TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 281, Number 2, February 1984

HOMOMORPHISMS OF COCOMPACT FUCHSIAN GROUPS ON $\mathrm{PSL}_2(Z_{p^n}[x]/(f(x)))$

BY

JEFFREY COHEN

ABSTRACT. We obtain conditions under which $\mathrm{PSL}_2(Z_{p^n}[x]/(f(x)))$ is a factor of (l, m, n). Using this, certain results about factors of cocompact Fuchsian groups are obtained. For example, it is shown that:

(i) Γ has infinitely many simple nonabelian factors.

(ii) Γ has factors with nontrivial center.

(iii) For each n, there exists m such that Γ has at least n factors of order m.

Further, all factored normal subgroups can be taken torsion-free. Also, new Hurwitz groups and noncongruence subgroups of the modular group are obtained.

1. Introduction. Any cocompact Fuchsian group Γ may be represented as a (discrete) subgroup of $\mathrm{PSL}_2(R)$ where R is an algebraic number ring. The group Γ, therefore, has finite factors which are subgroups of $\mathrm{PSL}_2(\bar{R})$, where $\bar{R}$ is a finite quotient ring of R. For $R = GF(q)$ this situation has been investigated in [7] with Γ restricted to the class of triangle groups. We shall rework [7] for more general R and obtain generalizations of Theorems 6, 7, and 8 of that paper. Explicitly, new noncongruence subgroups of the modular group and new Hurwitz groups will be constructed.

From our results on factors of triangle groups it is not particularly difficult to obtain results on factors of arbitrary cocompact Fuchsian groups Γ. For example, the proof of a folk theorem emerges. This is a demonstration that Γ always has simple nonabelian factors, a fact which seems not to be found in the existing literature and which will enable us to generalize the Bundgaard-Nielsen-Fox theorem and a result of Leech as was promised in [1]. While investigating Hurwitz groups, Leech [5] found a miscalculation in [9], an early and otherwise excellent paper pertaining to Hurwitz groups. This led Leech to ask whether a Hurwitz group could have a nontrivial center—a question he answered affirmatively in [6] and which could also be resolved by the methods of [1], as noted there. Here, however, it shall be further established that any cocompact Γ has a torsion-free normal subgroup N such that Γ/N has nontrivial center. Finally, we shall generalize a result of [1] by proving (see Theorem 8) that no bound exists for the number of factors of Γ having fixed order.

Received by the editors June 30, 1980 and, in revised form, April 22, 1981.

1980 *Mathematics Subject Classification.* Primary 20H10: Secondary 20H05, 20H15, 20H25.

Key words and phrases. Cocompact Fuchsian group, noncongruence subgroup of the modular group, Hurwitz group, simple factor, factor with center, matrix group over $Z_{p^n}[x]$.

0002-9947/84 $1.00 + $.25 per page

2. Ring theoretic preliminaries. Let $q = p^m$ for p a prime number. Then $GF(q)$ (the field of q elements) is the homomorphic image of $Z[\alpha]$ where α satisfies a polynomial $f(x) \in Z[x]$ of degree m which is irreducible modulo p. We define $Z_{p^n}[\alpha]$ to be the ring homomorphic image of $Z[\alpha]$ modulo p^n, or more explicitly,

$$Z_{p^n}[\alpha] = \left\{ \sum_{i=0}^{m-1} a_i \alpha^i : a_i \in Z_{p^n} \right\} \simeq \frac{Z_{p^n}[x]}{(f(x))}$$

with multiplication subject to $f(\alpha) = 0$.

PROPOSITION 1. $|Z_{p^n}[\alpha]| = (p^n)^n = q^n$.

As usual, if R is a ring denote its group of invertible elements by R^*.

PROPOSITION 2. $|Z_{p^n}^*[\alpha]| = q^{n-1}(q-1)$. *In fact* $\{p\sigma : \sigma \in Z_{p^{n-1}}[\alpha]\}$ *is the set of noninvertibles of* $Z_{p^n}[\alpha]$.

PROOF. Let $Z_{p^n}[\alpha] \xrightarrow{\pi} Z_p[\alpha]$ be the natural epimorphism. We need only show that $\sigma \in Z_{p^n}^*[\alpha]$ if and only if $\pi(\sigma) \neq 0$. If $\pi(\sigma) \neq 0$, then as $Z_p[\alpha]$ is a field one can choose τ so $\pi(\tau) = (\pi(\sigma))^{-1}$. Thus $\pi(\sigma\tau) = \pi(\sigma) \cdot \pi(\tau) = 1$ so that $\sigma\tau = 1 + pV$ for some $V \in Z_{p^{n-1}}[\alpha]$. Letting $\sigma' = \tau \sum_{i=0}^{n-1} (-pV)^i$ it follows that $\sigma\sigma' = 1 + (-1)^{n-1}(pV)^n = 1$ so that σ is invertible; since invertibles map to invertibles, the converse is clear.

3. Matrix groups over $Z_{p^n}[\alpha]$. As usual, let $\mathrm{SL}_2(R)$ denote the group of all 2×2 matrices of unit determinant. Bucking tradition, define $\mathrm{PSL}_2(R) = \mathrm{SL}_2(R)/\{\pm I\}$; the reason for this definition is that for $R = Z_{2^n}[\alpha]$, $\mathrm{PSL}_2(R)$ usually has nontrivial center.

PROPOSITION 3. *Let* $\mathrm{SL}_2(Z_{p^2}[\alpha]) \xrightarrow{\theta} \mathrm{SL}_2(Z_p[\alpha])$ *be the canonical homomorphism. Then the* $\mathrm{SL}_2(Z_{p^2}[\alpha])$*-conjugacy classes of* $\ker\theta$ *satisfy the following*:

(i) *If* $p \neq 2$, *each nonidentity class contains a unique representative of the form* $I + p\left(\begin{smallmatrix} 0 & \sigma \\ 1 & 0 \end{smallmatrix}\right)$ *with* $\sigma \in Z_p[\alpha]$, *unless* $\sigma = 0$ *in which case there is another class whose representative is obtained by conjugation of* $I + p\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ *by a matrix with nonsquare determinant. In each nonidentity class the number of elements is given by*

(a) $q(q-1)$ *if* σ *is not a square and there are precisely* $\frac{1}{2}(q-1)$ *classes*,

(b) $q(q+1)$ *if* $\sigma \neq 0$ *is a square with* $\frac{1}{2}(q-1)$ *such classes*,

(c) $\frac{1}{2}(q+1)(q-1)$ *if* $\sigma = 0$ *with* 2 *classes*.

(ii) *If* $p = 2$, *there are* $(2^m + 1)(2^m - 1)$ *conjugates of* $I + 2\left(\begin{smallmatrix} 0 & \sigma \\ 1 & 0 \end{smallmatrix}\right)$ *with* 2^m *classes of this type. Further there exist* 2^m *central elements* $\left(\begin{smallmatrix} 1+2\tau & 0 \\ 0 & 1+2\tau \end{smallmatrix}\right)$ *with* $\tau \in Z_2[\alpha]$.

