J. reine angew. Math. **549** (2002), 1—21

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 2002

Counting subgroups in nilpotent groups and points on elliptic curves

By *Marcus du Sautoy* at Oxford

1. Introduction

We shall explain how to use zeta functions of groups to generate a hierarchy within the class of finitely generated nilpotent groups indexed by certain subrings of the Grothendieck ring of varieties.

The zeta function of a group was introduced by Grunewald, Segal and Smith in [7] to provide a new invariant for a finitely generated nilpotent group G. It is defined as a Dirichlet series encoding the number $a_n^{\leqq}(G)$ of all subgroups of index n in G:

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

They also defined the normal zeta function of G:

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

where the coefficients $a_n^{\triangleleft}(G)$ of the Dirichlet series record the number of normal subgroups of index n in G. The expression as a sum over subgroups suggests that this is a natural non-commutative generalization of the zeta function of a number field.

These zeta functions decompose as Euler products of local factors: for $* \in \{\leqq, \triangleleft\}$

$$\zeta_G^{*}(s) = \prod_{p \text{ prime}} \zeta_{G,p}^{*}(s)$$

where

$$\zeta_{G,p}^{*}(s) = \sum_{n=0}^{\infty} a_{p^n}^{*}(G) p^{-ns}.$$

The local factors were proved in [7] to be rational functions in p^{-s}. One of the major open problems raised in [7] was the dependence on p of these local factors. The authors speculated that the analogy with the zeta function of a number field might imply a finitely uniform description for these local factors.

This was clarified in recent work with Grunewald [4]. We show that it is the Weil zeta function counting points on varieties mod p on varieties which offers the better analogy rather than the zeta function of a number field. It is this recent work together with work of myself and Loeser [5] on the concept of an associated motivic zeta function which reveals a path from nilpotent groups to subrings of the Grothendieck ring of algebraic varieties.

In [4] we have provided an explicit formula for these local factors which depends on counting points mod p on an explicit system of subvarieties E_i ($i \in T$, T finite) of a variety Y defined over $\mathbb{Z}$: for each subset I of T there exists a rational function $W_I(X, Y) \in \mathbb{Q}(X, Y)$ such that for almost all primes p

$$\zeta^*_{G,p}(s) = \sum_{I \subset T} c_I(p) W_I(p, p^{-s}) \tag{1.1}$$

where

$$c_I(p) = \mathrm{card}\{a \in Y(\mathbb{F}_p) \colon a \in E_i(\mathbb{F}_p) \text{ if and only if } i \in I\}. \tag{1.2}$$

The varieties E_i are the irreducible components corresponding to a resolution of singularities of a polynomial $F_G(\boldsymbol{X})$ defined from a presentation for G (or rather its associated Lie algebra L).

To attach some subring of the Grothendieck ring to the nilpotent group G, the idea is to look at the ring generated by the varieties that we need to count points on mod p to get an explicit expression like (1.1). However, this expression involves many choices: a choice of a presentation for G, a choice of a resolution of singularities, and a choice of simplicial decomposition of an associated cone in which we count lattice points. Not only that, but non-isomorphic varieties can have the same number of points mod p. So on its own the explicit expression derived in [4] is not enough to attach in some well-defined manner some subring of the Grothendieck ring to G. It is the concept of an associated motivic zeta function attached to these zeta functions which allows one to *canonically* associate a subring of the Grothendieck ring to G. This motivic zeta function takes its values in the Grothendieck ring and by "taking the trace of Frobenius" of the motivic zeta function one recovers the original zeta functions $\zeta^*_{G,p}(s)$. The motivic zeta function is however independent of a presentation and resolution. Hence the subring generated by the coefficients of the zeta function is canonically associated to the group G.

