcal{K}$ ile $\mathcal{K}$'nın tüm yerlerinin kümesini gösterelim. Dikkat edelim ki, eğer $\mathcal{O}$ bir değer halkası ve $\mathcal{P}$ de onun maksimal ideali ise o zaman $\mathcal{O}$ değer halkası $\mathcal{P}$ yeri ile tek şekilde belirlenebilir, yani $\mathcal{O} = \mathcal{O}_\mathcal{P} = \{z \in \mathcal{K} \mid z^{-1} \notin \mathcal{P}\}$'dir. Burada $\mathcal{P}$, $\mathcal{O}_\mathcal{P}$'nin maksimal ideali olduğundan $\mathcal{O}_\mathcal{P}/\mathcal{P}$ bölüm cismi de $\mathcal{P}$'nin kalanlar sınıfı cismi (residue class field) olarak isimlendirilir. $\mathcal{O}_\mathcal{P}/\mathcal{P}$'nin $\mathbb{F}_q$ üzerindeki genişleme derecesi, $\mathcal{P}$ yerinin derecesi olarak adlandırılır. Yani $\deg \mathcal{P} = [\mathcal{O}_\mathcal{P}/\mathcal{P} : \mathbb{F}_q]$'dur.

$D = \sum_{\mathcal{P}\in\mathbb{P}_\mathcal{K}} n_\mathcal{P}\mathcal{P}$ formal toplamı bölen (divisor) olarak adlandırılır. Burada not etmek gerekir ki bu formal toplamda $n_\mathcal{P}$ tamsayılarının sadece sonlu tanesi sıfırdan farklı olabilir. Böylelikle bir D böleninin derecesi $\deg D = \sum_{\mathcal{P}\in\mathbb{P}_\mathcal{K}} n_\mathcal{P} \deg \mathcal{P}$ şeklinde tanımlanır. $D(\mathcal{K})$ ifadesi $\mathcal{K}$'nın tüm bölenlerinin kümesini göstersin. Biliyoruz ki bu küme sonsuz elemanlı bir abelyan gruptur. $D^0(\mathcal{K})$ kümesi $D(\mathcal{K})$'nın $\deg D = 0$ şartını sağlayan D bölenlerini içeren alt kümesi olsun. $D^0(\mathcal{K})$, $D(\mathcal{K})$'nın bir alt grubudur. $\mathcal{P}(\mathcal{K}) \subset D^0(\mathcal{K})$ kümesi $\mathcal{K}$'nın temel bölenlerini (principal divisors) içeren küme olsun. O zaman

$$Jac(\mathcal{K}) = D^0(\mathcal{K})/\mathcal{P}(\mathcal{K})$$

bölüm grubu $\mathcal{K}$'nın Jacobian'ı olarak adlandırılır.

Herhangi iki $D = \sum_{\mathcal{P}\in\mathbb{P}_\mathcal{K}} n_\mathcal{P}\mathcal{P}, D' = \sum_{\mathcal{P}\in\mathbb{P}_\mathcal{K}} n'_\mathcal{P}\mathcal{P} \in D(\mathcal{K})$ böleni için eğer her $\mathcal{P} \in \mathbb{P}_\mathcal{K}$ için $n_\mathcal{P} \geq n'_\mathcal{P}$ oluyorsa $D \geq D'$ deriz. Eğer her $\mathcal{P} \in \mathbb{P}_\mathcal{K}$ için $n_\mathcal{P} = 0$ oluyorsa D'ye sıfır bölen (zero divisor) deriz ve $D = 0$ şeklinde gösteririz. $n \geq 0$ tamsayıları için

$$A_n = |\{A \in D(\mathcal{K}) : A \geq 0 \text{ and } \deg A = n\}|$$

şeklinde tanımladığımız A_n sonlu bir sayıdır. Buna göre zeta fonksiyonu

$$Z_\mathcal{K}(t) = \sum_{n=0}^{\infty} A_n t^n \in \mathcal{C}[[t]]$$

kuvvet serisi olarak tanımlanır.

Cebirsel eğriler teorisi fonksiyon cisimler teorisi ile denk bir yapıya sahiptir. Cebirsel eğriler ve fonksiyon cisimleri arasındaki ilişkiyi inceleyen kısa bir çalışma olarak (Stichtenoth, 2000, Appendix B) referansını verebiliriz. Şimdi yukardaki zeta fonksiyonunu kullanarak χ eğrisinin L-polinomunu (ya da tekabül eden fonksiyon cisminin L-polinomunu) tanımlayabiliriz. Aşağıdaki teorem sonlu cisimler üzerindeki cebirsel eğriler

için en önemli sonuçlardan biridir (Stichtenoth, 2000).

Teorem 2.6.1. *$\mathbb{F}_q$ üzerinde tanımlı χ eğrisinin tam sabit cismi (full constant field) $\mathbb{F}_q$ olsun, $F = \mathbb{F}_q(x, y)$ de ona tekabül eden fonksiyon cismi olsun. O zaman*

1. *Bir $L_F(t) = 1 + a_1 t + a_2 t^2 + \cdots + a_{2g-1} t^{2g-1} + q^g t^{2g} \in \mathbb{Z}[t]$ polinomu mevcuttur öyle ki*

$$Z_F(t) = \frac{L_F(t)}{(1-t)(1-qt)}.$$

   Burada $L_F(t)$ polinomu χ'nin (ya da F'in) L-polinomu olarak adlandırılır. Ayrıca belirtelim ki g burada χ'nin (ya da F'in) cinsidir.

2. *$a_{2g-i} = q^{g-i} a_i$, $1 \leq i \leq g$.*

3. *$L_F(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$, $\alpha_i \in \mathcal{C}$.*

4. *Hasse-Weil Teoremi aşağıdakine denktir:*

$$\log |\alpha_i| = \frac{1}{2} \text{ for } i = 1, 2, \ldots, 2g.$$

Not edelim ki bu teorem (hala bir açık problem olan) klasik Riemann Hipotezi'nin pozitif karakteristikteki karşılığıdır.

$\mathbb{F}_q$ üzerindeki χ eğrisi için $F = \mathbb{F}_q(x, y)$ bu eğriye karşılık gelen fonksiyon cismi ve $N(\chi)$ de bu eğrinin rasyonel noktalarının sayısı olsun, yani F'nin bir dereceli yerlerinin sayısı olsun. O zaman Hasse-Weil Teoremi bize $N(\chi)$ için

$$q + 1 - 2g\sqrt{q} \leq N(\chi) \leq q + 1 + 2g\sqrt{q}$$

şeklindeki sınırları verir (burada g ile F'nin cinsi gösteriliyor). Serre bunu biraz daha geliştirmiştir:

$$q + 1 - g\lfloor 2q^{1/2} \rfloor \leq N(\chi) \leq q + 1 + g\lfloor 2q^{1/2} \rfloor.$$

Hasse-Weil sınırlarına ulaşan eğriler olduğunu biliyoruz. Eğer eğri üst sınıra ulaşırsa eğriye maksimal eğri denir, eğer alt sınıra ulaşırsa da minimal eğri ismini alır. Ama genelde $N(\chi)$ sayısını belirlemek zordur. $N(F.\mathbb{F}_{q^i})$ ifadesi bir i tamsayısı için F'nin $\mathbb{F}_{q^i}$ üzerindeki bir dereceli yerlerinin sayısını göstersin. F'nin L-polinomunu belirlemek için $N(F.\mathbb{F}_{q^i})$ sayısını tüm $\mathbb{F}_{q^i}/\mathbb{F}_q$ genişlemeleri için belirlemek gerekir ($i = 1, 2, \ldots, g$). Bu şekilde L-polinomu $L_F(t) = 1 + a_1 t + \cdots + a_{2g-1} t^{2g-1} + q^g t^{2g} \in \mathbb{Z}[t]$ bize tüm $N(F.\mathbb{F}_{q^i})$ sayılarını verir her $i \in \mathbb{Z}^+$ için. Bunun da ötesinde $L_F(t)$ bize bazı "geometrik" bilgileri de verir. Örneğin:

- $L_F(1)$: F'nin sınıf sayıları (Stichtenoth, 2000, Teorem 5.1.15),
- Jacobian varyetesinin p-rankı (ya da Hasse-Witt değişmezi) (Stichtenoth, 1979),
- Eğrinin (ya da Jacobian'ının) Newton çokgeni (Manin, 1963).

Eğer izdüşümsel doğruyu, yani $\chi = \mathbb{P}^1$'i, ya da $F = \mathbb{F}_q(x)$'i düşünürsek o zaman cins sıfır olur ve bu bize $L_F(t) = 1$ ve $Z_F(t) = \frac{1}{(1-t)(1-q^t)}$ olduğunu söyler. Eğer $\mathbb{F}_q$ üzerinde cinsi $g \geq 1$ olan maksimal χ eğrisini düşünürsek o zaman q bir tam kare olmalıdır ve $L_\chi(t) = (1-\sqrt{q}t)^{2g}$ olur. Eğer $\mathbb{F}_q$ üzerinde cinsi $g \geq 1$ olan minimal χ eğrisini düşünürsek o zaman yine q bir tam kare olmalıdır ve $L_\chi(t) = (1+\sqrt{q}t)^{2g}$ olur. Belirtmeliyiz ki genel olarak $\mathbb{F}_q$ üzerinde cinsi g olan maksimal (veya minimal) eğrilerin olup olmadığı hala bir açık problemdir. $\mathbb{F}_q$ üzerinde cinsi $g \geq 1$ olan maksimal eğriler için biliyoruz ki $g \leq \dfrac{(\sqrt{q}+1)\sqrt{q}}{2}$. Ayrıca birasyonel izomorfizm altında $\mathbb{F}_{q^2}$ üzerindeki Hermitian eğrisi $H:\ y^q + y = x^{q+1}$, cinsi $\frac{(q+1)q}{2}$ olan tek maksimal eğridir (bakınız (Rück and Stichtenoth, 1994)).

$\mathbb{F}_q$ üzerinde bir E elliptik eğrisini dikkate alalım. Hasse-Weil Teoremi ile, bir $-2\sqrt{q} \leq -b \leq 2\sqrt{q}$ için E'nin rasyonel yerlerinin sayısı $N(E) = q + 1 - b$ olur. Genel olarak Hasse-Weil aralığının hangi değerlerinin ulaşılabilir olduğunu bilmiyoruz. Burada $g = 1$ için, tam olarak sadece Waterhouse'un (Waterhouse, 1969) aşağıdaki sonucunu biliyoruz (Rück, 1987) ve (Voloch, 1989).

2.6.3 Gereç, Yöntem ve Sonnuçlar

p bir tek asal olsun. Pozitif tamsayılar e ve m için $q = p^e$ olmak üzere $\mathbb{F}_q$ ve $\mathbb{F}_{q^m}$ ifadeleri sırasıyla q ve q^m elemanlı sonlu cisimleri göstersin. n sayısı m'yi bölen bir tamsayı ve $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}$ ifadesi ilgili iz fonksiyonu olsun. h negatif olmayan bir tamsayı ve $\alpha, \gamma \in \mathbb{F}_{q^m}$ öyle ki $\gamma \neq 0$ olsun.

$$N(m,n) = \left| \left\{ x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}} \left(\gamma x^{q^h+1} - \alpha \right) = 0 \right\} \right|.$$

χ eğrisi Artin-Schreier tipi

$$\chi: \quad y^{q^n} - y = \gamma x^{q^h+1} - \alpha \tag{2.1}$$

eğrisi olsun. Burada χ eğrisinin cinsi $g(\chi) = \dfrac{(q^n-1)q^h}{2}$ ve eğrinin $\mathbb{F}_{q^m}$-rasyonel noktalarının sayısı $N(\chi)$ için Hilbert'in Teorem 90'ını kullanarak

$$N(\chi) = 1 + q^n N(m,n)$$

buluruz. Bundan dolayı $N(\chi)$ sayısını belirlemek $N(m,n)$ sayısını belirlemek ile aynıdır. Bu sayı (Özbudak and Saygı, 2014)'de tam olarak çok yerde belirlenmiştir ve bütünlüğü bozmamak adına bu sonuçları Ek kısmında verdik. Bu sonuçları ve (Stichtenoth, 2000, Kısım 5)'teki bazı teknikleri kullanarak bazı durumlarda L-polinomu $L_\chi(t)$'yi aşağıda elde ettik.

q, m ve n verilmiş olsun. Buna göre χ'nin L-polinomu $L_\chi(t)$'yi hesaplamak için aşağıdaki adımları kullanıyoruz.

1. $l \in \mathbb{Z}^+$ için $N(lm,n)$'yi hesapla.
2. $S(lm,n) = q^n N(lm,n) - q^{lm}$ hesapla.
3. $L'_\chi(t)$ ifadesi $L_\chi(t)$'nin türevi olmak üzere $\dfrac{L'_\chi(t)}{L_\chi(t)} = \displaystyle\sum_{l=1}^{\infty} S(lm,n)t^{l-1}$ hesapla.
4. İki tarafın da integralini al ve $L_\chi(t)$ ifadesini elde etmek için sadeleştirmeler yap.

