

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

BAZI KONGRÜANS DENKLEMLERİNİN ÇÖZÜMÜ
İÇİN ÇİZGE TEMELLİ BİR YAKLAŞIM

YÜKSEK LİSANS TEZİ

Hacer FENNİBAY

ŞUBAT 2021
TRABZON



KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

BAZI KONGRÜANS DENKLEMLERİNİN ÇÖZÜMÜ İÇİN
ÇİZGE TEMELLİ BİR YAKLAŞIM

Hacer FENNİBAY

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünde
“YÜKSEK LİSANS (MATEMATİK)”
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih :18.01.2021

Tezin Savunma Tarihi :16.02.2021

Tez Danışmanı : Prof. Dr. Bahadır Özgür GÜLER

Trabzon 2021

ÖNSÖZ

Yüksek lisans öğrenimim boyunca, tez konusunun belirlenmesinden yapılan çalışmaların tamamlanmasına kadar geçen süreçte yardımlarını esirgeyemeyen ve zorlandığım dönemlerde göstermiş olduğu destek ve sabır için danışman hocam sayın Prof. Dr. Bahadır Özgür GÜLER' e sonsuz teşekkürlerimi, saygılarımı ve şükranlarımı sunarım.

Lisans ve yüksek lisans öğrenim sürecim boyunca üzerimde emek ve destekleri büyük olan sayın Prof. Dr. Mehmet AKBAŞ ve Prof. Dr. Zameddin İSMAİLOV hocalarıma ve Karadeniz Teknik Üniversitesi'ndeki diğer tüm saygıdeğer hocalarıma çok teşekkür ederim. Ayrıca öğrenimim boyunca gönül yoldaşlığı yağıtığım, her zaman yanımda olan canım dostum Esra ERTEM AYDIN başta olmak üzere; Burak ÇELİKTUTAN, Tuğba GÜDÜK ve adını buraya sığdıramayacağım bütün dostlarıma ve arkadaşlarıma teşekkür ederim.

Son olarak beni büyüten, bugünlere gelmemde en çok emeği olan, tüm hayatım boyunca beni maddi ve manevi her yönden destekleyen sevgili anneme, babama, abilerim ve ablama sonsuz teşekkürlerimi sunarım.

Hacer FENNİBAY

Trabzon, 2021

TEZ ETİK BEYANNAMESİ

Yüksek Lisans Tezi olarak sunduğum “Bazı Kongrüans Denklemlerinin Çözümü İçin Çizge Temelli Bir Yaklaşım” başlıklı bu çalışmayı baştan sona kadar danışmanım Prof. Dr. Bahadır Özgür GÜLER’in sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuvarlarda 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.

16/02/2021

Hacer FENNİBAY

İÇİNDEKİLER

	<u>Sayfa No</u>
ÖNSÖZ	III
TEZ BEYANNAMESİ	IV
İÇİNDEKİLER	V
ÖZET	VI
SUMMARY	VII
ŞEKİLLER DİZİNİ	VIII
TABLolar DİZİNİ	IX
SEMBOLLER DİZİNİ	X
1. GENEL BİLGİLER	1
1.1. Giriş	1
1.2. Gruplar ve Topolojik Gruplar	1
1.3. Öklidyen Olmayan Kristal Yapılı Gruplar	7
1.4. $PSL(2, \mathbb{R})'$ deki Parabolik ve Eliptik Alt Grupları	8
1.5. Ayırık Gruplar ve Riemann Yüzeyleri	9
1.6. Modüler Grup	10
1.7. $\Gamma(N)$ ve $\Gamma_0(N)$ Kongrüans Alt Grupları	15
1.8. $\Gamma_B(N)$ Normalliyenin Yapısı	16
1.9. Kuadratik Kalanlar	17
2. YAPILAN ÇALIŞMALAR	28
2.1. Transitif Hareketin Sağlandığı Köşe Kümelerinin Belirlenmesi	28
2.1.1. İmp primitif Hareket ve Blok Şartı	28
2.1.2. Kenar Şartının Elde Edilmesi	28
2.1.3. Devrelerin Elde Edilmesi	29
2.2. $N = 2^6 \cdot p^2$	31
2.3. $N = 2^4 \cdot 3^2 \cdot p^2$	37
2.4. $N = 2^6 \cdot 3^2 \cdot p^2$	44
3. İRDELEME	52
4. SONUÇLAR	53
5. ÖNERİLER	54
6. SKAYNAKLAR	55
ÖZGEÇMİŞ	

Yüksek Lisans Tezi

ÖZET

BAZI KONGRÜANS DENKLEMLERİNİN ÇÖZÜMÜ İÇİN
ÇİZGE TEMELLİ BİR YAKLAŞIM

Hacer FENNİBAY

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı
Danışman: Prof. Dr. Bahadır Özgür GÜLER
2021, 57 Sayfa

Bu tez çalışmasında $Nor(N)$ ' nin üçgen grup olmasını sağlayan üç durum ayrı ayrı incelenmiştir. Bunun için her durumda

1. transitif hareketin sağlandığı köşe kümeleri belirlendi,
2. imprimitif hareketi mümkün kılan altgrubun belirlenmesiyle iki köşenin aynı blokta olma şartları belirlendi,
3. ikili transitif özelliği; kenar şartları elde edildi,
4. kenar şartının yardımıyla altgraflarda ne tür devreler olduğu araştırıldı.

Bu çalışma iki ana bölümden meydana geldi. Birinci bölümde problemimizle ilişkili cebir ve sayılar teorisinden bazı temel bilgiler özetlenmeye çalışıldı. Bölüm sonunda analiz ve cebir arasında köprü kuran problem bir örnek olarak gösterildi. İkinci bölümde altyörüngesel graflar yordamıyla metot ve hesaplamalarımız ortaya kondu.

Anahtar Kelimeler: Modüler grup, Alt yörüngesel graflar, Normalliyen

Master Thesis

SUMMARY

A GRAPH-BASED APPROACH FOR THE SOLUTION OF SOME CONGRUENCE EQUATIONS

Hacer FENNİBAY

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Mathematics Graduate Program
Supervisor: Prof. Dr. Bahadır Özgür GÜLER
2021, 57 Pages

In this thesis, three cases that make $Nor(N)$ is a triangular group were examined separately. For this, in each case concerned that

1. vertex sets where transitive action is provided were determined,
2. the conditions for the two corners to be in the same block by determining the subgroup that makes imprimitive movement is possible, were determined,
3. double transitive properties which means that edge condition were founded,
4. what types of circuits are in the subgraph using the edge condition are investigated.

The present study consists of two main chapters. In the first part, we try to summarize some general knowledge which are related our problem from algebra and number theory. At the end of the section we show an example which uses a bridge between algebra and analysis. In the second part we expressed our method and calculations via suborbital graphs.

Key Words: Modular group, Suborbital graphs, Normalizer

ŞEKİLLER DİZİNİ

Sayfa No

Şekil 1.	Γ nın F temel bölgesi	14
----------	--------------------------------------	----



TABLÖLAR DİZİNİ

Sayfa No

Tablo 1.	$2^6.p^2$ için bölen sayısı	31
Tablo 2.	$2^6.p^2$ için $(d, N/d)$ –durumları	31
Tablo 3.	$2^4.3^2.p^2$ için bölen sayısı	37
Tablo 4.	$2^4.3^2.p^2$ için $(d, N/d)$ –durumları	38
Tablo 5.	$2^6.3^2.p^2$ için bölen sayısı	44
Tablo 6.	$2^6.3^2.p^2$ için $(d, N/d)$ –durumları	45



SEMBOLLER DİZİNİ

$\mathbb{N}$	: Doğal sayılar kümesi
$\mathbb{C}$	: Kompleks sayılar kümesi
$\mathbb{C}_\infty$	: Genişletilmiş kompleks sayılar kümesi
$\mathbb{U}$	: Üst yarı düzlem
$\mathbb{R}$	: Reel sayılar kümesi
$\mathbb{Q}$	: Rasyonel sayılar kümesi
$\hat{\mathbb{Q}}$	: Genişletilmiş rasyonel sayılar kümesi
Γ	: Modüler grup
$\mathbb{Z}$	: Tam sayılar kümesi
$PSL(2, \mathbb{R})$	: Reel katsayılı lineer kesirli dönüşümlerin grubu
Gx	: x noktasının G yörüngesi
G_x	: x noktasının G deki sabitleyeni
$\approx$	: G – invariant denklik bağıntısı
$a \rightarrow b$	: a dan b ye (yönlendirilmiş) bir kenar
$a b$	: a sayısı b sayısını böler
$ G:H $	: G nin H içindeki indeksi
∞	: Sonsuz
$[\infty]$	: Sonsuz Bloğu
$\Gamma_B(N)$	: $\Gamma_0(N)$ nin $PSL(2, \mathbb{R})$ deki normalliyeni
$\Gamma_0(N)$	: Modüler Grubun bir kongrüans alt grubu

1. GENEL BİLGİLER

1.1. Giriş

Birçok disiplinde sınıflandırma mevcut yapının daha kolay ele alınmasını, incelenmesini sağlar. Bununla birlikte alt disiplinler arası bağlantı ve linklerin kurulması bir o kadar önemlidir. Literatürde analiz, geometri, cebir ve sayılar teorisinin dahlinin olduğu çok sayıda hibrit çalışma mevcuttur. Örneğin Cebirin Esas Teoremi, kompleks fonksiyonlar teorisinin standart içeriğindeki kavramlardan biridir. Rolle teoreminin kimi cebirsel denklemlerin köklerinin araştırılmasındaki rolü, ortalama değer teoreminin pek çok eşitsizliğin doğruluğunu kanıtlamasındaki rolü bu yaklaşıma örnek gösterilebilir. Bu tez çalışmasında yine kompleks fonksiyonlar teorisinin standart içeriğinde yer alan doğrusal kesirli lineer dönüşümler(Möbiüs dönüşümleri) temel alınacaktır. Möbiüs dönüşümlerinin bazı özel alt sınıflarının genişletilmiş rasyonel sayılar kümesi üzerindeki grup hareketinin neticesinde ortaya çıkan çizgeler ve bunların Farey çizgeleri ile olan ilişkisinin beraberinde nasıl kimi kongrüans denklemlerinin çözümlerini ürettiğini göreceğiz.

Birinci bölümde, grup, normal altgrup, topolojik grup kavramları verilecek, ardından permütasyon grupları, Fuchs grupları, modüler grup ve kongrüans alt grupları detaylandırılacaktır. Sonrasında sayılar teorisindeki iki karesel toplamı problemi tanıtılacak ve B. Fine'nın çözüm için verdiği metot ve bunun nasıl geliştirildiği paylaşılacaktır. Buradaki metot Modüler grubun grup yapısının özelliklerini kullanması açısından önemlidir. Bu tez çalışmasında da benzer yaklaşımla, çözümleri normalliyenin grup yapısı verecektir. İkinci bölümde çizgelerin nasıl elde edildiğine dair metot verilip ardından bunun normalliyene uygulanması ve elde edilen sonuçlar verilmiştir.

1.2. Gruplar ve Topolojik Gruplar

Tanım 1.2.1.

$G \neq \emptyset$ olan bir küme olsun.

i) $G \times G$ kümesi üzerinde tanımlı ve G 'de değerler alan bir fonksiyona G üzerindeki bir ikili işlem denir.

$*$: $G \times G \rightarrow G$ tanımlı bir ikili işlem olmak üzere $(g_1, g_2) \in G \times G$ 'nin bu işlem altındaki görüntüsü $*(g_1, g_2) = g_1 * g_2$ ile gösterilir.

ii) Üzerinde en az bir ikili işlem tanımlanmış boş olmayan bir kümeye bir cebirsel yapı denir. $G \neq \emptyset$ ve $*$, G üzerinde bir ikili işlem ise bu cebirsel yapı $(G, *)$ ile gösterilir.

Tanım 1.2.2.

" $*$ ", $G \neq \emptyset$ üzerinde bir ikili işlem olsun.

G_1) $\forall a, b \in G$ için $a * b \in G$ (kapalılık özelliği)

G_2) $\forall a, b, c \in G$ için $a * (b * c) = (a * b) * c$ (birleşme özelliği)

G_3) $\exists e \in G$ öyle ki $\forall a \in G$ için $e * a = a * e = a$ (birim eleman özelliği)

G_4) $\forall a \in G$ için $\exists a^{-1} \in G$ öyle ki $a * a^{-1} = a^{-1} * a = e$ (ters eleman özelliği)

şartlarını sağlıyorsa $(G, *)$ ikilisine bir grup denir.

Eğer $\forall a, b \in G$ için $a * b = b * a$ ise $(G, *)$ ikilisine değişmeli veya abel grubu denir. Burada $a * b$ yerine kısaca ab ile gösterilecektir.

Tanım 1.2.3.

$A \neq \emptyset$ bir küme olsun. $S(A) := \{f | f: A \rightarrow A \text{ birebir ve örten}\}$ olmak üzere $(S(A), \circ)$ bir gruptur ve bu grubun elemanlarına permütasyonlar denir. Eğer $|A| = k$ ise $S(A) =: S_k$ yazılır ve bu gruba k . dereceden simetrik grup denir. $(S(A), \circ)$ grubunun alt gruplarına da A kümesi üzerinde permütasyon grupları denir.

Tanım 1.2.4.

G bir grup $\emptyset \neq H \subseteq G$ olsun. Eğer H, G deki işleme göre bir grup ise H ye G nin bir alt grubu denir ve $H \leq G$ ile gösterilir.

$H \leq G$ ise $e_G \in H$ dır. Dolayısıyla $\{e_G\}$ ve G, G 'nin alt gruplarıdır. Bu alt gruplara 'aşikâr alt grup' denir. G grubunun trivialden farklı alt gruplarına 'öz alt grup' denir.

Önerme 1.2.5.

$(G, *)$ bir grup ve $\emptyset \neq H \subset G$ olsun. Bu taktirde,

$$H \leq G \Leftrightarrow \text{i) } \forall a, b \in H \text{ için } a * b \in H$$

$$\text{ii) } \forall a \in H \text{ için } a^{-1} \in H$$

Önerme 1.2.6.[19]

$(G, *)$ bir grup ve $\emptyset \neq H \subset G$ olsun. $H \leq G \Leftrightarrow \forall a, b \in H \text{ için } a * b^{-1} \in H$ dır.

Tanım 1.2.7.[19]

G bir grup ve $H \leq G$ olsun. G üzerindeki kongruans bağıntısı $a, b \in G$ için $a \equiv b(H) \Leftrightarrow ab^{-1} \in H$ olarak tanımlansın. H alt grubuna göre tanımlanan $" \equiv "$ bağıntısı G üzerinde bir denklik bağıntısıdır. $" \equiv "$ bağıntısına göre $a \in G$ nin denklik sınıfı $\bar{a} = Ha := \{ha : h \in H\}$ alt kümesidir. Ha ya H alt grubuna göre $a \in G$ nin sağ denklik sınıfı(sağ yan sınıfı) denir.

Tanım 1.2.8.[19]

G bir grup ve $H \leq G$ olsun. $a, b \in G$ için $a \equiv b(H) \Leftrightarrow ab^{-1} \in H$ ile tanımlı $" \equiv "$ bağıntısı G üzerinde bir denklik bağıntısıdır. Bu denklik bağıntısına göre $a \in G$ nin denklik sınıfı $\bar{a} = aH := \{ah : h \in H\}$ alt kümesidir. aH ya H alt grubuna göre $a \in G$ nin sol denklik sınıfı(sol yan sınıfı) denir.

Tanım 1.2.9.[19]

G bir grup ve $H \leq G$ olsun. $H \leq G$ alt grubuna göre sağ ve sol yan sınıfların sayısı eşittir. Bu sayıya H nın G içindeki indeksi denir ve $|G:H|$ ile gösterilir.

Tanım 1.2.10.

G bir grup ve $H \not\leq G$ olsun. G de $H \subset M$ olan her M alt grubu için $M = G$ ise H ya G de bir maksimal alt grup denir.

Teorem 1.2.11.

G bir grup ve $N \leq G$ olsun. Bu taktirde aşağıdaki ifadeler birbirine denktir.

$$\text{i) } \forall a \in G, \forall x \in N \text{ için } axa^{-1} \in N$$

$$\text{ii) } \forall a \in G \text{ için } aNa^{-1} \subset N$$

$$iii) \forall a \in G \text{ için } aNa^{-1} = N$$

$$i) \forall a \in G \text{ için } aN = Na$$

Tanım 1.2.12.

Yukarıdaki teoremin denk koşullarından birini gerçekleyen G nin bir N alt grubuna normal alt grup denir ve $N \trianglelefteq G$ ile gösterilir.

Bu tanım ile $\{e_G\}$ ve G , G 'nin normal alt gruplarıdır. Bu normal alt gruplara 'trivial alt grup' denir.

Tanım 1.2.13.

G bir grup ve $N \leq G$ olsun. Bu taktirde $N(H) := \{g \in G : gH = Hg\}$ kümesine H nin G deki normalliye denir.

Tanım 1.2.14.

G bir grup, $M \subset G$ olsun. $\bigcap_{M \subset H, H \leq G} H =: \langle M \rangle \leq G$ ye M nin ürettiği alt grup denir.

M kümesinin elemanlarına $\langle M \rangle$ grubun üreteçleri denir. $K \leq G$ ve $M \subset K$ ise $\langle M \rangle \leq K$ olduğundan $\langle M \rangle$ alt grubu M i içeren G nin en küçük alt grubudur.

Tanım 1.2.15.

Bir G grubu için $G = \langle M \rangle$ olacak şekilde bir $M \subset G$ mevcut ise G ye M ile üretilmiştir denir.

$G = \langle M \rangle$ olsun.

i) $|M| < \infty$ ise G ye sonlu üretenli grup denir.

ii) $M = \{a\}$ ise G ye a ile üretilen devirli grup denir ve $G = \langle a \rangle$ ile gösterilir.

Tanım 1.2.16.

$X \neq \emptyset$ verilen bir küme, $\tau \subset \wp(X)$ olsun. τ ailesine;

i) $\emptyset \in \tau$ ve $X \in \tau$,

ii) $\forall U, V \in \tau$ için $U \cap V \in \tau$,

iii) $\forall \{O_i\}_{i \in I} \subset \tau$ için $\bigcup_{i \in I} O_i \in \tau$ şartları sağlanıyor ise X üzerinde bir topoloji adı verilir. X e de bir topolojik uzay denir ve (X, τ) ile gösterilir.

Tanım 1.2.17.[22]

$(G, *)$ bir grup ve aynı zamanda bir topolojik uzay olsun. Bu taktirde her $g, h \in G$ için;

$$i) \quad \begin{aligned} F: G \times G &\rightarrow G \\ (g, h) &\rightarrow g * h \end{aligned}$$

$$ii) \quad \begin{aligned} f: G &\rightarrow G \\ g &\rightarrow g^{-1} \end{aligned}$$

dönüşümleri sürekli ise G ye bir topolojik grup adı verilir.

Tanım 1.2.18.[22]

G bir topolojik grup ve X bir topolojik uzay olsun. Bu taktirde $\Lambda: G \times X \rightarrow X$, $\Lambda(g, x) = g\Lambda x := gx$ ile tanımlanan Λ dönüşümü sürekli ve $\forall g_1, g_2 \in G, \forall x \in X$ için;

$$i) \quad g_1(g_2x) = (g_1g_2)x$$

$$ii) \quad e\Lambda x = x$$

koşulları sağlanıyor ise (G, X, Λ) üçlüsüne bir topolojik dönüşüm grubu adı verilir.

