ASSOCIATING CURVES OF LOW GENUS TO INFINITE NILPOTENT GROUPS VIA THE ZETA FUNCTION

BY

CORNELIUS GRIFFIN

The Mathematical Institute
24–29 St. Giles', Oxford OX1 3LB, England
e-mail: griffinc@maths.ox.ac.uk

ABSTRACT

It is known from work of du Sautoy and Grunewald in [duSG1] that the zeta functions counting subgroups of finite index in infinite nilpotent groups depend upon the behaviour of some associated system of algebraic varieties on reduction mod p. Further to this, in [duS1, duS2] du Sautoy constructed a group whose local zeta function was determined by the number of points on the elliptic curve $E: Y^2 = X^3 - X$. In this work we generalise du Sautoy's construction to define a class of groups whose local zeta functions are dependent upon the number of points on the reduction of a given elliptic curve with a rational point. We also construct a class of groups that behave the same way in relation to any curve of genus 2 with a rational point. We end with a discussion of problems arising from this work.

1. Introduction

In [GSS] Grunewald, Segal and Smith introduced the notion of a zeta function for an infinite group G encoding (normal) subgroups of finite index:

$$\zeta_G(s) = \sum_{H <_f G} |G:H|^{-s} \quad \text{and} \quad \zeta_G^{\triangleleft}(s) = \sum_{H \triangleleft_f G} |G:H|^{-s}.$$

In particular, they considered these functions for an infinite nilpotent group, as for groups of this type, the global zeta functions split as an Euler product of local zeta functions:

$$\zeta_G^{\star}(s) = \prod_{p \text{ prime}} \zeta_{G,p}^{\star}(s) = \prod_p \sum_{H \star_p G} |G:H|^{-s},$$

Received October 10, 2002

where $\star \in \{\leq, \triangleleft\}$. Since then most effort in this subject area has gone into understanding the nature of these local factors for specific torsion free nilpotent groups. In [GSS] it was shown that there exists a Lie algebra L over $\mathbb{Z}$ associated to G so that for almost all primes we have

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

where $\zeta^{\star}_{L,p}(s)$ counts subalgebras/ideals of finite index in L.

Furthermore, the authors demonstrated that $\zeta^{\star}_{L,p}(s)$ could be expressed as a p-adic integral over $Tr_d(\mathbb{Z}_p)$, the upper triangular $d \times d$ matrices over $\mathbb{Z}_p$, and by applying some model theory and work of Denef [D] established the rationality in p^{-s} of these functions.

By evaluating the integrals explicitly, du Sautoy and Grunewald demonstrated an intriguing link between the zeta function and the arithmetic of some algebraic varieties. In particular, they showed that the zeta function of an infinite nilpotent torsion free group is dependent upon the number of points on the reduction mod p of some associated system of algebraic varieties. The question then is: what type of varieties can arise in the evaluation of the zeta function of an infinite torsion free nilpotent group?

Du Sautoy provided the first interesting answer [duS1, duS2] to this question by constructing a group $G(E)$ for which we have

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

for rational functions P_1, P_2 and for the elliptic curve $E : Y^2 = X^3 - X$. In [GSS] the authors asked whether every torsion free nilpotent group should have a finitely uniform (normal) zeta function. In other words, given any such group should we expect that finitely many rational functions will describe all the local zeta functions as p varies. Du Sautoy exploited well known arithmetic properties of the above elliptic curve to show that for this group the zeta function is not finitely uniform.

The aim of this paper is to extend this work of du Sautoy and produce a larger class of algebraic varieties whose reduction mod p is encoded in the subgroup structure of some infinite nilpotent group. In particular, we prove

Theorem 1: *Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational point in $\mathbb{Q}$. Then there exists a 9 generated, class 2 infinite torsion-free nilpotent group G, associated Lie algebra L, associated lines M_1, M_2 and rational functions $P_1, \ldots, P_5 \in \mathbb{Q}(X, Y)$ so that for almost all primes p, in particular including* *primes dividing neither the discriminant nor the coefficients of the curve, we have*

$$\begin{aligned}\zeta^{\triangleleft}_{G,p}(s) = \zeta^{\triangleleft}_{L,p}(s) =& P_1(p,p^{-s}) + |E(\mathbb{F}_p)|P_2(p,p^{-s}) + |M_1 \cap E(\mathbb{F}_p)|P_3(p,p^{-s}) \\ &+ P_4(p,p^{-s})|M_2 \cap E(\mathbb{F}_p)| + P_5(p,p^{-s})|M_1 \cap M_2 \cap E(\mathbb{F}_p)|.\end{aligned}$$

Furthermore, $P_2 \not\equiv 0$.

THEOREM 2: *Let C be a curve of genus 2 over $\mathbb{Q}$ with a rational point in $\mathbb{Q}$. Then there exists a 15 generated, class 2 torsion-free nilpotent group G and associated Lie algebra L, $l \in \mathbb{N}$, rational functions $P, Q_1, \ldots, Q_l \in \mathbb{Q}(X,Y)$ and varieties $V_1, \ldots, V_l$ defined over $\mathbb{Q}$ so that for almost all primes p*

$$\zeta^{\triangleleft}_{G,p}(s) = \zeta^{\triangleleft}_{L,p}(s) = |C(\mathbb{F}_p)|P(p,p^{-s}) + \sum_{i=1}^{l} |V_i(\mathbb{F}_p)|Q_i(p,p^{-s}).$$

Furthermore, it is strictly necessary to count points on the curve C in the evaluation of the zeta function. In particular, the V_i are varieties of genus smaller than 2 and C occurs in the subring of the motivic zeta function one can associate to the group G.

The method of proof is as follows: given a torsion free nilpotent group with a presentation

$$G = \langle X_1, \ldots, X_d : [X_i, X_j] = \prod_{k=1}^{d} X_k^{a_{ij}^k} \rangle$$

we take the Lie algebra L associated to G via the Mal'cev correspondence which has a presentation

$$L = \langle e_1, \ldots, e_d : (e_i, e_j) = \sum_{k=1}^{d} a_{ij}^k e_k \rangle.$$

For details on this correspondence consult [Se].

Defining C_j for $j = 1, \ldots, d$ to be the matrices with (i,k)-entry $c_{ik}(j)$ where

$$(e_i, e_j) = \sum_{k=1}^{d} c_{ik}(j) e_k,$$

it is known that [duSG1]

$$\zeta^{\triangleleft}_{L,p}(s) = (1-p^{-1})^{-d} \int_{V_p^{\triangleleft}} |m_{11}|^{s-1} \cdots |m_{dd}|^{s-d} |dx|$$

where here we define

$$V_p^{\triangleleft} = \{M \in Tr_d(\mathbb{Z}_p) : \underline{m_i} C_j M^+ = m_{11} \cdots m_{dd}(Y_{ij}^1, \ldots, Y_{ij}^d) \text{ for some } Y_{ij}^k \in \mathbb{Z}_p\}$$

and $|dx|$ is the normalized Haar measure on $Tr_d(\mathbb{Z}_p)$. Here we have denoted by $Tr_d(\mathbb{Z}_p)$ the $d \times d$ upper triangular matrices with entries from $\mathbb{Z}_p$, by $\underline{m_i}$ the i-th row of the matrix M and by M^+ the adjoint matrix of M. We then evaluate this integral by parts.

The paper is organised as follows: we prove Theorem 1 in Sections 2 and 3, and then Theorem 2 in Section 4. In Section 5 we discuss the associated problems of evaluating the zeta functions attached to the groups in question that count all subgroups of finite index, not merely normal subgroups. In Section 6 we discuss some problems arising from this work. We include in an Appendix the determinants arising in the calculation of the zeta functions in Sections 2 and 3.

This work is part of the author's PhD thesis, Nottingham, 2002, carried out with the support of an EPSRC studentship, and under the supervision of Professor Ivan Fesenko. The work was prepared for publication whilst the author was the holder of a GTEM post-doctoral research fellowship at the University of Heidelberg. The author would like to thank EPSRC and the University of Heidelberg for their financial support, and also I. Fesenko, M. du Sautoy and M. Edjvet for their helpful comments.

