New Trends in Mathematical Sciences

http://dx.doi.org/10.20852/ntmsci.2018.251

Congruence conditional signature problem

Murat Beşenk

Pamukkale University, Faculty of Arts and Sciences, Department of Mathematics, Denizli, Turkey

Received: 23 August 2017, Accepted: 21 September 2017
Published online: 19 February 2018.

Abstract: In this study, we examine properties of some subgroups of the modular group which can be characterized by algebraic and combinatoric. And also we investigate subgraphs of special congruence subgroup of modular group.

Keywords: Genus, cusp, signature, graph.

1 Introduction

Let $SL(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z} \;\; ad-bc=1 \right\}$. Consider the action of the group $SL(2,\mathbb{Z})$ on the upper half-plane $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im} z > 0\}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\tau = \dfrac{a\tau+b}{c\tau+d}$, $\tau \in \mathbb{H}$, in particularly the subgroup $SL(2,\mathbb{Z})$ acts on $\mathbb{H}$ discontinually. And also we recall that in many papers authors use the projective special linear group $PSL(2,\mathbb{Z}) = SL(2,\mathbb{Z})/\{\pm I\}$ instead of $SL(2,\mathbb{Z})$. The group $PSL(2,\mathbb{Z})$ is known the modular group, denoted by Γ, which consists of the transformations

$$z \to \frac{az+b}{cz+d} \;\text{ with }\; a,b,c,d \in \mathbb{Z}, \;\; ad-bc=1.$$

We note that for convenience, the modular group and its subgroups will be represented by matrices with the understanding that a matrix and its negative will be identified. Γ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. These satisfy the relations $S^4 = 1$, $(ST)^3 = S^2$ in $SL(2,\mathbb{Z})$. Moreover, one can show that these generate all relations $\langle S,T \mid S^4, S^2(ST)^3 \rangle$ is a presentation of the group $SL(2,\mathbb{Z})$. A congruence subgroup of level N of the modular group is a subgroup which contains $\Gamma(N) = \left\{ \gamma \in SL(2,\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod N) \right\}$ for some positive integer N. That is, any group G such that $\Gamma(N) < G < \Gamma$ is called a congruence subgroup of level N. Congruence subgroups are a class of arithmetic subgroups which are easy to describe. For example the following are some well-known congruence subgroups:

$$\Gamma_0(N) = \left\{ \gamma \in SL(2,\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (mod N) \right\}, \Gamma_1(N) = \left\{ \gamma \in SL(2,\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (mod N) \right\}.$$

In particular, all congruence subgroups of level N are very important number theory and group theory. Besides, we note that the existence of noncongruence subgroups of $SL(2,\mathbb{Z})$ was first announced by Felix Klein. Their construction of the

* Corresponding author e-mail: muratbesenk@gmail.com

subgroups used generators to define them.

Now we will take another subgroup of modular group,

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

We point out a few interesting properties of the group.

Remark. (i) If $n|N$, then $\Gamma_{0,n}(N)$ is a congruence subgroup of level N, and $\Gamma_1(N) \subseteq \Gamma_{0,n}(N) \subseteq \Gamma_0(N)$.
(ii) For all $N \in \mathbb{Z}^+$, $\Gamma_{0,1}(N) = \Gamma_0(N)$.

Lemma 1. *If $n|N$, then* $\Gamma_{0,n}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : N|c, \;\; a^2 \equiv 1(mod n) \right\}$.

Proof. Given $N|c$ and $n|N$, we must show that $a \equiv d(mod n)$ if and only if $a^2 \equiv 1(mod n)$. Therefore $d \equiv a(mod n) \Leftrightarrow$ because $gcd(a,n) = 1$, $ad \equiv a^2(mod n) \Leftrightarrow ad - bc \equiv a^2 - bc(mod n) \Leftrightarrow$ as $n|c$ $1 \equiv a^2(mod n)$. Hence this prove is completed.

