ISRAEL JOURNAL OF MATHEMATICS 109 (1999), 157–172

ZETA FUNCTIONS RELATED TO THE GROUP $SL_2(\mathbb{Z}_p)$

BY

ISHAI ILANI*

Dolev, D.N. Modiin, 71935, Israel
e-mail: ilani@netmedia.net.il

ABSTRACT

An explicit formula is given for the number of subgroups of index p^n in the principle congruence subgroups of $SL_2(\mathbb{Z}_p)$ (for odd primes p), and for the zeta function associated with the group. Asymptotically this number is cnp^n, where c is a constant depending on the congruence subgroup. Also, the zeta function of the i-th congruence subgroup coincides with the partial zeta function of the 3-generated subgroups of the $i+1$-th congruence subgroup, and for each index p^n the ratio between 2-generated subgroups and 3-generated subgroups tends to $p-1$: 1, as n tends to infinity.

1. Introduction

Let G be a finitely generated group; let $a_n = a_n(G)$ be the number of subgroups of G of index n.

Interest in the function $G \to \{a_n(G)\}_{n=1}^{\infty}$ and the related zeta function $\zeta_G(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ has grown in the last few years and some interesting results were obtained. Two of the most interesting results are:

THEOREM A ([dS]): *If G is a finitely generated, (topologically), compact, p-adic analytic group, then*

$$\zeta_{G,p}(s) := \sum_{n=0}^{\infty} a_{p^n} p^{-sn}$$

is a rational function in the variable p^{-s}.

* This work is part of the author's Ph.D. thesis carried out at the Hebrew University of Jerusalem under the supervision of Prof. A. Lubotzky. I wish to thank Prof. Lubotzky for his continual interest and encouragement without which this paper would not have been published.
Received February 4, 1997

THEOREM B ([LMS]): *A finitely generated, residually finite group has polynomial subgroup growth if and only if it is virtually soluble of finite rank.*

An important ingredient in the proof of Theorem B is the characterization of finitely generated analytic pro-p groups as the pro-p groups with polynomial subgroup growth.

Remark: Using this characterization, Theorem A can actually be stated as a characterization of finitely generated, analytic pro-p groups.

Naturally, these results draw attention to the computation of zeta functions of analytic pro-p groups. A few explicit formulae can be found in [GSS], where the zeta functions of various nilpotent groups have been calculated (mainly "normal" zeta functions).

In this paper I shall give some explicit formulae for semi-simple groups, namely, the principle congruence subgroups of $\mathrm{SL}_2(\mathbb{Z}_p)$ (for an odd prime p).

We shall employ the following theorem, which is a particular case of theorem 2 of [I].

THEOREM 3: *Let $G \leq I + M_n(p\mathbb{Z}_p)$ be a uniform pro-p group of dimension $\leq p$. Then the map: $\log\colon G \to M_n(p\mathbb{Z}_p)$ induces a bijection between the subgroups (normal subgroups) of G, and the Lie subalgebras (ideals) of $\log(G)$ (where $\log(G)$ is given the structure of a Lie algebra over $\mathbb{Z}_p$, coming from the associative algebra $M_n(\mathbb{Q}_p)$).*

Thus instead of counting finite index subgroups, we may count finite index subalgebras, of the Lie algebra (over $\mathbb{Z}_p$), associated with the group. In our case, set

$$\begin{aligned} G_i &:= \ker\bigl(\mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{Z}/p^i\mathbb{Z})\bigr) \\ &= \{I + A \mid \det(I + A) = 1 \text{ and } A \in M_2(p^i\mathbb{Z}_p)\}, \\ L_i &:= \mathfrak{sl}_2(p^i\mathbb{Z}_p) = \{A \in M_2(p^i\mathbb{Z}_p) \mid \operatorname{trace}(A) = 0\}. \end{aligned}$$

If p is an odd prime, then for all $i \geq 1$,

$$G_i = \log(L_i); \qquad L_i = \exp(G_i),$$

and it follows immediately that $G_{i+1} = G_i^p$, and G_i is a uniform pro-p group of dimension 3.

We shall actually show two methods of computation.

1. THE FINITE QUOTIENTS METHOD. In this method, instead of computing $a_{p^n}(L_i)$, we shall compute $a_{p^n}(L_k^i)$, where $L_k^i := L_i/L_k$. As we shall see, from

a certain point on, $1/p$ of the subalgebras of index p^{n-1}, and rank 2 of L_{k-1}^i, can be lifted to a subalgebra of index p^n and rank 2 of L_k^i. This will be used to compute the number of the subalgebras, of index p^n, and rank ≤ 2 of L_k^i, and summing over all k's will finally give the result for $a_{p^n}(L_i)$.

2. p-ADIC INTEGRATION METHOD. This method follows [GSS]. With every subalgebra of index p^n of L_i, we associate a measurable set of upper triangular matrices, such that if A is a matrix associated with a subalgebra H of finite index, then $|\det(A)|^{-1} = (L_i\colon H)$. Integrating an appropriate function over all the matrices A with $|\det(A)|^{-1} = p^n$ will lead to $a_{p^n}(L_i)$. In principle the second method is more general, and can be used to compute also the zeta function of $\mathfrak{sl}_2(2^i\mathbb{Z}_2)$, but in practice it is complicated, while the first method is straightforward.

Both methods mentioned above compute the zeta functions in each of the congruence subalgebras directly, but the following interesting observation, by Lubotzky and du Sautoy, can also be helpful in computing the zeta functions of the congruence subalgebras of uniform 3-dimensional algebras, by computing the zeta function of the algebra.