Yukarıdaki koşullar sağlanıyorsa G ye X üzerinde hareket ediyor veya G, X üzerinde bir hareket grubudur denir. Bu yapıyı (G, X, Λ) yerine kısaca (G, X) ile göstereceğiz.

Tanım 1.2.19.

(G, X) bir topolojik dönüşüm grubu ve $x, y \in X$ olsun.

$x \approx y: \Leftrightarrow \exists g \in G: y = gx$ olarak tanımlanırsa $" \approx "$ bağıntısı X üzerinde bir denklik bağıntısıdır. $" \approx "$ bağıntısının her bir denklik sınıfına hareketin yörüngeleri adı verilir. $x \in X$ noktasını içeren yörüngeye x in yörüngesi adı verilir ve bu $[x]$ ile gösterilir. Böylece $[x] = \{y \in X: x \approx y\} = \{y \in X: \exists g \in G, y = gx\} = Gx$ dir.

Tanım 1.2.20.

(G, X) bir topolojik dönüşüm grubu, G, X üzerinde hareket etsin ve $x, y \in X$ keyfi olsun. $g(x) = y$ olacak şekilde bir $g \in G$ elamanı varsa G ye X üzerinde geçişli olarak(transitif) hareket ediyor denir.

Tanım 1.2.21.[22]

(G, X) bir topolojik dönüşüm grubu ve $x \in X$ keyfi olsun.

$G_x := \{g \in G | gx = x\}$ kümesine x noktasının sabitleyeni denir.

Tanım 1.2.22.

G bir grup, H ve M G nin iki alt grubu olsun. $H = gMg^{-1}$ olan bir $g \in G$ varsa H ve M alt gruplarına eşlenik alt gruplar denir.

Lemma 1.2.23.

(G, X) bir topolojik dönüşüm grubu ve $x, y \in X, g \in G$ olmak üzere $y = gx$ olsun. Bu taktirde, $S_{gx} = gS_xg^{-1}$ dir. Yani bir yörüngedeki farklı iki elemanın sabitleyenleri eşlenik alt gruplardır.

Tanım 1.2.24.

Hiperbolik geometride iki noktayı birleştiren minimal uzunluklu eğrilere geodezikler denir.

Tanım 1.2.25.

$n \in \mathbb{N}$ için $1 \leq a \leq n$ ve $(a, n) = 1$ olan a tamsayılarının sayısı $\varphi(n)$ ile gösterilir ve bu φ fonksiyonuna Euler fonksiyonu adı verilir.

Sonuç 1.2.26.[38]

$\mathbb{U}_n := \{a \in \mathbb{N} : 1 \leq a \leq n, (a, n) = 1\} \mod n$ ye göre çarpma işlemine göre bir gruptur ve $m = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$, m nin asal çarpanlara ayrılışı ise bu taktirde;

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right) = m \prod_{p \text{ asal}} \left(1 - \frac{1}{p}\right) \text{ dir. } \blacksquare$$

1.3. Öklidyen Olmayan Kristal Yapılı Gruplar

G , $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$ genişletilmiş kompleks düzleminin aşağıda verilen biçimdeki dönüşümlerin grubu olsun:

- i) $z \mapsto \frac{az+b}{cz+d}$ $a, b, c, d \in \mathbb{R}, ad - bc = 1$
- ii) $z \mapsto \frac{a\bar{z}+b}{c\bar{z}+d}$ $a, b, c, d \in \mathbb{R}, ad - bc = -1$.

G nin her elemanı $\mathcal{U} = \{z \in \mathbb{C} : \text{Im } z > 0\}$ üst yarı düzleminden kendine bir komformal ya da anti-komformal homeomorfizmdir. i. tipindeki dönüşümlerin kümesi G de indeksi 2 olan bir alt grup oluşturur. Bu grup G^0 ile ifade edilir. G^0 grubu genellikle $PSL(2, \mathbb{R})$ ile ifade edilir. Biz de çalışmamızda bu notasyonu kullanacağız. G ye $\mathbb{R}^4$ ün bir alt kümesi gözüyle bakarak yani, $\{(a, b, c, d) : a, b, c, d \in \mathbb{R}, ad - bc = \pm 1\}$ kümesi ile ifade ederek, G üzerinde bir topoloji inşa edilebilir. Dolayısıyla bu G topolojik grubu iki bileşene sahiptir. Bunlardan biri $PSL(2, \mathbb{R})$ diğeri de $G \setminus PSL(2, \mathbb{R})$ dir.

Tanım 1.3.1.

G nin bir ayrık alt grubuna Öklidyen olmayan kristal yapılı grup ya da kısaca NEC grubu denir.

Tanım 1.3.2.

$PSL(2, \mathbb{R})$ de içeren bir NEC grubuna Fuchs grubu denir.

i) tipindeki elemanlar yön korurlar. Bu tipteki dönüşümler sabit noktalarına göre aşağıdaki üç tipten birine sahiptirler. Sabit noktalar, $z = \frac{az+b}{cz+d}$ ikinci dereceden denklemi çözülerek bulunur.

i. Eğer $|a + d| = 2$ ise dönüşüme paraboliktir denir. Bu durumda genişletilmiş reel sayılar üzerinde tek bir sabit nokta vardır.

ii. $|a + d| > 2$ ise dönüşüme hiperbolik denir. Bu durumda genişletilmiş reel sayılar üzerinde farklı iki reel sabit noktası vardır.

iii. $|a + d| < 2$ ise dönüşüme eliptiktir denir. Bu durumda biri üst yarı düzlemde olan iki kompleks eşlenik sabit noktası vardır.

1.4. $PSL(2, \mathbb{R})$ deki Parabolik ve Eliptik Alt Grupları

Teorem 1.4.1.[22]

$PSL(2, \mathbb{R})$ nin bir parabolik (eliptik, hiperbolik) elemanının $PSL(2, \mathbb{R})$ deki merkezleyeni, aynı sabit nokta kümesine sahip tüm parabolik (eliptik, hiperbolik) elemanlardan oluşur.

Teorem 1.4.2.[22]

Her abel Fuchs grubu devirlidir.

Yukarıdaki iki teoremden, $PSL(2, \mathbb{R})$ deki bir Fuchs grubunun aşağıdaki gibi üç çeşit olduğunu görürüz.

C , $PSL(2, \mathbb{R})$ nin herhangi bir alt grubu olmak üzere C ye abeldir denir ancak ve ancak C devirlidir. Böylece C nin birimden farklı tüm elemanları aynı sabit nokta kümesine sahiptir ve aynı tiptendir ki bunlar parabolik, eliptik veya hiperboliktir. Bir Λ Fuchs grubunun parabolik (eliptik) alt grupları, parabolik(eliptik) elemanlardan oluşan $C \leq \Lambda$ birimden farklı devirli ve bu özellik altında maksimal olan alt gruplar olarak tanımlanır. Λ nın t (veya ϵ) parabolik (eliptik) sınıf sayısı, Λ nın parabolik (eliptik) alt gruplarının eşlenik sınıf sayısıdır.

Tanım 1.4.3.

Eğer $\gamma(r) = r$ olacak şekilde Λ nın bir γ parabolik elemanı varsa bir $r \in \hat{\mathbb{Q}}$ noktası bir Λ Fuchs grubunun bir cusp ı olarak adlandırılır. Benzer şekilde, eğer $\sigma(z) = z$ olacak şekilde bir $\sigma \in \Lambda$ eliptik elmanı varsa bir $z \in \mathcal{U}$ noktasına Λ nın bir eliptik noktası denir.

Lemma 1.4.4.[22]

Eğer A ve B , bir G grubunun alt grupları ve $C = A \cap B$ ise $|B:C| \leq |G:A|$

Lemma 1.4.5.[36]

$\gamma \in \Lambda$ hiperbolik ve $t \in \Lambda$, γ daki gibi bir ve yalnız bir sabit noktaya sahip olsun. Bu durumda Λ Fuchs değildir.

Sonuç 1.4.6.

Λ nın parabolik sınıf sayısı, Λ nın $\widehat{\mathbb{Q}}$ daki yörüngelerinin sayısıdır.

1.5. Ayrık Gruplar ve Riemann Yüzeyleri

$PSL(2, \mathbb{R})$ nin $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ matrisini $\mathbb{R}^4$ ün (a, b, c, d) noktasıyla ifade edeceğimizi söylemiştik. Böylece $PSL(2, \mathbb{R})$ bir topolojik grup olur ve $U \cap \Omega = \{I\}$ olacak şekilde I birim matrisinin $PSL(2, \mathbb{R})$ de bir U komşuluğu olan bir Ω ayrık alt grubunu tanımlarız. $PSL(2, \mathbb{R})$ nin ayrık bir alt grubu Fuchs grup olarak adlandırılır. Sonlu eş hacimli her sonlu üretilmiş Fuchs grup aşağıdaki gösterime sahiptir.

Üreteçler: $a_1, b_1, \dots, a_g, b_g, x_1, \dots, x_r, p_1, \dots, p_s$

Bağıntılar: $x_1^{m_1} = x_2^{m_2} = \dots = x_r^{m_r} = \prod_{i=1}^g a_i b_i a_i^{-1} b_i^{-1} \prod_{j=1}^r x_j \prod_{k=1}^s p_k = 1$

burada $m_1, \dots, m_r \geq 2$ tamsayılarıdır. Bu durumda bu grubun simgesi $(g; m_1, \dots, m_r; s)$ şeklindedir.

$a_1, b_1, \dots, a_g, b_g$ elemanları hiperbolik, $m_1, \dots, m_r$ sırasına karşılık gelen $x_1, \dots, x_r$ elemanları eliptik ve $p_1, \dots, p_s$ elemanları paraboliktir [1].

Γ bir Fuchs grubudur ve $(0; 2, 3; 1)$ simgesine sahiptir. Parabolik elemanlar sonsuz mertebeli eliptik elemanlar olarak düşünüldüğünden Γ nın simgesini sıklıkla

$$(0; 2, 3, \infty)$$

şeklinde yazarız. Ayrıca, bir ayrık grubun her alt grubu ayrık olduğundan Γ nın tüm alt grupları Fuchs grubudur.

Her Λ Fuchs grubu $PSL(2, \mathbb{R})$ nin bir alt grubu olduğundan eliptik elemanlar hariç $\mathcal{U}$ üzerinde hareket eder ve standart topolojiyle bölüm uzayı bir yüzeydir. $\mathcal{U}/\Lambda$ yüzeyini bir Riemann yüzeyi yapmak için gerekli olan kompleks yapıyı $\mathcal{U}$ üzerinden $\mathcal{U}/\Lambda$ yüzeyine transfer edebiliriz. Eğer Λ , eliptik elemanlara da sahipse sonuç yine bir Riemann yüzeyidir fakat

$$\mathcal{U} \rightarrow \mathcal{U}/\Lambda$$

projeksiyonu dallıdır. Bu prosedür için ayrıntıları [22] kaynakta görebiliriz.

Tanım 1.5.1.

X bir topolojik uzay olsun. X in bir örtüm uzayı, bir $\tilde{X}$ uzayından oluşan bir ikilidir ve sürekli $p: \tilde{X} \rightarrow X$ dönüşümü aşağıdaki şartı sağlar:

Her $x \in X$, $p^{-1}(U)$ nun her yay bileşeni p tarafından U üzerine topolojik olarak resmedilecek biçimde bir yay bağlantılılığı U açık komşuluğuna sahiptir.

Basit bağlantılı bir örtüm uzayı, evrensel örtüm uzayı olarak adlandırılır ve örtümlerin izomorfizmine göre tektir [39].

Özellikle, her Riemann yüzeyi bir evrensel örtüme sahiptir. Bu evrensel örtüm, basit bağlantılı bir Riemann yüzeyidir ve konform denklige göre yalnızca üç yüzey vardır.

Teorem 1.5.2.[22]

Her basit bağlantılı Riemann yüzeyi aşağıdakilerden birine konform eşdeğerdir:

- (i) Σ Riemann yüzeyi
- (ii) $\mathbb{C}$ Kompleks Düzlem
- (iii) $\mathcal{U}$ üst yarı düzlem

Bu Riemann yüzeylerinin otomorfizm grupları aşağıdaki gibidir:

Teorem 1.5.3.[22]

- (i) $Aut(\Sigma) = PSL(2, \mathbb{C})$
- (ii) $Aut(\mathbb{C}) = \{z \rightarrow az + b: a, b \in \mathbb{C}, a \neq 0\}$
- (iii) $Aut(\mathcal{U}) = PSL(2, \mathbb{R})$

1.6. Modüler Grup

Tanım 1.6.1.

$w = \frac{az+b}{cz+d}$, $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$ formundaki tüm möbius dönüşümlerinin kümesi modular grup olarak adlandırılır ve Γ ile gösterilir. Bu grup aşağıdaki gibi 2×2 tipinde tamsayılar matrisi ile temsil edilir. Yani;

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

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

Teorem 1.6.2.[42]

Γ modular grubu, $A^2 = B^3 = I$ ile verilen $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ve $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ elemanları tarafından üretilir.

İspat:

$\Phi(z) = \frac{az+b}{cz+d}$; $a, b, c, d \in \mathbb{Z}$ ve $ad - bc = 1$ dönüşümlerinden oluşan G -grubu $\tau(z) = z + 1, \sigma(z) = -\frac{1}{z}$ dönüşümleri ile üretilir.

Üç durumda inceleyelim;

1. $a = 0$ olsun. Bu durumda,

$$bc = -1$$

$$\Rightarrow b = -c = 1$$

$$\Rightarrow b = -c = -1.$$

Böylece $\Phi(z) = \frac{\pm 1}{\pm z + d} = \sigma \tau^{\pm d}(z)$.

Gerçekten de;

$$\tau(z) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \tau^2(z) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \dots, \tau^d(z) = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}$$

$$\sigma(z) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ olduğundan}$$

$$\sigma \tau^d = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} = -\frac{1}{z+d} \text{ bulunur.}$$

Burada $\tau(z) = z + 1$ olduğundan $\tau^{-1}(z) = z - 1$ dir. Yani, $\tau^{-1}(z) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ dir.

$$(\tau^{-1})^2(z) = \tau^{-2}(z) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}. \text{ Böylece}$$

$$\tau^{-d}(z) = \begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix} \text{ olur.}$$

$$\sigma\tau^{-d} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -d \end{pmatrix} = \frac{-1}{z-d} = \frac{1}{-z+d}.$$

2. $|a| = 1$ olsun.

$\frac{-az-b}{-cz-d} = \frac{az+b}{cz+d}$ özdeş olduklarından $a = 1$ alabiliriz. Böylece $d - bc = 1$. Burada

$$\Phi(z) = \frac{z+b}{cz+d} \xrightarrow{\sigma} \frac{-cz-d}{z+b} \xrightarrow{\tau^c} -\frac{1}{z+b}$$

Gerçekten, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ 1 & b \end{pmatrix}$ ve $\tau^c(z) = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ olduğundan

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -c & -d \\ 1 & b \end{pmatrix} = \begin{pmatrix} 0 & \overbrace{bc-d}^{-1} \\ 1 & b \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & b \end{pmatrix}. \text{ Bu yüzden, } \sigma\tau^c \Phi(z) = -\frac{1}{z+b}$$

ile **2.** durumu **1.** durumuna dönüşür. (Orada Φ nın σ ve τ ile üretildiği gösterilmişti.)

3. $|a| > 1$ olsun. Bu durumun **2.** duruma indirgenebileceğini göstereceğiz.

Strateji şu: Φ -dönüşümünden, yeni bir $\Phi_1(z) = \frac{a_1 z + b_1}{c_1 z + d_1}$ öyle ki $|a_1| < |a|$, $|c_1| < |c|$

özellğinde dönüşüm tanımlamak. Eğer bu mümkün olursa $|a_1|$ gittikçe 1'e yaklaşır ve

tekrarlı bu işlem yapıldığında, en sonunda Φ_n - dönüşümünde $|a_n| = 1$ olur.

Φ_1 - dönüşümünü alalım. $|a| > |c|$ olduğunu varsayalım. Aksi durumda $|a| < |c|$ ise Φ

yerine $\sigma\Phi$ alınır.

$$\Phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ iken } \sigma\Phi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}.$$

Şimdi iddia: $\exists n \in \mathbb{Z}$ öyle ki $|a - nc|$, hem $|a|$, hem de $|c|$ ' den daha küçüktür. (Aslında

$n := \left\lfloor \frac{a}{c} \right\rfloor$ dir.)

Örneğin, $T = \begin{pmatrix} 7 & 3 \\ 2 & 1 \end{pmatrix}$ alınırsa $7.1 - 3.2 = 1$ olup $T \in \Phi$ dır.

$|7| > |2|$ ve $n = \left\lceil \frac{7}{2} \right\rceil = 3$ alınırsa $|a - nc| = |7 - 3 \cdot 2| = 1$.

$a - nc$ terimi $\tau^{-n}(z) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ olduğu hatırlanırsa

$$\tau^{-n}\Phi(z) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - cn & b - dn \\ c & d \end{pmatrix} = \frac{(a-cn)z + (b-dn)}{cz + d}$$

Burada σ ile işleme girdiğinde (daha önce gösterildiği gibi) $(a - cn)$ ile c 'nin yer değiştirdiği görülür. Dolayısıyla,

$$\Phi_1(z) = \sigma \tau^{-n} \Phi(z) = \frac{-cz - d}{(a - cn)z + (b - dn)} \quad \text{dönüşümü, stratejide bahsi geçen, aranan} \\ \Phi_1 \text{ --dönüşümüdür. } \dots (*)$$

Yine, örneğimiz üzerinde değerlendirelim; $|a| > |c|$ idi.

$$\tau^{-n}\Phi(z) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \text{ ve } \Phi_1(z) = \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix}, a_1 = -2 \text{ olup } a = 7 \text{ dikkate alındığında} \\ |-2| < |7| \text{ sağlanmış olur.}$$

Süreci 2. Tekrarla devam ettirelim; $|-2| > |1|$. Burada yalnızca σ' yı uygulamak yetecektir:

$$\sigma \Phi_1(z) = \begin{pmatrix} -1 & 0 \\ -2 & -1 \end{pmatrix} \text{ ve } \det = 1 \in \Phi$$

$|a_2| = |-1| = 1$ olup, arzu edilen **2.** durumuna indirgenme gerçekleşmiş olur.

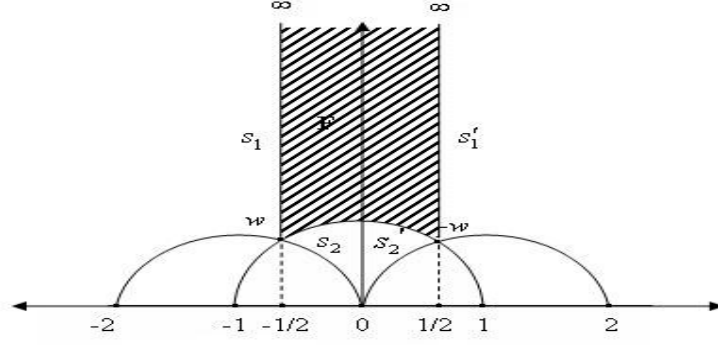
Tanım 1.6.3.

