KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

$\Gamma_0(N)$ KONGRÜANS ALT GRUBUNUN $PSL_2(\mathbb{R})$ DEKİ NORMALLİYENİNİN ALT YÖRÜNGESEL GRAFLARI

DOKTORA TEZİ

Bahadır Özgür GÜLER

EYLÜL 2006
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

$\Gamma_0(N)$ KONGRÜANS ALT GRUBUNUN $PSL_2(\mathbb{R})$ DEKİ NORMALLİYENİNİN ALT YÖRÜNGESEL GRAFLARI

Bahadır Özgür GÜLER

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"Doktor"
Ünvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 26. 06. 2006
Tezin Savunma Tarihi : 04. 09. 2006

Tez Danışmanı : Prof. Dr. Mehmet AKBAŞ
Jüri Üyesi : Prof. Dr. Sabahattin BALCI
Jüri Üyesi : Prof. Dr. Abdullah ÇAVUŞ
Jüri Üyesi : Prof. Dr. Hilmi ZENGİN
Jüri Üyesi : Yrd. Doç. Dr. Sema DİKMENOĞLU

Enstitü Müdürü : Emin Zeki BAŞKENT

Trabzon 2006

ÖNSÖZ

Bu çalışmada, $\mathscr{N}or$(N) nin 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 aşamasında bizi sabırla dinleyen, tavsiye ve eleştirileriyle tezin şekillenmesinde emeği geçen sayın hocam Prof. Dr. Abdullah ÇAVUŞ a şükranlarımı sunarım.

Literatür araştırması sırasında yönlendirme ve desteğinden ötürü Dr. Süleyman UZUN a teşekkür ederim.

Ayrıca yetişmemde emeği geçen KTÜ Matematik bölümünün değerli tüm hocalarına, çalışmalarımı daha iyi yürütebilmem için gerekli esnekliği sağlayan KTÜ Rize Fen-Edebiyat Fakültesi dekanı Prof. Dr. Nazmi Turan OKUMUŞOĞLU na, çalışma süresi boyunca moral desteklerinden ötürü başta Arş. Gör. Yavuz KESİCİOĞLU ve Arş. Gör. Serkan KADER olmak üzere, Arş. Gör. Ümit TERZİOĞLU, Neslihan BAYRAM, Arş. Gör. İshak CUMHUR, Murat BEŞENK, KTÜ Rize Fen-Edebiyat Fakültesindeki tüm asistan arkadaşlarıma ve hayatım boyunca desteklerini hiç esirgemeyen sevgili aileme çok teşekkür ederim.

Bahadır Özgür GÜLER

Trabzon, 2006

İÇİNDEKİLER

ÖZET

$\Gamma_0(N)$ Kongrüans Alt Grubunun $Psl_2(\mathbb{R})$ deki Normalliyeninin Alt Yörüngesel Grafları

Bahadır Özgür GÜLER

Bu çalışmada, esas amacımız alt yörüngesel graflar üzerinde yaptığımız çalışmaların $\mathcal{N}or(N)$ nin simgesindeki invaryantların bulunmasına yardımcı olacağı düşüncesidir.

Bölüm 1'de $PSL_2(\mathbb{R})$, Γ-Modüler grubu ve $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$-Kongrüans alt gruplarının bazı özellikleri verildi. Ayrıca bazı kongrüans alt gruplarının normalliyenleri ve ayrık gruplar, Riemann yüzeyleri, temel bölgeler, graf teori, imprimitif hareket ile ilgili ihtiyaç duyduğumuz temel tanımlar verildi.

Bölüm 2'de $\mathcal{N}or(N)$ nin yapısını daha iyi anlamak için bazı önemli alt gruplarından ve periyotlarından bahsedildi. Son olarak $\mathcal{N}or(N)$ nin alt yörüngesel grafları elde edildi.

Anahtar Kelimeler : $PSL_2(\mathbb{R})$, Γ, $\Gamma_0(N)$, $\mathcal{N}or(N)$, Transitif Permütasyon Grubu, Alt Yörüngesel Graf

SUMMARY

Suborbital Graphs for the normalizer of $\Gamma_0(N)$ in $PSL_2(\mathbb{R})$

Bahadır Özgür GÜLER

In this thesis, the main thinking is that our attempts on suborbitals might help to find invariants of the signature of the normalizer $\mathcal{N}or(N)$.

In Chapter 1, we give some of the properties of $PSL_2(\mathbb{R})$, Γ-Modular group, $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$-Congruence Subgroups. We also give the normalizer of some congruence subgroups and the preliminary definitions we require for discrete groups, Riemann surfaces, fundamental domains, graph theory and imprimitive action.

In Chapter 2, some important subgroups and periods of $\mathcal{N}or(N)$ which enable us to understand its structure are described. Finally we obtain the suborbital graphs of $\mathcal{N}or(N)$.

Key Words : $PSL_2(\mathbb{R})$, Γ, $\Gamma_0(N)$, $\mathcal{N}or(N)$, Transitive Permutation Group, Suborbital Graph

ŞEKİLLER DİZİNİ

SEMBOLLER DİZİNİ

$\mathbb{C}$	Kompleks sayılar kümesi
$\hat{\mathbb{C}}$	Genişletilmiş kompleks sayılar kümesi
φ(a)	Euler fonksiyonu
Γ	Modüler grup
$\Gamma_0(N)$	Γ nın $N\|c$ olan bir alt grubu
$\mathbb{N}$	Doğal sayılar kümesi
$\mathcal{N}or$(N)	$\Gamma_0(N)$ nin $PSL_2(\mathbb{R})$ deki normalliyeni
$\mathrm{PSL}_2(\mathbb{R})$	Gerçel katsayılı, lineer, kesir dönüşümlerinin grubu
$\mathbb{P}$	Asal sayılar kümesi
$\mathbb{R}$	Reel sayılar kümesi
$\hat{\mathbb{R}}$	Genişletilmiş reel sayılar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\hat{\mathbb{Q}}$	Genişletilmiş rasyonel sayılar kümesi
$\mathcal{U}$	$\mathbb{C}$ de üst yarı düzlem
$\mathbb{Z}$	Tam sayılar kümesi
A⊂B	A kümesi B kümesinin alt kümesidir
A ≤ B	A grubu B grubunun alt grubudur
A⊲B	A grubu B grubunun normal alt grubudur
$\|A:B\|$	B alt grubunun A daki indeksi
$a\|b$	*a* sayısı *b* sayısını böler
$a\nmid b$	*a* sayısı *b* sayısını bölmez
$a\\|b$	*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

1. GENEL BİLGİLER

1.1. Giriş

Tanım 1. G bir grup ve aynı zamanda bir topolojik uzay olsun.

i) $F: \underset{(x,y)}{G\times G} \underset{\to}{\to} \underset{xy}{G}$

ii) $f: \underset{x}{G} \underset{\to}{\to} \underset{x^{-1}}{G}$

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

Tanım 2. G bir grup ve X≠∅ bir küme olsun. Aşağıdaki şartları sağlayan bir $\varphi: G\times X \to X$ fonksiyonu varsa G ye X üzerinde *hareket ediyor*(*act on*) denir,

i) $\forall g_1, g_2 \in G$ ve $\forall x \in X$ için $\varphi(g_1 g_2, x) = \varphi(g_1, \varphi(g_2, x))$

ii) $1\in G$ birim eleman ise $\forall x\in X$ için $\varphi(1, x) = x$

Burada G bir topolojik grup, X bir topolojik uzay ve φ dönüşümü sürekli ise $[G, X]$ çiftine bir topolojik dönüşüm grubu denir.

Önerme 1. G, X üzerinde hareket etsin. " $x \approx y :\Leftrightarrow gx = y$ olacak biçiminde bir $g\in G$ elemanı vardır" X üzerinde bir denklik(eşdeğerlik) bağıntısıdır.

Tanım 3. " $\approx$ " bağıntısının eşdeğerlik sınıflarına hareketin *yörünge*leri denir. Ayrıca $x\in X$ noktasını içeren yörünge x in yörüngesi denir ve bu Gx ile gösterilir. Bu tanıma göre $Gx = \{gx \mid g\in G\}$ dir. $x \approx y$ olduğunda Gx ve Gy yörüngelerine *eşleniktir* denir.

Tanım 4. G, X üzerinde hareket etsin ve $x,y\in X$ keyfi olsun. gx=y olacak biçiminde bir $g\in G$ elemanı varsa G ye X üzerinde *transitif* olarak hareket eder. Bu tanıma göre hareket transitif ise $\forall x \in X$ için Gx=X elde edilir. Yani bir tek yörünge vardır.

Önerme 2. $[G, X]$ bir topolojik dönüşüm grubu τ, X üzerindeki topoloji ve $P: \underset{x}{X} \underset{\to}{\to} \underset{Gx}{X/G}$

olsun. Bu takdirde $\tau_G := \{A \subset X/G \mid P^{-1}(A) \in \tau\}$ ailesi X/G üzerinde P yi sürekli yapan en ince topolojidir.

Genel olarak X/G bölüm uzayına *yörünge uzayı* adı verilir.

Tanım 5. G, X üzerinde hareket etsin ve $x \in X$ olsun. $G_x := \{g \in G \mid gx = x\}$ alt grubuna x in G deki sabitleyeni(*stabiliser*) denir.

Tanım 6. G bir grup olsun. $H = \{g \in G \mid \forall x \in G, gx = xg\}$ kümesine G nin *merkez*i denir.

Tanım 7. G bir grup olsun. $G = \langle a \rangle$ olacak şekilde bir $a \in G$ varsa G ye bir devirli(*cyclic*) grup denir.

Tanım 8. G bir grup ve $H < G$ olsun. $\mathcal{N}_G(H) := \{g \in G \mid gHg^{-1} = H\}$ kümesine H nın G deki normalliyeni(*normalizer*) denir. Normalliyen H yı normal alt grup olarak içeren en büyük kümedir.

Tanım 9. $N \in \mathbb{Z}$ olmak üzere, $p^2 \mid N$ olacak şekilde bir $p \in \mathbb{P}$ yoksa N ye karesiz (*square-free*) denir.

Tanım 10. Bir T-dönüşümünün periyodu (veya mertebesi(*order*)), $T^m = I$ eşitliğini sağlayan en küçük pozitif tamsayıdır. Böyle bir m-tamsayısı yoksa T *sonsuz* periyotludur.

Tanım 11. $N \in \mathbb{Z}$ için $1 \leq a \leq N$ ve (a,N)=1 olan a tamsayılarının sayısı $\varphi(N)$ ile gösterilir ve bu fonksiyona *Euler fonksiyonu* denir. $m = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ ise

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right) \text{ dir.}$$

1.2. $PSL_2(\mathbb{R})$ Grubu

$SL_2(\mathbb{R})$ ile katsayıları reel ve determinantı 1 olan 2×2 tipindeki matrislerin grubunu

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, \ ad - bc = 1 \right\}$$

gösterelim. $SL_2(\mathbb{R})$ nin kendi merkezi $\{\pm I\}$ ile bölümünden

$$PSL_2(\mathbb{R}) = SL_2(\mathbb{R}) / \{\pm I\}$$

grubu elde edilir. Burada

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ ve } \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

elemanları özdeş olarak aynı kabul edilir ve aynı elemanla temsil edilir.

$PSL_2(\mathbb{R})$ grubu $\mathcal{U} = \{ z \in \mathbb{C} : \mathrm{Im}(z) > 0 \}$ üst-yarı düzlemi üzerinde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \to \frac{az + b}{cz + d}$$

ile hareket eder. $\mathcal{U}$ üzerinde ds-metriği (hiperbolik uzunluk)

$$ds^2 = \frac{dx^2 + dy^2}{y^2} = \frac{|dz|^2}{y^2}, \quad (z = x + iy)$$

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

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

dir. Böylelikle $\mathcal{U}$ hiperbolik geometri için uygun bir model olurken, $PSL_2(\mathbb{R})$ de onun konform otomorfizmalarının grubuna tam olarak karşılık gelir. $\mathcal{U}$ nun $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ daki sınırı $\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ dir ve $PSL_2(\mathbb{R})$ onun üzerinde de tıpkı $\mathcal{U}$ daki gibi hareket eder (Jones ve Singerman, 1987, sf. 221–225).

$PSL_2(\mathbb{R})$'nin elemanlarının klasik sınıflandırılması sabit nokta kümelerine göre yapılır. Buna göre $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ biçimindeki bir eleman iz (*trace*)'ine göre

$$|a+d| = 2 \text{ ise parabolik}$$

$$|a+d| > 2 \text{ ise hiperbolik}$$

$$|a+d| < 2 \text{ ise eliptik}$$

şeklinde sınıflandırılır.

Buna göre bir parabolik eleman $\mathcal{U}$ nun sınırı üzerindeki bir sabit noktayla, bir hiperbolik eleman $\mathcal{U}$ nun sınırı üzerindeki iki sabit noktayla ve bir eliptik eleman $\mathcal{U}$ daki bir sabit noktayla hareket eder.

G, $PSL_2(\mathbb{R})$ nin bir alt grubu olsun. G'nin bir parabolik elemanının $\mathcal{U}$ nun sınırında sabit bıraktığı noktaya G'nin bir *parabolik noktası* veya *cusp*'ı denir. G'nin parabolik noktalarının kümesine G'nin *cusp kümesi* denir. G'nin cusp kümesindeki keyfi x_1, x_2 için $gx_1 = x_2 : g \in G$ olacak şekilde bir eleman bulunamıyorsa bu noktalara G-eşdeğersiz denir. G'nin G-eşdeğersiz noktalarının sayısına G'nin *parabolik sınıf sayısı* denir.

1.3. Modüler Grup

$PSL_2(\mathbb{R})$ nin üzerinde en çok çalışılan alt grubu olan Modüler grup,

$$\Gamma = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) \big/ \{\pm I\} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{R}) : a, b, c, d \in \mathbb{Z} \right\}$$

ile tanımlanır. Şimdi $PSL_2(\mathbb{R})$ nin aşağıdaki elemanlarını göz önüne alalım;

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad Z = XY = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

X 2-mertebeli bir eliptik eleman, Y 3-mertebeli bir eliptik eleman ve Z bir parabolik elemandır. Γ, X ile Z ve X ile Y =XZ tarafından üretilir. Modüler grubu üçgen grupların bir üyesi olarak ele almakta mümkündür. Bir üçgen grup (l, m, n) ile gösterilir, burada l, m, n $\in \mathbb{Z}$ veya ∞ dur, ve

$$\left\{x, y, z : x^{l} = y^{m} = z^{n} = xyz = 1\right\}$$

bağıntısına sahiptir. Geometrik bir yorum için, bir X uzayında $\frac{\pi}{l}, \frac{\pi}{m}, \frac{\pi}{n}$ açılı bir T-üçgeni göz önüne alınmalıdır, burada X küre, Euclid düzlemi ya da hiperbolik düzlemdir. Bu durumda *T* nin kenarlarında X in yansımaları tarafından üretilen grup 2-indeksli bir alt gruba sahiptir ve (l, m, n)'ye izomorf konform dönüşümlerden meydana gelir. X uzayı l, m, n tamsayıları tarafından belirlenir ve

$$\frac{1}{l} + \frac{1}{m} + \frac{1}{n} > 1 \text{ ise Küre,}$$

$$\frac{1}{l} + \frac{1}{m} + \frac{1}{n} = 1 \text{ ise Euclid Düzlemi,}$$

$$\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1 \text{ ise Hiperbolik Düzlemdir}$$

(Jones ve Singerman, 1987, sf. 238–239).

Γ yı bir üçgen grup olarak ele alırsak,

$$\Gamma \simeq (2, 3, \infty)$$

izomorfizması elde edilir. Γ nın cusp kümesi $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ ve Γ bunun üzerinde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \frac{x}{y} \to \frac{a\frac{x}{y} + b}{c\frac{x}{y} + d} = \frac{ax + by}{cx + dy} \quad , \quad \frac{x}{y} \in \hat{\mathbb{Q}}$$

ile hareket eder. Bir başka gösterimle $\frac{x}{y} : (x, y) = 1$ indirgenmiş formu alındığında $SL_2(\mathbb{Z})$ 2×1'lik bir vektör üzerinde

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

ile hareket eder. Eğer (x, y)=1 ve ad−bc=1 ise $\frac{ax + by}{cx + dy}$ indirgenmiş formdadır.

Aksini varsayalım; $\frac{ax + by}{cx + dy}$ indirgenmiş formda olmasın. Buna göre

$$\exists n \in \mathbb{Z} \text{ ö.k. } n \mid ax+by \text{ ve } n \mid cx+dy.$$

Bu durumda $\exists$ k, $l \in \mathbb{Z}$ $ax+by=kn$ (1) ve $cx+dy=ln$ (2). (1) eşitliğinin her iki tarafı d ile (2) de –b ile çarpıldığında

$$(ad-bc)x=(kd-bl)n\ldots(\mathrm{I})$$

benzer şekilde (1) –c ve (2) a ile çarpıldığında

$$(ad-bc)y=(al-ck)n\ldots(\mathrm{II})$$

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

1.4. Ayrık Gruplar ve Riemann Yüzeyleri

$PSL_2(\mathbb{R})$ nin $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$-elemanını $\mathbb{R}^4$ ün (a,b,c,d) öyle ki $ad-bc=1$-elemanı ile tanımladığımızda $PSL_2(\mathbb{R})$ nin bir topolojik-grup yapısına sahip olduğu görülür. Bu uzayda bir $\Lambda \subset PSL_2(\mathbb{R})$ alt grubunun ayrık olması için gerek ve yeter şart I-birim matrisinin bir U-komşuluğu vardır öyle ki $U \cap \Lambda = \{I\}$ olmasıdır. $PSL_2(\mathbb{R})$ nin bir ayrık alt grubuna aynı zamanda *Fuchsian grup* adı verilir. 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)

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

Simge : (g ; $m_1, \ldots, m_r$; s)

burada *g*-grubun cinsini, m_i-eliptik elemanların mertebelerini ve s-parabolik sınıf sayısını temsil etmektedir. Simge, üzerinde çalışılan grubun invaryantlarını ortaya koyması bakımından son derece önemlidir (Beardon, 1983, sf. 268).

Γ bir Fuchsian gruptur ve simgesi

$$(0; 2,3 ; 1)$$

biçimindedir. Ayrıca bir ayrık grubun tüm alt grupları da ayrık olduğundan Γ'nın bütün alt grupları Fuchsian'dır.

Teorem 1. Λ bir sonlu üretilmiş Fuchsian grubu ve Λ_0, Λ nın M< ∞ indeksli bir normal alt grubu olsun. Bu durumda,

$$\text{Parabolik Sınıf Sayısı} = M\sum_{i=1}^{s} 1/r_i \quad , \quad r_i = e^{p_i \,(\mathrm{mod}\, \Lambda_0)}$$

$$\text{Eliptik Sınıf Sayısı} = M\sum_{i\in\Omega} 1/t_i \quad , \quad t_i = e^{x_i \,(\mathrm{mod}\, \Lambda_0)}, \quad \Omega = \{ i \mid 1 \le i \le n,\ t_i < m_i \}$$

(Akbaş, 1989, sf.56).

