Beşenk et al. *Journal of Inequalities and Applications* 2013, **2013**:106
http://www.journalofinequalitiesandapplications.com/content/2013/1/106

Journal of Inequalities and Applications
a SpringerOpen Journal

RESEARCH Open Access

Circuit lengths of graphs for the Picard group

Murat Beşenk[1], Bahadır Ö Güler[1*], Ali H Değer[1] and Yavuz Kesicioğlu[2]

*Correspondence: boguler@ktu.edu.tr
[1]Faculty of Science, Department of Mathematics, Karadeniz Technical University, Trabzon, 61080, Turkey
Full list of author information is available at the end of the article

Abstract
In this paper, we examine some properties of suborbital graphs for the Picard group. We obtain edge and circuit conditions, then propose a conjecture for the graph to be forest. This paper is an extension of some results in (Jones *et al.* in The Modular Group and Generalized Farey Graphs, pp. 316-338, 1991).

1 Introduction

Let $\mathbb{Q}(i) := \{\frac{\alpha}{\beta} + i\frac{\gamma}{\delta} \mid \frac{\alpha}{\beta}, \frac{\gamma}{\delta} \in \mathbb{Q}\}$ be a quadratic extension of the rational numbers. $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$. The Picard group is denoted by $\mathbf{P}$ and contains all linear fractional transformations

$$\bar{A} : z \to \frac{az+b}{cz+d}, \quad \text{where } a,b,c,d \in \mathbb{Z}[i] \text{ and } ad-bc=1.$$

$\mathbf{P}$ is an important subgroup of $PSL(2,\mathbb{C})$. On the other hand,

$$SL\big(2,\mathbb{Z}(i)\big) = \left\{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : a,b,c,d \in \mathbb{Z}[i] \text{ and } ad-bc=1\right\}$$

is a subgroup of $SL(2,\mathbb{C})$.

Let us consider the map $\theta : SL(2,\mathbb{Z}[i]) \mapsto PSL(2,\mathbb{Z}[i])$, $\theta(A) = \bar{A}$. Since

$$\theta(AB) = \overline{AB} = \bar{A}\bar{B} = \theta(A)\theta(B),$$

θ is a surjective homomorphism. It is clear that $\mathrm{Ker}(\theta) = \{\pm I\}$. Hence, the relation between A and $\bar{A}$ is given by the isomorphism

$$A/\{\pm I\} \cong \bar{A},$$

that is, $\mathbf{P} = PSL(2,\mathbb{Z}[i]) \cong SL(2,\mathbb{Z}[i])/\{\pm I\}$.

In this study, we consider the action of the Picard group on the set $\hat{\mathbb{Q}}(i) := \mathbb{Q}(i) \cup \{\infty\}$ in the spirit of the theory of permutation groups and a graph arising from this action in hyperbolic geometric terms.

2 The action of $\mathbf{P}$ on $\hat{\mathbb{Q}}(i)$

Any element of $\hat{\mathbb{Q}}(i)$ is represented as a reduced fraction $\frac{x}{y}$ with $x,y \in \mathbb{Z}[i]$ and $(x,y)=1$. ∞ is represented as $\frac{1}{0} = \frac{-1}{0} = \frac{i}{0} = \frac{-i}{0}$. As $\frac{x}{y} = \frac{\varepsilon x}{\varepsilon y}$, where ε is a unit, the representation is not unique. Since $T(\frac{x}{y}) = T(\frac{\varepsilon x}{\varepsilon y})$, we have a well-defined action of $\mathbf{P}$ on $\hat{\mathbb{Q}}(i)$. The action of $\mathbf{P}$ on $\hat{\mathbb{Q}}(i)$ now becomes

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

Note that as $ad - bc = 1$ and $(x,y) = 1$, it follows that $(ax + by, cx + dy) = 1$ and so $(ax + by)/(cx + dy)$ is a reduced fraction.