Bir Λ Fuchs grubu verildiğinde, aşağıdaki özellikleri sağlayan bir $F \subset \mathbb{U}$ kapalı kümesine Λ nın bir F temel bölgesi denir:

$$\text{i) } \bigcup_{T \in \Lambda} T(F) = \mathbb{U}$$

$$\text{ii) } \forall T \in \Lambda \setminus \{I\} \text{ için } \overset{\circ}{F} \cap T(\overset{\circ}{F}) = \emptyset$$

Buna göre; $F = \left\{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 \geq 1, |x| \leq \frac{1}{2}, y > 0 \right\}$ kümesi Γ modüler grubu için bir temel bölgedir.



Şekil 1. Γ nın F temel bölgesi

$T(z) = z + 1$ için $T(s_1) = s_1'$ ve $U(z) = -\frac{1}{z}$ için $U(s_2) = s_2'$ olduğundan (s_1, s_1') ve (s_2, s_2') kongrü kenar çiftleridir. Bu nedenle T ve U dönüşümleri Γ modüler grubunu üretir.

Teorem 1.6.4.[23]

- i) Γ nın $\hat{\mathbb{Q}}$ üzerindeki hareketi transitiftir.
- ii) $\hat{\mathbb{Q}}$ nın herhangi bir noktasının sabitleyeni sonsuz devirlidir.

İspat:

i) $\forall v = \frac{a}{b}, w = \frac{c}{d} \in \hat{\mathbb{Q}}$ elemanları için $T\left(\frac{a}{b}\right) = \frac{c}{d}$ olan $T \in \Gamma$ dönüşümünün varlığını göstermeliyiz. Bunun için $\forall v = \frac{a}{b} \in \hat{\mathbb{Q}}$ elemanının $\Gamma(\infty) = \{g(\infty) : g \in \Gamma\}$ da olduğunu göstermemiz yeterlidir. Çünkü; $k(\infty) = \frac{a}{b}$ ve $l(\infty) = \frac{c}{d}$ olan $k, l \in \Gamma$ mevcut ise $T := lk^{-1}$ ile $T\left(\frac{a}{b}\right) = \frac{c}{d}$ dir. $v = \frac{a}{b} \in \hat{\mathbb{Q}}$ olsun. Bu durumda $(a, b) = 1$ olduğundan $\exists x, y \in \mathbb{Z}$ öyleki $ax - by = 1$ dir. Böylece, $g := \begin{pmatrix} a & x \\ b & y \end{pmatrix} \in \Gamma$ dir ve $\begin{pmatrix} a & x \\ b & y \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ olduğundan $g(\infty) = \frac{a}{b}$ dir. Dolayısıyla $\frac{a}{b}, \infty$ un yörüngesindedir. Yani; Γ nın $\hat{\mathbb{Q}}$ üzerindeki hareketi transitiftir.

ii) $\hat{\mathbb{Q}}$ nın herhangi iki elemanının sabitleyenleri Γ da eşlenik olduklarından ∞ un sabitleyeni olan Γ_∞ u göz önüne almak yeterlidir. $\Gamma_\infty = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\} = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ dir.

Gerçekten; $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\infty$ olsun. O halde $T(\infty) = \infty$ dur.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow a = 1$ ve $c = 0$ dir ve ayrıca $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\infty \subset \Gamma$ olduğundan $ad - bc = 1$ dir. $1 \cdot d - b \cdot 0 = 1 \Rightarrow d = 1$ dir. O halde $T = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, $b \in \mathbb{Z}$ formundadır. Yani; $\Gamma_\infty = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$ dir. Böylece $\Gamma_\infty \mathbb{Z} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ elemanı ile üretilen sonsuz devirli bir gruptur. Dolayısıyla $\widehat{\mathbb{Q}}$ da herhangi bir noktanın sabitleyeni sonsuz devirli bir gruptur.

1.7. $\Gamma(N)$ ve $\Gamma_0(N)$ Kongrüans Alt Grupları

Tanım 1.7.1.

N pozitif bir tam sayı olmak üzere, modüler grubun $\Gamma(N)$ temel kongrüans alt grubu aşağıdaki küme ile tanımlanır:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

ve modüler grubun $\Gamma(N)$ temel kongrüans alt grubunu içeren herhangi bir alt grubuna kongrüans alt grubu denir.

Bazı bilindik kongrüans alt gruplar aşağıdaki şekildedir:

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid a \equiv d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\}$$

ve

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N} \right\}.$$

$\Gamma_1(N)$ nin tanımında yer alan $d \equiv 1 \pmod{N}$ kongrüansı, $a \equiv 1 \pmod{N}$, $c \equiv 0 \pmod{N}$ kongrüansları ve $ad - bc = 1$ determinantından elde edilebilir. Açıkça görülür ki bu alt gruplar arasında $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \Gamma$ bağıntısı vardır.

Diğer yandan $\Gamma(N)$, Γ nin bir normal alt grubudur ve dolayısıyla da $\Gamma_1(N)$ ve $\Gamma_0(N)$ nin de normal alt grubudur.

Ayrıca $\Gamma_1(N)$ de $\Gamma_0(N)$ nin normal alt grubudur. Burada $\Gamma(N)$ nin, Γ nın bir normal alt grubu olduğu aşağıdaki şekilde gösterilebilir:

$\psi: \mathbb{Z} \rightarrow \mathbb{Z}_N$ doğal halka homomorfizmi, Γ dan $PSL(2, \mathbb{Z}_N)$ ye tanımlı aşağıdaki şekilde bir $\tilde{\psi}$ grup homomorfizmi tanımlanmasına yardımcı olur:

$$\tilde{\psi}: \Gamma \rightarrow PSL(2, \mathbb{Z}_N), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a_N & b_N \\ c_N & d_N \end{pmatrix}.$$

Buradan $\tilde{\psi}$ nın çekirdeğinin $\Gamma(N)$ olduğu görülebilir. Ayrıca, $\Gamma_0(N)$ alt grubu $N > 1$ iken Γ nın bir normal alt grubu değildir. Diğer yandan, $\Gamma(N), \Gamma_1(N)$ ve $\Gamma_0(N)$ gruplarının Γ daki indeksleri sonludur. $N > 2$ için

$$\Gamma(N) \text{ nin } \Gamma \text{ daki indeksi } |\Gamma: \Gamma(N)| = \frac{N^3}{2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

$$\Gamma_0(N) \text{ nin } \Gamma \text{ daki indeksi } |\Gamma: \Gamma_0(N)| = N \prod_{p|N} \left(1 + \frac{1}{p}\right),$$

$$\Gamma_1(N) \text{ nin } \Gamma \text{ daki indeksi } |\Gamma: \Gamma_1(N)| = \frac{N^2}{2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \text{ dir. } N = 2 \text{ için bu indeksler}$$

$$|\Gamma: \Gamma_0(2)| = 3, |\Gamma: \Gamma_1(2)| = 3, |\Gamma: \Gamma(2)| = 6$$

şeklindedir. Diğer alt grupların birbirlerindeki indeksleri ise yukarıdaki formüller kullanılarak hesaplanabilir. $N > 2$ için

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

ve

$$|\Gamma_1(N): \Gamma(N)| = \frac{|\Gamma: \Gamma(N)|}{|\Gamma: \Gamma_1(N)|} = N \text{ elde edilir.}$$

1.8. $\Gamma_B(N)$ Normalliyeinin Yapısı

$PSL(2, \mathbb{R})$ nin ayrık alt gruplarına Fuchs grubu denir. Literatürde en iyi bilinen Fuchs grubu Γ modüler grubudur. Γ modüler grubu oldukça zengin bir alt grup ailesine sahiptir. Bilhassa kongrüans alt grupları ve kuvvet grupları üzerine yapılmış pek çok çalışma mevcuttur.

Kongrüans alt gruplarından biri olan $\Gamma_0(N)$, özellikle Klein, Fricke ve diğer kişiler tarafından geniş olarak çalışılmıştır. Bu bölümde, $\Gamma_0(N)$ nin $PSL(2, \mathbb{R})$ deki normalliyeni olan $\Gamma_B(N)$ nin yapısı hakkında bilgi vereceğiz.

$\Gamma_B(N)$ normalliyeni ilk olarak [34] de tanımlanmıştır. [8] deki tanım kullanılırsa normalliyen,

$$\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix}$$

matrislerine karşılık gelen dönüşümlerden oluşur ki burada tüm elemanlar tam sayıdır, h ise $h^2|N$ şartını sağlayan, 24 ün en büyük böleni ve $e > 0$, N/h^2 nin tam bölenidir. Ayrıca determinantı e dir. (Eğer $m|K$ ve $(m, K/m) = 1$ ise m ye K nin tam böleni denir ve bu $m||K$ ile ifade edilir.) $\Gamma_B(N)$, birinci çeşit, sonlu üretilmiş bir Fuchs grubudur.

$$\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix}$$

matrisi bir Möbius dönüşümü temsil eder ve bu tipteki tüm matrislerin kümesi matris çarpımı ile bir grup oluşturur.

1.9. Kuadratik Kalanlar

Tanım 1.9.1. [27]

p bir tam sayı olmak üzere, eğer $p > 1$ ve p nin 1 ve kendisinden başka bir böleni yok ise p ye asal sayı denir. 1 den büyük ve asal olmayan sayıya bileşik sayı denir. a ve b iki tam sayı ve ortak asal çarpana sahip değilseler a ve b ye aralarında asaldır denir. $a \in \mathbb{Z}$ ve $a < -1$ ise, $a = (-1)b$ ve b asal veya bileşik sayıdır.

Lemma 1.9.2. [27]

1 den büyük her tam sayı ya asaldır ya da asal sayıların bir çarpımıdır.

İspat :

Asal olmayan ve asal sayıların çarpımı olarak yazılamayan sayıların en küçüğü k olsun. Dolayısıyla açıktır ki k bir bileşik sayıdır.

Bu durumda, $k = ab$ olacak şekilde a ve b tam sayıları vardır. $a < k, b < k$ dir. O halde a ve b ya asaldır veya asal sayıların bir çarpımıdır. Bu durumda da k iki(veya daha çok) asal sayının çarpımıdır.

Teorem 1.9.3.

Sonsuz çoklukta asal sayı vardır.

Tanım 1.9.4.

$a, b, m \in \mathbb{Z}, m > 0$ olsun.

$$a \equiv b \pmod{m} \Leftrightarrow m \mid b - a$$

olarak tanımlı bağıntıya kongrüans, m ye $\pmod{m}$, b ye de a nın m - $\pmod{m}$ göre kalanı denir.

Lemma 1.9.5.

Bir m pozitif tamsayısı için, $a \equiv b \pmod{m}$ ifadesi bir denklik bağıntısıdır. (Yansıyan, Simetrik, Geçişken)

Tanım 1.9.6. [27] (Derecesi İki Olan Kongrüanslar)

p bir asal sayı olmak üzere $ax^2 + bx + c \equiv 0 \pmod{p}$ kongrüanslarını ele alacağız. Burada akla ilk gelen $ax^2 + bx + c \equiv 0 \pmod{p}$ kongrüansında görülen ikinci dereceden formuldür.

Bu ise $ax^2 + bx + c = 0$ denkleminin çözümlerinin

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

şeklinde olduğunu verir.

Eğer reel çözümlerle ilgilenilirse bu taktirde $b^2 - 4ac$ ifadesi negatif, sıfır veya pozitif olacaktır. Halbuki $ax^2 + bx + c \equiv 0 \pmod{p}$ kongrüansının x tamsayı çözümleri aranmaktadır. Tabii ki $b^2 - 4ac$ tam kare değilse bu takdirde tam kökler olmayacaktır. Bunun için $b^2 - 4ac$ ifadesinin $\pmod{p}$ ye göre bir y sayısının karesine denk olması yeterli olacaktır. O halde $x = \frac{-b \pm y}{2a}$ alınabilir.

Fakat $x = \frac{-b \pm y}{2a}$ eşitliğinin bir tamsayı olduğunu söylemek henüz mümkün değildir. Yani

$$2ax \equiv -b + y \pmod{p}$$

Kongrüansının tamsayı çözümü var mıdır? Bu tip bir kongrüansın çözümünün olması için

$[(a, m) = 1$ ise $ax \equiv b \pmod{m}$ kongrüansı tam birtek çözüme sahiptir.]

$(2a, p) = 1$ olmalıdır. $p \nmid a$ olduğunu kabul edebiliriz. Aksi halde

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

kongrüansı ikinci dereceden kongrüans formuna uymaz.

Eğer $p = 2$ ise bu taktirde kongrüansın çözümünü bulmak kolaydır.

Eğer $y^2 \equiv b^2 - 4ac \pmod{p}$ ve $x, 2ax \equiv -b + y \pmod{p}$ nin bir çözümü ise bu taktirde $x, ax^2 + bx + c \equiv 0 \pmod{p}$ kongrüansının bir çözümüdür.

$ax^2 + bx + c \equiv 0 \pmod{p}$ kongrüansının bütün çözümleri bu yolla bulunabilir.

Tanım 1.9.7.

Bir $p \in \mathbb{P}$ asal sayısının $x, y \in \mathbb{Z}$ olmak üzere

$p = x^2 + y^2$ formundadır $\Leftrightarrow p \equiv 1 \pmod{4}$. Bu koşulu sağlayan asallara Pisagor asalları denir.

$$5 = 1^2 + 2^2 \quad 17 = 1^2 + 4^2 \quad 37 = 1^2 + 6^2$$

$$13 = 2^2 + 3^2 \quad 29 = 2^2 + 5^2 \quad 41 = 4^2 + 5^2$$

➤ $p \equiv 3 \pmod{4}$ asallarının hiçbirisi böyle ifade edilemez.

3, 7, 11, 19, 23 ve 31

Tanım 1.9.8. (Karesel Sayı)

Bir tam sayının karesi olan sayılardır.

1, 4, 9, 16, 25, ...

Tanım 1.9.9. [27]

$p \nmid a$ olsun.

Eğer; $x^2 \equiv a \pmod{p}$ kongrüansı çözülebilirse a ya $\pmod{p}$ nin bir kuadratik kalanı (rezidü) denir.

Eğer, $x^2 \equiv a \pmod{p}$ çözüme sahip değil ise a ya $\pmod{p}$ nin bir kuadratik non-rezidü denir.

- Bir $q \in \mathbb{Z}$ ye $\pmod{n}$ kuadratik rezidü denir, eğer $\pmod{n}$ e göre bir karesel sayıya kongrü ise. Yani, $\exists x \in \mathbb{Z}$ öyle ki $x^2 \equiv q \pmod{n}$

Teorem 1.9.10. [27]

$1 \leq a \leq p - 1$ eşitsizliğini sağlayan a sayısının tam yarısı $\pmod{p}$ ye göre kuadratik kalandır.

Teorem 1.9.11.[48] (The Fundamental Theorem of Arithmetic)

Bu teorem *Euclid* tarafından ortaya atılmış, *Gauss* tarafından da ispatlanmıştır. Bu teorem der ki; herhangi bir doğal sayı (1 olmasın), bir takım asal sayıların çarpımı olarak yazılabilir. Yani her doğal sayının açılımı, benzersizdir. Bu teorem, benzersiz çarpanlara ayırma teoremi olarak da adlandırılır. Aritmetiğin temel teoremi, Öklid teoremlerinin ilkinin bir sonucudur [18].

İspat:

Bu durumda teoremin ispatı, 2 ifadeden oluşur. Birincisi; her doğal sayının (1 hariç) bir takım asal sayılar tarafından çarpım hâlinde yazılabilmesi, ikincisi ise benzersiz olmasıdır. Öncelikle asal çarpanlara ayırmanın varlığını kanıtlayalım. 2 doğal sayısı ile başlayalım. 2 zaten bir asal sayı olduğu için $2 = 2$ olarak asal çarpanlarına ayırdık diyebiliriz. Farz edelim ki bu teoriyi çürütecek en küçük doğal sayı n olsun. Eğer n asal ise, kanıtlanmıştır. Eğer n bileşik ise, 1 ve kendisi için asal bölenleri vardır. Öyleyse a ve b olan 2 doğal sayı vardır.

$$a \cdot b = n \text{ ve } a, b < n .$$

Tümevarımdan yola çıkarak a ve b 'yi asal çarpanlarına ayıralım. p_i ve q_j asalları için $a = p_1 \cdot p_2 \cdot \dots \cdot p_n$ ve $b = q_1 \cdot q_2 \cdot \dots \cdot q_s$.

Öyleyse, $(p_1 \cdot p_2 \cdot \dots \cdot p_n) \times (q_1 \cdot q_2 \cdot \dots \cdot q_s) = n$ ile gösterilebilir. Bu da, n 'nin asal çarpanlarına ayrılması için gereklidir.

Böylece matematiğin tümevarım yöntemine göre herhangi bir sayı, asalların çarpımına göre açıklanabilir.

Sırada, herhangi bir doğal sayının asal çarpanlarına ayrılmasının her doğal sayı için benzersiz bir asal dizilime sahip olduğunu göstereceğiz. Bunun için iki yardımcı ifadeye(teoreme) ihtiyacımız var.

Lemma 1.9.12.

İki pozitif tamsayı olan a ve b nin bütün tamsayılarla olan seti $\{ax + by\}$, a ve b 'nin x ve y katsayıları ile lineer kombinasyonlarıdır. Bu tamsayı kümesini S ile gösterelim. Bu S kümesinin içindeki elemanların da 0'dan büyük elemanlarının olduğu alt kümeyi P ile gösterelim. Bu alt küme P 'nin içinden $d = \min\{ax + by\}$ alalım. Öyleyse d , a ve b 'nin en büyük ortak böleni olur.

İspat:

Öncelikle d 'nin a 'yı böldüğünü gösterelim. Tamsayıların bölünmesinin genel formülünü uygularsak $a = md + r$, $0 \leq r < d$... (1). Bölme işleminden kalanımız olan r 'nin, 0 olduğunu göstereceğiz. x ve y tamsayıları ile $d = ax + by$ yazılabilir. Bunu da (1) eşitliğinde yerine yazalım. $a = m(ax + by) + r = (m \cdot a \cdot x) + (m \cdot b \cdot y) + r$ olur. Bunu da $r = -(m \cdot a \cdot x) - (m \cdot b \cdot y) + a$ olarak yazabiliriz. Buradan da son eşitlikteki r 'nin a ve b katsayılarına da baktığımızda S kümesine ait bir elemandır. Farz edelim ki $r > 0$, öyleyse r , P 'nin bir alt kümesine aittir. Bu sebepten r , d 'den ya büyük ya da eşit olmalı. Çünkü d , P 'nin en küçük elemanıydı. Bu da (1) deki $r < d$ ile çelişir. Öyleyse $r = 0$ 'dır. Böylece d 'nin a 'yı böldüğü gösterilmiş olur. Benzer şekilde d , b 'yi de böler. Böylece d , a ve b 'nin ortak bir böleni olur. $d = ax + by$ gibi bir forma sahip olduğundan a ve b 'nin herhangi bir ortak böleni de d 'yi böler. Bundan dolayı da d , a ve b 'nin en büyük ortak böleni olur. Sonuç olarak Lemma 1 kanıtlanmış olur.

