Can. J. Math., Vol. XXXII, No. 6, 1980, pp. 1474–1481

CONGRUENCE SUBGROUPS OF THE PICARD GROUP

BENJAMIN FINE

Introduction. The Picard group $\Gamma = PSL_2(\mathbf{Z}[i])$ is the group of linear fractional transformations

$$z' = \frac{az + b}{cz + d}$$

with $ad - bc = \pm 1$ and a, b, c, d Gaussian integers.

Γ is of interest as an abstract group and in automorphic function theory. In an earlier paper [**1**], a decomposition of Γ as a free product with amalgamated subgroup was given and this was utilized to investigate Fuchsian subgroups. Karrass and Solitar used a similar decomposition to characterize abelian and nilpotent subgroups. Maskit [**6**], Mennicke [**7**] and Fine [**2**], used Γ to generate faithful representations of Fundamental Groups of Riemann Surfaces while more recently Wielenberg [**10**] represented certain knot and link groups as subgroups of Γ. In this paper, we will examine the structure of the congruence subgroups of Γ. Our technique will be to use the decomposition cited above [**1**], together with the Karrass–Solitar subgroup structure theory for free products with amalgamations [**3**]. Finally, we give a conjecture and some results concerning Fuchsian subgroups which are contained in congruence subgroups.

2. Congruence subgroups. If (α) is an ideal in $\mathbf{Z}[i]$, (necessarily principal), $\Gamma(\alpha)$ the *principal congruence subgroup* mod (α) consists of those transformations congruent to the identity transformation modulo (α).That is, those maps $z' = \dfrac{az + b}{cz + d}$ whose matrix $\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies

$$a \equiv d \equiv 1 \bmod (\alpha) \quad \text{and} \quad b \equiv c \equiv 0 \bmod (\alpha).$$

It is well known that in the modular group $M = PSL_2(\mathbf{Z})$ the principal congruence subgroups are free groups of finite rank ([**4**], [**8**]). There are two essentially different proofs of this, which we will briefly reiterate since the ideas of both will be explored relative to the Picard Group. The first proof is group theoretic and uses the fact that M is a free product of finite groups. A principal congruence subgroup H is torsion free and therefore it follows from the Kurosh Theorem that H is itself free. This

Received April 10, 1979.

idea will be pursued in Γ to give a structure theory for the $\Gamma(\alpha)$. The second proof is function theoretic and depends on the result that a principal congruence subgroup H of M being of finite index in M must be a finitely generated Fuchsian group [**4**]. Since H is torsion free and contains parabolic elements, it must be free [**8**]. The ideas in the second proof will lead to conjecture in Section 3 relating to Fuchsian subgroups of Γ contained in congruence subgroups.

Our main theorem is the following:

THEOREM 1. *If* $(\alpha) \neq (1 + i)$ *or* (2) *then* $\Gamma(\alpha)$ *is an* HNN *group with finitely generated free part* F *and base* K. K *is a free product with amalgamations of finitely many free groups, each of finite rank. Further, both the amalgamated subgroups in* K *and the associated subgroups in* $\Gamma(\alpha)$ *are conjugates of subgroups of the modular group* M.

See [**3**] for terminology regarding HNN groups.

Before giving the proof, we will give some needed preliminaries. First, we state the decomposition of Γ, which will be used throughout.

THEOREM. [**1**] Γ *is a free product of* G_1 *and* G_2 *with an amalgamated subgroup* H. G_1 *is the free product of* S_3 *and* A_4 *with a* 3-*cycle amalgamated,* G_2 *is* $S_3 * D_2$ *with a* 2-*cycle amalgamated, and* $H \cong PSL_2(\mathbf{Z}) = M$.

The proof of this is in [**1**]. It is important to note that generators can be found for Γ so that Γ has the form given in the theorem while in terms of these generators H is precisely the modular group, not just isomorphic to it.

