KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

Γ^2 , Γ^3 VE HECKE GRUPLARININ NORMALLİYENİ VE GRAFLAR

DOKTORA TEZİ

Zeynep ŞANLI

OCAK 2019
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

Γ^2 , Γ^3 VE HECKE GRUPLARININ NORMALLİYENİ VE GRAFLAR

ZEYNEP ŞANLI

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"DOKTOR(MATEMATİK)"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 06 / 12 /2018
Tezin Savunma Tarihi : 18 / 01 /2019

Tez Danışmanı : Prof. Dr. Mehmet AKBAŞ

Trabzon 2019

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Matematik Anabilim Dalında
Zeynep ŞANLI Tarafından Hazırlanan

Γ^2 , Γ^3 VE HECKE GRUPLARININ NORMALLİYENİ VE GRAFLAR

başlıklı bu çalışma, Enstitü Yönetim Kurulunun 11 /12/2018 gün ve 1782 sayılı kararıyla oluşturulan jüri tarafından yapılan sınavda
DOKTORA TEZİ
olarak kabul edilmiştir.

Jüri Üyeleri

Başkan :	**Prof. Dr. Mehmet AKBAŞ**	…...……………………………....
Üye :	**Prof. Dr. Ahmet Hakan YILMAZ**	…...…………………………...…
Üye :	**Prof. Dr. Funda KARAÇAL**	……...……………………...……
Üye :	**Prof. Dr. Ruşen YILMAZ**	……...……………………...……
Üye :	**Doç. Dr. Murat BEŞENK**	……...……………………...……

Prof. Dr. Sadettin KORKMAZ
Enstitü Müdürü

ÖNSÖZ

Bu çalışma, Γ Modüler grubunun alt gruplarından Γ^2, Γ^3 alt gruplarının kongrüans alt gruplarının normalliyenini, Hecke grubunun $\lambda = 5$ olması durumunda özel bir kongrüans alt grubunun normalliyenini göstermek ve buradan elde edilecek sonuçları sunmak amacı ile Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında doktora tez çalışması olarak yapılmıştır.

Konunun belirlenmesinden, çalışmanın tamamlanmasına kadar olan süreçte emeğiyle, öneri ve yönlendirmeleriyle önemli katkıda bulunan danışman hocam Sayın Prof. Dr. Mehmet AKBAŞ'a en içten dileklerimle saygı ve şükranlarımı sunuyorum. Aynı zamanda bu tez aşamasında değerli görüş ve tavsiyeleri ile katkıda bulunan tez izleme jüri üyesi hocalarım, Prof. Dr. Funda KARAÇAL ve Prof. Dr. Ahmet Hakan YILMAZ'a teşekkürü bir borç bilirim. Bu tezi tamamlama sürecinde verdikleri destekten dolayı ve öğrenim sürecinde katkı sağlayan Matematik Bölümündeki tüm değerli öğretim üyelerine ve araştırma görevlisi arkadaşlarıma teşekkür ederim.

Tüm eğitim-öğretim hayatım boyunca maddi ve manevi desteklerini esirgemeyen aileme ve sevgili eşim Levent'e çok teşekkür ederim.

Zeynep ŞANLI

Trabzon 2019

TEZ ETİK BEYANNAMESİ

Doktora Tezi olarak sunduğum “ Γ^2, Γ^3 VE HECKE GRUPLARININ NORMALLİYENİ VE GRAFLAR” başlıklı bu çalışmayı baştan sona kadar danışmanım Prof. Dr. Mehmet AKBAŞ’ın sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuarlarda yaptığımı/yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim. 18/01/2019

Zeynep ŞANLI

İÇİNDEKİLER

Sayfa No

Doktora Tezi

ÖZET

Γ^2 , Γ^3 VE HECKE GRUPLARININ NORMALLİYENİ VE GRAFLAR

Zeynep ŞANLI

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Matemtik Anabilim Dalı
Danışman: Prof. Dr. Mehmet AKBAŞ
2019, 71 Sayfa

Bu tezde [8] de verilen " $I=(2)^{\alpha}I'$, $\mathbb{Z}[\lambda_5]$ in bir ideali ve $(2,I')=1$ olsun. Bu takdirde $H_0^5(I)$ kongrüans alt grubunun H^5 Hecke grubundaki normalliyeni, $\alpha=\alpha'-\min\left(2,\left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$ olmak üzere $H_0^5((2)^{\alpha'}I')$ dır." konjektürün I nın bir karesiz ideal olması durumunda ispatı yapıldı. Ayrıca Γ modüler grubunun alt grupları olan Γ^2 ve Γ^3 te sırasıyla kongrüans alt grupları olan $\Gamma_0^2(n)$ ve $\Gamma_0^3(n)$ için normalliyen hesaplandı. Ek olarak $\Gamma_{0,n}(N)$ kongrüans alt grubunun alt yörüngesel grafları incelendi.

Birinci bölümde konu ile ilgili genel bilgiler ve literatürdeki bazı önemli tanım, teorem ve sonuçlar verildi.

İkinci bölümde ise yukarıda belirtilen gruplar için normalliyen hesaplandı. Bunlarla ilgili teorem ve sonuçlar verildi. Bunların yanı sıra $\Gamma_{0,n}(N)$ kongrüans alt grubunun alt yörüngesel graflarını incelemek için gerekli olan indeks hesapları yapıldı ve kenar şartları belirlendi.

Anahtar Kelimeler: Hecke grubu, modüler grup, alt yörüngesel graf, normalliyen, indeks

PhD. Thesis

SUMMARY

THE NORMALIZERS OF THE GROUPS Γ^2 , Γ^3 AND HECKE AND GRAPHS

Zeynep ŞANLI

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Mathematics Graduate Program
Supervisor: Prof. Dr. Mehmet AKBAŞ
2019, 71 Pages

In this thesis, it is shown that the conjecture "Let $I = 2^{\alpha}I'$, where $(2, I') = 1$, be an ideal of $\mathbb{Z}[\lambda_5]$. Then the normalizer of $H_0^5(I)$ in H^5, is $H_0^5((2)^{\alpha'}I')$ where $\alpha = \alpha' - \min\left(2, \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$." in [8] is proved when I is a nonsquare ideal of $\mathbb{Z}[\lambda_5]$. Moreover, in the subgroups Γ^2 and Γ^3, subgroups of modular group Γ, the normalizers of the congruence subgroups $\Gamma_0^2(n)$ and $\Gamma_0^3(n)$, the congruence subgroups of Γ^2 and Γ^3 are found respectively. In addition, the suborbital graph of the congruence subgroup $\Gamma_{0,n}(N)$ is examined.

In the first chapter, some necessary definitions, notations and results for the preceeding chapters are given.

In the second chapter, the normalizers of the above mentioned groups are determined. Some theorems and conclusions related to these are given. In addition to these, in order to examine the suborbital graph of the congruence subgroup $\Gamma_{0,n}(N)$ the necessary index calculations are given and edge conditions are determined.

Key Words: Hecke group, godular group, guborbital graph, normalizer, index

SEMBOLER DİZİNİ

Γ	: Modüler grup
Γ^2	: Modüler grubun elemanlarının karelerinin ürettiği grup
Γ^3	: Modüler grubun elemanlarının küplerinin ürettiği grup
$\Gamma_0(N)$	: Modüler grubun $c \equiv 0\ mod\ n$ olan alt grubu
$\Gamma_{0,n}(N)$	: $\Gamma_0(N)$ nin elemanlarının $a \equiv d\ mod\ n$ olan alt grubu
${\Gamma^2}_0(N)$	: Γ^2 grubunun $c \equiv 0\ mod\ n$ olan alt grubu
${\Gamma^3}_0(N)$	: Γ^3 grubunun $c \equiv 0\ mod\ n$ olan alt grubu
H^5	: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ elemanları tarafından üretilen Hecke grubu
$H_0^5(I)$	: Hecke grubunun $c \equiv 0\ mod\ I$ olan grubu
$\lvert A{:}\,B \rvert$	: B grubunun A grubundaki indeksi
Gx	: x noktasının G yörüngesi
G_x	: x noktasının G'deki sabitleyeni
$\mathbb{Z}$	: Tamsayılar kümesi
$\mathbb{Q}$	: Rasyonal sayılar kümesi
$\widehat{\mathbb{Q}}$	: Genişletilmiş rasyonel sayılar kümesi
$\mathbb{R}$	: Reel sayılar kümesi
$\mathbb{C}$	: Kompleks sayılar kümesi
$\mathbb{C}_\infty$	: Genişletilmiş kompleks sayılar kümesi
λ	: $\frac{1+\sqrt{5}}{2}$ irrasyonel sayısı
$\mathbb{Z}[\lambda]$	: $a, b \in \mathbb{Z}$ olmak üzere $a + b\lambda$ şeklindeki sayılar
$PSL(2, \mathbb{R})$	: Gerçel katsayılı, lineer, kesir dönüşümlerinin grubu
$\varphi(N)$	: Euler Fonksiyonu

1. GENEL BİLGİLER

1.1. Giriş

19. yüzyılın sonlarına doğru ayrık gruplar teorisine temel teşkil edecek bazı önemli sonuçlar ilk defa Henry Poincare tarafından göz önüne getirilmiş ve eliptik fonksiyonlar teorisinin genelleştirilmesi için kullanılmıştır. Fuchsian grupları adı verilen ve sistematik çalışmasını Henry Poincare'nin geliştirdiği bu ayrık grupların invaryant bıraktığı fonksiyonlar üzerinde birçok bilim adamı çalışmalar yapmıştır. Lineer kesirli dönüşümler grubu özellikle 19. yüzyılda Öklid olmayan geometriler ve İnvaryant teorinin keşfiyle birlikte büyük önem kazanmış, topolojik grup yapısına uygun olması nedeniyle gerek analiz, gerekse cebirsel yöntemlerle derinlemesine incelenmiştir. Eliptik eğrilerin aritmetiği, integral kuadratik formlar ve eliptik modüler fonksiyonlar teorisindeki önemi nedeniyle en çok Γ modüler grubunun kongrüans alt grupları olan $\Gamma(\mathrm{N}), \Gamma_1(\mathrm{N}), \Gamma_0(\mathrm{N}), \Gamma^0(\mathrm{N})$ grupları üzerinde çalışılmıştır. Son yıllarda sayılar teorisinde de Γ modüler grubunun kongrüans alt grupları Pierre de Fermat'ın 1637 yılında ifade ettiği son teoremin ispatında oldukça önemli bir yer teşkil ettiği görülmektedir.

Daha sonra ise Eriche Hecke , 1936 yılında " Über die Bestimmung Dirichletcher Reichen durch ihre Funktionalgleichungen" adlı çalışmasında, λ sabit bir pozitif tamsayı olmak üzere,

$$T(z) = -\frac{1}{z}\ ,\ \ U(z) = z + \boldsymbol{\lambda}$$

kesirli doğrusal dönüşümleri ile üretilen ve $H(\lambda)$ ile gösterilen grupları tanıtmıştır [7]. Burada $S = TU$ alınırsa

$$S(z) = -\frac{1}{z+\lambda}$$

elde edilir. Bu gruplar, $H(\lambda)$ bir Fuchsian grup olduğundan Dirichlet serilerinin çalışmasında kullanılır. Hecke grupları ile ilgili olarak David Rosen, 1963 yılında "An arithmetic characterization of the parabolic points of $G(2\cos\frac{\pi}{5})$" adlı makalesinde $\lambda =$

$\lambda_q = 2cos\frac{\pi}{q},\ q = 5$ olması durumunda $G(\lambda)$ nın parabolik noktalarını karakterize etmiştir [20].

1990 yılında Mehmet Akbaş ve David Singerman'ın yaptıkları çalışmada $\Gamma_0(\mathrm{N})$ nin $PSL(2,\mathbb{R})$ deki normalliyeni araştırılmıştır [3]. Bu normalliyen $\Gamma_0(\mathrm{N})$ ile ilişkili Riemann yüzeyleri üzerindeki Weierstrass noktaları ile ilgili çalışmalarda ve Modüler formlarda önemli bir rol oynamaktadır.

2000 yılında ise Hecke gruplarının temel kongrüans alt grupları üzerinde Mong-Lung Lang, Chong-Hai Lim ve Ser-Peow Tan tarafından bazı çalışmalar yapılmıştır. " Principal Congruence Subgroups of the Hecke Groups" adlı bu makalede $q > 3$ bir tek tamsayı, G_q bir Hecke grubu, (τ), $\mathbb{Z}[\lambda_q]$ nun bir asal ideali ve $G(q,\tau), G_q$ nun temel kongrüans alt grubu olmak üzere $\left[G_q: G(q,\tau)\right] \coloneqq G(q,\tau)$ temel kongrüans alt grubunun G_q daki indeksinin formülü elde edilmiştir. Ayrıca bu makalede $[G_1(q,\tau), G(q,\tau)]$ ve $[G_0(q,\tau), G_1(q,\tau)]$ indislerinin formülleri verilmiştir. Son olarak q bir asal sayı olması durumunda $G(q,\tau)$ geometrik invaryantları için formüller ortaya çıkmıştır [11].

Mong-Lung Lang'ın 2001 yılında yayınlanan "Normalizers of the Congruence Subgroups of the Hecke Groups G_4 and G_6" adlı çalışmasında $PSL(2,\mathbb{R})$ de $\Gamma_0(\mathrm{m}) + \mathrm{w}_2$ ve $\Gamma_0(\mathrm{m}) + \mathrm{w}_3$ tanımlanmıştır. Bu tip normalliyenlerin tanımı, G_4 ve G_6 Hecke gruplarının $G_4^0(A)$ ve $G_6^0(A)$ kongrüans alt gruplarının $PSL(2,\mathbb{R})$' deki normalliyenlerini tanımlamaya olanak sağlamıştır [13].

Yine Mong-Lung Lang tarafından 2007 yılında yapılan " The Structure of the Normalizers of the Congruence Subgroups of the Hecke Group G_5" adlı çalışmada şu gösterilmiştir: $\lambda = 2cos\frac{\pi}{5}$ ve τ da $\mathbb{Z}[\boldsymbol{\lambda}]$ nın bir asal ideal olsun. $G_0(\tau)$ nun $PSL(2,\mathbb{R})$ deki G_5 Hecke grubundaki normalliyeni $N(G_0(\tau))$ ile gösterilmek üzere, $N\big(G_0(\tau)\big) = G_0\left(\frac{\tau}{h}\right)$ dir. Burada h; 4 ün en büyük bölenidir ve h^2, τ yu böler [14].

Charles C. Sims tarafından 1967 yılında yayımlanan " Graphs and Finite Permutation Groups" adlı makalede ([24]) ve Gareth A. Jones, David Singerman ve K. Wicks'in, 1991 yılında yayınlanan " The Modular Group and Generalized Farey Graphs" adlı çalışmasında ([10]) alt yörüngesel graflar ve bu graflardaki devre uzunlukları incelenmiştir. S.P. Chan , M.L. Lang , C.H. Lim 1994 yılında "The invariants of the

Congruence Subgroups $G_0(\beta)$ of the Hecke Group G_5" adlı çalışmada $\beta \subset \mathbb{Z}[\lambda]$ sıfırdan farklı bir ideal olmak üzere $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \lambda_5 \\ 0 & 1 \end{pmatrix}$ elemanları tarafından üretilen G_5 Hecke grubunda Γ modüler grubunun $\Gamma_0(\mathrm{N})$ alt grubuna karşılık gelen $G_0(\beta)$ kongrüans alt grubun simgesindeki invaryantlar bulunmuş ve $G_0(\beta)$ grubunun üretici eliptik elemanlarının mertebelerinin 2 veya 5 olduğu gösterilmiştir [5]. M. Akbaş'ın 2001 yılındaki " On Suborbital Graphs for the Modular Group" adlı çalışmasında devre uzunlukları ile ayrık grupların üretici eliptik elemanlarının mertebeleri arasındaki ilişki ortaya konmuştur [2].

1.2. Topolojik Gruplar

Tanım 1.2.1.[9] $(G,\cdot)$ bir grup ve aynı zamanda bir topolojik uzay olsun. Bu takdirde her $g, h \in G$ için

i. $m: G \times G \longrightarrow G$

$(g,h) \rightarrow g \cdot h$

ii. $i: G \longrightarrow G$

$g \rightarrow g^{-1}$

dönüşümleri sürekli ise G ye bir topolojik grup denir.

Tanım 1.2.2.[9] G bir topolojik grup ve X bir topolojik uzay olsun. Bu taktirde

$$\Lambda: G \times X \longrightarrow X$$

$$\Lambda(g,x) = g\Lambda x =: gx$$

sürekli bir dönüşüm ve her $g_1, g_2 \in G$ ve her $x \in X$ için

i. $(g_1 g_2)x = g_1(g_2 x)$

ii. $ex = x$ (e G' nin birimi)

şartları sağlanıyorsa $[G, X, \Lambda]$ üçlüsüne veya $[G, X]$ ikilisine bir topolojik dönüşüm grubu adı verilir. Bu durumda G ye X üzerinde bir hareket grubu denir.

Tanım 1.2.3.[9] Δ bir topolojik uzayın alt kümesi olsun. Eğer her $x \in \Delta$ için $U \cap \Delta = \{x\}$ olacak şekilde bir U komşuluğu varsa Δ ya ayrıktır denir.

Örneğin, $\mathbb{Z}$ tamsayılar kümesi $\mathbb{R}$ nin bir ayrık alt kümesidir. $\mathbb{R}$ nin her bir sonlu alt kümesi de $\mathbb{R}$ nin bir ayrık alt kümesidir. $\left\{\frac{1}{n}\middle| n \in \mathbb{Z},\ n \neq 0\right\}$ kümesi $\mathbb{R}$ nin ayrık bir alt kümesidir. Ancak $A = \left\{\frac{1}{n}\middle| n \in \mathbb{Z},\ n \neq 0\right\} \cup \{0\}$ kümesi $\mathbb{R}$ nin ayrık bir alt kümesi değildir.

Lemma 1.2.4.[19] $[G, X]$ bir topolojik dönüşüm grubu ve $x, y \in X$ olsun. Bu taktirde

$$x \approx y :\Leftrightarrow \exists g \in G : gx = y$$

şeklinde tanımlanan " $\approx$ " bağıntısı X üzerinde bir denklik bağıntısıdır.

Tanım 1.2.5. " $\approx$ " bağıntısının denklik sınıflarına hareketin yörüngeleri denir. Ayrıca $x \in X$ noktasını içeren yörüngeye x in yörüngesi denir ve bu $Gx := \{gx | g \in G\}$ kümesidir.

Tanım 1.2.6. G, X üzerinde hareket etsin ve $x, y \in X$ keyfi olsun. $gx = y$ olacak biçimde bir $g \in G$ elemanı varsa G ye X üzerinde transitif olarak hareket ediyor denir. Bu tanıma göre hareket transitif ise $\forall x \in X$ için $Gx = X$ elde edilir. Yani bir tek yörünge vardır. Yörünge grubun transitif olarak hareket ettiği kümedir.

Tanım 1.2.7. G bir grup ve $H < G$ olsun. H alt grubuna göre sağ ve sol denklik sınıflarının sayısı aynıdır. Bu sayıya H alt grubunun G içerisindeki indeksi denir ve $|G : H|$ ile gösterilir.

Tanım 1.2.8.[9] G, X üzerinde hareket etsin ve $x \in X$ olsun. $G_x := \{g \in G | gx = x\}$ kümesine x noktasının sabitleyeni denir.

Sonuç 1.2.9. [9] G_x sabitleyeni G nin bir alt grubudur.

Sonuç 1.2.10.[9] $x, y \in X$ ve $g \in G$ olmak üzere $y = gx$ olsun. Bu takdirde G_x ve G_y eşleniktir.

İspat: $G_{gx} = gG_xg^{-1}$ olduğu açıktır.

Lemma 1.2.11.[19] G, X üzerinde hareket etsin ve $x \in X$ olsun. Bu durumda $|Gx| = |G : G_x|$ dir.

İspat: $Gx = \{gx | g \in G\}$ ve $G_x = \{g \in G | \ \forall x \in X$ için $gx = x\}$ olduğunu biliyoruz.

$Y \coloneqq \{gG_x : g \in G\}$ için $\alpha: Gx \longrightarrow Y, \alpha(gx) \coloneqq gG_x$ şeklinde tanımlansın.

i. α nın iyi tanımlı olduğunu gösterelim. $g_1, g_2 \in G$ ve $x \in X$ olsun. Eğer $g_1x = g_2x$ ise $\alpha(g_1x) = \alpha(g_2x)$ midir?

$$g_1x = g_2x \Rightarrow {g_2}^{-1}g_1x = {g_2}^{-1}(g_1x) = {g_2}^{-1}g_2x = x \Rightarrow {g_2}^{-1}g_1 \in G_x$$

dir. Şimdi ${g_2}^{-1}g_1 \in G_x \Rightarrow g_1G_x = g_2G_x$ yani ${g_2}^{-1}g_1 \in G_x \Rightarrow {g_2}^{-1}g_1G_x = G_x$ olduğunu gösterelim. $h \in G_x$ olsun.

$${g_2}^{-1}g_1hx = {g_2}^{-1}g_1x = x \Rightarrow {g_2}^{-1}g_1G_x \subset G_x \qquad (*)$$

$$g_2hx = g_2x = g_1x \Rightarrow g_1^{-1}g_2hx = x \Rightarrow g_1^{-1}g_2h \in G_x \Rightarrow h \in {g_2}^{-1}g_1G_x \Rightarrow G_x \subset {g_2}^{-1}g_1G_x \qquad (**)$$

olup $(*)$ ve $(**)$ dan ${g_2}^{-1}g_1G_x = G_x$ dir. Böylece

$$g_1x = g_2x \Rightarrow g_1G_x = g_2G_x \Rightarrow \alpha(g_1x) = \alpha(g_2x)$$

bulunur.

ii. α nın birebir olduğunu gösterelim. $g_1, g_2 \in G$ ve $x \in X$ için $\alpha(g_1x) = \alpha(g_2x)$ olsun. $\alpha(g_1x) = \alpha(g_2x) \Rightarrow g_1G_x = g_2G_x \Rightarrow {g_2}^{-1}g_1 \in G_x \Rightarrow {g_2}^{-1}g_1x = x$ dir. $g_1x = g_2{g_2}^{-1}g_1x = g_2({g_2}^{-1}g_1x) = g_2x$ olup α birebirdir.

iii. α nın örten olduğunu gösterelim. $v \in Y$ olsun. Buna göre $v = gG_x$ olacak şekilde bir $g \in G$ vardır. Buradan $\alpha(gx) = gG_x = v$ olup α örtendir.

