



T.C.
BİLECİK ŞEYH EDEBALI ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
MATEMATİK YÜKSEK LİSANS PROGRAMI

ÇEŞİTLİ TİPLERDEKİ KUADRATİK FORMLARLA TAMSAYILARIN TEMSİLİ

YÜKSEK LİSANS TEZİ

ŞEVVAL DÜNDAR

TEZ DANIŞMANI
PROF. DR. İLKER İNAM

BİLECİK, 2026

10824656

T.C.
BİLECİK ŞEYH EDEBALI ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
MATEMATİK YÜKSEK LİSANS PROGRAMI

ÇEŞİTLİ TİPLERDEKİ KUADRATİK FORMLARLA TAMSAYILARIN TEMSİLİ

YÜKSEK LİSANS TEZİ

ŞEVVAL DÜNDAR

TEZ DANIŞMANI
PROF. DR. İLKER İNAM

BİLECİK, 2026

10824656

BEYAN

“Çeşitli Tiplerdeki Kuadratik Formlarla Tamsayıların Temsili” adlı yüksek lisans tezinin hazırlık ve yazım aşamasında bilimsel araştırma ve etik kurallarına uyduğumu, [Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Faaliyetlerinde Üretken Yapay Zekâ Kullanımına Dair Etik Rehberine](#) uygun olarak tez/dönem projemi hazırladığımı, başkalarının eserlerinden yararlandığım bölümlerde bilimsel etik kurallarına uygun olarak atıfta bulunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, çalışmamın herhangi bir kısmının başka bir tez/dönem projesi olarak sunulmadığını, aksinin tespit edilmesi durumunda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Şevval Dünder

../../2026

İmza

	YAPAY ZEKÂ KULLANIMINA İLİŞKİN ÖĞRENCİ BEYAN FORMU	BŞEÜ-KAYSİS Belge	DFR-516
		İlk Yayın Tarihi/Sayısı	30.04.2026/16
		Revizyon Tarihi	00
		Revizyon No.su	00
		Toplam Sayfa	1

Bölüm I. Yapay Zekâ Kullanım Durumu
☒ Bu tezin/projenin yazım süreçlerinde yapay zekâ tabanlı araçlardan faydalandım .
☐ Bu tezin/projenin yazım süreçlerinde yapay zekâ tabanlı herhangi bir araçtan faydalanmadım .

Bölüm II. Yapay Zekâ Kullanım Detayları
<i>*Bu bölüm yalnızca yapay zekâ kullanımı beyan edilmiş ise doldurulacaktır. Aksi durumda boş bırakılmalıdır.</i>
Tezinizde/projenizde kullandığınız <u>yapay zekâ araçlarını</u> ve <u>sürümünü</u> listeleyiniz: OpenAI ChatGPT (GPT-5 serisi)
Yapay zekâ araçlarını tezin/projenin aşağıdaki aşamalarında ilgili amaçlar için kullandım. (Birden fazla seçenek işaretlenebilir):
☐ Cümle oluşturma
☐ Literatür tarama
☐ Çeviri
☐ Düzenleme/dil kontrolü
☐ Veri işleme ve analizi
☐ Veri görselleştirme
☐ Görüntü üretme
☒ Kaynakça düzenleme
☐ Diğer (Belirtiniz):.....
Bu çalışmada yapay zekâ kullanımı Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Faaliyetlerinde Üretken Yapay Zekâ Kullanımına Dair Etik Rehber'e ve akademik dürüstlük ilkelerine uygun şekilde gerçekleştirilmiş olup yapay zekâ araçlarından alınan destek, etik kurallar ve kaynak gösterme esaslarına uygun biçimde belirtilmiştir. Yapay zekâ kullanımı, çalışmanın özgünlüğüne, bilimsel etik kurallarına ve ilgili mevzuata aykırı olmayacak biçimde gerçekleştirilmiştir. Usulsüz yapay zekâ kullanımı (örneğin: kaynak göstermeksizin metin üretimi, otomatik içerik üretiminin özgün eser gibi sunulması, yanıltıcı kaynak gösterimi vb.) tarafımdan kesinlikle yapılmamıştır. Yapay zekâ araçlarının sağladığı bilgilerin doğruluğunu kontrol ettiğimi, yanlış veya eksik bilgi bulunması halinde tüm sorumluluğun tarafıma ait olduğunu; ayrıca çalışmamla ilgili bu beyana aykırı bir durumun herhangi bir zamanda tespit edilmesi durumunda ortaya çıkabilecek akademik ve hukuki sonuçları kabul ettiğimi beyan ederim.

Şevval Dünder

...../.. /2026

İmza

ÖN SÖZ

Bu tez, yalnızca akademik bir çalışmanın tamamlanması değil; hayatımın hangi yöne gideceğini anlamaya çalıştığım yıllarda başlayan ve zamanla bana hem akademik hem de kişisel anlamda çok şey öğreten bir yolculuğun sonucudur.

Öncelikle, yüksek lisans eğitimim boyunca bilgi ve tecrübesiyle bana yol gösteren, çalışma alanımı şekillendirmemde büyük katkısı bulunan ve tezimin her aşamasında desteğini hissettiğim kıymetli danışmanım Prof. Dr. İlker İNAM'a en içten teşekkürlerimi sunarım. Modüler formlar ve kuadratik formlar üzerine çalışmaya başladığım bu süreçte, yalnızca matematiksel anlamda değil, bir probleme nasıl yaklaşılmaması ve akademik bir çalışmanın nasıl sabırla inşa edilmesi gerektiği konusunda da kendisinden çok şey öğrendim. Bana duyduğu güven, ihtiyaç duyduğum zamanlarda verdiği cesaret ve akademik yolculuğuma kattığı her şey için kendisine gönülden teşekkür ederim.

Lisans eğitimimden bugüne kadar üzerimde emeği bulunan, matematiğe bakışımı geliştiren ve bugün sahip olduğum akademik birikimin oluşmasına katkı sağlayan tüm kıymetli hocalarıma da ayrı ayrı teşekkür ederim. Her birinden öğrendiğim bilgi ve edindiğim bakış açısı, yalnızca bu tezin değil, öğretmenlik ve akademik hayatımın da bir parçası olmuştur.

Hayatım boyunca aldığım her kararın arkasında duran, başarabileceğime kimi zaman benden daha çok inanan ve bugün olduğum insanın temelini oluşturan sevgili aileme ne kadar teşekkür etsem azdır. Attığım her yeni adımda yanımda olduklarını bilmek, en zor zamanlarda bile bana devam edebilme gücü verdi. Bana sundukları sevgi, emek, sabır ve koşulsuz destek için onlara minnettarım.

Ve hayatımın en önemli yol arkadaşına, sevgili eşime...

Bu süreçte yalnızca tez yazan bir yüksek lisans öğrencisi değildim. Aynı zamanda ders anlatan, öğrencilerine yetismeye çalışan, kendi öğretmenlik yolunu kurmaya çabalayan ve zaman zaman bütün bunların arasında yorulan biriydim. Bütün bu koşuşturmanın içinde en yakınım olan, sevincimi de kaygımı da yorgunluğumu da paylaşan kişi hep sendin.

Aynı mesleği paylaşmanın ötesinde, hayallerimi anlayan, yapmak istediklerimi küçümsemeden dinleyen, yorulduğum zamanlarda yükümü paylaşan ve birlikte kurduğumuz hayatın içerisinde bana kendi hayallerimin peşinden gidebileceğim bir alan açan yol arkadaşım olduğun için sana yürekten teşekkür ederim. Bugün geriye dönüp baktığımda, bu tezin satırları arasında senin sabrının, desteğinin ve bana duyduğun güvenin de izleri olduğunu biliyorum.

Yüksek lisansa başladığım gün ile bu satırları yazdığım gün arasında yalnızca akademik olarak ilerlemedim; ben de değiştim.

Bir zamanlar mezuniyetinin ardından hayatının hangi yöne gideceğini anlamaya çalışan genç bir matematik öğrencisiyken, bugün yüzlerce öğrencinin hayatına dokunmuş bir öğretmen olarak bu tezin son cümlelerini yazıyorum. Öğretmenlik yaparken akademiden, akademik çalışmalarımı sürdürürken öğretmenlikten vazgeçmemeyi öğrendim. Zaman zaman yoruldum, bazı şeyleri erteledim, bazı yolların düşündüğümünden daha uzun olduğunu gördüm; fakat bütün bunların sonunda başladığım bir işi tamamlamanın verdiği huzurun ne kadar kıymetli olduğunu da öğrendim.

Bu nedenle bu çalışma benim için yalnızca matematiksel sonuçlardan oluşan bir yüksek lisans tezi değildir. Aynı zamanda, hayatın bütün telaşına rağmen insanın başladığı yere dönüp yarım bıraktığı bir hayali tamamlayabileceğinin küçük bir hatırlatıcısıdır.

Bu süreçte yanımda olan, bana inanan, bilgisiyle, sevgisiyle veya yalnızca güzel bir sözleriyle yoluma dokunan herkese gönülden teşekkür ederim.

Ve son olarak, bu tezi yirmi iki yaşında mezun olmaya çalışan, önünde nasıl bir hayat olduğunu henüz bilmeyen ama matematiği ve öğretmeyi çok seven o genç halime ithaf etmek istiyorum. O günlerde geleceğin nasıl şekilleneceğini bilmiyordun.

Ama yine de yürümeye devam ettin.

İyi ki vazgeçmedin.

ÖZET

Dokuz bölümden oluşan bu çalışmada matematikte uzun yıllardır popülerliğini kaybetmemiş problemlerden birisi olan tamsayıların temsili problemi farklı tipteki kuadratik formlarla ele alınmıştır. Daha kesin olarak bu problemde kuadratik formların üzerine denklik koşulu konularak elde edilen kongrüent kuadratik formlar kullanılmıştır. Literatürde güncel bir çalışma olan (Mondal, 2026) incelenmiştir. Buna göre tamsayıların temsili ile eliptik eğrilerin üzerindeki nokta sayısı arasındaki ilişki ortaya konmuştur. Bunun için kongrüent kuadratik formların teta serileri Eisenstein ve cusp kısımlarını ayrıştırılmış. Modülerite Teoremi sayesinde cusp forma karşılık gelen Fourier katsayıları ile kongrüent kuadratik formun teta serisine karşılık gelen Fourier katsayıları kıyaslanarak temsil sayıları ile eliptik eğri nokta sayısı arasındaki bağlantı ortaya konmuştur. Sayılar teorisi, aritmetik geometri ve karmaşık analizdeki farklı konuları bir araya getiren bu çalışma derleme niteliğindedir.

Anahtar Kelimeler: Kuadratik formlar, tamsayıların temsili, kongrüent kuadratik formlar, modüler formlar, eliptik eğriler

ABSTRACT

This nine-chapter study addresses the problem of integer representation, a long-standing and popular problem in mathematics, using different types of quadratic forms. More specifically, it utilizes congruent quadratic forms obtained by applying equivalence conditions to existing quadratic forms. A recent study in the literature (Mondal, 2026) is examined, revealing the relationship between the representation of integers and the number of points on elliptic curves. To this end, the Eisenstein and cusp parts of the theta series of congruent quadratic forms are decomposed. Using the Modularity Theorem, the Fourier coefficients corresponding to the cusp form are compared with the Fourier coefficients corresponding to the theta series of the congruent quadratic form, revealing the connection between the number of representations and the number of points on the elliptic curve. This work, which brings together different topics in number theory, arithmetic geometry, and complex analysis, is a compilation.

Keywords: Quadratic forms, integer representation, congruent quadratic forms, modular forms, elliptic curves.

