FIRST VERSION OF THIS PAPER

TORSION POINTS ON VARIETIES AND HOMOLOGY OF ABELIAN COVERS

Peter Sarnak */
STANFORD UNIVERSITY
1988

Section 1. Let T^r or simply T denote the r-torus $\mathbb{R}^r/\mathbb{Z}^r$. Its subgroup of torsion elements, i.e. those points all of whose coordinates are rational will be denoted by $\mathrm{tor}(T)$. By a real analytic function on T we mean a function ϕ on $\mathbb{R}^r$ which is real analytic and $\mathbb{Z}^r$ periodic. All functions on T considered in this paper will be real analytic. For each such ϕ, let V_ϕ be its divisor

$$V_\phi = \{\theta \in T \mid \phi(\theta) = 0\}.$$

The condition that $\phi|_\ell \not\equiv 0$ for any affine line of $\mathbb{R}^r$ is the same as saying that V contains no one parameter subgroup of T nor any translate thereof. We will refer to this situation by saying that V contains no lines.

Theorem 1. Assume V contains no lines then there is a constant C depending on V only such that

(a) $$|G \cap V| \leq C|G|^{1-\frac{3}{2r+1}}$$

for any finite subgroup G of T.

*/ This work was supported in part by the NSF under Grant DMS85-04329 and the PYI Award under Grant DMS84-51759.

(b) If moreover ϕ is a trigonometric polynomial then there is a C' such that $|G \cap V| \leq C'$ for any finite subgroup G, that is $|V \cap \mathrm{tor}(T)| < \infty$.

Remarks. (1) The condition that V contains no lines is clearly essential.

(2) Part (b) may be restated as follows. Let $p \in \mathbb{C}[z_1, z_1^{-1}, \ldots, z_r, z_r^{-1}]$ be a Laurent polynomial in r-variables. If $p(z_1, \ldots, z_r)$ has infinitely many zeros of the form $(\zeta_1, \zeta_2, \ldots, \zeta_r)$ where the ζ's are roots of unity then V_p (which is contained in the algebraic torus $(\mathbb{C}^*)^r$) contains an algebraic subtorus or translate thereof.

In this form this statement was conjectured by Lang [L2]. For $r=2$ it is in fact a known theorem see Lang [L3] and Liardet [LI].

(3) The exponent in part (a) is certainly not optimal. However for large r it is not too far from the optimal. This may be seen by considering the variety

$$V = \{\theta \mid \theta_1^2 + \theta_2^2 + \ldots + \theta_r^2 = 1/2\}$$

in T^r. V clearly contains no lines. Taking for G the group of n-torsion points; $(\mathbb{Z}/n\mathbb{Z})^r$ one finds that $G \cap V$ contains as many as Cn^{r-2} or $C|G|^{1-2/r}$ points.

Our methods for bounding $|G \cap V|$ are local in nature and hence as the following example in dimension $r=2$ shows, the methods cannot do better than exponent $\frac{1}{4}$. The example is the analytic arc

$$A = \{y=x^2 : -\tfrac{1}{2} \leq x \leq \tfrac{1}{2}\} \tag{1.1}$$

in T^2. If n is a perfect square and $G_n = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ then $G_n \cap V$ is of order $\sqrt{n}$. We add however that for a globally analytic curve V in T^2 (which contains no line) we know of no example for which $|G_n \cap V| \geq cn^{\varepsilon_o}$ for infinitely many n (c, $\varepsilon_o > 0$ and fixed).

These questions in Dimension 2 are closely related to the problem of bounding the number of points, $S_n(C)$ on a strictly convex curve C and with rational coordinates of denominator n. Jarnik [J] has shown that

$$S_n(C) = O(n^{2/3}) . \tag{1.2}$$

In fact he proves the stronger general statement that if C is a strictly convex curve in $\mathbb{R}^2$ of length ℓ, then the number of lattice points (in $\mathbb{Z}^2$) on C is at most

$$\max (10, 10\ell^{2/3}) . \tag{1.3}$$

Swinnerton-Dyer [S W] has improved the estimate (1.2) under the assumption that C is 3-times continuously differentiable showing

(1.4) $$S_n(C) = O(n^{3/5}) .$$

Swinnerton-Dyer also gives examples of C^k strictly convex curves for which $S_n(C) \geq n^{1/k}$ for infinitely many n. Note however that if we extend the arc A in (1.1) above, in a C^∞ way to give a strictly convex C^∞ closed curve, then for this C we will have $S_n(C) \geq n^{1/2}$, for infinitely many n. It seems reasonable to conjecture that the exponent $\frac{1}{2}$ is the optinal one for C^∞ strictly convex curves.

We apply Theorem 1 to study the Betti numbers of abelian coverings of a given compact manifold. Essentially what we find is that these behave in an asymptotically linear way in the degree of the cover. For example we show that if the k-th Betti number, $\beta_k(M)$ of a compact smooth orientable manifold is zero, then there is a $P = P(M)$ such that $\beta_k(M') = 0$ for any covering M' of M whose group of deck transformations $G(M'/M)$ is of prime order $p \geq P$. (1.5)

(1.5) is interesting only in the case that there are abelian covers of M of arbitrary degree i.e. that $\beta_1(M) > 0$. We henceforth assume for simplicity that $H_1(M,\mathbb{Z}) \tilde{=} \mathbb{Z}^r$ with $r \geq 1$. The character group of $\Gamma = \Pi_1(M)$ and of $H_1(M,\mathbb{Z})$, is thus identified with $(C^*)^r$. Such characters will be denoted by χ. The unitary characters are in this way identified with T^r. Let K be a triangulation of M and $\tilde{K}$ its universal cover. The fundamental group Γ acts freely on $\tilde{K}$ as deck

transformations. Following Ray-Singer [R-S] we think of K as embedded in $\tilde{K}$ as a fundamental domain for the action of Γ. In this way we get a preferred basis for the Γ invariant q-chains, (with coefficient in $\mathbb{C}$) on $\tilde{K}$, viz the q-simplices of K. In a similar way we get a preferred basis for the finite dimensional space $C_q(\tilde{K},\chi)$ of q-chains on $\tilde{K}$ which transform by Γ with a twist by the character χ. The boundary operator $\partial_q^\chi : C_q(\tilde{K},\chi) \to C_{q-1}(\tilde{K},\chi)$ when computed as a matrix in this preferred basis will have entries which are polynomials in χ and χ^{-1}. Also using this basis we obtain an adjoint $(\partial_q^\chi)^* : C_q(\tilde{K},\chi) \to C_{q+1}(\tilde{K},\chi)$. The combinatorial χ twisted Laplacian $\Delta_q^{(c)}(\chi)$ is defined by

$$\Delta_q^{(c)}(\chi) = (\partial_{q-1}^\chi)^* \partial_q^\chi + \partial_{q+1}^\chi \partial_q^* \quad . \tag{1.6}$$

One checks just as with usual Hodge theory that

$$\dim \ker \Delta_q^{(c)}(\chi) = \beta_q(\chi) \tag{1.7}$$

where $\beta_q(\chi)$ is the dimension of the q-th homology of χ twisted chains on $\tilde{K}$. We also note that the entries of our matrix representation of $\Delta_q^c(\chi)$ are polynomials in χ and χ^{-1}. In order to investigate $\beta_q(\chi)$ as a function of χ we consider the characteristic polynomial

$$P_q(\lambda, \chi) = \det(\lambda + \Delta_q^{(c)}(\chi)) \quad . \tag{1.8}$$

In view of the previous remarks P is a polynomial in λ and a Laurent polynomial in χ. Define $\ell_q(M)$ to be the least natural number ℓ for which

$$Q_q(\chi) = \frac{\partial^\ell P_q(\lambda,\chi)}{\partial\lambda^\ell}\Big|_{\lambda=0} \not\equiv 0 . \tag{1.9}$$

We have that $Q_q(\chi)$ is a trigonometric polynomial on T and let V_q be its divisor. Using Theorem 1 part (b) we will prove

Theorem 2. If V_q contains no lines then

$$\beta_q(M') = \ell_q(M)n + O(1)$$

for any abelian cover M' of M, of degree n.

In this theorem if V_q contains lines then the possible behavior of $\beta_q(M')$ is more complicated in view of the possibility of $(G(M'/M))^*$ lying on such a line. One can nevertheless still develop a similar formula though we do not do so here.

The formula in Theorem 2 may be viewed as a generalization to abelian covers of the Riemann-Hurwitz formula

$$\beta_1(M') = (\beta_1(M) - 2)n + 2 \tag{1.10}$$

for a regular covering M' of degree n of a compact surface M of genus > 0.

The integers $\ell_q(M)$ have an interpretation in terms of L^2-cohomology. In fact one could also have developed the above (especially the variety V_q) using Hodge theory. Suppose σ is a Riemannian metric on M. We let $\Delta_q(\chi)$ be the Laplacian on χ twisted q-forms. Let $\tilde{M}_{ab}$ denote the maximal abelian cover of M with the lifted metric. Using the results of Donnelly [D 2] it is easily seen that

$$\ell_q(M) = \beta^q(\tilde{M}_{ab}) \tag{1.11}$$

where $\beta^q(\tilde{M}_{ab})$ is the von-Neumann Γ-dimension of the L^2 harmonic q-forms on $\tilde{M}_{ab}$ and $\Gamma = G(\tilde{M}_{ab}/M)$, see Atiyah [A] for definitions.

From their definition in (0.8) above we see that

$$\begin{cases} 0 \leq \ell_q(M) \leq \beta_q(M) \\ \ell_o(M) = \ell_m(M) = 0 \quad \text{where } m = \dim M \\ \ell_j(M) = \ell_{m-j}(M) \quad \text{(Poincarè duality).} \end{cases} \tag{1.12}$$

Moreover using Atiyah's L^2-index theorem [A], or simply Theorem 2 together with the multiplicative properties of the Euler number under covers we also have the relation

$$\sum_{j=1}^{m-1} (-1)^j \ell_j(M) = \chi(M) . \tag{1.13}$$

For $q = 1$ the inequality (1.12) can be slightly improved: We will show

(1.14) $$\ell_1(M) \leq \beta_1(M) - 1 .$$

As a consequence of this and Theorem 2 we have the following general fact: If $H_1(M,\mathbb{Z}) \tilde{=} \mathbb{Z}$ then there is a constant $C = C(M)$ such that $\beta_1(M') \leq C$ for all abelian (i.e. cyclic) covers M' of M.

(1.15)

The methods above may be combined with part (a) of Theorem 1 to give similar results for the dimensions of the spaces of automorphic forms in abelian covers. Let M be a compact locally symmetric space of Rank 1 (if the rank of M is ≥ 2 then $\beta_1(M) = 0$ by a result of Kashdan [KA]). Let Δ denote the Laplacian on functions on M. For $\lambda \geq 0$ let $N_\lambda(M)$ denote the dimension of the space of eigenfunctions of Δ on M with eigenvalue λ. Then under conditions similar to Theorem 2 we have

(1.16) $$N_\lambda(M') = \ell_\lambda(M)n + O(n^{1-\frac{3}{2r+1}})$$

where M' is an abelian cover of M of degree n, and $\ell_\lambda(M)$ are integers determined as follows: We let $F(\lambda,\chi) = \det(\lambda - \Delta(\chi))$, $\lambda \in \mathbb{C}$, $\chi \in T$. In this case the determinant is defined through a regularization, see [R-S]. Using the analysis in Sarnak [S 1] one can show that $F(\lambda,\chi)$ is real analytic. So one proceeds as above but this time $Q(\chi)$ is real analytic and not a trigonometric polynomial and we need to appeal to part (a) of Theorem 1.