Lemma 1.9.13.

p asal sayısı; a ve b sayılarının çarpımı olan $a.b$ ' yi bölerse, a veya b ' yi de böler.

İspat: Diyelim ki p asal sayımız a ' yı bölemiyor. Öyleyse b ' yi bölmeli. p , a ' yı bölemediğinden ve asal olduğundan en büyük ortak bölenleri 1' dir.

Öyleyse x ve y tamsayıları ve $(p.x) + (a.y) = 1$ gibi bir form olmalı. Her iki tarafı b ile çarparsak $(p.b.x) + (a.b.y) = b$ olur. Varsayımdan p ' nin $a.b$ ' yi böldüğünü biliyoruz. Öyleyse p , $a.b.y$ ' yi de böler. Öyleyse p , $p.b.x$ ' i ve dolayısıyla b ' yi de böler. Sonuç olarak Lemma 1.8.13. kanıtlanmış olur.

Şimdi, herhangi bir doğal sayının çarpanlarına ayrılmasının benzersizliğinin kanıtını basitçe açıklayabiliriz. Varsayalım ki çarpanlarına ayrılmış bir doğal sayımız var. Bu varsayım altında da en küçük doğal sayımız olan n ' nin bir kaç çarpanı vardır. $n = (p_1.p_2....p_n) = (q_1.q_2....q_s)$ olsun. Öyleyse $p_1, q_1, q_2....q_r$ yi böler. **Lemma 1.8.13'** den p_1, q_s yi böler. Ayrıca diyelim ki p_1, q_1 i böler. p_1 ve q_1 asal olduğundan $p_1 = q_1(n/p_1)$ ' in $(n/p_1) < n$ ve $(n/p_1) = p_2....p_n = q_2....q_s$ gibi iki farklı şekilde çarpanlarına ayrılmış olsun. (n/p_1) , n den küçük olduğundan; varsayımsal olarak en küçük doğal sayının iki farklı çarpanlara ayrımı vardır.

Yukarıdaki (n/p_1) için çarpanlarına ayırma işlemi aslında özdeştir. Yani tüm $i = 2, ..., r = s$ için $r = s$ ve $p_1 = q_s$ dir. Böylece n ' nin çarpanları aslında özdeştir. Dolayısıyla herhangi bir pozitif tamsayının çarpanlarına ayrılması tektir. ■

Elemanter sayılar teorisinin en güzel teoremlerinden birisi Fermat' ın iki kare teoremidir.

Teorem 1.9.14. (İki Kare Teoremi)

Bir p – asalı iki kare toplamı olarak ifade edilebilir $\Leftrightarrow -1(modp)$ ye göre bir quadratik rezidü ise. $(\exists x \in \mathbb{Z}: x^2 \equiv -1(modp))$

Bu teorem [18]' da birkaç yolla kanıtlanmış ve keyfi $n \in \mathbb{Z}$ genişlemesi de sağlanmıştır. $n = u^2 + v^2$ ise $(u, v) = 1$ ve $-1(modn)$ bir quadratik rezidü. Burada bu teorem için yeni bir kanıt vereceğiz.

Bu kanıt $M = PSL_2(\mathbb{Z})$ – modüler grubunun bir serbest çarpım yapısına sahip olmasından yararlanır. Bu kanıt birkaç nedenden ötürü ilginçtir ; birincisi, temel olarak sayılar teorisinden bağımsızdır, ikincisi, genel tam sayılar için sonucu doğrudan ve çabucak ispatlar.

Son olarak, ispattaki teknik $\mathbb{Z}$ den daha geniş kare toplam özelliğine sahip halkaları dikkate aldığımızda da kullanılabilir.

İki kare teoremini sağlayan halkalar (genel yapıları aşağıda verildi) kare toplam halkaları diye adlandırılıp [12] incelendi. Genel bir kural olarak; bir halka üzerinde tanımlı 2×2 özel lineer grubu bir serbest çarpımla ayrışabiliyorsa, o halka kare toplam özelliğininide sağlar [12].

Teorem 1.9.15.[11]

Bir $n \in \mathbb{Z}^+$ iki kare toplamıdır, eğer $-1(mod n)$ bir quadratik rezidü ise. Tersine $n = u^2 + v^2: (u, v) = 1$ ise $-1(mod n)$ bir quadratik rezidüdür.

İspat :

$z' = \frac{az+b}{cz+d} : a, b, c, d \in \mathbb{Z}$ ve $ad - bc = 1$ lineer kesirli dönüşümlerin $M = PSL_2(\mathbb{Z})$ – modüler grubunu göz önüne alalım. [35] ve [41] biliyoruz ki M , 2 –devirli bir grupla 3 –devirli bir grubun serbest çarpımıdır ($M = \mathbb{Z}_2 * \mathbb{Z}_3$). Üstelik bu gerçek sayılar teorisinden bağımsız olarak süreksiz grupların metotlarıyla çözülmüştür [35],[41]. Bu yüzden M' de grup olarak 2 mertebeli her eleman konjuge [41]. Şimdi

$T = \left(z' = -\frac{1}{z}\right)$ 2 mertebeli olup, M' dedir. Dolayısıyla 2 mertebeli her eleman T' ye konjuge olmak zorundadır.

$U = \left(z' = \frac{az+b}{cz+d}\right) \in M$ olsun. U ve T konjuge olacağından,

$$UTU^{-1} = \left(\frac{az+b}{cz+d}\right) \left(-\frac{1}{z}\right) \left(\frac{dz-b}{-cz+d}\right) = \frac{-(ac+bd)z + (a^2+b^2)}{-(c^2+d^2)z + (ac+bd)} \dots (1)$$

Burada çarpım matris çarpımı yardımıyla yapılır.

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, U^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$TU^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} dz-b \\ -cz+d \end{pmatrix} = \begin{pmatrix} -c & a \\ -d & b \end{pmatrix}$$

$$UTU^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -c & a \\ -d & b \end{pmatrix} = \begin{pmatrix} -ac - bd & a^2 + b^2 \\ -c^2 - d^2 & ac + bd \end{pmatrix} = \begin{pmatrix} -(ac + bd) & a^2 + b^2 \\ -(c^2 + d^2) & ac + bd \end{pmatrix}$$

Görüldüğü üzere $UTU^{-1} = \frac{-(ac+bd)z+(a^2+b^2)}{-(c^2+d^2)z+(ac+bd)}$ olduğu açıktır.

Bu yüzden M' de 2 mertebeli her eleman (1) –formunda olmak zorundadır. $n > 0$ ve $n \in \mathbb{Z}$ olsun. $-1(mod n)$ ' e göre bir quadratik rezidü olsun. Bu durumda

$$\exists l, k \in \mathbb{Z} \text{ öyle ki } l^2 + 1 = kn. \text{ Bu yüzden } z' = \frac{lz+n}{-kz-l} \dots (2)$$

Katsayıları tam sayı olup, determinantı +1 dir, bu yüzden de M' dedir. Üstelik iz(trace)' i 0 dır. M' de izi= 0 olan elemanlarının mertebesi 2 dir [41]. Dolayısıyla bu dönüşüm 2 mertebeli olup T ye konjugedir. Bu yüzden (2),(1) formunda olup $a, b \in \mathbb{Z}$ için $n = a^2 + b^2$ eşitliği elde edilir.

Tersine $a, b \in \mathbb{Z}$ ve $(a, b) = 1$ olmak üzere $n = a^2 + b^2$ olsun. $(a, b) = 1$ olduğundan $\exists c, d \in \mathbb{Z}$ öyle ki $ad - bc = 1$. Bu yüzden

$$z' = \frac{az + b}{cz + d} \dots (3)$$

dönüşümü M' dedir. (3) ile $T = \left(z' = -\frac{1}{z}\right)$ nin konjugasyonu, $n = a^2 + b^2$ olduğundan,

$$z' = \frac{(ac + bd)z + (a^2 + b^2)}{-(c^2 + d^2) + (ac + bd)} = \frac{az + n}{mz - \alpha}$$

dönüşümünü verir. Konjugasyon determinantı koruduğundan $-\alpha^2 - mn = 1$ veya $\alpha^2 + 1 = -mn$. Bu yüzden $-1(mod n)$ 'e göre bir quadratik rezidüdür.

Tanım 1.9.16.(Altyörüngesel graflar)

$X \neq \emptyset$ bir küme ve $\Delta \subset X \times X$ bir bağıntı olsun. $G = (X, \Delta)$ ikilisine bir graf denir. X 'in elemanlarına grafın köşeleri ve Δ 'nın elemanlarına grafın kenarları denir. $(a, b) \in \Delta$ ise bu durum $a \rightarrow b$ ile gösterilir. $a \rightarrow b$ veya $b \rightarrow a$ ise a ile b bir kenar ile bağlanmıştır

denir. Bu durumda a ve b ye komşu köşeler denir. $a = a_0, a_1, \dots, a_n = b$ bir G grafının köşelerinin bir dizisi olsun.

Her $1 \leq i \leq n$ için a_{i-1} ile a_i bir kenar ile bağlanmışlarsa a 'dan b 'ye n uzunluklu bir yol vardır denir. Eğer $a = b$ ve $a_0, a_1, \dots, a_{n-1}$ köşelerinin tümü farklı ise bu yola n kenarlı bir devre denir. Ayrıca a_i, a_{i+1} ikilileri için $a_i \rightarrow a_{i+1}$ ise bu devreye yönelmiş bir devre denir.

[23]'de Γ Modüler grubunun cusp kümesi olan $\widehat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ genişletilmiş rasyonel sayılar kümesi üzerindeki grup hareketinin neticesinde ortaya çıkan altyörüngesel graflar incelenmiş, bunların literatürce iyi bilinen Farey grafının bir genellemesi olduğu gösterilmiştir. Bu çalışmadan sonra diğer sonlu üretilmiş Fuchs gruplarının altyörüngesel grafları da benzer şekilde incelenmiştir [3, 4, 7, 14, 15, 16, 17, 24, 25, 26, 28, 29, 30, 31].

Tanım 1.9.17.(Grup Hareketi)

$\widehat{\mathbb{Q}}$ 'nın her elemanı $\frac{x}{y} : x, y \in \mathbb{Z}$ ve $(x, y) = 1$ olduğu biliniyor. Burada

$\infty = 1/0 = -1/0$ ile gösterilmiştir. Γ 'nın $\widehat{\mathbb{Q}}$ üzerindeki grup hareketi $\Gamma \times \widehat{\mathbb{Q}} \rightarrow \widehat{\mathbb{Q}}$ ise

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

ile tanımlanır. $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$ ve $(x, y) = 1$ olduğundan elde edilen rasyonel her zaman indirgenmiş formda olur.

Tanım 1.9.18.(Transitif Hareket)

“Her $\alpha, \beta \in \widehat{\mathbb{Q}}$ için $\exists g \in \Gamma$ öyle ki $g(\alpha) = \beta$ ” koşulu sağlanıyorsa ilgili grup hareketi transitif(geçişli) denir. Γ 'nın $\widehat{\mathbb{Q}}$ üzerinde transitif hareket ettiği [23]'de Bezout eşitliğinin yardımıyla gösterilmiştir.

Tanım 1.9.19.(İmprimitif Hareket)

G bir grup, Ω boştan farklı bir küme olmak üzere (G, Ω) herhangi bir permütasyon grubu olsun. Ω üzerinde tanımlı bir $\approx$ denklik bağıntısına G -invariant denir: “ $\alpha \approx \beta (\alpha, \beta \in \Omega)$ olduğunda $\forall g \in G$ için $g(\alpha) \approx g(\beta)$ ” sağlanıyorsa.

Birim ve evrensel denklik bağıntıları bu koşulu otomatikman sağlar. Eğer bunların dışında bir G -invariant denklik bağıntısı mevcutsa (G, Ω) ya bir imprimitif permütasyon grubu denir.

Transitiflik ve imprimitiflik arasındaki ilişkiye gelince, (G, Ω) imprimitif ise otomatikman transitiftir, ancak tersi doğru değildir. Tersinin de doğru olabilmesi için gerek ve yeter şart aşağıdaki teoremle verilmiştir;

Teorem 1.9.20. [23]

(G, Ω) transitif permütasyon grubu olsun. (G, Ω) nın primitif olması için gerek ve yeter koşul $\forall \alpha \in \Omega$ için α nın G deki sabitleyeni G_α , G nin bir maksimal alt grubudur.

Buna göre,

$$G_\alpha < H < G$$

alındığında G transitif hareket ettiğinden Ω 'nın her elemanı $g(\alpha)$ şeklinde yazılabilir. Bu yüzden Ω üzerinde iyi tanımlı bir G -invariant denklik bağıntısı:

$$g_1(\alpha) \approx g_2(\alpha) \Leftrightarrow g_1 \in g_2 H$$

ile tanımlanabilir ve böylece (G, Ω) transitif ve imprimitif permütasyon grubu olur. Transitif hareketten ötürü tek yörünge mevcutken imprimitif hareketin neticesi olarak oluşan denklik sınıfları nedeniyle yörünge bloklara parçalanır. Blokların sayısı $|G:H|$ indeksi ile hesaplanır.

Tanım 1.9.21.(Blok Dizayını)

Bu bölümde $(\Gamma, \widehat{\mathbb{Q}})$ transitif permütasyon grubunu göz önüne alacağız. Keyfi eleman olarak ∞ 'un Γ 'daki sabitleyeni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ eşitliği kullanılarak

$\Gamma_\infty = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ olarak kolayca hesaplanır. Böylece H grubunun seçimi için modüler grup ve kongrüans alt gruplarının anlatıldığı bölümden de görüleceği üzere $\Gamma_1(n)$ ve $\Gamma_0(n)$ en doğal adaylardır. [4], [23]' de $\Gamma_\infty < \Gamma_0(n) < \Gamma$ bağıntısı çalışılırken [28]' de $\Gamma_\infty < \Gamma_1(n) < \Gamma$ bağıntısı çalışılmıştır. Bu seçimlerin graflar üzerindeki etkisi ise aşağıdaki gibidir. $|\Gamma:\Gamma_0(n)|$ indeksi $|\Gamma:\Gamma_1(n)|$ indeksinden daha küçük olduğu için birinci

durumda daha az blok sayısı olmasına karşın altgrafın devre açısından daha zengin olması muhtemeldir. Nitekim ilgili çalışmalar da bu düşünceyi desteklemektedir. Ancak hangi grafın daha makbul olduğu çalışılan problemin tabiatına bağlı olarak değişkenlik gösterir.

Tanım 1.9.22.(Devreler)

(G, Ω) bir transitif permütasyon grubu olsun. G nin $\Omega \times \Omega$ üzerinde $g \in G$ ve $(\alpha, \beta) \in \Omega \times \Omega$ olmak üzere

$$g: (\alpha, \beta) \rightarrow (g(\alpha), g(\beta))$$

ile tanımlı hareketini göz önüne alalım. Bu hareketin yörüngelerine G nin alt yörüngeleri denir. (α, β) yı içeren alt yörünge $O(\alpha, \beta)$ ile gösterilsin. $O(\alpha, \beta)$ dan bir $G(\alpha, \beta)$ alt yörüngesel grafi aşağıdaki gibi elde edilir: $G(\alpha, \beta)$ 'nın köşeleri Ω nın köşeleridir ve $x, y \in \Omega$ için $(\alpha, \beta) \in O(\alpha, \beta)$ ise x den y ye yönelmiş bir kenar vardır denir, $x \rightarrow y$ ile gösterilir. Bu kenar $\mathbb{H}$ üst yarı düzleminde bir hiperbolik geodezik olarak çizilir.

$v_i \in \Omega$ olmak üzere $v_1 \rightarrow v_2 \rightarrow \dots v_n \rightarrow v_1$ ve $v_i \neq v_j (i \neq j)$ konfigürasyonuna n uzunluklu bir devre denir. [4]' de grubun alt yörüngesel graflarındaki devrelerle, eliptik üreteçleri arasındaki ilişki ortaya konmuştur. Bu ilişki, eliptik elemanların mertebelerinin grubun invaryantlarından biri olması nedeniyle, simge problemi açısından son derece önemlidir.

2. YAPILAN ÇALIŞMALAR

Öncelikle çizgenin elde edilmesi için izlenen metot aşağıdaki 4 aşamada özetlenmiştir. Bu metodu daha ayrıntılı incelemek için [23] çalışmasına bakılabilir.

2.1. Transitif Hareketin Sağlandığı Köşe Kümelerinin Belirlenmesi

Üçgen grup olduğunda $\widehat{\mathbb{Q}}$ üzerinde transitif hareket otomatikman sağlanmaktadır. $\widehat{\mathbb{Q}}$ üzerinde transitif hareketin sağlanmadığı durumlarda ise transitifliğin sağlandığı maksimal altküme bulmak üzere [14]'de yapıldığı gibi, öncelikle $\Gamma_0(n)$ nin yörüngeleri;

Teorem.[14] $d|N$ olsun. $(a, d) = 1$ olmak üzere $\frac{a}{d}$ rasyonel sayısının $\Gamma_0(n)$ altındaki yörüngesi $\left\{ \frac{x}{y} \in \widehat{\mathbb{Q}} : (N, y) = d, a \equiv x \frac{y}{d} \pmod{d, N/d} \right\}$ kümesidir. Burada $\begin{pmatrix} a \\ d \end{pmatrix}$ yörüngelerinin sayısı $\varphi(n)$ Euler fonksiyonu olmak üzere $\varphi(d, N/d)$ sayısıdır.

ile elde edilir. Sonraki adımda bu yörüngeler, $Nor(N)$ 'nin elemanları ile birlikte değerlendirilerek, ki bu durumda N 'nin seçimine bağlı olarak bir sürü varyasyon ortaya çıkacaktır, maksimal altkümeye ulaşılır.

2.1.1. İmpremitif Hareket ve Blok Şartı

Burada $Nor(N)$ 'nin altgruplarının grup yapısını bilmek önemlidir. ∞ 'un

$Nor(N)$ ' deki sabitleyeni $Nor(N)_\infty = \left\langle \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix} \right\rangle$ şeklinde olduğu biliniyor. Bu bölümde $Nor(N)_\infty < H < Nor(N)$ şartını sağlayacak H altgruplarının seçimi yapılacaktır. Blok sayısı $|Nor(N):H|$ indeksi ile belirlendiğinden, indeksin küçük olması bloktaki köşe noktalarının sayısının artması ve devre oluşma ihtimalinin artmasını sağlar. Bu nedenle kapsama bağıntısına göre $Nor(N)$ 'e en yakın altgrup seçilmeye çalışılacaktır. $\Gamma_0(n), \Gamma_W(n), \Gamma_C(n)$ altgrupları H için doğal adaylardır. Çalıştığımız grupların hepsi sonlu üretilmiş olduklarından eleman bazında yapılacak ekleme-çıkarma ile istenen blok dizaynı sağlanacaktır.

2.1.2. Kenar Şartının Elde Edilmesi

Graflarda devrelerin varolup olmadığını test etmede temel araç, kenar şartıdır.

