A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups.

Marcus du Sautoy
DPMMS
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB
dusautoy@dpmms.cam.ac.uk
http://www.dpmms.cam.ac.uk/~dusautoy

August 10, 2000

1 Introduction

Grunewald, Segal and Smith introduced the notion of the zeta function of a group G in [8]:

$$\zeta_G^{\leq}(s) = \sum_{H \leq G} |G : H|^{-s} = \sum_{n=1}^{\infty} a_n^{\leq}(G) n^{-s}$$

where $a_n^{\leq}(G)$ denotes the number of subgroups of index n in G. The definition of this zeta function as a sum over subgroups makes it look like a non-commutative version of the Dedekind zeta function of a number field. They proved that for finitely generated, torsion-free nilpotent groups the global zeta function can be written as an Euler product of local factors which are rational functions in p^{-s} :

$$\begin{aligned}\zeta_G^{\leq}(s) &= \prod_{p \text{ prime}} \zeta_{G,p}^{\leq}(s) \\ &= \prod_{p \text{ prime}} Z_p^{\leq}(p, p^{-s})\end{aligned}$$

where for each prime p, $\zeta_{G,p}^{\leq}(s) = \sum_{n=0}^{\infty} a_{p^n}^{\leq}(G)p^{-ns}$ and $Z_p^{\leq}(X,Y) \in \mathbb{Q}(X,Y)$.

Similar definitions and results were also obtained for the zeta function $\zeta_G^{\triangleleft}(s)$ counting normal subgroups.

One of the major questions raised in the paper [8] is the variation with p of these local factors $Z_p^{\leq}(X,Y)$. Many of the examples showed a uniform behaviour as the prime varied. For example, if G is the discrete Heisenberg group

$$G = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$$

then for all primes p

$$\zeta_{G,p}^{\leq} = \frac{(1-p^{3-3s})}{(1-p^{-s})(1-p^{1-s})(1-p^{2-2s})(1-p^{3-2s})}.$$

However, if one takes the Heisenberg group with entries now from some quadratic number field then it was shown in [8] that the local factors $Z_p^{\triangleleft}(X,Y)$ counting normal subgroups depend on how the prime p behaves in the quadratic number field. The authors of [8] were lead by such examples and the analogy with the Dedekind zeta function of a number field to ask whether the local factors always demonstrated a Cebotarev density type behaviour, depending on the behaviour of primes in number fields. In particular they speculated in [8] that it was 'plausible' that the following question has a positive answer:

Question *Let G be a finitely generated nilpotent group and $* \in \{\leq, \triangleleft\}$. Do there exist finitely many rational functions $W_1(X,Y), \dots, W_r(X,Y) \in \mathbb{Q}(X,Y)$ such that for each prime p there is an i for which*

$$\zeta_{G,p}^{*}(s) = W_i(p, p^{-s})?$$

If the answer is 'yes' we say that the local zeta functions $\zeta_{G,p}^{*}(s)$ of G are *finitely uniform*. If there is one rational function $W(X,Y)$ such that

$\zeta^*_{G,p}(s) = W(p, p^{-s})$ for almost all primes then we say that the local zeta functions $\zeta^*_{G,p}(s)$ of G are *uniform.*

Grunewald, Segal and Smith elevated this question to a conjecture in the case that G is a free nilpotent group. In [8] they confirmed the conjecture in the case that G is a free nilpotent group of class 2. In recent work with Grunewald [6], we have also confirmed the conjecture for the case that G is a two generator free nilpotent group of arbitrary class.

The question of the behaviour of these local factors has gained extra significance in the light of recent work of mine on counting the number $f(p, n)$ of non-isomorphic finite p-groups that exist of order p^n. Higman's PORC conjecture [10] asserts that for fixed n, the number $f(p, n)$ is given by a polynomial in p whose coefficients depend on the residue class of p modulo some fixed integer N, (**P** olynomial **O**n **R**esidue **C**lasses). In [1] and [2] it is explained how this conjecture is directly related to whether certain local zeta functions attached to free nilpotent groups are finitely uniform.

The examples of Grunewald, Segal and Smith hinted that the behaviour of the local factors as one varied the prime would be related to the behaviour of primes in number fields. However recent work [4] and [5] with Grunewald shows that this first impression if misplaced. The behaviour is rather governed by a different question, namely how the number of points $\bmod p$ on a variety varies with p.

In [4] and [5], we show that for each finitely generated nilpotent group G there exists an explicit system of subvarieties E_i $(i \in T,\ T$ finite) of a variety Y defined over $\mathbb{Z}$ and, for each subset I of T, a rational function $W_I(X, Y) \in \mathbb{Q}(X, Y)$ such that for almost all primes p

$$\zeta^*_{G,p}(s) = \sum_{I \subset T} c_I(p) W_I(p, p^{-s})$$

where

$$c_I(p) = \mathrm{card}\{a \in Y(\mathbb{F}_p) : a \in E_i(\mathbb{F}_p) \text{ if and only if } i \in I\}.$$

So the analogy with the Dedekind zeta function of a number field is too simplistic, rather it is the Weil zeta function of an algebraic variety over $\mathbb{Z}$ that offers a better analogy.

In contrast to the behaviour of primes in number fields, the number of points $\bmod p$ on a variety can vary wildly with the prime p and certainly does not have a finitely uniform description.

Example 1.1 *([11], 18.4) Let E be the elliptic curve $E = Y^2 - X^3 + X$. Put*

$$|E(\mathbb{F}_p)| = \left|\left\{(x,y) \in \mathbb{F}_p^2 : y^2 - x^3 + x = 0\right\}\right|.$$

If $p \equiv 3 \pmod 4$ then $|E(\mathbb{F}_p)| = p$. However if $p \equiv 1 \pmod 4$ then

$$|E(\mathbb{F}_p)| = p - 2a,$$

where $p = a^2 + b^2$ and $a + ib \equiv 1 \pmod{(2+2i)}$.

(Note that $|E(\mathbb{F}_p)|$ is one less than the value N_p given in [11], 18.4 since N_p counts the number of points on the projective version of E. This includes one extra point at infinity not counted in the affine coordinates.)

However, despite this theoretical advance which moves the problem into the behaviour of varieties $\bmod p$, it was not clear still whether exotic varieties like elliptic curves could arise in the setting of zeta functions of groups. It might be that the question of Grunewald, Segal and Smith would still have a positive answer since the varieties that arise out of the analysis of myself and Grunewald were always rational where the number of points $\bmod p$ is uniform in p.