Riemann Yüzeyi. X bir bağlantılı, Hausdorff topolojik uzayı olsun. Bir $U \subset X$ açık alt kümesi ve bir $z : U \to V \subset \mathbb{C}$ homoemorfizmasından meydana gelen bir (U,z) çiftine X in bir *koordinat komşuluğu* denir. (U_1, z_1) ve (U_2, z_2) koordinat komşulukları uyumlu (*compatible*) denir; eğer

$$z_1 \circ z_2^{-1} : z_2(U_1 \cap U_2) \to z_1(U_1 \cap U_2)$$

fonksiyonu holomorfik ise. Koordinat komşuluklarının bir $(U_i,z_i)_{i\in I}$ ailesine,

(i) $X = \cup(U_i)$

(ii) $\forall (i,j) \in I \times I$ için (U_i,z_i) ile (U_j,z_j) uyumludur,

koşullarının sağlanması halinde bir koordinat örtüm(*coordinate covering*) denir. İki örtümün birleşimlerinin de bir örtüm meydana getirmesi halinde bu örtümler eşdeğerdir denir. Bu örtümlerin kümesi üzerinde bir eşdeğerlik bağıntısı tanımlar ve eşdeğerlik sınıfına da bir *kompleks yapı* adı verilir.

Tanım 12. Bir bağlantılı, Hausdorff topolojik uzayına bir kompleks yapıyla birlikte bir Riemann yüzeyi adı verilir.

$\mathbb{R}^2$ deki açık kümelere homeomorf kümelerle oluşturulmuş bir açık örtümü mevcut 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 $\mathcal{U} \to \mathcal{U}/\Lambda$ izdüşümü dallanmıştır. Ancak oluşan yüzey kompakt değildir, bunu sağlamak için $\mathcal{U}$ yerine $\mathcal{U} \cup \{\infty\}$ alınır (Jones ve Singerman, 1987, sf. 249–250).

.

Teorem 2. Her basit bağlantılı Riemann yüzeyi aşağıdakilerden birine konform eşdeğerdir:

(i) Σ-Riemann Küresi

(ii) $\mathbb{C}$-Kompleks Düzlem

(iii) $\mathcal{U}$-Üst Yarı Düzlem

(Jones ve Singerman, 1987, sf. 200).

.

Bu Riemann yüzeylerinin otomorfizm grupları aşağıdaki gibidir;

Teorem 3. **(i)** Aut(Σ)=$PSL_2(\mathbb{C})$

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

(iii) Aut($\mathcal{U}$)=$PSL_2(\mathbb{R}$

(Jones ve Singerman, 1987, sf. 232).

Teorem 4. $\mathcal{U}/\Lambda$ kompakt ise Λ parabolik eleman içermez (Jones ve Singerman, 1987, sf. 254).

1.5. Modüler Grubun Kongrüans Alt Grupları

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

Keyfi $N\in\mathbb{Z}$ için Γ nın temel kongrüans alt grubu

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

ile tanımlanır. Γ'nın $\Gamma(N)$-temel kongrüans alt grubunu içeren herhangi bir alt grubuna *kongrüans alt grubu* denir. Üzerinde çalışılan bazı kongrüans alt grupları;

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

$$\Gamma_0(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : c\equiv 0 \ (\text{mod } N)\right\}$$

$$\Gamma^0(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : b\equiv 0 \ (\text{mod } N)\right\}.$$

Bunlar arasındaki ilişkiyi keyfi $N\in\mathbb{Z}$ için

$$\Gamma(N)\leq\Gamma_1(N)\leq\Gamma_0(N)\leq\Gamma$$

biçimindedir.

Ayrıca $\Gamma(N)\lhd\Gamma$ dır, 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

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

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

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

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

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

$$\left|\Gamma_1(N):\Gamma(N)\right| = \frac{\left|\Gamma:\Gamma(N)\right|}{\left|\Gamma:\Gamma_1(N)\right|} = N$$

$\Gamma_0(N)$, $\Gamma_1(N)$ ve $\Gamma(N)$'nin de cusp kümesi $\hat{\mathbb{Q}}$'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 (Schoeneberg, 1974, sf.78–79).

1.6. Bazı Kongrüans Alt Gruplarının Normalliyenleri

Teorem 5. $\Gamma(N)$'nin $PSL_2(\mathbb{R})$ deki normalliyeni Γ'dır.

İspat. $\aleph$, $\Gamma(N)$'nin $PSL_2(\mathbb{R})$ deki normalliyeni olsun.

$$\Gamma(N) \lhd \Gamma < PSL_2(\mathbb{R})$$

olduğundan, $\Gamma \leq \aleph$. Ancak $\aleph$, $PSL_2(\mathbb{R})$ de döngüsel-olmayan bir Fuchsian grubunun normalliyenidir, dolayısıyla o da Fuchsian'dır. Fuchsian gruplarının sonlu indekse sahip tüm alt gruplarının bir sınıflandırmasını bulabiliriz, buradan Γ nın herhangi bir Fuchsian grubunun sonlu indeksli bir alt grubuna karşılık gelmediği görülür. Diğer taraftan Γ yı sonsuz-indeksli bir alt grup olarak içeren hiçbir G-Fuchsian grubu yoktur, aksi halde G nin herhangi bir temel bölgesinin alanı 0 olurdu. Sonuç olarak $\Gamma \leq \aleph$ olamaz, $\Gamma = \aleph$ elde edilir.

Teorem 6. $\Gamma_1(N)$'nin $PSL_2(\mathbb{Z})$ deki normalliyeni $\begin{cases}\Gamma_0(N), & N \neq 4 \text{ için}\\ \Gamma_0(2), & N = 4 \text{ için}\end{cases}$ dir.

İspat. $\Gamma_1(N)$'nin $PSL_2(\mathbb{Z})$ deki normalliyeni $\aleph$ olsun. $\Gamma_1(N) \lhd \Gamma_0(N)$ olduğundan $\Gamma_0(N) \subset \aleph$. Tersini gösterelim;

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \aleph \quad ve \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$$

alalım. Buradan,

$$A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} A^{-1} \in \Gamma_1(N)$$

ve daha açık yazıldığında,

$$\begin{pmatrix} ad - ac - bc & * \\ cd - c^2 - cd & -bc + ac + ad \end{pmatrix} \in \Gamma_1(N)$$

böylece,

$$\begin{pmatrix} 1 - ac & * \\ -c^2 & 1 + ac \end{pmatrix} \in \Gamma_1(N)$$

buna göre,

$$-c^2 \equiv 0 (\bmod N) \text{ ve } 1 - ac \equiv 1 + ac \equiv 1 (\bmod N) \text{ ya da}$$

$$-c^2 \equiv 0 (\bmod N) \text{ ve } 1 - ac \equiv 1 + ac \equiv -1 (\bmod N)$$

Birinci durumda $-c^2 \equiv 0 (\bmod N)$ ve $ac \equiv 0 (\bmod N)$ kongrüanslarından $N \mid c^2$ ve $N \mid ac$. Eğer $(a,N)=1$ olduğunu gösterirsek, $N \mid ac$ olduğundan $N \mid c$, dolayısıyla aradığımız neticeyi $A \in \Gamma_0(N)$ 'yi elde etmiş oluruz. Şüphesiz $(a,N) \neq 1$ ise $\exists\, p \in \mathbb{P}$ öyle ki $p \mid a$ ve $p \mid N$. $N \mid c^2$ olduğundan $p \mid c^2$ ve p-asal olduğundan $p \mid c$. Ancak $p \mid a$ ve $p \mid c$ olması çelişkidir, çünkü $(a, c)=1$.

İkinci durumda $1 - ac \equiv -1 (\bmod N)$ ve $1 + ac \equiv -1 (\bmod N)$ denklemlerinden $2 \equiv -2 (\bmod N)$ elde edilir. Böylece $N \mid 4$ yani $N=1, 2$, veya 4. Bu durumlarda $\Gamma_1(N) = \Gamma_0(N)$, dolayısıyla normalliyenlerin sırasıyla $\Gamma_0(1)$, $\Gamma_0(2)$ ve $\Gamma_0(4)$'e karşılık geldiği görülür.

Teorem 7. $\Gamma_0(N)$'nin $PSL_2(\mathbb{R})$ deki normalliyeni

$$\mathcal{N}\boldsymbol{or}(\mathbf{N}) = \left\{ \begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix} : \det = e > 0 \right\}$$

ile tanımlanır. 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" demek $\left(r, s/r\right) = 1$ anlamındadır.

Öncelikle $\Gamma_0(N)$ nin PSL2(ℤ) deki $\mathcal{N}or_{PSL_2(\mathbb{Z})}(N)$ -normalliyeninin nasıl elde edildiğini göstereceğiz.

Lemma 1. $N=\sigma^2 q \geq 1$ ve q -karesiz olsun. Bu durumda σ nın $\mathcal{N}or_{PSL_2(\mathbb{Z})}(N) = \Gamma_0(N/\Delta_1)$ eşitliğini sağlayan bir Δ_1 böleni mevcuttur.

Lemma 2. Her $A=\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ ve σ için $\varepsilon | (d\text{-}a)$ koşulunu sağlayan bir ε-böleni mevcut olsun. Bu durumda $\varepsilon | \Delta_1$ dir.

Newman yaptığı ispatlarla $\Delta_1 = h$ olduğunu gösterdi ve ayrıca yukarıdaki lemmaları kullanarak Teorem 4 ün ispatını da yapmıştır.

Teorem 8: $N=2^{\alpha} 3^{\beta} N_0 \geq 1$, $(N_0, 6) = 1$ ve $u=\min\left(3, \left[\frac{\alpha}{2}\right]\right)$, $v=\min\left(1, \left[\frac{\beta}{2}\right]\right)$ ve ayrıca [x], küçük veya eşit x olan en büyük tam sayı olmak üzere $\mathcal{N}or_{PSL_2(\mathbb{Z})}(N) = \Gamma_0\left(\frac{N}{2^u 3^v}\right)$ dir (Lehner ve Newman, 1964).

Teorem 7 nin ispatı : M -normalliyeninin keyfi bir elemanı olsun ve matris gösterimi olarak da $M=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL_2(\mathbb{R})$ alalım. Bu takdirde

$$M\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} M^{-1} = \begin{pmatrix} 1-\alpha\gamma & \alpha^2 \\ -\gamma^2 & 1+\alpha\gamma \end{pmatrix} \in \Gamma_0(N) \qquad (1)$$

$$M\begin{pmatrix}1 & 1\\ N & 1\end{pmatrix}M^{-1}=\begin{pmatrix}1+N\beta\delta & -N\beta^2\\ N\delta^2 & 1-N\beta\delta\end{pmatrix}\in\Gamma_0(N) \qquad (2)$$

(1) ve (2) den $\alpha=\sqrt{u}t_1$, $\beta=\sqrt{\frac{a}{b}}\frac{l_1}{k}$, $\xi=\sqrt{g}t_2$, $\gamma=\sqrt{s}l_2$ burada $u, t_1, a, b, l_1, k, g, t_2, s, l_2$ hepsi birer tam sayı; $(a,b)=(a,k)=(b,l_1)=1$ ve u, s, g, a, b karesizdir. (2) de $N\beta^2$ bir tam sayıdır, bu yüzden

$$bk|N \qquad (3)$$

elde edilir. $\alpha\gamma$ bir tam sayı olduğundan u=s ve $\beta\xi$ bir rasyonel sayı olduğundan $\sqrt{g\frac{a}{b}}$ bir rasyonel sayıdır, bu ise g=ab eşitliğini verir, çünkü g, a, b karesizdir. Bu yüzden

$$M=\begin{pmatrix}\sqrt{u}t_1 & \sqrt{\frac{a}{b}}\frac{l_1}{k}\\ \sqrt{u}l_2 & \sqrt{ab}t_2\end{pmatrix}$$

$$\det M=\sqrt{uab}t_1t_2-\sqrt{u\frac{a}{b}}\frac{l_1}{k}l_2=1 \qquad (4)$$

dolayısıyla buradan $$k\sqrt{ab}t_1t_2-\sqrt{u\frac{a}{b}}l_1l_2=k$$

$$k^2uat_1^2t_2^2+u\frac{a}{b}l_1^2l_2^2-2kl_1l_2t_1t_2ua=k^2$$

Bu $u\frac{a}{b}l_1^2l_2^2$ nin bir tam sayı olması gerektiğini söyler ancak $(a,b)=(a,k)=1$ olduğundan a=1 olmak zorundadır.

(4) kullanıldığında

$$\sqrt{ub}t_1t_2-\sqrt{\frac{u}{b}}\frac{l_1}{k}l_2=1$$

elde ederiz. Böylece

$$b\sqrt{u}t_1t_2-\sqrt{u}\frac{l_1}{k}l_2=\sqrt{b}$$

$$\sqrt{u}\left(bt_1t_2-\frac{l_1}{k}l_2\right)=\sqrt{b}$$

dolayısıyla $\sqrt{\frac{u}{b}}=\dfrac{1}{bt_1t_2-\frac{l_1l_2}{k}}$ bir rasyonel sayıdır. u ve b karesiz olduğundan u=b eşitliği elde edilir. Buna göre

$$M=\begin{pmatrix} \sqrt{u}t_1 & \dfrac{l_1}{k\sqrt{u}} \\ \sqrt{u}l_2 & \sqrt{u}t_2 \end{pmatrix} \tag{5}$$

u=b olduğundan (3) den $N\equiv 0\left(\mathrm{mod}\ uk^2\right)$ dir. Öyleyse q karesiz olmak üzere $N=\sigma^2 q$ dur. $\sigma^2 q\equiv 0\left(\mathrm{mod}\ uk^2\right)$ ve σ^2, N yi bölen en büyük karesiz olduğundan $k^2|\sigma^2$, buradan $k|\sigma$ dır.

$ul_2^{\ 2}$, $\sigma^2 q$ ile bölünebilir olduğundan $\sigma^2 \mid l_2^{\ 2}$ dolayısıyla $\sigma \mid l_2$ dir. Buna göre z bir tam sayı olmak üzere $l_2=\sigma z$ dir. Şimdi $k|\sigma$ olduğundan

$$\left(\frac{\sigma}{k}\right)^2 q\equiv 0\left(\mathrm{mod}\ u\right)$$

$$\det M=ut_1t_2-\frac{l_1l_2}{k}=ut_1t_2-l_1\frac{\sigma}{k}z=1$$

bu yüzden $\left(u,\dfrac{\sigma}{k}\right)=1$, buradan $\left(u,\dfrac{\sigma^2}{k^2}\right)=1$ dir. Böylece $u|q$ dur. Dolayısıyla

$$M=\sqrt{u}\begin{pmatrix} t_1 & \dfrac{l_1}{ku} \\ l_2 & t_2 \end{pmatrix}$$

Yukarıdan $l_2^{\ 2}=\sigma^2\dfrac{q}{u}q_1$ dir. Bu yüzden q_1, s bir tam sayı olmak üzere $\dfrac{q}{u}s^2$ biçiminde olmak zorunda, buradan $l_2=\sigma qs/u$ eşitliği elde edilir. Böylece

$$M=\sqrt{u}\begin{pmatrix} t_1 & \dfrac{l_1}{ku} \\ s\sigma q/u & t_2 \end{pmatrix}$$

Şimdi $t=l_1\sigma/k$ olsun. Bu durumda

$$M=\sqrt{u}\begin{pmatrix} t_1 & \dfrac{t}{u\sigma} \\ s\sigma q/u & t_2 \end{pmatrix}$$

M nin asıl biçimini elde etmek amacıyla $\forall A=\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\in\Gamma_0(N)$ için $MAM^{-1}\in\Gamma_0(N)$ bağıntısını kullanalım. Matris çarpımı gerçekleştirildiğinde

$$\forall A\in\Gamma_0(N) \text{ için } (a\text{-}d)t_1t\equiv(a\text{-}d)st_2\equiv 0(\bmod\sigma)$$

elde edilir. Şimdi $\forall A=\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\in\Gamma_0(N)$ için $\varepsilon_1=\varepsilon_1(N)=\mathrm{EBOB}(a\text{-}d)$ tanımlayalım, burada EBOB ile $\forall A=\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\in\Gamma_0(N)$ için (a-d) nin en büyük ortak böleni gösterilmektedir. Daha sonra $\varepsilon_2=(\varepsilon_1,\sigma)$ yazalım. Buradan $t_1t=st_2\equiv 0(\bmod\sigma/\varepsilon_2)$ olduğu görülür. Lemma 1 ve Lemma 2 kullanıldığında $\varepsilon_2\,|\,h$ (esasında $h=\varepsilon_2$) ve her $A=\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\in\Gamma_0(N)$ için $a\text{-}d\equiv 0(\bmod h)$ sonucu çıkar.Bu yüzden $t_1t=st_2\equiv 0(\bmod\sigma/h)$ denkliğini elde ederiz. $t_1t\equiv 0(\bmod\sigma/h)$ olması $\Delta\,|\,\sigma/h$ olmak üzere $t_1=r\Delta$ olduğunu gösterir, böylece $t=x\sigma/h\Delta$ dır. Benzer şekilde $st_2\equiv 0(\bmod\sigma/h)$ ve $(t_1,s)=1$ olduğundan $s=y\sigma/h\Delta$ ve $t_2=v\Delta$, $\Delta\,|\,\sigma/h$ elde ederiz. Bu yüzden

$$M=\sqrt{u}\begin{pmatrix} r\Delta & \dfrac{x}{u\sigma\Delta} \\ \dfrac{yN}{hu\Delta} & u\Delta \end{pmatrix} \tag{6}$$

elde edilir, (6) Lehner ve Newman tarafından verilen biçimdir.

$$M=\sqrt{u}\begin{pmatrix} r\Delta\sqrt{u} & \dfrac{x}{h\Delta\sqrt{u}} \\ \dfrac{vN}{h} & v\Delta\sqrt{u} \end{pmatrix},\ \det M=1$$

$$M=\begin{pmatrix} ru\Delta^2 & \frac{x}{h} \\ \frac{vN}{h} & vu\Delta^2 \end{pmatrix},\ \det M=u\Delta^2$$

$\det M=rvu^2\Delta^4-xyN/h^2=u\Delta^2$ dir. $u|q$ ve $\Delta \mid \sigma/h$ olduğundan $u\Delta^2 \mid \sigma^2 q/h^2=\frac{N}{h^2}$ dir.

Diğer yandan $\det M=u\Delta^2$ olduğunu biliyoruz. Bu yüzden $u\Delta^2 \parallel \frac{N}{h^2}$ dir. Dolayısıyla

$$M=\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix},\ \det=e>0,\ e \parallel \frac{N}{h^2}$$

biçimindedir. Lemma 2 kullanıldığında, tersine olarak bu biçimdeki elemanların $PSL(2,\mathbb{R})$ de $\Gamma_0(N)$ nin $\Gamma_B(N)$ normalliyenine ait olacağı görülebilir.