Second, the following lemma is necessary:

LEMMA. *For every* $\alpha \in \mathbf{Z}\,(i)$, $\Gamma(\alpha)$ *is normal and of finite index in* Γ. *If* $(\alpha) \neq (1 + i)$ *or* (2), $\Gamma(\alpha)$ *is torsion free.*

Proof (of lemma). This is essentially the same as the proof in [**8**]. Since $\Gamma(\alpha)$ is the kernel of the map $\Gamma \rightarrow PSL_2(\mathbf{Z}[i]/_{(\alpha)})$ given by

$$\frac{az + b}{cz + d} \rightarrow \frac{a'z + b'}{c'z + d'}$$

where a', b', c', d' are the images of a, b, c, d under the natural map

$$\mathbf{Z}[i] \rightarrow \mathbf{Z}[i]/_{(\alpha)},$$

it is normal. Further, since $\mathbf{Z}[i]$ is a Euclidean ring, $\mathbf{Z}[i]/_{(\alpha)}$ consists mod (α) of those Gaussian integers with norms less than the norm of α. Therefore, $\mathbf{Z}[i]/_{(\alpha)}$ is a finite ring and $PSL_2(\mathbf{Z}[i]/_{(\alpha)})$ is a finite group. Since

$$|PSL_2(\mathbf{Z}[i]/_{(\alpha)}| = |\Gamma : \Gamma(\alpha)|,$$

$\Gamma(\alpha)$ has finite index. Finally if $V: z' \rightarrow \dfrac{az + b}{cz + d}$ has finite order, then trace

$V = 0$ or 1, [**4**], while if $V \in \Gamma(\alpha)$, trace $V \equiv 2 \bmod (\alpha)$. If trace $V = 1$ then $1 \equiv 2 \bmod (\alpha)$ which is impossible for a non-unit. If trace $V = 0$, then $0 \equiv 2 \bmod (\alpha)$ which is possible only if $\alpha|2$. Therefore, in this case $(\alpha) = (2)$ or $(1 + i)$, and for all other α, $\Gamma(\alpha)$ is torsion-free.

Now the proof of Theorem 1:

Proof. Let $(\alpha) \subset \mathbf{Z}[i]$, $(\alpha) \neq (1 + i)$ or (2), then from the preceding lemma, it follows that $\Gamma(\alpha)$ is a normal torsion-free subgroup of finite index in Γ. Since $\Gamma(\alpha)$ has finite index and the Picard group is finitely generated, $\Gamma(\alpha)$ is also finitely generated.

Since the Picard group Γ is a free product with amalgamated subgroup, $\Gamma = (G_1 * G_2{:}H)$ (G_1, G_2 and H as in the theorem stated above) it is a consequence of the Karrass–Solitar subgroup theorem (Theorem 5 in [**3**]) that $\Gamma(\alpha)$ is an HNN group. Its base K is then a tree product whose vertices are conjugates of G_1, or G_2 intersected with $\Gamma(\alpha)$, and whose amalgamated subgroups are conjugates of H, that is the modular group, intersected with $\Gamma(\alpha)$. The associated subgroups are then also conjugates of $H \cap \Gamma(\alpha)$. Since $\Gamma(\alpha)$ is normal, conjugates of G_1, G_2 or H intersected with $\Gamma(\alpha)$ are simply conjugates of $\Gamma(\alpha) \cap G_1$, $\Gamma(\alpha) \cap G_2$, or $\Gamma(\alpha) \cap H$. Therefore, what we must show is that the vertices and free part have the structure and finite rank conditions as in the statement of the theorem.

Since $\Gamma(\alpha)$ is of finite index in Γ and $\Gamma(\alpha) \not\subset PSL_2(\mathbf{Z})$ ($\Gamma(\alpha)$ always contains a non-real translation) it follows from Karrass-Solitar (Theorem 10 in [**3**]) that $\Gamma(\alpha) \cap H$ has finite index in $H \cong PSL_2(\mathbf{Z})$, and therefore $\Gamma(\alpha) \cap H$ is finitely generated. Note that if n is an integer $\Gamma(n) \cap H$ is just the principal congruence subgroup of level n in $PSL_2(\mathbf{Z})$. Therefore, $\Gamma(\alpha)$ is itself finitely generated, and so from Lemma 8 in [**3**] it follows that the free part F is finitely generated and the base K is a tree product of finitely many of its vertices. Since conjugates of $\Gamma(\alpha) \cap H$ are the amalgamated subgroups in K, Theorem 4 in [**3**] allows us to conclude that each vertex is finitely generated. What is left to show is that the vertices are free groups.