İÇİNDEKİLER

Sayfa

ÖN SÖZ.....	i
ABSTRACT	iv
TABLolar LİSTESİ	vi
KISALTMALAR VE SİMGELER LİSTESİ	vii
1.GİRİŞ VE ÖN BİLGİLER	1
3.KONGRÜENT TETA SERİLERİ VE KUADRATİK FORMLAR.....	13
3.1 S ve V Operatörlerinin Özellikleri.....	14
4. S VE V OPERATÖRLERİYLE BAZ ELDE EDİLMESİ	18
5. $\theta k, 2$ TETA SERİLERİ	19
5.1. $\theta 0, 2$ 'nin Analizi.....	19
5.2. $\theta 1, 2$ 'nin Analizi.....	19
6. $\theta k, 4(\tau)$ TETA SERİLERİ.....	21
6.1. $\theta 1, 4(\tau) = \theta 3, 4(\tau)$ 'nün Analizi.....	21
6.2. $\theta 0, 4$ ve $\theta 2, 4$ Analizi	21
7. $\theta k, 3$ TETA SERİLERİ	23
7.1. $\theta 0, 3$ Analizi.....	23
7.2. $\theta 1, 3$ Analizi.....	24
8. $\theta k, 6$ TETA SERİLERİ	26
9. NOKTA SAYIMI VE TETA SERİLERİ.....	28
9.1 $y^2 = x^3 + 1$ Eliptik Eğrisi.....	28
9.2 Teorem 1.7'nin İspatı.....	28
KAYNAKÇA	33

TABLÖLAR LİSTESİ

	Sayfa
Tablo 2.1. Kongrüent kuadratik formlar ve eliptik eğriler	11
Tablo 5.1. Bazı teta serilerinin cusp yerleri.....	24
Tablo 9.1. Eliptik eğriler ve kongrüent kuadratik formlar.....	36

KISALTMALAR VE SİMGELER LİSTESİ

$\mathbb{R}$: Reel Sayılar

$\mathbb{C}$: Karmaşık Sayılar

1.GİRİŞ VE ÖN BİLGİLER

Bu çalışmada literatürde güncel bir sonuç olan (Mondal, 2026)'de yer alan ve çeşitli denklik kavramına sahip tam sayı temsillerinin sayısı ile sonlu cisim üzerine tanımlı eliptik eğrilerin üzerindeki nokta sayısı arasındaki ilişkiyi veren sonuçları ele alacaktır.

İlk olarak çalışmada kullanılacak notasyonu tanıtalım.

$\vec{x} \in \mathbb{Z}^n$ olmak üzere $Q(\vec{x})$ ile gösterilen kuadratik form, n değişkenli ikinci dereceden homojen bir polinom olarak tanımlanır. Burada tamsayı katsayılı kuadratik formlarla çalışılacaktır. $A \in M_n(\mathbb{Z})$ pozitif definite ve $A_{ii} \equiv 0 \pmod{2}$ özelliğini sağlayan simetrik matris olsun. Bu özellikteki matrislere çift matris adı verilir.

Eğer $Q(\vec{x}) = \frac{1}{2} \vec{x}^t A \vec{x}$ oluyorsa A matrisine, $Q(\vec{x})$ pozitif definite formla eşleşen matris denir.

Bir Q kuadratik formu verilsin. Bu durumda $Q(\vec{x}_0) = l$ olacak şekilde belli bir $\vec{x}_0 \in \mathbb{Z}^n$ varsa bu durumda Q kuadratik formu $l \in \mathbb{Z}$ tamsayısını temsil eder denir. Tüm doğal sayıları temsil eden kuadratik formlara evrensel kuadratik form adı verilir. Lagrange 1770'de her bir pozitif tam sayının dört karenin toplamı şeklinde ifade edilebileceğini ispatlamıştır. Ardından (Ramanujan, 1917)'de tüm evrensel üçlü kuadratik formların listesi verilmiştir. Daha sonra (Bhargava ve Hanke, 2011)'de evrensel üçlü kuadratik formlar için ispatlanmıştır. $\mathbb{H}$ üst karmaşık düzlemi göstermek üzere yani $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ olmak üzere ve $\tau \in \mathbb{H}$, $q := e^{2\pi i \tau}$ için $Q(\vec{x})$ bir pozitif definite kuadratik formuyla eşleşen Q serisi Q_q ile gösterilir ve

$$Q_q(\tau) = \sum_{\vec{x} \in \mathbb{Z}^n} q^{Q(\vec{x})}$$

olarak tanımlanır.

Kuadratik formlarla modüler formlar arasında oldukça yakın bir ilişki vardır. Modüler formlar, üst yarı düzlem üzerinde tanımlı olup belirli dönüşüm özelliklerini sağlayan karmaşık değerli holomorf fonksiyonlardır. Bu fonksiyonlar sayılar teorisi, cebirsel geometri ve otomorfik formlar teorisinde merkezi bir rol oynar.

$k \geq 0$ tamsayısı için bir $f: \mathbb{H} \rightarrow \mathbb{C}$ fonksiyonu aşağıdaki şartları sağlıyorsa ağırlığı k olan bir modüler form olarak adlandırılır:

1. f holomorftur.

2. Her $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ için

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

eşitliği sağlanır.

3. f , ilgili grubun bütün cusp noktalarında holomorftur.

Burada Γ , modüler grup $SL_2(\mathbb{Z})$ yani girdileri tamsayı ve determinatı 1 olan matris grubu veya onun bir denklik alt grubu olabilir. Örneğin pozitif bir N tam sayısı için

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

kümesi, tam modüler grubun önemli bir denklik alt grubudur.

Bu durumda ağırlığı k olan bir modüler form, yukarıdaki dönüşüm koşulunu yalnızca $\Gamma_0(N)$ elemanları için sağlar. Bu uzay genellikle $M_k(\Gamma_0(N))$ ile gösterilir.

Eisenstein serileri modüler form teorisinin temel örneklerini oluşturur. Çift indeksli kafes noktaları üzerinden tanımlanırlar. $k \geq 4$ çift olmak üzere,

$$G_k(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(mz+n)^k}$$

serisi mutlak yakınsaktır ve ağırlığı k olan bir modüler form verir. Normalleştirilmiş Eisenstein serisi

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

şeklinde yazılır. Burada $q = e^{2\pi iz}$, B_k Bernoulli sayıları ve $\sigma_r(n) = \sum_{d|n} d^r$

sigma-bölen fonksiyonudur.

Dikkat edilirse ağırlığı 4'ten büyük olan çift tamsayı ağırlığa sahip olan Eisenstein serileri modüler form olur. Ancak ağırlığın 2 olması halinde oldukça ilginç özelliklere sahip Eisenstein serisi elde edilir. Buna göre ağırlık 2 Eisenstein serisi

$$E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n$$

olarak tanımlanır.

Diğer Eisenstein serilerinden farklı olarak E_2 , klasik anlamda modüler form değildir. Bunun yerine

$$E_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 E_2(z) + \frac{12}{2\pi i} c(cz+d)$$

dönüşüm kuralını sağlar. Bu nedenle E_2 , *quasimodüler form* olarak adlandırılır. Quasimodüler formlar, modüler formların doğal bir genişlemesi olup diferansiyel işlemler altında kapalı olmaları nedeniyle önemlidir.

Bu çalışmada kullanılacak olan bir diğer önemli konu ise eliptik eğrilerdir. Buna göre bir eliptik eğri, karakteristiği 2 ve 3 olmayan bir cisim üzerinde

$$E: y^2 = x^3 + Ax + B$$

şeklindeki Weierstrass denklemiyle tanımlanan ve $4A^3 + 27B^2 \neq 0$ koşulunu sağlayan düzgün cebirsel eğridir. Üzerinde cebirsel yapı kurabilmek adına $\mathcal{O}$ ile gösterilen sonsuzdaki noktanın da eliptik eğri üzerinde olduğu kabul edilir.

Eliptik eğri üzerindeki noktalar, sonsuzdaki nokta ile birlikte doğal bir abelyen grup oluşturur. Buradaki işlem şu şekilde tanımlanır: P ve Q gibi iki noktadan geçen doğru eliptik eğriyi mutlaka üçüncü bir noktada keser. $P + Q$ ise bu noktanın x -eksenine göre simetriği olarak tanımlanır (Silverman, 1994). Bu grup yapısı sayılar teorisindeki birçok problemin incelenmesinde temel rol oynar.

E_1 ve E_2 eliptik eğrileri verilsin. Bir izogeni $\phi: E_1 \rightarrow E_2$ şeklinde tanımlanan ve grup yapısını koruyan, sabit olmayan rasyonel bir dönüşümdür. İzogeniler çekirdekleri sonlu olan morfizmalardır. İki eliptik eğri arasında bir izogeni bulunuyorsa bu eğriler izojen olarak adlandırılır.

İzogeniler, eliptik eğrilerin sınıflandırılmasında ve modülerlik teorisinde önemli bir yere sahiptir.

Bir eliptik eğri E için

$$E(K)_{\text{tors}} = \{P \in E(K) : nP = \mathcal{O} \text{ olacak şekilde bir } n > 0 \text{ vardır} \}$$

kümesine torsiyon alt grubu denir. Bu alt grup sonlu olup, elemanları sonlu mertebeli noktalardan oluşur. Özellikle rasyonel sayılar cismi üzerinde torsiyon alt gruplarının olası yapıları Mazur Teoremi ile tamamen sınıflandırılmıştır.

Bir

$$f(z) = \sum_{n \geq 1} a_n q^n$$

Hecke özformu için

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Dirichlet serisi tanımlanır. Uygun koşullar altında bu fonksiyon Euler çarpımı, analitik devam ve fonksiyonel denklem özelliklerine sahiptir.

Bir eliptik eğri $E/\mathbb{Q}$ için her asal p sayısına

$$a_p = p + 1 - \#E(\mathbb{F}_p)$$

katsayısı atanır. Buna karşılık gelen L -fonksiyonu (iyi asallar için)

$$L(E, s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

şeklinde tanımlanır. Bu fonksiyon eliptik eğrinin aritmetik özellikleri hakkında derin bilgiler içerir.

Modülerite Teoremi, her rasyonel eliptik eğrinin uygun bir modüler forma karşılık geldiğini ifade eder. Daha açık olarak, her $E/\mathbb{Q}$ eliptik eğrisi için ağırlığı 2 olan bir yeni form f vardır ve $L(E, s) = L(f, s)$ eşitliği sağlanır. Bu sonuç, başlangıçta Taniyama-Shimura-Weil varsayımı olarak ortaya atılmış, daha sonra çalışmalarla tamamen ispatlanmıştır. Teorem, özellikle Fermat'ın Son Teoremi'nin ispatında kritik rol oynamıştır.

Schoof algoritması, sonlu cisimler üzerindeki eliptik eğrilerin nokta sayısını polinom zamanda hesaplamak amacıyla geliştirilmiş bir algoritmadır. Algoritmanın temel fikri, Frobenius dönüşümünün izini çeşitli küçük asal sayılar modulo hesaplamak ve daha sonra bu bilgileri Çin Kalan Teoremi yardımıyla birleştirmektir.

Bir sonlu cisim üzerindeki eliptik eğri için

$$\#E(\mathbb{F}_q) = q + 1 - t$$

olduğundan, algoritma önce t 'nin çeşitli asallar modülündeki değerlerini belirler ve ardından gerçek değeri elde eder.

Schoof algoritması, eliptik eğri kriptografisinin gelişiminde dönüm noktası olarak kabul edilmektedir.

2.KONGRÜENT TETA SERİLERİ

Bu bölümde çalışmanın esas konusunu oluşturan kongrüent teta serileri tanıtılacaktır. Kuadratik formlara modüler aritmetikten gelen bir koşul koyulması bu teoriye bambaşka bir soluk getirmiştir. Kuadratik formların modüler formlarla bağlantısı ve dahası modüler formların eliptik eğrilerle bağlantısı nedeniyle konulan bu koşul farklı alanlarda açık problemlerin ortaya çıkmasına neden olmuştur. İlk başta tanımla başlayalım.

Tanım 2.1. $Q(\vec{x})$, $x_i \equiv a_i \pmod{S_i}$ denklik koşullarını sağlayan bir kuadratik form olsun. Bu durumda $(Q(\vec{x}), (\vec{a}, \vec{S}))$ çiftine bir kongrüent kuadratik form adı verilir. Bir kongrüent kuadratik forma karşılık gelen teta serisi kongrüent teta serisi olarak adlandırılır ve

$$\theta_{(Q(\vec{x}), (\vec{a}, \vec{S}))}(\tau) = \sum_{\vec{x} \equiv \vec{a} \pmod{\vec{S}}} q^{Q(\vec{x})}$$

olarak tanımlanır.