2. Proof of Theorem 1

Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational point in $\mathbb{Q}$. By means of a linear shift in X, Y we may assume that $0 \in E(\mathbb{Q})$ and so E has an equation of the form [M1]

$$Y^2 + a_1 Y + a_2 XY = X^3 + a_3 X^2 + a_4 X.$$

A transformation $Y \mapsto Y - (a_2/2)X$ enables us to write the curve as

$$Y^2 + \alpha_3 Y = X^3 + \alpha_1 X^2 + \alpha_2 X$$

or projectively as

$$Y^2 Z + \alpha_3 Y Z^2 = X^3 + \alpha_1 X^2 Z + \alpha_2 X Z^2.$$

Notice that this curve may be expressed as the determinant of the following matrix:

$$F = (f_{ij}) := \begin{pmatrix} \alpha_1 X + \alpha_2 Z & X & Y + \alpha_3 Z \\ X & Z & 0 \\ Y & 0 & X \end{pmatrix}$$

for appropriate $\alpha_i \in \mathbb{Z}$. We define the Lie algebra L to be

$$L = \langle A_1, A_2, A_3, B_1, B_2, B_3, X, Y, Z : (A_i, B_j) = f_{ij}(X, Y, Z)\rangle.$$

So how does the calculation of the zeta function associated to this Lie algebra differ from that presented in [duS1]? The simple answer is: not a lot. The working is made more difficult due to the fact that the matrix in this case is not symmetric and so a lot of details that could be brushed under the carpet previously now have to be confronted head on. Also, the measure of sets that we need to calculate to show the dependence on the curve is more difficult to realise. In any case I will now proceed to give the calculations in full. Notice that these calculations are only valid when we consider the local zeta function of L at primes p not dividing non-zero members of the set $\{\alpha_1, \alpha_2, \alpha_3\}$ and also not dividing the discriminant of the elliptic curve. At these primes the calculations can still be performed but they lead to a long unilluminating case analysis that the reader can perform for his/herself.

As outlined above we may write the zeta function as an integral

$$\zeta^{\triangleleft}_{L,p}(s) = (1 - p^{-1})^{-9} \int_{V_p^{\triangleleft}} |m_{11}|^{s-1} \cdots |m_{99}|^{s-9} |dx|.$$

However, the algebra we are working with is class 2 and so we may rewrite this integral as

$$\zeta^{\triangleleft}_{L,p}(s) = (1 - p^{-1})^{-9} \int_{W_p^{\triangleleft}} |m_{11}|^{s-1} \cdots |m_{66}|^{s-6} |n_1|^{s-7} |n_2|^{s-8} |n_3|^{s-9} |dm| \cdot |dn|$$

where now dm and dn are respectively the additive Haar measures on $Tr_6(\mathbb{Z}_p)$ and $Tr_3(\mathbb{Z}_p)$, and $W_p^{\triangleleft}$ consists of pairs of matrices

$$(M, N) \in Tr_6(\mathbb{Z}_p) \times Tr_3(\mathbb{Z}_p)$$

so that for $j = 1, 2, 3$ we have

$$(m_{i4}, m_{i5}, m_{i6}) C(j) N^{+} = (\alpha_0(j), \beta_0(j), \gamma_0(j)) n_1 n_2 n_3$$

whereas for $j = 4, 5, 6$

$$(m_{i1}, m_{i2}, m_{i3}) C(j) N^{+} = (\alpha_0(j), \beta_0(j), \gamma_0(j)) n_1 n_2 n_3.$$

Here $\alpha_0(j), \beta_0(j), \gamma_0(j) \in \mathbb{Z}_p$,

$$N = \begin{pmatrix} n_1 & a & b \\ 0 & n_2 & c \\ 0 & 0 & n_3 \end{pmatrix},$$

and

$$C(1)=\begin{pmatrix}\alpha_1 & 0 & \alpha_2\\ 1 & 0 & 0\\ 0 & 1 & \alpha_3\end{pmatrix},\quad C(2)=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 0 & 0\end{pmatrix},\quad C(3)=\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 0\\ 1 & 0 & 0\end{pmatrix},$$
$$C(4)=\begin{pmatrix}\alpha_1 & 0 & \alpha_2\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix},\quad C(5)=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 0 & 0\end{pmatrix},\quad C(6)=\begin{pmatrix}0 & 1 & \alpha_3\\ 0 & 0 & 0\\ 1 & 0 & 0\end{pmatrix}.$$

Without confusion we can now suppress which case we are dealing with and write α_0 etc. for $\alpha_0(j)$. In other words, we are integrating by parts: we fix a basis for the centre of the algebra and count bases for the abelianisation lying above this particular central basis. Then we count occurrences of bases for the centre. It is worth remarking here that currently this method has only been made to work for class 2 algebras. A major challenge in the subject is to formulate a similar method of integration by parts that will enable one to evaluate algebras of higher class. We may now write the zeta function as a sum

$$\zeta^{\triangleleft}_{L,p}(s)=\sum_{\substack{M_1,\dots,M_6,\\ N_1,N_2,N_3\in\mathbb{N}}} p^{-M_1 s}\cdots p^{-N_3(s-8)}\mu(M_1,\dots,N_3)$$

where now $\mu(M_1,\dots,N_3)$ is the measure of those matrices (M,N) with p^{M_i},p^{N_i} replacing m_i,n_i. So evaluating the sum now reduces to the problem of calculating the measure of this set. It is in this measure that the elliptic curve and associated lines will appear. The measure can again be written as a p-adic integral

$$\mu(M_i,N_i)=\int_{(a,b,c)\in\mathbb{Z}_p}\mu(\Omega_1)\cdots\mu(\Omega_6)\Bigl(\sum_{m\geq 1}\mu(\Omega_1)(p^{-m}-p^{-m-1})\Bigr)^3|da|\cdot|db|\cdot|dc|$$

where 1) Ω_1 is the set of $(m_2,m_3)\in\mathbb{Z}_p^2$ so that for $j=4,5,6$ there exists $(\alpha_0,\beta_0,\gamma_0)\in\mathbb{Z}_p^3$ so that

$$(p^{M_1},m_2,m_3)C(j)N^+=(\alpha_0,\beta_0,\gamma_0)p^{N_1+N_2+N_3},$$

2) Ω_2 is the set of $m_3\in\mathbb{Z}_p$ so that for $j=4,5,6$ there exists $(\alpha_0,\beta_0,\gamma_0)\in\mathbb{Z}_p^3$ so that

$$(0,p^{M_2},m_3)C(j)N^+=(\alpha_0,\beta_0,\gamma_0)p^{N_1+N_2+N_3},$$

and 3)

$$\Omega_3=\begin{cases}1 & \text{if } (0,0,p^{M_3})C(j)N^+=(\alpha_0,\beta_0,\gamma_0)p^{N_1+N_2+N_3},\\ 0 & \text{otherwise.}\end{cases}$$

We can similarly define $\Omega_4, \dots, \Omega_6$ as follows:

4) Ω_4 is the set of $(m_5, m_6) \in \mathbb{Z}_p^2$ so that for $j = 1, 2, 3$ there exists $(\alpha_0, \beta_0, \gamma_0) \in \mathbb{Z}_p^3$ so that

$$(p^{M_4}, m_5, m_6)C(j)N^+ = (\alpha_0, \beta_0, \gamma_0)p^{N_1+N_2+N_3},$$

5) Ω_5 is the set of $m_6 \in \mathbb{Z}_p$ so that for $j = 1, 2, 3$ there exists $(\alpha_0, \beta_0, \gamma_0) \in \mathbb{Z}_p^3$ so that

$$(0, p^{M_5}, m_6)C(j)N^+ = (\alpha_0, \beta_0, \gamma_0)p^{N_1+N_2+N_3},$$

and 6)

$$\Omega_6 = \begin{cases} 1 & \text{if } (0, 0, p^{M_6})C(j)N^+ = (\alpha_0, \beta_0, \gamma_0)p^{N_1+N_2+N_3}, \\ 0 & \text{otherwise.} \end{cases}$$

Following the notation of du Sautoy we set $\tilde{b} := ac - bp^{N_2}$ and then one can check that investigating the above conditions, we can rewrite them as follows:

Evaluating $\mu(\Omega_i)$. To calculate the value of $\mu(\Omega_1)$ notice that the conditions for a point to be in the set become

$$(\alpha_1 p^{M_1+N_2+N_3} + m_2 p^{N_2+N_3}, p^{M_1+N_2+N_3}, m_3 p^{N_2+N_3}) \equiv 0 \bmod p^{N_1+N_2+N_3},$$

$$(p^{M_1}, m_2, m_3)\begin{pmatrix} -a\alpha_1 & -a & p^{N_1} \\ -a & 0 & 0 \\ p^{N_1} & 0 & -a \end{pmatrix} \equiv 0 \bmod p^{N_1+N_2}$$

and

$$(p^{M_1}, m_2, m_3)\begin{pmatrix} \alpha_1\tilde{b} + \alpha_2 p^{N_1+N_2} & \tilde{b} & -cp^{N_1} + \alpha_3 p^{N_1+N_2} \\ \tilde{b} & p^{N_1+N_2} & 0 \\ -cp^{N_1} & 0 & \tilde{b} \end{pmatrix}$$

is $0 \bmod p^{N_1+N_2+N_3}$.