Despite this theoretical work it was unclear what sort of varieties could possibly appear in expressions for $\zeta^*_{G,p}(s)$. Indeed the speculations in the original paper of Grunewald, Segal and Smith [7] implied that it was plausible that one only got varieties whose number of points mod p were finitely uniform (i.e. given by a polynomial in p depending on some finite partition of primes), e.g. rational varieties or Artin motives. So all nilpotent groups would sit at the bottom of the hierarchy we are proposing.

In this paper we present examples which show that these zeta functions contain in general a much richer algebraic geometry than simply rational varieties. In particular we prove

Theorem 1.1. *For each elliptic curve $E = y^2 + x^3 - Dx$, define a nilpotent group $G(E)$ by the following presentation*:

$$G(E) = \left\langle \begin{array}{c} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3\colon [x_1, x_4] = y_3^D, [x_1, x_5] = y_1, [x_1, x_6] = y_2, \\ [x_2, x_4] = y_1, [x_2, x_5] = y_3, [x_3, x_4] = y_2, [x_3, x_6] = y_1 \end{array} \right\rangle.$$

Then there exist two rational functions $P_1(X, Y)$ and $P_2(X, Y) \in \mathbb{Q}(X, Y)$ such that for almost all primes p:

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

A corollary to results proved in a previous paper [3] in the case of $D = 1$ implies that the rational functions $P_1(X, Y)$ and $P_2(X, Y)$ are non-zero, i.e. that one can't avoid counting points on the elliptic curve E. The proof depends on counting the number of normal subgroups of index p^5 and can easily be adapted to prove the same result for general D.

In section 5 we shall explain the concept of the associated motivic zeta function developed in [5] which will imply the following:

Corollary 1.2. *The curve E is canonically attached to the nilpotent group $G(E)$.*

The methods developed in this paper offer the hope to show that nilpotent groups can involve arbitrary varieties. However there is one class of groups of which it is still conjectured that the associated varieties are all rational, namely free nilpotent groups (see [7]). This conjecture has been demonstrated to have more significance than first realised. In [1] and [2] it is explained why this conjecture relates to Higman's PORC conjecture that the number $f(p, n)$ of p-groups of order p^n is given, for each fixed n, by polynomials in p depending only on the residue class of p modulo some fixed integer N_n.

Acknowledgements. I would like to thank the Royal Society for support in the form of a University Research Fellowship. I would also like to thank the Max Planck Institut in Bonn where the group $G(E)$ flashed into my head one evening and for invaluable conversations with Fritz Grunewald during my time at the MPI. Thanks are also due to my Ph.D. student Christopher Voll who corrected a number of errors in the original manuscript.

2. Nilpotent groups and elliptic curves

Let $L(E)$ be the class two nilpotent Lie algebra over $\mathbb{Z}$ of dimension 9 as a free $\mathbb{Z}$-module given by the following presentation:

$$L(E) = \left\langle \begin{array}{c} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3\colon (x_1, x_4) = Dy_3, (x_1, x_5) = y_1, (x_1, x_6) = y_2, \\ (x_2, x_4) = y_1, (x_2, x_5) = y_3, (x_3, x_4) = y_2, (x_3, x_6) = y_1 \end{array} \right\rangle$$

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

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

where $a^{\triangleleft}_{p^n}(L)$ is the number of ideals of L of index p^n. Section 4 of [7] confirms the following:

Proposition 2.1. *For almost all primes p,*

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

It therefore suffices to prove:

Theorem 2.2. *There exist two rational functions $P_1(X,Y)$ and $P_2(X,Y) \in \mathbb{Q}(X,Y)$ such that for p coprime to $2D$*:

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

We begin by recalling something of the proof of (1.1) in [4] which will motivate the direction for the proof of Theorem 2.2. The proof of this explicit formula breaks up into a number of stages:

(1) We show how to express $\zeta^{\triangleleft}_{L(E),p}(s)$ as something we call a cone integral. Cone integrals are defined for a set of cone integral data consisting of polynomials $\mathscr{D} = \{f_0(\boldsymbol{x}), g_0(\boldsymbol{x}), \ldots, f_l(\boldsymbol{x}), g_l(\boldsymbol{x})\}$ by

$$Z_{\mathscr{D}}(s,p) = \int_{V_p(\mathscr{D})} |f_0(\boldsymbol{x})|^s |g_0(\boldsymbol{x})|\,|d\boldsymbol{x}|$$

where

$$V_p(\mathscr{D}) = \big\{\boldsymbol{x} \in \mathbb{Z}_p^m \colon v\big(f_i(\boldsymbol{x})\big) \leqq v\big(g_i(\boldsymbol{x})\big) \text{ for } i = 1,\ldots,l\big\}$$

and $|d\boldsymbol{x}|$ is the additive Haar measure on $\mathbb{Z}_p^m$. The cone integrals in the case of counting ideals in a Lie algebra L of dimension d are defined as follows: let $C_j = \big(c_{ik}(j)\big)$ be the $d \times d$ matrix defined by $(e_i, e_j) = \sum_{k=1}^{d} c_{ik}(j)e_k$. Let $M = (m_{ij})$ be an upper triangular matrix whose rows we shall call $\boldsymbol{m}_i$ and denote by $M^{\dagger}$ the adjoint matrix. Then define polynomials $g^{\triangleleft}_{ijk}(m_{rs})$ in the entries of this triangular matrix to be the kth entry of the d-tuple $\boldsymbol{m}_i C_j M^{\dagger}$. The cone conditions defining $\zeta^{\triangleleft}_{L,p}(s)$ are given then by

$$V_p(\mathscr{D}) = \big\{\boldsymbol{x} \in \mathbb{Z}_p^m \colon v(m_{11}\cdots m_{dd}) \leqq v\big(g^{\triangleleft}_{ijk}(m_{rs})\big) \text{ for } i,j,k = 1,\ldots,d\big\}$$

and $\zeta^{\triangleleft}_{L,p}(s)$ can be expressed in terms of the associated cone integral by

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

(2) If the polynomials involved in the cone integrals are all monomial then the calculation reduces to a discrete problem about summing lattice points representing the valuations of the variables m_{ij} satisfying various linear inequalities. We explain in the next step why this is uniform in p. But in general the polynomials $g^{\lhd}_{ijk}(m_{rs})$ are far from monomial. To overcome this problem we do a resolution of singularities on the polynomial $F_L(M) = m_{11} \cdots m_{dd} \prod\limits_{i,j,k} g^{\lhd}_{ijk}(m_{rs})$ which results in a partition of the resolved space into regions on which the polynomial $F_L(M)$ now becomes monomial. The partitioning of this space naturally leads to the problem of counting points on the associated irreducible components E_i $(i \in T)$ of the resolution of singularities of $F_L(M)$. This is the only place where the evaluation of this integral depends in some essential way on p. Apart from throwing away finitely many primes at various points (e.g. where the resolution has bad reduction) the integral is uniform outside this partitioning.

(3) This reduces our integral to a finite sum $\sum\limits_{I \subset T} c_I(p) Z_I(s)$, where the coefficients $c_I(p)$ defined in (1.2) capture the essential dependence on p, and the $Z_I(s)$ are cone integrals with respect to monomial polynomials of the following shape:

$$Z_I(s) = \int\limits_{V_p(I)} |y_1|^{a_{0i_1}s+b_{0i_1}} \cdots |y_r|^{a_{0i_r}s+b_{0i_r}} |d\boldsymbol{y}|$$

where $I = \{i_1, \ldots, i_r\}$ and

$$V_p(I) = \{\boldsymbol{y} \in (p\mathbb{Z}_p)^m\colon v(|y_1|^{a_{ji_1}} \cdots |y_r|^{a_{ji_r}}) \leqq v(|y_1|^{b_{ji_1}} \cdots |y_r|^{b_{ji_r}}) \text{ for } j = 1, \ldots, l\}.$$