$\mathcal{N}or(N)$, ilk kez 1964 yılında Lehner ve Newman tarafından $\Gamma_0(N)$'nin "Weierstrass noktaları" ile ilgili çalışmalarında kullanıldı, daha sonra 1974'de Ogg normalliyenin "basit gruplar"la ilişkisini ortaya koydu, 1978'de Pizer Hecke'in "modüler formlar"la ilgili iddiasının normalliyenle olan bağlantısını gösterdi. 1979 yılında yine basit gruplarla ilgili bir çalışmada Conway ve Norton $\mathcal{N}or(N)$'nin yukarıda da kullandığımız bilinen en iyi tanımını verdiler.

1.7. Bazı Kongrüans Alt Gruplarının Yan Sınıfları

Teorem 9. $N\in\mathbb{Z}$ olsun. $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B=\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ matrisleri aşağıdaki kongrüans alt gruplarının aynı yan sınıfına aittir:

(i) $\Gamma_0(N) \Leftrightarrow ac'-ca' \equiv 0 (\mathrm{mod}\, N)$

(ii) $\Gamma_1(N) \Leftrightarrow a\equiv a'(\mathrm{mod}\, N),\ c\equiv c'(\mathrm{mod}\, N)$ veya,

$a\equiv -a'(\mathrm{mod}\, N),\ c\equiv -c'(\mathrm{mod}\, N)$

(iii) $\Gamma(N) \Leftrightarrow a\equiv a'(\mathrm{mod}\, N),\ b\equiv b'(\mathrm{mod}\, N),\ c\equiv c'(\mathrm{mod}\, N),\ d\equiv d'(\mathrm{mod}\, N)$ veya,

$a\equiv -a'(\mathrm{mod}\, N),\ b\equiv -b'(\mathrm{mod}\, N),\ c\equiv -c'(\mathrm{mod}\, N),\ d\equiv -d'(\mathrm{mod}\, N)$

İspat. Burada elemanter grup teorisinden çok iyi bilinen bir neticeyi kullanacağız; bir G-grubunun g_1 ve g_2 gibi keyfi iki elemanı verildiğinde bunların bir H alt grubunun aynı yan-sınıfına ait olmaları için gerek ve yeter koşul $g_1^{-1}g_2 \in H$.

Sonuç olarak A, B nin $\Gamma_0(N)$ nin aynı yan-sınıfına ait olmaları için gerek ve yeter şart $A^{-1}B \in \Gamma_0(N)$, yani

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

$\Gamma_0(N)$ nin bir elemanıdır, bu da $ac' - ca' \equiv 0 (\mathrm{mod}\, N)$ olması ile mümkündür.

(ii) nin ispatı için öncelikle $a \equiv a' (\mathrm{mod}\, N)$ ve $c \equiv c' (\mathrm{mod}\, N)$ olduğunu farz edelim. Öte yandan A nın determinantından gelen ad–bc=1 eşitliğini de kullandığımızda

$$da' - bc' \equiv da - bc \equiv 1 (\mathrm{mod}\, N)$$

kongrüansı elde edilir. Benzer şekilde B nin determinantı kullanıldığında

$$-cb' + ad' \equiv -c'b' + a'd' \equiv 1 (\mathrm{mod}\, N)$$

ve son olarak,

$$-ca' + ac' \equiv -ca + ac \equiv 0 (\mathrm{mod}\, N)$$

Bunun anlamı yukarıda hesapladığımız $A^{-1}B$, $\Gamma_1(N)$ nin bir elemanıdır ve bundan dolayı A ve B, $\Gamma_1(N)$ nin aynı yan sınıfındadırlar.

$a \equiv -a' (\mathrm{mod}\, N)$, $c \equiv -c' (\mathrm{mod}\, N)$ durumu da benzer şekilde yapılır.

(ii) nin ispatını tamamlamak için şimdi de A ve B nin, $\Gamma_1(N)$ nin aynı yan sınıfında olduklarını farz edelim. Ayrıca o yan sınıftan bir

$$C = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$

elemanını keyfi seçip sabit tutalım. O yan sınıfta A ve B yi içeren keyfi matris C ile $\Gamma_1(N)$ nin bir elemanının çarpımı olarak yazılabilir. Bu yüzden A=CD öyle ki

$$D=\begin{pmatrix} 1+Na_2 & b_2 \\ Nc_2 & 1+Nd_2 \end{pmatrix} \in \Gamma_1(N)$$

olsun, diğer bir deyişle

$$A=\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} 1+Na_2 & b_2 \\ Nc_2 & 1+Nd_2 \end{pmatrix}=\begin{pmatrix} a_1+Na_1a_2+Nb_1c_2 & * \\ c_1+Nc_1a_2+Nd_1c_2 & * \end{pmatrix}$$

ve buradan

$$a \equiv a_1 (\operatorname{mod} N)\,,\quad c \equiv c_1 (\operatorname{mod} N) \text{ veya,}$$

$$a \equiv -a_1 (\operatorname{mod} N)\,,\ c \equiv -c_1 (\operatorname{mod} N)$$

Aynı işlemler B için yapıldığında

$$a' \equiv a_1 (\operatorname{mod} N)\,,\quad c' \equiv c_1 (\operatorname{mod} N) \text{ veya,}$$

$$a' \equiv -a_1 (\operatorname{mod} N)\,,\ c' \equiv -c_1 (\operatorname{mod} N)$$

Bu sonuçlar birleştirildiğinde

$$a \equiv a' (\operatorname{mod} N)\,,\quad c \equiv c' (\operatorname{mod} N) \text{ veya,}$$

$$a \equiv -a' (\operatorname{mod} N)\,,\ c \equiv -c' (\operatorname{mod} N)$$

(ii) nin ispatını bitiren netice elde edilir.

(iii) nin ispatı da (ii) nin kanıtı gibi yapılır. Eğer

$$a \equiv a' (\operatorname{mod} N)\,,\ b \equiv b' (\operatorname{mod} N)\,,\ c \equiv c' (\operatorname{mod} N)\,,\ d \equiv d' (\operatorname{mod} N)$$

ise, determinantla birlikte yorumlandığında

$$da' - bc' \equiv -cb' + ad' \equiv 1 (\operatorname{mod} N) \text{ ve } -ca' + ac' \equiv 0 (\operatorname{mod} N)\,.$$

Böylece istenen 1. ve 3. kongrüans denklemleri elde edildi, ayrıca

$$db' - bd' \equiv db - bd \equiv 0 (\operatorname{mod} N)$$

denklemiyle beraber göz önüne alındığında $A^{-1}B \in \Gamma(N)$ olduğu görülür

$a \equiv -a' (\operatorname{mod} N)$, $b \equiv -b' (\operatorname{mod} N)$, $c \equiv -c' (\operatorname{mod} N)$, $d \equiv -d' (\operatorname{mod} N)$ durumu benzer şekilde yapılır.

Tersine olarak A ve B, $\Gamma(N)$ nin aynı yan sınıfındaki iki matris olsun. O yan sınıftan bir

$$C=\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$

elemanını keyfi seçip sabit tutalım. A yı C ile

$$D=\begin{pmatrix} 1+Na_2 & Nb_2 \\ Nc_2 & 1+Nd_2 \end{pmatrix} \in \Gamma(N)$$

elemanının çarpımı olarak yazabiliriz, yani

$$A=\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} 1+Na_2 & Nb_2 \\ Nc_2 & 1+Nd_2 \end{pmatrix}$$

eşitliğinden

$$A=\begin{pmatrix} a_1+Na_1a_2+Nb_1c_2 & Na_1b_2+b_1+Nb_1d_2 \\ c_1+Nc_1a_2+Nd_1c_2 & Nc_1b_2+d_1+Nd_1d_2 \end{pmatrix}$$

elde edilir. Buna göre

$$a \equiv a_1 \pmod N,\ b \equiv b_1 \pmod N,\ c \equiv c_1 \pmod N,\ d \equiv d_1 \pmod N \text{ veya,}$$

$$a \equiv -a_1 \pmod N,\ b \equiv -b_1 \pmod N,\ c \equiv -c_1 \pmod N,\ d \equiv -d_1 \pmod N$$

Aynı işlemler B için yapıldığında

$$a' \equiv a_1 \pmod N,\ b' \equiv b_1 \pmod N,\ c' \equiv c_1 \pmod N,\ d' \equiv d_1 \pmod N \text{ veya,}$$

$$a' \equiv -a_1 \pmod N,\ b' \equiv -b_1 \pmod N,\ c' \equiv -c_1 \pmod N,\ d' \equiv -d_1 \pmod N.$$

Elde edilen bu neticeler birleştirildiğinde

$$a \equiv a' \pmod N,\ b \equiv b' \pmod N,\ c \equiv c' \pmod N,\ d \equiv d' \pmod N \text{ veya,}$$

$$a \equiv -a' \pmod N,\ b \equiv -b' \pmod N,\ c \equiv -c' \pmod N,\ d \equiv -d' \pmod N$$

Böylece (iii) nin, dolayısıyla önermenin ispatı tamamlanmış olur.

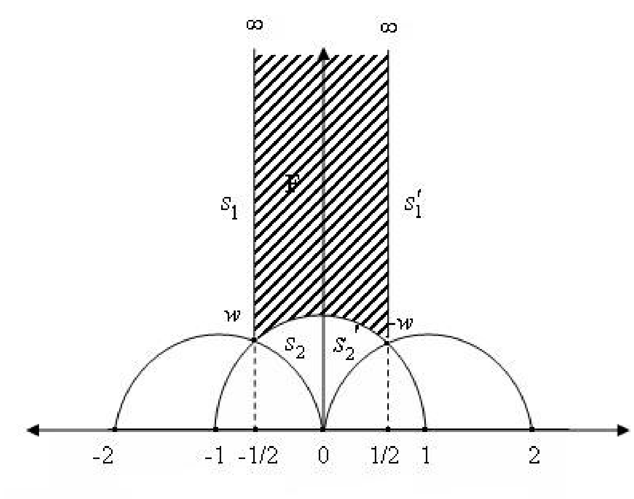
1.8. Temel Bölgeler

Bir Λ-Fuchsian grubu verildiğinde, aşağıdaki özellikleri sağlayan bir $F \subset \mathcal{U}$ kapalı kümesine Λ nın bir F-temel bölgesi(*fundamental region*) denir:

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

(ii) $\forall T \in \Lambda \setminus \{I\}$ için $\mathring{F} \cap T(\mathring{F}) = \varnothing$

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



Şekil 1. Γ nın F temel bölgesi

T(z)= z+1 için $T(s_1) = s_1'$ ve $U(z) = -\frac{1}{z}$ için $U(s_2) = s_2'$ olduğundan (s_1, s_1') ve (s_2, s_2') kongrü kenar çiftleridir. Bu nedenle T ve U dönüşümleri Γ modüler grubunu üretir(Schoeneberg, 1974, sf.17–18).

Λ bir Fuchsian grubu olsun. Bu takdirde Λ' nın herhangi bir temel bölgesinin hiperbolik alanı;

$$\mu(\Lambda) = 2\pi\left\{2(g-1) + \sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right) + s\right\}.$$

(Beardon, 1983, sf. 269).

Hiperbolik ölçüm yardımıyla son derece kullanışlı olan Riemann-Hurwitz formülü elde edilir; Λ bir Fuchsian grubu ve $\Omega \leq \Lambda$ olsun. Buna göre $|\Lambda : \Omega| < \infty$ ise

$$|\Lambda : \Omega| = |\Lambda / \Omega| = \frac{\mu(\Lambda)}{\mu(\Omega)}.$$

Teorem 10. $a,b \in \hat{\mathbb{R}}$ olsun. $\mathcal{U}$'da a'yı b'ye birleştiren geodezik (iki nokta arasındaki en kısa yol) iki türlü olabilir;

(i) $a \in \mathbb{R}$'den $b = \infty$'a giden reel eksene dik doğru-parçası

(ii) $a, b \in \mathbb{R}$'yi birleştiren merkezi reel eksen üzerinde olan yarı-çember

Dikkat edilecek olursa yukarıdaki temel bölgenin sınırının da geodeziklerden oluştuğu görülür. $PSL_2(\mathbb{R})$, izometrilerin bir grubu olarak geodezikleri geodeziklere resmeder (Jones ve Singerman, 1987, sf. 223–224).

1.9. Temel Bölgenin Cinsi

Bir kompakt, yönlendirilebilir X-Riemann yüzeyini göz önüne alalım. X de reellerin kapalı birim aralığının bir homeomorf resmine bir 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 (*closed curve*) adı verilir. Öklid düzlemindeki bir kapalı dairenin X deki bir homeomorf resmine X üzerinde bir *polygon* 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 kesişimler 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(*vertex*), kenar(*edge*) ve yüz(*face*) ün anlamı açıktır. Bunların sayısını sırasıyla v,e ve f ile göstereceğiz.

Teorem 11 (Euler). X in her poligonal ayrışmasında v–e+f sayısı invaryant kalır (Schoeneberg, 1974, sf.93).

Tanım 13. $g := 1 - \frac{v-e+f}{2}$ kesişmeyen ve X i parçalamayan kapalı eğrilerin maksimal sayısıdır(Schoeneberg,1974,sf.93). Bu önemli topolojik invaryanta X in cinsi(*genus*) denir.

Teorem 12. $\Gamma_0(N)$ kongrüans alt grubunun temel bölgesinin cinsi

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

formülü ile verilir. Burada

$$\varepsilon_\rho = \begin{cases} 0 & \text{eğer } 9 \mid N \\ \prod_{p \mid N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{aksi halde} \end{cases} \quad , \quad \varepsilon_i = \begin{cases} 0 & \text{eğer } 4 \mid N \\ \prod_{p \mid N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{aksi halde} \end{cases}$$

ve $\sigma_\infty = \sum_{t \mid N} \varphi\left(\left(t, \frac{N}{t}\right)\right)$ biçimindedir(Schoeneberg, 1974, sf.103).

N≤ 25 için elde edilen sonuçları verelim;

g=0 N=1, …, 10, 12, 13, 16, 25 için;

g=1 N=11, 14, 15, 17, …, 21 için;

g=2 N=22, 23 için;

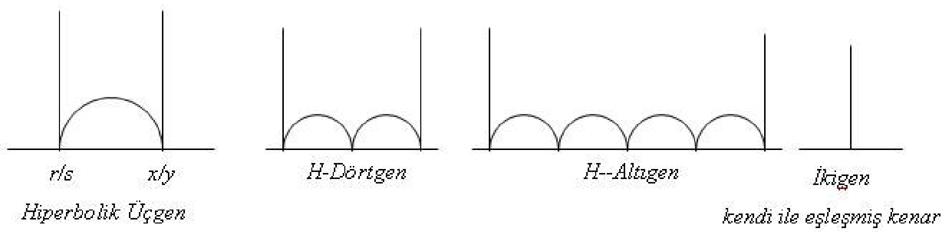
g=3 N=24 için .

1.10. Graf Teori

$X \neq \emptyset$ 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 denir. $(a,b) \in \Delta$ ise bu durum $a \rightarrow b$ ile gösterilir. Eğer $a \rightarrow b$ veya $a \leftarrow b$ ise a ve b ye bir kenar ile bağlanmıştır denir. Bu durumda a ve b ye komşu köşeler denir.

G=(X,Δ) bir graf ve A⊂ X olsun. $G' = (A, \Delta \cap A \times A)$ grafına köşe kümesi A olan G nin bir alt grafı denir.

$a = a_0, a_1, \ldots, a_n = b$ bir G-grafının köşelerinin bir dizisi olsun. Eğer 1≤ i ≤ 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 (*triangle*), dört kenarlı bir devreye bir dörtgen (*rectangle*) ve altı kenarlı bir devreye bir altıgen (*hexagon*) denir.



Şekil 2. Devreler

G=(X,Δ) bir graf olsun. X üzerinde bir ≈-bağıntısını şöyle tanımlayalım:

a≈b :⟺ a=b veya a'dan b'ye bir yol vardır.

Açık olarak, ≈ bir eşdeğerlik bağıntısıdır. X in kendisi bu bağıntının eşdeğerlik sınıflarından birine eşitse G-grafına bağlantılıdır denir.

Eğer X_1, ≈-bağıntısının bir eşdeğerlik sınıfına eşitse $(X_1, \Delta \cap X_1 \times X_1)$ 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 (Tsuzuku, 1982, sf. 186-187).

Şimdi anlattıklarımıza daha açıklık kazandırması için çok iyi bilinen Farey Grafını örnek verelim: m ≥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 F_m ile gösterilir, örneğin

$$F_4 \text{ için: } \ldots, -\frac{1}{3}, -\frac{1}{4}, 0, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1, \frac{5}{4}, \frac{4}{3}, \ldots$$

Açık olarak $F_1 \subset F_2 \subset F_3 \subset \ldots$ ve $\bigcup_{m\geq 1} F_m = \mathbb{Q}$'dur. Farey grafı ile Farey dizileri arasındaki bağıntıyı veren aşağıdaki teoremi verelim:

Teorem 13. $\frac{r}{s}, \frac{x}{y} \in \mathbb{Q}$ olsun. Bu takdirde aşağıdakiler eşdeğerdir;

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

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

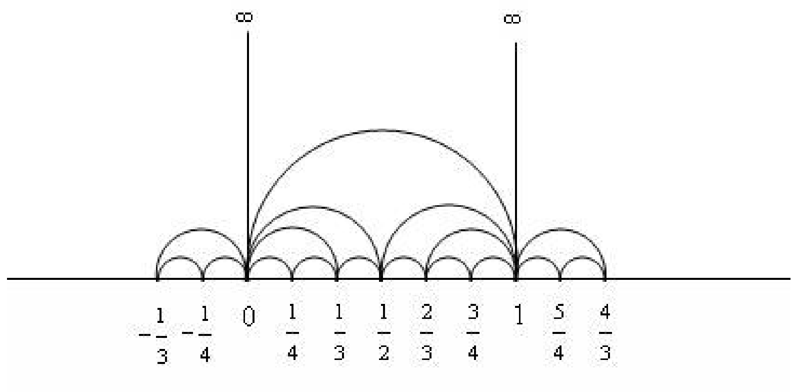
(iii) $\frac{r}{s}$ ve $\frac{x}{y}$ bir m doğal sayısı için F_m'nin ardışık terimleridir (Jones vd., 1991).

F nin komşu iki köşesini üst-yarı düzlemde bulunan ve bu iki köşeden geçen merkezi reel eksende ve reel eksene dik yarı-çemberlerle bağlayalım. Bu durumda F nin kenarlarıyla ilgili aşağıdaki önemli sonucu verebiliriz.

Teorem 14. F nin kenarları $\mathcal{U} = \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$ üst-yarı düzleminde kesişmezler.

