ASIAN J. MATH.
Vol. 1, No. 4, pp. 764–768, December 1997

006

THREE-MANIFOLD SUBGROUP GROWTH, HOMOLOGY OF COVERINGS AND SIMPLICIAL VOLUME*

ALEXANDER REZNIKOV† AND PIETER MOREE‡

1. Introduction. This paper is concerned with the conjecture, communicated to the first author by A. Lubotzky and A. Shalev:

CONJECTURE 1.1. *Let M be a hyperbolic three-manifold. Let $f(d)$ denote the number of subgroups of index d in $\pi_1(M)$. There exists an absolute positive constant C_1 such that, for infinitely many d, $f(d) > \exp(C_1 d)$.*

This conjecture follows easily from the following one:

CONJECTURE 1.2. *Let M be as above. For any prime p there exists infinitely many d, for which there exists a d-sheeted covering N of M such that*

$$rank_p\,(H_1(N)) > C_2 d, \tag{1}$$

where C_2 is an absolute positive constant.

Observe that for any finitely generated group G, and a subgroup H of index d, $\mathrm{rank}_p\,(H_1(H)) \leq \mathrm{const} \cdot d$, so that (1) is sharp up to a constant.

A much weaker growth rate than conjectured in (1), namely, $\mathrm{rank}_p\,(H_1(N)) > (\log d)^{2-\epsilon}$ has been proved by Shalev [Sh]. It follows from the Class Tower Theorem of [R1] that $\mathrm{rank}_p\,(H_1(N)) > (\log d)^2$.

These conjectures about the subgroup growth should be compared with the results of [Tu] and [SW] concerning the word growth of $\pi_1(M)$.

Here we prove the following result for a priori a much wider class of manifolds than hyperbolic manifolds (given the present status of the hyperbolization conjecture). Recall the definition of rich fundamental groups given in [R1]:

(R) A closed irreducible three-manifold satisfies condition (R) if either

(a) the Casson invariant $\lambda(M) > \sharp($ representations of $\pi_1(M)$ in $SL_2(\mathbb{F}_5))$ or

(b) M is hyperbolic.

MAIN THEOREM 1.1. *Suppose the three-manifold M is a rational homology sphere (that is $H_1(M,\mathbb{Q}) = 0$) satisfying (R). Then for all, but at most two, primes ℓ with $\ell \equiv 3 \pmod 4$, there exists a positive α such that for infinitely many d, there exists a d-sheeted covering N of M such that either the inequality $rank_\ell\, H_1(N) > c\,d^\alpha$, or $rank_{\mathbb{Z}}\, H_1(N) > c\,d^{1/3}$, holds.*

As a corollary we have:

THEOREM 1.2 (SUBGROUP GROWTH). *Let M be as in the Main Theorem. Then for infinitely many d, $f(d) > \exp(C\,d^\alpha)$.*

Strategy of the proof. Step 1. By Theorem 9.1 of [R1], $\pi_1(M)$ admits a Zariski dense representation to $SL_2(\mathbb{C})$. We use the strong approximation of [We] to find surjective maps from $\pi_1(M)$ onto $SL_2(\mathbb{F}_q)$, where $\mathbb{F}_q$ are residue fields of an algebraic number field K.

Step 2. If ℓ is a prime, q, s are prime powers such that ℓ divides both $|SL_2(\mathbb{F}_q)|$ and $|SL_2(\mathbb{F}_s)|$, and $1 \to \pi_1(N) \to \pi_1(M) \to SL_2(\mathbb{F}_q) \times SL_2(\mathbb{F}_s) \to 1$ is a Galois covering,

---

* Received July 10, 1997; accepted for publication (in revised form) February 6, 1998.

† Department of Mathematical Sciences, University of Durham, Durham DH1 3LE, England (reznikov@mpim-bonn.mpg.de, reznikov@daphne.polytechnique.fr).

‡ Max-Planck-Institut für Mathematik, Gottfried-Claren-Str. 26, 53225 Bonn, Germany (moree @mpim-bonn.mpg.de).

then $H_1(N)_{(\ell)}$, the ℓ-torsion part of $H_1(N)$, is nontrivial. This is proved in Proposition 2.1. Moreover, the action of $SL_2(\mathbb{F}_q)$ in $H_1(N)_{(\ell)}$ is nontrivial (Proposition 2.2).
Step 3. Using Theorem 3.2 it follows that for appropriate ℓ, q the ℓ-rank of $H_1(N)_{(\ell)}$ must be $\sim p$, where q is a power of p.