We end this section by remarking that for general covers M' of M the behavior of the individual $\beta_k(M')$ is difficult to approximate. However for a "tower of coverings" M_n converging to the universal cover $\tilde{M}$ of M (see deGeorge and Wallach [D-W]) of degree d_n, Donnelly [D 1] has shown that

$$\lim_{n \to \infty} \frac{1}{d_n} \beta_k(M_n)$$

exists and is closely related to the von-Neumann dimensions $\beta^k(\tilde{M})$.

Section 2. Proof of Theorem 1.

Throughout this section we assume that V satisfies the hypothesis that it contains no lines. The set of lines in $\mathbb{R}^r$ may be topologized in an obvious way.

Lemma 2.1. For $p \in V \cap \ell$, where ℓ is a line, there is a number $C = C(p,\ell)$ and neighborhoods M of ℓ and N of p such that,

$$|\ell' \cap N \cap V| \leq C(p,\ell)$$

for $\ell' \in M$.

Proof. The claim is clearly local, so we may take $p = 0 \in \mathbb{R}^r$ and ℓ to be the line $\{(x_1,0,\ldots,0) | x_1 \in \mathbb{R}\}$. By hypothesis $\phi(x_1,0,\ldots,0) = f(x_1)$ is real analytic and not identically zero. A neighborhood of lines about ℓ

is contained in the set of lines of the form

$$\ell_{u,v} = \{uz + v \mid z \in \mathbb{R}\} \quad \text{where}$$

$|u| = 1$ and u is close to $(1,0,\ldots,0)$ and v close to $0 \in \mathbb{R}^r$. For u,v as above and N a small neighborhood of 0 the cardinality of $\ell_{u,v} \cap N \cap V$ is the number of distinct zeros of $f_{u,v}(z) = \phi(uz + v)$ in the corresponding neighborhood of $z = 0$.

Now $f(z)$ and $f_{u,v}(z)$ extend to be complex analytic in z in some neighborhood $|z| < \varepsilon_1$ say. There is $0 < \varepsilon_2 < \varepsilon_1$ such that $f(z) \neq 0$ for $0 < |z| \leq \varepsilon_2$. Let $0 < \eta = \min\{|f(z)| : |z| = \varepsilon_2\}$. By continuity we can choose a small neighborhood M of (u,v)'s about $((1,0,\ldots,0), (0,\ldots,0))$ such that

$$|f_{u,v}(z) - f(z)| < \eta \leq |f(z)| \quad \text{for} \quad |z| = \varepsilon_2 .$$

It follows that $f_{u,v}(z)$ has the same number m of complex zeros (with multiplicity) as does $f(z)$ in $|z| < \varepsilon_2$. In particular it follows that $f_{u,v}(z)$ for $(u,v) \in M$ has at most this number of real zeros in $|z| < \varepsilon_2$. Hence for a suitable small neighborhood N of 0 in $\mathbb{R}^r$ we have $\ell' \in M \Rightarrow |\ell' \cap V \cap N| \leq m$. This proves Lemma 2.1.

Lemma 2.2: Let $V' = V \cap \overline{B(0,2)}$, there is a constant C such that

$$|V' \cap \ell| \leq C \quad \text{for all lines } \ell.$$

Proof. Again topologize the set of lines (affine) in $\mathbb{R}^r$. The subset K of those lines meeting $\overline{B(0,1)}$ is compact. Hence to prove Lemma 2.2 it suffices to show that for each $\ell \in K$ there is a neighborhood $N(\ell)$ of ℓ and a number $C(\ell)$ such that $|\ell' \cap V'| \leq C(\ell)$ for $\ell' \in N(\ell)$.

Now for $\ell \in K$ we have $\ell \cap V' = F_\ell$ is a finite set $\{p_1,\ldots,p_r\}$ say. If $p \in V'$ and $p \notin F_\ell$ then clearly a neighborhood $N(p)$ of p exists s.t. $N(p) \cap \ell = \phi$. For $p = p_j \in F_\ell$ there is by Lemma 1.1 a neighborhood $N(p_j)$ of p_j and a neighborhood $M_{p_j}(\ell)$ of ℓ such that

$$|\ell' \cap N(p_j) \cap V'| \leq C(p_j,\ell) .$$

The $N(p)$'s and $N(p_j)$ cover the compact set V', so we have a finite subcover $N(q_1),\ldots,N(q_s)$ and $N(p_1),\ldots,N(p_r)$. For each q_ν there is a neighborhood $M_\nu(\ell)$ of ℓ s.t. $\ell' \cap M_\nu(\ell) \Rightarrow \ell' \cap V' = \phi$. If $M = \bigcap_\nu M_\nu \cap \bigcap_j N_j$ then $\ell' \in M \Rightarrow |\ell' \cap V'| \leq \sum_{j=1}^{r} C(p_j,\ell)$. As pointed out before this proves the lemma.

We turn to the proof of Theorem 1. Let G be an arbitrary finite subgroup of $T = \mathbb{R}^r/\mathbb{Z}^r$ and denote by n the order of G. Let L be the lattice in $\mathbb{R}^r$

$$L = \{g+n \mid g \in G,\ n \in \mathbb{Z}^r\} . \tag{2.1}$$

Clearly $L/\mathbb{Z}^r \equiv G$ and so

$$\mathrm{Vol}(L) = \frac{1}{n} . \tag{2.2}$$

We may in this way think of $G \cap V$ as

$$L \cap V \cap \mathfrak{F}$$

where

$$\mathfrak{F} = (-1/2, 1/2\,]^r \tag{2.3}$$

is the usual fundamental domain for $\mathbb{Z}^r$.

It is known from the geometry of numbers, see Lekkerkerker [LE p.126] that we can find a basis $\xi_1, \ldots, \xi_r$ of L such that ξ_1 has least length of the non-zero elements of L and

$$\text{(2.4)} \quad \begin{cases} \text{(1)} \quad |\xi_j| \le C\,|\xi_{j+1}| \qquad j = 1, \ldots, r-1 \,. \\ \text{(2)} \quad \text{If } \rho_j = \operatorname{dist}(\xi_j, L(\xi_1, \ldots, \xi_{j-1})) \text{ then} \\ \qquad\qquad \rho_j \le |\xi_j| \le C\,\rho_j \,. \end{cases}$$

Here and in what follows C is a constant depending on r only (sometimes on V too) and from one line to the next C may stand for different constants. $L(\xi_1, \ldots, \xi_t)$ is the linear space spanned by $\xi_1, \ldots, \xi_t$.

From (2.4) it follows that

$$\frac{1}{n} = \operatorname{Vol}(L) \le |\xi_1| \cdots |\xi_r| \le \frac{C}{n} \,. \tag{2.5}$$

The following statement is easily checked:

Let W be a subspace of $\mathbb{R}^r$ and let $a \in \mathbb{R}^r$ then if $\operatorname{dist}(\xi, W) \geq \eta|\xi|$ then

$$\{t \mid \phi \neq (t\xi + W) \cap \overline{B(a,2)}\} \tag{2.6}$$

is an interval of length at most $2\eta^{-1}$.

For each $(m_2, m_3, \ldots, m_r)$ we want to bound

$$|\{m_1 \mid m_1\xi_1 + \sum_{j=2}^{r} m_j\xi_j \in V \cap \mathfrak{F}\}|. \tag{2.7}$$

This number is at most

$$|\{t \mid t\xi_1 + \sum_{j=2}^{r} m_j\xi_j \in V \cap \mathfrak{F}\}|.$$

From Lemma 2.2 this is $O(1)$ i.e. For each $(m_2, \ldots, m_r)$

$$|\{m_1 \mid m_1\xi_1 + \sum_{j=2}^{r} m_j\xi_j \in V \cap \mathfrak{F}\}| \leq C. \tag{2.8}$$

Hence to bound $|L \cap V \cap \mathfrak{F}|$ we have

$$\begin{aligned} |L \cap V \cap \mathfrak{F}| &= |\{(m_1, \ldots, m_r) \mid \sum_{j=1}^{r} m_j\xi_j \in V \cap \mathfrak{F}\}| \\ &\leq \sum_{m_2, \ldots, m_r} |\{m_1 \mid m_1\xi_1 + \sum_{j=2}^{r} m_j\xi_j \in V \cap \mathfrak{F}\}| \qquad (2.9) \\ &\leq C\,|\{(m_2, \ldots, m_r) \mid (\mathbb{R}\xi_1 + \sum_{j=2}^{r} m_j\xi_j) \cap \overline{B(0,2)} \neq \phi\}|. \end{aligned}$$

We claim the cardinality of the last set is

$$\leq C|\xi_1|n \tag{2.10}$$

and hence

$$|G \cap V| = |L \cap V \cap \mathfrak{F}| \leq C|\xi_1|n \ . \tag{2.11}$$

To see (2.10) begin by first bounding the number of m_r's. This number is

$$\leq \#\{m_r | [m_r\xi_r + L(\xi_1,\ldots,\xi_{r-1})] \cap \overline{B(0,2)} \neq \phi\} \ .$$

But from (2.4) and (2.6) the interval of t's

$$\{t \mid t\xi_r + L(\xi_1,\ldots,\xi_{r-1}) \cap \overline{B(0,2)} \neq \phi\}$$

has length $O(1)$ hence

$$\#\, m_r\text{'s} \leq \max[C|\xi_r|^{-1}, 1] \ . \tag{2.12}$$

For each m_r one can bound the number of m_{r-1}'s in the same way. Continuing this way leads to

$$(2.13)\qquad |G \cap V| = |L \cap V \cap \mathfrak{F}| \leq C|\xi_2|^{-1}|\xi_3|^{-1} \dots |\xi_r|^{-1}$$

$$\leq Cn|\xi_1|, \quad \text{from (2.5)}.$$

(2.13) already gives a weak version of Theorem 1 part (a) since from (2.4) we have

$$(2.14)\qquad |\xi_1|^r \leq \frac{C}{n}$$

$$\text{or} \quad |\xi_1| \leq Cn^{-1/r}.$$

Hence

$$(2.15)\qquad |G \cap V| \leq Cn^{1-\frac{1}{r}}.$$

Actually this weak form (2.15) suffices to prove Theorem 1 part b as will be seen.

We now develop the stronger estimate claimed in part (a) of Theorem 1. Assume now that $r \geq 2$.

We need to consider also intersections of V by affine planes. Let P denote a plane in $\mathbb{R}^r$. $P \cap V \cap \mathfrak{F}$, if not empty will consist of a finite number of analytic arcs, none of which is a straight line. We call an arc in P strictly curved if it is either strictly convex or concave. Clearly by real analyticity $P \cap V \cap \mathfrak{F}$ can be broken into a finite number of such strictly curved arcs. By compactness

arguments similar to the ones of Lemmas 2.1 and 2.2, which we do not repeat here, we have

Lemma 2.3. There is a constant C depending on V only such that $P \cap (\mathfrak{F} \cap V)$ decomposes into at most C disjoint strictly curved analytic arcs of length at most C.