Thus we have

Lemma 2.1: *$\mu(\Omega_1)$ is given by:*

$$\mu(\Omega_1) = \begin{cases} 0, & \text{if } M_1 < N_1 \\ p^{-2N_1}\mu(\Omega'), & \text{if } M_1 \geq N_1 \end{cases}$$

where Ω_1' is the set of those $(m_2, m_3) \in \mathbb{Z}_p^2$ so that

$$(p^{M_1}, m_2, m_3)(S_1, S_2) \equiv 0 \bmod p^{N_2+N_3}$$

and

$$(S_1, S_2) = \begin{pmatrix} -a\alpha_1 p^{N_3} & -ap^{N_3} & p^{N_1+N_3} \\ -ap^{N_3} & 0 & 0 \\ p^{N_1+N_3} & 0 & -ap^{N_3} \end{matrix} \cdots$$

$$\cdots \begin{matrix} \alpha_1\tilde{b} + \alpha_2 p^{N_1+N_2} & \tilde{b} & -cp^{N_1} + \alpha_3 p^{N_1+N_2} \\ \tilde{b} & p^{N_1+N_2} & 0 \\ -cp^{N_1} & 0 & \tilde{b} \end{pmatrix}.$$

So given a solution (p^{M_1}, X, Y) to this congruence, all other solutions will be of the form $(p^{M_1}, X, Y) + (0, m_2, m_3)$ where here (m_2, m_3) is a solution to the congruence

$$(m_2, m_3) \begin{pmatrix} -ap^{N_3} & 0 & 0 \\ p^{N_1+N_3} & 0 & -ap^{N_3} \end{matrix} \cdots$$

$$\cdots \begin{matrix} \tilde{b} & p^{N_1+N_2} & 0 \\ -cp^{N_1} & 0 & \tilde{b} \end{pmatrix} \equiv 0 \bmod p^{N_2+N_3}. \tag{2.1}$$

So to sum up, the value for $\mu(\Omega_1)$ is contained in the following

PROPOSITION 2.2: *If $M_1 < U_1 + U_2 - W_1 - W_2 - W_3 + N_1 + N_2 + N_3$ then $\mu(\Omega_1) = 0$. For all other values of M_1 we have*

$$\mu(\Omega_1) = p^{U_1+U_2-(N_1+N_2+N_3)}.$$

Here we have defined

$$U_1 := \min\{u_1, N_2 + N_3\} \quad \text{and} \quad U_2 := \min\{u_2, N_2 + N_3\}$$

with

$$u_1 := \min\{v(detX) : X \text{ a } 1 \times 1 \text{ minor of matrix in (2.1)}\}$$

and

$$u_2 := \min\{v(detX) : X \text{ a } 2 \times 2 \text{ minor of matrix in (2.1)}\} - u_1.$$

We can evaluate these by hand and so find that

$$u_1 = \min\{v(a) + N_3, N_1 + N_3, v(\tilde{b}), N_1 + N_2, v(c) + N_1\}$$

and

$$u_2 = \min\{2v(a) + 2N_3, v(b) + N_1 + N_2 + N_3, 2N_1 + N_2 + N_3, v(a) + v(\tilde{b}) + N_3,$$
$$v(a) + N_1 + N_2 + N_3, v(c) + 2N_1 + N_2, 2v(\tilde{b}), v(\tilde{b}) + N_1 + N_2\} - u_1.$$

Similarly we have set

$$W_i = \min\{N_2 + N_3, w_i\}$$

with the w_i defined as the u_i were above. Thus one may check, using the determinants evaluated in the Appendix to this paper, that we have the following values for w_1, w_2, w_3:

$$\begin{aligned} w_1 = \min\{&v(a) + N_3, N_1 + N_3, v(\tilde{b}), N_1 + N_2, v(c) + N_1, \\ &v(\alpha_3 p^{N_2} - c) + N_1, v(\alpha_1 \tilde{b} + \alpha_2 p^{N_1+N_2})\}; \end{aligned}$$

$$\begin{aligned} w_2 = \min\{&v(a) + N_1 + 2N_3, v(a) + N_1 + N_2 + N_3, v(a) + v(\tilde{b}) + N_3, 2v(\tilde{b}), \\ &v(a) + v(\alpha_3 p^{N_2} - c) + N_1 + N_3, v(\tilde{b}) + N_1 + N_3, 2N_1 + N_2 + N_3, \\ &2(N_1 + N_2), v(\tilde{b}) + v(\alpha_3 p^{N_2} - c) + N_1, v(\alpha_3 p^{N_2} - c) + 2N_1 + N_2, \\ &v(\tilde{b}) + N_1 + N_2, 2(N_1 + N_3), v(b) + N_1 + N_2 + N_3, v(c) + 2N_1 + N_2, \\ &v(c - \alpha_3 p^{N_2}) + 2N_1 + N_3, v(a) + v(c) + N_1 + N_3, v(c) + 2N_1 + N_3, \\ &v(c) + v(\tilde{b}) + N_1, v(c) + 2N_1 + v(\alpha_3 p^{N_2} - c), 2v(a) + 2N_3\} - w_1; \end{aligned}$$

and finally:

$$\begin{aligned} w_3 = \min\{&3v(a) + 3N_3, v(a) + v(b) + N_1 + N_2 + N_3, 2v(a) + v(\tilde{b}) + 2N_3, \\ &v(b) + 2N_1 + N_2 + N_3, 3N_1 + N_2 + 2N_3, 2v(a) + N_1 + 2N_3, \\ &v(\tilde{b}) + v(b) + N_1 + N_2 + N_3, v(\alpha_3 p^{N_2} - c) + v(b) + 2N_1 + N_2 + N_3, \\ &v(\alpha_3 p^{N_2} - c) + 3N_1 + N_2 + N_3, v(a) + v(c) + 2N_1 + N_2 + N_3, \\ &v(a) + 2v(\tilde{b}) + N_3, v(c) + 3N_1 + N_2 + N_3, v(a) + v(\tilde{b}) \\ &+ N_1 + N_3, v(a) + 2N_1 + N_2 + N_3, v(-\tilde{b}^3 + \alpha_1 \tilde{b}^2 p^{N_1+N_2} \\ &+ \alpha_2 \tilde{b} p^{2(N_1+N_2)} - c^2 p^{2N_1} p^{N_1+N_2} + \alpha_3 c p^{2N_1} p^{N_1+N_2})\} - w_1 - w_2. \end{aligned}$$

We can similarly evaluate $\Omega_2, \ldots, \Omega_6$ and get the following values for these functions:

PROPOSITION 2.3:

$$\mu(\Omega_2) = \begin{cases} 0 & \textit{if } M_2 < V_1 - (U_1 + U_2) + N_1 + N_2 + N_3, \\ p^{V_1 - (N_1 + N_2 + N_3)} & \textit{otherwise;} \end{cases}$$

where V_1 is defined to be

$$V_1 := \min\{N_1 + N_3, v(a) + N_3, v(c) + N_1, v(\tilde{b}), N_2 + N_3\}.$$

PROPOSITION 2.4: *Ω_3 is 1 if and only if*

$$\begin{aligned} &M_3 \geq N_1, M_3 \geq N_3, M_3 + v(a) \geq N_1 + N_2, \\ &M_3 + v(\tilde{b}) \geq N_1 + N_2 + N_3, M_3 + v(c) \geq N_2 + N_3 \end{aligned}$$

and is 0 *otherwise.*

In an entirely similar fashion one can establish

PROPOSITION 2.5: $\mu(\Omega_4) = 0$ *if* $M_4 < U_4 + U_5 - (W_1 + W_2 + W_3) + N_1 + N_2 + N_3$ *and for all other values of* M_4 *we have*

$$\mu(\Omega_4) = p^{U_4+U_5-(N_1+N_2+N_3)};$$

$$\mu(\Omega_5) = \begin{cases} 0 & \textit{if } M_5 < V_4 - (U_4 + U_5) + N_1 + N_2 + N_3, \\ p^{V_4-(N_1+N_2+N_3)} & \textit{otherwise;} \end{cases}$$

and Ω_6 *is* 1 *if and only if*

$$M_6 \geq N_1, M_6 + v(a) \geq N_1 + N_2, M_6 \geq N_2,$$
$$M_6 + v(-cp^{N_1} + \alpha_3 p^{N_1+N_2}), M_6 + v(\tilde{b}) \geq N_1 + N_2 + N_3$$

where the U_i, V_i *are defined as before.*

One can check that the only case that leads to non-monomial conditions on the entries of the matrix occurs when we evaluate U_5:

$$\begin{aligned} u_5 = \min\{&2v(a) + 2N_3, v(a) + N_1 + N_2 + N_3, v(\tilde{b}) + N_1 + N_2, \\ &v(a) + v(\tilde{b}) + N_3, v(b) + N_1 + N_2 + N_3, 2N_1 + N_2 + N_3, \\ &v(\alpha_3 p^{N_2} - c) + 2N_1 + N_2, 2v(\tilde{b})\} - u_4. \end{aligned}$$