It may in principle happen, that just one surjective map $\pi_1(M) \xrightarrow{\alpha} SL_2(\mathbb{F}_q)$ is not enough to produce nontrivial ℓ-homology in N, where $\pi_1(N) = \operatorname{Ker}\alpha$ (see Step 2 above). We will prove that if this phenomenon happens for infinitely many p, then M is hyperbolic in a weak sense (the Gromov simplicial volume is positive).

For a number field K, we denote $\mathcal{O}$ its ring of integers, and for a finite set S of primes we denote $\mathcal{O}_S$ its localisation at S.

THEOREM 1.3 (WEAK HYPERBOLIZATION). *Let M be atoroidal. Let $\rho : \pi_1(M) \to SL_2(\mathcal{O}_S)$ be a Zariski dense representation. Suppose that for infinitely many primes ℓ, there exists a rational prime $p \equiv \pm 1 \pmod{\ell}$ and a prime ideal $\mathfrak{p} \subset \mathcal{O}$ over p with residue field $\mathbb{F}_q$, such that the covering N defined by $1 \to \pi_1(N) \to \pi_1(M) \to SL_2(\mathbb{F}_q) \to 1$ has trivial ℓ-homology. Then M has positive Gromov invariant.*

REMARK. It is enough to demand that $\ell \nmid |H_3(SL_2(\mathcal{O}_s)|_{\text{tors}}$, so given the field K, the conditions can be effectively checked.

2. Homology of $SL_2(\mathbb{F}_q) \times SL_2(\mathbb{F}_s)$-coverings. Let M be a closed acyclic 3-manifold. In this section, we will study $SL_2(\mathbb{F}_q) \times SL_2(\mathbb{F}_s)$-coverings of M where q and s are prime powers and ℓ divides the orders of $SL_2(\mathbb{F}_q)$ and $SL_2(\mathbb{F}_s)$, but not qs.

PROPOSITION 2.1. *Let $1 \to \pi_1(N) \to \pi_1(M) \to SL_2(\mathbb{F}_q) \times SL_2(\mathbb{F}_s) \to 1$ be a Galois covering. Then either $b_1(N) > 0$, or $(H_1(N))_{(\ell)} \neq 0$.*

Proof. If N is a ℓ-homology sphere, then the spectral sequence of the covering inplies the direct product $SL_2(\mathbb{F}_q) \times SL_2(\mathbb{F}_s)$ has periodic ℓ-cohomology, multiplicatively generated by the Euler class. See [CE]. It follows [CE] that any abelian ℓ-group in $SL_2(\mathbb{F}_q) \times SL_2(\mathbb{F}_s)$ should be cyclic, which is obviously wrong. □

Consider the tower of coverings $Q \to N \to M$, where $1 \to \pi_1(N) \to \pi_1(M) \to SL_2(\mathbb{F}_q) \to 1$ and $1 \to \pi_1(Q) \to \pi_1(N) \to SL_2(\mathbb{F}_s) \to 1$ are exact. Suppose $(H_1(M))_{(\ell)} = 0$. Then either $(H_1(N))_{(\ell)} \neq 0$, or $(H_1(N))_{(\ell)} = 0$ and $(H_1(Q))_{(\ell)} \neq 0$. Replacing M by N in the latter case, we can assume that the first case holds.

PROPOSITION 2.2. *Suppose $1 \to \pi_1(N) \to \pi_1(M) \to SL_2(\mathbb{F}_q) \to 1$ is a Galois covering of rational homology spheres. Suppose $H_1(M)_{(\ell)} = 0$ and $H_1(N)_{(\ell)} \neq 0$. Then the natural action of $SL_2(\mathbb{F}_q)$ in $H^1(N, \mathbb{F}_\ell)$ is nontrivial.*

Proof. By Quillen [Qu], the cohomology ring $H^*(SL_2(\mathbb{F}_q), \mathbb{Z})_\ell$ is freely generated by one element of degree 4. Let $W = H^1(N, \mathbb{F}_\ell)$, then as an $SL_2(\mathbb{F}_q)$-module, $H^2(N, \mathbb{F}_\ell) \approx W^*$. The spectral sequence of the covering will look like

$$\begin{array}{llllllllll}
\mathbb{F}_\ell & 0 & 0 & \mathbb{F}_\ell & \mathbb{F}_\ell & \dots & & & & \\
\multicolumn{5}{l}{H^i(SL_2(\mathbb{F}_q), W^*)} & & & & & \Rightarrow H^{i+j}(M, \mathbb{F}_\ell) \\
\multicolumn{5}{l}{H^i(SL_2(\mathbb{F}_q), W)} & & & & & \\
\mathbb{F}_\ell & 0 & 0 & \mathbb{F}_\ell & \mathbb{F}_\ell & 0 & 0 & \mathbb{F}_\ell & \dots &
\end{array}$$