Dolayısıyla $|Gx| = |Y| = |G : G_x|$ elde edilir.

Tanım 1.2.12. G bir grup olsun. $C \coloneqq \{g \in G | \forall x \in G$ için $gx = xg\}$ kümesine G nin merkezi denir.

Tanım 1.2.13. Bir T dönüşümünün periyodu (veya mertebesi) $T^m = I$ eşitliğini sağlayan en küçük pozitif tam sayıdır. Böyle bir m sayısı yoksa T' ye sonsuz periyotludur denir.

Tanım 1.2.14. $n \in \mathbb{N}$ için $1 \leq a \leq n$ ve $(a, n) = 1$ olan a tamsayılarının sayısı $\varphi(n)$ ile gösterilir. Bu fonksiyona Euler fonksiyonu denir.

$n = {p_1}^{r_1}{p_2}^{r_2} \cdots {p_s}^{r_s}$ ise bu taktirde

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$

dir.

1.3. Modüler Grup

Tanım 1.3.1. $PSL(2, \mathbb{R})$ grubunun

$$\Gamma \coloneqq PSL(2, \mathbb{Z}) = \left\{ z \longrightarrow \frac{az+b}{cz+d} \middle| \, a, b, c, d \in \mathbb{Z} \text{ ve } ad - bc = 1 \right\}$$

alt grubuna Modüler Grup adı verilir. Bu grup aşağıdaki gibi 2×2 lik tam sayılar matrisleriyle de temsil edilebilir:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, det\ A = 1.$$

A ve $-A$ aynı dönüşümü temsil ettiğinden söz konusu matris negatifi ile eş alınır. Böylece, bu tez içerisinde, matris ve dönüşüm arasında bir ayrım yapılmayacaktır. Ayrıca

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ ve } \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}, k \neq 0$$

matrisleri yine aynı dönüşümü temsil ettiğinden matris hesaplamalarında uygun olduğu yerde bu matrisler eşit olarak yazılabilir. (Burada determinantın 1 olma şartı aranmayacaktır.) Aşağıdaki teorem Γ modüler grubunun $T(z) = z + 1$ ve $U(z) = -\frac{1}{z}$ dönüşümleri ile üretildiğini göstermektedir.

Teorem 1.3.2.[23] Γ modüler grubu $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ve $U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ matrisleriyle üretilir. ■

1.4. Γ nın $\widehat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ Üzerindeki Hareketi

$\widehat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ genişletilmiş rasyonel sayılar kümesinin her elemanı $x, y \in \mathbb{Z}$ ve $(x, y) = 1$ olmak üzere bir x/y indirgenmiş kesri olarak gösterilebilir. $x/y = -x/-y$ olduğundan bu gösterim tek değildir. ∞ u $1/0 = -1/0$ olarak gösterelim. Γ nın $\widehat{\mathbb{Q}}$ üzerindeki hareketi

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \frac{x}{y} \to \frac{ax+by}{cx+dy}$$

dir. $T \in \Gamma$ olmak üzere

$$T\left(\frac{x}{y}\right) = \frac{a\frac{x}{y}+b}{c\frac{x}{y}+d} = \frac{ax+by}{cx+dy} \text{ ve } T\left(\frac{-x}{-y}\right) = \frac{-ax-by}{-cx-dy} = \frac{ax+by}{cx+dy} = T\left(\frac{x}{y}\right)$$

olduğundan Γ grubunun $\widehat{\mathbb{Q}}$ üzerindeki hareketi iyi tanımlıdır. Eğer $(x, y) = 1$ ve $ad - bc = 1$ ise $\frac{ax+by}{cx+dy}$ indirgenmiş kesirdir [10].

Teorem 1.4.1.[10] Γ nın $\widehat{\mathbb{Q}}$ üzerindeki hareketi transitiftir. ■

Teorem 1.4.2.[10] $\widehat{\mathbb{Q}}$ nın herhangi bir noktasının sabitleyeni sonsuz devirlidir. ■

1.5. Modüler Grubun Kongrüans Alt Grupları

Tanım 1.5.1. n pozitif tamsayı olmak üzere Γ grubunun temel kongrüans alt grubu

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| \, a \equiv d \equiv 1 \ (mod\, n),\ b \equiv \ c \equiv 0 \ (mod\, n) \right\}$$

ile tanımlanır. Γ grubunun $\Gamma(n)$ temel kongrüans alt gruplarını içeren herhangi bir alt grubuna kongrüans alt grubu denir. Üzerinde en çok çalışılan bazı kongrüans alt grupları

$$\Gamma_1(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| \, a \equiv d \equiv 1 \ (mod\, n),\ c \equiv 0 \ (mod\, n) \right\},$$

$$\Gamma_0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| \, c \equiv 0 \ (mod\, n) \right\},$$

$$\Gamma^0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| \, b \equiv 0 \ (mod\, n) \right\}$$

gruplarıdır. $n \in \mathbb{Z}$ olmak üzere $\Gamma(n) \leq \Gamma_1(n) \leq \Gamma_0(n) \leq \Gamma$ biçimindedir.

Ayrıca $\Gamma(n)$, Γ grubunun normal bir alt grubudur, dolayısıyla $\Gamma(n)$ grubu $\Gamma_0(n)$ ve $\Gamma_1(n)$ gruplarının da normal alt grubudur. Diğer taraftan $\Gamma_1(n) \lhd \Gamma_0(n)$ dir. Buna göre indeksler $n > 2$ için

$$|\Gamma: \Gamma_0(n)| = n \prod_{p|n} \left(1 + \frac{1}{p}\right), \ |\Gamma: \Gamma_1(n)| = \frac{n^2}{2} \prod_{p|n} \left(1 - \frac{1}{p^2}\right),$$

$$|\Gamma: \Gamma(n)| = \frac{n^3}{2} \prod_{p|n} \left(1 - \frac{1}{p^2}\right)$$

dir.

$n = 2$ durumunda $|\Gamma: \Gamma_0(2)| = 3, |\Gamma: \Gamma_1(2)| = 3, |\Gamma: \Gamma(2)| = 6$ dir. $n > 2$ için yukarıda verilen indekslerden aşağıdaki sonuçlar kolayca elde edilir;

$$|\Gamma_0(n): \Gamma_1(n)| = \frac{|\Gamma: \Gamma_1(n)|}{|\Gamma: \Gamma_0(n)|} = \frac{n}{2} \prod_{p|n} \left(1 - \frac{1}{p}\right), \ |\Gamma_1(n): \Gamma(n)| = \frac{|\Gamma: \Gamma(n)|}{|\Gamma: \Gamma_1(n)|} = n.$$

$\Gamma_0(n), \Gamma_1(n)$ ve $\Gamma(n)$ gruplarının cusp kümesi de $\hat{\mathbb{Q}}$ dır. Çünkü bu gruplar Γ grubunun sonlu indeksli alt gruplarıdır ve bir Λ Fuchsian grubunun sonlu indeksli herhangi bir alt grubu da Λ ile aynı cusp kümesine sahiptir [17].

Teorem 1.5.2.[10] $n > 1$ olmak üzere $\Gamma_0(n)$ grubunun $\hat{\mathbb{Q}}$ üzerindeki hareketi transitif değildir. ■

1.6. Γ^2 Modüler Alt Grubu

Γ^2 ile Γ modüler grubunun elemanlarının karelerinin ürettiği grubu göstereceğiz ve kolaylıkla görülür ki $\Gamma^2 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma: ab + bc + cd \equiv 0 \ mod 2\right\}$ dır. Buradan Γ^2 grubunun elemanları $a, b, c, d \in \mathbb{Z}$ olmak üzere, $\begin{pmatrix} 2a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & 2b \\ 2c & d \end{pmatrix}, \begin{pmatrix} a & b \\ c & 2d \end{pmatrix}$ matris gösterimlerinden birine sahiptir.

1.7. Γ^3 Modüler Alt Grubu

Γ^3 ile Γ modüler grubunun elemanlarının küplerinin ürettiği grubu göstereceğiz. [17] den görüleceği gibi $\Gamma^3 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma: ab + cd \equiv 0 \ mod 3\right\}$ şeklinde gösterilir. Buradan kolaylıkla Γ^3 grubunun elemanları $a, b, c, d \in \mathbb{Z}$ olmak üzere, $\begin{pmatrix} 3a & b \\ c & 3d \end{pmatrix}, \begin{pmatrix} a & 3b \\ 3c & d \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ matris gösterimlerinden birine sahiptir. İlk iki tip gösterime sahip elemanların Γ^3 te olacağı aşikardır. Üçüncü tip elemanlara gelince

$a, b, c, d \not\equiv 0\ (mod 3)$ olmak üzere $ad - bc = 1$ koşulunu gerçekleyen elemanlardır, yani;

$a, b, c, d \not\equiv 0\ (mod 3)$ olmak üzere $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^3$ ancak ve ancak $T \in \Gamma$ dır.

1.8. Hecke Grupları

$T: z \longrightarrow -\frac{1}{z}$ ve $U(z) = z + \lambda, (\lambda \in \mathbb{R})$ elemanları ile üretilen $PSL(2, \mathbb{R})$ nin alt gruplarının ayrık olması durumu özel bir önem taşır. Bu durumda karşımıza "λ nın hangi değerleri için bu gruplar ayrık olur? " sorusu çıkmaktadır. λ nın $\lambda = \lambda_q = 2cos\frac{\pi}{q}, q \geq 3$ değerleri için yukarıda verilen grupların ayrık olduğu Hecke tarafından gösterilmiştir.

Tanım 1.8.1.[14] Yukarıda tanımlanan ve ayrık oldukları Hecke tarafından verilmiş gruplara özel olarak Hecke grupları denir ve $\lambda = \lambda_q = 2cos\frac{\pi}{q}$ değerine karşılık gelen Hecke grubunu G_q ile gösterelim. T ve U dönüşümlerinin $PSL(2, \mathbb{R})$ deki matris gösterimlerini kullanırsak,

$$G_q = \langle T, U \rangle = \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix} \rangle$$

dir. $q = 3$ olması durumunda $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ olur. Bu durumda G_3 Hecke grubu, Γ modular grubu olarak karşımıza çıkar. Herhangi bir G_q Hecke grubu için

$$S \coloneqq TU = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & \lambda_q \end{pmatrix}$$

tanımlansın. Bu durumda

$$G_q = \langle T, U \rangle = \langle T, S \rangle$$

olur. G_q Hecke grupları T ve S ile üretilen devirli grupların serbest çarpımıdır. Dolayısıyla

$$G_q = \langle T, S\rangle \cong \mathbb{Z}_2 * \mathbb{Z}_q$$

dur.

G_q nun kongrüans alt gruplarını aşağıdaki gibi tanımlayabiliriz: β, $\mathbb{Z}[\lambda]$ nın bir ideali olmak üzere

$$G_0(\beta) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_q : c \in \beta\right\}, G^0(\beta) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_q : b \in \beta\right\},$$

$$G^1(\beta) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_q : a-1, c, d-1 \in \beta\right\},$$

$$G(\beta) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_q : a-1, b, c, d-1 \in \beta\right\}$$

dır. Hecke gruplarıyla çalışmanın başlıca güçlüklerinden biri

$$PSL_2(\mathbb{Z}[\lambda]) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1, a, b, c, d \in \mathbb{Z}[\lambda]\right\}$$

nın herhangi bir elemanının G_q Hecke grubuna ait olup olmadığına karar vermekteki zorluktur. Gerçekten Γ dan başka sadece G_4 ve G_6 Hecke gruplarının elemanları aşağıdaki matrislerden oluşmaktadır: G_4 ün elemanları

$$\left\{\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix} : ad - 2bc = 1\right\} \text{ ve } \left\{\begin{pmatrix} a\sqrt{2} & b \\ c & d\sqrt{2} \end{pmatrix} : 2ad - bc = 1\right\},$$

G_6 nın elemanları

$$\left\{\begin{pmatrix} a & b\sqrt{3} \\ c\sqrt{3} & d \end{pmatrix} : ad - 3bc = 1\right\} \text{ ve } \left\{\begin{pmatrix} a\sqrt{3} & b \\ c & d\sqrt{3} \end{pmatrix} : 3ad - bc = 1\right\}$$

şeklindedir. G_4 ve G_6 nın bu iki tip elamanlarına sırasıyla çift ve tek elemanlar denir.

Peki G_5 in elemanları nelerdir? Bu problemi çözmek için 1952 yılında David Rosen, doktora tezinde, sürekli kesirlerin yeni bir çeşidi olan λ_q kesirlerini ortaya atmıştır. λ_q kesirleri nelerdir? λ_q kesirleri

$$r_0\lambda + \frac{\varepsilon_1}{r_1\lambda + \frac{\varepsilon_2}{r_2\lambda + \frac{\varepsilon_3}{\ddots}}} =: [r_0; \varepsilon_1 : r_1\lambda, \varepsilon_2 : r_2\lambda, \dots]$$

şeklindeki sürekli kesirlerdir. Burada, genellikle, sabit bir q için $\lambda = 2Cos\frac{\pi}{q}, q \geq 3, \varepsilon_i = \pm 1$ ve $r_i \in \mathbb{Z}^+, i \geq 1, r_0 \in \mathbb{Z}$ dir. Bu sürekli kesir bir "en yakın tamsayı algortiması" ile geliştirilmiştir. Eğer ξ bir reel sayı ise biz ξ ye en yakın λ nın bir tamsayı katını araştırıyoruz. Yani, eğer "{ }" en yakın tamsayıyı gösteriyorsa bu taktirde $\left\{\frac{\xi}{\lambda}\right\} = r_0$ yazacağız. Burada $-\frac{1}{2} \leq r_0 - \frac{\xi}{\lambda} < \frac{1}{2}$ yani r_0 eşitsizlikte tek türlü belirlenir.

$$r_0\lambda - \frac{\lambda}{2} < \xi \leq r_0\lambda + \frac{\lambda}{2} \qquad (1)$$

Böylece $\xi = r_0\lambda + \frac{\varepsilon_1}{\xi_1}$ dir. Burada eğer $r_0\lambda < \xi$ ise $\varepsilon_1 > 0$ ve $r_0\lambda > \xi$ ise $\varepsilon_1 < 0$ olduğundan $\xi_1 = \frac{\varepsilon_1}{\xi - r_0\lambda} > 0$ olduğu görülür. Eğer $\xi = n\lambda + \frac{\lambda}{2} = (n+1)\lambda - \frac{\lambda}{2}$ ise bu taktirde (1) eşitsizliğinden $r_0 = n$ ve $\varepsilon_1 = 1$ dir. Bu taktirde $r_0\lambda - \frac{\lambda}{2} < \xi \leq r_0\lambda + \frac{\lambda}{2}$ ifadesi $\xi_1 \geq \frac{2}{\lambda} > 1 > \frac{\lambda}{2}$ olduğunu vurgular ve böylece $r_1 = \left\{\frac{\xi_1}{\lambda}\right\} \geq 1$. Bu şekilde devam edersek $\xi_m > \frac{\lambda}{2}$ olduğunu buluruz ki bu $r_m \geq 1$ $(m \geq 1)$ olduğunu vurgular [22].

Bundan sonra λ kesri λ_5 kesrini gösterecektir. Şimdi λ kesrine bir örnek verelim.

Örnek 1.8.2. $1 \in \mathbb{Z}$ nin λ kesirlerine ayrılmış şeklinin $\lambda - \frac{1}{\lambda}$ olduğunu gösterelim.

En yakın tamsayı algoritmasını uygulayalım. $\xi = 1$ olsun. ξ ye en yakın λ nın bir tam sayı katını araştıracağız. Bu tamsayı r_0 olsun. Bu taktirde

$$r_0 = \left\{\frac{\xi}{\lambda}\right\} = \left\{\frac{1}{\lambda}\right\} = \left\{\frac{1}{1.618}\right\} = \{0{,}618\} = 1$$

dir. $r_0\lambda = \lambda = 1{,}618 > \xi = 1$ olduğundan $\varepsilon_1 = -1$ dir. Böylece $\xi = r_0\lambda + \frac{\varepsilon_1}{\xi_1}, \xi_1 = \frac{\varepsilon_1}{\xi - r_0\lambda}$ eşitliklerinden

$$\xi = \lambda - \frac{1}{\xi_1},\ \xi_1 = \frac{-1}{1-\lambda}$$

elde edilir. Şimdi ξ_1 e en yakın tamsayı algoritmasını uygulayalım. λ nın ξ_1 e en yakın tamsayı katı r_1 olsun. Bu taktirde

$$r_1 = \left\{\frac{\xi_1}{\lambda}\right\} = \left\{\frac{-1}{\lambda - \lambda - 1}\right\} = 1$$

dir. Burada $\lambda^2 = \lambda + 1$ olduğuna dikkat edelim. $r_1\lambda = \lambda = 1{,}61803 < \xi_1 = \frac{-1}{1-\lambda} = \frac{1}{0.618} =$ $1{,}61812$ olduğundan $\varepsilon_2 = 1$ dir. Böylece

$$\xi_1 = \lambda + \frac{1}{\xi_2},\ \xi_2 = \frac{1}{\frac{-1}{1-\lambda} - \lambda} = \frac{1}{\frac{-1-\lambda+\lambda+1}{1-\lambda}} = \frac{1}{0} = \infty$$

olup $\xi_1 = \lambda + \frac{1}{\infty} = \lambda$ bulunur. Buradan $\xi = \lambda - \frac{1}{\lambda}$ dir. Yani 1 in λ-kesirlerine ayrılmış şekli $\lambda - \frac{1}{\lambda}$ dır.■

λ-kesirlerine ayırma işlemi her zaman çok kolay değildir. Bunu aşağıdaki örnekte görebiliriz.

Örnek 1.8.3. $\frac{3+7\lambda}{5-2\lambda}$ ifadesini λ kesirlerine ayıralım.

En yakın tamsayı algoritmasını kullanacağız. $\xi = \frac{3+7\lambda}{5-2\lambda}$ olsun. Buna göre λ nın ξ ye en yakın bir tamsayı katını araştıracağız. Bu tamsayı r_0 olsun. Bu taktirde

$$r_0 = \left\{\frac{\xi}{\lambda}\right\} = \left\{\frac{\frac{3+7\lambda}{5-2\lambda}}{\lambda}\right\} = \left\{\frac{3+7\lambda}{5\lambda-2\lambda-2}\right\} = \left\{\frac{3+7\lambda}{3\lambda-2}\right\} = \left\{\frac{14{,}632}{2{,}854}\right\} = \{5{,}127\} = 5$$

dir. $r_0\lambda = 5\lambda = 8{,}09 < \xi = \frac{3+7\lambda}{5-2\lambda} = 8{,}294$ olduğundan $\varepsilon_1 = 1$ dir. Böylece $\xi = r_0\lambda + \frac{\varepsilon_1}{\xi_1}, \xi_1 = \frac{\varepsilon_1}{\xi - r_0\lambda}$ eşitliklerinden

$$\xi = 5\lambda + \frac{1}{\xi_1},\ \xi_1 = \frac{1}{\frac{3+7\lambda}{5-2\lambda} - 5\lambda} = \frac{5-2\lambda}{3+7\lambda-25\lambda+10\lambda+10} = \frac{5-2\lambda}{13-8\lambda}$$

bulunur. Şimdi ξ_1 e en yakın tamsayı algoritmasını uygulayalım.

$$r_1 = \left\{\frac{\xi_1}{\lambda}\right\} = \left\{\frac{5-2\lambda}{13\lambda-8\lambda-8}\right\} = \left\{\frac{5-2\lambda}{5\lambda-8}\right\} = \left\{\frac{1{,}764}{0{,}089}\right\} = \{19{,}820\} = 20$$

dir. $r_1\lambda = 20\lambda = 32{,}36 > \xi_1 = \frac{5-2\lambda}{13-8\lambda} = 31{,}5$ olduğundan $\varepsilon_2 = -1$ dir. Böylece

$$\xi_1 = 20\lambda - \frac{1}{\xi_2},\ \ \xi_2 = \frac{-1}{\frac{5-2\lambda}{13-8\lambda} - 20\lambda} = \frac{8\lambda-13}{5-2\lambda-260\lambda+160\lambda+160} = \frac{8\lambda-13}{-102\lambda+165}$$

elde edilir. Buna göre

$$\xi = 5\lambda + \cfrac{1}{20\lambda - \cfrac{1}{\xi_2}}$$

dir. Şimdi ξ_2 ye en yakın tamsayı algoritmasını uygulayalım.

$$r_2 = \left\{\frac{\xi_2}{\lambda}\right\} = \left\{\frac{8\lambda - 13}{-102\lambda - 102 + 165\lambda}\right\} = \left\{\frac{8\lambda - 13}{63\lambda - 102}\right\} = \left\{\frac{-0{,}056}{-0{,}065}\right\} = \{0{,}861\} = 1$$

olup $r_2\lambda = \lambda = 1{,}618 > \xi_2 = \frac{8\lambda-13}{-102\lambda+165} = \frac{-0{,}056}{-0{,}036} = 1{,}55$ olduğundan $\varepsilon_3 = -1$ dir. Böylece

$$\xi_2 = \lambda - \frac{1}{\xi_3}, \xi_3 = \cfrac{-1}{\cfrac{8\lambda - 13}{-102\lambda + 165} - \lambda} = \frac{102\lambda - 165}{8\lambda - 13 + 102\lambda + 102 - 165\lambda} = \frac{102\lambda - 165}{-55\lambda + 89}$$

elde edilir. Buna göre

$$\xi = 5\lambda + \cfrac{1}{20\lambda - \cfrac{1}{\lambda - \cfrac{1}{\xi_3}}}$$

bulunur. Şimdi ξ_3 ye en yakın tamsayı algoritmasını uygulayalım.

$$r_3 = \left\{\frac{\xi_3}{\lambda}\right\} = \left\{\frac{102\lambda - 165}{-55\lambda - 55 + 89\lambda}\right\} = \left\{\frac{102\lambda - 165}{34\lambda - 55}\right\} = \left\{\frac{0{,}036}{0{,}012}\right\} = 3$$

olup $r_3\lambda = 3\lambda = 4{,}854 > \xi_3 = \frac{102\lambda-165}{-55\lambda+89} = \frac{0{,}036}{0{,}009} = 4$ olduğundan $\varepsilon_4 = -1$ dir. Böylece

$$\xi_3 = 3\lambda - \frac{1}{\xi_4}, \xi_4 = \cfrac{-1}{\cfrac{102\lambda - 165}{-55\lambda + 89} - 3\lambda} = \cfrac{-1}{\cfrac{102\lambda - 165 + 165\lambda + 165 - 267\lambda}{-55\lambda + 89}} = \frac{-1}{0} = \infty$$

olup $\xi_3 = 3\lambda - \frac{1}{\infty} = 3\lambda$ bulunur. Böylece ξ nin λ kesirlerine ayrılmış şekli

$$\frac{3 + 7\lambda}{5 - 2\lambda} = 5\lambda + \cfrac{1}{20\lambda - \cfrac{1}{\lambda - \cfrac{1}{3\lambda}}}$$

dır. ■

Teorem 1.8.4.[22] Her reel sayı bir tek λ kesir gösterimine sahiptir. ■

G_5 Hecke grubunun elamanlarını belirlemek için aşağıdaki teorem yardımcı olabilir.