In order to show that evaluating the zeta function of the group depends on counting points on the elliptic curve mod p it will be sufficient then to calculate the measure of the following set. For all natural numbers $A, B, \tilde{B}, C, F, G, H$ we need to find the value of

$$\begin{aligned} \mu_{A,B,\tilde{B},C,F,G,H} := \mu\{(a,b,c) \in \mathbb{Z}_p^3\colon &v(a) = A, v(\tilde{b}) = \tilde{B}, v(c) = C, v(b) = B \\ &v(cp^{N_1} + \alpha_3 p^{N_1+N_2}) = G, v(\alpha_1\tilde{b} + \alpha_2 p^{N_1+N_2}) = H, \\ &v(-\tilde{b}^3 + \alpha_1\tilde{b}^2 p^{N_1+N_2} + \alpha_2\tilde{b}p^{2(N_1+N_2)} - c^2p^{2N_1}p^{N_1+N_2} \\ &+ \alpha_3 cp^{N_1}p^{2(N_1+N_2)}) = F\}. \end{aligned}$$

The first thing to notice is that, writing Φ for the set $(b/c + p^{N_2-C}\mathbb{Z}_p) \cup p^A\mathbb{Z}_p^*$, we have

$$\mu(\Phi) = \begin{cases} 0, & \text{if } B \neq A + C, N_2 - C > \min\{A, B - C\}, \\ p^{-A}(1 - p^{-1}), & \text{if } B \neq A + C, N_2 - C \leq \min\{A, B - C\}, \\ p^{C-N_2}, & \text{if } B = A + C, A + C > N_2, \\ p^{-A}, & \text{if } B = A + C, A + C \leq N_2; \end{cases}$$

it is sufficient for us to evaluate

$$\begin{aligned}\mu_{\tilde B,C,F,G,H} := \mu\{(\tilde b, c) \in \mathbb{Z}_p^2\colon v(\tilde b) = \tilde B, v(c) = C, v(\alpha_3 p^{N_1+N_2} - cp^{N_1}) = G,\\ v(\alpha_1 \tilde b + \alpha_2 p^{N_1+N_2}) = H, v(-\tilde b^3 + \alpha_1 \tilde b^2 p^{N_1+N_2} + \alpha_2 \tilde b p^{2(N_1+N_2)}\\ - c^2 p^{2N_1} + \alpha_3 c p^{N_1} p^{2(N_1+N_2)}) = F\}.\end{aligned}$$

Thus by changing the value of C, writing (b, B) for $(\tilde b, \tilde B)$ and N for $N_1 + N_2$ we need to calculate the value of

$$\begin{aligned}\mu_{B,C,F,G,H} := \mu\{(b, c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v(-c + \alpha_3 p^N) = G,\\ v(\alpha_1 \tilde b + \alpha_2 p^N) = H, v(-b^3 + \alpha_1 b^2 p^N + \alpha_2 b p^{2N}\\ - c^2 p^N + \alpha_3 c p^{2N}) = F\}.\end{aligned}$$

We split the analysis into three sections:

(1) $N \leq B, C$;
(2) $B < N, B \leq C$;
(3) $C < B, N$.

Case 1: $N \leq B, C$.

Setting $b' = b/p^N, c' = c/p^N$ and replacing b', c' by b, c respectively, we must evaluate in this instance

$$\begin{aligned}\mu\{(b, c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v(\alpha_3 - c) = G,\\ v(\alpha_1 b + \alpha_2) = H, v(b^3 - \alpha_1 b^2 - \alpha_2 b + c^2 - \alpha_3 c) = F\}.\end{aligned}$$

Notice that the calculations which follow assume that $\alpha_1\alpha_2\alpha_3 \neq 0$. The special cases that follow when this is not the case are all handled in the same way and so we suppress the details.

Notice also that the above set can be expressed as a Boolean combination of sets of the form

$$\begin{aligned}\{(b, c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v(\alpha_3 - c) \geq G,\\ v(\alpha_1 b + \alpha_2) \geq H, v(b^3 - \alpha_1 b^2 - \alpha_2 b + c^2 - \alpha_3 c) \geq F\}.\end{aligned}$$

We write $d(B, C, F, G, H)$ for the measure of this set and evaluate this. The first thing to notice is:

Lemma 2.6: *Suppose $B, C > 0$. Then $G = 0 = H$, otherwise $d(B, C, F, G, H)$ is 0. When $G = 0 = H$ then the measure depends upon the value of F in relation to that of B and C. Namely:*

(1) *if $F \leq \min\{B, C\}$ then $d(B, C, F, 0) = p^{-C}p^{-B}(1 - p^{-1})^2$;*

(2) *if $F < \min\{B, C\}$ then $d(B, C, F, 0) = 0$ unless $B = C$ when $d(B, C, F, 0)$ $= p^{-F}p^{-C}(1 - p^{-1})$.*

Next consider what happens for $C > 0, B = 0$. As in Lemma 2.6 we require $G = 0$ in order to get a non-zero value for the measure. We encapsulate what happens in this instance in the next

LEMMA 2.7: *Suppose that $C > 0 = B = G$. Then*

(1) *$H > 0 \Rightarrow F = 0$ or the measure is zero. In the case $H > 0, F = 0$ we must evaluate*

$$\mu\{(b, c) \in \mathbb{Z}_p^2\colon v(b) = 0, v(c) = C, v(\alpha_1 b + \alpha_2) \geq H\}$$

which is dependent upon the number of points on the line $\{\alpha_1 b + \alpha_2 = 0\}(\mathbb{F}_p)$. This is uniform in p and so can be neglected.

(2) *If $G = 0 = H$ then $1 \leq F \leq C \Rightarrow d(0, C, F, 0, 0) = 2p^{-F}p^{-C}(1 - p^{-1})$.*

Next we consider the case $B > 0, C = 0$. As previously it is immediate that to get a non-zero value for the measure we require that $H = 0$. When $H = 0$ we evaluate

$$d'(B, 0, F, G, 0) = \mu\{v(b) = B, v(c) = 0, v(\alpha_3 - c) = G,$$
$$v(b^3 - \alpha_1 b^2 - \alpha_2 b + c^2 - \alpha_3 c) \geq F\}.$$

LEMMA 2.8:

(1) *If $F > \min\{B, G\}$ then $d'(B, 0, F, G, 0) = 0$.*

(2) *If $F \leq \min\{B, G\}$ then $d'(B, 0, F, G, 0)$ depends upon the number of points on the line $\{\alpha_3 - c = 0\}(\mathbb{F}_p)$ and so is uniform in p.*

Finally, we must consider what happens when $B = C = 0$. In this case we want to calculate a value for

$$d_{0,0,F,G,H} = \mu\{(b, c) \in \mathbb{Z}_p^2\colon v(b) = 0, v(c) = 0, v(\alpha_3 - c) \geq G,$$
$$v(\alpha_1 b + \alpha_2) \geq H, v(b^3 + \alpha_1 b^2 + \alpha_2 b + c^2 + \alpha_3 c) \geq F\}.$$

The dependence on the varieties described in Theorem 1 will be born out of the following

LEMMA 2.9: *Let $K \geq 1$, let $(b, c) \in (\frac{\mathbb{Z}}{p^K\mathbb{Z}})$ with*

$$A_1 b^3 + A_2 b^2 + A_3 b + A_5 c^2 + A_6 c \equiv 0 \bmod p^K.$$

where here p is a prime dividing neither the discriminant nor the coefficients of the curve. Then there exist p pairs $(b_1, c_1) \in (\frac{\mathbb{Z}}{p^{K+1}\mathbb{Z}})$ so that $b \equiv b_1$, $c \equiv c_1 \bmod p^{K+1}$ and

$$A_1 b_1^3 + A_2 b_1^2 + A_3 b_1 + A_5 c_1^2 + A_6 c_1 \equiv 0 \bmod p^{K+1}. \tag{2.2}$$

Proof: Setting $b_1 = b + \beta p^K$ and $c_1 = c + \gamma p^K$ we want to count pairs $(\beta, \gamma) \in \{0, \dots, p-1\}^2$ so that (2.2) is satisfied. Expand this equation and notice that we may write

$$A_1 b^3 + \cdots + A_6 c = tp^K$$

for some $t \in \mathbb{N}$, and then it follows that we are looking for solutions of the linear congruence (in terms of β and γ)

$$t + \beta(3b^2 A_1 + 2bA_2 + A_3) + \gamma(2A_5 + A_6) \equiv 0 \bmod p.$$

The only way this congruence cannot have p solutions is when both the coefficients of β and γ are zero mod p. But this happens only when p divides the discriminant of the curve, contradicting the hypothesis we made. Thus the result is proved. ∎

We will split the calculation of the measure into a case analysis dependent upon the values of F, G, H:

(1) $F, G, H = 0$;
(2) $G, H = 0$;
(3) $F, H = 0$;
(4) $F, G = 0$;
(5) $F = 0$;
(6) $G = 0$;
(7) $H = 0$;
(8) $F, G, H \neq 0$.

1) We have $d(0,0,0,0,0) = \mu(\mathbb{Z}_p^* \times \mathbb{Z}_p^*)$, which is uniform in p and so can be neglected.