Let V be a vertex. Then V is a conjugate of $\Gamma(\alpha) \cap G_1$ or of $\Gamma(\alpha) \cap G_2$. We show that $V_1 = \Gamma(\alpha) \cap G_1$ or $V_1 = \Gamma(\alpha) \cap G_2$ must be free groups. Any conjugate is then free. Since V_1 is contained in $\Gamma(\alpha)$ it must be torsion-free and we prove that torsion-free subgroups of G_1 or G_2 are free groups. Suppose V_1 is torsion-free, $V_1 \subseteq G_1$. G_1 is a free product with amalgamated subgroup, $G_1 = \langle S_3 * A_4; \mathbf{Z}_3\rangle$ each factor being finite. By the Karass–Solitar subgroup theorem, V_1 is an HNN group with free part F_{V_1} and base K_{V_1}. Each vertex of K_{V_1} is a conjugate of a subgroup of S_3 or A_4 and therefore must be finite. But $K_{V_1} \subseteq V_1$ and so is torsion-free. So each vertex is trivial, and $V_1 = F_{V_1}$. Therefore, if $V_1 \subseteq G_1$, it is either trivial or free. Since G_2 is also a free product with amalgamated subgroup of finite factors, an identical argument works if $V_1 \subseteq G_2$. In any case a non-trivial vertex must be a free group (and since finitely-generated) of finite rank.

Now we handle the two special cases, that is, when $\alpha = 1 + i$, and when $\alpha = 2$.

THEOREM 2. *$\Gamma(1 + i)$ has index 6 in Γ and is decomposable as a free product of two groups with amalgamated subgroup; $\Gamma(1 + i) = \langle H_1 * H_2 : U\rangle$. In particular*

$$H_1 \cong D_{2*\mathbf{Z}_2}[(\mathbf{Z}_2 * \mathbf{Z}_2) *_{\mathbf{Z}} (\mathbf{Z}_2 * \mathbf{Z}_2)] \quad and \quad H_2 \cong \mathbf{Z}_2 * D_2$$

while U, the amalgamated subgroup, is $\mathbf{Z} * \mathbf{Z}_2$. $\Gamma(2)$ has index 24, and is a subgroup of index 4 in $\Gamma(1 + i)$. $\Gamma(2)$ has similar but more complicated generalized free product decomposition.

Proof. In [**2**], the following is given as a presentation for the Picard group.

$$\Gamma = \langle a, l, t, u; a^2 = l^2 = (al)^2 = (tl)^2 = (ul)^2 = (at)^3 = (ual)^3 = [t, u] = 1\rangle$$

where a is $z' = -1/z$, t is $z' = z + 1$, u is $z' = z + 1$, l is $z' = -z$.

Since $(1 + i)|2$, $(2) \subset (1 + i)$, and $1 \equiv -1 \bmod (1 + i)$ it follows that $l \in \Gamma(1 + i)$. Further since $1 + i \equiv 0 \bmod (1 + i)$ then tu, which is $z' = z + (1 + i)$, is also in $\Gamma(1 + i)$. Therefore, since $\Gamma(1 + i) \lhd \Gamma$, $\Gamma(1 + i)$ must contain as a subgroup, $N(l, tu)$, the normal closure in Γ of the elements l and tu.

