T. C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MODÜLER FORMLAR, ELİPTİK EĞRİLER VE UYGULAMALARI

İlker İNAM

Prof. Dr. Osman BİZİM
(Danışman)

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA–2011

TEZ ONAYI

İlker İNAM tarafından hazırlanan "Modüler Formlar, Eliptik Eğriler ve Uygulamaları" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Danışman : Prof. Dr. Osman BİZİM

Üye: Prof. Dr. Osman BİZİM İmza
Uludağ Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Üye: Prof. Dr. İsmail Naci CANGÜL İmza
Uludağ Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Üye: Prof. Dr. Gökay KAYNAK İmza
Uludağ Üniversitesi Fen Edebiyat Fakültesi
Fizik Anabilim Dalı

Üye: Doç. Dr. Recep ŞAHİN İmza
Balıkesir Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Üye: Yrd. Doç. Dr. Kazım BÜYÜKBODUK İmza
Koç Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Kadri ARSLAN

Enstitü Müdürü

U.Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

../../….

İmza

İlker İNAM

ÖZET

Doktora Tezi

MODÜLER FORMLAR, ELİPTİK EĞRİLER VE UYGULAMALARI

İlker İNAM

Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Osman BİZİM

Bu çalışmada matematiğin son dönemdeki popüler iki teorisi, Eliptik Eğriler ve Modüler Formlar ele alınmıştır. İspatlandıktan sonra "Modülarite Teoremi" adını alan Taniyama-Shimura-Weil Konjektürü sayesinde birbirine bağlanan bu iki teorinin çeşitli uygulamaları mevcuttur. Bu çalışmada, bu teorilerin birbirleriyle olan ilişkisi kullanılarak Eliptik Eğriler Teorisi'nde yer alan bir açık problem, Modüler Formlar Teorisi kullanılarak çözülmüştür. Birinci bölümde, çalışmanın ilerleyen kısımlarında kullanılacak olan bazı kavramlar tanıtılmıştır. İkinci bölümde Eliptik Eğriler Teorisi'ne giriş yapılmış, sonlu cisimler üzerinde tanımlı bazı eliptik eğri aileleri hakkında elde edilen sonuçlar verilmiştir. Bu bölümün son kısmında $\mathbb{Q}$ üzerinde tanımlı eliptik eğrilerin özellikleri ele alınmış ve bazı uygulamalar yapılmıştır. Üçüncü bölüm modüler formlara ayrılmıştır. Tamsayı ve yarım tamsayı ağırlıklı formlar tanıtılmış, bu formlar üzerindeki Hecke operatörlerinin tanımları verilmiştir. Bu bölüm yukarıda adı geçen Modülarite Teoremi'nin ifadesinin verilmesi ile sona ermiştir. Çalışmanın temelini oluşturan dördüncü ve son bölümünde, rastgele seçilen bir eliptik eğrinin Selmer grubunun mertebesinin hesaplanması problemi ele alınmıştır. Literatürde bu haliyle çözümü bulunmayan problem eliptik eğrilerin twist ailelerine kısıtlanarak modüler formların analitik fonksiyonlar olması özelliği yardımıyla kısmen çözülmüştür. Bunun için matematiğin ödüllü konjektürlerinden Birch ve Swinnerton-Dyer Konjektürü'nün doğru olduğu kabul edilmiş ve J. L. Waldspurger'in önemli bir teoremi kullanılmıştır. Hesaplanan Selmer grubu mertebelerinin dağılımı basit bir fonksiyon yardımıyla ifade edilmiştir.

Anahtar Kelimeler: Eliptik Eğriler, Modüler Formlar, Yarım Tamsayı Ağırlıklı Modüler Formlar, Eliptik Eğrilerin Selmer Grupları
2011, vii + 87 sayfa.

ABSTRACT

PhD Thesis

MODULAR FORMS, ELLIPTIC CURVES AND THEIR APPLICATIONS

Ilker INAM

Uludağ University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Prof. Dr. Osman BIZIM

In this work, two recent popular theories of mathematics, namely Elliptic Curves and Modular Forms are discussed. The Taniyama-Shimura-Weil Conjecture which is also named as "Modularity Theorem" after proven, connects these two theories and it has various applications. Using the relationship of these theories an open problem on the Theory of Elliptic Curves is solved by Modular Forms Theory. In the first chapter of the work, some of the concepts which will be used later are introduced. In the second chapter, the theory of elliptic curves is introduced and some results for the families of elliptic curves over finite fields are obtained. In the last section of this chapter, the properties of the elliptic curves defined over rational numbers were observed and some applications are given. The third chapter is reserved for modular forms. Integer and half-integer weight forms are introduced and also the definition of Hecke operator is given. This chapter ended with the statement of Modularity Theorem which is mentioned above. The fourth and final chapter of the work which is the essential part of this thesis, the problem of computing the order of the Selmer group of a randomly selected elliptic curve is considered. In this case, there is no solution of this problem in the literature but restricting twist families of elliptic curves, this problem is partly solved by using the fact that modular forms are analytic functions. While this problem is being solved, it is assumed that one of the award-winning conjectures of the mathematics called the Birch and Swinnerton-Dyer Conjecture is true and an important theorem of J. L. Waldspurger is used. The distribution of the computed orders of Selmer groups expressed with a simple function.

Key words: Elliptic Curves, Modular Forms, Half-Integral Weight Forms, Selmer Groups of Elliptic Curves
2011, vii + 87 pages.

ÖNSÖZ VE TEŞEKKÜR

Matematik dahil olmak üzere birçok bilim dalında doktora sonrası çalışmaları da kapsayacak şekilde "önü açık" bir doktora tezi konusu ve problemi bulmak çok önemli, önemli olduğu kadar da oldukça zordur. Bu bağlamda Eliptik Eğriler ve Modüler Formlar gibi son senelerin popüler konularından birisini tez konum olarak belirleyen, bu çalışmanın ortaya çıkışında her türlü desteğini ve fedakarlığını esirgemeyen danışman hocam Sayın Prof. Dr. Osman BİZİM'e şükranlarımı sunarım. Benim gibi zor bir öğrencinin doktora öğrenimi boyunca kimi zaman düştüğü umutsuzlukların üstesinden gelmesi için elinden geleni yapan değerli hocamın katkıları yadsınamaz. Ekim 2008-Mart 2009 tarihleri arasında Erasmus öğrenci değişimi programı kapsamında beni Duisburg-Essen Üniversitesi'nde ağırlayan Prof. Dr. Gerhard Frey'e ve tüm sorularımı bıkmadan usanmadan e-mail yoluyla cevaplayan Prof. Dr. Gabor Wiese'ye teşekkürü bir borç bilirim. Bana birçok konuda yardımcı olan ve yurtdışına açılmamı sağlayan Prof. Dr. İsmail Naci CANGÜL'e, bana destek olan oda arkadaşım Araş. Gör. Aysun YURTTAŞ'a teşekkür ederim. Doktora tezimi 107T311 numaralı araştırma projesi ile destekleyen TÜBİTAK'a şükranlarımı sunuyorum.

Çalışmanın arka planında olmasına rağmen bana sürekli destek olan ve ona ayırmam gereken zamandan fedakarlık eden sevgili eşim Betül İNAM'a, beni bugünlere getiren kıymetli anne ve babam ile sevgili kardeşim Ayşegül İNAM'a ayrıca teşekkür ederim.

Bu çalışma doktora öğrenimim sırasında kaybettiğim rahmetli dedem, anneannem ve özellikle büyükbabama ithaf edilmiştir.

İlker İNAM
.. / .. / ….

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler/Kısaltmalar	Açıklama
Aut(A)	A nın otomorfizmlerinin grubu
E/F	E, F cisminin bir cisim genişlemesi
$\mathrm{Aut}_F(E)$	E/F nin tüm otomorfizmlerinin kümesi
Gal(E/F)	E nin F üzerindeki Galois grubu
M^G	M nin G-invaryant alt grubu
$O = [0, 1, 0]$	Sonsuzdaki nokta
	E eliptik eğrisinin diskriminantı
j	E eliptik eğrisinin j-invaryantı
	E eliptik eğrisi ile eşleşen invaryant diferensiyel
$\oplus$	E eliptik eğrisi üzerindeki toplama işlemi
Q_p	$\mathbb{F}_p$ de ikinci dereceden kalanların kümesi
$E(\mathbb{Q})$	E eliptik eğrisi üzerindeki rasyonel noktaların kümesi
$E_{tors}(\mathbb{Q})$	E eliptik eğrisinin torsiyon alt grubu
r	E eliptik eğrisinin rankı
$L_E(s)$	E eliptik eğrisinin L-serisi
N_E	E eliptik eğrisinin kondüktörü
$GL_2(R)$	Genel lineer grup
$SL_2(R)$	Özel lineer grup
$\widetilde{\mathbb{C}}$	Riemann küresi
$SL_2(\mathbb{Z})$,	Modüler grup
$PSL_2(\mathbb{R})$	Projektif özel lineer grup
$(\ )$	Temel denklik alt grubu
$_0(\ )$, $_1(\ )$	Hecke tipindeki modüler gruplar
$M_k(\ )$	k-ağırlıklı modüler formların uzayı
$S_k(\ )$	k-ağırlıklı cusp formların uzayı
T_m	m. Hecke operatörü
$Sha_{\mathbb{Q}}(E)$	E eliptik eğrisinin Tate-Shafarevich grubu
$S_{\mathbb{Q}}(E)$	E eliptik eğrisinin Selmer grubu
[:]	İndeks
Re(z)	z karmaşık sayısının gerçel kısmı
İm(z)	z karmaşık sayısının sanal kısmı
$\backslash M_m$	M_m nin orbit uzayı

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bu kısımda çalışmanın ilerleyen bölümlerinde kullanılacak olan bazı temel kavramlar tanıtılacaktır. Oldukça derin teorilere dayanan bu kavramlarla ilgili ayrıntılar tanımların alındığı (Weibel 1994), (Lang 2002), (Fried ve Jarden 2004), (Spanier 1995), (Brown 1972), (Serre 1979) ve (Serre 2002) kaynaklarında bulunabilir.

1.1 Tanım. R bir halka, A toplamsal bir abel grubu olsun.

$$R \times A \to A, (r, x) \mapsto r \cdot x$$

biçiminde tanımlanan dönüşüm her $r, s \in R$, her $x, y \in A$ için

i. $r \cdot (x + y) = r \cdot x + r \cdot y$

ii. $(r + s) \cdot x = r \cdot x + s \cdot x$

iii. $(r \cdot s)x = r \cdot (s \cdot x)$

iv. $1_R \cdot x = x$ (eğer R nin 1_R elemanı varsa)

özelliklerini gerçekliyorsa bu dönüşümle birlikte A grubuna bir *sol R-modülü* adı verilir.

1.2 Tanım. G bir çarpımsal grup, A toplamsal bir abel grubu olsun. $Aut(A)$, A nın otomorfizmlerinin grubunu göstermek üzere G den $Aut(A)$ ya tanımlı bir homomorfizm bulunabiliyor ise *G grubu A nın sol tarafında hareket ediyor* denir.

Bu tanım aslında,

$$G \times A \to A, (s, x) \mapsto s \cdot x$$

biçiminde tanımlanan dönüşümün

$$1 \cdot a = a$$

$$s \cdot (a + a') = s \cdot a + s \cdot a'$$

$$(s \cdot t) \cdot a = s \cdot (t \cdot a)$$

özelliklerine sahip olduğunu gösterir, bu dönüşümle birlikte A grubuna *bir sol G-modülü* adı verilir.

1.3 Tanım. G_0, G_1, …, G_n gruplar ve f_1, f_2, …, f_n, $f_i : G_{i-1} \to G_i$ özelliğindeki grup homomorfizmleri olsun. Eğer her bir homomorfizmin görüntüsü ardışık homomorfizmin çekirdeği oluyor ise

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \ldots \xrightarrow{f_n} G_n$$

dizisine bir *tam dizi* denir.

1.4 Uyarı 1. Tanıma dikkat edilirse $f_{i+1} \circ f_i \equiv 0$ dır.

2. Uygulamada gruplar-grup homomorfizmleri yanında vektör uzayları-lineer dönüşümler, modüller-modül homomorfizmleri, çiftleri için de tam dizi kavramı kullanılabilmektedir.

3. Bir tam dizi sonlu sayıda grup ve homomorfizmden oluşabildiği gibi dizideki grup ve homomorfizmlerin sayısı sonlu olmak zorunda değildir.

1.5 Tanım. Başlangıcı ve sonu $\{0\}$ aşikar modülünden oluşan beş elemanlı tam diziye *kısa tam dizi* adı verilir. Sonsuz elemanlı tam diziye ise *uzun tam dizi* adı verilir.

1.6 Örnek. $G_i = \mathbb{Z} / 4\mathbb{Z}$ ve $f_i(x),\ x \mapsto 2 \cdot x$ olarak alınırsa

$$\ldots \xrightarrow{\times 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\times 2} \ldots$$

bir uzun tam dizi olur. Gerçekten de her bir adımda çekirdek ve görüntü $\{0, 2\}$ alt grubundan başka bir şey değildir.

1.7 Uyarı. E, F cisminin bir cisim genişlemesi olsun ve bu durum E/F ile gösterilsin. E/F nin tüm otomorfizmlerinin kümesi $Aut_F(E)$ olmak üzere, $Aut_F(E)$ fonksiyonların bileşkesi işlemine göre bir grup oluşturur.

1.8 Tanım. Eğer E/F bir Galois genişlemesi ise $Aut_F(E)$ grubuna *E nin F üzerindeki Galois grubu* denir ve bu grup Gal(E/F) ile gösterilir. Özel olarak, $\overline{F}$, F cisminin

cebirsel kapanışı olmak üzere, F nin cisim genişlemesi $\overline{F}$ olsun. F cismini sabit bırakan tüm otomorfizmlerinin Galois grubuna *F nin mutlak Galois grubu* denir.

1.9 Uyarı. G sonlu bir grup olsun. Her $g \in G$ ve $x \in M$ için $f(gx) = g(fx)$ özelliğindeki grup homomorfizmleri ile birlikte tüm G-modüllerinin koleksiyonu bir kategori olur. G-modüllerinin bu kategorisi yeterli içine dönüşümlerle birlikte bir abelyen kategori olur.

1.10 Tanım. C ve D iki kategori olmak üzere

$$F : C \to D$$

dönüşümü verilsin. Her bir $X \in C$ için $F(X) \in D$ ve her bir $f : X \to Y \in C$ morfizmi için

i. Her $X \in C$ için $F(I_X) = I_{F(X)}$

ii. Her $f : X \to Y$ ve $g : Y \to Z$ için

$$F(g \circ f) = F(g) \circ F(f)$$

olacak biçimde bir $F(f) : F(X) \to F(Y) \in D$ morfizmi var ise F ye C den D ye bir *funktor* denir.

1.11 Tanım. M bir G-modülü olsun. M nin

$$M^G := \{ x \in M : \text{her } g \in G \text{ için } gx = x \}$$

biçiminde tanımlanan alt grubuna *G-invaryant alt grubu* denir.

1.12 Tanım. Her bir M G-modülünü kendisinin G-invaryant bir alt grubuna resmeden dönüşüm bu kategoriden abelyen kategoriye bir funktor belirtir. Bu funktor sol tamdır, ancak sağ tam olmak zorunda değildir. Böylece bu funktorların sağ türetilmiş funktorları oluşturabilir. Bu funktorların değer kümeleri abel gruplarıdır. Bu grup $H^n(G, M)$ ile gösterilir ve G nin katsayıları M de olan *n. kohomoloji grubu* adı verilir. Özel olarak G bir Galois grubu ise $H^n(G, M)$ ye *n. Galois kohomoloji grubu* denir.

1.13 Tanım. R bir birimli değişmeli halka, M, N ve L birer R-modülleri olsun. Eğer

$$e : M \times N \longrightarrow L$$

dönüşümü R-iki lineer bir dönüşüm ise yani her $r \in R$, m, m_1, $m_2 \in M$ ve n, n_1, $n_2 \in N$ için

$$e(rm, n) = e(m, rn) = re(m, n),$$
$$e(m_1 + m_2, n) = e(m_1, n) + e(m_2, n),$$
$$e(m, n_1 + n_2) = e(m, n_1) + e(m, n_2)$$

özelliklerini gerçekliyor ise e dönüşümüne bir *eşleme* (*pairing*) *dönüşümü* denir. Eğer her $m \in M$ için $e(m, m) = 0$ oluyor ise *eşleme dönüşümü alternedir* denir.

1.14 Tanım. $\mathbb{K}$ bir cisim ve $\mathbb{K}^\times$, $\mathbb{K}$ nın çarpımsal alt grubu olsun. $(\Psi, +, \geq)$ tam sıralı bir abel grubu olmak üzere Ψ üzerindeki grup yapısı ve sıralama bağıntısı $\Psi \cup \{\infty\}$ a şu şekilde genişletilsin:

i. Her $\alpha \in \Psi$ için $\infty \geq \alpha$ dir.

ii. Her $\alpha \in \Psi$ için $\infty + \alpha = \alpha + \infty = \infty$ dur.

Bu durumda her $a, b \in \mathbb{K}$ için

i. "$v(a) = \infty \Leftrightarrow a = \infty$"

ii. $v(ab) = v(a) + v(b)$

iii. $v(a + b) \geq \min(v(a), v(b))$

özelliklerini gerçekleyen

$$v : \mathbb{K} \longrightarrow \Psi \cup \{\infty\}$$

dönüşümüne $\mathbb{K}$ cisminin bir *valüasyonu* denir. Bu durumda $(\mathbb{K}, v)$ ikilisine *valüasyonlu cisim* denir.

1.15 Uyarı. $\mathbb{K}$ bir cisim ve $\mathbb{L}$ bu cismin cisim genişlemesi olsun. $\mathbb{K}$ üzerindeki valüasyonların $\mathbb{L}$ cismine genişletilmişlerinin kümesini bulma problemi valüasyonların dağılma teorisinin oluşmasına yol açar. Cisim genişlemesinin Galois olması durumunda bu problem ve bu kümenin yapısı daha iyi anlaşılabilir.

1.16 Tanım. ($\mathbb{K}$, v) valüasyonlu cisim ve $\mathbb{L}$, $\mathbb{K}$ nın sonlu Galois cisim genişlemesi olsun. S_v, v valüasyonunun $\mathbb{L}$ deki genişletilmelerinin denklik sınıflarının kümesi ve G, $\mathbb{L}$ nin, $\mathbb{K}$ üzerindeki Galois grubu olsun. $\sigma : L \to L$ bir otomorfizm ve $[w] \in S_v$ olmak üzere *G nin S_v üzerindeki etkisi* $\sigma[w] = [w \circ \sigma]$ olarak verilir. v valüasyonunun $\mathbb{L}$ deki genişletilmişi w olsun. w nin *ayrışma grubu* $[w]$ nin G_w kalımlaştırıcı alt grubu olarak tanımlanır.

2. ELİPTİK EĞRİLER

Bu bölümde yer alan tanımlar çoğunlukla teorinin en önemli kaynağı olarak kabul edilen ve konuyla ilgili makalelerde en çok atıf alan Joseph H. Silverman'ın "The Arithmetic of Elliptic Curves" isimli kitabından alınmıştır (Silverman 1986).

2.1 Giriş

Cebirsel Geometri'nin en önemli ve popüler konularından birisi olan eliptik eğriler kabaca belirli bir taban noktasına sahip, cinsi 1 olan cebirsel eğriler olarak tanımlanır. $\mathbb{P}^2$, projektif düzlemi göstermek üzere bu özellikteki eğriler, $\mathbb{P}^2$ de ∞ dan geçen doğru üzerinde tek bir noktaya sahip kübik eşitliğin geometrik yeri olarak yazılabilir. Böylece aşağıdaki tanım verilebilir.

2.1.1 Tanım. $\mathbb{K}$ bir cisim ve $\overline{\mathbb{K}}$, $\mathbb{K}$ cisminin cebirsel kapanışı olsun. $a_1, \ldots, a_6 \in \overline{\mathbb{K}}$ ve $O = [0, 1, 0]$ yukarıda adı geçen taban noktası olmak üzere

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

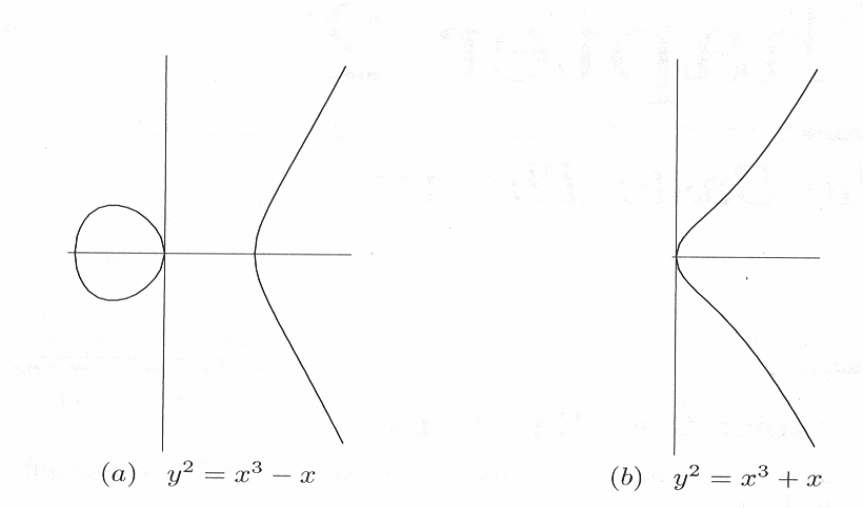
eşitliğini gerçekleyen noktaların geometrik yerine $\mathbb{K}$ *üzerinde tanımlı eliptik eğri* denir.

2.1.2 Uyarı. Çalışma boyunca Eliptik Eğriler Teorisi'ne geometrik bir bakıştan daha çok aritmetik bir yaklaşım söz konusu olacağından Tanım 2.1.1 homojen olmayan koordinatlar kullanılarak aşağıdaki şekilde ifade edilebilir.

2.1.3 Tanım. $\mathbb{K}$ herhangi bir cisim olsun. $a_1, \ldots, a_6 \in \mathbb{K}$ olmak üzere

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.1)$$

eşitliğini gerçekleyen noktaların geometrik yerine $\mathbb{K}$ cismi üzerinde *E eliptik eğrisi* denir.



Şekil 2.1 Eliptik Eğri Örnekleri

(2.1) eşitliğine Weierstrass eşitliği adı verilir. İlerleyen kısımlarda bir eliptik eğri üzerindeki noktaların kümesinin bir grup olduğu görülecektir, bu nedenle "*sonsuzdaki nokta*" adı verilen ve $O = [0, 1, 0]$ ile gösterilen noktanın daima *E* eliptik eğrisi üzerinde olduğu kabul edilecektir.

2.1.4 Uyarı. $\mathbb{K}$ cisminin karakteristiği 2 veya 3 ten farklı olması durumunda (2.1) eşitliği daha basit hale getirilebilir ($\mathbb{K}$ cisminin karakteristiğinin 2 veya 3 olması durumları dikkate alınmayacak olup bu konuyla ilgili ayrıntılı bilgi (Silverman 1986) da bulunabilir).

$\mathbb{K}$ cisminin karakteristiği 2 veya 3 ten farklı olsun. Bu durumda

$$y \to \frac{1}{2}(y - a_1x - a_3)$$

dönüşümü yapılarak ve tam kareye tamamlama metodu kullanılarak,

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3,$$
$$b_6 = a_3^2 + 4a_6,$$

olmak üzere, E eliptik eğrisi

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

biçiminde yazılabilir.

