KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

NEC GRUPLARIN SİMGELERİ VE GRAFLAR

DOKTORA TEZİ

Serkan KADER

MART 2008
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

NEC GRUPLARIN SİMGELERİ VE GRAFLAR

Serkan KADER

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

Tezin Enstitüye Verildiği Tarih : 27.02.2008
Tezin Savunma Tarihi : 28.03.2008

Tez Danışmanı : Prof. Dr. Mehmet AKBAŞ
Jüri Üyesi : Prof. Dr. Zameddin İSMAYILOV
Jüri Üyesi : Prof. Dr. Hilmi ZENGİN
Jüri Üyesi : Prof. Dr. Abdullah ÇAVUŞ
Jüri Üyesi : Prof. Dr. Metin BAŞARIR

Enstitü Müdür V. : Doç. Dr. Salih TERZİOĞLU

Trabzon 2008

ÖNSÖZ

Bu çalışmada, $\mathcal{N}or(p)$ nin ve $\hat{\Gamma}$ genişletilmiş modüler grubun alt yörüngesel grafları incelendi.

Öncelikle, tez konusunu seçen ve çalışma süresince yardımlarını esirgemeyen sayın hocam Prof. Dr. Mehmet AKBAŞ a teşekkür eder, saygılarımı sunarım.

Tez önerisi ve raporlar aşamasındaki yardımlarından dolayı Prof. Dr. Zameddin ISMAYILOV' a ve Prof. Dr. Hilmi ZENGİN' e şükranlarımı sunarım.

Çalışma süresi boyunca moral desteklerinden ötürü başta Yrd. Doç. Dr. Atakan T. YAKUT, Yrd. Doç. Dr. Bahadır Ö. GÜLER, Arş Gör. Ahmet KAYA olmak üzere Arş. Gör. Yavuz KESİCİOĞLU'na, Neslihan B. SACİHAN'a, Murat BEŞENK'e, KTÜ Matematik Bölümündeki tüm hocalarıma, başta Arş. Gör. Ali Hikmet DEĞER ve Arş. Gör. Mehmet KUNT olmak üzere tüm Araştırma Görevlisi arkadaşlarıma, ayrıca eşim Esma'ya ve benim yetişmem uğrunda her türlü zorluklara katlanan ve desteklerini hiç esirgemeyen anneme, babama ve ablalarıma çok teşekkür ederim.

Serkan KADER
Trabzon 2008

İÇİNDEKİLER

ÖZET

Bu çalışmada, esas amacımız PSL$(2,\mathbb{R})$ nin bazı ayrık alt gruplarının simgesini elde etmektir.

Birinci bölümde Öklid olmayan kristalize grupların yapısı irdelendi. PSL$(2,\mathbb{R})$, Γ-Modüler grubu, kongrüans alt gruplarının bazı özellikleri, bu kongrüans alt gruplarının normalliyenleri ve ayrıca ayrık gruplar, Riemann yüzeyleri, temel bölgeler, graf teori, imprimitif hareket ile ilgili ihtiyaç duyduğumuz temel tanımlar verildi.

İkinci bölümde $\mathcal{N}or(p)$ nin alt yörüngesel grafları göz önüne alındı. Daha sonra $\hat{\Gamma}$ genişletilmiş modüler grubun $\hat{\mathbb{Q}}$ üzerinde transitif ve imprimitif olarak hareket ettiği gösterildi. $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ daki yörünge sayısı hesaplandı. Ayrıca $\hat{\Gamma}$ nın $\hat{\mathbb{Q}}$ üzerindeki hareketiyle oluşan grafta kenar ve devre şartları belirlendi.

Anahtar Kelimeler: PSL$(2,\mathbb{R})$, Γ, $\mathcal{N}or(p)$, $\hat{\Gamma}$, $\hat{\Gamma}_0(N)$, Transitif permütasyon grubu, Alt Yörüngesel Graf

SUMMARY

Signatures of the NEC Groups and Graphs

In this thesis, our main purpose is to find signatures of some Fuchsian groups of the group PSL$(2,\mathbb{R})$ by considering suborbital graphs.

In Chapter 1, the structure of Non-Euclidean Crystalllographic Groups is discussed and some properties of PSL$(2,\mathbb{R})$, Γ-Modular group, congruence subgroups, normalizers of the congruence subgroups and also the preliminary definitions we require for discrete groups, Riemann surfaces, fundamental domains, graph theory and imprimitive action are given.

In Chapter 2, the suborbital graphs of $\mathcal{N}or(p)$ are examined. It is shown that $\hat{\Gamma}$ acts transitively and imprimitively on $\hat{\mathbb{Q}}$ and then the number of orbit of $\hat{\Gamma}_0(N)$ in $\hat{\mathbb{Q}}$ is calculated. Moreover, edge and circuit conditions on the graph arising from the action of $\hat{\Gamma}$ on $\hat{\mathbb{Q}}$ are determined.

Key Words: PSL$(2,\mathbb{R})$, Γ, $\mathcal{N}or(p)$, $\hat{\Gamma}$, $\hat{\Gamma}_0(N)$, Transitive permutation group, Suborbital graph

ŞEKİLLER DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

$\mathbb{C}$	: Kompleks sayılar kümesi
$\mathbb{C}_\infty$	: Genişletilmiş kompleks sayılar kümesi (Riemann Küresi)
$\varphi(a)$	: Euler fonksiyonu
Γ	: Modüler grup
$\Gamma_0(N)$	: Γ nın $N\mid c$ olan bir alt grubu
$\hat{\Gamma}$	: Genişletilmiş Modüler grup
$\hat{\Gamma}_0(N)$	: $\hat{\Gamma}$ nın $N\mid c$ olan bir alt grubu
$\mathcal{N}or(N)$	: $\Gamma_0(N)$ nin PSL(2,$\mathbb{R}$) deki normalliyeni
PSL(2,$\mathbb{R}$)	: Gerçel katsayılı, lineer, kesir dönüşümlerinin grubu
$\mathbb{R}$	: Reel sayılar kümesi
$\hat{\mathbb{R}}$	: Genişletilmiş reel sayılar kümesi
$\mathbb{Q}$	: Rasyonel sayılar kümesi
$\hat{\mathbb{Q}}$	: Genişletilmiş rasyonel sayılar kümesi
$\mathbb{Z}$	: Tam sayılar kümesi
$\mathbb{N}$	: Doğalsayılar kümesi
$\mathcal{U}$	: $\mathbb{C}$ de üst yarı düzlem
$A\subset B$	: A kümesi B kümesinin alt kümesidir
$A\backslash B$	: A kümesinin B kümesinden farkı
$A \leq B$	: A grubu B grubunun alt grubudur
$\lvert A:B \rvert$	: B alt grubunun A daki indeksi
$a\mid b$	: a sayısı b sayısını böler
$a\nmid b$	: a sayısı b sayısını bölmez
$a\parallel b$	: a sayısı b sayısının bir tam bölenidir
$a\equiv b(\mathrm{mod}\,n)$	: n sayısı $(a-b)$ sayısını böler
(a,b)	: a ile b sayısının en büyük ortak böleni

$\overset{\circ}{F}$	: F kümesinin içi
Gx	: x noktasının G -yörüngesi
G_x	: x noktasının G deki sabitleyeni
$\mu(E)$	: E kümesinin hiperbolik alanı
$l(C)$	: Parçalı, sürekli, diferansiyellenebilir bir C eğrisinin hiperbolik uzunluğu

1. GENEL BİLGİLER

1.1. Giriş

Ayrık gruplar teorisinde sonlu üretilmiş grupların simgelerinin elde edilmesi üzerine yapılmış çok sayıda çalışma vardır.

İlk olarak R. Fricke, $\mathrm{PSL}(2,\mathbb{R})$ nin $\Gamma_0(N)$ yi normalleştiren elemanlarına örnekler verdi. Fakat Lehner ve Newman' ın [17] çalışmalarına kadar normalliyen kavramı üzerinde pek fazla durulmadı. [17] de Lehner ve Newman $\Gamma_0(N)$ nin Weierstrass noktaları ile ilişkisini çalıştılar ve normalliyeni direkt olarak hesapladılar. Fakat normalliyenin elemanlarının net bir şekilde karakterize edilmesi Conway ve Norton [8] tarafından verildi.

1973 yılında Bernd Fischer ve Bob Griess'in, bağımsız olarak, mertebesi

$$2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$$

olan yeni bir basit M grubu için deliller üretmesi ve [10] da Robert L. Griess'in varlığını ispatlamasının ardından bu yeni basit grubun özellikle $\Gamma_0(N)$ nin $\mathrm{PSL}(2,\mathbb{R})$ deki normalliyeni ile ilgili olması normalliyeni tekrar ön plana getirmiştir.

Conway ve Norton, [8] de bu basit M grubunu *Monster* olarak adlandırdı. Daha sonra Ogg [20] de $|M|$ yi bölen p asalları için $\mathrm{PSL}(2,\mathbb{R})$ de $\mathcal{N}or(p)$ normalliyeninin belirlediği fonksiyon cisminin sıfır cinsine sahip olduğunu gösterdi. [22] de A. Pizer bu asalların, 2-ağırlıklı modüler formlarla quaternion cebir teta-serisini ilişkilendiren Hecke konjektürünü sağlayan yegane asallar olduğunu gösterdi.

[8] de Conway ve Norton

$$T_m = q^{-1} + 0 + H_1(m)q + H_2(m)q^2 + \ldots$$

serisinin $\Gamma_0(N)$ ile $\mathcal{N}or(N)$ arasındaki bir gruptan ortaya çıkan sıfır cinsli bir fonksiyon cisminin normalleştirilmiş üreteci olduğu ileri sürdü. Bu şekilde ortaya çıkan modüler gruplar belli bir doğal parametrizasyona sahiptir ve ayrıca Leech latisinin belli otomorfizmalarının özdeğerleri cinsinden ifade edilebilen modüler fonksiyonlar için pek çok formül vardır.

N karesiz ise, Helling [13] te $\mathcal{N}or(N)$ gruplarının maksimal ayrık gruplar olduğunu ve Γ modüler grubu ile orantılı olan her ayrık Δ grubunun bu gruplardan birine eşlenik olduğunu gösterdi. Ayrıca Δ ile belirlenen fonksiyon cisminin cinsi sıfır ise $\mathcal{N}or(N)$ ile belirli fonksiyon cisminin cinsi de sıfırdır ve eşlenik yapan her eleman

$$z \to \frac{pz+q}{r}; \quad p, q \text{ ve } r \text{ ortak çarpanı olamayan tam sayılar,}$$

biçimindedir.

Normalliyen, $\mathrm{PSL}(2,\mathbb{R})$ nin ayrık bir alt grubu ve sonlu üretilmiş olduğundan topolojik ve geometrik özelliklerini veren bir simgeye sahiptir. Bu simge problemi bir bakıma bir ayrık grubun kimliğidir. Bu kimlikteki periyotları (üretici eliptik elemanların mertebeleri) ve parabolik sınıf sayılarını bulma problemi ayrık gruplar üzerine çalışan bilim adamlarının bu yolda daha fazla çaba sarfetmelerini gerektirmektedir. *N* nin karesiz olması durumunda simge problemini Maclachlan [18] de çözmüştür. Fakat *N* nin keyfi olması durumu hala açıktır. Ancak [4] te Akbaş ve Singerman normalliyenin parabolik sınıf sayısı verdiler ve 3, 4 ve 6 mertebeli eliptik üretici elemanlar tam olarak belirlediler. Dolayısı ile geriye 2 mertebeli üretici elemanların sayısını ve *g* cinsini bulmak kalmıştır.

1.2. Topolojik Gruplar

Tanım 1.1. $(G,\cdot)$ bir grup ve aynı zamanda bir topolojik uzay olsun. Bu takdirde

i) $M : G\times G \longrightarrow G$, $(g,h) \longrightarrow g\cdot h$

ii) $m : G \longrightarrow G$, $g \longrightarrow g^{-1}$

dönüşümleri sürekli ise *G* ye bir *topolojik grup* denir.

Tanım 1.2. *G* bir topolojik grup ve *X* bir topolojik uzay olsun. Bu takdirde

$$\wedge : G\times X \longrightarrow X, \quad (g,x) \longrightarrow \wedge(g,x) =: g\wedge x$$

sürekli bir dönüşüm ve

(i) $g\wedge(h\wedge x) = gh\wedge x$, $g,h\in G,\ x\in X$

(ii) $e\wedge x = x$, $e\in G,\ x\in X$

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

Önerme 1.1. $\left[G, X\right]$ bir topolojik dönüşüm grubu ve $x,y \in X$ olsun. Bu takdirde

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

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

Tanım 1.3. "$\approx$" bağıntısının denklik sınıflarına *hareketin yörüngeleri* denir. Ayrıca $x \in X$ noktasını içeren yörüngeye *x-in yörüngesi* denir ve bu $Gx := \{gx \mid g \in G\}$ kümesidir.

Tanım 1.4. G, X üzerinde hareket etsin ve $x,y \in X$ keyfi olsun. $gx = y$ olacak biçimde bir $g \in G$ elemanı varsa G ye X üzerinde *transitif olarak hareket ediyor* denir.

Bu tanıma göre hareket transitif ise $\forall x \in X$ için $Gx = X$ elde edilir. Yani bir tek yörünge vardır.

Önerme 1.2. $\left[G, X\right]$ bir topolojik dönüşüm grubu olsun. $p : \begin{array}{ccc} X & \longrightarrow & X/G \\ x & \longrightarrow & Gx \end{array}$ dönüşümünü göz önüne alalım. Bu durumda

$$\text{"}U \subset X/G \text{ açıktır} :\Leftrightarrow p^{-1}(U) \subset X \text{ açıktır"}$$

tanımı ile verilen açık kümelerin topolojisi ile X/G ye bir *yörünge uzayı* diyeceğiz. p dönüşümü açıkça süreklidir ve *projeksiyon* olarak adlandırılır.

Tanım 1.5. G, X üzerinde hareket etsin ve $x \in X$ olsun. $G_x := \{g \in G \mid gx = x\}$ kümesine x noktasının *sabitleyeni* denir.

Tanım 1.6. G bir grup olsun. $C := \{g \in G \mid \forall x \in G \text{ için } gx = xg\}$ kümesine G nin *merkezi* denir.

Tanım 1.7. G bir grup olsun. $G = \langle a \rangle$ olacak şekilde bir $a \in G$ varsa G ye *bir devirli grup* denir.

Tanım 1.8. G bir grup ve $H < G$ olsun. $\mathcal{N}_G(H) := \left\{ g \in G \mid gHg^{-1} = H \right\}$ kümesine H nın G deki *normalliyeni* denir. Normalliyen, H yı normal alt grup olarak içeren en büyük kümedir.

Tanım 1.9. Bir T dönüşümünün *periyodu* (veya *mertebesi*) $T^m = I$ eşitliğini sağlayan en küçük pozitif tamsayıdır. Böyle bir m yoksa T ye *sonsuz periyotludur* denir.

Tanım 1.10. $N \in \mathbb{Z}$ için $1 \le a \le N$ ve $(a, N) = 1$ olan a tamsayılarının sayısı $\varphi(N)$ ile gösterilir. Bu fonksiyona *Euler fonksiyonu* denir.

$m = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$ ise bu takdirde

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right).$$

1.3. Öklid Olmayan Kristalize Gruplar

1) $\mathcal{G}$ ile $\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\}$ genişletilmiş kompleks düzlemin

$$\text{(A)} \quad \left\{ z \to \frac{az+b}{cz+d} \mid a,b,c,d \in \mathbb{R} \text{ ve } ad - bc = 1 \right\}$$

$$\text{(B)} \quad \left\{ z \to \frac{a\bar{z}+b}{c\bar{z}+d} \mid a,b,c,d \in \mathbb{R} \text{ ve } ad - bc = -1 \right\}$$

biçimindeki dönüşümlerin grubunu gösterelim. $\mathcal{G}$ nin her bir elemanı $\mathcal{U} := \{ z \in \mathbb{C} \mid \operatorname{Im} z > 0 \}$ üst yarı düzlemin kendi üzerine bir konform veya ters konform homeomorfizmasıdır.

(A) biçimindeki dönüşümlerin grubunu $\mathrm{PSL}(2,\mathbb{R})$ ile göstereceğiz. Bu grup $\mathcal{G}$ de 2 indeksli bir alt gruptur. $\mathcal{U}$ nun her konform homeomorfizmi $\mathrm{PSL}(2,\mathbb{R})$ dedir [14].

$\mathcal{G}$ üzerinde bir topolojik yapı aşağıdaki biçimde oluşturulabilir:

$\tau = \{(a,b,c,d) : ad - bc = \pm 1\} \subset \mathbb{R}^4$ alt kümesini alalım. Bu alt küme üzerinde $\mathbb{R}^4$ deki adi topolojinin kondurduğu alt uzay topolojisini göz önüne alalım. Bu τ alt uzayında (a,b,c,d) ile $(-a,-b,-c,-d)$ noktalarını özdeşleştirirsek $\mathcal{G}$, özdeşlik topolojisi ile bir topolojik grup yapısına sahip olur. $\mathcal{G}$ topolojik grubu $\mathrm{PSL}(2,\mathbb{R})$ ve $\mathcal{G} \setminus \mathrm{PSL}(2,\mathbb{R})$ olmak üzere iki bileşene sahiptir.

$\mathcal{G}$ nin ayrık alt gruplarına *Öklid olmayan kristalize gruplar*, kısaca *NEC grupları*, adı verilir. $\mathrm{PSL}(2,\mathbb{R})$ deki bir NEC grubuna ise bir *Fuchsian grup* denir. Eğer bir NEC grubu (B) türündeki elemanları yani ters yönlendirilmiş elemanları içeriyorsa buna *özel bir NEC grubu* diyeceğiz. $\mathcal{U}$ üst yarı düzlemi, Öklid olmayan (hiperbolik) düzlemin bir modeline aşağıdaki biçimde dönüştürülebilir:

Bir yay elemanının *ds* hiperbolik uzunluğu

$$ds^2 = \frac{dx^2 + dy^2}{y^2}$$

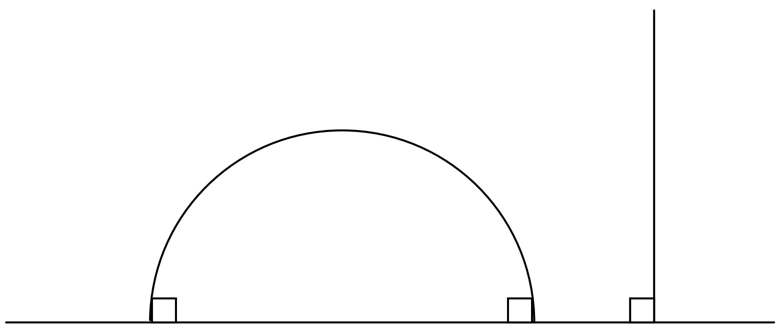
ile tanımlanır. Böylece parçalı, sürekli, diferansiyellenebilir bir C eğrisinin hiperbolik uzunluğu

$$l(C) := \int_C ds = \int_C \frac{\sqrt{dx^2 + dy^2}}{y}$$

ve ölçülebilir bir E kümesinin hiperbolik alanı

$$\mu(E) := \iint_E \frac{dxdy}{y^2}$$

olarak tanımlanır. Yukarıdaki metriğin geodezikleri, reel eksene dik yarı çemberler ve yarı doğrulardır. Bunlar *hiperbolik doğrular* olarak adlandırılır.



Şekil 1.1 Hiperbolik doğrular

$\mathcal{U}$ üst yarı düzlemde iki nokta arasındaki hiperbolik uzaklık, bu iki noktayı birleştiren bir tek hiperbolik doğru parçasının uzunluğudur. Bu metrikle tanımlanan topoloji, bilinen Öklid topolojisine eş değerdir. Yani bir topolojideki açık küme, diğer topolojide de açıktır. Hiperbolik uzaklık ve alan $\mathrm{PSL}(2,\mathbb{R})$ nin dönüşümleri altında invaryant kalır [14].

2) Şimdi $\mathcal{G}$ nin elemanlarını yön durumlarına ve sabit nokta kümelerine göre sınıflandıralım:

($\mathbf{A^*}$) $T \in \mathrm{PSL}(2,\mathbb{R})\backslash\{I\}$ dönüşümünün sabit noktalarını bulalım. Bunun için, $\dfrac{az+b}{cz+d}=z$ yazılırsa,

$$cz^2+\left(d-a\right)z-b=0 \tag{1}$$

denklemi elde edilir. Bu denklemin kökleri T nin sabit noktalarıdır. T nin en fazla iki sabit noktası vardır. (1) denkleminin kökleri ise,

$$z_{1,2}=\frac{-\left(d-a\right)\mp\sqrt{\left(a+d\right)^2-4}}{2c}$$

olarak bulunur. Burada üç durum söz konusudur;

1°) $|a+d|>2$ ise, iki farklı sabit nokta vardır ve bunlar $\mathbb{R}\cup\{\infty\}$ üzerindedirler. Bu durumda T ye bir *hiperbolik dönüşüm* adı verilir.

2°) $|a+d|=2$ ise, birbirine eşit iki sabit nokta vardır ve bunlar $\mathbb{R}\cup\{\infty\}$ üzerindedirler. Bu durumda T ye bir *parabolik dönüşüm* adı verilir.

3°) $|a+d|<2$ ise, birbirinin eşleniği olan iki kompleks sabit nokta vardır. Bu sabit noktalardan biri açıkça $\mathcal{U}$ kümesindedir. Bu durumda T -ye bir *eliptik dönüşüm* adı verilir.

($\mathbf{B^*}$) Şimdi de $T \in \mathcal{G}\setminus \mathrm{PSL}(2,\mathbb{R})$ olsun. Bu durumda $z=\dfrac{a\overline{z}+b}{c\overline{z}+d}$ yazılırsa

$$cz\overline{z}+dz-a\overline{z}-b=0 \tag{2}$$

denklemi elde edilir. (2) denkleminde $z=x+iy$ ve $\overline{z}=x-iy$ ifadeleri yerlerine yazılırsa,

$$c(x+iy)(x-iy)+d(x+iy)-a(x-iy)-b=0 \Rightarrow$$

$$c(x^2+y^2)+dx-ax+i(dy+ay)-b=0 \Rightarrow$$

$$\left.\begin{array}{r} c(x^2+y^2)+(d-a)x-b=0 \\ (d+a)y=0 \end{array}\right\}$$

biçiminde iki durum elde edilir. Bu iki durumu inceleyelim:

1°) $a+d \neq 0$ ise $y=0$ dır. Bu durumda $cx^2+(d-a)x-b=0$ denklemi elde edilir. Bu denklemin diskriminantı

$$\Delta=(d-a)^2+4bc=d^2-2ad+a^2+4bc$$

dir. Buradan $ad-bc=-1$ eşitliği kullanılırsa $\Delta=(a+d)^2+4>0$ elde edilir. Dolayısıyla T nin iki farklı sabit noktası vardır ve bunlar $\mathbb{R}\cup\{\infty\}$ üzerindedirler. Bu durumda T ye bir *kayan-yansıma* denir.

2°) $a+d=0$ ise $(a+d).y=0$ eşitliği özdeş olarak gerçekleşeceğinden $c(x^2+y^2)+(d-a)x-b=0$ eşitliği gereği T nin sabit noktaları kümesi bir çemberdir. $a+d=0$ ve $ad-bc=-1$ eşitlikleri yardımıyla bu çemberin merkezinin $\left(\frac{a}{c},0\right)$ ve yarıçapının $\frac{1}{|c|}$ olduğu görülür. Bu durumda T dönüşümüne bir *yansıma* adı verilir.

Buna göre $\mathcal{G}$ nin, hiperbolik, parabolik, eliptik, kayan-yansıma ve yansıma diye adlandırılan beş tip elemanı vardır.

Tanım 1.11. T_1 ve T_2 , $\mathcal{G}$ grubunun herhangi iki elemanı olsun. $T_1=TT_2T^{-1}$ olacak şekilde bir $T\in\mathcal{G}$ elemanı varsa T_1 ve T_2 birbirinin *eşleniğidir* denir.

Önerme 1.3. T_1 ve T_2 birbirinin eşleniği iseler aynı tiptendirler.

$\mathcal{G}$ nin elemanlarını *iz* (trace) lerine, $a+d$, ve ayrıca determinantlarına göre sınıflandırabiliriz.

$\mathcal{G}$ nin eşlenik elemanlarının aynı tip olduğu gerçeği kullanıldığında, dönüşümlerin her biri bir doğal gösterime sahiptir. Doğal gösterimler aşağıdaki şekilde sınıflandırılır:

Eleman Türü	Doğal Gösterim
Hiperbolik	$z \to \lambda z \quad (\lambda > 1)$
Eliptik	$z \to w, \quad \dfrac{w-i}{w+i} = e^{i\theta}\dfrac{z-i}{z+i}, \quad \theta \neq 2\mathrm{n}\pi$
Parabolik	$z \to z \pm 1$
Kayan-yansıma	$z \to \lambda \overline{z} \quad (\lambda < -1)$
Yansıma	$z \to -\overline{z}$

Tanım 1.12. Λ bir Fuchsian grubu olsun. Bu takdirde

$$\text{(i)} \ \bigcup_{T\in\Lambda} T(F) = \mathcal{U} \qquad \text{(ii)} \ \forall T \in \Lambda \setminus \{I\} \text{ için } \mathring{F} \cap T(\mathring{F}) = \varnothing .$$

şartlarını sağlayan F kapalı kümesine Λ için bir *temel bölge* adı verilir.

F yi iki şekilde elde edebiliriz:

Tanım 1.13 (Dirichlet Bölgesi**).** Λ bir NEC grup ve $p \in \mathcal{U}$, $\forall \gamma \in \Lambda \setminus \{I\}$ için $\gamma(p) \neq p$ koşulunu sağlayan bir nokta olsun. d hiperbolik metrik olmak üzere

$$F = \{ z \in \mathcal{U} \mid \forall g \in \Lambda \text{ için } d(z,p) \leq d(g(z),p) \}$$

kümesine, Λ için *Dirichlet Bölgesi* denir.

Tanım 1.14 (Ford Bölgesi**).** $\Lambda \leq \mathrm{PSL}(2,\mathbb{R})$, $T \in \Lambda$ ve $T(z) = \dfrac{az+b}{cz+d}$, $c \neq 0$ olsun. $I(T) : |cz+d|^2 = 1$ çemberi, T nin *izometrik çemberi* olarak adlandırılır. $|T'(z)| = 1 \Leftrightarrow z \in I(T)$ olduğundan izometrik çember, diferansiyel Öklid uzunluğunu değiştirmeden T ile dönüştürülen noktaların geometrik yeridir. F_∞; Λ da sonsuzun Λ_∞ sabitleyeni için bir temel bölge ve K; Λ nın tüm izometrik çemberlerinin dışında kalan bölge ise $F = F_\infty \cap K$, Λ için bir temel bölgedir.