The purpose of this paper is to present an example of a nilpotent group G whose zeta function depends on the behaviour $\bmod p$ of the number of points on the elliptic curve $E = Y^2 - X^3 + X$. The group G is a Hirsch length 9, class two nilpotent group given by the following presentation:

$$G = \left\langle \begin{array}{c} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 : [x_1, x_4] = y_3, [x_1, x_5] = y_1, [x_1, x_6] = y_2 \\ [x_2, x_4] = y_1, [x_2, x_5] = y_3, [x_3, x_4] = y_2, [x_3, x_6] = y_1 \end{array} \right\rangle$$

where all other commutators are defined to be 1. To see where the elliptic curve is hiding in this presentation, take the determinant of the 3×3 matrix (a_{ij}) with entries $a_{ij} = [x_i, x_{j+3}]$. The elliptic curve is encoded into the presentation in a manner which offers hope that an arbitrary variety can be realised in a similar fashion. We come back to this question in a future paper. However we content ourselves in this current paper with offering a proof of the following negative answer to the question of Grunewald, Segal and Smith:

Theorem 1.1 *The local zeta functions $\zeta^{\leq}_{G,p}(s)$ and $\zeta^{\triangleleft}_{G,p}(s)$ are not finitely uniform.*

Acknowledgements I should like to thank the Royal Society for support in the form of a University Research Fellowship. I should also like to thank the Max Planck Institut in Bonn where this group flashed into my head one evening and for invaluable conversations with Fritz Grunewald during my time at the MPI.

2 Counting points on elliptic curves

Here we establish the following reduction of Theorem 1.1. In the following two sections we establish that our hypothesis in this Theorem is indeed true.

Theorem 2.1 *Let $* \in \{\leq, \triangleleft\}$. Suppose there exist $N \in \mathbb{N}$ and two polynomials $f_1(X)$ and $f_2(X)$ with $f_2(X) \neq 0$ such that for almost all primes p*

$$a^*_{p^N}(G) = f_1(p) + |E(\mathbb{F}_p)| f_2(p)$$

where $|E(\mathbb{F}_p)| = \left\{(b,c) \in \mathbb{F}_p^2 : b - b^3 + c^2 = 0\right\}$. Then $\zeta^*_{G,p}(s)$ is not finitely uniform.

Proof Suppose that $\zeta^*_{G,p}(s)$ is finitely uniform. Then there are finitely many rational functions $W_1(X,Y), \dots, W_r(X,Y) \in \mathbb{Q}(X,Y)$ such that for every prime number p there is a $j \in \{1, \dots, r\}$ for which

$$\zeta^*_{G,p}(s) = W_j(p, p^{-s}).$$

Each of the $W_j(X,Y)$ can be expanded as a power series in Y with coefficients in $\mathbb{Q}(X)$.

We turn to the description of the number of points $|E(\mathbb{F}_p)|$ given in Example 1.1. Let $\mathcal{P}$ be the set of primes p which satisfy $p \equiv 1 \mod 4$. For every $p \in \mathcal{P}$ choose a_p and b_p such that $p = a_p^2 + b_p^2$ and $a_p + ib_p \equiv 1$ (mod $(2+2i)$) and put $\pi_p = a_p + b_p i \in \mathbb{Z}[i]$.

We shall deduce from the assumption that the $\zeta^*_{G,p}(s)$ are finitely uniform the statement:

(A) *There are finitely many $c_1, \dots, c_l \in \mathbb{Z}$ such that for every $p \in \mathcal{P}$ there is a $j \in \{1, \dots, l\}$ with $a_p = c_j$.*

Then we shall show that **(A)** contradicts a theorem of E. Hecke [9].

Assume that $W(X,Y)$ is one of the $W_1(X,Y),\dots,W_r(X,Y)$ such that the set $\mathcal{P}_0$ of those $p \in \mathcal{P}$ with

$$\zeta^*_{G,p}(s) = W(p, p^{-s})$$

is infinite. Then there is a rational function $R_N(X) \in \mathbb{Q}(X)$ such that

$$R_N(p) = a^*_{p^N}(G) = f_1(p) + |E(\mathbb{F}_p)| f_2(p)$$

for all $p \in \mathcal{P}_0$. Since $f_2(X)$ is a non-zero polynomial, this implies then that there is a rational function $R(X) \in \mathbb{Q}(X)$ such that

$$R(p) = |E(\mathbb{F}_p)|$$

for all $p \in \mathcal{P}_0$. Write now

$$R(X) = \frac{S(X)}{T(X)}$$

with $S(X)$ and $T(X) \in \mathbb{Z}[X]$ chosen such that they are coprime elements of $\mathbb{Q}[X]$. Choose $M \in \mathbb{N}$, $L_1(X)$ and $L_2(X) \in \mathbb{Z}[X]$ with

$$L_1(X)S(X) + L_2(X)T(X) = M.$$

For $p \in \mathcal{P}_0$ the value $R(p)$ is an integer, hence $T(p)$ divides $S(p)$. This implies that $T(p)$ divides M. Since $\mathcal{P}_0$ is infinite $T(X)$ then has to be a constant. From Example 1.1 for $p \in \mathcal{P}$, $|E(\mathbb{F}_p)| = p - 2a_p$. Hence there is a polynomial $\widetilde{R(X)} \in \mathbb{Q}(X)$ such that

$$\widetilde{R(p)} = 2a_p$$

for all $p \in \mathcal{P}_0$. Now $\pi_p \cdot \overline{\pi_p} = p$ and $\pi_p + \overline{\pi_p} = 2a_p$. These imply

$$\pi_p^2 - \widetilde{R(p)}\pi_p + p = 0.$$

Hence π_p is one of the two complex numbers

$$\widetilde{R(p)}/2 \pm \sqrt{\widetilde{R(p)}^2/4 - p}.$$

Since π_p cannot be real we get

$$4p > \widetilde{R(p)}^2$$

for all $p \in \mathcal{P}_0$. This implies that $\widetilde{R(X)}$ is constant. In fact $\widetilde{R(X)} \in 2\mathbb{Z}$. This proves **(A)**.

Let us consider the implications of **(A)**. We associate to every $z \in \mathbb{C}$ with $z \neq 0$ the number

$$a(z) := \frac{z}{|z|} \in S^1 \subset \mathbb{C}.$$

By the main result of Chapter 9 in [9] we find that the set $\{a(\pi_p) : p \in \mathcal{P}\}$ is dense in S^1. In fact Hecke proves that

$$|\{p \in \mathcal{P} : p \leq T, a(\pi_p) \in J(\delta)\}| \sim \frac{\delta}{4\pi} \cdot \frac{T}{\log T} \tag{1}$$

where $J = J(\delta)$ is any segment of length $\delta > 0$ on S^1.