İspat. F grafında $\frac{r}{s} \rightarrow \frac{x}{y}$ ve $\frac{r'}{s'} \rightarrow \frac{x'}{y'}$ kenarlarının kesiştiğini kabul edelim. $ry - sx = \pm 1$ olduğu göz önüne alınarak $S(z) := \frac{yz - x}{-sz + r}$ seçildiğinde $S \in \Gamma$ ve $S\left(\frac{r}{s}\right) = \infty, S\left(\frac{x}{y}\right) = 0$ dır. Ayrıca $S\left(\frac{r'}{s'}\right)$ ve $S\left(\frac{x'}{y'}\right)$ F de komşu köşelerdir.

Γ nın elemanları geodezikleri geodeziklere resmettiğinden $S\left(\frac{r'}{s'}\right)$ yi $S\left(\frac{x'}{y'}\right)$ye birleştiren reel eksene dik yarı-çember, 0 noktasını ∞ noktasına birleştiren Re(z)=0 doğru-parçası ile $\mathcal{U}$ da kesişir. Dolayısıyla 0 noktası $S\left(\frac{r'}{s'}\right)$ ile $S\left(\frac{x'}{y'}\right)$ komşu köşeleri arasındadır. Bu ise bir önceki önermeye göre çelişkidir.



Şekil 3. Farey Grafı

1.11. İmprimitif Hareket

$X \neq \emptyset$ bir küme olsun. $\xi : X \to X$ bire-bir, örten ise ξ ye X in bir *permütasyon*u denir. X in tüm permütasyonlarının kümesi S^X ile gösterilir.

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

G, X üzerinde bir permütasyon grubu olsun. Bu taktirde, G, X üzerinde hareket eder. Gerçekten $g \in G$ ise $g: X \to X$ bire-bir ve örten bir dönüşümdür. Bu durumda $gx := g(x)$ olarak alınırsa $(g_1 g_2)x = g_1(g_2 x)$ ve $1x = x$ olduğu açıktır. Bu harekete G nin X üzerindeki doğal hareketi denir ve "(G,X) permütasyon grubu" ifadesi kullanılır.

(G,X) bir transitif permütasyon grubu ve R, X üzerinde bir eşdeğerlik bağıntısı olsun. $\forall(x,y) \in R$ ve $\forall g \in G$ için $(g(x),g(y)) \in R$ ise R ye bir G-*invaryant eşdeğerlik bağıntısı* denir. Bir G-invaryant eşdeğerlik bağıntısının denklik sınıflarına eşdeğerlik bağıntısının *blok*ları denir. Bu tanıma göre;

i) Özdeşlik bağıntısı : $(x, y) \in R \Leftrightarrow x = y$

ii) Evrensel bağıntı : $R = X \times X$

bağıntılarının G-invaryant eşdeğerlik bağıntıları olduğu açıktır (trivial bağıntılar).

X üzerinde trivial bağıntıların dışında bir G-invaryant eşdeğerlik bağıntısı yoksa (G,X) e *primitif*, aksi halde *imprimitif* denir (Biggs ve White, 1979).

Lemma 3. (G,X) bir transitif permütasyon grubu, $H \leq G$ ve bir $\alpha \in X$ için $G_\alpha \leq H$ olsun. Bu takdirde

$$R := \{ (g(\alpha), gh(\alpha)) : g \in G, h \in H \}$$

bir G-invaryant eşdeğerlik bağıntısıdır. Ayrıca

$$R \text{ özdeşlik bağıntısıdır} \Leftrightarrow H = G_\alpha$$

(Biggs ve White, 1979).

Lemma 4. (G,X) bir transitif permütasyon grubu olsun.

$$(G,X) \text{ primitif} \Leftrightarrow \forall x \in X \text{ için } G_x, X \text{ in maksimal bir alt grubudur}$$

(Biggs ve White, 1979).

Teorem 15. (G,X) bir transitif permütasyon grubu olsun. $G_\alpha < H < G$ ise

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

iyi tanımlı bir *G*-invaryant eşdeğerlik bağıntısıdır. Denklik sınıflarının sayısı da $|G:H|$ indeksidir(Biggs ve White, 1979).

1.12. Alt Yörüngesel Graflar

(G,X) bir transitif permütasyon grubu olsun. G nin $X \times X$ üzerinde $g \in G$ olmak üzere

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

ile tanımlı hareketini göz önüne alalım. Bu hareketin yörüngelerine G nin alt yörüngeleri denir. (α,β) yı içeren alt yörüngeyi $O(\alpha,\beta)$ ile gösterelim. $O(\alpha,\beta)$ dan bir $G(\alpha,\beta)$ alt yörüngesel grafını aşağıdaki gibi elde edelim.

$G(\alpha,\beta)$ nın köşeleri X in elemanlarıdır, x, $y \in X$ noktaları için $(x, y) \in O(\alpha,\beta)$ 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 $O(\beta,\alpha)$ da alt yörüngedir. $O(\alpha,\beta) = O(\beta,\alpha)$ veya $O(\alpha,\beta) \neq O(\beta,\alpha)$ dır. Birinci durumda $G(\alpha,\beta) = G(\beta,\alpha)$ dır ve $G(\alpha,\beta)$ grafında $x \rightarrow y$ ise yine $G(\alpha,\beta)$ grafında $y \rightarrow x$ sağlanır. Bu durumda $G(\alpha,\beta)$ grafına kendisiyle eşleşmiş graf diyeceğiz. İkinci durumda G(α,β) grafında x$\rightarrow$ y ise G(β,α) grafında y$\rightarrow$ x sağlanır. Bu durumda ise G(α,β) ve G(β,α) graflarına «birbirleriyle eşleşmiş graf» diyeceğiz.

$O(\alpha,\alpha)=\{(x,x): x\in X\}$, $X\times X$ in köşegenidir. $O(\alpha,\alpha)$ ya uygun G(α,α) alt yörüngesel grafına aşikar 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, daha sonra Biggs ve White sonlu gruplar için uygulamaları üzerinde durmuşlar, ardında da Tsuzuku bu düşünceleri bir kitapta toparlamıştır.

2. YAPILAN ÇALIŞMALAR VE BULGULAR

N-karesiz için $\mathcal{N}or$(N) nin simgesi bulunmuştur (Maclachlan, 1981). N-keyfi olduğu durumda g-cinsi ve 2-periyotların dışında yine simgenin tüm invaryantları bulunmuştur (Akbaş ve Singerman, 1992). Hurwitz formülü dikkate alındığında normalliyenin bir temel bölgesinin hiperbolik ölçümünün kullanılmasıyla tüm simgenin elde edileceği görülür. Bu tezde amacımız normalliyenin alt yörüngesel graflarını elde ederek bu problemin çözülmesi yolunda bir yaklaşım getirmektir.

2.1. $\mathcal{N}or$(N) nin Alt Grupları

Bu bölümde çalışmalarımızda zaman zaman önemli kolaylıklar sağlayan ve $\mathcal{N}or$(N) nin yapısını anlamamıza yardımcı olan bazı alt gruplarını vereceğiz:

$\mathcal{N}or$(N) de determinantı 1 olan dönüşümlerin kümesi, $\mathcal{N}or$(N) nin bir alt grubudur ve $\Gamma_C(N)$ ile gösterilir.

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

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

$W_e=\begin{pmatrix} ae & b \\ cN & de \end{pmatrix}$ biçimindeki matrislere karşılık gelen dönüşümlerin kümesi bir gruptur ve $\Gamma_W(N)$ ile gösterilir, burada $e\,\|\,N$ ve $\det W_e =$ e>0 dır. $\Gamma_W(N)$ nin elemanları Atkin-Lehner dönüşümleri olarak adlandırılır(Akbaş, 1989, sf.36).

Şimdi gerekli olan $\mathcal{N}or$(N) de $\Gamma_0(N)$ nin indeksini hesaplayalım. $\Gamma_C(N)$, $\mathcal{N}or$(N) nin 2^{ρ} indeksli normal bir alt grubudur, burada ρ, N/h^2 nin farklı asal çarpanlarının sayısıdır. $\Gamma_0(N)\le\Gamma_C(N)$ olduğu açıktır.

Buna göre indeks $|\Gamma_C(N):\Gamma_0(N)|=h^2\tau$ dur, burada $\tau=\left(\frac{3}{2}\right)^{\varepsilon_1}.\left(\frac{4}{3}\right)^{\varepsilon_2}$

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

şeklindedir. Gerçekten,

$\Gamma_C(N)$, determinantı 1 olan $\begin{pmatrix} a & b/h \\ cN/h & d \end{pmatrix}$ biçimindeki dönüşümlerin kümesi olduğundan , yukarıdaki ifadelerden yararlanarak;

$$|\Gamma_C(N):\Gamma_0(N)|=N\prod_{p|N}\left(1+\frac{1}{p}\right)\ \Big/\ N/h^2\prod_{p|(N/h^2)}\left(1+\frac{1}{p}\right)=h^2\tau$$

burada

$$\tau=\prod_{p|N}\left(1+\frac{1}{p}\right)\ \Big/\ \prod_{p|(N/h^2)}\left(1+\frac{1}{p}\right)$$

şeklindedir.

Şimdi her r tam sayısı için h(r) yi $(h(r))^2\,|\,r$ olmak üzere 24 ün en büyük böleni olacak şekilde yazalım. N, $2^\alpha 3^\beta K$ ve $(K,6)=1$ olacak şekilde yazıldığında, eğer $\alpha=2,4,6$ veya $\beta=2$ ise $\tau\neq 1$ olduğu görülür.

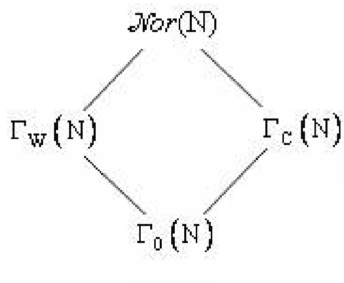
ρ ve τ yukarıdaki gibi olmak üzere $|\mathcal{N}or(N):\Gamma_0(N)|=2^\rho h^2\tau$ dur.

Buradan $2^\rho h^2\tau=2^r h^2 s$ eşitliği kolayca elde edilir, burada r,ρ ve τ yukarıdaki gibi ve

$$s_2=\begin{cases}3/4\ , & 2|(h(2^\alpha))^2\ \|\ N\\ 1\ , & \text{aksi takdirde}\end{cases}\quad ,\quad s_3=\begin{cases}2/3\ , & (h(3^\beta))^2=9\ \|\ N\\ 1\ , & \text{aksi takdirde}\end{cases}$$

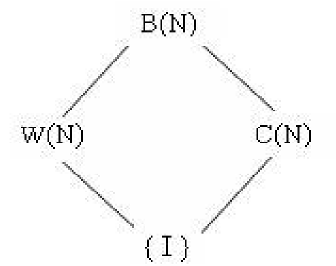
olmak üzere $s=s_2 s_3$ şeklindedir (Akbaş, 1989, sf.38).

$\mathcal{N}or$(N) nin her V elemanı $W\in\Gamma_W(N)$ ve $T\in\Gamma_C(N)$ olmak üzere bir WT çarpımı olarak yazılabilir**.** Şimdiye kadar bahsedilen normalliyenin alt gruplarına göre aşağıdaki diyagramı elde ederiz;



veya $B(N)=\dfrac{\mathcal{N}or(N)}{\Gamma_0(N)}$, $C(N)=\dfrac{\Gamma_C(N)}{\Gamma_0(N)}$, $W(N)=\dfrac{\Gamma_W(N)}{\Gamma_0(N)}$ olarak tanımlandığında,

$|B(N)|=2^{\rho}h^2\tau=2^r h^2 s$, $|C(N)|=h^2\tau$, $|W(N)|=2^r$ burada ρ ve s yukarıdaki gibi ve r, *N* nin farklı asal bölenlerinin sayısıdır. Böylece;



$|W(N)\cap C(N)|=2^{r-\rho}$ dur. Dolayısıyla;

$$|W(N)\cap C(N)|=\begin{cases}4\ , & 3^2 \,\|\, N \text{ ve } 2^{2\delta} \,\|\, N\ ,\ \delta=1,2\vee 3 \text{ ise}\\ 2\ , & 3^2 \,\|\, N \text{ veya } 2^{2\delta} \,\|\, N \text{ ise}\\ 1\ , & \text{aksi takdirde}\end{cases}$$

Bu yüzden yalnızca son durumda B(N), W(N) ve C(N) nin bir yarı-direkt çarpımıdır.

Şimdi bu alt grupların yardımıyla normalliyendeki eliptik elemanların mertebelerini ortaya koyan, daha sonraki bölümlerde irdeleyeceğimiz alt yörüngesel graflarla doğrudan ilişkisi olan ve graflardaki devrelerle birlikte yorumlandığında sayılar teorisinde ilginç neticeler veren aşağıdaki teoremi ispatlayalım.

Teorem 16. N keyfi bir pozitif tam sayı olsun. Bu durumda 𝒩or(N) yalnızca 2, 3, 4 ve 6 mertebeli periyotlara sahip olabilir ve üstelik;

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

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

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,

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

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,

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

(Singerman, 1970).

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

i) e=1 ise E^3=I

ii) e=2 ise E^4=I

iii) e=3 ise E^6=I

(i), (ii), (iii) için benzer yolla hesaplamalar yapalım. e=1 olduğundan ve a+d=1 kabul edebileceğimizden $E=\begin{pmatrix} a & b/h \\ cN/h & d \end{pmatrix}$ dir. detE=1 kullanıldığında $E^2=\begin{pmatrix} a-1 & b/h \\ cN/h & d-1 \end{pmatrix}$ ve E^3=I elde ederiz. a+d $\neq 0$ ve e>3 olan durumlara baktığımızda $|(a+d)\sqrt{e}| \geq 2$ elde edilir. Buna göre E ya parabolik ya da hiperboliktir. Dolayısıyla her iki durumda da E sonsuz mertebelidir.

a) Farzedelim ki $\mathcal{N}or$(N) nin 4. mertebeden bir periyoda sahip olsun. Bu durumda e=2 dir.

Buna göre $2^k \parallel N$ ve k=1, 3, 5, 7 dir.Böylece E eliptik elemanı $\begin{pmatrix} 2a & b/h \\ cN/h & 2d \end{pmatrix}$ biçimindedir ve $\det E = 4ad - bcN/h^2 = 2$ dir. d=1-a eşitliği kullanıldığında $(2a-1)^2 \equiv -1 \pmod{N/h^2}$ denklemi elde edilir. Bu kongrüans denkleminin bir çözümü olması için gerek ve yeter şart $p_i \equiv 1 \pmod 4$ olmak üzere $N/h^2 = 2p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, i=2,…,r olmasıdır.

Şimdi $\mathcal{N}or(N)$ nin 4. mertebeden t tane periyoda sahip olduğunu varsayalım. $E = \begin{pmatrix} 2a & b/h \\ cN/h & 2d \end{pmatrix}$, 4. mertebeden keyfi bir eliptik eleman olsun. Dolayısıyla buradan

$$E^2 = \begin{pmatrix} 4a-2 & 2b/h \\ 2cN/h & 4d-2 \end{pmatrix} = \begin{pmatrix} 2a-1 & b/h \\ cN/h & 2d-1 \end{pmatrix} \in \Gamma_C(N)$$

dir. Bu yüzden 4. mertebeden her periyot, $2 \bmod \Gamma_C(N)$ bileşenine sahiptir.Dolayısıyla $\Gamma_C(N) \cong \Gamma_0(N/h^2)$ ve $|\mathcal{N}or(N) : \Gamma_C(N)| = 2^{r-1}$ olduğundan $\Gamma_C(N)$, 2. mertebeden en az $t\,2^{r-1}$ tane periyoda sahiptir. Teorem 11 den $t=1$ sonucunu elde ederiz.

b) $\mathcal{N}or(N)$ nin 6. mertebeden bir periyoda sahip olsun. Dolayısıyla 3 veya $3^3 \parallel N$ dir. (a) da olduğu gibi

$$E = \begin{pmatrix} 3a & b/h \\ cN/h & 3d \end{pmatrix} \quad \text{ve} \quad \det E = 3$$

olsun. $\det E = 9ad - bcN/h^2 = 3$ dür. d=1-a eşitliği kullanıldığında $3a(1-a) - bcN/3h^2 = 1$ eşitliğini elde ederiz. Bu $2 \nmid N/h^2$ olduğunu söyler. Buradan $(6a-3)^2 \equiv -3 \pmod{N/3h^2}$ elde ederiz. Bu kongrüans denkleminin bir çözüme sahip olması için gerek ve yeter koşul $N/3h^2$ nin tüm p_i asal bölenlerinin mod3 e göre 1 e kongrü olmasıdır.

Şimdi $\mathcal{N}or(N)$ nin 6. mertebeden t tane periyoda sahip olduğunu farzedelim. (a) da olduğu gibi $\mathcal{N}or(N)$ de 6. mertebeden tüm periyotların $2 \bmod \Gamma_C(N)$ bileşenine sahip olduğunu ve bu yüzden $\Gamma_C(N)$ nin 3. mertebeden en az $t\,2^{r-1}$ tane periyoda sahip olacağını görebiliriz. Teorem 1 ve Teorem 11 kullanıldığında $t=1$ elde edilir.

c) $\mathcal{Nor}$(N) 3. mertebeden bir periyoda sahip ise e=1 dir.

$$E=\begin{pmatrix} a & b/h \\ cN/h & d \end{pmatrix} \text{ ve } \det E=1$$

olsun. detE=ad–bcN/h^2=1dir. Buradan a(1–a)–bcN/h^2=1dir.

Böylece $(2a-1)^2+4bcN/h^2=-3$ dür. Bu yüzden $3|N/h^2$ ise $3|(2a-1)^2$ ve dolayısıyla $3^2|(2a-1)^2$ dir. Bu $3^2\nmid N/h^2$ olduğunu gösterir. Sonuç olarak $(2a-1)^2\equiv-3\left(\mathrm{mod}\,N/h^2\right)$ dir. Bu kongrüans denkleminin bir çözüme sahip olması için gerek ve yeter şart ; $p_i\equiv1(\mathrm{mod}\,3)$ olmak üzere $N/h^2=3^{\alpha_2}p_3^{\alpha_3}...p_r^{\alpha_r}$, $\alpha_2\le1$, $i=3,...,r$ dir. Şimdi $\mathcal{Nor}$(N), 3. mertebeden bir periyoda sahip ise $3\nmid N/h^2$ olduğunu gösterelim. Eğer $N/h^2=3p_3^{\alpha_3}...p_r^{\alpha_r}$, $p_i\equiv1(\mathrm{mod}\,3)$, i=3,…,r ise Teorem 11 kullanıldığında $\Gamma_C(N)$ nin 3. mertebeden tam olarak 2^{r-2} tane periyoda sahip olduğu ve 2. mertebeden hiçbir periyodunun olmadığını görürüz. Bu durumda Teorem 1 den $2^{r-2}=2^{r-1}M\sum\limits_{i\in\Omega}\frac{1}{t_i}$ dir. Dolayısıyla $\mathcal{Nor}$(N), 3. mertebeden bir periyoda sahip olsaydı, t_i lerden en az biri 1 olacaktı, ki bu imkansızdır. Bu yüzden $\mathcal{Nor}$(N) nin 3. mertebeden periyotlara sahip olması için gerek ve yeter koşul $N/h^2=3p_3^{\alpha_3}...p_r^{\alpha_r}$, $p_i\equiv1(\mathrm{mod}\,3)$, i=3,…,r dir. $\mathcal{Nor}$(N) nin 3. mertebeden t tane periyodu olduğunu kabul edelim, buradan $\Gamma_C(N)$ nin 3. mertebeden $t\,2^{r-2}$ tane periyoda sahip olduğu görülür. Ancak $\Gamma_C(N)$, 3. mertebeden tam $t\,2^{r-2}$ tane periyoda sahiptir. Bu yüzden t=1 dir.