Transitif hareket nedeniyle altgrafların hepsi birbirine izomorftur, bu nedenle tek bir altgraf üzerinde çalışmak yeterlidir. İşlem kolaylığı açısından, şimdiye kadar olduğu gibi ∞ bloğu üzerinde çalışmak öncelikli tercih olacaktır. Buna göre, her yörünge $v = u/n$ ve $(u, n) = 1$ olmak üzere bir (∞, v) çiftini içereceğinden $(\infty, u/n)$ çiftini $(r/s, x/y)$ çiftine resmeden $g \in Nor(N)$ dönüşümleri ve bunların köşeler üzerinde dönüşümün tabiatından kaynaklanan kısıtlamaları elde edilecektir. Burada N 'nin seçimine bağlı olarak kenar şartlarının sayısı artış-azalış göstermektedir.

2.1.3. Devrelerin Elde Edilmesi

Bu bölümde eliptik eleman ve devre arasında 1 – 1 bir ilişki olduğu varsayımı altında, N 'nin seçimi hangi üçgen gösterimi veriyorsa, o gösterimin işaret ettiği devrenin varlığı gösterilmeye çalışılacaktır. Burada izlenen metod: ilgili devreyi temsil eden keyfi konfigürasyonu transitif hareket sayesinde, ∞ ile başlayıp- biten temel konfigürasyona resmetmek ve sonrasında bu konfigürasyon üzerinde kenar şartını uygulamaktır.

$Nor(N)$ de determinantı 1 olan dönüşümlerin kümesi $Nor(N)$ nin bir alt grubudur ve $\Gamma_C(N)$ ile gösterilir.

$$\Gamma_0(N/h^2) = \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix} \Gamma_C(N) \begin{pmatrix} 1 & 0 \\ 0 & h \end{pmatrix}$$

$$\Gamma_C(N), \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix} \text{ ile } \Gamma_0(N/h^2) \text{ nin bir eşleniğidir.}$$

$W_e = \begin{pmatrix} ae & b \\ cN & de \end{pmatrix}$ biçimindeki matrislere karşılık gelen dönüşümlerin kümesi bir gruptur ve $\Gamma_W(N)$ ile gösterilir, burada $e \parallel N$ ve $\det W_e = e > 0$ dır. $\Gamma_W(N)$ nin elemanları

Atkin-Lehner dönüşümleri olarak adlandırılır.

Teorem 2.1.3.1.

N keyfi bir pozitif tam sayı olsun. Bu durumda $Nor(N)$ yalnızca 2, 3, 4 ve 6 mertebeli periyotlara sahip olabilir ve üstelik;

a) $Nor(N)$, 4. mertebeden en çok bir periyoda sahiptir. $Nor(N)$ nin 4. mertebeden bir periyoda sahip olması için gerek ve yeter şart,

$$N/h^2 = 2p_2^{\alpha_2} \dots p_r^{\alpha_r} \text{ ve } i = 2, \dots, r \text{ olmak üzere } 2 \parallel N/h^2 \text{ ve } p_i \equiv 1(\text{mod}4).$$

b) $Nor(N)$, 6. mertebeden en çok bir periyoda sahiptir. $Nor(N)$ nin 6. mertebeden bir periyoda sahip olması için gerek ve yeter şart,

$$N/h^2 = 3p_2^{\alpha_2} \dots p_r^{\alpha_r} \text{ ve } i = 2, \dots, r \text{ olmak üzere } 3 \parallel N/h^2 \text{ ve } p_i \equiv 1(mod 3).$$

c) $Nor(N)$, 3. mertebeden en çok bir periyoda sahiptir. $Nor(N)$ nin 3. mertebeden bir periyoda sahip olması için gerek ve yeter şart,

$$N/h^2 = p_3^{\alpha_3} \dots p_r^{\alpha_r} \text{ ve } i = 3, \dots, r \text{ olmak üzere } p_i \equiv 1(mod 3) \text{ olmasıdır [1].}$$

İspat : $Nor(N)$ nin elemanları $\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix}$ biçimindedir, burada $e \parallel N/h^2$,

$det = e > 0$ ve $h, h^2/N$ şartını sağlayan 24 ün en büyük bölenidir. Buradan basit bir hesaplamayla, $E = \begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix}$ bir eliptik eleman ve $a + d = 0$ ise $E^2 = I$ olduğu görülür. $a + d = \pm 1$ farzedilirse E eliptik elemanı için aşağıdaki üç olasılık söz konusudur ;

i) $e = 1$ ise $E^3 = I$

ii) $e = 2$ ise $E^4 = I$

iii) $e = 3$ ise $E^6 = I$

i), ii), iii) için benzer yolla hesaplamalar yapalım. $e = 1$ olduğundan ve $a + d = 1$

kabul edebileceğimizden $E = \begin{pmatrix} a & b/h \\ cN/h & d \end{pmatrix}$ dir. $det E = 1$ kullanıldığında

$$E^2 = \begin{pmatrix} a-1 & b/h \\ cN/h & d-1 \end{pmatrix} \text{ ve } E^3 = I \text{ elde ederiz. } a + d \neq 0 \text{ ve } e > 3 \text{ olan durumlara}$$

baktığımızda $|(a+d)\sqrt{e}| \geq 2$ elde edilir. Buna göre E ya parabolik ya da hiperboliktir. Dolayısıyla her iki durumda da E sonsuz mertebelidir.

a) Farzedelim ki $Nor(N)$ nin 4. mertebeden bir periyoda sahip olsun. Bu durumda $e = 2$

dir. Buna göre $2^k \parallel N$ ve $k = 1, 3, 5, 7$ dir. Böylece E eliptik elemanı $\begin{pmatrix} 2a & b/h \\ cN/h & 2d \end{pmatrix}$

biçimindedir ve $det E = 4ad - bc N/h^2 = 2$ dir. $d = 1 - a$ eşitliği kullanıldığında

$(2a - 1)^2 \equiv -1 \pmod{N/h^2}$ denklemi elde edilir. Bu kongrüans denkleminin bir çözümü olması için gerek ve yeter şart $p_i \equiv 1 \pmod{4}$ olmak üzere $N/h^2 = 2p_2^{\alpha_2} \dots p_r^{\alpha_r}$ ve $i = 2, \dots, r$ olmasıdır. Diğer durumlar benzer şekilde elde edilir.

2.2. $N = 2^6 \cdot p^2$

$N = 2^6 \cdot p^2$ olsun.

$$\alpha = 6, \beta = 0, h = 2^{\min\{3,3\}} \cdot 3^{\min\{1,0\}} = 2^3 = 8$$

$$N/h^2 = 64p^2/64 = p^2, e = 1, p^2$$

$$T_1 = \begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix}, \quad T_2 = \begin{pmatrix} ap^2 & b/8 \\ 8p^2c & dp^2 \end{pmatrix}$$

$$ad - bcp^2 = 1 \quad \quad \quad adp^4 - bcp^2 = p^2$$

$$(adp^2 - bc = 1)$$

Tablo 1. $2^6 \cdot p^2$ için bölen sayısı $7 \times 3 = 21$

1	2	2^2	2^3	2^4	2^5	2^6
p	$2 \cdot p$	$2^2 \cdot p$	$2^3 \cdot p$	$2^4 \cdot p$	$2^5 \cdot p$	$2^6 \cdot p$
p^2	$2 \cdot p^2$	$2^2 \cdot p^2$	$2^3 \cdot p^2$	$2^4 \cdot p^2$	$2^5 \cdot p^2$	$2^6 \cdot p^2$

Tablo 2. $(d, N/d)$ –durumları :

$d = 1$	$(1, 64p^2) = 1$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
$d = 2$	$(2, 32p^2) = 2$	$\begin{pmatrix} 1 \\ 2 \end{pmatrix}$
$d = 4$	$(4, 16p^2) = 4$	2 tane $\begin{pmatrix} * \\ 2^2 \end{pmatrix}$
$d = 8$	$(8, 8p^2) = 8$	4 tane $\begin{pmatrix} * \\ 2^3 \end{pmatrix}$
$d = 16$	$(16, 4p^2) = 4$	2 tane $\begin{pmatrix} * \\ 2^4 \end{pmatrix}$
$d = 32$	$(32, 2p^2) = 2$	$\begin{pmatrix} 1 \\ 2^5 \end{pmatrix}$

Tablo 2' nin devamı

$d = 64$	$(64, p^2) = 1$	$\binom{1}{2^6}$
$d = p$	$(p, 64p) = p$	$p - 1 \text{ tane } \binom{*}{p}$
$d = 2p$	$(2p, 32p) = 2p$	$p - 1 \text{ tane } \binom{*}{2p}$
$d = 4p$	$(4p, 16p) = 4p$	$2p - 2 \text{ tane } \binom{*}{4p}$
$d = 8p$	$(8p, 8p) = 8p$	$4p - 4 \text{ tane } \binom{*}{8p}$
$d = 16p$	$(16p, 4p) = 4p$	$2p - 2 \text{ tane } \binom{*}{16p}$
$d = 32p$	$(32p, 2p) = 2p$	$p - 1 \text{ tane } \binom{*}{32p}$
$d = 64p$	$(64p, p) = p$	$p - 1 \text{ tane } \binom{*}{64p}$
$d = p^2$	$(p^2, 64) = 1$	$\binom{1}{p^2}$
$d = 2p^2$	$(2p^2, 32) = 2$	$\binom{1}{2p^2}$
$d = 4p^2$	$(4p^2, 16) = 4$	$2 \text{ tane } \binom{*}{4p^2}$
$d = 8p^2$	$(8p^2, 8) = 8$	$4 \text{ tane } \binom{*}{8p^2}$
$d = 16p^2$	$(16p^2, 4) = 4$	$2 \text{ tane } \binom{*}{16p^2}$
$d = 32p^2$	$(32p^2, 2) = 2$	$\binom{1}{2^5 p^2}$
$d = 64p^2$	$(64p^2, 1) = 1$	$\binom{1}{2^6 p^2}$

$$\widehat{\mathbb{Q}}(2^6 \cdot p^2) = \binom{1}{1} \cup \binom{1}{2} \cup \binom{1}{2^2} \cup \binom{1}{2^3} \cup \binom{1}{2^4} \cup \binom{1}{2^5} \cup \binom{1}{2^6} \cup \binom{1}{p^2} \cup \binom{1}{2p^2} \cup \binom{1}{2^2 p^2} \cup \binom{1}{2^3 \cdot p^2} \cup \binom{1}{2^4 \cdot p^2} \cup \binom{1}{2^5 \cdot p^2} \cup \binom{1}{2^6 \cdot p^2}$$

$\binom{1}{1}$ in $Nor(2^6 \cdot p^2)$ ile hareketine bakalım.

1. Tip $T_1 = \begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix}$, $\det T_1 = ad - bcp^2 = 1$

$$\begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{a + b/8}{8p^2c + d} = \frac{8a + b}{2^3(8p^2c + d)} \quad \dots (*)$$

1. b tek ve d tek ise $*$ $= \frac{8a+b}{2^3(8p^2c+d)} \in \left(\frac{1}{2^3} \right)$

2. b tek, d çift ve $2 \parallel d$ ise $*$ $= \frac{8a+b}{2^4(4p^2c+d_0)} \in \left(\frac{1}{2^4} \right)$

3. b tek, d çift ve $2^2 \parallel d$ ise $*$ $= \frac{8a+b}{2^5(2p^2c+d_0)} \in \left(\frac{1}{2^5} \right)$

4. b tek, d çift ve $2^3 \parallel d$ ise $*$ $= \frac{8a+b}{2^6(p^2c+d_0)} \in \left(\frac{1}{2^6} \right)$

5. b çift, d tek ve $2 \parallel b$ ise $*$ $= \frac{4a+b_0}{2^2(8p^2c+d)} \in \left(\frac{1}{2^2} \right)$

6. b çift, d tek ve $2^2 \parallel b$ ise $*$ $= \frac{2a+b_0}{2(8p^2c+d)} \in \left(\frac{1}{2} \right)$

7. b çift, d tek ve $2^3 \parallel b$ ise $*$ $= \frac{a+b_0}{8p^2c+d} \in \left(\frac{1}{1} \right)$

2. Tip $T_2 = \begin{pmatrix} ap^2 & b/8 \\ 8p^2c & dp^2 \end{pmatrix}$, $\det T_2 = adp^2 - bc = 1$

$$\begin{pmatrix} ap^2 & b/8 \\ 8p^2c & dp^2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{ap^2 + b/8}{8p^2c + dp^2} = \frac{8ap^2 + b}{2^3 \cdot p^2(8c + d)} \quad \dots (**)$$

1. b tek ve d tek ise $*$ $= \frac{8ap^2+b}{2^3 \cdot p^2(8c+d)} \in \left(\frac{1}{2^3 p^2} \right)$

2. b tek, d çift ve $2 \parallel d$ ise $*$ $= \frac{8ap^2+b}{2^4 p^2(4c+d_0)} \in \left(\frac{1}{2^4 p^2} \right)$

3. b tek, d çift ve $2^2 \parallel d$ ise $*$ $= \frac{8ap^2+b}{2^5 p^2(2c+d_0)} \in \left(\frac{1}{2^5 p^2} \right)$

4. b tek, d çift ve $2^3 \parallel d$ ise $*$ $= \frac{8ap^2+b}{2^6 p^2(c+d_0)} \in \left(\frac{1}{2^6 p^2} \right)$

5. b çift, d tek ve $2 \parallel b$ ise $*$ $= \frac{4ap^2+b_0}{2^2 p^2(8c+d)} \in \left(\frac{1}{2^2 p^2} \right)$

$$6. b \text{ çift, } d \text{ tek ve } 2^2 \parallel b \text{ ise } * = \frac{2ap^2+b_0}{2p^2(8c+d)} \in \left(\frac{1}{2p^2} \right)$$

$$7. b \text{ çift, } d \text{ tek ve } 2^3 \parallel b \text{ ise } * = \frac{ap^2+b_0}{p^2(8c+d)} \in \left(\frac{1}{p^2} \right)$$

$$h = 8 \ N/h^2 = p^2 \text{ olduğundan } \rho = 1$$

$$\varepsilon_1 = 1, \ \varepsilon_2 = 0 \text{ olduğundan } \tau = 3/2$$

$$\text{İndeks} = 2 \cdot 8^2 \cdot \frac{3}{2} = 192, |\Gamma_C(N): \Gamma_0(N)| = h^2 \tau = 8^2 \cdot \frac{3}{2} = 96, |\Gamma_B(N): \Gamma_C(N)| = 2$$

$$\text{ve } G_\infty = \left\langle \begin{pmatrix} 1 & 1/8 \\ 0 & 1 \end{pmatrix} \right\rangle$$

$$[0] = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^5 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^6 \end{pmatrix}$$

$$[\infty] = \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^2 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^5 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^6 \cdot p^2 \end{pmatrix}$$

$$T_1 = \begin{pmatrix} a & b \\ 64p^2c & d \end{pmatrix} \in \Gamma_0(N), \quad \underbrace{ad}_{tek} - 16 \cdot bcp^2 = 1$$

$$T_{2,3} = \begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix} \in \Gamma_C(N), \quad \underbrace{ad}_{tek \vee çift} - bcp^2 = 1, \quad \begin{matrix} 8 \nmid a & (T_2) \\ 8|a & (T_3) \end{matrix}$$

$$\mathbf{Kenar} : r/s, \ x/y \in [\infty], \ r/s \mapsto x/y \in F(\infty, u/p^2) \Leftrightarrow$$

$$(i) \ 64p^2 \parallel s \Rightarrow x \equiv \pm ur \pmod{p^2}, \ y \equiv \pm us \pmod{p^2}, \ ry - sx = \pm p^2$$

$$(ii) \ 8p^2 \parallel s \Rightarrow x \equiv \pm 8ur \pmod{p^2}, \ y \equiv \pm 8us \pmod{p^2}, \ ry - sx = \pm 8p^2$$

$$(iii) \ p^2 \parallel s \Rightarrow x \equiv \pm 64ur \pmod{p^2}, \ y \equiv \pm 64us \pmod{p^2}, \ ry - sx = \pm p^2$$

$$\mathbf{İspat} : \ r/s \mapsto x/y \in F(\infty, u/p^2) \text{ ve}$$

I. durum

$$64p^2 \parallel s \text{ olsun. Bu durumda } (\infty, u/p^2) \xrightarrow{T} (r/s \mapsto x/y) \text{ olan } T = T_1$$

$$\begin{pmatrix} a & b \\ 64p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{64p^2c} = \frac{r}{s} \xRightarrow{a \text{ tek}} \begin{cases} r = a \\ s = 64p^2c \end{cases}$$

$$\begin{pmatrix} a & b \\ 64p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{au + bp^2}{64p^2cu + dp^2} \Rightarrow \begin{matrix} x \equiv ur \pmod{p^2} \\ y \equiv us \pmod{p^2} \end{matrix}$$

$$\det = 1 \text{ ve } (u, p^2) = 1 \text{ den } ry - sx = p^2$$

II. durum

$8p^2 \parallel s$ olsun. Bu durumda

$$T_2 = \begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix}, \quad a - \text{tek} \text{ olur.}$$

$$\begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{8p^2c} = \frac{r}{s} \Rightarrow \begin{cases} r = a \\ s = 8p^2c \end{cases}$$

$$\begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{au + bp^2/8}{8p^2cu + dp^2} = \frac{8au + bp^2}{64p^2cu + 8dp^2} = \frac{x}{y}$$

$$x \equiv \pm 8ur \pmod{p^2} \quad y \equiv \pm 8us \pmod{p^2}$$

$$\begin{pmatrix} 8a & b \\ 8p^2c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} 8a & 8au + bp^2 \\ 8p^2c & 8p^2cu + dp^2 \end{pmatrix} = \begin{pmatrix} 8r & x \\ s & y/8 \end{pmatrix}$$

$$\det = 8\det = p^2ry - sx = 8p^2$$

III. durum

$p^2 \parallel s$ olsun. Bu durumda

$$T_3 = \begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix}, \quad a - \text{çift } (8|a) \text{ olur.}$$

$$\begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{8p^2c} \frac{a_0}{8|a|p^2c} = \frac{r}{s} \Rightarrow \begin{cases} r = a_0 \\ s = p^2c \end{cases}$$

$$\begin{pmatrix} a & b/8 \\ 8p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{au + bp^2/8}{8p^2cu + dp^2} = \frac{8au + bp^2}{64p^2cu + 8dp^2} = \frac{x}{y}$$

$$x \equiv \pm 64ur \pmod{p^2} \quad y \equiv \pm 64us \pmod{24p^2}$$

$$\begin{pmatrix} 8a & b \\ 8p^2c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} 8a & 8au + bp^2 \\ 8p^2c & 8p^2cu + dp^2 \end{pmatrix} = \begin{pmatrix} 64r & x \\ 8s & y/8 \end{pmatrix}$$

$$8(ry - sx) = 8p^2 \Rightarrow ry - sx = p^2$$

Devre : Üçgen içerir $\Leftrightarrow 64u^2 \pm 8u + 1 \equiv 0 \pmod{p^2}$

İspat : Transitif hareketten:

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \xrightarrow{<} \frac{x}{y} \rightarrow \frac{1}{0}$$

$\frac{x}{y} \rightarrow \frac{1}{0}$ kenarı için $y = p^2$ veya $y = 8p^2$ elde edilir.

$y = p^2$ olsun. Bu durumda üçgen

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \xrightarrow{<} \frac{x}{p^2} \rightarrow \frac{1}{0}$$

halini alır.