Teorem 1.8.5.[21] $\mathrm{V} = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix}$, $\mathrm{ad} - \mathrm{bc} = 1, \mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d} \in \mathbb{Z}[\lambda]$ olsun. $V \in \mathrm{G}_5 \Leftrightarrow$

i. $\frac{b}{d} = r_0\lambda + \cdots + \frac{\varepsilon_n}{r_n\lambda} = \frac{P_n}{Q_n}, \frac{a}{c} = \frac{P_{n-1}}{Q_{n-1}},$ (3)

ii. $\frac{a}{c} = r_0\lambda + \cdots + \frac{\varepsilon_n}{r_n\lambda} + \frac{\varepsilon_{n+1}}{r_{n+1}\lambda} = \frac{P_{n+1}}{Q_{n+1}}, \frac{b}{d} = \frac{P_n}{Q_n},$ (4)

Eğer $i)$ sağlanıyor ise $V = \begin{pmatrix} vP_{n-1} & P_n \\ vQ_{n-1} & Q_n \end{pmatrix}$, $ii)$ sağlanıyor ise $V = \begin{pmatrix} vP_{n+1} & P_n \\ vQ_{n+1} & Q_n \end{pmatrix}$ şeklindedir. Burada $v = \pm 1,\ detV = 1$ olacak şekilde seçilir.■

Teorem 1.8.6.[21] $\mathrm{V} = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix}$, $\mathrm{ad} - \mathrm{bc} = 1, \mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d} \in \mathbb{Z}[\lambda_q]$ olsun ve $\frac{b}{d}$ nin sonlu bir λ_q-kesir gösterimine sahip olduğunu varsayalım. Bu taktirde $V \in \mathrm{G_q} \Leftrightarrow V, (3)$ veya (4) şeklindedir. ■

Örnek 1.8.7.[21] $V = \begin{pmatrix} -(9\lambda + 4) & 35\lambda + 24 \\ -(2\lambda + 3) & 13\lambda + 6 \end{pmatrix}$ olsun. $R = \frac{35\lambda+24}{13\lambda+6}$ yı en yakın tamsayı algoritmasını kullanarak λ-kesirleri cinsinden yazarsak $R = 2\lambda - \cfrac{1}{2\lambda + \cfrac{1}{\lambda - \cfrac{1}{3\lambda}}}$ elde edilir.

Buradan $P_3 = 35\lambda + 24$ ve $Q_3 = 13\lambda + 6$ bulunur. Böylece b ve d Teorem 1.8.6. yı sağlar. Sondan bir önceki yakınsaklık $2\lambda - \cfrac{1}{2\lambda + \frac{1}{\lambda}} = \frac{9\lambda+4}{2\lambda+3}$ dür. Teorem 18.6. nın şartlarını sağlamak için $a = -(9\lambda + 4) = -P_2,\ c = -(2\lambda + 3) = -Q_2$ seçilebilir. Buna göre V, (3) şeklinde olduğundan $V \in \mathrm{G}_5$ dir.

Örnek 1.8.8.[21] $A = \begin{pmatrix} -(22\lambda + 13) & 11\lambda + 13 \\ -(7\lambda + 5) & 7\lambda - 1 \end{pmatrix}$, $detA = 1$ olup (3) veya (4) şeklinde olmadığından $A \notin G_5$ dir.

1.9. İndirgenmiş Form

Tanım 1.9.1.[15] $x,\ G_5$ in bir cusp noktası, yani $x \in \widehat{\mathbb{Q}}(\lambda)$ olsun. Eğer

i. $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G_5$ olacak şekilde $c, d \in \mathbb{Z}[\lambda]$ vardır,

ii. $b \geq 0$,

iii. $x = \infty$ ise, indirgenmiş form $-\frac{1}{0}$ veya $\frac{1}{0}$ dır,

şartları sağlanıyorsa $x = \frac{a}{b}$ ye bir indirgenmiş form adı verilir. Eğer ∞, sıralanmış cusp noktalarının solunda ise indirgenmiş form $-\frac{1}{0}$, sağında ise $\frac{1}{0}$ olarak alınır.

Açıkça $(a, b) = 1$ dir. Buradan eğer $(a', b') = 1$ olmak üzere $x = \frac{a'}{b'}$ ise bu taktirde, μ , $\mathbb{Z}[\lambda]$ da bir birim olmak üzere $a = \mu a', b = \mu b'$ dür.

İndirgenmiş form, genelde, oldukça karmaşık olabilir. Örneğin 1 ve $\frac{21}{34}$ ün indirgenmiş formları sırasıyla

$$\frac{\lambda}{\lambda} \quad \text{ve} \quad \frac{193776765+313537392\lambda}{313733810+507631968\lambda} = \frac{21\lambda^{36}}{34\lambda^{36}}$$

dır.

Lemma 1.9.2.[15] Bir $x \neq \infty$ cusp noktasının indirgenmiş formu tektir. ■

Sonuç 1.9.3.[15] Eğer $\frac{a_1}{b_1}$ ve $\frac{a_2}{b_2}$, $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ olan iki indirgenmiş form ise bu taktirde $a_1 = a_2$ ve $b_1 = b_2$ dir. ■

Lemma 1.9.4.[15] $\frac{a}{b} > 0$ $(b > 0)$ bir indirgenmiş form olsun. Bu taktirde $b \in \mathbb{N} \Leftrightarrow b = 1$ dir. ■

Sonuç 1.9.5.[15] Eğer $x \neq \infty$ bir cusp noktası ve $x = \frac{a}{b}$ indirgenmiş formda ise bu taktirde $b = 1 \Leftrightarrow$ bir $m \in \mathbb{Z}$ için $x = m\lambda$ dır. ■

Bu sonuca göre $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G_5 \Leftrightarrow b = m\lambda, m \in \mathbb{Z}$ ve benzer şekilde $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in G_5 \Leftrightarrow c = n\lambda,\ n \in \mathbb{Z}$ dir.

Tanım 1.9.6. Eğer (x_i, x_j) bir çift doğru (even line) ise bu taktirde

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = x_i,\ \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = x_j$$

olacak şekilde bir $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G_5$ vardır $(b \neq 0,\ d \neq 0)$.

Lemma 1.9.7.[15] Varsayalım ki $x_i = \frac{a_i}{b_i}$ ve $x_j = \frac{a_j}{b_j}$ indirgenmiş formda olmak üzere $x_i, x_j \in \mathbb{Q}[\lambda]$ ve $x_i < x_j$ dir. Bu taktirde aşağıdaki ifadeler birbirine eşittir:

i. $\begin{pmatrix} a_j & a_i \\ b_j & b_i \end{pmatrix} \in G_q$

ii. (x_i, x_j) bir çift doğrudur.

iii. $a_j b_i - a_i b_j = 1$ dir.

1.10. Cebirsel Sayı Cisimleri

Tanım 1.10.1.[4] Sıfır bölensiz, birimli, değişmeli halkaya bir tamlık bölgesi denir.

Örnek 1.10.2. m tam kare olmayan bir tam sayı olsun. Bu taktirde $\mathbb{Z} + \mathbb{Z}\sqrt{m} \coloneqq \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$ kümesi bir tamlık bölgesidir. Burada $\sqrt{m}$ sayısı $x^2 - m = 0$ denkleminin bir köküdür. Dolayısıyla $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ ye "Kuadratik Bölge" denir.

Örnek 1.10.3. F bir cisim olsun. $F[x] \coloneqq \{p(x)\ polinomu : katsayıları\ F\ de\}$ kümesi bir tamlık bölgesidir.

Tanım 1.10.5.[4] D bir tamlık bölgesi, $a \in D$ olsun. $a|1$ ise a ya D tamlık bölgesinin "birimi" (unit) adı verilir. D nin birimlerinin kümesini $U(D)$ ile göstereceğiz.

Tanım 1.10.6.[4] D bir tamlık bölgesi, $I \subset D$ olsun. Bu taktirde

i. $\forall a, b \in I$ için $a + b \in I$ ve

ii. $\forall a \in I$ ve $\forall r \in D$ için $ra \in I$

ise I ya D nin bir ideali adı verilir.

Tanım 1.10.7.[4] D bir tamlık bölgesi ve $a \in D$ olsun. $\langle a \rangle = \{ra : r \in D\}$ idealine bir Esas ideal denir. Buna göre $\langle 0 \rangle = \{0\}$ ve $\langle 1 \rangle = D$ esas ideallerdir.

Tanım 1.10.8.[4] D tamlık bölgesine bir esas ideal bölgesi adı verilir $\Leftrightarrow$ D nin her ideali esas idealdir.

Teorem 1.10.9.[4] $\mathbb{Z}[\lambda]$ bir esas ideal bölgesidir. Burada $\lambda = \frac{1+\sqrt{5}}{2}$ dir. ■

Teorem 1.10.10.[4] D bir tamlık bölgesi, $P \subset D$ bir öz ideal olsun. P asal idealdir $\Leftrightarrow$ $ab \in P$ ise $a \in P$ veya $b \in P$ dir.

Örnek 1.10.11. $I =< x^2 + 1 >$ ideali $\mathbb{C}[x]$ te bir asal ideal değildir. Çünkü $x \mp i \in \mathbb{C}[x]$, $(x+i)(x-i) = x^2 + 1 \in I$ fakat $x \mp i \notin I$.

Tanım 1.10.12.[4] A ve B, $A \subset B$ olan tamlık bölgeleri olsun. $b \in B$ elemanına A üzerinde "tam"dır denir:$\Leftrightarrow$ $a_0, a_1, \dots, a_{n-1} \in A$ olmak üzere b elemanı bir

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

monik polinom denklemini sağlar.

Her $a \in A$ elemanı A üzerinde tamdır. Çünkü a, $x - a \in A[x]$ in bir köküdür.

Tanım 1.10.13.[4] $\mathbb{Z}$ üzerinde tam olan bir kompleks sayıya bir cebirsel tamsayı denir.

Tanım 1.10.14.[4] A ve B, $A \subset B$ olan tamlık bölgeleri olsun. Farz edelim ki A bir cisim ve $b \in B$ de A üzerinde tamdır. Bu taktirde b ye A cismi üzerinde cebirsel denir.

Tanım 1.10.15.[4] $\mathbb{Q}$ üzerinde cebirsel olan bir kompleks sayıya cebirsel sayı denir.

Teorem 1.10.16.[4] Tüm cebirsel tamsayıların kümesi bir tamlık bölgesidir. ■

Tanım 1.10.17.[9] G bir grup ve $H < G$ olsun.

$$N_G(H) \coloneqq \{g \in G | gH = Hg\}$$

kümesine H nin G deki normalliyeni denir.

1.11. Bir Kuadratik Cisim Üzerindeki Cebirsel Tamsayılar

Burada, bir $x^2 + ax + b \in \mathbb{Q}[x]$ indirgenemez kuadratik polinomunun bir $\alpha \in \mathbb{C}$ kökü ile $\mathbb{Q}$ nun birleşmesinden elde edilen $\mathbb{Q}(\alpha)$ cismindeki cebirsel tamsayıları belirleyeceğiz. Yani $\mathbb{Q}(\alpha)$, $\mathbb{C}$ nin $\mathbb{Q}$ ve α yı içeren en küçük cismidir. $x^2 + ax + b, \mathbb{Q}[x]$ de indirgenemez olduğundan $\alpha \notin \mathbb{Q}$ olduğuna dikkat edelim. $\alpha^2 + a\alpha + b = 0$ olmak üzere

$$\mathbb{Q}(\alpha) = \{x + y\alpha | x, y \in \mathbb{Q}\}$$

cismine bir “kuadratik cisim” veya “$\mathbb{Q}$ nun bir kuadratik genişlemesi” denir.

Teorem 1.11.1.[4] K bir kuadratik cisim olsun. Bu taktirde $K = \mathbb{Q}(\sqrt{m})$ olacak şekilde bir tek karesiz m tamsayısı vardır. ■

Şimdi m karesiz bir tamsayı olmak üzere $K = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ kuadratik cismindeki cebirsel tamsayıları belirleyeceğiz. K daki cebirsel tamsayıların kümesi “O_K” ile gösterilir.

Teorem 1.11.2 [4]. K kuadratik bir cisim ve m, $K = \mathbb{Q}(\sqrt{m})$ olacak şekilde birtek karesiz tamsayı olsun. Bu taktirde K daki cebirsel tamsayıların O_K kümesi

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m} & , \text{eğer } m \not\equiv 1(mod4) \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) & , \text{ eğer } m \equiv 1(mod4) \end{cases}$$

dir. ■

1.12. Bir Kuadratik Elemanın Normu ve İzi

Tanım 1.12.1.[4] Eğer K bir kuadratik cisim ise bu taktirde bir m karesiz tam sayısı için $K = \mathbb{Q}(\sqrt{m})$ dir. $\alpha \in K$ olsun. Bu taktirde $\exists\ r, s \in \mathbb{Q}$ için $\alpha = r + s\sqrt{m}$ dir.

α’ nın izi:

$$tr(\alpha) = \alpha + \alpha' = 2r$$

ve α’ nın normu:

$$N(\alpha) = \alpha\alpha' = r^2 - s^2m$$

dir. Eğer $\alpha \in O_K$ ise bu taktirde $tr(\alpha) \in \mathbb{Z}$ ve $N(\alpha) \in \mathbb{Z}$ dir.

Teorem 1.12.2.[4] K n. dereceden bir cebirsel sayı cismi ve $\alpha, \beta \in K$ olsun. Bu taktirde

$$tr(\alpha + \beta) = tr(\alpha) + tr(\beta) \text{ ve } N(\alpha\beta) = N(\alpha)N(\beta)$$

dır. ■

Aşağıdaki teorem bir birimin normu hakkındadır.

Teorem 1.12.3.[4] K n. dereceden bir cebirsel sayı cismi olsun.

i. Eğer α, O_K nın bir birimi ise bu taktirde $N(\alpha) = \pm 1$ dir.

ii. Eğer $\alpha \in O_K$ ve $N(\alpha) = \pm 1$ ise bu taktirde α, O_K nın bir birimidir. ∎

Teorem 1.12.4.[4] K bir cebirsel sayı cismi olsun. Eğer $\alpha \in O_K$, p bir rasyonel asal sayı ve $N(\alpha) = \pm p$ ise bu taktirde α indirgenemezdir. ∎

Teorem 1.12.5.[4] K, n. dereceden bir cebirsel sayı cismi, O_K , K nın tamsayılar halkası ve $\alpha \in O_K$ olsun. Bu taktirde $N(\langle\alpha\rangle) = |N(\alpha)|$ dır. ∎

Aşağıdaki teoremde $\langle\alpha\rangle$ esas idelinin normunu α nın $\mathbb{Q}$ üzerindeki minimal polinomunun sabit terimi cinsinden belirleyeceğiz.

Teorem 1.12.6.[4] K, n. dereceden bir cebirsel sayı cismi, $\alpha \in K$ ve $irr_{\mathbb{Q}}(\alpha) = x^m + b_{m-1}x^{m-1} + \cdots + b_0 \in \mathbb{Q}[x]$ olsun. Bu taktirde $N(\langle\alpha\rangle) = |b_0|^{n/m}$ dir. ∎

2. YAPILAN ÇALIŞMALAR

2.1. H^q nun Kongrüans Alt Grupları

Modüler grubun esas kongrüans alt gruplarının tanımlarına benzer şekilde, $\mathbb{Z}[\lambda_q]$ nun herhangi bir I ideali için $G \coloneqq PSL(2, \mathbb{Z}[\lambda_q])$ nin esas kongrüans altgruplarını tanımlayabiliriz.

Tanım 2.1.1.[8] $G(I) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G: a-1, b, c, d-1 \in I\right\}$ alt grubuna G nin I ya karşılık gelen esas kongrüans alt grubu adı verilir. Benzer şekilde I idealine karşılık gelen özel kongrüans alt grupları,

$$G_1(I) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G: a-1, c, d-1 \in I\right\}$$

ve

$$G_0(I) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G: c \in I\right\}$$

olarak tanımlanır.

Yukarıda verilen kongrüans alt grubu tanımlarından

$$G(I) \leq G_1(I) \leq G_0(I) \leq G$$

olduğu açıktır. Diğer yandan $G(I) \trianglelefteq G$ ve $G_1(I) \trianglelefteq G_0(I)$ dır.

Teorem 2.1.2.[8] P ler I nın farklı asal bölenleri olmak üzere,

i. [G:G(I)] = $N(I)^3 \prod_{P|I}(1 - \frac{1}{N(P)^2})$

ii. [G:G_1(I)] = $N(I)^2 \prod_{P|I}(1 - \frac{1}{N(P)^2})$

iii. [G:G_0(I)] = $N(I) \prod_{P|I}\left(1 + \frac{1}{N(P)}\right)$

dir. ■

Tanım 2.1.3.[8] H, G nin herhangi bir alt grubu ve $I, \mathbb{Z}[\lambda_q]$ nin bir ideali olsun. Bu durumda,

$$H(I) \coloneqq G(I) \cap H$$

$$H_1(I) \coloneqq G_1(I) \cap H$$

$$H_0(I) \coloneqq G_0(I) \cap H$$

alt gruplarına, H nın özel kongrüans alt grupları denir. Bu tanımda $H = H^q$ alınırsa, H^q nun özel kongrüans alt grupları,

$$H^q(I) \coloneqq G(I) \cap H^q$$

$$H_1^q(I) \coloneqq G_1(I) \cap H^q$$

$$H_0^q(I) \coloneqq G_0(I) \cap H^q$$

olur. Dolayısıyla $H^q(I) \leq H_1^q(I) \leq H_0^q(I) \leq H^q$, $H^q(I) \trianglelefteq H^q$ ve $H_1^q(I) \trianglelefteq H_0^q(I)$ dir.

2.2. H^q nun Özel Kongrüans Alt Gruplarının Yansınıfları

$A, B \in H^q$ ve $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ olsun.

Önerme 2.2.1.[8] $I, \mathbb{Z}[\lambda_q]$ nun bir ideali olsun. Bu takdirde,

- **i.** A, B matrisleri $H_0^q(I)$ nın aynı yansınıfındadır $\Leftrightarrow ac' - ca' \equiv 0 \ mod \ I,$
- **ii.** A, B matrisleri $H_1^q(I)$ nın aynı yansınıfındadır $\Leftrightarrow a \equiv a' \ mod \ I, c \equiv c' mod \ I, a \equiv -a' mod \ I, c \equiv -c' mod \ I,$
- **iii.** A, B matrisleri $H^q(I)$ nın aynı yansınıfındadır $\Leftrightarrow a \equiv a' \ mod \ I, b \equiv b' mod \ I \ c \equiv c' mod \ I, d \equiv d' mod \ I$ veya $a \equiv -a' \ mod \ I, b \equiv -b' mod \ I \ c \equiv -c' mod \ I, d \equiv -d' mod \ I$

2.3. $H_0^5(I)$ nın H^5 teki Normalliyeni

Lemma 2.3.1.[25] $I = (2) = 2\mathbb{Z}[\lambda]$ ve $A \in H^5$ olsun. Bu takdirde

$$A \in H_0^5(I) \Leftrightarrow A \equiv \pm \begin{pmatrix} 1 & r\lambda \\ 0 & 1 \end{pmatrix} mod \ I, \qquad r = 0{,}1.$$

Teorem 2.3.2. $I', \mathbb{Z}[\lambda_q]$ nun bir karesiz ideali olmak üzere $(2, I') = 1$ ve $I = (2)^\alpha I'$ olsun. Bu takdirde,

$$N_{\boldsymbol{H}^5}\left(H_0^5(I)\right) = H_0^5\left((2)^{\alpha'} I'\right), \qquad \alpha' = \alpha - min\left\{2, \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right\}$$

dir.