Örnek 2.2. Klasik Jacobi Teta Fonksiyonu

$$\theta_2(\tau) := \sum_{n \in \mathbb{Z}} q^{\frac{(2n+1)^2}{8}}, \theta_3(\tau) := \sum_{n \in \mathbb{Z}} q^{\frac{n^2}{2}},$$

göz önüne alırsak bu durumda $\vec{a} = (a, a, a, a) \in \mathbb{Z}^4$, $a \in \mathbb{Z}$ olmak üzere kongrüent teta serisi sırasıyla

$$\theta_2^4(4\tau) = \theta_{\frac{1}{2}(x_1^2+x_1^2+x_1^2+x_1^2)(\vec{1}, \vec{2})}$$

ve

$$\theta_3(2\tau)^4 = \theta_{x_1^2+x_2^2+x_3^2+x_4^2, (\vec{0}, \vec{1})}$$

şeklinde olur.

Bilinen teta serilerinin modüler formlarla olan ilişkisi kongrüent serileri içinde geçerlidir. Belirli seviyeler için ağırlık değişken sayısına bağlı olarak değişen modülerlik özelliklerini sağlarlar. Kongrüent teta serileri üzerine yapılan bazı çalışmalar (Beli, 2022) ve (Sun, 2015) olup, (Cho, 2018)'de tam sayıların kongrüent theta serileri yardımıyla temsil sayıları üzerine bir çalışma yapmıştır.

Kongrüent teta serilerini Eisenstein serileri ve cusp form olarak iki parçaya ayırmak doğal olarak kongrüent teta serilerinin Fourier serileri hakkında bazı özellikleri ortaya çıkarır. (Mondal, 2026)'da $Q(\vec{x}) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ olmak üzere $(Q(\vec{x}), (a_i, S_i))$ kongrüent kuadratik form üzerine çalışmıştır. Bu nedenle ilgili çalışmadaki Q notasyonu kaldırılmıştır.

Üstelik sadece $\vec{a} = s \cdot \vec{1}$ ve $\vec{S} = M \cdot \vec{1}$ sütun vektörleriyle ilgilenildiği için $Q_{S,M}$ notasyonu kullanılacaktır. Bu nedenle r_s

$$r_{s,M}(n) = |\{\vec{x} \in \mathbb{Z}^4 | x_1^2 + x_2^2 + x_3^2 + x_4^2 = n, \quad x_i \equiv s \pmod{M}\}|$$

olmak üzere

$$Q_{S,M}(\tau) = \sum_{\vec{x} \in \mathbb{Z}^4, x_i \equiv S \pmod{M}} q^{x_1^2 + x_2^2 + x_3^2 + x_4^2} = \sum_{n=1}^{\infty} r_{s,M}(n) q^n$$

şeklindeir. (Sun, 2015)'e göre $Q_{S,M}$, 2 ağırlıklı bir modüler formdur ve Eisenstein ve cusp form olarak iki parçaya ayrılır. Burada Γ üzerindeki k ağırlıklı modüler formlar ve Eisenstein serilerinin uzayları sırasıyla $\mathcal{M}_k(\Gamma)$ ve $\mathcal{E}_k(\Gamma)$ ile gösterilir. (Bringmann and Kane, 2022)'de S ve V gibi iki operatör yardımıyla $\hat{E}_2$ Eisenstein serisini istenilen seviyedeki modüler forma dönüştürecek iki operatör tanımlanmıştır.

Tanım 2.3. $\mathbb{H}$ üst yarı düzlem üzerinde tanımlı f fonksiyonu

$$f(\tau) = \sum_{n \geq 0} c_f(n) q^n$$

biçiminde bir Fourier serisi ile temsil edilsin. Bu durumda $M \in \mathbb{N}$ ve $m \in \mathbb{Z}$ için S ile gösterilen eleyici operatör

$$f|S_{M,m} := \sum_{\substack{n \geq 0 \\ n \equiv m \pmod{M}}} c_f(n) q^n.$$

olarak tanımlanır.

$d \in \mathbb{Q}$ için V operatörü ise

$$f|V_d(\tau) := f(d\tau) = \sum_{n \geq 0} c_f(n) q^{dn}$$

olarak tanımlanır. Dikkat edilirse bu iki operatör daha düşük seviyeye sahip 2 ağırlıklı Eisenstein uzayları için bir baz elde etmekte kullanılır. Buna göre (Mondal, 2026)'da aşağıdaki ana sonuç verilmiştir.

Teorem 2.4. (Mondal, 2026) $\mathcal{E}_2(\Gamma_0(p^k))$ uzayı için baz aşağıdaki gibi elde edilir:

- (i) Herhangi bir p asalı ve k tek sayısı için $\mathcal{E}_2(\Gamma_0(p^k))$ 'nin bir bazı

$$\{f \mid V_p: f \in \mathcal{E}_2(\Gamma_0(p^{k-1}))\}' \text{nin bir bazı}\}$$

kümesinden elemanlar içerir.

- (ii) $p = 2$ ve $k \leq 3$ için $\mathcal{E}_2(\Gamma_0(2^{2k}))$ 'nin bir bazı $\{\hat{E}_2 \mid S_{2^k,m}(\tau) \mid m \in (\mathbb{Z}/2^k\mathbb{Z})^\times\} \cup \{f \mid V_2: f \in \text{bir bazı } (\mathcal{E}_2(\Gamma_0(p^{k-1})))\}$.

$k > 3$ için $\hat{E}_2$ 'ya S ve V operatörlerini uygulamak $\mathcal{E}_2(\Gamma_0(2^{2k}))$ için tam bir baz elde etmeye yaramaz.

- (iii) $p = 3$ için $\mathcal{E}_2(\Gamma_0(3^2))$ uzayı için bir baz $\hat{E}_2 \mid S_{3,1}(\tau), \hat{E}_2 \mid S_{3,2}(\tau), \hat{E}_2 \mid (3V_3 - S_{3,0})(\tau)$.

yardımıyla verilebilir. Benzer şekilde $k > 1$ için $\hat{E}_2$ 'ya S ve V operatörlerini uygulamak $\mathcal{E}_2(\Gamma_0(3^{2k}))$ için tam bir baz elde etmeye yaramaz.

- (iv) Farklı diğer tek p asalları için sadece S ve V operatörlerini kullanarak $\mathcal{E}_2(\Gamma_0(p^k))$ uzayı için tam bir baz elde edilmesi mümkün değildir.

Örnek 2.5. Burada kongrüent teta serileriyle tamsayı temsiline dair bir uygulama ele alınacaktır. Buna göre $r_{1,3}(n)$ 'in ilk değerleri

$$r_{1,3}(n) = \{x_1^2 + x_2^2 + x_3^2 + x_4^2 = n; x_1, x_2, x_3, x_4 \equiv 1 \pmod{3}\}$$

koşullarını sağlayan sıralı tam sayı dörtlülerinin sayısını göstermektedir. Küçük n değerleri için doğrudan hesaplama yapılabilir. $x_i \equiv 1 \pmod{3}$ olduğundan küçük mutlak değerler için izin verilen değerler

$$x_i = 1, -2, 4, -5, \dots$$

şeklinindedir. Dolayısıyla $n \leq 8$ için yalnızca 1 ve -2 değerlerinin kareleri olan 1 ve 4 dikkate alınır. Örneğin

$$r_{1,3}(4) = |\{x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4, x_1, x_2, x_3, x_4 \equiv 1 \pmod{3}\}| = 1$$

olur. Gerçekten de

$$4 = 1^2 + 1^2 + 1^2 + 1^2$$

olduğu için denklik koşulunu sağlayan tek sıralı dörtlü $(1, 1, 1, 1)$ olur. Benzer şekilde

$$7 = (-2)^2 + 1^2 + 1^2 + 1^2$$

ve $-2 \equiv 1 \pmod{3}$ olduğundan -2 'nin dört farklı konumda bulunması nedeniyle $(-2, 1, 1, 1)$, $(1, -2, 1, 1)$, $(1, 1, -2, 1)$, $(1, 1, 1, -2)$ olmak üzere toplam dört çözüm elde edilir. Böylece

$$r_{1,3}(7) = 4$$

olarak elde edilir. Diğer taraftan $n = 1, 2, 3, 5, 6, 8$ için dört adet izin verilen karenin toplamı n 'yi vermeyeceğinden bu değerler için $r_{1,3}(n) = 0$ olacaktır.

Uyarı 2.6. Dikkat edilirse $r_{1,3}(n)$ yukarıdaki kümenin eleman sayısı olarak tanımlandığından bu sayı (x_1, x_2, x_3, x_4) sıralı dörtlüleri sadece $x_1 + x_2 + x_3 + x_4$ 'ün tek sayı olması durumunda ortaya çıkar. Tüm permütasyonlar dikkate alındığında her bir çözüm $r_{1,3}(n)$ sayısına toplam 4 katkı yapar. Böylece aşağıdaki teoremin ispatı yapılmış olur.

Teorem 2.7. (Mondal, 2026) $n \in \mathbb{N}$, bir tek sayı olsun. Bu durumda $r_{1,3}(n)$ sayısı 4 ile bölünür.

$r_{1,3}(n)$ sayısını daha iyi analiz edebilmesi için $\theta_{1,3}(\tau)$ üreteç fonksiyonunu modülerliğini kullanmaya ihtiyaç duymaktayız. Kongrüent θ serileriyle eliptik eğriler ve modüler formlar arasında bir ilişki ortaya koyabilmek için kongrüent θ serileri ayrıştırılacak $\eta(6\tau)^4$ 'ün cusp form kısmı analiz edilecek ve bu cusp forma karşılık gelen eliptik eğrinin özelliklerini kullanılacaktır.

Teorem 2.8. (Mondal, 2026) $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi $y^2 = x^3 + 1$ eşitliğiyle verilsin. $N_p(k)$ ile sonsuzdaki nokta dahil olmak üzere bu eğri üzerindeki F_{p^k} rasyonel noktaların sayısı gösterilsin. Bu durumda $p \equiv 1 \pmod{6}$ tüm asallar için;

$$r_{1,3}(p) = \frac{1}{3}N_p(1)$$

olur. Daha genel olarak aşağıdaki eşitlik doğrudur:

$$3r_{1,3}(p^k) = \begin{cases} N_p(k) + 3p \cdot r_{1,3}(p^{k-2}) & k \geq 3 \\ N_p(k) & k = 1, 2. \end{cases} \quad (2.1)$$

vardır. Başka bir deyişle $p_1 \equiv 1 \pmod{6}$ için

$$r_{1,3}(p^{2k+1}) = \frac{1}{3}[N_p(2k+1) + pN_p(2k-1) + \dots + p^kN_p(1)]$$

$p > 3$ için

$$r_{1,3}(p^{2k+2}) = \frac{1}{3} [N_p(2k+2) + pN_p(2k) + \dots + p^k N_p(2)]$$

olur.

Örnek 2.9. $r_{1,3}(7) = \frac{1}{3} N_7(1)$ olduğunu biliyoruz. Buna göre $E : y^2 = x^3 + 1$ eliptik eğrisi üzerinde

$$(0,1)$$

$$(0,-1)$$

$$(1,3)$$

$$(1,-3)$$

$$(2,3)$$

$$(2,-3)$$

$$(3,0)$$

$$(4,3)$$

$$(4,-3)$$

$$(5,0)$$

$$(6,0)$$

$$\mathcal{O}$$

olmak üzere toplam 12 nokta olup

$$r_{1,3}(7) = \frac{1}{3} 12 = 4$$

elde edilir.

Örnek 2.10. $p = 103$ olsun. Bu durumda $r_{1,3}(103) = 28$ olup $\eta(6\tau)^4$ fonksiyonunun Fourier açılımındaki q^{103} teriminin a_{103} Fourier katsayısı 28'dir. Kolayca görülebilir ki;

$$3r_{1,3}(p) = p + 1 - a_p = \#\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + 1 \pmod{p}\}.$$

Aşağıda Teorem 2.8'in bir genelleştirilmesi verilecektir. Daha kesin olarak $n \equiv 1 \pmod{6}$ olması durumunda $r_{1,3}(n)$ için bir genel formül verilecektir. Bu sayede kongrüent kuadratik formlarla eliptik eğri üzerindeki nokta sayısı arasında daha genel bir ilişki verilecektir.