Returning to bounding $L \cap V \cap \mathfrak{F}$ we have

$$(2.16) \quad \left|\{(m_1,\dots,m_r) \mid \sum_{j=1}^{r} m_j \xi_j \in V \cap \mathfrak{F}\}\right| \leq \sum_{(m_3,\dots,m_r)} \#\{(m_1,m_2) \mid m_1\xi_1 + m_2\xi_2 \in -(m_3\xi_3 + \dots + m_r\xi_r) + V \cap \mathfrak{F}\}.$$

For each $(m_3,\dots,m_r)$ the plane

$$P_{(m_3,\dots,m_r)} = \mathbb{R}\xi_1 + \mathbb{R}\xi_2 + (m_3\xi_3 + \dots + m_r\xi_r),$$

meets $V \cap \mathfrak{F}$, either in the empty set, or in a union of at most C strictly curved arcs, a typical one of which we denote by $\Gamma_{(m_3,\dots,m_r)}$. We need to bound (in the case that $[(V \cap \mathfrak{F})] \cap P_{(m_3,\dots,m_r)} \neq \phi$) the intersection

$$(2.17) \quad \begin{cases} |\Gamma_{(m_3,\dots,m_r)} \cap L_1| & \text{where} \\ L_1 = \{m_1\xi_1 + m_2\xi_2 \mid (m_1,m_2) \in \mathbb{Z}^2\}. \end{cases}$$

Lemma 2.4.

$$|\Gamma_{(m_3,\ldots,m_r)} \cap L_1| \leq C|\xi_1|^{-2/3} .$$

Before proving this lemma note that by an argument similar to (2.13) above we find that the number of $(m_3,m_4,\ldots,m_r)$ for which $(V \cap \mathfrak{F}) \cap P_{(m_3,\ldots,m_r)} \neq \phi$ is $O(|\xi_3|^{-1}|\xi_4|^{-1} \ldots |\xi_r|^{-1})$ and hence Lemma 2.4 implies that

$$(2.18) \quad |V \cap G| = |L \cap V \cap \mathfrak{F}| \leq C|\xi_1|^{-2/3}|\xi_3|^{-1} \ldots |\xi_r|^{-1} \leq C|\xi_1|^{1/3}|\xi_2|n .$$

Proof of Lemma 2.4. From Lemma 2.3, Γ is a strictly curved analytic arc of length at most C. Let $A : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map

$$Ae_1 = \xi_1 , \; Ae_2 = \xi_2 \quad \text{where} \quad e_1 = (1,0), \; e_2 = (0,1).$$

Then

$$|\Gamma \cap L_1| = |A^{-1}\Gamma \cap A^{-1}L_1| = |A^{-1}\Gamma \cap \mathbb{Z}^2| .$$

Now $A^{-1}\Gamma$ is a strictly convex curve in the plane and we want to bound the number of standard lattice points on $A^{-1}\Gamma$. If its length is $\ell \geq 1$ then Jarnik's theorem see (1.3) asserts that

$$|A^{-1}\Gamma \cap \mathbb{Z}^2| \leq C\ell + 2/3 \quad . \tag{2.19}$$

An upper bound on ℓ is $|\xi_1|^{-1}$, which follows from (2.4). (2.19) and this bound on ℓ yield Lemma 2.4.

We have established from (2.18) and (2.13) that

$$|G \cap V| \leq C \min\{|\xi_1|^{1/3} |\xi_2| n, |\xi_1| n\} . \tag{2.20}$$

Again from (2.4)

$$|\xi_2| \leq C(n|\xi_1|)^{-\frac{1}{r-1}} \quad .$$

Hence

$$|G \cap V| \leq C \min\{ |\xi_1|^{\frac{1}{3} - \frac{1}{r-1}} n^{1 - \frac{1}{r-1}} , |\xi_1| n \}$$

and so

$$|G \cap V| \leq C n^{1 - \frac{3}{2r+1}} \quad .$$

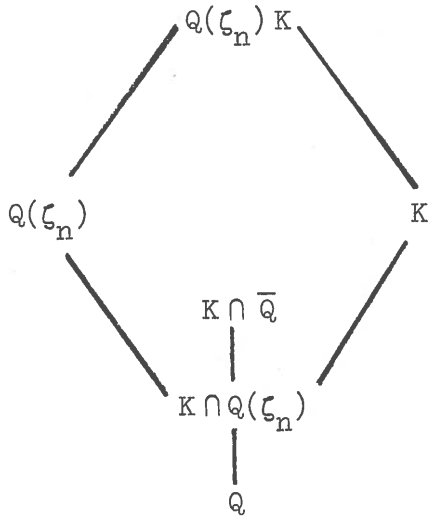
This completes part (a) of Theorem 1.

We now prove part (b). Let $p(\theta_1, \ldots, \theta_r)$ be the trigonometric polynomial

$$p(\theta_1, \ldots, \theta_r) = \sum_{|m| \leq M} a_m e(\langle \theta, m \rangle) \tag{2.21}$$

Let K be the finitely generated extension of Q, $K = Q(\{a_m\}_{|m| \leq M})$. We claim that for n large enough there can be no point $(\theta_1, \theta_2, \ldots, \theta_r) \in \mathrm{tor}(T) \cap V$ of order n, i.e. a point $(\frac{x_1}{n}, \frac{x_2}{n}, \ldots, \frac{x_r}{n}) \in V$ with $x_j \in \mathbb{Z}$ and $(x_1, x_2, \ldots, x_r, n) = 1$ cannot exist. Clearly this will imply the result.

Suppose such a point exists. Consider the inclusion diagram of fields



Here $Q(\zeta_n)$ is the cyclotomic field Q adjoin the n^{th} root of 1, $\zeta_n = e(\frac{1}{n})$ and $\bar{Q}$ is the algebraic closure of Q. Since K is finitely generated $[K \cap \bar{Q}, Q]$ is finite and hence

$$[K \cap Q(\zeta_n) : Q] \leq B \tag{2.22}$$

where B is independent of n. Now $Q(\zeta_n)/Q$ is Galois of degree $\phi(n)$

(ϕ being the Euler function) and its Galois group is $(\mathbb{Z}/_{n\mathbb{Z}})^*$. For $s \in (\mathbb{Z}/_{n\mathbb{Z}})^*$ we have the automorphism $\sigma_s : \zeta_n \to \zeta_n^s$. It follows, see Lang [L 1] Theorem 1.12, that $Q(\zeta_n)K/K$ is Galois with Galois group isomorphic to that of $GAL(Q(\zeta_n)/K \cap Q(\zeta_n)) \triangleq G_n$. From (2.22) we get

$$|G_n| \geq \phi(n)/B \ . \tag{2.23}$$

Moreover for each $\sigma_s \in G_n$ (here $(s,n) = 1$) the corresponding automorphism $\tilde{\sigma}_s$ of $Q(\zeta_n)K/K$ sends $\zeta_n \to \zeta_n^s$. We have

$$\sum_{|m| \leq M} a_m \ e\left(\frac{\langle x,m\rangle}{n}\right) = 0, \quad x = (x_1,\ldots,x_r) \qquad \text{i.e.}$$

$$\sum_{|m| \leq M} a_m \ \zeta_n^{\langle x,m\rangle} = 0 \ .$$

Applying $\tilde{\sigma}_s \in G_n$ to this, gives

$$\sum_{|m| \leq M} a_m \ \zeta_n^{sr\langle x,m\rangle} = 0 \qquad \text{or}$$

$$\sum_{|m| \leq M} a_m \ e\left(\frac{\langle sx,m\rangle}{n}\right) = 0 \ .$$

That is

$$\left(\frac{sx_1}{n} , \frac{sx_2}{n} , \ldots , \frac{sx_r}{n} \right) \in V .$$

Since $(\frac{x_1}{n} , \ldots , \frac{x_r}{n})$ is of exact order n, it follows that for $1 \leq s_1 < n$, $1 \leq s_2 < n$, $s_1 \neq s_2$, $s_1(\frac{x_1}{n}, \ldots, \frac{x_r}{n})$ and $s_2(\frac{x_1}{n}, \ldots, \frac{x_r}{n})$ are distinct in T. We have therefore constructed $\phi(n)/B$ points in V of the form $s(\frac{x_1}{n}, \ldots, \frac{x_r}{n})$ with $1 \leq s < n$. All these points lie in the finite subgroup G of T generated by $(\frac{x_1}{n}, \ldots, \frac{x_r}{n})$,

$$G = \langle (\frac{x_1}{n} , \ldots , \frac{x_r}{n}) \rangle$$

whose order $|G| = n$. We therefore have

$$(2.24) \qquad \begin{cases} |G \cap V| \geq \phi(n)/B & \text{and} \\ |G| = n . \end{cases}$$

Since $\phi(n) \gg \dfrac{n}{\log \log n}$ (see Hardy-Wright [H-W] page 267) we are clearly led to a contradiction of (2.15) for n large enough.

This completes the proof of Theorem 1.

Section 3. In this section we prove Theorem 2 as well as the other claims made in Section 1. If $\beta_q(X)$ is the number defined in (1.7) then it is easy to see that for M' an abelian cover of M and $G(M'|M)$ the corresponding group of deck transformations we have

$$\beta_q(M') = \sum_{\chi \in (G(M'|M))^*} \beta_q(\chi) \,. \tag{3.1}$$

The summation running over the unitary characters (i.e. dual group) of $G(M'|M)$. In particular each $\chi \in (H_1(M,\mathbb{Z}))^*$.

Except for the claim (1.5) we are assuming that $H_1(M,\mathbb{Z}) \tilde{=} \mathbb{Z}^r$ so that $H_1(M,\mathbb{Z}) = T^r$. For the case considered in (1.5) it is clear that if $|G(M'|M)| = p$, a large enough prime, then any $\chi \neq 1$ which of order p appearing in (3.1) must lie on the connected component of the identity in $H_1(M,\mathbb{Z})^*$. Hence even in this case we need only consider this connected component which is again T^r.

From (1.7), (1.8) and the definition of $\ell_q(M)$ it is clear that

$$\begin{cases} \beta_q(\chi) = \ell_q(\chi) + \mathcal{E}_q(\chi) \qquad \text{with} \\ \min\left\{1, \dfrac{\operatorname{ord} Q_q(\chi)}{2}\right\} \leq \mathcal{E}_q(\chi) \leq \dfrac{\operatorname{ord} Q_q(\chi)}{2} \end{cases} \tag{3.3}$$

and where $\operatorname{ord} Q(\xi)$ is the order of vanishing of Q at ξ. The reason for dividing the order by two in (3.3) is that $Q_k(\chi)$ vanishes to even order

since the eigenvalues of $\Delta_q^{(c)}(\chi)$ are nonnegative and hence each one vanishes to even order.

In as much as T is compact it follows that $\operatorname{ord} Q_q(\chi)$ is bounded above by a constant depending only on M. Combining this remark with (3.1) and (3.3) we have

$$\beta_q(M') = \ell_q(M)n + O(|G^* \cap V_q|) \tag{3.4}$$

for any $M'|M$ abelian of order n and with abelian deck group G.

Theorem 2 follows from (3.4) and Theorem 1 part (b) (recall as was observed after (1.9) that in this case $Q_q(\chi)$ is indeed a trigonometric polynomial).