2.2. $\mathcal{Nor}$(N) nin $\hat{\mathbb{Q}}$ Üzerindeki Hareketi

Teorem 17: Γ**,** $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket eder.

İspat: $\frac{a}{b},\frac{c}{d}\in\hat{\mathbb{Q}}$; $\frac{a}{b}\neq\frac{c}{d}$ 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 $\xi\circ\eta^{-1}\in\Gamma$ dönüşümü vardır. Dolayısıyla Γ , $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket eder (Jones vd., 1991).

Teorem 18. $\Gamma_0(N)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketi transitif değildir.

İspat. Aksini varsayalım ve $0, \infty\in\hat{\mathbb{Q}}$ seçelim. Bu durumda $\Gamma_0(N)$ nin

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

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

Teorem 19. $N\in\mathbb{Z}$ 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

$$\alpha_1\leq 7,\ \alpha_2\leq 3, \text{ ve } \alpha_i\leq 1 : i = 3, \dots, n$$

olmasıdır (Akbaş ve Singerman, 1992).

İmprimitif hareket açısından ele alındığında transitiflik vazgeçilmez şartımızdır. Dolayısıyla bu koşulun sağlanmadığı durumlarda yapılacak iş transitifliğin sağlandığı maksimal alt kümeyi bulmaktır. Şimdi bu konuda bize büyük kolaylık sağlayacak olan aşağıdaki sonucu elde edelim.

Lemma 5. Bir $\dfrac{k}{s}\in\mathbb{R}$, ($s\neq 0$, $(k,s)=1$) rasyonel sayısı verildiğinde $A\begin{pmatrix} k \\ s \end{pmatrix}=\begin{pmatrix} k_1 \\ s_1 \end{pmatrix}$, $s_1|N$

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

$$Nck + ds = (N,s) \ldots (1)$$

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

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

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) deki koşulları sağlayan, hem de $(Nc_*, d_*) = 1$ şartını sağlayan bir $\{c_*, d_*\}$ çiftinin varolduğunu 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 $d_2 = d_1 - \frac{q_0 Nk}{(N,s)}$ q_0 diyelim. (1) eşitliği yüzünden $\left(q_0, \frac{Nk}{(N,s)}\right)$=1 dir, bu yüzden (2) de n=1 alarak $q_0 | d_1$ 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. $d_2 = d_1 - \frac{q_0 Nk}{(N,s)}$ 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 taktirde şu sonucu ulaşılır;

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

$\vdots \qquad \vdots$

$d_{k_0+1} = d_{k_0} - \frac{q_0 q_1 \ldots q_{k_0-1} Nk}{(N,s)}$ (ve dolayısıyla d_{k_0+1}'de q_0, q_1, …, 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 $A\left(\frac{k}{s}\right) = \left(\frac{k_1}{s_1}\right)$, $s_1 \mid N$ dir.

Lemma 6. $d|N$ ve $(a_1,d)=(a_2,d)=1$ olsun. Bu durumda $t = \left(d, \frac{N}{d}\right)$ olmak üzere,

$$\begin{pmatrix} a_1 \\ d \end{pmatrix} \text{ ve } \begin{pmatrix} a_2 \\ d \end{pmatrix} \text{ eşleniktir } \Leftrightarrow a_1 \equiv a_2 \pmod{t}.$$

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

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

$$aa_1 - a_2 \equiv 0 \pmod{d_1} \Rightarrow aa_1 - a_2 \equiv 0 \pmod{t}$$

detA dan $ad \equiv 1 \pmod{t}$ elde edilir ve yukarıdan $d \equiv 1 \pmod{t}$ dir. Bu yüzden $a \equiv 1 \pmod{t}$. $aa_1 - a_2 \equiv 0 \pmod{t}$ olduğundan $a_1 \equiv a_2 \pmod{t}$ dir.

Teorem 20. $d|N$ olsun. $\frac{a}{d}$ nin $\Gamma_0(N)$ ile hareketiyle oluşan yörünge

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

kümesidir. Üstelik $\begin{pmatrix} a \\ d \end{pmatrix}$, $d|N$ yörüngelerinin sayısı $\varphi\big(d, N/d\big)$, φ-Euler fonkiyonudur (Akbaş ve Singerman, 1992).

İspat . $\eta(N) = \sum_{d|N} \varphi\left((d, N/d)\right)$ -parabolik sınıf sayısı ve Lemma 6 kullanılırsa kolayca gösterilebilir.

2.3. N-karesiz için $\mathcal{N}or$(N) nin Alt Yörüngesel Grafları

N nin seçiminden dolayı $\mathcal{N}or$(N), $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket eder.

G= $\mathcal{N}or(N)$, H=Γ_0(N) ve Ω=$\hat{\mathbb{Q}}$ olarak seçildiğinde, N>1 için

$$\Gamma_\infty < \Gamma_0(\mathrm{N}) < \mathcal{N}or(\mathrm{N})$$

olduğu açıktır.

$\approx$ ile Γ_0(N) tarafından $\hat{\mathbb{Q}}$ üzerine indirgenen $\mathcal{N}$-invaryant eşdeğerlik bağıntısını gösterelim. Diğer taraftan

$$v=\frac{r}{s},\ w=\frac{x}{y}\in\hat{\mathbb{Q}} \quad \text{öyle ki} \quad \begin{matrix}(s,N)=e_1\\(y,N)=e_2\end{matrix} \quad \text{ve} \quad \begin{matrix}s=s_1e_1\\y=y_1e_2\end{matrix}$$

alalım. Buna göre $e=N/e_1$ ve $f=N/e_2$ ise $\mathcal{N}or$(N) nin

$$g=\begin{pmatrix}re & *\\ s_1N & d_1e\end{pmatrix}, \det g=e \quad \text{ve} \quad g'=\begin{pmatrix}yf & *\\ y_1N & d_2f\end{pmatrix}, \det g'=f$$

elemanlarının ∞ u sırasıyla v ve w ya resmettiği görülür. Buradan da

$$v\approx w \Leftrightarrow e=f$$

gerek ve yeter şartı elde edilir. İmprimitif hareketin neticesinde oluşan blokların sayısı

$$\Psi(\mathrm{N})=\left|\mathcal{N}or(\mathrm{N}):\Gamma_0(\mathrm{N})\right|.$$

Lemma 7. $\Psi(N)=2^r$ öyle ki r, N yi bölen asal çarpanların sayısıdır (Akbaş ve Başkan, 1996).

Teorem 21. $\frac{r}{s}\rightarrow\frac{x}{y}\in\Delta_{u,n}$ olması için gerek ve yeter şart $\exists e\in\mathbb{Z}$ **:** $e \mid N$ ve $\frac{N}{e} \mid s$.

Ayrıca (n,e)=e_n , $n=n_1e_n$, $e=e_1e_n$ ise

a) $ry-sx=n_1$ ve $x\equiv e_1ur \pmod{n_1}$, $y\equiv e_1us \pmod{n_1}$ ya da

b) $ry-sx=n_1$ ve $x\equiv -e_1ur \pmod{n_1}$, $y\equiv -e_1us \pmod{n_1}$

(Akbaş ve Başkan, 1996).

İspat. $\frac{r}{s}\rightarrow\frac{x}{y}\in\Delta_{u,n}$ olsun. Bu durumda $\exists$ T$\in$ $\mathcal{N}or$(N) ö.k.

$$\left(\infty, \frac{u}{n}\right) \xrightarrow{T} \left(\frac{r}{s}, \frac{x}{y}\right) : T(\infty) = \frac{r}{s}\ ,\ T\left(\frac{u}{n}\right) = \frac{x}{y} \text{ dir.}$$

$T(\infty) = \dfrac{ae}{cN} = \dfrac{r}{s}$ ve $T\left(\dfrac{u}{n}\right) = \dfrac{aeu+bn}{cNu+dn} = \dfrac{x}{y}$.

Determinant $ade^2 - bcN = e$ olduğundan $r = a$ ve $s = cN/e$, yani $N/_{e|s}$ elde ederiz.

$\begin{pmatrix} ae & b \\ cN/e & d \end{pmatrix}$ matrisinin determinantı 1 olduğundan

$$(aeu+bn, cNu/e+dn) = 1 .$$

Böylece,

$$\begin{pmatrix} ae & b \\ cN & de \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & n \end{pmatrix} = \begin{pmatrix} ae & aeu+bn \\ cN & cNu+den \end{pmatrix} = \begin{pmatrix} ae & e_n(ae_1u+bn_1) \\ cN & e_ne_1(cNu/e+dn) \end{pmatrix}$$

$$= \begin{pmatrix} (-1)^i er & (-1)^j e_n x \\ (-1)^i es & (-1)^j e_n y \end{pmatrix}$$

burada i, j =0,1, elde edilir. i, j =0 ise

$$ae = er,\ e_n(ae_1u+bn_1) = e_nx,\ cN = es,\ e_ne_1(cNu/e+dn) = e_ny .$$

Buradan $x = ae_1u + bn_1$ ve $y = cNue_1/e + dne_1$, dolayısıyla $x = e_1ur \pmod{n_1}$ ve $y = e_1us \pmod{n_1}$. Determinant alındığında $ry - sx = n_1$ şartının da sağlandığı görülür, böylece (a) gerçeklenir. Benzer şekilde

i=1 ve j=0 için (b)

i=j=-1 için (a)

i=0 ve j=1 için (b)

elde edilir.

Tersine olarak (a) nın sağlandığını kabul edelim. Bu durumda $\exists$ b,d$\in \mathbb{Z}$ ö.k.

$$x = e_1ur + bn_1 \text{ ve } y = e_1us + dne_1$$

Şimdi $\begin{pmatrix} re & b \\ se & de \end{pmatrix} \in \mathcal{N}or(N)$ olduğunu ve ∞' u $\dfrac{r}{s}$ ye, $\dfrac{u}{n}$ yi $\dfrac{x}{y}$ ye resmettiğini gösterelim.

$ry - sx = n_1$ ve $N/_{e|s}$ olduğu göz önüne alındığında $rde^2 - bse = e$ bulunur, bu da yukarıdaki matrisin $\mathcal{N}or(N)$ nin elemanı olduğunu gösterir.

Son olarak $\frac{re}{se}=\frac{r}{s}$ ve $\frac{reu+bn}{seu+den}=\frac{e_n(re_1u+bn_1)}{e_n(se_1u+dn)}=\frac{x}{y}$. Böylece

$$(re_1u+bn_1, se_1u+de_1n)=1.$$

(b) sağlandığında da ispat benzer şekilde yapılır.

Teorem 22. $\Delta_{u,n}$ kendisiyle-eşleşmiştir : $\Leftrightarrow \exists\, e \mid N$ ö.k. $N \mid ne$ ve u^2e =-1(mod n) (Akbaş ve Başkan, 1996).

İspat $\Delta_{u,n}$ kendisiyle-eşleşmiş olsun. Bu durumda $\exists$ T$\in$ $\mathcal{N}or$(N) ö.k.

$$\left(\infty,\frac{u}{n}\right)\xrightarrow{T}\left(\frac{u}{n},\infty\right).$$

$\mathcal{N}or$(N) nin bunu gerçekleyen elemanı T=$\begin{pmatrix} ue & b \\ ne & -ue \end{pmatrix}$, detT=e biçiminde olmak zorundadır.

Buradan da $e \mid N$, $N \mid ne$ ve u^2e =-1(modn) kolayca elde edilir.

Tersine olarak $e \mid N$ ö.k. $N \mid ne$ ve u^2e =-1(modn) olsun. u^2e =-1(modn) olduğundan $\exists\, b \in \mathbb{Z}$ ö.k. $-u^2e$ -bn=1, yani $-u^2e$ $-$bne=e. Bu yüzden

$$\begin{pmatrix} ue & b \\ ne & -ue \end{pmatrix} \in \mathcal{N}or(N)$$

ve istenen koşullar sağlanır.

2.4. N=qp^2 için $\mathcal{N}or$(N) nin Alt Yörüngesel Grafları

Burada q=1 veya q$\in \mathbb{P}$, p≥3 ve p$\in \mathbb{P}$, q≠p olsun. N nin seçiminden ötürü $\mathcal{N}or(N)$ $\hat{\mathbb{Q}}$ üzerinde transitif değildir. Bu durumda amacımız $\mathcal{N}or$(N) nin $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket ettiği maksimal alt kümeyi elde etmektir.

Lemma 8. $\Gamma_0(qp^2)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketinin yörüngeleri;

i) $\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\q\end{pmatrix},\begin{pmatrix}1\\p^2\end{pmatrix},\begin{pmatrix}1\\qp^2\end{pmatrix}$

ii) $\begin{pmatrix}1\\ p\end{pmatrix},\begin{pmatrix}2\\ p\end{pmatrix},\ldots,\begin{pmatrix}p-1\\ p\end{pmatrix}$

iii) $\begin{pmatrix}1\\ qp\end{pmatrix},\begin{pmatrix}t_2\\ qp\end{pmatrix},\ldots,\begin{pmatrix}t_{p-1}\\ qp\end{pmatrix}$

biçimindedir. Burada 1, t_2, …, t_{p-1} lerin herhangi iki tanesi mod p ye göre kongrü değiller ve t_i , i=2, 3, …, p-1 ler $q\nmid i$ veya $q|i$ durumuna göre i ya da p+i ye eşittir.

Lemma 9. $\mathcal{N}or(qp^2)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketinin yörüngeleri, $l\in\{1,2,\ldots,p-1\}$ olmak üzere, aşağıdaki gibidir:

1. a) $q\nmid l$ ve $l\not\equiv p \pmod q$ ise $\begin{pmatrix}l\\ p\end{pmatrix}\cup\begin{pmatrix}p-l\\ p\end{pmatrix}\cup\begin{pmatrix}l\\ qp\end{pmatrix}\cup\begin{pmatrix}p-l\\ qp\end{pmatrix}$

   b) $q\nmid l$ ve $l\equiv p \pmod q$ ise $\begin{pmatrix}l\\ p\end{pmatrix}\cup\begin{pmatrix}p-l\\ p\end{pmatrix}\cup\begin{pmatrix}l\\ qp\end{pmatrix}\cup\begin{pmatrix}2p-l\\ qp\end{pmatrix}$

2. $q|l$ ise $\begin{pmatrix}l\\ p\end{pmatrix}\cup\begin{pmatrix}p-l\\ p\end{pmatrix}\cup\begin{pmatrix}p+l\\ qp\end{pmatrix}\cup\begin{pmatrix}p-l\\ qp\end{pmatrix}$

3. $\begin{pmatrix}1\\ 1\end{pmatrix}\cup\begin{pmatrix}1\\ q\end{pmatrix}\cup\begin{pmatrix}1\\ p^2\end{pmatrix}\cup\begin{pmatrix}1\\ qp^2\end{pmatrix}$.

İspat. Yalnızca (1) i ispatlayalım, diğerleri de benzer şekilde yapılır.

$T=\begin{pmatrix}ae & b\\ qp^2c & de\end{pmatrix}\in\mathcal{N}or(qp^2)$ olsun. Bu durumda e=1, q, p^2, qp^2 olmak zorundadır.

i) e=1 olsun. $T\begin{pmatrix}l\\ p\end{pmatrix}=\begin{pmatrix}a & b\\ qp^2c & d\end{pmatrix}\begin{pmatrix}l\\ p\end{pmatrix}=\dfrac{al+bp}{qp^2cl+dp}$, det=e=1 olduğundan

$$(al+bp,\ qp^2cl+dp)=1.$$

$\begin{pmatrix}al+bp\\ p(qpcl+d)\end{pmatrix}=\begin{pmatrix}x\\ p\end{pmatrix}$ elde edilir, çünkü (qp^2, $p(qpcl+d)$)= p. Buradan

$x\equiv (al+bp)(qpcl+d) \bmod p$ ve $ad-bc(qp^2)=1$ olduğundan $x\equiv l \pmod p$.

ii) e=q olsun. $T\begin{pmatrix}1\\ p\end{pmatrix}=\begin{pmatrix}aq & b\\ qp^2 & dq\end{pmatrix}\begin{pmatrix}l\\ p\end{pmatrix}=\dfrac{qal+bp}{qp^2cl+qdp}$.

$\begin{pmatrix} qa & b \\ qp^2c & d \end{pmatrix}$ nin determinantı 1 olduğundan

$$(\, qa l + bp \,,\, pc l + d \,) = 1.$$

Dolayısıyla $\begin{pmatrix} qa l + bp \\ qp(pc l + d) \end{pmatrix} = \begin{pmatrix} x \\ qp \end{pmatrix}$ elde edilir, çünkü (qp^2, $qp(pcl+d)$)= qp. Buradan

$x \equiv (qal+bp)(pcl+d) \bmod p$ ve determinant kullanıldığında

$$x \equiv l \pmod p.$$

Buna göre $\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} l \\ qp \end{pmatrix}$ aynı yörüngede olmak zorundadır.

iii) $e=p^2$ olsun. $T\begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} ap^2 & b \\ qp^2c & dp^2 \end{pmatrix}\begin{pmatrix} l \\ p \end{pmatrix} = \dfrac{apl + b}{qpcl + dp^2}$.

$\begin{pmatrix} apl + b \\ p(qcl + dp) \end{pmatrix} = \begin{pmatrix} x \\ p \end{pmatrix}$ elde edilir, çünkü (qp^2, $p(qcl+dp)$)= p. Buradan

$x \equiv (apl+b)(qcl+dp) \bmod p$ ve determinant kullanıldığında

$$x \equiv -l \pmod p.$$

Buna göre $\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ p \end{pmatrix}$ aynı yörüngede olmak zorundadır.

iv) $e=qp^2$ olsun. $T\begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} aqp^2 & b \\ qp^2c & dqp^2 \end{pmatrix}\begin{pmatrix} l \\ p \end{pmatrix} = \dfrac{aqpl + b}{qpcl + dqp^2}$.