İspat: $X = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in N_{\boldsymbol{H}^5}\left(H_0^5(I)\right)$ keyfi bir matris olsun. Bu takdirde her $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_0^5(I)$ için, normalliyen tanımından,

$$A = \begin{pmatrix} x & z \\ y & t \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & z \\ y & t \end{pmatrix}^{-1} \in H_0^5(I)$$

dir. Yukarıdaki matris çarpımı yapılırsa ,

$$A = \begin{pmatrix} axt - bxy + czt - dzy & * \\ ayt - by^2 + ct^2 - dty & * \end{pmatrix} \in H_0^5(I)$$

olur. $H_0^5(I)$ nın tanımından

$$c \equiv 0 \; mod \; I$$

$$ayt - by^2 + ct^2 - dty \equiv 0 \; mod \; I$$

olduğundan

$$ayt - by^2 - dty \equiv 0 \; mod \; I$$

dır. Diğer yandan

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

olarak alırsak yukarıdaki denklik bağıntısı

$$\lambda y^2 \equiv 0 \; mod \; I$$

olur ve $(-1 + \lambda)\lambda = 1$ olduğundan

$$y^2 \equiv 0 \; mod \; I$$

elde ederiz. Son ifadeyi $ayt - by^2 - dty \equiv 0 \; mod \; I$ kongrüans denkleminde yerine yazarsak

$$(a - d)ty \equiv 0 \; mod \; I$$

olur. Bu takdirde her $x \in \mathbb{Z}[\lambda]$ için, yukarıdaki ifade

$$(a-d)xty \equiv 0 \ mod \ I$$

olur. Ayrıca, $|X| = xt - yz = 1$ olduğundan xt yerine $1 + yz$ yazılırsa

$$(a-d)y \equiv 0 \ mod \ I$$

elde edilmiş olur. Diğer yandan $\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right| = ad - bc = 1$ ve $c \equiv 0 \ mod \ I$ olduğundan

$$ad \equiv 1 \ mod \ I$$

olur. Sondan bir önceki denklem a ile çarpılırsa

$$(a^2 - 1)y \equiv 0 \ mod \ I$$

elde ederiz. Ayrıca $I \subseteq (2)^{\alpha} I' \subseteq (2)^{\alpha} \cap I' \subset (2) \cap I'$, $\alpha \geq 1$, $I = (2)^{\alpha} I'$ ve $y^2 \equiv 0 \ mod \ I$ olduğundan

$$y^2 \equiv 0 \ mod \ 2^{\alpha}$$

ve

$$y^2 \equiv 0 \ mod \ I'$$

olur. Yine yukarıdaki zincirden $\alpha \geq 1$ için

$$y^2 \equiv 0 \ mod \ 2$$

dır. (2) ideali asal ideal olduğundan

$$y \equiv 0 \ mod \ 2$$

dir. Diğer yandan I' karesiz ideal olduğundan asal ideallerin çarpımı şeklinde yazılabilir. Yani $1 \leq i \leq n$ için P_i asal ideal olmak üzere $I' = P_1 P_2 \dots P_n$ dir. Böylece $y^2 \equiv 0 \ mod \ I' \Longrightarrow y^2 \in I'$ olup $y^2 = p_1 p_2 \dots p_n (k + l\lambda)$ olacak şekilde $(k + l\lambda) \in \mathbb{Z}[\lambda]$ vardır.

p_1 asal olduğundan $p_1 | y^2 \Longrightarrow p_1 | y$

p_2 asal olduğundan $p_2 | y^2 \Longrightarrow p_2 | y$

$\ddots$

p_n asal olduğundan $p_n|y^2 \Longrightarrow p_n|y$

dir ve buradan da

$$p_1p_2 \dots p_n|y \Longrightarrow y \in I' \Longrightarrow y \equiv 0 \; mod \; I'$$

olur. Öte yandan $n \in \mathbb{Z}^+$ keyfi olmak üzere

$$\dots 2^{n+1}\mathbb{Z}[\lambda] \subset 2^n\mathbb{Z}[\lambda] \subset \cdots \subset 2^2\mathbb{Z}[\lambda] \subset 2\mathbb{Z}[\lambda] \subset \mathbb{Z}[\lambda]$$

zincirini ele alalım. Burada y için bir $\alpha' \in \mathbb{N}$ sayısı

$$y \in (2)^{\alpha'} \text{ ve } y \notin (2)^{\alpha'+1}$$

olacak şekilde mevcuttur. Birinci ifadenin karesi alınırsa

$$y^2 \in (2)^{2\alpha'}$$

olur. Aynı zamanda $y^2 \in (2)^{\alpha}$ olduğundan $\alpha \leq 2\alpha'$ elde edilir.

Burada $\alpha < \alpha'$ olması durumunda $y \equiv 0 \; mod \; I'$ ve $y \equiv 0 \; mod \; 2^{\alpha'}$ olduğundan $y^2 \equiv 0 \; mod \; 2^{\alpha'}I'$ elde edilir. $\alpha < \alpha'$ olduğundan $(2)^{\alpha'} \subset (2)^{\alpha}$ dür ve böylece

$$y^2 \equiv 0 \; mod \; I$$

elde edilir.

Şimdi de $\alpha' \leq \alpha$ durumunu inceleyelim. Bu durumda $0 \leq \alpha - \alpha'$ olur. Ayrıca $\alpha \leq 2\alpha'$ olduğundan

$$\alpha \leq 2\alpha' \Longrightarrow \frac{\alpha}{2} \leq \alpha' \leq \alpha$$

elde edilir. Diğer yandan Lemma 2.3.2. den

$$\text{ya } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} mod \; 2 \text{ ya da } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} mod \; 2$$

dir. Burada her iki durum için de

$$a \equiv 1 \; mod \; 2$$

olur. Buradan da

$$a + 1 \equiv 0 \; mod \; 2 \text{ ve } a - 1 \equiv 0 \; mod 2$$

ve böylece

$$a^2 - 1 \equiv 0 \; mod \; 2^2$$

elde edilir. Ayrıca $y \in 2^{\alpha'}\mathbb{Z}[\lambda]$ olduğundan

$$(a^2 - 1)y \in 2^{\alpha'+2}\mathbb{Z}[\lambda]$$

dır. Diğer yandan $(a^2 - 1)y \equiv 0 \; mod \; I$ olduğundan

$$\alpha \leq \alpha' + 2 \Longrightarrow 0 \leq \alpha - \alpha' \leq 2$$

elde ederiz. Bu durumda α değerleri için en küçük $\alpha' \in \mathbb{N}$ sayılarını belirlemek yeterlidir.

$\alpha = 1$ için $\frac{\alpha}{2} \leq \alpha' \leq \alpha$ dan $\frac{1}{2} \leq \alpha' \Longrightarrow \alpha' \in \mathbb{Z}^+$

$0 \leq \alpha - \alpha' \leq 2$ dan $0 \leq 1 - \alpha' \leq 2 \Longrightarrow \alpha' = 1$

olur.

$\alpha = 2$ için $\frac{\alpha}{2} = 1 \leq \alpha' \Longrightarrow \alpha' \in \mathbb{Z}^+$

$0 \leq 2 - \alpha' \leq 2 \Longrightarrow \alpha' = 1, 2$

olup $\alpha' = 1$ olur.

$\alpha = 3$ için $\frac{\alpha}{2} = \frac{3}{2} \leq \alpha' \Longrightarrow \alpha' \in \mathbb{Z}^+ \setminus \{1\}$

$0 \leq 3 - \alpha' \leq 2 \Longrightarrow \alpha' = 1, 2, 3$

olup $\alpha' = 2$ dir. Bu takdirde $\alpha \in \{1,2,3\}$ için yukarıdaki çözümlerden

$$\alpha' = \begin{cases} 1 = 1 - \left[\!\left[\frac{1}{2}\right]\!\right], \alpha = 1 \\ 1 = 2 - \left[\!\left[\frac{2}{2}\right]\!\right], \alpha = 2 \\ 2 = 3 - \left[\!\left[\frac{3}{2}\right]\!\right], \alpha = 3 \end{cases}$$

olur. Şimdi de $\alpha \geq 4$ olduğu durumu inceleyelim. Bu durumda, $\alpha = \beta + 4$ olacak şekilde bir $\beta \in \mathbb{N}$ sayısı mevcuttur. Bu takdirde,

$$\alpha' \geq \frac{\alpha}{2} = \frac{\beta + 4}{2} = \frac{\beta}{2} + 2 \geq 2 \Longrightarrow \alpha' \geq 2$$

olur.

$$0 \leq \beta + 4 \leq \alpha' + 2 \Longrightarrow \beta + 2 \leq \alpha'$$

elde ederiz. Buradan her $\beta \in \mathbb{N}$ için $\alpha' = \beta + 2, \beta + 3, \beta + 4$ olabilir. Ancak yukarıdaki şartları sağlayan en küçük $\alpha' \in \mathbb{Z}^+$ sayısını alacağımızdan $\alpha' = \beta + 2$ olur. Bu durumda, $\alpha \geq 4$ için

$$\alpha' = \beta + 2 = \beta + 4 - 2 = \alpha - 2 \Longrightarrow \alpha' = \alpha - 2$$

olur. Böylece her $\alpha \in \mathbb{Z}^+$ için

$$y \equiv 0 \ mod \ 2^{\alpha'} I'$$

ve

$$N_{\boldsymbol{H}^5}\left(H_0^5(I)\right) \leq H_0^5((2)^{\alpha-2} I')$$

elde ederiz. Dolayısıyla α değerlerine karşılık gelen α' için

$$\alpha' = \alpha - min\left\{2, \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right\}$$

ve

$$N_{\boldsymbol{H}^5}\left(H_0^5((2)^{\alpha} I')\right) \leq H_0^5\left((2)^{\alpha'} I'\right)$$

olduğu görülür.

Şimdi de $\alpha' = \alpha - min\left\{2, \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right\}$ için

$$H_0^5\left((2)^{\alpha'} I'\right) \leq N_{\boldsymbol{H}^5}\left(H_0^5((2)^{\alpha} I')\right)$$

olduğunu gösterelim. Bunun için

$$X = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in H_0^5\big((2)^{\alpha'} I'\big)$$

keyfi olsun. Bu durumda

$$y \equiv 0 \; mod \; ((2)^{\alpha'} I')$$

dür. Buradan

$$y = 2^{\alpha'}(x_0 + y_0\lambda)(u + v\lambda)$$

olacak şekilde bir $u + v\lambda \in \mathbb{Z}[\lambda]$ ve $x_0 + y_0\lambda \in I'$ vardır. y nin karesi alınırsa,

$$y^2 = 2^{2\alpha'}(x_0 + y_0\lambda)^2(u + v\lambda)^2$$

olur. $\alpha \leq 2\alpha'$ olduğundan,

$$y^2 = 2^{\alpha}(x_0 + y_0)[2^{2\alpha' - \alpha}(x_0 + y_0\lambda)(u + v\lambda)^2]$$

$$\Rightarrow y^2 \in 2^{\alpha}(x_0 + y_0)\mathbb{Z}[\lambda]$$

$$\Rightarrow y^2 \equiv 0 \; mod \; (2)^{\alpha} I'$$

elde ederiz. Diğer yandan, her $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_0^5(I)$ için $a^2 - 1 \equiv 0 \; mod \; 2^2$ olduğundan

$$a^2 - 1 = 2^2(x + y\lambda)$$

olacak şekilde bir $x + y\lambda \in \mathbb{Z}[\lambda]$ mevcuttur. $y = 2^{\alpha'}(x_0 + y_0\lambda)(u + v\lambda)$ ve $a^2 - 1 = 2^2(x + y\lambda)$ taraf tarafa çarpılırsa, $\mathbb{Z}[\lambda]$ değişmeli halka olduğundan,

$$(a^2 - 1)y \equiv 2^{\alpha' + 2}(x_0 + y_0\lambda)(u + v\lambda)(x + y\lambda)$$

olur. Ayrıca $\alpha \leq \alpha' + 2$ olduğundan yukarıdaki ifadeyi

$$(a^2 - 1)y \equiv 2^{\alpha}(x_0 + y_0\lambda)[2^{\alpha' + 2 - \alpha}(u + v\lambda)(x + y\lambda)]$$

olarak yazabiliriz. Böylece

$$(a^2 - 1)y \equiv 0 \; mod \; (2)^{\alpha} I'$$

elde ederiz. Son bağıntıdan ve $y^2 \equiv 0 \; mod \; (2)^{\alpha} I'$ olmasından

$$X = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in N_{\boldsymbol{H}^5}\left(H_0^5((2)^{\alpha}I')\right)$$

elde edilmiş olur. Burada X matrisi keyfi alındığından

$$H_0^5\left((2)^{\alpha'}I'\right) \leq N_{\boldsymbol{H}^5}\left(H_0^5((2)^{\alpha}I')\right)$$

olur ve tüm bunların sonucu olarak

$$N_{\boldsymbol{H}^5}\left(H_0^5(I)\right) = H_0^5\left((2)^{\alpha'}I'\right), \qquad \alpha' = \alpha - min\left\{2, \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right\}$$

olduğu ispatlanmış olur.

Sonuç 2.3.4. $I, \mathbb{Z}[\lambda]$ nın bir karesiz ideali olmak üzere

$$N_{\boldsymbol{H}^5}\left(H_0^5(I)\right) = H_0^5(I)$$

dır.

İspat: Bir önceki teoremin ispatından $N_{\boldsymbol{H}^5}\left(H_0^5(I)\right) \leq H_0^5(I)$ olduğu kolayca görülür.

Diğer taraftan $H_0^5(I) \leq N_{\boldsymbol{H}^5}\left(H_0^5(I)\right)$ olduğunu gösterelim. Bunun için $X = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in H_0^5(I)$ alalım. Göstermemiz gereken her $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_0^5(I)$ olmak üzere $XKX^{-1} \in H_0^5(I)$ olması gerektiğidir. Bu da aşikardır. Böylece her iki durumun sonucu olarak

$$N_{\boldsymbol{H}^5}\left(H_0^5(I)\right) = H_0^5(I)$$

dır.

2.4. Bazı Kongrüans Alt Gruplarının Normalliyenleri

Bu bölümde sırasıyla Γ^2 ve Γ^3 modüler alt gruplarının kongrüans alt grupları olan $\Gamma_0^2(n)$ ve $\Gamma_0^3(n)$ nin normalliyenlerini hesaplayacağız. İlk olarak gerekli olan tanım ve teoremleri vermekle başlayalım.

Tanım 2.4.1.[8] H, X üzerinde hareket eden bir grup olsun. X in H eksenleri, aşağıdaki bağıntı altında X in trivial olmayan sabitleyenli noktalar kümesinin denklik sınıflarıdır.

$$x_1 \sim x_2 \qquad \Leftrightarrow \qquad S_{x_1} \sim S_{x_2}$$

Yani bir eksen, trivial olmayan aynı sabitleyenli tüm noktaları içeren X in bir altkümesidir.

Başka bir deyişle, eğer H nin bir elemanı X in bir elemanını sabit bırakırsa x in ekseni üzerindeki tüm noktaları sabit bırakır.

Lemma 2.4.2.[8] G bir grup ve $H \leq G$ olsun. G nin kendi üzerindeki transitif hareketi

$$g_1(g_2H) = (g_1g_2)H$$

ile H nin sol yan sınıfları üzerinde bir transitif hareket oluşturur.

G nin H yansınıfı H nin kendisidir.

Lemma 2.4.3.[8] H nin G ekseni $N(H)$ dir, yani H nin G deki normalliyenidir.

İspat: Açıkça H nin G deki sabitleyeni H nin kendisidir. Çünkü $\forall g \in G$ için $gH = H \Leftrightarrow g \in H$ dir. Gerçekten, $\forall\, g \in G$ için

$$gg_1H = g_1H \Leftrightarrow {g_1}^{-1}gg_1H = H \Leftrightarrow {g_1}^{-1}gg_1 \in H \Leftrightarrow g \in g_1H{g_1}^{-1}$$

dir. Bu yüzden g_1H, H nin G eksenidir $\Leftrightarrow g_1H{g_1}^{-1} = H$ yani $g_1 \in N(H)$.

Teorem (Dirichlet Teoremi) 2.4.4. q ve l aralarında asal tamsayılar olsun. Bu durumda $k \in \mathbb{Z}$ olmak üzere $l + kq$ formunda sayısız çoklukta asal sayı vardır. ■

Teorem (Çin Kalan Teoremi) 2.4.5. [4] $m_1,\ m_2, \dots, m_n \in \mathbb{Z}$ ve her $i \neq j$ için $(m_i, m_j) = 1$ olsun. Herhangi bir $b_1, b_2, \dots, b_n \in \mathbb{Z}$ için

$$x \equiv b_1 \ mod\ m_1$$

$$x \equiv b_2 \ mod\ m_2$$

$$\vdots$$

$$x \equiv b_n \ mod\ m_n$$

dir. Ayrıca $m = m_1\, m_2 \dots m_n$ olmak üzere, burada sözü edilen x tamsayısı m modunda tek türlü belirlidir. ■

Önerme 2.4.6. n pozitif bir tamsayı olsun. $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B=\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\in\Gamma^k$ olmak üzere A,B $\Gamma_0^k(n)$, $(k=2,3)$ nin aynı yansınıfındadır $\Leftrightarrow$ $ac'-ca'\equiv 0\ mod\ n$.

İspat: Bu önermenin ispatında aşağıda belirtilen temel grup teorinin bir sonucu kullanılacaktır.

$g_1,g_2\in G$ bir H altgrubunun aynı yansınıfındadır ancak ve ancak $g_1^{-1}g_2\in H$ dir.

Bu yüzden, A,B $\Gamma_0^k(n)$ nin aynı yansınıfındadır ancak ve ancak $A^{-1}B\in\Gamma_0^k(n)$ dir. Yani,

$$A^{-1}B=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}=\begin{pmatrix} da'-bc' & db'-bd' \\ -ca'+ac' & -cb'+ad' \end{pmatrix}\in\Gamma_0^k(n)$$

olup $ac'-ca'\equiv 0\ mod\ n$ dir.

Teorem 2.4.7. $n=2^\alpha 3^\beta n_0\geq 1,\ (n_0,6)=1$ olsun. $N_{\Gamma^2}(\Gamma_0^2(n))$, $\Gamma_0^2(n)$ nin Γ^2 deki normalliyeni olmak üzere

$$N_{\Gamma^2}(\Gamma_0^2(n))=\begin{cases}\Gamma_0^2(3^{\beta'}n_0)\ , & \alpha<2\\ \Gamma_0^2(2^{\alpha'}3^{\beta'}n_0), & \alpha\geq 2\end{cases}$$

$$\alpha'=mak\left(\alpha-4,\alpha-3-\left[\!\left[\frac{\alpha-3}{2}\right]\!\right]\right),\qquad \beta'=mak(\beta-1,\beta-\left[\!\left[\frac{\beta}{2}\right]\!\right])$$

İspat: Γ^2 nin $\Gamma_0^2(n)$ kosetleri üzerindeki hareketini düşünelim. Önerme 2.2.3. ten bu kosetler aşağıdaki denklik bağıntısının Γ^2 deki sınıflarıdır.

$$\begin{pmatrix} k & m \\ l & t \end{pmatrix}\sim\begin{pmatrix} k' & m' \\ l' & t' \end{pmatrix}\ \Leftrightarrow\ kl'-k'l\equiv 0\ mod\ n.$$

İlk sütunlar arasında bir işlem söz konusu olduğundan $\begin{pmatrix} k & m \\ l & t \end{pmatrix}$ nin $\Gamma_0^2(n)$ kosetini $\left[\frac{k}{l}\right]$ sembolü ile göstereceğiz. Böylece yukarıdaki $\sim$ bağıntısı

$$\left[\frac{k}{l}\right]=\left[\frac{k'}{l'}\right]\ \Leftrightarrow\ kl'-k'l\equiv 0\ mod\ n$$

durumuna döner. Γ^2 bu semboller üzerinde aşağıdaki gibi hareket eder.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left[\frac{k}{l}\right] = \left[\frac{ak+bl}{ck+dl}\right]$$

Şimdi $\Gamma_0^2(n)$ nin Γ^2 eksenini bulalım ki bu da $\Gamma_0^2(n)$ tarafından sabit bırakılan kosetlerin birleşimidir. Bu durumda

$$\begin{pmatrix} a & b \\ cn & d \end{pmatrix}\left[\frac{k}{l}\right] = \left[\frac{k}{l}\right] \; , \forall a,b,c,d \in \mathbb{Z} \, , \qquad ad - bcn = 1$$

dir. Buradan

$$\left[\frac{ak+bl}{cnk+dl}\right] = \left[\frac{k}{l}\right]$$

veya

$$(ak+bl)l - (cnk+dl)k \equiv 0 \; mod \; n$$

$$akl + bl^2 - dkl \equiv 0 \; mod \; n$$

olur. Bundan sonraki işlemleri Γ^2 nin üç ayrı eleman tipi için ayrı ayrı yapacağız.

A. $\begin{pmatrix} k & m \\ l & t \end{pmatrix} \in \Gamma^2$ olmak üzere $k, t \; tek \; l, m \; çift$ olma durumu:

$$k = x, \; t = w, \quad l = 2y, \quad m = 2z \quad x \; ve \; w \; tek \; .$$

Bu durumda yukarıdaki kongrüans bağıntısı

$$2axy + 4by^2 - 2dxy \equiv 0 \; mod \; n$$

olur. Şimdi de $\Gamma_0^2(n)$ nin elemanları da üç farklı tipten oluştuğundan bunlar için de ayrı ayrı inceleyeceğiz.

a. İlk olarak $a \; ve \; d \; tek, b \; ve \; c \; çift$ olma durumu:

$$a = a_0, \; d = d_0, \quad b = 2b_0, \; c = 2c_0 \; , \; a_0 \; ve \; d_0 \; tek$$

Bu takdirde yukarıdaki durum

$$2a_0xy + 8b_0y^2 - 2d_0xy \equiv 0 \; mod \; n$$

olup bu durum $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \Gamma_0^2(n)$ için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$2xy + 8y^2 \equiv 2xy \ mod\ n$$

yani,

$$8y^2 \equiv 0 \ mod\ n$$

olur ve yukarıdaki durum

$$8y^2 \equiv 0 \ mod\ n$$

$$2(a_0 - d_0)xy \equiv 0 \ modn$$

olur. Sistemin ikinci kongrüansını w ile çarpalım. Yani,

$$2(a_0 - d_0)xwy \equiv 0 \ mod\ n$$

$$xw - 4yz = 1$$

olduğundan $xw = 1 + 4yz$ yazılırsa

$$2(a_0 - d_0)(1 + 4yz)y \equiv 0 \ mod\ n$$

$$2(a_0 - d_0)y + 8y^2z(a_0 - d_0) \equiv 0 \ mod\ n$$

ve

$$8y^2 \equiv 0 \ mod\ n$$

olduğundan sistemin son durumu

$$8y^2 \equiv 0 \ mod\ n$$

$$2y(a_0 - d_0) \equiv 0 \ mod\ n$$

olur.