Observation: [LdS]. For every odd prime-p, and for every 3-dimensional uniform Lie algebra L,

$$\zeta_{L_{i+1},p}(s) - \zeta_{\mathbb{Z}_p^3}(s) = p^{2-s}\big(\zeta_{L_i,p}(s) - \zeta_{\mathbb{Z}_p^3}(s)\big)$$

where L_i is the i-th congruence subalgebra of L.

The main results of this paper are:

THEOREM 1: *Let p be an odd prime, G_i, L_i as above, $a_{p^n,i} := a_{p^n}(G_i) = a_{p^n}(L_i)$. Then*

$$a_{p^n,i} = \begin{cases} \frac{p^3}{(p-1)^2(p+1)}p^{2n} - \frac{p}{(p-1)^2}p^n + \frac{1}{(p-1)^2(p+1)}, & n \leq i; \\ \begin{pmatrix} \frac{p+1}{2(p-1)}(n-i)p^{i+n} + \frac{p^3-p-1}{(p-1)^2(p+1)}p^{i+n} \\ -\frac{p}{(p-1)^2}p^n + \frac{p^{(3i+n)/2}}{(p-1)^2} + \frac{1}{(p-1)^2(p+1)} \end{pmatrix}, & \begin{matrix} n \geq i, \text{ and} \\ n+i \equiv 0 \pmod 2; \end{matrix} \\ \begin{pmatrix} \frac{p+1}{2(p-1)}(n-i+1)p^{i+n} - \frac{p}{(p-1)^2(p+1)}p^{i+n} \\ -\frac{p}{(p-1)^2}p^n + \frac{p^{(3i+n+1)/2}}{(p-1)^2} + \frac{1}{(p-1)^2(p+1)} \end{pmatrix}, & \begin{matrix} n > i, \text{ and} \\ n+i \equiv 1 \pmod 2. \end{matrix} \end{cases}$$

The zeta function of G_i, (L_i), is

$$\zeta_{G_i}(s) = \frac{1}{(1-p^{-s})(1-p^{1-s})(1-p^{2-s})} - \frac{p^{2i+5}p^{-(1+i)s}}{(p-1)(p^2-1)(1-p^{2-s})} + \frac{p^{2i+1}p^{-(1+i)s}}{p-1}\left(\frac{(p+1)}{(1-p^{1-s})^2(1+p^{1-s})} + \frac{p^{1-s}(p^3-p-1)-p}{(p^2-1)(1-p^{2-2s})} + \frac{p^{-s}+1}{(p-1)(1-p^{1-2s})}\right).$$

Notation

$\langle X\rangle$	The (closed) group generated by the set X.
G^p	The (closed) group generated by the p-th powers of G.
$\mathfrak{Lie}X$	The (closed) Lie algebra over $\mathbb{Z}_p$, generated by the set X.
$[x,y]$	The Lie algebra product of x, y.
$\mathrm{d}(G)$	The minimal cardinality of a (topological) generating set for G.
$\mathrm{rk}(G)$	The (subgroup) rank of G, $(= \sup\{\mathrm{d}(H) \mid H \text{ a closed subgroup of } G\})$.
$\dim(G)$	The dimension of G.
$\overline{X}$	The leading term of X (defined after Theorem 2.3).
$\nu(x)$	The p-adic valuation of x.
$\mathbb{Z}_p$	The p-adic integers.
$\mathbb{Q}_p$	The p-adic numbers.
$\mathbb{F}_p$	The field with p elements.
$a_{p^n}(G)$	The number of subgroups of index p^n in G, $(\#\{H \le G \mid (G\colon H) = p^n\})$
L_i	$\mathfrak{sl}_2(p^i\mathbb{Z}_p)$.
L_k^i	L_i/L_k.
$a_{k,n}^i$	The number of subalgebras of index p^n in L_k^i.
$b_{k,n}^i$	The number of subalgebras of index p^n, and rank ≤ 2 in L_k^i.
$\tilde{a}_{k,n}^i$	The number of subgroups of index p^n in $(p^i\mathbb{Z}/p^k\mathbb{Z})^3$.
$\tilde{b}_{k,n}^i$	The number of subgroups of index p^n, and rank ≤ 2 in $(p^i\mathbb{Z}/p^k\mathbb{Z})^3$.

2. Theoretical part of the finite quotients method

As we have mentioned, the algebras L_i are uniform of dimension 3. It follows that every finite index subalgebra of L_i is of rank 3. (For large enough j, it contains L_j, which is a Lie algebra generated by 3 generators.) The quotients L_k^i, are also of rank 3, but they contain subalgebras of rank ≤ 2. The following lemma characterises the subalgebras of L_k^i, which have rank 3.

LEMMA 2.1: *Let L be a subalgebra of L_k^i. Then* $\mathrm{rk}(L) = 3$ *if and only if*

$$L_k^{k-1} = \ker(L_k^i \to L_{k-1}^i) \leq L.$$

Proof: L_k^{k-1} is an abelian Lie algebra, and as an additive group it is an elementary abelian group of order p^3; thus if $L_k^{k-1} \leq L$, then $\mathrm{rk}(L) = 3$.

On the other hand, if $\mathrm{rk}(L) = 3$, then there exists a subalgebra $K \leq L$, with $\mathrm{d}(K) = 3$. If $L_k^{k-1} \not\leq L$, say $l \in L_k^{k-1} \setminus L$, then $\mathfrak{Lie}\{K, l\} \cong K \oplus \mathfrak{Lie}\{l\}$, since L_k^{k-1} is central in L_k^i ($[L_{k-1}, L_i] \subset L_{k+i-1} \subset L_k$). But $\mathrm{d}(\mathfrak{Lie}\{K, l\}) = 4$, contradicting the fact that $\mathrm{rk}(L_k^i) = 3$. ∎

This simple observation has an important consequence.