Aşağıdaki eşitlikler yardımıyla eliptik eğri daha basit bir şekilde ifade edilebilir:

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4,$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9\, b_2b_4b_6,$$
$$j = \frac{c_4^3}{\Delta},$$
$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

Aritmetik işlemler sonucunda $4b_8 = b_2b_6 - b_4^2$ ve $1728\Delta = c_4^3 - c_6^2$ olduğu kolayca görülebilir.

Üstelik $\mathbb{K}$ cisminin karakteristiğinin 2 veya 3 ten farklı olması halinde

$$(x, y) \to \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

dönüşümü yardımıyla E eliptik eğrisi

$$E : y^2 = x^3 - 27c_4x - 54c_6$$

biçiminde ifade edilebilir. Eliptik eğrilerin bu şekildeki ifadesine "*Kısa Weierstrass formu*" adı verilir.

2.1.5 Tanım. $E : y^2 = x^3 - 27c_4x - 54c_6$ olmak üzere, Δ sayısına *E eliptik eğrisinin diskriminantı*, j sayısına *E eliptik eğrisinin j-invaryantı*, ω ya *E eliptik eğrisinin Weierstrass eşitliği ile eşleşen invaryant diferensiyeli* adı verilir.

2.1.6 Tanım. $\mathbb{K}$ cismi üzerinde E eliptik eğrisi

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

biçiminde tanımlı ve $P = (x_0, y_0)$, E eliptik eğrisi üzerinde bir nokta olsun, yani bu nokta eğrinin Weierstrass eşitliğini gerçeklesin. Eğer

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$$

ise P noktasına *singüler nokta* adı verilir. En az bir singüler noktaya sahip eliptik eğriye *singüler eğri* denir.

2.1.7 Uyarı. P noktası E eliptik eğrisi üzerinde bir singüler nokta ise $f(x, y)$ fonksiyonu P noktasında belli $\alpha, \beta \in \overline{\mathbb{K}}$ için

$$f(x, y) - f(x_0, y_0) = [(y - y_0) - \alpha(x - x_0)]\,[(y - y_0) - \beta(x - x_0)] - (x - x_0)^3$$

biçiminde bir Taylor açılımına sahiptir. Bu açılım yardımıyla aşağıdaki tanım verilebilir.

2.1.8 Tanım. Yukarıdaki seri açılımında $\alpha \neq \beta$ ise P singüler noktasına *düğüm* (*node*) *noktası*, $\alpha = \beta$ ise P singüler noktası *doruk* (*cusp*) *noktası* olarak adlandırılır.

Eğer P bir düğüm noktası ise

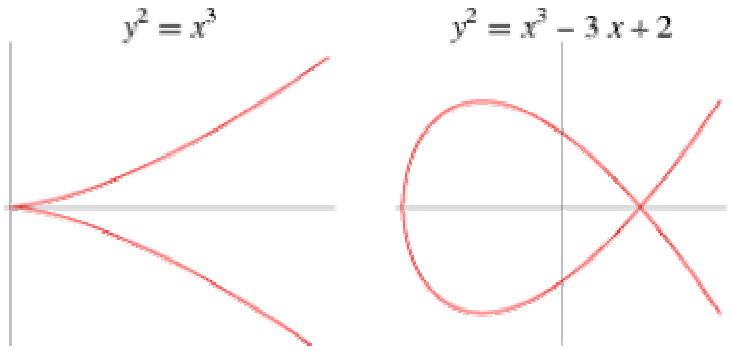
$$y - y_0 = \alpha(x - x_0) \text{ ve } y - y_0 = \beta(x - x_0)$$

doğruları E eliptik eğrisinin P noktasındaki teğet doğruları olur. Eğer P noktası bir doruk noktası ise

$$y - y_0 = \alpha(x - x_0),$$

E eliptik eğrisinin P noktasından geçen teğet doğrusu olur.

2.1.9 Örnek. E: $y^2 = x^3$ singüler eğrisi için (0, 0) noktası doruk (cusp) noktası, E: $y^2 = x^3 - 3x + 2$ singüler eğrisi için (1, 0) noktası düğüm (node) noktasıdır.



Doruk Düğüm

Şekil 2.2 Singüler Eğriler ve Singüler Noktalar

2.1.10 Uyarı 1. Tanım 2.1.5 de belirtilen j-invaryant yardımıyla, eliptik eğrilerin Weierstrass eşitliklerinde uygun değişken değişimleri yapılarak eliptik eğriler izomorfizm sınıflarına ayrılabilir. $u, r, s, t \in \overline{\mathbb{K}}$ ve $u \neq 0$ olmak üzere

$$x = u^2 x' + r,$$
$$y = u^3 y' + u^2 s x' + t$$

değişken değişimi $O = [0, 1, 0]$ noktasını ve Weierstrass eşitliğini koruyan tek değişken değişimidir. Yukarıdaki değişken değişimi altında değişmeyen tek değer olan j–invaryant, eliptik eğrilerin izomorfizm sınıflarının bir değişmezidir ve eşitliğin seçiminden de bağımsızdır. Cebirsel olarak kapalı cisimlerde bu önermenin tersi de doğrudur.

2. Karakteristiği 2 ve 3 ten farklı olan $\mathbb{K}$ cisimleri üzerinde tanımlanan eliptik eğrilerin Weierstrass eşitliklerinin uygun bir değişken değişimi yardımıyla basitleştirilebileceği görüldü. İlerleyen kısımlarda da görülebileceği gibi eliptik eğrilerin üzerinde

çalışılacağı $\mathbb{K}$ cismi değiştirilerek zengin sonuçlar elde edilebilir. Bu nedenle $\mathbb{K} = \mathbb{Q}$ durumu da dahil eliptik eğrileri tüm karakteristiklerde ele almak oldukça önemlidir.

$A, B \in \overline{\mathbb{K}}$ için E eliptik eğrisinin

$$y^2 = x^3 + Ax + B \tag{2.2}$$

biçiminde Weierstrass eşitliğine sahip olduğu kabul edilebilir. Bu durumda

$$\Delta = -16(4A^3 + 27B^2)$$

$$j = \frac{-1728(4A)^3}{\Delta}$$

olur. Bu halde $\overline{\mathbb{K}}^*$, $\mathbb{K}$ cisminin kapanışındaki çarpımsal tersleri olan elemanların kümesi olmak üzere, Weierstrass eşitliğinin bu formunu koruyan tek değişken değişimi belli bir $u \in \overline{\mathbb{K}}^*$ için

$$x = u^2 x',$$
$$y = u^3 y'$$

olup, bu değişken değişimi yardımıyla

$$u^4 A' = A,$$
$$u^6 B' = B,$$
$$u^{12} \Delta' = \Delta,$$
$$j' = j$$

elde edilir.

2.1.11 Uyarı 1. Weierstrass eşitliğiyle verilen E eliptik eğrileri aşağıdaki şekilde sınıflandırılabilir:

i. E singüler değildir $\Leftrightarrow \Delta \neq 0$ dır.

ii. E bir düğüm noktasına sahiptir $\Leftrightarrow \Delta = 0$ ve $c_4 \neq 0$ dır.

iii. E bir doruk noktasına sahiptir $\Leftrightarrow \Delta = 0$ ve $c_4 = 0$ dır.

2. $\overline{\mathbb{K}}$ üzerinde iki eliptik eğri izomorftur $\Leftrightarrow$ Bu iki eliptik eğri aynı j–invaryanta sahiptir.

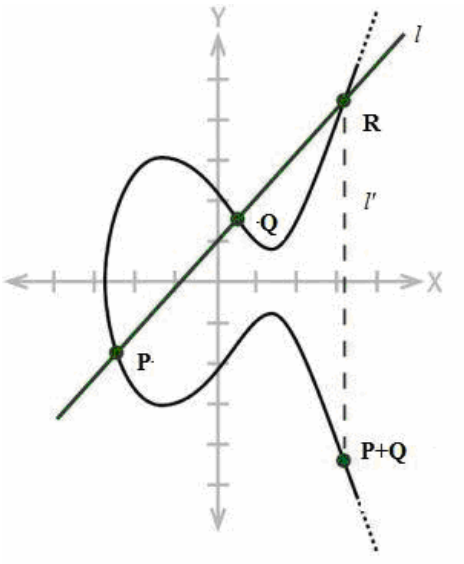
3. $j_0 \in \overline{\mathbb{K}}$ olsun. Bu durumda $\mathbb{K}$ üzerinde j–invaryantı j_0 olan bir E eliptik eğrisi vardır.

2.2 Eliptik Eğrilerin Grup Yapısı

Bu kısımda şu ana kadar yalnızca nokta kümesi olarak ele alınan eliptik eğrilerin, üzerinde tanımlanan işlem yardımıyla aslında bir abel grubu olduğu görülecektir. Böylece eliptik eğriler üzerinde cebirsel işlemler yapılabilecektir.

2.2.1 Tanım. $E \subseteq \mathbb{P}^2$ bir eliptik eğri, $O = [0, 1, 0]$ ve $P, Q \in E$ olsun (Şekil 2.3).

P ve Q noktalarından geçen doğru l olarak adlandırılsın. E eliptik eğrisinin Weierstrass eşitliğinin derecesi 3 olduğundan l doğrusu ile E eliptik eğrisi P ve Q dışında R gibi üçüncü bir noktada kesişir. l' doğrusu R ve O noktalarından geçen doğru olsun. Bu durumda *P ve Q noktalarının toplamı* $P + Q$ ile gösterilir ve l' doğrusunun R ve O noktaları dışında E ile kesiştiği üçüncü nokta olarak tanımlanır.



Şekil 2.3 Eliptik Eğri Üzerindeki Toplama İşlemi

2.2.2 Uyarı 1. $P = Q$ olması halinde, yani noktaların kendisi ile toplanması halinde l doğrusu, E eliptik eğrisinin teğet doğrusu olarak alınır.

2. $\mathbb{P}^2$ deki teknik kaygılar nedeniyle "formal" olarak verilen bu tanım uygulamada genellikle şu şekilde düşünülebilir: "E bir eliptik eğri ve $P, Q \in E$ olsun. $P + Q$, P ve Q noktasından geçen l doğrusunun E eliptik eğrisi ile kesiştiği üçüncü noktanın x–eksenine göre simetriği olan nokta olarak tanımlanır."

2.2.3 Önerme. (Silverman 1986) Tanım 2.2.1 de tanımlanan + toplama işlemi aşağıdaki özelliklere sahiptir:

i. l doğrusu, E eliptik eğrisini birbirinden farklı olması gerekmeyen P, Q ve R gibi üç noktada kessin. Bu durumda

$$(P + Q) + R = O,$$

ii. Her $P \in E$ için

$$P + O = P,$$

iii. Her $P, Q \in E$ için

$$P + Q = Q + P,$$

iv. $P \in E$ olsun. E eliptik eğrisinin $-P$ ile gösterilen öyle bir noktası vardır ki

$$P + (-P) = O,$$

v. Her P, Q ve $R \in E$ için

$$(P + Q) + R = P + (Q + R),$$

vi. E eliptik eğrisi üzerinde tanımlanan + işlemi ile birlikte birim elemanı O olan abel grubudur,

vii. E eliptik eğrisi $\mathbb{K}$ cismi üzerinde tanımlansın. Bu durumda

$$E(\mathbb{K}) = \{ (x, y) \in \mathbb{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \} \cup \{O\}$$

E eliptik eğrisinin bir alt grubudur.

2.2.4 Uyarı. $\mathbb{K}$ cismi değiştirilerek Eliptik Eğriler Teorisi zenginleştirilebilir. $\mathbb{K}$ cismi $\mathbb{Q}$ rasyonel sayılar cismi, $\mathbb{F}_p$ sonlu cismi, $\mathbb{C}$ karmaşık sayılar cismi gibi global cisimler olabileceği gibi $\mathbb{Q}_p$ p–adik rasyonel sayılar cismi gibi yerel cisimler de göz önüne alınabilir. $\mathbb{K} = \mathbb{Q}$ ve $\mathbb{F}_p$ olması durumları çalışmanın kapsamında yer almaktadır.

2.3 Sonlu Cisimler Üzerindeki Eliptik Eğriler

Bu kısımda sonlu cisimler üzerindeki eliptik eğriler ele alınacak ve elde edilen bazı sonuçlar verilecektir.

p bir asal sayı, $r \in \mathbb{N}$, $q = p^r$ ve $\mathbb{K}$ karakteristiği q olan ve $\mathbb{K} = \overline{\mathbb{K}}$ özelliğinde bir (mükemmel) cisim olsun. $\mathbb{K}$ üzerinde tanımlı E eliptik eğrisinin en önemli aritmetik özelliği üzerindeki rasyonel noktaların sayısıdır. a_1, a_2, a_3, a_4 ve $a_6 \in \mathbb{K}$ olmak üzere

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

eşitliğinin en fazla $2q + 1$ tane çözümü olabileceğinden bu sayı E eliptik eğrisi üzerindeki rasyonel noktaların sayısı için doğal bir üst sınırdır.

Diğer yandan Emil Artin'in doktora tezinde (Artin 1921) konjektür olarak verilen ve 1930'lu yıllarda Helmut Hasse tarafından ispatlanan aşağıdaki teorem $E(\mathbb{K})$ nın eleman sayısı için literatürdeki en iyi sınırdır.

2.3.1 Teorem. (Silverman 1986) E, q elemandan oluşan $\mathbb{K}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$| \#E(\mathbb{K}) - q - 1 | \leq 2\sqrt{q}$$

olur.

2.3.2 Uyarı 1. $\mathbb{K}$ cismi üzerinde rastgele seçilen ikinci dereceden bir denklemin çözülebilme olasılığı $\frac{1}{2}$ olduğundan tahmin edilebilir olan bu öngörünün doğru olduğu Helmut Hasse tarafından gösterilmiştir.

2. Bu sonuç sadece eliptik eğriler üzerinde değil, sonlu cisimler üzerinde tanımlı cinsi 1 den büyük olan tüm cebirsel eğriler için de geçerlidir. Bu durumda Hasse eşitsizliğinin sağ tarafının cebirsel eğrinin cinsi ile çarpılması gerekir. Dikkate alınan eliptik eğrilerin, cinsleri 1 olan cebirsel eğriler olduğu hatırlanırsa Teorem 2.3.1 in genel Hasse eşitsizliğinin özel bir hali olduğu görülür.

3. Aşağıdaki örnekte de görüleceği üzere, Hasse Teoremi olarak da adlandırılan bu sonuç nokta sayısı için bir üst sınır vermekle kalmayıp bazen Cebir ve Sayılar Teorisi'nin elementer sonuçları ile birleştirilerek kesin nokta sayısını bulmak için de kullanılmaktadır.

2.3.3 Örnek 1. $\mathbb{K} = \mathbb{F}_{101}$ cismi üzerinde $E : y^2 = x^3 + 7x + 1$ eliptik eğrisi göz önüne alınırsa $(0, 1) \in E(\mathbb{K})$ olduğu açıktır. Doğrudan hesaplama yöntemiyle $(0, 1)$ noktasının mertebesinin 116 olduğu görülebilir. Lagrange Teoremi gereği noktanın mertebesi grubun mertebesini böleceğinden, $k \in \mathbb{Z}$ olmak üzere $\#E(\mathbb{K}) = 116 \cdot k$ olur.

Diğer yandan Hasse Teoremi gereği

$$101 + 1 - 2\sqrt{101} \leq \#E(\mathbb{K}) \leq 101 + 1 + 2\sqrt{101}$$

olur. Böylece $82 \leq \#E(\mathbb{K}) \leq 122$ elde edilir. Bu eşitsizlikten de $\#E(\mathbb{K}) = 116$ olduğu görülür.

2. $\mathbb{K} = \mathbb{F}_{103}$ cismi üzerinde $E : y^2 = x^3 + 7x + 12$ eliptik eğrisi göz önüne alınırsa $\{ (-1, 2), (19, 0) \} \subseteq E(\mathbb{K})$ olduğu görülebilir. Yine doğrudan hesaplama yöntemiyle (–1, 2) noktasının mertebesinin 13 ve (19, 0) noktasının mertebesinin de 2 olduğu bulunabilir. Böylece $k \in \mathbb{Z}$ olmak üzere $\#E(\mathbb{K}) = 26 \cdot k$ olur. Hasse Teoremi gereği $84 \leq \#E(\mathbb{K}) \leq 124$ eşitsizliği elde edilir, bu eşitsizlikten de $\#E(\mathbb{K}) = 104$ olarak bulunur.

2.3.4 Uyarı 1. Yeterince büyük p sayıları için eğri üzerindeki noktanın mertebesini bulma problemi zorlaştığı gibi, "Hasse aralığı" olarak adlandırılan

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{K}) \leq p + 1 + 2\sqrt{p}$$

aralığı da genişler. Bu durumda eliptik eğri üzerinde birkaç nokta daha bulunup, mertebeleri hesaplanarak olasılıklar en aza indirgenebilir.

2. $E(\mathbb{K})$ nın mertebesinin hesaplanması ve bir $P \in E(\mathbb{K})$ nın mertebesinin bulunması problemi Şifreleme Teorisi'nin problemlerinden biri olup, bunun için bazı yöntemler geliştirilmiştir. Bunlardan bir tanesi "*Baby Step-Giant Step*" adlı yöntemdir (bu yöntem hakkında detaylı bilgi (Shanks 1971) de bulunabilir).

3. Önerme 2.2.3 te $E(\mathbb{K})$ nın E nin bir alt grubu olduğu belirtilmişti. $E(\mathbb{K})$ nın mertebesini hesaplamak kadar, sonlu mertebeye sahip olduğundan, $E(\mathbb{K})$ nın izomorf olduğu grupları, yani grup yapılarının ne olduğunu bilmek de oldukça önemlidir.

2.3.5 Teorem. (Washington 2003) E, $\mathbb{K} = \mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda iki durum söz konusudur.

i. Belirli bir $n \geq 1$ tamsayısı için

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n,$$

ii. $n_1 \mid n_2$ özelliğindeki $n_1, n_2 \geq 1$ tamsayıları için

$$E(\mathbb{F}_p) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

dir.

2.3.6 Uyarı. Genellikle yukarıdaki teoremdeki ilk durum söz konusudur. İkinci durumu gerçekleyen eliptik eğriler ve $\mathbb{K} = \mathbb{F}_p$ cisimleri ise oldukça az olduğu halde, aşağıdaki örnek bununla ilgilidir.

2.3.7 Örnek. $\mathbb{F}_7$ üzerinde $E : y^2 = x^3 + 2$ eliptik eğrisi göz önüne alındığında basit bir hesaplama ile

$$E(\mathbb{F}_7) = \{ O, (0, 3), (0, 4), (3, 1), (3, 6), (5, 1), (5, 6), (6, 1), (6, 6) \}$$

olduğu bulunabilir. E üzerindeki tüm noktalar 3 mertebelidir. Biri diğerinin katı olmayan E üzerindeki iki nokta $E(\mathbb{F}_7)$ nin 9 mertebeli bir alt grubunu üretir. Hasse Teoremi gereği

$$3 \leq \#E(\mathbb{F}_7) \leq 13$$

olduğu görülür. Böylece $\#E(\mathbb{F}_7) = 9$ olup

$$E(\mathbb{F}_7) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

olur. Bu durum ise aşağıdaki teorem ile açıklanabilir.

2.3.8 Teorem. (Washington 2003) E, $\mathbb{K} = \mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri ve

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$$

olsun. Bu durumda ya $p = n^2 + 1$, ya $p = n^2 \pm n + 1$ ya da $p = (n \pm 1)^2$ dir.

2.4 Sonlu Cisimler Üzerindeki Eliptik Eğrilerin Grup Mertebeleri

$A, B \in \mathbb{F}_p$ olmak üzere $y^2 = x^3 + Ax + B$ eliptik eğrisi üzerindeki rasyonel noktaların sayısını hesaplamak için farklı yöntemler geliştirilmiştir. Yeterince küçük p asalları için $\#E(\mathbb{F}_p)$ yi hesaplamak için Legendre sembolünün kullanılması bu yöntemlerden birisidir, bu sembol kullanılarak eğrinin mertebesi aşağıdaki teorem yardımıyla hesaplanabilir.

2.4.1 Teorem. (Washington 2003) $A, B \in \mathbb{F}_p$ olmak üzere, $E : y^2 = x^3 + Ax + B$ olsun. Bu durumda

$$\# E(\mathbb{F}_p) = p + 1 + \sum_{x \in F_q} \left(\frac{x^3 + Ax + B}{p} \right)$$

olur.

2.4.2 Sonuç. (Washington 2003) $A, B \in \mathbb{F}_p$ olmak üzere $x^3 + Ax + B$ polinomu göz önüne alınırsa

$$\left| \sum_{x \in F_p} \left(\frac{x^3 + Ax + B}{p} \right) \right| \leq 2\sqrt{p}$$

olur.

2.4.3 Uyarı. p asal sayısı büyütüldüğünde Teorem 2.4.1 de verilen yöntem kullanılarak nokta sayısını hesaplamak zaman alabilir. Literatürde yer alan diğer yöntemlerin kullanılması halinde de yeterince büyük p asalı için $\mathbb{F}_p$ üzerinde tanımlı eliptik eğrilerin nokta sayısını hesaplamak bazen zor, bazen de imkansız olabilir. Bu durumda Rene Schoof'un (1985) ortaya attığı ve Arthur O. L. Atkin ile Noam Elkies'in geliştirdikleri (Blake ve ark. 2000) "Schoof algoritması" adı verilen yöntem kullanılabilir. "Baby step-Giant step" yönteminde en fazla $\sqrt[4]{p}$ adıma ihtiyaç olduğu halde, "Schoof Algoritması"

yönteminde en fazla $(\log p)^8$ adıma ihtiyaç duyulmaktadır. Nokta sayısı hesaplama ile ilgili diğer bir yöntem (Satoh 2002) de verilmiştir.

İlerleyen teknoloji ile birlikte bilgisayar tabanlı hesaplamalarda Schoof algoritması kullanılarak yüzlerce haneye sahip p asalları için $\mathbb{F}_p$ üzerinde tanımlı E eliptik eğrisinin üzerindeki rasyonel nokta sayısı süratli bir şekilde hesaplanabilmektedir.

2.4.4 Uygulama. MAGMA cebir programı (Bosma ve ark. 1997) kullanılarak, sonlu cisimler üzerinde tanımlı singüler olmayan eliptik eğrilerin rasyonel noktaları ve bunların sayısı aşağıdaki şekilde hesaplanır:

Girdi. p asal sayısı ve $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_p$

Çıktı. $\mathbb{F}_p$ üzerinde tanımlı $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ için $\#E(\mathbb{F}_p)$

Komutlar ise

```
>E:=EllipticCurve([GF(p) | a1, a2, a3, a4, a6]);
>A:=RationalPoints;
>#E;
>#A;
```

dır. Örneğin $\mathbb{F}_7$ üzerinde tanımlı $E : y^2 - xy + y = x^3 - x^2 + x + 2$ eliptik eğrisi üzerindeki rasyonel noktaların sayısını bulan komutlar ve programın çıktısı

```
>E:=EllipticCurve([GF(7) | –1 , –1, 1, 1, 2]);
>#E;
>5
```

dir. Diğer yandan E eliptik eğrisi üzerindeki rasyonel noktalar projektif düzlem koordinatlarında aşağıdaki komutlar yardımıyla bulunabilir:

```
>E:=EllipticCurve([GF(7) | –1 , –1, 1, 1, 2]);
>A:=RationalPoints; A;
> { @ (0 : 1 : 0), (0 : 1 : 1), (0 : 5 : 1), (6 : 1 : 1), (6 : 6 : 1) @ }
```

Burada (0 : 1 : 0), O noktasıdır. Elde edilen koordinatları kullanabilmek için, çıktıdaki projektif (X : Y : Z) koordinatlarının

$$x = \frac{X}{Z} \text{ ve } y = \frac{Y}{Z}$$

dönüşümü kullanılarak dik koordinat sistemine dönüştürülmesi gerekir. O noktası hariç projektif koordinatlara sahip eğri üzerindeki tüm rasyonel noktaların Z bileşenlerinin 1 olması, projektif düzlemin özelliklerinden kaynaklanmaktadır.