Teorem 2.11. (Mondal, 2026) $p_1, \dots, p_k$ farklı asalların herhangi bir kümesi olsun ve $\alpha_1, \dots, \alpha_k$ sayıları

$$\alpha_i = \begin{cases} 2\mathbb{N} & , \quad p_i \equiv 5 \pmod{6} \\ \mathbb{N} & , \quad p_i \equiv 1 \pmod{6} \end{cases}$$

olmak üzere $n = \prod_i p_i^{\alpha_i} \equiv 1 \pmod{6}$ üzerinden seçilsin. Bu takdirde $\alpha_\ell \eta(6\tau)^4$ cusp formunun ℓ . Fourier katsayısı olmak üzere $r(n)$ aşağıdaki gibi bir ayrışımaya sahiptir:

$$r_{1,3}(n) = \sum_{i=1}^k \left(\prod_{j=i+1}^k (\sigma_1(p_j^{\alpha_j})) \prod_{j=1}^{i-1} (\alpha_{p_j^{\alpha_j}}) \right) r_{1,3}(p_i^{\alpha_i}).$$

Uyarı 2.12. Teorem 2.7 ve 2.8 beraber dikkate alındığında $p \equiv 1 \pmod{6}$ için $N_p(1)$ 'in 12 ile bölündüğü görülür. Üstelik Teorem 2.8' nin direkt bir sonucu olarak herhangi bir $m \in \mathbb{N}$ için

$$3r_{1,3}(p^m) \equiv N_p(m) \pmod{p}$$

olur. Aşağıdaki tabloda Teorem 2.8'deki sonuca benzer olarak sonuçlar elde edilebilecek bazı örnekler (Cho, 2018)'den faydalanılarak verilmiştir.

Dikkat edilirse $\hat{E}_2|_{S_{M,m}}, \hat{E}_2|_{S_{M,m}}|V_d$ biçimindeki elemanlar tarafından üretilen Eisenstein serileri tüm durumlarda ilgili teta serisinin Eisenstein parçasını çıkarmak için çok önemli bir araç olduğu görülür.

Tablo 2.1. Kongrüent kuadratik formlar ve eliptik eğriler

Kuadratik form Q	Denklik koşulu	Eliptik Eğri E	CM	$N_p^E(1)$ ve $r_Q(p)$ arasındaki ilişki	Asal sayılar üzerindeki denklik koşulu
$x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$	$x_1, x_3, x_4 \equiv 1 \pmod{2}, x_2 \equiv 0 \pmod{2}$	$y^2 = x^3 + 4x$	$Q(\sqrt{-1})$	$r_Q(p) = N_p^E(1)$	$p \equiv 1 \pmod{4}$

x_1^2 $+ x_1x_2$ $+ x_2^2$ $+ x_3^2$ $+ x_3x_4$ $+ x_4^2$	x_1, x_2, x_3 $\equiv 1(mod3), x_4$ $\equiv 0(mod3)$	$y^2 + y$ $= x^3$	$Q(\sqrt{-3})$	$r_Q(p) = N_p^E(1)$	$p \equiv 1(mod3)$
x_1^2 $+ x_1x_2$ $+ 2x_2^2$ $+ x_3^2$ $+ x_3x_4$ $+ 2x_4^2$	x_1, x_4 $\equiv 1(mod2), x_2, x_3$ $\equiv 0(mod2)$	$y^2 + xy$ $+ y$ $= x^3$ $- x$	Yok	$r_Q(p) = 2N_p^E(1)$	p $\equiv 1(mod2), p$ $\not\equiv 7(mod14)$

3.KONGRÜENT TETA SERİLERİ VE KUADRATİK FORMLAR

Bu bölümde kongürent formların teta serileri ve kuadratik formlar arasındaki ilişki ele alınacaktır. Kuadratik formların teta serileri modüler formların çok önemli bir örneğidir. Teta serileri üzerine denklik koşulu koymak modüler formlar üzerindeki problemi çalışırken oldukça ilgi çekici olacaktır.

n, Q kuadratik formundaki değişken sayısı olmak üzere A matrisiyle eşleşen Q kuadratik formun diskriminantı D ile gösterilir ve

$$D = (-1)^{\frac{n}{2}} \det(A)$$

olarak tanımlanır.

Alışıldığı gibi Q kuadratik formun seviyesi N sayısı NA^{-1} girdileri çift tam sayı olacak şekilde en küçük n doğal sayı olacak şekilde tanımlanır. Dikkat edilirse hem seviye hem de diskriminant kongürent teta serilerinin modüleritesini belirlemede çok önemli rol oynar.

Burada $Q_{s,m}$ ile $Q_{s,m}(\vec{x})$ kuadratik formuyla eşleşen teta serisi (ve tersi) gösterilecektir.

Kuadratik formların teta serilerinin modülerliği oldukça iyi bilinmektedir. Teta serilerinin üzerine denklik koşulu konulduğu zaman buna karşılık gelen serinin modülerliği aşağıda gösterilecektir. Hatırlanacağı üzere $M_k(\Gamma, x)$ modüler form uzayı herhangi bir $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ için

$$f|_k \gamma(\tau) := (c\tau + d)^{-k} f(\gamma\tau) = \chi(d) f(\tau),$$

koşulunu sağlayan f modüler formlarından oluşur. Burada $\tau \in \mathbb{H}$ 'tır. İlk olarak aşağıdaki iki teorem verilecektir.

Teorem 3.1. (Cho, 2018) $Q_{s,m}(\vec{x})$ pozitif tanımlı n değişkenli tam sayı katsayılı kongrüent kuadratik formu olsun. Burada n çift tam sayı ve s bir doğal sayı $Q_{s,m}$ buna karşılık gelen teta serisi olsun. Bu takdirde D ve N sırasıyla $Q_{s,m}(\vec{x}), Q_{s,m}$ kuadratik formun diskriminantı ve seviyesi ile $\left(\frac{D}{\cdot}\right)$ Kronecker sembolü olmak üzere

$$\theta_{s,M} \in \mathcal{M}_{\frac{n}{2}} \left(\Gamma_0(M^2 N) \cap \Gamma_1(M), \left(\frac{D}{\cdot}\right) \right) \cong \bigoplus_{\substack{\chi \pmod{M} \\ \chi(-1) = (-1)^{\frac{n}{2}}}} \mathcal{M}_{\frac{n}{2}} \left(\Gamma_0(M^2 N), \chi \cdot \left(\frac{D}{\cdot}\right) \right)$$

olur.

Uyarı 3.2. (Mondal, 2026)'da çalışılan kuadratik form $x_i \equiv k \pmod{M}$ olmak üzere $Q_{k,M}(\vec{x}) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ biçimindeki pozitif tanımlı tam sayı kongürent kuadratik form olup bu forma karşılık gelen matris

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

olarak verilir. Dikkat edilirse $\det(A) = 16$ olup, bu nedenle diskriminant $D = 16$ olur. Bu ise $\left(\frac{D}{\cdot}\right)$ krocker sembolünün aşıkâr olmasını gerektirir. $N = 4$ 'tür. Böylece Teorem 3.1 gereği

$$\theta_{k,M} \in \mathcal{M}_2(\Gamma_0(4M^2) \cap \Gamma_1(M)) \cong \bigoplus_{\chi(-1)=1} \chi \pmod{M} \mathcal{M}_2(\Gamma_0(4M^2), \chi)$$

elde edilir.

3.1 S ve V Operatörlerinin Özellikleri

S ve V operatörlerini pratikçe uygulayabilmek adına basit formüller elde etmek oldukça önemlidir. Aşağıda verilecek olan teorem S ve V için sonlu bir toplam formülü vermektedir. Bu formüller farklı cusp noktasındaki Eisenstein elemanlarının değerlerinin kolayca hesaplamaya ve $f|S_{M,m}$ ile $f|V_d$ fonksiyonlarının analitikliğini kontrol etmeye yarayacaktır.

Teorem 3.1.1. (Mondal, 2026) f kayma dönüşümü altında invaryant olan fonksiyon $d, m, M, d \in \mathbb{N}$ olsun. Bu takdirde $\zeta_M = e^{\frac{2\pi i}{M}}$ olmak üzere $\tau \in \mathbb{H}$

$$f|S_{M,m}(\tau) = \frac{1}{M} \sum_{j=0}^{M-1} f\left(\tau + \frac{j}{M}\right) \zeta_M^{-jm}$$

ve

$$f|S_{M,m}|V_d(\tau) = \frac{1}{M} \sum_{j=0}^{M-1} f\left(d\tau + \frac{j}{M}\right) \zeta_M^{-jm},$$

olur.

Eğer

$$f(\tau) = \hat{E}_2(\tau) := 1 - \frac{3}{\pi \text{Im}(\tau)} - 24 \sum_{n \geq 1} \sigma_1(n) q^n$$

olarak alınırsa bu fonksiyon $SL_2(\mathbb{Z})$ için 2 ağırlıklı analitik olmayan modüler Eisenstein serisi olduğu kolayca görülebilir. Bu takdirde Teorem 3.1.1. kullanılarak cusp noktalarından $\hat{E}_2|_{S_{M,m}}$ ve $\hat{E}_2|_{V_d}$ fonksiyonlarının değerleri hesaplanabilir (Bringmann ve Kane, 2022).

Teorem 3.1.2. (Mondal, 2026) $\frac{h}{k} \in \mathbb{Q}$ için

$$-\lim_{z \rightarrow 0^+} z^2 \hat{E}_2|_{S_{M,m}} \left(\frac{h}{k} + \frac{iz}{k} \right) = \frac{1}{M^3} \sum_{j=0}^{M-1} \text{ebob}(Mh + jk, Mk)^2 \zeta_M^{-jm}, \quad (3.1)$$

$$-\lim_{z \rightarrow 0^+} z^2 \hat{E}_2|_{S_{M,m}}|_{V_d} \left(\frac{h}{k} + \frac{iz}{k} \right) = \frac{1}{M^3 d^2} \sum_{j=0}^{M-1} \text{ebob}(Mdh + jk, Mk)^2 \zeta_M^{-jm} \quad (3.2)$$

olur.

Uyarı 3.1.3. Eşitlik (3.2)'de $M = 1$, $m = 0$ yazılırsa

$$\lim_{x \rightarrow 0^+} x^2 \hat{E}_2|_{V_d} \left(\frac{h}{k} + \frac{i\pi}{k} \right) = \frac{1}{d^2} \cdot \text{ebob}(hd, k)^2$$

elde edilir. Analitik olmayan $\hat{E}_2$ modüler Eisenstein serisine S ve V operatörleri uygulanarak analitik modüler formlar elde edebiliriz.

Lemma 3.1.4. (Mondal, 2026) d ve $m \in \mathbb{Z}$, M verilen pozitif tam sayılar için $\tau \in \mathbb{H}$ olmak üzere

(i) $m > 0$ için

$$\hat{E}_2|_{S_{M,m}}(\tau) \in \mathcal{M}_2(\Gamma_1(M^2))$$

ve

$$\hat{E}_2|_{S_{M,m}}|_{V_d}(\tau) \in \mathcal{M}_2(\Gamma_0(\text{ekok}(4, d)) \cap \Gamma_1(M^2)).$$

(ii) Eğer $m = 0$ ise bu takdirde

$$\hat{E}_2|(dV_d - S_{d,0})(\tau) \in \mathcal{M}_2(\Gamma_0(\text{ekok}(4, d)) \cap \Gamma_1(d^2))$$

olur.

Γ_0 için $\hat{E}_2$ Eisenstein serisini S operatörü uygulandığında elde edilecek sonuçların inceleyeceğiz. Belli bir N için $\Gamma_0(N)$ üzerindeki hemen hemen tüm kongrüent teta serileri modüler olduğundan modifiye edilen $\hat{E}_2|S_{M,m}$ fonksiyonunun $\gamma \in \Gamma_0(N)$ etkisini inceleyeceğiz.

Teorem 3.1.5. (Mondal, 2026) $M \in \mathbb{N}$ ve $m \in \mathbb{Z}$ olsun. Bu takdirde $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M^2)$ için

$$\hat{E}_2|S_{M,m}|\gamma(\tau) = \hat{E}_2|S_{M,a^2m}(\tau)$$

olur. Üstelik $\hat{E}_2|S_{M,m}(\tau)$ serisi $\Gamma_1(M^2)$ dönüşümü altında invaryanttır.