L-polinomlar hakkında elde ettiğimiz nümerik sonuçları vermeden önce, Hermitian eğriler ve bizim (2.1) formatındaki eğrilerimiz arasındaki bağlantıyı belirtmek istiyoruz.

Açıklama 2.6.2. Bizim (2.1) formatındaki eğrilerimiz aşağıdaki formatta olan tüm Hermitian eğrilerini kapsar.

$$y^q + y = x^{q+1} (\mathbb{F}_{q^2} \text{ üzerinde}).$$

(2.1)'de eğer $n = 1$, $h = 1$, $m = 2$ ve $\alpha = 0$ alırsak ve y değişkenini bazı sıfırdan farklı $c \in \mathbb{F}_{q^2}$ için $y = cz$ olarak değiştirirsek

$$(cz)^q - cz = \gamma x^{q+1}.$$

c^q ile bölerek

$$z^q - \frac{1}{c^{q-1}} z = \frac{\gamma}{c^q} x^{q+1}.$$

O zaman $\dfrac{1}{c^{q-1}} = -1$ ve $\dfrac{\gamma}{c^q} = 1$ olmalı. ω, $\mathbb{F}_{q^2} \setminus \{0\}$ çarpımsal grubunun bir üreteci olsun. O zaman $c = w^{\frac{q+1}{2}}$ ve $\gamma = c^q = w^{\frac{q(q+1)}{2}}$ seçerek istediğimiz sonucu elde ederiz.

Yukardaki adımları takip ederek bazı eğrilerin L-polinomlarını aşağıdaki şekilde hesapladık.

Örnek 2.6.3. *χ, $\mathbb{F}_{q^4}$ üzerinde $y^q - y = x^{q+1}$ eğrisi olsun. O zaman bu eğrinin L-polinomu*

$$L_\chi(t) = \left(1 - q^2 t\right)^{q(q-1)}.$$

Örnek 2.6.4. *χ, $\mathbb{F}_{q^2}$ üzerinde $y^q - y = x^{q+1}$ eğrisi olsun. O zaman bu eğrinin L-polinomu*

$$L_\chi(t) = (1 - qt)^{\frac{q^2-1}{2}} (1 + qt)^{\frac{(q-1)^2}{2}}.$$

Örnek 2.6.5. *χ, $\mathbb{F}_{q^4}$ üzerinde $y^q - y = x^{q^2+1}$ eğrisi olsun. O zaman bu eğrinin L-polinomu*

$$L_\chi(t) = \left(1 - q^2 t\right)^{\frac{(q^2+1)(q-1)}{2}} \left(1 + q^2 t\right)^{\frac{(q^2-1)(q-1)}{2}}.$$

Örnek 2.6.6. *χ, $\mathbb{F}_{q^6}$ üzerinde $y^q - y = x^{q^4+1}$ eğrisi olsun. O zaman bu eğrinin L-polinomu*

$$L_\chi(t) = \begin{cases} (1 + q^3 t)^{q-1} (1 - q^{24} t^8)^{\frac{q^4(q-1)}{8}} & , q \equiv 3 \mod 4, \\ (1 - q^3 t)^{q-1} (1 - q^{24} t^8)^{\frac{q^4(q-1)}{8}} & , q \equiv 1 \mod 4. \end{cases}$$

Örnek 2.6.7. *χ, $\mathbb{F}_{q^5}$ üzerinde $y^q - y = x^{q^4+1}$ eğrisi olsun. O zaman bu eğrinin L-polinomu*

$$L_\chi(t) = \begin{cases} (1 - q^5 t)^{q-1} (1 - q^{40} t^{16})^{\frac{(q^4-1)(q-1)}{16}} & , q \equiv 3 \mod 4, \\ \dfrac{(1 - q^5 t^2)^{\frac{q-1}{2}} (1 - q^5 t)^{q-1} (1 - q^{40} t^{16})^{\frac{(q^4-1)(q-1)}{16}}}{(1 + q^5 t^2)^{\frac{q-1}{2}}} & , q \equiv 1 \mod 4. \end{cases}$$

Örnek 2.6.8. *χ, $\mathbb{F}_{q^4}$ üzerinde $y^{q^2} - y = x^{q+1}$ eğrisi olsun. O zaman bu eğrinin L-polinomu*

$$L_\chi(t) = \begin{cases} (1 - q^2 t)^{2(q^2-1)} (1 + q^2 t)^{q^2-1} & , q = 3, \\ (1 - q^2 t)^{q^2-1} (1 - q^6 t^3)^{\frac{4(q^2-1)}{3}} & , q = 5. \end{cases}$$

Aşağıdaki sonuç bize $L_\chi(t)$'nin bazı durumlarda $q+1$'in çarpanlarına göre değiştiğini gösteriyor.

Teorem 2.6.9. *χ, $\mathbb{F}_{q^2}$ üzerinde $y^{q^2} - y = x^{q+1}$ eğrisi olsun. θ bir tek asal ve ν_0 ile ν_1 pozitif tamsayılar olmak üzere $q + 1 = 2^{\nu_0} \theta^{\nu_1}$ olsun.O zaman bu eğrinin L-polinomu*

$$\left(\frac{1 - q^\theta t^\theta}{1 + q^\theta t^\theta}\right)^{\frac{q^2-1}{2\theta}} \left(\prod_{i=1}^{\nu_0} \left(1 - q^{2^i} t^{2^i}\right)^{\frac{q^2-1}{2}}\right) \left(\prod_{i=1}^{\nu_1} \left(1 - q^{2\theta^i} t^{2\theta^i}\right)^{\frac{(q^2-1)(\theta-1)}{\theta}}\right) \left(\prod_{i=2}^{\nu_0} \prod_{j=1}^{\nu_1} \left(1 - q^{2^i \theta^j} t^{2^i \theta^j}\right)^{\frac{(q^2-1)(\theta-1)}{2\theta}}\right)$$

öyle ki

$$P = \left(\frac{1-q^{\theta}t^{\theta}}{1+q^{\theta}t^{\theta}}\right)^{\frac{q^2-1}{2\theta}}.$$

Eğer ν_0 bir pozitif tamsayı olmak üzere $q+1=2^{\nu_0}$ şeklinde bir sınırlandırma yaparsak aşağıdaki sonucu elde ederiz. Belirtelim ki q bir asalın kuvveti ve $q+1=2^{\nu_0}$ olacak şekilde sonsuz sayıda ν_0 değeri olması için Mersenne asalları konjektürünün sağlanması gerek ve yeter koşuldur (Huppert, 1982, Bölüm IX, Lemma 2.7).

Ek Sonuç 2.6.10. *χ, $\mathbb{F}_{q^2}$ üzerinde $y^{q^2}-y=x^{q+1}$ eğrisi olsun. Ayrıca ν_0 bir pozitif tamsayı olmak üzere $q+1=2^{\nu_0}$ olsun. O zaman eğrinin L-polinomu*

$$\prod_{i=1}^{\nu_0}\left(1-q^{2^i}t^{2^i}\right)^{\frac{q^2-1}{2}}.$$

Teorem 2.6.9'ün ispatındaki metotların benzerlerini kullanarak aşağıdaki sonucu elde ederiz. Vurgulamak istiyoruz ki aşağıdaki L-polinomları $\mathbb{F}_q$'nun karakteristiğine bağlıdır.

Önerme 2.6.11. *χ, $\mathbb{F}_{q^6}$ üzerinde $y^q-y=x^{q^4+1}+\alpha$ eğrisi olsun. $A=\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_q}(\alpha)\neq 0$ olduğunu farz edelim ve $p=char(\mathbb{F}_q)$ olsun. O zaman L-polinomu*

$$L_{\chi}(t)=\begin{cases}\dfrac{\left(1-q^{3p}t^{p}\right)^{\frac{q}{p}}\left(1-q^{24p}t^{8p}\right)^{\frac{q(q^4-1)}{8p}}}{\left(1-q^3t\right)\left(1-q^{24}t^8\right)^{\frac{q^4-1}{8}}} & , q\equiv 1 \mod 4,\\ \dfrac{\left(1+q^{3p}t^{p}\right)^{\frac{q}{p}}\left(1-q^{24p}t^{8p}\right)^{\frac{q(q^4-1)}{8p}}}{\left(1+q^3t\right)\left(1-q^{24}t^8\right)^{\frac{q^4-1}{8}}} & , q\equiv 3 \mod 4.\end{cases}$$

2.7 Galois Halkalarında Polinom Çarpımı

Proje kapsamında çalışılan konu hakkında gerekli bilgiler, yöntem ve bulgular 3 alt bölüm altında toplanmıştır. Elde edilen sonuç bir dergiye değerlendirilmesi için gönderilmiştir.

2.7.1 Giriş

Galois halkaları kriptografi, kodlama teorisi, iletişim ve sinyal işleme alanlarındaki uygulamaları nedeniyle son zamanlarda büyük ilgi çekmiştir (Krishna and Sun, 1995), (Krishna and Lin, 1994a), (Krishna and Lin, 1994b), (Lint, 1999). Bu çalışmada $\mathbb{Z}_4$ üzerindeki Galois halkalarına yoğunlaşılmasının sebebi, buralardaki iyi hata düzeltme kodlarının varlığıdır (Hammons and Sole, 1994). Abrahamsson, Galois halkasındaki iki

polinomun çarpımı için okul yöntemi (schoolbook method) tabanlı çarpıcılar önermiştir (Abrahamsson, 2004). Bu çarpıcıların alan karmaşıklığı üsseldir. Bundan dolayı verimlilik konusunda bazı problemleri vardır.

2.7.2 Matematiksel Altyapı

p asal bir sayı ve k, m pozitifi tamsayılar olsun. $\mathbb{Z}_{p^k}$, p^k modülüne göre tamsayılar halkası olsun. $f(x) \in \mathbb{Z}_{p^k}[x]$ derecesi n ve $(x^{p^n-1} - 1)$'yi bölen monik indirgenemez olsun. $\mathbb{Z}_{p^k}[x]/ < f(x) >$ halkası $GR(p^k, n)$ ile gösterilir ve karakteristiği p^k, mertebesi p^{kn} olan Galois halkası olarak isimlendirilir. $k = 1$ olduğu durumda $GR(p^k, n)$, $\mathbb{F}_{p^n}$ sonlu cismine dönüşür. Ayrıca, $n = 1$ ise $GR(p^k, n)$, $\mathbb{Z}_{p^k}$ halkası olur. $f(x) \in \mathbb{Z}_{p^k}[x]$ hem $\mathbb{Z}_{p^k}$ hem de $\mathbb{F}_p$ üzerinde indirgenemez ise $f(x)$ temel (basic) indirgenemez polinom olarak adlandırılır. Bu çalışmada, $f(x)$, $\mathbb{Z}_4$ üzerinde derecesi n olan temel indirgenemez polinom olmak üzere karakteristiği 4, mertebesi 4^n olan Galois halkası $R = GR(4, n) \cong \mathbb{Z}_4[x]/ < f(x) >$'dir.

$n \times n$ boyutundaki Toeplitz matrisi $(T_{i,j})$, $2 \leq i, j \leq n$ için $T_{i,j} = T_{i-1,j-1}$ özelliğini sağlayan bir matristir. ℓ pozitif bir tamsayı olmak üzere $m \in \{2, 3\}$ ve $n = m^\ell$ olsun. A, $n \times n$ boyutunda Toeplitz matris, B, $n \times 1$ boyutunda sütun vektörü ve $C = A \cdot B$ $\mathbb{Z}_4$ üzerinde olsun. (Winograd, 1980) ve (Fan and Hasan, 2007) çalışmalarında verilen yöntemi değiştirerek aşağıdaki formüller elde edilir. Öncelikle $n = 2^\ell$ durumunu ele alalım.

$$\begin{bmatrix} A_0 & A_1 \\ A_2 & A_0 \end{bmatrix} \cdot \begin{bmatrix} B_0 \\ B_1 \end{bmatrix} = \begin{bmatrix} C_0 \\ C_1 \end{bmatrix}$$

Burada A_0, A_1 ve A_2 $\frac{n}{2} \times \frac{n}{2}$ boyutunda Toeplitz matrislerdir. B_0, B_1, C_0 ve C_1, $\frac{n}{2} \times 1$ boyutunda sütun vektörleridir. (Winograd, 1980)'da verilen yöntemi $\mathbb{Z}_4$ için uyarlarsak:

$$\begin{aligned} P_0 &= (A_0 + A_1)B_1 \\ P_1 &= (A_0 + A_2)B_0 \\ P_2 &= A_0(B_0 - B_1) = A_0(B_0 + 3B_1) \end{aligned}$$

olmak üzere,

$$\begin{aligned} C_0 &= P_0 + P_2 \\ C_1 &= P_1 - P_2 = P_1 + 3P_2 \end{aligned}$$