2.4.5 Uyarı. p asal olmak üzere $\#E(\mathbb{F}_p)$ bilindiği zaman $n \in \mathbf{N}$ için $q = p^n$ olmak üzere $\#E(\mathbb{F}_q)$ da hesaplanabilir.

2.4.6 Teorem. (Washington 2003) E eliptik eğrisi, $n \in \mathbf{N}$ için $q = p^n$ olmak üzere $E(\mathbb{F}_q)$ sonlu cismi üzerinde tanımlı ve $\#E(\mathbb{F}_p) = q + 1 - a$ olsun. Ayrıca

$$X^2 - ax + q = (X - \alpha)(X - \beta)$$

ise $n \geq 1$ için

$$\#E(\mathbb{F}_q) = q^n + 1 - (\alpha^n + \beta^n)$$

olur.

2.5 Bazı Özel Eliptik Eğri Aileleri

Bu kısımda, sonlu cisimler üzerinde tanımlı olan eliptik eğriler üzerinde yapılan çalışmalar sonucunda elde edilen bazı sonuçlar verilecektir.

1. $\mathbb{F}_p$ Üzerinde Tanımlı $E_c : y^2 = x^3 + cx$ ($c \in \mathbb{F}_p$), Eliptik Eğri Ailesi Üzerindeki Rasyonel Noktaların Sayısı

Sonlu cisimler üzerinde tanımlı belirli bir eliptik eğri üzerindeki rasyonel noktaların sayısının ve bu noktaların oluşturduğu grubun yapısının bilinmesi kadar, sonlu cisim üzerinde tanımlı eliptik eğri ailelerinin nokta sayılarının sınıflandırılması da oldukça önemli bir problemdir. Bir parametreli eliptik eğri aileleri için bazı durumlarda nokta sayıları parametreye bağlı olarak sınıflandırılabilir. Örneğin $\mathbb{F}_p$ üzerinde tanımlı

$$E_c : y^2 = x^3 + cx,\ c \in \mathbb{F}_p$$

eliptik eğri ailesi üzerindeki rasyonel noktaların sayısı c parametresine bağlı olarak modülo 8 de sınıflandırılabilir. Park ve arkadaşları (2003) çalışmasında E_c eğri ailesi üzerindeki rasyonel nokta sayısını aşağıdaki şekilde sınıflandırmıştır:

2.5.1 Teorem. (Park ve ark. 2003) $\mathbb{F}_p$ üzerinde $E_c : y^2 = x^3 + cx$ eliptik eğri ailesi verilsin ve $p \equiv 1, 5 \pmod 8$ olsun. Bu durumda

$$\#E_c(\mathbb{F}_p) \equiv \begin{cases} 0 \pmod 8 & c,\ \mathbb{F}_p\text{' de 4. dereceden kalan} \\ 4 \pmod 8 & c,\ \mathbb{F}_p\text{' de 2.dereceden kalan ama 4. dereceden kalan degil} \\ 2 \pmod 8 & c,\ \mathbb{F}_p\text{' de 2. dereceden kalan degil} \end{cases}$$

olur.

Bu eliptik eğri ailesi üzerinde yapılan bazı hesaplamalar sonucunda yukarıdaki teoremde bir yanlışlık olduğu belirlenmiştir. Bu durum aşağıdaki örnek ele alınarak açıklanabilir.

2.5.2 Örnek 1. $p = 29$ ve $c = 4$ olsun. c sayısı modülo 29 da ikinci dereceden kalan fakat, 4. dereceden kalan değildir. Teorem 2.5.1 e göre $\#E(\mathbb{F}_{29}) \equiv 4 \pmod 8$ olması beklenmektedir, halbuki

```
>E:=EllipticCurve([GF(29) | 0, 0, 0, 4, 0]);
>#E;
>40
```

olup $\#E(\mathbb{F}_{29}) \equiv 0 \pmod 8$ dir. Aynı sınıfta kalan c değerleri için de benzer sonuçlar elde edilir.

2. $p = 29$ ve $c = 7$ olsun. c sayısı modülo 29 da dördüncü dereceden kalandır. Yine aynı teoreme göre $\#E(\mathbb{F}_{29}) \equiv 0 \pmod 8$ olması beklenmektedir. Halbuki

```
>E:=EllipticCurve([GF(29) | 0, 0, 0, 7, 0]);
```

>#E;

>20

olup $\#E(\mathbb{F}_{29}) \equiv 4 \pmod 8$ dir. Aynı sınıfta kalan c değerleri için de benzer sonuçlar elde edilir.

2.5.3 Uyarı. Teorem 2.5.1 in ispatı incelendiğinde (Park ve ark. 2003) de yer alan (3–7) ve (3–8) numaralı formüller, sırasıyla, $p \equiv 1 \pmod 8$ ve $p \equiv 5 \pmod 8$ için geçerli olduğu halde teoremin ispatında beraber kullanılmıştır. Bu formülün ayrı ayrı kullanılması halinde aşağıdaki sonuç elde edilir;

2.5.4 Teorem. (İnam ve ark. 2007a) $\mathbb{F}_p$ üzerinde $E_c : y^2 = x^3 + cx$ eliptik eğri ailesi verilsin.

i. $p \equiv 1 \pmod 8$ ise bu durumda

$$\#E_c(\mathbb{F}_p) \equiv \begin{cases} 0 \pmod 8 & c,\ \mathbb{F}_p\text{' de 4. dereceden kalan} \\ 4 \pmod 8 & c,\ \mathbb{F}_p\text{' de 2.dereceden kalan ama 4. dereceden kalan degil} \\ 2 \pmod 8 & c,\ \mathbb{F}_p\text{' de 2. dereceden kalan degil} \end{cases}$$

ii. $p \equiv 5 \pmod 8$ ise bu durumda

$$\#E_c(\mathbb{F}_p) \equiv \begin{cases} 4 \pmod 8 & c,\ \mathbb{F}_p\text{' de 4. dereceden kalan} \\ 0 \pmod 8 & c,\ \mathbb{F}_p\text{' de 2.dereceden kalan ama 4. dereceden kalan degil} \\ 2 \pmod 8 & c,\ \mathbb{F}_p\text{' de 2. dereceden kalan degil} \end{cases}$$

2. Sonlu Cisimler Üzerinde Tanımlı Frey Eliptik Eğrileri

Eliptik eğriler ile modüler formlar arasındaki ilişki çalışmanın ilerleyen kısımlarında ele alınacaktır. Ancak Frey eliptik eğrileri, Modülarite Teoremi (daha önce Taniyama-Shimura-Weil Konjektürü) ile Fermat'ın Son Teoremi arasındaki ilişkiyi ortaya koymaktadır. Bu eğrilerin özel bir sınıfının sonlu cisimler üzerindeki nokta sayılarının sınıflandırılması çalışmanın sonuçlarından birisi olduğu için bu bölümde yer almaktadır.

Fermat'ın Son Teoremi ile eliptik eğriler arasında sıkı bir ilişki vardır (Wiles 1995). Taniyama'nın 1955'de Japonya'nın Nikko kentinde düzenlenen Sayılar Teorisi

konferansında ortaya attığı konjektürün yanlış olan ilk versiyonu Shimura tarafından 1957'de düzeltilmiştir. Andre Weil tarafından 1967'de yeniden ifade edilen ve düzenlenen konjektür kabaca "$\mathbb{Q}$ üzerindeki her bir eliptik eğrinin modüler olduğunu söylemektedir" (Bu konjektüre daha sonra tekrar değinilecektir). 1985'te Gerhard Frey, Fermat'ın Son Teoremi'ndeki o anda bilinen ters örneklerin aslında modüler olmayan eliptik eğriler olduğunu düşünmekle beraber Taniyama-Shimura-Weil Konjektürü'nün Fermat'ın Son Teoremi'ni gerektirdiğini iddia etmiştir. Böylece Jean Pierre Serre'nin katkıları, Ken Ribet'in bu iddiayı ispatlaması (Ribet 1990a) ve (Ribet 1990b) ile Fermat'ın Son Teoremi'nin ispatında önemli bir yol kat edilmiştir (Anonim 2011a).

p asal ve $a, b, c \in \mathbb{Z}$ için Fermat eşitliğinin $a^p + b^p = c^p$ gerçeklendiği varsayılsın. Bu eşitlik uygun değişken değişimi yardımıyla, Gerhard Frey'in modüler olmadığını iddia ettiği, $\mathbb{Q}$ üzerinde tanımlı

$$y^2 = x\,(x - a^p)\,(x - b^p)$$

eğri ile ifade edilir.

$a^p = -b^p = n \in \mathbb{F}_p$ olmak üzere Frey eliptik eğrilerinin $y^2 = x^3 - n^2x$ ailesinin nokta sayıları ile ilgili, ispatı daha öncekilerden değişik ve daha basit olarak verilmiş olan çalışmanın sonuçlarından birisi (İnam ve ark. 2007b) de yer almıştır.

2.5.5 Teorem. (İnam ve ark. 2007b) $\mathbb{F}_p$ üzerinde $E_n : y^2 = x^3 - n^2x$ eliptik eğri ailesi verilsin ve $p \equiv 1 \pmod 8$ olsun. Bu durumda

$$\#E_n(\mathbb{F}_p) \equiv \begin{cases} 0 \pmod 8 & : n \in Q_p \\ 4 \pmod 8 & : n \notin Q_p \end{cases}$$

olur, burada Q_p, $\mathbb{F}_p$ de ikinci dereceden kalanların kümesidir.

Teoremin ispatı için bazı ön hazırlıklar gerekmektedir.

2.5.6 Önerme. (Ireland ve Rosen 1981) p tek asal sayı olsun. Bu durumda

$$\sum_{y=0}^{p-1}\left(\frac{y^2+c}{p}\right)=\begin{cases}-1 & :c\not\equiv 0\,(\mathrm{mod}\,p)\\ p-1 & :c\equiv 0\,(\mathrm{mod}\,p)\end{cases}$$

olur.

2.5.7 Sonuç. p tek asal sayı olsun. Bu durumda

$$\sum_{i=1}^{p-1}\left(\frac{i^2-n^2}{p}\right)=\begin{cases}-1 & :c\not\equiv 0\,(\mathrm{mod}\,p)\\ p-1 & :c\equiv 0\,(\mathrm{mod}\,p)\end{cases}$$

olur.

İspat. Önerme 2.5.6 da $c = n^2$ alınarak sonuç elde edilir.

$E_n : y^2 = x^3 - n^2x$ Frey eliptik eğrilerinin üzerindeki rasyonel noktaların sayısı Wilson Teoremi yardımıyla Legendre sembolü kullanılarak hesaplanabilir.

2.5.8 Teorem. $p \equiv 1 \pmod 4$ özelliğindeki asallar için

$$\prod_{\substack{i=1\\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)=\begin{cases}+1 & :p\equiv 1\,(\mathrm{mod}8)\\ -1 & :p\equiv 5\,(\mathrm{mod}8)\end{cases}$$

olur.

İspat. Sonuç 2.5.7 gereği

$$\sum_{i=0}^{p-1}\left(\frac{i^2-n^2}{p}\right)=\left(\frac{-n^2}{p}\right)+2\sum_{1=1}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)=-1$$

olur. $n \equiv 0 \pmod p$ olması halinde $y^2 = x^3 - n^2x$ eğrisi singüler bir eğri olur ki, singüler eğriler bu çalışmanın kapsamı dışındadır.

$p \equiv 1, 5 \pmod 8$ olduğundan $-n^2 \in Q_p$ ve böylece $\left(\frac{-n^2}{p}\right)=+1$ dir. Dolayısıyla

$$\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)=-1 \qquad (2.3)$$

elde edilir.

$$M = \left\{ 1 \le i \le \frac{p-1}{2} : \left(\frac{i^2 - n^2}{p} \right) = +1 \right\}$$

ve

$$N = \left\{ 1 \le i \le \frac{p-1}{2} : \left(\frac{i^2 - n^2}{p} \right) = -1 \right\}$$

olmak üzere (2.3) eşitliği gereği N kümesinin eleman sayısı M kümesinin eleman sayısından bir fazladır. Çünkü $i = n$ ve $i = p - n$ için $i^2 - n^2 \equiv 0 \pmod{p}$ olduğu bilinmektedir. Üstelik n ya da $p - n$ değerlerinden yalnızca birisi $(1, \frac{p-1}{2})$ aralığında kalır. Böylece n ya da $p - n$ değerlerinden yalnızca birisi için $i^2 - n^2$, p ile bölünebilir, yani sadece bu değer için $\left(\frac{i^2 - n^2}{p} \right) = 0$ olur. i nin diğer tüm değerleri için $\left(\frac{i}{p} \right)$ değeri ya +1 ya da –1 olur. Üstelik (2.3) eşitliği gereği bu toplamdaki elemanların sayısı çifttir, böylece –1'lerin sayısı +1'lerin sayısından bir fazla olur. O halde

$$\prod_{\substack{i=1 \\ i \ne n}}^{\frac{p-1}{2}} \left(\frac{i^2 - n^2}{p} \right) = (-1)^{|N|} = (-1)^{\frac{p-1}{4}}$$

olur.

2.5.9 Önerme. (Park ve ark. 2003) $p \equiv 1 \pmod 4$ özelliğindeki asallar için

$$\prod_{\substack{i=1 \\ i \ne n}}^{\frac{p-1}{2}} \left(\frac{i}{p} \right) = \begin{cases} +1 & : p \equiv 1 \pmod 8 \\ -1 & : p \equiv 5 \pmod 8 \end{cases}$$

olur.

Frey eliptik eğrileri üzerindeki nokta sayıları öncelikle eğri üzerindeki ikinci mertebeden noktaların sayısına bağlıdır. Diğer yandan Neal Koblitz'e (1984) göre bir eliptik eğri üzerindeki ikinci mertebeden noktalar ise $(x, 0)$ formunda olan noktalardır. $E[m]$ ile E eliptik eğrisi üzerindeki m. mertebeden noktaların kümesi gösterilsin, yani

$$E[m] = \{ P \in E_n(\mathbb{F}_p) : mP = O \}$$

olsun.

2.5.10 Lemma. E_n, $\mathbb{F}_p$ üzerinde tanımlı Frey eliptik eğrileri olsun. Bu durumda

$$\#E_n[2] = 4$$

olur.

İspat. Bir eliptik eğri üzerindeki ikinci mertebeden noktalar ikinci bileşenleri sıfır olan noktalardır ve bunlar $(x, 0)$, $(p - x, 0)$, $(0, 0)$ ve O noktalarıdır.

Tüm bu ön hazırlıklarla beraber nokta sayısını hesaplamak için

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)\left(\frac{i^2-n^2}{p}\right) = \prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)$$

çarpımının hesaplanması gereklidir. İkinci derecede kalanlar ile nokta sayıları arasındaki ilişki aşağıdaki önerme yardımıyla verilmiştir.

2.5.11 Önerme *i.* $p \equiv 1 \pmod 8$ özelliğindeki asallar için

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right) = \begin{cases} +1 & : \ n \in Q_p \\ -1 & : \ n \notin Q_p \end{cases}$$

ii. $p \equiv 5 \pmod 8$ özelliğindeki asallar için

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right) = \begin{cases} -1 & : \ n \in Q_p \\ +1 & : \ n \notin Q_p \end{cases}$$

olur.

İspat *i.* $p \equiv 1 \pmod 8$ olsun. Bu durumda çarpımda tek sayıda eleman vardır. Böylece $n \in Q_p$ olması halinde $\left(\frac{n}{p}\right) = +1$ olduğundan

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right) = +1,$$

ve $n \notin Q_p$ olması halinde $\left(\frac{n}{p}\right) = -1$ olduğundan

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=-1$$

olur.

ii. $p \equiv 5 \pmod 8$ olsun. Bu durumda çarpımda çift sayıda eleman vardır. Böylece $n \in Q_p$ olması halinde $\left(\frac{n}{p}\right) = 1$ olduğundan

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=-1,$$

$n \notin Q_p$ olması halinde $\left(\frac{n}{p}\right) = -1$ olduğundan

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=+1$$

olur.

Teorem 2.5.5 in ispatı. $p \equiv 1 \pmod 8$ olsun. Böylece $n \in Q_p$ ise Önerme 2.5.11 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=+1,$$

olup, Teorem 2.5.8 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)=+1$$

olur. O halde $1 \le i \le \frac{p-1}{2}$ için $\left(\frac{i}{p}\right)\left(\frac{i^2-n^2}{p}\right) = +1$ eşitliğini gerçekleyen i sayıları çift sayıdadır. Böylece Lemma 2.5.10 gereği

$$\#E_n(\mathbb{F}_p) \equiv 0 \pmod 8$$

olur.

Benzer şekilde $n \notin Q_p$ ise Önerme 2.5.11 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=-1,$$

olup, Teorem 2.5.8 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)=-1$$

olur. O halde $1\le i\le\frac{p-1}{2}$ için $\left(\frac{i}{p}\right)\left(\frac{i^2-n^2}{p}\right)=-1$ eşitliğini gerçekleyen i sayıları tek sayıdadır. Böylece Lemma 2.5.10 gereği

$$\#E_n(\mathbb{F}_p)\equiv 4 \pmod 8$$

olur.

$p\equiv 5 \pmod 8$ olsun. Böylece $n\in Q_p$ ise Önerme 2.5.11 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=-1,$$

olup, Teorem 2.5.8 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)=+1$$

olur. O halde $1\le i\le\frac{p-1}{2}$ için $\left(\frac{i}{p}\right)\left(\frac{i^2-n^2}{p}\right)=+1$ eşitliğini gerçekleyen i sayıları çift sayıdadır. Böylece Lemma 2.5.10 gereği

$$\#E_n(\mathbb{F}_p)\equiv 0 \pmod 8$$

olur.

Benzer şekilde $n\notin Q_p$ ise Önerme 2.5.11 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=+1,$$

olup, Teorem 2.5.9 gereği

$$\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)\prod_{\substack{i=1 \\ i\neq n}}^{\frac{p-1}{2}}\left(\frac{i^2-n^2}{p}\right)=-1$$

olur. O halde $1\le i\le\frac{p-1}{2}$ için $\left(\frac{i}{p}\right)\left(\frac{i^2-n^2}{p}\right)=-1$ eşitliğini gerçekleyen i sayıları tek sayıdadır. Böylece Lemma 2.5.10 gereği

$$\#E_n(\mathbb{F}_p)\equiv 4 \pmod 8$$

olur ve ispat tamamlanır.

2.5.12 Uyarı. Hesaplamalar yapılırken $i = n$ durumu, yani (0, 0) noktası Lemma 2.5.10 da dikkate alınmıştır.

2.6 $\mathbb{Q}$ Üzerinde Tanımlı Eliptik Eğriler

Bölüm başında E eliptik eğrisinin herhangi bir $\mathbb{K}$ cismi üzerinde tanımlanabileceği belirtilmişti. $\mathbb{K} = \mathbb{Q}$ durumunda akla gelen ilk soru eliptik eğri üzerindeki rasyonel noktaların sayısı olmuştur. Bu sayının sonsuz olması beklenen bir cevap olduğu halde bu sayı sonlu da olabilir, özellikle bu sayının sonlu olması durumları oldukça ilginçtir. Diğer yandan, $\mathbb{K} = \mathbb{Q}$ halinde $E(\mathbb{Q})$, E nin bir abelyen alt grubu olduğundan $E(\mathbb{Q})$ nun grup yapısının belirlenmesi de bu durumun önemli problemlerinden birisidir. Buradan hareketle eliptik eğriler üzerinde farklı yapılar oluşturulmuştur. $E(\mathbb{Q})$ nun grup yapısıyla ilgili olarak verilen aşağıdaki teorem $\mathbb{Q}$ cismi için verildiği halde her hangi bir $\mathbb{K}$ sayı cismi üzerinde de geçerlidir.

2.6.1 Mordell-Weil Teoremi. (Silverman 1986) E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda $E(\mathbb{Q})$ sonlu üreteçli bir gruptur.

2.6.2 Tanım. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. E eğrisinin sonlu mertebeli noktalarının oluşturduğu alt gruba E nin *torsiyon alt grubu* denir ve bu alt grup $E_{\text{tors}}(\mathbb{Q})$ ile gösterilir. r negatif olmayan tamsayı olmak üzere $E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$ grubuna E nin *Mordell-Weil grubu* ve r sayısına da *E nin rankı* denir.

2.6.3 Uyarı 1. E eliptik eğrisi için

$$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$$

dir.

2. Trygve Nagell ve Elisabeth Lutz'in 1930'larda bağımsız olarak ispatladığı aşağıdaki teorem kullanılarak bir E eliptik eğrisi verildiğinde $E_{\text{tors}}(\mathbb{Q})$ u belirlemek mümkündür.

2.6.4 Lutz-Nagell Teoremi. (Washington 2003)

$$E : y^2 = x^3 + Ax + B, \quad (A, B \in \mathbb{Z})$$

$\mathbb{Q}$ üzerinde bir eliptik eğri, $P = (x, y) \in E(\mathbb{Q})$ noktası ise sonlu mertebeli olsun. Bu durumda $x, y \in \mathbb{Z}$'dir ve $y \neq 0$ olması halinde

$$y^2 \mid 4A^3+27B^2$$

olur.

Aşağıdaki sonuç Mordell-Weil Teoremi'nin direk bir sonucudur.

2.6.5 Sonuç. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda $E_{\text{tors}}(\mathbb{Q})$ sonludur.

2.6.6 Uyarı 1. $r = 0$ durumunda $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi üzerinde sonlu tane rasyonel nokta olacağı, yani $E(\mathbb{Q})$ nun sonlu olacağı açıktır. Bu özellikteki eliptik eğriler bu çalışma için oldukça önemli bir eğri ailesi oluşturmaktadır.

2. $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi verildiğinde $E_{\text{tors}}(\mathbb{Q})$ nun izomorf olabileceği tüm gruplar Barry Mazur'un (1977) ve (1978) aşağıdaki teoremiyle verilmiştir.

2.6.7 Teorem. (Mazur 1977, 1978) E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$E_{\text{tors}}(\mathbb{Q}) = \begin{cases} \mathbb{Z}_n & : 1 \le n \le 10, n = 12 \\ \mathbb{Z}_n \oplus \mathbb{Z}_n & : 1 \le n \le 4 \end{cases}$$

olur. Bundan başka bu gruplardan her birisi için $E_{\text{tors}}(\mathbb{Q})$ bu gruplara izomorf olacak şekilde bir E eliptik eğrisi de vardır.

2.6.8 Uyarı 1. Yukarıdaki teoremler yardımıyla $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisinin torsiyon alt grubunu belirlemek mümkün olduğu halde verilen bir eliptik eğrinin rankını hesaplamak çok daha zordur ve genel olarak bir eliptik eğrinin rankını hesaplayabilecek bir yöntem de yoktur. Bazı eliptik eğrilerin rankları, bazı programlar yardımıyla kolayca hesaplanabildiği halde bazılarının rankları ise hesaplanamamaktadır.