2) It follows simply from Lemma 2.9 that

$$d(0,0,F,0,0) = p^{-F+1} d(0,0,1,0,0) = p^{-F+1}(|E(\mathbb{F}_p| - 1).$$

3) We have $d(0,0,0,G,0) = (1-p^{-1})p^{-G}$. Notice that this expression actually involves counting points on the line $\{\alpha_3 - c = 0\}(\mathbb{F}_p)$ but this is suppressed due to the uniformity of this variety.

4) In an identical fashion, we have $d(0,0,0,0,H) = (1-p^{-1})p^{-H}$.

5) $d(0,0,0,G,H) = p^{-G-H}$; here we are counting points on the intersection $\{\alpha_3 - c = 0\} \cap \{\alpha_1 b + \alpha_2 = 0\}(\mathbb{F}_p)$.

6) $d(0,0,F,0,1) = p^{-F+1}(E \cap \{\alpha_1 b + \alpha_2 = 0\}(\mathbb{F}_p))$ and the case for a general H follows as a simple recurrence relation.

7) $d(0,0,F,1,0) = p^{-F+1}(E \cap \{\alpha_3 - c = 0\}(\mathbb{F}_p))$ and the case for a general G follows as a simple recurrence relation.

8) $d(0,0,F,1,1) = p^{-F+1}(E \cap \{\alpha_1 b + \alpha_2 = 0\} \cap \{\alpha_3 - c = 0\}(\mathbb{F}_p))$ and the case for general G, H follows as a simple recurrence relation.

This completes the case $N \leq B, C$. Notice that this is as stipulated by the work of du Sautoy and Grunewald in [duSG1] in that finitely many varieties, and their intersections, arise in the evaluation of the local zeta function.

Case 2: $B < N, B \leq C$.

Setting $b' = p^N/b, c' = c/b$ and replacing as before we must evaluate, for $B \geq 1, C \geq 0$,

$$\mu\{(b,c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v(b\alpha_3 - c) = G,$$
$$v(\alpha_1 + \alpha_2 b) = H, v(1 + \alpha_1 b + \alpha_2 b^2 + c^2 b + \alpha_3 c b^2) = F\}.$$

Using the same notation as before we can see that $F, H > 0 \Rightarrow d(B,C,F,G,H)$ is 0. The only non-trivial measures arising here are contained in

Lemma 2.10: *Suppose that $F = 0 = H$. Then*
(1) $G > \min\{B,C\} \Rightarrow d(B,C,0,G,0) = 0,$
(2) $\min\{B,C\} \geq G \Rightarrow p^{-B}p^{-C}(1-p^{-1})^{-2}.$

Case 3: $C < B, N$.

As is now becoming familiar, we set $b' = b/c, c' = p^N/c$ and relabelling as before we must evaluate for $B, C > 0$

$$\mu\{(b,c) \in \mathbb{Z}_p^2 : v(b) = B, v(c) = C, v(\alpha_3 c - 1) = G,$$
$$v(\alpha_1 b + \alpha_2 c) = H, v(b^3 - \alpha_1 b^2 c - \alpha_2 b c^2 + c - \alpha_3 c^2) = F\}.$$

We again immediately notice that $G > 0$ will give us a set of measure 0. The remaining cases, with the usual notation, are encapsulated in the following

Lemma 2.11:
(1) *If $F \leq \min\{3B, C\}$ and $H \leq \min\{B,C\}$ then*

$$d(B,C,F,0,H) = p^{-C}p^{-B}(1-p^{-1})^2;$$

(2) *if either $F > \min\{3B,C\}$ and $3B \neq C$, or $H > \min\{B,C\}$ and $B \neq C$, then $d(B,C,F,0,H) = 0$;*
(3) *if $F > \min\{3B,C\}, 3B = C$ and $H \leq \min\{B,C\}$ then*

$$d(B,3B,F,0,H) = p^{-F}p^{-B}(1-p^{-1});$$

(4) *if* $H > \min\{B, C\}, B = C$ *and* $F \leq \min\{3B, C\}$ *then*

$$d(B, C, F, 0, H) = p^{-H}p^{-B}(1 - p^{-1}).$$

So to finish I will briefly outline why the calculations I have performed lead to the theorem stated in the Introduction. This is exactly as contained in [duS1] and so I only include it for completeness. The calculations carried out here are sufficient to prove

PROPOSITION 2.12: *There exists a finite partition* $\bigcup_{i\in S}\Delta_i$ *of* $\mathbb{R}^9$ *defined by linear inequalities with coefficients in* $\mathbb{Q}$ *and for all* $i \in S$ *polynomials* P_i, Q_i, R_i, S_i, T_i *in* $\mathbb{Q}(X)$ *and linear functions* $\alpha_i, \beta_i, \gamma_i, \delta_i, \epsilon_i$ *so that if*

$$\Delta = (A, B, \tilde{B}, C, F, G, H, N_1, N_2) \in \mathbb{N}^9 \cap \Delta_i$$

then

$$\begin{aligned}\mu\{\dots\} =& P_i(p)p^{\alpha_i(\Delta)} + Q_i(p)|E(\mathbb{F}_p)|p^{\beta_i(\Delta)} + R_i(p)|E \cap M_1(\mathbb{F}_p)|p^{\gamma_i(\Delta)}\\ &+ S_i(p)|E \cap M_2(\mathbb{F}_p)|p^{\delta_i(\Delta)} + T_i(p)|E \cap M_1 \cap M_2(\mathbb{F}_p)|p^{\epsilon_i(\Delta)}.\end{aligned}$$

From this result, together with the values we worked out for the functions $\Omega_1, \dots, \Omega_6$ one can deduce that there exists a finite partition $\bigcup_{i\in S}\Delta_i$ of $\mathbb{R}^{18}$ defined by linear inequalities with coefficients in $\mathbb{Q}$ and for all $i \in S$ polynomials P_i, Q_i, R_i, S_i in $\mathbb{Q}(X)$ and linear functions $\alpha_i, \beta_i, \gamma_i, \delta_i, \epsilon_i, a_i, b_i, c_i, d_i, e_i$ so that if $\Lambda = (A, B, \tilde{B}, C, F, G, H, M_1, \dots, M_6, N_1, N_2, N_3)$ then

$$\begin{aligned}\zeta^{\triangleleft}_{L,p} = \sum_{i\in S}\sum_{\Lambda\in\mathbb{N}^{18}\cap\Delta_i} & P_i(p)p^{\alpha_i(\Lambda)+a_i(\Lambda)s} + Q_i(p)|E(\mathbb{F}_p)|p^{\beta_i(\Lambda)+b_i(\Lambda)s}\\ &+ R_i(p)|E \cap M_1(\mathbb{F}_p)|p^{\gamma_i(\Lambda)+c_i(\Lambda)s}\\ &+ S_i(p)|E \cap M_2(\mathbb{F}_p)|p^{\delta_i(\Lambda)+d_i(\Lambda)s}\\ &T_i(p)|E \cap M_1 \cap M_2(\mathbb{F}_p)|p^{\epsilon_i(\Lambda)+e_i(\Lambda)s}.\end{aligned}$$

Adding all this together is almost sufficient to prove Theorem 1. It is merely necessary to check that the rational function P_2 is not identically equal to 0.

3. Completion of the proof of Theorem 1

Although the Theorem is now complete, in order to show that this collection of nilpotent groups really does encode the arithmetic of the elliptic curves it is necessary to show that the rational function we have called P_2 is non-zero. As things stand we have merely shown the existence of such a function without saying anything about what it looks like. To show the function is non-zero, it is sufficient to show that counting subalgebras of some small p-power index in L is dependent on counting points on the reduction of the elliptic curves in question. This is a simple exercise in solving some congruences $\bmod p$.

So again let $L = L(E)$ be the Lie algebra with presentation as described earlier. Throughout this calculation we will assume we are dealing with a prime p not dividing $\alpha_1\alpha_2\alpha_3$ as this will simplify greatly the work involved. Then to count ideals of index p^5 say, it will be sufficient to count the number of pairs of matrices $\left((m_{ij}), \begin{pmatrix} n_1 & a & b \\ 0 & n_2 & c \\ 0 & 0 & n_3 \end{pmatrix}\right)$ so that the following four conditions are satisfied:

(1) $m_{ij}, n_k \in \mathbb{Z}$;
(2) $0 \leq m_{ij} < m_{jj}, \quad 0 \leq a < n_2, \quad 0 \leq b, c < n_3$;
(3) $m_{jj} = p^{M_j}, n_j = p^{N_j}, \quad M_1 + \cdots + N_3 = 5$;
(4) for $i = 1, \ldots, 6$,

$$j = 1,2,3 \Rightarrow (m_{i4}, m_{i5}, m_{i6})C(j)N^+ = (\alpha_0, \beta_0, \gamma_0)n_1n_2n_3,$$
$$j = 4,5,6 \Rightarrow (m_{i1}, m_{i2}, m_{i3})C(j)N^+ = (\alpha_0, \beta_0, \gamma_0)n_1n_2n_3.$$

Now the first thing to notice is that if we work out the left hand side of condition (4) for all the relevant values of i, j and α_i then we can immediately deduce the following

Lemma 3.1: *$M_1, \ldots, M_6 \geq N_1; M_3, M_6 \geq N_2; M_2, M_5 \geq N_3$. Hence $N_1 = 0$ and $0 \leq N_2, N_3 \leq 1$ and furthermore $N_2 + N_3 = 0, 1$.*

To make the analysis that follows more tractable, we again split the working into several separate cases.