PROOF. The kernel of θ consist of those matrices $I + pA$ where the trace of A is congruent to 0 modulo p. Thus $|\ker\theta| = q^3$ and $|\mathrm{SL}_2(Z_{p^2}[\alpha])| = q^4(q+1)(q-1)$ so that to establish the proposition it suffices to compute the orders of the centralizers of all elements in question. A simple computation yields that the centralizer in $\mathrm{SL}_2(Z_{p^2}\alpha)$ of $I + p\left(\begin{smallmatrix} 0 & \sigma \\ 1 & 0 \end{smallmatrix}\right)$ is

$$\left\{ \begin{pmatrix} a & \sigma c + pk \\ c & a + ph \end{pmatrix} : a, c \in Z_{p^2}[\alpha], h, k \in Z_p[\alpha], a^2 - \sigma c^2 + p(ah - ck) = 1 \right\}.$$

Therefore if σ is not a square, choosing a and c so that not both are noninvertible while choosing h and k arbitrary makes the quadratic polynomial take an invertible value. Since this polynomial takes all nonzero values modulo p, it is clear it takes all values in $Z_{p^2}[\alpha]$. By Proposition 2, the centralizer has order

$$(q^4 - q^2)(q)(q)/q(q-1) = q^3(q+1).$$

If $\sigma \neq 0$ is a square not both of a and c are noninvertible. Now under this restriction, however, the quadratic can equal 0 modulo p if $a \in \{\pm c\sqrt{\sigma} + \tau p: c \in Z_{p^2}^*[\alpha],\ \tau \in Z_p[\alpha]\}$. This set has cardinality $(p,2)^{-1}2(q^2 - q)q$. Thus the centralizer order is given by

$$\frac{[(q^4 - q^2) - 2(q^2 - q)q](q)(q)}{(q^2 - q)} = q^3(q-1) \quad \text{if } p \neq 2,$$

$$\frac{[(q^4 - q^2) - (q^2 - q)q](q)(q)}{(q^2 - q)} = q^4 = 2^{4m} \quad \text{if } p = 2.$$

If $\sigma = 0$ and $p = 2$, the above argument goes through. If $\sigma = 0$ and $p \neq 2$ we have that $a = \pm 1 + pt$ with $t \in Z_p[\alpha]$, $c \in Z_{p^2}[\alpha]$ and $k \in Z_p[\alpha]$ may be chosen arbitrary forcing h. Thus the centralizer has order $2q(q^2)(q) = 2q^4$. Since the determinant of any matrix centralizing $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ has square determinant, one obtains another class in the prescribed manner. To see that all conjugacy classes have been accounted for, note that

$$\det\begin{pmatrix}0 & \sigma\\ 1 & 0\end{pmatrix} = -0$$

and that

$$1 + \tfrac{1}{2}(q-1)\,q(q-1) + \tfrac{1}{2}(q-1)\,q(q+1) + 2\tfrac{1}{2}(q+1)(q-1) = q^3,$$

$$2^m(2^m+1)(2^m-1) + 2^m = 2^{3m}.$$

Both answers are the same number as $|\ker\theta|$.

COROLLARY 1. *Suppose $p \neq 2$ and $\operatorname{tr}(A) \equiv \operatorname{tr}(B) \equiv 0 \pmod p$. Then $I + pA$ is $\mathrm{SL}_2(Z_{p^2}[\alpha])$-conjugate to $I + pB$ if and only if $\det A \equiv \det B \pmod p$, provided $\det A \not\equiv 0$. If $\det A \equiv 0$ then there is one other nonidentity conjugacy class.*

Suppose $p = 2$ and that A and B are not multiples of I with $\operatorname{tr}(A) \equiv \operatorname{tr}(B) \equiv 0 \pmod 2$. Then $I + pA$ and $I + pB$ are conjugate if and only if $\det A \equiv \det B \pmod 2$.

PROPOSITION 4. *Let $n \geq 3$,*

$$A = \begin{pmatrix} 1 + pa & 1 + pc \\ pb & 1 + pd \end{pmatrix}.$$

Then over $Z_{p^2}[\alpha]$,

$$A^n = \begin{pmatrix} 1 + p\left[na + \binom{n}{2}b\right] & n + p\left[\binom{n}{2}a + \binom{n}{3}b + nc + \binom{n}{2}d\right] \\ npb & 1 + p\left[\binom{n}{2}b + nd\right] \end{pmatrix}.$$

In particular if $p \geqslant 5$,

$$A^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

PROOF. (Induction on n.)

COROLLARY 2. *For* $p \geqslant 5$, $\mathrm{SL}_2(Z_{p^2}[\alpha])$ *contains no subgroup isomorphic to* $\mathrm{SL}_2(Z_p[\alpha])$.

PROOF. Since $\mathrm{PSL}_2(Z_p[\alpha])$ is simple, the only nontrivial normal subgroup of $\mathrm{SL}_2(Z_p[\alpha])$ is $\langle \pm 1 \rangle$. Thus any subgroup G of $\mathrm{SL}_2(Z_{p^2}[\alpha])$ with $G \simeq \mathrm{SL}_2(Z_p[\alpha])$ must meet $\operatorname{Ker}\theta$ trivially. Hence θ/G is an isomorphism so that G contains an element of the form A. Thus $I \neq A^p \in G \cap \operatorname{Ker}\theta$.

For $n \geqslant n'$ let $\theta_{n'}^n$: $\mathrm{SL}_2(Z_{p^n}[\alpha]) \to \mathrm{SL}_2(Z_{p^{n'}}[\alpha])$ denote the canonical homomorphism. Then the following are clear:

$$\theta_n^n = \text{identity}, \qquad \theta_1^2 = \theta;$$
$$\theta_{n''}^{n'}\theta_{n'}^n = \theta_{n''}^n \quad \text{whenever } n \geqslant n' \geqslant n''.$$

LEMMA 1. $\operatorname{Ker}\theta_{n-1}^n$ *is an elementary abelian p-group of order* q^3.

PROOF. Since $\operatorname{Ker}\theta_{n-1}^n = \{I + p^{n-1}A\colon \operatorname{tr} A \equiv 0 \pmod p\}$, it follows that $|\operatorname{Ker}\theta_{n-1}^n| = q^3$. To see that $\operatorname{Ker}\theta_{n-1}^n$ is elementary abelian, note that since $2n - 2 \geqslant n$,

$$\begin{aligned}(1 + p^{n-1}A)(1 + p^{n-1}B) &= p^{n-1}(A + B) + p^{2n-2}AB + I \\ &\equiv 1 + p^{n-1}(A + B) \pmod{p^n}.\end{aligned}$$

Thus $(I + p^{n-1}A)^p \equiv I + p^{n-1}(pA) \equiv I$ so that $\operatorname{Ker}\theta_{n-1}^n$ has exponent p.

A simple induction now yields

PROPOSITION 5.

$$|\mathrm{SL}_2(Z_{p^n}[\alpha])| = q^{3n-2}(q+1)(q-1),$$
$$|\mathrm{PSL}_2(Z_{p^n}[\alpha])| = \begin{cases} q(q+1)(q-1), \\ \frac{1}{2}q^{3n-2}(q+1)(q-1) & \text{otherwise}. \end{cases}$$

THEOREM 1. *Suppose* $G \leqslant \mathrm{SL}_2(Z_{p^2}[\alpha])$ *and* $\theta(G) = \mathrm{Sl}_2(Z_p[\alpha])$. *If* $p = 3$, *further assume tat* $G \cap \operatorname{Ker}\theta \neq (1)$. *Then* $G = \mathrm{SL}_2(Z_{p^2}[\alpha])$ *when* $p \neq 2$.