Her sonlu üretilmiş Fuchsian grubu da aşağıdaki gibi bir gösterime sahiptir:

Üreticiler : $a_1, b_1, \ldots, a_g, b_g$ (hiperbolik)
$x_1, \ldots x_r$ (eliptik)
$p_1, \ldots, p_s$ (parabolik)

$$\text{Bağıntılar : } x_1^{m_1} = \ldots = x_r^{m_r} = \prod_{i=1}^{g} \mathrm{a}_i b_i a_i^{-1} b_i^{-1} \prod_{j=1}^{r} x_j \prod_{k=1}^{s} p_k = 1$$

$$\text{Simge : } (\ g\ ;\ m_1, \ldots, m_r\ ;\ s\ ).$$

Burada g-grubun cinsini, m_i- üretici eliptik elemanların mertebelerini ve s-parabolik sınıf sayısını temsil etmektedir. Simge, üzerinde çalışılan grubun invaryantlarını ortaya koyması bakımından son derece önemlidir [5].

Tanım 1.15. X bir bağlantılı, Hausdorff topolojik uzayı olsun. Bir $A \subset X$ ve $B \subset \mathbb{C}$ açık alt kümeler olmak üzere $\varphi : A \rightarrow B$ homoemorfizmasına X üzerinde bir *kompleks kart* ve (A, φ) çiftine X in bir *koordinat komşuluğu* denir.

Tanım 1.16. Eğer $\varphi_1 \circ \varphi_2^{-1} : \varphi_2(A_1 \cap A_2) \rightarrow \varphi_1(A_1 \cap A_2)$ fonksiyonu holomorf ise (A_1, φ_1) ve (A_2, φ_2) *koordinat komşulukları uyumludur* denir.

Tanım 1.17. Koordinat komşuluklarının bir $(A_i, \varphi_i)_{i \in I}$ ailesini alalım.

(1) $X = \cup(A_i)$

(2) $\forall (i,j) \in I \times I$ için (A_i, φ_i) ile (A_i, φ_j) uyumludur,

koşullarının sağlanması halinde $(A_i, \varphi_i)_{i \in I}$ ailesine bir *örtüm* adı verilir. İki örtümün birleşimlerinin de bir örtüm meydana getirmesi halinde bu *örtümler eşdeğerdir* denir. Bu örtümlerin kümesi üzerinde bir denklik bağıntısı tanımlanır ve denklik sınıfına da bir *kompleks yapı* adı verilir.

Tanım 1.18 (Riemann Yüzeyi**).** Bir bağlantılı Hausdorff topolojik uzayına bir kompleks yapıyla birlikte bir *Riemann yüzeyi* adı verilir.

Her noktasının bir komşuluğu $\mathbb{R}^2$ nin bir açık alt kümesine homeomorf olan bir bağlantılı Hausdorff uzayına bir *yüzey* adı verilir. Eliptik eleman içermeyen keyfi bir Λ-Fuchsian grubu da PSL($2, \mathbb{R}$) nin bir alt grubu olarak $\mathcal{U}$ üzerinde hareket eder ve bölüm topolojisi ile meydana gelen bölüm uzayı bir yüzeydir. Diğer taraftan $\mathcal{U}$ daki kompleks yapı $\mathcal{U}/\Lambda$-yüzeyine transfer edildiğinde bir Riemann yüzeyi elde edilir. Eğer Λ eliptik eleman içeriyorsa sonuç yine bir Riemann yüzeyidir, ancak bu durumda $\mathcal{U} \rightarrow \mathcal{U}/\Lambda$

izdüşümü dallanmıştır. Ancak oluşan yüzey kompakt değildir, bunu sağlamak için $\mathcal{U}$ yerine $\mathcal{U} \cup \{\infty\}$ alınır [14].

Teorem 1.1 [14]**.** Her basit bağlantılı Riemann yüzeyi aşağıdakilerden birine konform eşdeğerdir:

(i) $\mathbb{C}_\infty$-Riemann Küresi

(ii) $\mathbb{C}$-Kompleks Düzlem

(iii) $\mathcal{U}$-Üst Yarı Düzlem.■

Bu Riemann yüzeylerinin otomorfizm grupları aşağıdaki gibidir;

Teorem 1.2 [14]. **(i)** $Aut(\mathbb{C}_\infty) = \mathrm{PSL}(2,\mathbb{R})$

(ii) $Aut(\mathbb{C}) = \{z \to az + b : a, b \in \mathbb{C}, a \neq 0\}$

(iii) $\mathrm{Aut}(\mathcal{U}) = \mathrm{PSL}(2,\mathbb{R})$.■

Teorem 1.3 [14]. $\mathcal{U}/\Lambda$ kompakt ise Λ parabolik eleman içermez.■

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

Teorem 1.4 [7]**.** PSL(2,$\mathbb{R}$) nin bir parabolik (eliptik, hiperbolik) elemanının PSL(2,$\mathbb{R}$) deki merkezleyeni, aynı sabit nokta kümeli tüm parabolik (eliptik, hiperbolik) elemanlardan meydana gelir.■

Teorem 1.5 [14]**.** Her Abel, Fuchsian grup devirlidir.■

Tanım 1.19. Λ bir Fuchsian grup olsun. Λ nın birim elemandan ve parabolik (eliptik) elemanlardan oluşan devirli bir maksimal alt grubuna Λ nın bir *parabolik* (*eliptik*) *alt grubu* denir.

Tanım 1.20. Bir Λ Fuchsian grubunun parabolik (eliptik) alt gruplarının eşlenik sınıflarının sayısına Λ Fuchsian grubunun *parabolik* (*eliptik*) *sınıf sayısı* denir.

Tanım 1.21. Λ bir Fuchsian grup olsun. Bir $r \in \hat{\mathbb{Q}} := \mathbb{Q} \cup \{\infty\}$ noktası keyfi verildiğinde $\gamma(r) = r$ olacak şekilde bir $\gamma \in \Lambda$ parabolik elemanı bulunabiliyorsa, bu noktaya Λ Fuchsian grubunun bir *parabolik noktası* veya *cusp*'ı denir.

Benzer şekilde $z \in \mathcal{U}$ noktası keyfi verildiğinde $\sigma(z) = z$ olacak şekilde bir $\sigma \in \Lambda$ eliptik elemanı bulunabiliyorsa bu noktaya , Λ nın bir *eliptik noktası* adı verilir.

1.5. Modüler Grup

Tanım 1.22. $\mathrm{PSL}(2,\mathbb{R})$ nin

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

alt grubuna *Modüler grup* adı verilir. Bu grup aşağıdaki gibi 2x2 lik tamsayılar matrisiyle de temsil edilebilir:

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

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

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

matrisleri yine aynı dönüşümü temsil ettiğinden, matris hesaplamalarında uygun olduğu yerde bu matrisleri eşit gibi yazabiliriz (burada determinantın 1 olma şartı aranmayabilir). Aşağıdaki teorem, Γ nın $T(z) = z + 1$ ve $U(z) = -\dfrac{1}{z}$ dönüşümleriyle üretildiğini göstermektedir.

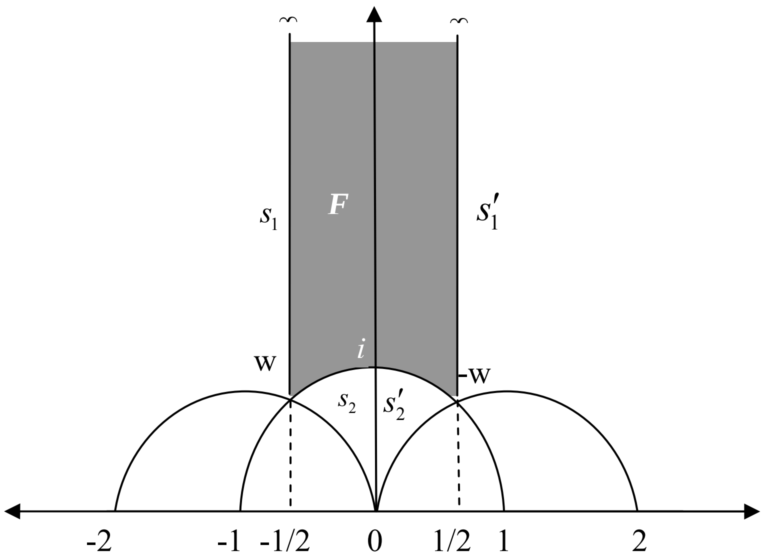
Teorem 1.6. Γ modüler grubu T=$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ve U=$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ matrisleriyle üretilir.

İspat . Önce Γ için Ford bölgesini bulalım. Γ da ∞ un sabitleyeni Γ_∞ ile gösterilsin.

$F_\infty = \left\{ z \in \mathcal{U} : |\operatorname{Re} z| \le \frac{1}{2} \right\}$ olsun. Bu F_∞ şeridi , Γ_∞ sabitleyeni için bir temel bölgedir. En geniş izometrik çemberler 1 yarıçaplıdır ve bu çemberlerin merkezleri reel eksen üzerindeki tam sayılardır. Sadece merkezleri 0,-1,1 olan üç çember F_∞ ile kesişir. Burada $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ ve $-\bar{\rho} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ olmak üzere 0-merkezli çember $\rho, -\bar{\rho}$ da; 1-merkezli çember $-\bar{\rho}$ da; -1 merkezli çember ρ da F_∞ ile kesişir. Diğer çemberlerin yarıçapı $\frac{1}{2}$ den küçük veya eşittir. Bu nedenle şekilde görüldüğü gibi F bölgesi üzerinde bu çemberler önem taşımaz. Buna göre;

$$F = \left\{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 \ge 1, |x| \le \frac{1}{2} , \ y > 0 \right\}$$

kümesi Γ modüler grubu için bir temel bölgedir.



Şekil 1. Γ nın F temel bölgesi

$T(z) = z + 1$ için $T(z) = s_1'$ 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. Burada T bir parabolik eleman ve U, 2. mertebeden bir eliptik elemandır. Buna göre; $TU = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ 3. mertebeden bir eliptik, $V := TU$ olmak üzere $\Gamma, U(z) = -\frac{1}{z}$ ve

$V(z)=\dfrac{z-1}{z}$ elemanlarıyla da üretilir. Dolayısıyla da $U^2=V^3=I$ dır. Buradan Γ nın üreticileri U, T, V olduğundan Γ nın simgesi $(0;2,3,\infty)$ olur.■

Şimdi de Γ nın cusp kümesi $\hat{\mathbb{Q}}:=\mathbb{Q}\cup\{\infty\}$ üzerindeki hareketini inceleyelim. $\hat{\mathbb{Q}}$ nın elemanları $(x,y)=1$ olmak üzere $\dfrac{x}{y}$ olarak yazılabilir. Burada $\infty=\dfrac{1}{0}=-\dfrac{1}{0}$ dır. $\dfrac{x}{y}=\dfrac{-x}{-y}$ olduğundan bu gösterim tek türlü değildir. $T\in\Gamma$ ise

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

olduğundan Γ nın $\hat{\mathbb{Q}}$ üzerindeki hareketi iyi tanımlıdır.

Eğer $(x,\ y)=1$ ve $ad-bc=1$ ise $\dfrac{ax+by}{cx+dy}$ indirgenmiş formdadır.

Aksini varsayalım; $\dfrac{ax+by}{cx+dy}$ indirgenmiş formda olmasın. Buna göre $n\mid ax+by$ ve $n\mid cx+dy$ olacak şekilde bir $n\in\mathbb{Z}$ elemanı vardır. Bu durumda $k,\ell\in\mathbb{Z}$ için $ax+by=kn$ …(1) ve $cx+dy=\ell n$ … (2) dir.

(1) eşitliğinin her iki tarafı d ile (2) de $-b$ ile çarpıldığında

$$(ad-bc)x=(kd-b\ell)n \qquad \text{(I)}$$

ve benzer şekilde (1) eşitliği $-c$ ve (2) eşitliği a ile çarpıldığında

$$(ad-bc)y=(a\ell-ck)n \qquad \text{(II)}$$

elde edilir. (I) ve (II) den $n\mid x,y$ çelişkisi elde edilir.

Teorem 1.7 [14]. Γ **,** $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket eder.

İspat. $\dfrac{a}{b},\dfrac{c}{d}\in\hat{\mathbb{Q}}$; $\dfrac{a}{b}\neq\dfrac{c}{d}$ ve $(a,b)=(c,d)=1$ olsun. Bu durumda $a\beta-b\alpha=1$ ve $c\delta-d\gamma=1$ olacak şekilde $\alpha,\beta,\delta,\gamma\in\mathbb{Z}$ tam sayıları vardır. Burada $\xi(z)=\dfrac{az+\alpha}{bz+\beta}$ ve

$\eta(z)=\dfrac{cz+\gamma}{dz+\delta}$ şeklinde tanımlanırsa $\xi(\infty)=\dfrac{a}{b}$ ve $\eta(\infty)=\dfrac{c}{d}$ olacak şekilde bir $\varphi:=\eta\xi^{-1}\in\Gamma$ dönüşümü vardır. Dolayısıyla Γ, $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket eder.■

Teorem 1.8. Γ nın ∞ noktasının sabitleyeni Γ_∞ sonsuz devirli bir gruptur. ■

İspat. $T\in\Gamma$ ve $T(\infty)=\infty$ olsun. $T(z)=\dfrac{az+b}{cz+d}$ ise $T(\infty)=\infty$ olduğundan $c=0$ ve $ad=1$ dir. Buradan $T(z)=\dfrac{a}{d}z+\dfrac{b}{d}=a^2z+m=z+m$ $(m=b$ veya $m=-b)$ bulunur. Dolayısıyla $U(z)=z+1$ olmak üzere $\Gamma_\infty=\left\langle\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\rangle$ dur.■

1.6. Modüler Grubun Kongrüans Alt Grupları

Kongrüans alt grupları eliptik eğrilerin aritmetiği, integral kuadratik formlar, eliptik modüler formlar gibi konulardaki önemleri itibariyle Modüler grubun üzerlerinde en çok çalışılan alt gruplardır. İlk çalışmalar F.Klein, R. Fricke, A. Hurwitz tarafından yapılmış, sonraki dönemde A. Ogg, B. Schoeneberg, J. P. Serre bu konudaki çalışmaları ileri seviyelere taşımışlardır.

Tanım 1.23. N pozitif tamsayı olmak üzere Γ nın *temel kongrüans alt grubu*

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

ile tanımlanır. Γ nın $\Gamma(N)$-temel kongrüans alt gruplarını içeren herhangi bir alt kümesine *kongrüans alt grubu* denir. Üzerinde en çok çalışılan bazı kongrüans alt grupları;

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

$$\Gamma_0(N):=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma \mid c\equiv 0 \bmod N\right\};\quad \Gamma^0(N):=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma \mid b\equiv 0 \bmod N\right\}$$

gruplarıdır.

Ayrıca $\Gamma(N) \lhd \Gamma$ nın normal bir alt grubudur, dolayısıyla $\Gamma(N), \Gamma_0(N)$ ve $\Gamma_1(N)$nin de normal alt grubudur. Diğer taraftan $\Gamma_1(N) \lhd \Gamma_0(N)$ dir. Buna göre indeksler $N>2$ için

$$\mu_0(N) := |\Gamma : \Gamma_0(N)| = N\prod_{p|N}\left(1+\frac{1}{p}\right), \quad |\Gamma : \Gamma_1(N)| = \frac{N^2}{2}\prod_{p|N}\left(1-\frac{1}{p^2}\right),$$

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

dir.

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

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

$\Gamma_0(N)$, $\Gamma_1(N)$ ve $\Gamma(N)$'nin cusp kümesi de $\hat{\mathbb{Q}}$ dır. Çünkü bunlar Γ nın sonlu indeksli alt gruplarıdır ve bir Λ-Fuchsian grubunun sonlu indeksli herhangi bir alt grubu da Λ ile aynı cusp kümesine sahiptir [24].

Teorem 1.9. $\Gamma_0(N)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketi transitif değildir.

İspat. Aksini varsayalım ve $0, \infty \in \hat{\mathbb{Q}}$ seçelim. Bu durumda

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

olacak şekilde bir $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ elemanı vardır.

Bu eşitlikten $b = 1$ ve $d = 0$ elde edilir. Determinant göz önüne alındığında bunun $c = -1$ ve $N=1$ olmasıyla, diğer bir ifadeyle ancak $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma$ olması durumunda mümkün olduğu görülür.■

1.7. Temel Bölgenin Cinsi

Bir kompakt, yönlendirilebilir X- Riemann yüzeyini göz önüne alalım. X de reellerin kapalı birim aralığının bir homeomorf resmine X üzerinde bir *basit yay* (*simple arc*) adı verilir. Bir yayın bitim noktası ile bir sonrakinin başlangıç noktasının birleşimiyle oluşan yayların sonlu bir dizisine X üzerinde bir *eğri* (*curve*) denir.

Bir eğrinin başlangıç noktası ile bitim noktası çakışıyorsa bu eğriye bir *kapalı eğri* adı verilir. Öklid düzlemindeki bir kapalı dairenin X deki bir homeomorf resmine X üzerinde bir *poligon* adı verilir.

Şimdi $\Im$, X üzerinde sonlu sayıdaki noktada kesişen sonlu sayıda eğrinin meydana getirdiği bir sistem olsun. Ayrıca $\Im$ nın bütünleyenlerinin bağlantılı bileşenlerinin kapanışları poligonlar olsun ve kesişimleri de ya tek bir nokta ya tek bir kenar ya da boş küme olsun. Eğrilerin böyle bir sistemine X in bir *poligonal ayrışması* denir.

Bir poligonal ayrışmada meydana gelen köşe, kenar ve yüz'ün anlamı açıktır. Bunların sayısını sırasıyla v,e ve f ile göstereceğiz.

Teorem 1.10 (Euler**)** [24]. X in her poligonal ayrışmasında $v-e+f$ sayısı invaryant kalır.■

Tanım 1.24. $g := 1 - \dfrac{v-e+f}{2}$**,** kesişimleri boş olan ve X i ayrıştırmayan kapalı eğrilerin maksimal sayısıdır. Bu önemli topolojik invaryanta X in *cinsi* (*genus*) denir.

Teorem 1.11 [24]. $\Gamma_0(N)$ kongrüans alt grubunun temel bölgesinin cinsi

$$g = 1 + \frac{\mu_0(N)}{12} - \frac{\varepsilon_\rho}{3} - \frac{\varepsilon_i}{4} - \frac{\sigma_\infty}{2}$$

dir. Burada

$$\varepsilon_\rho = \begin{cases} 0 & , \ 9 \mid N \\ \prod\limits_{p\mid N}\left(1+\left(\dfrac{-3}{p}\right)\right) & , \ 9 \nmid N \end{cases} \quad , \quad \varepsilon_i = \begin{cases} 0 & , \ 4 \mid N \\ \prod\limits_{p\mid N}\left(1+\left(\dfrac{-1}{p}\right)\right) & , \ 4 \nmid N \end{cases}$$

dir ve $\sigma_\infty = \sum\limits_{t\mid N} \varphi\left(\left(t, N/t\right)\right)$ biçimindedir . φ-Euler fonksiyonu olmak üzere,

$$\left(\frac{-1}{p}\right):=\begin{cases}0 & , \quad p=2\\ 1 & , \quad p\equiv 1 \bmod 4\\ -1 & , \quad p\equiv 3 \bmod 4\end{cases} \quad , \quad \left(\frac{-3}{p}\right):=\begin{cases}0 & , \quad p=3\\ 1 & , \quad p\equiv 1 \bmod 3\\ -1 & , \quad p\equiv 2 \bmod 3\end{cases}$$

dir.■

$N\leq 25$ için elde edilen sonuçları verelim;

g=0 N=1, …, 10, 12, 13, 16, 18, 25 için;

g=1 N=11, 14, 15, 17, 19, 20, 21, 24 için;

g=2 N=22, 23 için;

1.8. Bazı Kongrüans Alt Gruplarının Normalliyenleri

Teorem 1.12 [11]. $\Gamma(N)$'nin $PSL(2,\mathbb{R})$ deki normalliyeni Γ dır.■

Teorem 1.13 [11]. $\Gamma_1(N)$'nin Γ daki normalliyeni $\begin{cases}\Gamma_0(N), & N\neq 4\\ \Gamma_0(2), & N=4\end{cases}$ dir.■

Teorem 1.14 [1]. $\Gamma_0(N)$'nin $PSL(2,\mathbb{R})$ deki *normalliyeni*

$$\mathcal{N}or(N):=\left\{\begin{pmatrix} ae & b/h \\ cN/h & de\end{pmatrix} : ade^2-bcN/h^2=e>0\right\}$$

dir. Buradaki bütün harfler tamsayı, $e\| N/h^2$ ve h, $h^2 | N$ şartını sağlayan 24'ün en büyük bölenidir. ($r\|s$ yani "r, s'nin bir tam bölenidir $:\Leftrightarrow \left(r, s/r\right)=1$ dir).■

Teorem 1.15 [4]. N keyfi bir pozitif tam sayı olsun. Bu durumda $\mathcal{N}or(N)$ yalnızca 2, 3, 4 ve 6 mertebeli periyotlara sahip olabilir ve üstelik

(a) $\mathcal{N}or(N)$, 4. mertebeden en çok bir periyoda sahiptir. $\mathcal{N}or(N)$ nin 4. mertebeden bir periyoda sahip olması için gerek ve yeter şart,

$N/h^2=2p_2^{\alpha_2}\ldots p_r^{\alpha_r}$ ve i=2,…, r olmak üzere, $2\,\|\,N/h^2$ ve $p_i\equiv 1 \bmod 4$ olmasıdır.

(b) $\mathcal{N}or(N)$, 6. mertebeden en çok bir periyoda sahiptir. $\mathcal{N}or(N)$ nin 6. mertebeden bir periyoda sahip olması için gerek ve yeter şart,

$N/h^2 = 3p_2^{\alpha_2}...p_r^{\alpha_r}$ ve i=2,…, r olmak üzere, $3 \,||\, N/h^2$ ve $p_i \equiv 1 \bmod 3$ olmasıdır.

(c) $\mathcal{N}or(N)$, 3. mertebeden en çok bir periyoda sahiptir. $\mathcal{N}or(N)$ nin 3. mertebeden bir periyoda sahip olması için gerek ve yeter şart,

$N/h^2 = p_3^{\alpha_3}...p_r^{\alpha_r}$ ve i=3,…, r olmak üzere, $p_i \equiv 1 \bmod 3$ olmasıdır.■

Teorem 1.16 [4]. $N \in \mathbb{Z}$ keyfi ve $N = 2^{\alpha_1}3^{\alpha_2}p_3^{\alpha_3}\dots p_n^{\alpha_n}$ asal çarpanlarına parçalanışı olsun. $\mathcal{N}or(N)$ nin $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket etmesi için gerek ve yeter şart

$$\alpha_1 \leq 7,\ a_2 \leq 3, ve\ \alpha_i \leq 1\ :\ i = 3,\ \dots,\ n$$

olmasıdır.■

Teorem 1.17 [21]. ρ, N/h^2 nin farklı asal çarpanlarının sayısı olsun ve

$$\varepsilon_1 = \begin{cases} 1 \ ; & 2^2, 2^4, 2^6 \,||\, N \\ 0 \ ; & \text{aksi takdirde} \end{cases}, \quad \varepsilon_2 = \begin{cases} 1 \ ; & 9 \,||\, N \\ 0 \ ; & \text{aksi takdirde} \end{cases}$$

olmak üzere $\tau = \left(\frac{3}{2}\right)^{\varepsilon_1} . \left(\frac{4}{3}\right)^{\varepsilon_2}$ olsun. Bu takdirde $\Gamma_0(N)$' nin $\mathcal{N}or(N)$ deki indeksi

$|\,\mathcal{N}or(N) : \Gamma_0(N)| = 2^{\rho}h^2\tau$ dur.■

Lemma 1.1. Bir $\frac{k}{s} \in \mathbb{R}$ $(s \neq 0)$, $(k,s) = 1$ rasyonel sayısı verildiğinde $A\left(\frac{k}{s}\right) = \left(\frac{k_1}{s_1}\right)$, $s_1 \,|\, N$ koşulunu sağlayan bir $A \in \Gamma_0(N)$ vardır.

İspat. $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k \\ s \end{pmatrix} = \begin{pmatrix} ak + bs \\ Nck + ds \end{pmatrix}$ dir. Buna göre

$$Nck + ds = (N, s) \tag{1*}$$

eşitliğini sağlayan $\{c,d\}$ çiftlerini buluruz, dolayısıyla $s_1=(N,s)$ isteneni sağlar. $\left(\dfrac{Nk}{(N,s)},\dfrac{s}{(N,s)}\right)=1$ olduğundan (1*) eşitliğini sağlayan bir $\{c_0,d_0\}$ çifti mevcuttur. Bu yüzden (1*) ın genel çözümü;

$$\left.\begin{aligned} c &= c_0+\frac{s}{(N,s)^n} \\ d &= d_0-\frac{Nk}{(N,k)^n},\ n\in\mathbb{Z} \end{aligned}\right\} \qquad (2^*)$$

olarak elde edilir.

$N=q_0^{\alpha_0}q_1^{\alpha_1}\ldots q_{k_0}^{\alpha_{k_0}}$, N nin asal çarpanlara parçalanışı olsun. Hem (2*) daki koşulları sağlayan, hem de $(Nc_*,d_*)=1$ şartını sağlayan bir $\{c_*,d_*\}$ çiftinin var olduğunu göstermek zorundayız. $(d_0,N)=1$ ise ispatlamaya değer bir şey yoktur. $(d_0,N)>1$ ise d_0, N ile ortak bölene sahiptir, buna q_0 diyelim. diyelim. (1*) eşitliğinden dolayı $\left(q_0,\dfrac{Nk}{(N,s)}\right)=1$ dir, bu yüzden (2*) da n=1 alarak $q_0\nmid d_1$ şartını sağlayan bir d_1 tamsayısı elde ederiz.