The claim (1.5) follows easily from the arguments used to prove Theorem 1 (b). In fact in this case the trigonometric polynomial $P_q(0,\chi)$ satisfies $P_q(0,\chi) \neq 0$ since $\beta_q(M) = 0$. Moreover an examination of the representation of ∂_q^{χ} as a matrix in (1.6) shows that its entries are polynomials in χ and χ^{-1} with integral coefficients. It follows that $P_q(0,\chi) \in \mathbb{Z}[\chi, \chi^{-1}]$. Hence in this application the field K in Figure (2.1) is in fact Q. The action of the Galois group in this case shows that if V_{P_q} contains an element $(\frac{x_o}{p}, \ldots, \frac{x_r}{p})$ of order a prime p, then it contains $s(\frac{x_o}{p}, \ldots, \frac{x_r}{p})$ for $1 \leq s \leq p-1$. That is V_{Q_o} contains all elements of the subgroup $G = \langle (\frac{x_o}{p}, \ldots, \frac{x_r}{p}) \rangle$ other than 0. We have seen

that such a subgroup contains an element $\xi \neq 0$ with $\|\xi\| = O(p^{-1/r})$. Since we are assuming $P_q(0,0) \neq 0$ the above would lead to a contradiction. That is for p large we have $\beta_q(\chi) = 0$ for any χ of order p and so (3.1) implies $\beta_q(M') = 0$ for $|M'|M| = p$, proving (1.5).

In this proof of (1.5) we made serious use of the fact that $P_q \in \mathbb{Z}[X, X^{-1}]$. It would be nice to drop the condition of the coefficients being in Q. We are able to do so if we assume the Riemann hypothesis for L functions viz the E.R.H.

Proposition 3.1. Assume E.R.H. If $P(\theta_1,\ldots,\theta_r)$ is a trigonometric polynomial with $P(0) \neq 0$ then there is P_o such that $P(\theta) \neq 0$ for any $\theta \in \mathrm{tor}(T)$ of prime order $p \geq P_o$.

Proof. Following the analysis of the proof of Theorem 1 part (b) we have the Galois group of $KQ(\zeta_p)/K$ is isomorphic to a subgroup H of $GAL(Q(\zeta_p)/Q)$. Moreover $|(\mathbb{Z}/_{p\mathbb{Z}})^*/H| \leq B$ for some constant B. If $y = (\frac{x_1}{p}, \frac{x_2}{p}, \ldots, \frac{x_r}{p}) \in V_P$ and is order p then $hy \in V_P$ for each $h \in H$. As usual we have some $t \in (\mathbb{Z}/_{p\mathbb{Z}})^*$ such that

$$\xi = ty \quad \text{has} \quad \|\xi\| \leq C_1 p^{-1/r}. \tag{3.5}$$

Under the G.R.H. we claim that we can find $m \in \mathbb{Z}/_{p\mathbb{Z}}$ with $|m| \leq C_2(\log p)^{3B}$ such that m lies in the multiplicative coset

(3.6) $$m \in t^{-1} H .$$

Given this it follows that

$$hy = tmy = m\xi .$$

From (3.5) and the above bound on m

(3.7) $$\|hy\| \leq C_4 (\log p)^{3B} p^{-1/r} .$$

Now $hy \in V_P$ and since $P(0) \neq 0$, the result follows from the continuity of P. To prove (3.6) we recall the result of Wang [W] which asserts that under the E.R.H., $(\mathbb{Z}/p\mathbb{Z})^*$ has a primitive root g with

(3.8) $$|g| \leq C (\log p)^3 .$$

We must show that any coset of H in $(\mathbb{Z}/p\mathbf{Z})^*$ has a representative in $[1, C (\log p)^{3B}]$. By exponentiation

$$H \tilde{=} \{t \in \mathbb{Z}/(p-1)\mathbb{Z} \mid g^t \in H\} = \tilde{H} .$$

Also

$$|(\mathbb{Z}/(p-1)\mathbb{Z})/H| \leq B .$$

Clearly then any coset of $\tilde{H}$ in $\mathbb{Z}/(p-1)\mathbb{Z}$ has a representative $0 \leq \eta < B$. Hence each coset of H in $(\mathbb{Z}/p\mathbb{Z})^*$ has a representative g^η ,

$0 \leq \eta < B$ and so from (3.8) such a representative is $O((\log p)^{3B})$.

We turn to the proof of (1.14). This may be derived from the following useful variational formula. We assume as in the paragraph before (1.11) that M carries a metric and all computations are relative to this metric. Let $0 \neq w \in HAR^1(M)$ be a harmonic 1-form. As in Phillips-Sarnak [ ] or Sarnak [ ] one may form a 1-parameter subgroup of characters $\chi_{\theta w}$, $\theta \in \mathbb{R}$, of $\Pi_1(M)$. Corresponding to this family we have a family of selfadjoint operators $\Delta_q(\chi_{\theta w})$ on $\Lambda^q(M)$ - the exterior q-forms. According to Kato [ ] we can choose eigenvalues $0 \leq \lambda_0(\theta) \leq \lambda_1(\theta) \ldots$ and eigenvectors $u_0(\theta), u_1(\theta), \ldots$, varying analytically in θ. Here if $\lambda_0(0) = 0$ then clearly $\left.\frac{d\lambda_0}{d\theta}\right|_{\theta=0} = 0$ (since $\lambda_0(\theta) \geq 0$) and also $u_0 = u_0(0) \in HAR^q(M)$. The following formula for the second derivative of λ_0 at $\theta = 0$ generalizes the one in Phillips-Sarnak [P-S] and is easily verified

$$(3.8) \qquad \left.\frac{d^2\lambda_0}{d\theta^2}\right|_{\theta=0} = \|P_{q+1}(w \wedge u_0)\|_2^2 + \|P_{q-1}(*(w \wedge *u_0))\|_2^2$$

where P_q is the orthogonal projector of $\Lambda^q(M) \to HAR^q(M)$.

Applying this to $q = 1$ one sees that for at least one of the elements of $HAR^1(M)$

$$(3.9) \qquad \left.\frac{d^2\lambda_0}{d\theta^2}\right|_{\theta=0} > 0$$

since for $w = w_o$

$$\left.\frac{d^2\lambda}{d\theta^2}\right|_{\theta=0} = \left(\int_M w_o \wedge \overline{*w_o}\right)^2 > 0 .$$

(3.9) asserts that at least one $\lambda_o(\theta)$ for which $\lambda_o(0) = 0$ is not $\equiv 0$. Hence $\ell_1(M) \leq \beta_1(M) - 1$.

Another proof of (1.14) was pointed out to me by Deligne. Using module theory and a calculation with Laurent polynomials (see Fried and Dyer [D-F] for such a set up) one can show that for ℓ even

$$\beta_q(\chi) - \beta_{q+1}(\chi) + \ldots + \beta_{q+\ell}(\chi)$$

is lower semi-continuous in χ, that is it can only jump down as χ is deformed. Since $\beta_{-1}(\chi) \equiv 0$ and $\beta_o(\chi)$ jumps down by 1 as χ moves away from $\chi = 1$ we see from considering

$$\beta_{-1}(\chi) - \beta_o(\chi) + \beta_1(\chi)$$

that $\beta_1(\chi)$ must also jump down by at least 1 as χ moves from $\chi \equiv 1$. This clearly implies $\ell_1(M) \leq \beta_1(M) - 1$.

Acknowledgements.

I would like to thank the many mathematicians with whom I discussed various aspects of this work, especially E. Bombieri, P. Deligne, H. Iwaniec and B. Randol.

References.

[A] M. Atiyah, "Elliptic operators, discrete groups and von-Neumann algebras", Asterisque 32-33 (1976) 43-72.

[D-W] de George and N. Wallach, "Limit formulas for multiplicities in $L^2(\Gamma\backslash G)$", Annal. of Math. 107 (1978) 133-150.

[D 1] H. Donnelly, "On the spectrum of towers", Proc. A.M.S. Vol.87, No.2, 1983.

[D 2] H. Donnelly, "On L^2-Betti numbers for abelian groups", Canadian Math. Bull, Vol.24(1) 1981.

[D-F] W. Dyer and D. Fried, "Homology of free abelian covers", I and II Bull. London Math. Soc. 19 (1987) 350-352.

[H-W] G. Hardy and E. Wright, "An introduction to the theory of numbers", Claredon Press 1978, (5th edition).

[J] V. Jarnik, "Ueber die Gitterpunkte auf konvexen Kurven", Math. Zeit 24 (1925) 500-518.

[K] T. Kato, "Perturbation theory of linear operators", Springer-New York 1966.

[L 1] S. Lang, "Algebra", Addison Wesley.

[L 2] S. Lang, "Division points on curves", Anali de Math. pura et applicata (IV) LXX (1965) 229-234.

[L 3] S. Lang, "Fundamentals of Diophantine Geometry", Springer Verlag 1983.

[L I] P. Liardet, "Sur une conjecture de Serge Lang", C.R. Acad. Sci. Paris 279 (1974) 435-437.

[L E] C. G. Lekkerkerker, "Geometry of numbers", North Holland 1969.

[P-S] R. Phillips and P. Sarnak, "Geodesics in homology classes", Duke Math. Jnl. 55 (1988) 287-297.

[R-S] D. Ray and I. Singer, "R-torsion and the Laplacian ...", Adv. Math. 7 (1975) 145-210.

[S 1] P. Sarnak, "Special values of Selberg zeta function", in Vol. for Selberg's 70th birthday 1987.

[S 2] P. Sarnak, "On cusp forms II", preprint 1988.

[S W] H. P. F. Swinnerton-Dyer, "The number of lattice points on a convex curve", Jnl. of Number Theory 6, 128-135 (1974).

[W] Y. Wang, "On the least primitive root of a prime", Acta Math. Sinica 10, 1961, 1-14.

[K A] Kashdan, D., Functional Analysis and its Applications , 1967.

SECOND VERSION (ANU TECHNICAL REPORT 1988)
(FINAL VERSION APPEARS IN THE ISRAEL JNL OF MATHEMATICS, JOINT WITH S. ADAMS)

is onto for each integer $N \geq 1$. The congruence groups $\Gamma(N)$ are then defined by

$$\Gamma(N) = \ker(R_N \circ \phi). \tag{1.3}$$

Clearly $\Gamma/\Gamma(N) \simeq H(\mathbf{Z}/N\mathbf{Z})$ and $K(N) = \tilde{K}/\Gamma(N)$ is an $H(\mathbf{Z}/N\mathbf{Z})$ Galois covering of $K(1)$.

The two most interesting examples of congruence groups are the cases

(i) The map ϕ in (1.1) is an isomorphism in which case $\Gamma(N)$ is the familiar principal congruence subgroup of $H(\mathbf{Z})$ of level N.