PROOF. Let $H = G \cap \operatorname{Ker}\theta$. Then by Lemma 1, $\operatorname{Ker}\theta$ is abelian so that $H \lhd \langle \operatorname{Ker}\theta, G\rangle = \mathrm{SL}_2(Z_{p^2}[\alpha])$, because θ/G is surjective. By Corollary 2 if $p \geqslant 5$, then $H \neq (1)$ and, by hypothesis, if $p = 3$, $H \neq (1)$. Thus H is a union of conjugacy classes so that by Proposition 3 there exist nonnegative integers a, b, c, i with

$$(*) \quad p^i = |H| = 1 + aq(q-1) + bq(q+1) + \tfrac{1}{2}c(q+1)(q-1),$$
$$1 \leqslant i \leqslant 3m, \quad 0 \leqslant c \leqslant 2, \quad 0 \leqslant a, b \leqslant \tfrac{1}{2}(q-1).$$

Thus p divides $1 + \frac{1}{2}c(q+1)(q-1) = \frac{1}{2}[cq^2 + (2-c)]$. As $(p,2) = 1$, we have $p \mid (2-c)$ so that by $(*)$ $c = 2$. Therefore by Proposition 3 and normality of H, H contains all $\mathrm{GL}_2(Z_{p^2}[\alpha])$-conjugates of $S = p\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Hence for all $\sigma \in Z_p^*[\alpha]$, by Corollary 1,

$$T = 1 + p\begin{pmatrix} 0 & \sigma \\ 0 & 0 \end{pmatrix} \in H.$$

By multiplicative closure $ST \in H$ and

$$ST = 1 + p\begin{pmatrix} 0 & \sigma \\ 1 & 0 \end{pmatrix}.$$

By Proposition 3, H contains elements from each $\mathrm{SL}_2(Z_{p^2}[\alpha])$-conjugacy class of $\operatorname{Ker}\theta$. This, together with the normality of H, yields that $H = \operatorname{Ker}\theta$, proving the result.

THEOREM 2. *Suppose* $G \leqslant \mathrm{SL}_2(Z_{p^n}[\alpha])$ *and* θ_1^n/G *is surjective.*
(a) *If* $p \geqslant 5$, *then* $G = \mathrm{SL}_2(Z_{p^n}[\alpha])$.
(b) *If* $p = 3$ *and* $\theta_2^n(G) \cap \operatorname{Ker}\theta_1^2 \neq (1)$, *then* $G = \mathrm{SL}_2(Z_{3^n}[\alpha])$.
(c) *If* $p = 2$, θ_3^n/G *is surjective, and* $\theta_4^n(G) \cap \operatorname{Ker}\theta_3^4 \neq (1)$ *then* $G = \mathrm{SL}_2(Z_{2^n}[\alpha])$.

PROOF. If $n = 2$ this is just Theorem 1. Suppose $n > 2$ is minimal for a counterexample. Since by hypothesis

$$\mathrm{SL}_2\big(Z_p[\alpha]\big) = \theta_1^n(G) = \theta_1^{n-1}\theta_{n-1}^n(G),$$

it follows by induction that

$$\theta_{n-1}^n(G) = \mathrm{SL}_2\big(Z_{p^{n-1}}[\alpha]\big)$$

and therefore

$$\mathrm{SL}_2\big(Z_{p^n}[\alpha]\big) = G \cap (\operatorname{Ker}\theta_{n-1}^n).$$

Let p be a Sylow p-subgroup of G and $H = P \cdot (\operatorname{Ker}\theta_{n-1}^n)$ so that H is a Sylow p-subgroup of $\mathrm{SL}_2(Z_{p^n}[\alpha])$. Let $T \in \operatorname{Ker}\theta_{n-1}^n$; then

$$T = I + p^{n-1}A = \begin{pmatrix} 1 + p^{n-1}a & p^{n-1}c \\ p^{n-1}b & 1 - p^{n-1}a \end{pmatrix}.$$

Define

$$S = \begin{cases} I + p^{n-2}A & \text{if } n \geqslant 4, \\ \big(1 + \frac{1}{2}p^2(a^2 + bc)\big)(1 + pA) & \text{if } n = 3. \end{cases}$$

Then if $n \geqslant 4$,

$$\det S = 1 - p^{2n-4}(a^2 + bc) = 1.$$

If $n = 3$,

$$\begin{aligned} \det S &= \big[1 + \tfrac{1}{2}p^2(a^2 + bc)\big]^2\big[1 - p^2(a^2 + bc)\big] \\ &= \big[1 + p^2(a^2 + bc)\big]\big[1 - p^2(a^2 + bc)\big] = 1. \end{aligned}$$

Therefore $S \in \operatorname{Ker} \theta_1^n$ a normal p-subgroup of $\mathrm{SL}_2(Z_{p^n}[\alpha])$ so that S is a member of every Sylow p-subgroup and in particular $S \in H$. Now if $n \geqslant 4$,

$$S^p = \left(1 + p^{n-2}A\right)^p = 1 + p^{n-1}A + p^n \sum_{j=2}^{p} \binom{p}{j} p^{j(n-2)-n} A^j$$

$$= 1 + p^{n-1}A = T.$$

If $n = 3$ a similar calculation shows that $S^p = T$. Thus T is in the Frattini subgroup of H so that $P = H$ and the result follows.

THEOREM 3. *Suppose* $Z_3[\alpha]$ *is not* $GF(3)$. *Then* $\mathrm{SL}_2(Z_{3^n}[\alpha])$ *contains no subgroup isomorphic to* $\mathrm{SL}_2(Z_3[\alpha])$ *unless* $n = 1$.

PROOF. Suppose $n \geqslant 2$ and $G \leqslant \mathrm{SL}_2(Z_{3^n}[\alpha])$ with $G \simeq \mathrm{SL}_2(Z_3[\alpha])$ and $Z_3[\alpha] \neq GF(3)$. Then $\mathrm{PSL}_2(Z_3(\alpha)) \not\leftarrow \mathrm{SL}_2(Z_3[\alpha])$ so that θ_1^n/G is an isomorphism. Let $\bar{G} = \theta_2^n(G)$; then $\theta_1^2/\bar{G}$ is an isomorphism. Let $\sigma \in Z_{3^2}[\alpha]$ be arbitrary; then since $\theta_1^2/\bar{G}$ is an isomorphism, there exists a unique $K \in \bar{G}$ with

$$K = \begin{pmatrix} 1 + 3a & \sigma + 3b \\ 3c & 1 + 3d \end{pmatrix}.$$

As $\det K = 1$, we deduce $a + d \equiv c\sigma \pmod 3$. Thus remembering we are working modulo 3^2,

$$K^3 = \begin{pmatrix} 1 & 3(\sigma + c\sigma^2) \\ 0 & 1 \end{pmatrix} \in \operatorname{Ker} \theta_1^2 \cap \bar{G} = \{1\}.$$