From **(A)** we infer by an elementary geometric argument that there is a segment $J = J(\delta)$ of length $\delta > 0$ on S^1 such that

$$\{p \in \mathcal{P} : p \leq T, a(\pi_p) \in J(\delta)\} = \emptyset.$$

(Consider the lines in $\mathbb{C}$ of constant real part $c_1, \ldots, c_l$.) This contradiction proves Theorem 2.1.□

Remark Given any elliptic curve E defined over $\mathbb{Q}$ and a prime p so that the reduction $\overline{E}$ modulo p is again an ellitpic curve, the number N_p of points on $\overline{E}$ over $\mathbb{F}_p$ can always be written as

$$N_p - p - 1 = -\pi_p - \overline{\pi_p}$$

where $\pi_p \in \mathbb{C}$ satisfies $\pi_p \cdot \overline{\pi_p} = p$. (Note that N_p counts the number of points on the projective curve which includes a point at infinity.) If E has complex multiplication then the density of the set of angles $a(\pi_p)$ (p a prime of good reduction for E) in S^1 can always be deduced from the more general distribution law analogous to (1) proved by Hecke. If E doesn't have complex multiplication then the $a(\pi_p)$ are conjectured to satisfy the Sato-Tate distribution law. This law is different from (1) but also implies the density of the angles. Unfortunately it isn't proved for a single elliptic curve E.

3 Counting normal subgroups

To prove Theorem 1.1 for the local zeta functions counting normal subgroups it suffices, by Theorem 2.1, to prove that there exist two polynomials $f_1(X)$ and $f_2(X)$ with $f_2(X) \neq 0$ such that for almost all primes p

$$a^{\triangleleft}_{p^5}(G) = f_1(p) + |E(\mathbb{F}_p)| f_2(p)$$

where $|E(\mathbb{F}_p)| = \left\{(b,c) \in \mathbb{F}_p^2 : b - b^3 + c^2 = 0\right\}$.

We begin by linearizing the problem and moving to the associated Lie algebra of G. Let L be the class two nilpotent Lie algebra over $\mathbb{Z}$ of dimension 9 defined as a free $\mathbb{Z}$-module given by the following presentation:

$$L = \left\langle \begin{array}{c} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 : (x_1, x_4) = y_3, (x_1, x_5) = y_1, (x_1, x_6) = y_2 \\ (x_2, x_4) = y_1, (x_2, x_5) = y_3, (x_3, x_4) = y_2, (x_3, x_6) = y_1 \end{array} \right\rangle$$

where all other commutators are defined to be 0. Then $L \otimes \mathbb{Q}$ is the $\mathbb{Q}$-Lie algebra associated to the torsion-free finitely generated nilpotent group G under the Mal'cev correspondence. We can define zeta functions associated to L similarly to those associated to G :

$$\zeta^*_{L,p}(s) = \sum_{n=0}^{\infty} a^*_{p^n}(L) p^{-ns}$$

where $* \in \{\leq, \triangleleft\}$ and $a^{\leq}_{p^n}(L)$ is the number of subalgebras of L of index p^n and $a^{\triangleleft}_{p^n}(L)$ is the number of ideals of L of index p^n. Section 4 of [8] confirms the following:

Proposition 3.1 *For almost all primes p,*

$$\zeta^*_{G,p}(s) = \zeta^*_{L,p}(s).$$

There is a one-to-one correspondence between additive subgroups of L of index p^n and integer triangular matrices $(m_{ij})_{1 \leq i \leq j \leq 9}$ satisfying (1) $0 \leq m_{ij} < m_{jj}$ and (2) $m_{11} \dots m_{99} = p^n$. The correspondence is defined by $(m_{ij}) \mapsto$ additive span of $\mathbf{m}_i$ $(i = 1, \dots, 9)$ where

$$\begin{aligned} \mathbf{m}_i &= m_{ii}x_i + \cdots + m_{i6}x_6 + m_{i7}y_1 + m_{i8}y_2 + m_{i9}y_3 \text{ for } i = 1, \dots, 6 \\ \mathbf{m}_7 &= m_{77}y_1 + m_{78}y_2 + m_{79}y_3 \\ \mathbf{m}_8 &= m_{88}y_2 + m_{89}y_3 \\ \mathbf{m}_9 &= m_{99}y_3 \end{aligned}$$

To count the number of ideals of index p^n we must count the number of such matrices which define basis for ideals rather than just additive subgroups.

Let

$$\begin{aligned} C(1) &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ C(2) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \\ C(3) &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Then for $i, j = 1, 2, 3$ we have

$$\begin{aligned} (x_i, x_{j+3}) &= C_{i1}(j)y_1 + C_{i2}(j)y_2 + C_{i3}(j)y_3 \\ &= C_{j1}(i)y_1 + C_{j2}(i)y_2 + C_{j3}(i)y_3 \end{aligned}$$

To count the number of ideals of index p^5, it suffices to count how many matrices there are of the form

$$\left((m_{ij})_{1 \le i \le j \le 6}, \begin{pmatrix} n_1 & a & b \\ & n_2 & c \\ & & n_3 \end{pmatrix} \right)$$

where

(A) $m_{ij}, n_{ij} \in \mathbb{Z}$;

(B) $m_{ii} = p^{a_i}, n_i = p^{b_i}$ and $a_1 + \cdots + a_6 + b_1 + b_2 + b_3 = 5$;

(C) $0 \le m_{ij} < m_{jj}$, $0 \le a < n_2, 0 \le b, c < n_3$;

(D) for $i = 1, \ldots, 6, \epsilon = 0$ or 3 and $j = 1, 2, 3$ there exists $\left(\lambda^j_{i\varepsilon+1}, \lambda^j_{i\varepsilon+2}, \lambda^j_{i\varepsilon+3}\right) \in \mathbb{Z}_p^3$ such that

$$(m_{i\varepsilon+1}, m_{i\varepsilon+2}, m_{i\varepsilon+3})\, C(j) N^{\dagger} = \left(\lambda^j_{i\varepsilon+1} n_1 n_2 n_3, \lambda^j_{i\varepsilon+2} n_1 n_2 n_3, \lambda^j_{i\varepsilon+3} n_1 n_2 n_3\right)$$

where $N^{\dagger}$ is the adjoint matrix

$$N^{\dagger} = \begin{pmatrix} n_2 n_3 & -a n_3 & ac - n_2 b \\ 0 & n_3 n_1 & -c n_1 \\ 0 & 0 & n_1 n_2 \end{pmatrix}.$$

That condition (D) is equivalent to the statement that the associated matrix defines an ideal can be found in section 5 of [5].