$a_0d_0 - 4b_0c_0n = 1$ ve $(a_0, n) = 1$ olduğundan $a_0d_0 \equiv 1 \ mod\ n$ dir. Bu yüzden kongrüans her iki taraftan a_0 ile çarpılıp yukarıdakiler kullanılırsa,

$$2y({a_0}^2 - a_0d_0) \equiv 0 \ mod\ n$$

$$2y({a_0}^2 - 1) \equiv 0 \ mod \ n$$

olur. Şu ana kadar yaptıklarımızı özetleyecek olursak

$$8y^2 \equiv 0 \ mod \ n$$

$$2y(a_0 - 1)(a_0 + 1) \equiv 0 \ mod \ n, \quad (a_0, n) = 1 \text{ olan } \forall \ a_0 \text{ için}$$

Çin kalan teoreminden, p asal olmak üzere p^k kuvvetleri için ayrı ayrı çözmek yeterlidir. Bu durumda incelenecek üç durum vardır.

i. $p = 2$ olsun. $p|n$ ve $(a_0, n) = 1$ olduğundan a tektir. Bu yüzden $(a_0, n) = 1$ olan $\forall \ a_0$ için

$$(a_0 - 1)(a_0 + 1) \equiv 0 \ mod \ 8$$

dir. Fakat

$$(a_0 - 1)(a_0 + 1) \not\equiv 0 \ mod \ 16$$

olan bir a_0 daima bulabiliriz. Ayrıca Dirichlet teoreminden $({a_0}', n) = 1$ olacak şekilde $16k + 3$ formunda bir ${a_0}'$ asalı bulabiliriz. Böylece

$$({a_0}' - 1)({a_0}' + 1) \equiv 8 \ mod \ 16$$

ve sistem

$$8y^2 \equiv 0 \ mod \ 2^\alpha$$

$$16y \equiv 0 \ mod \ 2^\alpha$$

olur ve çözüm

$$y \equiv 0 \ mod \ 2^{\alpha'}$$

$$\alpha' = mak\left(\alpha - 4, \alpha - 3 - \left[\!\left[\frac{\alpha - 3}{2}\right]\!\right]\right), \ \alpha \geq 2$$

dir.

ii. Şimdi $p = 3$ olsun. $3|n$ ve $(a_0, n) = 1$ olduğundan $a_0 \equiv \pm 1 \ mod \ 3$ tür. Bu yüzden, $(a_0, n) = 1$ olan $\forall \ a_0$ için

$$(a_0 - 1)(a_0 + 1) \equiv 0 \; mod \; 3,$$

dir. Fakat

$$(a_0 - 1)(a_0 + 1) \not\equiv 0 \; mod \; 9$$

olan bir a_0 daima bulabiliriz. Ayrıca Dirichlet teoreminden $(a_0', n) = 1$ olacak şekilde $9k + 2$ formunda bir a_0' asalı bulabiliriz. Böylece

$$(a_0' - 1)(a_0' + 1) \equiv 3 mod \; 9$$

ve sistem

$$8y^2 \equiv 0 \; mod \; 3^\beta$$

$$6y \equiv 0 \; mod \; 3^\beta$$

olur. $(2,3) = 1$ olduğundan

$$y^2 \equiv 0 \; mod \; 3^\beta$$

$$3y \equiv 0 \; mod \; 3^\beta$$

dir ve çözüm

$$y \equiv 0 \; mod \; 3^{\beta'}$$

$$\beta' = mak(\beta - 1, \beta - [\![\tfrac{\beta}{2}]\!])$$

dir.

iii. $p \geq 5$ olsun. Dirichlet teoreminden $(a_0', n) = 1$ olacak şekilde $pk + 2$ formunda

bir a_0' asalı bulabiliriz. Böylece

$$(a_0' - 1)(a_0' + 1) \equiv 3 mod \; p,$$

$$((a_0' - 1)(a_0' + 1), p) = 1$$

olduğundan çözüm s, p nin en büyük kuvveti olmak üzere,

$$y \equiv 0 \; mod \; p^s$$

dir. Bu durumda (A)(a) (ii)ve (iii) den sistemin çözümü

$$y \equiv 0 \; mod \; 2^{\alpha'} 3^{\beta'} n_0 \;\; , \quad \alpha \geq 2$$

olarak bulunur.

Son olarak $\alpha = 0 \; ve \; 1$ durumunu inceleyelim. Her iki durumda da sistem

$$y^2 \equiv 0 \; mod \; n$$

$$(a_0 - d_0)y \equiv 0 \; mod \; n$$

olur ve çözüm yukarıdaki gibi devam eder. Böylece

$$y \equiv 0 \; mod \; 3^{\beta'} n_0 \;\; , \quad \alpha < 2$$

olarak bulunur.

b. İkinci olarak $a \; çift \; b, c, d \; tek$ olma durumuna bakalım. Bu durumda $\alpha = 0$ olmak zorundadır. $b_0, c_0, d_0 \; tek$ olmak üzere

$$a = 2a_0, \;\; d = d_0, \quad b = b_0, \;\; c = c_0$$

alındığında

$$4a_0xy + 4b_0y^2 - 2xyd_0 \equiv 0 \; mod \; n$$

$$2xy(2a_0 - d_0) + 4by^2 \equiv 0 \; mod \; n$$

olup bu durum $\begin{pmatrix} 2\frac{(n+1)}{2} & 1 \\ n & 1 \end{pmatrix} \in \Gamma_0^2(n)$ için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$2xyn + 4y^2 \equiv 0 \; mod \; n$$

yani,

$$4y^2 \equiv 0 \; mod \; n$$

olur ve yukarıdaki durum

$$4y^2 \equiv 0 \; mod \; n$$

$$(2a_0 - d_0)2xy \equiv 0\ modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını w ile çarpalım. Yani,

$$2(2a_0 - d_0)xwy \equiv 0\ mod\ n$$

ve $xw - 4yz = 1$ olduğundan $xw = 1 + 4yz$ yazılırsa

$$2(2a_0 - d_0)(1 + 4yz)y \equiv 0\ mod\ n$$

$$2(2a_0 - d_0)y + 8y^2z(2a_0 - d_0) \equiv 0\ mod\ n$$

elde edilir ve

$$4y^2 \equiv 0\ mod\ n$$

olduğundan sistemin son durumu

$$4y^2 \equiv 0\ mod\ n$$

$$2y(2a_0 - d_0) \equiv 0\ mod\ n$$

olur. $(2,3) = 1$ olduğunu kullanırsak

$$y^2 \equiv 0\ mod\ n$$

$$y(2a_0 - d_0) \equiv 0\ mod\ n$$

dir.

i. $p = 3$ için $p|n$ ve $(2a_0, n) = 1$ olduğundan $2a_0 \equiv \pm 1\ mod\ 3$ tür. $a_0 = 1$ için $\begin{pmatrix} 2 & b_1 \\ n & d_1 \end{pmatrix} \in \Gamma_0^2(n)$ olan $b_1, d_1 \in \mathbb{Z}$ vardır. d_1 tek alınabilir. Böylece

$$y^2 \equiv 0\ mod\ 3^\beta$$

$$3y \equiv 0\ mod\ 3^\beta$$

olup çözüm

$$y \equiv 0\ mod\ 3^{\beta'}$$

$$\beta' = mak(\beta - 1, \beta - \left[\!\left[\frac{\beta}{2}\right]\!\right])$$

dür.

ii. Şimdi de $p \geq 5$ olsun. Yine $a_0 = 1$ için $\begin{pmatrix} 2 & b_1 \\ n & d_1 \end{pmatrix} \in \Gamma_0^2(n)$ olan $b_1, d_1 \in \mathbb{Z}$ vardır. d_1 tek alınabilir. Böylece

$$y \equiv 0 \; mod \; p^s$$

olur. Sonuç olarak

$$y \equiv 0 \; mod \; 3^{\beta'} n_0$$

dır.

c. Üçüncü olarak d $çift$ b, c, a tek olma durumuna bakalım. Bu durumda $\alpha = 0$ olmak zorundadır. b_0, c_0, a_0 tek olmak üzere

$$a = a_0, \;\; d = 2d_0, \;\; b = b_0, \;\; c = c_0$$

olsun. Dolayısı ile

$$2a_0xy + by^2 - 4xyd_0 \equiv 0 \; mod \; n$$

$$2xy(a_0 - 2d_0) + by^2 \equiv 0 \; mod \; n$$

olup bu durum $\begin{pmatrix} 1 & 1 \\ n & 2\frac{(n+1)}{2} \end{pmatrix} \in \Gamma_0^2(n)$ için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$2xyn + y^2 \equiv 0 \; mod \; n$$

yani,

$$y^2 \equiv 0 \; mod \; n$$

olur ve yukarıdaki durum

$$y^2 \equiv 0 \; mod \; n$$

$$(a_0 - 2d_0)2xy \equiv 0 \; modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını w ile çarpalım. Yani,

$$2(a_0 - 2d_0)xwy \equiv 0 \; mod \; n$$

$$xw - 4yz = 1$$

olduğundan $xw = 1 + 4yz$ yazılırsa ve

$$2(a_0 - 2d_0)(1 + 4yz)y \equiv 0 \; mod \; n$$

$$2(a_0 - 2d_0)y + 8y^2z(a_0 - 2d_0) \equiv 0 \; mod \; n$$

ve

$$y^2 \equiv 0 \; mod \; n$$

olduğundan sistemin son durumu

$$y^2 \equiv 0 \; mod \; n$$

$$2y(a_0 - 2d_0) \equiv 0 \; mod \; n$$

olur. $(2,3) = 1$ olduğunu kullanırsak, son durum

$$y^2 \equiv 0 \; mod \; n$$

$$y(a_0 - 2d_0) \equiv 0 \; mod \; n$$

dir.

i. $p = 3$ için, $p|n$ ve $(a_0, n) = 1$ olduğundan, $a_0 \equiv \pm 1 \; mod \; 3$ tür. Her taraf a_0 ile çarpılırsa

$$y^2 \equiv 0 \; mod \; n$$

$$y({a_0}^2 - 1) \equiv 0 \; mod \; n$$

olur ve işlem (A)(a)(ii) deki gibi devam eder.

ii. $p \geq 5$ için de sonuç (A)(a)(iii) teki gibidir.

B. $\begin{pmatrix} k & m \\ l & t \end{pmatrix} \in \Gamma^2$ olmak üzere $k \; çift \;\; l, m, t \; tek$ olma durumu; yani

$$k = 2x, \; t = w, \quad l = y, \quad m = z \quad y, z \; ve \; w \; tek$$

durumunu göz önüne alalım. Yine burada $\Gamma_0^2(n)$ elemanları için ayrı ayrı incelemeler yapacağız.

a. İlk olarak $a\ ve\ d\ tek, b\ ve\ c\ çift$ olma durumu:

$$a = a_0,\ \ d = d_0,\ \ \ b = 2b_0,\ \ c = 2c_0\ ,\ \ a_0\ ve\ d_0\ tek$$

$$2a_0xy + 2b_0y^2 - 2d_0xy \equiv 0\ mod\ n$$

Bu durumda $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \Gamma_0^2(n)$ için de kongrüans doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$2y^2 \equiv 0\ mod\ n$$

$$(a_0 - d_0)2xy \equiv 0\ modn$$

olur. Sistemin ikinci kongrüansını w ile çarpalım. Yani,

$$2(a_0 - d_0)xwy \equiv 0\ mod\ n.$$

$2xw - yz = 1$ olduğundan $2xw = 1 + yz$ yazılırsa

$$(a_0 - d_0)(1 + yz)y \equiv 0\ mod\ n$$

$$(a_0 - d_0)y + y^2z(a_0 - d_0) \equiv 0\ mod\ n$$

$(a_0 - d_0)$ çift olduğundan, kongrüansın son durumu

$$2y^2 \equiv 0\ mod\ n$$

$$(a_0 - d_0)y \equiv 0\ modn$$

olur. Burada $\alpha \geq 2$ için çözüm yoktur. Aksi takdirde y daima çift olur. Fakat matrisin seçimi gereği bu mümkün değildir. O halde $\alpha = 0\ ve\ 1$ için durumu inceleyelim.

$\alpha = 0\ ve\ 1$ için

$$y^2 \equiv 0\ mod\ n$$

$$(a_0 - d_0)y \equiv 0\ mod\ n$$

olup çözüm (A)(a) (ii) ve (iii) teki gibidir.

Yani,

$$y \equiv 0 \; mod \; 3^{\beta'} n_0 \;, \quad \alpha < 2.$$

b. İkinci olarak a $çift$ b, c, d tek olma durumuna bakalım. Bu durumda $\alpha = 0$ olmak zorundadır. b_0, c_0, d_0 tek olacak şekilde

$$a = 2a_0, \;\; d = d_0, \quad b = b_0, \;\; c = c_0$$

olsun. Dolayısı ile

$$4a_0xy + b_0y^2 - 2d_0xy \equiv 0 \; mod \; n$$

$$2xy(2a_0 - d_0) + by^2 \equiv 0 \; mod \; n$$

olup bu durum $\begin{pmatrix} 2\frac{(n+1)}{2} & 1 \\ n & 1 \end{pmatrix} \in \Gamma_0^2(n)$ için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$2xyn + y^2 \equiv 0 \; mod \; n$$

yani,

$$y^2 \equiv 0 \; mod \; n$$

olur ve yukarıdaki durum

$$y^2 \equiv 0 \; mod \; n$$

$$(2a_0 - d_0)2xy \equiv 0 \; modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını w ile çarpalım. Yani,

$$2(2a_0 - d_0)xwy \equiv 0 \; mod \; n.$$

$2xw - yz = 1$ olduğundan $2xw = 1 + yz$ yazılırsa

$$(2a_0 - d_0)(1 + yz)y \equiv 0 \; mod \; n$$

$$(2a_0 - d_0)y + y^2z(2a_0 - d_0) \equiv 0 \; mod \; n$$

elde edilir ve

$$y^2 \equiv 0 \; mod \; n$$

olduğundan, sistemin son durumu

$$y^2 \equiv 0 \; mod \; n$$

$$y(2a_0 - d_0) \equiv 0 \; mod \; n$$

olup sonuç (A)(b) deki gibidir.

c. Üçüncü olarak $d \; çift \; b, c, a \; tek$ olma durumuna bakalım. Bu durumda $\alpha = 0$ olmak zorundadır. $b_0, c_0, a_0 \; tek$ olmak üzere

$$a = a_0, \;\; d = 2d_0, \;\; b = b_0, \;\; c = c_0$$

alalım. Bu durumda

$$a_0 xy + by^2 - 2xyd_0 \equiv 0 \; mod \; n$$

$$xy(a_0 - 2d_0) + by^2 \equiv 0 \; mod \; n$$

olup bu durum $\begin{pmatrix} 1 & 1 \\ n & 2\frac{(n+1)}{2} \end{pmatrix} \in \Gamma_0^2(n)$ için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$xyn + y^2 \equiv 0 \; mod \; n$$

yani,

$$y^2 \equiv 0 \; mod \; n$$

olur ve yukarıdaki durum

$$y^2 \equiv 0 \; mod \; n$$

$$(a_0 - 2d_0)xy \equiv 0 \; modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını $2w$ ile çarpalım. Yani,

$$2(a_0 - 2d_0)xwy \equiv 0 \; mod \; n.$$

$2xw - yz = 1$ olduğundan $2xw = 1 + yz$ yazılırsa

$$2(a_0 - 2d_0)(1 + yz)y \equiv 0 \; mod \; n$$

$$2(a_0 - 2d_0)y + 2y^2z(a_0 - 2d_0) \equiv 0 \; mod \; n$$

elde edilir ve

$$y^2 \equiv 0 \; mod \; n$$

olduğundan, sistemin son durumu

$$y^2 \equiv 0 \; mod \; n$$

$$2y(a_0 - 2d_0) \equiv 0 \; mod \; n$$

olur. $(2,3) = 1$ olduğunu kullanırsak

$$y^2 \equiv 0 \; mod \; n$$

$$y(a_0 - 2d_0) \equiv 0 \; mod \; n$$

Bundan sonraki işlemler (A)(c) deki gibidir.

C. $\begin{pmatrix} k & m \\ l & t \end{pmatrix} \in \Gamma^2$ olmak üzere $t \; çift \;\; l, m, k \; tek$ olma durumu:

$$k = x, \; t = 2w, \quad l = y, \quad m = z \quad y, z \; ve \; x \; tek$$

Yine burada $\Gamma_0^2(n)$ elemanları için ayrı ayrı incelemeler yapacağız.

a. İlk olarak $a \; ve \; d \; tek, b \; ve \; c \; çift$ olma durumu:

$$a = a_0, \;\; d = d_0, \;\; b = 2b_0, \;\; c = 2c_0 \,, \;\; a_0 \; ve \; d_0 \; tek$$

$$a_0xy + 2b_0y^2 - d_0xy \equiv 0 \; mod \; n \,.$$

Bu durumda $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \Gamma_0^2(n)$ için de kongrüans doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$2y^2 \equiv 0 \; mod \; n$$

$$(a_0 - d_0)xy \equiv 0 \; modn$$

olur. Sistemin ikinci kongrüansını $2w$ ile çarpalım. Yani,

$$2(a_0 - d_0)xwy \equiv 0\ mod\ n.$$

$2xw - yz = 1$ olduğundan $2xw = 1 + yz$ yazılırsa

$$(a_0 - d_0)(1 + yz)y \equiv 0\ mod\ n$$

$$(a_0 - d_0)y + y^2 z(a_0 - d_0) \equiv 0\ mod\ n$$

elde edilir ve $(a_0 - d_0)$ çift olduğundan, kongrüansın son durumu

$$2y^2 \equiv 0\ mod\ n$$

$$(a_0 - d_0)y \equiv 0\ modn$$

olur. Burada $\alpha \geq 2$ için çözüm yoktur. Aksi takdirde y daima çift olur. Fakat matrisin seçimi gereği bu mümkün değildir. O halde $\alpha = 0\ ve\ 1$ için durumu inceleyelim.

$\alpha = 0\ ve\ 1$ için

$$y^2 \equiv 0\ mod\ n$$

$$(a_0 - d_0)y \equiv 0\ mod\ n$$

olup çözüm (A)(a) (ii) ve (iii) teki gibidir.

b. İkinci olarak $a\ çift\ b, c, d\ tek$ olma durumuna bakalım. Bu durumda $\alpha = 0$ olmak zorundadır. $b_0, c_0, d_0\ tek$ olmak üzere

$$a = 2a_0,\ \ d = d_0,\ \ \ b = b_0,\ \ c = c_0$$

alalım. Bu durumda

$$2a_0 xy + b_0 y^2 - d_0 xy \equiv 0\ mod\ n$$

$$xy(2a_0 - d_0) + by^2 \equiv 0\ mod\ n$$

olup bu durum $\begin{pmatrix} 2\frac{(n+1)}{2} & 1 \\ n & 1 \end{pmatrix} \in \Gamma_0^2(n)$ için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$xyn + y^2 \equiv 0\ mod\ n$$

yani,

$$y^2 \equiv 0 \; mod \; n$$

olur ve yukarıdaki durum

$$y^2 \equiv 0 \; mod \; n$$

$$(2a_0 - d_0)xy \equiv 0 \; modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını $2w$ ile çarpalım. Yani,

$$2(2a_0 - d_0)xwy \equiv 0 \; mod \; n$$

$2xw - yz = 1$ olduğundan $2xw = 1 + yz$ yazılırsa

$$(2a_0 - d_0)(1 + yz)y \equiv 0 \; mod \; n$$

$$(2a_0 - d_0)y + y^2 z(2a_0 - d_0) \equiv 0 \; mod \; n$$

elde edilir ve

$$y^2 \equiv 0 \; mod \; n$$

olduğundan sistemin son durumu

$$y^2 \equiv 0 \; mod \; n$$

$$y(2a_0 - d_0) \equiv 0 \; mod \; n$$

olup sonuç (A)(b) deki gibidir.

c. Üçüncü olarak $d \; çift \; b, c, a \; tek$ olma durumuna bakalım. Bu durumda $\alpha = 0$ olmak zorundadır.

$$a = a_0, \;\; d = 2d_0, \;\; b = b_0, \;\; c = c_0 \; , \quad b_0, c_0, a_0 \; tek$$

Bu durumda

$$a_0 xy + by^2 - 2xyd_0 \equiv 0 \; mod \; n$$

$$xy(a_0 - 2d_0) + by^2 \equiv 0 \; mod \; n$$

olup bundan sonraki işlemler (A)(c) deki gibidir.

Böylece (A),(B) ve (C) den çözüm,

$$y \equiv 0 \ mod\ 3^{\beta'} n_0 \ , \qquad \alpha < 2,$$

$$y \equiv 0 \ mod\ 2^{\alpha'} 3^{\beta'} n_0 \ , \quad \alpha \geq 2$$

olur.

Sonuç 2.4.8. $n \geq 1$ ve $(n, 6) = 1$ olsun. Bu takdirde

$$N_{\Gamma^2}\left(\Gamma_0^2(n)\right) = \Gamma_0^2(n)$$

dir.