Now

$$\Gamma/_{N(l,tu)} = \{a, t; a^2 = t^2 = (at)^3 = 1\} \cong S_3$$

which we found by letting $l = 1$ and $tu = 1$ in the presentation for Γ above and then simplifying. Therefore, $|\Gamma : N(l, tu)| = 6$. Further, $\mathbf{Z}[i]/_{(1+i)} \cong GF(2)$ the Galois field with 2 elements, so

$$\Gamma/_{\Gamma(1+i)} \cong PSL_2(GF(2)) \cong S_3.$$

From this $|\Gamma : \Gamma(1 + i)| = 6$ also, from which it follows that $\Gamma(1 + i) = N(l, tu)$. Using this we get a presentation for $\Gamma(1 + i)$.

Choosing coset representatives $1, a, t, at, ata, atat$ with $\bar{a} = a$, $\bar{t} = t$, $\bar{u} = u$, $\bar{l} = 1$, for $N(l, tu)$ in Γ, and then employing the Reidemeister–Shreier process we get the following presentation (after simplification) for $N(l, tu) = \Gamma(1 + i)$:

$$\Gamma(1 + i) = \langle l, m, n, A, B; l^2 = (An)^2 = (Bm)^2 = m^2 = n^2(mn)^2 = (Al)^2 = (Bl)^2 = (AB)^2 = 1\rangle$$

https://doi.org/10.4153/CJM-1980-116-7 Published online by Cambridge University Press

with

$$l = l; z' = -z, n = ltu; z' = -z - i - 1, n = a(tu^{-1}l)\, a = a(lt^{-1}u)a;$$

$$z' = \frac{-z}{(1-i)z+1}\,; A = u^{-1}t; z' = z + (1-i), B = a(tu)a;$$

$$z' = \frac{-z}{(1+i)z-1}\,.$$

Let

$$H_1 = \langle m, n, A, B; m^2 = n^2 = (mn)^2 = (mA)^2 = (nB)^2 = (AB)^2 = 1\rangle$$

and let

$$H_2 = \langle l, A, B, l^2 = (lA)^2 = (lB)^2 = (AB)^2 = 1\rangle.$$

Then $\Gamma(1+i)$ is given by $H_1 * H_2$ with the identifications $A = A$, $B = B$.

What we must show then is that H_1, H_2 have the structure given in the statement of the theorem and that the identifications yield isomorphisms of subgroups; that is that $\langle A, B\rangle \cong \mathbf{Z} * \mathbf{Z}_2$ in both H_1 and H_2.

Applying Tietze transformations, H_1 can be rewritten as

$$H_1 = \langle m, c, x, z; m^2 = c^2 = (nc)^2 = x^2 = (xz)^2 = (zc)^2 = 1\rangle$$

by letting $c = mn$, $x = mA$, $z = mABn$.

Therefore,

$$H_1 \cong \langle m, c, z; m^2 = c^2 = (mc)^2 = 1\rangle * \langle x; z, c;$$
$$x^2 = z^2 = c^2 = (zc)^2 = 1\rangle$$

with the identification $c = c$.

Calling H_{11} the group defined by $\langle m, c, z, m^2 = c^2 = (mc)^2 = 1\rangle$, we see that $H_{11} \cong D_2$, while the group H_{12}, defined by $\langle x, c, z; x^2 = (xz)^2 = c^2 = (zc)^2 = 1\rangle$ is isomorphic to $(\mathbf{Z}_2 * \mathbf{Z}_2) *_{\mathbf{Z}} (\mathbf{Z}_2 * \mathbf{Z}_2)$ where this means that H_{12} is the free product of two infinite dihedral groups with an infinite cyclic group amalgamated. The identification yields isomorphic subgroup $\langle c\rangle = \mathbf{Z}_2$ in each case. Further, the subgroup generated by A, B is $\langle xm, x^{-1}nz\rangle \cong \mathbf{Z} * \mathbf{Z}_2$.

Now

$$H_2 = \langle l, A, B; l^2 = (lA)^2 = (lB)^2 = (AB)^2 = 1\rangle$$
$$\cong \langle l, \alpha, \beta; l^2 = \alpha^2 = \beta^2 = (\alpha\beta)^2 = 1\rangle$$

letting $\alpha = lA$, $\beta = lB$.