2. (Rubin ve Silverberg 2002) de eliptik eğrilerin rankları hakkındaki tarihsel süreç bulunabilir. Mordell-Weil grubunun tanımına dikkat edilirse, bir eliptik eğrinin rankının aslında E nin üzerindeki rasyonel noktalarının kümesine bağlı olduğu açıktır.

3. Büyük ranka sahip eliptik eğrilerin varlığı problemi güncel bir problem olup, bu çalışmanın hazırlandığı sırada literatürdeki ranklarla ilgili rekor Noam Elkies'e ait olup (2006),

$$E : y^2 + xy + y = x^3 - x^2 -$$
$$20067762415575526585033208209338542750930230312178956502x +$$
$$3448161179503055646703298569039072037485594435931918036126600829629193$$
$$9448732243429$$

eliptik eğrisi üzerinde sonsuz mertebeli bir birinden bağımsız 28 nokta hesaplandığından bu eliptik eğrinin rankı en az 28 dir. Literatürdeki diğer kayıtlara (Anonim 2011b) de erişilebileceği gibi keyfi dereceli ranka sahip olan eliptik eğrilerin varlığı da konjektür olarak ifade edilmiştir (Silverman 1986).

2.7 Eliptik Eğrilerin Kuadratik Twistleri

Çalışmada kullanılan yöntem için eliptik eğrilerin kendileri kadar onların kuadratik twistleri de oldukça önemli olduğundan bu kısımda verilen bir eğri için kuadratik twist kavramı tanımlanacaktır.

2.7.1 Tanım. E, $\mathbb{Q}$ üzerinde bir eliptik eğri, D içinde kare sayı bulundurmayan bir tamsayı ve E eliptik eğrisi

$$E : y^2 = x^3 - g_2x - g_3$$

biçiminde verilmiş olsun. *E eliptik eğrisinin D-kuadratik twisti* E_D ile gösterilir ve

$$E_D : y^2 = x^3 - g_2 D^2x - g_3D^3$$

biçiminde tanımlanır.

2.7.2 Uyarı. E ile twisti olan E_D eliptik eğrisi $\mathbb{Q}$ üzerinde izomorf olmadıkları halde $\mathbb{Q}(\sqrt{D})$ üzerinde birbirine izomorfturlar.

2.8 Eliptik Eğrilerin *L*-Fonksiyonları, *L*-Serileri ve Kondüktör

Bu kısımda eliptik eğrilerle modüler formlar arasında köprü görevi gören, eliptik eğriler için karmaşık değerli olan "*L*-Fonksiyonları" ele alınacaktır. Bu kısma kadar sadece aritmetik özellikleri ele alınan eliptik eğrilerin, *L*-Fonksiyonları yardımıyla

diğer özellikleri de incelenecektir ve bu fonksiyonların analitik özellikleri kullanılarak eliptik eğrilerin L-Serileri verilecektir. Son olarak bir eliptik eğrinin kondüktörü tanımlanacaktır.

Verilen herhangi bir eliptik eğrinin, gerektiğinde uygun değişken değişimleri yapılarak $A, B \in \mathbb{Z}$ olmak üzere $y^2 = x^3 + Ax + B$ biçiminde ifade edilebileceği daha önce belirtilmiştir.

2.8.1 Tanım. p bir asal sayı ve $E : y^2 = x^3 + Ax + B$ ($A, B \in \mathbb{Z}$) olsun. Eğer A ve B, modülo p de indirgendiğinde $y^2 \equiv x^3 + Ax + B \pmod{p}$ singüler olmayan bir eliptik eğri oluyor ise *E eliptik eğrisi modülo p de iyi indirgemeye sahiptir*, aksi takdirde *E eliptik eğrisi modülo p de kötü indirgemeye sahiptir* denir.

2.8.2 Uyarı 1. E eliptik eğrisinin modülo p de iyi ya da kötü indirgemeye sahip olması durumu tamamen E nin diskrimantına bağlı olup, Δ nın büyümesi halinde onu bölecek olan asal sayıların da artacağı fakat bunların sayısının yine de sonlu ise olacağı açıktır.

2. Bu kısımda eliptik eğrilerin L-Fonksiyonlarını tanımlamak için gerekli ön hazırlıklar yapılacaktır, ilk olarak Zeta fonksiyonları ele alınacaktır.

2.8.3 Tanım. E, $\mathbb{F}_p$ cismi üzerinde tanımlı bir eliptik eğri ve $N_n = \#E(\mathbb{F}_{p^n})$ olsun. Bu durumda *E eliptik eğrisinin Z-fonksiyonu* $Z_E(T)$ ile gösterilir ve

$$Z_{E,\,p}(T) = e^{\sum_{n=1}^{\infty} \frac{N_n}{n} T^n}$$

olarak tanımlanır.

2.8.4 Uyarı. E eliptik eğrisinin Z-fonksiyonu bu eğrinin aritmetik özelliklerini bir üreteç fonksiyonun katsayıları yardımıyla incelemeye yarar. Bu fonksiyon uygulamada daha çok aşağıdaki önermede verildiği şekliyle kullanılır.

2.8.5 Önerme. (Washington 2003) E, $\mathbb{F}_p$ üzerinde bir eliptik eğri ve $\#E(\mathbb{F}_p) = p + 1 - a$ olsun. Bu durumda

$$Z_{E,p}(T) = \frac{pT^2 - aT + 1}{(1-T)(1-pT)}$$

olur.

2.8.6 Tanım. $s \in \mathbb{C}$ olmak üzere E eliptik eğrisinin zeta fonksiyonu $\zeta_E(s)$ ile gösterilir ve İm$(z) > 0$, $q = e^{2\pi iz}$ olmak üzere

$$\zeta_{E,p}(s) = Z_{E,p}(q^{-s})$$

olarak tanımlanır.

2.8.7 Uyarı. Tanımda yer alan fonksiyona "zeta" fonksiyonu denilmesinde bu fonksiyonun da klasik Riemann-Zeta fonksiyonu ile benzer bir fonksiyonel eşitliği gerçeklemesinin rolü büyüktür. Riemann-Zeta fonksiyonu için verilen aşağıdaki konjektür, Riemann Hipotezi olarak adlandırılır.

2.8.8 Konjektür. (Riemann 1859) $s \in \mathbb{C}$ olmak üzere

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Riemann-Zeta fonksiyonu için $0 \le \text{Re}(s) \le 1$ ve $\zeta(s) = 0$ ise $\text{Re}(s) = \frac{1}{2}$ dir.

2.8.9 Teorem. (Washington 2003) E sonlu cisim üzerinde tanımlı bir eliptik eğri olmak üzere

i. $\zeta_{E,p}(s) = \zeta_{E,p}(1 - s)$,

ii. $\zeta_{E,p}(s) = 0$ ise $\text{Re}(s) = \frac{1}{2}$

dir.

2.8.10 Uyarı 1. $\#E(\mathbb{F}_p) = p + 1 - a_p$ olsun. E eliptik eğrisinin L-Fonksiyonu "yaklaşık" olarak

$$\prod_{iyi\ p}\left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \tag{2.4}$$

Euler çarpımı olarak tanımlanır. Tanımdaki "yaklaşık" nitelemesinin sebebi, bu tanımda sadece E eliptik eğrisinin kötü indirgemeye sahip olduğu p asallarının dikkate alınmayışıdır.

2. Dikkat edilirse (2.4) ifadesi $\zeta_{E,p}(s)$ nin paydasından başka bir şey değildir.

2.8.11 Tanım. E eliptik eğrisi modülo p de kötü indirgemeye sahip olsun. Bu durumda $x^3 + Ax + B$ polinomunun modülo p de katlı kökleri vardır. Buna göre

i. $x^3 + Ax + B$ polinomunun modülo p de 3 katlı kökü varsa *E eliptik eğrisi modülo p de toplamsal indirgemeye sahiptir*,

ii. $x^3 + Ax + B$ polinomunun modülo p de 2 katlı kökü varsa *E eliptik eğrisi modülo p de çarpımsal indirgemeye sahiptir* denir. Üstelik singüler noktadaki teğet doğrunun eğimi $\mathbb{F}_p$ de kalıyor ise *E parçalanmış çarpımsal indirgemeye*, aksi takdirde *E parçalanmamış çarpımsal indirgemeye sahiptir* denir.

2.8.12 Örnek. $E : y^2 = x\,(x + 35)(x - 55)$ eliptik eğrisi göz önüne alınsın. E eliptik eğrisi modülo 5 de indirgenirse

$$E : y^2 = x^3$$

halini alır, bu durumda 3 katlı kök olduğundan, E eliptik eğrisinin modülo 5 deki kötü indirgemesinin çeşidi toplamsal indirgemedir. Diğer yandan aynı eğri modülo 7 de

$$y^2 = x^2\,(x + 1)$$

biçiminde bir kötü indirgemeye sahip olup, (0, 0) noktasındaki teğetin eğimi $\mathbb{F}_7$ de kaldığı için parçalanmış çarpımsal indirgemeye sahip olup, modülo 11 de indirgendiğinde

$$y^2 = x^2\,(x + 2)$$

biçimindeki kötü indirgemenin çeşidi parçalanmamış çarpımsal indirgemedir.

2.8.13 Uyarı. $\mathbb{F}_p$ cisminin karakteristiğinin 2 ve 3 olması halinde E eliptik eğrisinin kötü indirgemesinin çeşidi eğrinin Weierstrass eşitliği yardımıyla belirlenir.

2.8.14 Tanım. E, $\mathbb{F}_p$ üzerinde tanımlı ve modülo p de kötü indirgemeye sahip olan bir eliptik eğri olsun. Bu durumda a_p sayısı

$$a_p = \begin{cases} 0 & : E,\ p\text{'de toplamsal indirgemeye sahip} \\ 1 & : E,\ p\text{'de parçalanmış çarpimsal indirgemeye sahip} \\ -1 & : E,\ p\text{'de parçalanmamis çarpimsal indirgemeye sahip} \end{cases} \tag{2.5}$$

biçiminde tanımlanır.

2.8.15 Tanım. E, $\mathbb{Q}$ üzerinde bir eliptik eğri ve iyi p asalları için $a_p = p + 1 - \#E(\mathbb{F}_p)$, kötü p asalları için (2.5) eşitliğindeki gibi olsun. *E eliptik eğrisinin L-Fonksiyonu*

$$L_E(s) = \prod_{\text{kötü } p} \left(1 - a_p p^{-s}\right)^{-1} \prod_{\text{iyi } p} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

Euler çarpımı olarak tanımlanır. (a_p üzerindeki $| a_p | \le \sqrt{2p}$ Hasse sınırı yukarıdaki çarpımın $\mathrm{Re}(s) > \frac{3}{2}$ özelliğindeki s sayıları için yakınsak olmasını gerektirdiğinden $L_E(s)$ fonksiyonu iyi tanımlıdır (Washington 2003).)

E eğrisinin L-Fonksiyonunun her bir $\left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$ iyi çarpanı, $a_{p^2} = a_p{}^2 - p$ olmak üzere

$$\left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} = 1 + a_p p^{-s} + a_{p^2} p^{-2s} + \ldots$$

biçiminde bir seri açılımına sahiptir.

2.8.16 Tanım. Tüm p asalları üzerinden çarpım alınmak üzere *E eğrisinin L-Serisi*

$$L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

olarak tanımlanır. Burada $n = \prod_j p_j^{e_j}$ biçiminde ise $a_n = \prod_j a_{p_j e_j}$ dir. ($L_E(s)$ serisi de $\mathrm{Re}(s) > \frac{3}{2}$ özelliğindeki s sayıları için yakınsak bir seridir.)

2.8.17 Tanım. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ve p bir asal sayı olsun. δ_p, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ nın p deki E eliptik eğrisinin $\mathsf{T}_p(E)$ Tate modülünün atalet grubu üzerindeki vahşi dallanmanın ölçümü ve

$$f_p := \begin{cases} 0: & E,\ p \text{ de iyi indirgemeye sahip} \\ 1: & E,\ p \text{ de carpimsal indirgemeye sahip} \\ 2: & E,\ p \text{ de toplamsal indirgemeye sahip ve } p \neq 2,3 \\ 2+\delta_p: & E,\ p \text{ de toplamsal indirgemeye sahip ve } p = 2,3 \end{cases}$$

olmak üzere E eliptik eğrisinin *kondüktörü* N_E ile gösterilir ve

$$N_E := \prod_P p^{f_p}$$

olarak tanımlanır (Silverman 1986).

2.8.18 Örnek 1. $E : y^2 + y = x^3 - x^2 + 2x - 2$ eliptik eğrisi göz önüne alınsın. E nin p asalında iyi ya da kötü indirgemeye, kötü indirgemeye sahipse de bu indirgemenin çeşidi öncelikle bu eğrinin diskriminantına bağlıdır. E eğrisi için $\Delta = -875$ olduğundan bu sayıyı bölen asallar için E eliptik eğrisi kötü indirgemeye sahip, diğer asallar için iyi indirmeye sahiptir. f_p nin tanımına dikkat edilirse E eğrisinin iyi indirgemeye sahip olduğu asalların, N_E sayısına herhangi bir etkisi yoktur. 875 sayısının asal çarpanları 5 ve 7 olup, $p = 5$ için E eğrisinin kötü indirgemesi toplamsal, $p = 7$ için E eğrisinin kötü indirgemesi ise çarpımsal indirgemedir. O halde

$$N_E = 25 \cdot 7 = 175$$

olur.

2. $E : y^2 = x^3 + x^2 + 4x + 4$ eliptik eğrisi göz önüne alınsın. E eğrisinin $p = 5$ ve $p = 2$ de kötü indirgemeye sahiptir. $p = 5$ deki kötü indirgemenin çeşidi çarpımsal indirgeme

olup $f_p = 1$ olup, $p = 2$ deki kötü indirgemenin çeşidi toplamsal indirgeme ve $\delta_p = 0$ olup $f_p = 2$ dir. Böylece E eğrinin kondüktörü

$$N_E = 5 \cdot 2^2 = 20$$

olur.

3. MODÜLER FORMLAR

Modüler formlar çalışmanın asıl ikinci bölümünü oluşturmaktadır. Bu bölümde modüler form ve buna bağlı kavramlar tanımlanacak, bunların temel özellikleri üzerinde durulacaktır.

3.1 Giriş

Bu kısımda modüler grup ve alt grupları tanımları hatırlatıldıktan sonra bu gruplara bağlı olarak tanımlanan modüler formlar tanımlanacaktır.

3.1.1 Tanım. R herhangi bir değişmeli halka ve R^*, R halkasının tersi olan elemanlarının çarpımsal grubu olsun. $a, b, c, d \in R$ ve $\det g = ad - bc \in R^*$ olmak üzere

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

biçimindeki matrislerin grubuna *genel lineer grup* denir ve bu grup $GL_2(R)$ biçiminde gösterilir. Özel olarak, $GL_2(R)$ nin determinantı 1 olan matrislerini oluşturduğu alt gruba ö*zel lineer grup* denir ve bu grup $SL_2(R)$ biçiminde gösterilir.

3.1.2 Uyarı 1. $GL_2(R)$ nin matrislerin çarpma işlemine göre bir grup olduğu açıktır.

2. Yukarıdaki tanımda $R = \mathbb{R}$, $\mathbb{Z}$ veya $\mathbb{Z}_n$ alınabilir. Bu çalışmada ilk iki durum ile ilgilenilecektir.

3.1.3 Tanım. $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ ve $z \in \mathbb{C}$ olmak üzere $\widetilde{\mathbb{C}} = \mathbb{C} \cup \{ \infty \}$ Riemann küresinin kesirli lineer dönüşümleri

$$gz := \frac{az + b}{cz + d}, \; g\infty := \frac{a}{c} = \lim_{z \to \infty} gz \tag{3.1}$$

olarak tanımlanır. Böylece, $g\dfrac{-d}{c} = \infty$ ve $c = 0$ olması halinde $g\infty = \infty$ olur.

3.1.4 Uyarı 1. (3.1) biçimindeki dönüşümlerin kümesi fonksiyonların bileşkesi işlemine göre bir grup oluşturur. Bu grubun elemanlarının $\widetilde{\mathbb{C}}$ kümesi üzerinde grup etkisi vardır, yani her $g_1, g_2 \in SL_2(\mathbb{R})$ ve $z \in \widetilde{C}$ için $g_1(g_2 z) = (g_1 g_2)z$ olur.

2. Dikkat edilirse $g = -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{R})$ matrisinin de (3.1) eşitliği kullanılarak özdeşlik elemanını vereceği açıktır. Bundan başka $\pm I$ matrisleri $\widetilde{\mathbb{C}}$ üzerinde aşikar olarak hareket eden tek matrislerdir. Gerçektende her $z \in \mathbb{C}$ için

$$\frac{az+b}{cz+d} = z$$

eşitliği dikkate alınırsa $cz^2 + (d - a)z - b = 0$ ve dolayısıyla $b = c = 0$ ve $a = d$ olarak bulunur. Bu özellikteki matrisler içinde determinantı 1 olan matrisler sadece $\pm I \in SL_2(\mathbb{R})$ dir.

3. Yukarıdaki tartışma nedeniyle, özdeşlikten farklı her bir elemanı aşikar olmayan harekete sahip dönüşümlerin kümesi $SL_2(\mathbb{R}) / \{ \pm I \}$, *projektif özel lineer grup* olarak adlandırılır ve $PSL_2(\mathbb{R})$ ile gösterilir.

4. $H = \{ z \in \mathbb{C} : \text{İm}(z) > 0 \}$, yani $\mathbb{H}$ üst yarı düzlem olsun. Dikkat edilirse $SL_2(\mathbb{R})$'nin elemanları $\mathbb{H}$'yi korur, yani her $z \in \mathbb{C}$ için $\text{İm}(z) > 0$ ise $\text{İm}(gz) > 0$ dir.

3.1.5 Tanım. $SL_2(\mathbb{R})$ nin

$$\Gamma := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \}$$

biçiminde tanımlanan alt grubuna *modüler grup* denir ve $SL_2(\mathbb{Z})$ ile gösterilir.

3.1.6 Tanım. N doğal sayısı için $SL_2(\mathbb{Z})$ nin

$$\Gamma(N) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : b \equiv c \equiv 0, a \equiv d \equiv 1 \bmod N \}$$

olarak tanımlanan alt grubuna *temel denklik alt grubu* denir. $SL_2(\mathbb{Z})$ nin

$$\Gamma_0(N) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N \}$$

$$\Gamma_1(N) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0, a \equiv d \equiv 1 \bmod N \}$$

olarak tanımlanan alt gruplarına da *Hecke tipindeki modüler grupları* denir.

3.1.7 Uyarı 1. N =1 durumunda

$$SL_2(\mathbb{Z}) = \Gamma_0(1) = \Gamma_1(1) = \Gamma(1)$$

olduğu açıktır.

2. Dikkat edilirse

$$SL_2(\mathbb{Z}) \supseteq \Gamma_0(1) \supseteq \Gamma_1(1) \supseteq \Gamma(1)$$

olup, üstelik $M \mid N$ özelliğindeki M ve N doğal sayıları için

$$\Gamma_0(M) \supseteq \Gamma_0(N), \Gamma_1(M) \supseteq \Gamma_1(N), \Gamma(M) \supseteq \Gamma(N)$$

olur.

3. Tanım 3.1.6 daki N sayısına $\Gamma_0(N)$, $\Gamma_1(N)$ ve $\Gamma(N)$ alt gruplarının seviyesi denir.

4. $\Gamma(N) \trianglelefteq \Gamma(1)$ dir.

3.1.8 Önerme. (Koblitz 1984) Γ modüler grup ve $\overline{\Gamma} = \Gamma / \{ \pm I \}$ olsun. Bu durumda $\overline{\Gamma}$ grubu

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \mapsto z + 1,$$

$$S := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : z \mapsto -\frac{1}{z}$$

dönüşümleri tarafından üretilir.

3.1.9 Tanım. $f(z)$, $\mathbb{H}$ üzerinde tanımlı meremorf bir fonksiyon ve k bir pozitif tamsayı olsun. $f(z)$ fonksiyonu her $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ için

$$f(\gamma z) = (cz + d)^k . f(z) \tag{3.2}$$

ve özel olarak T ve S elemanları için

$$f(z + 1) = f(z),$$
$$f(-1/z) = (-z)^k f(z)$$

eşitliklerini gerçeklesin. Üstelik $f(z)$, sonsuzda meremorf, yani $q = e^{2\pi i z}$ olmak üzere

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$$

(3.3)

Fourier serisinin $n < 0$ özelliğinde en fazla sonlu sayıda a_n katsayısı sıfırdan farklı olsun. Bu durumda $f(z)$ fonksiyonuna $\Gamma = SL_2(\mathbb{Z})$ için *k-ağırlıklı modüler fonksiyon* denir.

$f(z)$, $\Gamma = SL_2(\mathbb{Z})$ için k-ağırlıklı modüler fonksiyon olsun. Eğer $f(z)$, $\mathbb{H}$ üzerinde ve $z = \infty$ da analitik (yani her $n < 0$ için $a_n = 0$) ise $f(z)$ fonksiyonuna $\Gamma = SL_2(\mathbb{Z})$ *için k-ağırlıklı modüler form* adı verilir ve bu fonksiyonların kümesi $M_k(\Gamma)$ ile gösterilir.

Eğer $a_0 = 0$, yani modüler form sonsuzda sıfır oluyor ise $f(z)$ ye $\Gamma = SL_2(\mathbb{Z})$ için *k–ağırlıklı cusp form* denir ve bu fonksiyonların kümesi de $S_k(\Gamma)$ ile gösterilir. $f(z)$ modüler fonksiyonunun (formunun) (3.3) deki seri açılımına $f(z)$ fonksiyonunun (formunun) *q-açılımı* denir.

3.1.10 Uyarı 1. k tek sayı ise Γ için sıfırdan farklı k ağırlıklı modüler fonksiyon yoktur. Bu durum (3.2) de $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ alınarak k sayısının daima çift olması gerektiği görülebilir.

2. Belirli bir ağırlığa sahip modüler fonksiyonlar, modüler formlar ve cusp formların kümesi fonksiyonların bileşkesi ve skaler ile çarpım işlemleri ile birlikte bir karmaşık vektör uzayı olurlar. Buna ek olarak k_1 ağırlıklı bir modüler fonksiyon (ya da form) ile k_2 ağırlıklı bir modüler fonksiyonun (ya da formun) çarpımı $k_1 + k_2$ ağırlıklı, bölümü ise $k_1 - k_2$ ağırlıklı bir modüler fonksiyon (form) olur. Özel olarak sıfır ağırlıklı modüler fonksiyonların kümesi bir cisimdir (Miyake 2006).

3. $\boldsymbol{F} := \{ z \in \mathbb{H} : \mathrm{Re}(z) \le \frac{1}{2}, |z| > 1 \}$, Γ modüler grubunun temel bölgesi ve $z = x + iy$ olsun. $d\nu(z) = y^{-2}dxdy$ olmak üzere

$$< \ , \ > : M_k \times S_k \to \mathbb{C}, < f, g > := \int_F f(z)\overline{g(z)}\dot{I}m(z)^k \, d\nu(z)$$

biçiminde tanımlanan iç çarpım fonksiyonuna *Petersson iç çarpımı* denir. Bu iç çarpımla birlikte modüler formlar uzayı bir iç çarpım uzayı olur.