Define $c_{\mathbf{a},\mathbf{b}}$ to be the number of matrices with $(\mathbf{a},\mathbf{b}) = (a_1,\dots,a_6,b_1,b_2,b_3)$ fixed and $a_1+\cdots+a_6+b_1+b_2+b_3=5$. Then

$$a^{\triangleleft}_{p^5} = \sum_{\mathbf{a},\mathbf{b}} p^{6(b_1+b_2+b_3)} c_{\mathbf{a},\mathbf{b}}.$$

Theorem 3.2 *$c_{\mathbf{a},\mathbf{b}}$ is given by a polynomial in p except for one case where $(\mathbf{a},\mathbf{b}) = (0,1,1,0,1,1,0,0,1)$ in which case*

$$c_{\mathbf{a},\mathbf{b}} = (|E(\mathbb{F}_p)| - 1).$$

Proof There is one easy case when $(b_1,b_2,b_3) = (0,0,0)$. There are then no conditions arising from (D) and it is just a matter of counting the number of matrices $(m_{ij})_{1\le i\le j\le 6}$ for the various cases of a_i. This is given then by a polynomial in p.

So we may assume that there is at least one p distributed amongst the n_i.

The following lemma forces some of the distribution of the p's:

Lemma 3.3 *(1)* $a_2, a_5 \ge b_3$;
(2) $a_2, a_5 \ge b_1$;
(3) $a_1, a_4 \ge b_1$; *and*
(4) $a_3, a_6 \ge b_2, b_1$.

Proof (1) follows from

$$(p^{a_2}x_2 + m_{23}x_3, x_5) = p^{a_2}y_3$$

hence $a_2 \ge b_3$. Similarly symmetry implies that $a_5 \ge b_3$.

For (2) consider

$$(p^{a_2}x_2 + m_{23}x_3, x_4) = p^{a_2}y_1 + m_{23}y_2$$

which implies $a_2 \ge b_1$; and similarly $a_5 \ge b_1$.

For (3) we have

$$(p^{a_1}x_1 + m_{12}x_2 + m_{13}x_3, x_5) = p^{a_1}y_1 + m_{12}y_3$$

which implies $a_1 \geq b_1$; and similarly $a_4 \geq b_1$.

Considering $(p^{a_3}x_3, x_i)$ and $(p^{a_6}x_6, x_i)$ implies that $a_3, a_6 \geq b_2, b_1$ giving (4). $\square$

This forces already $b_1 = 0$ if we only have five p to distribute.

Suppose $b_3 = 0$ which implies that $c = b = 0$.

Lemma 3.4 *If* $\mathbf{b} = (0, b_2, 0)$ *and* $b_2 > 0$ *then* $c_{\mathbf{a},\mathbf{b}} = 0$ *unless* $\mathbf{a} = (1,0,1,1,0,1)$ *in which case* $c_{\mathbf{a},\mathbf{b}} = 1$.

Proof Note that $a_3, a_6 \geq b_2 \geq 1$ in this case and hence $b_2 = 1$. Since $b_3 = 0$ the conditions in (D) just reduce to solving $(m_{i\varepsilon+1}, m_{i\varepsilon+2}, m_{i\varepsilon+3})$ satisfying

$$\begin{aligned}
(m_{i\varepsilon+2}, m_{i\varepsilon+3}) \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} &= (\lambda^1_{i\varepsilon+1}, \lambda^1_{i\varepsilon+2}p) \\
(m_{i\varepsilon+1}, 0) \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} &= (\lambda^2_{i\varepsilon+1}, \lambda^2_{i\varepsilon+2}p) \\
(m_{i\varepsilon+3}, m_{i\varepsilon+1}) \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} &= (\lambda^3_{i\varepsilon+1}, \lambda^3_{i\varepsilon+2}p)
\end{aligned}$$

If $a = 0$ these conditions force $m_{i\varepsilon+1} = 0 = m_{i\varepsilon+3} \mod p$. Hence $(a_1, \ldots, a_6) = (1,0,1,1,0,1)$ and all entries above the diagonal in (m_{ij}) must be zero. For $1 \leq a \leq p-1$ we get that $m_{i\varepsilon+j} = 0 \mod p$ for $j = 1,2,3$. This is not possible given that $a_1 + \cdots + a_6 \leq 4$. $\square$

Note that we can't have $b_3, b_2 \geq 1$ since $a_3, a_6 \geq b_2$ and $a_1, a_5 \geq b_3$.

Hence we are left with the case of $(0,0,b_3)$ and $b_3 \geq 1$.

Lemma 3.5 *If* $\mathbf{b} = (0,0,b_3)$ *and* $b_3 \geq 1$ *then* $c_{\mathbf{a},\mathbf{b}}$ *is polynomial in* p *unless* $\mathbf{a} = (0,1,1,1,0,1,1)$ *in which case*

$$c_{\mathbf{a},\mathbf{b}} = (|E(\mathbb{F}_p)| - 1)\,.$$

Proof We know that $a_2, a_5 \geq b_3$ so again this forces $b_3 = 1$. So (D) reduces to the following

$$\begin{aligned}
-m_{i\varepsilon+2}b - m_{i\varepsilon+3}c + m_{i\varepsilon+1} &= \lambda^1_{i\varepsilon+3}p && (2)\\
-m_{i\varepsilon+1}b + m_{i\varepsilon+2} &= \lambda^2_{i\varepsilon+3}p && (3)\\
-m_{i\varepsilon+3}b - m_{i\varepsilon+1}c &= \lambda^3_{i\varepsilon+3}p. && (4)
\end{aligned}$$

Considering $i=3$ and 6 gives us that either $m_{33}=m_{66}=p$ or $b=0=c$. Suppose we are in the second case. Then the conditions reduce to $m_{i\varepsilon+1}=0=m_{i\varepsilon+2} \mod p$. This gives a polynomial expression in p.

So we may suppose finally that one of b or c is non-zero. In which case $(a_1,\dots,a_6)=(0,1,1,0,1,1)$.

Consider firstly $i=1$ and $\varepsilon=0$. If $b=0$ then since $m_{11}=1$ equation (4) implies $c=0$ but this contradicts (2). So we may assume $b\neq 0$. Then we get a solution if and only if $1=b^2-c^2/b \mod p$ and then m_{12} and m_{13} are determined. The same applies for $i=4$ and $\varepsilon=3$.