(ii) The group H is Abelian and hence the homomorphism ϕ factors through $H_1(K, \mathbf{Z}) \simeq \Gamma/[\Gamma, \Gamma]$. In this case $H(\mathbf{Z}) = \mathbf{Z}^r$ for some $r \geq 0$. The most interesting case is that of r being $\beta_1(\Gamma)$. Some concrete example of (ii) are the following

(a) Fermat Curves: The Fermat curves $F(N)$ may be uniformized as $\Phi(N) \,|\, \mathbf{H}$, where

$$\Phi(1) = \Gamma(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2 \right\}$$

$$\Phi(N) = \ker(R_N \circ \phi),$$

where $\phi : \Gamma(2) \to \mathbf{Z}^2$ is the projection on homology. $R_N : \mathbf{Z}^2 \to (\mathbf{Z}/N\mathbf{Z})^2$ is as above, reduction mod N and $\mathbf{H}$ is the upper half plane. For more details see Lang [L1]. Actually to be more precise $F(N)$ is the compactification (branched) of $\Phi(N) \,|\, \mathbf{H}$. Note that while $\Phi(N)$ is a congruence group in our sense it is not so according to the usual definition [S].

(b) Links in S^3: Let $L \subset S^3$ be a μ–component link; that is disjoint union of μ circles. Let $\Gamma = \pi_1(S^3 \,|\, L)$. It is well known and easily seen that $H_1(S^3 \,|\, L) \simeq \mathbf{Z}^\mu$. Let $\phi : \Gamma \to \mathbf{Z}^\mu$ be the Abelianizer and R_N as above. We get in this way for each N a uniquely defined $(\mathbf{Z}/N\mathbf{Z})^\mu$ covering $M(N)$ of $S^3 \,|\, L$. When L is a knot (i.e., $\mu = 1$) these are the well studied cyclic covers [F–1].

(c) Hirzebruch Surfaces [Hh]: Let $\ell_1, \ldots, \ell_r$ be an arrangement of lines in $\mathbf{P}^2(\mathbf{R}) \subset \mathbf{P}^2(\mathbf{C})$. The Hirzebuch surface $E(N)$ for $N \geq 1$ is the $(\mathbf{Z}/N\mathbf{Z})^{r-1}$ branched cover of $\mathbf{P}^2(\mathbf{C})$ branched over $\ell_1, \ldots, \ell_r$, see [Ha] for a discussion. Hirzebruch computed the characteristic numbers of $E(N)$. Their Betti numbers for certain $\ell_1, \ldots, \ell_r$ and N were computed by Ishida [I] and Hironaka [Ha].

Before turning to our results we consider a related problem. Let G be a semisimple real, complex, or p–adic group. Let $\Gamma \leq G$ be a lattice. The right regular representation of G on $L^2(\Gamma\backslash G)$ decomposes into $\oplus_{i=1}^{\infty} V_i$ where V_i are irreducible unitary representations of G. We

denote by $\hat{G}$ the set of equivalence classes of such representations. One of the fundamental problems in automorphic form theory is to determine $m(\pi, \Gamma)$, the multiplicity with which some $\pi \in \hat{\Gamma}$ appears in the above decomposition. It is known [B–W] that for certain π's this multiplicity corresponds to cohomology of Γ. We call such π's cohomological. Now let $\Gamma(N) < \Gamma$ be a congruence family in the sense defined above. Our aim is to study $m(\pi, \Gamma(N))$ as a function of N.

Note that the group $H(\mathbf{Z}/N\mathbf{Z}) \times G$ acts unitarily on $L^2(\Gamma(N) \,|\, G)$ by

$$(h, g)\, f(x) \to f(h^{-1} x\, g)\,. \tag{1.4}$$

Decomposing this into irreducibles we get multiplicities $m(\rho \otimes \pi, \Gamma(N))$ with $\rho \in H(\widehat{\mathbf{Z}/N\,\mathbf{Z}})$. For $\nu \geq 1$ and integer, we define the ν–dimensional part of $m(\pi, \Gamma(N))$ to be

$$^{(\nu)}m(\pi, \Gamma(N)) = \sum_{\substack{\dim \rho = \nu \\ \rho \in H(\widehat{\mathbf{Z}/N\,\mathbf{Z}})}} m(\rho, \Gamma(N))\,.$$

We can recover $m(\pi, \Gamma(N))$ by

$$m(\pi, \Gamma(N)) = \sum_{\nu=1}^{\infty} {}^{(\nu)}m\,(\pi, \Gamma(N))$$

(the sum of course is finite).

Returning to the simplicial complex setting, we have $H(\mathbf{Z}/N\mathbf{Z})$ acting as Galois group of $K(N)/K(1)$ and hence $H(\mathbf{Z}/N\mathbf{Z})$ acts on the cohomology groups $H^k(K(N))$. Decomposing this action into irreducible gives

$$H^k(K(N)) = \bigoplus_i W_i\,.$$

We define the ν–dimensional part of the kth Betti number $^{(\nu)}\beta\,(k, K(N))$ to be

$$^{(\nu)}\beta\,(k, \Gamma(N)) = \dim \left(\sum_{\dim W_i = \nu} W_i \right)\,. \tag{1.5}$$

We observe that if H is Abelian then $^{(1)}\beta\,(k, \Gamma(N)) = \beta(k, \Gamma(N))$ and $^{(1)}m\,(\pi, \Gamma(N)) = m(\pi, \Gamma)$ since all irreducibles of H are 1–dimensional.

Definition 1.1. A sequence $a(n)$, $n \geq 1$, is polynomial periodic if there are periodic $b_j(n)$, $j = 1, \ldots, q$ such that $a(n) = \sum_{j=0}^{q} b_j(n)\, n^j$.

We can now state the periodicity theorem

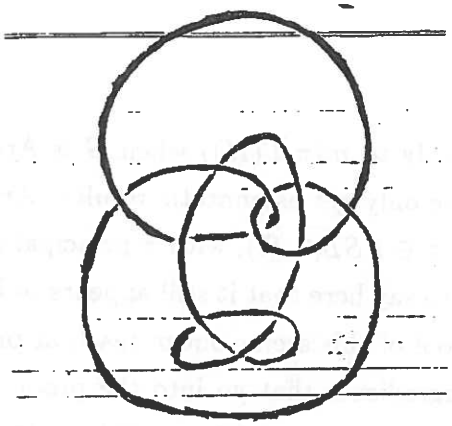


Fig 1.5

Theorem 1.2. *Assume that H is either unipotent or semisimple then*

(i) If $\Gamma = \pi_1(K)$ is as above and $\Gamma(N)$, $N \geq 1$, a congruence family, then ${}^{(\nu)}\beta(k, \Gamma(N))$ is polynomial periodic in N.

(ii) If G is Archimedian and π is cohomological or if G is p-adic and π is arbitrary then ${}^{(\nu)}m(\pi, \Gamma(N))$ is polynomial periodic in N.

Remark 1.3. Since the general H is roughly a semidirect product of a unipotent part with a semisimple part (recall that H has strong approximation) we expect that the Theorem is valid for the general H.

Corollary 1.4. *Let L be a μ-compact link in S^3 and set $M(N)$ to be the $(\mathbf{Z}/N\mathbf{Z})^\mu$ cover of S^3 branched along L then $\beta(1, M(N))$ is polynomial periodic.*

This Corollary in the case of knots is known and due to Goeritz [G] and Zariski [Z]. In fact, for knots one can show that the sequence is periodic (i.e., $q = 0$ in Definition 1.1). In general this is not so as the following example shows: The link L in figure 1.5 has two components. We can write down $\beta(1, M^u(N))$ compactly for all N by use of the generating function $\sum_{N=1}^{\infty} \beta(N)/N^s$. In Section 4 we show[1]

$$\sum_{N=1}^{\infty} \frac{\beta(1, M^u(N))}{N^s} = 2\left(1 + 2^{-s} + 6^{-s}\right)\zeta(s) + 2 \cdot 6^{-s}\zeta(s-1), \tag{1.6}$$

where $\zeta(s) = \sum_{N=1}^{\infty} N^{-s}$. Here $M^u(N)$ in the unbranched $(\mathbf{Z}/N\,\mathbf{Z})^2$ covering of $S^3 \mid L$.

Corollary 1.6. *Let $E^u(N)$ be the unbranched Hirzebruch surfaces over a fixed configuration of lines then the irregularities $\beta(1, E^u(N))$ are polynomial periodic in N.*

In Hironaka [Ha] a method for computing the difference between the irregularity of the Branched and Unbranched surface is developed. It would be interesting to determine if polynomial periodicity holds for the branched covers $E(N)$.

[1] This form gives more information than polynomial periodicity and it holds in general.

Our Theorem does not apply to $m(\pi, \Gamma(N))$ when G is Archimedean and π is not cohomological. In these cases we only get asymptotic results. An analysis of $m(\pi, \Phi(N))$ for $\Phi(N)$ the Fermat groups and $\pi \in PS\widehat{L(2, \mathbf{R})}$, with π principal or complimentary series will be given elsewhere. Suffice it to say here that it still appears to be the case that $m(\pi, \Phi(N))$ is periodic in N, though a proof of this seems out of reach at present.

There are a number of ingredients that go into the proof of Theorem 1.2. In Section 2 we discuss the variety of representations of Γ into $GL(\nu, \mathbf{C})$ and the important algebraic subsets connected with the cohomology problem. In Section 3 the problem of counting torsion points on algebraic subsets is studied. Specifically let T be an r–dimensional real torus and let $V \subset T$ be an algebraic subset (i.e., the zero set of a trigonometric polynomial or intersection of such sets). Denote by $\mathrm{tor}\,(T)$ the set of torsion points (i.e., elements of finite order in T). The following was conjectured by Lang [L2];

Proposition 1.7. *There are a finite number of rational planes $\pi_1, \ldots, \pi_\ell$ (a rational plane is a closed connected subgroup of T or a translate thereof by a torsion point) contained in V such that*

$$\mathrm{tor}\,(T) \cap V = \mathrm{tor}\,(T) \bigcap \left(\bigcup_{j=1}^{\ell} \pi_j \right).$$

In Section 3 an elementary and algorithmic proof of this Proposition is given. Given V it produces the planes $\pi_1, \ldots, \pi_\ell$ which is crucial for the purposes of computing the periodicities and polynomials. Another proof of this conjecture (as has been pointed out to me) apparently is contained in the work of Laurant [LT]. The importance of Proposition 1.7 lies in the fact that as far as torsion goes we may linearize V, that is replace it by planes. It is this that is responsible for the polynomial periodicity. In Section 4 we complete the proof of the Theorem and its Corollary.