Thus, $H_2 \cong \mathbf{Z}_2 * D_2$ while the subgroup generated by A, B is

$$\langle l\alpha, l\beta\rangle \cong \mathbf{Z} * \mathbf{Z}_2.$$

Therefore, H_1 and H_2 have the desired structure and the identifications yield isomorphisms of subgroups.

An identical technique can be utilized to find the structure of $\Gamma(2)$. Since $l \in \Gamma(2)$ and $\Gamma(2) \lhd \Gamma$, $N(l) \subseteq \Gamma(2)$ where as before $N(l)$ is the normal closure in Γ of l. Letting $l = 1$ we get

$$\Gamma/_{N(l)} = \langle a, t, u; a^2 = t^2 = (at)^3 = (au)^3 = u^2 = [t, u] = 1\rangle$$

which has order 24 [**1**], so $|\Gamma : N(l)| = 24$. Examining the 24 coset representatives for $N(l)$ in Γ with $\bar{a} = a$, $\bar{t} = t$, $\bar{u} = u$, $\bar{l} = 1$ (see [**9**]) then writing them as transformations, it can be seen that none of them are congruent to the identity mod 2. Therefore, $N(l)$ must be equal to $\Gamma(2)$ and $\Gamma(2)$ must have index 24. Since $\Gamma(2) \subset \Gamma(1 + i)$ it has index 4 in $\Gamma(1 + i)$. Using the same coset representatives and the Reidemeister–Shreier process, we get a presentation for $\Gamma(2)$ from which we can deduce the complicated decomposition. In particular,

$$\Gamma(2) \cong \langle K_1 * K_2; V\rangle \quad \text{where} \quad K_1 \cong (\mathbf{Z}_2 * \mathbf{Z}_2) *_{\mathbf{Z}} (\mathbf{Z}_2 * \mathbf{Z}_2)$$

and

$$K_2 \cong ((\mathbf{Z}_2 * \mathbf{Z}_2) *_{\mathbf{Z}} (\mathbf{Z}_2 * \mathbf{Z})] *_{V_1}$$
$$([(\mathbf{Z}_2 * \mathbf{Z}_2) *_{\mathbf{Z}} (\mathbf{Z}_2)] *_{(\mathbf{Z}_2 * \mathbf{Z}_2)} [(\mathbf{Z}_2 * \mathbf{Z}_2) *_{\mathbf{Z}} (\mathbf{Z}_2 * \mathbf{Z}_2)])$$

where V_1 the amalgamated subgroup in K_2 is $\mathbf{Z}_2 * \mathbf{Z}_2$ and V the amalgamated subgroup in $\Gamma(2)$ is $\cong \mathbf{Z}_2 * \mathbf{Z}_2 * \mathbf{Z} * \mathbf{Z}$. Note that our notation $(\mathbf{Z}_2 * \mathbf{Z}_2) *_{\mathbf{Z}} (\mathbf{Z}_2 * \mathbf{Z}_2)$ stands for the free product of 2 infinite dihedral groups with an infinite cyclic subgroup amalgamated.

We mention that an algebraic procedure for obtaining faithful non-Fuchsian representations of Riemann surface groups in Γ was given in [**2**], and the images are all contained in $\Gamma(2)$.

3. Fuchsian subgroups. Since Γ is nowhere discontinuous in $\mathbf{C}$ [**4**], Fuchsian subgroups are of infinite index. The ideas of the function theoretic proof of the freeness of the principal congruence subgroups of the modular group cannot be carried over to Γ directly. However, these ideas can be applied to Fuchsian subgroups which are contained in congruence subgroups. If $(\alpha) \neq (1 + i)$ or (2) and $F \subseteq \Gamma(\alpha)$, F Fuchsian, then F is torsion-free and thus either free or a Riemann surface group [**4**]. If F has parabolic elements, it is free. Also if F is contained in the modular group, it is free. We then conjecture:

Conjecture 1. A Fuchsian group entirely contained in a principal congruence subgroup $\Gamma(\alpha)$, $\alpha \neq (1 + i)$ or (2), is free. Since the most visible examples of Fuchsian subgroups of the $\Gamma(\alpha)$ are the subgroups of $\Gamma(\alpha) \cap PSL_2(\mathbf{Z})$, a stronger form of the conjecture would be

https://doi.org/10.4153/CJM-1980-116-7 Published online by Cambridge University Press

Conjecture 1′. A Fuchsian subgroup entirely contained in $\Gamma(\alpha)$, $(\alpha) \neq (1 + i)$ or (2) must be conjugate to a subgroup of the modular group.