Bu dönüşümleri kullanarak S ve V operatörleri altında $\mathcal{E}_2(\Gamma_0(N))$ 'nin tüm invaryant elemanlarını bulmaya çalışacağız. İlk olarak p tek asal sayı olmak üzere $(\mathbb{Z}/p^n\mathbb{Z})^\times$ ve $(\mathbb{Z}/2^n\mathbb{Z})^\times$ grupları için bir yapı teoremi vereceğiz.

Lemma 3.1.6 (Mondal, 2026) $n \geq 2$ için

- (i) $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}_2 \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$ olur. Buradaki izomorfizm $\phi: \mathbb{Z}_2 \times (\mathbb{Z}/2^{n-2}\mathbb{Z}) \rightarrow (\mathbb{Z}/2^n\mathbb{Z})^\times$ olmak üzere $\phi(i, j) = (-1)^i(5)^j$ olarak verilir.
- (ii) Bir p tek asalı için $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle g \rangle$ ve $(g + p)$ olur. Burada $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ olur.

Şimdi $\Gamma_0(M^2)$ nin etkisi altında invaryant kalan elemanları bulmaya çalışacağız.

Teorem 3.1.7. (Mondal, 2026) Eğer $f(\tau) = \sum_{m \in \mathbb{Z}/m\mathbb{Z}} \alpha_m \hat{E}_2|S_{M,m}(\tau)$, $\Gamma_0(M^2)$ etkisi altında invaryant kalan bir eleman ise bu takdirde tüm $a \in (\mathbb{Z}/M^2\mathbb{Z})^\times$ için $\alpha_{a^2m} = \alpha_m$ olur.

Teorem 3.1.8. (Mondal, 2026) Belli bir c_m katsayıları için

$$f = \sum_{m \in (\mathbb{Z}/2^n\mathbb{Z})^\times} c_m \hat{E}_2|S_{2^n,m} \in M_2(\Gamma_1(2^{2n}))$$

olarak verilsin. Bu takdirde $f \in M_2(\Gamma_0(2^{2n}))$ olması için gerek ve yeter şart

$$f \in \text{Span}\{\hat{E}_2|S_{2^j,m} : j = 1, \dots, \min(3, n), m \in (\mathbb{Z}/2^j\mathbb{Z})^\times\}.$$

olmasıdır.

Uyarı 3.1.9. p tek asal olması halinde $\mathcal{E}_2(\Gamma_0(p^2))$ uzayında yalnızca 3 tane bağımsız eleman olup; bunlar $\hat{E}_2|(S_{p,0} - pV_p)$, $\sum_{\left(\frac{a}{p}\right)=1} \hat{E}_2|S_{p,a}$ ve $\sum_{\left(\frac{b}{p}\right)=-1} \hat{E}_2|S_{p,b}$ şeklindedir.

Burada $\left(\frac{\cdot}{p}\right)$ Legendre sembolü gösterilmektedir.

Örnek 3.1.10. $n = 4$ için $5^2 \equiv 9 \pmod{16}$, $5^4 \equiv 1 \pmod{16}$ dikkat edilirse 2. koşulda $c_m = c_m$ durumu elde edilir. Öte yandan ilk koşul bize

$$c_1 = c_9, \quad c_3 = c_{11}, \quad c_5 = c_{13}, \quad c_7 = c_{15}$$

olmasını gerektirir. O halde invaryant elemanlar

$$\begin{aligned} \hat{E}_2|_{S_{16,1}} + \hat{E}_2|_{S_{16,9}} &= \hat{E}_2|_{S_{8,1}}, \\ \hat{E}_2|_{S_{16,3}} + \hat{E}_2|_{S_{16,11}} &= \hat{E}_2|_{S_{8,3}}, \\ \hat{E}_2|_{S_{16,5}} + \hat{E}_2|_{S_{16,13}} &= \hat{E}_2|_{S_{8,5}}, \\ \hat{E}_2|_{S_{16,7}} + \hat{E}_2|_{S_{16,15}} &= \hat{E}_2|_{S_{8,7}}. \end{aligned}$$

Aşağıdaki teorem Eisenstein elemanlarını sadeleştirmek için kullanılacaktır.

Teorem 3.1.11. (Mondal, 2026) ℓ tek sayı olmak üzere

$$\hat{E}_2|_{S_{2^k, \ell}}|_{V_2} = \frac{1}{3} \hat{E}_2|_{S_{2^{k+1}, 2\ell}}.$$

olur.

4. S VE V OPERATÖRLERİYLE BAZ ELDE EDİLMESİ

Bu bölümde belli bir k sayısına kadar olan asallar için Teorem 2.4'ün ispatı yardımıyla $\Gamma_0(p^k)$ üzerinde 2 ağırlıklı Eisenstein serisi uzayları için bir baz üretmeye yarayacak bir metot verilecektir. Doğal olarak k 'nın büyük değerleri için metot zorlaşacak olup bununla ilgili genel bir tartışma verilecektir.

Modüler formlar uzayında uzayın boyutu ile $\Gamma_0(N)$ 'nin cusp sayıları arasında yakın bir ilişki vardır. Gerçekten de (Cohen and Strömberg, 2017: 300)'de Teorem 8.5.21'deki boyut formülleri kullanılarak

$$\dim\left(\mathcal{E}_2\left(\Gamma_0(N)\right)\right) = e(N) - 1 \quad (4.1)$$

olduğu görülür. Burada $e(N)$, $\Gamma_0(N)$ 'nin denk olmayan cuspların sayısıdır. Bu sayı (Cohen and Strömberg, 2017: 298)'de yer alan Önerme 8.5.15'de tam olarak verilmiştir.

Teorem 4.1. (Cohen ve Strömberg, 2017) $\Gamma_0(N)$ nin cusplarının sayısı

$$e(N) = \sum_{d|N} \phi\left(\text{obeb}\left(d, \frac{N}{d}\right)\right) \quad (4.2)$$

Burada $\phi(n)$ Euler- ϕ fonksiyonudur. Herhangi bir p asalı için (4.1) ve (4.2) eşitlikleri birleştirilerek aşağıdaki formül elde edilir:

$$\dim\left(\mathcal{E}_2\left(\Gamma_0(p^k)\right)\right) = \begin{cases} (p+1)p^{\frac{k}{2}-1} - 1, & k \text{ çift,} \\ 2p^{\frac{k+1}{2}} - 1 & k \text{ tek.} \end{cases}$$

Uyarı 4.2. Bu Eisenstein serisi uzaylarının indislenmiş baz elemanlarının bir listesi (Mondal, 2026) makalesinde Ek A ve Ek B'de verilmiştir. Bu elemanlar kongrüent teta serilerinden Eisenstein serileri elde etmekte kullanılacaktır.

5. $\theta_{k,2}$ TETA SERİLERİ

Bu bölümde $\theta_{k,2}$ kongürent serileri analiz edilecektir.

5.1. $\theta_{0,2}$ 'nin Analizi

Dikkat edilirse eşitsizlik (1.1)'den

$$\theta_3(8\tau)^4 = \left(\sum_{n \in \mathbb{Z}} q^{8\frac{n^2}{2}} \right)^4 = \left(\sum_{n \in \mathbb{Z}} q^{(2n)^2} \right)^4 = \theta_{0,2}(\tau).$$

elde edilir. (Li vd., 2018)'de verilen özdeşliğe göre

$$\theta_3(2\tau)^4 = \mathbb{E}_{4,1}(\tau) + 8\mathbb{E}_{4,2}(\tau)$$

olur. Böylece

$$\theta_{0,2}(\tau) = (\mathbb{E}_{4,1} + 8\mathbb{E}_{4,2})|V_4(\tau) = \mathbb{E}_{16,1}(\tau) + 8\mathbb{E}_{16,5}(\tau) \quad (5.1)$$

olarak bulunur. Dikkat edilirse $\theta_{0,2}$ serisinde cusp form kısmı 0'dır. Bu nedenle Eisenstein elemanlarına ve uygulanan operatörler kullanılarak aşağıdaki sonuç elde edilir.

Teorem 5.1.1. (Mondal, 2026) Herhangi bir $n \in \mathbb{N} \cup \{0\}$ için

$$r_{0,2}(n) = \begin{cases} 1, & n = 1, \\ 24 \left[\sigma_1\left(\frac{n}{4}\right) - 2\sigma_1\left(\frac{n}{8}\right) \right], & n \equiv 0 \pmod{8}, n > 1, \\ 8\sigma_1\left(\frac{n}{4}\right), & n \equiv 4 \pmod{8}, \\ 0, & \text{diğer durumlar.} \end{cases}$$

olur.

5.2. $\theta_{1,2}$ 'nin Analizi

Dikkat edilirse

$$\theta_{1,2}(\tau) = 16q^4 + 64q^{12} + 96q^{20} + 128q^{28} + O(q^{36}).$$

şeklindedir. Bir kez daha Teorem 2.4 kullanılarak

$$\theta_{1,2}(\tau) \in \mathcal{M}_2(\Gamma_0(16) \cap \Gamma_1(2)).$$

olduğu görülür. $\theta_{1,2}$ için cusp noktalarından aşağıdaki değerler elde edilir.

Tablo 5.1. Bazı teta serilerinin cusp yerleri

$\Gamma_0(16)$ 'nın cusp'ları	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{3}{4}$	$\frac{1}{2}$	0	∞
$\theta_{1,2}$ değerleri	1	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{16}$	$-\frac{1}{64}$	0

Bu nedenle (Mondal, 2026) Ek A'da yer alan tabloya kıyaslama yapılarak

$$\theta_{1,2}(\tau) = 16\mathbb{E}_{16,5}(\tau). \quad (5.2)$$

olarak bulunur.

$\theta_{1,2}(\tau)$ 'nin de cusp form kısmı yoktur. Bir önceki duruma benzer şekilde elde edilir.

Herhangi bir $n \in \mathbb{N} \cup \{0\}$,

$$r_{1,2}(n) = \begin{cases} 16\sigma_1\left(\frac{n}{4}\right), & n \equiv 4 \pmod{8} \\ 0, & \text{diğer durumlar} \end{cases}$$

6. $\theta_{k,4}(\tau)$ TETA SERİLERİ

Bu bölümde $\theta_{k,4}(\tau)$ kongrüent teta serilerinin detaylı bir analizi yapılacaktır. İlk olarak bu seriler Eisenstein serileri ve cusp form kısımlarına ayrıştırılacaktır. Ardından Fourier açılımları yardımıyla $\theta_{k,4}(\tau)$ 'nın Fourier katsayıları kesin olarak formülize edilecektir. Kaldı ki bu Fourier katsayıları $\theta_{k,4}(\tau)$ kongrüent kuadratik formu tarafından doğal sayıların temsil sayısıdır. Üstelik bu Fourier açılımlarını Magma, SageMath ve Pari/GP gibi matematik-bilgisayar programları yardımıyla etkili şekilde hesaplanır.

$k = 1$ ve $k = 3$ durumunda aynı seriler elde edilir. İlk olarak bu durumla başlanacaktır.

6.1. $\theta_{1,4}(\tau) = \theta_{3,4}(\tau)$ 'nin Analizi

Gerekli işlemler yapılarak;

$$\begin{aligned}\theta_{1,4}(\tau) &= \sum_{\substack{x_i \in \mathbb{Z} \\ x_i \equiv 1(4)}} q^{x_1^2 + x_2^2 + x_3^2 + x_4^2} = \sum_{\substack{x_i \in \mathbb{Z} \\ x_i \equiv 3(4)}} q^{(-x_1)^2 + (-x_2)^2 + (-x_3)^2 + (-x_4)^2} = \theta_{3,4}(\tau) \\ &= q^4 + 4q^{12} + 6q^{20} + 8q^{28} + 13q^{36} + O(q^{44})\end{aligned}$$

elde edilir. Üstelik,

$$\theta_{1,2}(\tau) = \left(\sum_{m \in \mathbb{Z}} q^{(4m+1)^2} + q^{(4m+3)^2} \right)^4 = \left(2 \sum_{m \in \mathbb{Z}} q^{(4m+1)^2} \right)^4 = 16\theta_{1,4}(\tau).$$

Teorem 4.2 kullanılarak $r_{1,4}(n) = r_{3,4}(n)$ için aşağıdaki sonuç elde edilir.