Teorem 2.4.9. $n = 2^{\alpha} 3^{\beta} n_0 \geq 1$, $(n_0, 6) = 1$ olsun. $N_{\Gamma^3}\left(\Gamma_0^3(n)\right)$, $\Gamma_0^3(n)$ nin Γ^3 deki normalliyeni olmak üzere

$$N_{\Gamma^3}\left(\Gamma_0^3(n)\right) = \begin{cases} \Gamma_0^3\left(2^{\alpha'} n_0\right) \ , & \beta < 2 \\ \Gamma_0^3\left(2^{\alpha'} 3^{\beta-2} n_0\right), & \beta \geq 2 \end{cases}$$

$$\alpha' = mak\left(\alpha - 3, \alpha - \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$$

İspat: Γ^3 ün $\Gamma_0^3(n)$ kosetleri üzerindeki hareketini düşünelim. Önerme 2.2.3. ten bu kosetler aşağıdaki denklik bağıntısının Γ^3 deki sınıflarıdır.

$$\begin{pmatrix} k & m \\ l & t \end{pmatrix} \sim \begin{pmatrix} k' & m' \\ l' & t' \end{pmatrix} \iff kl' - k'l \equiv 0 \ mod\ n$$

Burada bizim için önemli olan Γ^3 nin herhangi bir elemanının ilk sütunu olduğudur.. Bu yüzden $\begin{pmatrix} k & m \\ l & t \end{pmatrix}$ nin $\Gamma_0^3(n)$ kosetini $\left[\frac{k}{l}\right]$ sembolü ile göstereceğiz. Böylece yukarıdaki $\sim$ bağıntısı $\left[\frac{k}{l}\right] = \left[\frac{k'}{l'}\right] \iff kl' - k'l \equiv 0 \ mod\ n$

durumuna döner. Γ^3 bu semboller üzerinde aşağıdaki gibi hareket eder.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[\frac{k}{l}\right] = \left[\frac{ak + bl}{ck + dl}\right].$$

Şimdi $\Gamma_0^3(n)$ nin Γ^3 eksenini bulalım, ki bu da $\Gamma_0^3(n)$ tarafından sabit bırakılan kosetlerin birleşimidir. Bu durumda

$$\begin{pmatrix} a & b \\ cn & d \end{pmatrix}\left[\frac{k}{l}\right] = \left[\frac{k}{l}\right] \,, \forall a,b,c,d \in \mathbb{Z}\,, \qquad ad - bcn = 1$$

dir. Buradan

$$\left[\frac{ak+bl}{cnk+dl}\right] = \left[\frac{k}{l}\right]$$

veya

$$(ak+bl)l - (cnk+dl)k \equiv 0 \; mod \; n$$

$$akl + bl^2 - dkl \equiv 0 \; mod \; n$$

olur. Bundan sonraki işlemleri Γ^3 nin üç ayrı eleman tipi için ayrı ayrı yapacağız.

A. $\begin{pmatrix} k & m \\ l & t \end{pmatrix} \in \Gamma^3$ olmak üzere $k \equiv 0 \; mod \; 3, t \equiv 0 \; mod \; 3, l \equiv \pm 1 \; mod \; 3, m \equiv \pm 1 \; mod \; 3$ olma durumunu göz önüne alalım. Bu durumda

$$k = 3x,\; t = 3w,\; y = l,\; z = m$$

dersek, yukarıdaki kongrüans bağıntısı

$$3axy + by^2 - 3dxy \equiv 0 \; mod \; n$$

olur. Şimdi de $\Gamma_0^3(n)$ nin elemanları da üç farklı tipten oluştuğundan bunlar için de ayrı ayrı inceleyeceğiz.

a. İlk olarak $b \equiv 0 \; mod \; 3, c \equiv 0 \; mod \; 3, a \equiv \pm 1 \; mod \; 3, d \equiv \pm 1 \; mod \; 3$olma durumu:

$$a = a_0,\;\; d = d_0,\;\;\; b = 3b_0,\;\; c = 3c_0$$

Bu takdirde yukarıdaki durum

$$3a_0xy + 3b_0y^2 - 3d_0xy \equiv 0 \; mod \; n$$

olup bu durum $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \in \Gamma_0^3(n)$ için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$3xy + 3y^2 \equiv 3xy \; mod \; n$$

yani,

$$3y^2 \equiv 0 \; mod \; n$$

olur ve yukarıdaki durum

$$3y^2 \equiv 0 \; mod \; n$$

$$3(a_0 - d_0)xy \equiv 0 \; modn$$

halini alır. Sistemin ikinci kongrüansını $9w$ ile çarpalım. Yani,

$$27(a_0 - d_0)xwy \equiv 0 \; mod \; n \; .$$

$9xw - yz = 1$ olduğundan, $9xw = 1 + yz$ yazılırsa,

$$3(a_0 - d_0)(1 + yz)y \equiv 0 \; mod \; n$$

$$3(a_0 - d_0)y + 3y^2z(a_0 - d_0) \equiv 0 \; mod \; n$$

ve

$$3y^2 \equiv 0 \; mod \; n$$

olduğundan sistemin son durumu

$$3y^2 \equiv 0 \; mod \; n$$

$$3y(a_0 - d_0) \equiv 0 \; mod \; n$$

olur.

$a_0d_0 - 9b_0c_0n = 1$ ve $(a_0, n) = 1$ olduğundan $a_0d_0 \equiv 1 \; mod \; n$ dir. Bu yüzden kongrüans her iki taraftan a_0 ile çarpılıp yukarıdakiler kullanılırsa,

$$3y({a_0}^2 - a_0d_0) \equiv 0 \; mod \; n$$

$$3y({a_0}^2 - 1) \equiv 0 \; mod \; n$$

elde edilir. Şu ana kadar yaptıklarımızı özetleyecek olursak

$$3y^2 \equiv 0 \; mod \; n$$

ve $(a_0, n) = 1$ olan $\forall\, a_0$ için

$$3y(a_0 - 1)(a_0 + 1) \equiv 0 \; mod \; n$$

dir. Çin kalan teoreminden, p asal olmak üzere, p^k kuvvetleri için ayrı ayrı çözmek yeterlidir. Bu durumda incelenecek üç durum vardır.

i. $p = 2$ olsun. $p|n$ ve $(a_0, n) = 1$ olduğundan a_0 tektir. Bu yüzden $(a_0, n) = 1$ olan $\forall\, a_0$ için

$$(a_0 - 1)(a_0 + 1) \equiv 0 \; mod \; 8$$

dir. Fakat

$$(a_0 - 1)(a_0 + 1) \not\equiv 0 \; mod \; 16$$

olan bir a_0 daima bulabiliriz. Ayrıca Dirichlet teoreminden $(a_0{}', n) = 1$ olacak şekilde $16k + 3$ formunda bir $a_0{}'$ asalı bulabiliriz. Böylece

$$(a_0{}' - 1)(a_0{}' + 1) \equiv 8 mod \; 16$$

ve sistem

$$3y^2 \equiv 0 \; mod \; 2^\alpha$$

$$24y \equiv 0 \; mod \; 2^\alpha$$

olur. $(2,3) = 1$ olduğundan

$$y^2 \equiv 0 \; mod \; 3^\beta$$

$$8y \equiv 0 \; mod \; 3^\beta$$

dir ve çözüm $\alpha' = mak\left(\alpha - 3, \alpha - \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$ olmak üzere,

$$y \equiv 0 \; mod \; 2^{\alpha'}$$

olarak elde edilir.

ii. Şimdi $p = 3$ olsun. $3|n$ ve $(a_0, n) = 1$ olduğundan, $a_0 \equiv \pm 1 \; mod \; 3$ tür. Bu yüzden, $(a_0, n) = 1$ olan $\forall\, a_0$ için

$$(a_0 - 1)(a_0 + 1) \equiv 0 \ mod \ 3$$

tür. Fakat

$$(a_0 - 1)(a_0 + 1) \not\equiv 0 \ mod \ 9$$

olan bir a_0 daima bulabiliriz. Ayrıca Dirichlet teoreminden $(a_0{}', n) = 1$ olacak şekilde $9k + 2$ formunda bir $a_0{}'$ asalı bulabiliriz. Böylece

$$(a_0{}' - 1)(a_0{}' + 1) \equiv 3 \ mod \ 9$$

elde edilir. Dolayısı ile sistem

$$3y^2 \equiv 0 \ mod \ 3^\beta$$

$$9y \equiv 0 \ mod \ 3^\beta$$

olur. Burada sadece $\beta = 0 \ ve \ 1$ olması durumunda çözüm vardır. Aksi takdirde $y \equiv 0 \ mod \ 3$ olur ve bu da matrisin yapısından dolayı mümkün değildir. O halde $\beta = 0 \ ve \ 1$ için durumu inceleyelim.

$$y \equiv 0 \ mod \ 3^{\beta'}$$

$$\beta' = mak(\beta - 2, \beta - 1 - \left[\!\left[\frac{\beta-1}{2}\right]\!\right])$$

dir. Burada $\beta = 0 \ ve \ 1$ için $\beta' = 0$ dır.

iii. $p \geq 5$ olsun. Dirichlet teoreminden $(a_0{}', n) = 1$ olacak şekilde $pk + 2$ formunda

bir $a_0{}'$ asalı bulabiliriz. Böylece

$$(a_0{}' - 1)(a_0{}' + 1) \equiv 3 mod \ p,$$

$$((a_0{}' - 1)(a_0{}' + 1), p) = 1$$

olduğundan çözüm, s, p nin en büyük kuvveti olmak üzere,

$$y \equiv 0 \ mod \ p^s$$

dir. Bu durumda (A)(a) (i), (ii),(iii) ten sistemin çözümü

$$y \equiv 0 \ mod \ 2^{\alpha'} n_0 \ , \quad \beta < 2$$

olarak bulunur.

b. İkinci olarak $a \equiv 0\ mod\ 3, d \equiv 0\ mod\ 3, b \equiv \pm 1\ mod\ 3, c \equiv \pm 1\ mod\ 3$ olma durumu:

$$a = 3a_0,\ \ d = 3d_0,\ \ \ b = b_0,\ \ c = c_0\ .$$

Burada $\beta = 0$ olmak zorundadır.

Bu durumda,

$$9a_0xy + b_0y^2 - 9d_0xy \equiv 0\ mod\ n$$

kongrüans denklemini elde etmiş oluruz. Bu denklemin çözümünü bulmak için aşağıdaki iki matrisi kullanacağız.

- $n \equiv -1\ mod\ 3$ olmak üzere $\begin{pmatrix} 3\,\frac{(n+1)}{3} & 1 \\ n(2+n) & 3\,\frac{(n+1)}{3} \end{pmatrix} \in \Gamma_0^3(n)$,
- $n \equiv \ \ 1\ mod\ 3$ olmak üzere $\begin{pmatrix} 3\,\frac{(n-1)}{3} & 1 \\ n(n-2) & 3\,\frac{(n-1)}{3} \end{pmatrix} \in \Gamma_0^3(n)$.

Böylece yukarıdaki kongrüans bağıntısı her iki durumda da

$$y^2 \equiv 0\ mod\ n$$

olur ve yukarıdaki durum

$$y^2 \equiv 0\ mod\ n$$

$$9(a_0 - d_0)xy \equiv 0\ modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını w ile çarpalım. Yani,

$$9(a_0 - d_0)xwy \equiv 0\ mod\ n.$$

$9xw - yz = 1$ olduğundan, $9xw = 1 + yz$ yazılırsa,

$$(a_0 - d_0)(1 + yz)y \equiv 0\ mod\ n$$

$$(a_0 - d_0)y + y^2z(a_0 - d_0) \equiv 0\ mod\ n$$

ve

$$y^2 \equiv 0 \; mod \; n$$

olduğundan sistemin son durumu

$$y^2 \equiv 0 \; mod \; n$$

$$y(a_0 - d_0) \equiv 0 \; mod \; n$$

olur.

i. $p = 2$ olsun. $p|n$ ve $(a_0, n) = 1$ olduğundan a_0 tektir. Bu yüzden $(a_0, n) = 1$ olan $\forall \; a_0$ için

$$(a_0 - 1)(a_0 + 1) \equiv 0 \; mod \; 8$$

dir. Fakat

$$(a_0 - 1)(a_0 + 1) \not\equiv 0 \; mod \; 16$$

olan bir a_0 daima bulabiliriz. Ayrıca Dirichlet teoreminden $(a_0{}', n) = 1$ olacak şekilde $16k + 3$ formunda bir $a_0{}'$ asalı bulabiliriz. Böylece

$$(a_0{}' - 1)(a_0{}' + 1) \equiv 8 mod \; 16$$

ve sistem

$$y^2 \equiv 0 \; mod \; 2^\alpha$$

$$8y \equiv 0 \; mod \; 2^\alpha$$

olup çözüm, $\alpha' = mak\left(\alpha - 3, \alpha - \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$ olmak üzere,

$$y \equiv 0 \; mod \; 2^{\alpha'} \; .$$

ii. $p \geq 5$ için çözüm (iii) teki gibidir. Sonuç olarak

$$y \equiv 0 \; mod \; 2^{\beta'} n_0$$

dır.

c. Üçüncü olarak $a \equiv \pm 1\ mod\ 3, d \equiv \pm 1\ mod\ 3, b \equiv \pm 1\ mod\ 3, c \equiv \pm 1\ mod\ 3$ olma durumu:

$$a = a_0,\ \ d = d_0,\ \ \ b = b_0,\ \ c = c_0$$

Burada $\beta = 0$ olmak zorundadır.

Bu durumda,

$$3a_0xy + by^2 - 3xyd_0 \equiv 0\ mod\ n$$

$$3xy(a_0 - d_0) + by^2 \equiv 0\ mod\ n$$

olup bu durum

- $n \equiv -1\ mod\ 3$ olmak üzere $\begin{pmatrix} 1 & 1 \\ n & n+1 \end{pmatrix} \in \Gamma_0^3(n)$
- $n \equiv \ \ 1\ mod\ 3$ olmak üzere $\begin{pmatrix} 1 & -1 \\ n & 1-n \end{pmatrix} \in \Gamma_0^3(n)$

için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı her iki durumda da

$$y^2 \equiv 0\ mod\ n$$

olur ve yukarıdaki durum

$$y^2 \equiv 0\ mod\ n$$

$$3(a_0 - d_0)xy \equiv 0\ modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını $3w$ ile çarpalım. Bu durumda

$$9(a_0 - d_0)xwy \equiv 0\ mod\ n$$

elde edilir. $9xw - yz = 1$ olduğundan, $9xw = 1 + yz$ yazılırsa

$$(a_0 - d_0)(1 + yz)y \equiv 0\ mod\ n$$

$$(a_0 - d_0)y + y^2z(a_0 - d_0) \equiv 0\ mod\ n$$

ve

$$y^2 \equiv 0\ mod\ n$$

olduğundan sistemin son durumu

$$y^2 \equiv 0 \; mod \; n$$

$$y(a_0 - d_0) \equiv 0 \; mod \; n$$

olur ve çözüm yukarıdaki gibi devam eder.

B. $\begin{pmatrix} k & m \\ l & t \end{pmatrix} \in \Gamma^3$ olmak üzere $k, t \equiv \pm 1 \; mod \; 3$, $l, m \equiv 0 \; mod \; 3$ olma durumu:

$$k = x, \qquad t = w, \quad l = 3y, \quad m = 3z$$

Yine burada $\Gamma_0^3(n)$ elemanları için ayrı ayrı incelemeler yapacağız.

a. İlk olarak $a, d \equiv \pm 1 \; mod \; 3$, $b, c \equiv 0 \; mod \; 3$ olma durumu:

$$a = a_0, \;\; d = d_0, \;\; b = 3b_0, \;\; c = 3c_0$$

$$3a_0xy + 27b_0y^2 - 3d_0xy \equiv 0 \; mod \; n$$

Bu durumda $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \in \Gamma_0^3(n)$ için de kongrüans doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$27y^2 \equiv 0 \; mod \; n$$

$$3(a_0 - d_0)xy \equiv 0 \; modn$$

olur. Sistemin ikinci kongrüansını w ile çarpalım. Bu durumda

$$3(a_0 - d_0)xwy \equiv 0 \; mod \; n$$

elde edilir. $xw - 9yz = 1$ olduğundan, $xw = 1 + 9yz$ yazılırsa

$$3(a_0 - d_0)(1 + 9yz)y \equiv 0 \; mod \; n$$

$$3(a_0 - d_0)y + 27y^2z(a_0 - d_0) \equiv 0 \; mod \; n$$

olup kongrüansın son durumu

$$27y^2 \equiv 0 \; mod \; n$$

$$3(a_0 - d_0)y \equiv 0 \; modn$$

olur. $p = 2$ asalı için çözüm $\alpha' = mak\left(\alpha - 3, \alpha - \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$ olmak üzere,

$$y \equiv 0 \; mod \; 2^{\alpha'}$$

dir.

i. Şimdi $p = 3$ ve $p|n$ olsun. (a_0, n)=1 olduğundan $a_0 \equiv \pm 1 \; mod \; 3$ olup çözüm yapıldığında

$$y \equiv 0 \; mod \; 3^{\beta'}, \quad \beta' = \beta - 2 \;, \beta \geq 2$$

elde edilir.

ii. $p \geq 5$ için yukarıdakilere benzer şekilde

$$y \equiv 0 \; mod \; n_0$$

olup genel çözüm

$$y \equiv 0 \; mod \; 2^{\alpha'} 3^{\beta'} n_0 \quad , \quad \beta' = \beta - 2 \;, \beta \geq 2$$

olarak bulunur.

b. İkinci olarak $a, d \equiv 0 \; mod \; 3$, $b, c \equiv \pm 1 \; mod \; 3$ olma durumu:

$$a = 3a_0, \;\; d = 3d_0, \quad b = b_0, \;\; c = c_0$$

Bu durumda,

$$9a_0xy + b_0y^2 - 9d_0xy \equiv 0 \; mod \; n$$

$$9xy(a_0 - d_0) + by^2 \equiv 0 \; mod \; n$$

olup bu durum (A)(b) de seçilen matrisler için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$y^2 \equiv 0 \; mod \; n$$

olur ve yukarıdaki durum

$$y^2 \equiv 0 \; mod \; n$$

$$9(a_0 - d_0)xy \equiv 0\ modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını w ile çarpıp gerekli düzenlemeleri yaptığımızda sistemin son durumu

$$y^2 \equiv 0\ mod\ n$$

$$9y(a_0 - d_0) \equiv 0\ mod\ n$$

olup sonuç (A)(b) deki gibidir.

c. Üçüncü olarak $a, b, c, d \equiv \pm 1\ mod\ 3$ olma durumu:

$$a = a_0,\ \ d = d_0,\ \ \ b = b_0,\ \ c = c_0\ .$$

Bu durumda $\beta = 0$ olmak zorundadır.

Böylece,

$$3a_0xy + 9b_0y^2 - 3xyd_0 \equiv 0\ mod\ n$$

$$3xy(a_0 - d_0) + 9by^2 \equiv 0\ mod\ n$$

olup bu durum (A)(c) de seçilen matrisler için de doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$9y^2 \equiv 0\ mod\ n$$

$$3(a_0 - d_0)xy \equiv 0\ modn$$

durumuna dönüşür. Sistemin ikinci kongrüansını w ile çarpıp düzenlersek

$$9y^2 \equiv 0\ mod\ n$$

$$3y(a_0 - d_0) \equiv 0\ mod\ n$$

olur. Bundan sonraki işlemler (A)(c) deki gibi devam eder.

C. $\begin{pmatrix} k & m \\ l & t \end{pmatrix} \in \Gamma^3$ olmak üzere $k, l, m, t \equiv \pm 1\ mod\ 3$ olma durumu:

$$k = x, \qquad t = w, \quad l = y, \quad m = z$$

Yine burada $\Gamma_0^3(n)$ elemanları için ayrı ayrı incelemeler yapacağız.

a. İlk olarak $a, d \equiv \pm 1\ mod\ 3,\ \ b, c \equiv 0\ mod\ 3$ olma durumu:

$$a = a_0,\ \ d = d_0,\ \ \ b = 3b_0,\ \ c = 3c_0$$

$$a_0 xy + 3b_0 y^2 - d_0 xy \equiv 0\ mod\ n\ .$$

Bu durumda $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \in \Gamma_0^3(n)$ için de kongrüans doğrudur. Böylece yukarıdaki kongrüans bağıntısı

$$3y^2 \equiv 0\ mod\ n$$

$$(a_0 - d_0)xy \equiv 0\ modn$$

olur. Sistemin ikinci kongrüansını $3w$ ile çarpalım. Böylece son durum

$$3y^2 \equiv 0\ mod\ n$$

$$3(a_0 - d_0)y \equiv 0\ modn$$

olarak elde edilir. p asal olmak üzere $p \geq 2$ için çözüm (i), (ii) ve (iii) teki gibidir.

b. İkinci olarak $a, d \equiv 0\ mod\ 3,\ \ b, c \equiv \pm 1\ mod\ 3$ olma durumu:

$$a = 3a_0,\ \ d = 3d_0,\ \ \ b = b_0,\ \ c = c_0$$

Bu durumda $\beta = 0$ olmak zorundadır.

Böylece,

$$3a_0 xy + 9b_0 y^2 - 3d_0 xy \equiv 0\ mod\ n$$

$$3xy(a_0 - d_0) + 9b_0 y^2 \equiv 0\ mod\ n$$

olup bu durumdan sonrası (A)(b) deki gibidir.

c. Üçüncü olarak $a, b, c, d \equiv \pm 1\ mod\ 3$ olma durumuna bakalım. Bu durumda $\beta = 0$ olmak zorundadır.

$$a = a_0,\ \ d = d_0,\ \ \ b = b_0,\ \ c = c_0\ .$$

Böylece,

$$a_0xy + by^2 - xyd_0 \equiv 0 \; mod \; n$$

$$xy(a_0 - d_0) + by^2 \equiv 0 \; mod \; n$$

olup bundan sonraki işlemler (A)(c) deki gibi devam eder. Dolayısı ile teoremin ispatı tamamlanmış olur.

Sonuç 2.4.10. $n \geq 1$ ve $(n, 6) = 1$ olsun. Bu takdirde

$$N_{\Gamma^3}\left(\Gamma_0^3(n)\right) = \Gamma_0^3(n)$$

dir.