$n = 2$ durumunda C'yi hesaplamak için ihtiyaç duyulan çarpma işlemi sayısı 3, toplama işlemi sayısı 3 ve çıkarma işlemi sayısı 2'dir. (Fan and Hasan, 2007) referansında verilen karmaşıklık hesapları karakteristiği 4 olan Galois halkaları için güncellenirse şu

sonuçlar elde edilir:

$$\begin{aligned} \#carpma &= n^{log_2 3} \\ \#toplama &= \frac{11}{2} n^{log_2 3} - 7n + 0.5 \\ \#cikarma &= n \end{aligned}$$

Benzer şekilde $n = 3^\ell$ olsun.

$$\begin{bmatrix} A_0 & A_1 & A_2 \\ A_3 & A_0 & A_1 \\ A_4 & A_3 & A_0 \end{bmatrix} \cdot \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} = \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix}$$

Burada A_0, A_1, A_3 ve A_4 $\frac{n}{3} \times \frac{n}{3}$ boyutundaki Toeplitz matrisleri ve B_0, B_1, B_2, C_0, C_1 ve C_2, $\frac{n}{3} \times 1$ boyutundaki sütun vektörleri olsun.

$$\begin{aligned} P_0 &= (A_0 + A_3 + A_4)B_0 \\ P_1 &= (A_0 + A_1 + A_3)B_1 \\ P_2 &= (A_0 + A_1 + A_2)B_2 \\ P_3 &= A_0(B_0 - B_2) = A_0(B_0 + 3B_2) \\ P_4 &= A_1(B_1 - B_2) = A_1(B_1 + 3B_2) \\ P_5 &= A_3(B_0 - B_1) = A_3(B_0 + 3B_1) \end{aligned}$$

olmak üzere

$$\begin{aligned} C_0 &= P_2 + P_3 + P_4 \\ C_1 &= P_1 - P_4 + P_5 = P_1 + 3P_4 + P_5 \\ C_2 &= P_0 - P_3 - P_5 = P_0 + 3P_3 + 3P_5 \end{aligned}$$

$n = 3$ durumunda C'yi hesaplamak için ihtiyaç duyulan çarpma işlemi sayısı 6, toplama işlemi sayısı 8 ve çıkarma işlemi sayısı 6'dır. (Fan and Hasan, 2007) referansında verilen karmaşıklık hesapları karakteristiği 4 olan Galois halkaları için güncellenirse şu

sonuçlar elde edilir:

$$\begin{aligned} \#carpma &= n^{log_3 6} \\ \#toplama &= \frac{24}{5} n^{log_3 6} - 7n + \frac{1}{5} \\ \#cikarma &= 2n \end{aligned}$$

Tablo 2.1'de belirtilen Galois halkasındaki iki polinomun çarpımı için ihtiyaç duyulan çarpma, toplama ve çıkarma sayıları verilmiştir. Tablo 2.1'de $n = m^\ell$ olarak kabul edilmiştir. $\mathbb{Z}_4$'de elemanların çıkarma işlemi 3 ile çarpım olarak düşünülebilir.

Tablo 2.1: Çarpma İşleminin Asimtotik Karmaşıklığı

m	$\mathbb{Z}_4$'deki çarpma sayısı	$\mathbb{Z}_4$ toplama sayısı	$\mathbb{Z}_4$'deki çıkarma sayısı
2	$n^{log_2(3)}$	$\frac{11}{2} n^{log_2(3)} - 7n + \frac{1}{2}$	n
3	$n^{log_3(6)}$	$\frac{24}{5} n^{log_3(6)} - 7n + \frac{1}{5}$	$2n$

2.7.3 Gereç, Yöntem ve Sonuçlar

Katsayıları $\mathbb{Z}_4$ üzerinde olan $a(x)$ ve $b(x)$ polinomlarının çarpımı Toeplitz matrisi ve vektör çarpımı şeklinde yapılabilir.

Teorem 2.7.1. *$f(x) = x^n + x + 1$, $\mathbb{Z}_4$ üzerinde temel indirgenemez polinom olsun. $a(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ ve $b(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ katsayıları $\mathbb{Z}_4$'de olan n terimli polinomlar ve $a(x) \cdot b(x) \pmod{f(x)} \equiv c(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ olsun. $c(x)$'in katsayıları $C = A_1 B + A_2 B$ şeklinde hesaplanabilir. Burada,*

$$A_1 = \begin{bmatrix} a_1 & a_0 + 3a_{n-1} & 3(a_{n-1} + a_{n-2}) & \cdots & 3(a_3 + a_2) & 3(a_2 + a_1) \\ a_2 & a_1 & a_0 + 3a_{n-1} & \cdots & 3(a_4 + a_3) & 3(a_3 + a_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 + 3a_{n-1} \\ a_0 & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 2a_{n-1} & 2a_{n-2} & \cdots & 2a_2 & 2a_1 \end{bmatrix}, B = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-2} \\ b_{n-1} \end{bmatrix}, C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_{n-1} \\ c_0 \end{bmatrix}$$

A_1B, Toeplitz matrisi ve vektör çarpımıdır.

Örnek 2.7.2. *$f(x) = x^4 + x + 1$, $\mathbb{Z}_4$ üzerinde temel indirgenemez polinomdur. $A = a_3x^3 + a_2x^2 + a_1x + a_0$ ve $B = b_3x^3 + b_2x^2 + b_1x + b_0$, $\mathbb{Z}_4$ üzerinde 4 terimli polinomlar ve $A \cdot B = C' = c'_6x^6 + \cdots + c'_0$, $A \cdot B \pmod{f(x)} = C = c_3x^3 + \cdots + c_0$ olsun.*

$$\begin{aligned} x^4 &= -x - 1 = 3x + 3 \\ x^5 &= 3x^2 + 3x \\ x^6 &= 3x^3 + 3x^2 \end{aligned}$$

$$\begin{aligned} c'_0 &= a_0b_0 \\ c'_1 &= a_0b_1 + a_1b_0 \\ c'_2 &= a_0b_2 + a_2b_0 + a_1b_1 \\ c'_3 &= a_0b_3 + a_3b_0 + a_1b_2 + a_2b_1 \\ c'_4 &= a_1b_3 + a_3b_1 + a_2b_2 \\ c'_5 &= a_2b_3 + a_3b_2 \\ c'_6 &= a_3b_3 \end{aligned}$$

ve

$$\begin{aligned}
c_0 &= 3c'_4 + c'_0 \\
c_0 &= 3a_1b_3 + 3a_2b_2 + 3a_3b_1 + a_0b_0 \\
c_1 &= 3c'_5 + 3c'_4 + c'_1 \\
c_1 &= 3(a_1 + a_2)b_3 + 3(a_2 + a_3)b_2 + (a_0 + 3a_3)b_1 + a_1b_0 \\
c_2 &= 3c'_6 + 3c'_5 + c'_2 \\
c_2 &= 3(a_2 + a_3)b_3 + (a_0 + 3a_3)b_2 + a_1b_1 + a_2b_0 \\
c_3 &= 3c'_6 + c'_3 \\
c_3 &= (a_0 + 3a_3)b_3 + a_1b_2 + a_2b_1 + a_3b_0
\end{aligned}$$

olmak üzere

$$\begin{aligned}
C' &= c'_6(3x^3 + 3x^2) + c'_5(3x^2 + 3x) + c'_4(3x + 3) + c'_3x^3 + c'_2x^2 + c'_1x + c'_0 \\
C &= (3c'_6 + c'_3)x^3 + (3c'_6 + 3c'_5 + c'_2)x^2 + (3c'_5 + 3c'_4 + c'_1)x + 3c'_4 + c'_0
\end{aligned}$$

$$C = \begin{bmatrix} a_1 & a_0 + 3a_3 & 3(a_2 + a_3) & 3(a_1 + a_2) \\ a_2 & a_1 & a_0 + 3a_3 & 3(a_2 + a_3) \\ a_3 & a_2 & a_1 & a_0 + 3a_3 \\ a_0 & 3a_3 & 3a_2 & 3a_1 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_0 \end{bmatrix}$$

$$C = \left(\begin{bmatrix} a_1 & a_0 + 3a_3 & 3(a_2 + a_3) & 3(a_1 + a_2) \\ a_2 & a_1 & a_0 + 3a_3 & 3(a_2 + a_3) \\ a_3 & a_2 & a_1 & a_0 + 3a_3 \\ a_0 & a_3 & a_2 & a_1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 2a_3 & 2a_2 & 2a_1 \end{bmatrix} \right) \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Açıklama 2.7.3. $\mathbb{Z}_4$'de her elemanın tersi bulunmadığından Çinli Kalan Teoremine dayalı çarpma yöntemleri karakteristiği 4 olan Galois halkasında kullanılamamaktadır. Aynı zamanda, Karatsuba-Ofman yöntemi, önerilen bu yöntem ile aynı sayıda çarpma işlemine ihtiyaç duymasına rağmen, ihtiyaç duyulan çıkarma işlemi sayısı önerilen yöntemdekinden daha fazladır. Buna ek olarak, Karatsuba-Ofman yöntemini herhangi bir n için formülize etmek kolay değildir.

Aritmetik Karmaşıklık

ℓ pozitif tamsayı olmak üzere $m \in \{2, 3\}$ ve $n = m^\ell$ olsun. M_n, A_n ve S_n sırasıyla ihtiyaç duyulan çarpma (mults), toplama (adds) ve çıkarma (subs) işlemlerinin sayısı Tablo 2.1'de verilmiştir. Tablo 2.2 önerilen yönteme göre iki polinomun çarpımı için R'deki çarpma, toplama ve çıkarma işlem sayılarını göstermektedir. 2 ile çarpmanın sadece bir kaydırma işlemine ve bunun neredeyse maliyetsi olduğunu hatırlatmakta fayda var. Benzer şekilde 3 ile çarpım bir sayının tersi olarak hesaplanabilmektedir.

Tablo 2.2: R'deki Çarpma İşlemi İçin Asimtotik Karmaşıklık

Z_4'deki çarpma sayısı	Z_4'deki toplama sayısı	Z_4'deki çıkarma sayısı	2 veya 3 ile çarpma
M_n	$A_n + (n-1)$	S_n	$2n-2$

Açıklama 2.7.4. $n \in \{2, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900\}$ olsun. $f(x) = x^n + x + 1$, $f(x) = x^n + x - 1$, $f(x) = x^n - x + 1$ ve $f(x) = x^n - x - 1$, $\mathbb{Z}_4$ üzerinde temel indirgenemez polinomlardır. Bu sonuçlar Magma Computational Algebra Software kullanılarak elde edilmiştir (Bosma and Playoust, 1997).

Çarpıcı Tasarımı

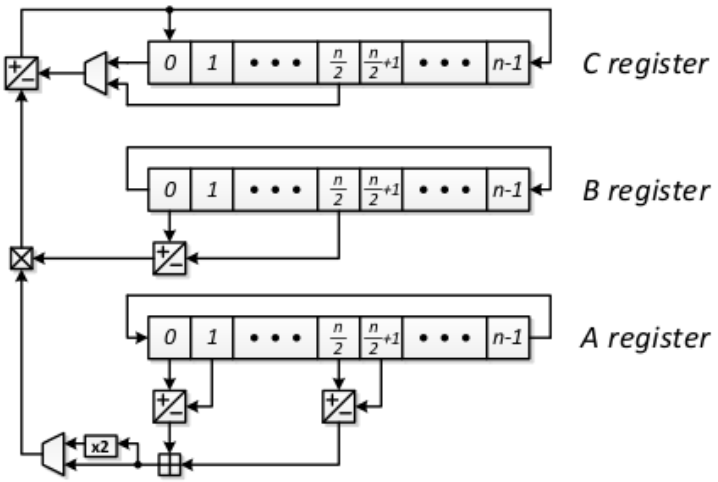
Şekil 2.4 $n = 2^\ell$ durumu için önerilen yöntemin dizisel çarpıcısını göstermektedir. Çarpıcı 3 kayıt, 2 girdi elemanı A ve B, bir çıktı elemanından C oluşmaktadır. Başlangıçta girdi kaydı girdi polinomları ile (a_0 ve b_0 en soldaki kayıt elemanına) yüklenir.

2.8 Çok Boyutlu Sanki-Devirsel ve Konvolusyon Kodları

Bu alt bölümde çok boyutlu sanki-devirsel ve konvolusyon kodları hakkında sonuçlar yer almaktadır. Sunulan sonuçlar, proje kapsamında 29-30 Mayıs 2014 tarihlerinde Boğaziçi Üniversitesinde düzenlenen çalıştayda sunulmuştur.

2.8.1 Giriş

Sanki-devirsel (SD) kodlar, devirsel kodların zengin bir cebirsel yapıya sahip genellemeleridir (Ling and Solé, 2001). SD kodlar, iyi parametrelere sahip kodlar üretmenin yanı sıra (Chen, 2007; Daskalov and Hristov, 2003; Gulliver and Bhargava,



Şekil 2.4: Dizisel çarpım

1991) asimptotik olarak iyi bir ailedirler (Dey, 2004; Kasami, 1974; Ling and Solé, 2003). Konvolusyonel kodlar da sanki-devirsel kodlarla yakından ilişkilili olan önemli bir kod sınıfıdır. İki kod ailesi arasındaki temel fark, konvolusyonel kodların blok kod olmamasıdır (McEliece, 1998). Her konvolusyonel kodun serbest uzaklığı, ilişkili olduğu sanki-devirsel kodun minimum uzaklığı tarafından alttan sınırlıdır (Lally, 2006).