COROLLARY 2.2:

$$a_{k,n}^i = a_{k-1,n}^i + b_{k,n}^i, \tag{1}$$

$$a_{p^n}(L_i) = a_{n+i,n}^i = \sum_{n/3+i \leq j \leq n+i} b_{j,n}^i. \tag{2}$$

Proof: The first part follows immediately from Lemma 2.1, together with the homomorphism theorems.

The second part follows from the fact that $b_{k,n}^i = 0$ for $k > n + i$. This follows from the fact that the additive group of L_k^i is isomorphic to $(p^i\mathbb{Z}/p^k\mathbb{Z})^3 \cong (\mathbb{Z}/p^{k-i}\mathbb{Z})^3$, and therefore $|L_k^i| = p^{3(k-i)}$. If L is a subalgebra of rank 2 and index p^n of L_k^i, then $p^n|L| = p^{3(k-i)}$. L is a sum of two cyclic subalgebras, and since the exponent of L_k^i is p^{k-i}, $|L| \leq p^{2(k-i)}$, and thus $n \geq k-i$. The right hand side follows from the first part, and the limits of summation follow considering the fact that $|L_j^i| = p^{3(j-i)}$, and therefore L_j^i does not contain subalgebras of index $> p^{3(j-i)}$, so $j \geq n/3 + i$, while on the other hand we just proved that $b_{j,n}^i = 0$ for $j > n + i$. ∎

The computation of $b_{k,n}^i$ will be based on the following theorem:

THEOREM 2.3: *Let p be an odd prime, $b_{k,n}^i$ as above, $i > 0$, $k \geq i$, $n \geq 0$. Then*

$$b_{k,n}^i = \begin{cases} \tilde{b}_{k,n}^i, & n \geq 2k - 3i, \\ \frac{p^2(p+1)}{p^2+p+1} b_{k-1,n-1}^i, & k - i \leq n = 2k - 3i - 1, \\ p b_{k-1,n-1}^i, & k - i \leq n \leq 2k - 3i - 2, \\ 0, & n < k - i. \end{cases}$$

Remarks:

(1) Every matrix $A \in L_i$ (or in L_k^i) can be written as a series, $A = \sum_j p^j A_j$, where all the coefficients of A_j are integers between 0 and $p-1$.

(2) The **valuation** of A (denoted $\nu(A)$) is defined by $\nu(A) := \inf\{j | A_j \neq 0\}$.

(3) $A_{\nu(A)}$ is called the **leading term** of A (and will be denoted $\overline{A}$), and since $A \in \mathfrak{sl}_2(p^i\mathbb{Z}_p)$ it follows that $\overline{A}$ can be viewed as a matrix in $\mathfrak{sl}_2(\mathbb{F}_p)$.

(4) In the finite algebras L_k^i, if $\nu(A) \geq k$, then $A = 0$.

(5) If $A \neq 0 \in L_k^i$, then the order of A is $p^{k-\nu(A)}$, and $\overline{A} = \overline{p^j A}$ for all $j < k - \nu(A)$.

(6) The additive group of L_k^i is isomorphic to $(\mathbb{Z}/p^{k-i}\mathbb{Z})^3$, and therefore the number of elements of order p^j (for $1 \leq j \leq k-i$) in L_k^i is $p^{3(j-1)}(p^3-1)$.

In order to prove Theorem 2.3 we shall need the following lemma and corollary.

LEMMA 2.4: *Let p be an odd prime, and let $C = \left(\begin{smallmatrix} c_1, & c_2 \\ c_3, & -c_1 \end{smallmatrix}\right) \neq 0$, $B = \left(\begin{smallmatrix} b_1, & b_2 \\ b_3, & -b_1 \end{smallmatrix}\right) \neq 0$ be matrices in $\mathfrak{sl}_2(\mathbb{F}_p)$. Then:*

(1) $\operatorname{Im}\operatorname{ad} C = \left\{ \left(\begin{smallmatrix} x_1, & x_2 \\ x_3, & -x_1 \end{smallmatrix}\right) | 2c_1x_1 + c_3x_2 + c_2x_3 = 0 \right\}$.

(2) $C \in \operatorname{Im}\operatorname{ad} C$ *if and only if* $\det(C) = 0$.

(3) *If* $\det(C) = 0$, *then* $\operatorname{ad} C$ *is a nilpotent linear map of rank* 2 *(i.e.* $\dim(\operatorname{Im}\operatorname{ad} C) = 2$*), and if* $\det(C) \neq 0$, *then* $\operatorname{ad} C$ *is diagonalizable with the eigenvalues* $0, \pm 2\sqrt{-\det(C)}$.

(4) *If* $\det(C) = 0$ *then* C *is an eigenvector of* $\operatorname{ad} B$ *if and only if* $B \in \operatorname{Im}\operatorname{ad} C$, *and if* $\{B, C\}$ *is a linearly independent set, then the corresponding eigenvalue is not* 0.

(5) *If* $\det(C) \neq 0$ *and* C *is an eigenvector of* $\operatorname{ad} B$, *then* $B = aC$, *for some* $a \in \mathbb{F}_p$ *(and the corresponding eigenvalue is of course* 0*).*

COROLLARY 2.5: *Let L be a plane in $\mathfrak{sl}_2(\mathbb{F}_p)$, defined by the equation $2c_1x_1 + c_3x_2 + c_2x_3 = 0$, Then:*

(1) *If* $\left(\begin{smallmatrix} c_1, & c_2 \\ c_3, & -c_1 \end{smallmatrix}\right) = C \in L$, *then the set* $\{A, B, [A, B]\}$ *is a linearly dependent set for all* $\{A, B\} \subset L$.