$(d_1,N)>1$ ise d_1, N ile bir ortak çarpana sahiptir, buna q_1 diyelim. $d_2=d_1-\dfrac{q_0Nk}{(N,s)}$ olsun, bu durumda d_2'de q_0 ve q_1 çarpanları yoktur. $(d_2,N)>1$ ise d_2, N ile bir ortak çarpana sahiptir, buna q_2 diyelim. Bu işlem sürdürüldüğü takdirde şu sonucu ulaşılır;

$d_3=d_2-\dfrac{q_0q_1Nk}{(N,s)}$ (ve dolayısıyla d_3'de q_0, q_1, q_2 çarpanları yoktur)

$\vdots \qquad \vdots$

$d_{k_0+1}=d_{k_0}-\dfrac{q_0q_1\cdots q_{k_0-1}Nk}{(N,s)}$ (ve dolayısıyla d_{k_0+1}'de, $q_0,q_1,\ldots,q_{k_0}$ çarpanları yoktur)

Böylece $(d_{k_0+1},N)=1$ dir. $d_*=d_{k_0+1}+1$ olsun ve c'ye de c_* diyelim, buna göre $(Nc_*,d_*)=1$ dir. Buradan çıkan sonuç şudur; en az bir $A\in\Gamma_0(N)$ elemanı mevcut (aslında sonsuz çoklukta) öyle ki $A\begin{pmatrix}k\\s\end{pmatrix}=\begin{pmatrix}k_1\\s_1\end{pmatrix}$, $s_1|N$ dir.■

Lemma 1.2. $d_1 \mid N$ ve $(a_1,d_1)=(a_2,d_1)=1$ olmak üzere $A\begin{pmatrix} a_1 \\ d_1 \end{pmatrix}=\begin{pmatrix} a_2 \\ d_1 \end{pmatrix}$ olsun. Bu takdirde $t=\left(d_1,\dfrac{N}{d_1}\right)$ olmak üzere $a_1 \equiv a_2 \mod t$ dir.

İspat. $A=\begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ alınırsa $A\begin{pmatrix} a_1 \\ d_1 \end{pmatrix}=\begin{pmatrix} aa_1+bd_1 \\ Na_1c+dd_1 \end{pmatrix}=\begin{pmatrix} a_2 \\ d_1 \end{pmatrix}$ dir. Bu yüzden

$$Na_1c+dd_1=d_1 \text{ veya } \frac{N}{d_1}a_1c+d=1$$

$$aa_1-a_2 \equiv 0 \mod d_1 \Rightarrow aa_1-a_2 \equiv 0 \mod t$$

$\det A$ dan $ad \equiv 1 \mod t$ elde edilir ve yukarıdan $d \equiv 1 \mod t$ dir. Bu yüzden $a \equiv 1 \mod t$. $aa_1-a_2 \equiv 0 \mod t$ olduğundan $a_1 \equiv a_2 \mod t$ dir.■

Lemma 1.3 [1]. $d \mid N$ ve $(a_1,d)=(a_2,d)=1$ olsun. Bu durumda $t=\left(d,\dfrac{N}{d}\right)$ olmak üzere

$$\begin{pmatrix} a_1 \\ d \end{pmatrix} \text{ ve } \begin{pmatrix} a_2 \\ d \end{pmatrix} \; \Gamma_0(N) \text{ altında eşleniktir} \Leftrightarrow a_1 \equiv a_2 \mod t.$$

İspat . Teorem 1.11 ve Lemma 1.2 den ispat aşikardır.■

Teorem 1.18. $d \mid N$ olsun. $\dfrac{a}{d}$ nin $\Gamma_0(N)$ ile hareketiyle oluşan yörünge

$$\begin{pmatrix} a \\ d \end{pmatrix}=\left\{\frac{x}{y}\in\hat{\mathbb{Q}}:(N,y)=d,\, a\equiv x\frac{y}{d}\mod\left(d,\frac{N}{d}\right)\right\}$$

kümesidir. Üstelik $\begin{pmatrix} a \\ d \end{pmatrix}$, $d \mid N$ yörüngelerinin sayısı $Y=\sum_{d\mid N}\varphi\left(\left(d,{}^{N}\!/_{d}\right)\right)$, φ-Euler fonkiyonudur [4].

1.9. İmprimitif Hareket

Tanım 1.25. (i) $X\neq\emptyset$ bir küme olsun. $\xi : X\rightarrow X$ bire-bir, örten ise ξ'ye X' in bir *permütasyonu* denir. X in tüm *permütasyonlarının kümesi* S^X ile gösterilir.

(ii) $\xi_1,\xi_2 \in S^X$ ise $\xi_1 o \xi_2 \in S^X$ olduğu açıktır. S^X grubuna X üzerinde *simetrik grup* denir. S^X in alt gruplarına da X üzerinde *permütasyon grupları* denir.

Tanım 1.26. G, X üzerinde bir permütasyon grubu olsun. Bu takdirde G, X üzerinde hareket eder. Gerçekten $g\in G$ ise g:$G\to G$ bire-bir ve örten bir dönüşümdür. Bu durumda $gx:=g(x)$ olarak alınırsa $(g_1g_2)x = g_1(g_2x)$ ve $1x = x$ olduğu açıktır. Bu harekete G nin X üzerindeki *doğal hareketi* denir ve "(G,X) *permütasyon grubu*" ifadesi kullanılır.

Tanım 1.27. (G,X) bir transitif permütasyon grubu ve "$\approx$", X üzerinde bir denklik bağıntısı olsun. $x,y\in X$ için $x \approx y$ olduğunda $\forall g\in G$ için $g(x) \approx g(y)$ ise "$\approx$" bağıntısına bir *G-invaryant denklik bağıntısı* denir.

Tanım 1.28. Bir G-invaryant denklik bağıntısının denklik sınıflarına *denklik bağıntısının blokları* denir.

Bu tanıma göre;

i) *Özdeşlik bağıntısı*: $x \approx y \Leftrightarrow x = y$

ii) *Evrensel bağıntı*: $\forall x,y\in X$ için $x \approx y$

bağıntılarının G-invaryant denklik bağıntıları olduğu açıktır. Bu bağıntılara *aşikâr* (*trivial*) *bağıntılar* adı verilir.

Tanım 1.29 [7]**.** X üzerinde yukarıdaki aşikâr bağıntıların dışında bir G-invaryant denklik bağıntısı yoksa (G,X)'e *primitif*, aksi halde *imprimitif* denir.

Lemma 1.4 [7]**.** (G,X) bir transitif permütasyon grubu, $H\leq G$ ve bir $\alpha\in X$ için $G_\alpha \leq H$ olsun. Bu takdirde $g\in G$, $h\in H$ için

$$g(\alpha) \approx gh(\alpha))$$

bir G-invaryant denklik bağıntısıdır. Ayrıca

"$\approx$"özdeşlik bağıntısıdır $\Leftrightarrow H = G_\alpha$, "$\approx$" evrensel bağıntıdır $\Leftrightarrow H=G$ dir.■

Lemma 1.5 [7]**.** (G,X) bir transitif permütasyon grubu olsun. (G,X) hareketi primitiftir $\Leftrightarrow$ $\forall x\in X$ için G_x, X in maksimal bir alt grubudur.■

Teorem 1.19 [7]**.** (G,X) bir transitif permütasyon grubu olsun. $G_\alpha \lneq H \lneq G$ ise

$$g(\alpha) \approx h(\alpha) \;\Leftrightarrow\; g^{-1}h \in H$$

iyi tanımlı bir G-invaryant denklik bağıntısıdır. Denklik sınıflarının sayısı da $|G:H|$ indeksidir.■

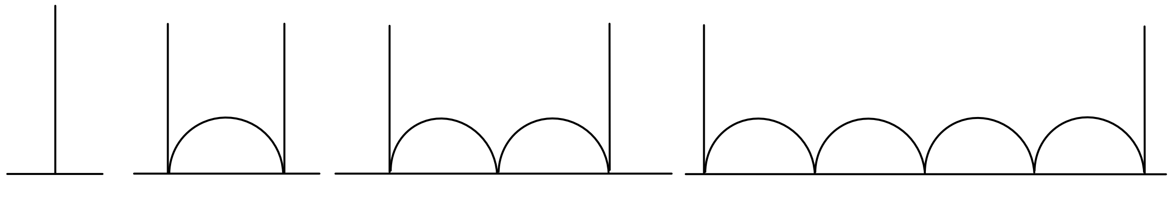
1.10. Graf Teori

Tanım 1.30. $X \neq \varnothing$ bir küme, $\Delta \subset X{\times}X$ bir bağıntı olsun. G=(X,Δ) ikilisine bir *graf* (graph) denir. X in elemanlarına *grafın köşeleri* ve Δ'nın elemanlarına *grafın kenarları* adı verilir.

(a,b)∈Δ ise bu durum $a \rightarrow b$ ile gösterilir. Eğer (a,b)∈Δ veya (b,a)∈Δ ise a ile b *bir kenar ile bağlanmıştır* denir. Bu durumda a ve b ye *komşu köşeler* denir.

Tanım 1.31. G=(X,Δ) bir graf ve $A \subset X$ olsun. $G' = (A, \Delta \cap A \times A)$ grafına *köşe kümesi A olan G nin bir alt grafi* adı verilir.

Tanım 1.32. $a = a_0, a_1, \ldots, a_n = b$ bir G-grafının köşelerinin bir dizisi olsun. Eğer $1 \leq i \leq n$ için a_{i-1} ve a_i bir kenar ile bağlanmışlarsa a'dan b'ye *n-uzunluğunda bir yol vardır* denir. Eğer a=b ve $a_0, a_1, \ldots, a_{n-1}$ 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 *yönlenmiş bir devre* (*circuit*) denir. Üç kenarlı bir devreye bir *üçgen*, dörtkenarlı bir devreye bir *dörtgen* ve altı kenarlı bir devreye bir *altıgen* denir.



İkigen Hiper. Üçgen Hiper. Dörtgen Hiperbolik Altıgen

Şekil 1.3 Devreler

Tanım 1.33. $G=(X,\Delta)$ bir graf olsun. X üzerinde bir $\approx$-bağıntısını şöyle tanımlayalım:

"$a\approx b :\Leftrightarrow a=b$ veya a'dan b'ye bir yol vardır ".

Açık olarak, $\approx$ bir denklik bağıntısıdır.

Tanım 1.34. (i) X in kendisi bu $\approx$-bağıntısı altında denklik sınıfı ise G-grafına *bağlantılıdır* denir.

(ii) Eğer X_1, $\approx$-bağıntısı altında bir denklik sınıfı ise $(X_1, \Delta \cap X_1 \times X_1)$ bağlantılı bir graftır ve bu grafa G-grafının *bağlantılı bileşeni* denir.

İki grafın köşeleri arasında 1-1 ve örten bir dönüşüm mevcut ve bu dönüşüm komşu köşeleri, komşu köşelere gönderiyorsa bu iki grafa *izomorf graflar* denir [28].

1.11. Alt Yörüngesel Graflar

Tanım 1.35. (G,X) bir transitif permütasyon grubu olsun. G nin $X\times X$ üzerindeki hareketini $g\in G$ olmak üzere

$$g:(\alpha,\beta)\rightarrow(\,g(\alpha),\ g(\beta)\,)\ ,\ (\alpha,\beta)\in X\times X$$

ile tanımlayalım. Bu hareketin yörüngelerine G nin *alt yörüngeleri* denir. (α,β) yı içeren alt yörüngeyi $\boldsymbol{O}(\alpha,\beta)$ ile gösterelim.

$\boldsymbol{O}(\alpha,\beta)$ dan bir $G(\alpha,\beta)$ alt yörüngesel grafını aşağıdaki gibi elde edelim:

$G(\alpha,\beta)$ nın köşeleri X in elemanlarıdır. Yukarıda da verildiği gibi, x, $y\in X$ noktaları için $(x, y)\in\boldsymbol{O}(\alpha,\beta)$ ise x den y ye yönlenmiş bir kenar vardır ve bu durum $x\rightarrow y$ olarak gösterilir. Bu kenarı $\mathcal{U}$-üst yarı düzleminde bir hiperbolik geodezik olarak çizebiliriz.

Açık olarak $\boldsymbol{O}(\beta,\alpha)$ da alt yörüngedir. $\boldsymbol{O}(\alpha,\beta)=\boldsymbol{O}(\beta,\alpha)$ veya $\boldsymbol{O}(\alpha,\beta)\neq\boldsymbol{O}(\beta,\alpha)$ dır.

(i) $\boldsymbol{O}(\alpha,\beta)=\boldsymbol{O}(\beta,\alpha)$ ise $G(\alpha,\beta)=G(\beta,\alpha)$ dır ve bu graf karşılıklı yönlendirilmiş kenarlardan oluşur. Yani, $G(\alpha,\beta)$ grafında $x\rightarrow y$ ise yine $G(\alpha,\beta)$ grafında $y\rightarrow x$ dir. Bu durumda $G(\alpha,\beta)$ grafına *kendisiyle eşleşmiş graf* denir.

(ii) $\boldsymbol{O}(\alpha,\beta)\neq\boldsymbol{O}(\beta,\alpha)$ ise $G(\beta,\alpha)$, $G(\alpha,\beta)$ nın oklarının ters yönlendirilmişlerinden ibarettir. Yani, $G(\alpha,\beta)$ grafında $x\rightarrow y$ ise $G(\beta,\alpha)$ grafında $y\rightarrow x$ dir. Bu durumda ise $G(\alpha,\beta)$ ve $G(\beta,\alpha)$ graflarına *birbirleriyle eşleşmiş graflar* denir.

$\boldsymbol{O}(\alpha,\alpha)=\{(x,x):\ x\in X\}$, $X\times X$ in köşegenidir. $\boldsymbol{O}(\alpha,\alpha)$ ya uygun $G(\alpha,\alpha)$ alt yörüngesel grafına *aşikâr alt yörüngesel graf* denir. Bu graf her bir köşesi $\alpha\in X$ olan bir sıçramadan ibarettir.

G, X üzerinde transitif olarak hareket ettiğinden blokları transitif olarak permüte eder, dolayısıyla alt grafların hepsi izomorftur.

Yukarıda özetlenen fikirler ilk defa Sims tarafından ortaya konmuş [26], daha sonra Biggs ve White sonlu gruplar için uygulamaları üzerinde durmuşlar [7], ardında da Tsuzuku bu düşünceleri bir kitapta toparlamıştır [28].

Önerme 1.4 [15]**.** G', (G,X) transitif permütasyon grubu için bir alt yörüngesel graf olsun. Bu takdirde

(i) G, G'-nin otomorfizmalarının bir grubu olarak hareket eder.

(ii) G, G'-nin köşeleri üzerinde transitif olarak hareket eder.

(iii) Eğer G' kendisiyle eşleşmiş ise bu takdirde G, G'-nin ardışık köşelerinin sıralı çiftleri üzerinde transitif olarak hareket eder.

(iv) Eğer G' kendisiyle eşleşmiş değil ise bu takdirde G, G'-nin kenarları üzerinde transitif olarak hareket eder.■

Şimdi $G:=\Gamma$ ve $X:=\hat{\mathbb{Q}}$ alalım. Γ- nın $\hat{\mathbb{Q}}$ üzerindeki hareketi transitif olduğundan her bir alt yörünge bir $v\in\hat{\mathbb{Q}}$ için (∞,v) ikilisini ihtiva eder öyle ki $N\geq 1$ ve $(u,N)=1$ olmak üzere $v=\dfrac{u}{N}$ dir. Bu altyörüngeyi $O_{u,N}$ ile ve buna karşılık gelen $G(\infty,v)$ alt yörüngesel grafını da $G_{u,N}$ ile göstereceğiz.

Eğer $v=\infty$ ise $G_{1,0}=G_{-1,0}$ aşikâr alt yörüngesel graftır. Böylece kabul edelim ki $v\in\mathbb{Q}$ dir. Eğer $v'\in\mathbb{Q}$ ise bu takdirde $O(\infty,v)=O(\infty,v')\Leftrightarrow v$ ve v' Γ_∞ nın aynı yörüngesindedir. Yani $\exists g\in\Gamma_\infty$ öyle ki $g(v)=v'$.

Teorem 1.20 [15]**.** $\dfrac{r}{s}\rightarrow\dfrac{x}{y}\in G_{u,N}$ $\Leftrightarrow$

(i) $x\equiv ur \bmod N$, $y\equiv us \bmod N$, $ry-sx=N$ veya

(ii) $x\equiv -ur \bmod N$, $y\equiv -us \bmod N$, $ry-sx=-N$

olmasıdır.■

Sonuç 1.1 [15]. $uv \equiv -1 \bmod N$ ise bu takdirde $G_{u,N}$ ile $G_{v,N}$ eşleşmiş alt yörüngesel graflardır.■

Sonuç 1.2 [15]. $G_{u,N}$ kendisiyle eşleşmiştir $\Leftrightarrow$ $u^2 \equiv -1 \bmod N$ dir.■

Γ, $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket ettiğinden blokları transitif olarak permüte eder. Dolayısıyla altgrafların hepsi izomorftur. $F\left(\infty, \dfrac{u}{N}\right)$ ile köşeleri $[\infty]:=\left\{\dfrac{x}{y} \in \hat{\mathbb{Q}} : y \equiv 0 \bmod N\right\}$ - bloğunun elemanları olan $G\left(\infty, \dfrac{u}{N}\right)$ alt yörüngesel grafının alt grafını göstereceğiz. Kısaca $F\left(\infty, \dfrac{u}{N}\right)$ yerine $F_{u,N}$ yazacağız.

Teorem 1.21 [15]. $\Gamma_0(N)$, $F_{u,N}$ nin köşelerini ve kenarlarını transitif olarak permüte eder.■

Teorem 1.22 [15]. **(i)** $F_{u,N}$ nin her v köşesi için $v \to -v$ dönüşümü $F_{u,N}$ den $F_{-u,N}$ grafına bir izomorfizmadır.

(ii) $M \mid N$ ise $F_{u,N}$ nin her v köşesi için $v \to \dfrac{Nv}{M}$ dönüşümü $F_{u,N}$ den $F_{u,M}$ grafına bir izomorfizmadır.■

2. YAPILAN ÇALIŞMALAR VE BULGULAR

2.1. $\mathcal{N}or\,(p)$ nin $\hat{\mathbb{Q}}$ Üzerindeki Alt Yörüngesel Grafları

p bir asal sayı olmak üzere $\Gamma_0(p)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma \;\middle|\; c\equiv 0 \bmod (p)\right\}$, yani $\Gamma_0(p)=\left\{\begin{pmatrix} a & b \\ pc & d \end{pmatrix}\in\Gamma \;\middle|\; ad-pbc=1\right\}$ özel kongrüans alt grubunun normalliyeni,

$$\mathcal{N}or(p):=\left\{\begin{pmatrix} \mathrm{ae} & \mathrm{b} \\ \mathrm{pc} & \mathrm{de} \end{pmatrix}\in \mathrm{PSL}\,(2,\mathbb{R}) \;\middle|\; ade^2-bcp=e\;,\; e=1\,\text{veya}\; p\right\}$$

kümesidir (Teorem 1.14).

Buna göre ∞ un normalliyendeki sabitleyeni $N_\infty:=\left\langle\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right\rangle$ kümesidir. Bu durumda $N_\infty \lneq \Gamma_0(p) \lneq \mathcal{N}or(p)$ dir. Dolayısı ile Lemma 1.5 e göre $\mathcal{N}or(p)$, $\hat{\mathbb{Q}}$ üzerinde impirimitif olarak hareket eder. Böylece $\approx$, $\hat{\mathbb{Q}}$ üzerinde $\Gamma_0(p)$ ile indirgenmiş $\mathcal{N}or(p)$ invaryant denklik bağıntısını göz önüne alabiliriz.

Eğer $v=\dfrac{r}{s}$ ve $w=\dfrac{x}{y}\in\hat{\mathbb{Q}}$ elemanlarını $(s,p)=e_1$, $(y,p)=e_1'$, $s=s_1e_1$, $y=y_1e_1'$, $e_2=\dfrac{p}{e_1}$ ve $e_2'=\dfrac{p}{e_1'}$ olacak şekilde seçersek, determinantlar sırası ile e_2 ve e_2' olmak üzere

$g_1:=\begin{pmatrix} re_2 & b_1 \\ s_1p & d_1e_2 \end{pmatrix}$, $g_2:=\begin{pmatrix} xe_2' & b_2 \\ y_1p & d_2e_2' \end{pmatrix}\in\mathcal{N}or\,(p)$ ve $v=g_1(\infty)$ ve $w=g_2(\infty)$ dir. Böylece

$$v_{e_2}\approx w_{e_2'}\Leftrightarrow e_2=e_2'$$

dir. Buna göre ∞ un bloğu,

$$[\infty]:=\left\{\frac{x}{y}\in\hat{\mathbb{Q}}: y\equiv 0 \bmod p\right\}$$

şeklinde elde edilir.

$(\mathcal{N}or(p),\hat{\mathbb{Q}})$ transitif permütasyon grubu olduğundan $(\mathcal{N}or(p),\hat{\mathbb{Q}}^2)$ bir permütasyon grubudur ve $\mathcal{N}or(p)$ nin $\hat{\mathbb{Q}}^2$ üzerindeki hareketi; $(\alpha,\beta)\in\hat{\mathbb{Q}}^2$ ve $g\in\mathcal{N}or(p)$ olmak üzere $g(\alpha,\beta):=(g(\alpha),g(\beta))$ şeklindedir. Bu hareketin yörüngelerine "*$\mathcal{N}or(p)$ nin alt yörüngeleri* " denir. (α,β) yı içeren alt yörüngeyi $\boldsymbol{O}(\alpha,\beta)$ ile gösterelim. $\boldsymbol{O}(\alpha,\beta)$ alt yörüngesinden bir $\Delta(\alpha,\beta)$ alt yörüngesel grafını şu şekilde elde edebiliriz: $\Delta(\alpha,\beta)$ nın köşeleri $\hat{\mathbb{Q}}$ nın elemanları ve $(a,b)\in\boldsymbol{O}(\alpha,\beta)$ ise *a-dan b-ye yönlendirilmiş bir kenar vardır* denir ve bu durum $a\rightarrow b$ ile gösterilir.

Eğer $\boldsymbol{O}(\alpha,\beta)=\boldsymbol{O}(\beta,\alpha)$ ise bu takdirde graf karşılıklı yönlendirilmiş kenar çiftlerini, yani $a\leftrightarrow b$, ihtiva eder ve bu durum $(a,b)\in\boldsymbol{O}(\alpha,\beta)$ ise a — b ile gösterilir. Bu durumda yönlendirilmemiş bir graf elde edilir ve buna " *kendisiyle eşleşmiş graf* " denir.
$\boldsymbol{O}(\alpha,\beta)\neq\boldsymbol{O}(\beta,\alpha)$ ise bu takdirde $\Delta(\beta,\alpha)$, $\Delta(\alpha,\beta)$ nın oklarının ters yönlendirilmişlerinden ibarettir. Bu durumda $\Delta(\alpha,\beta)$ ile $\Delta(\beta,\alpha)$ ya " *eşleşmiş alt yörüngesel graflar* "denir.

$\mathcal{N}or(p)$, $\hat{\mathbb{Q}}$ üzerinde transitif olduğundan her alt yörünge, $v\in\hat{\mathbb{Q}}$ olmak üzere, bir (∞,v) çiftini içerir. Eğer $p>0$ için $v=\dfrac{u}{p}$ ve $(u,p)=1$ ise $\boldsymbol{O}(\infty,\dfrac{u}{p})$ alt yörüngesini kısaca $\boldsymbol{O}_{u,p}$ ile ve alt yörüngesel grafı da $\Delta_{u,p}$ ile göstereceğiz.

$F(\infty,\dfrac{u}{p})$ ile köşeleri $[\infty]$- bloğunun elemanları olan $\Delta(\infty,\dfrac{u}{p})$ alt yörüngesel grafının alt grafını göstereceğiz. Kısaca $F(\infty,\dfrac{u}{p})$ yerine $F_{u,p}$ yazacağız.

Teorem 2.1. $\dfrac{r}{s},\dfrac{x}{y}\in[\infty]$ olsun. Bu takdirde $\dfrac{r}{s}\rightarrow\dfrac{x}{y}$ nin $F_{u,p}$ de bir kenar olması için gerek ve yeter şart

(a) $x\equiv ur \bmod p$, $y\equiv us \bmod p$, $ry-sx=p$ veya

(b) $x\equiv -ur \bmod p$, $y\equiv -us \bmod p$ ve $ry-sx=-p$

olmasıdır.

İspat. $\frac{r}{s} \to \frac{x}{y}$ $F_{u,p}$ de bir kenar olsun. Bu takdirde $g(\infty) = \frac{r}{s}$ ve $g(\frac{u}{p}) = \frac{x}{y}$ olacak şekilde $g \in \mathcal{N}or(p)$ elemanı vardır.

$$g\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}ae & b\\ pc & de\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{ae}{pc} = \frac{r}{s} \text{ ve } g\begin{pmatrix}u\\p\end{pmatrix} = \begin{pmatrix}ae & b\\ pc & de\end{pmatrix}\begin{pmatrix}u\\p\end{pmatrix} = \frac{aeu+bp}{p(cu+de)} = \frac{x}{y}$$

dir. Burada $e = 1$ olmalıdır. Gerçekten, $e \neq 1$ ise, yani $e = p$ ise bu takdirde

$$\begin{pmatrix}ap & b\\ pc & dp\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{ap}{cp} = \frac{a}{c} = \frac{r}{s}$$

olur ki buradan $p \mid c$ olmak zorundadır. Bu ise det $= p$ olması ile çelişir. Dolayısıyla $e = 1$ olmak zorundadır. Yani,

$$g = \begin{pmatrix}a & b\\ pc & d\end{pmatrix} \in \mathcal{N}or\,(p)$$

şeklindedir. Bu durumda,

$$g\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a & b\\ pc & d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{a}{pc} = \frac{r}{s}$$

dir. Buradan $r = a$ ve $s = pc$ yani $p \mid s$ dir. Ayrıca

$$g\begin{pmatrix}u\\p\end{pmatrix} = \begin{pmatrix}a & b\\ pc & d\end{pmatrix}\begin{pmatrix}u\\p\end{pmatrix} = \frac{au+bp}{p(cu+d)} = \frac{x}{y}$$

dir. Buradan $x = \pm(au + pb)$ ve $y = \pm p(cu + d)$ elde edilir. Sonuç olarak, i,j = 0,1 olmak üzere

$$\begin{pmatrix}a & b\\ pc & d\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix} = \begin{pmatrix}a & au+pb\\ pc & p(cu+d)\end{pmatrix} = \begin{pmatrix}(-1)^i r & (-1)^j x\\ (-1)^i s & (-1)^j y\end{pmatrix} \qquad (1)$$

elde edilir.

Eğer i = j = 0 ise bu takdirde $x \equiv ur \bmod p$, $y \equiv us \bmod p$ ve (1) de determinant alınırsa $ry - sx = p$ bulunur.