Bir boyutlu durumda olduğu kadar kapsamlı çalışılmamış olsalar da, çok boyutlu konvolusyonel kodlar da literatürde incelenmişlerdir (Waterhouse, 1969). Bu çalışmanın amacı, SD kodların çok boyutlu benzerlerini tanımlamak ve bir boyutta SD kodlarla konvolusyon kodları arasındaki ilişkinin, çok boyutlu konvolusyon kodları ile çok boyutlu SD kodlar arasında da var olduğunu göstermektir.

2.8.2 Sanki-Devirsel ve Konvolusyonel Kodlar

$\mathbb{F}_q$, q elemanlı sonlu cisim olsun. m ve ℓ pozitif tam sayılarını, m ve q aralarında asal olacak şekilde seçelim. $\mathbb{F}_q$ üzerinde tanımlı, boyu $m\ell$ olan doğrusal C kodunun kod sözleri ℓ pozisyonluk öteleme altında kapalıysa ve ℓ bu özelliği sağlayan en küçük tam sayı ise, C koduna indeksi ℓ olan SD kod denir. C'nin kod sözlerini aşağıdaki gibi $m \times \ell$ matrisler formunda yazarsak

$$c = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix}, \tag{2.1}$$

ℓ pozisyonluk öteleme altında kapalılığın satır ötelemesi altında kapalılıkla aynı olduğu kolayca görülebilir. $\ell = 1$ özel durumunda C'nin devirsel kod olduğu açıktır. Dolayısıyla SD kod, devirsel kodun bir genellemesidir.

Polinom halkası $\mathbb{F}_q[x]$'in $I = \langle x^m - 1 \rangle$ ideali için $R := \mathbb{F}_q[x]/I$ bölüm halkasını alalım. Yukarıda $m \times \ell$ matrisler olarak yazılan her c elemanı, R^ℓ'deki bir elemana aşağıdaki gibi eşleştirilebilir:

$$\begin{array}{rcl} \phi : \quad \mathbb{F}_q^{m\ell} & \longrightarrow & R^\ell \\ c = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \longmapsto & \vec{c}(x) := (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \end{array} \tag{2.2}$$

Burada, her $0 \leq j \leq \ell - 1$ için,

$$c_j(x) := c_{0,j} + c_{1,j}x + c_{2,j}x^2 + \cdots + c_{m-1,j}x^{m-1} \in R$$

şeklinde tanımlıdır. $\mathbb{F}_q^{m\ell}$'de satır öteleme operasyonunun R^ℓ'de koordinat-koordinat x ile çarpmaya denk geldiğini belirtelim. Dolayısıyla SD bir kodu, ϕ eşleştirmesi ile R^ℓ'e taşırsak, elde edeceğimiz yapı R^ℓ içerisinde bir R alt modüldür.

C'nin kod sözlerinin diğer bir polinom temsili için iki değişkenli polinom halkası $\mathbb{F}_q[x, y]$ ile $J = \langle x^m - 1, y^\ell - 1 \rangle$ idealini düşünelim. $S := \mathbb{F}_q[x, y]/J$ bölüm halkası da R-modül yapısına sahiptir ve R^ℓ ile izomorftur. Bu sayede SD bir C kodunu S içinde de R alt modül olarak düşünebiliriz.

Boyu $m\ell$ olan ve (2.1)'deki gibi yazılmış kod sözleri hem satır hem de sütun ötelemesi altında kapalı olan kodlara 2D devirsel kod denir (Ikai and Kojima, 1975; Imai, 1977). Her 2D devirsel kodun bir ℓ indeksli SD kod olduğu açıktır. Sütun ötelemesi altında kapalılık ise S halkası içinde y ile çarpma altında kapalılık demektir. Bu nedenle 2D devirsel kodlar S halkasının idealleridir.

Şimdi SD kodların tanımlandıkları sonlu cismin bazı genişlemeleri üzerinde daha kısa doğrusal kodlara ayrıldığı birleşik yapıdan bahsedelim. Bunun için ilk önce $x^m - 1$ polinomunu $\mathbb{F}_q[x]$ içinde indirgenemez faktörlere ayıralım:

$$x^m - 1 = f_1(x)f_2(x)\ldots f_s(x) \tag{2.3}$$

m ve q aralarında asal olduklarından (2.3) eşitliğindeki indirgenemez faktörler

birbirlerinden farklıdırlar. Çinlilerin Kalan Teoremi bize şu halka izomorfizmasını verir:

$$R \cong \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle f_i(x)\rangle. \tag{2.4}$$

Tüm f_i polinomları indirgenemez olduklarından, her $i = 1, \ldots, s$ için (2.4)'deki bölüm halkalarının hepsi $\mathbb{F}_q$ cisminin birer genişlemesidir. Bunlara $\mathbb{E}_i := \mathbb{F}_q[x]/\langle f_i(x)\rangle$ dersek (2.4) kullanılarak aşağıdaki izomorfizma elde edilir:

$$R^\ell \cong \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell. \tag{2.5}$$

Dolayısıyla, SD $C \subset R^\ell$ kodu, her $C_i \subset \mathbb{E}_i^\ell$ boyu ℓ olan $\mathbb{E}_i$-doğrusal kodlar olmak üzere

$$C = C_1 \oplus \cdots \oplus C_s \tag{2.6}$$

şeklinde parçalanır. C_i kodlarına C'nin bileşenleri (constituents) denir (detaylar için bkz. (Ling and Solé, 2001)).

Ayrıca her $\mathbb{E}_i$, boyu m ve kontrol polinomu $f_i(x)$ olan bir minimal devirsel koda izomorftur. Bu kodun primitif kare eş üretecine θ_i diyelim. Eğer C_i, $\mathbb{E}_i$ üzerinde boyu ℓ olan bir doğrusal kod ise, $\langle\theta_i\rangle$ ile birleştirilmesi (concatenation) $\langle\theta_i\rangle\square C_i$ ile gösterilir. $\langle\theta_i\rangle$ ve C_i kodlarına sırasıyla iç ve dış kod denir. SD kodların birleştirme yoluyla elde edilmesini Jensen şöyle vermiştir:

Teorem 2.8.1. *(Jensen, 1985) $C \subset R^\ell$ bir SD kod ise her $\mathbb{E}_i$ üzerinde boyu ℓ olan öyle doğrusal C_i kodları vardır ki C kodu $C = \oplus_{i=1}^{s}\langle\theta_i\rangle\square C_i$ şeklinde parçalanır. Tersi de geçerlidir.*

Aslında, (2.6)'daki bileşenler ile birleştirme ifadesindeki dış kodlar aynıdır ((Güneri and Özbudak, 2013, Teorem 4.1)).

$C \subset \mathbb{F}_q[x]^\ell$ mertebesi k olan bir $\mathbb{F}_q[x]$ alt modül ise C'ye (ℓ, k) konvolusyonel kod denir. $\mathbb{F}_q[x]$ temel ideal bölgesi olduğundan her konvolusyonel kod serbest alt modüldür. $\mathbb{F}_q[x]$'deki polinomların ağırlığı sıfırdan farklı terim sayısıdır. C'nin kod sözlerinin ağırlığı ise koordinatlarının ağırlıkları toplamıdır. C'nin serbest uzaklığı $(d_f(C))$, kod sözlerinin ağırlıklarının minimumu olarak tanımlanır (detaylar için bkz. (McEliece, 1998)).

Yeniden $R = \mathbb{F}_q[x]/\langle x^m - 1\rangle$ olsun ve aşağıdaki izdüşümü düşünelim:

$$\begin{aligned} \Phi : \mathbb{F}_q[x] &\longrightarrow R \\ f(x) &\mapsto f'(x) := f(x) \mod \langle x^m - 1\rangle. \end{aligned} \tag{2.7}$$

$\mathbb{F}_q[x]^\ell$'deki elemanların koordinatlarının Φ altındaki görüntüsünü düşünürsek, her pozitif m tam sayısı için verilen her (ℓ, k) konvolusyonel kodla ilişkili boyu $m\ell$ ve indeksi ℓ olan bir SD kod olduğu barizdir.

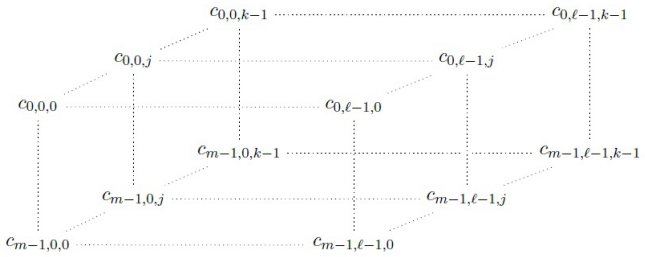
$$\begin{array}{ccc} C & \longrightarrow & C' \\ \vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x)) & \mapsto & \vec{c'}(x) = (c'_0(x), \ldots, c'_{\ell-1}(x)). \end{array} \tag{2.8}$$

C konvolusyonel kodunun serbest uzaklığının, ilişkili SD kod C''nin minimum uzaklığı tarafından alttan sınırlı olduğu Lally tarafından ispatlanmıştır ((Lally, 2006)).

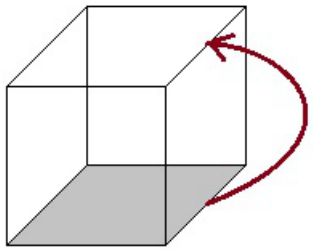
Teorem 2.8.2. *((Lally, 2006, Teorem 2)) Her (ℓ, k) konvolusyonel kod C ve ilişkili SDkod C' için, $d_f(C) \geq d(C')$.*

2.8.3 Çok Boyutlu SD ve Konvolusyonel Kodlar ve Sonuçlar

Bu bölümde çok boyutlu SD kodları, vektörel temsili mümkün olan 3-boyutlu durumdan başlayarak tanıtacağız. SD ve 2D devirsel kodların, ilki bir diğeri iki tür öteleme altında kapalı 2-boyutlu kodlar olduklarını hatırlayalım. Şimdi ise C kodu $\mathbb{F}_q$ üzerinde tanımlanmış $m\ell k$ uzunluğunda bir doğrusal kod olsun. C'nin kod sözlerini $m \times \ell \times k$ boyutlarında küpler olarak yazabiliriz:

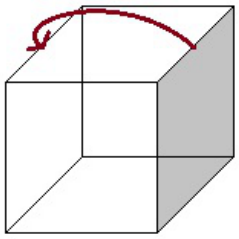


Bu şekilde yazılan kod sözleri alttan-üste, sağdan-sola ve arkadan-öne yüz ötelemeleri altında kapalıysa C koduna 3-boyutlu (3D) devirsel kod denir.

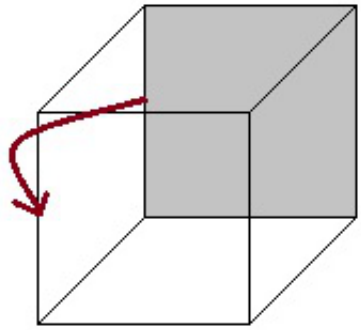


Şekil 2.5: Küp 1

Çok boyutlu devirsel kodlar kapsamlı olarak incelenmişlerdir (bkz. (Güneri, 2004; Güneri and Özbudak, 2008; Saints and Heegard, 1993)). SD ve 2D devirsel



Şekil 2.6: Küp 2



Şekil 2.7: Küp 3

kodların ilişkisine benzer bir biçimde, 2-boyutlu sanki-devirsel kodları (2DSD) artık tanımlayabiliriz.

Tanım 2.8.3. $\mathbb{F}_q$ üzerinde tanımlı, boyu $m\ell k$ ve (**??**)'daki gibi yazılmış kod sözleri alttan-üste ve sağdan-sola yüz ötelemeleri altında kapalı olan C koduna 2DSD kod denir.