Consider next $i=1,2,3$ and $\varepsilon=3$. We have the following system

$$\begin{aligned}-m_{i5}b-m_{i6}c &= \lambda^1_{i\varepsilon+3}p\\ m_{i5} &= \lambda^2_{i\varepsilon+3}p\\ -m_{i6}b &= \lambda^3_{i\varepsilon+3}p.\end{aligned}$$

This implies then that $m_{i5}=m_{i6}=0$.

Finally we must consider $i=2$, $\varepsilon=0$ and $i=5,\varepsilon=3$. This case reduces to

$$\begin{aligned}-pb-m_{i\varepsilon+3}c &= \lambda^1_{i\varepsilon+3}p\\ -m_{i\varepsilon+3}b &= \lambda^3_{i\varepsilon+3}p.\end{aligned}$$

This again implies that $m_{i\varepsilon+3}=0$. Hence once (b,c) is a non-zero point on the elliptic curve the matrix (m_{ij}) is determined. Hence when $(\mathbf{a},\mathbf{b})=(0,1,1,0,1,1,0,0,1)$ we get

$$c_{\mathbf{a},\mathbf{b}}=(|E(\mathbb{F}_p)|-1)\,.$$

□

Lemmas 3.4 and 3.5 suffice to prove Theorem 3.2 and hence confirm a negative answer for the question of Grunewald, Segal and Smith in the case of normal subgroups.

Corollary 3.6 *The local zeta functions $\zeta^{\triangleleft}_{G,p}(s)$ of G are not finitely uniform.*

4 Counting Subgroups

To settle the question of counting all subgroups it is sufficient to consider the subgroups of index p^3.

We have to count how many matrices there are of the form

$$\left((m_{ij})_{1\leq i\leq j\leq 6}\,, \begin{pmatrix} n_1 & a & b \\ & n_2 & c \\ & & n_3 \end{pmatrix} \right)$$

where

(A) $m_{ij}, n_{ij} \in \mathbb{Z}$;
(B) $m_{ii} = p^{a_i}, n_i = p^{b_i}$ and $a_1 + \cdots + a_6 + b_1 + b_2 + b_3 = 3$;
(C) $0 \leq m_{ij} < m_{jj}$, $0 \leq a < n_2, 0 \leq b, c < n_3$;
(D) for $i < j \in \{1, \ldots, 6\}$, there exists $\left(\lambda_{ij}^1, \lambda_{ij}^2, \lambda_{ij}^3\right) \in \mathbb{Z}_p^3$ such that

$$(m_{ii}, \ldots, m_{i6}) \left(\sum_{l=j}^{6} m_{jl} D(l) \right) N^{\dagger} = \left(\lambda_{ij}^1 n_1 n_2 n_3, \lambda_{ij}^2 n_1 n_2 n_3, \lambda_{ij}^3 n_1 n_2 n_3 \right)$$

where $N^{\dagger}$ is the adjoint matrix

$$N^{\dagger} = \begin{pmatrix} n_2 n_3 & -a n_3 & ac - n_2 b \\ 0 & n_3 n_1 & -c n_1 \\ 0 & 0 & n_1 n_2 \end{pmatrix}$$

and

$$\begin{aligned} D(l) &= \begin{pmatrix} -C(l) \\ 0 \end{pmatrix} \text{if } l = 1, 2, 3 \\ D(l) &= \begin{pmatrix} 0 \\ C(l-3) \end{pmatrix} \text{if } l = 4, 5, 6 \end{aligned}$$

That condition (D) is equivalent to the statement that the associated matrix defines a subalgebra can be found in section 5 of [5].

Define $c_{\mathbf{a},\mathbf{b}}$ to be the number of matrices with $(\mathbf{a}, \mathbf{b}) = (a_1, \ldots, a_6, b_1, b_2, b_3)$ fixed and $a_1 + \cdots + a_6 + b_1 + b_2 + b_3 = 3$. Then

$$a_{p^3}^{\leq} = \sum_{\mathbf{a},\mathbf{b}} p^{6(b_1+b_2+b_3)} c_{\mathbf{a},\mathbf{b}}.$$

We prove the following which is sufficient to prove that the local zeta functions $\zeta_{G,p}^{\leq}(s)$ of G are not finitely uniform:

Theorem 4.1 *$c_{\mathbf{a},\mathbf{b}}$ is given by a polynomial in p except for the following cases*

(1) $(\mathbf{a},\mathbf{b}) = (0,1,1,0,0,0,0,0,1)$ *in which case*

$$c_{\mathbf{a},\mathbf{b}} = \left(|E(\mathbb{F}_p)| - 1\right).$$

(2) $(\mathbf{a},\mathbf{b}) = (0,0,0,0,1,1,0,0,1)$ *in which case*

$$c_{\mathbf{a},\mathbf{b}} = p^6\left(|E(\mathbb{F}_p)| - 1\right).$$

(3) $(\mathbf{a},\mathbf{b}) = (0,0,1,0,1,0,0,0,1)$ *and* $(0,1,0,0,0,1,0,0,1)$ *in which case*

$$c_{\mathbf{a},\mathbf{b}} = p\left(|E(\mathbb{F}_p)| - 1\right).$$

(4) $(\mathbf{a},\mathbf{b}) = (0,0,1,0,0,1,0,0,1)$ *in which case*

$$c_{\mathbf{a},\mathbf{b}} = p\left(|A(\mathbb{F}_p)|\right)$$

where $|A(\mathbb{F}_p)|$ is the number of triples $(a,b,c) \in \mathbb{F}_p^3$ with a, b non-zero satisfying

$$a(b + c^2 - b^3) + cb(1-b) = 0.$$

(Note that this can still be expressed as a Boolean combination of points on E and various affine lines.)

Proof As before the case of $(b_1, b_2, b_3) = (0,0,0)$ is straightforward. There are then no conditions arising from (D) and it is just a matter of counting the number of matrices $(m_{ij})_{1\le i\le j\le 6}$ for the various cases of a_i. This is given then by a polynomial in p.

Lemma 4.2 *If $(b_1, b_2, b_3) = (b_1, 0, 0)$ with $b_1 > 0$ then $c_{\mathbf{a},\mathbf{b}}$ is polynomial in p.*

Proof Condition (D) reduces to $1 \le i < j \le 6$

$$p^{b_1} | \left(m_{i1}m_{j5} + m_{i2}m_{j4} - m_{i4}m_{j2} + m_{i3}m_{j6} - m_{i6}m_{j3}\right).$$

We list a number of these where the equation is indexed by the choice of (i, j)

$$p^{b_1}|m_{33}m_{66} \tag{3,6}$$
$$p^{b_1}|m_{22}m_{44} + m_{23}m_{46} \tag{2,4}$$
$$p^{b_1}|m_{11}m_{55} + m_{13}m_{56} \tag{1,5}$$
$$p^{b_1}|m_{33}m_{46} \tag{3,4}$$
$$p^{b_1}|m_{33}m_{56} \tag{3,5}$$

If $m_{66} = 1$ then $m_{56} = m_{46} = 0$ and the first three equations imply that there are too many p's to have to distribute. So $m_{66} = p$ or p^2. But the same argument implies that at least one of m_{56} or m_{46} must be prime to p in which case the last two equations imply $m_{33} = p$ and $m_{66} = p$. So if $b_2 = b_3 = 0$ then the only case where we get something to count is for $(\mathbf{a}, \mathbf{b}) = (0, 0, 1, 0, 0, 1, 1, 0, 0)$.