If the action of $SL_2(\mathbb{F}_q)$ in W were trivial, then this would reduce to

$$\begin{array}{lllllllll} \mathbb{F}_\ell & 0 & 0 & \mathbb{F}_\ell & \mathbb{F}_\ell & 0 & 0 & \dots & \\ W^* & 0 & 0 & W^* & W^* & 0 & 0 & & \Rightarrow H^{i+j}(M,\mathbb{F}_\ell) \\ W & 0 & 0 & W & W & 0 & 0 & & \\ \mathbb{F}_\ell & 0 & 0 & \mathbb{F}_\ell & \mathbb{F}_\ell & 0 & 0 & & \end{array}$$

Then we see that W^* which is indexed by $(4k+3,2)$ in the E^2-term is not hit by any differential and survives in E^∞. This contradicts the finite-dimensionality of $H^*(M)$. □

3. A variant of Artin's primitive root conjecture. In 1927 Artin conjectured that if $a \neq -1$ or a square, then a is a primitive root mod p for infinitely many primes p or, in other words, $< a >\cong \mathbb{F}_p^*$ for infinitely many primes p. Under the assumption that the Riemann Hypothesis holds for certain number fields, a quantitative version of the conjecture was proved by Hooley [Ho]. The best known unconditional result to date is due to Heath-Brown [HB]. His main result has the following theorem as a corollary:

THEOREM 3.1. *Let q, r and s be three distinct primes. Then at least one of them is a primitive root for infinitely many primes.*

In the proof of the Main Theorem we will use the following variant of Heath-Brown's result:

THEOREM 3.2. *Let q, r, s be three distinct primes each congruent to* 3 (mod 4). *Then for at least one of them, say q, there are infinitely many primes p such that q is a primitive root mod p and, moreover,* $p \equiv \pm 1 \pmod q$. *Furthermore, the estimate* $|\{p \leq x : < q >\cong \mathbb{F}_p^*,\ p \equiv -1 \pmod q\}| \gg x(\log x)^{-2}$ *holds true.*

(Notice that if $\ell \equiv 1 \pmod 4$ with ℓ a prime, then, by quadratic reciprocity, there are no primes p such that $p \equiv \pm 1 \pmod \ell$ and $< \ell >\cong \mathbb{F}_p^*$.)

Proof of Theorem 3.2. Let q, r, s be nonzero integers which are multiplicatively independent. Suppose none of $q,\ r,\ s,\ -3qr,\ -3qs,\ qrs$ is a square. Suppose, moreover, there exists a prime p_0 such that

$$(\frac{-3}{p_0}) = (\frac{q}{p_0}) = (\frac{r}{p_0}) = (\frac{s}{p_0}) = -1 \textit{ and } (p_0 - 1, 16qrs)|8. \qquad (2)$$

Then it follows from the proof of Theorem 1 of [HB] that $N'_{q,r,s}(x)$, the number of primes $p \leq x$ for which at least one of $q,\ r,\ s$ is a primitive root and such that, moreover, $p \equiv p_0 \pmod{16qrs}$, satisfies $N'_{q,r,s}(x) \gg x(\log x)^{-2}$.

Now let q, r and s be three distinct primes $\equiv 3 \pmod 4$. Then none of the integers $q,\ r,\ s,\ -3qr,\ -3qs$ and qrs is a square. We are done if we can find a prime p_0 such that $p_0 \equiv -1 \pmod{qrs}$ and such that, moreover, p_0 satisfies (2). Using quadratic reciprocity we see that any prime p_0 satisfying $p_0 \equiv 2 \pmod 3$, $p_0 \equiv 1 \pmod 4$, $p_0 \not\equiv 1 \pmod{16}$ and $p_0 \equiv -1 \pmod{qrs}$ (there are actually infinitely many of them), will meet the demands. □

The conjecture alluded to in the heading of this section, is the conjecture that if $\ell \not\equiv 1 \pmod 4$, ℓ a prime, then there are infinitely many primes p such that $p \equiv \pm 1 \pmod \ell$ and $< \ell >\cong \mathbb{F}_p^*$. On the generalized Riemann hypothesis this can be shown to be true, and moreover a quantitative version can be established [Mo].