Case 1: $N_2 = N_3 = 0$

This is easily dealt with. In this case $N = \mathrm{Id}_3$, no conditions arise from (4) and we merely have to count all matrices (m_{ij}) that can occur. This is uniform and polynomial in p and so can be encompassed under the umbrella of a rational function of p, p^{-s} in the evaluation of the zeta function. As such it doesn't concern us here.

Case 2: $N_2 = 1, N_3 = 0$.

It follows from the conditions stipulated above that $N_3 = b = c = 0$ and $0 \leq a \leq p - 1$. Then condition (4) becomes

$$(m_{i4}, m_{i5}, m_{i6}) \begin{pmatrix} \alpha_1 p & -a\alpha_1 & \alpha_2 p \\ p & -a & 0 \\ 0 & 1 & \alpha_3 p \end{pmatrix} \equiv 0 \bmod p,$$

$$(m_{i1}, m_{i2}, m_{i3}) \begin{pmatrix} \alpha_1 p & -a\alpha_1 & ap \\ \alpha_3 p & -a & 0 \\ 0 & 1 & 0 \end{pmatrix} \equiv 0 \bmod p,$$

$$(m_{i4}, m_{i5}, m_{i6}) \begin{pmatrix} p & -a & 0 \\ 0 & 0 & p \\ 0 & 0 & 0 \end{pmatrix} \equiv 0 \bmod p,$$

$$(m_{i4}, m_{i5}, m_{i6}) \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ p & -a & 0 \end{pmatrix} \equiv 0 \bmod p,$$

$$(m_{i1}, m_{i2}, m_{i3}) \begin{pmatrix} p & -a & 0 \\ 0 & 0 & p \\ 0 & 0 & 0 \end{pmatrix} \equiv 0 \bmod p,$$

$$(m_{i1}, m_{i2}, m_{i3}) \begin{pmatrix} 0 & 1 & \alpha_3 p \\ 0 & 0 & 0 \\ p & -a & 0 \end{pmatrix} \equiv 0 \bmod p.$$

So if $a = 0$ then the only thing these matrices tell us is that $m_{i6} \equiv 0 \bmod p$, from whence it follows that $m_{i4} = m_{i3} = m_{i1} \equiv 0 \bmod p$ and thus the number of matrices in this case is again uniform and polynomial in p. If, on the other hand, $1 \leq a \leq p-1$ then we see that $m_{i1} \equiv 0 \equiv m_{i4} \bmod p$ and so $\underline{a} = (1, 0, 1, 1, 0, 1)$ and again we will get a uniform expression.

Case 3: Suppose finally that $N_3 = 1$, $N_2 = 0 = a$.

In this case the conditions the matrices must satisfy become

$$(\alpha_2 - b\alpha_1)m_{i4} + bm_{i5} + (\alpha_3 - c)m_{i6} \equiv 0 \bmod p, \tag{3.1}$$

$$bm_{i4} + m_{i5} \equiv 0 \bmod p, \tag{3.2}$$

$$-cm_{i4} + bm_{i6} \equiv 0 \bmod p, \tag{3.3}$$

$$(\alpha_2 + b\alpha_1)m_{i1} + bm_{i2} - cm_{i3} \equiv 0 \bmod p, \tag{3.4}$$

$$bm_{i1} + m_{i2} \equiv 0 \bmod p, \tag{3.5}$$

$$(-c + \alpha_3 b)m_{i1} + bm_{i3} \equiv 0 \bmod p. \tag{3.6}$$

Recall that we already know that p divides m_{22}, m_{55} by Lemma 3.1 and this is confirmed by equations (3.2), (3.5). Setting $i = 3, 6$ allows us to deduce the following congruences involving entries on the diagonal of (m_{ij}):

$$-bm_{66} \equiv 0 \bmod p, \tag{3.7}$$

$$(\alpha_3 - c)m_{66} \equiv 0 \bmod p, \tag{3.8}$$

$$-bm_{33} \equiv 0 \bmod p, \tag{3.9}$$

$$cm_{33} \equiv 0 \bmod p. \tag{3.10}$$

So we do a case-by-case analysis, dependent on the values of $b, \alpha_3 - c, c \bmod p$.

SUBCASE 3.2: $b \not\equiv 0 \bmod p$ so that p does not divide b.

We can immediately see that p divides m_{33}, m_{66} and so $\underline{a} = (0,1,1,0,1,1)$. Setting $i = 1$ tells us that

$$\begin{aligned} m_{12} &\equiv -b \bmod p, \\ m_{13} &\equiv \frac{-(c-\alpha_3)}{b} \bmod p, \\ (\alpha_2 + \alpha_1 b) + b m_{12} - c m_{13} &\equiv 0 \bmod p, \end{aligned}$$

and so we have uniquely determined m_{12}, m_{13} in terms of b, c, from which it follows by elementary analysis that $(b,c) \in E(\mathbb{F}_p)$.

An entirely similar process gives us the same information about m_{45}, m_{46}. So now to deduce that in this case we have no alternative but to count points on the reduction of the elliptic curve, it will be sufficient to demonstrate what values the other entries in the matrix M can take.

Recall we know from the four conditions that $m_{i4} = 0 \ \forall i < 4$. So we need to investigate how to determine the remaining values of $m_{i2}, m_{i3}, m_{i5}, m_{i6}$. This is easily done simply by examining the equations for values of i running from 1 through 5 and one can see that all the outstanding values are uniquely determined by the choice of point (b,c) on the reduction of the curve.

SUBCASE 3.3: $b \equiv 0 \bmod p$.

The 6 conditions then become

$$\begin{aligned} \alpha_2 m_{i4} + (\alpha_3 - c) m_{i6} &\equiv 0 \bmod p, \\ m_{i5} &\equiv 0 \bmod p, \\ -c m_{i4} &\equiv 0 \bmod p, \\ \alpha_2 m_{i1} - c m_{i3} &\equiv 0 \bmod p, \\ m_{i2} &\equiv 0 \bmod p, \\ (\alpha_3 - c) m_{i1} &\equiv 0 \bmod p. \end{aligned}$$

From these equations it is possible to show that in two of the cases which can occur, namely 1) $c, \alpha_3 - c \not\equiv 0 \bmod p$ and 2) $c \equiv 0 \bmod p, \alpha_3 - c \not\equiv 0 \bmod p$, the fact that we are working with ideals of index p^5 means that no such matrices can occur. It seems reasonable, however, that if we increase the exponent of p then matrices will occur that bear witness to these congruences. However, suppose we look at the final possible case $c \not\equiv 0 \bmod p, \alpha_3 - c \equiv 0 \bmod p$. In this case the conditions become

$$\begin{aligned} \alpha_2 m_{i4} &\equiv 0 \bmod p, \\ m_{i5} &\equiv 0 \bmod p, \\ c m_{i4} &\equiv 0 \bmod p, \\ \alpha_2 m_{i1} - c m_{i3} &\equiv 0 \bmod p, \\ m_{i2} &\equiv 0 \bmod p, \end{aligned}$$

and so the only constraints the coefficients are bound by are

$$m_{22}, m_{33}, m_{44}, m_{55} \equiv 0 \bmod p.$$

It can again be checked that this leads to a polynomial uniform expression in p. This finishes the calculation and demonstrates that it really is necessary to count points on the elliptic curve; there is no quirk which ensures a simple expression after all. Thus Theorem 1 is proved. ∎

4. Proof of Theorem 2

First let us recall what Theorem 2 stated:

THEOREM 2: *Let C be a curve of genus 2 over $\mathbb{Q}$ with a rational point in $\mathbb{Q}$. Then there exists a 15 generated, class 2 torsion-free nilpotent group G and associated Lie algebra L, $l \in \mathbb{N}$, rational functions $P, Q_1, \ldots, Q_l \in \mathbb{Q}(X, Y)$ and varieties $V_1, \ldots, V_l$ so that for almost all primes p*

$$\zeta^{\triangleleft}_{G,p}(s) = \zeta^{\triangleleft}_{L,p}(s) = |C(\mathbb{F}_p)| P(p, p^{-s}) + \sum_{i=1}^{l} |V_i(\mathbb{F}_p)| Q_i(p, p^{-s}).$$

Furthermore, it is strictly necessary to count points on the reduction of the curve C in the evaluation of the zeta function. In particular, the V_i are varieties of genus smaller than 2 and C occurs in the subring of the motivic zeta function one can associate to the group G.