A partial result along these lines is:

THEOREM 3. *A finitely generated Fuchsian group* $F \subset \Gamma(\alpha)$ *with* $(\alpha) \neq (1 + i)$ *or* (2) *and having either trivial or non-cyclic intersection with all conjugates of the modular group is free.*

Proof. If $F \subset \Gamma(\alpha)$, $(\alpha) \neq (1 + i)$ or (2), then F must be torsion-free. Since F is a subgroup of Γ, from Karrass–Solitar, it is an HNN group whose base is a tree product. Since F is torsion-free, the same argument as in Theorem 1 shows that each vertex is a free group. Assume that F intersects all conjugates of M trivially. Since M is the amalgamated subgroup in Γ, a result of Karrass–Solitar is that F must be the free product of the free part and its vertices. Each vertex, however, is free so F being a free product of free groups is free.

Now assume that F has non-trivial, non-cyclic intersection with some conjugate of M. There is no loss of generality in assuming that this intersection is with M itself (using a conjugate of F is necessary). We can further assume that F contains no parabolic elements for if it did, it would be free. So F is purely hyperbolic. Suppose $T, U \in PSL_2(\mathbf{Z})) \cap F$ with T, U hyperbolic and $\langle T, U \rangle$ non-cyclic. Since the only abelian subgroups of a Fuchsian group are cyclic, it follows that T and U do not commute. Therefore, T, U have distinct sets of fixed points [**4**]. Further, the fix points of T, U are on the real axis, since T, U are real and hyperbolic. F, being a Fuchsian group, has a principal fixed circle C, and the fixed points of hyperbolic maps in F lie on C. Therefore, C has at least 3 points (the fixed points of T, U) in common with the real axis and so must be the real axis. Therefore, the fixed circle of F is the real axis and $F \subseteq PSL_2(\mathbf{R})$. But

$$PSL_2(\mathbf{R}) \cap \Gamma = PSL_2(\mathbf{Z})$$

so F is entirely contained in the modular group. Since it is torsion-free, it must be free.

REFERENCES

1. B. Fine, *Fuchsian subgroups of the Picard group*, Can. J. Math. *28* (1976), 481–485.

2. ——— *The structure of* $PSL_2(R)$, Annals of Mathematics, Study *79* on Discontinuous Groups and Riemann Surface (1974).

3. A. Karrass and D. Solitar, *The subgroups of a free product of two groups with an amalgamated subgroup*, Trans. Amer. Math. Soc. *150* (1970), 227–255.

4. J. Lehner, *Discontinuous groups and automorphic functions*, Math Surveys No. *8*, Amer. Math. Soc. (Providence, R.I., 1964).

5. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory* (Interscience, Wiley, New York, 1966).

6. B. Maskit, *On a class of Kleinian groups*, Ann. Academia Scient. Fennical, I. Mathematica, Helsinki (1969), 1–7.

7. J. Mennicke, *A note on regular coverings of closed orientable surfaces*, Proc. Glasgow Math. Assoc. *5* (1969), 49–66.

8. M. Newman, *Integral matrices* (Academic Press, N.Y., 1972).

9. H. Waldinger, *On the subgroups of the Picard group*, Proc. Amer. Math. Soc. *16* (1965), 1375–1378.

10. N. Wielenberg, *The structure of certain subgroups of the Picard group* (to appear in Univ. of Pittsburgh Press).

Fairfield University,
Fairfield, Connecticut