Teorem 6.1.1. (Mondal, 2026)

Herhangi bir $n \in \mathbb{N} \cup \{0\}$

$$r_{1,4}(n) = r_{3,4}(n) = \begin{cases} \sigma_1\left(\frac{n}{4}\right), & n \equiv 4(\text{mod}8) \\ 0, & \text{diğer durumlar} \end{cases}$$

olur.

6.2. $\theta_{0,4}$ ve $\theta_{2,4}$ Analizi

Lemma 6.2.1. (Mondal, 2026)

$k = 0, 2$ olmak üzere $\theta_{k,4}(\tau)$ kongrüent teta serileri için aşağıdaki ayrışım doğrudur:

$$\theta_{2,4}(\tau) = 16\mathbb{E}_{64,11}(\tau) = -\frac{2}{3}\hat{E}_2|_{S_{2,1}}|_{V_{16}}(\tau)$$

$$\theta_{0,4}(\tau) = \mathbb{E}_{64,1}(\tau) + 8\mathbb{E}_{64,11}(\tau) = \hat{E}_2|(2V_2 - S_{2,0})|_{V_{16}}(\tau) - \frac{1}{3}\hat{E}_2|_{S_{2,1}}|_{V_{16}}(\tau).$$

İspat.

Dikkat edilirse $\theta_{1,2}(4\tau) = \left(\sum_{n \in \mathbb{Z}} q^{4 \cdot (2n+1)^2}\right)^4 = \left(\sum_{n \in \mathbb{Z}} q^{(4n+2)^2}\right)^4 = \theta_{2,4}(\tau)$ olur.

(5.2) eşitliği kullanılarak

$$\theta_{2,4}(\tau) = 16\mathbb{E}_{64,11} = -\frac{2}{3}\hat{E}_2|_{S_{2,1}}|_{V_{16}}(\tau)$$

elde edilir.

$$\theta_{0,2}(4\tau) = \left(\sum_{n \in \mathbb{Z}} q^{4 \cdot (2n)^2}\right)^4 = \left(\sum_{n \in \mathbb{Z}} q^{(4n)^2}\right)^4 = \theta_{0,4}(\tau)$$

olarak bulunur. Bu nedenle eşitlik (5.1) gereği

$$\theta_{0,4}(\tau) = \mathbb{E}_{64,1}(\tau) + 8\mathbb{E}_{64,11}(\tau)$$

olur ki bu da ispatı bitirir.

$\theta_{0,4}$ ve $\theta_{2,4}$ ’ nun ayrışımalarına bakarak aşağıdaki önerme elde edilir.

Teorem 6.2.2. (Mondal, 2026) Herhangi bir $n \in \mathbb{N} \cup \{0\}$ için

$$r_{2,4}(n) = \begin{cases} 16\sigma_1\left(\frac{n}{16}\right), & n \equiv 16(\text{mod}32), \\ 0, & \text{diğer durumlar} \end{cases}$$

$$r_{0,4}(n) = \begin{cases} 1, & \text{if } n = 1 \\ 24\left[\sigma_1\left(\frac{n}{16}\right) - 2\sigma_1\left(\frac{n}{32}\right)\right], & n \equiv 0(\text{mod}32) \\ 8\sigma_1\left(\frac{n}{16}\right), & n \equiv 16(\text{mod}32), \\ 0, & \text{diğer durumlar} \end{cases}$$

olur.

7. $\theta_{k,3}$ TETA SERİLERİ

Bu bölümde $mod\ 3$ ' teki denk kuadratik formlar üzerinde durulacaktır. Başka bir deyişle $Q_{k,3}$ tarafından temsil edilen tamsayılar araştırılacaktır. Teorem 2.4 gereği;

$$\theta_{k,3} \in \mathcal{M}_2(\Gamma_0(36) \cap \Gamma_1(3)) = \bigoplus_{\chi(-1)=1} \mathcal{M}_2(\Gamma_0(36), \chi) = \mathcal{M}_2(\Gamma_0(36))$$

Kolayca görülebilir $\dim(\mathcal{M}_2(\Gamma_0(36))) = 12$ ve $\dim(\mathcal{S}_2(\Gamma_0(36))) = 1$ olup böylece $\dim(\mathcal{E}_2(\Gamma_0(36))) = 11$ olarak elde edilir.

Eisenstein serilerinin uzayında bir bazı üretebilmek için S ve V operatörlerinin yardımıyla ve uygun bir sabit terim kullanılarak $\mathcal{E}_2(\Gamma_0(36))$ uzayının tüm elemanları aşağıda listelenmiştir:

$$\begin{aligned} B_1 &:= \hat{E}_2 | (2V_2 - S_{2,0}) | V_9(\tau) = 2\hat{E}_2 | V_{18} - \hat{E}_2 | S_{2,0} | V_9(\tau), \\ B_2 &:= c\hat{E}_2 | S_{6,1}(\tau), \quad B_3 := c\hat{E}_2 | S_{6,5}(\tau), \\ B_4 &:= c\hat{E}_2 | S_{3,1}(\tau), \quad B_5 := c\hat{E}_2 | S_{3,1} | V_2(\tau), \quad B_6 := c\hat{E}_2 | S_{3,1} | V_4(\tau), \\ B_7 &:= c\hat{E}_2 | S_{3,2}(\tau), \quad B_8 := c\hat{E}_2 | S_{3,2} | V_2(\tau), \quad B_9 := c\hat{E}_2 | S_{3,2} | V_4(\tau), \\ B_{10} &:= c\hat{E}_2 | S_{2,1}(\tau), \quad B_{11} := c\hat{E}_2 | S_{2,1} | V_3(\tau), \quad B_{12} := c\hat{E}_2 | S_{2,1} | V_9(\tau). \end{aligned}$$

$\dim(\mathcal{E}_2(\Gamma_0(36))) = 11$ olduğundan listedeki bazı elemanlar lineer bağımlı olmak zorundadır. Kolayca görülebilir ki $B_2 + B_3 + 4B_{11} - 3B_{12} - B_9 = 0$.

O halde $\mathcal{E}_2(\Gamma_0(36)) = \mathbb{C}[B_1, \dots, B_{11}]$, $\Gamma_0(36)$ ' nın denk olmayan cuspları aşağıdaki gibidir:

$$0, \frac{1}{18}, \frac{1}{12}, \frac{1}{9}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}, \infty.$$

(2.1), (2.2) ve (2.3) eşitlikleri kullanılarak $\mathcal{E}_2(\Gamma_0(36))$ 'nın tüm baz elemanlarının cusp noktasındaki değerleri (Mondal, 2026) Ek D' de yer almaktadır. Bu değerler kullanılarak farklı k değerleri için $\theta_{k,3}(\tau)$ ' ün analizi yapılacaktır.

7.1. $\theta_{0,3}$ Analizi

Dikkat edilirse;

$$\theta_3(18\tau)^4 = \left(\sum_{n \in \mathbb{Z}} q^{18\frac{n^2}{2}} \right)^4 = \left(\sum_{n \in \mathbb{Z}} q^{(3n)^2} \right)^4 = \theta_{0,3}(\tau).$$

Hatırlanacağı üzere $\theta_3(2\tau)^4 = \mathbb{E}_{4,1}(\tau) + 8\mathbb{E}_{4,2}(\tau)$ ve böylece

$$\theta_{0,3}(\tau) = (\mathbb{E}_{4,1} + 8\mathbb{E}_{4,2}) | V_9(\tau) = 2\hat{E}_2 | V_{18}(\tau) - \hat{E}_2 | S_{2,0} | V_9(\tau) - \frac{1}{3} \hat{E}_2 | S_{2,1} | V_9(\tau)$$

olarak bulunur. Tüm bunlar göz önüne alındığında aşağıdaki teorem elde edilir.

Teorem 7.1.1. (Mondal, 2026)

$$\text{Herhangi bir } n \in \mathbb{N} \cup \{0\} \text{ için } r_{0,3}(n) = \begin{cases} 1, & n = 1 \\ 24 \left[\sigma_1\left(\frac{n}{9}\right) - 2\sigma_1\left(\frac{n}{18}\right) \right], & n \equiv 0(\text{mod}18) \\ 8\sigma_1\left(\frac{n}{9}\right), & n \equiv 9(\text{mod}18) \\ 0, & \text{diğer durumlar} \end{cases}$$

olur.

7.2. $\theta_{1,3}$ Analizi

Önceki durumlarda cusp formlar hep 0 olarak gelmişti. Burada diğer durumlardan farklı olarak $\theta_{1,3}(\tau)$ cusp kısmına sahiptir. Bu ise analizi bir nebze zorlaştırmaktadır. İlk olarak $\theta_{1,3}(\tau)$ 'nin Fourier açılımını verelim.

$$\theta_{1,3}(\tau) = q^4 + 4q^7 + 6q^{10} + 4q^{13} + q^{16} + 4q^{19} + 12q^{22} + 12q^{25} + \dots$$

dikkat edilirse $n \equiv 1,4 (\text{mod}6)$ olmadıkça $r_{1,3}(n) = 0$ ' dır. $\Gamma_0(36)$ cusp yerlerinde $\mathcal{E}_2(\Gamma_0(36))$ 'nin baz elemanlarının değerleri (Mondal, 2026) Ek D' de verilmiştir.

Herhangi bir c cuspundaki aşağıdaki lineer birleşimi kullanacağız.

$$\theta_{1,3}(\tau) = \sum_{i=1}^{11} \ell_i B_i.$$

Lineer denklem sistemleri çözülerek aşağıdaki çözümler bulunmuştur:

$$\ell_2 = \frac{1}{3}, \ell_6 = -2, \ell_8 = 1.$$

Kabul edelim ki verilen teta serisinin aşağıdaki gibi bir Eisenstein serisi ve cusp form ayrışımı olsun.

$$\theta_{1,3}(\tau) = E_{1,3}(\tau) + f_{1,3}(\tau).$$

O halde Eisenstein serisi parçası aşağıdaki gibi gösterilir:

$$E_{1,3} = -\frac{1}{24} \left(\frac{1}{3} \hat{E}_2 |S_{6,1} - 2\hat{E}_2 |S_{3,1}|V_4 + \hat{E}_2 |S_{3,2}| V_2 \right).$$

Buradan hareketle cusp form şu şekilde elde edilir:

$$\begin{aligned}
f_{1,3}(\tau) &= \theta_{1,3}(\tau) - E_{1,3}(\tau) \\
&= -\frac{1}{3}(q - 4q^7 + 2q^{13} + 8q^{19} - 5q^{25} - 4q^{31} - 10q^{37} + 8q^{43} + 9q^{49} + \dots)
\end{aligned}$$

Üstelik $f_{1,3}(\tau) \in \mathcal{S}_2(\Gamma_0(36))$ şeklindedir. Bu ağırlık ve seviye için cusp form uzayının boyutu 1 olduğundan bu uzayda $\eta(\tau)$ Dedekind eta fonksiyonu olmak üzere, aynı zamanda normalleştirilmiş Hecke eigenform olan $\eta(6\tau)^4$ formu bu uzayı üretir. Sturm sınırına kadar Fourier açılımları kıyaslanarak $-3f_{1,3}(\tau) = \eta(6\tau)^4$ elde edilir. Böylece aşağıdaki teoremin ispatı elde edilir.

Teorem 7.2.1. (Mondal, 2026) Herhangi bir $n \in \mathbb{N} \cup \{0\}$ için

$$r_{1,3}(n) = \begin{cases} \sigma_1\left(\frac{n}{2}\right) - 2\sigma_1\left(\frac{n}{4}\right), & n \equiv 4(\text{mod}12), \\ \sigma_1\left(\frac{n}{2}\right) & n \equiv 10(\text{mod}12), \\ \frac{1}{3}\sigma_1(n) - \frac{1}{3}a(n), & n \equiv 1(\text{mod}6), \\ 0, & \text{diğer durumlar,} \end{cases}$$

olup burada $\eta(6\tau)^4 = \sum_{n \geq 1} a(n)q^n$ şeklindedir. Dikkat edilirse $\theta_{1,3}(\tau) = \theta_{2,3}(\tau)$ dir. Böylece herhangi bir $n \in \mathbb{N} \cup \{0\}$ için $n \in \mathbb{N}, r_{1,3}(n) = r_{2,3}(n)$ olduğu elde edilir.