$\begin{pmatrix} aqpl + b \\ qp(cl + dp) \end{pmatrix} = \begin{pmatrix} x \\ qp \end{pmatrix}$ elde edilir, çünkü (qp^2, $qp(cl+dp)$)= qp. Buradan

$x \equiv (aqpl+b)(cl+dp) \bmod p$ ve determinant kullanıldığında

$$x \equiv -l \pmod p.$$

Buna göre $\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ qp \end{pmatrix}$ aynı yörüngede olmak zorundadır.

Sonuç 1. $\mathcal{N}or(\mathrm{qp}^2)$ nin $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket ettiği maksimal alt küme

$$\hat{\mathbb{Q}}(\mathrm{qp}^2) = \begin{pmatrix}1\\1\end{pmatrix} \cup \begin{pmatrix}1\\\mathrm{q}\end{pmatrix} \cup \begin{pmatrix}1\\\mathrm{p}^2\end{pmatrix} \cup \begin{pmatrix}1\\\mathrm{qp}^2\end{pmatrix} .$$

Şimdi imprimitif hareketi irdeleyelim. $\mathrm{T} = \begin{pmatrix}\mathrm{aq} & \mathrm{b}\\ \mathrm{qp}^2\mathrm{c} & \mathrm{dq}\end{pmatrix}$ elemanını göz önüne alalım ve $N_0 = \langle \Gamma_0(\mathrm{qp}^2), \mathrm{T}\rangle$ ile tanımlayalım. Bu durumda $|\mathcal{N}or(\mathrm{qp}^2) : N_0| = 2$. Diğer taraftan

$$\mathrm{G} = \mathcal{N}or(\mathrm{qp}^2),\ \mathrm{H} = N_0 \text{ ve } \Omega = \hat{\mathbb{Q}}(\mathrm{qp}^2)$$

olarak seçildiğinde,

$$\mathcal{N}or(\mathrm{qp}^2)_\infty < N_0 < \mathcal{N}or(\mathrm{qp}^2)$$

olduğu açıktır.

$\approx$ ile N_0 tarafından $\hat{\mathbb{Q}}(\mathrm{qp}^2)$ üzerine indirgenen $\mathcal{N}$-invaryant eşdeğerlik bağıntısını gösterelim. . İmprimitif hareketin neticesinde oluşan bloklar

$$[0] = \begin{pmatrix}1\\1\end{pmatrix} \cup \begin{pmatrix}1\\\mathrm{q}\end{pmatrix} \quad \text{ve} \quad [\infty] = \begin{pmatrix}1\\\mathrm{p}^2\end{pmatrix} \cup \begin{pmatrix}1\\\mathrm{qp}^2\end{pmatrix}$$

olduğu açıktır.

Teorem 23. $\frac{\mathrm{r}}{\mathrm{s}}, \frac{\mathrm{x}}{\mathrm{y}} \in [\infty]$ olsun. Bu durumda bir $\frac{\mathrm{r}}{\mathrm{s}} \rightarrow \frac{\mathrm{x}}{\mathrm{y}} \in \mathrm{F}_{\mathrm{u},\mathrm{p}^2}$ kenarının olması için gerek ve yeter koşul

(i) $\mathrm{p}^2 | \mathrm{s}$ ve $\mathrm{qp}^2 \nmid \mathrm{s}$ ise a) $\mathrm{x} \equiv \mathrm{qur} (\mathrm{mod}\, \mathrm{p}^2),\ \mathrm{y} \equiv \mathrm{qus} (\mathrm{mod}\, \mathrm{qp}^2),\ \mathrm{ry} - \mathrm{sx} = \mathrm{p}^2$ veya

b) $\mathrm{x} \equiv -\mathrm{qur} (\mathrm{mod}\, \mathrm{p}^2),\ \mathrm{y} \equiv \mathrm{qus} (\mathrm{mod}\, \mathrm{qp}^2),\ \mathrm{ry} - \mathrm{sx} = -\mathrm{p}^2$

(ii) $\mathrm{qp}^2 | s$ ise a) $\mathrm{x} \equiv \mathrm{ur} (\mathrm{mod}\, \mathrm{p}^2),\ \mathrm{y} \equiv \mathrm{us} (\mathrm{mod}\, \mathrm{p}^2),\ \mathrm{ry} - \mathrm{sx} = \mathrm{p}^2$ veya

b) $\mathrm{x} \equiv -\mathrm{ur} (\mathrm{mod}\, \mathrm{p}^2),\ \mathrm{y} \equiv -\mathrm{us} (\mathrm{mod}\, \mathrm{qp}^2),\ \mathrm{ry} - \mathrm{sx} = -\mathrm{p}^2$

olmasıdır.

İspat. $\frac{\mathrm{r}}{\mathrm{s}} \rightarrow \frac{\mathrm{x}}{\mathrm{y}} \in \mathrm{F}_{\mathrm{u},\mathrm{p}^2}$ olsun. (i) $\mathrm{p}^2 | \mathrm{s}$ ve $\mathrm{qp}^2 \nmid \mathrm{s}$ kabul edelim. Bu durumda $\exists$ T$\in$ $\mathcal{N}or(\mathrm{qp}^2)$ ö.k.

$$\left(\infty, \frac{\mathrm{u}}{\mathrm{n}}\right) \xrightarrow{\mathrm{T}} \left(\frac{\mathrm{r}}{\mathrm{s}}, \frac{\mathrm{x}}{\mathrm{y}}\right) : \mathrm{T}(\infty) = \frac{\mathrm{r}}{\mathrm{s}}\ ,\ \mathrm{T}\left(\frac{\mathrm{u}}{\mathrm{p}^2}\right) = \frac{\mathrm{x}}{\mathrm{y}} .$$

$qp^2 \nmid s$ olduğundan $T=\begin{pmatrix} aq & b \\ qp^2c & dq \end{pmatrix}$ biçiminde olmak zorundadır.

$T(\infty)=\dfrac{qa}{qp^2c}=\dfrac{(-1)^i r}{(-1)^i s}$ eşitliğinden $r=(-1)^i a$ ve $s=(-1)^i p^2 c$, i=0,1.

$T\left(\dfrac{u}{p^2}\right)=\dfrac{qau+bp^2}{qp^2cu+qdp^2}=\dfrac{(-1)^j x}{(-1)^j y}$, j=0,1. $\begin{pmatrix} aq & b \\ p^2c & d \end{pmatrix}$ matrisinin determinantı 1,

$$(u, p^2)=1 \text{ ve } (qau+bp^2, q)=1$$

olduğundan

$$(qau+bp^2, qp^2cu+qdp^2)=1.$$

Dolayısıyla $x=(-1)^j(qau+bp^2)$, $y=(-1)^j(qp^2cu+qdp^2)$.

Buradan $x=(-1)^{j+i}qau \pmod{p^2}$ ve $y=(-1)^{j+i}qsu \pmod{p^2}$ elde edilir.

Diğer taraftan i, j=0,1 için

$$\begin{pmatrix} aq & b \\ qp^2c & qd \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix}=\begin{pmatrix} (-1)^i qr & (-1)^i x \\ (-1)^i qs & (-1)^i y \end{pmatrix}.$$

Determinanttan $ry-sx=\pm p^2$ elde edilir. Böylece ispatın (i)-kısmı tamamlanır.

Şimdi $qp^2 | s$ kabul edelim. Bu durumda

$$T=\begin{pmatrix} a & b \\ qp^2c & d \end{pmatrix}, \det T=1$$

biçiminde olmak zorundadır. Bu yüzden $T(\infty)=\dfrac{a}{qp^2c}=\dfrac{(-1)^i r}{(-1)^i s}$ eşitliğinden

$$a=(-1)^i r \text{ ve } qp^2c=(-1)^i s.$$

Benzer şekilde $T\left(\dfrac{u}{p^2}\right)=\dfrac{au+bp^2}{qp^2cu+dp^2}=\dfrac{(-1)^j x}{(-1)^j y}$ ifadesinden

$$x=(-1)^{j+i}ur \pmod{p^2} \text{ ve } y=(-1)^{j+i}us \pmod{p^2}$$

elde edilir. i = j =0 veya 1 ise (ii) a) i=1 ve j=0 veya i=0 ve j=1 durumlarında da (ii) b) elde edilir.

Ters yönlü ispatı yalnızca (i) a) için yapalım, diğerleri de benzer şekildedir. $p^2|s$ ve $qp^2\nmid s$, ayrıca $x\equiv qur(\bmod p^2)$, $y\equiv qus(\bmod qp^2)$, $ry-sx=p^2$ kabul edelim. Bu durumda $\exists$ b,d$\in\mathbb{Z}$ ö.k. $x=qur+bp^2$ ve $y=qsu+qdp^2$. $ry-sx=\pm p^2$ olduğundan $qrd-bs=1$, yani $q^2rd-qbs=q$ elde edilir. Buna göre $T_0=\begin{pmatrix} qr & b \\ qs & qd \end{pmatrix}\in N_0$ ve $T(\infty)=\frac{r}{s}$, $T\left(\frac{u}{p^2}\right)=\frac{x}{y}$ olduğu açıktır.

Lemma 10. $\mathcal{Nor}(qp^2)$ nin F_{u,p^2} alt yörüngesel grafının kenarları $\mathcal{U}$ da kesişmez.

İspat. Genellikten bir şey kaybetmeksizin, $\hat{\mathbb{Q}}(qp^2)$ üzerindeki hareket transitif olduğundan $\infty\to\frac{u}{p^2}$, $\frac{x_1}{y_1p^2}\to\frac{x_2}{y_2p^2}$ ve $\frac{x_1}{y_1p^2}<\frac{u}{p^2}<\frac{x_2}{y_2p^2}$ alabiliriz.

$\frac{x_1}{y_1p^2}\to\frac{x_2}{y_2p^2}$ ve $\frac{x_1}{y_1p^2}<\frac{u}{p^2}<\frac{x_2}{y_2p^2}$ olduğundan

$$x_1y_2-x_2y_1=-1 \text{ ve } \frac{x_1}{y_1}<u<\frac{x_2}{y_2}$$

elde edilir. Buradan $\frac{x_1}{y_1}-\frac{x_2}{y_2}<u-\frac{x_2}{y_2}<0$. Buna göre $\frac{y_2x_1-x_2y_1}{y_1y_2}<\frac{uy_2-x_2}{y_2}<0$.

Dolayısıyla $\frac{-1}{y_1}<uy_2-x_2<0$, bu ise bir çelişkidir.

Teorem 24. $\mathcal{Nor}(qp^2)$ nin F_{u,p^2} alt yörüngesel grafının bir dörtgen içermesi için gerek ve yeter şart q=2 ve $2u^2\pm 2u+1\equiv 0 \ (\bmod p^2)$ olmasıdır.

İspat. F_{u,p^2} nin bir $\frac{k_0}{l_0}\to\frac{m_0}{n_0}\to\frac{s_0}{t_0}\to\frac{x_0}{y_0}\to\frac{k_0}{l_0}$ dörtgeni içerdiğini kabul edelim. N_0 F_{u,p^2} nin kenar ve köşelerini transitif olarak permüte ettiğinden, verilen dörtgeni N_0 altında $\frac{1}{0}\to\frac{m}{p^2}\to\frac{x}{y}\to\frac{k}{l}\to\frac{1}{0}$ dörtgenine resmedebiliriz. Üstelik genellikten bir şey kaybetmeden $\frac{m}{p^2}<\frac{x}{y}<\frac{k}{l}$ farzedebiliriz. Burada sürekli bir önceki teoremi kullanacağız. $\frac{k}{l}\rightarrow\frac{1}{0}$ dan $l = p^2$ elde edilir. $\frac{1}{0}\rightarrow\frac{m}{p^2}$ den $m \equiv u \pmod{p^2}$. $\frac{m}{p^2}\rightarrow\frac{x}{y}$ den

$$x \equiv -qmu \pmod{p^2}\ ,\ \ y \equiv -qmu \pmod{qp^2}\ \text{ ve } my - p^2x = -p^2$$

Dolayısıyla $\exists\ y_1 \in \mathbb{Z}$ ö.k. $y = qp^2 y_1$, ve $x \equiv -qu^2 \pmod{p^2}$. Üstelik,

$$mq\,y_1 - x = -1 \tag{3}$$

$\frac{k}{l}\rightarrow\frac{1}{0}$ kenarından,

$$quk \equiv -1 \pmod{p^2} \tag{4}$$

(3) kullanıldığında ve $\frac{x}{qp^2y_1}\rightarrow\frac{k}{p^2}$ kenarından

$$k \equiv -u\,(\,mq\,y_1+1\,) \pmod{p^2}\ \text{ ve } (mq\,y_1+1\,) - q\,y_1\,k = -1 \tag{5}$$

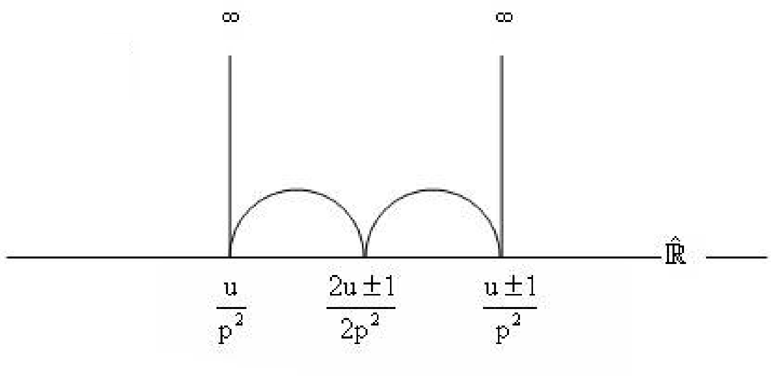
Bu durumda

$$q\,y_1\ (m-k) = -2 \tag{6}$$

Sonuç olarak q=1 veya q=2 . q=1 ise $y_1 = 1$ veya 2, $m-k = -1, -2$. $y_1 = 1$ ise $k = m+2$. (5) kullanıldığında $m+2 = -u\,(\,m+1\,) \pmod{p^2}$. Dolayısıyla $u^2 + 2u + 2 \equiv 0 \pmod{p^2}$. (4) kullanıldığında $u\,(\,m+2\,)+1 \equiv 0 \pmod{p^2}$ veya $u^2 + 2u + 1 \equiv 0 \pmod{p^2}$. Buradan $1 \equiv 0 \pmod{p^2}$ çelişkisi elde edilir.

Şimdi $y_1 = 2$ olsun. Bu durumda $m-k = -1$, yani $k = m+1$. (4) den $u^2 + u + 1 \equiv 0 \pmod{p^2}$. (3) den $x = 1+2m$. $x \equiv -qu^2 \pmod{p^2}$ olduğundan $2m+1 \equiv -u^2 \pmod{p^2}$ veya $u^2 + 2u + 1 \equiv 0 \pmod{p^2}$. Böylece $u^2 + u + 1 \equiv 0 \pmod{p^2}$ ile birlikte $u \equiv 0 \pmod{p^2}$ çelişkisi elde edilir. Sonuç olarak q=2, dolayısıyla da $y_1 = 1$ olmak zorundadır. $x \equiv -qu^2 \pmod{p^2}$ ve $mq\,y_1 - x = -1$ den $2u^2 + 2u + 1 \equiv 0 \pmod{p^2}$ elde edilir.

$\frac{m}{p^2}>\frac{x}{y}>\frac{k}{l}$ eşitsizliğinde $2u^2 - 2u + 1 \equiv 0 \pmod{p^2}$ elde edilir.



Şekil 4. $\mathcal{N}or$(N) deki H-Dörtgen

Tersine olarak q=2 ve $2u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$ farzedelim. Bu durumda bir önceki teoremden

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{2u \pm 1}{2p^2} \rightarrow \frac{u \pm 1}{p^2} \rightarrow \frac{1}{0}$$

devresinin F_{u,p^2} de bir dörtgen olduğu görülür.

Teorem 25. $\mathcal{N}or(qp^2)$ nin F_{u,p^2} alt yörüngesel grafının bir altıgen içermesi için gerek ve yeter şart q=3 ve $3u^2 \pm 3u + 1 \equiv 0 \pmod{p^2}$ olmasıdır.

İspat. Bir önceki teoremden görüldüğü üzere bu altıgen

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \underset{<}{\rightarrow} \frac{x_1}{qy_1p^2} \underset{<}{\rightarrow} \frac{x_2}{y_3p^2} \underset{<}{\rightarrow} \frac{x_3}{qy_3p^2} \underset{<}{\rightarrow} \frac{x_4}{p^2} \rightarrow \frac{1}{0} \tag{7}$$

biçiminde seçilebilir. Buradaki tüm harfler pozitif tamsayıdır. İkinci kenardan $x_1 \equiv -qu^2 \pmod{p^2}$ ve $x_1 = qu\,y_1 + 1$ elde edilir. Buradan

$$qu^2 + qu\,y_1 + 1 \equiv 0 \pmod{p^2} \tag{8}$$

denklemini elde edeceğiz. Altıncı kenardan $x_4 \equiv u + y_1 \pmod{p^2}$ olduğu açıktır. Devremiz periyodik ve periyodu da 1 olduğundan, her bir kenara 1 eklenmesi durumunda $0 < y_1 \leq p^2$ olmak zorundadır. Aksi halde Lemma 10 gereği y_1, y_2, y_3 ler den birisi 0 olmak zorunda ki bu çelişkidir. (7) den

$$T = \begin{pmatrix} -qu & \frac{qu^2+quy_1+1}{p^2} \\ qp^2 & qu+qy_1 \end{pmatrix} \in N_0$$

Buradan $\dfrac{x_1}{qy_1p^2} = \dfrac{quy_1+1}{qy_1p^2} = T^2\begin{pmatrix}1\\0\end{pmatrix}$ olduğu hemen çıkar. Sonraki adımda $\dfrac{x_2}{y_2p^2} = T^3\begin{pmatrix}1\\0\end{pmatrix}$ olduğunu gösterelim. Bunun için öncelikle $\dfrac{x_2}{y_2p^2} \le T^3\begin{pmatrix}1\\0\end{pmatrix}$ olduğunu göstermeliyiz. Aksi halde $\dfrac{x_2}{y_2p^2} < T^3\begin{pmatrix}1\\0\end{pmatrix}$ olur, öyle kabul edelim, yani $\dfrac{u(qy_1^2-1)+y_1}{p^2(qy_1^2-1)} < \dfrac{x_2}{y_2p^2}$. Dolayısıyla

$$u\,y_2\,(q\,y_1^{\,2}-1) + y_1\,y_2 < x_2(q\,y_1^{\,2}-1) \tag{9}$$

elde edilir. $\dfrac{quy_1+1}{qy_1p^2} \rightarrow \dfrac{x_2}{y_2p^2}$ ve $\dfrac{u}{p^2} < \dfrac{x_2}{y_2p^2}$ olduğundan, Teorem 11 kullanıldığında

$qu\,y_1^{\,2}\;y_2 + y_1\,y_2 = q\,x_2\,y_1^{\,2} - y_2$ ve $-u\,y_2 > -\,x_2$ elde edilir. (9) dan

$qu\,y_1^{\,2}\;y_2 - uy_2 + y_1\,y_2 < q\,x_2\,y_1^{\,2} - u\,y_2$. Buna göre $-y_1 + y_1\,y_2 < 0$, bu bir çelişkidir. Bu yüzden $\dfrac{x_2}{y_2p^2} \le T^3\begin{pmatrix}1\\0\end{pmatrix}$. Bu durumda altıgenin bir köşesi $T^3\begin{pmatrix}1\\0\end{pmatrix}$ olmalıdır, aksi halde Lemma 13 ile bir çelişki elde edilir. Bu yüzden eşitliğin sağlanmadığı durumda,

$T^3\begin{pmatrix}1\\0\end{pmatrix} = \dfrac{x_4}{p^2}\left(= \dfrac{u+y_1}{p^2}\right.$ bu da çelişki) olur. Sonuç olarak $\dfrac{x_2}{y_2p^2} = T^3\begin{pmatrix}1\\0\end{pmatrix}$.