Example 1. Let $n = 8$. Then $a^2 \equiv 1(mod 8) \Leftrightarrow gcd(a,2) = 1$, and $a^2 \equiv 1(mod 3) \Leftrightarrow gcd(a,3) = 1$. Whereas, for any prime integer $p > 3$, there exists no such nontrivial modulus m such that $a^2 \equiv 1(mod m) \Leftrightarrow gcd(a,p) = 1$.

2 Fundamental domain and cusps

We start by quickly recalling the basic notation of fundamental domain for modular group and cusp used in this work. We also mention a little stabilizer. If we get Γ then a system of coset representatives for the quotient $\Gamma \setminus SL(2,\mathbb{Z})$ is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\}.$$

Consequently using this, one can draw the following picture of a fundamental domain for Γ. Let F be the closed subset of $\mathbb{H}$ given by $F := \{z \in \mathbb{H} : |Rez| \leq \frac{1}{2} \text{ and } |z| \geq 1\}$. Here we write $\omega = exp(2\pi i/3)$ for the unique third root of unity in the upper half plane. Actually every point in $\mathbb{H}$ is equivalent, under the action of $SL(2,\mathbb{Z})$, to a point of F. If $z, z_0 \in F$ are two distinct points that are in the same $SL(2,\mathbb{Z})$-orbit, then either $z_0 = z \pm 1$ or $z_0 = -\frac{1}{z}$. There are two points at infinity that are in the closure of F in the Riemann sphere, but not in $\mathbb{H}$, namely ∞ ad 0. If we remove the Γ orbits of ω and i from upper half plane, then the action becomes free and its quotient space is a Riemann surface with hyperbolic metric. It is acquainted with that it is the two punctured plane $\mathbb{C} \setminus \{0,1\}$. If we hold on keeping the points with finite stabilizers then the quotient $\Gamma \setminus \mathbb{H}$ is a modular curve.

We will give only the statement since the following lemma is known.

Lemma 2. *Let z be in F and let $Stab_{SL(2,\mathbb{Z})}z$ be the stabiliser of z in $SL(2,\mathbb{Z})$. Then $Stab_{SL(2,\mathbb{Z})}$ is*

(1) *cyclic of order 6 generated by* $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ *if* $z = \omega$,

(2) *cyclic of order 6 generated by* $TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ *if* $z = \omega + 1$,

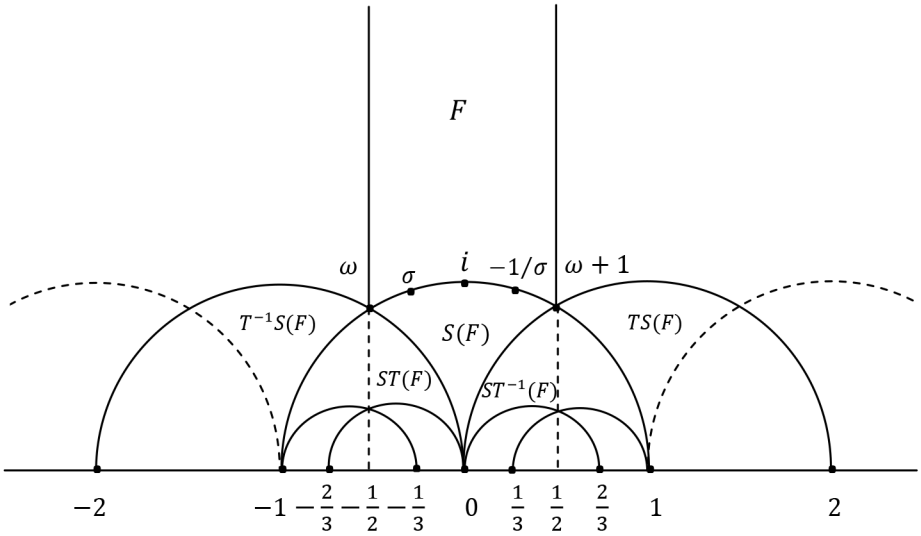

Fig. 1: Fundamental domain for Γ.