$\frac{u}{p^2} \xrightarrow{<} \frac{x}{p^2}$ kenarı için $x \equiv -64u^2 \pmod{p^2}$ ve $x = u + 1$ elde edilir. Buradan da $64u^2 + u + 1 \equiv 0 \pmod{p^2}$ bulunur.

$\frac{x}{p^2} \rightarrow \frac{1}{0}$ kenarı için $1 \equiv -64ux \pmod{p^2}$ bulunur. $x = u + 1$ kullanılırsa $64u^2 + 64u + 1 \equiv 0 \pmod{p^2}$ elde edilir ki bu $64u^2 + u + 1 \equiv 0 \pmod{p^2}$ olmasıyla çelişir.

O halde $y = 8p^2$ dir ve üçgen

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \xrightarrow{<} \frac{x}{8p^2} \rightarrow \frac{1}{0}$$

şeklindedir.

$\frac{u}{p^2} \xrightarrow{<} \frac{x}{8p^2}$ kenarı için $x \equiv -64u^2 \pmod{p^2}$ ve $x = 8u + 1$ elde edilir. Buradan da

$$64u^2 + 8u + 1 \equiv 0 \pmod{p^2} \text{ bulunur.}$$

$\frac{x}{8p^2} \rightarrow \frac{1}{0}$ kenarı için $1 \equiv -8ux \pmod{p^2}$ bulunur. $x = 8u + 1$ kullanılırsa

$$64u^2 + 8u + 1 \equiv 0 \pmod{p^2} \text{ elde edilir.}$$

$$\textbf{Sonuç} : \frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{8u+1}{8p^2} \rightarrow \frac{1}{0}$$

Teorem 2.2.1.

$u \in \mathbb{Z}$ olmak üzere $64u^2 \pm 8u + 1$ ifadesinin asal bölenleri $p \equiv 1 \pmod{3}$ formundadır.

İspat. $u \in \mathbb{Z}$ keyfi ve $p \mid 64u^2 \pm 8u + 1$, $p \in \mathbb{P}$ asal olsun. Bu durumda yukarıdaki devre varlığının yeter şartı dikkate alındığında $Nor(2^6 \cdot p)$ grubunda, $Nor(2^6 \cdot p^2)'$ de olduğu gibi

$$= \begin{pmatrix} -2^6 \cdot u & (64u^2 \pm 8u + 1)/p \\ -2^6 \cdot p & 64u \pm 8u \end{pmatrix}$$

3. mertebeden eliptik üreticinin varlığı bilinmektedir. Buradan [2] Teorem 2'nin sonucu olarak $p \equiv 1(mod 3)$ olduğu ortaya çıkar.

2.3. $N = 2^4 \cdot 3^2 \cdot p^2$

$N = 2^4 \cdot 3^2 \cdot p^2$ olsun.

$$\alpha = 4, \beta = 2, h = 2^{\min\{3,2\}} \cdot 3^{\min\{1,1\}} = 2^2 \cdot 3 = 12$$

$$N/h^2 = 2^4 \cdot 3^2 \cdot p^2 / 2^4 \cdot 3^2 = p^2, e = 1 \vee p^2$$

$$T_1 = \begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix}, \quad T_2 = \begin{pmatrix} ap^2 & b/12 \\ 12p^2c & dp^2 \end{pmatrix},$$

$$ad - bcp^2 = 1 \quad \quad \quad adp^4 - bcp^2 = p^2$$

Tablo 3. $2^4 \cdot 3^2 \cdot p^2$ için bölen sayısı $5 \times 3 \times 3 = 45$

1	2	2^2	2^3	2^4
p	$2 \cdot p$	$2^2 \cdot p$	$2^3 \cdot p$	$2^4 \cdot p$
p^2	$2 \cdot p^2$	$2^2 \cdot p^2$	$2^3 \cdot p^2$	$2^4 \cdot p^2$
3	$2 \cdot 3$	$2^2 \cdot 3$	$2^3 \cdot 3$	$2^4 \cdot 3$
$3 \cdot p$	$2 \cdot 3 \cdot p$	$2^2 \cdot 3 \cdot p$	$2^3 \cdot 3 \cdot p$	$2^4 \cdot 3 \cdot p$
$3 \cdot p^2$	$2 \cdot 3 \cdot p^2$	$2^2 \cdot 3 \cdot p^2$	$2^3 \cdot 3 \cdot p^2$	$2^4 \cdot 3 \cdot p^2$
3^2	$2 \cdot 3^2$	$2^2 \cdot 3^2$	$2^3 \cdot 3^2$	$2^4 \cdot 3^2$
$3^2 \cdot p$	$2 \cdot 3^2 \cdot p$	$2^2 \cdot 3^2 \cdot p$	$2^3 \cdot 3^2 \cdot p$	$2^4 \cdot 3^2 \cdot p$
$3^2 \cdot p^2$	$2 \cdot 3^2 \cdot p^2$	$2^2 \cdot 3^2 \cdot p^2$	$2^3 \cdot 3^2 \cdot p^2$	$2^4 \cdot 3^2 \cdot p^2$

Tablo 4. $(d, N/d)$ – durumları :

$d = 1$	$(1, 144p^2) = 1$	$\binom{1}{1}$
$d = 2$	$(2, 72p^2) = 2$	$\binom{1}{2}$
$d = 4$	$(4, 36p^2) = 4$	$\varphi(4) = 2^2(1 - 1/2) = 2$ $\binom{1}{4}, \binom{3}{4}$
$d = 8$	$(8, 18p^2) = 2$	$\binom{1}{8}$
$d = 16$	$(16, 9p^2) = 1$	$\binom{1}{16}$
$d = p$	$(p, 144p) = p$	$\binom{1}{p}, \binom{2}{p}, \dots, \binom{p-1}{p}$
$d = 2p$	$(2p, 72p) = 2p$	$\varphi(2p) = p - 1$ $\binom{2k+1}{2p}$
$d = 4p$	$(4p, 36p) = 4p$	$\varphi(4p) = 2p - 2$ $\binom{2k+1}{4p}$
$d = 8p$	$(8p, 18p) = 2p$	$\varphi(8p) = p - 1$ $\binom{2k+1}{4p}$
$d = 16p$	$(16p, 9p) = p$	$\varphi(16p) = p - 1$ $\binom{2k+1}{8p}$
$d = p^2$	$(p^2, 144) = 1$	$\binom{1}{p^2}$
$d = 2p^2$	$(2p^2, 72) = 2$	$\binom{1}{2p^2}$
$d = 4p^2$	$(4p^2, 36) = 4$	$\varphi(4) = 2$ $\binom{1}{4p^2}, \binom{3}{4p^2}$
$d = 8p^2$	$(8p^2, 18) = 2$	$\binom{1}{8p^2}$
$d = 16p^2$	$(16p^2, 9) = 1$	$\binom{1}{16p^2}$
$d = 3$	$(3, 48p^2) = 3$	$\varphi(3) = 2$ $\binom{1}{3}, \binom{2}{3}$
$d = 6$	$(6, 24p^2) = 6$	$\varphi(6) = 2$ $\binom{1}{6}, \binom{5}{6}$
$d = 12$	$(12, 12p^2) = 12$	$\varphi(12) = [12(1 - \frac{1}{2})(1 - \frac{1}{3})$ $= 4]$ $\binom{1}{12}, \binom{5}{12}, \binom{7}{12}, \binom{11}{12}$

Tablo 4' ün devamı

$d = 24$	$(24, 6p^2) = 6$	$\binom{1}{24}, \binom{23}{24}$
$d = 48$	$(48, 3p^2) = 3$	$\binom{1}{48}, \binom{47}{48}$
$d = 3p$	$(3p, 48p) = 3p$	$\varphi(3p) = 2p - 2$ $\binom{2k}{3p}$
$d = 6p$	$(6p, 24p) = 6p$	$\varphi(6p) = 2p - 2$ $\binom{\circ}{6p}$
$d = 24p$	$(24p, 6p) = 6p$	$\varphi(6p) = 2p - 2$ $\binom{\circ}{24p}$
$d = 48p$	$(48p, 3p) = 3p$	$\varphi(3p) = 2p - 2$ $\binom{\circ}{48p}$
$d = 3p^2$	$(3p^2, 48) = 3$	$\binom{1}{3p^2}, \binom{2}{3p^2}$
$d = 6p^2$	$(6p^2, 24) = 4$	$\binom{1}{6p^2}, \binom{5}{6p^2}$
$d = 12p^2$	$(12p^2, 12) = 12$	$\varphi(12)=4$ $\binom{1}{12p^2}, \binom{5}{12p^2}, \binom{7}{12p^2}, \binom{11}{12p^2}$
$d = 24p^2$	$(24p^2, 6) = 4$	$\varphi(4) = 2$ $\binom{1}{24p^2}, \binom{23}{24p^2}$
$d = 48p^2$	$(48p^2, 3) = 3$	$\binom{a_1}{48p^2}, \binom{a_2}{48p^2}$
$d = 9$	$(9, 16p^2) = 1$	$\binom{1}{9}$
$d = 18$	$(18, 8p^2) = 2$	$\binom{1}{18}$
$d = 36$	$(36, 4p^2) = 4$	$\binom{1}{36}, \binom{35}{36}$
$d = 72$	$(72, 2p^2) = 2$	$\binom{1}{72}$
$d = 144$	$(144, p^2) = 1$	$\binom{1}{144}$
$d = 9p$	$(9p, 16p) = p$	$\binom{1}{9p}, \binom{2}{9p}, \dots, \binom{p-1}{9p}$
$d = 18p$	$(18p, 8p) = 2p$	$\binom{a_1}{18p}, \dots, \binom{a_p}{18p}$
$d = 36p$	$(36p, 4p) = 4p$	$\varphi(4p) = 2p - 2$ $\binom{a_1}{36p}, \dots, \binom{a_p}{36p}$
$d = 72p$	$(72p, 2p) = 2p$	$\varphi(2p) = p - 1$ $\binom{a_1}{72p}, \dots, \binom{a_p}{72p}$

Tablo 4' ün devamı

$d = 144p$	$(144p, p) = p$	$\begin{pmatrix} a_1 \\ 144p \end{pmatrix}, \dots, \begin{pmatrix} a_p \\ 144p \end{pmatrix}$
$d = 9p^2$	$(9p^2, 16) = 1$	$\begin{pmatrix} 1 \\ 9p^2 \end{pmatrix}$
$d = 18p^2$	$(18p^2, 8) = 2$	$\begin{pmatrix} 1 \\ 18p^2 \end{pmatrix}$
$d = 36p^2$	$(36p^2, 4) = 4$	$\varphi(4) = 2$ $\begin{pmatrix} a_1 \\ 36p^2 \end{pmatrix}, \dots, \begin{pmatrix} a_p \\ 36p^2 \end{pmatrix}$
$d = 72p^2$	$(72p^2, 2) = 2$	$\begin{pmatrix} 1 \\ 72p^2 \end{pmatrix}$
$d = 144p^2$	$(144p^2, 1) = 1$	$\begin{pmatrix} 1 \\ 144p^2 \end{pmatrix}$

$$\mathbb{Q}(2^4 \cdot 3^2 \cdot p^2) =$$

$$\begin{aligned} & \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \cdot 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \cdot 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \cdot 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \\ & \cup \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3^2 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \cdot 3^2 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \cdot 3^2 \cdot p^2 \end{pmatrix} \\ & \cup \begin{pmatrix} 1 \\ 2^4 \cdot 3^2 \cdot p^2 \end{pmatrix} \end{aligned}$$

$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ 'in $Nor(2^4 \cdot 3^2 \cdot p^2)$ ile hareketine bakalım.

1. Tip $\begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix}$, $\det = ad - bcp^2 = 1$

$$\begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{a+b/12}{12p^2c+d} = \frac{12a+b}{12(12p^2c+d)} \quad \dots (*)$$

1. $ad - tek$ ve $6 \parallel b$ ise $*$ = $\frac{2a+b_0}{2(12p^2c+d)} \in \begin{pmatrix} 1 \\ 2 \end{pmatrix}$

2. $2 \parallel d$ ve $3 \parallel b$ ise $*$ = $\frac{4a+b_0}{2^3(6p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2^3 \end{pmatrix}$

3. $4 \parallel d$ ve $3 \parallel b$ ise $*$ = $\frac{4a+b_0}{2^4(3p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2^4 \end{pmatrix}$

4. $3 \parallel d$ ve $4 \parallel b$ ise $*$ = $\frac{3a+b_0}{3^2(4p^2c+d_0)} \in \begin{pmatrix} 1 \\ 3^2 \end{pmatrix}$

5. $3 \parallel d$ ve $2 \parallel b$ ise $*$ = $\frac{6a+b_0}{2 \cdot 3^2(4p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2 \cdot 3^2 \end{pmatrix}$

$$6. \quad 6 \parallel d \text{ ve } b, c - \text{tek} \text{ ise } * = \frac{12a+b}{2^3 \cdot 3^2 (2p^2 c + d_0)} \in \left(\frac{1}{2^3 \cdot 3^2} \right)$$

$$7. \quad 12 \parallel d \text{ ve } b, c - \text{tek} \text{ ise } * = \frac{12a+b}{2^4 \cdot 3^2 (p^2 c + d_0)} \in \left(\frac{1}{2^4 \cdot 3^2} \right)$$

2. tip elemanlar ve a, b, c, d nin aynı seçimleri ile diğer yörüngeler benzer şekilde hesaplanır.

$$h = 12 \quad N/h^2 = p^2 \text{ old } \rho = 1$$

$$\varepsilon_1 = 1, \varepsilon_2 = 1 \text{ old } \tau = 3/2 \cdot 4/3 = 2$$

$$\text{İndeks} = 2.144.2 = 576$$

$$H = \Gamma_C(2^4 \cdot 3^2 \cdot p^2) \text{ seçilirse } |\Gamma_B(N) : \Gamma_C(N)| = 2, \quad G_\infty = \left\langle \begin{pmatrix} 1 & 1/12 \\ 0 & 1 \end{pmatrix} \right\rangle$$

$$[0] = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \cdot 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \cdot 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \cdot 3^2 \end{pmatrix}$$

$$[\infty] = \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^4 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3^2 \cdot p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \cdot 3^2 \cdot p^2 \end{pmatrix}$$

$$\cup \begin{pmatrix} 1 \\ 2^3 \cdot 3^2 \cdot p^2 \end{pmatrix} \begin{pmatrix} 1 \\ 2^4 \cdot 3^2 \cdot p^2 \end{pmatrix}$$

$\Gamma_C(2^4 \cdot 3^2 \cdot p^2)'$ deki üç tip eleman:

$$T_1 = \begin{pmatrix} a & b \\ 144p^2c & d \end{pmatrix} \in \Gamma_0(N), \quad \underbrace{ad}_{\text{tek}} - bcp^2 \cdot 144 = 1$$

$$T_{2,3} = \begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \in \Gamma_C(N), \quad \underbrace{\underbrace{ad}_{\text{tek}}}_{\substack{\vee \\ \text{çift} \\ \text{olabilir}}} - bcp^2 = 1$$

Kenar : $r/s, x/y \in [\infty], r/s \mapsto x/y \in F(\infty, u/p^2) \Leftrightarrow$

$$(i) \quad 2^4 \cdot 3^2 \cdot p^2 \parallel s \Rightarrow x \equiv \pm ur \pmod{p^2}, y \equiv \pm us \pmod{p^2}, ry - sx = \pm p^2$$

$$(ii) \quad 2^2 \cdot 3 \cdot p^2 \parallel s \Rightarrow x \equiv \pm 2^2 \cdot 3 \cdot ur \pmod{p^2}, y \equiv \pm 2^2 \cdot 3 \cdot us \pmod{p^2},$$

$$ry - sx = \pm p^2$$

$$(iii) \quad p^2 \parallel s \Rightarrow x \equiv \pm 2^4 \cdot 3^2 \cdot ur \pmod{p^2}, y \equiv \pm 2^4 \cdot 3^2 \cdot us \pmod{p^2},$$

$$ry - sx = \pm p^2$$

İspat : $r/s \mapsto x/y \in F(\infty, u/p^2)$ ve

I. durum

$2^4 \cdot 3^2 \cdot p^2 \parallel s$ olsun. Bu durumda $(\infty, u/p^2) \xrightarrow{T} (r/s \mapsto x/y)$ olan $T = T_1$

$$\begin{pmatrix} a & b \\ 144p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{144p^2c} = \frac{r}{s} \xrightarrow{a\text{-tek}} \begin{cases} r = a \\ s = 144p^2c \end{cases}$$

$$\begin{pmatrix} a & b \\ 144p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{\tilde{a}^r u + bp^2}{\underbrace{144p^2cu + dp^2}_s} \Rightarrow \begin{cases} x \equiv ur \pmod{p^2} \\ y \equiv us \pmod{p^2} \end{cases}$$

$$ry - sx = p^2$$

II. durum

$12p^2 \parallel s$ olsun. Bu durumda

$$T_2 = \begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix}, \quad ad - tek \quad \text{olur.}$$

$$\begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{12p^2c} = \frac{r}{s} \xrightarrow{a\text{-tek}} \begin{cases} r = a \\ s = 12p^2c \end{cases}$$

$$\begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{au + bp^2/12}{12p^2cu + dp^2} = \frac{12au + bp^2}{144p^2cu + 12dp^2} = \frac{x}{y}$$

$$x \equiv 12ur \pmod{p^2} \quad y \equiv 12us \pmod{p^2}$$

$$\begin{pmatrix} 12a & b \\ 12p^2c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} 12a & 12au + bp^2 \\ 12p^2c & 12p^2cu + dp^2 \end{pmatrix} = \begin{pmatrix} 12r & x \\ s & y/12 \end{pmatrix}$$

$$\det = 12 \quad \det = p^2$$

$$ry - sx = 12p^2$$

III. durum

$p^2 \parallel s$ olsun. Bu durumda

$$T_3 = \begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \quad \text{ve } 12|a \quad \text{olsun.}$$

$$\begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{12p^2c} \overline{12|a} \frac{a_0}{p^2c} = \frac{r}{s} \Rightarrow \begin{cases} r = a_0 \\ s = p^2c \end{cases}$$

$$\begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{au + bp^2/12}{12p^2cu + dp^2}$$

$$= \frac{12au + bp^2}{144p^2cu + 12dp^2} \overline{12|a} \frac{144a_0u + bp^2}{144p^2cu + 12dp^2} = \frac{x}{y} \Rightarrow \begin{cases} x \equiv 144ur \pmod{p^2} \\ y \equiv 144us \pmod{p^2} \end{cases}$$

$$\begin{aligned}
\begin{pmatrix} a & b/12 \\ 12p^2c & d \end{pmatrix} \times 12 &= \begin{pmatrix} 12a & b \\ 144p^2c & 12d \end{pmatrix} \xrightarrow{12|a} \begin{pmatrix} 144\overbrace{a_0}^r & b \\ 144\underbrace{p^2c}_s & 12d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u & p^2 \end{pmatrix} \\
&\div 144 \\
&= \begin{pmatrix} r & x \\ s & y \end{pmatrix} \Rightarrow ry - sx = \pm p^2
\end{aligned}$$

Devre : Üçgen içerir $\Leftrightarrow 144u^2 \pm 12u + 1 \equiv 0 \pmod{p^2}$

İspat : Transitif hareketten:

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{x}{yp^2} \rightarrow \frac{1}{0}, \quad y = 1 \text{ veya } 12$$

1. durum

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{x}{p^2} \rightarrow \frac{1}{0} \text{ olsun.}$$

$$2. \text{ kenardan, } p^2 \parallel s \text{ old. } up^2 - xp^2 = -p^2$$

$$\Rightarrow u - x = -1$$

$$\Rightarrow x = u + 1$$

$$\text{Üstelik, } u + 1 \equiv -144u^2 \pmod{p^2}$$

$$144u^2 + u + 1 \equiv 0 \pmod{p^2} \dots (1)$$

2. durum

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{x}{12p^2} \rightarrow \frac{1}{0} \text{ olsun.}$$

$$2. \text{ kenardan } 12up^2 - xp^2 = -p^2 \quad (p^2 \parallel s)$$

$$\Rightarrow x = 12u + 1$$

$$3. \text{ kenardan, } \frac{12u+1}{12p^2} \rightarrow \frac{1}{0}$$

$$1 \equiv -12u(12u + 1) \pmod{p^2}$$

$$\textbf{Sonuç : } 144u^2 + 12u + 1 \equiv 0 \pmod{p^2}$$

$$3. \text{ kenardan, } p^2 \parallel s \text{ old. } 1 \equiv -144u(u + 1) \pmod{p^2}$$

$$144u^2 + 144u + 1 \equiv 0 \pmod{p^2} \dots (2)$$

(1) ve (2)' den $143u + 1 \equiv 0 \pmod{p^2}$

13.11. $u + 1 \equiv 0 \pmod{p^2}$ ve $(u, p^2) = 1$ olduğundan çelişki
(karesiz)

Teorem 2.3.1

$u \in \mathbb{Z}$ olmak üzere $144u^2 \pm 12u + 1$ ifadesinin asal bölenleri $p \equiv 1 \pmod{3}$ formundadır.