Şimdi son olarak

$$\frac{x_3}{qy_2p^2} = T^4\begin{pmatrix}1\\0\end{pmatrix} = \frac{quy_1(qy_1^2-2)+qy_1^2-1}{qp^2y_1(qy_1^2-2)}$$

eşitliğini elde edelim. Yukarıda olduğu gibi $\dfrac{x_3}{qy_3p^2} > T^4\begin{pmatrix}1\\0\end{pmatrix}$ olsun. Buradan

$$quy_3y_1(qy_1^2-2) + qy_1^2y_3 - y_3 < x_3y_1(qy_1^2-2) \tag{10}$$

$\dfrac{u(qy_1^2-1)+y_1}{p^2(qy_1^2-1)} \rightarrow \dfrac{x_3}{qy_3p^2}$ olduğundan, Teorem 22 den

$$x_3y_1(qy_1^2-1) = y_1 + qy_1^2y_3 + quy_1y_3(qy_1^2-1) \tag{11}$$

Bunu (10) da yerine yazdığımızda

$$y_1\,(x_3 - quy_3) < y_1 + y_3 \tag{12}$$

$\dfrac{x_3}{qy_3p^2} \to \dfrac{u+y_1}{p^2}$ olduğundan,

$$x_3 = quy_3 + qy_1y_3 - 1 \qquad (13)$$

Bu durumda (12) den

$$qy_1^{\,2}y_3 < 2y_1 + y_3 \qquad (14)$$

eşitsizliği elde edilir. Diğer taraftan Teorem 22 ile altıgenden aşağıdaki beş kongrüans denklemi elde edilir,

$$x_1 \equiv -qu^2 (\mathrm{mod}\, p^2)$$

$$x_2 \equiv -ux_1 (\mathrm{mod}\, p^2)$$

$$x_3 \equiv -qux_2 (\mathrm{mod}\, p^2)$$

$$x_4 \equiv -ux_3 (\mathrm{mod}\, p^2)$$

$$1 \equiv -qux_4 (\mathrm{mod}\, p^2)$$

Bu kongrüanslardan $q^3u^6+1 \equiv 0(\mathrm{mod}\ p^2)$ sonucu kolayca çıkar. Bu ve (8) deki kongrüanstan

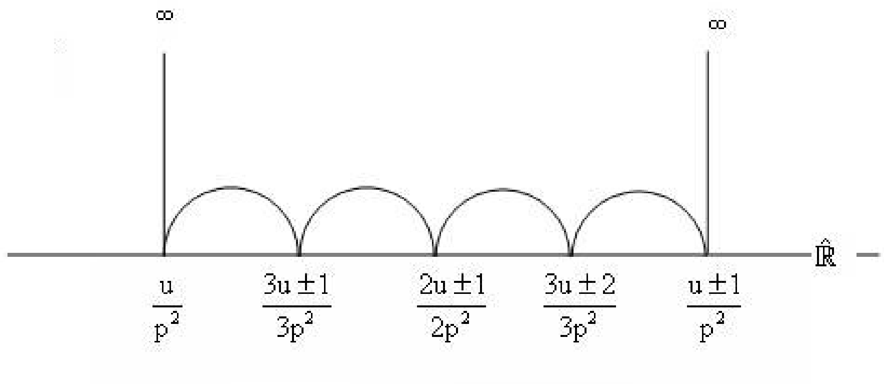
$$y_1(qy_1^{\,2} - 1) \equiv 0(\mathrm{mod}\ p^2) \qquad (15)$$

Şimdi (14) e geri dönelim. Bu eşitsizlik yalnızca $qy_1^{\,2} = 2$, 3 veya 4 için sağlanır. Ancak (15) kongrüansı bir çelişki doğurur. Bu yüzden $\dfrac{x_3}{qy_3p^2} \le T^4\begin{pmatrix}\frac{1}{0}\end{pmatrix}$. Yukarıda olduğu gibi $T^4\begin{pmatrix}\frac{1}{0}\end{pmatrix}$ altıgende bir köşe olmak zorundadır. Böylece $T^4\begin{pmatrix}\frac{1}{0}\end{pmatrix} = \dfrac{x_3}{qy_3p^2} \vee \dfrac{x_4}{p^2} \vee \dfrac{1}{0}$.

$T^4\begin{pmatrix}\frac{1}{0}\end{pmatrix} = \dfrac{quy_1(qy_1^{\,2}-2)+qy_1^{\,2}-1}{qp^2y_1(qy_1^{\,2}-2)} = \dfrac{x_4}{p^2} = \dfrac{u+y_1}{p^2}$ ise $qy_1(qy_1^{\,2}-2)=1$, bu bir çelişkidir. $T^4\begin{pmatrix}\frac{1}{0}\end{pmatrix} = \dfrac{1}{0}$ ise $qy_1^{\,2}-2 = 0$. Ancak bu (15) ile çelişir. Bu yüzden $T^4\begin{pmatrix}\frac{1}{0}\end{pmatrix} = \dfrac{x_3}{qy_3p^2}$.

Dolayısıyla $T^4\begin{pmatrix}\frac{1}{0}\end{pmatrix} = \dfrac{quy_1(qy_1^{\,2}-2)+qy_1^{\,2}-1}{qp^2y_1(qy_1^{\,2}-2)} \to \dfrac{x_4}{p^2} = \dfrac{u+y_1}{p^2}$ elde edilir. Buradan

$quy_1(qy_1^{\,2}-2)+qy_1^{\,2}-1-(u+y_1)qy_1(qy_1^{\,2}-2) = -1$. Bu eşitlikten de $qy_1^{\,2}(3-qy_1^{\,2}) = 0$ elde edilir. Bu $q=3$ ve $y_1=1$ neticesini verir. Dolayısıyla sonuçta $q=3$ ve $3u^2 + 3u + 1 \equiv 0$ $(\mathrm{mod}\ p^2)$ elde edilir. Eğer devre azalan alınsaydı, $q=3$ ve $3u^2-3u + 1 \equiv 0(\mathrm{mod} p^2)$ sonucu bulunacaktı.



Şekil 5. $\mathcal{N}or$(N) deki H-Altıgen

Tersine olarak $3u^2 \pm 3u + 1 \equiv 0 (\mathrm{mod}\ p^2)$ olsun. Bu durumda Teorem 22 den

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{3u \pm 1}{3p^2} \rightarrow \frac{2u \pm 1}{2p^2} \rightarrow \frac{3u \pm 2}{3p^2} \rightarrow \frac{u \pm 1}{p^2} \rightarrow \frac{1}{0} \tag{16}$$

devresinin F_{u,p^2} de bir altıgen olduğu görülür. ■

2.5. $N=2^2p^2$ ($h \neq 1$) için $\mathcal{N}or$(N) nin Alt Yörüngesel Grafları

Burada $N = 2^2p^2$ alınırsa , $h = 2^{\min\{3, [\alpha/2]\}} 3^{\min\{1,[\beta/2]\}} = 2$ olduğundan ve

$\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix}$, $e \| N/h^2$ göz önüne alınırsa det = e =1, p^2 olabilir. Yani; normalliyenin elemanları

$$\begin{pmatrix} a & b/2 \\ 2p^2c & d \end{pmatrix}, \ \det=1 \quad \text{ve} \quad \begin{pmatrix} ap^2 & b/2 \\ 2p^2c & dp^2 \end{pmatrix}, \ \det=p^2$$

olabilir. Ayrıca N nin seçiminden ötürü $\mathcal{N}or$(N) $\hat{\mathbb{Q}}$ üzerinde transitif değildir.

Lemma 11. $\Gamma_0(2^2p^2)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketinin yörüngeleri;

(i) $\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \begin{pmatrix} 1 \\ 2^2 \end{pmatrix}; \begin{pmatrix} 1 \\ p^2 \end{pmatrix}; \begin{pmatrix} 1 \\ 2^2p^2 \end{pmatrix}; \begin{pmatrix} 1 \\ 2 \end{pmatrix}; \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix}$

(ii) $\begin{pmatrix}1\\p\end{pmatrix},\begin{pmatrix}2\\p\end{pmatrix},\ldots,\begin{pmatrix}p-1\\p\end{pmatrix}$

(iii) $\begin{pmatrix}1\\2p\end{pmatrix},\begin{pmatrix}p+2\\2p\end{pmatrix},\begin{pmatrix}3\\2p\end{pmatrix},\begin{pmatrix}p+4\\2p\end{pmatrix},\ldots,\begin{pmatrix}2p-1\\2p\end{pmatrix}$

(iv) $\begin{pmatrix}1\\2^2p\end{pmatrix},\begin{pmatrix}p+2\\2^2p\end{pmatrix},\begin{pmatrix}3\\2^2p\end{pmatrix},\begin{pmatrix}p+4\\2^2p\end{pmatrix},\ldots,\begin{pmatrix}2p-1\\2^2p\end{pmatrix}$.

Teorem 26. $\mathcal{N}or(2^2p^2)$ nin $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket ettiği maksimal alt kümelerden biri

$$\hat{\mathbb{Q}}(2^2p^2)=\begin{pmatrix}1\\1\end{pmatrix}\cup\begin{pmatrix}1\\2\end{pmatrix}\cup\begin{pmatrix}1\\2^2\end{pmatrix}\cup\begin{pmatrix}1\\p^2\end{pmatrix}\cup\begin{pmatrix}1\\2p^2\end{pmatrix}\cup\begin{pmatrix}1\\2^2p^2\end{pmatrix} \text{ dir.}$$

İspat. Yapılması gereken $\begin{pmatrix}1\\1\end{pmatrix}$-yörüngesinin $\mathcal{N}or(2^2p^2)$ ile hareketini incelemektir. $\begin{pmatrix}a & b/2\\2p^2c & d\end{pmatrix}$, det=1 elemanı göz önüne alındığında:

$\begin{pmatrix}a & b/2\\2p^2c & d\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}a+b/2\\2p^2c+d\end{pmatrix}=\begin{pmatrix}2a+b\\2(2p^2c+d)\end{pmatrix}$ elemanını E ile gösterelim, elde edilir.

(i) b-tek ve d-tek olduğunda, açıkça E$\in\begin{pmatrix}1\\2\end{pmatrix}$, dolayısıyla $\begin{pmatrix}1\\1\end{pmatrix}\cup\begin{pmatrix}1\\2\end{pmatrix}$

(ii) b-tek ve d-çift olduğunda, $E_0=\begin{pmatrix}2a+b\\2^2(p^2c+d_0)\end{pmatrix}\in\begin{pmatrix}1\\2^2\end{pmatrix}$, dolayısıyla

$$\begin{pmatrix}1\\1\end{pmatrix}\cup\begin{pmatrix}1\\2\end{pmatrix}\cup\begin{pmatrix}1\\2^2\end{pmatrix}$$

$\begin{pmatrix}ap^2 & b/2\\2p^2c & dp^2\end{pmatrix}$, det=$p^2$ elemanı göz önüne alındığında:

$\begin{pmatrix}ap^2 & b/2\\2p^2c & dp^2\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}2ap^2+b\\2p^2(2c+d)\end{pmatrix}$ elemanını D ile gösterelim, elde edilir.

(iii)b-tek ve d-tek olduğunda, açıkça D$\in\begin{pmatrix}1\\2p^2\end{pmatrix}$, dolayısıyla $\begin{pmatrix}1\\1\end{pmatrix}\cup\begin{pmatrix}1\\2\end{pmatrix}\cup\begin{pmatrix}1\\2^2\end{pmatrix}\cup\begin{pmatrix}1\\2p^2\end{pmatrix}$

(iv) b-çift ve d-tek olduğunda, $D=\begin{pmatrix} ap^2+b_0 \\ p^2(2c+d) \end{pmatrix} \in \begin{pmatrix} 1 \\ p^2 \end{pmatrix}$, dolayısıyla

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

(v) b-tek ve d-çift olduğunda, $D=\begin{pmatrix} ap^2+b_0 \\ 2^2p^2(c+d_0) \end{pmatrix} \in \begin{pmatrix} 1 \\ 2^2p^2 \end{pmatrix}$, dolayısıyla

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

Şimdi imprimitif hareketi irdeleyelim;

$$G_\infty = \mathcal{N}or_\infty(2^2p^2) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \quad \text{ve} \quad \Omega = \hat{\mathbb{Q}}(2^2p^2)$$

$$H = N_0(2^2p^2) = \left\langle \left\{ \Gamma_0(2^2p^2), \underbrace{\begin{pmatrix} a & b/2 \\ 2p^2c & d \end{pmatrix}}_{A}, \underbrace{\begin{pmatrix} ap^2 & b \\ 2^2p^2c & dp^2 \end{pmatrix}}_{B} \right\} \right\rangle$$

$$G = \mathcal{N}or(2^2p^2)$$

olarak tanımlandığında

$$\mathcal{N}or_\infty(2^2p^2) < N_0(2^2p^2) < \mathcal{N}or(2^2p^2)$$

olduğu açıktır.

Burada $A^3=I \Leftrightarrow a+d=\pm 1$ ve $B^2=I$ dır. Dolayısıyla

$$\left|\mathcal{N}or(2^2p^2):\Gamma_0(2^2p^2)\right| = 12 \quad \text{ve} \quad \left|N_0(2^2p^2):\Gamma_0(2^2p^2)\right| = 6$$

olduğundan $\left|\mathcal{N}or(2^2p^2):N_0(2^2p^2)\right| = 2$ olarak elde edilir.

Açıkça $\mathcal{N}or(2^2p^2) = N_0(2^2p^2) \cup \begin{pmatrix} 2^2p^2a & b \\ 2^2p^2c & 2^2p^2d \end{pmatrix} N_0(2^2p^2)$ biçimindedir.

$\approx$ ile $N_0(2^2p^2)$ tarafından $\hat{\mathbb{Q}}(2^2p^2)$ üzerine indirgenen $\mathcal{N}$-invaryant eşdeğerlik bağıntısını gösterelim. . İmprimitif hareketin neticesinde

$$[\infty]=\begin{pmatrix}1\\2^2\end{pmatrix}\cup\begin{pmatrix}1\\p^2\end{pmatrix}\cup\begin{pmatrix}1\\2p^2\end{pmatrix}\cup\begin{pmatrix}1\\2^2p^2\end{pmatrix} \quad \text{ve} \quad [0]=\begin{pmatrix}1\\1\end{pmatrix}\cup\begin{pmatrix}1\\2\end{pmatrix}$$

blokları elde edilir.

Teorem 27. $\frac{r}{s},\frac{x}{y}\in[\infty]$ olsun. Bu durumda bir $\frac{r}{s}\to\frac{x}{y}\in F_{u,p^2}$ kenarı vardır $\Leftrightarrow$

(i) $2^2p^2|\,s$ ise $x\equiv\pm\,ur \pmod{p^2}$, $y\equiv\pm\,us \pmod{p^2}$ ve $ry-sx=\pm p^2$

(ii) $2p^2|\,s$ ise $x\equiv\pm\,2ur \pmod{p^2}$, $y\equiv\pm\,2us \pmod{p^2}$ ve $ry-sx=\pm\,2p^2$

(iii) $p^2|\,s$ ise $x\equiv\pm\,4ur \pmod{p^2}$, $y\equiv\pm\,4us \pmod{p^2}$ ve $ry-sx=\pm p^2$

(iv) $2^2|\,s$ ise $x=ur+b : b\in\mathbb{Z}$, $y\equiv\pm\,us \pmod{p^2}$ ve $ry-sx=\pm\,1$

İspat. "Gerek Şart": $\frac{r}{s}\to\frac{x}{y}\in F_{u,p^2}$ olduğundan

$$\exists\, T\in \mathcal{Nor}(2^2p^2) \text{ ö.k. } \left(\infty,\frac{u}{p^2}\right)\xrightarrow{T}\left(\frac{r}{s},\frac{x}{y}\right) : T(\infty)=\frac{r}{s}\,,\; T\left(\frac{u}{p^2}\right)=\frac{x}{y} \text{ dir.}$$

(i) $2^2p^2|\,s$ ise T=$\begin{pmatrix}a & b\\ 2^2p^2c & d\end{pmatrix}$ olmak zorundadır. $ad-2^2p^2bc=1$ olduğundan a-çift olamaz.

$$T(\infty)=\frac{a}{2^2p^2c}=\frac{r}{s} \;\Rightarrow\; r=a \quad , \quad s=2^2p^2c$$

$$T\left(\frac{u}{p^2}\right)=\frac{au+bp^2}{2^2p^2cu+dp^2}=\frac{x}{y} \;\Rightarrow\; x\equiv\pm ur \pmod{p^2} \quad , \quad y\equiv\pm us \pmod{p^2}$$

Ayrıca $\begin{pmatrix}a & b\\ 2^2p^2c & d\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & p^2\end{pmatrix}=\begin{pmatrix}a & au+bp^2\\ 2^2p^2c & 2^2p^2cu+dp^2\end{pmatrix}$ matrisinin yukarıdaki eşitliklerle beraber $\begin{pmatrix}r & x\\ s & y\end{pmatrix}$ ve $ry-sx=\pm p^2$ olduğu açıktır.

(ii) $2p^2|\,s$ ise T=$\begin{pmatrix}a & b/2\\ 2p^2c & d\end{pmatrix}$ ve ($ad-p^2bc=1$ olduğundan a tek ya da çift olabilir) a-tek olmak zorundadır.

$$T(\infty)=\frac{a}{2p^2c}=\frac{r}{s} \;\Rightarrow\; r=a \quad , \quad s=2p^2c$$

$$T\left(\frac{u}{p^2}\right)=\frac{2au+bp^2}{2^2p^2cu+2dp^2}=\frac{x}{y} \;\Rightarrow\; x\equiv\pm 2ur \pmod{p^2} \quad , \quad y\equiv\pm 2us \pmod{p^2}$$

Ayrıca $\begin{pmatrix} a & b \\ 2^2p^2c & d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix}=\begin{pmatrix} a & au+bp^2/2 \\ 2p^2c & 2p^2cu+dp^2 \end{pmatrix}$ matrisinin her elemanı 2 ile

çarpıldığında $\begin{pmatrix} 2a & 2au+bp^2 \\ 2^2p^2c & 2^2p^2cu+2dp^2 \end{pmatrix}$ matrisinin determinantının yukarıdaki eşitliklerle

beraber değerlendirildiğinde ry–sx=$\pm\, 2p^2$ olduğu görülür.