(2) *If* $\left(\begin{smallmatrix} c_1, & c_2 \\ c_3, & -c_1 \end{smallmatrix}\right) = C \notin L$, *and the set* $\{A, B\} \subset L$ *is linearly independent, then* $\{A, B, [A, B]\}$ *is a basis for* $\mathfrak{sl}_2(\mathbb{F}_p)$.

Proof of Lemma 2.4: With respect to the basis: $\left\{ \left(\begin{smallmatrix} 1, & 0 \\ 0, & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 1 \\ 0, & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 0 \\ 1, & 0 \end{smallmatrix}\right) \right\}$, the matrix representing $\operatorname{ad} C$ is

$$\begin{pmatrix} 0 & c_3 & -c_2 \\ 2c_2 & -2c_1 & 0 \\ -2c_3 & 0 & 2c_1 \end{pmatrix}.$$

This is a matrix of rank 2, and each of its columns satisfies the equation $2c_1x_1 + c_3x_2 + c_2x_3 = 0$, thus it follows that this equation defines $\operatorname{Im}\operatorname{ad} C$. C satisfies this equation if and only if $\det(C) = 0$.

The characteristic polynomial of $\operatorname{Im}\operatorname{ad} C$ is $t^3 - 4(c_1^2 + c_2c_3)t$, with the eigenvalues $0, \pm 2\sqrt{-\det(C)}$. Thus if $\det(C) = 0$, then $\operatorname{Im}\operatorname{ad} C$ is nilpotent with nilpotency rank 2, so $(\operatorname{ad} C)^2 \neq 0$, but $(\operatorname{ad} C)^3 = 0$. Therefore $\operatorname{span} C = \ker \operatorname{ad} C = \operatorname{Im}(\operatorname{ad} C)^2$. If $B \in \operatorname{Im}\operatorname{ad} C$, then $\operatorname{ad} C(B) = -\operatorname{ad} B(C) \in \operatorname{span} C$, thus C is an eigenvector of $\operatorname{ad} B$, and if $\{B, C\}$ is linearly independent, then the eigenvalue is nonzero.

If $D \notin \operatorname{Im}\operatorname{ad} C$, and C is an eigenvector of $\operatorname{ad} D$, then $\{B, C, D\}$ is a basis of $\mathfrak{sl}_2(\mathbb{F}_p)$ whose images generate a 1-dimensional subspace, which contradicts the fact that $\operatorname{Im}\operatorname{ad} C$ is 2-dimensional.

The last part follows since when $\det(C) \neq 0$, $C \notin \operatorname{Im}\operatorname{ad} C$. ∎

Proof of Corollary 2.5: If $C \in L$, then for every linear independent set $\{A, B\} \subset L$ we may assume that $B = aA + cC$, thus proving the first part.

For the second part, assume $\{A, B\} \subset L$ is linearly independent, but $\{A, B, [A, B]\}$ is dependent. Then we may assume that $[A, B] = aA + bB$ with $b \neq 0$. This implies that

$$[B + a/bA, A] = -b(B + a/bA).$$

Thus $B + a/bA$ is an eigenvector of $\operatorname{ad} A$, with a nonzero eigenvalue. From Lemma 2.4, we know that this implies that $L = \operatorname{Im}\operatorname{ad}(B + a/bA)$ and this implies that C is a scalar multiple of $B + a/bA$, which contradicts the assumption that $C \notin L$.

Proof of Theorem 2.3: Let L be a subalgebra of index $\geq p^{2k-3i}$ (i.e. $|L| \leq p^k$). Suppose we choose a generating set for the additive group of L, with linearly independent leading terms. Suppose A, B are elements of the generating set. Then

$$|\langle A, B\rangle| = |\langle A\rangle||\langle B\rangle| = p^{k-\nu(A)}p^{k-\nu(B)}.$$

Since $|L| \leq p^k$, deduce that $\nu(A) + \nu(B) \geq k$. But $\nu[A, B] \geq \nu(A) + \nu(B) \geq k$ (in fact, if $\overline{A}, \overline{B}$ are linearly independent, then $\nu[A, B] = \nu(A) + \nu(B)$, and $\overline{[A, B]} = [\overline{A}, \overline{B}]$), thus $[A, B] = 0$ in L_k^i, and L is abelian. Thus, every additive subgroup of order $\leq p^k$ of L_k^i is also an abelian subalgebra, and this proves the first part of the theorem.

The last part has already been proved (see Corollary 2.2), and it remains to prove the middle parts of the theorem.

Suppose $k-i \leq 2k-3i-1$, i.e. $k \geq 2i+1$, and L is a subalgebra of rank ≤ 2, and index $p^{2k-3i-2}$, of L^i_{k-1}. Note that $|L| = p^{k-1}$, and since the exponent of L^i_{k-1} is less than p^{k-1}, deduce that $\mathrm{rk}(L) = 2$. Thus we may assume that $L = \mathfrak{Lie}\{A, B\}$, with $\overline{A}, \overline{B}$ linearly independent, $\nu(A) = l, \nu(B) = j$, and $l + j = k - 1$, and the defining equation of $\mathrm{span}\{\overline{A}, \overline{B}\}$ is $2c_1x_1 + c_3x_2 + c_2x_3 = 0$, i.e.,

$$\mathrm{span}\{\overline{A}, \overline{B}\} = \left\{ \begin{pmatrix} x_1, & x_2 \\ x_3, & -x_1 \end{pmatrix} \middle| 2c_1x_1 + c_3x_2 + c_2x_3 = 0 \right\}.$$

If $\left(\begin{smallmatrix} c_1, & c_2 \\ c_3, & -c_1 \end{smallmatrix}\right)$ is not in this plane, then by Corollary 2.5, $\{\overline{A}, \overline{B}, [\overline{A}, \overline{B}]\}$ is a basis for $\mathfrak{sl}_2(\mathbb{F}_p)$, and thus, as a subalgebra of L^i_k, L is of rank 3, since it contains the subalgebra generated by

$$p^{k-1}\overline{A}, p^{k-1}\overline{B}, p^{k-1}[\overline{A}, \overline{B}],$$

which is an abelian subalgebra of order p^3.