Theorem 2.1 *The action of* $\mathbf{P}$ *on* $\hat{\mathbb{Q}}(i)$ *is transitive.*

Proof It is enough to prove that the orbit containing ∞ is $\hat{\mathbb{Q}}(i)$. If $x/y \in \hat{\mathbb{Q}}(i)$ (in reduced form), then as $(x,y) = 1$, there exist $\alpha, \beta \in \mathbb{Z}[i]$ with $x\alpha - y\beta = 1$. Then the element $\begin{pmatrix} x & \beta \\ y & \alpha \end{pmatrix}$ of $\mathbf{P}$ sends ∞ to x/y. □

We now consider the imprimitivity of the action of $\mathbf{P}$ on $\hat{\mathbb{Q}}(i)$, beginning with a general discussion of the primitivity of permutation groups. Let (G, Δ) be a transitive permutation group, consisting of a group G acting on a set Δ transitively. An equivalence relation $\approx$ on Δ is called *G-invariant* if, whenever $\alpha, \beta \in \Delta$ satisfy $\alpha \approx \beta$, then $g(\alpha) \approx g(\beta)$ for all $g \in G$. The equivalence classes are called blocks, and the block containing α is denoted by $[\alpha]$.

We call (G, Δ) *imprimitive* if Δ admits some G-invariant equivalence relation different from

(i) the identity relation $\alpha \approx \beta$ if and only if $\alpha = \beta$;

(ii) the universal relation $\alpha \approx \beta$ for all $\alpha, \beta \in \Delta$.

Otherwise (G, Δ) is called *primitive*. These two relations are supposed to be trivial relations. Clearly, a primitive group must be transitive, for if not, the orbits would form a system of blocks. The converse is false, but we have the following useful result in [1].

Lemma 2.2 *Let* (G, Δ) *be a transitive permutation group.* (G, Δ) *is primitive if and only if* G_α*, the stabilizer of* $\alpha \in \Delta$*, is a maximal subgroup of* G *for each* $\alpha \in \Delta$*.*

From the above lemma we see that whenever, for some α, $G_\alpha < H < G$, then Δ admits some G-invariant equivalence relation other than the trivial cases. Because of the transitivity, every element of Δ has the form $g(\alpha)$ for some $g \in G$. Thus one of the nontrivial G-invariant equivalence relations on Δ is given as follows:

$$g(\alpha) \approx g'(\alpha) \quad \text{if and only if} \quad g' \in gH.$$

The number of blocks (equivalence classes) is the index $|G : H|$ and the block containing α is just the orbit $H(\alpha)$.

We can apply these ideas to the case where G is the $\mathbf{P}$ and Δ is $\hat{\mathbb{Q}}(i)$.

Lemma 2.3 *The stabilizer of* ∞ *in* $\hat{\mathbb{Q}}(i)$ *is the set of* $\{\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} : \alpha \in \mathbb{Z}[i]\}$ *denoted by* $\mathbf{P}_\infty$.

Definition 2.4 $\mathbf{P}_1(N) := \{T \in \mathbf{P} \mid a \equiv d \equiv 1 (\bmod N), c \equiv 0 (\bmod N)\}$ is a subgroup of $\mathbf{P}$.

It is clear that $\mathbf{P}_\infty < \mathbf{P}_1(N) < \mathbf{P}$. We will define an equivalence relation $\approx$ induced on $\hat{\mathbb{Q}}(i)$ by $\mathbf{P}$. We must point out that this equivalence relation is different from the one in [2]. Here let us take the group $\mathbf{P}_1(N)$ instead of $\mathbf{P}_0(N) := \{T \in \mathbf{P} | c \equiv 0 (\operatorname{mod} N)\}$. The purpose of our work is related to this choice. We now collect some information on permutation groups (see [3]). Given a permutation group G on a finite set Δ, some natural questions arise as follows:

- Orbit problem: What are the orbits of G?
- Block problem: Is G primitive? If not, find a nontrivial block for G.

Actually, it is more important to find the minimal nontrivial blocks for G because many computations dealing with permutation groups work better with it. In this meaning, the choice of decomposition-$|G:H|$ is substantial.

Hence, our aim is to see how graphs are affected by decomposition $|\mathbf{P}:\mathbf{P}_1(N)|$.

Now let $r/s, x/y \in \hat{\mathbb{Q}}(i)$. Corresponding to these, there are two matrices

$$T_1 := \begin{pmatrix} r & k \\ s & l \end{pmatrix}, \qquad T_2 := \begin{pmatrix} x & m \\ y & t \end{pmatrix}$$

in $\mathbf{P}$ for which $T_1(\infty) = r/s$, $T_2(\infty) = x/y$. Now $r/s \approx x/y$ iff $T_1^{-1}T_2 \in \mathbf{P}_1(N)$, so $r/s \approx x/y$ iff $x \equiv r (\operatorname{mod} N)$ and $y \equiv s (\operatorname{mod} N)$. Here, the number $\eta(N)$ of blocks is $|\mathbf{P}:\mathbf{P}_1(N)|$.