These in turn can be expressed as a sum over lattice points $\boldsymbol{n} = (n_1, \ldots, n_m)$ corresponding to the valuations $n_i = v(y_i)$:

$$Z_I(s) = (1 - p^{-1})^r p^{m-r} \sum_{\boldsymbol{n} \in \Lambda} (p^{-(a_{0i_1}s+b_{0i_1}+1)n_1 - \cdots - (a_{0i_r}s+b_{0i_r}+1)n_r})$$

where

$$\Lambda = \{\boldsymbol{n} \in \mathbb{N}^m_{>0}\colon a_{ji_1}n_1 + \cdots + a_{ji_r}n_r \leqq b_{ji_1}n_1 + \cdots + b_{ji_r}n_r \text{ for } j = 1, \ldots, l\}.$$

The evaluation of $Z_I(s)$ is therefore independent of p thanks to the following proposition contained in [4] which we shall use later on in this paper:

Proposition 2.3. *Suppose there exists a finite partition $\bigcup\limits_{i \in S} \Theta_i$ of $\mathbb{R}^d$ defined by linear inequalities with coefficients over $\mathbb{Q}$ and for each $i \in S$ linear functions $\alpha_i(\boldsymbol{x})$ and $\beta_i(\boldsymbol{x})$ defined over $\mathbb{Q}$. Then there exist rational functions $H_i(X, Y) \in \mathbb{Q}(X, Y)$ such that for each $i \in S$*

$$\sum_{\boldsymbol{n} \in \mathbb{N}^d \cap \Theta_i} p^{-\alpha(\boldsymbol{n})s - \beta(\boldsymbol{n})} = H_i(p, p^{-s}).$$

These geometric progressions can be calculated by decomposing each cone Θ_i defined by the linear inequalities into open simplicial cones with fundamental regions of volume 1.

Our strategy in proving Theorem 2.2 is that once we have established the shape of the cone integrals depending on the presentation of $L(E)$, we shall perform a direct analysis to partition our integral according to points on the elliptic curve such that the individual integrals reduce to sums of lattice points of the shape detailed in Proposition 2.3.

Our direct analysis calculates the integral by parts exploiting the fact that in a class two nilpotent Lie algebra, the algebra splits into two abelian sections. We first integrate the 'top', the abelianisation, with respect to some fixed choice of basis for the centre. We then integrate the 'bottom', the centre, with respect to the functions introduced in the evaluation of the top. The analysis avoids the direct application of a resolution of singularities although there is in fact a hidden blow-up at the heart of some of the case analysis in considering the integral of the bottom.

Note that the analysis could be carried through to its ultimate conclusion resulting in an explicit evaluation of the zeta function. However the analysis in (3) involving a simplicial decomposition of cones C, although uniform in p, results in general in a very complicated case analysis. Since this paper has its focus in the dependence on p of these local factors, we have chosen to subsume these complications under the umbrella of a uniform calculation.

Proof of Theorem 2.2. Let

$$C(1) = \begin{pmatrix} 0 & 0 & D \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$C(2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

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

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

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

From the analysis described above in (1) from [4] we can express the zeta function $\zeta^{\triangleleft}_{L(E),p}(s)$ for all primes p by the following cone integral:

$$(2.1)\quad \zeta^{\triangleleft}_{L(E),p}(s) = (1 - p^{-1})^{-9} \int_{V_p} |m_{11}|^{s-1} \cdots |m_{66}|^{s-6} |n_1|^{s-7} |n_2|^{s-8} |n_3|^{s-9} |dm|\,|dn|$$

where dm and dn are additive Haar measures on $\mathrm{Tr}_6(\mathbb{Z}_p)$ and $\mathrm{Tr}_3(\mathbb{Z}_p)$ respectively and V_p consists of all pairs of matrices

$$(M,N) = \left((m_{ij}), \begin{pmatrix} n_1 & a & b \\ 0 & n_2 & c \\ 0 & 0 & n_3 \end{pmatrix} \right) \in \mathrm{Tr}_6(\mathbb{Z}_p) \times \mathrm{Tr}_3(\mathbb{Z}_p)$$