2. Representation varieties and cohomology

Let K be a finite simplicial complex $\tilde{K}$ and $\Gamma = \pi_1(K)$ as in Section 1. If R is a finite dimensional unitary representation of Γ in $GL(V)$ then the R–twisted cochain complex $C(\tilde{K}, R)$ is defined by

$$C^q(\tilde{K}, R) = \{F : C_q(\tilde{K}) \to V\,,\ F \text{ is linear and} \tag{2.1}$$
$$F(\gamma\,\sigma) = R(\gamma)\,F(\sigma) \text{ for } \gamma \in \Gamma\}$$

We have a coboundary operator

$$\delta^{(q)} : C^q(\tilde{K}, R) \to C^{q+1}(\tilde{K}, R)$$

given by

$$(\delta^q F)(\sigma) = F(\partial\sigma)\,. \tag{2.2}$$

The cohomology groups $H^*(\Gamma, R)$ are defined in the usual way (here and elsewhere $C_q(\tilde{K})$ is to be taken with complex coefficients). Our first problem is to determine the behavior of $\beta^{(q)}(\Gamma, R) = \dim H^{(q)}(\Gamma, R)$ as a function of R. While the variety of all (up to equivalence) representations of Γ in $GL(\nu, \mathbf{C})$ can be quite complicated, the set of those which have finite image (which are all that we need consider) is much more tractable. In fact as is shown in Lubotzky–Magid [L–M], it follows from a theorem of Jordan, see [C–R], that all such R's which are irrducible and of dimension ν factor through a fixed quotient Δ of Γ. Moreover Δ is Abelian by finite. Rudnick [R] gives a description of the variety $V(\Delta, \nu)$ of all irreducible representations (up to equivalence) of such a Δ. In what follows we will denote by $T(B)$ the torus of 1–dimensional unitary characters of a group B. Rudnick shows that there are finite index subgroups $H_1, \ldots, H_L$ of Δ such that

$$V(\Delta, \nu) \subseteq \bigcup_{j=1}^{L} \left(\bigcup_{\chi \in T(H_j)} \mathrm{Ind}_{H_j}^{\Delta}(\chi) \right)\,. \tag{2.3}$$

We are thus led to examine the functions

$$F_j(\chi) = \beta^{(k)}(\Gamma, \mathrm{Ind}_{H_j}^{\Delta}(\chi))\,,\ \chi \in T(H_j)\,. \tag{2.4}$$

To do so we will use Hodge theory in the form of the finite combinatorial Laplacian. For our purposes this has the advantage of dealing with the automorphic form problem in the same way.

As in Ray–Singer [R–S] choose a preferred basis $F_{i,j}^{(q)} = \widetilde{\sigma_i^{(q)} \otimes e_j}$ of $C^q(\tilde{K}, R)$ as follows: Let $e_1, \ldots, e_m$ be an orthonormal basis of V and let $\sigma_1^{(q)}, \ldots, \sigma_{\nu_q}^{(q)}$ be the set of q–simplices of K (which we think of as embedded in $\tilde{K}$). For $i = 1, \ldots, \nu_q$, $j = 1, \ldots, m$

$$\widetilde{\sigma_i^{(q)} \otimes e_j}\,(\gamma\,\sigma_\ell^{(q)}) = \begin{cases} 0 & \text{if } i \neq \ell \\ R(\gamma)\,e_j & \text{if } i = \ell. \end{cases} \tag{2.5}$$

Then δ has a matrix representation relative to the bases $F_{i,j}^{(q)}$ and $F_{i,j}^{(q+1)}$. Using these bases we may define δ^* and also the combinatorial Laplacian $\Delta_{(c)}^q : C^q(\tilde{K}, R) \to C^q(\tilde{K}, R)$ by

$$\Delta_{(c)}^q = (\delta^{(q+1)})^*\,\delta^q + \delta^{q-1}(\delta^q)^*\,. \tag{2.6}$$

As with the usual Hodge theory

$$\dim\ker \Delta^q_{(c)} = \beta^{(q)}(\Gamma, R)\,. \tag{2.7}$$

Returning to our R's of the form (2.4), let $\psi : \Gamma \to \Delta$ be the projection and denote by $R(\chi)$ the representation of Γ given by

$$R(\chi) = \mathrm{Ind}_H^{\Delta}(\chi)_0\,\psi\,. \tag{2.8}$$

Let $H\,\delta_1, H\,\delta_2, \ldots, H\,\delta_\mu$ be coset representatives of H in Δ. An orthonormal basis of $V = V(\mathrm{Ind}_H^{\Delta}(\chi))$ can be chosen in the form $e_1, \ldots, e_\mu$ when

$$e_j(h\,\delta_r) = \begin{cases} \chi(h) & \text{if } j = t \\ 0 & \text{otherwise.} \end{cases} \tag{2.9}$$

Proposition 2.1. *The matrix of $\Delta^q_{(c)}(R(\chi))$ relative to the basis $\widetilde{\sigma_i^{(q)}} \otimes e_j$ of $C^q(\tilde{K}, R(\chi))$ has entries which are trigonometric polynomials in χ.*

The proof is a straightforward verification. We note for later that Proposition 2.1 holds equally well with $R(\chi)$ replaced by

$$\tilde{R}(\chi) = R_0 \otimes \chi\,, \tag{2.10}$$

where R_0 is a ν–dimensional representation of Γ. For $\lambda \in \mathbf{C}$ and $\chi \in T(H)$ let $p(\lambda, \chi)$ denote the characteristic polynomial

$$p(\lambda, \chi) = \det(\lambda - \Delta^q_{(c)}(R(\chi)))\,.$$

Define the algebraic subsets of $T(H)$, $V_0 \supset V_1 \supset V_2 \ldots$ by

$$\begin{aligned} V_1 &= \{\chi \mid p(0, \chi) = 0\} \\ V_j &= \left\{\chi \;\middle|\; \frac{\partial^{j-1} p}{\partial \lambda^{j-1}}(0, \chi) = 0\right\} \cap V_{j-1} \end{aligned} \tag{2.12}$$

In view of Proposition 2.1 the V_j's are indeed algebraic. Note that

$$V_j = \{\chi \mid \beta^{(q)}(\Gamma, R(\chi)) \geq j\}\,. \tag{2.13}$$

Hence

$$\beta^{(q)}(\Gamma, R(\chi)) = \sum_{j \geq 1} \varepsilon(\chi, V_j)\,, \qquad \text{where } \varepsilon(\chi, V) = \begin{cases} 1 & \text{if } \chi \in V \\ 0 & \text{if } \chi \notin V \end{cases} \tag{2.14}$$

The last sum is finite since $V_j = \emptyset$ for large j.

Now recall that only the $R(\chi)$'s which are of finite image play a role in our analysis. For these clearly $\chi \in T(H)$ must be a torsion point, that is we are interested in $\beta^{(q)}(\Gamma, R(\chi))$ for $\chi \in \text{tor}\,(T(H))$. Applying the linearization Proposition 1.7 we conclude that for each V_j there are planes $\pi_1^{(j)}, \ldots, \pi_{\ell_j}^{(j)}$ and integers $m_1^{(j)}, \ldots, m_{\ell_j}^{(j)}$ (which come from inclusion–exclusion) such that for $\chi \in \text{tor}\,(T(H))$

$$\varepsilon(\chi, V_j) = \sum_{\mu=1}^{\ell_j} m_\mu^{(j)}\, \varepsilon(\chi, \pi_m^{(j)})\,. \tag{2.15}$$

Combining this with (2.14) we obtain our basic formula for $F_j(\chi)$ in (2.4) (we drop the index j).

Proposition 2.2. *There are planes $\pi_1, \ldots, \pi_L$ and integers $m_1, \ldots, m_L$ such that for $\chi \in$ tor $(T(H))$*

$$\beta^{(q)}(\Gamma, R(\chi)) = \sum_{\mu=1}^{L} m_\mu\, \varepsilon(\chi, \pi_\mu)\,.$$

Thus far we have examined only the cohomological case, $\Gamma = \pi_1(K)$. To deal with part (ii) of Theorem 1.2 when Γ is a lattice in a p–adic group G, one proceeds along similar lines. Let $m(\pi, \Gamma, R(\chi))$ have the obvious meaning, where $\chi \in T(H)$ as above. Now say G is rank 1 (actually it is only for rank 1 that the variety of representation of Γ into $GL(\nu, \mathbf{C})$ is not zero dimensional) then by the duality theorem [G–G–P], $m(\pi, \Gamma, R(\chi))$ may be realized as the dimension of a certain eigenvalue of a vector valued Laplacian over the finite graph $\Gamma\backslash G/U$, U being a maximal compact subgroup of G. Hence the setup is identical to what we have and the only change needed is that in (2.6) we are interested in the general eigenvalue of Δ rather than just $\lambda = 0$. Of course there was nothing special about $\lambda = 0$ in what followed. One proceeds to derive an expression for $m(\pi, \Gamma, R(\chi))$ where $\chi \in \text{tor}\,(T(H))$, just like the one in Proposition 2.2.

We remark that in the Archimedean case $\Gamma\backslash G/U$ is a compact manifold but unfortunately $\det(\Delta(R(\chi)))$ is no longer a trigonometric polynomial in χ. One can show that it is real analytic in χ but we will not pursue this here.

3. Torsion points on varieties and linearization

We turn to the proof of Proposition 1.7. The approach below is simpler than our original and was suggested by Paul Cohen.

Lemma 3.1. *Let $\alpha_1, \ldots, \alpha_k$ be non zero complex numbers then there is a number $M = M(\alpha_1, \ldots, \alpha_k)$ such that any solution in roots of unity $\varepsilon_1, \ldots, \varepsilon_R$ of*

$$\sum_{j=1}^{R} \alpha_j \varepsilon_j = 0 \tag{3.1}$$

satisfies

$$(\varepsilon_j \varepsilon_k^{-1})^{\nu} = 1 \tag{3.1}'$$

for some $j \neq k$ and some $1 \leq \nu \leq M$.

Proof: We begin by assuming that $\alpha_1, \ldots, \alpha_R \in \mathbf{Q}$ in which case we show M may be chosen to be $(R+1)^{R+1}$. Let $\varepsilon_1, \ldots, \varepsilon_R$ be a solution of (3.1) and assume the conclusion of (3.1)' fails. Let n be the l.c.m. of the orders of $\varepsilon_1, \ldots, \varepsilon_R$. If the factorization of n is $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ then we may write

$$\varepsilon_j = (\zeta_{p_1^{e_1}})^{\nu_j^{(1)}} (\zeta_{p_2^{e_2}})^{\nu_j^{(2)}} \ldots (\zeta_{p_k^{e_k}})^{\nu_j^{(k)}}, \tag{3.2}$$

where $\zeta_m = e(1/m) = \exp(2\pi i/m)$. Now if some p_j, say p_1 is larger than $R+1$ then we proceed as follows:

There is some ε_j for which $(\nu_j^{(1)}, p_1) = 1$. We may write (3.1) as

$$\sum_{j=1}^{R} (\alpha_j \eta_j \zeta_{p_1^{e_1-1}}^{\lambda_j}) \zeta_{p_1^{e_1}}^{\nu_j} = 0, \tag{3.3}$$

where $\eta_j \zeta_{p_1^{e_1-1}}^{\lambda_j} \zeta_{p_1^{e_1}}^{\nu_j} = \varepsilon_j$, $0 \leq \nu_j \leq p_1 - 1$, η_j is a $p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$ root of 1 and $(\nu_1, p_1) = 1$. Thus (3.3) gives an equation for $\zeta_{p_1^{e_1}}$ over the field $K = \mathbf{Q}(\zeta_{p_1^{e_1-1}}, \zeta_{p_2^{e_2}}, \ldots, \zeta_{p_k^{e_k}})$ of degree at most $p_1 - 1$. The extension $K(\zeta_{p_1^{e_1}})$ over K has degree $p_1 - 1$ and since $R < p_1 - 1$ (3.3) is impossible (since then (3.3) is not the cyclotomic equation) unless the equation trivializes. In this case one can proceed inductively since the power e_1 has been reduced and the side conditions of the Lemma persist.