Thus $\sigma + c\sigma^2 \equiv 0 \pmod 3$ so that either (i) $\sigma \equiv 0 \pmod 3$ or (ii) $c \equiv \sigma^{-1} \pmod 3$. Thus for all $\sigma \in Z_{3^2}^*[\alpha]$,

$$K = \begin{pmatrix} 1 + 3a & \sigma + 3b \\ -3/\sigma & 1 - 3(a+1) \end{pmatrix}. \tag{1}$$

Let $\sigma, \tau \in Z_{3^2}^*[\alpha]$. Then by multiplicative closure $\bar{G}$ contains a unique element of the form

$$\begin{pmatrix} 1 + 3a & \sigma + 3b \\ -3/\sigma & 1 - 3(a+1) \end{pmatrix} \begin{pmatrix} 1 + 3x & \tau + 3y \\ -3/\tau & 1 - 3(x+1) \end{pmatrix} \tag{2}$$

$$= \begin{pmatrix} 1 + 3(a + x - \sigma/\tau) & \tau + \sigma + 3(a\tau + y - \sigma(x+1) + b) \\ -3(1/\sigma + 1/\tau) & 1 - 3(\tau/\sigma + a + x + 2) \end{pmatrix}.$$

Now if $\sigma^{-1} + \tau^{-1} \not\equiv 0 \pmod 3$, then comparing (1) and (2) yields

$$a + x - \sigma/\tau \equiv \tau/\sigma + a + x + 1 \pmod 3$$

which yields

$$\sigma \equiv \tau \pmod 3$$

so that $Z_3[\alpha] = GF(3)$.

COROLLARY 3. *If* $Z_3[\alpha] \neq GF(3)$, $G \leqslant \mathrm{SL}_2(Z_{3^n}[\alpha])$, *and* θ_1^n/G *is an epimorphism, then* $G = \mathrm{SL}_2(Z_{3^n}[\alpha])$.

PROOF. $\theta_2^n(G) \cap \operatorname{Ker} \theta_1^2 \neq \{1\}$, else $\theta_2^n(G)$ is mapped isomorphically onto $\mathrm{SL}_2(Z_3[\alpha])$ contradicting Theorem 3. Thus by Theorem 2(b), $G = \mathrm{SL}_2(Z_{3^n}[\alpha])$.

The next order of business is the characteristic 2^n case.

THEOREM 4. *Suppose $Z_2[\alpha]$ is neither GF(2) nor GF(4), $G \leqslant \mathrm{SL}_2(Z_4[\alpha])$, and θ_1^2/G is an epimorphism. Then $G \cap \operatorname{Ker} \theta_1^2$ contains some noncentral element.*

PROOF. Negate. By surjectivity, for $G \in Z_4[\alpha]$ there exists K in G:

$$K = \begin{pmatrix} 1 + 2a & \sigma + 2b \\ 2c & 1 + 2d \end{pmatrix}$$

so that

$$K^2 = \begin{pmatrix} 1 + 2c\sigma & 2\sigma(1 + a + d) \\ 0 & 1 + 2c\sigma \end{pmatrix}.$$

From $\det K = 1$ follows $a + d \equiv c\sigma \pmod 2$. As $K^2 \in G \cap \operatorname{Ker} \theta_1^2$, by hypothesis either (i) $\sigma \equiv 0 \pmod 2$ or (iii) $a + d \equiv 1 \pmod 2$. Thus for all $\sigma \in Z_4^*[\alpha]$, there exists $K \in G$ with

$$K = \begin{pmatrix} 1 + 2a & \sigma + 2b \\ 2/\sigma & 3 + 2a \end{pmatrix}.$$

Moreover any L with $\theta_1^2(L) = \left(\begin{smallmatrix} 1 & \sigma \\ 0 & 1 \end{smallmatrix}\right)$ has the form K. By multiplicative closure for all $\sigma, \tau \in Z_4^*[\alpha]$, G contains

$$\begin{pmatrix} 1 + 2a & \sigma + 2b \\ 2/\sigma & 3 + 2a \end{pmatrix}\begin{pmatrix} 1 + 2x & \tau + 2y \\ 2/\tau & 3 + 2x \end{pmatrix}$$
$$= \begin{pmatrix} 1 + 2(a + x + \sigma/\tau) & \tau - \sigma + 2(a\tau + y + b + \sigma x) \\ 2(1/\sigma + 1/\tau) & 1 + 2(\tau/\sigma + a + x) \end{pmatrix}.$$

Thus either $\sigma^{-1} + \tau^{-1} \equiv 0 \pmod 2$ which gives $\sigma \equiv \tau \pmod 2$ or (by comparison with K) $(\tau - \sigma)^{-1} \equiv \tau^{-1} + \sigma^{-1} \pmod 2$. Hence if σ and τ are distict invertibles of $Z_2[\alpha]$, then $\sigma^2 + \sigma\tau + \tau^2 \equiv 0 \pmod 2$ so $Z_2[\alpha] \leqslant GF(4)$ contrary to hypothesis.

LEMMA 2. *For $G \leqslant \mathrm{SL}_2(Z_4[\alpha])$ and $Z_2[\alpha] \not\leqslant GF(4)$ if θ_1^2/G is surjective, then $G = \mathrm{SL}_2(Z_4[\alpha])$.*

PROOF. Let $H = G \cap \operatorname{Ker} \theta_1^2$ so that $H \lhd \mathrm{SL}_2(Z_4[\alpha])$ and hence H is a union of conjugacy classes. By Theorem 4, H contains some noncentral element so that by Proposition 3(ii) there exists $\sigma \in Z_2[\alpha]$ with $A_\sigma \in H$ where

$$A_\sigma = I + 2\begin{pmatrix} 0 & \sigma \\ 1 & 0 \end{pmatrix}.$$

Let

$$A'_\sigma = I + 2\begin{pmatrix} \sqrt{(1 + \alpha^2)\sigma} & \alpha\sigma \\ \alpha & \sqrt{(1 + \alpha^2)\sigma} \end{pmatrix}$$

so that

$$A_\sigma A'_\sigma = I + 2\begin{pmatrix} \sqrt{(1+\alpha^2\sigma} & (\alpha+1)\sigma \\ \alpha+1 & \sqrt{(1+\alpha^2)\alpha} \end{pmatrix} \overset{\text{def}}{=} 1 + 2B.$$

By normality of H and Corollary 1, A'_σ and $A_\sigma A'_\sigma$ are elements of H. Since $\det B \equiv 0 \pmod 2$, H contains all $I + 2C$ where $\det C = 0 \pmod 2$. Thus the following belong to H for $\tau \in Z_2[\alpha]$:

$$\left[I + 2\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right]\left[I + 2\begin{pmatrix} 0 & \tau \\ 0 & 0 \end{pmatrix}\right] = I + 2\begin{pmatrix} 0 & \tau \\ 1 & 0 \end{pmatrix},$$

$$\left[I + 2\begin{pmatrix} \tau & \tau^2 \\ 1 & \tau \end{pmatrix}\right]\left[I + 2\begin{pmatrix} 0 & \tau^2 \\ 1 & \tau \end{pmatrix}\right] = I + 2\begin{pmatrix} \tau & 0 \\ 0 & \tau \end{pmatrix}.$$

By Proposition 3(ii), H contains representatives of all conjugacy classes of $\operatorname{Ker}\theta_1^2$. Since H is normal, this implies that $H = \operatorname{Ker}\theta_1^2$.