Using the results in [4, 5], we have the following

Theorem 2.5 *The index* $|\mathbf{P}:\mathbf{P}_1(N)| = N^2 \prod_{p|N}(1-\frac{1}{p^2})$, *where* $N \in \mathbb{Z}[i]$ *and* N *is not a unit.*

Proof Firstly, we define $\mathbf{P}(N) = \{T \in \mathbf{P} | a \equiv d \equiv 1 (\operatorname{mod} N), b \equiv c \equiv 0 (\operatorname{mod} N)\}$. Let $\mu(N) := |\mathbf{P}:\mathbf{P}(N)|$. Equivalently, this is the number of solutions of $ad - bc \equiv 1 (\operatorname{mod} N)$. By the Chinese reminder theorem, $\mu(N_1N_2) = \mu(N_1)\mu(N_2)$ for $(N_1, N_2) = 1$. Hence, we can restrict ourselves to powers of a prime $N = p^\alpha$.

(i) Suppose that $a \not\equiv 0 (\operatorname{mod} p)$. There are $\varphi(p^\alpha)$ residue classes $a \operatorname{mod} p^\alpha$, where $\varphi(n)$ denotes Euler's function. To each of these classes for a, the numbers b and c may be chosen arbitrarily $\operatorname{mod} p^\alpha$. $d \operatorname{mod} p^\alpha$ is uniquely determined. In this case there are altogether $\varphi(p^\alpha)p^{2\alpha}$ solutions.

(ii) Suppose that $a \equiv 0 (\operatorname{mod} p)$. There are $p^{\alpha-1}$ residue classes $a \operatorname{mod} p^\alpha$. Corresponding to each of these, $d \operatorname{mod} p^\alpha$ may be chosen arbitrarily since in the case $(p, bc) = 1$, there are $\varphi(p^\alpha)$ possibilities for $b \operatorname{mod} p^\alpha$ and $c \operatorname{mod} p^\alpha$ is again uniquely determined. Hence there are $\varphi(p^\alpha)p^{2\alpha-1}$ additional solutions.

Together we obtain $p^{3\alpha}(1-\frac{1}{p^2})$. Consequently, we have $\mu(N) = N^3 \prod_{p|N}(1-\frac{1}{p^2})$ since $|\mathbf{P}_1(N):\mathbf{P}(N)| = N$, $|\mathbf{P}:\mathbf{P}_1(N)| = N^2 \prod_{p|N}(1-\frac{1}{p^2})$ as required. □

3 Suborbital graphs of P on $\hat{\mathbb{Q}}(i)$

In [6], Sims introduced the idea of suborbital graphs of a permutation group G acting on a set Δ. These are graphs with a vertex-set Δ, on which G induces automorphisms. We summarize Sims' theory as follows.

Let (G, Δ) be transitive permutation group. Then G acts on $\Delta \times \Delta$ by $g(\alpha, \beta) = (g(\alpha), g(\beta))$ $(g \in G,\ \alpha, \beta \in \Delta)$. The orbits of this action are called *suborbitals* of G. The orbit containing (α, β) is denoted by $O(\alpha, \beta)$. From $O(\alpha, \beta)$ we can form a *suborbital graph* $G(\alpha, \beta)$: its vertices are the elements of Δ, and there is a directed edge from γ to δ if $(\gamma, \delta) \in O(\alpha, \beta)$. A directed edge from γ to δ is denoted by $\gamma \to \delta$. If $(\gamma, \delta) \in O(\alpha, \beta)$, then we will say that there exists an edge $\gamma \to \delta$ in $G(\alpha,\beta)$. In this paper our calculation concerns $\mathbf{P}$, so we can draw this edge as a hyperbolic geodesic in the upper half-plane $\mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$, see [7].