We may therefore assume that $p_j \leq R+1$ for each j. We write (3.1) as

$$\sum_{j=1}^{R} \alpha_j \, e\left(\frac{m_1^{(j)}}{p_1^{e_1}} + \frac{m_2^{(j)}}{p_2^{e_2}} + \ldots + \frac{m_k^{(j)}}{p_k^{e_k}}\right) = 0, \tag{3.4}$$

where now

$$\varepsilon_j = e\left(\frac{m_1^{(j)}}{p_1^{e_1}} + \ldots + \frac{m_k^{(j)}}{p_k^{e_k}}\right).$$

For $r = (r_1, r_2, \ldots, r_k)$ with $p_j \nmid r_j$ we obtain from (4.2) and the Galois action of $\mathbf{Q}(\zeta_n)/\mathbf{Q}$

$$\sum_{j=1}^{R} \alpha_j \, e\left(\frac{r_1 m_1^{(j)}}{p_1^{e_1}} + \ldots + \frac{r_k m_k^{(j)}}{p_k^{e_k}}\right) = 0 .$$

Multiplying this equation by $\overline{e\left(\frac{r_1 m_1^{(1)}}{p_1^{e_1}} + \ldots + \frac{r_k m_k^{(1)}}{p_k^{e_k}}\right)}$ and summing over $r_j \bmod p_j^{e_j}$, $p_j \nmid r_j$, we get

$$0 = \alpha_1 \, \phi(n) \pm \sum_{j=2}^{R} \alpha_j \sum_{r_j \bmod p_j^{f_j}} e\left(\frac{r_1 (m_1^{(j)} - m_1^{(1)})}{p_1^{e_1}} + \ldots + \frac{r_k (m_k^{(1)} - m_k^{(1)})}{p_k^{e_k}}\right) , \tag{3.5}$$

where $f_j = e_j$ or $e_j - 1$. If for a fixed j in the above type of sum $m_\nu^{(j)} - m_\nu^{(1)}$ are all divisible by $p_\nu^{f_\nu}$ then $m^{(j)} \equiv m^{(1)} \bmod \left(\frac{n}{p_1 p_2 \ldots p_k}\right)$ and hence

$$(\epsilon_1 \epsilon_j^{-1})^{p_1 p_2 \ldots p_k} = 1 .$$

This is contrary to our assumption since $p_1 p_2 \ldots p_k < (R+1)^{R+1}$. Hence for each j at least one of $m_\nu^{(j)} - m_\nu^{(1)}$ is not divisible by $p_\nu^{f_\nu}$. It follows that all the series in (3.5) vanish and hence $\alpha_1 = 0$. This completes the proof for the case of most interest to us viz. $\alpha_j \in \mathbf{Q}$. In general one argues in a similar case with $\mathbf{Q}$ replaced by the finitely generated field $K = \mathbf{Q}(\alpha_1, \ldots, \alpha_r)$ and the Galois group of $\mathbf{Q}(\zeta_n)$ replaced by that of $K\,\mathbf{Q}(\zeta_n)$ over K. We leave the details to the reader.

We proceed now with the proof of Proposition 1.7. The proof is by induction on the dimension of the torus T. We are allowing here a torus to be of the form $T = (\mathbf{R}/\mathbf{Z})^k \times A$, where A is a finite Abelian group. In such a case T is of dimension k and the algebraic sets are algebraic sets at each connected component of T. When $\dim T = 1$ the result is clear since in this case a connected component of T is either all of the set V, or V meets the component in a finite set. In the general case if $\dim T = r$ and V is given by equations

$$p_1(t) = p_2(t) = \ldots = p_m(t) = 0$$

on a connected component of T, then either these equations are all redundant and V contains this connected component which is then one of the π's, or say $p_1(t)$ is not trivially true. Say

$$p_1(t) = \sum_{\lambda \in F} a_\lambda \, \lambda(t) , \tag{3.6}$$

where F is a finite subset of the dual group T^*. The sets

$$\Pi_{\lambda,\mu,\nu} = \{t \mid (\lambda \, \mu^{-1})^\nu(t) = 1\} \tag{3.7}$$

for $\lambda \neq \mu$, $\lambda, \mu \in F$, and $1 \leq \nu \leq M(a_\lambda)$, where M is the constant from Lemma 3.1, are all finite unions of rational planes of dimension $r-1$. Hence since the restriction of an algebraic set to a plane is algebraic we conclude by induction that the torsion points of $T \cap V$ contained in the union of the finite set of $\Pi_{\lambda,\mu,\nu}$'s are all on a finite number of rational planes in V. On the other hand Lemma 3.1 asserts that there are no torsion points of $T \cap V$ outside of this union. This completes the proof of Proposition 1.7.

We note that the above proof is effective and produces the planes inductively. An example of this procedure is carried out in the next Section.

4. Proof of the Theorem

We now complete the proof of Theorem 1.2 part (i). Part (ii) is proved similarly. From our setup $H(\mathbf{Z}/N\,\mathbf{Z})$ is the Galois group of the covering $\tilde{K}/\Gamma(N)$ over $\tilde{K}/\Gamma(1)$. Hence we may decompose $C^q(\tilde{K}/\Gamma(N))$ into invariant subspaces according to the irreducible representations of $H(\mathbf{Z}/N\,\mathbf{Z})$. Since the action of $H(\mathbf{Z}/N\,\mathbf{Z})$ on fibers of the covering is simple and transitive and acts on these by the regular representation it follows that

$$\beta(q, \Gamma(N)) = \sum_{R \in \widehat{H(\mathbf{Z}/N\,\mathbf{Z})}} d(R)\, \beta(q, \Gamma, R)\,, \tag{4.1}$$

where $d(R) = \dim R$. Hence

$$^{(\nu)}\beta\,(q, \Gamma(N)) = \nu \sum_{\substack{R \in H(\mathbf{Z}/N\,\mathbf{Z}) \\ \dim R = \nu}} \beta(q, \Gamma, R)\,. \tag{4.2}$$

These R's are irreducible ν–dimensional and of course finite representations of Γ–this explains the assumption made in Section 2. To use the formula for $\beta(q, \Gamma, R(\chi))$ developed in Proposition 2.2 we need to know which χ's come up in (4.2).

Assume H is unipotent, then $H(\mathbf{Z})$ is a finitely generated nilpotent (discrete) group. In this case, the representation variety $V(\Delta, \nu)$ in (2.3) takes an even simpler form, see Lubotzky–Magid [L–M]

$$V(\Delta, \nu) = \bigcup_{j=1}^{L} \bigcup_{\chi \in T(H(\mathbf{Z}))} R_j \otimes \chi\,, \tag{4.3}$$

where R_j is an irreducible (finite) representation of $H(\mathbf{Z})$ of dimension ν. Moreover, the representation in different classes $R_j \otimes T(H(\mathbf{Z}))$ and $R_k \otimes T(H(\mathbf{Z}))$ for $k \neq j$ are inequivalent.

It is possible that $R_j \otimes \chi' \simeq R_j \otimes \chi$ for some $\chi \neq \chi'$ and in this case $\{\chi : R_j \otimes \chi \simeq R_j\}$ is a finite subgroup of $T(H(\mathbf{Z}))$. For simplicity we assume this group is $\{1\}$–the modifications needed to deal with the general case dividing by this finite group are straightforward.

In order to apply (4.2) we need to identify the subset of $V(\Delta, \nu)$ above which correspond to the irreducible representations of $H(\mathbf{Z}/N\mathbf{Z})$ of dimension ν. To begin with we do this for $\nu = 1$, i.e., for the subgroup $T(H(\mathbf{Z}/N\mathbf{Z}))$ of $T(H(\mathbf{Z}))$. Now the map

$$H'(\mathbf{Z}) \to H'(\mathbf{Z}/N\,\mathbf{Z})$$

is onto ($'$ denotes the commutator subgroup), as is

$$\mathbf{Z}^r \simeq H(\mathbf{Z})/H'(\mathbf{Z}) \to H(\mathbf{Z}/N\,\mathbf{Z})/H'(\mathbf{Z}/N\,\mathbf{Z}) \simeq (\mathbf{Z}/N\,\mathbf{Z})^r\,.$$

Correspondingly,

$$T(H(\mathbf{Z}/N\,\mathbf{Z})) = \{\chi \in T(H(\mathbf{Z})) \mid \chi^n = 1\}\,. \tag{4.4}$$

Let $H(N)$ be the congruence subgroup defined by

$$\{1\} \to H(N) \to H(\mathbf{Z}) \to H(\mathbf{Z}/N\,\mathbf{Z}) \to \{1\}\,.$$

Lemma 4.1. *Let R be a finite dimensional representation of $H(\mathbf{Z})$ then $\{N \mid R|_{H(N)} = 1\}$ is of the form $\{\lambda N_0 \mid \lambda \in \mathbf{N}\}$ for some N_0.*

We call N_0 the conductor of R (if the above set is empty then N_0 is defined to be ∞.

Proof: It suffices to prove that if $R|_{H(N)} = 1$ and $R|_{H(M)} = 1$ then $R|_{H(N,M)} = 1$. Inductively (on the length of the central series) this is so for $H'(\mathbf{Z})$. Also $H(\mathbf{Z})/H'(\mathbf{Z}) \simeq \mathbf{Z}^r$ with $\mathbf{Z}$ structure and since $R|_{N\mathbf{Z}^r} = 1$ and $R|_{M\mathbf{Z}^r} = 1$ it follows that $R|_{(N,M)\mathbf{Z}^r} = 1$ and the result follows.

Let R_j be one of the representations in (4.3). We can assume by replacing R_j by $R_j \otimes \chi$ for suitable χ that the conductor of R_j is minimal among the conductors of $R_j \otimes \chi$, $\chi \in T(H(\mathbf{Z}))$. Let $N_j = \mathrm{cond}\,(R_j)$. With this choice we have

Lemma 4.2. *$N_j \mid \mathrm{cond}\,(R_j \otimes \chi)$ for any $\chi \in \mathrm{tor}\,(T(H(\mathbf{Z})))$.*

Proof: If $p^e \mid N_j$ and $p^e \nmid \mathrm{cond}\,(R_j \otimes \chi)$ then write $\chi = \chi_p \otimes \chi_m$ where $(m, p) = 1$ and where χ_p has conductor a power of p and χ_m conductor prime to p. One checks that $\mathrm{cond}\,(R_j \otimes \chi_p) \leq N_j/p$ since $p^e \nmid \mathrm{cond}\,(R_j \otimes \chi)$. But this contradicts our choice of R_j.

It follows that if $\mathrm{cond}\,(R_j \otimes \chi) | N$ then $N_j | N$. Let ${}^{(\nu)}H(\mathbf{Z}/N\,\mathbf{Z})^\wedge$ denote the set irreducible representations of $H(\mathbf{Z}/N\,\mathbf{Z})$ in dimension ν.

Proposition 4.3. *We have the disjoint union*

$$ {}^{(\nu)}H(\mathbf{Z}/N\,\mathbf{Z})^\wedge = \bigcup_{j=1}^{L} B(N,j)\,, $$

where

$$ B(N,j) = \begin{cases} \phi & \text{if } N_j \not| N \\ \{R_j \otimes \chi \,|\, \chi^N = 1\} & \text{if } N_j | N. \end{cases} $$

Proof: This is clear from the previous Lemmas.