As this result follows along very similar lines to Theorem 1, a lot of details will be swept under the carpet. It is known (see [M2, Ch. 1] for example) that every curve of genus 2 over $\mathbb{Q}$ is of the form

$$Y^2 = a_0 X^6 + \cdots + a_6$$

and so every curve of genus 2 with a rational point is of the form

$$Y^2 + bY = a_0 X^6 + \cdots + a_5 X$$

or projectively of the form

$$Y^2Z^4 + bYZ^5 = a_0X^6 + \cdots + a_5XZ^5$$

and so is expressible as the determinant of

$$G := \begin{pmatrix} Y & X & \beta_1X & 0 & \beta_2X+\beta_3Z & \beta_4Z \\ 0 & Z & X & \beta_5Z & 0 & 0 \\ 0 & 0 & Z & X & 0 & 0 \\ 0 & 0 & 0 & Z & X & 0 \\ 0 & 0 & 0 & 0 & Z & X \\ \beta_6X & 0 & 0 & 0 & 0 & Y+\beta_7Z \end{pmatrix}.$$

Thus we will count ideals of p-power index in

$$L := \langle A_1, \ldots, A_6, B_1, \ldots, B_6, X, Y, Z : (A_i, B_j) = g_{ij}(X,Y,Z)\rangle.$$

For an algebra of this size, it becomes very difficult to evaluate the integral that would give us a full description of the zeta function encoding the ideal structure of L. Thus for this algebra, we will content ourselves with evaluating the coefficients of the zeta function for small powers of p in order to demonstrate that evaluating the zeta function does depend upon the number of points on the genus 2 curve as claimed. Given the work of du Sautoy and Grunewald in [duSG1] this will be sufficient to prove Theorem 2. This will follow exactly as for the elliptic curve example already considered, and in fact the details are very similar also. Recall that in order to count ideals of index p^n in L it is necessary and sufficient to count all pairs of matrices $((m_{ij}), \begin{pmatrix} n_1 & a & b \\ 0 & n_2 & c \\ 0 & 0 & n_3 \end{pmatrix})$ so that the following four conditions are satisfied:

(1) $m_{ij}, n_k \in \mathbb{Z}$,
(2) $0 \le m_{ij} < m_{jj}$, $0 \le a < n_2$, $0 \le b, c < n_3$,
(3) $m_{jj} = p^{M_j}, n_j = p^{N_j}$, $M_1 + \cdots + N_3 = n$,
(4) for $i = 1, \ldots, 6$,

$$j = 1, \ldots, 6 \Rightarrow (m_{i7}, \ldots, m_{i12})C(j)N^+ = (\alpha_0, \beta_0, \gamma_0)n_1n_2n_3,$$
$$j = 7, \ldots, 12 \Rightarrow (m_{i1}, \ldots, m_{i6},)C(j)N^+ = (\alpha_0, \beta_0, \gamma_0)n_1n_2n_3,$$

where the matrices $C(1), \ldots, C(12)$ are defined as in the elliptic curve example. Then if a_n denotes the number of ideals of index p^n in the algebra L, then

$$a_n = \sum_{<(\underline{a},\underline{b})>=n} c_{(\underline{a},\underline{b})} p^{12(b_1+b_2+b_3)}$$

where $c_{(\underline{a},\underline{b})}$ denotes the number of pairs of matrices satisfying the above conditions with diagonal entries p^{a_i}, p^{b_i} respectively. Also note that by $< (\underline{a}, \underline{b}) >$ we mean the sum of the entries in the vectors. Again we immediately get some restrictions on the values the diagonal entries of the matrices can take which are included in the next

LEMMA 4.1:
(1) $a_1, \ldots, a_7, a_9, \ldots, a_{12} \geq b_1$,
(2) $a_2, a_4, a_5, a_{12} \geq b_3$,
(3) $a_6, a_{12} \geq b_2$.

We consider the case $n = 11$, as in this instance it is a simple task to demonstrate the dependence on the curve of the number of ideals of given index. The first thing to notice is that the above Lemma forces $b_1 = 0$. We consider the case

$$(\underline{a}, \underline{b}) >= (0,1,1,1,1,1,0,1,1,1,1,1,0,0,1).$$

In other words, we are counting pairs of matrices (M, N) in which

$$N = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & p \end{pmatrix},$$

the diagonal entries of M are $(1,p,p,p,p,p,1,p,p,p,p,p)$ and condition (4) above has now reduced to (replacing b by $-b$)

$$\begin{aligned}
cm_{i7} + bm_{i8} + \beta_1 bm_{i9} + (\beta_2 b + \beta_3)m_{i11} + \beta_4 m_{i12} &\equiv 0 \bmod p, \\
m_{i8} + bm_{i9} + \beta_5 m_{i10} &\equiv 0 \bmod p, \\
m_{i9} + bm_{i10} &\equiv 0 \bmod p, \\
m_{i10} + bm_{i11} &\equiv 0 \bmod p, \\
m_{i11} + bm_{i12} &\equiv 0 \bmod p, \\
\beta_6 bm_{i7} + (\beta_7 - c)m_{i12} &\equiv 0 \bmod p, \\
-cm_{i1} + bm_{i6} &\equiv 0 \bmod p, \\
bm_{i1} + m_{i2} &\equiv 0 \bmod p, \\
\beta_1 bm_{i1} + bm_{i2} + m_{i3} &\equiv 0 \bmod p, \\
\beta_5 m_{i2} + bm_{i3} + m_{i4} &\equiv 0 \bmod p, \\
(\beta_2 b + \beta_3)m_{i1} + bm_{i4} + m_{i5} &\equiv 0 \bmod p, \\
\beta_4 m_{i1} + bm_{i5} + (\beta_7 - c)m_{i6} &\equiv 0 \bmod p.
\end{aligned}$$

Notice that if $b, c = 0$, then these conditions reduce even further and we get a uniform number of pairs of matrices, regardless of the prime p. The interesting case is when b and c are non-zero. In this case, as for the case of the elliptic curve example, it is simple to see that the number of pairs of matrices that occur is dependent on counting points on the reduction of the curve. For M is uniquely determined and the above conditions imply that the number of various N that can occur is $|C(\mathbb{F}_p)| - 1$. Theorem 2 now follows as in the work of du Sautoy in [duS2] which we mirrored in Section 3 of this paper. ∎

Remark: It is possible to complete this working and get a full description of a_{11}. However for the purposes of the Theorem we have sufficient detail.

5. Counting all subalgebras

We have given a fairly complete description of the zeta function counting ideals of the Lie algebras considered in the proofs of Theorems 1 and 2. We now digress slightly and consider the problem of counting all subalgebras in the Lie algebra L associated to the elliptic curve of Theorem 1. It is natural, given the presentation of L, to suspect that evaluating the zeta function counting all subalgebras of L will depend on counting points on the same varieties. Again it is known, from [dSG1], that

$$\zeta^{\leq}_{L,p}(s) = (1 - p^{-1})^{-9} \int_{W_p} |m_{11}|^{s-1} \cdots |m_{99}|^{s-9} |dx|$$

and we again simplify to write

$$\zeta^{\leq}_{L,p}(s) = (1 - p^{-1})^{-9} \int_{W_p} |m_{11}|^{s-1} \cdots |n_3|^{s-9} |dm| \cdot |dn|,$$

where now W_p consists of upper triangular matrices $M \in Tr_6(\mathbb{Z}_p)$ so that for all $1 \leq i, j \leq 6$,

$$\underline{m}_i \left(\sum_{l=j}^{6} m_{jl} D(l) \right) N^{+} \in n_1 n_2 n_3 \mathbb{Z}_p^3$$

where

$$D(1) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ -\alpha_1 & 0 & -\alpha_2 \\ -1 & 0 & 0 \\ 0 & -1 & -\alpha_3 \end{pmatrix}$$

and $D(2), \ldots, D(6)$ are defined similarly. As we have done above, it is possible to explicitly count all subalgebras of L of small p-power index, and these calculations, which are too lengthy to be included here, lead me to pose a

PROBLEM 5.1: *Given the algebra $L(E)$ associated to the elliptic curve E and nilpotent group $G(E)$, do there exist rational functions P_1, P_2, P_3, P_4, P_5 so that for almost all primes*

$$\begin{aligned}\zeta^{\le}_{G,p}(s) = \zeta^{\le}_{L,p}(s) =& P_1(p, p^{-s}) + |E(\mathbb{F}_p)|P_2(p, p^{-s}) + |M_1 \cap E(\mathbb{F}_p)|P_3(p, p^{-s})\\ &+ P_4(p, p^{-s})|M_2 \cap E(\mathbb{F}_p)| + P_5(p, p^{-s})|M_1 \cap M_2 \cap E(\mathbb{F}_p)|\end{aligned}$$

for the same lines M_1, M_2?

The stumbling block to proving this isn't one of conception: all the machinery would appear to be in place. However, the conditions lead to a very complicated case analysis which I have not yet carried out.