If, on the other hand, $\left(\begin{smallmatrix} c_1, & c_2 \\ c_3, & -c_1 \end{smallmatrix}\right) = C \in \mathrm{span}\{\overline{A}, \overline{B}\}$, then we may assume that $C = \overline{A}$, and thus

$$[A, B] = p^{k-1}[\overline{A}, \overline{B}] = \pm 2p^j \sqrt{-\det \overline{B}}\, \overline{A},$$

and L is a subalgebra of rank 2, even when it is viewed as a subalgebra of L^i_k.

Stated more precisely, this means that if $\tilde{A} \in \pi^{-1}(A), \tilde{B} \in \pi^{-1}(B)$, where π denotes the natural projection, $\pi\colon L^i_k \to L^i_{k-1}$, then the subalgebra generated by $\tilde{A}, \tilde{B}$ is a subalgebra of rank 2, and index $p^{2k-3i-1}$, of L^i_k. Define an equivalence relation on $L^i_k \times L^i_k$ by $(A, B) \sim (C, D)$ if they generate the same subalgebra. It is easy to see that $|\pi^{-1}(A) \times \pi^{-1}(B)| = p^6$, and the equivalence classes of this set are of size p^4, thus if L can be lifted to a rank 2 algebra of L^i_k, then it can be lifted in p^2 different ways.

The number of planes which satisfy the above condition, $\left(\left(\begin{smallmatrix} c_1, & c_2 \\ c_3, & -c_1 \end{smallmatrix}\right) = C \in \mathrm{span}\{\overline{A}, \overline{B}\}\right)$, is $p + 1$, while the total number of planes in $\mathfrak{sl}_2(\mathbb{F}_p)$ is $p^2 + p + 1$. Putting all this together yields the second part of Theorem 2.3.

Suppose now that $k - i \leq n \leq 2k - 3i - 2$, and let L be a subalgebra of index p^{n-1}, and rank 2 of L^i_{k-1}.

From the previous case it follows that we can find $A, B \in L$, s.t. $\{\overline{A}, \overline{B}\}$ is linearly independent, and $\mathrm{ad}\,\overline{B}(\overline{A}) = 2\sqrt{-\det \overline{B}}\, \overline{A}$.

For the above A, B, denote by $\mathfrak{H}$ the following set of subalgebras:

$$\mathfrak{H} := \left\{ \mathfrak{Lie}\{B, A + D\} | D \in L^i_{k-1}, \nu(D) + \nu(B) \geq k - 1 \right\}.$$

PROPOSITION 2.6: *The subalgebras of L^i_{k-1} which are contained in $\mathfrak{H}$ are isomorphic, but only $1/p$ of them can be lifted to a subalgebra of rank 2 of L^i_k.*

Proof: The map

$$A \mapsto A + D, \quad B \mapsto B$$

can be extended to an isomorphism of $\mathfrak{Lie}\{A, B\}$ and $\mathfrak{Lie}\{A + D, B\}$, since $[A + D, B] = [A, B] = aA + bB$ with $a \equiv 2p^{\nu(B)}\sqrt{-\det \overline{B}} \pmod{p^{\nu(B)+1}}$, and $t(A + D) = tA$ for all t with $\nu(t) \geq \nu(B)$.

If we consider A, B as elements of L^i_k, then $[A, B] = aA + bB + C$, with $\nu(C) \geq k - 1$. Thus as a subalgebra of L^i_k, $\mathfrak{Lie}\{A, B\}$ is of rank 2 if and only if $\overline{C} = x\overline{A} + y\overline{B}$, for some $x, y \in \mathbb{F}_p$. More generally, if $\alpha := k - 1 - \nu(B)$ and $D = \sum_{j \geq \alpha} p^j D_j$, then

$$\begin{aligned}[A + D, B] = [A, B] + [D, B] =& aA + bB + C + p^{k-1}[D_\alpha, \overline{B}] \\ =& a(A + D) + bB + (p^{k-1}[D_\alpha, \overline{B}] - aD + C) \\ =& a(A + D) + bB \\ &+ p^{k-1}\Big([D_\alpha, \overline{B}] - 2\sqrt{-\det \overline{B}}D_\alpha + \overline{C}\Big),\end{aligned}$$

and the subalgebra $\mathfrak{Lie}\{A + D, B\}$ is of rank 2 if and only if

$$[D_\alpha, \overline{B}] - 2\sqrt{-\det \overline{B}}D_\alpha + \overline{C} \in \operatorname{span}\{\overline{A}, \overline{B}\}.$$

Consider the linear map $T\colon \mathfrak{sl}_2(\mathbb{F}_p) \to \mathfrak{sl}_2(\mathbb{F}_p)$,

$$T(X) := \operatorname{ad}\overline{B}(X) - 2\sqrt{-\det \overline{B}}X.$$

$\operatorname{ad}\overline{B}$ is diagonalizable with eigenvalues $2\sqrt{-\det \overline{B}}$, 0, $-2\sqrt{-\det \overline{B}}$, and eigenvectors $\overline{A}, \overline{B}, E$, and thus T will be diagonalizable with the same eigenvectors, and the eigenvalues (respectively) $0, -2\sqrt{-\det \overline{B}}, -4\sqrt{-\det \overline{B}}$, and thus $\operatorname{Im} T = \operatorname{span}\{\overline{B}, E\}$. It follows that p^2 out of p^3 possibilities for choosing D_α will lead to a subalgebra of rank 2. (All one has to do is to adjust the E coordinate of D_α with that of C, and the other 2 coordinates can be chosen freely.) Therefore the probability that an algebra contained in $\mathfrak{H}$ is of rank 2, is $1/p$. (Note that choosing D uniformly induces a uniform probability on $\mathfrak{H}$.)