THEOREM 5. *If* $G \leqslant \mathrm{SL}_2(Z_{2^n}[\alpha])$, $n \geqslant 3$, *and* θ_2^n/G *is surjective, then* $G = \mathrm{SL}_2(Z_{2^n}[\alpha])$.

PROOF. (Induction on n.) We need only show that $\operatorname{Ker}\theta_{n-1}^n$ is contained in the Frattini subgroup ϕ of a Sylow 2-subgroup of $\mathrm{SL}_2(Z_{2^n}[\alpha])$.

Case $n = 3$. Note first that

$$\operatorname{Ker}\theta_1^3 = \left\{I + 2A : A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a \equiv \frac{-d + 2bc}{2d+1} \pmod 4\right\}.$$

Squaring a typical element of $\operatorname{Ker}\theta_1^3$ yields a typical element of ϕ:

$$\begin{pmatrix} 1+2a & 2b \\ 2c & 1+2d \end{pmatrix}^2 = \begin{pmatrix} 1+4(d^2+d+c+bc) & 4b \\ 4c & 1+4(d^2+d+bc) \end{pmatrix}.$$

As $a \to a^2$ sets up a (2.1) correspondence on $Z_2[\alpha]$ we note that these squares form a subgroup of index 2 in $\operatorname{Ker}\theta_2^3$. Since some diagonal matrix lies in the nontrivial coset it merely remains to show that all diagonal matrices are in ϕ. Let

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 4c & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & 4c \\ 0 & 1 \end{pmatrix}.$$

Then $STS^{-1}T^{-1}U \in \phi$ and a calculation shows that $[S, T]U = (1 + 4c)I$. Inductive step: If $n \geqslant 4$ and $\operatorname{tr} A = 0$, then $\det(1 + 2^{n-2}A) = 1$. Thus if $1 + 2^{n-1}A \in \operatorname{Ker}\theta_{n-1}^n$ then $1 + 2^{n-1}A = (1 + 2^{n-2}A)^2 \in \phi$.

COROLLARY 4. *If* $G \leqslant \mathrm{SL}_2(Z_{2^n}[\alpha])$, $Z_2[\alpha] \nleqslant GF(4)$, *and* θ_1^n/G *is an epimorphism, then* $G = \mathrm{SL}_2(Z_{2^n}[\alpha])$.

PROOF. This is an immediate consequence of Theorem 5 and Lemma 2.

4. Some more ring theory. For x an indeterminate and $f(x) \in Z[\alpha][z]$ let $f_i(x)$ denote the canonical image of $f(x)$ in $Z_{p^i}[\alpha][x]$.

LEMMA 3. *Suppose that over* $Z[\alpha][x]$, $f(x)g(x) = h(x)$, $\deg h = \deg h_1$ *and* $(f_1, g_1) \equiv 1 \pmod p$. *Then for each* n, *there exist unique* $\tilde f_n, \tilde g_n \in Z_{p^n}[\alpha][x]$ *with*

(i) $\deg \tilde f_n = \deg f_1$, $\deg f_n$, $\deg \tilde g_n = \deg g_1$,

(ii) $\tilde f_n \equiv f \pmod p$, $\tilde g_n \equiv g \pmod p$,

(iii) $h_n(x) = \tilde f_n(x)\tilde g_n(x)$.

PROOF. By induction $h_n(x) = \bar f_n(x)\bar g_n(x) + p^{n-1}k(x) \in Z_p[\alpha][x]$, $\deg \bar f_n = \deg f_1$, $\deg \bar g_n = \deg g_1$, $\bar f_n \equiv f_1 \pmod p$, and $\bar g_n \equiv g_1 \pmod p$. Thus following Euclid, there exists $S(x)$, $t(x) \in Z_p[\alpha][x]$ with

(a) $\deg s < \deg f$,

(b) $s\bar g_n + t\bar f_n \equiv k \pmod p$. Take

$$\tilde f_n(x) = \bar f_n(x) + p^{n-1}S(x), \qquad \tilde g_n(x) = \tilde g_n(x) + p^{n-1}t(x).$$

Then

$$\tilde f_n \tilde g_n = \bar f_n \bar g_n + p^{n-1}\left(S\bar g_n + t\bar f_n\right) \equiv h_n \pmod{p^n}.$$

From (a) $\deg \tilde f_n = \deg \bar f_n = \deg f_1$ so that

$$\deg \tilde g_n = \deg h_n - \deg \tilde f_n = \deg h - \deg f = \deg g_1.$$

Uniqueness follows similarly.

REMARK 1. Lemma 3 obviously extends to n factors by an easy induction.

COROLLARY 5. $Z_{p^n}[\alpha]$ *is isomorphic to* $Z_{p^n}[\beta]$ *iff* $|Z_{p^n}[\alpha]| = |Z_{p^n}[\beta]|$.

PROOF. Suppose $g(x) \in Z[x]$ is a monic polynomial with $g_n(\beta) = 0$ and such that $g_1(x)$ is irreducible. As all irreducible polynomials of degree m split over $Z_p[\alpha] = GF(q)$, it follows from Remark 1 that $g_n(x)$ is a product of linear factors over $Z_{p^n}[\alpha]$. Taking the constant term β' of one of these and mapping β' to β induces an isomorphism.

5. Generation theorems for $\mathrm{PSL}_2(Z_{p^n}[\sigma])$. In this section certain results that appear in [7] for $n = 1$ will be shown to hold for arbitrary n. Just as in [7], denote by $E_n(\alpha, \beta, \gamma)$ the set of all (A, B, C) with $\operatorname{trace} A = \alpha$, $\operatorname{trace} B = \beta$, $\operatorname{trace} C = \gamma$, $\det A = \det B = \det C = 1$, $ABC = 1$.

THEOREM 5. *If* $\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma \not\equiv 4 \pmod p$, *then* $E_n(\alpha, \beta, \gamma) \neq \phi$. *In fact if* $\bar\alpha \equiv \alpha$, $\bar\beta \equiv \beta$, *and* $\bar\gamma \equiv \gamma \pmod p$ *and* $(A_1, B_1, C_1) \in E_1(\bar\alpha, \bar\beta, \bar\gamma)$, *then there exists* $(A_n, B_n, C_n) \in E_n(\alpha, \beta, \gamma)$ *congruent to* $(A_1, B_1, C_1) \pmod p$.

PROOF. Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

and as in [7] find that $(A, B, B^{-1}A^{-1}) \in E_n(\alpha, \beta, \gamma)$ if $f(z, w) = 1 + Z^2 + w^2 + \alpha zw - \beta w - \gamma z \equiv 0 \pmod{p^n}$ is solvable. In [7] this was proven possible with $n = 1$ after perhaps permuting (α, β, γ) which we assume done. By induction there exist z, w, $\tau \in Z_{p^{n-1}}[\sigma]$ with $f(z, w) \equiv \tau p^n \pmod{p^{n+1}}$. In an attempt to solve the equation by perturbing (z, w) let $\tilde z = z + ip^n$ and $\tilde w = w + jp^n$, so that

$$f(\tilde z, \tilde w) = \tau p^n + \left[i(2z + \alpha w - \gamma) + j(\alpha z + 2w - \beta)\right] p^n.$$

If $2z + \alpha w - \gamma \in Z_{p^{n+1}}^*[\sigma]$, then taking $i \equiv \tau/(2z + \alpha w - \gamma)$ and $j \equiv 0 \pmod p$ yields the desired solution with a similar statement for $\alpha z + 2w - \beta$. This procedure fails only if

$$\begin{aligned} 2z + \alpha w &\equiv \gamma \\ \alpha z + 2w &= \beta \end{aligned} \qquad (\text{mod } p) \tag{1}$$

which we shall show cannot occur.