4. Proof of the Main Theorem. By Theorem 9.1 of [R1], there is a Zariski dense representation of $\pi_1(M)$ in $SL_2(\bar{\mathbb{Q}})$. Let K be the splitting field of this representation, and let $n = [K : \mathbb{Q}]$. By [We], for almost all rational primes p the reduction modulo any prime over p in K will define a surjective map $\pi_1(M) \to SL_2(\mathbb{F}_q), q = p^m, m \leq n$, and moreover, for two such primes p, f the map $\pi_1(M) \to SL_2(\mathbb{F}_q) \times SL_2(\mathbb{F}_s)$, $q = p^m, s = f^r$, is surjective. From now on we only look at primes congruent to -1 modulo ℓ. Suppose that the ℓ-part of the homology of one such $SL_2(\mathbb{F}_s)$-covering N is zero. If this happens for ℓ big enough, this alone has far reaching consequences for the nature of M (the Gromov invariant is positive), as we will see in the proof of Theorem 1.3. Now we just notice that, by Proposition 2.1, we can relabel N by M and assume that for the rest of the primes p, either the ℓ-part of the homology of the $SL_2(\mathbb{F}_q)$-covering is nontrivial, or these coverings have positive b_1. In the first case, by Proposition 2.2, the action of $SL_2(\mathbb{F}_q)$ in $H^1(N, \mathbb{F}_\ell)$ is nontrivial. Since $PSL_2(\mathbb{F}_q)$ is simple, any element of order p in $SL_2(\mathbb{F}_q)$ also acts nontrivially. If $m = \dim H^1(N, \mathbb{F}_\ell)$, then we see that p divides $|GL_m(\mathbb{F}_\ell)|$, so that $p|(\ell - 1)(\ell^2 - 1) \cdots (\ell^{m-1} - 1)$. By Theorem 3.2 for appropriate ℓ, there are infinitely many primes p such that the order of ℓ in $\mathbb{F}_p^*$ equals $p - 1$. It follows that $m \geq p$. On the other hand, $|SL_2(\mathbb{F}_q)| \sim q^3$ and $n = \log_p q$ is bounded above by the degree of the number field, over which the representation of $\pi_1(M)$ is defined. Finally, $m >$ const $\cdot |SL_2(\mathbb{F}_q)|^\alpha$, where $1/3\alpha$ is the degree of the splitting field. The proof is complete in this case. In the other case, we get infinitely many $SL_2(\mathbb{F}_q)$-coverings with $b_1(N) > 0$. Since $b_1(M) = 0$, the representation of $SL_2(\mathbb{F}_q)$ in $H_1(N, \mathbb{C})$ does not have a trivial constituent. However, the smallest nontrivial irreducible representation of $SL_2(\mathbb{F}_q)$ has dimension $\sim q$, so $b_1(N) > d^{1/3}$. □

Proof of Theorem 1.2. Let N be as above and $m = \operatorname{rank}_\ell(H_1(N)) > Cd^\alpha$. There are at least ℓ^{m-1} subgroups of index ℓ in $H_1(N)_{(\ell)}$. So there are at least $\ell^{Cd^\alpha - 1}$ subgroups of index ℓd in $\pi_1(M)$. □

Proof of Theorem 1.3. Suppose the Gromov invariant of M is zero. By Proposition 5.4 of [R2], for representation $\sigma : \pi_1(M) \to SL_2(K)$, the homology class $\sigma_*[M] \in H_3(SL_2(K), \mathbb{Z})$ is torsion. This applies to the representation $\rho : \pi_1(M) \to SL_2(\mathcal{O}_S)$. Since the real cohomology of $SL_2(\mathcal{O}_S)$ and $SL_2(K)$ are isomorphic, $\rho_*[M] \in H_3(SL_2(\mathcal{O}_S))$ is also torsion. Now, the $H_i(SL_2(\mathcal{O}_S))$ are finitely generated [BS], so for some $0 \neq N \in \mathbb{Z}$, we have $N \cdot \rho_*[M] = 0$. From now on we assume that ℓ does not divide N. Then $\rho_*[M]_{(\ell)} \in (H_3(SL_2(\mathcal{O}_S))_{\text{tors}})_{(\ell)} = 0$. For any surjective homomorphism $SL_2(\mathcal{O}_S) \xrightarrow{\beta} SL_2(\mathbb{F}_q)$, we will have $0 = (\beta\rho)_*[M]_{(\ell)} \in H_3(SL_2(\mathbb{F}_q))_{(\ell)}$. On the other hand by Quillen [Qu], $H_3(SL_2(\mathbb{F}_q))_{(\ell)} \neq 0$ if $\ell | p^2 - 1$. Consider the homology spectral sequence of the covering $1 \to \pi_1(N) \to \pi_1(M) \to SL_2(\mathbb{F}_q) \to 1$:

$$\begin{matrix} H_i(SL_2(\mathbb{F}_q), \mathbb{Z}) \\ H_i(SL_2(\mathbb{F}_q), H_2(N)) \\ H_i(SL_2(\mathbb{F}_q), H_1(N)) \\ H_i(SL_2(\mathbb{F}_q), \mathbb{Z}) \end{matrix} \quad \Rightarrow H_{i+j}(M, \mathbb{Z})$$