Condition (D) then reduces to the following:

$$\begin{aligned} & p|\left(1 + m_{13}m_{56}\right) \\ m_{36} &= m_{46} = m_{23} = 0. \end{aligned}$$

The matrices satisfying this condition are clearly given by a polynomial in p. □

Note that the above implies that in general if $b_1 > 0$ then $a_3 = a_6 = b_1 = 1$. So we suppose now that $b_1 = 0$.

Lemma 4.3 *If $\mathbf{b} = (0, b_2, 0)$ with $b_2 > 0$ then $c_{\mathbf{a},\mathbf{b}}$ is polynomial in p.*

Proof Condition (D) becomes now that for $1 \leq i < j \leq 6$

$$p^{b_2}|m_{i1}m_{j6} + m_{i3}m_{j4} - m_{i4}m_{j3} - a\left(m_{i1}m_{j5} + m_{i2}m_{j4} - m_{i4}m_{j2} + m_{i3}m_{j6} - m_{i6}m_{j3}\right).$$

If $a = 0$ then we have, taking $(i, j) = (1, 6)$ and $(3, 4)$

$$\begin{aligned} & p^{b_2}|m_{11}m_{66} \\ & p^{b_2}|m_{33}m_{44} \end{aligned}$$

This means that at least one of the columns above m_{33} or m_{44} contains zeros. Hence condition (D) reduces to

$$\begin{aligned} & p^{b_2}|m_{11}m_{j6} \\ & p^{b_2}|m_{33}m_{44}. \end{aligned}$$

This is polynomial in p.

Suppose now that $a \neq 0$.

Taking $(i,j) = (3,6)$ gives us that $p^{b_2}|m_{33}m_{66}$. So again this implies $b_2 = 1$. So we have two p to distribute and at least one must be at m_{33} or m_{66}.

Suppose $m_{33} = 1$ which means that $m_{i3} = 0$. Then:

$$p| - am_{33}m_{56} \tag{3,5}$$
$$p|m_{11}m_{56} - am_{11}m_{55} \tag{1,5}$$

This implies then that $p|m_{11}m_{55}$. But taking $(i,j) = (2,4)$ we get $p|m_{22}m_{44}$. Hence again we have too many p's.

So we may suppose $m_{33} = p$ or p^2.

Suppose $m_{66} = 1$. Then $(i,j) = (2,6)$ gives $p| - am_{23}m_{66}$, i.e. $m_{23} = 0$. Applying this now to $(i,j) = (2,4)$ implies $p|m_{22}m_{44}$. But $(i,j) = (1,5)$ implies that $p| - am_{11}m_{55}$ since $m_{56} = 0$. This gives a contradiction since we only have one p to distribute amongst $m_{11}, m_{22}, m_{44}, m_{55}$.

So we are only left with the case that $(\mathbf{a}, \mathbf{b}) = (0,0,1,0,0,1,0,1,0)$. The condition (D) reduces then to the following conditions on m_{i3}, and m_{i6} :

$$p|m_{26} - a(m_{13}m_{26} - m_{16}m_{23}) \tag{1,2}$$
$$p|m_{36} - a(m_{13}m_{36}) \tag{1,3}$$
$$p|m_{46} + m_{13} - a(m_{13}m_{46}) \tag{1,4}$$
$$p|m_{56} - a(1 + m_{13}m_{56}) \tag{1,5}$$
$$p|am_{23}m_{36} \tag{2,3}$$
$$p|m_{23} - a(1 + m_{23}m_{46}) \tag{2,4}$$
$$p|am_{23}m_{56} \tag{2,5}$$

(1,5) and (2,4) imply that $m_{56} \neq 0$ and $m_{23} \neq 0$. But since $a \neq 0$ this contradicts $(2,5)$. Hence we have no solutions when $a \neq 0$. $\square$

Note that the above analysis also showed that with at least one p at b_2 there have to be two p's amongst the m_{ii}. Hence b_3 is forced to be 0.

Finally we come to the analysis which will provide us with something depending on the number of points on the elliptic curve E. We have $\mathbf{b} = (0,0,b_3)$. The condition (D) becomes now:

$$p^{b_3}|m_{i1}m_{j4} + m_{i2}m_{j5} - m_{i5}m_{j2} - c\left(m_{i1}m_{j6} + m_{i3}m_{j4} - m_{i4}m_{j3}\right)$$
$$-b\left(m_{i1}m_{j5} + m_{i2}m_{j4} - m_{i4}m_{j2} + m_{i3}m_{j6} - m_{i6}m_{j3}\right).$$

Lemma 4.4 *If* $(\mathbf{a},\mathbf{b}) = (0,1,1,0,0,0,0,0,1)$ *then* $c_{\mathbf{a},\mathbf{b}} = (|E(\mathbb{F}_p)| - 1)$.

Proof We only need to consider $i \in \{1,2,3\}$ and $j \in \{4,5,6\}$. The conditions reduce to the following:

$$\begin{aligned}
&p|1 - cm_{13} - bm_{12} && (1,4)\\
&p|m_{12} - b && (1,5)\\
&p| - c + bm_{13} && (1,6)\\
&p|cm_{23} - b && (2,4)\\
&p| - bm_{23} && (2,6)
\end{aligned}$$

If $b = 0$ we get that $c = 0$ and hence there are no solutions by (1,4). So suppose $b \neq 0$. Then $m_{23} = 0$ and for every value of (b,c) on the elliptic curve we get a unique solution for m_{12} and m_{13}. Hence $c_{\mathbf{a},\mathbf{b}} = (|E(\mathbb{F}_p)| - 1)$.□

Lemma 4.5 *If* $(\mathbf{a},\mathbf{b}) = (0,0,0,0,1,1,0,0,1)$ *then* $c_{\mathbf{a},\mathbf{b}} = (|E(\mathbb{F}_p)| - 1)\, p^6$.