Case I. $p \neq 2$. Multiplying the first equation in (1) by z, the second by w, and adding yields

$$2(z^2 + \alpha zw + w^2) \equiv \beta w + \gamma z \pmod p;$$

since $f(z, w) \equiv 0 \pmod p$ this implies that

$$\beta w + \gamma z - 2 \equiv 0 \pmod p. \tag{3}$$

An immediate consequence of (1) is that $(4 - \alpha^2)z \equiv 2\gamma - \alpha\beta$ and $(4 - \alpha^2)w \equiv 2\beta - \alpha\gamma$ so that using (3) one finds

$$2(4 - \alpha^2) \equiv (\beta w + \gamma z)(4 - \alpha^2) \equiv \beta(2\beta - \alpha\gamma) + \gamma(2\gamma - \alpha\beta) \pmod p$$

which simplifies to $\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma \equiv 4$, contrary to assumption.

Case II. $p = 2$. The previously mentioned permutation need only be effected if $\alpha \equiv 0$. By hypothesis $(\alpha, \beta, \gamma) \not\equiv 0 \pmod 2$. By (1) $w = \gamma/\alpha$ and $z = \beta/\alpha$ so that

$$0 \equiv f(z, w) \equiv 1 + \beta^2/\alpha^2 + \gamma^2/\alpha^2 + \alpha\beta\gamma/\alpha^2 - \gamma\beta/\alpha$$

which implies the same contradiction as obtained in Case I.

COROLLARY 7. *Suppose* $p \nmid lmn$ *and there exists* $\{\pm\bar{A}\}, \{\pm\bar{B}\} \in \mathrm{PSL}_2(Z_p[\sigma])$ *such that*

(i) $(\operatorname{tr}\bar{A})^2 + (\operatorname{tr}\bar{B})^2 + (\operatorname{tr}\overline{AB})^2 - (\operatorname{tr}\bar{A})(\operatorname{tr}\bar{B})(\operatorname{tr}\overline{AB}) \not\equiv 4 \pmod p$,

(ii) $\bar{A}^l \equiv \bar{B}^m \equiv \bar{A}\bar{B}\bar{C} \equiv \bar{C} \equiv I \pmod{\pm I}$.

Then there exist $A, B, C \in \mathrm{SL}_2(Z_{p^r}[\sigma])$ *such that*

$$\theta_1^r(A) = \bar{A}, \quad \theta_1^r(B) = \bar{B}, \quad \theta_1^r(C) = \bar{C}$$

and

$$A^l \equiv B^m \equiv C^n \equiv ABC = I \pmod{\pm I}.$$

PROOF. Since $p \nmid |\bar{A}|$, it follows that $\bar{A}$ diagonalizes with primitive sth roots of unity on the diagonal where $S \in \{l, 2, l\}$. Thus the trace of $\bar{A}$ is the homomorphic image of $\lambda = \sqrt[s]{1} + 1/\sqrt[s]{1}$, taken as a member of an algebraic number ring. Exactly the same holds for $\bar{B}$ and $\bar{C}$ where one obtains say u and v. Mapping λ, u, v modulo p^r and applying Theorem 5 proves the corollary, since the projective order of a matrix with characteristic polynomial $x^2 - \lambda x + 1$ is l.

It is worth noting that the quadratic form condition of Theorem 5 is equivalent to the statement that the trace of $A^{-1}B^{-1}AB$ is not equal to 2. Another fact of utility is that $\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma - 4$ is -4 times the determinant of the quadratic form $q(\xi, \eta, \zeta) = \xi^2 + \eta^2 + \zeta^2 + \alpha\eta\zeta + \beta\zeta\xi + \gamma\xi\eta$. Thus if $p \neq 2$, the Q factors if and only if this quantity vanishes. That Q also factors in characteristic 2 precisely under

the same condition is easily checked. In [7] any triple $(A, B, C) \in E_1(\alpha, \beta, \gamma)$ that causes $Q(\alpha, \beta, \gamma)$ to factor is called singular and it is proven that such triples always generate solvable groups.

DEFINITION. A finite group is said to be a $(l, m, n) := \langle x, y, z: x^l = y^m = z^n = xyz = 1\rangle$; this latter group is called a triangle group.

COROLLARY 8. *Suppose* $Z_p[\sigma] \neq GF(q)$ *for* $q \in \{2, 3, 4\}$. *Then* $\mathrm{PSL}_2(Z_{p^r}[\sigma])$ *is a* (l, m, n)*-group iff* $\mathrm{PSL}_2(Z_p[\sigma])$ *is, provided that* $p \nmid lmn$.

PROOF. Since $\mathrm{PSL}_2(Z_p[\sigma])$ is not solvable, no generating (l, m, n) triple can be singular. Thus if $\mathrm{PSL}_2(Z_p[\alpha])$ has a generating (l, m, n) triple, then by Corollary 7, this triple lifts modulo p^r. By Theorem 1 and Corollaries 3 and 4 this new triple must generate $\mathrm{PSL}_2(Z_{p^r}[\sigma])$.

COROLLARY 9. $\mathrm{SL}_2(Z_{p^r})$ *can be generated by two elements of trace* 2 *whose product has trace* -2, *provided that* $p \neq 2$.

PROOF. A matrix realization of $(2, 2, -2)$ is

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix}.$$

The result follows from parts (a) and (b) of Theorem 2 since over Z_9 the relation $I \neq B^3 \in \mathrm{Ker}\,\theta_1^2$ holds.

This is our analogue of Theorem 7 of [7]. The analogues of Theorems 5, 6, and 8 of [7] follow.

COROLLARY 10. *Suppose* $Z_p[\sigma] \neq GF(q)$ *for* $q \in \{2, 3, 4\}$ *and that* $Z_p[\sigma] = Z_p[\bar{\alpha}, \bar{\beta}, \bar{\gamma}]$. *Assume that* $(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ *is neither exceptional, singular, nor irregular* (*see* [7] *for definition*), *and that* $(\alpha, \beta, \gamma) \in (Z_{p^r}[\sigma])^3$ *is congruent modulo* p *to* $(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$. *Then there exist* $(A, B, C) \in E_n(\alpha, \beta, \gamma)$ *such that* $\langle A, B\rangle = \mathrm{SL}_2(Z_{p^r}[\sigma])$.

Next, a result of Newman (see [8]) will be slightly strengthened.

COROLLARY 11. *If* $|Z_p[\sigma]| \geqslant 13$, *then* $\mathrm{PSL}_2(Z_{p^r}[\sigma])$ *is a factor of the modular group modulo a noncongruence subgroup. In particular if* n *has a prime divisor* $\geqslant 13$, *and* Γ *denotes the modular group and* Γ_n *the principal congruence subgroup at level* n, *then there exists* $N \lhd \Gamma$ *with* $\Gamma/N \simeq \Gamma/\Gamma_n$.