Benzer şekilde $i = 1, j = 0$ (veya $i = 0, j = 1$) ise bu takdirde $x \equiv -ur \bmod p$, $y \equiv -us \bmod p$ ve (1) de determinant alınırsa $ry - sx = -p$ elde edilir.

Şimdi tersine; (a) geçerli ise bu takdirde $x = ur + pb$ ve $y = us + pd$ olacak şekilde $b,d \in \mathbb{Z}$ elemanları vardır. Bu değerler $ry - sx = p$ eşitliğinde yerine yazılırsa

$$r(us + pd) - s(ur + pb) = p \Rightarrow rus + rpd - rus - spb = p \Rightarrow p(rd - sb) = p \Rightarrow rd - sb = 1$$

bulunur. Buradan, $p \mid s$ olduğundan, $\begin{pmatrix} r & b \\ s & d \end{pmatrix} \in \mathcal{N}or(p)$ dir ve bu dönüşüm ∞-u $\frac{r}{s}$' ye ve $\frac{u}{p}$' yi $\frac{x}{y}$' ye resmeder.

Benzer şekilde; eğer (b) geçerli ise bu takdirde $x = -ur + pk$ ve $y = -us + p\ell$ olacak şekilde $k, \ell \in \mathbb{Z}$ elemanları vardır. Bu değerler $ry - sx = -p$ eşitliğinde yerine yazılırsa

$$r(-us + p\ell) - s(-ur + pk) = -p \Rightarrow -rus + rp\ell + rus - spk = -p \Rightarrow p(r\ell - sk) = -p$$
$$\Rightarrow r\ell - sk = -1 \Rightarrow -r\ell + sk = 1$$

elde edilir. Buradan, $p \mid s$ olduğundan, $\begin{pmatrix} r & -k \\ s & -\ell \end{pmatrix} \in \mathcal{N}or(p)$ dir ve bu dönüşüm de ∞-u $\frac{r}{s}$'ye ve $\frac{u}{p}$' yi $\frac{x}{y}$' ye resmeder.■

Teorem 2.2. $F_{u,p}$ nin bir yönlendirilmiş üçgen ihtiva etmesi için gerek ve yeter şart $u^2 \pm u + 1 \equiv 0 \bmod p$ olmasıdır.

İspat. $\frac{a}{b} \to \frac{c}{d} \to \frac{k}{\ell} \to \frac{a}{b}$ $F_{u,p}$de bir yönlendirilmiş üçgen olsun. Teorem 1.21 den $\Gamma_0(p)$, $F_{u,p}$ nin kenarlarını transitif olarak permüte ettiğinden bu üçgeni $\infty \to \frac{u}{p} \to \frac{x}{y} \to \infty$ olarak alabiliriz.

$\frac{x}{y} \to \frac{1}{0}$ olduğundan Teorem 2.1 den $1 \equiv -ux \bmod p$ ve $-y = -p$, yani $y = p$ dir.

$\frac{u}{p} \to \frac{x}{y}$ olduğundan $\frac{u}{p} \to \frac{x}{p}$ dir. Yine Teorem 2.1 den $x \equiv u^2 \bmod p$ ve $u - x = 1$, yani $x = u - 1$ dir. Buradan $u^2 - u + 1 \equiv 0 \bmod p$ bulunur.

Diğer taraftan $x \equiv -u^2 \bmod p$ ve $u - x = -1$ dir. Böylece $u^2 + u + 1 \equiv 0 \bmod p$ elde edilir.

Şimdi tersine $u^2 \pm u + 1 \equiv 0 \bmod p$ olsun. Buradan $\pm u + 1 \equiv -u^2 \bmod p$ dir. Buradan da $u + 1 \equiv -u^2 \bmod p$ ve $-u + 1 \equiv -u^2 \bmod p$ dir. $u + 1 \equiv -u^2 \bmod p$ ise bu takdirde $\frac{u}{p} < \frac{u+1}{p}$ olmak üzere $\frac{u}{p} \to \frac{u+1}{p}$ elde edilir. $-u + 1 \equiv -u^2 \bmod p$ ise $u - 1 \equiv u^2 \bmod p$ dir. Buradan

$\frac{u}{p} > \frac{u-1}{p}$ olmak üzere $\frac{u}{p} \to \frac{u-1}{p}$ elde edilir. Böylece $\infty \to \frac{u}{p} \to \frac{u\pm 1}{p} \to \infty$ $F_{u,p}$ de yönlendirilmiş bir üçgendir.■

NOT: $F_{u,p}$ bir üçgen içerir ise Teorem 2.2 den $u^2 \pm u + 1 \equiv 0 \bmod p$ dir. Buradan $\begin{pmatrix} u & \frac{u^2 \pm u + 1}{p} \\ p & -u \pm 1 \end{pmatrix} \in \Gamma_0(p)$ dir ve bu eleman 3. mertebeden bir eliptik elemandır. Böylece bir üçgen verildiğinde ondan hareketle $\Gamma_0(p)$ de 3. mertebeden bir eliptik elemana ulaşabiliyoruz.

Tersine $\Gamma_0(p)$ de herhangi bir 3. mertebeden eliptik eleman verildiğinde bir üçgen elde edilebilir şöyle ki;

$\begin{pmatrix} a & b \\ p & c \end{pmatrix} \in \Gamma_0(p)$ 3. mertebeden eliptik eleman olsun. Bu takdirde $F_{a,p}$ de $\frac{1}{0} \to \frac{a}{p} \to \frac{a^2 + pb}{p(a+c)} \to \frac{1}{0}$ üçgeni vardır ve ayrıca

$$\begin{pmatrix} a & b \\ p & c \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{a}{p}; \quad \begin{pmatrix} a & b \\ p & c \end{pmatrix}\begin{pmatrix} a \\ p \end{pmatrix} = \frac{a^2 + pb}{p(a+c)}; \quad \begin{pmatrix} a & b \\ p & c \end{pmatrix}\begin{pmatrix} a^2 + pb \\ p(a+c) \end{pmatrix} = \frac{1}{0}$$

dir. $\frac{a^2 + pb}{p(a+c)} \to \frac{1}{0}$ olduğundan $a + c = 1$, yani $c = 1 - a$ olmak zorundadır. O halde $\Gamma_0(p)$ deki 3. mertebeden eliptik eleman $\begin{pmatrix} a & b \\ p & 1-a \end{pmatrix}$ dır ve $F_{a,p}$ de buna karşılık gelen üçgen $\frac{1}{0} \to \frac{a}{p} \to \frac{a^2 + pb}{p} \to \frac{1}{0}$ dır.

Tanım 2.1 (Legendre Sembolü **)** [23]**.** p tek asal sayı olsun. $\left(\frac{\bullet}{p}\right)$ değerlerine *Legendre sembolü* denir ve

$$\left(\frac{a}{p}\right) := \begin{cases} 1 \ , & p \nmid a \text{ ve } x^2 \equiv a \bmod p \text{ çözümü var} \\ 0 \ , & p \mid a \\ -1, & p \nmid a \text{ ve } x^2 \equiv a \bmod p \text{ çözümü yok} \end{cases}$$

şeklinde tanımlanır.

Teorem 2.3 (Euler Kriteri **)** [23]**.** Eğer p tek asal sayı ve $(a,p)=1$ ise bu takdirde

$$\left(\frac{a}{p}\right)=1 \text{ dir } \Leftrightarrow (a)^{\frac{p-1}{2}} \equiv 1 \bmod p$$

dir veya, denk olarak,

$$\left(\frac{a}{p}\right) \equiv (a)^{\frac{p-1}{2}} \bmod p$$

dir **.■**

Aşağıdaki teorem Legendre sembollerinin hesaplanmasında bize kolaylık sağlayacaktır.

Teorem 2.4[23]. **(i)** $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(ii) $a \equiv b \bmod p$ ise, bu takdirde $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$

(iii) $\left(\frac{a^2}{p}\right)=1$ ve böylece $\left(\frac{1}{p}\right)=1$

(iv) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

dir .■

Teorem 2.5 [23]**.** p ve q farklı tek asal sayılar ise, bu takdirde

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

dir.■

Teorem 2.6. $u^2 \pm u+1 \equiv 0 \bmod p$ olması için gerek ve yeter şart $x^2 \equiv -3 \bmod p$ nin çözümünün var olmasıdır.

İspat. $''\Rightarrow''$ $u^2 \pm u+1 \equiv 0 \bmod p$ ise $\frac{1}{0} \to \frac{u}{p} \to \frac{u \pm 1}{p} \to \frac{1}{0}$ üçgeni vardır. Bu takdirde bu üçgene karşılık gelen $\Gamma_0(p)$ deki 3 mertebeli eliptik eleman $\begin{pmatrix} -u & \frac{u^2 \pm u+1}{p} \\ -p & u \pm 1 \end{pmatrix}$ dir. Bu durumda, determinant 1 olduğundan,

$$-u(u \pm 1)+u^2 \pm u+1=1$$

dir. $u^2 \pm u + 1 \equiv 0 \bmod p$ olduğundan $u^2 \pm u + 1 = kp$ olacak şekilde bir $k \in \mathbb{Z}$ mevcuttur. Buna göre,

(a) $-u(u+1) + kp = 1 \Rightarrow -u^2 - u - 1 + kp = 0 \Rightarrow 4u^2 + 4u + 4 - 4kp = 0$

$\Rightarrow 4u^2 + 4u + 1 + 3 - 4kp = 0 \Rightarrow (2u+1)^2 + 3 - 4kp = 0$

$\Rightarrow (2u+1)^2 \equiv -3 \bmod p \Rightarrow$ $x^2 \equiv -3 \bmod p$ nin bir çözümü $x = 2u + 1$ dir.

(b) $-u(u-1) + kp = 1 \Rightarrow -u^2 + u - 1 + kp = 0 \Rightarrow 4u^2 - 4u + 4 - 4kp = 0$

$\Rightarrow 4u^2 - 4u + 1 + 3 - 4kp = 0 \Rightarrow (2u-1)^2 + 3 - 4kp = 0$

$\Rightarrow (2u-1)^2 \equiv -3 \bmod p \Rightarrow$ $x^2 \equiv -3 \bmod p$ nin bir çözümü $x = 2u-1 =$ dir.

(a) ve (b) den $u^2 \pm u + 1 \equiv 0 \bmod p$ ise $x^2 \equiv -3 \bmod p$ nin çözümü vardır.

$"\Leftarrow"$ $x^2 \equiv -3 \bmod p$ nin çözümü var olsun. Bu takdirde $x^2 = -3 + p\ell$ olacak şekilde bir $\ell \in \mathbb{Z}$ vardır. Buradan $x^2 + 3 - p\ell = 0$ olup buradan da $x^2 - 2x + 2x + 1 + 2 - p\ell = 0$ dir. x tek ise,

(c) $(x^2 - 2x + 1) + 2x + 2 - p\ell = 0 \Rightarrow (x-1)^2 + 2(x+1) - p\ell = 0$

$\Rightarrow x - 1 = 2u$ ise $x + 1 = 2u + 2$ dir. Buna göre

$4u^2 + 4u + 4 - p\ell = 0 \Rightarrow 4u^2 + 4u + 4 \equiv 0 \bmod p \Rightarrow u^2 + u + 1 \equiv 0 \bmod p$ bulunur.

(d) $(x^2 + 2x + 1) - 2x + 2 - p\ell = 0 \Rightarrow (x+1)^2 - 2(x-1) - p\ell = 0$

$\Rightarrow x + 1 = 2u$ ise $x - 1 = 2u - 2$ dir. Buna göre

$4u^2 - 4u + 4 - \ell p = 0 \Rightarrow 4u^2 - 4u + 4 \equiv 0 \bmod p \Rightarrow u^2 - u + 1 \equiv 0 \bmod p$ bulunur.

(c) ve (d) den $x^2 \equiv -3 \bmod p$ nin çözümü var ise $u^2 \pm u + 1 \equiv 0 \bmod p$ dir.

Şimdi x çift, yani $x = 2m$ olsun. $x^2 \equiv -3 \bmod p$ olduğundan

$$(2m)^2 \equiv -3 \bmod p \Rightarrow \left(\underbrace{(2m+1)p - 2m}_{y}\right)^2 \equiv -3 \bmod p$$

dir. y tek olduğundan (c) ve (d) ye göre $v^2 \pm v + 1 = 0 \bmod p$ olacak şekilde $v \in \mathbb{Z}$ tamsayısı vardır.■

Teorem 2.7. $x^2 \equiv -3 \bmod p$ nin çözümünün var olması için gerek ve yeter şart $p = 3$ veya $p \equiv 1 \bmod 3$ olmasıdır.

İspat. "$\Rightarrow$": $x^2 \equiv -3 \bmod p$ nin çözümü var olsun. Bu takdirde $\left(\frac{-3}{p}\right) = 1$ dir. Teorem 2.4 e göre

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = 1$$

olur. Buradan ve p tek olduğundan $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$ olmak zorundadır. Teorem 2.5 e göre

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}}$$

olduğundan

$$(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$$

dir, yani $\left(\frac{p}{3}\right) = 1$ dir. Euler Kriteri gereğince $p \equiv 1 \bmod 3$ bulunur.

"$\Leftarrow$" : $p = 3$ ise $x^2 \equiv -3 \bmod p$ nin çözümü vardır ve o da 0 dır.

$p \equiv 1 \bmod 3$ olsun. $x^2 \equiv -3 \bmod p$ çözülebilir mi?

Eğer çözülebilirse $\left(\frac{-3}{p}\right) = 1$ olmalı. $p \equiv 1 \bmod 3$ olduğundan Euler Kriteri'ne göre $\left(\frac{p}{3}\right) = 1$ dir.

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = 1 \qquad (*)$$

ve ayrıca

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$$

idi. $\left(\frac{p}{3}\right) = 1$ olduğundan $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$ bulunur. Bu $(*)$ da yerine yazılırsa

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} = (-1)^{p-1} \overset{\substack{p\text{ tek}\\ \text{asal sayı}}}{=} 1$$

edilir ki bu $x^2 \equiv -3 \bmod p$ nin çözülebilir olduğunu gösterir.■

Teorem 2.8. $F_{1,1}$ de bütün üçgenler eşleniktir.

İspat. $y \neq 0$ olmak üzere $F_{1,1}$ de $\frac{x}{y} \to \frac{k}{\ell} \to \frac{m}{n} \to \frac{x}{y}$ üçgenini alalım. $\frac{x}{y} < \frac{k}{\ell} < \frac{m}{n}$ olsun. Bu durumda $x\ell - ky = -1$, $kn - m\ell = -1$ ve $ym - xn = 1$ dir.

$\frac{x}{y} \to \frac{k}{\ell} \to \frac{m}{n} \to \frac{x}{y}$ üçgenini $\frac{1}{0} \to \frac{0}{1} \to \frac{1}{1} \to \frac{1}{0}$ üçgenine resmeden dönüşüm $T := \begin{pmatrix} \ell & -k \\ y & -x \end{pmatrix}$ tir. Gerçekten;

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \ell & -k \\ y & -x \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\ell - ky \\ xy - xy \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$T\begin{pmatrix} k \\ \ell \end{pmatrix} = \begin{pmatrix} \ell & -k \\ y & -x \end{pmatrix}\begin{pmatrix} k \\ \ell \end{pmatrix} = \begin{pmatrix} k\ell - k\ell \\ yk - x\ell \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$T\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} \ell & -k \\ y & -x \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} m\ell - kn \\ ym - xn \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

dir. $\frac{1}{0} \to \frac{0}{1} \to \frac{1}{1} \to \frac{1}{0}$ üçgenini $\frac{1}{0} \rightleftarrows \frac{-1}{1} \rightleftarrows \frac{0}{1} \rightleftarrows \frac{1}{0}$ üçgenine resmeden dönüşüm ise $S := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ dir. Buna göre $\frac{x}{y} \to \frac{k}{\ell} \to \frac{m}{n} \to \frac{x}{y}$ üçgenini $\frac{1}{0} \rightleftarrows \frac{-1}{1} \rightleftarrows \frac{0}{1} \rightleftarrows \frac{1}{0}$ üçgenine resmeden dönüşüm

$$ST = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \ell & -k \\ y & -x \end{pmatrix} = \begin{pmatrix} \ell - y & -k + x \\ y & -x \end{pmatrix}$$

dir. Dolayısıyla Γ -daki bütün üçgenler $\frac{1}{0} \rightleftarrows \frac{-1}{1} \rightleftarrows \frac{0}{1} \rightleftarrows \frac{1}{0}$ üçgenine eşlenik olur ve $\frac{1}{0} \to \frac{-1}{1} \to \frac{0}{1} \to \frac{1}{0}$ üçgenine karşılık gelen 3. mertebeden eliptik eleman $Y := \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \in \Gamma$ dır ki bu eleman Γ- nın bir üretecidir.■

Teorem 2.9. $F_{1,1}$ de bütün ikili devreler eşleniktir.

İspat. $y \neq 0$ olmak üzere $F_{1,1}$ de $\frac{x}{y} \to \frac{u}{v} \to \frac{x}{y}$ ikili devresini alalım. $\frac{x}{y} < \frac{u}{v}$ olsun. Bu durumda $xv - uy = -1$ dir.

$\frac{x}{y} \to \frac{u}{v} \to \frac{x}{y}$ ikili devresini $\frac{1}{0} \to \frac{0}{1} \to \frac{1}{0}$ ikili devresine resmeden dönüşüm $A := \begin{pmatrix} v & -u \\ y & -x \end{pmatrix} \in \Gamma$ dır ve $\frac{1}{0} \to \frac{0}{1} \to \frac{1}{0}$ ikili devresine karşılık gelen 2. mertebeden eliptik $X := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ elemanı Γ- nın bir üretecidir. Buradan $F_{1,1}$ deki bütün ikili devreler eşleniktir.■

Teorem 2.10. $\Gamma_0(p)$ de 3. mertebeden iki eliptik eleman eşlenik ise bu eliptik elemanlara karşılık gelen ve $\frac{1}{0}$ ile başlayan devreler eşleniktir.

İspat. $K = \begin{pmatrix} a & c \\ pm & 1-a \end{pmatrix}$ ve $L := \begin{pmatrix} b & d \\ pn & 1-b \end{pmatrix} \in \Gamma_0(p)$ eliptik elemanları eşlenik olsun. Bu takdirde $\exists\ T := \begin{pmatrix} x & y \\ pz & w \end{pmatrix} \in \Gamma_0(p)$ öyle ki $TKT^{-1} = L$ dir. Buradan

$$\begin{pmatrix} x & y \\ pz & w \end{pmatrix} \begin{pmatrix} a & c \\ pm & 1-a \end{pmatrix} \begin{pmatrix} w & -y \\ -pz & x \end{pmatrix} = \begin{pmatrix} b & d \\ pn & 1-b \end{pmatrix}$$

$$\begin{pmatrix} x & y \\ pz & w \end{pmatrix} \begin{pmatrix} aw - pzc & -ay + xc \\ pmw + pz(a-1) & -pmy + x(1-a) \end{pmatrix} = \begin{pmatrix} b & d \\ pn & 1-b \end{pmatrix}$$

$$\begin{pmatrix} x(aw - pzc) + y\left[pmw + pz(a-1)\right] & x(-ay + xc) + y\left[-pmy + x(1-a)\right] \\ p\left[zaw - pz^2c + w(mw + z(a-1))\right] & pz(-ay + xc) + w\left[-pmy + x(1-a)\right] \end{pmatrix} = \begin{pmatrix} b & d \\ pn & 1-b \end{pmatrix}$$

olur. Buna göre

$$\begin{aligned} b &= axw - pzcx + pmyw + pzy(a-1) - pyza + pyza \\ &= a\underbrace{(xw - pyz)}_{=1} + p\left[-zcx + myw + zy(a-1) + yza\right] \\ &= a + p\left[-zcx + myw + zy(a-1) + yza\right] \end{aligned}$$

bulunur ki buradan $b \equiv a \bmod p$ elde edilir.

Ayrıca $n = zaw - pz^2c + w(mw + z(a-1))$ dir.

$K := \begin{pmatrix} a & c \\ pm & 1-a \end{pmatrix}$ ya karşılık gelen devre $\frac{1}{0} \to \frac{a}{pm} \to \frac{a^2+pcm}{pm} \to \frac{1}{0} \in F_{a,pm}$ ve

$L := \begin{pmatrix} b & d \\ pn & 1-b \end{pmatrix}$ ye karşılık gelen devre $\frac{1}{0} \to \frac{b}{pn} \to \frac{b^2+pdn}{pn} \to \frac{1}{0} \in F_{b,pn}$ dir yani

$$\frac{1}{0} \to \frac{a+p\left[-zcx+myw+zy(a-1)+yza\right]}{p\left[zaw-pz^2c+w(mw+z(a-1))\right]} \to \frac{\left[a+p\left[-zcx+myw+zy(a-1)+yza\right]\right]^2+pd\left[zaw-pz^2c+w(mw+z(a-1))\right]}{p\left[zaw-pz^2c+w(mw+z(a-1))\right]} \to \frac{1}{0}$$

dır. Buna göre

$$\begin{aligned} F_{a+p\left[-zcx+myw+zy(a-1)+yza\right],\,p\left[zaw-pz^2c+w(mw+z(a-1))\right]} &\to F_{a,pm} \\ v &\to \left[zaw-pz^2c+w(mw+z(a-1))\right]\frac{v}{m} \end{aligned}$$

dönüşümü ile bu devreler eşleniktir.■

Şimdi aşağıdaki teorem için $D_1 : \frac{1}{0} \to \frac{a}{pm} \to \frac{a-1}{pm} \to \frac{1}{0}$ ve $D_2 : \frac{1}{0} \to \frac{a}{p} \to \frac{a-1}{p} \to \frac{1}{0}$ devrelerini göz önüne alalım.

Teorem 2.11. $k \in \mathbb{Z}$ keyfi ve m sayısı, k^2+k+1, $4k^2+3$, $9k^2+3k+7$, $16k^2+8k+13$ sayılarından biri olmak üzere D_1 ve D_2 devreleri eşlenik ise $\Gamma_0(p)$ de karşılık gelen 3. mertebeden eliptik elemanlar da eşleniktir.

İspat. D_1 ve D_2 devreleri $z \to mz$ dönüşümü ile eşleniktirler.

Eğer $\underline{m = k^2+k+1}$ ise bu takdirde $a = k^2+1$ olup $\begin{pmatrix} k^2-k & \frac{-k^2+k-1}{p} \\ p & -1 \end{pmatrix} \in \Gamma_0(p)$ elemanı

ile $\begin{pmatrix} k^2+1 & \frac{-k^4-k^2-1}{p(k^2+k+1)} \\ p(k^2+k+1) & -k^2 \end{pmatrix}$ ve $\begin{pmatrix} k^2+1 & \frac{-k^4-k^2-1}{p} \\ p & -k^2 \end{pmatrix}$ eşleniktir, yani

$$\begin{pmatrix} k^2-k & \frac{-k^2+k-1}{p} \\ p & -1 \end{pmatrix}\begin{pmatrix} k^2+1 & \frac{-k^4-k^2-1}{p(k^2+k+1)} \\ p(k^2+k+1) & -k^2 \end{pmatrix}\begin{pmatrix} -1 & \frac{k^2-k+1}{p} \\ -p & k^2-k \end{pmatrix} = \begin{pmatrix} k^2+1 & \frac{-k^4-k^2-1}{p} \\ p & -k^2 \end{pmatrix}$$

dir.

$\underline{m=4k^2+3}$ ise bu takdirde $a=2k^2+k+2$ bulunur ki $\begin{pmatrix} 4k^2+4k+3 & \dfrac{2(-k^2-k-1)}{p} \\ 2p & -1 \end{pmatrix} \in \Gamma_0(p)$

elemanı ile $\begin{pmatrix} 2k^2+k+2 & \dfrac{-4k^4-4k^3-7k^2-3k-3}{p(4k^2+3)} \\ p(4k^2+3) & -2k^2-k-1 \end{pmatrix}$ ve $\begin{pmatrix} 2k^2+k+2 & \dfrac{-4k^4-4k^3-7k^2-3k-3}{p} \\ p & -2k^2-k-1 \end{pmatrix}$

eşleniktir, yani

$$\begin{pmatrix} 4k^2+4k+3 & \dfrac{2(-k^2-k-1)}{p} \\ 2p & -1 \end{pmatrix}\begin{pmatrix} 2k^2+k+2 & \dfrac{-4k^4-4k^3-7k^2-3k-3}{p(4k^2+3)} \\ p(4k^2+3) & -2k^2-k-1 \end{pmatrix}\begin{pmatrix} -1 & \dfrac{2(k^2+k+1)}{p} \\ -2p & 4k^2+4k+3 \end{pmatrix}=$$

$$=\begin{pmatrix} 2k^2+k+2 & \dfrac{-4k^4-4k^3-7k^2-3k-3}{p} \\ p & -2k^2-k-1 \end{pmatrix}$$

dir.

$\underline{m=9k^2+3k+7}$ ise $a=3k^2+2k+3$ olur. Buna göre $\begin{pmatrix} 9k^2+9k+8 & \dfrac{3(-k^2-k-1)}{p} \\ 3p & -1 \end{pmatrix} \in \Gamma_0(p)$

ile $\begin{pmatrix} 3k^2+2k+3 & \dfrac{-9k^4-12k^3-19k^2-10k-7}{p(9k^2+3k+7)} \\ p(9k^2+3k+7) & -3k^2-2k-2 \end{pmatrix}$ ve $\begin{pmatrix} 3k^2+2k+3 & \dfrac{-9k^4-12k^3-19k^2-10k-7}{p} \\ p & -3k^2-2k-2 \end{pmatrix}$

eşleniktir, yani

$$\begin{pmatrix} 9k^2+9k+8 & \dfrac{3(-k^2-k-1)}{p} \\ 3p & -1 \end{pmatrix}\begin{pmatrix} 3k^2+2k+3 & \dfrac{-9k^4-12k^3-19k^2-10k-7}{p(9k^2+3k+7)} \\ p(9k^2+3k+7) & -3k^2-2k-2 \end{pmatrix}\begin{pmatrix} -1 & \dfrac{3(k^2+k+1)}{p} \\ -3p & 9k^2+9k+8 \end{pmatrix}=$$

$$=\begin{pmatrix} 3k^2+2k+3 & \dfrac{-9k^4-12k^3-19k^2-10k-7}{p} \\ p & -3k^2-2k-2 \end{pmatrix}$$

dir.