satisfying: for $i = 1, \dots, 6$, $\varepsilon = 0$ or 3 and $j = 1,2,3$ there exists $(\lambda^j_{i\varepsilon+1}, \lambda^j_{i\varepsilon+2}, \lambda^j_{i\varepsilon+3}) \in \mathbb{Z}_p^3$ such that

$$(2.2) \quad (m_{i\varepsilon+1}, m_{i\varepsilon+2}, m_{i\varepsilon+3})C(j)N^\dagger = (\lambda^j_{i\varepsilon+1} n_1 n_2 n_3, \lambda^j_{i\varepsilon+2} n_1 n_2 n_3, \lambda^j_{i\varepsilon+3} n_1 n_2 n_3)$$

where $N^\dagger$ is the adjoint matrix

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

The integral (2.1) is the same as the sum:

$$\sum_{M_1,\dots,M_6,N_1,N_2,N_3 \in \mathbb{N}} p^{-M_1 s} \cdots p^{-M_6(s-5)} p^{-N_1(s-6)} p^{-N_2(s-7)} p^{-N_1(s-8)} \mu(M_1, \dots, M_6, N_1, N_2, N_3)$$

where $\mu(M_1, \dots, M_6, N_1, N_2, N_3)$ is the measure of the set of $\big((m_{ij})_{i<j}, a, b, c\big)$ satisfying (2.2) with m_{ii} replaced by p^{M_i} and n_j replaced by p^{N_j}.

3. Integrating by parts: the top

We look to establish an expression for $\mu(M_1, \dots, M_6, N_1, N_2, N_3)$ by calculating the measure modulo the matrix for the centre N. We integrate by parts by performing the integration on the matrix for the abelianisation. It will suffice by symmetry to calculate values for the following functions: for each M_1 and

$$N = \begin{pmatrix} p^{N_1} & a & b \\ & p^{N_2} & c \\ & & p^{N_3} \end{pmatrix} \in \mathrm{Tr}_3(\mathbb{Z}_p)$$

(1) $Z_1(M_1, N) = \mu(W_1)$ where W_1 consists of $(m_2, m_3) \in \mathbb{Z}_p^2$ such that for each $j = 1,2,3$ there exists $(\lambda^j_1, \lambda^j_2, \lambda^j_3) \in \mathbb{Z}_p^3$

$$(3.1) \quad (p^{M_1}, m_2, m_3)C(j)N^\dagger = (\lambda^j_1 p^{N_1+N_2+N_3}, \lambda^j_2 p^{N_1+N_2+N_3}, \lambda^j_3 p^{N_1+N_2+N_3});$$

(2) $Z_2(M_2, N) = \mu(W_2)$ where W_2 consists of $m_3 \in \mathbb{Z}_p$ such that for each $j = 1,2,3$ there exists $(\lambda^j_1, \lambda^j_2, \lambda^j_3) \in \mathbb{Z}_p^3$

$$(3.2) \quad (0, p^{M_2}, m_3)C(j)N^\dagger = (\lambda^j_1 p^{N_1+N_2+N_3}, \lambda^j_2 p^{N_1+N_2+N_3}, \lambda^j_3 p^{N_1+N_2+N_3});$$

(3) $Z_3(M_3, N) = 1$ if there exists $(\lambda^j_1, \lambda^j_2, \lambda^j_3) \in \mathbb{Z}_p^3$ such that

$$(0, 0, p^{M_3})C(j)N^\dagger = (\lambda^j_1 p^{N_1+N_2+N_3}, \lambda^j_2 p^{N_1+N_2+N_3}, \lambda^j_3 p^{N_1+N_2+N_3})$$

and 0 otherwise.