Proof Condition (D) reduces to the following:

$$\begin{aligned}
&p|m_{24} - m_{15} - cm_{26} - b(m_{25} - m_{14}) && (1,2)\\
&p|m_{34} - c(m_{36} - m_{14}) - b(m_{35} - m_{16}) && (1,3)\\
&p|1 - cm_{46} - bm_{45} && (1,4)\\
&p| - cm_{56} && (1,5)\\
&p|m_{35} + cm_{24} - b(m_{34} - m_{26}) && (2,3)\\
&p|m_{45} - b && (2,4)\\
&p| - c - bm_{46} && (3,4)\\
&p| - bm_{56} && (3,5)
\end{aligned}$$

Conditions (1,2), (1,3) and (2,3) determine the values of m_{24}, m_{34} and m_{35} respectively once everything else is chosen. The same analysis as before deals with the other equations and we get that $c_{\mathbf{a},\mathbf{b}} = (|E(\mathbb{F}_p)| - 1)\, p^6$. □

Lemma 4.6 *If* $(\mathbf{a},\mathbf{b}) = (a_1, a_2, 0, a_4, a_5, 0, 0, 0, b_3)$ *then* $c_{\mathbf{a},\mathbf{b}}$ *is polynomial in* p.

Proof (2,6) gives us $p^{b_3}|bm_{33}m_{66}$. Hence if there are no p's at a_3 or a_6 then $b = 0$ and $b_3 = 1$.

(2,5) gives us the following

$$p^{b_3}|m_{22}m_{55} - bm_{23}m_{56} = m_{22}m_{55}.$$

Hence one p must be at a_2 or a_5.

Consideration of (1,6) and (3,4) imply that $p|-cm_{11}m_{66}$ and $p|-cm_{33}m_{44}$. Hence $c = 0$ too since we only have one p to distribute. Then the condition (D) reduces just to

$$p^{b_3}|m_{i1}m_{j4} + m_{i2}m_{j5} - m_{i5}m_{j2}$$

Consideration of (1,4) implies that one p must be at a_4 or a_1. Hence at least one of the columns above m_{22} or m_{55} contains zeros. So condition (D) becomes

$$p|m_{11}m_{24} - m_{15}m_{22} \tag{1,2}$$
$$p|m_{11}m_{34} \tag{1,3}$$
$$p|m_{12}m_{55} \tag{1,5}$$
$$p|m_{22}m_{35} \tag{2,3}$$
$$p|m_{22}m_{45} \tag{2,4}$$
$$p|m_{22}m_{55}. \tag{2,5}$$

These conditions result in polynomial conditions on m_{ij}. □

Suppose now that one p is at a_3 or a_6. Then $b \neq 0$. Otherwise the analysis of the proof of the above lemma implies that another p must be at a_2 or a_5 (by (2,5)), that $c = 0$ and consequently a further p must be at a_4 or a_1 (by (1,4)) which exceeds the number of p we have to distribute.

Lemma 4.7 *If* $(\mathbf{a}, \mathbf{b}) = (0, 0, 1, 0, 0, 1, 0, 0, 1)$ *then*

$$c_{\mathbf{a},\mathbf{b}} = p\left(p^2 - |E(\mathbb{F}_p)| + 2\right).$$

Proof Condition (D) becomes:

$$p| - cm_{26} - b(m_{13}m_{26} - m_{16}m_{23}) \tag{1,2}$$
$$p| - cm_{36} - bm_{13}m_{36} \tag{1,3}$$
$$p|1 - c(m_{46} + m_{13}) - bm_{13}m_{46} \tag{1,4}$$
$$p| - cm_{56} - b(1 + m_{13}m_{56}) \tag{1,5}$$
$$p| - bm_{23}m_{36} \tag{2,3}$$
$$p| - cm_{23} - b(1 + m_{23}m_{46}) \tag{2,4}$$
$$p|1 - bm_{23}m_{56} \tag{2,5}$$

(2,5) implies that b, m_{23}, m_{56} are all non-zero and

$$m_{56} = 1/bm_{23} \mod p.$$

Given a non-zero value of m_{23} then (1,2) determines the value of m_{16} and (2,3) implies that $m_{36} = 0$ which in turn implies that (1,3) is satisfied. The interest comes in combining (1,4), (1,5), (2,4) and (2,5). Given m_{23} non-zero then we have determined the value of m_{56}, similarly we get:

$$\begin{aligned} m_{13} &= -c - bm_{23} \mod p \\ m_{46} &= -c/b - 1/m_{23} \mod p \end{aligned}$$

However we are then left with the following condition on m_{23} coming from (1,4) that m_{23} must be a solution $\mod p$ to the following equation:

$$m_{23}(b + c^2 - b^3) + cb(1 - b) = 0.$$

Recall that m_{23} and b are non-zero. If $b + c^2 - b^3 = 0$ then either (i) $c = 0$ or (ii) $b = 1$. In case (i) since $b + c^2 - b^3 = 0$, $b = 1$ or -1. Hence we get a contribution of $2(p - 1)$. In case (ii) $c = 0$ and we get a contribution of $(p - 1)$.

If $b + c^2 - b^3 \neq 0$, then to ensure that the solution for m_{23} is non-zero we must insist that $b \neq 0$ or $b \neq 1$ or $c \neq 0$. So we must remove also $(0, c)$ $c \neq 0$, $(1, c)$ $c \neq 0$, and $(b, 0)$ where $b \neq -1, 0, 1$. Hence this case contributes

$$p^2 - |E(\mathbb{F}_p)| - 2(p - 1) - (p - 3).$$

Hence for $(\mathbf{a}, \mathbf{b}) = (0, 0, 1, 0, 0, 1, 0, 0, 1)$ we have

$$c_{\mathbf{a},\mathbf{b}} = p\left(p^2 - |E(\mathbb{F}_p)| + 2\right).$$

The p on the outside comes from the fact that m_{26} is free. $\square$

We are left with distributing at most one p amongst a_3 and a_6. Hence one of m_{23} or m_{56} must be zero. This implies that the other p must then be given to a_2 or a_5 since (2,5) implies that

$$p^{b_3} | m_{22}m_{55} - bm_{23}m_{56} = m_{22}m_{55}.$$

We have done the cases of $(a_2, a_3) = (1, 1)$ and $(a_5, a_6) = (1, 1)$. This leaves us with two cases.