İspat. $u \in \mathbb{Z}$ keyfi ve $p \mid 144u^2 \pm 12u + 1$, $p \in \mathbb{P}$ asal olsun. Bu durumda yukarıdaki devre varlığının yeter şartı dikkate alındığında $Nor(2^4 \cdot 3^2 \cdot p)$ grubunda, $Nor(2^4 \cdot 3^2 \cdot p^2)'$ de olduğu gibi

$$= \begin{pmatrix} -2^4 \cdot 3^2 \cdot u & (144u^2 \pm 12u + 1)/p \\ -2^4 \cdot 3^2 \cdot p & 144u \pm 12u \end{pmatrix}$$

3. mertebeden eliptik üretecin varlığı bilinmektedir. Buradan [2] Teorem 2'nin sonucu olarak $p \equiv 1 \pmod{3}$ olduğu ortaya çıkar.

2.4. $N = 2^6 \cdot 3^2 \cdot p^2$

$N = 2^6 \cdot 3^2 \cdot p^2$ olsun.

$$\alpha = 6, \beta = 2, h = 2^{\min\{3,3\}} \cdot 3^{\min\{1,1\}} = 2^3 \cdot 3 = 24$$

$$N/h^2 = 2^6 \cdot 3^2 \cdot p^2 / 2^6 \cdot 3^2 = p^2, e = 1 \vee p^2$$

$$T_1 = \begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix}, \quad T_2 = \begin{pmatrix} ap^2 & b/24 \\ 24p^2c & dp^2 \end{pmatrix},$$

$$ad - bcp^2 = 1 \quad \quad \quad adp^4 - bcp^2 = p^2$$

Tablo 5. $2^6 \cdot 3^2 \cdot p^2$ için bölen sayısı $7 \times 3 \times 3 = 63$

1	2	2^2	2^3	2^4	2^5	2^6
p	$2 \cdot p$	$2^2 \cdot p$	$2^3 \cdot p$	$2^4 \cdot p$	$2^5 \cdot p$	$2^6 \cdot p$
p^2	$2 \cdot p^2$	$2^2 \cdot p^2$	$2^3 \cdot p^2$	$2^4 \cdot p^2$	$2^5 \cdot p^2$	$2^6 \cdot p^2$
3	$2 \cdot 3$	$2^2 \cdot 3$	$2^3 \cdot 3$	$2^4 \cdot 3$	$2^5 \cdot 3$	$2^6 \cdot 3$
$3 \cdot p$	$2 \cdot 3 \cdot p$	$2^2 \cdot 3 \cdot p$	$2^3 \cdot 3 \cdot p$	$2^4 \cdot 3 \cdot p$	$2^5 \cdot 3 \cdot p$	$2^6 \cdot 3 \cdot p$

Tablo 5' in devamı

$3.p^2$	$2.3.p^2$	$2^2.3.p^2$	$2^3.3.p^2$	$2^4.3.p^2$	$2^5.3.p^2$	$2^6.3.p^2$
3^2	2.3^2	$2^2.3^2$	$2^3.3^2$	$2^4.3^2$	$2^5.3^2$	$2^6.3^2$
$3^2.p$	$2.3^2.p$	$2^2.3^2.p$	$2^3.3^2.p$	$2^4.3^2.p$	$2^5.3^2.p$	$2^6.3^2.p$
$3^2.p^2$	$2.3^2.p^2$	$2^2.3^2.p^2$	$2^3.3^2.p^2$	$2^4.3^2.p^2$	$2^5.3^2.p^2$	$2^6.3^2.p^2$

Tablo 6. $(d, N/d)$ – durumları :

$d = 1$	$(1, 576p^2) = 1$	$\binom{1}{1}$
$d = 2$	$(2, 288p^2) = 2$	$\binom{1}{2}$
$d = 4$	$(4, 144p^2) = 4$	$\varphi(4) = 2$ $\binom{1}{4}, \binom{3}{4}$
$d = 8$	$(8, 72p^2) = 8$	$\varphi(8) = 4$ $\binom{1}{8}, \binom{3}{8}, \binom{5}{8}, \binom{7}{8}$
$d = 16$	$(16, 36p^2) = 4$	$\varphi(4) = 2$ $\binom{1}{16}, \binom{15}{16}$
$d = 32$	$(32, 18p^2) = 2$	$\varphi(2) = 1$ $\binom{1}{32}$
$d = 64$	$(64, 9p^2) = 1$	$\binom{1}{64}$
$d = p$	$(p, 576p) = p$	$p - 1 \text{ tane } \binom{*}{p}$
$d = 2p$	$(2p, 288p) = 2p$	$p - 1 \text{ tane } \binom{*}{2p}$
$d = 4p$	$(4p, 144p) = 4p$	$2p - 2 \text{ tane } \binom{*}{4p}$
$d = 8p$	$(8p, 72p) = 8p$	$4p - 4 \text{ tane } \binom{*}{8p}$
$d = 16p$	$(16p, 36p) = 4p$	$2p - 2 \text{ tane } \binom{*}{16p}$
$d = 32p$	$(32p, 18p) = 2p$	$p - 1 \text{ tane } \binom{*}{32p}$
$d = 64p$	$(64p, 9p) = p$	$p - 1 \text{ tane } \binom{*}{64p}$
$d = p^2$	$(p^2, 576) = 1$	$\binom{1}{p^2}$
$d = 2p^2$	$(2p^2, 288) = 2$	$\binom{1}{2p^2}$
$d = 4p^2$	$(4p^2, 144) = 4$	$2 \text{ tane } \binom{*}{4p^2}$

Tablo 6' nin devamı

$d = 8p^2$	$(8p^2, 72) = 8$	$4 \text{ tane } \binom{*}{8p^2}$
$d = 16p^2$	$(16p^2, 36) = 4$	$2 \text{ tane } \binom{1}{16p^2}$
$d = 32p^2$	$(32p^2, 18) = 2$	$\binom{1}{32p^2}$
$d = 64p^2$	$(64p^2, 9) = 1$	$\binom{1}{64p^2}$
$d = 3$	$(3, 192p^2) = 3$	$\varphi(3) = 2$ $\binom{1}{3}, \binom{2}{3}$
$d = 6$	$(6, 96p^2) = 6$	$\varphi(6) = 2$ $\binom{1}{6}, \binom{2}{6}$
$d = 12$	$(12, 48p^2) = 12$	$4 \text{ tane } \binom{*}{12}$
$d = 24$	$(24, 24p^2) = 24$	$8 \text{ tane } \binom{*}{24}$
$d = 48$	$(48, 12p^2) = 12$	$4 \text{ tane } \binom{*}{48}$
$d = 96$	$(96, 6p^2) = 6$	$2 \text{ tane } \binom{*}{96}$
$d = 192$	$(192, 3p^2) = 3$	$2 \text{ tane } \binom{*}{192}$
$d = 3p$	$(3p, 192p) = 3p$	$2p - 2 \text{ tane } \binom{*}{3p}$
$d = 6p$	$(6p, 96p) = 6p$	$2p - 2 \text{ tane } \binom{*}{6p}$
$d = 12p$	$(12p, 48p) = 12p$	$4p - 4 \text{ tane } \binom{*}{12p}$
$d = 24p$	$(24p, 24p) = 24p$	$8p - 8 \text{ tane } \binom{*}{24p}$
$d = 48p$	$(48p, 12p) = 12p$	$4p - 4 \text{ tane } \binom{*}{48p}$
$d = 96p$	$(96p, 6p) = 6p$	$2p - 2 \text{ tane } \binom{*}{96p}$
$d = 192p$	$(192p, 3p) = 3p$	$2p - 2 \text{ tane } \binom{*}{192p}$
$d = 3p^2$	$(3p^2, 192) = 3$	$2 \text{ tane } \binom{*}{3p^2}$
$d = 6p^2$	$(6p^2, 96) = 6$	$2 \text{ tane } \binom{*}{6p^2}$
$d = 12p^2$	$(12p^2, 48) = 12$	$4 \text{ tane } \binom{*}{12p^2}$
$d = 24p^2$	$(24p^2, 24) = 24$	$8 \text{ tane } \binom{*}{24p^2}$
$d = 48p^2$	$(48p^2, 12) = 12$	$4 \text{ tane } \binom{*}{48p^2}$
$d = 96p^2$	$(96p^2, 6) = 6$	$2 \text{ tane } \binom{*}{96p^2}$
$d = 192p^2$	$(192p^2, 3) = 3$	$2 \text{ tane } \binom{1}{192p^2}$

Tablo 6' nin devamı

$d = 9$	$(9, 64p^2) = 1$	$\binom{1}{9}$
$d = 18$	$(18, 32p^2) = 2$	$\binom{1}{18}$
$d = 36$	$(36, 16p^2) = 4$	$2 \text{ tane } \binom{*}{36}$
$d = 72$	$(72, 8p^2) = 8$	$4 \text{ tane } \binom{*}{72}$
$d = 144$	$(144, 4p^2) = 4$	$2 \text{ tane } \binom{*}{144}$
$d = 288$	$(288, 2p^2) = 2$	$\binom{1}{2^5 3^2}$
$d = 576$	$(576, p^2) = 1$	$\binom{1}{2^6 3^2}$
$d = 9p$	$(9p, 64p) = p$	$p - 1 \text{ tane } \binom{*}{9p}$
$d = 18p$	$(18p, 32p) = 2p$	$p - 1 \text{ tane } \binom{*}{18p}$
$d = 36p$	$(36p, 16p) = 4p$	$2p - 2 \text{ tane } \binom{*}{36p}$
$d = 72p$	$(72p, 8p) = 8p$	$4p - 4 \text{ tane } \binom{*}{72p}$
$d = 144p$	$(144p, 4p) = 4p$	$2p - 2 \text{ tane } \binom{*}{144p}$
$d = 288p$	$(288p, 2p) = 2p$	$p - 1 \text{ tane } \binom{*}{288p}$
$d = 576p$	$(576p, p) = p$	$p - 1 \text{ tane } \binom{*}{576p}$
$d = 9p^2$	$(9p^2, 64) = 1$	$\binom{1}{9p^2}$
$d = 18p^2$	$(18p^2, 32) = 2$	$\binom{1}{18p^2}$
$d = 36p^2$	$(36p^2, 16) = 4$	$2 \text{ tane } \binom{*}{36p^2}$
$d = 72p^2$	$(72p^2, 8) = 8$	$4 \text{ tane } \binom{*}{72p^2}$
$d = 144p^2$	$(144p^2, 4) = 4$	$2 \text{ tane } \binom{*}{144p^2}$
$d = 288p^2$	$(288p^2, 2) = 2$	$\binom{*}{288p^2}$
$d = 576p^2$	$(576p^2, 1) = 1$	$\binom{*}{576p^2}$

$$\widehat{\mathbb{Q}}(2^6 \cdot 3^2 \cdot p^2) =$$

$$\binom{1}{1} \cup \binom{1}{2} \cup \binom{1}{2^5} \cup \binom{1}{2^6} \cup \binom{1}{3^2} \cup \binom{1}{2 \cdot 3^2} \cup \binom{1}{2^5 \cdot 3^2} \cup \binom{1}{2^6 \cdot 3^2} \cup \binom{1}{p^2} \cup \binom{1}{2 \cdot p^2}$$

$$\cup \binom{1}{2^5 \cdot p^2} \cup \binom{1}{2^6 \cdot p^2} \cup \binom{1}{3^2 \cdot p^2} \cup \binom{1}{2 \cdot 3^2 \cdot p^2} \cup \binom{1}{2^5 \cdot 3^2 \cdot p^2} \cup \binom{1}{2^6 \cdot 3^2 \cdot p^2}$$

$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ 'in $Nor(2^6.3^2.p^2)$ ile hareketine bakalım.

1.Tip $\begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix}$, $det = ad - bcp^2 = 1$

$$\begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{a+b/24}{24p^2c+d} = \frac{24a+b}{24(24p^2c+d)} \quad \dots (*)$$

1. $a, d - tek$ ve $12 \parallel b$, $c - tek$ ise $*$ = $\frac{2a+b_0}{2(24p^2c+d)} \in \begin{pmatrix} 1 \\ 2 \end{pmatrix}$

2. $4 \parallel d$ ve $3 \parallel b$ $a - tek$, $c - tek$ ise $*$ = $\frac{8a+b_0}{2^5(6p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2^5 \end{pmatrix}$

3. $8 \parallel d$ ve $3 \parallel b$ $a - tek$, $c - tek$ ise $*$ = $\frac{8a+b_0}{2^6(3p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2^6 \end{pmatrix}$

4. $3 \parallel d$ ve $8 \parallel b$ $a - tek$, $c - tek$ ise $*$ = $\frac{3a+b_0}{3^2(8p^2c+d_0)} \in \begin{pmatrix} 1 \\ 3^2 \end{pmatrix}$

5. $3 \parallel d$ ve $4 \parallel b$ $a - tek$, $c - tek$ ise $*$ = $\frac{6a+b_0}{2.3^2(8p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2.3^2 \end{pmatrix}$

6. $12 \parallel d$ ve $b, c - tek$ ise $*$ = $\frac{24a+b}{2^5.3^2(2p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2^5.3^2 \end{pmatrix}$

7. $24 \parallel d$ ve $a, b, c - tek$ ise $*$ = $\frac{24a+b}{2^6.3^2(p^2c+d_0)} \in \begin{pmatrix} 1 \\ 2^6.3^2 \end{pmatrix}$

2. tip elemanlar ve a, b, c, d nin aynı seçimleri ile diğer yörüngeler benzer şekilde hesaplanır.

$$h = 24 \quad N/h^2 = p^2 \quad \text{old} \quad \rho = 1$$

$$\varepsilon_1 = 1 \quad , \quad \varepsilon_2 = 1 \quad \text{old} \quad \tau = 2$$

$$\text{İndeks} = 2.576.2$$

$$H = \Gamma_C(2^6.3^2.p^2) \text{ seçilirse } |\Gamma_B(N): \Gamma_C(N)| = 2 \quad , \quad G_\infty = \langle \begin{pmatrix} 1 & 1/24 \\ 0 & 1 \end{pmatrix} \rangle$$

$$[0] = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^5 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^6 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2.3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^5.3^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^6.3^2 \end{pmatrix}$$

$$[\infty] = \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2.p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^5.p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^6.p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3^2.p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2.3^2.p^2 \end{pmatrix}$$

$$\cup \begin{pmatrix} 1 \\ 2^5.3^2.p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^6.3^2.p^2 \end{pmatrix}$$

$\Gamma_C(2^4.3^2.p^2)$ 'deki üç tip eleman:

$$T_1 = \begin{pmatrix} a & b \\ 576p^2c & d \end{pmatrix} \in \Gamma_0(N) , \quad \underbrace{ad}_{\text{tek}} - bcp^2 \cdot 576 = 1$$

$$T_{2,3} = \begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \in \Gamma_c(N) , \quad \underbrace{\underbrace{ad}_{\text{tek}}}_{\substack{\vee \\ \text{\tiny çift} \\ \text{\tiny olabilir}}} - bcp^2 = 1$$

Kenar : r/s , $x/y \in [\infty]$, $r/s \mapsto x/y \in F(\infty, u/p^2) \Leftrightarrow$

$$(i) \quad 576p^2 \parallel s \Rightarrow x \equiv \pm ur \pmod{p^2}, y \equiv \pm us \pmod{p^2}, ry - sx = \pm p^2$$

$$(ii) \quad 24p^2 \parallel s \Rightarrow x \equiv \pm 24ur \pmod{p^2}, y \equiv \pm 24us \pmod{p^2}, ry - sx = \pm 24 p^2$$

$$(iii) \quad p^2 \parallel s \Rightarrow x \equiv \pm 576ur \pmod{p^2}, y \equiv \pm 576us \pmod{p^2}, ry - sx = \pm p^2$$

İspat : $r/s \mapsto x/y \in F(\infty, u/p^2)$ ve

I. durum

$2^6 \cdot 3^2 \cdot p^2 \parallel s$ olsun. Bu durumda $(\infty, u/p^2) \xrightarrow{T} (r/s \mapsto x/y)$ olan $T = T_1$

$$\begin{pmatrix} a & b \\ 576p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{576p^2c} = \frac{r}{s} \xrightarrow{a\text{-tek}} \begin{cases} r = a \\ s = 576p^2c \end{cases}$$

$$\begin{pmatrix} a & b \\ 576p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{\overset{r}{\tilde{a}}u + bp^2}{\underbrace{576p^2cu + dp^2}_s} \Rightarrow \begin{cases} x \equiv ur \pmod{p^2} \\ y \equiv us \pmod{p^2} \end{cases}$$

$$ry - sx = p^2$$

II. durum

$2^3 \cdot 3 \cdot p^2 \parallel s$ olsun. Bu durumda

$$T_2 = \begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} , \quad ad - \text{tek} \quad \text{olur.}$$

$$\begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{24p^2c} = \frac{r}{s} \xrightarrow{a\text{-tek}} \begin{cases} r = a \\ s = 24p^2c \end{cases}$$

$$\begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \frac{au + bp^2/24}{24p^2cu + dp^2} = \frac{24au + bp^2}{576p^2cu + 24dp^2} = \frac{x}{y}$$

$$x \equiv 24ur \pmod{p^2} \quad y \equiv 24us \pmod{p^2}$$

$$\begin{pmatrix} 24a & b \\ 24p^2c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} 24a & 24au + bp^2 \\ 24p^2c & 24p^2cu + dp^2 \end{pmatrix} = \begin{pmatrix} 24r & x \\ s & y/24 \end{pmatrix}$$

$$\det = 24 \quad \det = p^2 \quad \quad \quad ry - sx = 24p^2$$

III. durum

$p^2 \parallel s$ olsun. Bu durumda

$$T_3 = \begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \text{ ve } 24|a \text{ olsun.}$$

$$\begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{24p^2c} \frac{a_0}{24|a} \frac{a_0}{p^2c} = \frac{r}{s} \Rightarrow \begin{cases} r = a_0 \\ s = p^2c \end{cases}$$

$$\begin{aligned} \begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} &= \frac{au + bp^2/24}{24p^2cu + dp^2} \\ &= \frac{24au + bp^2}{576p^2cu + 24dp^2} \frac{576a_0u + bp^2}{24|a} \frac{576a_0u + bp^2}{576p^2cu + 24dp^2} = \frac{x}{y} \\ &\Rightarrow \begin{cases} x \equiv 576ur \pmod{p^2} \\ y \equiv 576us \pmod{p^2} \end{cases} \end{aligned}$$

$$\begin{aligned} \begin{pmatrix} a & b/24 \\ 24p^2c & d \end{pmatrix} \times 24 &= \begin{pmatrix} 24a & b \\ 576p^2c & 24d \end{pmatrix} = \begin{pmatrix} 576\widehat{a_0}^r & b \\ 576\widehat{p^2c}_s & 12d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u & p^2 \end{pmatrix} \\ &= \begin{pmatrix} 576r & x \\ 576s & y \end{pmatrix} \xrightarrow{\div 576} ry - sx = \pm p^2 \end{aligned}$$

Devre : Üçgen içerir $\Leftrightarrow 576u^2 \pm 24u + 1 \equiv 0 \pmod{p^2}$

İspat : Transitif hareketten :

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{x}{yp^2} \rightarrow \frac{1}{0}, \quad y = 1 \text{ veya } 24$$

1. durum

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{x}{p^2} \rightarrow \frac{1}{0} \text{ olsun.}$$

2. kenardan , $p^2 \parallel s$ old. $up^2 - xp^2 = -p^2$

$$\Rightarrow u - x = -1$$

$$\Rightarrow x = u + 1$$

Üstelik, $u + 1 \equiv -576u^2 \pmod{p^2}$

$$576u^2 + u + 1 \equiv 0 \pmod{p^2} \dots (1)$$

3. kenardan , $p^2 \parallel s$ old. $1 \equiv -576u(u + 1) \pmod{p^2}$

$$576u^2 + 576u + 1 \equiv 0 \pmod{p^2} \dots (2)$$

(1) ve (2)' den $575u + 1 \equiv 0 \pmod{p^2}$

$$23.25. u + 1 \equiv 0 \pmod{p^2}$$

$$\Rightarrow p = 5 \text{ yani } p \equiv 1(4) , p \equiv 1(mod 3) \text{ ile çelişir.}$$

Diğer $p \in \mathbb{P}'$ ler $(u, p^2) = 1$ olduğundan olamaz.