Finally, we shall show that the same applies if we extend $\mathfrak{H}$ to include all the subalgebras of L^i_{k-1}, which are isomorphic to $\mathfrak{Lie}\{A, B\}$. It is clear that choosing a monomorphism of $\mathfrak{Lie}\{A, B\}$ uniformly induces uniform probability on $\mathfrak{H}$.

We shall choose a monomorphism uniformly by the following mechanism:

1. Choose a monomorphism uniformly. This is equivalent to choosing A', B' which satisfy the same relations as A, B.
2. Choose D uniformly from all matrices in L^i_{k-1} with $\nu(D) \geq \alpha$, and our final choice is the algebra $\mathfrak{Lie}\{A' + D, B'\}$.

This way we have chosen a monomorphism uniformly, and therefore also a subalgebra of $\mathfrak{H}$ was chosen uniformly. Given A', B', the probability that $\mathfrak{Lie}\{A' + D, B'\}$ can be lifted to a subalgera of rank 2 of L^i_k, is $1/p$. Since this is the same for all A', B' this implies that $1/p$ of the subalgebras in $\mathfrak{H}$ can be lifted to a subalgebra of rank 2 of L^i_k. Since this is true for every equivalence class of isomorphic subalgebras of rank 2 and index p^{n-1} of L^i_{k-1}, the third part of Theorem 2.3 has been proved.

This ends the proof of Theorem 2.3, and we are left with the actual computation to be conducted.

3. Computation of $b^i_{k,n}$ and $a_{p^n}(L_i)$

PROPOSITION 3.1: $\tilde{b}^i_{k,n} =$

$$\begin{cases} 1, & n = 3(k-i), \\ p^{3(k-i)-n-2}(p^2+p+1)(p^{3(k-i)-n} + \frac{p^{3(k-i)-n-1}-1}{p-1}), & 2(k-i) \leq n < 3(k-i), \\ p^{3(k-i)-n-2}(p^2+p+1)(\frac{p^{n-(k-i)+1}-1}{p-1}), & (k-i) \leq n < 2(k-i), \\ 0, & n < (k-i). \end{cases}$$

Proof: In the spirit of Theorem 2.3, one can prove the following recursion formula:

$$\tilde{b}^i_{k,n} - \tilde{c}^i_{k,n} = p^2 \tilde{b}^i_{k-1,n-1} + p\tilde{c}^i_{k-1,n-1},$$

where $\tilde{c}^i_{k,n}$ denotes the number of cyclic subgroups of index p^n in $(\mathbb{Z}/p^{k-i}\mathbb{Z})^3$, and continue by induction on k. Recall that $\tilde{c}^i_{k,n} \neq 0$ if and only if $n \geq 2(k-i)$, and in that case

$$\tilde{c}^i_{k,n} = p^{6(k-i)-2n-2}(p^2+p+1).$$

Combine this formula and Theorem 2.3 to get: $b^i_{k,n} =$

(*)

$$\begin{cases} 1, & n = 3(k-i), \\ p^{3(k-i)-n-2}(p^2+p+1)(p^{3(k-i)-n} + \frac{p^{3(k-i)-n-1}-1}{p-1}), & 2(k-i) \leq n < 3(k-i), \\ p^{3(k-i)-n-2}(p^2+p+1)(\frac{p^{n-(k-i)+1}-1}{p-1}), & 2k-3i \leq n < 2(k-i), \\ p^{k-1}(p+1)(\frac{p^{n-(k-i)+1}-1}{p-1}), & k-i \leq n < 2k-3i. \\ 0, & n < (k-i). \end{cases}$$

(*) If $k \leq 2i$, then the lower limit of n is $k-i$, and the region $k-i \leq n < 2k-3i$ is empty.

Writing again with respect to the values of k gives $b^i_{k,n} =$

(*)
$$\begin{cases} 1, & k = \frac{n}{3} + i, \\ p^{3(k-i)-n-2}(p^2+p+1)(p^{3(k-i)-n} + \frac{p^{3(k-i)-n-1}-1}{p-1}), & \frac{n}{3}+i < k \leq \frac{n}{2}+i, \\ p^{3(k-i)-n-2}(p^2+p+1)(\frac{p^{n-(k-i)+1}-1}{p-1}), & \frac{n}{2}+i < k \leq \frac{n+3i}{2}, \\ p^{k-1}(p+1)(\frac{p^{n-(k-i)+1}-1}{p-1}), & \frac{n+3i}{2} < k \leq n+i, \\ 0, & n+i < k\ . \end{cases}$$

(*) If $n \leq i$, then the upper bound of k is $n+i$, and not $(n+3i)/2$, and the region $(n+3i)/2 < k \leq n+i$ is empty.