Once we have done this, the measure can be expressed as

$$\begin{aligned}&\mu(M_1,\dots,M_6,N_1,N_2,N_3)\\ &\quad = \int\limits_{(a,b,c)} Z_1(M_1,N)Z_2(M_2,N)Z_3(M_3,N)\left(\sum_M Z_1(M,N)(p^{-M}-p^{-(M+1)})\right)^3\\ &\qquad Z_1(M_4,N)Z_2(M_5,N)Z_3(M_6,N)|da|\,|db|\,|dc|.\end{aligned}$$

3.1. Calculating $Z_1(M_1,N)$. We shall begin by calculating a value for the function $Z_1(M_1,N)$.

Condition (3.1) is equivalent to the following conditions:

$$p^{M_1},m_2,m_3 \equiv 0 \bmod p^{N_1}, \tag{3.3}$$

$$(p^{M_1},m_2,m_3)\begin{pmatrix} 0 & -a & p^{N_1}\\ -a & 0 & 0\\ p^{N_1} & 0 & -a\end{pmatrix} \equiv 0 \bmod p^{N_1+N_2}, \tag{3.4}$$

$$(p^{M_1},m_2,m_3)\begin{pmatrix} Dp^{N_1+N_2} & ac-p^{N_2}b & -cp^{N_1}\\ ac-p^{N_2}b & p^{N_1+N_2} & 0\\ -cp^{N_1} & 0 & ac-p^{N_2}b\end{pmatrix} \equiv 0 \bmod p^{N_1+N_2+N_3}. \tag{3.5}$$

Since $(p^{M_1},m_2,m_3)\in p^{N_1}\mathbb{Z}_p^3$ by (3.3) we get that

$$Z_1(M_1,N)=\begin{cases}0 & \text{if } M_1<N_1,\\ p^{-2N_1}\bar{Z}(M_1-N_1,N) & \text{if } N_1\leqq M_1\end{cases}$$

where $\bar{Z}_1(M_1,N)$ is the measure of $(m_2,m_3)\in\mathbb{Z}_p^2$ satisfying

$$(p^{M_1},m_2,m_3)\begin{pmatrix} 0 & -a & p^{N_1}\\ -a & 0 & 0\\ p^{N_1} & 0 & -a\end{pmatrix} \equiv 0 \bmod p^{N_2}, \tag{3.6}$$

$$(p^{M_1},m_2,m_3)\begin{pmatrix} Dp^{N_1+N_2} & ac-p^{N_2}b & -cp^{N_1}\\ ac-p^{N_2}b & p^{N_1+N_2} & 0\\ -cp^{N_1} & 0 & ac-p^{N_2}b\end{pmatrix} \equiv 0 \bmod p^{N_2+N_3}. \tag{3.7}$$

We can write this as the problem of calculating the measure of $(m_2,m_3)\in\mathbb{Z}_p^2$ satisfying:

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

where

$$(S_1,S_2)=\begin{pmatrix} 0 & -ap^{N_3} & p^{N_1+N_3} & Dp^{N_1+N_2} & ac-p^{N_2}b & -cp^{N_1}\\ -ap^{N_3} & 0 & 0 & ac-p^{N_2}b & p^{N_1+N_2} & 0\\ p^{N_1+N_3} & 0 & -ap^{N_3} & -cp^{N_1} & 0 & ac-p^{N_2}b\end{pmatrix}. \tag{3.8}$$

Once we have the existence of one solution (p^{M_1}, M_2, M_3) then all the other solutions are of the form $(p^{M_1}, M_2, M_3) + (0, m_2, m_3)$ where (m_2, m_3) is a solution of

$$(m_2, m_3)(R_1, R_2) \equiv 0 \mod p^{N_2+N_3}$$

and

$$(3.9) \qquad (R_1, R_2) = \begin{pmatrix} -ap^{N_3} & 0 & 0 & ac - p^{N_2}b & p^{N_1+N_2} & 0 \\ p^{N_1+N_3} & 0 & -ap^{N_3} & -cp^{N_1} & 0 & ac - p^{N_2}b \end{pmatrix}.$$