(3) *cyclic of order 4 generated by* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *if* $z = i$,

(4) *cyclic of order 2 generated by* $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ *otherwise.*

Definition 1. *The projective line over* $\mathbb{Q}$ *is the extended rational number set* $\mathbb{P}^1 := \mathbb{Q} \cup \{\infty\}$.

The group $SL(2,\mathbb{Z})$ acts on $\mathbb{P}^1$ by the same formula giving the action on $\mathbb{H}$: $\gamma x = \frac{ax+b}{cx+d}$ for $\gamma \in SL(2,\mathbb{Z})$, $x \in \mathbb{P}^1$. Here the right-hand side is to interpreted as $\frac{a}{c}$ if $x = \infty$, and as ∞ if $cx + d = 0$.

Theorem 1. *The action of* $SL(2,\mathbb{Z})$ *on* $\mathbb{P}^1$ *is transitive.*

Proof. It suffices to show that for every $x \in \mathbb{Q}$, there exists $\gamma \in SL(2,\mathbb{Z})$ such that $\gamma\infty = x$. We write $x = \frac{a}{c}$ with a, c coprime integers. Then there exist integers r, s such that $ar + cs = 1$, the matrix $\gamma = \begin{pmatrix} a & -s \\ c & r \end{pmatrix}$ has the required property. One easily control that the stabilizer of ∞ in $SL(2,\mathbb{Z})$ is $SL(2,\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$. And we have a bijection

$$\Theta : SL(2,\mathbb{Z})/SL(2,\mathbb{Z})_\infty \longrightarrow \mathbb{P}^1, \quad \Theta(\gamma SL(2,\mathbb{Z})_\infty) = \gamma\infty$$

Definition 2. *Let* G *be a congruence subgroup. The set cusps of* G *is the set of* G *orbits in* $\mathbb{P}^1$*, i.e. the quotient* $Cusps(G) = G \setminus \mathbb{P}^1$.

Especially, we have a surjective map $\theta : G \setminus SL(2,\mathbb{Z}) \longrightarrow Cusps(G)$.

Example 2. Let $G = \Gamma_0(p)$, p is prime. To compute the set of cusps of $\Gamma_0(p)$, we determine $\Gamma_0(p)$ orbits in $\mathbb{P}^1$. The orbit of $\infty \in \mathbb{P}^1$ is

$$\Gamma_0(p) \cdot \infty = \left\{ \pm \begin{pmatrix} a & b \\ cp & d \end{pmatrix} \cdot \infty \;\middle|\; a,b,c,d \in \mathbb{Z} \text{ and } ad - bcp = 1 \right\} = \left\{ \frac{a}{cp} \;\middle|\; a,c \in \mathbb{Z},\ gcd(a,cp) = 1 \right\}.$$

Therefore we can write $\Gamma_0(p)\cdot\infty = \left\{\frac{r}{s} \;\middle|\; r,s\in\mathbb{Z},\ gcd(r,s)=1 \text{ and } p|s\right\}$. Likewise, the orbit of 0 is $\Gamma_0(p)\cdot 0 = \left\{\frac{b}{d} \;\middle|\; b,d\in\mathbb{Z},\ gcd(b,d)=1 \text{ and } p\nmid s\right\}$. From this description of the two orbits it is clear that every element of $\mathbb{P}^1$ is in exactly one of them. In particular, $\Gamma_0(p)$ has two cusps, namely the two elements ∞ and 0 of $\Gamma_0(p)\setminus\mathbb{P}^1$. And also there is an isomorphism

$$\Lambda : \Gamma_0(p)\setminus SL(2,\mathbb{Z}) \longrightarrow \kappa\setminus SL(2,\mathbb{Z}_p)$$

where $\kappa = \left\{ \pm\begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \;\middle|\; a\in\mathbb{Z}_p^*,\ b\in\mathbb{Z}_p \right\}$. It is known that $|SL(2,\mathbb{Z}_p)| = p(p-1)(p+1)$. Furthermore, the description above of κ implies $|\kappa| = p(p-1)$. Therefore we obtain the index is $|SL(2,\mathbb{Z}):\Gamma_0(p)| = \frac{|SL(2,\mathbb{Z})|}{|\kappa|} = p+1$.