3.1.11 Örnek. $k > 2$ çift tamsayı olsun. $z \in H$ için

$$G_k(z) := \sum_{m,n}{}' \frac{1}{(mz+n)^k}$$

biçiminde tanımlanan seriye *Eisenstein serisi* adı verilir. Burada $\sum'$ simgesi toplamın ikisi birden aynı anda sıfır olmayan m ve n tamsayı çiftleri üzerinden alındığını göstermektedir. Bu şekilde tanımlanan G_k fonksiyonu bir modüler formdur, yani $G_k(z) \in M_k(\Gamma)$ dır (Koblitz 1984). $G_k(z)$ nin q-açılımı hakkında aşağıda verilen önerme modüler formlar üzerinde aritmetik yapmayı kolaylaştırır.

3.1.12 Önerme. (Koblitz 1984) $k > 2$ çift tamsayı ve $z \in \mathbb{H}$ olsun. Bu durumda

$$G_k(z) = \sum_{m,n}' \frac{1}{(mz+n)^k}$$

fonksiyonunun

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right)$$

biçiminde bir q-açılımı vardır, burada $q = e^{2\pi iz}$, B_k, k. Bernoulli sayısı, $\zeta(k)$, Riemann-Zeta fonksiyonun k daki değeri ve

$$\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$$

dir.

3.1.13 Uyarı. Uygulamada modüler formların q-açılımındaki rasyonel katsayıları elde edebilmek için $G_k(z)$ nin *normalleştirilmiş* $E_k(z)$ *Eisenstein serisi*nin dikkate alınması gerekir. Bu seri

$$E_k(z) := \frac{1}{2\zeta(k)}\ G_k(z) = 1 - \frac{2k}{B_k}\sum \sigma_{k-1}q^n$$

biçiminde tanımlanır.

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$$

ve

$$E_{10}(z) = 1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n$$

serileri birer normalleştirilmiş serilerdir.

3.2 Hecke Operatörleri

3.2.1 Tanım. M_m katsayıları tamsayı, determinantı m olan 2×2 tipinde matrislerin kümesi ve $\Gamma = M_1$ modüler grup olsun. Ağırlığı k olan bir $f(z)$ modüler formu verilsin. Bu durumda $f(z)$ *üzerinde hareket eden m. Hecke operatörü* T_m ile gösterilir ve

$$T_m f(z) := m^{k-1} \sum_{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \backslash M_m} (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) \tag{3.4}$$

biçiminde tanımlanır.

3.2.2 Uyarı 1. Buradaki m^{k-1} çarpanı, tamsayı olan Fourier katsayılarının görüntüsünün de tamsayı olmasını gerçeklemektedir. (3.4) eşitliği düzenlenerek

$$T_m f(z) = m^{k-1} \sum_{\substack{a,d>0 \\ ad=m}} \frac{1}{d^k} \sum_{b (\mathrm{mod} d)} f\left(\frac{az+b}{cz+d}\right)$$

biçiminde ifade edilebilir.

2. $f(z) = \sum a_n q^n$ biçiminde bir q-açılımına sahipse T_m Hecke operatörü $T_m f(z) = \sum b_n q^n$ biçiminde bir q-açılımına sahiptir, burada

$$b_n = \sum_{r>0, r|(m,n)} r^{k-1} a_{mn/r^2}$$

dir.

3. Tanıma dikkat edilirse, T_m ve T_n, $f(z)$ modüler formu için Hecke operatörleri ise

$$T_m T_n f(z) = T_n T_m f(z)$$

olur.

4. $f(z)$ bir cusp form ise $a_0 = 0$ ve $T_m f(z)$ için tanım gereği $b_0 = 0$ olduğundan Hecke operatörleri S_k cusp formlar uzayını korur.

3.2.3 Tanım. $f(z) \in M_k(N)$ ve p bir asal sayı olsun. λ_p, $f(z)$ nin T_p ye karşılık gelen özdeğeri olmak üzere $p \nmid N$ özelliğindeki tüm p asalları için

$$T_p f(z) = \lambda_p \cdot f(z)$$

oluyor ise $f(z)$ ye bir *eigenform* denir.

3.2.4 Örnek. $\Delta := q\prod_{n=1}^{\infty}(1-q^n)^{24}$ şeklinde tanımlanan 12-ağırlıklı modüler form bir eigenformdur.

3.2.5 Tanım. Γ modüler grup, $M \mid N$ olmak üzere $\Gamma_0(N)$ ve $\Gamma_0(M)$, Γ nın denklik alt grupları ve d, N/M sayısını bölen bir tamsayı olsun. $g(z) \in M_k(\Gamma_0(M))$ olmak üzere $g(dz) \in M_k(\Gamma_0(N))$ biçimindeki modüler formlara $\Gamma_0(N)$ *nin eski formları* (*oldform*) adı verilir. Eski formlar tarafından gerilen uzayın dik tümleyeni olan modüler formların alt vektör uzayının elemanlarına *yeni form* (*newform*) denir.

3.3 Kuadratik Formlar ve Teta Serileri

Modüler formların çalışılmasının temel nedenlerinden birisi de herhangi bir tamsayının bir "kuadratik form" yardımıyla kaç türlü temsil edilebileceğinin araştırılmasıdır (Shimura 1973). Bu problemin çözümünde kullanılan kuadratik formlar için "teta serileri" oldukça önemli bir rol oynarlar.

3.3.1 Tanım. $a_{ij} \in \mathbb{Z}$ olmak üzere *n-değişkenli kuadratik form*

$$f(X_1, \ldots, X_n) := \sum_{i=1}^{n} a_{ii} X_i^{\,2} + \sum_{i>j} a_{ij} X_i X_j$$

biçiminde tanımlanır. $q = e^{2\pi i z}$, $z \in \mathbb{H}$ olmak üzere *f kuadratik formuna karşılık gelen teta serisi* $\theta(f)$ ile gösterilir ve

$$\theta(f)(z) := \sum_{(X_1,\ldots X_n)} q^{f(X_1,\ldots X_n)}$$

olarak tanımlanır.

3.3.2 Uyarı 1. Tanıma dikkat edilirse f bir kuadratik form ve $\theta(f)$ buna karşılık gelen teta serisi ise $\theta(f)$ nin a_m katsayısı m tamsayısının f kuadratik formu tarafından kaç türlü temsil edilebileceğini göstermektedir.

2. n-değişkenli kuadratik formlar $n\times n$ tipindeki matrisler yardımıyla temsil edilebilirler. Örneğin $n = 2$ durumunda $a, b \in \mathbb{Z}$ olmak üzere $f = aX^2 + bXY + cY^2$ kuadratik formuna karşılık gelen matris

$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

matrisidir. $f = aX^2 + bXY + cY^2$ *kuadratik formun diskriminantı* $\det(A)$ olarak tanımlanır.

3. Uygulamada genel olarak kuadratik formlar yerine matrisler kullanılır. Bu matrisler üzerinde aşağıdaki şekilde tanımlanan denklik bağıntısı yardımıyla, kuadratik formların teta serileri denklik sınıflarına ayrılabilir.

3.3.3 Tanım. R bir halka, f ve g iki kuadratik form, A ve B sırasıyla f ve g nin katsayı matrisleri olsun. Eğer $A = \alpha \cdot B$ olacak biçimde $\alpha \in SL_2(R)$ var ise f ve g kuadratik formlarına *R üzerinde benzerdir* denir.

3.3.4 Uyarı 1. Tanımlara dikkat edilirse f ve g'nin $\mathbb{Z}$'de benzer olması $\theta(f) = \theta(g)$ olmasını gerektirir. Dolayısıyla l kuadratik formların bir denklik sınıfı olmak üzere her $f \in l$ için $\theta(f)$ bir tektir.

2. Böylece $\mathbb{Z}$ üzerinde tanımlı kuadratik formların teta serileri üzerinde bir denklik bağıntısı tanımlanmış olur.

3. l kuadratik formların bir denklik sınıfı, $f \in l$ ve A, f'nin katsayı matrisi olsun. $N \in \mathbb{N}$ sayısı $N\cdot A^{-1}$ matrisi tamsayı katsayılı ve diyagonal üzerindeki elemanları çift sayı olacak

şekildeki en küçük doğal sayı ve D, f'nin diskriminantı olmak üzere t sayısı

$$t := \begin{cases} 2D : n \equiv 1 \pmod 2 \\ -D : n \equiv 2 \pmod 4 \\ D \ : n \equiv 0 \pmod 4 \end{cases}$$

olarak tanımlansın. χ_t, $\mathbb{Q}(\sqrt{t})$ ya karşılık gelen kuadratik karakter olsun. Bu notasyon ve ön hazırlık yardımıyla modüler formlar üzerinde aritmetik yapmayı kolaylaştıran ve "yarım tamsayı ağırlıklı modüler formlar" kavramına yol açan Goro Shimura'nın (1973) aşağıdaki sonucu verilebilir. Burada $M_{n/2}(N, \chi_t)$, ağırlığı $\frac{n}{2}$ olan N seviyeli, χ_t karakterli modüler formların uzayı gösterilmektedir. Dikkat edilirse n sayısının çift sayı olması halinde tamsayı ağırlıklı modüler formlar elde edilmektedir.

3.3.5 Teorem. (Shimura 1973) l, n-değişkenli kuadratik formların bir denklik sınıfı olmak üzere $\theta(l) \in M_{n/2}(N, \chi_t)$ dir.

3.3.6 Uyarı. Kuadratik formları cusp formlarda da kullanabilmek için bazı ek kavramlara gerek duyulmaktadır.

3.3.7 Tanım. f ve g kuadratik formlar olsun. Eğer f ve g hem $\mathbb{R}$ üzerinde hem de tüm p asalları için $\mathbb{Z}_p$ üzerinde benzer ise f ve g *kuadratik formlarının cinsleri aynıdır* denir.

3.3.8 Uyarı 1. Yukarıdaki tanım sadece denklik sınıflarına bağlı olduğundan kuadratik formların denklik sınıflarının cinsleri tanımlanabilir.

2. Cusp formlar ile kuadratik formların teta serilerinin arasındaki ilişki aşağıdaki teorem yardımıyla verilmiştir. Teoremdeki çıkartma işleminin yapılmasının nedeni cusp formların q-açılımında $a_0 = 0$ olmasıdır.

3.3.9 Teorem. (Siegel 1966) l_1 ve l_2 kuadratik formların aynı cinse sahip iki denklik sınıfı ise bu durumda $\theta(l_1) - \theta(l_2)$ bir cusp formdur.

3.3.10 Uyarı 1. Teorem 3.3.5 de n'nin tek olması durumu yeni bir teorinin doğmasına neden olmuş ve "Yarım Tamsayı Ağırlıklı Modüler Formlar Teorisi", Goro Shimura'nın (1973) çalışması ile şekil almıştır.

2. Doğal olarak yarım tamsayı ağırlıklı modüler formlara tek örnek kuadratik formların teta serileri değildir.

3.4 Yarım Tamsayı Ağırlıklı Modüler Formlar

Bu kısımda k tek tamsayı ve $\lambda = \frac{k-1}{2}$ olmak üzere $\frac{k}{2} = \lambda + \frac{1}{2}$ ağırlıklı modüler formlar incelenecektir. Doğal olarak bu özellikteki bir formun yani tamsayı ağırlıklı olmayan formun tamsayı ağırlıklı modüler formların tanımını da gerçeklemesi beklenir. Dolayısıyla yarım tamsayı ağırlıklı modüler formların da her $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = SL_2(\mathbb{Z})$ için

$$f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (cz+d)^{\lambda+\frac{1}{2}} f(z)$$

fonksiyonel eşitliğini gerçekleyeceği açıktır. Ancak bu basit gerçek karmaşık karekök fonksiyonu tanımlanırken logaritmanın iki dalından birisinin seçilme zorunluluğu nedeniyle oldukça karmaşık bir probleme dönüşür. Bu nedenle yarım tamsayı ağırlıklı formlarla ilgili tanımlar verilirken oldukça dikkatli olmak gerekir.

3.4.1 Tanım. $f(z)$ fonksiyonu herhangi bir $\gamma z = \frac{az+b}{cz+d}$ kesirli dönüşümü için

$$f(\gamma z) = (cz + d)^k f(z)$$

eşitliğini gerçeklesin. Bu eşitlikteki $(cz + d)^k$ terimine *otomorfi çarpanı* denir ve bu çarpan $J(\gamma, z)$ ile gösterilir.

3.4.2 Uyarı 1. Tanıma dikkat edilirse sıfırdan farklı $f(z)$ fonksiyonu için $J(\gamma, z)$ otomorfi çarpanın

$$f(\gamma z) = J(\gamma, z)\, f(z)$$

özelliğini sağladığı açıktır.

2. $J(\gamma, z)$ bir tek değildir, farklı $f(z)$ fonksiyonları için farklı otomorfi çarpanları bulunabilir. Örneğin $q = e^{2\pi i z}$, $\text{İm}(z) > 0$ olmak üzere

$$\Theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2}$$

fonksiyonun $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$ için otomorfi çarpanı

$$J(\gamma, z) = j(\gamma, z) := \left(\frac{c}{d}\right) \varepsilon_d^{-1} \sqrt{cz + d}$$

ve burada

$$\varepsilon_d = \begin{cases} 1 : d \equiv 1 \pmod 4 \\ i : d \equiv 3 \pmod 4 \end{cases}$$

dir. Bu otomorfi çarpanın sadece $\Gamma_0(4)$ için tanımlanması halinde d nin tek sayı olacağı ve dolayısıyla Legendre sembolünün iyi tanımlı olduğu açıktır.

3.4.3 Tanım. $U = \{ \pm i, \pm 1 \}$ ve $GL_2^+(\mathbb{Q})$ katsayıları pozitif rasyonel sayı olan genel lineer grup olmak üzere $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{Q})$ ve $\phi(z)$, belirli bir $u \in U^2 = \{\pm 1\}$ için,

$$\phi(z)^2 = u \frac{cz + d}{\sqrt{\det \alpha}}$$

özelliğinde bir analitik fonksiyon olsun. G kümesi bu özellikteki $(\alpha, \pm\phi(z))$ sıralı ikililerinin kümesi olmak üzere G'nin $(\alpha, \phi(z))$ ve $(\beta, \psi(z))$ *elemanlarının çarpımı*

$$(\alpha, \phi(z)) \cdot (\beta, \psi(z)) = (\alpha\beta, \phi(\beta z)\, \psi(z))$$

olarak tanımlanır.

3.4.4 Önerme. (Koblitz 1984) G kümesi Tanım 3.4.3 de verilen işlem yardımıyla bir grup olur.

3.4.5 Tanım. $k \in \mathbb{Z}$ ve $\xi = (\alpha, \phi(z)) \in G$ için $\mathbb{H}$ üzerinde tanımlı $f(z)$ fonksiyonları üzerinde $[\xi]_{k/2}$ *operatörü*

$$f(z) \mid [\xi]_{k/2} := f(\alpha z)\ \phi(z)^{-k}$$

olarak tanımlanır.

Γ', $\Gamma_0(4)$'ün bir alt grubu olsun ve $j(\gamma, z)$ çarpanı Γ' ne kısıtlanmış olsun.

$$\widetilde{\Gamma}' := \{\ \widetilde{\gamma} \mid \widetilde{\gamma} := (\gamma,\ j(\gamma, z)),\ \gamma \in \widetilde{\Gamma}'\ \}$$

olarak tanımlanır. Böylece yukarıdaki operatör $\widetilde{\Gamma}'$ için de tanımlanmış olur.

3.4.6 Tanım 1. $k \in \mathbb{Z}$ ve Γ', $\Gamma_0(4)$ ün sonlu indeksli bir alt grubu olsun. $f(z)$, her $\widetilde{\gamma} \in \widetilde{\Gamma}'$ için $[\widetilde{\gamma}]_{\frac{k}{2}}$ operatörleri altında invaryant kalan ve $\mathbb{H}$ üst yarı düzlemde meromorf olan bir fonksiyon olsun. Eğer $f(z)$, Γ' nün her bir cusp noktasında meromorf ise bu durumda $f(z)$ ye $\widetilde{\Gamma}'$ için $\frac{k}{2}$*-ağırlıklı bir modüler fonksiyon* denir.

2. Eğer $f(z)$, $\mathbb{H}$ nin tamamında ve tüm cusp noktalarında analitik bir fonksiyon ise bu durumda $f(z)$ ye $\widetilde{\Gamma}'$ için $\frac{k}{2}$*-ağırlıklı bir modüler form* denir. Bu özellikteki $f(z)$ fonksiyonlarının kümesi $M_{\frac{k}{2}}(\widetilde{\Gamma}')$ ile gösterilir.

3. Bundan başka $f(z)$ her bir cusp noktasında sıfır oluyor ise $f(z)$ ye $\widetilde{\Gamma}'$ için $\frac{k}{2}$*-ağırlıklı bir cusp form* denir. Bu özellikteki $f(z)$ fonksiyonların kümesi $S_{\frac{k}{2}}(\widetilde{\Gamma}')$ ile gösterilir.

Yarım tamsayı ağırlıklı modüler formlar üzerinde Hecke operatörünün etkisi aşağıdaki önerme yardımıyla ifade edilebilir:

3.4.7 Önerme. (Koblitz 1984) 4 | N, χ modülo N de verilen Dirichlet karakteri, $k = 2\lambda + 1$, p asal sayı, $z \in \mathbb{H}$ ve $q = e^{2\pi i z}$ olmak üzere $f(z) = \sum_{n=0}^{\infty} a_n q^n \in M_{k/2}(\widetilde{\Gamma}_0(N), \chi)$ yarım tamsayı ağırlıklı modüler form olsun. Bu durumda

$$T_{p^2} f(z) = \sum_{n=0}^{\infty} b_n q^n$$

dir, burada

$$b_n = a_{p^2 n} + \chi(p)\left(\frac{(-1)^{\lambda} n}{p}\right) p^{\lambda-1} a_n + \chi(p^2) p^{k-2} a_{n/p^2}$$

ve $\left(\frac{-}{p}\right)$ Legendre sembolünü göstermektedir, $p^2 \nmid n$ olması halinde $a_{n/p^2} = 0$ olarak alınmaktadır.

"Shimura-Shintani yükseltmesi" olarak adlandırılan aşağıdaki teorem yarım tamsayı ağırlıklı modüler formlarla tamsayı ağırlıklı modüler formlar arasındaki ilişkiyi ortaya koyar.

3.4.8 Teorem. (Shimura 1973) $\widetilde{f}$, $k + \frac{1}{2}$ ağırlıklı, f, $2k$ ağırlıklı bir modüler form ve T_n^2, $\widetilde{f}$'nin, T_n, f'nin Hecke operatörleri olsun. Bu durumda $\widetilde{f}$ verildiğinde $\widetilde{f}$ üzerindeki T_n^2 Hecke operatörünün özdeğeri, f üzerindeki T_n Hecke operatörünün özdeğerine eşit olacak şekilde $2k$ ağırlıklı bir f modüler formu bulunabilir.

3.4.9 Uyarı. Modüler formların aritmetiğinde kuadratik formların teta serilerini kullanmak önemli kolaylıklar sağlar. Diğer yandan Frey'e göre (1994) Hecke operatörlerinin modüler formlara etkisi kuadratik formların üzerindeki işlemler yardımıyla bulunabileceğinden Fourier katsayılarının hesaplanmasına gerek yoktur. 2 ve 3-değişkenli kuadratik formlar hali (Bungert 1990)'da bulunabilir. Bu çalışmada $k = \frac{1}{2}$

durumu ile ilgilenildiğinden $\frac{1}{2}$-ağırlıklı modüler formların uzayının teta serilerinin bir tabanı tarafından gerilmesi kolaylık sağlar.

3.4.10 Teorem. (Serre ve Stark 1977) 4 | N, χ modülo N'de tanımlı ve $\chi(-1) = 1$ özelliğinde bir Dirichlet karakteri olsun. $t \in \mathbb{N}$, ψ kondüktörü $r(\psi)$,

i. $\psi(-1) = 1$ ve 4. $r(\psi)^2 t \mid N$

ii. $(n, N) = 1$ özelliğindeki tüm $n \in \mathbb{Z}$'ler için $\chi(n) = \psi(n)\,\chi_t(n)$

özelliğinde bir ilkel karakter olmak üzere (ψ, t) ikililerinin kümesi $\Omega(N, X)$ olsun. Bu durumda

$$\{\ \Theta_{\psi,t} \mid \Theta_{\psi,t}(z) := \sum_{n=-\infty}^{\infty} \psi(n) q^{tn^2},\ (\psi, t) \in \Omega(N, X)\ \}$$

$M_{1/2}(N, \chi)$ için bir tabandır.

3.5 Modülarite Teoremi

Bu kısımda 2.Bölüm'de değinilen ve eliptik eğriler ile modüler formlar arasında köprü görevi kuran Modülarite Teoremi'ne yer verilecektir. Bu teorem ispatlanmadan önce Taniyama-Shimura-Weil Konjektürü olarak bilinmekteydi, problemin tarihçesi için (Darmon 1999)'a ulaşılabilir.

3.5.1 Teorem (Wiles 1995)(Breuil ve ark. 2001) E, $\mathbb{Q}$ üzerinde tanımlı kondüktörü N olan tamsayı katsayılı bir eliptik eğri ve her bir n için a_n, E eliptik eğrisinin L-fonksiyonunun n. katsayısı olsun. Bu durumda E eliptik eğrisine karşılık gelen N seviyeli 2-ağırlıklı $\sum a_n q^n$ Fourier açılımına sahip bir eigenform vardır. Denk olarak her bir eliptik eğri ile aynı L-Serisine sahip olan bir modüler form vardır.

3.5.2 Tanım. Modüler form ile aynı L-Serisine sahip olan E eliptik eğrisine *modüler eliptik eğri* adı verilir.

4. ELİPTİK EĞRİLERİN TWİST AİLELERİNİN SELMER GRUPLARI

4.1 Giriş

Bu bölümde eliptik eğrilerin Selmer gruplarının mertebeleri hakkında elde edilen bazı sayısal sonuçlar verilecektir. Çalışmada deneyimsel matematiğin yöntemleri kullanılarak elde edilen sonuçlar (İnam 2011) de yayınlanmıştır.

E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. E nin Mordell-Weil grubunu doğrudan hesaplamak çoğu zaman mümkün değildir. Bu problem E eliptik eğrisi üzerinde yeni cebirsel yapılar oluşturma ihtiyacını ortaya koymaktadır. Galois kohomolojilerinin getirdiği hesaplamaya yönelik kolaylıklar bu problemin çözülmesinde oldukça önemli bir adımdır. Bir sonraki kısımda tanımı verilecek olan E eliptik eğrisinin Tate-Shafarevich ve Selmer grupları kullanılarak E nin Mordell-Weil grubunun yapısını anlayabilmek için bazı hesaplamalar yapılabilir.

Literatürde bugüne kadar herhangi bir E eliptik eğrisinin Selmer grubunun mertebesini hesaplamaya yarayan bir algoritma bulunmamaktadır. Grubun mertebesi için oldukça kullanışlı bir formül veren Birch ve Swinnerton-Dyer Konjektürü'nün doğruluğunun kabul edilmesi bile mertebenin hesaplanmasındaki güçlüğü ortadan kaldıramamaktadır.

Ancak belirli bir eliptik eğrinin twist ailelerine yoğunlaşmak belirtilen problemi biraz da olsa kolaylaştırmaktadır. Bu eğrilerin L-Serileri için analitik bir fonksiyon oluşturarak Modüler Formlar Teorisi'ni kullanmak iyi bir fikirdir. Bu anlamda çalışmanın başlığını da oluşturan matematiğin derin teorilerinden ikisinin Modülarite Teoremi sayesinde birbirine bağlanması ve böylece bir teorideki problemlerin diğer teorideki yöntemler sayesinde çözülebilir olması çalışmanın temel dayanak noktası olmuştur.