2DSD kodların cebirsel yapısını tarif edebilmek için önce $S := \mathbb{F}_q[x,y]/\langle x^m - 1, y^\ell - 1\rangle$ bölüm halkasını kullanacağız. Yukarıda (2.5)'daki gibi verilen her 2DSD kod sözünü, S^k'da bir elemana (2.2)'ye benzer şekilde eşleştirebiliriz:

$$\begin{aligned} \phi' : \mathbb{F}_q^{m\times\ell\times k} &\longrightarrow S^k \\ (c_{i,j,t}) &\mapsto \vec{c}(x,y) = (c_0(x,y), \ldots, c_{k-1}(x,y)), \end{aligned} \tag{2.9}$$

öyle ki her $0 \le t \le k-1$ için,

$$c_t(x,y) = \sum_{i=0}^{m-1}\sum_{j=0}^{\ell-1} c_{i,j,t}x^i y^j \in S. \tag{2.10}$$

Yine benzer şekilde, üç değişkenli polinom halkası $\mathbb{F}_q[x,y,z]$ ve ideali $U = \langle x^m - 1, y^\ell - 1, z^k - 1\rangle$ için $P := \mathbb{F}_q[x,y,z]/U$ bölüm halkasını tanımlayalım. Bu durumda P ile S^k izomorf olduğundan C'yi P'nin içinde de görebiliriz. Bu izomorfizmalar sayesinde, kod sözlerinin alttan-üste, sağdan-sola ve arkadan-öne yüz ötelemeleri P içinde sırasıyla

x, y ve z ile çarpma altında kapalılık ile örtüşmektedir. Bu hazırlıktan sonra şu sonuca varmak kolaydır:

Önerme 2.8.4. *Her 2DSD kod S^k'nın (veya P'nin) bir S alt modülüdür. Ayrıca, her 3D devirsel kod P'nin bir idealidir.*

Açıklama 2.8.5. Aynen SD ve 2D devirsel kodlarda olduğu gibi, 3D devirsel kodlar da bir tane daha öteleme altında kapalılık özelliğine sahip özel 2DSD kod olarak görülebilir.

Artık daha yüksek boyutlu SD kodlara geçebiliriz. Bunun için önce aşağıdaki halkaları tanımlayalım:

$$\begin{aligned} R_1 &= \mathbb{F}_q[x_1]/\langle x_1^{m_1} - 1\rangle \\ R_2 &= \mathbb{F}_q[x_1, x_2]/\langle x_1^{m_1} - 1, x_2^{m_2} - 1\rangle \\ &\vdots \quad\quad \vdots \\ R_n &= \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle \\ R_{n+1} &= \mathbb{F}_q[x_1, \ldots, x_{n+1}]/\langle x_1^{m_1} - 1, \ldots, x_{n+1}^{m_{n+1}} - 1\rangle \end{aligned} \tag{2.11}$$

Burada tüm m_i'ler pozitif tam sayılardır ve m_1 ile q aralarında asal olarak kabul edilmiştir.

Tanım 2.8.6. C eğer R_{n+1}'in (veya $R_n^{m_{n+1}}$'in) bir R_n alt modülü ise C'ye boyu $m_1 \times \cdots \times m_{n+1}$ olan n-boyutlu (nD) sanki-devirsel kod (nDSD) denir.

Buna göre, boyu $m_1 \times \cdots \times m_{n+1}$ olan $(n+1)$D devirsel kodlar R_{n+1}'in idealleridir. $(n+1)$D devirsel kodların birleştirme yapısındaki dış kodların (veya bileşenlerinin) nD devirsel kodlar olduğu gösterilmiştir (Güneri and Özbudak, 2013). Benzer bir sonuç nDSD kodlar için de geçerlidir.

Teorem 2.8.7. *nDSD kodların birleştirme yapısındaki dış kodları (veya bileşenleri) $(n-1)$DSD kodlardır. Bunun tersi de doğrudur.*

Bu birleşik yapı sayesinde şu sonucu elde ederiz.

Teorem 2.8.8. *nDSD kodlar asimptotik olarak iyidir.*

Konvolusyonel kodlar da çok boyuta genellenmişlerdir. n-boyutlu (nD) (ℓ, k) konvolusyonel kod, $\mathbb{F}_q[x_1, \ldots, x_n]^\ell$'in mertebesi k olan $\mathbb{F}_q[x_1, \ldots, x_n]$ serbest alt modülüdür (Waterhouse, 1969). Bir boyutlu durumda olduğu gibi $\mathbb{F}_q[x_1, \ldots, x_n]$'deki polinomların ağırlığı sıfırdan farklı terim sayısıdır. C'nin kod sözlerinin ağırlığı da yine koordinatlarının ağırlıkları toplamıdır. C'nin serbest uzaklığı ($d_f(C)$), sıfırdan farklı kod sözlerinin ağırlıklarının minimumudur.

Boyu $m_1 \times \cdots \times m_{n+1}$ olan bir nDSD kodun $R_n^{m_{n+1}}$'in bir R_n alt modülü olduğunu hatırlayalım. $\ell = m_{n+1}$ dersek, (2.7)'deki izdüşümün çok boyutlu benzerini şöyle tanımlayabiliriz:

$$\begin{aligned} \Phi : \mathbb{F}_q[x_1, x_2, \ldots, x_n] &\longrightarrow R_n \\ f &\mapsto f' := f \mod \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle \end{aligned} \tag{2.12}$$

Böylece, verilen her ℓ boyundaki nD konvolusyonel kod C için ilişkili bir $m_1 \times \cdots \times m_n \times \ell$ boyunda nDSD kod C' bulabiliriz:

$$\begin{aligned} C &\longrightarrow C' \\ \vec{c} = (c_0, \ldots, c_{\ell-1}) &\mapsto \vec{c'} = \left(c'_0, \ldots, c'_{\ell-1}\right). \end{aligned} \tag{2.13}$$

Lally'nin sonucunun bir genellemesini, $\mathbb{F}_q[x,y]^\ell$'den tek elemanla üretilen 2D konvolusyonel kodların özel bir sınıfı için vereceğiz. Bunun için, verilen tek üreteçli 2D konvolusyonel kodu üreten vektörü (diyelim ki $(g_1(x,y), \ldots, g_\ell(x,y))$) $\mathbb{F}_q[x,y]$'dan bir polinomla çarptığımızda çıkan kod sözünün tüm koordinatlarının $\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle$ idealinde olmamasını garantilemek istiyoruz. Bir başka deyişle, aşağıdaki koşulu sağlayan tek üreteçli 2D konvolusyonel kodlara yoğunlaşıyoruz:

$$\{u(x,y) \in \mathbb{F}_q[x,y]; ug_i \in \langle x^{m_1} - 1, y^{m_2} - 1 \rangle, \forall i = 1, \ldots, \ell\} = \langle x^{m_1} - 1, y^{m_2} - 1 \rangle. \tag{2.14}$$

Teorem 2.8.9. *Eğer C, yukarıdaki (2.14) koşulunu sağlayan $\vec{g}(x,y) = (g_1(x,y), \ldots, g_\ell(x,y))$ vektörü ile üretilmiş (ℓ, k) 2D konvolusyonel kod ve C', $(\mathbb{F}_q[x,y]/\langle x^{m_1} - 1, y^{m_2} - 1 \rangle)^\ell$'deki ilişkili 2DSD kod ise, $d_f(C) \geq d(C')$.*

Bölüm 3

Tartışma ve Sonuç

Proje kapsamında yapılan çalışmalar ve elde edilen sonuçlar gözönüne alındığında ikili işbirliği çerçevesinde proje önerisinde belirtilen hedeflere ulaşıldığını düşünmekteyiz. Proje kapsamında elde edilen sonuçların öne çıkanları aşağıda özetlenmiştir.

- 2'den farklı herhangi bir asal sayının kuvveti olmak üzere $n|m$ şartını sağlayan keyfi h, n, m pozitif tam sayıları ve $\gamma, \alpha \in \mathbb{F}_{q^m}$, $\gamma \neq 0$ elemanları için $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ eğrisinin bir çok durumdaki $\mathbb{F}_{q^m}$-rasyonel noktalarının sayısı hesaplanmıştır.
- Birçok $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyon sınıfının genişletilemez olduğunu gösterilmiştir.
- İkinci dereceden kompleks sayı cisimlerinin dallanmış (ramified) genişlemelerinde minimal polinomlarının katsayıları küçük olan özel elemanlar ve eşleniklerinin hesaplaması verilmiştir.
- Galois halkasındaki iki polinomun çarpımı Toeplitz matrisi ve vektör çarpımı şeklinde ifade edilerek alt üssel alan karmaşıklığı elde edilmiştir.
- Sanki-devirsel kodların çok boyutlu benzerlerini tanımlamak ve bir boyutta sanki-devirsel kodlarla konvolusyon kodları arasındaki ilişkinin, çok boyutlu konvolusyon kodları ile çok boyutlu sanki-devirsel kodlar arasında da var olduğu gösterilmiştir.

Bölüm 2'de 8 alt bölüm halinde detayları belirtilen proje çalışmalarından elde edilen sonuçlar, proje sonuç raporu formatına uygun bir şekilde aşağıda maddeler halinde verilmiştir.

1. Sonlu cisimler üzerindeki cebirsel eğrilerin cinslerini (genus) ve rasyonel nokta sayılarını kesin olarak bulmak zor bir problemdir ve kriptografide önemli bir yere

sahiptir. 2'den farklı herhangi bir asal sayının kuvveti olmak üzere $n|m$ şartını sağlayan keyfi h, n, m pozitif tam sayıları ve $\gamma, \alpha \in \mathbb{F}_{q^m}$, $\gamma \neq 0$ elemanları için $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ eğrisinin bir çok durumdaki $\mathbb{F}_{q^m}$-rasyonel noktalarının sayısı hesaplanmıştır.

Mükemmel lineer olmayan fonksiyonlar, kriptografide önemli bir yeri olan bükük (bent) ve düzlemsel (planar) fonksiyonları içeren önemli bir sınıftır. Mükemmel lineer olmayan fonksiyonların hangi sınıflarının genişletilemez (non-extendable) olduğunu incelemek zor bir problemdir. Birçok $\mathbb{F}_q$-kuadratik mükemmel lineer olmayan fonksiyon sınıfının genişletilemez olduğunu gösterilmiştir.

Cebirsel eğrilerin bazı karakteristik özelliklerini hesaplamada kullanılan L-polinomlarını bulmada yeni sonuçlar elde edilmiştir.

2. Galois halkalarındaki polinomlar çarpımı işlemini alt üssel alan karmaşıklığı ile gerçekleştiren ilk yöntem olarak önerilmiştir. Galois halkasındaki polinom çarpımı Toeplitz matrisi ve vektör çarpımı olarak formüle edilmiştir. Ayrıca, sonlu cisimler üzerinde kullanılan polinom çarpma yöntemleri güncellenerek Galois halkalarındaki polinom çarpımına uyarlanmıştır. Galois halkasında polinom çarpımı için önerilen alt üssel alan karmaşıklığına sahip yöntem için dizisel çarpıcı tasarlanmıştır. Önerilen bu yöntemin, herhangi bir karakteristikteki Galois halkasına kolaylıkla uyarlanabileceğini gösterdik.

3. Eliptik eğri tabanlı kriptografide belirli sayıda noktası olan bir eliptik eğri bulmak önemli bir uygulamadır. Bunun başarılması için Hilbert sınıf polinomları kullanılabilir. Bu polinomlar ikinci dereceden kompleks sayı cisimlerinin değişmeli genişlemelerinde uygun elemanlar ve eşlenikleri kullanılarak elde edilir.

   Sınıf polinomu hesaplaması j değişmezi kullanılarak yapılırsa katsayıları oldukça büyük olan polinomlar elde edilir. Diğer taraftan katsayıları j değişmezinin minimal polinomundan çok daha küçük olan çeşitli elemanlar bulunmuştur, bkz. (Gee, 2001), (Enge and Morain, 2009), (Leprévost and Uzunkol, 2011) ve (Uzunkol, 2013).

   Bu proje kapsamında ikinci dereceden kompleks sayı cisimlerinin dallanmış (ramified) genişlemelerinde minimal polinomlarının katsayıları küçük olan özel elemanlar ve eşleniklerinin hesaplaması verilmiştir. Elde edilen minimal polinomlar literatürdeki benzerlerine göre büyük bir iyileşme göstermektedir.

   Ayrıca, Siegel fonksiyonlarının kesirlerinin katsayıları ufak polinomlar üreteceği gözlemi yapılmıştır. Çalışmalar iki ana başlık altında devam etmiştir: İlk başlık Siegel fonksiyonlarını etkili bir biçimde kullanarak sınıf cisimlerini üretmek üzerine

yoğunlaşmaktadır. Diğer başlık Weierstrass P-fonksiyonun minimal polinomlarının hesabı üzerinedir.

4. Diyelim ki $\mathcal{F} = (F_n)_{n\geq 0}$ herhangi bir sonlu $\mathbb{F}_q$ cismi üzerinde tanımlanan ikinci dereceli özyineli bir cebirsel fonksiyon cisimleri kulesi. Yani; $\mathcal{F}$ kulesi $\mathbb{F}_q$ üzerinde tanımlanan öyle bir kule ki bütün $n \geq 1$ için $[F_n : F_{n-1}] = 2$ dir. Herhangi bir $r \geq 1$ tam sayısı için $B_r(F_n)$ ve $g(F_n)$, $F_n/\mathbb{F}_2$ nin sırasıyla r mertebeli yerlerin sayısı ve cinsi olmak üzere $\beta_r(\mathcal{F}) := \lim_{n\to\infty} B_r(F_n)/g(F_n)$ olsun. Bu proje kapsamında, sonlu cisim $\mathbb{F}_2$ üzerinde ikinci dereceden ve potansiyeli iyi olan herhangi bir özyineli kule tanımlayan bütün $f(X,Y) = 0$ öyle ki $f(X,Y) \in \mathbb{F}_2(X,Y)$ bir rasyonel fonksiyon olan denklemlerin bir sınıflandırmasını verdik. Elde ettiğimiz her denklemin tanımladığı kulenin β_1 değerini hesapladık. Bu değerin birçok kule için sıfır olduğunu gördük. Bu çalışmada elde ettiğimiz bazı kulelerin β_1 değerini henüz elde edemedik. Bu değerlerin hesaplanmasında bazı sorunlarla karşılaştık. Bu sorunlar giderilerek bu kulelerin β_1 değeri hesaplanabilir mi? Elde ettiğimiz bütün kuleler ve bütün $r \geq 1$ için β_r değeri hesaplanabilir mi? Bu kuleleri elde etmek için kullandığımız denklemlerin sınıflandırması metodu $p \geq 3$ asal sayıları için de uygulanabilir mi? gibi olası önerilere de gelecekte bakmak mümkündür.