8. $\theta_{k,6}$ TETA SERİLERİ

Bu bölümde $\text{mod } 6$ 'daki kuadratik formlar incelenecektir. Benzer argümanlar kullanılacaktır. Teorem 2.4 gereği

$$\theta_{k,6} \in \mathcal{M}_2(\Gamma_0(144) \cap \Gamma_1(6)) = \bigoplus_{\chi(-1)=1} \mathcal{M}_2(\Gamma_0(144), \chi) = \mathcal{M}_2(\Gamma_0(144)).$$

(3.1), (3.2) denklemlerini kullanarak $\dim(\mathcal{E}_2(\Gamma_0(144))) = 23$ olarak bulunur. Bu uzayı gerebilecek olası elemanlar aşağıda listelenmiştir.

$$\begin{aligned} A_1 &:= \hat{E}_2 | (2V_2 - S_{2,0}) | V_{36}(\tau) = 2\hat{E}_2 | V_{72} - \hat{E}_2 | S_{2,0} | V_{36}(\tau), \\ A_2 &:= c\hat{E}_2 | S_{12,1}(\tau), A_3 := c\hat{E}_2 | S_{12,5}(\tau), A_4 := c\hat{E}_2 | S_{12,7}(\tau), A_5 := c\hat{E}_2 | S_{12,11}(\tau), \\ A_6 &:= c\hat{E}_2 | S_{6,1}(\tau), A_7 := c\hat{E}_2 | S_{6,1} | V_2(\tau), A_8 := c\hat{E}_2 | S_{6,1} | V_4(\tau), \\ A_9 &:= c\hat{E}_2 | S_{6,5}(\tau), A_{10} := c\hat{E}_2 | S_{6,5} | V_2(\tau), A_{11} := c\hat{E}_2 | S_{6,5} | V_4(\tau), \\ A_{12} &:= c\hat{E}_2 | S_{3,1}(\tau), A_{13} := c\hat{E}_2 | S_{3,1} | V_2(\tau), A_{14} := c\hat{E}_2 | S_{3,1} | V_4(\tau), \\ A_{15} &:= c\hat{E}_2 | S_{3,1} | V_8(\tau), A_{16} := c\hat{E}_2 | S_{3,1} | V_{16}(\tau), \\ A_{17} &:= c\hat{E}_2 | S_{3,2}(\tau), A_{18} := c\hat{E}_2 | S_{3,2} | V_2(\tau), A_{19} := c\hat{E}_2 | S_{3,2} | V_4(\tau), \\ A_{20} &:= c\hat{E}_2 | S_{3,2} | V_8(\tau), A_{21} := c\hat{E}_2 | S_{3,2} | V_{16}(\tau), \\ A_{22} &:= c\hat{E}_2 | S_{2,1}(\tau), A_{23} := c\hat{E}_2 | S_{2,1} | V_2(\tau), A_{24} := c\hat{E}_2 | S_{2,1} | V_3(\tau), \\ A_{25} &:= c\hat{E}_2 | S_{2,1} | V_4(\tau), A_{26} := c\hat{E}_2 | S_{2,1} | V_6(\tau), \\ A_{27} &:= c\hat{E}_2 | S_{2,1} | V_9(\tau), A_{28} := c\hat{E}_2 | S_{2,1} | V_{12}(\tau), A_{29} := c\hat{E}_2 | S_{2,1} | V_{18}(\tau), \end{aligned}$$

Eşitlik (2.1), (2.3) kullanılarak $\mathcal{E}_2(\Gamma_0(144))$ 'ün baz elemanlarındaki cusp değerleri bulunabilir.

Şimdi k nın farklı değerleri için $\theta_{k,6}$ değerleri incelenecektir.

İlk olarak $\theta_{0,6}$, $\theta_{2,6}$, ve $\theta_{3,6}$ dikkate alınacaktır.

Teorem 8.1. (Mondal, 2026) $n \in \mathbb{N} \cup \{0\}$ için

$$\begin{aligned}
r_{0,6}(n) &= \begin{cases} 1 & n = 1, \\ 24 \left[\sigma_1 \left(\frac{n}{36} \right) - 2 \sigma_1 \left(\frac{n}{72} \right) \right], & n \equiv 0 \pmod{72}, n > 1, \\ 8 \sigma_1 \left(\frac{n}{36} \right), & n \equiv 36 \pmod{72}, \\ 0, & \text{diğer durumlar} \end{cases} \\
r_{1,6}(n) = r_{5,6}(n) &= \begin{cases} \frac{2}{3} \sigma_1 \left(\frac{n}{4} \right) + \frac{1}{3} a_{\eta(6\tau)^4} \left(\frac{n}{4} \right), & n \equiv 4 \pmod{24}, \\ 0, & \text{diğer durumlar} . \end{cases} \\
r_{2,6}(n) = r_{4,6}(n) &= \begin{cases} \frac{1}{3} \sigma_1 \left(\frac{n}{4} \right) - \frac{1}{3} a_{\eta(6\tau)^4} \left(\frac{n}{4} \right), & n \equiv 4 \text{ or } 28 \pmod{48}, \\ -\frac{4}{3} \sigma_1 \left(\frac{n}{16} \right) + \frac{1}{3} \sigma_1 \left(\frac{n}{4} \right), & n \equiv 16 \pmod{48}, \\ \frac{1}{3} \sigma_1 \left(\frac{n}{4} \right), & n \equiv 40 \pmod{48}, \\ 0, & \text{diğer durumlar} . \end{cases} \\
r_{3,6}(n) &= \begin{cases} 16 \sigma_1 \left(\frac{n}{36} \right), & n \equiv 36 \pmod{72}, \\ 0, & \text{diğer durumlar} \end{cases}
\end{aligned}$$

Burada $a_{\eta(6\tau)^4}(k)$ katsayısı $\eta(6\tau)^4$, ün cusp formunun q açılımının k . katsayısıdır.

İspat.

$$\begin{aligned}
\theta_{0,6}(\tau) &= \sum_{\substack{\vec{x} \in \mathbb{Z}^4 \\ x_i \equiv 0 \pmod{6}}} q^{x_1^2 + x_2^2 + x_3^2 + x_4^2} = \sum_{\vec{y} \in \mathbb{Z}^4} q^{36y_1^2 + 36y_2^2 + 36y_3^2 + 36y_4^2} \\
&= \sum_{\vec{y} \in \mathbb{Z}^4} q^{4(9y_1^2 + 9y_2^2 + 9y_3^2 + 9y_4^2)} = \sum_{\substack{\vec{t} \in \mathbb{Z}^4 \\ t_i \equiv 0 \pmod{3}}} q^{4(t_1^2 + t_2^2 + t_3^2 + t_4^2)} \\
&= \theta_{0,3}(4\tau)
\end{aligned}$$

olur. Benzer olarak kolayca gösterilebilir ki $\theta_{2,6}(\tau) = \theta_{1,3}(4\tau)$, $\theta_{3,6}(\tau) = \theta_{1,2}(9\tau)$.

olur. Burada ispat Teorem 4.2, 6.1 ve 6.3'den görülebilir. $\theta_{1,6}(\tau)$ için Fourier açılımı

$$\theta_{1,6}(\tau) = q^4 + 4q^{28} + 10q^{52} + 16q^{76} + 19q^{100} + 20q^{124} + 22q^{148} + \dots$$

Dikkat edilirse $n \equiv 4 \pmod{24}$ olmadıkça $r_{1,6}(n) = 0$ olur. Üstelik $\Gamma_0(144)$ grubunun cusp noktalarındaki değerler kıyaslanarak $\theta_{1,6}(\tau) = \frac{2}{3} A_8 + \frac{1}{3} f \Big| V_4(\tau)$ elde edilir. Burada $f(\tau) = \eta(6\tau)^4$ 'tür. Bu da ispatı bitirir.

9. NOKTA SAYIMI VE TETA SERİLERİ

Modülerite teoremi gereği θ üzerinde tanımlı her eliptik eğriye 2 ağırlıklı ve seviyesi eliptik eğrinin kondüktörü ile aynı olan bir modüler (Hecke eigenform) form karşılık gelir. Bu nedenle bu ilişkinin özel bir hali burada kullanılabilir. Daha kesin olarak $\mathbb{F}_p$ cismi üzerinde tanımlı eliptik eğri üzerindeki nokta sayımı formülü ile aslında bir modüler form kuadratik formun teta serileri arasında bir ilişki mutlak olarak beklenebilir. Özelinde ise bu ilişki kongrüent kuadratik formlar için doğrudur. $\eta(6\tau)^4$ iki ağırlıklı bir Hecke eigenform olduğu için ilk olarak bu cusp formu analizine ihtiyaç duymaktayız.

9.1 $y^2 = x^3 + 1$ Eliptik Eğrisi

$\eta(6\tau)^4$ cusp formuna karşılık gelen eliptik eğri LMFDB veri tabanında 36.A etiketi ile verilen eliptik eğridir. Açık şekilde ifade edilecek olursa bu eğri $y^2 = x^3 + 1$ dir. 36 kondüktörüne sahip bu sınıflar 4 tane izojenik eğri mevcuttur. Buradaki modüler eğri $X_0(36)$ olup cinsi 1 dir ve $\mathbb{Q}$ üzerinde bir kanonik modele sahiptir. Dikkat edilirse bu eliptik eğrinin diskriminantı sadece $p = 3$ asalı çarpan olarak vardır. O halde $p \neq 3$ asalları için E eliptik eğrisi $\mathbb{F}_p$ üzerinde iyi indirgemeye sahiptir ve bu özellikte p değerleri için nokta sayısı hesabı yapılabilir. İlk olarak bu eliptik eğri ile ilgili temel özellikleri yazacağız.

Teorem 9.1.1. (Silverman, 1994) $E: y^2 = x^3 + 1$ eliptik eğrisi için aşağıdaki önermeler doğrudur.

$$(1) E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/6\mathbb{Z},$$

$$(2) \text{Eliptik eğrisi } (-3) \text{ e göre kompleks çarpıma sahiptir,}$$

$$(3) L(E, s) = L(\eta(6\tau)^4, s)$$

Dikkat edilirse $p \equiv 5 \pmod{6}$ için $\eta(6\tau)^4$ formunun L fonksiyonu a_p katsayısı 0 olur.

9.2 Teorem 1.7'nin İspatı

Bundan böyle $N_p^E(k)$ ile $\mathbb{F}_{p^k}$ sonlu cismi üzerinde tanımlı E eliptik eğrisi üzerindeki nokta sayısı gösterilecektir. Teorem 1.7 nin ispatına geçmeden önce bu nokta sayımı ile ilgili çeşitli bilinen özellikler ispatlanacaktır.

Teorem 9.2.1. (Silverman, 1994) (Weil Teoremi)

a_p ile E eliptik eğrisi L fonksiyonunun p . katsayısı gösterilsin. α ve β ise $x^2 - a_p x + p = 0$ ikinci derece denkleminin kökleri gösterilsin. Bu takdirde herhangi bir $k \in \mathbb{N}$ için

$$N_p^E(k) = p^k + 1 - \alpha^k - \beta^k$$

olur.

Teorem 9.2.2. (Mondal, 2026)

$a_n \eta(6\tau)^4$ cusp formunun η Fourier katsayısı olsun. Bu takdirde p asal ve $k \in \mathbb{N}$ olmak üzere a_{p^k} için aşağıdaki gibi 3 terimli indirgeme bağıntısı vardır:

$$a_{p^k} = a_p a_{p^{k-1}} - p \cdot a_{p^{k-2}}$$

a_{p^k} katsayısı α ve β 'nin kuvvetleri olarak ifade edilebilir.