2. durum

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{x}{24p^2} \rightarrow \frac{1}{0} \text{ olsun.}$$

2. kenardan $24up^2 - xp^2 = -p^2$

$$\Rightarrow x = 24u + 1$$

3. kenardan, $\frac{24u+1}{24p^2} \rightarrow \frac{1}{0}$

$$1 \equiv -24u(24u + 1) \pmod{p^2}$$

Sonuç : $576u^2 + 24u + 1 \equiv 0 \pmod{p^2}$

Teorem 2.4.1

$u \in \mathbb{Z}$ olmak üzere $576u^2 \pm 24u + 1$ ifadesinin asal bölenleri $p \equiv 1(mod 3)$ formundadır.

İspat. $u \in \mathbb{Z}$ keyfi ve $p \mid 576u^2 \pm 24u + 1$, $p \in \mathbb{P}$ asal olsun. Bu durumda yukarıdaki devre varlığının yeter şartı dikkate alındığında $Nor(2^6.3^2.p)$ grubunda, $Nor(2^6.3^2.p^2)'$ de olduğu gibi

$$= \begin{pmatrix} -2^6.3^2.u & (576u^2 \pm 24u + 1)/p \\ -2^6.3^2.p & 576u \pm 24u \end{pmatrix}$$

3. mertebeden eliptik üretecin varlığı bilinmektedir. Buradan [2] Teorem 2'nin sonucu olarak $p \equiv 1(mod 3)$ olduğu ortaya çıkar.

3. İRDELEME

Bir grubun bir küme üzerine etkisi çalışılırken bazı ek cebirsel yapılar inşa etmekte mümkündür. Bunlar içinde en çok uygulananlardan biri çizgelerdir. Çizge, köşeler ve bu köşeleri birbirine bağlayan kenarlardan oluşan bir tür ağ yapısıdır. Bu tez çalışmasında kompleks analizden iyi bilinen doğrusal kesirli lineer dönüşümlerin bazı özel alt sınıflarının genişletilmiş rasyonel sayılar kümesi üzerindeki geçişli grup etkisinin ortaya çıkardığı *yörünge çizgeleri* ele alınmıştır. Bu yaklaşım literatürde ilk kez 1967’de C. C. Sims tarafından uygulanmıştır.

Öte yandan kombinatorik, sonlu soyut nesneleri ele alıp, belli kriterleri sağlayan nesnelerin sayılması veya optimum nesnelerin bulunması problemlerini temel alır. 1991’de Jones, Singerman ve Wicks modüler grubun grup etkisi neticesinde ortaya çıkan yörünge çizgelerinin Farey çizgelerinin bir genellemesi olduğunu gösterip, bu çizgelerdeki kombinatorial problemleri ele aldılar. Bu çalışmada ise bir başka Fuchs grubunun grup etkisi ve yörünge çizgeleri ele alınmış, sayılar teorisindeki sonuçları üzerinde durulmuştur.

Bu tezdeki sonuçlar 118F018 kodlu “Bir Tür Modüler Grup için Altyörüngesel Graf Karakterizasyonu” adlı TÜBİTAK-1002 projesinde kullanılmıştır.

4. SONUÇLAR

Bu tez çalışmasında

- $64u^2 + 8u + 1 \equiv 0 \pmod{p}$
- $144u^2 + 12u + 1 \equiv 0 \pmod{p}$
- $576u^2 + 24u + 1 \equiv 0 \pmod{p}$

tipindeki kongrüans denklemlerinin çözümlerinin $p \equiv 1 \pmod{3}$ formunda olduğu ispat edildi. Burada sayılar teorisindeki klasik metotlar yerine Möbiüs dönüşümlerinin bazı özel alt sınıflarının grup özellikleri ve Farey çizgeleri kullanıldı. İzlenen yöntemde C.B. Fine'in "Bir p – asalı iki kare toplamı olarak ifade edilebilir $\Leftrightarrow -1 \pmod{p}$ ye göre bir quadratik rezidü ise. $(\exists x \in \mathbb{Z}: x^2 \equiv -1 \pmod{p})$ " teoremini kanıtlamak için,

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

modüler grubun grup yapısını kullanması gibi, yine bu çalışmada da

$$\Gamma_B(N) = \left\{ \begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix} \middle| \begin{array}{l} \text{tüm harfler tamsayı,} \\ \det = e \\ e \parallel N/h^2 \text{ şartını sağlayan } 24\text{'ün en büyük böleni} \end{array} \right\}$$

normalliyen grubunun üreteçlerinden istifade edildi. Böylece asal sayı sıklığının araştırılma probleminde $\zeta(z)$ -Riemann zeta fonksiyonunun oynadığı başat rol gibi, bir başka kompleks değerli fonksiyon, doğrusal kesirli lineer dönüşümlerin kimi kongrüans denklemlerinin çözümünü verebileceği ortaya kondu.

5. ÖNERİLER

Bu tez çalışmasında ilgili grup hareketi için $\Gamma_0(N)$ 'nin $PSL(2, \mathbb{R})$ 'deki normalliyeni kullanılmıştır. J. Conway'in "Understanding groups like $\Gamma_0(N)$ " makalesinde belirtildiği gibi sonlu üretilmiş ayrık(diskret) grupların birçoğu ile cebir ve sayılar teorisindeki önemlerine atfen literatürde pek çok çalışma yapılmıştır. Ancak bunların çoğu klasik cebirsel metotlar kullanılarak grup yapısının özelliklerinin anlaşılması üzerinedir. Oysa bu çalışmada grup hareketinin ürettiği çizgeler temel alınmış ve sayılar teorisine ait sonuçlar elde edilmiştir. Dolayısıyla yukarıda bahsi geçen "benzer gruplar" alınarak grup hareketinin ürettiği çizgeler çalışılabilir. Örneğin

$$R(z) = -\frac{1}{z} \text{ ve } T(z) = z + \lambda; \lambda \in \mathbb{R}, \lambda \geq 2 \text{ veya } \lambda = \lambda_q = 2\cos\left(\frac{\pi}{q}\right), q \in \mathbb{N}, q \geq 3$$

doğrusal kesirli lineer dönüşümlerin ürettiği ve " $PSL(2, \mathbb{R})$ 'nin ayrık alt gruplarını bulma" probleminin cevabı olan $H(\lambda)$ -Hecke grupları çalışılabilir. Literatürde Hecke gruplarının çizgelerinin çalışıldığı yayınlar vardır. Ancak bunlar $1 \leq \lambda < 2$ durumlarının ele alındığı kısıtlanışlardır($\lambda = 1$ durumu, $H(1) = \Gamma$ -Modüler gruba tekabül eder), $\lambda \geq 2$ durumu hala açık problemdir. Yine Γ 'nın $\Gamma(n), \Gamma_1(n), \Gamma_0(n)$ temel kongrüans alt gruplarının çalışıldığı gibi $H(\lambda)$ 'nın

$$\begin{aligned} \Gamma_p(\sqrt{m}) &= \{T \in H(\sqrt{m}) \mid T \equiv \pm I(p)\} \\ &= \left\{ \begin{pmatrix} a & \sqrt{m}b \\ \sqrt{m}c & d \end{pmatrix} : \begin{matrix} a \equiv d \equiv \pm 1(p) \\ b \equiv c \equiv 0(p) \end{matrix} \mid ad - bcm = 1 \right\} \end{aligned}$$

temel kongrüans alt grupları çalışılabilir. Bu istikametin önemi gelince, (G, Ω) transitif permütasyon grubu ele alınırken grup kadar, üzerinde hareket edilen küme de oldukça önemlidir. Γ ve $Nor(N)$ grupları için cusp kümesi $\widehat{\mathbb{Q}}$ idi. Ancak başka grup seçimleri farklı cusp kümelerini beraberinde getirecektir. Örneğin Hecke gruplarında λ' ya bağlı olarak $\widehat{\mathbb{Q}}(\sqrt{d})$ kuadratik cisimleri ile çalışılması muhtemeldir. Böylece Fine'in iki kare toplamını tamsayılarda ispatladıktan sonra aynı problemi "kare toplam halkaları" diye adlandırdığı halkalara genişletmesi gibi, buradaki sonuçlar ve benzerlerini başka sayı cisimlerine genişletme olanağı ortaya çıkacaktır.

6. KAYNAKLAR

1. Akbaş, M., The Normalizer of Modular Subgroups, Ph. D. Thesis, University of Southampton, 1989.
2. Akbaş, M. ve Singerman, D., The signature of the normalizer of $\Gamma_0(N)$, London Math. Soc., Lecture Notes, CUP, Cambridge, 165 (1992) 77-86.
3. Akbaş, M. ve Başkan, T., Suborbital Graphs for the Normalizer of $\Gamma_0(N)$, Tr. J. Of Math., 20 (1996) 379-387.
4. Akbaş, M., On Suborbital Graphs for The Modular Group, Bull. London Math. Soc., 33 (2001) 647-652.
5. Anderson James W., Hyperbolic Geometry, Springer-Verlay, 2000.
6. Beşenk, M., Simge Devirleri ve Graflar, Doktora Tezi, K.T.Ü, Fen Bilimleri Enstitüsü, Trabzon, 2009.
7. Beşenk, M., Güler, B. Ö., Değer, A. H. ve Kesicioğlu, Y., Circuit lengths of graphs for the Picard group. J. Inequal. Appl., 2013 (2013)106, 8.
8. Conway, J. H. ve Norton, S. P., Monstrous Moonshine, Bull. London Math. Soc., 11 (1979) 3, 308–339.
9. Fine, B., The HNN and Generalized Free Product Structure of Certain Linear Groups, Bull. A.M.S., 81 (1975), 413–416.
10. Fine, B., A Note on Quadratic Residues and Sums of Squares, submitted, Proceedings of AMS., (1976).
11. Fine, B., A Note on the Two-Square Theorem, Canad. Math. Bull., 20, 1 (1977) 93-94.
12. Fine, B., Sum of Squares Rings, Canadian Journal of Mathematics, 29, 1 (1977) 155-160.
13. Güler, B.Ö., $\Gamma_0(N)$ Kongrüans Alt Grubunun $PSL_2(\mathbb{R})$ deki Normalliyenin Alt Yörüngesel Grafları, Doktora Tezi, K.T.Ü, Fen Bilimleri Enstitüsü, Trabzon, 2006.
14. Güler, B. Ö., Beşenk, M., Değer, A. H. ve Kader, S., Elliptic elements and circuits in suborbital graphs. Hacet. J. Math. Stat., 40, 2 (2011) 203–210.
15. Güler, B. Ö., Beşenk, M., Kesicioğlu, Y. ve Değer, A. H., Suborbital graphs for the group Γ^2 , Hacet. J. Math. Stat., 44 (2015) 1033-1044.
16. Güler, B. Ö., Köroğlu, T. ve Şanlı, Z., Solutions to some congruence equations via suborbital graphs, Springerplus, 1327, 5 (2016) 1-11.

17. Güler, B. Ö., Beşenk, M. ve Kader, S., On congruence equations arising from suborbital graphs, Turkish J. Math., 43, 5 (2019) 2396-2404.
18. Hardy, G. H. ve Wright, E. M., An introduction to the Theory of Numbers, Oxford University Press, Oxford, 1979.
19. Hungerford, T.W., Algebra, Springer-Verlag, New York, 1989.
20. Jaipong, P. ve Tapanyo, W., Generalized classes of suborbital graphs for the congruence subgroups of the modular group, Algebra Discrete Math., 27, 1 (2019) 20–36.
21. Jaipong, P. ve Promduang, W., Chaichana, K., Suborbitalgraphs of the congruence subgroup $\Gamma_0(N)$, Beitr. Algebra Geom., 60 (2019), no. 1, 181–192.
22. Jones, G.A. ve Singerman, D., Complex Functions: An Algebraic and Geometric Viewpoint, Cambridge University Press, Cambridge, 1987.
23. 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.
24. Kader, S., Güler, B. Ö. ve Deger, A. H., Suborbital graphs for a special subgroup of the normalizer of $\Gamma_0(m)$, Iran. J. Sci. Technol. Trans. A Sci., 34, 4 (2010) 305–312.
25. Kader, S. ve Güler, B. Ö., On Suborbital Graphs for the Extended Modular Group $\hat{\Gamma}$, Graphs Combin., 29, 6 (2013) 1813–1825.
26. Kader, S., Circuits in suborbital graphs fort he normalizer, Graphs Combin., 33, 6 (2017) 1531–1542.
27. Karataş, B. ve Aktaş H., Sayılar Teorisi, Gaziosmanpaşa Üniversitesi, Fen-Edebiyat Fakültesi, Ders Notları Serisi 3, Tokat, 1998.
28. Kesicioğlu, Y., Akbaş, M. ve Beşenk, M., Connectedness of a suborbital graph for congruence subgroups, J. Inequal. Appl., 2013, 117 (2013) 7.
29. Keskin, R., Suborbital Graphs for the Normalizer of $\Gamma_0(m)$, European Juornal of Combinatorics, 27, 2 (2006) 193-206.
30. Keskin, R. ve Demirturk, B., On Suborbital Graphs for the Normalizer of $\Gamma_0(N)$, Electronic Journal of Combinatorics, 16, 1 (2009) R116.
31. Koroğlu, T., Güler, B. Ö. ve Şanlı, Z., Suborbital graphs for the Atkin-Lehner group, Turkish J. Math., 41, 2 (2017) 235–243.
32. Kulkarni, R.S., An Arithmetic–geometric Method in the Study of the Subgroups of the Modular Group, American J. Math., 113, 6 (1991) 1053-1133.
33. Legh, W. R., The Elements of The Theory of Algebraic Numbers, New York, (1918).

34. Lehner, J. ve Newman, M., Weierstrass Points of $\Gamma_0(n)$, Ann. of Math., 79, 2 (1964) 360–368.
35. Lehner, J., Discontinuous Groups and Automorphic Functions Math, Amer. Math. Soc., 8 (1964).
36. Lehner, J., A Short Course in Automorphic Functions, Holt, Rinehart and Winston, London, 1966.
37. Lehner, J. ve Newman, M., Real two-dimensional representations of the free product of two finite cyclic groups, Proc. Cambridge Philos. Soc., 62 (1966), 135–141.
38. Leveque, W.J., Fundamentals of Number Theory, Addison-Wesley, Reading, Mass., 1977.
39. Massey, W.S., A Basic Course in Algebraic Topology, Graduate Texts in Mathematics, 127. Springer-Verlag, New York, 1991.
40. Newman, M., The normalizer of certain modular subgroups. Canad. J. Math., 8 (1956) 29–31.
41. Newman, M., Integral Matrices, Academic Press, New York, 1972.
42. Schoneberg, B., Elliptic Modular Functions, Springer Verlag, Berlin, 1974.
43. Sims, C.C., Graphs and Finite Permutation Groups, Mathematische. Zeitschrift., 95 (1967) 76-86.
44. Singerman, D., Subgroups of Fuchsian groups and finite permutation groups, Bull. London Math.Soc., 2 (1970) 319-323.
45. Tunç, T., Modüler Grup ve Bir Özel Kongrüans Alt Grubunun Grafları, Yüksek Lisans Tezi, K.T.Ü., Fen Bilimleri Enstitüsü, Trabzon, 2013.
46. Yazıcı, N., Modüler Grubun Picard Grubundaki Normalleyeninin Alt Yörüngesel Grafları, Yüksek Lisans Tezi, K.T.Ü., Fen Bilimleri Enstitüsü, Trabzon, 2013.
47. Yazıcı Gözütok, N. ve Güler, B. Ö., Quadrilateral cell graphs of the normalizer with signature $(2, 4, \infty)$, Studia Scientiarum Mathematicarum Hungarica, 57, 3 (2020) 408-425.
48. Yıldız, F., Aritmetiğin Temel Teoreminin İspatı.
<http://www.fedget.com/aritmetigin-temel-teoreminin-ispatti/> 10.12.2020

ÖZGEÇMİŞ

2012-2013 Eğitim-Öğretim yılında Karadeniz Teknik Üniversitesi Fen Fakültesi Matematik Bölümüne girdi. 2017 yılında Karadeniz Teknik Üniversitesi Matematik Bölümü lisans eğitimini üçüncülükle ve bununla birlikte Karadeniz Teknik Üniversitesi Fatih Eğitim Fakültesi'nde pedagojik formasyonunu tamamlayarak mezun oldu.

2017-2018 Eğitim-Öğretim yılında Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı Tezli Yüksek Lisans programını kazandı. Yabancı dili İngilizcedir.