2.5. $\Gamma_{0,n}(N)$ Kongrüans Alt Grubunun Alt Yörüngesel Grafları

2.5.1. $\Gamma_{0,n}(N)$ Kongrüans Alt Grubu

[16] da görüleceği gibi $\Gamma_{0,n}(N)$ grubu, $\Gamma_0(N)$ kongrüans alt grubunun $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$, $a \equiv d \; mod \; n$ şartını sağlayan elemanlarından oluşur. Yani,

$$\Gamma_{0,n}(N) = \left\{\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N) \;\middle|\; a^2 \equiv 1 \text{ mod n}, \text{n}|\text{N}, \text{n} > 1\right\}$$

$$= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \;\middle|\; a \equiv \text{d mod n}\right\}$$

Açıkça $\Gamma_{0,n}(N) \leq \Gamma_0(N)$ dir.

$\Gamma_{0,n}(N)$ grubuna ait bazı ilginç sonuçlar aşağıda verilmiştir:

- Eğer $n|N$ ise, $\Gamma_{0,n}(N)$ grubu N düzeyli bir kongrüans alt grubudur ve $\Gamma_1(N) \leq \Gamma_{0,n}(N) \leq \Gamma_0(N)$ dir.
- $\forall \, N \in \mathbb{Z}^+$ için, $\Gamma_{0,1}(N) = \Gamma_0(N)$ dir.
- Eğer $n|N$ ise, $\Gamma_{0,n}(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \;|\; a \equiv 1 \text{ mod n}\right\}$ dir.
- $\Gamma_{0,n}(N) = \Gamma_0(N)$ ancak ve ancak $\forall \, a \in \mathbb{Z}$ için $(a, N) = 1, a^2 \equiv 1 \; modn$ [16].

Şimdi transitif permütasyon gruplarının imprimitif hareketini gözönüne alalım.

(G,Ω) bir Ω kümesi üzerinde hareket eden bir G grubundan oluşan bir permütasyon grubu olsun. Eğer $\alpha,\beta \in \Omega$ için $\alpha \approx \beta$ olduğunda $\forall\, g \in G$ için $g(\alpha) \approx g(\beta)$ oluyorsa "$\approx$" denklik bağıntısına Ω üzerinde bir $G-$ invaryant denklik bağıntısı denir; denklik sınıflarına da bloklar adı verilir. Böyle bağıntılara aşikar örnekler olarak;

i. özdeşlik bağıntısı, $\alpha \approx \beta \Leftrightarrow \alpha = \beta$;

ii. evrensel bağıntı, $\forall\, \alpha,\beta \in \Omega$ için $\alpha \approx \beta$.

Eğer Ω üzerinde i) ve ii) den farklı bir $G-$ invaryant denklik bağıntısı var ise (G,Ω) ya imprimitif aksi halde primitif denir. Açıkça bir primitif grup transitif olarak hareket etmek zorundadır. Eğer değil ise yörüngeler bir sistem bloğu oluşturmaz; tersi doğru değildir.

Önerme 2.5.2.[10] (G,Ω) bir transitif permütasyon grubu olsun. Bu takdirde (G,Ω) primitiftir $\Leftrightarrow$ bir $\alpha \in \Omega$ noktasının sabitleyeni olan G_α , $\forall\, \alpha \in \Omega$ için G nin bir maksimal alt grubudur.

Önerme 2.5.2 den $G_\alpha < H < G$ için (G,Ω) imprimitiftir. Şimdi aşikar olmayan bir denklik bağıntısını aşağıdaki şekilde verelim. Hareket transitif olduğundan Ω nın her elemanı $g(\alpha)$, $g \in G$ formundadır. Böylece aşağıdaki bağıntı,

$$g(\alpha) \approx g'(\alpha) \Leftrightarrow g' \in gH$$

aşikar olmayan bir G- invaryant denklik bağıntısıdır. Blokların sayısı $|G{:}H|$ indeks sayısına eşittir ve α yı kapsayan blok $H(\alpha)$ yörüngesidir. Biz burada $G = \Gamma_0(N)$, $\Omega = \widehat{\mathbb{Q}}(N)$ ve $H = \Gamma_{0,n}(N)$ alacağız.

2.6. $\Gamma_0(N)$ nin $\widehat{\mathbb{Q}}(N)$ Üzerindeki Hareketi

Bu bölümde $\Gamma_0(N)$ nin $\widehat{\mathbb{Q}}(N)$ üzerindeki transitif ve imprimitif hareketini tanımlayacağız. $\Gamma_0(N)(\infty) = \left\{\frac{a}{bN} : a,b \in \mathbb{Z}\right\}$ olduğundan $\left\{\frac{a}{bN} : a,b \in \mathbb{Z}\right\}$ kümesi $\Gamma_0(N)$ nin transitif olduğu en büyük kümelerden biridir. Bu kümeyi $\widehat{\mathbb{Q}}(N)$ ile gösterelim. Böylece $\Gamma_0(N)$, $\widehat{\mathbb{Q}}(N)$ üzerinde transitiftir. [10] daki Önerme 2.2 gereği $(\Gamma_0(N), \widehat{\mathbb{Q}}(N))$ transitif permütasyon grubu impirimitiftir. Yani, $n \nmid 24$ olması halinde $\Gamma_0(N)$ grubu $\widehat{\mathbb{Q}}(N)$ üzerinde impirimitif olarak hareket eder. Bu durumda $\Gamma_{0,n}(N)$ ile $\widehat{\mathbb{Q}}(N)$ üzerinde bir $\Gamma-$invaryant eşdeğerlik bağıntısı vardır, bu bağıntıyı $\tilde{\tilde{n}}$ ile gösterelim.$v = \frac{r}{sN}$ ve $w = \frac{x}{yN} \in \widehat{\mathbb{Q}}(N)$ alırsak; $\Gamma_0(N)$ nin transitifliğinden $v = g(\infty)$ ve $w = h(\infty)$ olan $g,h \in \Gamma_0(N)$ vardır.

Böylece $g=\begin{pmatrix} r & k \\ sN & l \end{pmatrix}$, $h=\begin{pmatrix} x & m \\ yN & t \end{pmatrix}$ yazarsak $\frac{r}{sN} \underset{n}{\approx} \frac{x}{yN} \Leftrightarrow g^{-1}h \in \Gamma_0(N)$ dir.

$$g^{-1}h=\begin{pmatrix} l & -k \\ -sN & r \end{pmatrix}\begin{pmatrix} x & m \\ yN & t \end{pmatrix}$$

$$=\begin{pmatrix} lx-kyN & lm-kt \\ -sNx+ryN & -smN+rt \end{pmatrix} \in \Gamma_{0,n}(N)$$

$$\Leftrightarrow (lx-kyN)^2 \equiv l^2x^2 \equiv 1 \; mod \; n$$

$$\Leftrightarrow x^2 \equiv l^{-2} \; mod \; n \,.$$

g nin determinantından $lr \equiv 1 \; mod \; n$, yani $r \equiv l^{-1} \; modn$ olduğunu kullanırsak, yukarıdaki ifade

$$x^2 \equiv r^2 \; mod \; n$$

olur. Sonuç olarak,

$$\frac{x}{yN} \underset{n}{\approx} \frac{r}{sN} \Leftrightarrow x^2 \equiv r^2 \; mod \; n$$

dir. Böylece bazı durumlarda $\frac{x}{yN} \underset{n}{\approx} \frac{x}{N}$ dir. Bu durumda kısa olması itibarı ile $\frac{x}{yN} \underset{n}{\approx} \frac{r}{sN}$ yerine kısaca $x \underset{n}{\approx} r$ yazabileceğiz. İmpirimitiflik gereği yukarıdaki eşdeğerlik sınıflarının sayısı

$$\varphi_N(n) \coloneqq |\Gamma_0(N) \colon \Gamma_{0,n}(N)|$$

dir. Şimdi bu $\varphi_N(n)$ sayısını, yani indeksi bulalım.

Önerme 2.6.1. $A=\{n \in N \mid n|N\}$ olsun. Bu takdirde $\varphi_N(n)\colon A \longrightarrow \mathbb{N}$ fonksiyonu bir çarpımsal fonksiyondur.

İspat: $n \in \mathbb{N}$ ve $n=kl$, $(k,l)=1$, $k,l>1$ olsun. Eğer $a \underset{n}{\approx} b$ ise kolayca görülür ki $a \underset{k}{\approx} b$ ve $a \underset{l}{\approx} b$ dir.

Tersine $a_1 \underset{k}{\approx} b_1$ ve $a_2 \underset{l}{\approx} b_2$ olduğunu farzedelim. Bu iki bağıntıyı kullanarak $a \underset{n}{\approx} b$ bağıntısını elde edeceğiz. $(k,l) = 1$ olduğundan, $a_1 + kx_1 = a_2 + ly_1$ ve $b_1 + kx_2 = b_2 + ly_2$ olacak şekilde x_1, x_2, y_1, y_2 tamsayıları vardır. Böylece

$$a_1 + kx_1 \underset{n=kl}{\approx} b_1 + kx_2$$

elde ederiz. Böylece denklik sınıflarının sayısı

$$\varphi_N(n) = \varphi_N(k).\varphi_N(l)$$

eşitliğini verir. ■

Şimdi, Önerme 2.6.1 i kullanarak, $n = p^\alpha$,p asal olmak üzere $\varphi_N(n)$ yi hesaplayalım.

Önerme 2.6.2. $N = 2^\alpha, n = 2^\beta, \beta < \alpha$ olsun. Bu takdirde, φ Euler fonksiyonu olmak üzere,

$$\varphi_N(2^\beta) = \begin{cases} 1, & \beta \leq 3 \\ \dfrac{\varphi(2^\beta)}{4}, & \beta > 3 \end{cases}$$

dir.

İspat: $\beta \leq 3$ olsun. Gösterelim ki, bütün $\frac{a}{b2^\alpha}$ sayıları $\underset{2^\beta}{\approx}$ altında denktir. Yani, $\frac{a}{b2^\alpha} \underset{2^\beta}{\approx} \frac{c}{d2^\alpha}$ dir. Bunun için $a^2 \equiv c^2 \; mod \; 2^\beta$ olduğunu gösterelim. a ve c tek sayılar olduğundan $a = 2a_0 - 1, c = 2c_0 - 1$ yazılabilecek şekilde $a_0, c_0 \in \mathbb{N}$ vardır. Buradan,

$$a^2 - c^2 = 4{a_0}^2 - 4a_0 + 1 - 4{c_0}^2 + 4c_0 - 1$$

$$= 4({a_0}^2 - {c_0}^2) - 4(a_0 - c_0)$$

$$= 4\left(\underbrace{{a_0}^2 - a_0}_{çift} - \underbrace{{c_0}^2 + c_0}_{çift}\right) \equiv 0 \; mod \; 2^3$$

tür. Böylece $a^2 \equiv c^2 \; mod \; 2^\beta$ dır. Yani $\beta \leq 3$ olması halinde $\varphi_{2^\alpha}(2^\beta) = 1$ dir.

Şimdi de $\beta > 3$ olsun. Bu durumda 2^β ile aralarında asal olan (pozitif) sayıların kümesi $\{1,3,5,\ldots,2^\beta - 1\}$ olur ki bunların sayısı $\varphi(2^\beta)$ tanedir. Böylece $\frac{1}{2^\alpha}, \frac{3}{2^\alpha}, \ldots, \frac{2^{\beta-1}-1}{2^\alpha}$ sayıları arasından $\underset{2^\beta}{\approx}$ ya göre denk olanları bulalım:

Açıkça, $1 \underset{2^\beta}{\approx} 2^\beta - 1, \ldots, l \underset{2^\beta}{\approx} 2^\beta - l$ dir. Buradan, $\frac{1}{2^\alpha}, \frac{3}{2^\alpha}, \ldots, \frac{2^\beta-1}{2^\alpha}$ sayıları, ki bunların sayısı açıkça $\frac{\varphi(2^\beta)}{2}$ dir, arasında birbirine denk olanları bulalım: Yine burada $\frac{m}{2^\alpha}$ ile $\frac{2^\beta - m}{2^\alpha}$ sayıları denktir. Gerçekten,

$$m^2 \equiv \left(2^{\beta-1} - m\right)^2 \, mod \, 2^\beta \iff m^2 \equiv 2^{2\beta-2} - m2^\beta + m^2 \;\; mod \, 2^\beta$$

dir. Böylece yukarıdaki sayılar $\frac{1}{2^\alpha}, \frac{3}{2^\alpha}, \ldots, \frac{2^{\beta-2}-1}{2^\alpha}$ olacaktır. Bunların sayısı $\frac{\varphi(2^\beta)}{4}$ tür. Şimdi gösterelim ki bunlar birbirinin sınıfında değildir. Kolaylık için paydaları atalım. Bu durumda $1,3,\ldots,2^{\beta-2} - 1$ elde edilir.Şimdi gösterelim ki bunlardan herhangi ikisi $\underset{2^\beta}{\approx}$ ya göre denk değildir. Farzedelim ki, $m, k \leq 2^{\beta-2} - 1$ ve $2^{\beta-2} - m \underset{2^\beta}{\approx} 2^{\beta-2} - k$

olsun. Bu durumda

$$(2^{\beta-2} - m\,)^2 \equiv \left(2^{\beta-2} - k\right)^2 \, mod \, 2^\beta$$

ve böylece

$$m^2 \equiv k^2 \, mod \, 2^\beta$$

dir. $m, k \leq 2^{\beta-2} - 1,\; 2||(m-k, m+k)$ olduğundan $m^2 \equiv k^2 \, mod \, 2^\beta$, yani $(m-k, m+k) \equiv 0 \, mod \, 2^\beta$ dan $2|m-k$ ve $2^{\beta-1}|m+k$ dır. Ancak, $m + k \leq 2^{\beta-2} - 1 + 2^{\beta-2} - 1 = 2^{\beta-1} - 2$ olduğundan $2^{\beta-1}|m+k$ olamaz. Böylece $m - k = 0$ dır. Yani $m = k$ dır. Sonuç olarak $\frac{1}{2^\alpha}, \frac{3}{2^\alpha}, \ldots, \frac{2^{\beta-2}-1}{2^\alpha}$ sayıları bütün farklı sınıfların temsilcileridir. Böylece ,

$$\varphi_N\left(2^\beta\right) = \frac{\varphi\left(2^\beta\right)}{4}, \quad \beta > 3$$

tür.■

Önerme 2.6.3. $p \geq 3$ asal , $N = p^{\alpha},\ n = p^{\beta}$ olsun. Bu takdirde,

$$\varphi_N\left(p^{\beta}\right) = \frac{\varphi\left(p^{\beta}\right)}{2}$$

dir.

İspat: Yukarıda yaptığımız gibi p^{β} dan küçük ve p ile aralarında asal $1,2,\dots,p-1,\dots p^{\beta}-1$ sayılarını gözönüne alalım. Temsilci olarak alınırsa $l \underset{p^{\beta}}{\approx} p^{\beta}-l$ olduğu açıktır. Bu durumda temsilci sayısı $\frac{\varphi(p^{\beta})}{2}$ ye iner ki, bu sayılar $1,2,\dots,p-1,\dots,\frac{p^{\beta}-1}{2}$ dir. Önerme 2.4.2. de yapıldığı gibi $k,l \leq \frac{p^{\beta}-1}{2},\ (k,p) = (l,p) = 1$ ise $k \underset{p^{\beta}}{\not\approx} l$ olduğunu gösterelim. Aksi halde $k^2 - l^2 \equiv 0\ mod\ p^{\beta}$ ise $k - l = pt_1,\ k + l = pt_2$ olup $p|2k \Longrightarrow p|k$ çelişkisi elde edilir. Dolayısı ile $k - l \equiv 0\ mod\ p^{\beta}$ veya $k + l \equiv 0\ mod\ p^{\beta}$ dır. $k \neq l$ ise bu iki durum söz konusu değildir. Dolayısıyla $k \underset{p^{\beta}}{\not\approx} l$ dir. Böylece,

$$\varphi_N\left(p^{\beta}\right) = \frac{\varphi\left(p^{\beta}\right)}{2}$$

dir.

Şu ana kadar yaptıklarımızı aşağıdaki önerme ile özetleyebiliriz:

Önerme 2.6.4. $n, N \in \mathbb{N},\ n|N$ ve $n = 2^{\alpha_1}3^{\alpha_2}{p_3}^{\alpha_3}\dots{p_r}^{\alpha_r}$ de n nin asal çarpanlarına ayrılışı olsun. Bu takdirde φ Euler fonksiyonu olmak üzere,

$$\varphi_N(n) = \begin{cases} \dfrac{1}{2^{r-1}}\varphi(3^{\alpha_2}{p_3}^{\alpha_3}\dots{p_r}^{\alpha_r})\,, & \alpha_1 \leq 3 \\ \dfrac{1}{2^{r+1}}\varphi(n)\ , & \alpha_1 > 3 \end{cases}$$

dir. ■

Sonuç 2.6.5. $n, N \in \mathbb{N},\ n|N$ olsun. Bu takdirde $\varphi_N(n) = 1$ olması için gerek ve yeter şart $n|24$ tür.

İspat: Yukarıdaki önermeden sonuç açıktır.

Sonuç 2.6.6. $n, N \in \mathbb{N},\ n|N$ olsun. Bu takdirde $n|24$ olması için gerek ve yeter şart $\Gamma_{0,n}(N) = \Gamma_0(N)$ olmasıdır. ■

Not: [16] daki Lemma 3.1. yukarıdaki önermenin basit bir sonucudur.

2. 7. $\Gamma_0(N)$ nin $\widehat{\mathbb{Q}}(N)$ üzerindeki Alt Yörüngesel Grafları

$(\Gamma_0(N), \widehat{\mathbb{Q}}(N))$ transitif permütasyon grubu olduğundan $\Gamma_0(N): \widehat{\mathbb{Q}}(N) \times \widehat{\mathbb{Q}}(N) \to \widehat{\mathbb{Q}}(N) \times \widehat{\mathbb{Q}}(N)$ hareketini gözönüne alalım. $g \in \Gamma_0(N)$ olmak üzere $g(\alpha, \beta) = (g(\alpha), g(\beta))$ hareketinin yörüngesi $\Gamma_0(N)$ nin alt yörüngeleri adını alır. (α, β) nın yörüngesi $O(\alpha, \beta)$ ile gösterilir. Bu yörüngeden hareketle $G(\alpha, \beta)$ alt yörüngesel grafını oluşturabiliriz. Bu grafın köşeleri $\widehat{\mathbb{Q}}(N)$ nin elemanları; $(a, b) \in O(\alpha, \beta)$ ise $a \to b$ ile gösterilir ve a dan b ye yönlü kenar adını alır. $\Gamma_0(N)$ nin $\widehat{\mathbb{Q}}(N)$ üzerindeki transitifliğinden her $O(\alpha, \beta)$ alt yörüngesi bir $\left(\infty, \frac{a}{bN}\right)$ çifti içerir. Biz burada kolaylık açısından $\left(\infty, \frac{u}{N}\right)$ alacağız. Bu durumda alt yörüngesi $O_{u,N}$ ve karşılık gelen grafı $G_{u,N}$ ile göstereceğiz. Buradan $G_{u,N} = G_{u'N'} \Leftrightarrow N = N'$ ve $u \equiv u' mod\ N$ dir. Bu durumda her bir N için tam $\varphi(N)$ tane farklı alt yörüngesel $G_{u,N}$ grafı vardır.

Önerme 2.7.1. $\frac{x}{yN} \to \frac{r}{sN} \in G_{u,N} : \Leftrightarrow$

i. $r \equiv ux\ mod\ N,\ \ xs - ry = 1$

veya

ii. $r \equiv -ux\ mod\ N,\ \ xs - ry = -1$

dir.

İspat: $\frac{x}{yN} \to \frac{r}{sN} \in G_{u,N}$ olsun. Bu takdirde, $\exists\, T \in \Gamma_0(N)$ öyle ki

$$T\left(\infty, \frac{u}{N}\right) = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix}$$

$$= \begin{pmatrix} a & au + bN \\ cN & cuN + dN \end{pmatrix} = \begin{pmatrix} x & r \\ yN & sN \end{pmatrix}$$

dir. Burada ya $a = x,\ au + bN = r,\ cN = yN,\ cu + d = s$ ve buradan $r \equiv ux\ mod\ N$ ve determinanttan $xs - ry = 1$, ya da $a = -x,\ au + bN = r,\ cN = -yN \Longrightarrow r \equiv -ux\ mod\ N$ ve yine determinanttan $xs - yr = -1$ dir.

İspatın diğer kısmını sadece $r \equiv ux \bmod N,\ xs - yr = 1$ olması halinde yapalım. $r \equiv ux \bmod N \Longrightarrow r = ux + bN$ olacak şekilde $b \in \mathbb{Z}$ vardır. $T = \begin{pmatrix} x & \frac{r-ux}{N} \\ yN & s-uy \end{pmatrix} \in \Gamma_0(N)$ dir ve açıkça $T(\infty) = \frac{x}{yN}$ ve $T\binom{u}{N} = \frac{r}{sN}$ dir.■

Gösterim. $F_{u,N}$ ile $G_{u,N}$ nin köşeleri $[\infty] = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ bloğunda olan alt grafını göstereceğiz.

Önerme 2.7.2. $\frac{x}{yN} \to \frac{r}{sN} \in G_{u,N}$ ve $\frac{u}{N} \in [\infty]$ olsun. Bu takdirde $\frac{x}{yN}$ ve $\frac{r}{sN}$ aynı bloktadır.