Example 3. The group $\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \;\middle|\; b\equiv 0 \pmod N \right\}$ congruence subgroup of modular group. Let $N=11$. Then the group $\Gamma^0(11)$ has index $|SL(2,\mathbb{Z}):\Gamma^0(11)| = 12$. It has two cusps: ∞ and 0. It has generated by 4 generators: T_∞ and T_0 which stabilize ∞ and 0 respectively and two parabolic generators A and B subject to one condition $T_\infty T_0 A B A^{-1} B^{-1} = I$.

Definition 3. *G is a group with no nontrivial normal subgroups. Then G is called a simple group.*

The importance of finite simple groups lies in their role as building blocks of finite groups. The important thing is the classification of finite simple groups. Indeed all finite simple groups were classified in 1983. In addition E. Mathieu discovered five strange finite simple groups. These groups were first called sporadic in the book of W. Burnside. The modern classification race started with the many papers. It was finally shown that every finite simple group is isomorphic to one of the following: **(1)** An alternating group A_n for $n\geq 5$. **(2)** A cyclic group $\mathbb{Z}_p$ of prime order p. **(3)** A simple group of Lie type over a finite field, e.g., $PSL(n,\mathbb{F}_q)$. **(4)** Some one of the sporadic simple groups. All 26 finite sporadic simple groups: Mathieu (5), Janko (2), Hall-Janko, Conway (3), Higman-Sims, Higman-Janko-Mckay, McLaughlin, Suzuki, Held, Rudvalis, Fischer (3), O'Nahn, Lyons, Harada-Norton, Thompson, Baby Monster and The Monster. The smallest sporadic group is the Mathieu group $\mathbb{M}_{11}$, which has order 7920, and the largest of the sporadic is known as the The Monster group, denoted $\mathbb{M}$ which has order approximately 8×10^{53}. Although the Monster group $\mathbb{M}$ was discovered within the context of finite simple groups, hints later began to emerge thet it might be strongly related to other branches of mathematics. One of these is the theory of modular functions and modular forms.

Let μ be the index, e_2 the number of inequivalent elliptic fixed point of order 2, e_3 the number of inequivalent elliptic fixed point of order 3 and h the number of inequivalent cusps. Thus, the Riemann-Hurwitz formula gives the genus as

$$g = 1+\frac{1}{2}\left(\frac{\mu}{6} - h - \frac{e_2}{2} - \frac{2e_3}{3}\right).$$

Genus is important in topological meaning for any group. It is known that the set $\mathbb{H}\setminus\Gamma$ of orbits has the structure of a Riemann surface with one point removed. This is a Riemann surface of genus 0. When we remove one point of it, we obtain a set that can be identified with $\mathbb{C}$. So, we have an isomorphism of Riemann surface $\varphi : \mathbb{H}\setminus\Gamma \longrightarrow \mathbb{C}$. One can obtain more examples adjoining to $\Gamma_0(N)$ the Fricke involution $\omega_N(z) = -\frac{1}{Nz}$, which of course can be realized as an element of $PSL(2,\mathbb{R})$. That is $\Gamma_0(N)^+ = \left\langle \Gamma_0(N), \frac{1}{\sqrt{N}}\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \right\rangle$. When N is a prime p, it is just the group $\Gamma_0(p)^+$

generated by $\Gamma_0(p)$ and the Fricke involution ω_p. Moreover we say that $\Gamma_0(p)^+$ has the genus 0 property if and only if $p = 2,3,5,7,11,13,17,19,23,29,31,41,47,59,71$. Since $|\mathbb{M}| = 2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$, these are the prime divisors of the order of the Monster group $\mathbb{M}$. We know that $\Gamma_{0,n}(N)$ is a Fuchsian group, a discrete subgroup of $PSL(2,\mathbb{R})$, whose fundamental domain has finite area, therefore it has a signature consisting of the geometric invariants $\sigma = (g; m_1, m_2, ..., m_r; s)$ where g is the genus of the compactified quotient space, $m_1, m_2, ..., m_r$ the periods of the elliptic generators, and s is parabolic class number. This signature problem is in a way the identity of discrete groups. But this problem very hard to solve. Actually, the main purpose in this study is to set the foundations of a new method that this method is named suborbital graphs.This way the signature problem transfer to the suborbital graphs.