The orbit $O(\beta,\alpha)$ is also a suborbital graph and it is either equal to or disjoint from $O(\alpha,\beta)$. In the latter case, $G(\beta,\alpha)$ is just $G(\alpha,\beta)$ with the arrows reserved and we call, in this case, $G(\alpha,\beta)$ and $G(\beta,\alpha)$ *paired suborbital graphs*. In the former case, $G(\alpha,\beta) = G(\beta,\alpha)$ and the graph consists of pairs of oppositely directed edges; it is convenient to replace each such pair by a single undirected edge so that we have a undirected graph which we call *self-paired*.

The above ideas are also described in the paper by Neumann [8] and in the books by Tsuzuku [9] and by Biggs and White [1], the emphasis being on applications to finite groups.

In this study, G and Δ will be $\mathbf{P}$ and $\hat{\mathbb{Q}}(i)$, respectively. Since $\mathbf{P}$ acts transitively on $\hat{\mathbb{Q}}(i)$, each suborbital contains a pair (∞, v) for some $v \in \hat{\mathbb{Q}}(i)$; writing $v = \frac{u}{N}$, we denote this suborbital by $O_{u,N}$ and the corresponding suborbital graph by $G_{u,N}$.

Definition 3.1 By a directed circuit in $G_{u,N}$, we mean a sequence $v_1, v_2, \dots, v_m$ of different vertices such that $v_1 \longrightarrow v_2 \longrightarrow \cdots \longrightarrow v_m \longrightarrow v_1$, where $m \geq 3$; an anti-directed circuit will denote a configuration like the above with at least an arrow (not all) reversed.

If $m = 3$, then the circuit, directed or not, is called a triangle.

If $m = 2$, then we will call the configuration $v_1 \longrightarrow v_2 \longrightarrow v_1$ a self-paired edge: it consists of a loop based at each vertex.

We call a graph a *forest* if it does not contain any circuits.

3.1 Graph $G_{u,N}$

We now investigate the suborbital graphs for the action $\mathbf{P}$ on $\hat{\mathbb{Q}}(i)$.

Theorem 3.2 *There is an edge $r/s \to x/y$ in $G_{u,N}$ iff there exists a unit $\varepsilon \in \mathbb{Z}[i]$ such that*

$$x \equiv \pm\varepsilon ur (\operatorname{mod} N), \qquad y \equiv \pm\varepsilon us (\operatorname{mod} N), \quad N = \varepsilon(ry - sx).$$

Proof We assume that there exists an edge $r/s \to x/y$ in $G_{u,N}$. Therefore there exist some T in $\mathbf{P}$ such that T sends the pair $(\infty, \frac{u}{N})$ to the pair $(\frac{r}{s}, \frac{x}{y})$, that is, $T(\infty) = \frac{r}{s}$ and $T(\frac{u}{N}) = \frac{x}{y}$. Let $T(z) = \frac{az+b}{cz+d}$; $a, b, c, d \in \mathbb{Z}[i]$. Then we have that $\frac{a}{c} = \frac{r}{s}$ and $\frac{au+bN}{cu+dN} = \frac{x}{y}$. Since $(a,c) = (r,s) = (x,y) = 1$, there exist the units $\varepsilon_0, \varepsilon_1 \in \mathbb{Z}[i]$ such that $a = \varepsilon_0 r$, $c = \varepsilon_0 s$ and $au + bN = \varepsilon_1 x$, $cu + dN = \varepsilon_1 y$. Hence, we have that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} \varepsilon_0 r & \varepsilon_1 x \\ \varepsilon_0 s & \varepsilon_1 y \end{pmatrix}.$$

From the determinant, we have $N = \varepsilon_0\varepsilon_1(ry - sx)$. As $\varepsilon_1 x = au + bN = \varepsilon_0 ur + bN$, $\varepsilon_1 y = cu + dN = \varepsilon_0 us + dN$, then $\varepsilon_1 x = \varepsilon_0 ur (\operatorname{mod} N)$, $\varepsilon_1 y = \varepsilon_0 us (\operatorname{mod} N)$. Thus, we obtain that $x \equiv \varepsilon_1^{-1}\varepsilon_0 ur (\operatorname{mod} N)$, $y \equiv \varepsilon_1^{-1}\varepsilon_0 us (\operatorname{mod} N)$ and $N = \varepsilon_0\varepsilon_1(ry - sx)$. Taking with $\varepsilon = \varepsilon_0\varepsilon_1$, we have that $x \equiv \pm\varepsilon ur (\operatorname{mod} N)$, $y \equiv \pm\varepsilon us (\operatorname{mod} N)$ and $N = \varepsilon(ry - sx)$.