$\underline{m=16k^2+8k+13}$ ise $a=12k^2+5k+10$ olup $\begin{pmatrix} 48k^2+16k+37 & \dfrac{4(-9k^2-3k-7)}{p} \\ 4p & -3 \end{pmatrix} \in \Gamma_0(p)$

elemanı ile

$$\begin{pmatrix} 12k^2+5k+10 & \dfrac{-144k^4-120k^3-253k^2-95k-91}{p(16k^2+8k+13)} \\ p(16k^2+8k+13) & -12k^2-5k-9 \end{pmatrix} \text{ ve } \begin{pmatrix} 12k^2+5k+10 & \dfrac{-144k^4-120k^3-253k^2-95k-91}{p} \\ p & -12k^2-5k-9 \end{pmatrix}$$

eşleniktir, yani

$$\begin{pmatrix} 48k^2+16k+37 & \dfrac{4(-9k^2-3k-7)}{p} \\ 4p & -3 \end{pmatrix}\begin{pmatrix} 12k^2+5k+10 & \dfrac{-144k^4-120k^3-253k^2-95k-91}{p(16k^2+8k+13)} \\ p(16k^2+8k+13) & -12k^2-5k-9 \end{pmatrix}\begin{pmatrix} -3 & \dfrac{4(9k^2+3k+7)}{p} \\ -4p & 48k^2+16k+37 \end{pmatrix}=$$

$$=\begin{pmatrix} 12k^2+5k+10 & \dfrac{-144k^4-120k^3-253k^2-95k-91}{p} \\ p & -12k^2-5k-9 \end{pmatrix}$$

dir.■

2.2. $\hat{\Gamma}$ Genişletilmiş Modüler Grupta Graflar

Tanım 2.2. $\hat{\Gamma}$ *genişletilmiş modüler grup*

$$\Gamma := \left\{ z \to \frac{az+b}{cz+d} : a,b,c,d \in \mathbb{Z}, ad-bc=1 \right\} \text{ ve}$$

$$\overline{\Gamma} := \left\{ z \to \frac{a\overline{z}+b}{c\overline{z}+d} : a,b,c,d \in \mathbb{Z}, ad-bc=-1 \right\}$$

olmak üzere $\hat{\Gamma} := \Gamma \cup \overline{\Gamma}$ şeklinde tanımlanır.

Γ modüler grubun $\hat{\Gamma}$- daki indeksi $|\hat{\Gamma} : \Gamma|$ = 2 dir. Buna göre $\hat{\Gamma}$- daki herhangi bir yansıma r ise

$$\hat{\Gamma} = \Gamma \cup r\Gamma$$

dır. $r : z \to -\overline{z}$ veya matris notasyonunda $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ olarak seçilirse $\hat{\Gamma}$- nın üreticileri ve bağıntıları aşağıdaki gibidir.

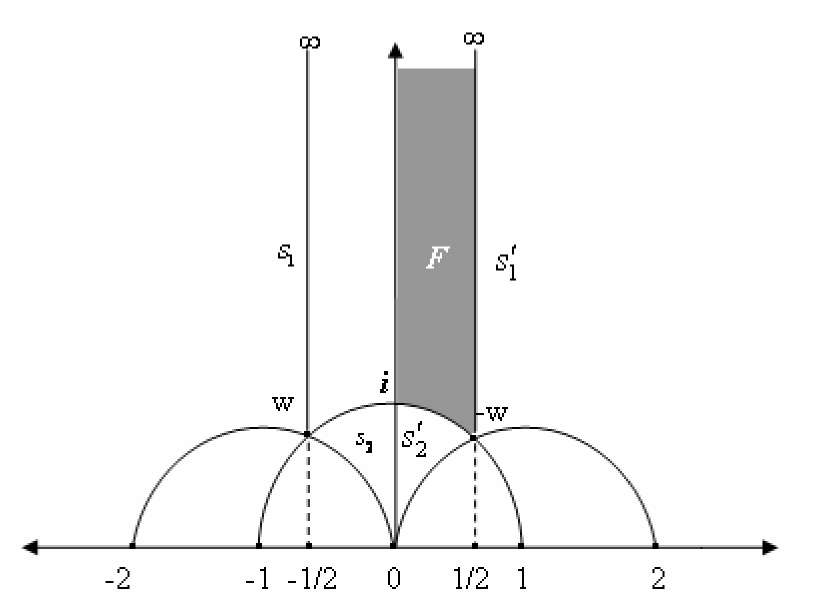
$\hat{\Gamma}$- nın üreticileri : $c_1 = r : z \to -\overline{z} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$c_2 \quad : z \to \dfrac{1}{\overline{z}} \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$c_3 \quad : \quad z \to -\overline{z}-1 \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$

ve $\hat{\Gamma}$ - nın bağıntıları : $(c_1 c_2)^2 = (c_2 c_3)^3 = (c_1 c_3)^\infty$.

Buna göre $\hat{\Gamma}$ - nın simgesi $\sigma(\hat{\Gamma}) = (0;+;[];\{(2,3,\infty)\})$ olur



Şekil 2.1 $\hat{\Gamma}$ genişletilmiş modüler grubun bir *F* temel bölgesi

2.3. $\hat{\Gamma}$-nın $\hat{\mathbb{Q}}$ Üzerindeki Hareketi

$(x, y) = 1$ olan $\forall x, y \in \mathbb{Z}$ sayıları için $\hat{\mathbb{Q}}$ - nın her bir elemanı $\frac{x}{y}$ indirgenmiş formu ile verilir. $\frac{x}{y} = \frac{-x}{-y}$ olduğundan bu gösterim tek türlü değildir. Burada $\infty = \frac{1}{0} = \frac{-1}{0}$ dır. Γ - nın $\hat{\mathbb{Q}}$ üzerinde, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ olmak üzere,

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

ile hareket ettiğini biliyoruz. Burada $(x, y) = 1$ ve $ad - bc = 1$ ise $\frac{ax+by}{cx+dy}$ indirgenmiş formda idi.

$\hat{\Gamma}$ - nın $\hat{\mathbb{Q}}$ üzerindeki hareketi, $\begin{pmatrix} a & b \\ -c & -d \end{pmatrix} \in \hat{\Gamma}$ olmak üzere,

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

şeklindedir. Burada $(x,y)=1$ ve $-ad+bc=-1$ ise $-\dfrac{ax+by}{cx+dy}$ indirgenmiş formdadır.

Lemma 2.1. (i) $\hat{\Gamma}$ - nın $\hat{\mathbb{Q}}$ üzerindeki hareketi transitiftir.

(ii) ∞ un sabitleyeni $\hat{\Gamma}_{\infty}=\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\rangle$ grubudur.

İspat. (i) Γ - nın $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket ettiğini biliyoruz [14]. Dolayısıyla $\hat{\Gamma}$ - nın $\hat{\mathbb{Q}}$ üzerindeki hareketi de transitiftir.

(ii) $T\in\Gamma$ ise ∞ un sabitleyeni $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dir. Şimdi $S=\begin{pmatrix} a & b \\ -c & -d \end{pmatrix}\in\hat{\Gamma}$, $-ad+bc=-1$, olsun. Bu durumda

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

olduğundan $a = 1$ ve $c = 0$ dır. $-ad+bc=-1$ olduğundan $-ad=1\Rightarrow d=-1$ dir. Buradan $\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$ ∞ un sabitleyenidir. Dolayısıyla

$$\hat{\Gamma}_{\infty}=\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\rangle=\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\rangle. \blacksquare$$

Şimdi $\hat{\Gamma}$- nın $\hat{\mathbb{Q}}$ üzerindeki imprimitif hareketine bakalım. İlk olarak permütasyon gruplarının primitifliğini ele alalım.

Tanım 2.3. $\hat{\Gamma}$ - nın *kongrüans alt grubu*,

$$\Gamma_0(N):=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma : c\equiv 0 \bmod N\right\}=\left\{\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\in\Gamma : ad-bcN=1\right\}$$

olmak üzere, $\hat{\Gamma}_0(N):=\left\langle \Gamma_0(N), \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ şeklindedir.

Buna göre $\hat{\Gamma}_\infty \lneq \hat{\Gamma}_0(N) \lneq \hat{\Gamma}$ dır. "$\approx$", $\hat{\mathbb{Q}}$ üzerinde $\hat{\Gamma}_0(N)$ ile indirgenmiş bir $\hat{\Gamma}$ - invaryant denklik bağıntısı olsun. Eğer $v=\dfrac{r}{s},\ w=\dfrac{x}{y}\in\hat{\mathbb{Q}}$ ise bu takdirde $\exists\ g:=\begin{pmatrix} r & -k_1 \\ s & -k_2\end{pmatrix},\ g':=\begin{pmatrix} x & -t_1 \\ y & -t_2\end{pmatrix}\in\hat{\Gamma}$ öyle ki $g(\infty)=v$ ve $g'(\infty)=w$ dır. Buradan

$$v\approx w \iff g^{-1}g'\in\hat{\Gamma}_0(N)$$

dır. Buna göre

(i) $g,\ g'\in\Gamma$ ise $v\approx w \iff ry-sx\equiv 0 \bmod N$ [15].

(ii) $g:=\begin{pmatrix} r & -k_1 \\ s & -k_2\end{pmatrix},\ g':=\begin{pmatrix} x & -t_1 \\ y & -t_2\end{pmatrix}\in\hat{\Gamma}$, det g = -1 ve det g' = -1 alalım. Bu durumda

$$g^{-1}\,g'=\begin{pmatrix} k_2 & -k_1 \\ s & -r\end{pmatrix}\begin{pmatrix} x & -t_1 \\ y & -t_2\end{pmatrix}=\begin{pmatrix} xk_2-yk_1 & -k_2t_1+k_1t_2 \\ sx-ry & -st_1+rt_2\end{pmatrix}\in\hat{\Gamma}_0(N)$$

olacağından $ry-sx\equiv 0 \bmod N$ olur.

O halde (i) ve (ii) den

$$"v\approx w \iff ry-sx\equiv 0 \bmod N"$$

bulunur.

Buna göre ∞ un bloğu,

$$[\infty]:=\left\{\frac{x}{y}\in\hat{\mathbb{Q}} : y\equiv 0 \bmod N\right\}$$

şeklinde verilir.

İmprimitif hareket sonucunda "$\approx$" altında denklik sınıflarının sayısı

$$\psi(N)=|\hat{\Gamma}:\hat{\Gamma}_0(N)|=N\prod_{p|N}\left(1+\frac{1}{N}\right)$$

dir.

Lemma 2.2. $d_1\,|\,N$ ve $(a_1,d_1)=(a_2,d_1)=1$ olsun. Bu durumda $\hat{\Gamma}_0(N)$ altında $\begin{pmatrix} a_1 \\ d_1\end{pmatrix}$ ile $\begin{pmatrix} a_2 \\ d_1\end{pmatrix}$ nin eşlenik olması için gerek ve yeter şart $a_1\equiv\pm\ a_2\ (\bmod t)$, $t=\left(d_1,\dfrac{N}{d_1}\right)$, olmasıdır.

İspat. Lemma 1.3 ten $\begin{pmatrix} a_1 \\ d_1 \end{pmatrix}$ ve $\begin{pmatrix} a_2 \\ d_1 \end{pmatrix}$ $\Gamma_0(N)$ altında eşleniktir $\Leftrightarrow a_1 \equiv a_2 \mod t$ .... (1)

olduğunu biliyoruz.

Şimdi $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ cN & d \end{pmatrix} = \begin{pmatrix} a & b \\ -cN & -d \end{pmatrix} \in \hat{\Gamma}_0(N)$, $\det B = -ad + bcN = -1$ olsun.

$$B\begin{pmatrix} a_1 \\ d_1 \end{pmatrix} = \begin{pmatrix} a & b \\ -cN & -d \end{pmatrix}\begin{pmatrix} a_1 \\ d_1 \end{pmatrix} = \begin{pmatrix} aa_1 + bd_1 \\ -Na_1c - dd_1 \end{pmatrix} = \begin{pmatrix} a_2 \\ d_1 \end{pmatrix}$$

dir. Bu yüzden $aa_1 + bd_1 = a_2$ ve $-Na_1c - dd_1 = d_1$ dir. Buradan

$$-\frac{N}{d_1}a_1c - d = 1 \quad \Rightarrow \quad d \equiv -1 \text{ mod } t$$

bulunur. Ayrıca $\det B = -ad + bcN = -1$ olduğundan

$$-ad \equiv -1 \text{ mod } t \;\Rightarrow\; -a \equiv 1 \text{ mod } t \;\Rightarrow\; a \equiv -1 \text{ mod } t$$

dir. Bunlar $aa_1 + bd_1 = a_2$ eşitliğinde yerine konulursa

$$aa_1 \equiv a_2 \text{ mod } d_1 \;\Rightarrow aa_1 \equiv a_2 \text{ mod } t \Rightarrow a_1 \equiv -a_2 \text{ mod } t \qquad (2)$$

(1) ve (2) den $a_1 \equiv \pm\, a_2$ mod t bulunur.■

Buna göre $\hat{\Gamma}_0(N)$ altında $\begin{pmatrix} a \\ d \end{pmatrix}$ ve $\begin{pmatrix} -a \\ d \end{pmatrix}$ eşlenik olup $\frac{a}{d}$ nin yörüngesi

$$\begin{bmatrix} a \\ d \end{bmatrix} = \begin{pmatrix} a \\ d \end{pmatrix} \cup \begin{pmatrix} -a \\ d \end{pmatrix} = \begin{pmatrix} a \\ d \end{pmatrix} \cup \begin{pmatrix} d-a \\ d \end{pmatrix}$$

şeklindedir.

Teorem 2.12. *N* bir tamsayı ve $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, $2 \nmid N$, *N* nin asal parçalanışı olsun. Bu takdirde $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı

$$\hat{Y} = 2^r + \sum_{\substack{d|N \\ d \nmid N}} \frac{\varphi\left(\left(d, N/d\right)\right)}{2}$$

dir.

İspat. N nin tam bölenleri $a_1, a_2, \ldots, a_{2^r}$ olsun. Bu durumda $1 \le i \le 2^r$ olmak üzere $\varphi\left(\left(a_i, N/a_i\right)\right) = \varphi(1) = 1$ dir. Buradan

$$\begin{pmatrix} 1 \\ a_1 \end{pmatrix}, \begin{pmatrix} 1 \\ a_2 \end{pmatrix}, \ldots, \begin{pmatrix} 1 \\ a_{2^r} \end{pmatrix}$$

öyle yörüngelerdir ki, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ dönüşümü bunları sabit bırakır ve bunların sayısı 2^r dir.

$d \mid N$ fakat $d \nparallel N$ olduğunda $2 \nmid N$ olduğundan $\left(d, N/d\right) > 2$ dir. Bu durumda $\varphi\left(\left(d, N/d\right)\right)$ çifttir. Buna göre $\Gamma_0(N)$ nin paydası d olan yörüngelerinin sayısı $\varphi\left(\left(d, N/d\right)\right)$ dir.

$\begin{pmatrix} b_1 \\ d \end{pmatrix}$ bir yörünge ise

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} b_1 \\ d \end{pmatrix} = \begin{pmatrix} -b_1 \\ d \end{pmatrix} \approx \begin{pmatrix} d-b_1 \\ d \end{pmatrix}, \quad (d-b_1, d) = 1$$

dir öyle ki $\begin{pmatrix} -b_1 \\ d \end{pmatrix} \neq \begin{pmatrix} d-b_1 \\ d \end{pmatrix}$ dir.

Dolayısıyla $\hat{\Gamma}_0(N)$ altında $\begin{bmatrix} b_1 \\ d \end{bmatrix} = \begin{pmatrix} b_1 \\ d \end{pmatrix} \cup \begin{pmatrix} d-b_1 \\ d \end{pmatrix}$ olduğundan $\hat{\Gamma}_0(N)$ nin paydası d olan yörüngelerinin sayısı $\dfrac{\varphi\left(\left(d, N/d\right)\right)}{2}$ dir.

Sonuç olarak $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı $\hat{Y} = 2^r + \sum_{\substack{d \mid N \\ d \nparallel N}} \dfrac{\varphi\left(\left(d, N/d\right)\right)}{2}$ bulunur.■

Teorem 2.13. $2 \mid N$ bir tamsayı ve $N = 2^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, N nin asal parçalanışı olsun ve $N_0 := p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ alalım. Bu durumda

(i) $\alpha_1 = 1$ ise yani $N = 2 p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ ise $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı

$$\hat{Y} = 2^r + \sum_{\substack{d \mid N \\ d \nparallel N}} \frac{\varphi\left(\left(d, N/d\right)\right)}{2}.$$

(ii) $\alpha_1 = 2$ ise yani $N = 2^2 p_2^{\alpha_2} ... p_r^{\alpha_r}$ ise $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı

$$\hat{Y} = 3 \cdot 2^{r-1} + \sum_{\substack{d \mid N \\ d \nmid\nmid N \\ d \neq 2\cdot (\, N_0 \text{ ın tam bölenleri})}} \frac{\varphi\left(\left(d, N/d\right)\right)}{2}.$$

(iii) $\alpha_1 \geq 3$ ise $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı

$$\hat{Y} = 2^{r+1} + \sum_{\substack{d \mid N \\ d \nmid\nmid N \\ d \neq 2\cdot (\, N_0 \text{ ın tam bölenleri}) \\ d \neq 2^{\alpha_1 - 1}\cdot (\, N_0 \text{ ın tam bölenleri})}} \frac{\varphi\left(\left(d, N/d\right)\right)}{2}.$$

İspat. (i) $\alpha_1 = 1$ ve $N = 2p_2^{\alpha_2} ... p_r^{\alpha_r}$ nin tam bölenleri $a_1, a_2, ..., a_{2^r}$ olsun. Bu durumda $1 \leq i \leq 2^r$ olmak üzere $\varphi\left(\left(a_i, N/a_i\right)\right) = \varphi(1) = 1$ dir. Buradan

$$\begin{pmatrix} 1 \\ a_1 \end{pmatrix}, \begin{pmatrix} 1 \\ a_2 \end{pmatrix}, ..., \begin{pmatrix} 1 \\ a_{2^r} \end{pmatrix}$$

öyle yörüngelerdir ki, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ dönüşümü bunları sabit bırakır ve bunların sayısı 2^r dir.

$\left(d, N/d\right) = 2$ olan *d*- ler olmadığından $\left(d, N/d\right) > 2$ dir. Bu durumda $\varphi\left(\left(d, N/d\right)\right)$ çifttir. Buna göre bir önceki teoremde olduğu gibi $\hat{\Gamma}_0(N)$ nin paydası *d* olan yörüngelerinin sayısı $\frac{\varphi\left(\left(d, N/d\right)\right)}{2}$ dir. Sonuç olarak $\alpha_1 = 1$ için $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı

$$\hat{Y} = 2^r + \sum_{\substack{d \mid N \\ d \nmid\nmid N}} \frac{\varphi\left(\left(d, N/d\right)\right)}{2} \text{ dir.}$$

(ii) $\alpha_1 = 2$ olsun. Yine bu durumda $N = 2^2 p_2^{\alpha_2} ... p_r^{\alpha_r}$ nin tam bölenlerinin oluşturduğu yörüngelerin sayısı 2^r dir.

Şimdi $\varphi\left(\left(d, N/d\right)\right) = \varphi(2) = 1$ olan $d \mid N$ olan *d* bölenlerini bulalım. $N_0 = p_2^{\alpha_2} ... p_r^{\alpha_r}$ nin tam bölenleri $b_1, b_2, ..., b_{2^{r-1}}$ olsun. $1 \leq i \leq 2^{r-1}$ olmak üzere $d = 2b_i$ ise

$$\left(d, {}^{N}\!/_{d}\right)=\left(2b_i, {}^{N}\!/_{2b_i}\right)=2 \;\Rightarrow \varphi\left(\left(2b_i, {}^{N}\!/_{2b_i}\right)\right)=\varphi(2)=1$$

olur. Buradan

$$\begin{pmatrix}1\\2b_1\end{pmatrix},\begin{pmatrix}1\\2b_2\end{pmatrix},\ldots,\begin{pmatrix}1\\2b_{2^{r-1}}\end{pmatrix}$$

öyle yörüngelerdir ki, $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ dönüşümü bunları sabit bırakır ve bunların sayısı 2^{r-1} dir. Başka da $\left(d, {}^{N}\!/_{d}\right)=2$ olan N nin d böleni yoktur. $d \mid N$, $d \nparallel N$ ve $d \neq 2\cdot$(N_0 ın tam bölenleri) ise $\left(d, {}^{N}\!/_{d}\right)>2$ dir. Bu durumda $\varphi\left(\left(d, {}^{N}\!/_{d}\right)\right)$ çifttir. Yine Lemma 2.2 ye göre $\hat{\Gamma}_0(N)$ nin paydası d olan yörüngelerinin sayısı $\dfrac{\varphi\left(\left(d, {}^{N}\!/_{d}\right)\right)}{2}$ dir.

Sonuç olarak $\alpha_1=2$ için $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$- daki yörünge sayısı

$$\hat{Y}=3\cdot 2^{r-1}+\sum_{\substack{d\mid N\\ d\nparallel N\\ d\neq 2\cdot(N_0 \text{ ın tam bölenleri})}}\frac{\varphi\left(\left(d, {}^{N}\!/_{d}\right)\right)}{2}.$$

(iii) $\alpha_1 \geq 3$ olsun. $N=2^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$ nin tam bölenleri $a_1,a_2,\ldots,a_{2^r}$ ise $1 \leq i \leq 2^r$ olmak üzere

$\varphi\left(\left(a_i, {}^{N}\!/_{a_i}\right)\right)=\varphi(1)=1$ olduğundan $\begin{pmatrix}1\\a_i\end{pmatrix}$ lerin sayısı 2^r …………(1) dir.

Şimdi $\varphi\left(\left(d, {}^{N}\!/_{d}\right)\right)=\varphi(2)=1$ olan N nin d bölenlerini bulalım. $N_0=p_2^{\alpha_2}\ldots p_r^{\alpha_r}$ nin tam bölenleri $b_1,b_2,\ldots,b_{2^{r-1}}$ olsun. Bu d lerden ilki (ii) de olduğu gibi $1 \leq i \leq 2^{r-1}$ olmak üzere $d=2b_i$ dir. $\varphi\left(\left(2b_i, {}^{N}\!/_{2b_i}\right)\right)=\varphi(2)=1$ olduğundan $\begin{pmatrix}1\\2b_i\end{pmatrix}$ lerin sayısı 2^{r-1} ………..(2) dir. Eğer $d=2^{\alpha_1-1}b_i$ ise $1 \leq i \leq 2^{r-1}$ için

$$\left(d, {}^{N}\!/_{d}\right)=\left(2^{\alpha_1-1}b_i, {}^{N}\!/_{2^{\alpha_1-1}b_i}\right)=2 \;\Rightarrow \varphi\left(\left(2^{\alpha_1-1}b_i, {}^{N}\!/_{2^{\alpha_1-1}b_i}\right)\right)=\varphi(2)=1$$

dir. Buradan $1 \leq i \leq 2^{r-1}$ için $\begin{pmatrix}1\\2^{\alpha_1-1}b_i\end{pmatrix}$ ler öyle yörüngelerdir ki, $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ dönüşümü bunları sabit bırakır ve bunların sayısı 2^{r-1} …………(3) dir.

Başka da $\left(d, N/d\right) = 2$ olan N nin d böleni yoktur. $d \mid N$, $d \nparallel N$, $d \neq 2\cdot$(N_0 ın tam bölenleri) ve $d \neq 2^{\alpha_1 - 1} \cdot$(N_0 ın tam bölenleri) ise $\left(d, N/d\right) > 2$ dir. Bu durumda $\varphi\left(\left(d, N/d\right)\right)$ çifttir. Yine Lemma 2.2 ye göre $\hat{\Gamma}_0(N)$ nin paydası d olan yörüngelerinin sayısı $\dfrac{\varphi\left(\left(d, N/d\right)\right)}{2}$ .....(4) dir.

Sonuç olarak (1), (2), (3) ve (4) ten $\alpha_1 \geq 3$ ise $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı

$$\hat{Y} = 2^r + 2^{r-1} + 2^{r-1} + \sum_{\substack{d \mid N \\ d \nparallel N \\ d \neq 2\cdot(\, N_0 \text{ ın tam bölenleri}) \\ d \neq 2^{\alpha_1 - 1}\cdot(\, N_0 \text{ ın tam bölenleri})}} \frac{\varphi\left(\left(d, N/d\right)\right)}{2} \quad \text{bulunur.} \blacksquare$$

Sonuç 2.1. N karesiz ise $\Gamma_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı, $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısına eşittir.

İspat. N karesiz olduğundan $N = p_1 p_2 \ldots p_r$ şeklindedir. N nin tam bölenleri $a_1, a_2, \ldots, a_{2^r}$ olsun. N nin bütün pozitif bölenleri tam bölen olduğundan, tam bölenlerin sayısı 2^r tanedir. Bu durumda $1 \leq i \leq 2^r$ olmak üzere $\varphi\left(\left(a_i, N/a_i\right)\right) = \varphi(1) = 1$ dir. Buradan $\Gamma_0(N)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısı

$$Y = \sum_{d \mid N} \varphi\left(\left(d, N/d\right)\right) = 2^r$$

dir.

$2 \mid N$ ise Teorem 2.13 (i) den $\hat{\Gamma}_0(N)$ nın $\hat{\mathbb{Q}}$ - daki yörünge sayısı $\hat{Y} = 2^r$ olur.

$2 \nmid N$ ise Teorem 2.12 den $\hat{\Gamma}_0(N)$ nın $\hat{\mathbb{Q}}$ - daki yörünge sayısı $\hat{Y} = 2^r$ olur.$\blacksquare$

Örnek 2.1. $2 \nmid N = 3^2 \cdot 5$ alalım. Buna göre N nin pozitif bölenleri; $1, 3, 5, 3\cdot 5, 3^2, 3^2 \cdot 5$ tir.

(i) $\Gamma_0(3^2 \cdot 5)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısını bulalım. $Y = \sum_{d \mid N} \varphi\left(\left(d, N/d\right)\right)$ idi. O halde

$$\left.\begin{array}{l}\varphi\left(1,3^2\cdot 5\right)=\varphi(1)=1,\ \ \varphi\left(3\cdot 5,3^2\cdot 5/_{3\cdot 5}\right)=\varphi(3)=2,\varphi\left(3,3^2\cdot 5/_{3}\right)=\varphi(3)=2\\ \varphi\left(3^2,3^2\cdot 5/_{3^2}\right)=\varphi(1)=1,\varphi\left(5,3^2\cdot 5/_{5}\right)=\varphi(1)=1\quad,\ \varphi\left(3^2\cdot 5,3^2\cdot 5/_{3^2\cdot 5}\right)=\varphi(1)=1\end{array}\right\}$$

$\Rightarrow Y=1+2+1+2+1+1=8$ bulunur.