Once we have a solution then the value of $\bar{Z}_1(M_1, N)$ is the measure of this set which is

$$p^{U_1+U_2-2(N_2+N_3)}$$

where

$$(3.10) \qquad \begin{aligned} U_1 &= \min\{u_1, N_2 + N_3\} \\ U_2 &= \min\{u_2, N_2 + N_3\}, \end{aligned}$$

and

$$\begin{aligned} u_1 &= \min\{v(\det X)\colon X \text{ is a } 1 \times 1 \text{ minor of } (R_1, R_2)\}, \\ u_2 &= \min\{v(\det X)\colon X \text{ is a } 2 \times 2 \text{ minor of } (R_1, R_2)\} - u_1. \end{aligned}$$

Put $\tilde{b} = ac - p^{N_2}b$ then in this case

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

$$u_2 = \min\left\{\begin{array}{c} 2\big(v(a) + N_3\big), v(acp^{N_1+N_3} - \tilde{b}p^{N_1+N_3}) = v(b) + N_1 + N_2 + N_3, \\ 2N_1 + N_2 + N_3, v(a) + v(\tilde{b}) + N_3, v(a) + N_1 + N_2 + N_3, \\ v(c) + 2N_1 + N_2, v(\tilde{b}^2), v(\tilde{b}) + N_1 + N_2 \end{array}\right\} - u_1.$$

We have to calculate a condition on M_1 that we have such a solution. Let H_1 be the minimal value of M_1 such that there is a solution of

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

Then the measure of all the solutions of $(m_1, m_2, m_3)(S_1, S_2) \equiv 0 \bmod p^{N_2+N_3}$ is

$$p^{-H_1+U_1+U_2-2(N_2+N_3)}.$$

But we have another expression for this measure, namely it is

$$p^{W_1+W_2+W_3-3(N_2+N_3)}$$

where

$$\begin{aligned} W_1 &= \min\{w_1, N_2+N_3\},\\ W_2 &= \min\{w_2, N_2+N_3\},\\ W_3 &= \min\{w_3, N_2+N_3\}, \end{aligned} \tag{3.11}$$

and

$$\begin{aligned} w_1 &= \min\{v(\det X)\colon X \text{ is a } 1\times 1 \text{ minor of } (S_1,S_2)\},\\ w_2 &= \min\{v(\det X)\colon X \text{ is a } 2\times 2 \text{ minor of } (S_1,S_2)\} - w_1,\\ w_3 &= \min\{v(\det X)\colon X \text{ is a } 3\times 3 \text{ minor of } (S_1,S_2)\} - w_1 - w_2. \end{aligned}$$

This provides us with a smooth way to understand the value of H_1.

An analysis of the 18 1×1 minors of (S_1,S_2), 45 2×2 minors and 20 3×3 minors of (S_1,S_2) reveals that

$$w_1 = \min\{v(a)+N_3, v(\tilde{b}), N_1+N_2, N_1+N_3, v(c)+N_1\},$$

$$w_2 = \min\left\{\begin{array}{c} 2\big(v(a)+N_3\big), v(a)+v(\tilde{b})+N_3, v(a)+v(c)+N_1+N_3,\\ v(a)+N_1+N_2+N_3, v(\tilde{b})+N_1+N_3, 2v(\tilde{b}), 2N_1+2N_2,\\ v(\tilde{b})+v(c)+N_1, 2N_1+2N_3, 2v(c)+2N_1, v(\tilde{b})+N_1+N_2, \end{array}\right\} - w_1,$$