(iii) $p^2|\, s$ ise **T=**$\begin{pmatrix} a & b/2 \\ 2p^2c & d \end{pmatrix}$ ve a-çift olmak zorundadır.

$$T(\infty)=\frac{a}{2p^2c}=\frac{a_0}{p^2c}=\frac{r}{s} \Rightarrow r=a_0 \quad , \quad s=p^2c$$

$$T\left(\frac{u}{p^2}\right)= \frac{2au+bp^2}{2^2p^2cu+2dp^2}=\frac{x}{y} \Rightarrow x\equiv \pm 4ur(\mathrm{mod}\, p^2) \quad , \quad y\equiv \pm 4us(\mathrm{mod}\, p^2)$$

Ayrıca $\begin{pmatrix} a & b \\ 2^2p^2c & d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix}=\begin{pmatrix} a & au+bp^2/2 \\ 2p^2c & 2p^2cu+dp^2 \end{pmatrix}$ matrisinin her elemanı 2 ile

çarpıldığında$\begin{pmatrix} 2a & 2au+bp^2 \\ 2^2p^2c & 2^2p^2cu+2dp^2 \end{pmatrix}$ matrisinin determinantının yukarıdaki eşitliklerle

beraber değerlendirildiğinde ry–sx= $\pm\, p^2$ olduğu görülür.

(iv) $2^2|\, s$ ise T=$\begin{pmatrix} ap^2 & b \\ 2^2p^2c & dp^2 \end{pmatrix}$ olmak zorundadır.

$ad-2^2p^2bc= p^2$ olduğundan a-çift olamaz.

$$T(\infty)=\frac{ap^2}{2^2p^2c}=\frac{r}{s} \Rightarrow r=a \quad , \quad s=2^2c$$

$$T\left(\frac{u}{p^2}\right)= \frac{au+b}{2^2cu+dp^2}=\frac{x}{y} \Rightarrow x=\pm ur+b \quad , \quad y\equiv \pm us(\mathrm{mod}\, p^2)$$

Ayrıca $\begin{pmatrix} ap & b/p \\ 2^2pc & dp \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix}=\begin{pmatrix} ap & aup+bp \\ 2^2pc & 2^2pcu+dp^3 \end{pmatrix}$ matrisinin her elemanı p ile

böländüğünde $\begin{pmatrix} a & au+b \\ 2^2c & 2^2cu+dp^2 \end{pmatrix}$ matrisinin determinantının yukarıdaki eşitliklerle

beraber değerlendirildiğinde ry–sx=±1 olduğu görülür.

"Yeter Şart":

(i) $2^2p^2|$ s ise $x \equiv \pm ur \pmod{p^2}$, $y \equiv \pm us \pmod{p^2}$ ve $ry-sx = \pm p^2$ olsun. Bu durumda

$\exists$ b,d$\in \mathbb{Z}$ öyleki $x = ur + bp^2$ ve $y = us + dp^2$ dir. Bu eşitlikler determinantta yerine konulduğunda

$$r(us + bp^2) - s(ur + dp^2) = rdp^2 - bsp^2 = p^2$$

elde edilir. Buna göre

$T_0 := \begin{pmatrix} r & b \\ s & d \end{pmatrix}$, $\det T_0 = 1$ ve $2^2p^2|$ s yani $N|s$ olduğu göz önüne alındığında

$$T_0 \in \Gamma_0(2^2p^2) \subset N_0(2^2p^2) \text{ dir.}$$

(ii) $2p^2|$ s ise $x \equiv \pm 2ur \pmod{p^2}$, $y \equiv \pm 2us \pmod{p^2}$ ve $ry-sx = \pm 2p^2$ olsun. Bu durumda

$\exists$ b,d$\in \mathbb{Z}$ öyleki $x = 2ur + bp^2$ ve $y = 2us + dp^2$ dir. Bu eşitlikler determinantta yerine konulduğunda

$$r(2us + bp^2) - s(2ur + dp^2) = rdp^2 - bsp^2 = 2p^2$$

eşitliğinin her iki tarafı $2p^2$ ile bölündüğünde $rd/2 - bs/2 = 1$. Buna göre

$$T_0 := \begin{pmatrix} r & b/2 \\ s & d/2 \end{pmatrix}, \ \det T_0 = 1 \text{ ve } 2p^2| \text{ s}$$

olduğundan $N_0(2^2p^2)$ nin A-formundaki bir elemanıdır.

(iii) $p^2|$ s ise $x \equiv \pm 4ur \pmod{p^2}$, $y \equiv \pm 4us \pmod{p^2}$ ve $ry-sx = \pm p^2$ olsun. Bu durumda

$\exists$ b,d$\in \mathbb{Z}$ öyleki $x = 4ur + bp^2$ ve $y = 4us + dp^2$ dir. Bu eşitlikler determinantta yerine konulduğunda

$$r(4us + bp^2) - s(4ur + dp^2) = rdp^2 - bsp^2 = p^2$$

elde edilir. Buna göre

$$T_0 := \begin{pmatrix} r & b/2 \\ 2s & d \end{pmatrix}, \ \det T_0 = 1 \text{ ve } 2p^2| \text{ s}$$

olduğundan $N_0(2^2p^2)$ nin A-formundaki bir elemanıdır.

(iv) $2^2|$ s ise x =ur+b : b$\in \mathbb{Z}$, $y \equiv \pm us \pmod{p^2}$ ve $ry-sx = \pm 1$ olsun. Bu durumda

$\exists$ d$\in \mathbb{Z}$ öyleki $y = us + dp^2$ dir. Bu eşitlikler determinantta yerine konulduğunda

$$r(us+dp^2)-s(ur+b)=rdp^2-bs=1$$

eşitliğinin her iki tarafı p^2 ile çarpıldığında $rdp^4-bsp^2=p^2$. Buna göre

$$T_0:=\begin{pmatrix} rp^2 & b \\ sp^2 & dp^2 \end{pmatrix},\ \det T_0=p^2 \quad \text{ve} \quad 2^2 \mid s$$

olduğundan $N_0(2^2p^2)$ nin B-formundaki bir elemanıdır. ■

Teorem 28. $\mathcal{N}or$(N) nin F_{u,p^2} alt yörüngesel grafının bir üçgen içermesi için gerek ve yeter koşul $4u^2 \pm 2u+1 \equiv 0 (\mathrm{mod}\ p^2)$ olmasıdır.

İspat. ″⇒″ $\hat{\mathbb{Q}}(2^2p^2)$ üzerindeki hareket transitif olduğundan, genellikten bir şey kaybetmeden devreyi

$$\infty \to \frac{w}{x} \to \frac{y}{z} \to \infty$$

biçiminde kabul edebiliriz. Teorem 26 (i)'den $w \equiv \pm u\ (\mathrm{mod}\ p^2)$, $x \equiv \pm k\, p^2 : k \in \mathbb{Z}$ ve $ry-sx=\pm p^2$, dolayısıyla $x=p^2$ dir.

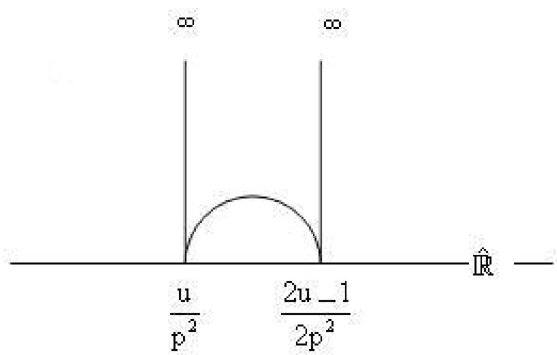
$$\frac{1}{0} \to \frac{u}{p^2} \to \frac{y}{z} \to \frac{1}{0}$$

Teorem 26 dan $ry-sx=\pm 1, \pm p^2, \pm 2p^2$, dolayısıyla $z=\pm 1, \pm p^2, \pm 2p^2$ olabilir.

(i) $z=1$ ise 2. kenardan Teorem 26 (iii) gereği $u-yp^2=\pm p^2$, ancak $(u, p^2)=1$ olduğundan bu bir çelişkidir.

(ii) $z=p^2$ ise 2. kenardan Teorem 26 (iii) gereği $up^2-yp^2=\pm p^2$ yani $y=u-1$, ayrıca $y \equiv \pm 4u^2\ (\mathrm{mod} p^2)$ olduğundan $4u^2 \pm u+1 \equiv 0 (\mathrm{mod}\ p^2)$ bağıntısı elde edilir. Bu ise 3. kenardan Teorem 26(iii) ile elde edilen $1 \equiv \pm 4u(u-1)(\mathrm{mod} p^2)$
yani $4u^2 \pm 4u+1 \equiv 0 (\mathrm{mod}\ p^2)$ bağıntısıyla çelişir.

(iii) $z=2p^2$ ise 2. kenardan Teorem 26 (iii) gereği $2up^2-yp^2=\pm p^2$ yani $y=2u-1$, ayrıca $y \equiv \pm 4u^2\ (\mathrm{mod} p^2)$ olduğundan $4u^2 \pm u+1 \equiv 0 (\mathrm{mod}\ p^2)$ bağıntısı elde edilir.Bu bağıntı 3. kenardan Teorem 26(iii) ile elde edilen $1 \equiv \pm 2u(2u-1)(\mathrm{mod} p^2)$ denklemiyle de örtüşür.



Şekil 6. $\mathcal{N}or$(N) deki H-Üçgen

″⇐″ $4u^2 \pm 2u + 1 \equiv 0 (\text{mod } p^2)$ olsun. Bu durumda Teorem 26 kullanıldığında

$$\frac{1}{0} \to \frac{u}{p^2} \to \frac{2u-1}{2p^2} \to \frac{1}{0}$$

F_{u,p^2} alt yörüngesel grafında bir üçgendir ■

3. İRDELEME

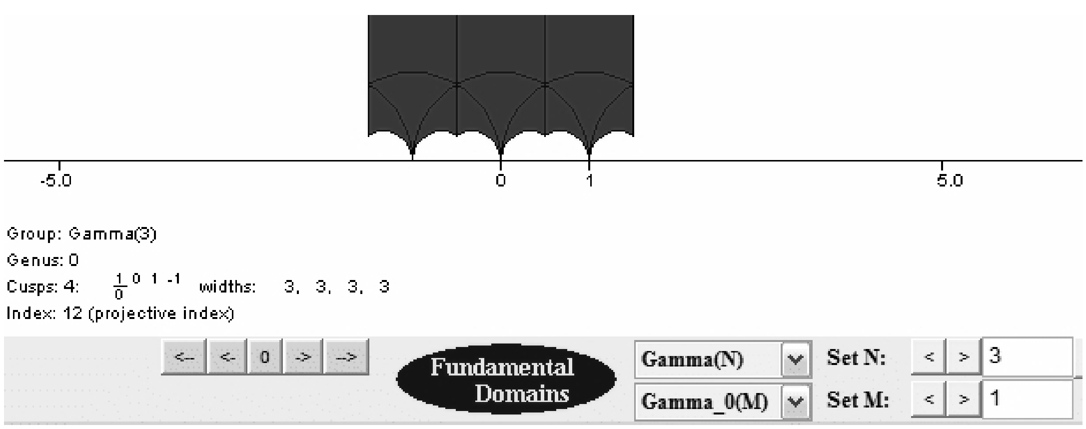
Bu tez çalışmasına başlarken amacımız $\mathcal{N}or$(N) nin simgesini tam olarak elde etmek, diğer bir ifadeyle eksik parametremiz olan g-cinsini hesaplamaktı. Literatür araştırması sonucunda bunun iki türlü mümkün olabileceği sonucuna varıldı;

1. **Hurwitz :** $\mu(Nor(n)) = 2\pi\left\{2(g-1)+\sum_{i=1}^{r}\left(1-{}^{1}\!/_{m_i}\right)+s\right\}$

2. **Shimura :** $g_0 - 1 = \frac{1}{2}W(n) + \left|Nor(n):\Gamma_0(n)\right|(g-1)$

1 ve 2 de g-cinsinin dışında bilinmeyen birer parametre var; 1 de $\mathcal{N}or$(N) nin hiperbolik ölçümü yani temel bölgesinin hiperbolik alanı, 2 de *W*(n) yani $\Gamma_0(\mathrm{N})$ nin $\mathcal{N}or$(N) üzerindeki toplam ramifikasyon mertebesi. Çalışmamızda 1 üzerinde gitmeye karar verdik.

Bu noktada temel bölge ile alt yörüngesel graf arasındaki ilişkiyi özetlemek gerekirse, kısaca döşemelerden(tessellations) bahsetmemiz gerekir. Şimdiye kadar değindiğimiz dönüşüm gruplarının üst-yarı düzleme göre bölüm gruplarının bir Riemann yüzeyi meydana getirdiğini gördük. Buna göre $\mathcal{U}/\mathcal{N}or$(N) bir Riemann yüzeyidir ve bir yüzey sembolüne yani döşemeye sahiptir. Bu döşeme cebirsel ve aritmetik metodlarla alt yörüngesel graflardan elde edilebileceği gibi temel bölgenin dönüşüm grubu altındaki resimlerinden elde etmekte mümkündür. Biz de bu ilişkiden yararlanarak alt yörüngesel grafların ortaya konmasının hiperbolik ölçümün hesaplanmasına yardımcı olacağı fikrinden hareketle bu çalışmayı yaptık. Benzer çalışmalar modüler grup ve onun kongrüans alt grupları için yapılmış, hatta program haline getirilmiştir :



4. SONUÇLAR

Şimdiye kadar $\mathcal{N}or$(N) ile ilgili yapılan çalışmalar incelendiğinde, elde edilen sonuçların, N-*karesiz* şartıyla ortaya koyulduğu görülecektir. Bu koşulun sağladığı en büyük avantaj transitifliktir. Bu çalışmada ise daha genel durumda sonuçlar elde edilmiş, özellikle de Bölüm 2.5 te $h \neq 1$ durumuyla birlikte tez içerisinde bahsi geçen bütün dönüşüm grupları arasında ilk kez rasyonel formlarla çalışma zaruriyeti ortaya çıkmıştır.

Keyfi N için bir çok varyasyonun oluşacağı muhakkaktır. Ancak bunların sınıflandırılması yapıldığında Bölüm 2.3, 2.4 ve 2.5 in izlenmesi gereken metod konusunda bir taban teşkil ettiği görülmektedir.

5. ÖNERİLER

Bu çalışmada $\mathcal{Nor}$(N) nin alt yörüngesel grafları elde edilmesine karşın, bunların yüzey sembolleri ile birlikte yorumu yapılmamıştır. Bu problemin aşılması durumunda simgenin tam olarak elde edileceği muhakkaktır. Bir başka çalışmada İrdelemede bahsettiğimiz Shimura formülü üzerinden de problemi ele aldık ve ramifikasyon mertebesini hesaplamaya çalıştık. Tam rakamı elde edemesekte bir alt sınıra ulaştığımızı iddia ediyoruz. Sonuç olarak simgenin bulunması problemi hala açıktır.

Alt yörüngesel graflardan elde edilen kongrüans denklemlerinin sayılar teorisiyle birlikte yorumu yapılmamıştır, buradan özellikle eliptik eğriler ve onların rasyonel noktaları ile ilgili önemli sonuçlar alınabilir.

Elde edilen sonuçlar için kullanımdaki pratiklik açısından HTML tabanlı, PHP ve ASP script dilleri kullanarak bir arayüz hazırlanabilir.

6. KAYNAKLAR

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

Akbaş, M. ve Singerman, D., 1992, The signature of the normalizer of $\Gamma_0(N)$, London Math.Soc., Lecture Notes 165, CUP, Cambridge, 77-86.

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

Akbaş, M., 2001, On suborbital graphs for the modular group, Bull. London Math. Soc., 33, 647-652.

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

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

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

Hardy, G. H. ve Wright, E. M., 1979, An introduction to the Theory of Numbers, Oxford University Press, Oxford.

Jones, G. A. ve Singerman, D., 1987, Complex Functions : An algebraic and geometric viewpoint, Cambridge University Press, Cambridge.

Jones , G. A., Singerman, D. ve Wicks, K., 1991, The modular group and generalized Farey Graphs, London Math. Soc. Lecture Notes 160, CUP, Cambridge, 316-318.

Lehner, J. ve Newman, M., 1964, Weierstrass points of $\Gamma_0(N)$, Annals of Mathematics, 79, 2, March.

Maclachlan, C., 1981, Groups of units of zero ternary quadratic forms, Proceedings of the Royal Society of Edinburg, 88A, 141-157.

Ogg, A. P., 1980, Modular functions, Proceedings of symposia in pure mathematics, 37.

Pizer, A., 1978, A note on a conjecture of Hecke, Pasific J. Math. , 79, 2, 541-548.

Schoeneberg, G., 1974, Elliptic Modular Functions, Springer Verlag, Berlin.

Sims, C. C., 1967, Graphs and finite permutation groups, Math. Z., 95, 76-86.

Singerman, D., 1970, Subgroups of Fuchsian groups and finite permutation groups, Bull. London Math. Soc., 2, 319-323.

Tsuzuku, T., 1982, Finite Groups and Finite Geometries, Cambridge University Press, Cambridge.

ÖZGEÇMİŞ

Bahadır Özgür Güler, 1978 yılında Ankara'da doğdu. İlk öğrenimini, İstanbul 30 Ağustos İlköğretim okulu, orta ve lise öğrenimini Ankara Ayrancı Lisesinde tamamladı. 1999 yılında K.T.Ü. Fen-Edebiyat Fakültesi Matematik bölümünden mezun oldu.

Aynı yıl K.T.Ü. Rize Fen-Edebiyat Fakültesi Matematik bölümü, Analiz ve Fonksiyonlar Teorisi Anabilim Dalında Araştırma Görevlisi oldu. 2002 yılında K.T.Ü. Fen Bilimleri Enstitüsü'nden Yüksek Lisans (Matematik) derecesini aldı ve aynı yerde doktora programına başladı. 1 Ekim 2005–30 Mayıs 2006 tarihleri arasında Erasmus-Sokrates değişim programıyla gittiği Ghent Üniversitesi(Belçika)'nde Prof. Dr. Jan Van Geel'in danışmanlığında "Eliptik Eğriler ve Modüler Grubun Kongrüans Alt Grupları" adlı proje çalışmasını Arş. Gör. Yavuz Kesicioğlu ile birlikte tamamladı. Halen K.T.Ü. deki görevine devam etmektedir.