PROOF. Let $|Z_p[\sigma]| = q$ and $n = q + 1$. As usual let γ be the trace of a 2×2 matrix over the algebraic integers, whose order is n and let γ_r denote γ's image in $Z_{p^r}[\sigma]$. It is how in [7] that any $(0, 1, \gamma_1)$ triple generates $\mathrm{PSL}_2([\sigma])$. Thus by Corollary 10 such a triple exists and lifts to a $(0, 1, \gamma_r)$ triple which generates $\mathrm{PSL}_2(Z_{p^r}[\sigma])$. That the normal subgroup is noncongruence follows at once from the Fricke-Wohlfahrt theorem of [**10**]. To prove the second part note that if $n = \prod_{S\in\Sigma} p_s^{\alpha s}$ then

$$\Gamma/\Gamma_\gamma \simeq \prod_{S\in\Sigma} \mathrm{SL}_2\left(Z_{p_s^{\alpha s}}\right)/\langle(-I, \ldots, -I)\rangle.$$

A fundamental result of Riemann surface theory appears in 3. This states that for Riemann surface S of genus g, $|\mathrm{Aut}\, S| \leqslant 84(g - 1)$ with equality occurring iff S is

uniformized by a group whose normalizer in $LF(2, R)$ is isomorphic to $(2, 3, 7)$. Because of this $(2, 3, 7)$ has been the object of much study and its finite factors are called Hurwitz groups.

COROLLARY 12. *The group* $\mathrm{PSL}_2(Z_{p^r}[\sigma])$ *is a Hurwitz group if and only if*
(i) $Z_{p^r}[\sigma] = GF(7)$, *or*
(ii) $Z_{p^r}[\sigma] = Z_{p^r}$ *if* $p \equiv \pm 1 \pmod 7$, *or*
(iii) $|Z_p[\sigma]| = p^3$ *otherwise.*

PROOF. This is a special case of Corollary 10. The reason that $\mathrm{PSL}_2(Z_{49})$ fails to be a Hurwitz group is that by Proposition 4 every element of order 7 lies in $\operatorname{Ker} \theta_1^2$.

If (i) appears unsatisfactory we refer the interested reader to [**2**] where all Hurwitz extensions of an abelian group by $\mathrm{PSL}_2(7)$ (and hence certain algebraic curves that cover the famous curve in [**4**]) are determined. Taking $p = 2$ in (iii) yields an infinite family of Hurwitz groups with nontrivial center. If a subgroup of order 2 is factored out of $\mathrm{PSL}_2([\sigma])$ one obtains a factor of $(2, 3, 7; 9)$ also found by Leech in [**6**].

PROPOSITION 5. *The center of* $\mathrm{PSL}_2(Z_{p^n}[\sigma])$ *is trivial unless* $p = 2$ *in which case its order is*

$$|Z_2[\sigma]| \text{ if } n \geqslant 3, \quad \tfrac{1}{2}|Z_2[\sigma]| \text{ if } n = 2, \quad 1 \text{ if } n = 1.$$

The center is composed of diagonal matrix cosets.

6. Three generalizations of Bundgaard-Nielsen-Fox.

PROPOSITION 6. *If* $(A, B, C) \in E(\alpha, \beta, \gamma)$ *then the trace of* AB^2 *is* $\beta\gamma - \alpha$.

LEMMA 4. *Each infinite exceptional triangle group has* $\mathrm{PSL}_2(p)$ *among its factors for infinitely many* p.

PROOF. $(-1, \sqrt{2}, \sqrt{2})$. By the results in [**7**] a matrix realization of this triple generates either S_4, $\mathrm{PSL}_2(p)$ or $\mathrm{PGL}_2(p)$—the latter depending on whether $p \equiv \pm 1 \pmod 8$ or not. By Proposition 6 some matrix in the generated group has trace 3. Now S_4 contains elements whose orders are 1, 2, 3, and 4 and no others so that if S_4 is generated then $3 \in \{0, \pm 1, \pm \sqrt{2}\}$ which cannot occur $p > 7$. (Actually $\mathrm{PSL}_2(7)$ is a $(3, 4, 4)$-group as well, since the commutator has order 7.) The remaining infinite exceptional triangle groups are handled as follows where $\theta^2 + \theta - 1 = 0$.

Group	Trace Triple
$(2, 5, 5)$	$(0, \theta, \theta)$
$(3, 5, 5)$	$(1, \theta, \theta)$
$(3, 3, 5)$	$(1, 1, \theta)$
$(5, 5, 5)$	(θ, θ, θ)

LEMMA 5. *Suppose* (l, m, n) *is not one of the following*: $(2, 2, n)$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$, $(2, 3, 6)$, $(2, 4, 4)$, *or* $(3, 3, 3)$. *Then there exist infinitely many prime numbers* p *such that* $\mathrm{PSL}_2(p)$ *is a homomorphic image of* (l, m, n) *where the generator of order* l *(resp.* m, n*) maps to an element of order* l *(resp.* m, n*).*

PROOF. By Dirichlet's theorem infinitely many primes are congruent to one modulo 2 lmn. Let p be one of these. Choose a homomorphism $(l, m, n) \to \mathrm{SL}_2(p)$ and suppose the associated trace triple is (α, β, γ). By Theorem 5 of [7] if $\mathrm{PSL}_2(Z_p)$ is not generated, then either (l, m, n) is exceptional, in which case Lemma 4 applies, or $g(\alpha, \beta, \gamma) := \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma = 4$. If no member of the trace triple is zero, then replacing α by $-\alpha$ yields a nonsingular triple. Suppose $\alpha = 0$ so that $l = 2$, fix β and note that g is a quadratic in γ. Thus for groups in our list there can be at most two traces associated with an element of order n and by symmetric argument the same holds for m. Hence $m, n \in \{2, 3, 4, 6\}$. To see that $(2, 6, 6)$ and $(2, 4, 6)$ should not be included in the above list consider the following triples and note that $Q \neq 0$: $(0, \sqrt{3}, \sqrt{3})$, $(0, \sqrt{2}, \sqrt{3})$.

We now consider the following group:

$$(\nu_1, \ldots, \nu_s; g) = \left\langle x_i, y_j, z_j : x_i^{\nu_i} = \prod_{i=1}^{s} x_i \prod_{j=1}^{t} [y_i, z_j] = 1, \quad i = 1, \ldots, s, j = 1, \ldots, g \right\rangle.$$

If $2g - 2 + \sum_{i=1}^{s}(1 - 1/\nu_i) > 0$, then Γ is called a cocompact Fuchsian group and is infinite. It is known that a homomorphism of Γ has torsion-free kernel if and only if x_i maps to an element of order ν_i for $i = 1, \ldots, s$. We set $(\nu_1, \ldots, \nu_s) = (\nu_1, \ldots, \nu_s; \theta)$.