This does lead one to another:

QUESTION 5.2: *Given a finite dimensional Lie ring L over $\mathbb{Z}$, do the same varieties always arise when one evaluates either the local zeta function counting all prime power index subalgebras or the local zeta function only counting all prime power index ideals?*

A proof would probably come from understanding the associated motivic zeta function better. For details consult [duSL].

6. Questions arising from this work

We have extended du Sautoy's work to produce a larger class of curves whose arithmetic is encoded in the subgroup structure of some nilpotent groups. Although in the genus 2 example we already see that things rapidly become more complicated as the degree of the curve increases, we may still in theory ask to what extent this method of producing curves as determinants holds good.

In 1921, Dickson [Di] considered the problem over $\mathbb{C}$ and gave a description of all homogeneous polynomials arising as the determinant of a matrix with linear entries; his methods were somewhat ad hoc. More recently, Beauville [Be] has used the theory of Cohen-Macauley sheaves to show in fact that any curve over $\mathbb{Q}$ can be written as the determinant of a matrix of linear forms. Thus it is in theory possible to extend further my examples and produce any curve as a determinant.

Here we have considered curves of small genus as they are classes of curves with a nice general description. It may be that one can define other classes of curves with general equations of this type, but it is known for instance [M2] that when one considers curves of genus 3, such curves do not have a description of a similar kind. There is no general formula giving every such curve.

Also notice we have stipulated that the curves we consider have a rational point. This is to keep notation as simple as possible. For example, it does not appear possible to write down a determinant giving an arbitrary elliptic curve; it seems that as one considers curves, one must consider alternative styles of presentation. The class of curves with a rational point contains a large proportion of all elliptic curves, conjecturally 70% of them [BM, W], and this class does have a nice expression as a determinant, as we have seen.

Similar work to that contained here has been carried out by Christopher Voll [V], who has also considered the problem of constructing groups whose subgroup structure encodes information about the reduction of some plane curves. He considers more generally curves over an algebraic number field, whose representation as a determinant is well known [Di]. He is able to give expressions for the zeta function of a Lie algebra whose Lie structure is defined similarly to that contained here. As such he demonstrates a relationship between plane curves over a number field and zeta functions counting certain restricted types of subalgebras of a Lie algebra defined over $\mathbb{Q}$. For more details consult his thesis.

Voll also completes the calculation for the zeta function counting points on the elliptic curve $E : Y^2 = X^3 - X$. By explicitly evaluating the rational functions, and applying a functional equation for the Weil zeta function encoding the number of points on $E(\mathbb{F}_p)$, he is able to demonstrate the existence of a functional equation for this zeta function. One can ask whether this phenomenon will hold in full generality, for instance for the zeta functions considered here. Denef and Meuser [DM] have shown that the Igusa zeta function has a functional equation; this zeta function is a special case of du Sautoy and Grunewald's cone integral with an empty cone condition. It is possible to construct a cone condition so that the associated cone integral does not satisfy a functional equation, but can such a cone condition come from a presentation for a nilpotent group? Or do the cone conditions arising from group presentations all have the necessary symmetry to ensure the existence of a functional equation for all group zeta functions? I thank Marcus du Sautoy for suggesting this reasoning to me.

To end this paper, I will now note the determinants arising from the 3×3 minors of the matrix (S_1, S_2) in the calculation of the zeta functions in Section 1 of this paper.

Appendix

In the interests of completeness, we include here the determinants arising from the 3×3 minors of the matrix (S_1, S_2). By repeatedly applying the condition $\min\{v(X+Y), v(X)\} = \min\{v(X), v(Y)\}$ and noticing that we have stipulated that p does not divide $\alpha_1\alpha_2\alpha_3$, it is relatively straightforward to see that the value for W_3 is as contained in the main body of the text. The same process enables one to evaluate W_2, U_2, U_5 but in the interests of brevity we suppress the details. Throughout (a_1, a_2, a_3) will denote the determinant arising from the matrix formed from the a_1, a_2, a_3 columns of (S_1, S_2) for $a_i \in \{1, \ldots, 6\}$:

$(1,2,3)$ $a^3p^{3N_3}$

$(1,2,4)$ $abp^{N_1+N_2+2N_3}$

$(1,2,5)$ $ap^{2N_1+N_2+2N_3}$

$(1,2,6)$ $-a^2\tilde{b}p^{2N_3}$

$(1,3,4)$ $-bp^{2N_1+N_2+2N_3} + \alpha_2 a^2 p^{N_1+N_2+2N_3}$

$(1,3,5)$ $p^{3N_1+N_2+2N_3} + a^2\tilde{b}p^{2N_3} - a^2\alpha_1 p^{N_1+N_2+3N_3}$

$(1,3,6)$ $a\tilde{b}p^{N_1+2N_3} + a^2(\alpha_3 p^{N_2} - c)p^{N_1+2N_3}$

$(1,4,5)$ $\tilde{b}bp^{N_1+N_2+N_3} + \alpha_2 p^{3N_1+2N_2+N_3} - \alpha_1 bp^{2N_1+2N_2+N_3}$

$(1,4,6)$ $(\alpha_3 p^{N_2} - c)bp^{2N_1+N_2+N_3} + \alpha_2 a\tilde{b}p^{N_1+N_2+N_3}$

$(1,5,6)$ $(\alpha_3 p^{N_2} - c)p^{3N_1+N_2+N_3} + a\tilde{b}^2p^{N_3} - a\tilde{b}p^{N_1+N_2+N_3}$

$(2,3,4)$ $-a^2\tilde{b}p^{2N_3}$

$(2,3,5)$ $-a^2p^{N_1+N_2+2N_3}$

$(2,3,6)$ 0

$(2,4,5)$ $-acp^{2N_1+N_2+N_3}$

$(2,4,6)$ $-a\tilde{b}^2p^{N_3}$

$(2,5,6)$ $a\tilde{b}p^{N_1+N_2+N_3}$

$(3,4,5)$ $cp^{3N_1+N_2+N_3} + a\tilde{b}^2p^{N_3} - \alpha_1 a\tilde{b}p^{N_1+N_2+N_3} - a\alpha_2 p^{2(N_1+N_2)+N_3}$

$(3,4,6)$ $\tilde{b}^2p^{N_1+N_3} + a\tilde{b}(\alpha_3 p^{N_2} - c)p^{N_1+N_3}$

$(3,5,6)$ $(\alpha_3 p^{N_2} - c)ap^{2N_1+N_2+N_3}$

$(4,5,6)$ $-\tilde{b}^3 + \alpha_1\tilde{b}^2p^{N_1+N_2} + \alpha_2\tilde{b}p^{2(N_1+N_2)} - c^2p^{2N_1}p^{N_1+N_2} + \alpha_3 cp^{2N_1}p^{N_1+N_2}$

So, for example, to get rid of the non-monomial expression

$$(\alpha_3 p^{N_2} - c)p^{3N_1+N_2+N_3} + a\tilde{b}^2p^{N_3} - a\tilde{b}p^{N_1+N_2+N_3}$$

coming from the determinant $(1,5,6)$ we apply the condition

$$\min\{v(X+Y), v(X)\} = \min\{v(X), v(Y)\}$$

to the determinants $(2,4,6)$ and $(2,5,6)$ to eliminate from consideration the terms $a\tilde{b}^2p^{N_3}$ and $a\tilde{b}p^{N_1+N_2+N_3}$. The same process allows us to neglect all non-monomial expressions except that arising from $(4,5,6)$.

References

[Be] A. Beauville, *Determinantal hypersurfaces*, Michigan Mathematical Journal **48** (2000), 39-64.

[BM] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil Group of elliptic curves*, Bulletin of the American Mathematical Society **23** (1990), 375–382.

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

[DM] J. Denef and D. Meuser, *A functional equation of Igusa's local zeta function*, American Journal of Mathematics **113** (1991), 1135-1152.

[Di] L. Dickson, *Determination of all general homogeneous polynomials expressible as determinants with linear elements*, Transactions of the American Mathematical Society **22** (1921), 167–179.

[duS1] M. du Sautoy, *Counting subgroups in nilpotent groups and points in elliptic curves*, Journal für die reine und angewandte Mathematik **549** (2002), 1–21.

[duS2] M. du Sautoy, *A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups*, Israel Journal of Mathematics **126** (2001), 269–288.

[duSG1] M. du Sautoy and F. J. Grunewald, *Analytic properties of zeta functions and subgroup growth*, Annals of Mathematics **152** (2000), 793–833.

[duSL] M. du Sautoy and F. Loeser, *Motivic zeta functions for infinite dimensional Lie algebras*, Ecole Polytechnique preprint series 2000-12.

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

[M1} J. S. Milne, *Lecture Notes on Elliptic Curves*, University of Michigan, 1996.

[M2] J. S. Milne, *Lecture Notes on Abelian Varieties*, University of Michigan, 1998.

[Se] D. Segal, *Polycyclic Groups*, Cambridge University Press, Cambridge, 1983.

[V] C. Voll, PhD Thesis, Cambridge, 2002.

[W] T. Womack, Computer search, Nottingham, 2002.