Conversely, we suppose that $x \equiv \pm\varepsilon ur (\operatorname{mod} N)$, $y \equiv \pm\varepsilon us (\operatorname{mod} N)$ and $N = \varepsilon(ry - sx)$. If the plus sign is valid, then there exist $b, d \in \mathbb{Z}[i]$ such that $x = \varepsilon ur + bN$, $y = \varepsilon us + dN$.

Taking with $a = \varepsilon r$ and $c = \varepsilon s$, then $x = au + bN$, $y = cu + dN$ and then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} \varepsilon r & x \\ \varepsilon s & y \end{pmatrix}.$$

As $\varepsilon(ry - sx) = N$, we have $ad - bc = 1$, so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{P}$ and hence $r/s \to x/y$ in $G_{u,N}$. If the minus sign is valid, then there exist $b, d \in \mathbb{Z}[i]$ such that $ix = -i\varepsilon ur + bN$, $iy = -i\varepsilon us + dN$. Taking with $a = -i\varepsilon r$ and $c = -i\varepsilon s$, then $ix = au + bN$, $iy = cu + dN$ and then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & N \end{pmatrix} = \begin{pmatrix} -i\varepsilon r & ix \\ -i\varepsilon s & iy \end{pmatrix}.$$

The result is the same. □

Theorem 3.3 *$G_{u,N}$ is self-paired iff $u^2 \equiv \mp\varepsilon^2 (\operatorname{mod} N)$.*

Proof We suppose that $G_{u,N}$ is self-paired. If $\infty \to x/y$, then it must also be $x/y \to \infty$. So, there exists $\varepsilon \in \mathbb{Z}[i]$ such that $(u0 - N1) = \varepsilon$. From the edge $1/0 \to u/N$, we have that $u \equiv \varepsilon u (\operatorname{mod} N)$ means that $\varepsilon \equiv 1 (\operatorname{mod} N)$. From the edge $u/N \to 1/0$, we obtain that $1 \equiv -\varepsilon u^2 (\operatorname{mod} N)$. Hence, $\varepsilon u^2 \equiv -\varepsilon (\operatorname{mod} N)$ and then $u^2 \equiv \mp\varepsilon^2 (\operatorname{mod} N)$.

Conversely, suppose that $u^2 \equiv \mp\varepsilon^2 (\operatorname{mod} N)$. Taking with $\varepsilon^2 u^2 \equiv \mp\varepsilon^4 (\operatorname{mod} N)$, we have that $\varepsilon^2 u^2 \equiv \mp 1 (\operatorname{mod} N)$. If $\varepsilon^2 u^2 \equiv -1 (\operatorname{mod} N)$, then there exists $b \in \mathbb{Z}[i]$ such that $\varepsilon^2 u^2 \equiv -1 + \varepsilon bN$. Hence $-\varepsilon^2 u^2 + \varepsilon bN = 1$. Let $T := \left(\begin{smallmatrix} -\varepsilon u & b \\ -\varepsilon N & \varepsilon u \end{smallmatrix}\right)$, then $T(\infty) = u/N$, $T(u/N) = \infty$ and $\det T = 1$. The case of $\varepsilon^2 u^2 \equiv 1 (\operatorname{mod} N)$ is similar. □

If $r/s \to x/y$ in $G_{u,N}$, then Theorem 3.2 implies that there exists $\varepsilon \in \mathbb{Z}[i]$ such that $ry - sx = \varepsilon N$, so $r/s \approx x/y$. Thus each connected component of $G_{u,N}$ lies in a single block for $\approx$, of which there are $\eta(N)$, so we have the following corollary.