3 Orbital graphs

We now explain imprimitivity of the action on $\Gamma_0(N)$ on $\mathbb{P}^1$. $(\Gamma_0(N), \mathbb{P}^1)$ is transitive permutation group, comprising of a group $\Gamma_0(N)$ acting on a set $\mathbb{P}^1$ transitively. $\upsilon_1, \upsilon_2 \in \mathbb{P}^1$ satisfy $\upsilon_1 \approx \upsilon_2$ then $\gamma(\upsilon_1) \approx \gamma(\upsilon_2)$ for all $\gamma \in \Gamma_0(N)$. In this case equivalence relation $\approx$ on $\mathbb{P}^1$ is invariant and equivalence classes form blocks. We say $(\Gamma_0(N), \mathbb{P}^1)$ imprimitive, if $\mathbb{P}^1$ accepts some invariant equivalence relation different from the identity relation and the universal relation. Otherwise $(\Gamma_0(N), \mathbb{P}^1)$ is primitive. These two relations are supposed to be trivial relations. In conclusion we have,

Theorem 2. (i) *$\Gamma_0(N)$ acts transitively on $\mathbb{P}^1$.*

(ii) *$\Gamma_0(N)_\infty$ is the stabilizer of ∞ in $\mathbb{P}^1$ is the set of* $\left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \;\middle|\; \alpha \in \mathbb{Z} \right\}$.

Proof. (i) It is enough to show that the orbit containing ∞ is $\mathbb{P}^1$. If $\frac{x}{y} \in \mathbb{P}^1$, then as $(x,y) = 1$, there exist $\eta_1, \eta_1 \in \mathbb{Z}$ with $x\eta_1 - y\eta_2 = 1$. Then the element $\begin{pmatrix} x & \eta_2 \\ y & \eta_1 \end{pmatrix}$ of $\Gamma_0(N)$ sends ∞ to $\frac{x}{y}$.

(ii) Since the action is transitive, stabilizers of any two points in $\mathbb{P}^1$ are conjugate. So it is sufficient to consider the stabilizer $\Gamma_0(N)_\infty$ of ∞. Let $K \in \Gamma_0(N)$. We can see that $K(\infty) = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. And then $a = 1$, $c = 0$, $d = 1$ and $b = \alpha \in \mathbb{Z}$. Hence $K = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$. Therefore $\Gamma_0(N)_\infty$ is the infinite cyclic group by the element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. That is, $\Gamma_0(N)_\infty = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$.

Remark. The elements of $\Gamma_{0,n}(N)$ like this $\begin{pmatrix} a & b \\ cN & a - nk \end{pmatrix}$, $k \in \mathbb{Z}$. It is clearly that for $N \neq 1$, $\Gamma_0(N)_\infty < \Gamma_{0,n}(N) < \Gamma_0(N)$.

We will define an equivalence relation $\approx$ induced on $\mathbb{P}^1$ by $\Gamma_0(N)$. Then $\Gamma_0(N)$ acts imprimitively on $\mathbb{P}^1$. Let $\xi_1 = \frac{\alpha_1}{\beta_1 N}$, $\xi_2 = \frac{\alpha_2}{\beta_2 N}$ be elements of $\mathbb{P}^1$. Then there are the elements $T_1 := \begin{pmatrix} \alpha_1 & \gamma_1 \\ \beta_1 N & \delta_1 \end{pmatrix}$ and $T_2 := \begin{pmatrix} \alpha_2 & \gamma_2 \\ \beta_2 N & \delta_2 \end{pmatrix}$ in $\Gamma_0(N)$ such that $T_1(\infty) = \xi_1$ and $T_2(\infty) = \xi_2$. So we have

$$\xi_1 \approx \xi_2 \quad \text{if only if} \quad T_1^{-1} T_2 \in \Gamma_{0,n}(N).$$