$\Gamma_0(3^2\cdot 5)$ nin $\hat{\mathbb{Q}}$ - daki yörüngeleri $\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}2\\3\end{pmatrix},\begin{pmatrix}1\\5\end{pmatrix},\begin{pmatrix}1\\3\cdot 5\end{pmatrix},\begin{pmatrix}2\\3\cdot 5\end{pmatrix},\begin{pmatrix}1\\3^2\end{pmatrix},\begin{pmatrix}1\\3^2\cdot 5\end{pmatrix}$ dir.

(ii) $\hat{\Gamma}_0(3^2\cdot 5)$ nın $\hat{\mathbb{Q}}$ - daki yörünge sayısını bulalım.

$d \parallel N$ olan d-ler; $1,5,3^2,3^2\cdot 5$ ve ayrıca $d\mid N$ fakat $d \nparallel N$ olan d bölenleri; $3,3\cdot 5$ tir.

$$\varphi\left(3,3^2\cdot 5/_{3}\right)=\varphi(3)=2,\varphi\left(3\cdot 5,3^2\cdot 5/_{3\cdot 5}\right)=\varphi(3)=2\,.$$

Teorem 2.12 den $r=2$ olmak üzere $\hat{Y}=2^2+\dfrac{2+2}{2}=6$ dır. Buna göre $\hat{\Gamma}_0(3^2\cdot 5)$ nın $\hat{\mathbb{Q}}$ - daki yörüngeleri $\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}1\\5\end{pmatrix},\begin{pmatrix}1\\3\cdot 5\end{pmatrix},\begin{pmatrix}1\\3^2\end{pmatrix},\begin{pmatrix}1\\3^2\cdot 5\end{pmatrix}$ tir.

Örnek 2.2. $2\mid N=2\cdot 3^2$ alalım. Buna göre N' nin pozitif bölenleri; $1,2,3,2\cdot 3,3^2,2\cdot 3^2$ tir.

(i) $\Gamma_0(2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısını bulalım. O halde

$$\left.\begin{array}{l}\varphi\left(1,2\cdot 3^2\right)=\varphi(1)=1,\ \ \varphi\left(2,2\cdot 3^2/_{2}\right)=\varphi(2)=1,\ \varphi\left(3,2\cdot 3^2/_{3}\right)=\varphi(3)=2\quad,\\ \varphi\left(2\cdot 3,2\cdot 3^2/_{2\cdot 3}\right)=\varphi(3)=2,\varphi\left(3^2,2\cdot 3^2/_{3^2}\right)=\varphi(1)=1,\varphi\left(2\cdot 3^2,2\cdot 3^2/_{2\cdot 3^2}\right)=\varphi(1)=1\end{array}\right\}$$

$\Rightarrow Y=1+1+2+2+1+1=8$. Buna göre $\Gamma_0(2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$ - daki yörüngeleri

$$\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}2\\3\end{pmatrix},\begin{pmatrix}1\\2\cdot 3\end{pmatrix},\begin{pmatrix}5\\2\cdot 3\end{pmatrix},\begin{pmatrix}1\\3^2\end{pmatrix},\begin{pmatrix}1\\2\cdot 3^2\end{pmatrix}$$

dir.

(ii) $\hat{\Gamma}_0(2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$ daki yörünge sayısını bulalım.

$d \parallel N$ olan d bölenleri; $1,2,3^2,2\cdot 3^2$ ve ayrıca $d\mid N$ fakat $d \nparallel N$ olan d bölenleri; $3,2\cdot 3$ tir.

$$\varphi\left(3, {}^{2\cdot 3^2}\!/_{3}\right)=\varphi(3)=2,\ \varphi\left(2\cdot 3, {}^{2\cdot 3^2}\!/_{2\cdot 3}\right)=\varphi(3)=2 \text{ dir.}$$

Teorem 2.13 (i) den $r=2$ olmak üzere $\hat{Y}=2^2+\dfrac{2+2}{2}=6$ bulunur. $\hat{\Gamma}_0(2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$ daki yörüngeleri $\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}1\\2\cdot 3\end{pmatrix},\begin{pmatrix}1\\3^2\end{pmatrix},\begin{pmatrix}1\\2\cdot 3^2\end{pmatrix}$ dir.

Örnek 2.3. $2^2 \mid N=2^2\cdot 3^2$ alalım. Buna göre N' nin pozitif bölenleri; $1,2,3,2\cdot 3,2^2,3^2,2^2\cdot 3,2\cdot 3^2,2^2\cdot 3^2$ tir.

(i) $\Gamma_0(2^2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$- daki yörünge sayısını bulalım.

$$\left.\begin{array}{l}
\varphi\left(1,2^2\cdot 3^2\right)=\varphi(1)=1,\varphi\left(2, {}^{2^2\cdot 3^2}\!/_{2}\right)=\varphi(2)=1,\ \varphi\left(3, {}^{2^2\cdot 3^2}\!/_{3}\right)=\varphi(3)=2\\
\varphi\left(2\cdot 3, {}^{2^2\cdot 3^2}\!/_{2\cdot 3}\right)=\varphi(2\cdot 3)=2,\varphi\left(2^2, {}^{2^2\cdot 3^2}\!/_{2^2}\right)=\varphi(1)=1,\varphi\left(3^2, {}^{2^2\cdot 3^2}\!/_{3^2}\right)=\varphi(1)=1,\\
\varphi\left(2\cdot 3^2, {}^{2^2\cdot 3^2}\!/_{2\cdot 3^2}\right)=\varphi(1)=1,\varphi\left(2^2\cdot 3, {}^{2^2\cdot 3^2}\!/_{2^2\cdot 3}\right)=\varphi(3)=2,\ \varphi\left(2^2\cdot 3^2, {}^{2^2\cdot 3^2}\!/_{2^2\cdot 3^2}\right)=\varphi(1)=1,
\end{array}\right\}$$

$\Rightarrow Y=1+1+2+2+1+1+2+1+1=12$ olur. Buna göre $\Gamma_0(2^2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$ daki yörüngeleri

$$\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}2\\3\end{pmatrix},\begin{pmatrix}1\\2\cdot 3\end{pmatrix},\begin{pmatrix}5\\2\cdot 3\end{pmatrix},\begin{pmatrix}1\\2^2\end{pmatrix},\begin{pmatrix}1\\3^2\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3\end{pmatrix},\begin{pmatrix}5\\2^2\cdot 3\end{pmatrix},\begin{pmatrix}1\\2\cdot 3^2\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3^2\end{pmatrix}$$

dir.

(ii) $\hat{\Gamma}_0(2^2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$ daki yörünge sayısını bulalım.

$d \parallel N$ olan d bölenleri; $1,2^2,3^2,2^2\cdot 3^2$, $d=2\cdot(N_0=3^2$ nin tam bölenleri$)$ olan d bölenleri $2,2\cdot 3^2$; ve ayrıca $d \mid N$ fakat $d \nparallel N$ ve $d\neq 2\cdot$ (3^2 nin tam bölenleri) olan d bölenleri; $3,2\cdot 3,2^2\cdot 3$ tür.

$$\varphi\left(3, {}^{2\cdot 3^2}\!/_{3}\right)=\varphi(3)=2,\varphi\left(2\cdot 3, {}^{2\cdot 3^2}\!/_{2\cdot 3}\right)=\varphi(2\cdot 3)=2,\varphi\left(2^2\cdot 3, {}^{2\cdot 3^2}\!/_{2^2\cdot 3}\right)=\varphi(3)=2$$

dir. Teorem 2.13 (ii) den $\hat{Y}=3\cdot 2+\dfrac{2+2+2}{2}=9$ dur. Burana göre $\hat{\Gamma}_0(2^2\cdot 3^2)$ nin $\hat{\mathbb{Q}}$ daki yörüngeleri $\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}1\\2\cdot 3\end{pmatrix}\begin{pmatrix}1\\2^2\end{pmatrix},\begin{pmatrix}1\\3^2\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3\end{pmatrix},\begin{pmatrix}1\\2\cdot 3^2\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3^2\end{pmatrix}$ dir.

Örnek 2.4. $N = 2^3 \cdot 3^2 \cdot 5$ alalım. Buna göre N' nin pozitif bölenleri; $1, 2, 3, 5, 2\cdot 3, 2\cdot 5, 3\cdot 5, 2\cdot 3\cdot 5, 2^2, 2^2\cdot 3, 2^2\cdot 5, 2^2\cdot 3\cdot 5, 3^2, 2\cdot 3^2, 3^2\cdot 5, 2\cdot 3^2\cdot 5, 2^2\cdot 3^2, 2^2\cdot 3^2\cdot 5, 2^3,$ $2^3\cdot 3, 2^3\cdot 5, 2^3\cdot 3\cdot 5, 2^3\cdot 3^2, 2^3\cdot 3^2\cdot 5$ tir.

(i) $\Gamma_0(2^3\cdot 3^2\cdot 5)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısını bulalım.

$$\left.\begin{aligned}
&\varphi\left(1, 2^3\cdot 3^2\cdot 5\right) = \varphi(1) = 1,\ \varphi\left(2, {2^3\cdot 3^2\cdot 5}/{2}\right) = \varphi(2) = 1,\ \varphi\left(3, {2^3\cdot 3^2\cdot 5}/{3}\right) = \varphi(3) = 2,\\
&\varphi\left(5, {2^3\cdot 3^2\cdot 5}/{5}\right) = \varphi(1) = 1,\quad \varphi\left(2\cdot 3, {2^3\cdot 3^2\cdot 5}/{2\cdot 3}\right) = \varphi(2\cdot 3) = 2,\\
&\varphi\left(2\cdot 5, {2^3\cdot 3^2\cdot 5}/{2\cdot 5}\right) = \varphi(2) = 1,\quad \varphi\left(3\cdot 5, {2^3\cdot 3^2\cdot 5}/{3\cdot 5}\right) = \varphi(3) = 2,\\
&\varphi\left(2\cdot 3\cdot 5, {2^3\cdot 3^2\cdot 5}/{2\cdot 3\cdot 5}\right) = \varphi(2\cdot 3) = 2,\quad \varphi\left(2^2, {2^3\cdot 3^2\cdot 5}/{2^2}\right) = \varphi(2) = 1,\\
&\varphi\left(2^2\cdot 3, {2^3\cdot 3^2\cdot 5}/{2^2\cdot 3}\right) = \varphi(2\cdot 3) = 2,\quad \varphi\left(2^2\cdot 5, {2^3\cdot 3^2\cdot 5}/{2^2\cdot 5}\right) = \varphi(2) = 1,\\
&\varphi\left(2^2\cdot 3\cdot 5, {2^3\cdot 3^2\cdot 5}/{2^2\cdot 3\cdot 5}\right) = \varphi(2\cdot 3) = 2\ ,\quad \varphi\left(3^2, {2^3\cdot 3^2\cdot 5}/{3^2}\right) = \varphi(1) = 1,\\
&\varphi\left(2\cdot 3^2, {2^3\cdot 3^2\cdot 5}/{2\cdot 3^2}\right) = \varphi(2) = 1,\quad \varphi\left(3^2\cdot 5, {2^3\cdot 3^2\cdot 5}/{3^2\cdot 5}\right) = \varphi(1) = 1,\\
&\varphi\left(2\cdot 3^2\cdot 5, {2^3\cdot 3^2\cdot 5}/{2\cdot 3^2\cdot 5}\right) = \varphi(2) = 1,\quad \varphi\left(2^2\cdot 3^2, {2^3\cdot 3^2\cdot 5}/{2^2\cdot 3^2}\right) = \varphi(2) = 1,\\
&\varphi\left(2^2\cdot 3^2\cdot 5, {2^3\cdot 3^2\cdot 5}/{2^2\cdot 3^2\cdot 5}\right) = \varphi(2) = 1,\ \varphi\left(2^3, {2^3\cdot 3^2\cdot 5}/{2^3}\right) = \varphi(1) = 1,\\
&\varphi\left(2^3\cdot 3, {2^3\cdot 3^2\cdot 5}/{2^3\cdot 3}\right) = \varphi(3) = 2,\ \varphi\left(2^3\cdot 5, {2^3\cdot 3^2\cdot 5}/{2^3\cdot 5}\right) = \varphi(1) = 1,\\
&\varphi\left(2^3\cdot 3\cdot 5, {2^3\cdot 3^2\cdot 5}/{2^3\cdot 3\cdot 5}\right) = \varphi(3) = 2,\ \varphi\left(2^3\cdot 3^2, {2^3\cdot 3^2\cdot 5}/{2^3\cdot 3^2}\right) = \varphi(1) = 1,\\
&\varphi\left(2^3\cdot 3^2\cdot 5, {2^3\cdot 3^2\cdot 5}/{2^3\cdot 3^2\cdot 5}\right) = \varphi(1) = 1
\end{aligned}\right\}$$

$$\Rightarrow Y = 1+1+2+1+2+1+2+2+1+2+1+2+1+1+1+1+1+1+1+2+1+2+1+1 = 32$$

Buna göre $\Gamma_0(2^3\cdot 3^2\cdot 5)$ nin $\hat{\mathbb{Q}}$ - daki yörüngeleri

$$\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\3\end{pmatrix}, \begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}1\\5\end{pmatrix}, \begin{pmatrix}1\\2\cdot 3\end{pmatrix}, \begin{pmatrix}5\\2\cdot 3\end{pmatrix}, \begin{pmatrix}1\\2\cdot 5\end{pmatrix}, \begin{pmatrix}1\\3\cdot 5\end{pmatrix}, \begin{pmatrix}2\\3\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2\cdot 3\cdot 5\end{pmatrix}, \begin{pmatrix}11\\2\cdot 3\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2^2\end{pmatrix},$$

$$\begin{pmatrix}1\\2^2\cdot 3\end{pmatrix}, \begin{pmatrix}5\\2^2\cdot 3\end{pmatrix}, \begin{pmatrix}1\\2^2\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2^2\cdot 3\cdot 5\end{pmatrix}, \begin{pmatrix}11\\2^2\cdot 3\cdot 5\end{pmatrix}, \begin{pmatrix}1\\3^2\end{pmatrix}, \begin{pmatrix}1\\2\cdot 3^2\end{pmatrix}, \begin{pmatrix}1\\3^2\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2\cdot 3^2\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2^2\cdot 3^2\end{pmatrix},$$

$$\begin{pmatrix}1\\2^2\cdot 3^2\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2^3\end{pmatrix}, \begin{pmatrix}1\\2^3\cdot 3\end{pmatrix}, \begin{pmatrix}5\\2^3\cdot 3\end{pmatrix}, \begin{pmatrix}1\\2^3\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2^3\cdot 3\cdot 5\end{pmatrix}, \begin{pmatrix}11\\2^3\cdot 3\cdot 5\end{pmatrix}, \begin{pmatrix}1\\2^3\cdot 3^2\end{pmatrix}, \begin{pmatrix}1\\2^3\cdot 3^2\cdot 5\end{pmatrix}.$$

(ii) $\hat{\Gamma}_0(2^3\cdot 3^2\cdot 5)$ nin $\hat{\mathbb{Q}}$ - daki yörünge sayısını bulalım.

$d \,\|\, N$ olan d-ler; $1,5,3^2,3^2\cdot 5,2^3,2^3\cdot 5,2^3\cdot 3^2,2^3\cdot 3^2\cdot 5$,

$d = 2\cdot(N_0 = 3^2\cdot 5 \text{ in tam bölenleri})$ olan d bölenleri; $2,2\cdot 5,2\cdot 3^2,2\cdot 3^2\cdot 5$;

$d = 2^2\cdot(N_0 = 3^2\cdot 5 \text{ in tam bölenleri})$ olan d bölenleri; $2^2,2^2\cdot 5,2^2\cdot 3^2,2^2\cdot 3^2\cdot 5$;

$d \mid N$, $d \nparallel N$, $d\neq 2\cdot(N_0 = 3^2\cdot 5 \text{ in tam bölenleri})$ ve $d\neq 2^2\cdot(N_0 = 3^2\cdot 5 \text{ in tam bölenleri})$

olan d bölenleri; $3,2\cdot 3,3\cdot 5,2\cdot 3\cdot 5,2^2\cdot 3,2^2\cdot 3\cdot 5,2^3\cdot 3,2^3\cdot 3\cdot 5$ dir.

$$\left.\begin{array}{ll}
\varphi\left(3,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{3}\right)=\varphi(3)=2 & ,\ \varphi\left(2^2\cdot 3,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{2^2\cdot 3}\right)=\varphi(2\cdot 3)=2 \\
\varphi\left(2\cdot 3,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{2\cdot 3}\right)=\varphi(2\cdot 3)=2 & ,\ \varphi\left(2^2\cdot 3\cdot 5,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{2^2\cdot 3\cdot 5}\right)=\varphi(2\cdot 3)=2 \\
\varphi\left(3\cdot 5,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{3\cdot 5}\right)=\varphi(3)=2 & ,\ \varphi\left(2^3\cdot 3,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{2^3\cdot 3}\right)=\varphi(3)=2 \\
\varphi\left(2\cdot 3\cdot 5,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{2\cdot 3\cdot 5}\right)=\varphi(2\cdot 3)=2 & ,\ \varphi\left(2^3\cdot 3\cdot 5,{}^{2^3\cdot 3^2\cdot 5}\!\big/_{2^3\cdot 3\cdot 5}\right)=\varphi(3)=2
\end{array}\right\}$$

Teorem 2.13 (iii) den $r=3$ olmak üzere $\hat{Y} = 2^{3+1} + \dfrac{2+2+2+2+2+2+2+2}{2} = 16+8=24$

tane yörünge var. Buna göre $\hat{\Gamma}_0(2^3\cdot 3^2\cdot 5)$ nin $\hat{\mathbb{Q}}$ - daki yörüngeleri

$$\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}1\\5\end{pmatrix},\begin{pmatrix}1\\2\cdot 3\end{pmatrix},\begin{pmatrix}1\\2\cdot 5\end{pmatrix},\begin{pmatrix}1\\3\cdot 5\end{pmatrix},\begin{pmatrix}1\\2\cdot 3\cdot 5\end{pmatrix},$$

$$\begin{pmatrix}1\\2^2\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 5\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3\cdot 5\end{pmatrix},\begin{pmatrix}1\\3^2\end{pmatrix},\begin{pmatrix}1\\2\cdot 3^2\end{pmatrix},$$

$$\begin{pmatrix}1\\3^2\cdot 5\end{pmatrix},\begin{pmatrix}1\\2\cdot 3^2\cdot 5\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3^2\end{pmatrix},\begin{pmatrix}1\\2^2\cdot 3^2\cdot 5\end{pmatrix},\begin{pmatrix}1\\2^3\end{pmatrix},\begin{pmatrix}1\\2^3\cdot 3\end{pmatrix},$$

$$\begin{pmatrix}1\\2^3\cdot 5\end{pmatrix},\begin{pmatrix}1\\2^3\cdot 3\cdot 5\end{pmatrix},\begin{pmatrix}1\\2^3\cdot 3^2\end{pmatrix},\begin{pmatrix}1\\2^3\cdot 3^2\cdot 5\end{pmatrix}$$

şeklindedir.

2.4. $\hat{\Gamma}$-nın $\hat{\mathbb{Q}}$ Üzerindeki Alt Yörüngesel Grafları

$\hat{\Gamma}$ - nın $\hat{\mathbb{Q}}$ üzerindeki hareketi transitif olduğundan her bir alt yörünge bir $v \in \hat{\mathbb{Q}}$ için (∞, v) ikilisini ihtiva eder öyle ki $N \geq 1$ ve $(u,N) = 1$ olmak üzere $v = \dfrac{u}{N}$ dir. Bu alt yörüngeyi $\hat{O}_{u,N}$ ile ve buna karşılık gelen $\hat{G}(\infty, v)$ alt yörüngesel grafı da $\hat{G}_{u,N}$ ile göstereceğiz.

Eğer $v = \infty$ ise $\hat{G}_{1,0} = \hat{G}_{-1,0}$ *aşikâr alt yörüngesel graf*tır. Böylece kabul edelim ki $v \in \mathbb{Q}$ dir. Eğer $v' \in \mathbb{Q}$ ise bu takdirde $\hat{O}(\infty, v) = \hat{O}(\infty, v') \Leftrightarrow v$ ve v' $\hat{\Gamma}_\infty$ nın aynı yörüngesindedir. Yani $\exists g \in \hat{\Gamma}_\infty$ öyleki $g(v) = v'$.

Teorem 2.14. $\dfrac{r}{s} \to \dfrac{x}{y} \in \hat{G}_{u,N}$ olması için gerek ve yeter şart

(i) $x \equiv ur \bmod N,\ y \equiv us \bmod N$, $ry - sx = N$ veya

(ii) $x \equiv -ur \bmod N,\ y \equiv -us \bmod N$, $ry - sx = -N$ veya

(iii) $x \equiv ur \bmod N,\ y \equiv us \bmod N$, $ry - sx = -N$ veya

(iv) $x \equiv -ur \bmod N,\ y \equiv -us \bmod N$ ve $ry - sx = N$

olmasıdır.

İspat. (i) ve (ii) şıklarının ispatı Teorem 1.20 den açıktır.

(iii) $'' \Rightarrow ''$: $\dfrac{r}{s} \to \dfrac{x}{y} \in \hat{G}_{u,N}$ olsun. Bu takdirde $\exists T := \begin{pmatrix} a & -b \\ c & -d \end{pmatrix} \in \hat{\Gamma},\ -ad + bc = -1$, öyle ki

$$\begin{pmatrix} a & -b \\ c & -d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} a & au - bN \\ c & cu - dN \end{pmatrix} = \begin{pmatrix} r & x \\ s & y \end{pmatrix}$$

dir. Buradan $a = r$ ve $c = s$ dir. Buna göre

$$x = au - bN \ \Rightarrow\ x \equiv au \bmod N \ \Rightarrow\ x \equiv ur \bmod N$$

$$y = cu - dN \ \Rightarrow\ y \equiv cu \bmod N \ \Rightarrow\ y \equiv us \bmod N$$

ve ayrıca determinattan $ry - sx = -N$ bulunur.

$'' \Leftarrow ''$: $x \equiv ur \bmod N,\ y \equiv us \bmod N$ ve $ry - sx = -N$ olsun. Buradan $\exists\ k, \ell \in \mathbb{Z}$ öyle ki $x = ur - kN$ ve $y = us - \ell N$ dir. Böylece

$$\begin{pmatrix} r & -k \\ s & -\ell \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} r & x \\ s & y \end{pmatrix}$$

dir ve $ry - sx = -N$ den

$$r(us - \ell N) - s(ur - kN) = -N \;\Rightarrow\; rus - r\ell N - sur + skN = -N \;\Rightarrow\; -r\ell + sk = -1$$

bulunur. Buradan $\begin{pmatrix} r & -k \\ s & -\ell \end{pmatrix} \in \hat{\Gamma}$ dır ve $\frac{r}{s} \to \frac{x}{y} \in \hat{G}_{u,N}$ dir.

(iv) $'' \Rightarrow ''$**:** $\frac{r}{s} \to \frac{x}{y} \in \hat{G}_{u,N}$ olsun. Bu takdirde $\exists T := \begin{pmatrix} a & -b \\ c & -d \end{pmatrix} \in \hat{\Gamma},\; -ad + bc = -1$, öyle ki

$$\begin{pmatrix} a & -b \\ c & -d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} a & au - bN \\ c & cu - dN \end{pmatrix} = \begin{pmatrix} r & -x \\ s & -y \end{pmatrix}$$

dir. Buradan $a = r$ ve $c = s$ dir. Buna göre

$$-x = au - bN \;\Rightarrow\; -x \equiv au \bmod N \;\Rightarrow\; x \equiv -ur \bmod N$$

$$-y = cu - dN \;\Rightarrow\; -y \equiv cu \bmod N \;\Rightarrow\; y \equiv -us \bmod N$$

ve ayrıca determinattan $-ry + sx = -N$ yani $ry - sx = N$ bulunur.

$'' \Leftarrow ''$**:** $x \equiv -ur \bmod N,\; y \equiv -us \bmod N$ ve $ry - sx = N$ olsun. Buradan $\exists\; t, v \in \mathbb{Z}$ öyle ki $x = -ur + tN$ ve $y = -us + vN$ dir. Böylece

$$\begin{pmatrix} r & -t \\ s & -v \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} r & -x \\ s & -y \end{pmatrix}$$

dir ve $ry - sx = N$ den

$$r(-us + vN) - s(-ur + tN) = N \;\Rightarrow\; -urs + rvN + sur - stN = N$$

olup buradan $rv - st = 1$, yani $-rv + st = -1$ bulunur. Böylece $\begin{pmatrix} r & -t \\ s & -v \end{pmatrix} \in \hat{\Gamma}$ dır ve $\frac{r}{s} \to \frac{x}{y} \in \hat{G}_{u,N}$ dir. ■

Sonuç 2.2. $uv \equiv \pm 1 \bmod N$ ise bu takdirde $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiş alt yörüngesel graflardır.

İspat. (I) $uv \equiv 1 \bmod N$ olsun. Bu takdirde Teorem 2.14 e göre aşağıdaki durumlara bakalım.

1. Durum $x \equiv ur \bmod N,\ y \equiv us \bmod N$ ve $ry - sx = N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv vur \bmod N \;\Rightarrow\; r \equiv vx \bmod N \\ vy \equiv vus \bmod N \;\Rightarrow\; s \equiv vy \bmod N \end{array}\right\} \text{ ve } sx - ry = -N$$

olduğundan $\dfrac{x}{y} \rightarrow \dfrac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.

2. Durum $x \equiv -ur \bmod N,\ y \equiv -us \bmod N$ ve $ry - sx = -N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv -vur \bmod N \;\Rightarrow\; r \equiv -vx \bmod N \\ vy \equiv -vus \bmod N \;\Rightarrow\; s \equiv -vy \bmod N \end{array}\right\} \text{ ve } sx - ry = N$$

olduğundan $\dfrac{x}{y} \rightarrow \dfrac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.

3. Durum $x \equiv ur \bmod N,\ y \equiv us \bmod N$ ve $ry - sx = -N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv vur \bmod N \;\Rightarrow\; r \equiv vx \bmod N \\ vy \equiv vus \bmod N \;\Rightarrow\; s \equiv vy \bmod N \end{array}\right\} \text{ ve } sx - ry = N$$

olduğundan $\dfrac{x}{y} \rightarrow \dfrac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.

4. Durum $x \equiv -ur \bmod N,\ y \equiv -us \bmod N$ ve $ry - sx = N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv -vur \bmod N \;\Rightarrow\; r \equiv -vx \bmod N \\ vy \equiv -vus \bmod N \;\Rightarrow\; s \equiv -vy \bmod N \end{array}\right\} \text{ ve } sx - ry = -N$$

olduğundan $\dfrac{x}{y} \rightarrow \dfrac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.