Corollary 3.4 *$G_{u,N}$ has at least $\eta(N)$ connected components; in particular, $G_{u,N}$ is not connected if N is not a unit.*

3.2 Subgraph $H_{u,N}$

As we saw, each $G_{u,N}$ is a disjoint union of $\eta(N)$ subgraphs, the vertices of each subgraph forming a single block with respect to the relation $\approx$. Since $\mathbf{P}$ acts transitively on $\hat{\mathbb{Q}}(i)$, it permutes these blocks transitively, so the subgraphs are all isomorphic. We let $H_{u,N}$ be the subgraph of $G_{u,N}$ whose vertices form the block $[\infty] := [\frac{1}{0}] = \{\frac{x}{y} \in \hat{\mathbb{Q}}(i) | x \equiv 1 (\operatorname{mod} N), y \equiv 0 (\operatorname{mod} N)\}$ so that $G_{u,N}$ consists of $\eta(N)$ disjoint copies of $H_{u,N}$.

Theorem 3.5 *Let $r/s, x/y \in [\infty]$. There is an edge $r/s \to x/y$ in $H_{u,N}$ iff there exists a unit $\varepsilon \in \mathbb{Z}[i]$ such that $x \equiv \varepsilon ur (\operatorname{mod} N)$ and $y \equiv -\varepsilon us (\operatorname{mod} N)$, where either $u = 1$ or $u = N - 1$ and $N = \varepsilon(ry - sx)$.*

Proof It is clear that $r \equiv 1 (\operatorname{mod} N)$ and $x \equiv 1 (\operatorname{mod} N)$. Since $r/s \to x/y$, we obtain that $x \equiv \pm\varepsilon ur (\operatorname{mod} N)$ by Theorem 3.2. Thus

(i) if $x \equiv \varepsilon ur (\operatorname{mod} N)$, then $u \equiv 1 (\operatorname{mod} N)$, giving $u = 1$;
(ii) if $x \equiv -\varepsilon ur (\operatorname{mod} N)$, then $u \equiv -1 (\operatorname{mod} N)$, giving $u = N - 1$.

Hence $r/s \to x/y$ in $H_{u,N}$ iff either $u = 1$ or $u = N - 1$. Opposite direction can be seen easily. □

Theorem 3.6 $\mathbf{P}_1(N)$ *permutes the vertices and the edges of* $H_{u,N}$ *transitively.*

Proof Suppose that $u, v \in [\infty]$. As $\mathbf{P}$ acts on $\hat{\mathbb{Q}}(i)$ transitively, $g(u) = v$ for some $g \in \mathbf{P}$. Since $u \approx \infty$ and $\approx$ is $\mathbf{P}$-invariant equivalence relation, $g(u) \approx g(\infty)$; that is, $v \approx g(\infty)$. Thus, as $v \approx g(\infty)$, $g \in \mathbf{P}_1(N)$.

Assume that $v, w \in [\infty]$, $x, y \in [\infty]$ and $v \to w, x \to y \in H_{u,N}$. Then $(v, w), (x, y) \in O(\infty, u/N)$. Therefore, for some $S, T \in \mathbf{P}$,

$$S(\infty) = v, \qquad S(u/N) = w; \qquad T(\infty) = x, \qquad T(u/N) = y.$$

Hence $S, T \in \mathbf{P}_1(N)$ as $S(\infty), T(\infty) \in [\infty]$. Furthermore, $TS^{-1}(v) = x$ and $TS^{-1}(w) = y$; that is, $TS^{-1} \in \mathbf{P}_1(N)$. □

Theorem 3.7 $H_{u,N}$ *contains directed triangles iff there exists a unit* $\varepsilon \in \mathbb{Z}[i]$ *such that* $\varepsilon^2 u^2 \mp \varepsilon u \pm 1 \equiv 0 (\mathrm{mod}\, N)$.

Proof Suppose that $H_{u,N}$ contains a directed triangle. Because of the transitive action, the form of the directed triangle can be taken as $\infty \to \frac{u}{N} \to \frac{r}{N} \to \infty$. Since the edge conditions in Theorem 3.5 have to be provided for the edge $\frac{u}{N} \to \frac{r}{N}$, there are two cases. In the first, there exists a unit $\varepsilon \in \mathbb{Z}[i]$ such that $(u - r)\varepsilon = 1$ and $r \equiv -\varepsilon u^2 (\mathrm{mod}\, N)$, giving $\varepsilon^2 u^2 + \varepsilon u - 1 \equiv 0 (\mathrm{mod}\, N)$. In the second, there exists a unit $\varepsilon \in \mathbb{Z}[i]$ such that $(u - r)\varepsilon = 1$ and $r \equiv \varepsilon u^2 (\mathrm{mod}\, N)$, giving $\varepsilon^2 u^2 - \varepsilon u + 1 \equiv 0 (\mathrm{mod}\, N)$. Consequently, we obtain that $\varepsilon^2 u^2 \mp \varepsilon u \pm 1 \equiv 0 (\mathrm{mod}\, N)$.