(Anonim 2011c)'ye göre 2011 yılı itibari ile matematikte ispatlanamamış, ödüllü 6 büyük konjektürden birisi olan Birch ve Swinnerton–Dyer Konjektürü'nün doğru olduğu kabul edilerek problemin çözümünün temel taşlarından birisi olarak ifade

edilebilecek Waldspurger Teoremi (Waldspurger 1981) kullanılabilir. Bu teorem, eliptik eğri ile eşleşen ve Shimura–Shintani yükseltilmesi yardımıyla elde edilen $\frac{3}{2}$-ağırlıklı eigenform bulunması halinde eliptik eğrilerin twist ailelerinin Selmer gruplarının mertebelerini hesaplamak için etkili bir yol gösterir. Bu durumun ayrıntıları, açıklamaları ve örnekleri (Antoniadis ve ark. 1990) da bulunabilir.

Bu çalışmada (Antoniadis ve ark. 1990) deki örnekler dikkate alınarak, bazı E eliptik eğrilerinin E_D twist ailelerinin Selmer gruplarının mertebeleri $D < 10^7$ için hesaplanmıştır. Kullanılan yöntem kısaca şu şekilde açıklanabilir:

E, $\mathbb{Q}$ üzerinde tanımlı ve Cremona veritabanına göre etiketlendirilmiş ve kondüktörü N_E olan bir eliptik eğri, D_0 ve D_1, modülo $4 \cdot N_E$ de aynı ikinci dereceden denklik sınıfında kalan iki tamsayı olsun. E_{D_0} ve E_{D_1} ise E eliptik eğrisinin sırasıyla D_0 ve D_1 twist çarpanları yardımıyla elde edilmiş olan twist eliptik eğrilerini göstersin. Yeterince küçük D_0 sayıları için elde edilen E_{D_0} twist eliptik eğrisinin Selmer grubunun mertebesi, bilinen yöntemler kullanılarak uzun hesaplamalar sonucu bulunabilir. Bu veriyi kullanarak Waldspurger Teoremi yardımıyla D_0 ile aynı denklik sınıfında kalan tüm D_1 twist çarpanlarının oluşturduğu twist eliptik eğrilerinin Selmer gruplarının mertebelerine ulaşılabilir.

Bu hesaplamalar yardımıyla aynı Selmer grubu mertebesine sahip olan eliptik eğrilerin tüm eğriler içindeki dağılımını açıklayacak olan basit bir yaklaşım fonksiyonu bulmak ve bu fonksiyonunun özelliklerini incelemek diğer bir problemdir. Bu çalışmada bu yaklaşım fonksiyonu elde edilmiş ve bu fonksiyonun seçilen mertebeden bağımsız olduğu, tüm eğriler için yaklaşım fonksiyonun sabit farkıyla aynı olduğu görülmüştür. Pozitif ranka sahip olan eliptik eğrilerin Selmer gruplarının mertebeleri 0 olarak tanımlanmıştır.

Bir eliptik eğrinin Tate-Shafarevich grubunun mertebesinin tam kare olması gerektiğinden yola çıkarak ve bu grubun Selmer grubu ile ilişkisi kullanılarak, karşılaştırma yapabilmek adına, Tate-Shafarevich grubunun mertebeleri hesaplanmıştır.

4.2 Eliptik Eğrilerin Selmer ve Tate–Shafarevich Grupları

$\mathbb{Q}$ üzerinde tanımlı eliptik eğrilerin cebirsel yapılarından ikisi olan Selmer ve Tate–Shafarevich grupları oldukça önemli bir araştırma alanı oluşturmaktadırlar. Bu kısımda bu gruplar tanımlanacak ve bu gruplar hakkında bazı bilgiler verilecektir. Bu grupları tanımlayabilmek için bazı ön hazırlıklara gerek vardır.

E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri, $\overline{\mathbb{Q}}$, $\mathbb{Q}$'nun cebirsel kapanışı ve

$$G_{\mathbb{Q}} := Aut_{\mathbb{Q}}(\overline{\mathbb{Q}}),$$

$\mathbb{Q}$'nun mutlak Galois grubu olsun. $m \in \mathbb{N}$ için $H^m(\mathbb{Q}, E)$ ile m. Galois kohomoloji grubu gösterilsin. Böylece her $m \in \mathbb{N}$ için $G_{\mathbb{Q}}$-modüllerinin

$$0 \longrightarrow E(\overline{\mathbb{Q}})[n] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{n} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

tam dizisi elde edilir.

(Serre 1979)'a göre Galois kohomoloji gruplarının yukarıda belirtilen kısa tam dizi ile eşleşmiş bir uzun tam dizisi vardır. Böylece bu uzun tam dizinin başlangıcı göz önüne alınarak E eliptik eğrisi ile eşleşen

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n]) \xrightarrow{\alpha} H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}}))[n] \longrightarrow 0. \qquad (4.1)$$

Kummer dizisi elde edilir.

4.2.1 Tanım. Her bir p asalı için $\mathbb{Q}$ nun p-adik valüasyona karşılık gelen $\overline{\mathbb{Q}}$ genişlemesi seçilsin. G_p, $G_{\mathbb{Q}}$ da karşılık gelen ayrışma grubu, P asal sayıların kümesi ve $\gamma_{p,n}$ dönüşümü

$$\gamma_{p,n} : H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n]) \longrightarrow H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}}))[n]$$

özelliğindeki kısıtlama dönüşümü olsun. Bu durumda E eliptik eğrisinin *Tate–Shafarevich grubu* $Sha_{\mathbb{Q}}(E)$ ile gösterilir ve

$$Sha_{\mathbb{Q}}(E)[n] := \bigcap_{p \in P} \ker(\gamma_{p,n})$$

olmak üzere

$$Sha_{\mathbb{Q}}(E) := \bigcup_{n \in \mathbb{N}} Sha_{\mathbb{Q}}(E)[n]$$

olarak tanımlanır. E eliptik eğrisinin *Selmer grubu* ise $S_{\mathbb{Q}}(E)$ ile gösterilir ve

$$S_{\mathbb{Q}}(E)[n] := \alpha^{-1}(Sha_{\mathbb{Q}}(E)[n])$$

olmak üzere

$$S_{\mathbb{Q}}(E) := \bigcup_{n \in \mathbb{N}} S_{\mathbb{Q}}(E)[n]$$

olarak tanımlanır.

Tanım dikkate alınırsa, bu grupların birbirleriyle oldukça ilginç ilişkilerinin olduğu görülür. E eliptik eğrisinin Selmer grubu ile Tate–Shafarevich grubu arasındaki bu ilişki aşağıdaki önerme yardımıyla verilmiştir.

4.2.2 Önerme. (Silverman 1986) E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ise

$$0 \longrightarrow E(\mathbb{Q}) / nE(\mathbb{Q}) \longrightarrow S_{\mathbb{Q}}(E)[n] \longrightarrow Sha_{\mathbb{Q}}(E)[n] \longrightarrow 0$$

dizisi tamdır.

4.2.3 Uyarı. Önerme 4.2.2'e dikkat edilirse $E(\mathbb{Q})$ sonlu ise yani rank($E(\mathbb{Q})$) = 0 ise, E eliptik eğrisinin Selmer grubu ile Tate-Shafarevich grubu arasındaki ilişki

$$\#S_{\mathbb{Q}}(E) = \#Sha_{\mathbb{Q}}(E) \cdot \#E(\mathbb{Q})_{tors}$$

şeklindedir.

Eliptik eğrilerin twist ailelerindeki eğrilerin Selmer gruplarını hesaplamak için Birch ve Swinnerton–Dyer konjektürünün (Birch ve Swinnerton–Dyer 1965) doğru olduğunun kabul edilmesi oldukça önemli bir adımdır. Aşağıda adı geçen konjektürün özel bir hali göz önüne alınmıştır.

4.3 Birch ve Swinnerton–Dyer Konjektürü

E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ve L_E, E eliptik eğrisinin L-fonksiyonu olsun. Bu durumda

$$\text{“}L_E(1) \neq 0 \Leftrightarrow E(\mathbb{Q}) \text{ sonlu bir gruptur”},$$

böylece E eliptik eğrisinin Selmer grubu sonludur ve üstelik

$$L_E(1) = \left(\int_{E^0(\mathbb{R})} |\, \omega_E \,| \right) \left(\prod_{p|N\cdot\infty} c_p \right) \frac{\#S_{\mathbb{Q}}(E)}{\#(E(\mathbb{Q}))^3} \tag{4.2}$$

dir, burada $E^0(\mathbb{R})$, $E(\mathbb{R})$ nin bağlantılı bileşeni, ω_E değeri E eliptik eğrisinin Néron diferensiyeli, $c_\infty = [E(\mathbb{R}) : E^0(\mathbb{R})]$ ve p asalları için $c_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$ dir.

4.3.1 Uyarı 1. Aksi belirtilmedikçe, çalışma boyunca Birch ve Swinnerton–Dyer Konjektürü'nün doğru olduğu kabul edilecektir.

2. Konjektürün (4.2) eşitliğindeki c_p sayılarına *yerel Tamagawa sayıları* adı verilir.

3. Yukarıda, kullanılacak olan, bazı özel halleri verilen Birch ve Swinnerton-Dyer Konjektürü'nün (4.2) eşitliğindeki eliptik eğrinin Selmer grubunun mertebesi dışındaki değerler, üzerlerinde oldukça yoğun bir çalışma yapılması halinde hesaplanabilirdirler. Bazı özel durumlarda ise eliptik eğrilerin Selmer gruplarının mertebelerini hesaplamak mümkün olabilir. Ancak bu durumda doğal olarak $E(\mathbb{Q})$ nun mertebesinin sonlu olduğu kabul edilmelidir.

4. Eliptik eğrinin Selmer grubunun mertebesi ile $L_E(1)$ değerlerini hesaplamak için modüler formların analitik özellikleri kullanılacaktır.

Hesaplamalardaki algoritmaların tamlığını, yani çalıştırabilir olduğunu ve sonuçların doğruluğunu test etmek için bir kriter (Cassels 1965)'te verilmiştir.

4.3.2 Teorem. (Cassels 1965) E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$\Gamma : Sha_{\mathbb{Q}}(E) \times Sha_{\mathbb{Q}}(E) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

alterne, 2-lineer eşleme (pairing) dönüşümü vardır ve bu dönüşümün çekirdeği eliptik eğrinin Tate–Shafarevich grubunun bölünebilir elemanlarının grubudur. Özel olarak eğer $S_{\mathbb{Q}}(E)$ sonlu mertebeli ise bu durumda $\#Sha_{\mathbb{Q}}(E)$ sayısı bir tam karedir.

4.4 Waldspurger Teoremi ve Sonuçları

E eliptik eğrisi $\mathbb{Q}$ üzerinde tanımlı ve rankı sıfır olan bir eliptik eğri olsun. Birch ve Swinnerton-Dyer Konjektürü kullanılarak E eliptik eğrisinin Selmer grubunun mertebelerinin hesaplanabileceği daha önce belirtilmişti. Dikkat edilirse ω_E Néron diferensiyelini, dolayısıyla $\int_{E^0(\mathbb{R})} |\omega_E|$ değerlerini ve yerel Tamagawa sayılarını hesaplamak kolaydır. ω_E transandantal bir sayı olup belirli bir haneye kadar hesaplanabilir. E eliptik eğrisinin Selmer grubunun mertebesinin hesaplanmasında en çok zamanı $L_E(1)$ değerini hesaplanması alır. Bu değeri hesaplamak için MAGMA

Cebir programında (Bosma ve ark 2007) bir rutin (kod) vardır. Örneğin bu rutin yardımı ile Cremona veritabanında "11a1" olarak verilen $\mathbb{Q}$ üzerinde tanımlı

$$y^2 + y = x^3 - x^2 - 10x - 20$$

eliptik eğrisi için $L_E(1)$ değeri virgülden sonra 30 basamak hassasiyetinde şu şekilde hesaplanır:

```
> E:=EllipticCurve("11a1");
> E;
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 10*x - 20 over Rational Field
> a:=LSeries(E);
> d:=Evaluate(a,1);
> d;
0.253841860855910684337758923351
```

E eliptik eğrisinin kondüktörü yeterince küçük olduğunda MAGMA Cebir programında $L_E(1)$ değerinin hesaplaması zaman almaz. Örneğin kondüktörü 11 olan yukarıdaki eliptik eğri için hesaplama süresi

```
> time d;
0.253841860855910684337758923351
Time: 0.000
```

olur. Ancak eliptik eğrinin kondüktörü büyüdükçe transandantal olan $L_E(1)$ değerini istenen hassaslık derecesinde hesaplama süresi, düzenli olmasa da, giderek artmaktadır. Örneğin

$$E : y^2 = x^3 - 87662765543106x + 57220550111643243204293265 6$$

eliptik eğrisinin kondüktörü 11520793560025904 olup Intel Core 2 Duo işlemcili 1 GB DDR2, 2.00 GHz sanal belleğe sahip dizüstü bilgisayarında kurulu MAGMA Cebir programında 1000 saatlik hesaplama sonucunda istenilen sonuca ulaşılamamıştır. Ancak Kısım 4.5'de verilecek olan algoritma kullanılarak bu eliptik eğri için $L_E(1)$ değeri

$$L_E(1) = 2.100720230610904181109276267 75$$

olarak bulunmuştur (yaklaşık 360 saniye). Buradaki E eliptik eğrisi "11a1" eğrisinin –8090677 ile twist edilmiş halidir.

Yukarıda verilen E eliptik eğrisinin seçimi çalışmanın hesaplama alanında rastgele yapılmış olup eliptik eğriler kondüktörlerine göre sıralandığında son örnekteki E eliptik eğrisi orta sıralarda yer almaktadır. Kondüktörü çok daha büyük olan E eliptik eğrileri için $L_E(1)$ değerini hesaplamak oldukça uzun zaman alıcı olduğu halde sonuca ulaşılacağına dair bir garanti de yoktur. Bu çalışmada Birch ve Swinnerton-Dyer Konjektürü ve Waldspurger Teoremi yardımıyla elde edilen algoritma yardımıyla çalışmanın hesaplama alanında yer alan tüm E eliptik eğrileri için $L_E(1)$ değerleri oldukça kısa bir sürede bulunmuş ve böylece bu E eliptik eğrilerin Selmer gruplarının mertebeleri hesaplanabilmiştir.

Bu hesaplama sürecindeki bir başka problem ise hesaplama yardımıyla $L_E(1) = 0$ özelliğindeki E eliptik eğrilerinin hangi eğriler olduklarının belirlenmesidir. Dikkat edilirse bu özellikteki eliptik eğrilerin ranklarının pozitif ve üzerinde sonsuz tane rasyonel nokta bulunduğu daha önce görülmüştü. Daha önce bu eliptik eğrilerin Selmer gruplarının mertebesi 0 olarak kabul edildiği de belirtilmişti.

E eliptik eğrileri üzerine kısıt konulmadan çalışma yapılması probleminin zorluğu Waldspurger Teoremi yardımıyla eliptik eğrilerin twist aileleri üzerinde ele alınması ile ortadan kalkar.

4.4.1 Waldspurger Teoremi. (Waldspurger 1981) E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ve f_E bu eğriye karşılık gelen yeni form olsun. $F_E \in S_{3/2}(N', \chi_1)$ bir eigenform ve $\boldsymbol{S}$, Shimura-Shintani yükseltmesi olmak üzere $\boldsymbol{S}(F_E) = f_E$ olduğu kabul edilsin. a_n, F_E nin n. Fourier katsayısı ve $n \cdot n_0$, N' ile aralarında asal olmak üzere içinde tam kare bulundurmayan $n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2}$ özelliğindeki n ve n_0 doğal sayıları için

$$a_{n_0}^2 \sqrt{n} L_{E_{-n}}(1) = a_n^2 \sqrt{n_0} L_{E_{-n_o}}(1)$$

olur. Üstelik $n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2}$ özelliğindeki n ve n_0 doğal sayıları için $a_{n_0} \neq 0$ dir $\Leftrightarrow$ $L_{E_{-n_o}}(1) = 0$ dır. $L_{E_{-n_o}}(1) \neq 0$ dir $\Leftrightarrow a_n \neq 0$ dır.

Waldspurger Teoremi, Birch ve Swinnerton–Dyer Konjektürü ile birleştirilerek çalışmanın temelini oluşturan aşağıdaki sonuç verilebilir.

4.4.2 Teorem. (Antoniadis ve ark. 1990) Waldspurger Teoremi'ndeki notasyon ve kabuller geçerli olsun. $a_{n_0} \cdot L_{E_{-n}}(1) \neq 0$ olmak üzere E eliptik eğrisinin E_{-n} ve E_{-n_0} twist eliptik eğrileri için Birch ve Swinnerton–Dyer Konjektürü'nün doğru olduğu kabul edilsin. Bu durumda ya rank($E_{-n}(\mathbb{Q})$) ≥ 2 dir ya da $d(n, n_0)$, n ve n_0 ın bölen yapısına bağlı 2 nin bir kuvveti olan bir sabit olmak üzere

$$\#S_{\mathbb{Q}}(E_{-n}) = d(n,n_0)\cdot\#S_{\mathbb{Q}}(E_{-n_0})\cdot\frac{a_n^2}{a_{n_0}^2} \tag{4.3}$$

olur.

4.5 $d(n, n_0)$ Sabitlerinin Hesaplanması

Bu kısımda Teorem 4.4.2'de yer alan ve asıl hesaplamada kullanılacak olan $d(n, n_0)$ sabitlerinin hesaplanışı üzerinde durulacaktır. Kondüktörü N_E olan E eliptik eğrisinin E_{-n} ve E_{-n_0} twist eliptik eğrileri Waldspurger Teoremi'ndeki gibi olsun. (4.2) ve (4.3) eşitlikleri dikkate alındığında $d(n, n_0)$ sabitlerinin Tamagawa sayılarına, E_{-n} ve E_{-n_0} twist eliptik eğrilerinin torsiyon alt gruplarına bağlı olduğu görülür. Eliptik eğrilerin twistlerinin bazı basit özellikleri kullanılarak $d(n, n_0)$ sabitlerinin reel periyotlara bağlı değildir, gerçekten de E_{-n} nin reel periyodu $\int_{E^0(\mathbb{R})} |\omega_{E_{-n}}|$ ve E_{-n_0} nin reel periyodu $\int_{E^0(\mathbb{R})} |\omega_{E_{-n_0}}|$ ise

$$\frac{\int_{E^0(\mathbb{R})} |\omega_{E_{-n}}|}{\int_{E^0(\mathbb{R})} |\omega_{E_{-n_0}}|} = \frac{\sqrt{n_0}}{\sqrt{n}}$$

dir. Dolayısıyla E_{-n} ve E_{-n_0} eğrileri için Waldspurger Teoremi uygulanıp, Teorem 4.4.2 deki (4.2) formülü ile oranlandığında reel periyotlar sadeleşmektedir.

$d(n, n_0)$ sabitlerinin torsiyon grubunun elemanlarından bağımsız olduğu şu şekilde görülebilir. E eğrisi üzerinde mertebesi 2 olan noktalar $(x, 0)$ biçiminde olduğundan her E ve E_{-n} twist eliptik eğri çifti için

$$E(\mathbb{Q})[2] = E_{-n}(\mathbb{Q})[2]$$

olur. Verilen bir E eliptik eğrisi için $\mathbb{Q}$ üzerinde mertebesi 2 den büyük torsiyon noktasına sahip olan çok az sayıda twist eliptik eğrisi vardır. Bu az sayıdaki twist eliptik eğrilerinin ihmal edilmesi ise istatistiksel sonucu değiştirmeyeceğinden E eliptik eğrisinin tüm twist ailelerinin üzerinde mertebesi 2 yi bölen rasyonel noktaların bulunduğu kabul edilebilir. Gerçekten de çalışmada ele alınan E eliptik eğrilerinin aşikar olmayan twist eliptik eğri ailelerinin tamamı bu özelliktedir. Böylece

$$\#E_{-n_0}(\mathbb{Q})[n] = \#E_{-n}(\mathbb{Q})[n]$$

olup $d(n, n_0)$ sabitleri torsiyon elemanlarından bağımsızdır. Dolayısıyla $d(n, n_0)$ sabitlerinin tamamen Tamagawa sayılarına bağlı olduğu sonucu elde edilir.

E eliptik eğrisinin tüm twistlerinin bağlantılı bileşenlerinin grubu $\mathbb{R}$ üzerinde eşit olduğundan $d(n, n_0)$ sabitlerinin hesaplanması yalnızca Archimedean olmayan Tamagawa sayılarına bağlıdır. E eliptik eğrisinin E_{-n} ve E_{-n_0} twistlerinin p asalındaki Tamagawa sayıları sırasıyla $c_{n,p}$ ve $c_{n_0,p}$ gösterilsin.

İlk olarak p asal sayısı $n_0 \cdot n \cdot N_E$ sayısı ile aralarında asal olsun. Bu durumda E_{-n} ve E_{-n_0} twist eliptik eğrileri modülo p de iyi indirgemeye sahip olduğundan Tamagawa sayıları $c_{n,p} = c_{n_0,p} = 1$ dir.

Öte yandan kabul gereği $-n$ ve $-n_0$, N_E nin bölenlerine göre karelerin aynı denklik sınıfında yer aldığı için yani $n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2}$ olduğundan N_E yi bölen tüm p asalları için E_{-n} ve E_{-n_0} twist eliptik eğrilerinin Néron modelleri birbirine eşittir. p asalı örneğin N_E ile aralarında asal olan n sayısının bir böleni olsun. p tek sayı ve E eliptik eğrisi modülo p de iyi indirgemeye sahip olduğundan (Silverman 1986) sayfa 359'daki çizelge kullanılabilir. Buna göre E eliptik eğrisinin Kodaira sembolü I_0 olup, $c_{n,p} = 4$ olur. Benzer sonuç doğal olarak $-n_0$ için de geçerlidir. Böylece aşağıdaki teoremin ispatı elde edilir:

4.5.1 Teorem. (İnam 2011) E, $\mathbb{Q}$ üzerinde tanımlı kondüktörü N_E olan bir eliptik eğri, p asal sayı, $-n$ ve $-n_0$ Waldspurger Teoremi'ndeki özellikleri gerçekleyen içinde tam kare bulundurmayan tamsayılar, E_{-n} ve E_{-n_0}, E eliptik eğrisinin twist eliptik eğrileri olsun. $c_{n,p}$ ve $c_{n_0,p}$ sırasıyla E_n ve E_{-n_0} twist eliptik eğrilerinin p asalı için Tamagawa sayıları olmak üzere

$$d(n,n_0) = \frac{\prod c_{n,p}}{\prod c_{n_0,p}} = \frac{4^{\#div(n)}}{4^{\#div(n_0)}} \tag{4.4}$$

dir, burada $\#div(-)$, "$-$" sayısının asal bölenlerinin sayısını göstermektedir.

4.5.2 Uyarı. Waldspurger Teoremi'ni $\{E_{-n}\}$ eliptik eğrilerin twist ailesine uygulayabilmek için teoremde adı geçen E eliptik eğrisine karşılık gelen F_E eigenformunun bulunması gerekir. Ardından F_E eigenformunun Fourier katsayılarının mümkün olduğu kadar çok sayıdasının çok hızlı bir şekilde hesaplamaya yarayacak bir algoritmanın yazılması gereklidir. Çalışmada ele alınan örnek eigenformlar ve algoritma bundan sonraki kısımda ele alınacaktır.