Since the map $H_3(M, \mathbb{Z}) \to H_3(SL_2(\mathbb{F}_q), \mathbb{Z})$ is zero, one of the two differentials $d_2 : H_3(SL_2(\mathbb{F}_q), \mathbb{Z})_{(\ell)} \to H_1(SL_2(\mathbb{F}_q), H_1(N))_{(\ell)}, d_3 : \operatorname{Ker} d_2 \to H_0(SL_2(\mathbb{F}_q), H_2(N))_{(\ell)}$ is nonzero. But if $H_2(N) \neq 0$ then N is hyperbolic [Th] and the Gromov invariant of M is positive. If $H_2(N) = 0$, then $d_2 \neq 0$, so $H_1(N)_{(\ell)} \neq 0$. □

Concluding remarks. Theorem 1.3 can be stated with reference made only to representations of $\pi_1(M)$ over finite fields:

THEOREM 1.4. *Let M be atoroidal.Suppose for infinitely many rational primes l, there exists a rational prime $p \equiv \pm 1 (mod\ l)$ and a surjective representation $\rho_l : \pi_1(M) \to SL_2(\mathbb{F}_q)$, where q is a power of p, such that the covering defined by* $1 \to$

$\pi_1(N) \to \pi_1(M) \to SL_2(\mathbb{F}_q) \to 1$ has trivial l-homology.Then M has positive Gromov invariant.

Proof. Let F be an ultrafilter product of $\mathbb{F}_q$, so $char(F) = 0$. Let $\rho : \pi_1(M) \to SL_2(\mathbb{F})$ be the ultrafilter product of ρ_l. Fix an isomorphism between the ultrafilter product of $\bar{\mathbb{F}}_q$ and $\mathbb{C}$, so F is a subfield of $\mathbb{C}$. If ρ is not rigid as a representation to $SL_2(\mathbb{C})$, then M is Haken, therefore hyperbolic.So we may assume ρ is rigid, therefore after a conjugation is defined over a number field K. In particular $[\mathbb{F}_q : \mathbb{F}_p]$ are bounded. Let $\bar{\rho}$ be the representation defined over K which is conjugate to ρ. Then $\bar{\rho}$ is defined over $\mathcal{O}(K)$ since otherwise M is Haken again. Since $Tr(\bar{\rho}) = Tr\rho$, the reductions of $\bar{\rho}$ are conjugate to ρ_l over a quadratic extension of $\mathbb{Q}$. Then the proof goes as in the Theorem 1.3.

REFERENCES

[BS] A.Borel, J.-P.Serre, *Corners and arithmetic groups*, Comm. Math. Helv. **48** (1973), pp. 436–491.

[CE] A.Cartan, S.Eilenberg, *Homological Algebra*, Princeton University Press, 1956.

[HB] R.Heath-Brown, *A remark on Artin's conjecture*, Quart. J. Math. Oxford **37** (1986), pp. 27–38.

[Ho] C.Hooley, *Artin's conjecture for primitive roots*, J. Reine Angew. Math. **225** (1967), pp. 209–220.

[Mo] P.Moree, *On an conjecture stronger than Artin's primitive root conjecture*, unpublished manuscript, 1996.

[Qu] D.Quillen, *On the cohomology and K-theory of general linear group over finite fields*, Ann. Math. **96** (1972), pp. 552–586.

[R1] A.Reznikov, *Three-manifolds class field theory (Homology of coverings for a nonvirtually b_1-positive manifold)*, Selecta Math. **3** (1997), pp. 361–399.

[R2] A.Reznikov, *Rationality of secondary classes*, Journ. Diff. Geom. **43** (1996), pp. 674–692.

[SW] P.Shalen, P.Wagreich, *Growth rates, $\mathbb{Z}_p$-homology, and volumes of hyperbolic 3-manifolds*, Trans. Amer. Math. Soc. **331**(1992), pp. 895–917..

[Sh] A.Shalev, Personal communication.

[Th] W.Thurston, *Three-dimensional manifolds, Kleinian groups and hyperbolic geometry*, Bull. Amer. Math. Soc. **6** (1982), pp. 357–382.

[Tu] V.Turaev, *Nilpotent homotopy type of closed 3-manifolds*, LNM **1060** (1984).

[We] B.Weisfeller, *Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups*, Ann.Math. **120** (1984), pp. 271–315.