Using the formula (see Corollary 2.2)

$$a_{p^n}(L_i) = \sum_{n/3+i \leq j \leq n+i} b^i_{j,n},$$

we get:

1. If $n \leq i$, then
$$\begin{aligned} a_{p^n}(L_i) &= a_{p^n}(\mathbb{Z}^3) = a_{p^n}(\mathbb{Z}_p^3) \\ &= \frac{p^3}{(p-1)^2(p+1)}p^{2n} - \frac{p}{(p-1)^2}p^n + \frac{1}{(p-1)^2(p+1)}. \end{aligned}$$
2. If $n \geq i$, set $\epsilon := 1$ if $n \equiv 0 (\mathrm{mod}\, 3)$, and $\epsilon := 0$ otherwise, and substitute the value of $b^i_{j,n}$, to get
$$\begin{aligned} a_{p^n}(L_i) = \epsilon &+ \sum_{j=1+i+[n/3]}^{i+[n/2]} p^{3(j-i)-n-2}(p^2+p+1) \\ &\qquad \times \left(p^{3(j-i)-n} + \frac{p^{3(j-i)-n-1}-1}{p-1}\right) \\ &+ \sum_{j=1+i+[n/2]}^{[(3i+n)/2]} \frac{p^{3(j-i)-n-2}(p^2+p+1)(p^{n-(j-i)+1}-1)}{p-1} \\ &+ \sum_{j=1+[(3i+n)/2]}^{i+n} \frac{p^{j-1}(p+1)(p^{n-(j-i)+1}-1)}{p-1}. \end{aligned}$$

This last expression is a sum of geometrical progressions, with quotients $1, p, p^2, p^3, p^6$, and summing them all up gives the results claimed in Theorem 1.

4. Computation by p-adic integration

In this section we will compute again the coefficients $a_{p^n}(L_i)$, and the associated zeta function, by p-adic integration. In principle this method is applicable for $p = 2$ as well (but we do not know if in this case the zeta function of the group $\ker\big(\mathrm{SL}_2(\mathbb{Z}_2) \to \mathrm{SL}_2(\mathbb{Z}/2^i\mathbb{Z})\big)$ coincides with the zeta functionof the Lie algebra $\mathfrak{sl}_2(2^i\mathbb{Z}_2)$).

We follow [GSS]. Let L be an algebra which is additively isomorphic to $(\mathbb{Z}_p)^k$. Fix a basis (over $\mathbb{Z}_p$) for L. Relative to this basis, every subalgebra, H, of L can be represented by a triangular basis, i.e. a basis of the form

$$\left\{ \begin{pmatrix} a_{11} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \\ 0 \\ \vdots \end{pmatrix}, \quad \cdots \quad , \begin{pmatrix} a_{1k} \\ a_2 k \\ a_{3k} \\ \vdots \\ a_{kk} \end{pmatrix} \right\},$$

and every $h \in H$ can be uniquely represented as a linear combination:

$$h = c_1 \begin{pmatrix} a_{11} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} a_{12} \\ a_{22} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + c_3 \begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \\ 0 \\ \vdots \end{pmatrix} + \cdots + c_k \begin{pmatrix} a_{1k} \\ a_2 k \\ a_{3k} \\ \vdots \\ a_{kk} \end{pmatrix},$$

with $c_1, c_2, \ldots, c_k \in \mathbb{Z}_p$. With this basis we associate the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \vdots & a_{1k} \\ 0 & a_{22} & a_{23} & \vdots & a_2 k \\ 0 & 0 & a_{33} & \vdots & a_{3k} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \vdots & a_{kk} \end{pmatrix},$$

and the index of H in L can be expressed as

$$(L\colon H) = |\det A|^{-1} = |a_{11}a_{22}\cdots a_{kk}|^{-1}.$$

If we consider the set of all triangular matrices (over $\mathbb{Z}_p$) as a measure space, with the measure ν, the product of the normalized Haar measure of $\mathbb{Z}_p$, then this set (denoted $T_k(\mathbb{Z}_p)$) is a measurable space and ν is a normalized Haar measure. Two matrices, A, B, represent the same subalgebra of L if and only if $B \in AT_k^*(\mathbb{Z}_p)$,

where $T_k^*(\mathbb{Z}_p) := \mathrm{GL}_k(\mathbb{Z}_p) \cap T_k(\mathbb{Z}_p)$. Thus the measure of the set of all matrices representing a given subalgebra H is (see [GSS] lemma 3.2)

$$\nu\big(AT_k^*(\mathbb{Z}_p)\big) = (1-1/p)^k |a_{11}|^k |a_{22}|^{k-1} \cdots |a_{kk}|^1.$$

It follows immediately that:

PROPOSITION 4.1: *Let $\mathfrak{A}$ denote the set of all triangular matrices which are associated with subalgebras of finite index in L, and let*

$$\mathfrak{A}_n := \{A \in \mathfrak{A} \,|\, |\det(A)| = p^{-n}\}$$

(i.e. $\mathfrak{A}_n$ is the set of all matrices associated with subalgebras of index p^n in L). Then

$$(1) \qquad a_{p^n}(L) = (1-1/p)^{-k} \int_{A \in \mathfrak{A}_n} |a_{11}|^{-k} |a_{22}|^{-(k-1)} \cdots |a_{kk}|^{-1} d\nu,$$

$$\zeta_{L,p}(s) = \sum_{n=0}^{\infty} a_{p^n}(L) p^{-sn}$$

$$(2) \qquad = (1-1/p)^{-k} \int_{A \in \mathfrak{A}} |a_{11}|^{s-k} |a_{22}|^{s-(k-1)} \cdots |a_{kk}|^{s-1} d\nu.$$

The application towards computing $\zeta_{\mathfrak{sl}_2(p^i\mathbb{Z}_p)}(s)$ is as follows:

Choose the following basis for $\mathfrak{sl}_2(p^i\mathbb{Z}_p)$, which contains a base for the Cartan subalgebra, and a base for each of the root spaces, namely

$$h = p^i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad x = p^i \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \quad y = p^i \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

The relations for this basis are

$$[h,x] = 2p^i x; \quad [h,y] = -2p^i y; \quad [x,y] = p^i h,$$

and the mapping

$$ah + bx + cy \mapsto \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

is a bijection of $\mathfrak{sl}_2(p^i\mathbb{Z}_p)$ and $(\mathbb{Z}_p)^3$.