(II) $uv \equiv -1 \bmod N$ olsun. Bu takdirde Teorem 2.14 e göre aşağıdaki durumlara bakalım.

1. Durum $x \equiv ur \bmod N,\ y \equiv us \bmod N$ ve $ry - sx = N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv vur \bmod N \;\Rightarrow\; r \equiv -vx \bmod N \\ vy \equiv vus \bmod N \;\Rightarrow\; s \equiv -vy \bmod N \end{array}\right\} \text{ ve } sx - ry = -N$$

olduğundan $\dfrac{x}{y} \rightarrow \dfrac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.

2. Durum $x \equiv -ur \bmod N$, $y \equiv -us \bmod N$ ve $ry - sx = -N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv -vur \bmod N \;\Rightarrow\; r \equiv vx \bmod N \\ vy \equiv -vus \bmod N \;\Rightarrow\; s \equiv vy \bmod N \end{array}\right\} \text{ ve } sx - ry = N$$

olduğundan $\frac{x}{y} \to \frac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.

3. Durum $x \equiv ur \bmod N$, $y \equiv us \bmod N$ ve $ry - sx = -N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv vur \bmod N \;\Rightarrow\; r \equiv -vx \bmod N \\ vy \equiv vus \bmod N \;\Rightarrow\; s \equiv -vy \bmod N \end{array}\right\} \text{ ve } sx - ry = N$$

olduğundan $\frac{x}{y} \to \frac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.

4. Durum $x \equiv -ur \bmod N$, $y \equiv -us \bmod N$ ve $ry - sx = N$ dir. Buradan

$$\left.\begin{array}{l} vx \equiv -vur \bmod N \;\Rightarrow\; r \equiv vx \bmod N \\ vy \equiv -vus \bmod N \;\Rightarrow\; s \equiv vy \bmod N \end{array}\right\} \text{ ve } sx - ry = -N$$

olduğundan $\frac{x}{y} \to \frac{r}{s} \in \hat{G}_{v,N}$ olur. Buradan $\hat{G}_{u,N}$ ile $\hat{G}_{v,N}$ eşleşmiştir.■

Sonuç 2.3. $\hat{G}_{u,N}$ nin kendisiyle eşleşmiş olması için gerek ve yeter şart $u^2 \equiv \pm 1 \bmod N$ olmasıdır.

İspat $'' \Rightarrow ''$**:** Kabul edelim ki $\hat{G}_{u,N}$ kendisiyle eşleşmiş olsun. Böylece $\exists T \in \hat{\Gamma}$ öyle ki $\left(\infty, \frac{u}{N}\right) \xrightarrow{T} \left(\frac{u}{N}, \infty\right)$ dur. Buradan $T = \begin{pmatrix} u & -b \\ N & -u \end{pmatrix} \in \hat{\Gamma}$ dir.

$$\det T = 1 \text{ ise } -u^2 + bN = 1 \Rightarrow u^2 \equiv -1 \bmod N$$

ve

$$\det T = -1 \text{ ise } -u^2 + bN = -1 \Rightarrow u^2 \equiv 1 \bmod N$$

bulunur.

$'' \Leftarrow ''$**:** $u^2 \equiv 1 \bmod N$ ise $-u^2 \equiv -1 \bmod N$ dir. Buradan $-u^2 + bN = -1$ olacak şekilde bir $b \in \mathbb{Z}$ vardır. Böylece $\begin{pmatrix} u & -b \\ N & -u \end{pmatrix} \in \hat{\Gamma}$ dır.

$u^2 \equiv -1 \bmod N$ ise $-u^2 \equiv 1 \bmod N$ dir. Buradan $-u^2 + bN = 1$ olacak şekilde bir $b \in \mathbb{Z}$ vardır. Böylece $\begin{pmatrix} u & -b \\ N & -u \end{pmatrix} \in \hat{\Gamma}$ dır ve $\begin{pmatrix} u & -b \\ N & -u \end{pmatrix}$ ile $\infty \to \frac{u}{N}$ ve $\frac{u}{N} \to \infty$ olur. Buradan $\hat{G}_{u,N}$ kendisiyle eşleşmiştir.■

$\hat{G}_{1,1}$ alt yörüngesel grafına *Farey Grafi* denir ve "$\hat{F}$" ile gösterilir. $\hat{G}_{1,1}$ alt yörüngesel grafının köşeleri $\hat{\mathbb{Q}}$- nın elemanlarıdır ve bu Sonuç 2.3' e göre kendisiyle eşleşmiştir. Teorem 2.14'e göre "$\frac{r}{s}$ ve $\frac{x}{y}$ $\hat{G}_{1,1}$ de ardışık köşelerdir $\Leftrightarrow ry - sx = \pm 1$" dir.

$m \geq 1$ ve $m \in \mathbb{N}$ olsun. Bütün $\frac{x}{y}, |y| \leq m$ rasyonel sayılarından oluşan kesin monoton artan diziye *m. mertebeden Farey dizisi* denir ve bu dizi "$\hat{F}_m$" ile gösterilir, örneğin

$$\hat{F}_4 \text{ için: } \ldots, -\frac{1}{3}, -\frac{1}{4}, 0, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1, \frac{5}{4}, \frac{4}{3}, \ldots$$

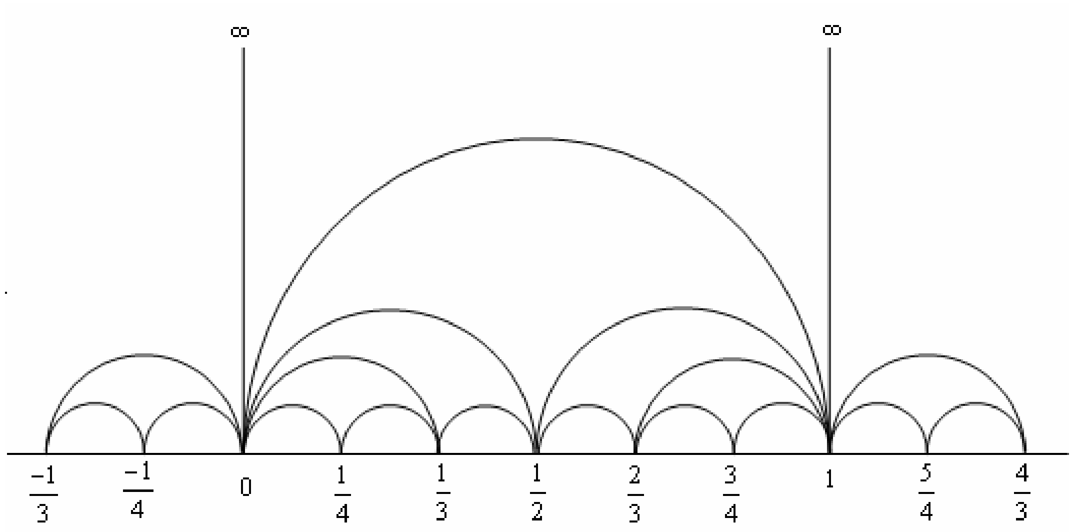
Açık olarak $\hat{F}_1 \subset \hat{F}_2 \subset \hat{F}_3 \subset \ldots$ ve $\bigcup_{m \geq 1} \hat{F}_m = \mathbb{Q}$'dur. Farey grafı ile Farey dizileri arasındaki bağıntıyı veren aşağıdaki önermeyi verelim.

Lemma 2.3. $\frac{r}{s}, \frac{x}{y} \in \mathbb{Q}$ olsun. Bu takdirde aşağıdakiler eşdeğerdir;

(i) $\frac{r}{s}$ ve $\frac{x}{y}$, $\hat{F}$ da komşu köşelerdir.

(ii) $ry - sx = \pm 1$

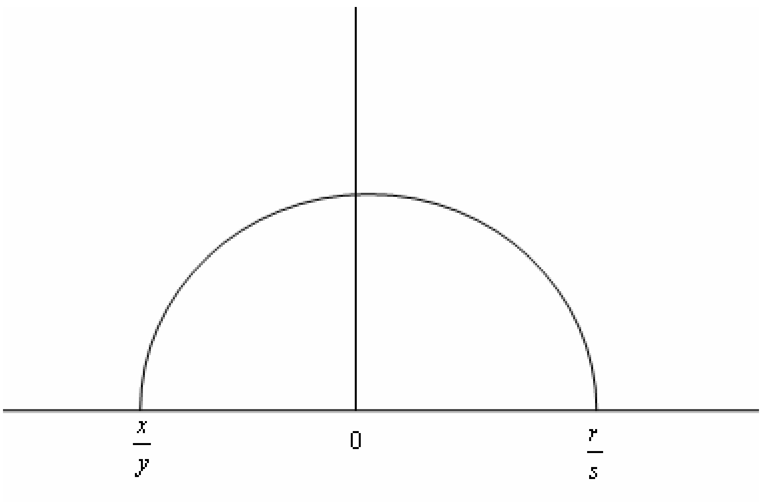
(iii) $\frac{r}{s}$ ve $\frac{x}{y}$, bir m doğal sayısı için, $\hat{F}_m$ nın ardışık terimleridir.■



Şekil 2.2 Farey Grafı

Sonuç 2.4. $\hat{F}$ -nın kenarları $\mathcal{U}=\{z\in\mathbb{C}:\mathrm{Im}(z)>0\}$ üst-yarı düzleminde kesişmezler.

İspat. $\frac{r}{s}\rightarrow\frac{x}{y}\in\hat{F}$ kenarını alalım. Burada $ry-sx=\pm 1$ dir. Kabul edelim ki 0 ile ∞-u birleştiren Re(z) = 0 doğrusu $\frac{r}{s}$ yi $\frac{x}{y}$ ye birleştiren doğruyu üst yarı düzlemde kessin. Bu takdirde $\frac{x}{y}<0<\frac{r}{s}$ alabiliriz.



Şekil 2.3 $\mathcal{U}$' da kesişen doğrular

Buna göre $ry-sx=1$ olur. $x<0$ ve $r,s,y>0$ olduğundan $1=ry-sx\geq 2$ çelişkisi elde edilir. Bu çelişkiden $\hat{F}$ -nın kenarlarının $\mathcal{U}$- da kesişmedikleri bulunur.■

2.5. $\hat{G}_{u,N}$ ve $\hat{F}_{u,N}$ Grafları

Bu bölümde $\hat{F} = \hat{G}_{1,1}$ in özelliklerinin diğer $\hat{G}_{u,N}$ alt yörüngesel graflarına nasıl genişletileceğini göstereceğiz. $\hat{\Gamma}$, $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket ettiğinden blokları transitif olarak permüte eder. Dolayısıyla alt grafların hepsi izomorftur.

Şimdi $\hat{F}\left(\infty, \frac{u}{N}\right)$ ile köşeleri $[\infty] := \left\{ \frac{x}{y} \in \hat{\mathbb{Q}} : y \equiv 0 \bmod N \right\}$- bloğunun elemanları olan $\hat{G}\left(\infty, \frac{u}{N}\right)$ alt yörüngesel grafının alt grafını göstereceğiz. Kısaca $\hat{F}\left(\infty, \frac{u}{N}\right)$ yerine $\hat{F}_{u,N}$ yazacağız.

Buna göre Teorem 2.14 den aşağıdaki teorem elde edilir.

Teorem 2.15. $\frac{r}{s}, \frac{x}{y} \in [\infty]$ olsun. Bu takdirde $\frac{r}{s} \rightarrow \frac{x}{y}$ nin $\hat{F}_{u,N}$ de bir kenar olması için gerek ve yeter şart

(i) $x \equiv ur \bmod N$, $ry - sx = N$ veya

(ii) $x \equiv -ur \bmod N$, $ry - sx = -N$ veya

(iii) $x \equiv ur \bmod N$, $ry - sx = -N$ veya

(iv) $x \equiv -ur \bmod N$, $ry - sx = N$

olmasıdır.■

Teorem 2.16. $\hat{\Gamma}_0(N)$, $\hat{F}_{u,N}$ nin köşelerini ve kenarlarını transitif olarak permüte eder.

İspat. (i) v ve w $\hat{F}_{u,N}$ de iki köşe olsun. $\hat{\Gamma}$- nın $\hat{\mathbb{Q}}$ üzerinde transitif olduğundan $\exists\ T \in \hat{\Gamma} : T(v) = w$ dır. Buna göre $\hat{\Gamma}$ blokları permüte eder ve $v, w \in [\infty]$ dur.

$v = \frac{k}{\ell N}$ ve $w = \frac{t}{sN}$ alalım. $T = \begin{pmatrix} a & -b \\ c & -d \end{pmatrix} \in \hat{\Gamma}$ için

$$\begin{pmatrix} a & -b \\ c & -d \end{pmatrix} \left(\frac{k}{\ell N} \right) = \frac{ak - b\ell N}{ck - d\ell N} = \frac{t}{sN}$$

olup buradan $N \mid ck$ dır ve $(k,N) = 1$ olduğundan $N \mid c$ bulunur. Böylece $T \in \hat{\Gamma}_0(N)$ olur ve $[\infty]$ bloğunu korur. Buradan $\hat{\Gamma}_0(N)$, $\hat{F}_{u,N}$ nin köşelerini transitif olarak permüte eder.

(ii) $\frac{r}{s} \to \frac{x}{y} \in \hat{F}_{u,N}$ ve $\frac{a}{b} \to \frac{c}{d} \in \hat{F}_{u,N}$ iki kenar olsun. Bu takdirde $\exists\ T_1, T_2 \in \hat{\Gamma}$ öyle ki $\left(\infty, \frac{u}{N}\right) \xrightarrow{T_1} \left(\frac{r}{s}, \frac{x}{y}\right)$ ve $\left(\infty, \frac{u}{N}\right) \xrightarrow{T_2} \left(\frac{a}{b}, \frac{c}{d}\right)$ dir. Buradan $T_2 T_1^{-1} : \left(\frac{r}{s}, \frac{x}{y}\right) \to \left(\frac{a}{b}, \frac{c}{d}\right)$ ve $T_2 T_1^{-1} \in \hat{\Gamma}_0(N)$ dir. Böylece $\hat{\Gamma}_0(N)$, $\hat{F}_{u,N}$ nin köşelerini transitif olarak permüte eder. ■

Teorem 2.17. $\hat{F}_{u,N}$ nin bir üçgen ihtiva etmesi için gerek ve yeter şart $u^2 \pm u + 1 \equiv 0 \bmod N$ olmasıdır. (∞ ile başlayan bir üçgen için, $u^2 - u + 1 \equiv 0 \bmod N$ ise üçgenin kenar şartları sırasıyla Teorem 2.15 deki (i),(i),(ii) veya (iv),(iii),(iii) ; $u^2 + u + 1 \equiv 0 \bmod N$ ise üçgendeki kenar şartları sırasıyla Teorem 2.15 deki (i),(ii),(ii) veya (iv),(iv),(iii) şeklindedir. Eğer üçgen ∞ ile başlamıyor ise bu üçgenin kenar şartları, ∞ ile başlayan üçgenin kenar şartlarının kendi aralarında yer değiştirmelerinden ibarettir).

İspat. $''\Rightarrow''$ Kabul edelim ki $\hat{F}_{u,N}$ bir üçgen ihtiva etsin. Teorem 2.16 ya göre bu üçgen 1. durumda $v \in \hat{F}_{u,N}$ için $\infty \to \frac{u}{N} \to v \to \infty$ formunda, 2. durumda $v_1 \in \hat{F}_{u,N}$ için $\infty \to \frac{-u}{N} \to v_1 \to \infty$ formundadır. Şimdi bu durumları inceleyelim.

1.Durum $v \to \infty$ olduğundan Teorem 2.15 e göre $\exists\ r \in \mathbb{Z} : v = \frac{r}{N}$ dir. Buna göre $\frac{u}{N} \to \frac{r}{N} \in \hat{F}_{u,N}$ olduğundan $u - r = \pm 1$ dir. Böylece üçgen $\frac{1}{0} \to \frac{u}{N} \to \frac{u \pm 1}{N} \to \frac{1}{0}$ şeklindedir.

(A) $\frac{1}{0} \xrightarrow[\text{(i)}]{} \frac{u}{N} \xrightarrow[\text{(i),(iv)}]{} \frac{u-1}{N} \xrightarrow[\text{(ii),(iii)}]{} \frac{1}{0}$ olsun. $\frac{u-1}{N} \to \frac{1}{0}$ göz önüne alınırsa

(1^0) (ii) geçerli ise bu takdirde $1 \equiv -u(u-1) \bmod N$

veya

(2^0) (iii) geçerli ise bu takdirde $1 \equiv u(u-1) \bmod N$.

(A.1) $\frac{u}{N} \to \frac{u-1}{N}$ için (i) kenar şartı geçerli olsun. Bu takdirde

$$u - 1 \equiv u^2 \bmod N \Rightarrow u^2 - u + 1 \equiv 0 \bmod N \qquad (1^*)$$

elde edilir. Buna göre

(A.1.a) (1^0) -ı (1^*)- da yerine yazarsak

$$u^2 - u - u^2 + u \equiv 0 \bmod N \;\Rightarrow 0 \equiv 0 \bmod N$$

bulunur ki bu $\frac{1}{0} \to \frac{u}{N} \to \frac{u-1}{N} \to \frac{1}{0}$ üçgeni için $u^2 - u + 1 \equiv 0 \bmod N$ ve kenar şartlarının sırasıyla (i),(i),(ii) olduğunu gösterir.

(A.1.b) (2^0) -ı (1^*)- da yerine yazarsak

$$u^2 - u + u^2 - u \equiv 0 \bmod N \;\Rightarrow 2u(u-1) \equiv 0 \bmod N$$

$$\Rightarrow u \equiv 0 \bmod N \text{ veya } u - 1 \equiv 0 \bmod N$$

elde edilir ki bu durum $(u,N) = 1$ ve $(u–1, N) = 1$ olmasıyla çelişir. Buna göre üçgen olma şartı $u^2 - u + 1 \equiv 0 \bmod N$ olduğunda kenar şartları sırasıyla (i),(i),(iii) olamaz.

(A.2) $\frac{u}{N} \to \frac{u-1}{N}$ için (iv) kenar şartı geçerli olsun. Bu takdirde

$$u - 1 \equiv -u^2 \bmod N \;\Rightarrow u^2 + u - 1 \equiv 0 \bmod N \qquad (2^*)$$

elde edilir. Buna göre

(A.2.a) (1^0) -ı (2^*)- da yerine yazarsak

$$u^2 + u + u^2 - u \equiv 0 \bmod N \;\Rightarrow 2u^2 \equiv 0 \bmod N \;\Rightarrow\; u \equiv 0 \bmod N$$

elde edilir ki bu $(u,N) = 1$ olmasıyla çelişir. Buna göre üçgen olma şartı $u^2 + u - 1 \equiv 0 \bmod N$ olamaz ve kenar şartları sırasıyla (i),(iv),(ii) olamaz.

(A.2.b) (2^0) -ı (2^*)- da yerine yazarsak

$$u^2 + u - u^2 + u \equiv 0 \bmod N \;\Rightarrow 2u \equiv 0 \bmod N \;\Rightarrow\; u \equiv 0 \bmod N$$

çelişkisi elde edilir ki bu durumda da üçgen olma şartı $u^2 + u - 1 \equiv 0 \bmod N$ olamaz ve kenar şartları sırasıyla (i),(iv),(iii) olamaz.

(B) $\frac{1}{0} \xrightarrow[\text{(i)}]{} \frac{u}{N} \xrightarrow[\text{(ii),(iii)}]{} \frac{u+1}{N} \xrightarrow[\text{(ii),(iii)}]{} \frac{1}{0}$ olsun. $\frac{u+1}{N} \to \frac{1}{0}$ göz önüne alınırsa

(3^0) (ii) geçerli ise bu takdirde $1 \equiv -u(u+1) \bmod N$

veya

(4^0) (iii) geçerli ise bu takdirde $1 \equiv u(u+1) \bmod N$

dir.

(B.1) $\frac{u}{N} \to \frac{u+1}{N}$ için (ii) kenar şartı geçerli olsun. Bu takdirde

$$u+1 \equiv -u^2 \bmod N \Rightarrow u^2+u+1 \equiv 0 \bmod N \qquad (3^*)$$

elde edilir. Buna göre

(B.1.a) (3^0) -ı (3^*)- da yerine yazarsak

$$u^2+u-u^2-u \equiv 0 \bmod N \Rightarrow 0 \equiv 0 \bmod N$$

bulunur ki bu $\frac{1}{0} \to \frac{u}{N} \to \frac{u+1}{N} \to \frac{1}{0}$ üçgeni için $u^2+u+1 \equiv 0 \bmod N$ ve kenar şartları sırasıyla (i),(ii),(ii) olduğunu gösterir.

(B.1.b) (4^0) -ı (3^*)- da yerine yazarsak

$$u^2+u+u^2+u \equiv 0 \bmod N \Rightarrow 2u(u+1) \equiv 0 \bmod N$$

$$\Rightarrow u \equiv 0 \bmod N \text{ veya } u+1 \equiv 0 \bmod N$$

elde edilir ki bu durum $(u,N) = 1$ ve $(u+1,N) = 1$ olmasıyla çelişir. Buna göre üçgen olma şartı $u^2+u+1 \equiv 0 \bmod N$ olduğunda kenar şartları sırasıyla (i),(ii),(iii) olamaz.

(B.2) $\frac{u}{N} \to \frac{u+1}{N}$ için (iii) kenar şartı geçerli olsun. Bu takdirde

$$u+1 \equiv u^2 \bmod N \Rightarrow u^2-u-1 \equiv 0 \bmod N \qquad (4^*)$$

elde edilir. Buna göre

(B.2.a) (3^0) -ı (4^*)- da yerine yazarsak

$$u^2-u+u^2+u \equiv 0 \bmod N \Rightarrow 2u^2 \equiv 0 \bmod N \Rightarrow u \equiv 0 \bmod N$$

elde edilir ki bu $(u,N) = 1$ olmasıyla çelişir. Buna göre üçgen olma şartı $u^2-u-1 \equiv 0 \bmod N$ olamaz ve kenar şartları sırasıyla (i),(iii),(ii) olamaz.

(B.2.b) (4^0) -ı (4^*)- da yerine yazarsak

$$u^2-u-u^2-u \equiv 0 \bmod N \Rightarrow 2u \equiv 0 \bmod N \Rightarrow u \equiv 0 \bmod N$$

çelişkisi elde edilir ki bu durumda da üçgen olma şartı $u^2-u-1\equiv 0 \bmod N$ olamaz ve kenar şartları sırasıyla (i),(iii),(iii) olamaz.

2.Durum $v_1\to\infty$ olduğundan Teorem 2.15 e göre $\exists\, r_1\in\mathbb{Z}\,:\, v_1=\dfrac{r_1}{N}$ dir. Buna göre $\dfrac{-u}{N}\to\dfrac{r_1}{N}\in\hat{F}_{u,N}$ olduğundan $-u-r_1=\pm 1$ dir. Böylece üçgen $\dfrac{1}{0}\to\dfrac{-u}{N}\to\dfrac{-u\pm 1}{N}\to\dfrac{1}{0}$ şeklinde olur.

(C) $\dfrac{1}{0}\xrightarrow[\text{(iv)}]{}\dfrac{-u}{N}\xrightarrow[\text{(ii),(iii)}]{}\dfrac{-u+1}{N}\xrightarrow[\text{(ii),(iii)}]{}\dfrac{1}{0}$ olsun. $\dfrac{-u+1}{N}\to\dfrac{1}{0}$ göz önüne alınırsa

(5^0) (ii) geçerli ise bu takdirde $1\equiv -u(-u+1) \bmod N$

veya

(6^0) (iii) geçerli ise bu takdirde $1\equiv u(-u+1) \bmod N$

dir.

(C.1) $\dfrac{-u}{N}\to\dfrac{-u+1}{N}$ için (ii) kenar şartı geçerli olsun. Bu takdirde

$$-u+1\equiv u^2 \bmod N \;\Rightarrow\; u^2+u-1\equiv 0 \bmod N \qquad (5^*)$$

elde edilir. Buna göre

(C.1.a) (5^0) -ı (5^*)- da yerine yazarsak

$$u^2+u-u^2+u\equiv 0 \bmod N \;\Rightarrow\; 2u\equiv 0 \bmod N \;\Rightarrow\; u\equiv 0 \bmod N$$

çelişkisi bulunur. Buna göre burada üçgen olma şartı $u^2+u-1\equiv 0 \bmod N$ olamaz ve kenar şartları sırasıyla (iv),(ii),(ii) olamaz.

(C.1.b) (6^0) -ı (5^*)- da yerine yazarsak

$$u^2+u+u^2-u\equiv 0 \bmod N \;\Rightarrow\; 2u^2\equiv 0 \bmod N \;\Rightarrow\; u\equiv 0 \bmod N$$

çelişkisi elde edilir. Böylece bu üçgen için $u^2+u-1\equiv 0 \bmod N$ üçgen olma şartı olamaz ve kenar şartları sırasıyla (iv),(ii),(iii) olamaz.

(C.2) $\dfrac{-u}{N}\to\dfrac{-u+1}{N}$ için (iii) kenar şartı geçerli olsun. Bu takdirde

$$-u+1\equiv -u^2 \bmod N \;\Rightarrow\; u^2-u+1\equiv 0 \bmod N \qquad (6^*)$$

elde edilir. Buna göre

(C.2.a) (5^0) -ı (6^*)- da yerine yazarsak

$$u^2 - u + u^2 - u \equiv 0 \text{ mod } N \Rightarrow -2u(-u+1) \equiv 0 \text{ mod } N$$
$$\Rightarrow u \equiv 0 \text{ mod } N \text{ veya } -u+1 \equiv 0 \text{ mod } N$$

elde edilir ki bu $(u,N) = 1$ ve $(-u+1,N) = 1$ olmasıyla çelişir. Buna göre üçgen olma şartı $u^2 - u + 1 \equiv 0 \text{ mod } N$ olduğunda kenar şartları sırasıyla (iv),(iii),(ii) olamaz.

(C.2.b) (6^0) -ı (6^*)- da yerine yazarsak

$$u^2 - u - u^2 + u \equiv 0 \text{ mod } N \Rightarrow 0 \equiv 0 \text{ mod } N$$

bulunur ki bu üçgen olma şartının $u^2 - u + 1 \equiv 0 \text{ mod } N$ olduğunu ve kenar şartlarının sırasıyla (i),(iv),(iii) olduğunu gösterir.