5. Catalan sayılarının özellikle kombinatorikte sıkça karşımıza çıkmasından dolayı modüler polinomun bu ifadesinde katsayı olarak bulunan Catalan sayılarının daha derin kombinatorik bir açıklaması olduğu aşikardır. (El-Guindy and Papanikolas, 2013; El-Guindy, 2013) çalışmalarında elde edilen sonuçlar da modüler polinomun tanımında bazı kombinatorik öğelerin varlığına işaret etmektedir. Bu bağlantıyı incelemek modüler polinomun aritmetik özellklerini anlamak için önemli bir adım oluşturacaktır. Proje kapsamında $\Phi_T(X,Y)$ modüler polinomunun katsayılarında karşımıza çıkan Catalan sayılarını kombinatorik yönden açıklamaya çalışmak yönünde girişimlerde bulunulmuş olsa da bu yönde tatmin edici bir cevap bulunulamamıştır. Benzer şekilde daha yüksek mertebeden Drinfeld modülleri için mertebe 2 durumundaki modüler polinoma benzer özelliklere sahip yapılar elde etmek yine başka sonlu cisimler üzerinde özyinelemeli bir şekilde tanımlı ve rasyonel noktalarının cinslerine oranının iyi davranış sergilediği eğri dizileri elde etmek için önemli bir adım oluşturacaktır. Çok daha zor ve kapsamlı olan bu soru üzerinde yürütülen çalışmalar ne yazık ki herhangi bir sonuç vermemiştir. Fakat yapılan çalışmalar bu problemlerin daha iyi anlaşılmasına ve bu konuda ileride de çalışmalara devam edilecek üniversitelerarası ve uluslararası ortak çalışmalara sebebiyet vermiş olması açısından çok faydalı olmuştur. Bu alandaki çalışmalara gelecekte de devam edilmesi öngörülmektedir. Oluşan bilgi birikimi ile beraber

gelecekteki ortak çalışmaların sonucunda tatmin edici sonuçlar elde edileneceği umulmaktadır.

6. Bir boyutlu durumda olduğu kadar kapsamlı çalışılmamış olsalar da, çok boyutlu konvolusyonel kodlar da literatürde incelenmişlerdir (Waterhouse, 1969). Bu çalışmanın amacı, sanki-devirsel kodların çok boyutlu benzerlerini tanımlamak ve bir boyutta sanki-devirsel kodlarla konvolusyon kodları arasındaki ilişkinin, çok boyutlu konvolusyon kodları ile çok boyutlu sanki-devirsel kodlar arasında da var olduğunu göstermektir.

Proje kapsamında, proje ekibinin yaptığı sunumlar şunlardır:

1. Sedat Akleylek, Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 8 Ekim 2012.

2. Alp Bassa, Drinfeld modular varieties and curves over finite fields with many points, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 8 Ekim 2012.

3. Seher Tutdere, Non-Asymptotic Lower Bounds for the Class Number of Function Fields over Finite Fields, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 8 Ekim 2012.

4. Dilek Buyruk, Classification of Non-Quadratic Algebraic Function Fields with Class Number Three, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 9 Ekim 2012.

5. Ömer Küçüksakallı, A recursive method for finding generating polynomials of class fields, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 9 Ekim 2012.

6. Dilek Buyruk, Algebraic Function Fields of Class Number Three, Carl von Ossietzky Universität Oldenburg, 4 Aralık 2012.

7. Ömer Küçüksakallı, Computing class number via elliptic units, Carl von Ossietzky Universität Oldenburg, 4 Aralık 2012.

8. Seher Tutdere, On Invariants of Towers and Non-asymptotic Bounds for the Class Number of Function Fields over Finite Fields, Carl von Ossietzky Universität Oldenburg, 4 Aralık 2012.

9. Sedat Akleylek, On the Generalisation of Special Moduli for Faster Interleaved Montgomery Modular Multiplication, Workshop on Algebraic Curves and Cryptography, 18 Temmuz 2013.

10. Ömer Kücüksakalli, Certain CM-class fields with smaller generators, Workshop on Algebraic Curves and Cryptography, 19 Temmuz 2013.

11. Ferruh Özbudak, A short introduction to bent functions, semifields and planar functions, Workshop on Algebraic Curves and Cryptography, 19 Temmuz 2013.

12. Ferruh Özbudak, Non-extendable $\mathbb{F}_q$-quadratic perfect nonlinear maps, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 29 Mayıs 2014.

13. Cem Güneri, Quasi-cyclic and convolutional codes, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 30 Mayıs 2014.

14. Seher Tutdere, Quadratic recursive towers of function fields over $\mathbb{F}_2$, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 30 Mayıs 2014.

Boğaziçi Üniversitesi'nde gerçekleştirilen Workshop on Mathematical Aspects of Curve-Based Cryptography etkinliğinde proje ekiplerinin yanısıra genç araştırmacılar (Dr. Murat Cenk), yüksek lisans ve doktora öğrencileri (Emrah Sercan Yılmaz, ODTÜ ve Buket Özkaya, SabancıÜniversitesi) sunum yapmışlardır.

- Emrah Sercan Yılmaz, Joux's algorithm for discrete logarithms in small characteristic, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 29 Mayıs 2014.

- Murat Cenk, New efficient multiplication algorithms for binary extension fields and applications to curve-based cryptography, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 30 Mayıs 2014.

- Buket Özkaya, Multidimensional quasi-cyclic and convolutional Codes, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 30 Mayıs 2014.

Almanya'daki ortak proje ekibinden (Carl von Ossietzky Universität Oldenburg) gelen proje üyeleri ülkemizde çesitli sunumlar yapmıştır. Bu sunumlar ile ilgili konularda üzerinde fikir alişverişi sağlanmıştır. Bunların detaylarıGelişme raporlarında belirtilmiştir.

1. Felix Braun-Munziger, Jacobians of genus two curves with prime order, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 8 Ekim 2012.

2. Osmanbey Uzunkol, Complex Multiplication and its applications, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 8 Ekim 2012.

3. Max Kronberg, Torsion subgroup of two dimensional abelian varieties with real multiplication, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 9 Ekim 2012.

4. Gerriet Möhlmann, Rank of an elliptic curve and an application in characteristic 2, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 9 Ekim 2012.

5. Wilke Trei, Sieving in hyperelliptic function fields of high genus, Workshop on Mathematical Aspects of Curve-Based Cryptography, ODTÜ, 9 Ekim 2012.

6. Christina Delfs, Isogenies between Supersingular Elliptic Curves over $\mathbb{F}_p$, ODTÜ Genel Seminer, 26 Kasım 2013.

7. Max Kronberg, Rational torsion on hyperelliptic curves of genus two, ODTÜ Genel Seminer, 27 Kasım 2013.

8. Gerriet Möhlmann, Elliptic Curves: Basic properties and relevant questions, SabancıÜniversitesi ve Gebze Yüksek Teknoloji Enstitüsü Genel Seminerler, 10-11 Aralık 2013.

9. Florian Hess, Zeta functions of abelian covers, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 29 Mayıs 2014.

10. Christian Neurohr, Construction of minimal relative quadratric extensions, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 29 Mayıs 2014.

11. Stefan Hellbusch, Riemann-Roch on graphs, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 29 Mayıs 2014.

12. Jan Steffen Müller, Canonical heights on Jacobian surfaces, Workshop on Mathematical Aspects of Curve-Based Cryptography, Boğaziçi Üniversitesi, 29 Mayıs 2014.

13. Stefan Hellbusch, Riemann-Roch on graphs, ODTÜ Genel Seminer, 15 Ekim 2014.

14. Christian Neurohr, Integration on Riemann Surfaces: Homology, ODTÜ Genel Seminer, 15 Ekim 2014.

Proje kapsamında ortaya çıkan sonuçlar aşağıda belirtilen yayınlarda toplanmıştır:

- Ömer Küçüksakallı, Osmanbey Uzunkol, *Certain CM-class fields with smaller generators*, hakem değerlendirilmesinde.
- Henning Stichtenoth, Seher Tutdere, *Quadratic recursive towers of function fields over* $\mathbb{F}_2$, XVI. Antalya Cebir Günleri'nde sunum yapıldı, 9-13 Mayıs 2014, dergiye gönderilme aşamasında.
- Ferruh Özbudak, Zülfükar Saygı, *Rational Points of the Curve* $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ *over* $\mathbb{F}_{q^m}$, Applications of Algebra and Number Theory (Essays in honor to Harald Niederreiter on the occasion of his 70th birthday) Eds: G. Larcher, F.Pillichshammer, A. Winterhof, C. Xing in Cambridge University Press, yayınlanmaya kabul edildi.
- Ferruh Özbudak, Alexander Pott, *Non-extendable* $\mathbb{F}_q$*-quadratic perfect nonlinear maps*, Open Problems in Mathematics and Computational Sciences, Editör Çetin Kaya Koç, ISBN $978-3-319-10682-3$, Springer, yayınlanmaya kabul edildi.
- Ferruh Özbudak, Zülfükar Saygı, *L-polynomials of the curve* $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ *over* $\mathbb{F}_{q^m}$, WAIFI 2014, LNCS, Springer, hakem değerlendirilmesinde.
- Sedat Akleylek, Ferruh Özbudak, *Multiplication in a Galois Ring*, hakem değerlendirilmesinde.

Projenin çıktılarını kısaca özetlemek istersek, zor ve kapsamlı olan "Eğri tabanlı kriptografi" konusu üzerinde yürütülen çalışmalar için bu raporda anlatılan sonuçlar elde edilmiştir. Bunların yanında yapılan çalışmalar bu problemlerin daha iyi anlaşılmasına ve bu konuda ileride de çalışmalara devam edilecek üniversitelerarası ve uluslararası ortak çalışmalara sebebiyet vermiş olması açısından çok faydalı olmuştur. Bu alandaki çalışmalara gelecekte de devam edilmesi öngörülmektedir. Oluşan bilgi birikimi ile beraber gelecekteki ortak çalışmaların sonucunda tatmin edici yeni sonuçlar elde edileneceği umulmaktadır.

Kaynakça

2014. http://www.manypoints.org/.

2014. Pari/gp, version 2.3.2.

Abrahamsson, B. 2004. Architectures for Multiplication in Galois Rings. M.Sc. Thesis, Linköpings Universitat.

Atkin, O. and Morain, F. 1993. Elliptic curves and primality proving. *Math. Comp.* 61:29–67.

Ball, S. and Brown, M. 2004. The six semifield planes associated with a semifield flock. *Advances in Mathematics* 189:68–87.

Bassa, A. 2006. Towers of function fields over cubic fields. Ph.D. Thesis, University of Essen.

Bassa, A. and Beelen, P. 2011. A proof of a conjecture by schweizer on the drinfeld modular polynomial $\phi_t(x, y)$. *Journal of Number Theory* 131:1276–1285.

Bassa, A. and Beelen, P. 2012. A closed form expression for the drinfeld modular polynomial $\phi_t(x, y)$. *Archiv der Mathematik* 99:237–245.

Bassa, A., B. P. G. A. and Stichtenoth, H. 2012. Towers of function fields over non-prime finite fields. *arXiv:1202.5922v2* .

Beelen, P., G. A. and Stichtenoth, H. 2004. On towers of function fields of artin-schreier type. *Bull Braz Math Soc, New Series* 35:151–164.

Beelen, P., G. A. and Stichtenoth, H. 2006. Towards a classification of recursive towers of function fields over finite fields. *Finite Fields Applications* 12:56–77.

Bettner, S. and Schertz, R. 2001. Lower powers of elliptic units. *Journal de Théorie des Nombres de Bordeaux* 13:339–351.

Bezerra, J., G. A. and Stichtenoth, H. 2005. An explicit tower of function fields over cubic finite fields and zink's lower bound. *J. Reine Angew. Math.* 589:159–199.

Blake, I., S. G. and Smart, N. 1999. Elliptic Curves in Cryptography. Cambridge University Press.

Blake, I., S. G. and Smart, N. 2005. Advances in Elliptic Curves in Cryptography. Cambridge University Press.