Conversely, let $\varepsilon \in \mathbb{Z}[i]$ be a unit such that $\varepsilon^2 u^2 \mp \varepsilon u \pm 1 \equiv 0 (\mathrm{mod}\, N)$. Theorem 3.2 implies that there is a directed triangle $\infty \to \frac{u}{N} \to \frac{\varepsilon u - 1}{\varepsilon N} \to \infty$ in $H_{u,N}$. □

Theorem 3.8 *If* $1 + i | N$, *then* $H_{u,N}$ *contains no anti-directed triangles.*

Proof Suppose that $H_{u,N}$ contains an anti-directed triangle. Because of the transitive action, we may assume that an anti-directed triangle has the form $\infty \to \frac{u}{N} \leftarrow \frac{r}{N} \to \infty$. From the second edge, there exists a unit $\varepsilon \in \mathbb{Z}[i]$ such that $(r - u)\varepsilon = 1$ and $u \equiv \pm \varepsilon ur (\mathrm{mod}\, N)$. Since $1 = r\varepsilon - \varepsilon u$, then $r\varepsilon - \varepsilon u \equiv \pm \varepsilon ur (\mathrm{mod}\, N)$, giving $r - u \equiv \pm r (\mathrm{mod}\, N)$. Hence we have that $N | r \pm r - u$ means that $N | 2r - u$ or $N | -u$. But $N | -u$ is impossible. Therefore, we obtain that $N | 2r - u$. If $1 + i | N$, then $1 + i | u$, which contradicts to $(u, N) = 1$. □

3.3 Some results

Example 3.9 Let us take that $N = 2 + i$.

(i) If $u = 1$, then $\varepsilon^2 u^2 + \varepsilon u - 1 \equiv 0 (\mathrm{mod}\, N)$ is satisfied for $\varepsilon = -i$.

(ii) If $u = 1 + i$, then $\varepsilon^2 u^2 + \varepsilon u - 1 \equiv 0 (\mathrm{mod}\, N)$ is satisfied for $\varepsilon = i$.

Thus, the subgraphs $H_{1,2+i}$ and $H_{1+i,2+i}$ have directed triangles.

Example 3.10 For $N = 2i$, there is no unit $\varepsilon \in \mathbb{Z}[i]$ which satisfies the congruence $\varepsilon^2 u^2 \mp \varepsilon u \pm 1 \equiv 0 (\mathrm{mod}\, N)$. So, the subgraphs $H_{1,2i}$ and $H_{2i-1,2i}$ have no directed triangles.

Observation 3.11 The transformation $\phi := \left(\begin{smallmatrix} -\varepsilon u & \varepsilon^2u^2-\varepsilon u+1/\varepsilon N \\ -\varepsilon N & \varepsilon u-1 \end{smallmatrix}\right)$ which is defined by means of the congruence $\varepsilon^2u^2 \mp \varepsilon u \pm 1 \equiv 0 (\operatorname{mod} N)$ is an elliptic element of order 3. Furthermore, it is easily seen that

$$\phi\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}u\\N\end{pmatrix}, \qquad \phi\begin{pmatrix}u\\N\end{pmatrix} = \begin{pmatrix}u-1/\varepsilon\\N\end{pmatrix},$$

$$\phi\begin{pmatrix}u-1/\varepsilon\\N\end{pmatrix} = \begin{pmatrix}1/\varepsilon\\0\end{pmatrix} = \frac{1}{0} = \frac{-1}{0} = \frac{i}{0} = \frac{-i}{0}.$$

In [10], authors examined conjugacy classes of elliptic elements in the Picard group. And they proved that there is only one class of third-order elliptic elements in **P**, which means that any elliptic transformation of order 3 is a conjugate to

$$z \longrightarrow -\frac{1}{z+1}$$

or its square. So, if our calculation is true, ϕ must be conjugate to this transformation. It is well known that the transformations T_1 and T_2 are conjugates iff there exists a transformation $T \in \mathbf{P}$ such that $T_1 = TT_2^{-1}T$. Let us give an example.