İspat: Önerme 2.5.2. den $r \equiv \pm ux \bmod N$ dir. Buradan $r \equiv \pm ux \bmod n$ ve böylece $r^2 \equiv u^2x^2 \bmod n$ dir. $\frac{u}{N} \in [\infty]$ olduğundan $u^2 \equiv 1 \bmod n$ dir. Böylece $r^2 \equiv x^2 \bmod n$ elde edilir. Yani, $\frac{x}{yN} \underset{n}{\approx} \frac{r}{sN}$ dir.■

Önerme 2.7.3. $x \le n,\ (x,n) = 1$ olsun. $x^2 \equiv 1 \bmod n$ olan x lerin sayısı, $n = 2^{\alpha_1}{p_2}^{\alpha_2} \dots {p_l}^{\alpha_l}$ ve $\beta = \begin{cases} 2, & \alpha_1 \ge 3 \\ 1, & \alpha_1 = 2 \\ 0, & \alpha_1 = 1 \end{cases}$ olmak üzere, $\eta(n) = 2^{\beta+l-1}$ dir.

İspat: İlk önce η nın çarpımsal olduğunu gösterelim. $n = n_1n_2$ ve $(n_1,n_2) = 1$ olsun. Bu durumda, $x^2 \equiv 1 \bmod n \Longleftrightarrow x^2 \equiv 1 \bmod n_1,\ x^2 \equiv 1 \bmod n_2$ dir. Önerme 2.4.1. in ispatındaki gibi η fonksiyonu çarpımsaldır.

a. 1) $n = 2^\alpha,\ \alpha > 3$ olsun. Bu durumda, $x \le n$ ve $(x,n) = 1$ ve de $x^2 \equiv 1 \bmod n$ olan x sayıları $1, 2^{\alpha-1} - 1, 2^{\alpha-1} + 1, 2^\alpha - 1$ dir. Gerçekten, $x^2 \equiv 1 \bmod n \Longrightarrow (x-1)(x+1) \equiv 0 \bmod (n = 2^\alpha)$.Açıkça$(x-1, x+1) = 2$. Bu durumda $x = 1,\ 2^{\alpha-1} - 1, 2^{\alpha-1} + 1, 2^\alpha - 1$ elde edilir ki bunlar 2^β tanedir.

2) $\alpha \le 3$ ise $(x,n) = 1$ olan her x için $x^2 \equiv 1 \bmod n$ dir.

b. $n = p^\alpha,\ p \ge 3$ olsun. Bu durumda $x^2 \equiv 1 \bmod p^\alpha$ olan x sayıları $1, p^\alpha - 1$ dir. Gerçekten $p|x-1$ ve $p|x+1$ olsa, $p|1-x,\ p|x+1$ den $p|2$ çelişkisi elde edilir. Bu durumda, ya $x - 1 \equiv 0 \bmod p^\alpha$ veya $x + 1 \equiv 0 \bmod p^\alpha$ dır. Buradan $x = 1$ ve $x = p^\alpha - 1$ dir. Böylece $\eta(p^\alpha) = 2$ dir. Bu durumda, $n = 2^{\alpha_1}{p_2}^{\alpha_2} \dots {p_l}^{\alpha_l}$, n nin asal çarpanlarına ayrılışı olmak üzere,

$$\eta(n) = \eta(2^{\alpha_1})\eta({p_2}^{\alpha_2}) \dots \eta({p_l}^{\alpha_l})$$

$$= 2^{\beta}.\ \underbrace{2 \dots 2}_{l-1\ tane} = 2^{\beta+l-1}$$

dir.

Önerme 2.7.4. $n = 2^{\alpha_1} {p_2}^{\alpha_2} \dots {p_l}^{\alpha_l} \in \mathbb{N}$ olsun. $(x, n) = 1$ olan her x için $x^2 \equiv 1\ mod\ n$ ancak ve ancak $n | 2^3 . 3$ tür.

İspat: $x \leq n$ ve $(x, n) = 1$ olan $x \in \mathbb{N}$ lerin sayısı, φ Euler fonksiyonu olmak üzere,

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = 2^{\alpha_1 - 1} {p_2}^{\alpha_2 - 1} \dots {p_l}^{\alpha_l - 1} (p_2 - 1) \dots (p_l - 1) = 2^{\beta+l-1}$$

dir. $\alpha_1 \geq 3$ ise $\eta(n) = 2^{l+1} = 2^{\alpha_1 - 1} {p_2}^{\alpha_2 - 1} \dots {p_l}^{\alpha_l - 1} (p_2 - 1) \dots (p_l - 1)$ dir. Böylece $\alpha_1 = 3$; $\alpha_2 = \cdots = \alpha_l = 1$ ve $p_2 - 1 \dots p_l - 1 | 2$ olmak zorundadır. Bu durumda, $l = 2$ ve $p_2 = 3$ olur. Böylece, $n | 2^3 . 3$ elde edilir. $\alpha_1 \leq 2$ durumu benzer şekilde gösterilir.

$n | 2^3 . 3$ için $x^2 \equiv 1\ mod\ n$ olma durumu Önerme 2.5.3. te gösterildi.

2.8. $F_{u,N}$ Grafı

Teorem 2.8.1. $\frac{x}{yN} \to \frac{r}{sN} \in F_{u,N} \iff$

i. $r \equiv ux\ mod\ N,\ \ xs - ry = 1$

veya

ii. $r \equiv -ux\ mod\ N,\ \ xs - ry = -1$

dir.

İspat: Önerme 2.7.1. de ispatlandı.

Not: G. Jones, D. Singerman ve Wicks in çalışmasında graflar en fazla üçgen içerebiliyorlardı [10]. Ancak, burada $n \nmid 24$ aldığımızda $F_{u,N}$ de bir üçgen içermediği aşağıdaki teorem ile verilecektir.

Teorem 2.8.2. $F_{u,N}$ grafı üçgen içermez.

İspat: Farzedelim ki $F_{u,N}$ bir $a \to b \to c \to a$ üçgeni içersin. Bu durumda $\Gamma_{0,n}(N)$ nin transitifliğinden $a = \infty$ ve $b = \frac{u}{N}$ alabiliriz. Bu durumda Teorem 2.8.1. den

$$\infty = \frac{1}{0} \to \frac{u}{N} \to \frac{u \pm 1}{N} \to \infty$$

elde edilir. Ancak köşeler $[\infty]$ bloğunda olduğunda $u^2 \equiv 1 \, mod \, n$ ve $(u \pm 1)^2 \equiv 1 \, mod \, n$ dir. Üçgenin var olması $u^2 \pm u + 1 \equiv 0 \, mod \, N$ olması demektir. Bu durumda, $u^2 \equiv 1 \, mod \, n$ den $2 \pm u \equiv 0 \, mod \, n$ dir. Böylece,

$$(u \pm 1)^2 \equiv 1 \, mod \, n \Longrightarrow u^2 \pm 2u + 1 \equiv 1 \, mod \, n \Longrightarrow 1 \pm 2u \equiv 0 \, mod \, n$$

$\Longrightarrow n|2 \pm u$ ve $n|1 \pm 2u$

dir. $n|2 + u$ ve $n|1 + 2u$ olduğunda $n|4 + 2u$ ve $n|1 + 2u$ dan $n|3$ elde edilir. Ancak biz $n \nmid 24$ almıştık. Benzer şekilde, $n|2 - u$ ve $n|1 - 2u$ olduğunda $n|4 - 2u$ ve $n|1 - 2u$ dan yine $n|3$ elde edilir. Böylece $F_{u,N}$ üçgen içermez. ■

Teorem 2.8.3. $n \nmid 24$, $n|N$ olsun. Bu takdirde, $F_{u,N}$ grafı bir ormandır.

İspat: Teorem 2.8.2. ve [2] den ispat tamamlanır.

Teorem 2.8.4. $n \nmid 24$, $n|N$ olsun. Bu takdirde $F_{u,N}$ grafı bağlantısızdır.

İspat: [10] daki Teorem 5.10. ispatı verir.

Teorem 2.8.5. $n \nmid 24$, $n|N$ olsun. $\Gamma_{0,n}(N)$ 3. mertebeden bir eliptik eleman içermez.

İspat: Aksine $\Gamma_{0,n}(N)$ 3. mertebeden bir eliptik eleman içersin. Bu durumda $\Gamma_{0,n}(N)$ de $T = \begin{pmatrix} a & b \\ cN & \pm 1 - a \end{pmatrix}$ gibi bir eleman vardır. $\begin{pmatrix} a & b \\ cN & 1 - a \end{pmatrix}$ alalım. Bu durumda $a(1 - a) - bcN = 1$ den $a - a^2 \equiv 1 \, mod \, N$ dir. Buradan, $a - a^2 - 1 \equiv 0 \, mod \, n$ dir. Böylece $a^2 - a + 1 \equiv 0 \, mod \, n$ dir. $a^2 \equiv 1 \, mod \, n$ den $-a + 2 \equiv 0 \, mod \, n$ dir. Dolayısıyla $n|2 - a$ dır. Diğer taraftan $(1 - a)^2 \equiv 1 \, mod \, n$ den $1 - 2a + a^2 \equiv 1 \, mod \, n \Longrightarrow -2a + a^2 \equiv 0 \, mod \, n$ dir. $a^2 \equiv 1 \, mod \, n$ den $-2a + 1 \equiv 0 \, mod \, n$ dir. Böylece, $n| -2a + 1$ dir. Dolayısıyla $n| -2a + 1$ ve $n|2 - a$ dır. Böylece, $n|3$ elde edilir. Bu hipotezle çelişir. Böylece $\Gamma_{0,n}(N)$ de 3. mertebeden bir eliptik eleman yoktur. ■

3. İRDELEME

Gareth A. Jones, David Singerman ve K. Wicks'in 1991 yılında yayınlanan " The Modular Group and Generalized Farey Graph" adlı çalışmasında alty örüngesel graflar ve bu graflardaki devre uzunlukları incelenmiştir [9]. Ioannis Panagioti Ivrissimitzis tarafından 1998 yılında yapılan "Congruence Subgroups of Hecke Grops and Regular Dessins" adlı doktora tezinde $\lambda_q = 2cos\frac{\pi}{q}\ , q \geq 3$ olmak üzere $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix}$ elemanları tarafından üretilen Hecke gruplarının $\lambda = 4$ ve 6 olması durumunda kongrüans altgruplarının normalliyenlerini hesaplamıştır. Ayrıca $\lambda = 5$ olması durumunda normalliyenin ne olabileceği konusunda bir konjektür bırakmıştır [8]. Daha sonra S. Uzun'un 2003 yılında tamamladığı doktora tezinde ise bu konjektür I idealinin $\mathbb{Z}[\lambda]$ nın bir asal ideali olması durumunda çözümü yapılmıştır [25]. 2005 yılında Kurt Ludwick tarafından yapılan "Congruence Restricted Modular Forms" adlı çalışmada $\Gamma_0(N)$ kongrans altgrubuna birtakım kısıtlmalar getirilerek elde edilen $\Gamma_{0,n}(N)$ kısıtlı kongrüans alt grupları incelenmiştir [16].

Bu tez çalışmasında dört problem ele alınmıştır. Birinci problemde Ioannis Panagioti Ivrissimitzis tarafından doktora tezinde konjektür olarak bırakılan problem, $I \subset \mathbb{Z}[\lambda]$ idealinin bir karesiz ideal olması durumunda ispatı yapıldı. İkinci ve üçüncü problemlerde ise $\Gamma_0^2(N)$ ve $\Gamma_0^3(N)$ gruplarının sırasıyla Γ^2 ve Γ^3 teki normalliyenleri hesaplandı ve bunlarla ilgili sonuçlar elde edildi. Son olarak $n|N$ olmak üzere $\Gamma_{0,n}(N)$ kısıtlı kongrüans alt grubunun $\Gamma_0(N)$ kongrans alt grubundaki indeksi hesaplandı ve $\Gamma_{0,n}(N)$ grubunun $\widehat{\mathbb{Q}}(N)$ üzerindeki alt yörüngesel grafları incelendi.

4. SONUÇLAR

Yaptığımız çalışmada elde edilen başlıca sonuçlar şunlardır:

1. n pozitif bir tamsayı olmak Γ^k deki herhangi iki elemanın hangi şartlarda $\Gamma_0^k(n)$, $(k = 2,3)$ nin aynı yansınıfında olacağı gösterildi. (Önerme 2.2.3.)
2. I', $\mathbb{Z}[\lambda_q]$ nun bir karesiz ideali olması durumunda $H_0^5(I)$ kongrüans altgrubunun H^5 Hecke grubundaki normalliyeni hesaplandı. (Teorem 2.3.2.)
3. I, $\mathbb{Z}[\lambda]$ nın bir karesiz ideali olmak üzere $N_{\boldsymbol{H}^5}\left(H_0^5(I)\right) = H_0^5(I)$ olduğu gösterildi. (Sonuç. 2.3.4.)
4. $n = 2^\alpha 3^\beta n_0 \geq 1$, $(n_0, 6) = 1$ olması halinde $N_{\Gamma^2}\left(\Gamma_0^2(n)\right)$, $\Gamma_0^2(n)$ nin Γ^2 deki normalliyeni hesaplandı ve bununla ilgili sonuç elde edilidi. (Teorem 2.4.7. ve Sonuç 2.2.8.)
5. $n = 2^\alpha 3^\beta n_0 \geq 1$, $(n_0, 6) = 1$ olması halinde $N_{\Gamma^3}\left(\Gamma_0^3(n)\right)$, $\Gamma_0^3(n)$ nin Γ^3 deki normalliyeni hesaplandı ve bununla ilgili sonuç elde edilidi. (Teorem 2.4.9 ve Sonuç 2.4.10.)
6. $\varphi_N(n)$ fonksiyonunun bir çarpımsal fonksiyon olduğu gösterildi. (Önerme 2.6.1.)
7. $N = 2^\alpha, n = 2^\beta$, $\beta < \alpha$ ve $p \geq 3$ asal , $N = p^\alpha$, $n = p^\beta$ olmak üzere $\varphi_N\left(2^\beta\right)$ fonksiyonu ayrı ayrı hesaplandı. Ayrıca bunlar yardımıyla $n, N \in \mathbb{N}$, $n|N$ ve $n = 2^{\alpha_1} 3^{\alpha_2} {p_3}^{\alpha_1} \ldots {p_r}^{\alpha_r}$ için $\varphi_N(n)$ fonksiyonu belirlendi (Önerme 2.6.2. , Önerme 2.6.3. ve Önerme 2.6.4.)
8. $\Gamma_0(N)$ grubunun $\widehat{\mathbb{Q}}(N)$ üzerindeki altyörüngesel grafları incelenmiş ve bunlarla ilgili kenar şartı verildi. (Teorem 2.7.1.)
9. $\Gamma_0(N)$ grubunun $\widehat{\mathbb{Q}}(N)$ üzerindeki alt yörüngesel graflarının üçgen içermediği ayrıca $n \nmid 24$, $n|N$ olduğu durumlarda bir orman olduğu, bağlantısız olduğu ve 3. mertebeden eliptik eleman içermediği gösterildi. (Teorem 2.8.2. , Teorem 2.8.3. , Teorem 2.8.4. ve Teorem 2.8.5.)

5. ÖNERİLER

1. I', $\mathbb{Z}[\lambda_q]$ bir ideali olmak üzere $(2, I') = 1$ ve $I = (2)^{\alpha} I'$ olsun. Bu takdirde, $H_0^5(I)$ nın H^5 teki normalliyeni hesaplanabilir.
2. $n \nmid N$ olması durumunda $\Gamma_{0,n}(N)$ nin $\Gamma_0(N)$ deki indeksi hesaplanabilir.
3. $n \nmid N$ olması durumunda $\Gamma_{0,n}(N)$ nin $\widehat{\mathbb{Q}}(N)$ üzerindeki alt yörüngesel grafları incelenebilir ve bu grafların bağlantılılığı, eliptik eleman içerip içermediği ve ayrıca orman olup olmadığı araştırılabilir.

Bu 3 problemde oldukça düşündürücü problemler olup çözülmeleri halinde literatüre önemli katkıları olacaktır.

6. KAYNAKLAR

1. Akbaş, M., The Normalizer of Modular Subgroups, Ph.D. thesis, University of Southampton, 1989.

2. Akbaş, M., On Suborbital Graphs for The Modular Group, Bull. London Math. Soc., 33 2001 647-652.

3. Akbaş, M. and Singerman, D., The normaliser of $\Gamma_0(\mathrm{N})$ in $PSL(2,\mathbb{R})$, Glasgov Mathematical Journal, 32 1990 317-327.

4. Alaca, Ş. and Williams, K.S., Introductory Algebraic Number Theory, Cambridge University Press, 2004.

5. Biggs, N.L. and White, A.T., Permutation groups and combinatorial structures, London Math. Soc. Lecture Notes 33, Cambridge University Press, Cambridge, 1979.

6. Chan, S.P., Lang, M.L., Lim, C.H. and Tan, S.P., The invariants of the Congruence Subgroups $\mathrm{G}_0(\beta)$ of the Hecke Group G_5, Illinois Journal Of Mathematics, 38, 4 1994 636-652.

7. Hecke, E., Über die Bestimmung Dirichletcher Reichen durch ihre Funktionalgleichungen, Math. Ann., 112 1936 664-699.

8. Ivrissimtzis, I.P., Congruence subgroups of Hecke groups and regular dessins, Ph D. Thesis, University of Southampton, 1998.

9. Jones, G.A. and Singerman, D., Complex Functions : An Algebraic and Geometric Viewpoint, Cambridge University Press, Cambridge, 1987.

10. Jones , G.A., Singerman, D. ve Wicks, K., The Modular Group and Generalized Farey Graphs, London Math. Soc. Lecture Notes, CUP, Cambridge, 160 1991 316–338.

11. Lang, M.L. and Tan, S.P., Normalizers of The Congruence Subgroups of The Hecke Groups G_5 II, Proceedings of The American Mathematical Society, 128, 8 2000 2271-2280.

12. Lang, M.L., Lim, C.H. and Tan, S.P., Principal Congruence Subgroups of the Hecke Groups, Journal of Number Theory, 85 2000 220-230.

13. Lang, M.L., Normalizers of the Congruence Subgroups of the Hecke Groups G_4 and G_6, Journal of Number Theory, 90 2001 31-43.

14. Lang, M.L., The Structure of the Normalizers of the Congruence Subgroups of the Hecke Group G_5, Bull. London Math. Soc., 39 2007 53-62.

15. Lang, M.L., Lim, C.H. and Tan, S.P., Independent Generators For Congruence Subgroups of Hecke Groups, Mathematische Zeitschrift, 220 1995 569-594.

16. Ludwick, K., Congruence Restricted Modular Forms, The Ramanujan Journal, 9 2005 341-356.

17. Ogg, A.P., Automorphismes des Courbes Modulaires, Seminaire Delange-Pisot, Poitou, 7 1974.

18. Rankin, R.A., Modular Forms and Functions, Cambridge University Press, 1977.

19. Rose, J.S., A Course on Group Theory, Cambridge University Press, Cambridge, 1978.

20. Rosen, D., An Arithmetic Characterization of the Parabolic Points of $G(2\, cos\frac{\pi}{5})$, Glasgow Mathematical Journal 6 1963 88-96.

21. Rosen, D., The Substitutions of the Hecke Group $\Gamma\left(2\cos\frac{\pi}{5}\right)$, Arch. Math., 46 1986 533-538.

22. Rosen, D., The Diaphantine Equation $ax + by = c$ In $\mathbb{Q}\sqrt{5}$ and Other Number Fields, Pacific Journal of Mathematics, 119, 2 1985 465-472.

23. Schoeneberg, B., Elliptic Modular Functions, Springer Verlag, Berlin, 1974.

24. Sims, C.C., Graphs and Finite Permutation Groups, Mathematische Zeitschrift, 95 1967 76-86.

25. Uzun, S., H^5 Hecke Grubunun Kongrüans Alt Grupları ve $H_0^5((2)^{\alpha}I')$ nin H^5 teki Normalliyeni, Doktora Tezi, Karadeniz Teknik Üniversitesi, 2003.

ÖZGEÇMİŞ

Zeynep Şanlı 1988 yılında Rize/Pazar'da doğdu. İlk, orta ve lise öğrenimini Pazar'da tamamladı. 2007-2010 yılları arasında Atatürk Üniversitesi Fen Fakültesi Matematik bölümünde lisans eğitimini tamamladı. 2010-2012 yıllları arasında Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim dalında Yüksek Lisansını derecesini aldı ve aynı enstitüde Doktora eğitimine başladı. 2013 yılında K.T.Ü Fen Fakültesi Matematik Bölümüne Araştırma Görevlisi olarak atandı. Evli ve bir çocuk sahibi olup, iyi derecede İngilizce bilmektedir.

Yayınlar

1. B.Ö.Güler, T.Kör, **Z. Şanlı,** Solutions to some congruence equations via suborbital graphs, Springer Plus, 5/1327-1337, 2016.
2. T.Kör, B.Ö.Güler, **Z. Şanlı,** Suborbital graphs for the Atkin-Lehner group, Turkish Journal of Mathematics, 10.3906/Mat-1602-10, 2016.
3. T.Köroğlu, B.Ö.Güler **Z. Şanlı,** Some Generalized Suborbital Graphs, 7 90-95, 2017.
4. **Z. Şanlı**, T.Köroğlu, B.Ö.Güler, Suborbital graphs of a power subgroup of the modular group, New Trends in Mathematical Sciences, **6**, No. 1, 139-144, 2018.
5. **Z. Şanlı**, T.Köroğlu, B.Ö.Güler, The Normalizer of $\Gamma_0^k(n)$, Mathematical Methods in the Applied Sciences, DOI: 10.1002/mma.5401, 2018.
6. **Z. Şanlı**, T.Köroğlu, New Conformable Fractional Hermite Hadamard Type Inequalities For Harmonically Convex Functions, Journal of Mathematical Analysis, Kabul Edildi, 2018.
7. **Z. Şanlı**, T.Köroğlu, M. Kunt, Improved Hermite Hadamard Type Inequalities for Harmonically Convex Functions via Katugampola Fractional Integrals, Communications Faculty of Sciences University of Ankara Series A1 Mathematics and Statistics, Kabul Edildi, 2018.
8. **Z. Şanlı**, Some midpoint type inequalities for Riemann Liouville fractional integrals, An International Journal, Kabul Edildi, 2018.