Bosma, W., C. J. and Playoust, C. 1997. The magma algebra system i: The user language. *Journal Symbolic Computation* 24:235–265.

Carlet, C., Charpin, P., and Zinoviev, V. 1998. Codes, bent functions and permutations suitable for des-like cryptosystems. *IEEE Transactions on Computers* 15:125–156.

Chen, E. 2007. New quasi-cyclic codes from simplex codes. *IEEE Trans. Inform. Theory* 53:1193–1196.

Chen, H. and Cramer, R. 2006. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. *In* Advances in cryptology—CRYPTO LNCS 4117, pp. 521–536. Springer.

Chudnovsky, D. and Chudnovsky, G. 1988. Algebraic complexities and algebraic curves over finite fields. *J. Complexity* 4:285–316.

Coulter, R.S.and Henderson, M. 2008. Commutative presemifields and semifields. *Advances in Mathematics* 217:282–304.

Cox, D. 1989. Primes of the Form $x^2 + ny^2$: Fermat, Class field Theory, and Complex Multiplication. New York, Wiley.

Daskalov, R. and Hristov, P. 2003. New binary one-generator quasi-cyclic codes. *IEEE Trans. Inform. Theory* 49:3001–3005.

Deuring, M. 1958. Die Klassenkörper der komplexen Multiplikation. Enzykl. d. math. Wiss., 2. Auflage.

Dey, B. 2004. On existence of good self-dual quasi-cyclic codes. *IEEE Trans. Inform. Theory* 50:1794–1798.

El-Guindy, A. 2013. Legendre drinfeld modules and universal supersingular polynomials. *arXiv:1308.0855* .

El-Guindy, A. and Papanikolas, M. A. 2013. Explicit formulas for drinfeld modules and their periods. *J. Number Theory* 133:1864–1886.

Enge, A. and Morain, F. 2009. Generalized weber functions i. *Preprint* .

Fan, H. and Hasan, A. 2007. A new approach to subquadratic space complexity parallel multipliers for extended binary fields. *IEEE Transactions on Computers* 56:224–233.

Freeman, D., S. M. and Teske, E. 2010. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology* 23:224–280.

Gaal, I. 2002. Diophantine Equations and Power Integral Bases. Birkhäuser Mathematik.

Garcia, A. and Stichtenoth, H. 1995. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Invent. Math.* 121:211–222.

Garcia, A. and Stichtenoth, H. 1996. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory* 121:248–273.

Garcia, A. and Stichtenoth, H. 1997. On towers and composite of towers of function fields over finite fields. *Finite Fields Applications* 3:257–274.

Garcia, A. and Stichtenoth, H. 2000. Skew pyramids of function fields are asymptotically bad. *In* Cryptography and Related Topics. Proceedings of a Conference in Guanajuato, pp. 111–113.

Gee, A. 2001. Class Fields by Shimura Reciprocity. Ph.D. Thesis, Universiteit Leiden.

Geer, V. and Vlugt, V. 2000. Tables of curves with many points. *Math. Comp.* 69:797–810.

Gekeler, E.-U. 1986. Drinfeld Modular Curves. Lecture Notes in Mathematics Vol. 1231.

Goss, D. 1997. Basic Structures of Function Field Arithmetic. Springer Verlag.

Gulliver, T. and Bhargava, V. 1991. Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes. *IEEE Trans. Inform. Theory* 37:552–555.

Güneri, C. 2004. Artin-schreier curves and weights of two-dimensional cyclic codes. *Finite Fields Appl.* 10:481–505.

Güneri, C. and Özbudak, F. 2008. Multidimensional cyclic codes and artin-schreier type hypersurfaces over finite fields. *Finite Fields Appl.* 14:44–58.

Güneri, C. and Özbudak, F. 2013. The concatenated structure of quasi-cyclic codes and an improvement of jensen's bound. *IEEE Trans. on Inform. Theory* 59:979–985.

Hammons, A.R., K. P. C. A.-S. N. and Sole, P. 1994. The $\mathbb{Z}_4$ linearity of kerdock, preparata, goethals and related codes. *IEEE Transactions on Information Theory* 40:301–319.

Hasegawa, T. 2007. Asymptotic behavior of higher degree places in towers of function fields over finite fields. Ph.D. Thesis, Waseda University, Japan.

Hasse, H. 1927–1931. Neue begründung der komplexen multiplikation i and ii. *J. reine angew. Math.* 157–165:115–139, 64–88.

Hasse, H. 1933. Beweis des analogons der riemannschen vermutung für die artinschen und f.k.schmidtschen kongruenzzetafunktionen in gewissen zyklischen fallen. *Vorlaufige Mitteilung. Nachr. Ges. Wiss. Göttingen I. Math.-Phys. Kl. Fachgr. I Math.* 42:253–262.

Herglotz, G. 1921. Über das quadratische reziprozitätsgesetz in imaginären quadratischen zahlkörpern. *Leipzig Ber.* 73:303–310.

Hess, F., S. H. and Tutdere, S. 2013. On invariants of towers of function fields over finite fields. *Journal of Algebra and Its Applications* 12:477–487.

Hirschfeld, J.W.P., K. G. and Torres, F. 2008. Algebraic curves over a finite field. Princeton University Press, Princeton, NJ.

Huppert, B. B. N. 1982. Finite Groups II. Springer-Verlag.

Ihara, Y. 1982. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28:721–724.

Ikai, T., K. H. and Kojima, Y. 1975. Two-dimensional cyclic codes. *Electronics and Communications in Japan* 57:27–35.

Imai, H. 1977. A theory of two-dimensional cyclic codes. *Information and Control* 34:1–21.

Ishai, Y., K. E. O. R. and Sahai, A. 2009. Zero-knowledge proofs from secure multiparty computation. *SIAM J. Comput.* 39:1121—-1152.

Jensen, J. 1985. The concatenated structure of cyclic and abelian codes. *IEEE Trans. on Inform. Theory* 31:788–793.

Jung, H.L., K. J. K. and Shin, D. H. 2011. Ray class invariants over imaginary quadratic fields. *Tohoku Math. J.* 63:413–426.

Kasami, T. 1974. A gilbert-varshamov bound for quasi-cyclic codes of rate 1/2. *IEEE Trans. on Inform. Theory* 20:679.

Klapper, A. 1997. Cross-correlations of quadratic form sequences in odd characteristic. *Designs, Codes and Cryptography* 11:289–305.

Klebel, M. 1996. Zur Theorie der Potenzganzheitzbasen bei relativen galoischen Zahlkörpern. Dissertation, Universität Augsburg.

Knuth, D. 1965. Finite semifields and projective planes. *Journal of Algebra* 2:153–270.

Krishna, H., K. B. and Lin, K.-Y. 1994a. Rings, fields, the chinese remainder theorem and an extension-part i: Applications to digital signal processing. *IEEE Transactions on Circuits and Systems-II: Analog and Digital, Signal Processing* 41:656–668.

Krishna, H., K. B. and Lin, K.-Y. 1994b. Rings, fields, the chinese remainder theorem and an extension-part i: Theory. *IEEE Transactions on Circuits and Systems-II: Analog and Digital, Signal Processing* 41:641–655.

Krishna, H., K. B. L. K.-Y. and Sun, J. 1995. Computational Number Theory and Digital Signal Processing. Boca Raton, CRC Press.

Küçüksakalli, O. 2011. Class numbers of ray class fields of imaginary quadratic fields. *Math. Comp.* 80:1099–1122.

Küçüksakalli, O. 2013. Class fields of arbitrary orders of imaginary quadratic number fields with smaller generators. *in preparation* .

Lally, K. 2006. Algebraic lower bounds on the free distance of convolutional codes. *IEEE Trans. on Inform. Theory* 52:2101–2110.

Lang, S. 1987. Elliptic Functions. Springer-Verlag, Graduate Texts in Math.

Laudera, A. G. and Wan, D. 2002. Computing zeta functions of artin-schreier curves over finite fields. *Journal of Complexity* 5:34–55.

Lebacque, P. 2007. Sur quelques proprietes asymptotiques des corps globaux. Ph.D. Thesis, Université de Marseille II, France.

Lenstra, H. W. J. 2002. On a problem of garcia, stichtenoth, and thomas. *Finite Fields and Their Applications* 8:166–170.

Leprévost, F., P. M. E. and Uzunkol, O. 2011. On the computation of class polynomials with "thetanullwerte" and its applications to the unit group computation. *Experimental Mathematics* 20:271–281.

Ling, S. and Solé, P. 2001. On the algebraic structure of quasi-cyclic codes i: finite fields. *IEEE Trans. on Inform. Theory* 47:2751–2760.

Ling, S. and Solé, P. 2003. Good self-dual quasi-cyclic codes exist. *IEEE Trans. on Inform. Theory* 49:1052–1053.

Lint, H. v. 1999. Introduction to Coding Theory. Springer.

Manin, Y. I. 1963. The theory of commutative formal groups over fields of finite characteristic. *Uspekhi Mat. Nauk* 18:6:3–90.

McEliece, R. 1998. Handbook of Coding Theory: The algebraic theory of convolutional codes. North-Holland, Amsterdam.

Morain, F. 2007. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Math. Comp.* 76:493–505.

Niederreiter, H. and Xing, C. 2001. Rational points on Curves over Finite Fields: Theory and Applications. Cambridge University Press.

Niederreiter, H. and Xing, C. 2009. Algebraic Geometry in Coding Theory and Cryptography. Princeton University Press.

Özbudak, F. and Pott, A. 2014. Uniqueness of F_q-quadratic perfect nonlinear maps from F_{q^3} to F_q^2. *Finite Fields and Their Applications* 29:49–88.

Özbudak, F. and Pott, A. 2015. Non-extendable F_q-quadratic perfect nonlinear maps. *In* Open Problems in Mathematics and Computational Sciences. Springer.

Özbudak, F. and Saygi, Z. 2014. Rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbb{F}_{q^m}$. *In* Applied Algebra and Number Theory. Cambridge University Press.

Ramachandra, K. 1964. Some applications of kronecker's limit formula. *Ann. of Math. 2* 80:104–148.

Rück, H.-G. 1987. A note on elliptic curves over finite fields. *Math. Comp.* 49:301–304.

Rück, H.-G. and Stichtenoth, H. 1994. A characterization of hermitian function fields over finite fields. *J. Reine Angew. Math.* 457:185–188.

Saints, K. and Heegard, C. 1993. Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using gröbner bases. *IEEE Trans. on Inform. Theory* 41:1733–1751.

Schertz, R. 1997. Construction of ray class fields by elliptic units. *Journal de Théorie des Nombres de Bordeaux* 9:383–394.

Shimura, G. 1971. Introduction to the Arithmetic Theory of Automorphic Functions. Princeton University Press.

Shparlinski, I.E., T. M. A. and Vladut, S. G. 1991. Curves with many points and multiplication in finite fields. Coding theory and algebraic geometry, Luminy.

Silverman, J. 1994. Advanced Topics in the Arithmetic of Elliptic Curves. Springer Verlag.

Stark, H. 1980. l-functions at $s = 1$. iv. first derivatives at $s = 0$. *Adv. in Math.* 35:197–235.

Stevenhagen, P. 2001. Hilbert's 12th problem, complex multiplication and shimura reciprocity. *Advanced Studies in Pure. Math. 30, 'Class Field Theory - its centenary and prospect'* pp. 161–176.

Stichtenoth, H. 1979. Die hasse-witt-invariante eines kongruenzfunktionenkorpers. *Arch. Math.* 33:357–360.

Stichtenoth, H. 2000. Algebraic Function fields and Codes. Springer-Verlag.

Stichtenoth, H. 2009a. Algebraic function fields and codes. 2nd Edition, Springer-Verlag.

Stichtenoth, H. 2009b. Algebraic function fields and codes. Graduate Texts in Mathematics 254, Springer Verlag.

Stichtenoth, H. and Tutdere, S. . 2014. Recursive artin-schreier towers of function fields over F_2. *In* XVI. Antalya Algebra Days, May 9-13 2014, Antalya, Turkey.

Tate, J. 1966. Endomorphisms of abelian varieties over finite fields. *Invent. Math.* 2:134–144.

Thakur, D. 2004. Function Field Arithmetic. World Scientific.

Tsfasman, M. and Vladut, S. 1991. Algebraic-geometric codes. Kluwer Academic Publishers Group.

Tsfasman, M., Vladut, S., and Nogin, D. 2007. Algebraic Geometric Codes: Basic Notations. American Mathematical Society- Providence.

Tsfasman, M. A. 1992. Some remarks on the asymptotic number of points. *Lecture Notes in Mathematics* 1518:178–192.

Tsfasman, M.A., V. S. and Nogin, D. 2007. Algebraic geometric codes: basic notions. American Mathematical Society, Providence, RI.

Tsfasman, M.A., V. S. and Zink, T. 1982. Modular curves, shimura curves and goppa codes, better than the varshamov–gilbert bound. *Math. Nachr.* 109:21—-28.

Tutdere, S. 2009a. On the asymptotic theory of towers of function fields over finite fields. Ph.D. Thesis, Sabancı University.