And so from the above we can easily calculate that $T_1^{-1}T_2 = \begin{pmatrix} \delta_1\alpha_2 - \gamma_1\beta_2 N & \delta_1\gamma_2 - \gamma_1\delta_2 \\ (\alpha_1\beta_2 - \alpha_2\beta_1)N & \alpha_1\delta_2 - \gamma_2\beta_1 N \end{pmatrix} \in \Gamma_{0,n}(N)$. Hence $\alpha_1\beta_2 - \alpha_2\beta_1 \equiv 0 \pmod{N}$ and $\delta_1\alpha_2 - \alpha_1\delta_2 + (\gamma_2\beta_1 - \gamma_1\beta_2)N \equiv 0 \pmod{n}$ are obtained. In addition that the number of the blocks under $\approx$ is given by the index $\Psi = |\Gamma_0(N) : \Gamma_{0,n}(N)|$. The index is coset numbers. Consequently we have the blocks

$$[\infty] := \{\frac{x}{y} \in \mathbb{P}^1 | (x,y) = 1 \text{ and } y \equiv 0 \pmod{N}\}, \quad [j] := \{\frac{x}{y} \in \mathbb{P}^1 | (x,y) = 1 \text{ and } x - jy \equiv 0 \pmod{N}\} \text{ where } j \neq \infty.$$

C. C. Sims introduced the idea of suborbital graphs for a finite permutation groups acting on a set. We use this idea as follows for $\Gamma_0(N)$ and $\mathbb{P}^1$.

Since $(\Gamma_0(N), \mathbb{P}^1)$ is transitive permutation group, then $\Gamma_0(N)$ acts on $\mathbb{P}^1 \times \mathbb{P}^1$ by

$$\Phi : \underset{(\gamma,(\alpha,\beta))}{\Gamma_0(N) \times (\mathbb{P}^1 \times \mathbb{P}^1)} \longrightarrow \underset{(\gamma(\alpha),\gamma(\beta))}{\mathbb{P}^1 \times \mathbb{P}^1}$$

where $\gamma \in \Gamma_0(N)$ and $\alpha, \beta \in \mathbb{P}^1$. The orbits of this action are suborbitals of $\Gamma_0(N)$. The orbit containing (α,β) is denoted by $O(\alpha,\beta)$. From $O(\alpha,\beta)$ we can form a suborbital graph $\mathbb{G}$. Its vertices are the elements of $\mathbb{P}^1$, and if $(\gamma,\delta) \in O(\alpha,\beta)$ there is a directed edge from γ to δ. Moreover $O(\alpha,\alpha)$ is diagonal of $\mathbb{P}^1 \times \mathbb{P}^1$. The corresponding suborbital graph called the trivial suborbital graph, it consists of a loop based at each vertex. By a circuit of length m, we mean a sequence $v_1 \to v_2 \to ... \to v_m \to v_1$ such that $v_i \neq v_j$ for $i \neq j$, where $m \geq 3$. If $m = 3$ or $m = 4$ the the circuit is known triangle or quadrilateral.

As $\Gamma_0(N)$ acts transitively on $\mathbb{P}^1$, it permutes the blocks transitively. Let F_∞ denote the subgraphs in $\mathbb{G}$ whose vertices form the block $[\infty]$. Similarly we may write subgraphs F_j are for other blocks, $j \neq \infty$.

Theorem 3. *Let* $\frac{\alpha_1}{\beta_1}$, *and* $\frac{\alpha_2}{\beta_2}$ *be in the block* $[\infty]$. *There is an edge* $\frac{\alpha_1}{\beta_1} \longrightarrow \frac{\alpha_2}{\beta_2}$ *in* F_∞ *if and only if either*

(i) $\alpha_2 \equiv u\alpha_1 \pmod{N}$, $\beta_2 \equiv u\beta_1 \pmod{N}$ *and* $\alpha_1\beta_2 - \beta_1\alpha_2 = N$, *or*
(ii) $\alpha_2 \equiv -u\alpha_1 \pmod{N}$, $\beta_2 \equiv -u\beta_1 \pmod{N}$ *and* $\alpha_1\beta_2 - \beta_1\alpha_2 = -N$.