(D) $\frac{1}{0} \xrightarrow[\text{(iv)}]{} \frac{-u}{N} \xrightarrow[\text{(i),(iv)}]{} \frac{-u-1}{N} \xrightarrow[\text{(ii),(iii)}]{} \frac{1}{0}$ olsun. $\frac{-u-1}{N} \rightarrow \frac{1}{0}$ göz önüne alınırsa

(7^0) (ii) geçerli ise bu takdirde $1 \equiv -u(-u-1) \text{ mod } N \Rightarrow 1 \equiv u(u+1) \text{ mod } N$

veya

(8^0) (iii) geçerli ise bu takdirde $1 \equiv u(-u-1) \text{ mod } N \Rightarrow 1 \equiv -u(u+1) \text{ mod } N$.

(D.1) $\frac{-u}{N} \rightarrow \frac{-u-1}{N}$ için (i) kenar şartı geçerli olsun. Bu takdirde

$$-u-1 \equiv -u^2 \text{ mod } N \Rightarrow u^2 - u - 1 \equiv 0 \text{ mod } N \qquad (7^*)$$

elde edilir. Buna göre

(D.1.a) (7^0) -ı (7^*)- da yerine yazarsak

$$u^2 - u - u^2 - u \equiv 0 \text{ mod } N \Rightarrow 2u \equiv 0 \text{ mod } N \Rightarrow u \equiv 0 \text{ mod } N$$

bulunur ki bu bir çelişkidir. Buradan bu üçgeni için $u^2 - u - 1 \equiv 0 \text{ mod } N$ üçgen olma şartı olamaz ve kenar şartları sırasıyla (iv),(i),(ii) olamaz.

(D.1.b) (8^0) -ı (7^*)- da yerine yazarsak

$$u^2 - u + u^2 + u \equiv 0 \text{ mod } N \Rightarrow 2u^2 \equiv 0 \text{ mod } N \Rightarrow u \equiv 0 \text{ mod } N$$

çelişkisi elde edilir. Buna göre yine üçgen olma şartı $u^2-u-1\equiv 0 \bmod N$ olamaz ve kenar şartları sırasıyla (iv),(i),(iii) olamaz.

(D.2) $\dfrac{-u}{N}\rightarrow\dfrac{-u-1}{N}$ için (iv) kenar şartı geçerli olsun. Bu takdirde

$$-u-1\equiv u^2 \bmod N \;\Rightarrow u^2+u+1\equiv 0 \bmod N \qquad (8^*)$$

elde edilir. Buna göre

(D.2.a) (7^0) -ı (8^*)- da yerine yazarsak

$$u^2+u+u^2+u\equiv 0 \bmod N \;\Rightarrow -2u(-u-1)\equiv 0 \bmod N$$

$$\Rightarrow\; u\equiv 0 \bmod N \text{ veya } -u-1\equiv 0 \bmod N$$

elde edilir ki bu $(u,N) = 1$ ve $(-u–1, N) = 1$ olmasıyla çelişir. Buna göre üçgen olma şartı $u^2+u+1\equiv 0 \bmod N$ olduğunda kenar şartları sırasıyla (iv),(iv),(ii) olamaz.

(D.2.b) (8^0) -ı (8^*)- da yerine yazarsak

$$u^2+u-u^2-u\equiv 0 \bmod N \;\Rightarrow 0\equiv 0 \bmod N$$

elde edilir ki bu üçgen için $u^2+u+1\equiv 0 \bmod N$ üçgen olma şartıdır ve kenar şartlarının sırasıyla (iv),(iv),(iii) olur.

Sonuç olarak $\infty\rightarrow\dfrac{u}{N}\rightarrow\dfrac{u\pm 1}{N}\rightarrow\infty$, $\hat{F}_{u,N}$ da bir üçgen ise

(A.1.a) dan $u^2-u+1\equiv 0 \bmod N$ ve kenar şartları sırasıyla (i),(i),(ii)

(B.1.a) dan $u^2+u+1\equiv 0 \bmod N$ ve kenar şartları sırasıyla (i),(ii),(ii)

dir ve $\infty\rightarrow\dfrac{-u}{N}\rightarrow\dfrac{-u\pm 1}{N}\rightarrow\infty$, $\hat{F}_{u,N}$ de bir üçgen ise

(C.2.b) den $u^2-u+1\equiv 0 \bmod N$ ve kenar şartları sırasıyla (iv),(iii),(iii)

(D.2.b) den $u^2+u+1\equiv 0 \bmod N$ ve kenar şartları sırasıyla (iv),(iv),(iii)

bulunur.

$'' \Leftarrow ''$ $u^2 \pm u + 1 \equiv 0 \bmod N$ olsun. Buna göre

1.Durum Teorem 2.15' e göre $\infty \to \frac{u}{N} \to \frac{u \pm 1}{N} \to \infty$ yönlendirilmiş üçgeni $\hat{F}_{u,N}$ dadır [14].

2.Durum **(a)** $u^2 - u + 1 \equiv 0 \bmod N$ olsun. Buradan $-u + 1 \equiv -u^2 \bmod N$ ve $1 \equiv u(-u+1) \bmod N$ bulunur. Buna göre $\frac{1}{0} \to \frac{-u}{N} \to \frac{-u+1}{N} \to \frac{1}{0}$ elde edilir ki, bu $\hat{F}_{u,N}$ da kenar şartları sırasıyla (iv),(iii),(iii) olan üçgendir.

(b) $u^2 + u + 1 \equiv 0 \bmod N$ ise $-u - 1 \equiv u^2 \bmod N$ ve $1 \equiv u(-u-1) \bmod N$ dir. Bu ikisinden $\frac{1}{0} \to \frac{-u}{N} \to \frac{-u-1}{N} \to \frac{1}{0}$ dir. Bu ise $\hat{F}_{u,N}$ da kenar şartları sırasıyla (iv),(iv),(iii) olan üçgendir.■

Örnek 2.5. $\frac{1}{0} \to \frac{3}{7} \to \frac{2}{7} \to \frac{1}{0}$ $\hat{F}_{4,7}$ da $u^2 + u + 1 \equiv 0 \bmod 7$ olan bir üçgendir ve uygun teoremdeki (iv),(iv),(iii) şartlarını sağlar.

$$\left.\begin{array}{ll} 3 \equiv -4 \cdot 1 \bmod 7 & , \quad ry - sx = 7 \\ 2 \equiv -4 \cdot 3 \bmod 7 & , \quad ry - sx = 7 \\ 1 \equiv 4 \cdot 2 \bmod 7 & , \quad ry - sx = -7 \end{array}\right\}$$

Ancak bu $F_{4,7}$ de bir üçgen değildir.

Örnek 2.6. $\frac{1}{13} \to \frac{3}{26} \to \frac{4}{39} \to \frac{1}{13}$ $\hat{F}_{3,13}$ da $u^2 + u + 1 \equiv 0 \bmod 13$ olan bir üçgendir ve uygun teoremdeki (iii),(iv),(iv) şartlarını sağlar.

$$\left.\begin{array}{ll} 3 \equiv 3 \cdot 1 \bmod 13 & , \quad ry - sx = -13 \\ 4 \equiv -3 \cdot 3 \bmod 13 & , \quad ry - sx = 13 \\ 1 \equiv -3 \cdot 4 \bmod 13 & , \quad ry - sx = 13 \end{array}\right\}.$$

$B = \begin{pmatrix} 12 & -1 \\ 13 & -1 \end{pmatrix} \in \hat{\Gamma}_0(13)$ alındığında

$$B\begin{pmatrix} 1 \\ 13 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ B\begin{pmatrix} 3 \\ 26 \end{pmatrix} = \begin{pmatrix} 10 \\ 13 \end{pmatrix},\ B\begin{pmatrix} 4 \\ 39 \end{pmatrix} = \begin{pmatrix} 9 \\ 13 \end{pmatrix}$$

olur. Buna göre $\frac{1}{13} \to \frac{3}{26} \to \frac{4}{39} \to \frac{1}{13}$ üçgeninin B altındaki resmi $\frac{1}{0} \xrightarrow[\text{(iv)}]{} \frac{10}{13} \xrightarrow[\text{(iv)}]{} \frac{9}{13} \xrightarrow[\text{(iii)}]{} \frac{1}{0}$ üçgenidir.

Örnek 2.7. $\frac{2}{7} \to \frac{3}{14} \to \frac{1}{7} \to \frac{2}{7}$ $\hat{F}_{2,7}$ da bir üçgendir fakat $F_{2,7}$ de bir üçgen değildir.

Gerçekten; aksini farzedelim. Yani bu $F_{2,7}$ de bir üçgen olsun. Bu takdirde $\frac{2}{7} \to \frac{3}{14}$ kenarı alındığında $2.14 - 3.7 = 7$ olduğundan $3 \equiv 2.2 \bmod 7$ olur ki bu bir çelişkidir. O halde verilen üçgen $F_{2,7}$ de değildir.

Teorem 2.18. $N > 1$ için $\hat{F}_{u,N}$ ters yönlendirilmiş üçgen ihtiva etmez.

İspat. Kabul edelim ki $\infty \to \frac{u}{N} \leftarrow \frac{r}{N} \to \frac{1}{0}$ ters yönlendirilmiş üçgeni verilmiş olsun. $\hat{F}_{u,N}$, bu üçgeni ihtiva etmez [15].

Şimdi $\hat{F}_{u,N}$, $\infty \to \frac{-u}{N} \leftarrow \frac{r_1}{N} \to \frac{1}{0}$ ters yönlendirilmiş üçgenini ihtiva etsin. Bu takdirde Teorem 2.15' e göre $\frac{-u}{N} \leftarrow \frac{r_1}{N}$ kenarından ya

$$-u \equiv -ur_1 \bmod N \;\Rightarrow\; r_1 \equiv 1 \bmod N \;,\; r_1 + u = 1$$

veya

$$-u \equiv ur_1 \bmod N \;\Rightarrow\; r_1 \equiv -1 \bmod N \;,\; r_1 + u = -1$$

olur. Bu iki durumda da $N > 1$ için $u \equiv 0 \bmod N$ çelişkisi elde edilir. Buna göre $\hat{F}_{u,N}$, ters yönlendirilmiş üçgenini ihtiva etmez.■

Teorem 2.19. $\hat{F}_{u,N}$ kendisiyle eşleşmiş ise buradaki devreye karşılık gelen dönüşüm ya bir yansımadır veya $\hat{\Gamma}_0(N)$ da 2. mertebeden bir eliptik elemandır.

İspat. $\hat{F}_{u,N}$ kendisiyle eşleşmiş olduğundan $u^2 \equiv \pm 1 \bmod N$ dir.

$u^2 \equiv 1 \bmod N$ ise $-u^2 \equiv -1 \bmod N$ dir. Buradan $-u^2 + k_0 N = -1$ olacak şekilde bir $k_0 \in \mathbb{Z}$ vardır. Buradan

$$A := \begin{pmatrix} u & -k_0 \\ N & -u \end{pmatrix} \in \hat{\Gamma}_0(N) \text{ , det } A = \text{-1 ve } u + (-u) = 0$$

olduğundan bu bir yansımadır ve $\frac{1}{0} \to \frac{u}{N} \to \frac{1}{0}$ devresine karşılık gelir.

$u^2 \equiv -1 \bmod N$ ise $-u^2 \equiv 1 \bmod N$ dir. Buna göre $-u^2 + k_1 N = 1$ olacak şekilde bir $k_1 \in \mathbb{Z}$ vardır. Buradan $B := \begin{pmatrix} u & -k_1 \\ N & -u \end{pmatrix} \in \hat{\Gamma}_0(N)$, det B = 1 ve $u + (-u) = 0$ olduğundan bu bir eliptik elemandır ve $B^2 = I$ olup 2. mertebedendir.■

Teorem 2.20. $\hat{\Gamma}_0(N)$ nin 3 mertebeli bir eliptik eleman ihtiva etmesi için gerek ve yeter şart $\forall N \in \mathbb{N}$ için ve bir $u \in U_N$ birimi için $\hat{F}_{u,N}$ nin bir üçgen ihtiva etmesidir

İspat. $''\Rightarrow''$ $\varphi = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$, $ad - bcN = 1$, dönüşümü eliptik olsun. Bu durumda determinanttan $ad \equiv 1 \bmod N$ dir. φ dönüşümü eliptik olduğundan $a + d = \mp 1 \;\Rightarrow\; d = -a \mp 1$ olur. Buna göre

$$a(-a \mp 1) \equiv 1 \bmod N \;\Rightarrow\; a^2 \pm a + 1 \equiv 0 \bmod N$$

bulunur. $(a, N) = 1$ olduğundan $\exists\, u \in U_N : u \equiv a \bmod N$ dir. Böylece $u^2 \pm u + 1 \equiv 0 \bmod N$ elde edilir ki Teorem 2.17'ye göre $\hat{F}_{u,N}$ bir üçgen ihtiva eder.

Determinant -1 ise eliptik eleman yoktur.

$''\Leftarrow''$ $\hat{F}_{u,N}$ bir üçgen ihtiva etsin. $\hat{\Gamma}_0(N)$, $\hat{F}_{u,N}$ nin köşeleri ve kenarlarını transitif olarak permüte ettiğinden bu üçgen ya

$$\frac{1}{0} \to \frac{u}{N} \to \frac{u \pm 1}{N} \to \frac{1}{0} \quad \text{veya} \quad \frac{1}{0} \to \frac{-u}{N} \to \frac{-u \pm 1}{N} \to \frac{1}{0}$$

şeklindedir. Eğer $\frac{1}{0} \to \frac{u}{N} \to \frac{u \pm 1}{N} \to \frac{1}{0}$ üçgeni alınırsa, buna karşılık gelen

$$\varphi_1 = \begin{pmatrix} -u & \dfrac{u^2 \pm u + 1}{N} \\ -N & u \pm 1 \end{pmatrix}$$ 3- mertebeli eliptik elemanı $\hat{\Gamma}_0(N)$ dedir.

$\frac{1}{0} \to \frac{-u}{N} \to \frac{-u \pm 1}{N} \to \frac{1}{0}$ üçgeni alınırsa buna karşılık gelen $\varphi_2 = \begin{pmatrix} -u & -\frac{u^2 \pm u + 1}{N} \\ N & u \pm 1 \end{pmatrix}$ 3-mertebeli eliptik elemanı $\hat{\Gamma}_0(N)$ dir.■

Teorem 2.21. $\frac{a}{b} \to \frac{c}{d} \to \frac{k}{\ell} \to \frac{a}{b}$ $\hat{F}_{u,N}$ da bir üçgen olsun. Bu takdirde $\hat{\Gamma}_0(N)$ da $\mu\left(\frac{a}{b}\right) = \frac{c}{d}$, $\mu\left(\frac{c}{d}\right) = \frac{k}{\ell}$, $\mu\left(\frac{k}{\ell}\right) = \frac{a}{b}$ şartını sağlayan 3- mertebeli bir tek μ eliptik elemanı vardır.

İspat. $\frac{a}{b} \to \frac{c}{d}$ $\hat{F}_{u,N}$ da bir kenar olduğundan Teorem 2.15'e göre $ad - bc = \pm N$ dir ve bir $\phi \in \hat{\Gamma}_0(N)$ için

$$\frac{a_1}{b_1} = \phi\left(\frac{a}{b}\right) \to \phi\left(\frac{c}{d}\right) = \frac{c_1}{d_1} \quad \text{ve} \quad a_1 d_1 - b_1 c_1 = \pm N$$

dir. Teorem 2.16'ya göre bir $\phi \in \hat{\Gamma}_0(N)$ elemanı vardır öyle ki $\phi\left(\frac{a}{b}\right) = \infty$ ve $\phi\left(\frac{c}{d}\right) = \frac{-u}{N}$ dir.

$$\frac{c_1}{d_1} \to \phi\left(\frac{k}{\ell}\right) = \frac{k_1}{\ell_1} \quad \text{ve} \quad c_1\ell_1 - k_1 d_1 = \pm N$$

olduğundan $\frac{k_1}{\ell_1} = \frac{-u \pm 1}{N}$ dir. Yani $\phi \in \hat{\Gamma}_0(N)$ elemanı $\frac{a}{b} \to \frac{c}{d} \to \frac{k}{\ell} \to \frac{a}{b}$ üçgenini $\frac{1}{0} \to \frac{-u}{N} \to \frac{-u \pm 1}{N} \to \frac{1}{0}$ üçgenine resmeder. Buna göre $u^2 \pm u + 1 \equiv 0 \bmod N$ dir ve $\frac{1}{0} \to \frac{-u}{N} \to \frac{-u \pm 1}{N} \to \frac{1}{0}$ üçgenine karşılık gelen $\varphi = \begin{pmatrix} -u & -\frac{u^2 \pm u + 1}{N} \\ N & u \pm 1 \end{pmatrix}$ dönüşümü $\hat{\Gamma}_0(N)$ dadır ve bu 3. mertebeden bir eliptik elemandır. Buna göre $\mu := \phi^{-1}\varphi\phi$ olarak tanımlanırsa μ, $\hat{\Gamma}_0(N)$ da 3- mertebeli bir eliptik elemandır ve istenilen şartları sağlar.■

Sonuç 2.5. N çift ise $\hat{F}_{u,N}$ üçgen ihtiva etmez.

İspat. Kabul edelim ki $\hat{F}_{u,N}$, $\dfrac{a}{bN}\xrightarrow[\text{(iv)}]{}\dfrac{c}{dN}\xrightarrow[\text{(iii)}]{}\dfrac{k}{\ell N}\xrightarrow[\text{(iii)}]{}\dfrac{a}{bN}$ üçgenini ihtiva etsin. Buna göre N çift ve $(a,bN)=1$, $(c,dN)=1$, $(k,\ell N)=1$ olduğundan a, c ve k sırasıyla $(a,N)=1$, $(c,N)=1$ ve $(k,N)=1$ olan tek tamsayılardır.

Kenar şartlarından

$$ad-bc=1\ ,\ c\ell-kd=-1\ ,\ bk-a\ell=-1$$

dir. $ad-bc=1$ in her iki tarafı k ile $c\ell-kd=-1$ in her iki tarafı a ile çarpılır ve taraf tarafa toplanırsa

$$c=k-a$$

elde edilir. a ve k tek olduğundan c nin çift olduğu bulunur ki, bu $(c,N)=1$ olmasıyla çelişir. O halde N çift ise $\hat{F}_{u,N}$ üçgen ihtiva etmez.■

3. İRDELEME

Bu çalışmada amacımız, PSL$(2,\mathbb{R})$ nin bazı ayrık alt gruplarının simgesini elde etmektir. [2], [15] ve [26] da özellikle [15] ve [26] tarafından ortaya atılan altyörüngesel graflardaki devre uzunluklarının, ayrık grupların üretici eliptik elemanlarının mertebeleri ile ilişkisi incelenmiştir. Böylece simge problemi altyörüngesel graflara taşınmıştır.

Literatürde mevcut olan iki yaklaşım

(1) Hurwitz : $\mu(\mathcal{N}or(N)) = 2\pi\left\{2(g-1)+\sum_{i=1}^{r}\left(1-\frac{1}{m_i}\right)+s\right\}$

(2) Shimura : $g_0 - 1 = \frac{1}{2}W(N) + |\,\mathcal{N}or(N) : \Gamma_0(N)\,|(g-1)$

eşitlikleridir. Bu konuda çok sayıda çalışma söz konusudur [8],[13], [20], [24], [25].

Ancak biz bunu farklı bir boyuta taşıdık. Bu da iki eliptik eleman eşlenik ise tanımını verdiğimiz karşılık gelen devrelerin de eşlenik olmasıdır. Bu problemin çözümü genelde henüz elde edilemedi.

Bunun yanında ikinci olarak, $\hat{\Gamma}$ genişletilmiş modüler grup üzerinde çalışılmıştır. Elde edilen sonuçlar, üzerinde çalışılmış diğer gruplardaki neticelerle mukayese edilmiştir.

4. SONUÇLAR

Yaptığımız çalışmada elde edilen başlıca sonuçlar şunlardır.

1) [2] de Akbaş, $\Gamma_0(N)$ de 3-mertebeli bir eliptik elemanın var olması için gerek ve yeter şartı $\forall n \in \mathbb{N}$ için vermiştir. Bu çalışmada Teorem 2.10 da p asal olmak üzere $\Gamma_0(p)$ nin 3 mertebeli iki eliptik elemanı eşlenik ise bunlara karşılık gelen devrelerin eşlenik olduğu bulundu.

2) Teorem 2.11 de devreler eşlenik ise özel durumlarda bunlara karşılık gelen 3. mertebeden eliptik elemanların eşlenik olduğu gösterildi.

3) $\hat{\Gamma}_0(N)$ nin $\hat{\mathbb{Q}}$- daki yörünge sayısı bulundu ve $\Gamma_0(N)$ nin $\hat{\mathbb{Q}}$- daki yörünge sayısı ile olan ilişkisi ortaya konmuştur.(Teorem 2.12, Teorem 2.13 ve Sonuç 2.1)

4) $\hat{\Gamma}$- nın $\hat{\mathbb{Q}}$ üzerindeki hareketinden oluşan alt yörüngesel graflardaki kenar şartı elde edilmiştir (Teorem 2.14).

5) $\hat{\Gamma}$- nın $\hat{\mathbb{Q}}$ üzerindeki hareketinden oluşan alt yörüngesel graflardaki devrelerle ilgili sonuçlar bulunmuştur.

5. ÖNERİLER

1) Teorem 2.11 de verilen durum genel halde çözülebilir.

2) $\hat{\Gamma}$ - nın $\hat{\mathbb{Q}}$ üzerindeki hareketinin neticesinde oluşan alt yörüngesel graflardaki kenar ve devre şartları verilmesine karşın orman (devre içermeyen graf) olma şartı incelenmemiştir. Bu problem araştırılabilir.

3) Alt yörüngesel graflardaki kenar şartı elde edilirken ortaya çıkan kongrüans denklemlerinin sayılar teorisiyle birlikte yorumu yapılmamıştır, araştırılabilir.

6. KAYNAKLAR

1. Akbaş, M., The Normalizer of Modular Subgroups, Ph.D. thesis, University of Southampton,1989.

2. Akbaş, M., On Suborbital Graphs for The Modular Group, Bull. London Math. Soc., 33 (2001) 647-652.

3. Akbaş, M. ve Başkan, T., Suborbital Graphs for The Normalizer of $\Gamma_0(N)$, Tr. J. Of Math., Tübitak, 20 (1996) 379-387.

4. 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.

5. Beardon, A. F., The Geometry of Discrete Groups, Springer Verlag, New York, 1983.

6. Beşenk, M., PSL(2, $\mathbb{R}$) deki $\Gamma_0(N)$ nin $\Gamma_B(N)$ Normalliyeninin Parabolik Sınıf Sayısı, Yüksek Lisans Tezi, Karadeniz Teknik Üniv., Trabzon, 2004.

7. Biggs, N. L. ve White, A. T., Permutation groups and combinatorial structures, London Math. Soc. Lecture Notes 33, Cambridge University Pres, Cambridge,1979.

8. Conway, J. H. ve Norton, S. P., Montrous Moonshine, Bull. London Math. Soc., 11 (1979) 308-339.

9. Değer, A. H., Süreksiz Gruplar ve Graflar, Yüksek Lisans Tezi, Karadeniz Teknik Üniv., Trabzon, 2006.

10. Griess, R. L., The Friendly Giant, Invent. Math. 69 (1982) 1–102.

11. Güler, B.Ö., $\Gamma_0(N)$ Kongrüans Alt Grubunun $PSL_2(\mathbb{R})$ deki Normalliyeninin Alt yörüngesel Grafları, Doktora Tezi, Karadeniz Teknik Üniv., Trabzon, 2006.

12. Hardy, G. H. ve Wright, E. M., An Introduction to The Theory of Numbers, Oxford University Press, Oxford, 1979.

13. Helling, H., On the commensurability class of rational modular group, London Math. Soc., 2 (1970) 67-72.

14. Jones, G. A. ve Singerman, D., Complex Functions : An Algebraic and Geometric Viewpoint, Cambridge University Press, Cambridge, 1987.

15. Jones , G. A., Singerman, D. ve Wicks, K., The Modular Group and Generalized Farey Graphs, London Math. Soc. Lecture Notes, CUP, Cambridge, 160 (1991) 316–318.

16. Kulkarni, R. S., An Arithmetic-Geometric Method in The Study of The Subgroups of The Modular Group, American Journal of Mathematics, 113 (1991) 1053-1133.

17. Lehner, J. ve Newman, M., Weierstrass points of $\Gamma_0(N)$, Annals of Mathematics Vol. 79, No.2, March, (1964) 360–368.

18. Maclachlan, C., Groups of Units of Zero Ternary Quadratic Forms, Proceedings of the Royal Society of Edinburg, 88 (1981) 141-157.

19. Newman, M., The Normalizer of Certain Modular Subgroups, Can. J. Math, 8 (1956) 29-31.

20. Ogg, A. P., Automorphismes des Courbes Modulaires, Seminaire Delange-Pisot, Poitou, 7, 1974.

21. Ogg, A. P., Modular functions, Proceedings of Symposia in Pure Mathematics, Vol. 37, 1980.

22. Pizer, A., A Note on a Conjecture of Hecke, Pasific J. Math. Vol. 79, 2 (1978) 541–548.

23. Rose, H. E., A Course in Number Theory, Oxford University Press, Oxford, 1988.

24. Schoeneberg, B., Elliptic Modular Functions, Springer Verlag, Berlin, 1974.

25. Shimura, G., Inroduction to The Arithmetic Theory of Automorphic Functions. Princeton Univ. Press, 1971.

26. Sims, C. C., Graphs and Finite Permutation Groups, Math. Z., 95 (1967) 76-86.

27. Singerman, D., Subgroups of Fuchsian Groups and Finite Permutation Groups, Bull. London Math. Soc. 2 (1970) 319–323.

28. Tsuzuku, T., Finite Groups and Finite Geometries, Cambridge University Pres, Cambridge,1982.

ÖZGEÇMİŞ

Serkan KADER, 1977 yılında Çankırı'da doğdu. İlk, orta ve lise öğrenimini Ankara'da tamamladı. 1995 yılında Niğde Üniversitesi Fen-Edebiyat Fakültesi Matematik bölümünü kazandı ve 1999 yılında aynı bölümden mezun oldu.

Aynı yıl Niğde Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü, Analiz ve Fonksiyonlar Teorisi Anabilim Dalında Araştırma Görevlisi olarak göreve başladı. 2002 yılında Niğde Üniversitesi Fen Bilimleri Enstitüsü'nden Yüksek Lisans (Matematik) derecesini aldı. Y.Ö.K. kanunun 35/b maddesi gereğince Eylül 2002 de Karadeniz Teknik Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde doktora programına başladı. Halen K.T.Ü. Fen Edebiyat Fakültesi Matematik Bölümünde Araştırma Görevlisi olarak görev yapmaktadır. İleri seviyede İngilizce bilmektedir.