Tutdere, S. 2009b. A recursive tower of function fields over $\mathbb{F}_2$. M.Sc. Thesis, Sabancı University.

Uzunkol, O. 2013. Generalized class invariants with 'thetanullwerte'. *Turk. J. Math.* 37:165–181.

Villa Salvador, S. 2006. Topics in the theory of algebraic function fields. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA.

Vladuts, S. and Drinfeld, V. 1983. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.* 1:68–69.

Voloch, J. 1989. A note on elliptic curves over finite fields. *Bull. Soc. Math. France* 116:455–458.

Washington, L. 1997. Introduction to Cyclotomic Fields. Springer Verlag.

Waterhouse, W. 1969. Abelian varieties over finite fields. *Ann. Sci. Ecole Norm.* 2:521–560.

Weil, A. 1948. Sur les courbes algebriques et les varietes qui s'en deduisent. *Act. Sc. et Ind.* 1041.

Winograd, S. 1980. Arithmetic Complexity of Computations. SIAM.

Zink, T. 1985. Degeneration of shimura surfaces and a problem in coding theory. *Fundamentals of computation theory, LNCS 199* 1041:503–511.

Mathematical Aspects of Curve Based Cryptography
May 29-30, 2014

Istanbul Center for Mathematical Sciences (IMBM), Bogazici University
(http://www.imbm.org.tr/contact.htm).

Organisers: Alp Bassa (alpbassa@gmail.com), Cem Güneri (guneri@sabanciuniv.edu), Seher Tutdere (stutdere@gmail.com)

The workshop includes constructive and algorithmic topics from finite fields, algebraic curves, coding theory and cryptography. The setting will be rather informal with sufficient time for discussions between the talks and on Friday afternoon. Participation is free of charge and everybody who is interested in attending is very welcome to do so. We ask however for a short notice to provide enough coffee, cookies and the like.
The workshop is supported by a BMBF (Federal Ministry of Education and Research, Germany) -TÜBİTAK project on mathematical aspects of curve-based cryptography (No: 112T011)

Speakers:

Murat Cenk (Middle East Technical University)
Cem Güneri (Sabancı University)
Stefan Hellbusch (Carl von Ossietzky University of Oldenburg)
Florian Hess (Carl von Ossietzky University of Oldenburg)
Jan Steffen Müller (Carl von Ossietzky University of Oldenburg)
Chrisitan Neurohr (Carl von Ossietzky University of Oldenburg)
Ferruh Özbudak (Middle East Technical University)
Buket Özkaya (Sabancı University)
Seher Tutdere (Gebze Institute of Technology)
Emrah Sercan Yılmaz (Middle East Technical University)

Program

Thursday, 29 May

10:15 - 10:30	Opening remarks
10:30 - 11:20	Florian Hess, Zeta functions of abelian covers
11:20 - 11:40	Coffee break

11:40 - 12:10	Christian Neurohr, Construction of minimal relative quadratric extensions
12:15 - 12:45	Stefan Hellbusch, Riemann-Roch on graphs
12:45 - 14:30	Lunch break
14:30 - 15:20	Jan Steffen Müller, Canonical heights on Jacobian surfaces
15:20 - 15:40	Coffee break
15:40 - 16:10	Emrah Sercan Yılmaz, Jouxs algorithm for discrete logarithms in small characteristic
16:10 - 16:40	Ferruh Özbudak, Non-extendable $\mathbb{F}_q$-quadratic perfect nonlinear maps
16:40 -	Free time for discussions.
.....	Dinner

Friday, 30 May

10:00 - 10:50	Murat Cenk, New efficient multiplication algorithms for binary extension fields and applications to curve-based cryptography
10:50 - 11:10	Coffee break
11:10 - 11:40	Cem Güneri, Quasi-cyclic and convolutional codes
11:40 - 12:10	Buket Özkaya, Multidimensional quasi-cyclic and convolutional Codes
12:10 - 12:20	break
12:20 - 12:50	Seher Tutdere, Quadratic recursive towers of function fields over $\mathbb{F}_2$
12:50 - 14:00	Lunch break
14:00 -	Free time for discussions.

Abstracts of talks

Murat Cenk, Middle East Technical University

New efficient multiplication algorithms for binary extension fields and applications to curve-based cryptography

The most needed arithmetic operation for the curve-based cryptography over binary fields is the efficient multiplication algorithms, and many research have been performed over the past decade for developing new multiplication algorithms for these kind of fields. In this talk, the best known algorithms for this aim are discussed. After being explained the requirements and cost metrics for cryptographic applications, algebraic and computer scientific methods that significantly improve the best known methods are presented.

Cem Güneri, Sabancı University

Quasi-cyclic and convolutional codes

We will give the basic algebraic structure of quasi-cylic codes and convolutional codes. The main difference between these families is that convolutional codes are not block codes. After introducing these codes, we will sketch the proof of a result which relates the free distance of a convolutional code to the minimum distance of an associated quasi-cyclic code. This talk will provide the background for the talk of Buket Ozkaya.

Stefan Hellbusch, Carl von Ossietzky University of Oldenburg

Riemann-Roch on graphs

We all know the Riemann-Roch theorem. I will talk about an analogue on a finite graph by M. Baker and S. Norine in [2] and related results of F. Shokrieh [3] and myself [1]. As in the classic case, we get divisors, an equivalence relation and a (abelian) divisor class group, which is the quotient group of degree 0 divisors and principal divisors. When fixing a base vertex, in each equivalence class there is exactly one reduced divisor and the divisor reduction is related with an interesting, so called, unconstrained chip firing game. Using Dhar's Burning Algorithm, the reduction can be done fast and we get an efficient arithmetic in the divisor class group. We will see some examples and conclude, that for each finite abelian group, there is a graph with this group as divisor class group. We also give a short view on a cryptographic perspective and contrary to F. Shokrieh in [3], we conclude that there are graphs suitable for cryptography.

References

[1] Stefan Hellbusch, Riemann-Roch Theorie auf Graphen und Anwendungen, 2013

[2] Matthew Baker, Serguei Norine, Riemann-Roch and Abel-Jacobi Theory on a finite Graph, 2007

[3] Farbod Shokrieh, The monodromy pairing and discrete logarithm on the Jacobian of finite graphs, 2010

Florian Hess, Carl von Ossietzky University of Oldenburg

Zeta functions of abelian covers

The computation of zeta functions of curves over finite fields has attracted a lot of interest in the last years with the main focus being on methods based on p-adic cohomology. In this talk I will not use p-adic cohomology, but class field theory to represent curves with large abelian automorphism groups. Based on this I describe a method to compute the zeta function via Artin L-series which is asymptotically close to optimal. The practical efficiency of the method will be demonstrated on the computer by some explicit examples.

Jan Steffen Müller, Carl von Ossietzky University of Oldenburg

Canonical heights on Jacobian surfaces

The canonical height is a quadratic form on the Mordell-Weil group of an abelian variety defined over a global field which measures the arithmetic complexity of a point. For several arithmetic applications, such as computing generators of the Mordell-Weil group and its regulator (which appears in the conjecture of Birch and Swinnerton-Dyer), it is crucial to have algorithms for computing the canonical height and for bounding its difference from the naive height. I will report on joint work in progress with Michael Stoll on such algorithms in the case of Jacobian surfaces.

Christian Neurohr, Carl von Ossietzky University of Oldenburg

Construction of minimal relative quadratric extensions

For a given transitive group and a signature, one wants to find the corresponding number field with minimal absolute discriminant. This can be done algorithmically by constructing all such number fields up to certain bounds. The method presented here targets imprimitive, transitive

groups of even degree, that have a subgroup of order 2.

Ferruh Özbudak, Middle East Techical University

Non-extendable $\mathbb{F}_q$-quadratic perfect nonlinear maps

Let q be a power of an odd prime. We give examples of non-extendable $\mathbb{F}_q$-quadratic perfect nonlinear maps. We also show that many classes of $\mathbb{F}_q$-quadratic perfect nonlinear maps are extendable. We also give a short survey of some of our recent results, which use some tools from algebraic curves over finite fields.
This is a report on a joint work with Alexander Pott.

Buket Özkaya, Sabancı University

Multidimensional Quasi-Cyclic and Convolutional Codes

Multidimensional generalization of convolutional codes have been introduced by Weiner. In this talk, we will define multidimensional generalization of quasi-cyclic codes and describe their algebraic structure. It turns out that the codes we introduce are right generalizations to obtain a relation with multidimensional convolutional codes, which exists in the classical 1D setting.

Seher Tutdere, Gebze Institute of Technology

Quadratic recursive towers of function fields over $\mathbb{F}_2$

Let $\mathbb{F}_q$ be a finite field ($q = p^k$ with p a prime and $k \geq 1$ an integer) and $F/\mathbb{F}_q$ be an algebraic function field of one variable with the field $\mathbb{F}_q$ as its full constant field. We denote by $B_r(F)$ and $g(F)$ the number of places of degree r for any positive integer r and the genus of $F/\mathbb{F}_q$, respectively. When $r = 1$, for all $k \geq 2$ and when $r \geq 2$, for all $k \geq 1$ there are many examples of recursive towers $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$ with positive limit $\beta_r(\mathcal{F}) = \lim_{n\to\infty} B_r(F_n)/g(F_n)$. However, it is not known whether there are any recursive towers over prime fields with positive β_1. We call a recursive tower $\mathcal{F} = (F_n)_{n\geq 0}$ a tower of degree p if each extension F_{n+1}/F_n (with $n \geq 0$) is an extension of degree p. In this talk we discuss all polynomials which define recursive quadratic towers over the field $\mathbb{F}_2$ (i.e., towers of degree 2) and the limit β_r of those towers for all $r \geq 1$.
This is a joint work with Henning Stichtenoth.

Emrah Sercan Ylmaz, Middle East Technical University

Jouxs Algorithm for Discrete Logarithms in Small Characteristic

Joux described a new algorithm for discrete logarithms in small characteristic. This algorithm is based on index calculus and a new method for generating multiplicative relations among elements of a small smoothness basis and a new descent strategy that allows to express the logarithm of an arbitrary finite field element in terms of the logarithm of elements from the smoothness basis.

TÜBİTAK
PROJE ÖZET BİLGİ FORMU

Proje Yürütücüsü:	Prof. Dr. FERRUH ÖZBUDAK
Proje No:	112T011
Proje Başlığı:	Eğri Tabanlı Kriptografiye Matematiksel Bakış
Proje Türü:	Uluslararası
Proje Süresi:	24
Araştırmacılar:	HENNİNG STİCHTENOTH, SEDAT AKLEYLEK, ÖMER KÜÇÜKSAKALLI, CEM GÜNERİ, ALP BASSA, DİLEK BUYRUK, SEHER TUTDERE
Danışmanlar:	
Projenin Yürütüldüğü Kuruluş ve Adresi:	ORTA DOĞU TEKNIK Ü. UYGULAMALI MATEMATİK ENSTİTÜSÜ
Projenin Başlangıç ve Bitiş Tarihleri:	15/09/2012 - 15/09/2014
Onaylanan Bütçe:	44000.0
Harcanan Bütçe:	18923.47
Öz:	Eliptik eğri tabanlı kriptografide belirli sayıda noktası olan bir eliptik eğri bulmak önemli bir uygulamadır. Ayrıca, kriptografi ve kodlama teorisindeki uygulamalar için çok rasyonel noktaya sahip eğrilere ihtiyaç duyulduğundan maksimal eğriler ve çok rasyonel noktaya sahip eğrilerin önemi aşikardır. Bunlara ek olarak, bu eğrilerin tanımlandığı yapılar üzerindeki aritmetiğin hızlandırılması güncel bir konudur. Cebirsel egrilerin kriptografi ve kodlama teorisinde çok önemli uygulamaları vardır. Bu uygulamalarda sonlu cisimlerin çesitli özellikleri ve bazı kombinatorik yöntemler kullanılır. Bu final raporunda, sonlu cisimler üzerindeki cebirsel eğrilerin cinslerini ve rasyonel nokta sayılarını bulma üzerine sonuçlar, mükemmel lineer olmayan fonksiyonların sınıfları ve bunların yarıcisimlerler olan ilişkileri, sonlu cisimler üzerindeki bazı cebirsel eğrilerin $L-$polinomları, Galois halkalarındaki aritmetik işlemleri, cebirsel fonksiyon cisimleri, ikinci dereceden kompleks sayı cisimlerinin dallanmış (ramified) genişlemelerinde minimal polinomlarının katsayıları küçük olan özel elemanlar ve eşleniklerinin hesaplanması, çok boyutlu sanki-devirsel ve konvolusyon kodları, sonlu cisimler üzerinde kuadratik lineer olmayan eşlemeler hakkında proje kapsamında yapılanlar belirtilmiştir.
Anahtar Kelimeler:	cebirsel eğri, kriptografi, polinom çarpımı, kuadratik form, kompleks sayı cisimleri, $L-$polinomu
Fikri Ürün Bildirim Formu Sunuldu Mu?:	Hayır