THEOREM 6. *Every cocompact Fuchsian group* Γ *has* $\mathrm{PSL}_2(Z_p)$ *as factor for infinitely many primes p where the associated normal subgroup is torsion-free.*

PROOF. Let $n = 8\prod_{i=1}^{s} \nu_i$ and choose p an odd prime where $p \equiv 1 \pmod{n}$. If $s \geq 3$, then setting $z_j = 1$ shows that the free product $(\nu_1, \ldots, \nu_s)$ with the free group of rank g is a factor of Γ. Without loss of generality $\nu_1 \geq \nu_2 \geq \cdots \geq \nu_s$. Pick $A_i \in \mathrm{PSL}_2(Z_p)$ so that $A_j^{\nu_j} = I = (\prod_{i=1}^{j} A_i)^k$ where $2 \leq j \leq s - 2$ and $K = \frac{1}{2}(p + 1)$. By the construction in Lemma 5 one may vary the choice of A_i so that $\langle A_1, A_2 \rangle$ or $\langle A_1, A_2, A_3 \rangle$ is $\mathrm{PSL}_2(Z_p)$ unless $s = 3$ and (ν_1, ν_2, ν_3) is one of the listed groups or $s = 4$ and $\nu = 2$ for each i. In either case if $g > 0$, then one picks an image c for y_1 so that $\langle A_1, C \rangle = \mathrm{PSL}_2(Z_p)$.

If $s \leq 2$, then Γ has as factor (i) $(\nu_1; 1)$ or (ii) $(\nu_1, \nu_2; 1)$. If (i) note that $\mathrm{PSL}_2(p)$ is a (ν_1, k, k) group and that for some $\alpha, \beta \in GF(p)$ this is exhibited by the trace triple (α, β, β). Suppose (x, y^{-1}, T) is a matrix realization of this triple. Then since all matrices of trace β are conjugate there exists $z \in \mathrm{PSL}_2(p)$ with $z^{-1}yz = T$ so that

$$xy, z = xy^{-1}z^{-1}yz = xy^{-1}T = I.$$

Case (ii) is handled similarly.

COROLLARY 13. *Every cocompact Fuchsian group* Γ *has infinitely many simple nonabelian factors.*

THEOREM 7. *Every cocompact Fuchsian group* Γ *has a torsion-free normal subgroup of finite index (in fact infinitely many such subgroups) such that* Γ/N *has nontrivial center.*

PROOF. If Γ has a nontrivial factor A, then choose a nonabelian factor Γ/M of Γ where M is torsion-free. By the Jordan-Hölder theorem $\Gamma/M \times A$ is a factor of Γ. If Γ has trivial abelianization, then $g = 0$ and the v_i are pairwise coprime so that $\mathrm{PSL}_2(Z_4[\sigma])$ is a factor of Γ for approximate σ. Choose a simple nonabelian factor of Γ as above and take the direct product

It is worth noting that Γ has factors with arbitrarily large center. To see this take a direct product of $\mathrm{SL}_2(Z_4[\sigma])$ with $\mathrm{SL}_2(p_i)$ for suitable prime p_i and factor out $\langle(-I, -I, \ldots, -I)\rangle$.

THEOREM 8. *Let* Γ *be a cocompact Fuchsian group. Then for each positive integer* n, *there exists* m *so that there are at least* n *torsion-free normal subgroups of* Γ *of index* m *whose factors are pairwise nonisomorphic.*

PROOF. Use Corollary 13 to obtain a torsion-free $N \lhd \Gamma$ with Γ/N a simple nonabelian group. Set $n = \exp(\Gamma/N)$ and $\zeta = e^{(2\pi i/n)}$. Then Γ/N acts on N/N' by conjugating and this action may be extended to $N/N' \otimes \mathbf{C}$. By a celebrated theorem of Brauer $Q(\zeta)$ is a splitting field for the irreducible characters of Γ/N. Thus (see §1, extension of Theorem 1) $N/N' \otimes \mathbf{C}(\zeta)$ is the Γ/N-module theoretic direct sum of two representations of degree g where $N \simeq (\ ;\ g)$. Equivalently, there exists a change of base matrix C with $C^{-1}(N\gamma)C$ block diagonal with two $g \times g$ blocks for each $\gamma \in \Gamma$. Now each entry of C is of the form $\sum_{s=0}^{\Phi(n)} C(s_j, i, j)\zeta^s$ where $C(s; i, j)$ is rational and clearly only finitely many primes are factors of the denominators of these rationals. By Dirichlet's theorem pick a prime number p with the following properties:

(i) $p \equiv 1 \pmod{n}$;

(ii) p does not divide the denominator of $C(s; i, j)$ for $s = 1, \ldots, \phi(n)$, $i, j = 1, \ldots, 2g$,

(iii) The Galois-theoretic norm of the determinant of C is not divisible by p.

By (i) for each i, there is a natural ring homomorphism $Z[\zeta] \to Z_{p^i}$. By (ii) this homomorphism may be applied to each entry of C. (Surely it may be applied to the entries of the integral matrices that represent the action of $N\gamma$.) By (iii) the image matrix $\overline{C}$ is invertible. Thus $\overline{C}^{-1}(N\gamma)\overline{C}$ is the direct sum of two $g \times g$-block diagonal matrices with entries in Z_{p^i}. Equivalently there exist $N_k \lhd \Gamma$, $k = 1, 2$, so that

$$N/N'N^{p^i} = N_1/N'N^{p^i} \oplus N_2/N'N^{p^i}.$$

Therefore if $j \leqslant i$, then $\Gamma/N'N_2^{p^j}$ is an extension of $(Z_{p^i})^g + (Z_{p^j})^g$ by Γ/N and $N/N'N_2^{p^j}$ is the Fitting subgroup because Γ/N is simple nonabelian. Hence letting $i + j = 2(n - 1)$ and varying i between 0 and $n - 1$ gives n nonisomorphic factors of Γ.

ACKNOWLEDGEMENT. The author wishes to thank Dr. Paul Venzke for help and encouragement in the early stages of this work. Thanks are also due to Cecilia Price for excellent typing.

REFERENCES

1. J. Cohen, *On Hurwitz extensions by* $PSL_2(7)$, Math. Proc. Cambridge Philos. Soc. **86** (1979), 395–400.

2. _____, *Compact Riemann surfaces with automorphism groups*, J. London Math. Soc. (to appear).

3. A. Hurwitz, *Über algebraische Gebilde mit eindeutigen transformationen in sich*, Math. Ann. **14** (1879), 403–442.

4. F. Klein, *Über die Transformationen Siebenter Ordung der elliptischen Funktionen*, Math. Ann. **14** (1879), 428–471.

5. J. Leech, *Generators for certain normal subgroups of* (2, 3, 7), Proc. Cambridge Philos. Soc. **61** (1965), 321–332.

6. _____, *Note on the abstract group* (2, 3, 7; 9), Proc. Cambridge Philos. Soc. **62** (1966), 7–10.

7. A. M. Macbeath, *Generators of the linear fractional groups*, Proc. Sympos. Pure Math., vol. 12, Amer. Math. Soc., Providence, R. I., 1967, pp. 14–32.

8. M. Newman, *Maximal normal subgroups of the modular group*, Proc. Amer. Math. Soc. **19** (1968), 1138–1144.

9. A. Sinkov, *On the group-defining relations* (2, 3, 7; 9), Ann. of Math. (2) **38** (1937), 577–584.

10. K. Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math. **8** (1964), 529–535.

DEPARTMENT OF MATHEMATICS, AUBURN UNIVERSITY, AUBURN, ALABAMA 36849