Lemma 4.8 *If* $(\mathbf{a}, \mathbf{b}) = (0,1,0,0,0,1,0,0,1)$ *then* $c_{\mathbf{a},\mathbf{b}} = p\left(|E(\mathbb{F}_p)| - 1\right).$

Proof $(\mathbf{a}, \mathbf{b}) = (0,1,0,0,0,1,0,0,1)$ gives rise to the following conditions:

$$p| - cm_{26} \tag{1,2}$$
$$p| - cm_{36} + bm_{16} \tag{1,3}$$
$$p|1 - cm_{46} - bm_{12} \tag{1,4}$$
$$p|m_{12} - cm_{56} - b \tag{1,5}$$
$$p|bm_{26} \tag{2,3}$$
$$p| - c - bm_{46} \tag{3,4}$$
$$p| - bm_{56} \tag{3,5}$$

We know that $b \neq 0$ by the argument preceding Lemma 4.7. Hence we get $m_{26} = m_{56} = 0$. Equation (1,3) determines the value of m_{16}. Equation (1,5) implies $m_{12} = b$. Equation (3,4) implies $m_{46} = -c/b$. Equation (1,4) can now only be solved if (b, c) is a solution to $b + c^2 - b^3 = 0 \mod p$.

m_{36} is free.

Hence if $(\mathbf{a}, \mathbf{b}) = (0,1,0,0,0,1,0,0,1)$ we have

$$c_{\mathbf{a},\mathbf{b}} = p\left(|E(\mathbb{F}_p)| - 1\right).$$

□

Lemma 4.9 *If* $(\mathbf{a}, \mathbf{b}) = (0,0,1,0,1,0,0,0,1)$ *then* $c_{\mathbf{a},\mathbf{b}} = p\left(|E(\mathbb{F}_p)| - 1\right).$

Proof $(\mathbf{a}, \mathbf{b}) = (0,0,1,0,1,0,0,0,1)$ gives rise to the following conditions:

$$p| - m_{15} - bm_{25} \tag{1,2}$$
$$p| - bm_{35} \tag{1,3}$$
$$p|1 - cm_{13} - bm_{45} \tag{1,4}$$
$$p| - c - bm_{13} \tag{1,6}$$
$$p|m_{35} \tag{2,3}$$
$$p|m_{45} - cm_{23} - b \tag{2,4}$$
$$p| - bm_{23} \tag{2,6}$$

Since $b \neq 0$ we get $m_{23} = m_{35} = 0$. (1,2) determines m_{15} and m_{25} is free. (1,6) implies $m_{13} = -c/b$. (2,4) implies $m_{45} = b$. Finally (1,4) only has a solution if (b, c) is a solution to $b + c^2 - b^3 = 0 \mod p$.

Hence if $(\mathbf{a},\mathbf{b})=(0,0,1,0,1,0,0,0,1)$ we have

$$c_{\mathbf{a},\mathbf{b}}=p\left(|E(\mathbb{F}_p)|-1\right).$$

$\square$

This completes the proof of Theorem 4.1.$\square$

Corollary 4.10 *The local zeta functions $\zeta^{\leq}_{G,p}(s)$ of G are not finitely uniform.*

Proof The analysis of Theorem 4.1 implies that there exist polynomials $f_1(X)$ and $f_2(X)$ such that

$$\begin{aligned} a^{\leq}_{p^3} &= \sum_{\mathbf{a},\mathbf{b}} p^{6(b_1+b_2+b_3)}c_{\mathbf{a},\mathbf{b}} \\ &= f_1(p)+f_2(p)|E(\mathbb{F}_p)| \\ &= |E(\mathbb{F}_p)|+c \mod p^7 \end{aligned}$$

where c is some constant independent of p. The second inequality confirms that $f_2(X)$ is non-zero. Therefore we can apply Theorem 2.1 to deduce the corollary.$\square$

In a future paper [3] we shall show

Theorem 4.11 *There exist two non zero rational functions $P_1(X,Y)$ and $P_2(X,Y)\in\mathbb{Q}(X,Y)$ such that for almost all primes p:*

$$\zeta^{\triangleleft}_{G,p}(s)=P_1(p,p^{-s})+|E(\mathbb{F}_p)|P_2(p,p^{-s}).$$

In other words, the elliptic curve is the only non-rational variety that is involved in counting normal subgroups in G. In recent work with Loeser [7], we have developed the concept of a motivic zeta function associated to any torsion-free finitely generated nilpotent group. This is a power series with coefficients in the Grothendieck ring of algebraic varieties. Let $\mathcal{L}$ denote the subring generated by the Lefschetz motive $\mathbf{L}=[\mathbb{A}^1_k]$. A corollary to the proof of Theorem 4.11 says that the coefficients of the motivic zeta function of G associated to $\zeta^{\triangleleft}_{G,p}(s)$ lie in the $\mathcal{L}$-submodule of the Grothendieck ring generated by the motive corresponding to the elliptic curve E. In [3] we explain how these ideas can be used to define a new invariant for nilpotent groups consisting of the smallest $\mathcal{L}$ -submodule containing the coefficients of the associated motivic zeta function. It would be interesting to know what this invariant is for the motivic zeta function associated to $\zeta^{\leq}_{G,p}(s)$. I would conjecture that despite the extra complications from counting subgroups, the motivic zeta function still has coefficients lying in the $\mathcal{L}$ -submodule generated by E.

References

[1] M.P.F. du Sautoy, *Zeta functions and counting finite p-groups*, Electronic Research Announcements of the American Math. Soc., **5** (1999),

[2] M.P.F. du Sautoy, *Counting finite p-groups and nilpotent groups*, preprint.

[3] M.P.F. du Sautoy, *Counting subgroups in nilpotent groups and points on elliptic curves*, preprint.

[4] M.P.F. du Sautoy and F.J. Grunewald, *Analytic properties of Euler products of Igusa-type zeta functions and subgroup growth of nilpotent groups,* C. R. Acad. Sci. Paris, **329**, Série I, (1999), 351-356.

[5] M.P.F. du Sautoy and F.J. Grunewald, *Analytic properties of zeta functions and subgroup growth*, M.P.I. preprint series 1999 (87) (to appear in Annals of Math.).

[6] M.P.F. du Sautoy and F.J. Grunewald, *Uniformity for 2-generator free nilpotent groups*, in preparation.

[7] M.P.F. du Sautoy and F. Loeser, *Motivic zeta functions of infinite dimensional Lie algebras*, preprint.

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

[9] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehung zur Verteilung der Primzahlen. Zweite Mitteilung.* Math. Zeit. **6**, (1920), 11–51.

[10] G. Higman, *Enumerating p-groups*, II, Proc. Lond. Math. Soc. **10** (1960), 566-582.

[11] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2d edition. Graduate texts in mathematics 84, Springer-Verlag, New York–Berlin–Heidelberg, 1993.