Proof. (i) Let $\frac{\alpha_1}{\beta_1} \longrightarrow \frac{\alpha_2}{\beta_2} \in F_\infty$, then there exists some $T := \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ such that $T(\infty) = \frac{a}{cN} = \frac{\alpha_1}{\beta_1}$ and $T(\frac{u}{N}) = \frac{au+b}{cuN+dN} = \frac{\alpha_2}{\beta_2}$. Hence $a = \alpha_1$, $cN = \beta_1$. Then these equations $\alpha_2 \equiv u\alpha_1 \pmod{N}$ and $\beta_2 \equiv u\beta_1 \pmod{N}$ are satisfied. So we have the matrix equation $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}$. If we take determinant, it is easily seen that $\alpha_1\beta_2 - \beta_1\alpha_2 = N$. Conversely, we suppose that $\alpha_2 \equiv u\alpha_1 \pmod{N}$, $\beta_2 \equiv u\beta_1 \pmod{N}$ and $\alpha_1\beta_2 - \beta_1\alpha_2 = N$. Then there exist integers ε_1 and ε_2 such that $\alpha_2 = u\alpha_1 + N\varepsilon_1$ and $\beta_2 = u\beta_1 + N\varepsilon_2$. In this case

$$\begin{pmatrix} \alpha_1 & \varepsilon_1 \\ \beta_1 & \varepsilon_2 \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} \alpha_1 & u\alpha_1 + N\varepsilon_1 \\ \beta_1 & u\beta_1 + N\varepsilon_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}$$

is obtained. Since $\alpha_1\beta_2 - \beta_1\alpha_2 = N$ from determinants we get $\alpha_1\varepsilon_2 - \beta_1\varepsilon_1 = 1$. Consequently, $\begin{pmatrix} \alpha_1 & \varepsilon_1 \\ \beta_1 & \varepsilon_2 \end{pmatrix} \in \Gamma_0(N)$ and $\frac{\alpha_1}{\beta_1} \longrightarrow \frac{\alpha_2}{\beta_2} \in F_\infty$.

(ii) The proof for minus sign is similar. We get above matrix equation with α_2 and β_2 replaced by $-\alpha_2$ and $-\beta_2$ so that $\frac{\alpha_1}{\beta_1} \longrightarrow \frac{-\alpha_2}{-\beta_2} \in F_\infty$.

Theorem 4. *The subgraph F_∞ contains a hyperbolic triangle if and only if $u^2 \pm u + 1 \equiv 0\,(modN)$.*

Proof. Assume first that F_∞ has a triangle $\frac{\alpha_0}{\beta_0} \longrightarrow \frac{\gamma_0}{\delta_0} \longrightarrow \frac{x_0}{y_0} \longrightarrow \frac{\alpha_0}{\beta_0}$. It can be easily shown that $\Gamma_{0,n}(N)$ permutes the vertices and edges of F_∞ transitively. Therefore we suppose that the above triangle is transformed under $\Gamma_{0,n}(N)$ to the $\frac{1}{0} \longrightarrow \frac{u}{N} \longrightarrow \frac{x_0}{y_0} \longrightarrow \frac{1}{0}$. Let $\frac{u}{N} < \frac{x_0}{y_0 N}$. Without loss of generality, from the edge of $\frac{u}{N} \longrightarrow \frac{x_0}{y_0 N}$ the equation of $x_0 \equiv -u^2 (modN)$ and from the $uy_0N - x_0N = -N$ equation, $x_0 = uy_0 + 1$ is achieved. For $y_0 = 1$ situation, $\frac{u}{N} \longrightarrow \frac{x_0}{N}$ and $x_0 = u+1$ eventually $\frac{u}{N} \longrightarrow \frac{u+1}{N}$ is found. Hence $u^2 + u + 1 \equiv 0\,(modN)$. And also $y_0 \neq 1$ can not be true because there is not an edge condition. Similarly if $\frac{u}{N} > \frac{x_0}{y_0 N}$ holds then we conclude that $u^2 - u + 1 \equiv 0\,(modN)$. Consequently we have $u^2 \pm u + 1 \equiv 0\,(modN)$.