Example 3.12 Let $N = 3$. If $u = 2$, then $\varepsilon^2u^2 - \varepsilon u + 1 \equiv 0(\operatorname{mod} N)$ is satisfied for $\varepsilon = 1$. Hence, $\frac{1}{0} \rightarrow \frac{2}{3} \rightarrow \frac{1}{3} \rightarrow \frac{1}{0}$ is a directed triangle in $H_{2,3}$. The corresponding elliptic element is $\phi = \left(\begin{smallmatrix} -2 & 1 \\ -3 & 1 \end{smallmatrix}\right)$. Furthermore, it can be easily seen that $\phi = \frac{-2z+1}{-3z+1}$ and $\psi = -\frac{1}{z+1}$ are conjugates.

Observation 3.13 It is well known that, because of the abstract group structure of **P** as a free product amalgamated with a modular group, each finite ordered elliptic element will be either of order 2 or 3. On the other hand, in [2, 11], authors give some results about a connection between the periods of elliptic elements of a chosen permutation group with the circuits in suborbital graphs of it. At this point, it is reasonable to conjecture the following.

Conjecture 3.14 $G_{u,N}$ is a forest if and only if it contains no triangles, that is, if and only if $\varepsilon^2u^2 \mp \varepsilon u \pm 1$ is not congruent to zero for modulo N.

Remark 3.15 A similar conjecture is given by Jones, Singerman and Wicks for the modular group in [12] and then proved by Akbaş [11]. In our case, the assertion which says that no edges cross to each other seems to be a problem.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
All authors completed the paper together, and read and approved the final manuscript.

Author details
[1]Faculty of Science, Department of Mathematics, Karadeniz Technical University, Trabzon, 61080, Turkey. [2]Faculty of Science and Arts, Department of Mathematics, Recep Tayyip Erdoğan University, Rize, 53100, Turkey.

Acknowledgements
Dedicated to Professor Hari M Srivastava.
The authors would like to thank Baris Kendirli for reading the first version of the manuscript and his enthusiastic support during XXV National Mathematics Symposium in Nigde. This work is partly supported by the research fund of Karadeniz Technical University (Project No: ARGEBD-9752).

Received: 23 November 2012 Accepted: 24 February 2013 Published: 18 March 2013

References

1. Bigg, NL, White, AT: Permutation Groups and Combinatorial Structures. London Mathematical Society Lecture Note Series, vol. 33. Cambridge University Press, Cambridge (1979)
2. Keskin, R: Suborbital graphs for the groups of modular and Picard modular. PhD thesis, Karadeniz Technical University, Trabzon, 1996
3. Dixon, JD, Mortimer, B: Permutation Groups. Graduate Texts in Mathematics, vol. 163. Springer, New York (1996)
4. Schoeneberg, B: Elliptic Modular Functions. Springer, Berlin (1974)
5. Hardy, GH, Wright, EM: An Introduction to the Theory of Numbers, 5th edn. Oxford University Press, Oxford (1979)
6. Sims, CC: Graphs and finite permutation groups. Math. Z. **95**, 76-86 (1967)
7. Jones, GA, Singerman, D: Complex Functions: an Algebraic and Geometric Viewpoint. Cambridge University Press, Cambridge (1987)
8. Neumann, PM: Finite permutation groups, edge-coloured graphs and matrices. In: Curran, MPJ (ed.) Topics in Group Theory and Computation. Academic Press, London (1977)
9. Tsuzuku, T: Finite Groups and Finite Geometries. Cambridge University Press, Cambridge (1982)
10. Yılmaz, N, Cangül, İN: Conjugacy classes of elliptic elements in the Picard group. Turk. J. Math. **24**, 209-220 (2000)
11. Akbaş, M: On suborbital graphs for the modular group. Bull. Lond. Math. Soc. **33**, 647-652 (2001)
12. Jones, GA, Singerman, D, Wicks, K: The Modular Group and Generalized Farey Graphs. London Mathematical Society Lecture Note Series, vol. 160, pp. 316-338. Cambridge University Press, Cambridge (1991)

doi:10.1186/1029-242X-2013-106
Cite this article as: Beşenk et al.: **Circuit lengths of graphs for the Picard group.** *Journal of Inequalities and Applications* 2013 **2013**:106.