4.6 Fourier Katsayılarının ve Selmer Grubunun Mertebesinin Hesaplanması

E, $\mathbb{Q}$ üzerinde tanımlı ve Cremona veritabanı formatında verilmiş, kondüktörü N_E olan bir eliptik eğri, F_E, E eliptik eğrisine karşılık gelen $\frac{3}{2}$-ağırlıklı eigenform olsun. Özel olarak bu çalışmada (Frey 1994) de yer alan ve Çizelge 4.1 de verilen örnekler ele alınmıştır.

Çizelge 4.1 Örnek Eliptik Eğriler ve Bunlara Karşılık Gelen Eigenformlar

E	F_E
11a1	$(\Theta(X^2+11Y^2) - \Theta(3X^2+2XY+4Y^2))\cdot\ \Theta_{id,11}$
14a1	$(\Theta(X^2+14Y^2) - \Theta(2X^2+7Y^2))\cdot\ \Theta_{id,14}$
17a1	$(\Theta(3X^2-2XY+23Y^2) - \Theta(7X^2+6XY+11Y^2))\cdot\ \Theta_{id,17}$
20a1	$(\Theta(X^2+20Y^2) - \Theta(4X^2+5Y^2))\cdot\ \Theta_{id,20}$
34a1	$(\Theta(X^2+17Y^2) - \Theta(2X^2+2XY+9Y^2))\cdot\ \Theta_{id,17}$

Çizelgede $\Theta(\cdot)$, iki değişkenli kuadratik formların teta serisi ve

$$\Theta_{\psi,t} := \sum_{n=-\infty}^{\infty} \psi(n) q^{tn^2}$$

karakteri ψ olan Fourier serisidir.

Çalışmada $F_E \in S_{3/2}(N', \chi_1)$ nin Fourier katsayılarını hesaplamak için aşağıdaki strateji takip edilmiştir.

4.6.1 Strateji (İnam 2011)

Adım 1. F_E nin q-açılımı hesaplanır, yani $F_E = \sum_{n=1}^{\infty} a_n q^n$ olacak biçimde bir Fourier serisi bulunur ve bu seri yardımıyla

$$L := \{ (n, a_n) : n \in \{ 1, \ldots, M \} \text{ tam kare bulundurmayan sayı } \}$$

listesi oluşturulur.

Adım 2. *Denklik Sınıflarının Seçimi:* Waldspurger Teoremi'ni uygulayabilmek için n ve n_0, N' ile aralarında asal ve $n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2}$ özelliğindeki tek sayılar olmak üzere – n ve $-n_0$ twist faktörleri yardımıyla oluşturulan eliptik eğriler göz önüne alınır. Yukarıdaki denklik koşulu hesaplamada zorluklar getirdiğinden bu ifade aşağıdaki ile değiştirilebilir, yani

$$n \equiv n_0 \ \ 8 \cdot \bmod \prod_{2 \neq p|N_E} p \ \Rightarrow \ n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2}$$

olur. Bu özellikteki twist faktörlerinin oluşturduğu twist eliptik eğri aileleri göz önüne alınır.

Adım 3. Yukarıdaki denklik sınıflarına karşılık gelen twist ailelerinin içerisinde tamamı pozitif ranka sahip olan tek eliptik eğrilerin oluşturduğu denklik sınıflarını silinir (F_E nin bu denklik sınıflarında yer alan tüm katsayıları sıfırdır).

Adım 4. $N_E = 11$ ve $N_E = 17$ durumları basitleştirilebilir. Waldspurger Teoremi'ne göre bu örneklerde denklik sınıfları sırasıyla modülo 88 ve modülo 136 ya göre bulunmalıdır. Ancak yapılan hesaplamalar sonucunda yukarıdaki örnekler için denklik sınıflarının sırasıyla modülo 44 ve modülo 68 olarak alınabileceği görülmüştür. Buna göre her bir eliptik eğri için denklik sınıfları aşağıdaki çizelgede verilmiştir.

Çizelge 4.2 Denklik Sınıfları

E	mod	n_0
11a1	44	1, 3, 5, 15, 23, 31, 37
14a1	56	1, 15, 23, 29, 37, 39, 53
17a1	68	3, 7, 11, 23, 31, 39
20a1	40	1, 21, 29
34a1	168	1, 13, 19, 21, 33, 35, 43, 53, 59, 67, 69, 77, 83, 89, 93, 101, 115, 117, 123

Adım 6. Belli bir n_0 tamsayısı için M bir tamsayı olmak üzere

$$x_{n_0}(M) := \#\{\ n : n < M,\ n \text{ tam kare bulundurmayan tamsayı } n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2}\ \}$$

ve

$$s_{n_0,0,E}(M) := \#\{n : n < M,\ n \text{ tam kare bulundurmayan tamsayı } n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2},\ a_n=0\}$$

fonksiyonları oluşturulur ve $s_{n_0,0,E}(M)/x_{n_0}(M)$ fonksiyonun grafiği çizilir.

Adım 7. $\alpha \in \mathbb{R}$ ve $\varepsilon \in [-0{,}02,\ 0{,}02]$ sayısı

$$\sigma(x_{n_0}(M)) = \alpha \frac{(\log\log(x_{n_0}(M))^{1+\varepsilon}}{\log(x_{n_0}(M))}$$

fonksiyonu $s_{n_0,0,E}(M)/x_{n_0}(M)$ fonksiyonuna "iyi" yaklaşacak şekilde seçilir.

Adım 8. Eğer $a_{n_0} = 0$ ise n_0 sayısı aynı denklik sınıfında $a_{n_0} \neq 0$ olacak şekildeki en küçük n sayısı olarak seçilir. Birch ve Swinnerton-Dyer konjektürü kullanarak

$$L_{E_{-n_0}}(1) \text{ ve } \#S_{\mathbb{Q}}(E_{-n_0})$$

değerleri ve

$\#E_{-n_0}(\mathbb{Q})_{tors}$ hesaplanır.

Adım 9. Kısım 4.5'de tanımlanan $d(n, n_0)$ sabitleri hesaplanır.

Adım 10. Birch ve Swinnerton-Dyer konjektürü gereği E_{-n} eliptik eğrisinin Selmer grubunun mertebesi, yani

$$s_{E_{-n}} := \frac{\#S_Q(E_{-n_0}) \cdot a_n^2}{d(n,n_0) \cdot a_{n_0}^2}$$

hesaplanır.

Adım 11. $t := \#E(\mathbb{Q})$ olmak üzere t sayısı hesaplanır. Dikkat edilirse E eğrisinin torsiyon alt grubu ile twistlerinin torsiyon alt grupları aynıdır.

Adım 12. M, k ve n_0 tamsayıları için

$$s_{n_0,k,E}(M) := \#\{\, n : n < M,\ n \text{ tam kare bulundurmayan tamsayı } n \equiv n_0 \bmod \prod_{p|N'} \mathbb{Q}_p^{*2},\ \frac{s_{E_{-n}}}{t} = k \,\}$$

fonksiyonu oluşturulur ve $s_{n_0,k,E}(M) / x_{n_0}(M)$ fonksiyonun grafiği çizilir.

Adım 13. $\alpha \in \mathbb{R}$ ve $\varepsilon \in [-0{,}02,\ 0{,}02]$ sayısını

$$\sigma(x_{n_0}(M)) = \alpha \frac{(\log\log(x_{n_0}(M))^{1+\varepsilon}}{\log(x_{n_0}(M))}$$

fonksiyonu $s_{n_0,k,E}(M) / x_{n_0}(M)$ fonksiyonuna "iyi" yaklaşacak şekilde seçilir.

4.6.2 Uyarı 1. Bu algoritmanın uygulanması sonucunda elde edilen tüm veriler (Anonim 2011d)'de bulunabilir.

2. $\#S_{\mathbb{Q}}(E_{-n})$, $d(n, n_0)$ ve $L_{E_{-n_0}}(1)$ değerleri hesaplandıktan sonra $L_{E_{-n}}(1)$ değeri Birch ve Swinnerton-Dyer Konjektürü kullanılarak

$$L_{E_{-n}}(1) = \frac{L_{E_{-n_0}}(1) \cdot \#S_{\mathbb{Q}}(E_{-n}) \cdot d(n, n_0)}{\#S_{\mathbb{Q}}(E_{-n_0})}$$

yardımıyla çok daha hızlı bir şekilde hesaplanabilir. Dikkat edilirse transandant olan $L_{E_{-n}}(1)$ değeri tamamen $L_{E_{-n_0}}(1)$ değerinin hassaslık derecesine bağlıdır, yani bu transandant sayının ondalık kısmında seçilecek olan basamak sayısı $L_{E_{-n}}(1)$ in basamak sayısını da belirleyecektir.

3. σ fonksiyonundaki α ve ε sabitleri şu şekilde belirlenir. Çalışmada $M = 10^7$ sınırına kadar elde edilen veriler kullanılarak belli bir E eliptik eğrisi ve n_0 tamsayısı için $I := [0, M]$ aralığının,

$I_i = [0, 50000i]$, her bir $i = 1, 2, \ldots, 200$ için

olarak tanımlanan alt aralıklarının

$$I_0 \subset I_1 \subset \ldots \subset I_n$$

biçiminde bir $\{ I_i \}_{i = 1, \ldots, 200}$ ailesi oluşturulsun. I aralığının bu şekilde 200 aralığa bölünmesi yapılan işlemler için anlamlıdır. İlk olarak max(I_i) = M_i olmak üzere $\frac{s_{n_0,k}(M_i)}{x_{n_0}(M_i)}$ değeri, daha sonra $\frac{\log(\log(x_{n_0}(M_i)))}{\log(x_{n_0}(M_i))}$ değeri hesaplanır. Bu iki değer karşılaştırılarak α_i sabiti bulunur. Bu işlemler tüm I_i aralıkları için tekrarlanır ve her bir aralık için α_i sabiti bulunur. Bu şekilde bulunan α_i sabitlerinin $x_{n_0}(M)$ değerine göre ağırlıklı ortalaması yardımıyla, her bir n_0 doğal sayısı için bir tek α sabiti bulunur. Bulunan bu α sabiti yardımıyla

$$\frac{s_{n_0,k}(x_{n_n}(M))}{x_{n_0}(M)} \quad \text{ve} \quad \alpha \frac{\log(\log(x_{n_0}(M)))}{\log(x_{n_0}(M))}$$

değerleri karşılaştırılarak, bu iki değeri birbirine daha da yaklaştırmak için [–0,02, 0,02] aralığında uygun bir ε sabiti seçilir, doğal olarak ε sabiti n_0 ile bir tek şekilde bellidir.

4.7 Sonuçlar

Bu kısımda ilk olarak eliptik eğrilerin twist ailelerinin Selmer gruplarının mertebelerinin dağılımları ele alınacak ve bu dağılım basit bir fonksiyonla ifade edilecektir. Daha sonra dağılımı belirten fonksiyon kullanılarak, bir Selmer grubunun belli bir k mertebesi için kondüktörü de seçilen belli bir değere kadar olan eliptik eğrilerin twist ailelerinden kaç eğrinin Selmer grubunun mertebesinin k olduğu yaklaşık olarak belirlenebilecektir. Son olarak dağılım fonksiyonu denilebilecek olan bu fonksiyonun grubun mertebesi olan k'dan bağımsız olduğu görülecektir. Deneyimsel yolla (hesaplama yoluyla) elde edilen bu sonuçlar literatüre birer konjektür olarak bırakılacaktır. Doğal olarak bu yolla elde edilen bu sonuçların ispatının şu an için mümkün olmadığı açıktır.

Çizelge 4.1'de yer alan keyfi fakat belli bir E eliptik eğrisi ve n_0 sayısına denk olan n sayıları ile bu eğrinin twistleri alınarak sonsuz çoklukta elemanı olan bir n_0-twist eliptik eğri ailesi elde edilebilir. Waldspurger Teoremi gereği belirtilen özellikteki n sayılarından içinde tam kare bulundurmayanların dikkate alınacağı açıktır. Yukarıdaki şekilde oluşturulan twist eğri ailesindeki eğrilerin Selmer gruplarının mertebeleri 4. Bölüm'de yer alan teknikle hesaplanabilir. Ayrıca Selmer grubunun mertebeleri kullanılarak (Cremona 1997)'de verilen diğer "BSD-verileri" de hesaplanabilir.

Bu kısmın başında belirtilen hedefe ulaşmak için aşağıdaki adımların gerçekleştirilmesi gereklidir:

1. İlk olarak her bir E eliptik eğrisi ve n_0 değeri için kondüktörü belli bir M doğal sayısına kadar olan twist eğri ailelerinde bulunan eliptik eğrilerin sayısının hesaplanması gereklidir.

2. n_0 sayısını bulunduran denklik sınıfının içinde tam kare bulundurmayan sayıların sayısının bilgisayar yardımıyla hesaplanması zor değildir.

3. Eliptik eğrinin Selmer grubunun mertebesi k olsun. Verilen bir k için belirlenen n_0-twist eğri ailesindeki eğrilerin içinde Selmer grubunun mertebesi k olanların sayısı hesaplanmalıdır.

4. Elde edilen veriler kullanılarak her bir E eliptik eğrisi için belli bir denklik sınıfında yer alan ve Selmer grubunun mertebesi k olan eliptik eğrilerin sayısı bu denklik sınıfındaki tüm eliptik eğrilerin sayısına oranına yaklaşan bir basit fonksiyon bulunmalıdır.

E bir eliptik eğri, n, n_0 ve N', Waldspurger Teoremi'ndeki özellikleri gerçekleyen sayılar olmak üzere $s_{E_{-n}}$, E_{-n} eliptik eğrisinin Selmer grubunun mertebesini göstersin. Yukarıda kullanılan k ve M tamsayıları için $s_{n_0,k,E}(M)$ ve $x_{n_0}(M)$, Strateji 4.6.1'de tanımlanan fonksiyonlar olmak üzere

$$q_{n_0,k,E} := \frac{s_{n_0,E,k}}{x_{n_0}}(M)$$

fonksiyonu tanımlansın.

Bu durumda $q_{n_0,k,E}$ fonksiyonları

$$\alpha \frac{\log\left(\log\left(x_{n_0}(M)\right)\right)^{1+\varepsilon}}{\log\left(x_{n_0}(M)\right)}$$

fonksiyonlarına "iyi yaklaşacak" biçimde $0 < \alpha < 1$ ve $\varepsilon \in [-0{,}02, 0{,}02]$ sayıları vardır.

Bu gözlem, Brian Birch tarafından öngörülen sonuçla aynıdır. Böylece aşağıdaki konjektür verilebilir.

4.7.1 Konjektür. (İnam 2011) E ve E', $\mathbb{Q}$ üzerinde tanımlı eliptik eğriler olsun. Waldspurger Teoremi'ni gerçekleyen her n, n_0 sayıları ve tüm k, k' sayıları için $\frac{q_{n_0,k,E}}{q_{n_0',k',E'}}$ fonksiyonlarının asimptotik davranışları,

$$c(M) := \log(\log(x(M))^{\delta}$$

fonksiyonunun sabit bir katı tarafından bellidir, burada δ mutlak değeri küçük olan reel sayı ve $x(M)$, M sayısına kadar olan içinde tam kare sayı bulundurmayan sayıları göstermektedir.

4.7.2 Uyarı. Doğal olarak Konjektür 4.7.1'de yer alan çarpımsal sabit $c(M)$ için daha kesin bir ifade kullanılmalı ve hangi parametrelere bağlı olduğu belirlenmelidir. Ancak çalışmada eliptik eğrilerin Selmer gruplarının mertebesinin hesaplanması ve bu değerlerin bir fonksiyon yardımıyla açıklanması hedeflenmektedir.

4.8 Gözlemler ve Örnekler

Konjektürden de görüleceği üzere yaklaşım fonksiyonu k dan bağımsızdır. Ancak α sabitleri değişmektedir. α sabitlerinin değişimini incelemek ve bir kural elde etmek için

(belki daha fazla veriyle) detaylı bir analiz yapılmalıdır. Çalışmada α sabitleri, Selmer gruplarının mertebeleri dikkate alınarak ve k sayısı için üst sınır 1000 olarak seçilerek hesaplama yapılmıştır. Dikkat edilirse çalışmadaki veriler konjektürün oluşması için yeterli olduğu halde α sabitlerinin analizi için yetersizdir. Örneğin eliptik eğrilerin twist ailelerindeki eliptik eğrilerin Selmer grupları arasında elde edilen en büyük k değeri 68121 olup, bu değer yalnızca bir kez bulunmaktadır.

4.8.1 Örnekler

Hesaplamalarda kullanılan örnekler için α sabitleri göz önüne alınırsa Waldspurger Teoremi'ndeki denklik sınıflarının temsilcilerinin modülo 4 yada 8 e göre sınıflandırılabileceği ve bu sınıflandırmada aynı sınıfta yer alan denklik sınıfları için α sabitlerinin hemen hemen aynı olduğu gözlenmiştir.

1. Durum. 11a1 eliptik eğrisi için modülo 4 te 1 e denk olan denklik sınıflarının temsilcilerinin oluşturduğu $K := \{ 1, 5, 37 \}$ ve modülo 4 te 3 e denk olan denklik sınıflarının temsilcilerinin oluşturduğu $L := \{ 3, 15, 23, 31 \}$ sınıfları vardır. Örneğin $k = 1$ için K sınıfında yer alan n_0 denklik sınıfları için α sabitleri sırasıyla 0,296, 0,299 ve 0,300 civarında iken aynı değerlerin L sınıfında yer alan n_0 denklik sınıfları için sırasıyla 0,458, 0,459, 0,469 ve 0,464 olduğu görülür.

2. Durum. 14a1 eliptik eğrisi için modülo 8 e göre bir ayrışım söz konusudur. Modülo 8 de 3 e denk olan n sayılarına karşılık gelen tüm eliptik eğriler tek olduğu için bu özellikteki n_0 değerleri Çizelge 4.2 de yer almamaktadır. Modülo 8 deki diğer sınıflar modülo 56 daki denklik sınıflarını birbirinden şu şekilde ayırır:

$$K := \{ 1 \}, L := \{ 29, 37, 53 \} \text{ ve } M := \{ 15, 23, 39 \}.$$

Örneğin $k = 9$ için K sınıfındaki n_0 denklik sınıfı için α sabitinin 0,85, L sınıfındaki n_0 denklik sınıfları için α sabitlerinin, sırasıyla, 0,195, 0,185 ve 0,192, M sınıfındaki n_0 denklik sınıfları için α sabitlerinin, sırasıyla, 0,559, 0,568 ve 0,536 olduğu görülür.

3. Durum. 17a1 eliptik eğrisi için modülo 4 te 1 e denk olan tüm denklik sınıflarına karşılık gelen twist eliptik eğrileri tek olduğundan bu değerler Çizelge 4.2 de yer

almamaktadır. Modülo 4 te 3 e denk olan tüm denklik sınıfları için örneğin k = 0 durumunda α sabitleri 0,33 civarındadır.

4. Durum. 20a1 eliptik eğrisi için modülo 4 te 1 e denk olan tüm denklik sınıflarına karşılık gelen twist eliptik eğrileri tek olduğundan bu değerler Çizelge 4.2 de yer almamaktadır. Modülo 4 te 3 e denk olan tüm denklik sınıfları için örneğin k = 225 durumunda α sabitleri 0,1 civarındadır.

5. Durum. 34a1 eliptik eğrisi için modülo 8 belirleyicidir. Eğer $n \equiv 7 \pmod 8$ ise bu durumda tek eliptik eğri sınıfı elde edilir, yani bu denklik sınıfları Çizelge 4.2 de bulunmaz. Modülo 8 deki diğer sınıflar

$$K := \{ 1, 33, 89 \}, L := \{ 19, 35, 43, 59, 67, 83, 115, 123 \}$$

ve

$$M := \{21, 53, 69, 77, 93, 101, 117\}$$

olur. Örneğin k = 1 durumunda α sabitleri K daki denklik sınıfları için 0,38, L deki denklik sınıfları için 0,47 ve M deki denklik sınıfları için 0,41 civarındadır.

4.8.2 Bazı Gerçek Değerler

Aşağıda çalışmada ele alınan her bir E eliptik eğrisi için belirtilen ilişkiyi ortaya koyan bazı sayısal sonuçlar verilmiştir. Daha önce verilen notasyon geçerli olmak üzere algoritmada $\sigma(x_{n_0}(M))$ fonksiyonu

$$\sigma(x_{n_0}(M)) = \alpha \frac{(\log\log(x_{n_0}(M))^{1+\varepsilon}}{\log(x_{n_0}(M))}$$

olarak tanımlanmıştı. Buna göre

Çizelge 4.3 E = 11a1, n_0 = 3, k = 4 ve $\varepsilon = 0{,}005$ için gerçek değerler

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
50000	0,106452	0,099558
1500000	0,074267	0,066593
3000000	0,066195	0,062381
4000000	0,062997	0,060786
5000000	0,060743	0,059604
10000000	0,053981	0,056209

Çizelge 4.4 E = 14a1, n_0 = 1, k = 16 ve $\varepsilon = 0{,}005$ için gerçek değerler

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
100000	0,082313	0,09115
1400000	0,066638	0,066978
2000000	0,06462	0,064665
5000000	0,060241	0,059394
8000000	0,056955	0,057011
10000000	0,055412	0,055946

Çizelge 4.5 E = 17a1, n_0 = 7, k = 324 ve $\varepsilon = 0{,}005$ için gerçek değerler

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
100000	0	0,818727
5000000	0,009965	0,010903
6000000	0,010771	0,010726
7000000	0,011213	0,01058
8000000	0,011651	0,010458
10000000	0,012272	0,010259

Çizelge 4.6 E = 20a1, n_0 = 1, k = 100 ve ε = 0,005 için gerçek değerler

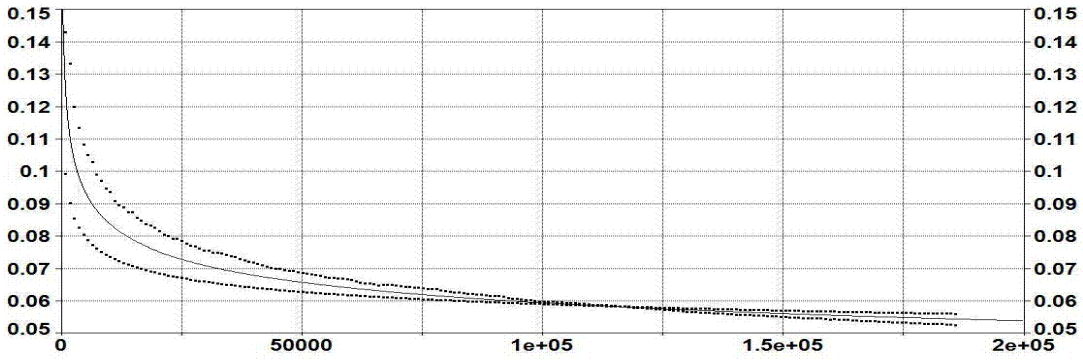
M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
500000	0,026748	0,038045
3000000	0,029427	0,031896
5000000	0,029764	0,030491
6000000	0,029958	0,030019
7000000	0,030039	0,029632
10000000	0,030132	0,028772

Çizelge 4.7 E = 34a1, n_0 = 1, k = 36 ve ε = 0,005 için gerçek değerler

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
3000000	0,066667	0,071691
5000000	0,069827	0,069099
6000000	0,068564	0,067903
7000000	0,0682	0,066996
8000000	0,067812	0,066096
10000000	0,067339	0,064759

4.8.3 Örnek Grafik

Bu kısımda sonuçlarla ilgili örnek bir grafik verilecektir. Aşağıdaki grafikte, x-ekseni üzerinde $x_{n_0}(M)$ nin $M = 10^7$ ye kadar olan değerleri görülmektedir. Burada $E = 11a1$, $n_0 = 1$ ve $k = 1$ olup başlangıçta üstte olan grafik $\frac{s_{1,1}(x_1(M))}{x_1(M)}$ fonksiyonun grafiği olup, alttaki grafik $\alpha = 0{,}295669$ olmak üzere $\alpha\frac{\log(\log(x_1(M)))^{1+\varepsilon}}{\log(x_1(M))}$ fonksiyonun grafiğidir.