On the other hand suppose that $u^2 \pm u + 1 \equiv 0\,(modN)$. Then, using Theorem 3., we see that $\frac{1}{0} \longrightarrow \frac{u}{N} \longrightarrow \frac{u \pm 1}{N} \longrightarrow \frac{1}{0}$ is a triangle in F_∞.

As a result this theory reveal the relationship between permutation groups and graphs .

Example 4. We can partition $\mathbb{P}^1$ into three disjoint subset, which are permuted by Γ. The index is $|\Gamma : \Gamma_0(2)| = 3$, these are $[0]$,$[1]$ and $[\infty]$, for $N > 1$. So action of Γ we have the set wise stabilizer of $[0]$ is $\Gamma_0(2)$. And $\Gamma/\Gamma_0(2) \simeq PSL(2,\mathbb{Z}_2) \simeq S_3$ where S_3 symmetric group. The automorphism group of preserving orientation and colors is $\Gamma(2)$ which is generated by $\varphi_1(z) = \frac{z}{-2z+1}$ and $\varphi_2(z) = \frac{z-2}{2z-3}$. Additionally this is a free group of rank 2.

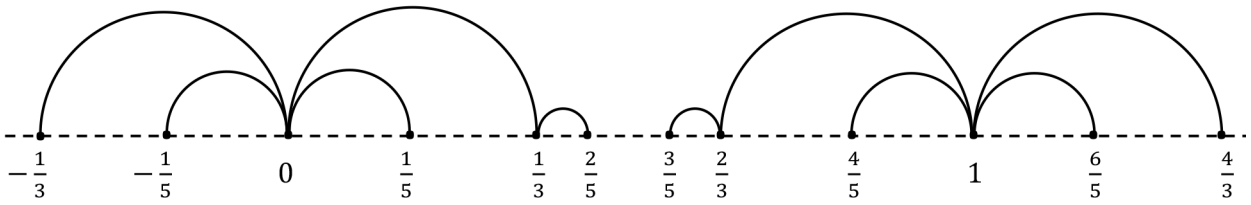

Fig. 2: Universal map for $[0]$ and $[1]$.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

All authors have contributed to all parts of the article. All authors read and approved the final manuscript.

References

[1] M. Akbaş, *On suborbital graphs for the modular group*, London Mathematical Society Lecture Note Series 33, (2001), 647–652.

[2] G. A. Jones, D. Singerman, K. Wicks, *The modular group and generalized Farey graphs*, London Mathematical Society Lecture Note Series 160, (1991), 316–338.

[3] C. C. Sims, *Graphs and finite permutation groups*, Mathematische Zeitschrift 95, (1967), 76–86.

[4] N. L. Biggs, A. T. White, *Permutation groups and combinatorial structures*, Cambridge University Press, Cambridge, 1979.

[5] K. Ludwick, *Congruence restricted modular forms*, The Ramanujan Joural 9, (2005), 341–356.

[6] R. A. Rankin, *Modular forms and functions*, Cambridge University Press, Cambridge, 2008.

[7] M. Beşenk, *Suborbital graphs of a extended congruence subgroup by Fricke involution*, AIP Conf. Proc. 1676, (2015), 1–6.

[8] B.Ö. Güler, M. Beşenk, Y. Kesicioğlu, A. H. Değer, *Suborbital graphs for the group* Γ^2, Hacettepe Journal of Mathematics and Statistics 44, (2015), 1033–1044.

[9] M. Beşenk, *Suborbital graphs for the invariance group*, Beykent Uni. Journal of Science and Engineering 10, (2017), 15–29.

[10] Y. Kesicioğlu, M. Akbaş, M. Beşenk, *Connectedness of a suborbital graph for congruence subgroups*, Journal of Inequalities and Applications 1, (2013), 117–124.