Suppose that the additive subgroup generated by

$$\begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} a_2 \\ b_2 \\ 0 \end{pmatrix}, \begin{pmatrix} a_3 \\ b_3 \\ c_3 \end{pmatrix}$$

is a subalgebra of $\mathfrak{sl}_2(p^i\mathbb{Z}_p)$. The index of this subalgebra is $|a_1b_2c_3|^{-1}$, and the measure of the set of triangular matrices associated with this subalgebra is $(1-1/p)^3|a_1|^3|b_2|^2|c_3|$. Thus (as we have already noted in Proposition 4.1)

$$a_{p^n}(\mathfrak{sl}_2(p^i\mathbb{Z}_p)) = \int_{A\in\mathfrak{A}_n} f(A)d\nu,$$

with

$$f(A) = (1-1/p)^{-3}p^n|a_1|^{-2}|b_2|^{-1}.$$

A matrix

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & b_2 & b_3 \\ 0 & 0 & c_3 \end{pmatrix}$$

represents a subalgebra of $\mathfrak{sl}_2(p^i\mathbb{Z}_p)$ if and only if the following conditions are satisfied (with the notation $\alpha_j = \nu(a_j), \beta_j = \nu(b_j)$):

$$\begin{aligned} &\beta_2 \le \nu(4) + i + \alpha_1 + \beta_3, \\ &\beta_2 \le \nu(4) + i + \alpha_2 + \beta_3, \\ &\alpha_1 \le \nu\big(b_2c_3 - 4a_2^2b_3/b_2 + 4a_2a_3\big) + i. \end{aligned} \tag{4.1}$$

These conditions follow from the fact that the Lie product of every pair of the generators must be contained in the additive subgroup generated by the generators.

An elaborate calculation (which can be obtained from the author) leads to the results declared in Theorem 1.

In principle, the p-adic integration method can be used to compute the zeta functions for the Lie algebras $\mathfrak{sl}_2(2^i\mathbb{Z}_2)$, and we leave it to the reader to complete the computation in this case.

5. Partial zeta functions

Denote by $a2_{p^n}(L_i)$ the number of 2-generated subgroups (subalgebras) of index p^n of L_i, and similarly, let $a2^i_{k,n}, b2^i_{k,n}$ be the analogs of $a^i_{k,n}, b^i_{k,n}$. Then it is easy to see that Corollary 2.2 applies to these numbers as well, i.e.

(1) $$a2^i_{k,n} = a2^i_{k-1,n} + b2^i_{k,n},$$

(2) $$a2_{p^n}(L_i) = a2^i_{n+i,n} = \sum_{n/3+i\le j\le n+i} b2^i_{j,n}.$$

The computation of $b2^i_{k,n}$ is very similar to that of $b^i_{k,n}$ and gives the following interesting results:

$$a3_{p^n}(L_i) = a_{p^n}(L_{i-1}),$$
$$a2_{p^n}(L_i) = a_{p^n}(L_i) - a_{p^n}(L_{i-1}).$$

Alternatively, one can prove directly that the map $H \to pH$ induces a bijection between the subalgebras of L_{i-1} and the 3-generated subalgebras of L_i, preserving the index.

As $n \to \infty$, the ratio between the 3-generated subgroups and the total number of subgroups of index p^n tends to $1/p$, thus the ratio between 3-generated subgroups and 2-generated subgroups tends to 1: $p - 1$.

References

[D] J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety*, Inventiones Mathematicae **77** (1984), 1–23.

[DvdD] J. Denef and L. van den Dries, *p-adic and real subanalytic sets*, Annals of Mathematics **128** (1988), 79–138.

[DdSMS] J. Dixon, A. Mann, D. Segal and M. du Sautoy, *Analytic Pro-p Groups*, London Mathematical Society Lecture Note Series 157, Cambridge University Press, 1991.

[dS] M. du Sautoy, *Finitely generated groups, p-adic analytic groups, and Poincaré series*, Bulletin of the American Mathematical Society **23** (1990), 121–126.

[dS2] M. du Sautoy, *Finitely generated groups, p-adic analytic groups, and Poincaré series*, Annals of Mathematics **137** (1993), 639–670.

[dS3] M. du Sautoy, *Zeta functions of groups and rings: uniformity*, Israel Journal of Mathematics **86** (1994), 1–23.

[GSS] F. J. Grunewald, D. Segal and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Inventiones Mathematicae **93** (1988), 185–223.

[H] P. Hall, *On a theorem of Frobenius*, Proceedings of the London Mathematical Society (2) **40** (1936), 468–499. Also in *Collected Works of P. Hall*, Oxford University Press, Oxford, 1988, pp. 129–160.

[I] I. Ilani, *Analytic pro-p groups and their Lie algebras*, Journal of Algebra **176** (1995), 34–58.

[J] N. Jacobson, *Lie Algebras*, Dover Publications, New York, 1979.

[L] M. Lazard, *Groupes analytiques p-adiques*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **26** (1965), 389–603.

[LdS] A. Lubotzky and M. du Sautoy, personal communication.

[LM] A. Lubotzky and A. Mann, *Powerful p-groups I*, Journal of Algebra **105** (1987), 484–505.

[LMS] A. Lubotzky, A. Mann and D. Segal, *Finitely generated groups of polynomial subgroup growth*, Israel Journal of Mathematics **82** (1993), 363–371.

[M] A. Mann, *The power structure of p-groups I*, Journal of Algebra **42** (1976), 121–135.

[Mc] A. Macintyre, *Rationality of p-adic Poincaré series: uniformity in p*, Annals of Pure and Applied Logic **49** (1990), 31–74.

[MKS] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Interscience Publishers, New York, 1966.

[Sr] J.-P. Serre, *Lie Algebras and Lie Groups*, W. A. Benjamin, New York, 1965.