Şekil 4.1 Sonuçlar İçin Örnek Grafik

4.9 α Değerlerinin Ağırlıklı Ortalamaları

E	n_0	0	1	4	9	16
11a1	1	0,140221	0,295669	0,204751	0,309679	0,184184
11a1	3	0,214424	0,458141	0,296646	0,445157	0,244439
11a1	5	0,139959	0,299438	0,199569	0,308824	0,186938
11a1	15	0,211029	0,458734	0,299005	0,442075	0,244968
11a1	23	0,208441	0,468673	0,304083	0,440648	0,23676
11a1	31	0,208064	0,46357	0,205327	0,441027	0,23975
11a1	37	0,14234	0,300449	0,205431	0,314227	0,18237

E	n_0	25	36	49	64	81
11a1	1	0,312985	0,179629	0,239533	0,144443	0,235818
11a1	3	0,423453	0,208141	0,27803	0,141689	0,258489
11a1	5	0,320314	0,180445	0,238248	0,140963	0,234221
11a1	15	0,415875	0,207029	0,278424	0,146673	0,249818
11a1	23	0,411152	0,20807	0,283056	0,149102	0,250205
11a1	31	0,412866	0,205186	0,277763	0,150807	0,254808
11a1	37	0,314151	0,171081	0,235285	0,143295	0,230991

E	n_0	100	121	144	169	196
11a1	1	0,149895	0,188637	0,115865	0,171031	0,091912
11a1	3	0,144478	0,144478	0,099708	0,158332	0,068375
11a1	5	0,151277	0,183852	0,117823	0,165406	0,089266
11a1	15	0,1391	0,1391	0,096762	0,156685	0,069026
11a1	23	0,140066	0,190515	0,09152	0,159746	0,070316
11a1	31	0,141375	0,185663	0,098614	0,162711	0,071718
11a1	37	0,152059	0,184835	0,112431	0,172438	0,08812

E	n_0	225	256	289	324	361
11a1	1	0,203897	0,076341	0,135676	0,07271	0,117004
11a1	3	0,178166	0,054526	0,113502	0,047742	0,097803
11a1	5	0,201578	0,076127	0,132841	0,070794	0,116838
11a1	15	0,185691	0,055885	0,117211	0,0487	0,094476
11a1	23	0,179255	0,058757	0,112958	0,048998	0,0973
11a1	31	0,18378	0,054368	0,116274	0,049585	0,0968
11a1	37	0,208334	0,079288	0,132626	0,06951	0,117505

E	n_0	0	1	4	9	16
14a1	1	0,283019	0,386791	0,349053	0,485425	0,289702
14a1	15	0,319039	0,483879	0,409463	0,559197	0,319645
14a1	23	0,336754	0,461198	0,402525	0,567646	0,312323
14a1	29	0,442312	0,172938	0,560877	0,194746	0,485192
14a1	37	0,42059	0,175757	0,589686	0,185407	0,492192
14a1	39	0,312339	0,493768	0,407928	0,536247	0,328624
14a1	53	0,447676	0,171374	0,571985	0,191641	0,472537

E	n_0	25	36	49	64	81
14a1	1	0,28595	0,326485	0,190388	0,148085	0,292196
14a1	15	0,314341	0,322687	0,235968	0,181454	0,290788
14a1	23	0,314975	0,331965	0,236908	0,173742	0,299374
14a1	29	0,099951	0,567019	0,071551	0,310347	0,086056
14a1	37	0,108121	0,544933	0,076132	0,32644	0,081628
14a1	39	0,327089	0,316292	0,251003	0,186261	0,27054
14a1	53	0,104698	0,561543	0,073051	0,321251	0,086696

E	n_0	100	121	144	169	196
14a1	1	0,142119	0,149737	0,159668	0,119627	0,087451
14a1	15	0,139186	0,150902	0,143504	0,116318	0,076208
14a1	23	0,134807	0,144059	0,150461	0,112789	0,072932
14a1	29	0,265114	0,039297	0,303978	0,03107	0,174705
14a1	37	0,276584	0,042321	0,285788	0,029985	0,18166
14a1	39	0,140236	0,14836	0,135962	0,11914	0,079435
14a1	53	0,264155	0,036761	0,306407	0,029676	0,174854

E	n_0	100	121	144	169	196
14a1	1	0,142119	0,149737	0,159668	0,119627	0,087451
14a1	15	0,139186	0,150902	0,143504	0,116318	0,076208
14a1	23	0,134807	0,144059	0,150461	0,112789	0,072932
14a1	29	0,265114	0,039297	0,303978	0,03107	0,174705
14a1	37	0,276584	0,042321	0,285788	0,029985	0,18166
14a1	39	0,140236	0,14836	0,135962	0,11914	0,079435
14a1	53	0,264155	0,036761	0,306407	0,029676	0,174854

E	n_0	0	1	4	9	16
17a1	3	0,337432	0,477285	0,501361	0,41195	0,402614
17a1	7	0,333173	0,480345	0,512958	0,411449	0,397752
17a1	11	0,331548	0,470597	0,506991	0,41595	0,398308
17a1	23	0,324727	0,469987	0,510093	0,413703	0,409981
17a1	31	0,332091	0,482396	0,496191	0,410295	0,405293
17a1	39	0,335686	0,481485	0,50061	0,403566	0,403538

E	n_0	25	36	49	64	81
17a1	3	0,291697	0,298922	0,227993	0,217491	0,190683
17a1	7	0,294852	0,305199	0,224537	0,209766	0,191861
17a1	11	0,29197	0,307093	0,224453	0,212266	0,194131
17a1	23	0,302838	0,296815	0,223042	0,212759	0,197424
17a1	31	0,299154	0,303459	0,219757	0,213895	0,19307
17a1	39	0,29654	0,302868	0,21993	0,218869	0,19364

E	n_0	100	121	144	169	196
17a1	3	0,155873	0,138493	0,129301	0,109835	0,086544
17a1	7	0,153253	0,134025	0,127087	0,109443	0,08902
17a1	11	0,152146	0,142299	0,1244	0,115795	0,090622
17a1	23	0,149471	0,136131	0,125797	0,115204	0,088695
17a1	31	0,153817	0,141537	0,128656	0,10723	0,086032
17a1	39	0,155061	0,139321	0,12622	0,110953	0,084326

E	n_0	225	256	289	324	361
17a1	3	0,10133	0,066479	0,070144	0,054392	0,063161
17a1	7	0,102284	0,066453	0,07182	0,052183	0,061862
17a1	11	0,101815	0,06621	0,073766	0,053459	0,060803
17a1	23	0,104502	0,066214	0,069106	0,055098	0,060021
17a1	31	0,106572	0,068254	0,071002	0,057448	0,058929
17a1	39	0,108346	0,065278	0,073044	0,055616	0,058537

E	n_0	0	1	4	9	16
20a1	1	0,268253	0,3465	0,315475	0,427111	0,27129
20a1	21	0,266462	0,337876	0,32056	0,431508	0,272359
20a1	29	0,267792	0,343135	0,317666	0,425236	0,271235

E	n_0	25	36	49	64	81
20a1	1	0,254326	0,307296	0,210761	0,179752	0,245513
20a1	21	0,253463	0,304903	0,209301	0,178783	0,246748
20a1	29	0,258567	0,308143	0,20873	0,178674	0,252364

E	n_0	100	121	144	169	196
20a1	1	0,144222	0,141449	0,171656	0,115768	0,095252
20a1	21	0,146098	0,144796	0,165373	0,115249	0,09443
20a1	29	0,14228	0,14178	0,1634	0,115021	0,09569

E	n_0	225	256	289	324	361
20a1	1	0,141739	0,076533	0,082182	0,091834	0,066588
20a1	21	0,147373	0,078015	0,082924	0,091549	0,067251
20a1	29	0,14228	0,081021	0,081558	0,091311	0,067867

E	n_0	0	1	4	9	16
34a1	1	0,300968	0,385865	0,387258	0,462396	0,28402
34a1	13	0,290206	0,415303	0,352209	0,474225	0,272241
34a1	19	0,353435	0,475157	0,436218	0,505167	0,317592
34a1	21	0,29167	0,415613	0,359182	0,472539	0,274045
34a1	33	0,30458	0,388798	0,381037	0,440285	0,291886
34a1	35	0,357437	0,47347	0,42035	0,504132	0,326558
34a1	43	0,355486	0,466179	0,44077	0,503479	0,323861
34a1	53	0,281215	0,413834	0,357105	0,470171	0,283536
34a1	59	0,345971	0,471297	0,436144	0,50406	0,327326
34a1	67	0,351665	0,467335	0,427308	0,512714	0,326024
34a1	69	0,290429	0,408492	0,366839	0,478386	0,275193
34a1	77	0,293768	0,41554	0,350608	0,478178	0,272873
34a1	83	0,352644	0,475251	0,440215	0,500611	0,328119
34a1	89	0,305732	0,396955	0,372179	0,443078	0,296228
34a1	93	0,283804	0,42395	0,358696	0,479956	0,279951
34a1	101	0,29705	0,412981	0,359811	0,476887	0,286045
34a1	115	0,34747	0,476572	0,438912	0,505538	0,321909
34a1	117	0,291683	0,420945	0,355004	0,476725	0,278145
34a1	123	0,354215	0,475638	0,437478	0,495364	0,32921

E	n_0	25	36	49	64	81
34a1	1	0,247423	0,309932	0,194351	0,177262	0,225383
34a1	13	0,271392	0,294956	0,199301	0,166857	0,230411
34a1	19	0,271006	0,324198	0,191454	0,171407	0,214279
34a1	21	0,265973	0,301452	0,19956	0,159942	0,230879
34a1	33	0,267835	0,311831	0,193117	0,172183	0,229097
34a1	35	0,275831	0,327544	0,189914	0,17779	0,220039
34a1	43	0,272699	0,317971	0,202658	0,174474	0,211269
34a1	53	0,277814	0,310885	0,201981	0,161572	0,229304
34a1	59	0,267928	0,327115	0,193429	0,175461	0,215779
34a1	67	0,273065	0,324959	0,192272	0,172805	0,212269
34a1	69	0,267456	0,29777	0,207129	0,162831	0,232521
34a1	77	0,272458	0,297814	0,201069	0,167444	0,227964
34a1	83	0,275118	0,314132	0,199511	0,174251	0,210163
34a1	89	0,255453	0,318219	0,207944	0,165966	0,226874
34a1	93	0,259963	0,297419	0,204218	0,165222	0,234308
34a1	101	0,254251	0,303388	0,197465	0,15854	0,23436
34a1	115	0,270414	0,323107	0,196365	0,177784	0,19878
34a1	117	0,260653	0,2887	0,202377	0,157916	0,244395
34a1	123	0,270226	0,335145	0,200594	0,170866	0,208101

E	n_0	100	121	144	169	196
34a1	1	0,128304	0,122231	0,147564	0,102664	0,082786
34a1	13	0,129592	0,130917	0,143784	0,100675	0,07895
34a1	19	0,130772	0,109944	0,140669	0,086182	0,077919
34a1	21	0,132753	0,126583	0,143338	0,106306	0,080138
34a1	33	0,131932	0,123085	0,140728	0,099784	0,082223
34a1	35	0,130884	0,111755	0,141213	0,08385	0,079269
34a1	43	0,128261	0,109375	0,13594	0,083931	0,071109
34a1	53	0,12997	0,126922	0,142644	0,100092	0,07645
34a1	59	0,137624	0,106901	0,140647	0,08392	0,074337
34a1	67	0,138161	0,108241	0,136687	0,090009	0,081168
34a1	69	0,127983	0,12296	0,146421	0,100218	0,072738
34a1	77	0,130561	0,122929	0,148044	0,098305	0,080768
34a1	83	0,130011	0,103015	0,141567	0,085853	0,077536
34a1	89	0,132737	0,115162	0,150665	0,0967	0,08984
34a1	93	0,127371	0,120887	0,147903	0,100794	0,071056
34a1	101	0,124347	0,118514	0,136806	0,10392	0,079833
34a1	115	0,13509	0,116645	0,140947	0,089575	0,075199
34a1	117	0,130015	0,124739	0,140575	0,104611	0,078912
34a1	123	0,135871	0,107328	0,133703	0,093233	0,07586

E	n_0	225	256	289	324	361
34a1	1	0,120486	0,06472	0,062951	0,070443	0,055249
34a1	13	0,120107	0,0621	0,0692	0,077468	0,055683
34a1	19	0,077919	0,059063	0,053673	0,070172	0,038649
34a1	21	0,118898	0,062197	0,06578	0,071127	0,056771
34a1	33	0,118185	0,059254	0,065998	0,072214	0,053245
34a1	35	0,092942	0,058685	0,050621	0,063069	0,039964
34a1	43	0,097305	0,057743	0,053748	0,069417	0,0381
34a1	53	0,120493	0,060345	0,065208	0,071921	0,049442
34a1	59	0,097042	0,061403	0,047947	0,065448	0,040482
34a1	67	0,09381	0,057656	0,066198	0,064485	0,038135
34a1	69	0,121028	0,065232	0,066193	0,066645	0,052697
34a1	77	0,120666	0,065448	0,067139	0,072256	0,052677
34a1	83	0,098931	0,058119	0,049453	0,067301	0,040662
34a1	89	0,117926	0,059319	0,062727	0,072717	0,055294
34a1	93	0,115051	0,060207	0,061973	0,076746	0,058861
34a1	101	0,123836	0,063449	0,070854	0,072985	0,058416
34a1	115	0,099212	0,057176	0,049053	0,065697	0,037937
34a1	117	0,120381	0,061819	0,067332	0,07149	0,054083
34a1	123	0,097763	0,057011	0,049838	0,06636	0,038657

KAYNAKLAR

Anonim, 2011a. http://en.wikipedia.org/wiki/Taniyama-Shimura_conjecture (Erişim Tarihi 05.02.2011).

Anonim, 2011b. http://web.math.hr/~duje/tors/rankhist.html (Erişim Tarihi 05.02. 2011).

Anonim, 2011c. http://www.claymath.org/millennium/ (Erişim Tarihi 05.02.2011).

Anonim, 2011d. http://homepage.uludag.edu.tr/~inam/ (Erişim Tarihi 05.02.2011).

Antoniadis, J., A., Bungert, M., Frey, G. 1990. Properties of twist of elliptic curves. *J. Reine Angew. Math.*. 405: 1–28.

Artin, E. 1921. Quadratische Körper im Gebiete der höheren Kongruenzen. *Ph.D. Thesis*, University of Leipzig, Germany.

Birch, B., Swinnerton–Dyer, H., P., F. 1965. Notes on elliptic curves II. *J. Reine Angew. Math.*. 218: 79–108.

Blake, I., F., Seroussi, G., Smart, N., P. 2000. Elliptic curves in cryptography. London Mathematical Society Lecture Notes Series volume 265. Cambridge University Press, Cambridge, the United Kingdom, 224 pp.

Bosma, W., Cannon, J., Playoust, C. 1997. The Magma algebra system. I. The user language. *J. Symbolic Comput.*. 24(3-4): 235-265.

Breuil, C., Conrad, B., Diamond F., Taylor R. 2001. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises." *J. Amer. Math. Soc.* **14**, 843-939.

Brown, K., S. 1972. Cohomology of groups. Graduate Texts in Mathematics 87. Springer-Verlag, USA, 306 pp.

Bungert, M. 1990. Konstruktion von Modulformen niedrigen Gewichts. IEM preprint No: 9, Essen, Germany.

Cassells, J. W. S. 1965. Arithmetic on curves genus 1 VII on conjectures of Birch and Swinnerton–Dyer conjecture. *J. Reine Angew. Math.*. 217: 180–199.

Cremona, J., E. 1997. Algorithms form modular elliptic curves. 2nd edition. Cambridge Univ. Press. Cambridge, the United Kingdom.

Darmon, H. 1999. A proof of the full Shimura-Taniyama-Weil conjecture is announced. *Not. Amer. Math. Soc.* **46**, 1397-1406.

Frey, G. 1994. Construction and arithmetical applications of modular forms of low weight. *CRM Proceedings & Lecture Notes Amer. Math. Soc*. 4, 1-21.

Fried, M. D., Jarden, M. 2004. Field Arithmetic. Ergebnisse der Mathematik (3) 11, Springer Heidelberg, Germany, 792 pp.

Ireland, K., Rosen, M. 1981. A classical introduction to modern number theory. Springer-Verlag, New York, USA, 389 pp.

İnam, İ., Soydan, G., Demirci, M., Bizim, O., Cangül, İ., N. 2007a. Corrigendum on "The number of points on elliptic curve $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8". *Comm. Korean Math. Soc*. 22(2): 207-208.

İnam, İ., Bizim, O., Cangül, İ., N. 2007b. Rational Points on Frey Elliptic Curves $y^2 = x^3 - nx$. *Adv. Studies in Contemporary Math.* 14 (1): 69-76.

İnam, İ. 2011. Selmer groups in twist families of elliptic curves. *Quaestiones Mathematicae*. Yayına kabul edildi.

Koblitz, N. 1984. Introduction to elliptic curves and modular forms. Springer-Verlag, New York, USA, 248 pp.

Lang, S. 2002. Algebra. Graduate Texts in Mathematics, 211. Springer-Verlag New York, USA, 528 pp.

Mazur, B. 1977. Modular curves and the Eisenstein ideal. *IHES Publ. Math.*. 47: 33-186.

Mazur, B. 1978. Rational isogenies of prime degree. *Invent. Math.*. 44: 129-162.

Miyake, T. 2006. Modular forms. Springer-Verlag, New York, USA, 335 pp.

Ogg, A. P. 1971. Rational points of finite order on elliptic curves. *Invent. Math.*. 9: 105–111.

Park, H., Kim, D., Lee, H. 2003. The number of points on elliptic curves $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8. *Commun. Korean Math. Soc.*. 18(1): 31-37.

Ribet, K. 1990a. From the Taniyama–Shimura conjecture to Fermat's last theorem. *Ann. Fac. Sci. Toulouse Math.* 11: 116-139.

Ribet, K. 1990b. On modular representations of Gal($\overline{Q}/Q$) arising from modular forms. *Invent. Math.* 100: 431-476.

Riemann, B. 1859. Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie*.

Rubin, K., Silverberg A. 2002. Ranks of elliptic curves. *Bulletin of AMS.* 39(4): 455–474.

Satoh, T. 2002. On p – adic point counting algorithms for elliptic curves over finite fields. Lecture Notes in Computer Sciences volume 2369. Springer-Verlag, Berlin, Germany, pp. 43-66.

Schoof, R. 1985. Elliptic curves over finite fields and the computation of squareroots mod p. *Math. Comp.* 44 (170): 483-494.

Serre, J., P., Stark, H., M. 1977. Modular forms of weight 1/2. Modular Functions of One Variable VI, Springer Lecture Notes in Mathematics, vol. 627, New York, USA.

Serre, J., P. 1979. Local fields. Springer-Verlag, USA, 241 pp.

Serre, J., P. 2002. Galois cohomology. Springer Monographs in Mathematics, 5, Springer-Verlag Berlin, Germany, 210 pp.

Shanks, D. 1971. Class number, a theory of factorization and genera. *Proc. Sympos. Pure Math., Vol. XX*, 415-440.

Shimura, G. 1957. Collected papers. Volume I, 1954-1965. Springer New York, USA, 816 pp.

Shimura, G. 1973. On modular forms of half integral weight. *Math. Annalen*. 97(2): 440-481.

Siegel, C., L, 1966. Über die analytische Theory der quadratischen Formen I. Ges. Abhandleungen Bd. Germany.

Silverman, J., H. 1986. The arithmetic of elliptic curves. Springer-Verlag, USA, 400 pp.

Spanier E., H. 1995. Algebraic Topology. Springer Berlin, Germany, 528 pp.

Waldspurger, J., L. 1981. Sur les coefficients de Fourier des formes modulaires de poids demi–entier. *J. Math. Pures et Appl.*. 60: 375–484.

Washington, J., L. 2003. Elliptic curves. Chapman&Hall/CRC, Florida, USA, 429 pp.

Weibel, Charles, A. 1994. An introduction to homological algebra. Cambridge Studies in Advanced Mathematics, 38. Cambridge University Press, The United Kingdom, 453 pp.

Weil, A. 1967. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Annalen*. **168**: 149–156

Wiles, A. 1995. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics*, Second Series **141** (3): 443–551.

ÖZGEÇMİŞ

Adı Soyadı : İlker İNAM
Doğum Yeri ve Tarihi : Bilecik, 15/07/1981
Yabancı Dili : İngilizce

Eğitim Durumu (Kurum ve Yıl)
Lise : İzmir Selma Yiğitalp Lisesi, 1999
Lisans : Uludağ Üniversitesi, 2003
Yüksek Lisans : Uludağ Üniversitesi, 2005

Çalıştığı Kurum ve Yıl : Uludağ Üniversitesi 2005 – …
İletişim (e–posta) : inam@uludag.edu.tr ilker.inam@gmail.com
Yayınları :

- **İnam, İ., Soydan, G., Demirci, M., Bizim, O., Cangül, İ., N. 2007a,** Corrigendum on "The number of points on elliptic curve $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8". *Comm. Korean Math. Soc*. 22(2):207-208.
- **İnam, İ., Bizim, O., Cangül, İ., N. 2007b,** Rational Points on Frey Elliptic Curves $y^2 = x^3 - nx$. *Adv. Studies in Contemporary Math.* 14 (1): 69-76.
- **İnam, İ. 2011,** Selmer groups in twist families of elliptic curves. *Quaestiones Mathematicae*. Yayına kabul edildi.

Form No: D-09

ULUDAĞ ÜNİVERSİTESİ

TEZ ÇOĞALTMA VE ELEKTRONİK YAYIMLAMA İZİN FORMU

Yazar Adı Soyadı	İlker İNAM
Tez Adı	Modüler Formlar, Eliptik Eğriler ve Uygulamaları
Enstitü	Fen Bilimleri Enstitüsü
Anabilim Dalı	Matematik
Tez Türü	Doktora Tezi
Tez Danışman(lar)ı	Prof. Dr. Osman BİZİM
Çoğaltma (Fotokopi Çekim) izni	X Tezimden fotokopi çekilmesine izin veriyorum ☐ Tezimin sadece içindekiler, özet, kaynakça ve içeriğinin % 10 bülümünün fotokopi çekilmesine izin veriyorum ☐ Tezimden fotokopi çekilmesine izin vermiyorum
Yayımlama izni	X Tezimin elektronik ortamda yayımlanmasına izin veriyorum ☐ Tezimin elektronik ortamda yayımlanmasının ertelenmesini istiyorum 1 yıl ☐ 2 yıl ☐ 3 yıl ☐ ☐ Tezimin elektronik ortamda yayımlanmasına izin vermiyorum

Hazırlamış olduğum tezimin belirttiğim hususlar dikkate alınarak, fikri mülkiyet haklarım saklı kalmak üzere Uludağ Üniversitesi Kütüphane ve Dökümantasyon Daire Başkanlığı tarafından hizmete sunulmasına izin verdiğimi beyan ederim.

Tarih :

İmza :