Lemma 9.2.3. (Mondal, 2026) a_{p^k} için aşağıdaki formül doğrudur:

$$a_{p^k} = \sum_{i=0}^k \alpha^i \beta^{k-i}$$

İspat. k üzerinden tümevarımla yapılacaktır. $k = 1$ için Teorem 8.2 kullanılarak $a_p = \alpha + \beta$ bulunur ki iddia doğrudur. $k = 2$ için Teorem 8.3'deki rekürans bağıntısı kullanılarak

$$a_{p^2} = a_p^2 - p a_1 = (\alpha + \beta)^2 - \alpha\beta = \alpha^2 + \alpha\beta + \beta^2$$

olur. Şimdi $k = m$ 'e kadar tüm k değerleri için förmülün doğru olduğunu kabul edelim bu takdirde $k = m$ ve $k = m - 1$ için sırasıyla

$$a_{p^{m-1}} = \sum_{i=0}^{m-1} \alpha^i \beta^{m-i-1} \tag{9.1}$$

$$a_{p^m} = \sum_{i=0}^m \alpha^i \beta^{m-i} \tag{9.2}$$

doğru olur. Nihayet $k = m + 1$ için Teorem 8.3 ve eşitlikler (9.1) ve (9.2) kullanılarak

$$\begin{aligned} a_{p^{m+1}} &= a_p a_{p^m} - p \cdot a_{p^{m-1}} \\ &= a_p \sum_{i=0}^m \alpha^i \beta^{m-i} - p \sum_{i=0}^{m-1} \alpha^i \beta^{m-i-1} \\ &= (\alpha + \beta) \cdot \sum_{i=0}^m \alpha^i \beta^{m-i} - \alpha\beta \cdot \sum_{i=0}^{m-1} \alpha^i \beta^{m-i-1} \\ &= \sum_{i=0}^{m+1} \alpha^i \beta^{m-i+1} \end{aligned}$$

Bu teoremin direkt bir sonucu olarak ve

$$\sigma_1(p^k) - p\sigma_1(p^{k-2}) = p^k + 1,$$

özdeşliği kullanılarak aşağıdaki sonuç elde edilir. Bu ise $r_{1,3}(p^k)$ için 3 terimli bir ilişki verir.

Sonuç 9.2.4. (Mondal, 2026) $N_p(k) = \sigma_1(p^k) - p\sigma_1(p^{k-2}) - (\alpha^k + \beta^k)$ olur.

Şimdi Teorem 1.7'nin ispatını verebiliriz. $p \equiv 1 \pmod{6}$ için ;

$$r_{1,3}(p) = \frac{1}{3}(\sigma_1(p) - a_p) = \frac{1}{3}(p + 1 - a_p) = \frac{1}{3}N_p(1)$$

elde edilir. Şimdi k üzerinden tümevarım yapacağız. $k = 1, 2$ için sonuç sırasıyla Lemma 8.4 ve Sonuç 8.5'den açıktır. O halde $k = m$ için eşitlik (1.2) doğru olsun yani

$$3r_{1,3}(p^m) = N(m) + 3p \cdot r_{1,3}(p^{m-2}).$$

Bu takdirde $k = m + 2$ için

$$\begin{aligned} 3r_{1,3}(p^{m+2}) &= \sigma_1(p^{m+2}) - a(p^{m+2}) \\ &= N(m+2) + p\sigma_1(p^m) + (\alpha^{m+2} + \beta^{m+2}) - a(p^{m+2}) \\ &= N(m+2) + p\sigma_1(p^m) - p \sum_{i=1}^m \alpha^i \beta^{m-i} \\ &= N(m+2) + 3p \cdot r_{1,3}(p^m) \end{aligned}$$

Elde edilir. Böylece sonuç gösterilmiş olur. Dikkat edilirse $p \equiv 5 \pmod{6}$ için $p^{2k+2} \equiv 1 \pmod{6}$ elde edilir ki benzer sonuç geçerlidir.

Uyarı 9.2.5. (Cho, 2018) Eliptik eğrilerle kongrüent kuadratik formlar arasındaki ilişki verilmiş olup bu sonuçlar Tablo 9.1'de özetlenmiştir. Dikkat edilirse bu tablodaki sonuçlar teoremdeki sonuçlara benzerdir.

Tablo 9.1. Eliptik eğriler ve kongrüent kuadratik formlar

Kuadratik form Q	Denklik koşulları	Eliptik Eğri E	CM	$N_p^E(1)$ ile $r(p)$ arasındaki ilişki	Denklik koşulundaki asallar
$x_1^2 + x_2^2 + x_3^2 + x_4^2$	$x_2, x_3, x_4 \equiv 0 \pmod{3},$ $x_1 \equiv 1 \pmod{3}$	$y^2 = x^3 + 1$	$\mathbb{Q}(\sqrt{-3})$	$3r(p) = 3p + 3 - 2N_p^E(1)$	$p \equiv 1, 7 \pmod{12}$

$x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$	$x_2, x_3, x_4 \equiv 0(\text{mod}2)$ $x_1 \equiv 1(\text{mod}2)$	$y^2 = x^3 + 4x$	$\mathbb{Q}(\sqrt{-1})$	$r(p) = 2p + 2 - N_p^E(1)$	$p \equiv 1(\text{mod}4)$
$x_1^2 + x_1x_2 + x_2^2 + x_3^2 + x_3x_4 + x_4^2$	$x_2, x_3, x_4 \equiv 0(\text{mod}3)$ $x_1 \equiv 1(\text{mod}3)$	$y^2 + y = x^3$	$\mathbb{Q}(\sqrt{-3})$	$3r(p) = 3p + 3 - 2N_p^E(1)$	$p \equiv 1(\text{mod}3)$
$x_1^2 + x_1x_2 + 2x_2^2 + x_3^2 + x_3x_4 + 2x_4^2$	$x_2, x_3, x_4 \equiv 0(\text{mod}2)$ $x_1 \equiv 1(\text{mod}2)$	$y^2 + xy + y = x^3 - x$	Yok	$3r(p) = 6p + 6 - 4N_p^E(1)$	$p \equiv 1(\text{mod}2)$

Örnek 9.2.6. $k = 7$ için böylece

$$a_{p^7} = \alpha^7 + \beta^7 + pa_p(\alpha^2 + \beta^2)^2 - p^3a_p$$

olur. O halde

$$\frac{1}{3}[N_p(7) + pN_p(5) + p^2N_p(3) + p^3N_p(1)] = \frac{1}{3}[\sigma_1(p^7) - a_{p^7}] = r_{1,3}(p^7).$$

elde edilir. Üstelik $k = 8$ için

$$a_{p^8} = \alpha^8 + \beta^8 + pa_p^2(\alpha^2 + \beta^2)(\alpha^2 + \beta^2 - p) - p^3(a_p^2 - \alpha^2 - \beta^2) + p^4.$$

olur.

O halde

$$\frac{1}{3}[N_p(8) + pN_p(6) + p^2N_p(4) + p^3N_p(2)] = \frac{1}{3}[\sigma_1(p^8) - a_{p^8}] = r_{1,3}(p^8).$$

olur.

Son olarak Teorem 1.9'daki genel ilişkiyi ispatlayalım. Eğer $n \not\equiv 1(\text{mod } 3)$ ise $r_{1,3}(n) = 0$ olduğu daha önce görülmüştür. Teorem 1.7' nin 3. Kısmı yardımıyla $n \equiv 1(\text{mod } 6)$ özelliğindeki bir doğal sayının asal çarpanlarına ayrılmasıyla $N_p(k)$ asal sayı sayılarıyla ilişkilendirilecektir. Dikkat edilirse p ve q farklı iki asalı ise:

$$r_{1,3}(p) = \frac{1}{3}[\sigma_1(p) - a_p], r_{1,3}(q) = \frac{1}{3}[\sigma_1(q) - a_q]$$

olur. Ancak

$$r_{1,3}(pq) = \frac{1}{3}[\sigma_1(pq) - a_{pq}] = \frac{1}{3}[\sigma_1(p)\sigma_1(q) - a_p a_q] \neq r_{1,3}(p)r_{1,3}(q)$$

olup $r_{1,3}(p)$ 'nin bir çarpımsal fonksiyon olmadığı açıktır.

Teorem 1.9'un ispatı için n 'nin asal çarpanlarındaki farklı asalların sayısı k olmak üzere k üzerinden tümevarım yapılacaktır. Tümevarımın ilk adımı $k = 1$ için aşıkardır. $k = 2$ için de aşıkardır. Sonra içinde aşıkardır. Sonra $k = m$ için hipotezin doğru olduğunu kabul edelim.

$$r_{1,3}\left(\prod_{j=1}^m p_j^{\alpha_j}\right) = \sigma_1(p_2^{\alpha_2}) \cdots \sigma_1(p_m^{\alpha_m}) r_{1,3}(p_1^{\alpha_1}) + \cdots + a_{p_1^{\alpha_1}} \cdots a_{p_{m-1}^{\alpha_{m-1}}} r_{1,3}(p_m^{\alpha_m}) \quad (9.3)$$

Böylece (8.3) kullanılarak $k = m + 1$ için

$$\begin{aligned} r_{1,3}\left(\prod_{i=1}^m p_i^{\alpha_i} \cdot p_{m+1}^{\alpha_{m+1}}\right) &= \sigma_1(p_2^{\alpha_2}) \cdots \sigma_1(p_m^{\alpha_m} p_{m+1}^{\alpha_{m+1}}) r_{1,3}(p_1^{\alpha_1}) + \cdots + a_{p_1^{\alpha_1}} \cdots a_{p_{m-1}^{\alpha_{m-1}}} r_{1,3}(p_m^{\alpha_m} p_{m+1}^{\alpha_{m+1}}) \\ &= \sigma_1(p_2^{\alpha_2}) \cdots \sigma_1(p_m^{\alpha_m}) \sigma_1(p_{m+1}^{\alpha_{m+1}}) r_{1,3}(p_1^{\alpha_1}) + \cdots \\ &\quad + a_{p_1^{\alpha_1}} \cdots a_{p_{m-1}^{\alpha_{m-1}}} \left[\sigma_1(p_{m+1}^{\alpha_{m+1}}) r_{1,3}(p_m^{\alpha_m}) + a_{p_m^{\alpha_m}} r_{1,3}(p_{m+1}^{\alpha_{m+1}}) \right] \\ &= \sum_{i=1}^{m+1} \left(\prod_{j=1}^{i-1} a_{p_j^{\alpha_j}} \prod_{l=i+1}^{m+1} \sigma_1(p_l^{\alpha_l}) \right) r_{1,3}(p_i^{\alpha_i}). \end{aligned}$$

elde edilir ki bu da ispatı bitirir.

KAYNAKÇA

- Beli, C. N. (2022). *Universal integral quadratic forms over dyadic local fields*. arXiv. <https://arxiv.org/abs/2008.10113>.
- Bhargava, M. (2000). On the Conway–Schneeberger fifteen theorem. In *Quadratic Forms and Their Applications*(Contemporary Mathematics, Vol. 272, pp. 27–37). American Mathematical Society. <https://doi.org/10.1090/conm/272/04395>
- Bringmann, K., & Kane, B. (2022). Conjectures of Sun about sums of polygonal numbers. *Matematica*, 1(4), 809–828. <https://doi.org/10.1007/s44007-022-00030-1>.
- Cho, B. (2018). On the number of representations of integers by quadratic forms with congruence conditions. *Journal of Mathematical Analysis and Applications*, 462(1), 999–1013. <https://doi.org/10.1016/j.jmaa.2017.12.060>.
- Cohen, H., & Strömberg, F. (2017). *Modular forms*. American Mathematical Society. <https://doi.org/10.1090/gsm/179>.
- Koblitz, N. (1993). *Introduction to elliptic curves and modular forms* (2nd ed.). Springer
- Miyake, T. (1989). *Modular forms*. Springer. <https://doi.org/10.1007/978-3-642-51497-9>.
- Mondal, K. (2026). Relating elliptic curve point-counting and solutions of quadratic forms with congruence conditions. *The Ramanujan Journal*, 69, 63. <https://doi.org/10.1007/s11139-026-01341-5>.
- Ramanujan, S. (1917). On the expression of numbers in the form $ax^2+by^2+cz^2+du^2$. *Proceedings of the Cambridge Philosophical Society*, 19, 11– 21.
- Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170), 483-494.
- Silverman, J. H. (1994). *Advanced topics in the arithmetic of elliptic curves*. Springer.
- Sun, Z.-W. (2015). On universal sums of polygonal numbers. *Science China Mathematics*, 58 (7), 1367–1396. <https://doi.org/10.1007/s11425-015-4994-4>
- Wiles, A. (1995). Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3), 443–551. <https://doi.org/10.2307/2118559>