Returning to (4.2) and using Proposition 4.3 we have

$$ {}^{(\nu)}\beta\,(q, \Gamma(N)) = \nu \sum_{j=1}^{L} \delta(N,j) \sum_{\chi^N=1} \beta(q, R_j \otimes \chi)\,, \tag{4.5} $$

where

$$ \delta(N,j) = \begin{cases} 0 & \text{if } N_j \not| N \\ 1 & \text{if } N_j | N. \end{cases} $$

By Proposition 2.2 and Remark 2.10 we get

$$ {}^{(\nu)}\beta\,(q, \Gamma(N)) = \nu \sum_{j=1}^{L} \delta(N,j) \sum_{\mu=1}^{\ell_j} m_\mu^{(j)} \sum_{\chi^N=1} \varepsilon(\chi, \pi_\mu^{(j)}) $$

for suitable rational planes $\pi_\mu^{(j)}$ and integers m_μ^j. Now a typical π is of the form $\zeta + B$ where B is a connected closed subgroup of $T(H(\mathbf{Z}))$ of dimension r say and $\zeta \in \mathrm{tor}\,(T)$. Let M be the least integer such that $t\zeta \in B$ then the series

$$ \sum_{\chi^N=1} \varepsilon(\chi, \pi) = \begin{cases} 0 & \text{if } M \not| N, \\ N^r & \text{if } M | N. \end{cases} \tag{4.7} $$

Substituting (4.7) in (4.6) gives the desired polynomial periodicity of ${}^{(\nu)}\beta\,(q, \Gamma(N))$. It in fact gives such a polynomial periodic sequence of rather special form.

This completes the proof if H is unipotent. If H is semisimple then the above analysis gives the result (but without any of the analysis of torsion points in torii) because of the following result, a proof of which is given by M. Larsen in the Appendix.

Z. RUDNICK

Proposition 4.4. *Let H be a semisimple group over $\mathbf{Q}_p$. Let $\mathbf{Z}_p$ denote the p–adic integers. There are only finitely many irreducible representations of the compact group $H(\mathbf{Z}_p)$ in any given dimension.*

With this one finds that there are only a finite number of R's (independent of N but depending on ν) that come into play in (4.2). As a result the Theorem is easy to establish.

The Corollaries for unbranched covers follows directly from the Theorem since H in these cases is Abelian and hence we need only take $\nu = 1$ to get the complete picture. For computational purposes say with links in S^3 we relate the varieties $V_1, V_2, \ldots$ of Section 2 to Alexander ideals [F–2]. In fact let L be a μ–component link we can think of $T(\Gamma) = (S^1)^\mu$, where $\Gamma = \pi_1(S^3 \mid L)$, as sitting in $(\mathbf{C}^*)^\mu$. The following Proposition which follows easily from Fox [F–2], see also [M–M] and Libgober [Lr].

Proposition 4.5. *Let $W_1 \supset W_2 \supset W_3 \ldots$ be the zero sets in $(\mathbf{C}^*)^\mu$ of the elementary Alexander ideals $E_1, E_2, \ldots$ of the link L. Then*

$$W_j \cap T = V_j \quad \text{for } j \neq \mu$$

and $(W_\mu \cap T) \cup \{1\} = V_\mu$.

Here the V_j's are the sets defined in (2.12) for $\beta^{(1)}$ and $H(\mathbf{Z}) = \mathbf{Z}^\mu = H_1(\Gamma, \mathbf{Z})$. The point is that the Alexander ideals are easy to compute. Thus for the link L in Figure 1.5 one finds (see [F–T])

$$E_1: \qquad (t_1 - 1, t_2 - 1)\,(1 - t_1 + t_1^2)\,(1 - 2\,t_1 - t_1^2\,t_2\,(2 - t_1))$$

$$E_2: \qquad (1 - t_1 + t_1^2, (1 + t_1)\,(1 + t_2))$$

$$E_3: \qquad (1)$$

Hence using linear torus variables $t_j = e(\theta_j)$ and Proposition 4.5 we have

$$V_1 = \{(0,0)\} \cup \{1 - e(\theta_1) + e(2\,\theta_1) = 0\} \cup \{1 - 2\,e(\theta_1) - e(2\,\theta_1)\,e(\theta_2)\,(2 - e(\theta_1)) = 0\}$$

$$V_2 = \left\{(0,0), \left(\frac{1}{6}, \frac{1}{2}\right), \left(\frac{5}{6}, \frac{1}{2}\right)\right\}$$

$$V_3 = \emptyset$$

Thus V_3 and V_2 are already linear. We apply the method of Section 3 to linearize V_1 and find two 1–dimensional rational planes viz.

$$\pi_1 = \{\theta_1 = 1/6\}, \qquad \pi_2 = \{\theta_1 = 5/6\}$$

and three zero dimensional planes

$$\pi_3 = \{(0,1/2)\}, \qquad \pi_4 = \{(1/2,0)\}, \qquad \pi_5 = \{(0,0)\}\,.$$

Using this in (4.6) and (4.7), with $\nu = 1$ and $\operatorname{cond} R_0 = \operatorname{cond} 1 = 1$ one obtains (1.6) after a little calculation.

Concerning Corollary 1.4 for branched coverings one uses instead of the Alexander polynomial of L the reduced Alexander polynomial as described in Mayberry and Murasugi [M–M]. Other than that the techniques apply directly and yield Corollary 1.4.

Acknowledgements. I would like to thank A. Adem, P. Cohen, D. Fried, and A. Lubotzky for illuminating discussions on various aspects of this paper.

References

[B–W] A. Borel and N. Wallach, *Continuous cohomology, discrete groups and representations of reductive groups,* Annals of Math. Studies 94, Princeton University Press 1976.

[C–R] C. Curtis and I. Reiner, *Methods of representation theory,* Wiley, New York 1981.

[F–T] R.H. Fox and A. Torres, *Dual presentations of the group of a knot,* Annals of Math. **59** (1954), 211–218.

[F–1] R.H. Fox, *A quick trip through knot theory,* in Topology of 3 manifolds; editor FORT.

[F–2] R.H. Fox, *Free differential calculus I, II, III,* Annals of Math.

[G–G–P] I. Gelfand, M. Graev, and I. Piatetsky–Shapiro, *Representation theory and automorphic functions,* W.B. Saunders, London 1969.

[G] L. Georite, *Die Bettischen Zahlen der Zyklische Voerlangerung der Knotenauschenraume,* Amer. Jnl. **56** (1934), 194–??.

[Ha] E. Hironaka, Ph.D. Thesis, Brown 1989.

[Hh] F. Hirzebruch, *Arrangements of lines and algebraic surfaces,* in "Arithmetic Geometry", volume in honor of I. Shafarevich, Birkhäuser 1983.

[I] M.N. Ishida, *The irregularities of Hirzebruch's surfaces of general type with* $C_1^2 = 3\,C_2$,

[K] M. Knesser, *Strong Approximation in Algebraic Groups,* Proc. Symp. A.M.S. Volume IX (1966).

[L1] S. Lang, *Introduction to algebraic and Abelian functions,* Springer–Verlag 1982.

[L2] S. Lang, *Fundamentals of Diophantine geometry,* Springer–Verlag 1983.

[Lt] M. Laurant, *Equations diophantine exponentielles,* Invent. Math. **78** (1984), 299–327.

[Lr] A. Libgober, *Betti numbers of Abelian covers,* Preprint 1989.

[L–M] A. Lubotzky and A. Magid, *Varieties of representations of finitely generated groups,* Memoirs of the A.M.S. **58** (1985) No. 336.

[M–M] J. Mayberry and K. Murasugi, *Torsion groups of Abelian coverings of links,* Trans. A.M.S. **271** (1982), 143–17?.

[R–S] D. Ray and I. Singer, *R–torsion and the Laplacian,* Adv. in Math. **7** (1975), 145–210.

[R] Z. Rudnick, *Representation varieties of solvable groups,* Journal of Pure and Appl. Algebra **45** (1987), 261–272.

[S] B. Schoenberg, *Elliptic modular functions,* Springer–Verlag, New York 1974.

[Z] O. Zariski, *On the topology of algebraic singularities,* Amer. Journal. **54** (1932), 453–46?.

Appendix

On Representations of Compact p-adic Groups

ZEÉV RUDNICK

Yale University

Let $\mathcal{G}$ be a Chevalley group, $\mathcal{G}(R)$ the corresponding group over the ring of integers R of a p-adic field of characteristic zero. In this note we give an a-priori proof of the finiteness of representations of $\mathcal{G}(R)$ in a given dimension; here, as throughout the rest of this note, all representations are assumed to be continuous.

We begin by noting that it suffices to prove this theorem for some normal open subgroup $\Gamma \lhd \mathcal{G}(R)$– since if ρ is any irreducible representation of $\mathcal{G}(R)$, then ρ injects into the induced representation:

$$\rho \hookrightarrow \mathrm{Ind}_{\Gamma}^{\mathcal{G}(R)} \mathrm{Res}_{\Gamma}^{\mathcal{G}(R)} \rho$$

and because $\mathcal{G}(R)/\Gamma$ is a finite group, there are only finitely many possibilities for ρ given its restriction to Γ.

From now on, for simplicity of exposition, I take $\mathcal{G} = SL(N)$, $R = Z_p$ the p-adic integers, and $p \neq 2, 3$. Let

$$\Gamma_l = \Gamma(p^l) = \left\{ \gamma \in SL(N, Z_p) \mid \gamma \equiv I \mod p^l \mathfrak{sl}(N, Z_p) \right\}$$

be the principal congruence subgroup of level p^l; here $\mathfrak{sl}(N, Z_p)$ is the Lie algebra of $SL(N, Z_p)$. We take $\Gamma = \Gamma_1$.

If ρ is a continuous finite dimensional representation of Γ, the *level* l_ρ of ρ is the least integer $l \geq 1$ such that ρ is trivial on Γ_l. In this case, ρ factors through the finite group $G_l = \Gamma/\Gamma_l$.

The finiteness result will follow from the following estimate:

PROPOSITION. *Let ρ be an irreducible representation of Γ of dimension n and level l. Then:*

$$l \ll J(n)^{1/\log_2 p} = f(n) \tag{1}$$

where $J(n)$ is the index of a normal, abelian subgroup of $\rho(\Gamma) = \rho(G_l)$; $J(n)$ depends only on n, not on ρ.

Indeed, assuming (1), any ρ of dimension n will factor through the finite group $G_{f(n)}$– so the number of such representations is finite.

To prove (1), we need a couple of lemmas. First, recall that since G_l is a p-group, it is in particular *solvable* (even nilpotent).

LEMMA 1. *G_l has solvable length given by*

$$\text{length}(G_l) = [\log_2(l-1)] + 1 \qquad , l \geq 2 \tag{2}$$

i.e., if $2^{k-1} < l \leq 2^k$ then $\text{length}(G_l) = k$.

PROOF: This follows from computing the commutator subgroups of Γ:

$$(\Gamma_k, \Gamma_k) = \Gamma_{2k}.$$

The inclusion $(\Gamma_k, \Gamma_k) \subseteq \Gamma_{2k}$ is obvious, and equality follows by applying the Campbell-Baker-Hausdorff formula. It is here that one has to use the exponential map

$$\exp : \mathfrak{sl}(N, pZ_p) \longrightarrow \Gamma.$$

Recall that the exponential series:

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

is p-adically convergent only for $|x|_p < 1$. ∎