$$w_3 = \min\left\{\begin{array}{c} 3\big(v(a)+N_3\big), v(a)+N_1+2N_3+v(b)+N_2,\\ v(a)+2N_1+2N_3+N_2, 2v(a)+v(\tilde{b})+2N_3,\\ 2N_1+N_2+2N_3+v(b), 3N_1+2N_3+N_2,\\ 3N_1+N_3+2N_2, 2N_1+N_3+v(c)+N_2+v(b),\\ 3N_3+N_2+N_3+v(c), 2v(a)+N_1+N_2+2N_3,\\ v(a)+v(c)+2N_1+N_2+N_3, v(a)+2v(\tilde{b})+N_3,\\ v(a)+v(\tilde{b})+N_1+N_2+N_3, v(a)+2N_1+2N_2+N_3,\\ v(b)+v(\tilde{b})+N_1+N_2+N_3, v(b)+2N_1+2N_2+N_3,\\ v\big(-\tilde{b}^3-(cp^{N_1})^2p^{N_1+N_2}+D\tilde{b}(p^{N_1+N_2})^2\big) \end{array}\right\} - w_1 - w_2.$$

(We have used in our analysis that $\min\{v(X+Y), v(X)\} = \min\{v(X), v(Y)\}$ and $\min\{v(X^2), v(XY), v(Y^2)\} = \min\{v(X^2), v(Y^2)\}$. Also recall that we have assumed that D is a unit in $\mathbb{Z}_p$ since p is coprime to D.)

In conclusion we have

Proposition 3.1.

$$Z_1(M_1,N) = \begin{cases} 0 & \textit{if } M_1 < U_1+U_2-(W_1+W_2+W_3)+N_1+N_2+N_3,\\ p^{U_1+U_2-2(N_1+N_2+N_3)} & \textit{otherwise}, \end{cases}$$

where U_1, U_2, W_1, W_2, W_3 *are defined as above in* (3.10) *and* (3.11).

3.2. Calculating $Z_2(M_2,N)$. As in the previous analysis

$$Z_2(M_2,N)=\begin{cases}0 & \text{if } M_2<N_1,\\ p^{-N_1}\overline{Z_2}(M_2-N_1,N) & \text{if } N_1\leqq M_2,\end{cases}$$

where $\overline{Z_2}(M_2,N)$ is the measure of $m_3\in\mathbb{Z}_p$ satisfying

$$(3.12)\qquad (0,p^{M_2},m_3)\begin{pmatrix}0 & -a & p^{N_1}\\ -a & 0 & 0\\ p^{N_1} & 0 & -a\end{pmatrix}\equiv 0 \bmod p^{N_2},$$

$$(3.13)\quad (0,p^{M_2},m_3)\begin{pmatrix}Dp^{N_1+N_2} & ac-p^{N_2}b & -cp^{N_1}\\ ac-p^{N_2}b & p^{N_1+N_2} & 0\\ -cp^{N_1} & 0 & ac-p^{N_2}b\end{pmatrix}\equiv 0 \bmod p^{N_2+N_3}.$$

We can write the evaluation of $\overline{Z_2}(M_2,N)$ as the problem of calculating the measure of $m_3\in\mathbb{Z}_p$ satisfying:

$$(0,p^{M_2},m_3)(S_1,S_2)\equiv 0 \bmod p^{N_2+N_3}$$

where (S_1,S_2) was defined in (3.8).

Once we have the existence of one solution $(0,p^{M_2},M_3)$ then all the other solutions are of the form $(0,p^{M_2},M_3)+(0,0,m_3)$ where m_3 is a solution of

$$m_3\cdot(p^{N_1+N_3}\quad 0\quad -ap^{N_3}\quad -cp^{N_1}\quad 0\quad ac-p^{N_2}b)\equiv 0 \bmod p^{N_2+N_3}.$$

Once we have a solution then the value of $\overline{Z_2}(M_2,N)$ is the measure of this set which is $p^{V_1-(N_2+N_3)}$ where

$$(3.14)\qquad V_1=\min\{(N_1+N_3),v(a)+N_3,v(c)+N_1,v(\tilde{b}),(N_2+N_3)\}.$$

Again we have to calculate a condition on M_2 that we have such a solution. Let H_2 be the minimal value of M_2 such that there is a solution of

$$(p^{M_2},m_3)(R_1,R_2)\equiv 0 \bmod p^{N_2+N_3}$$

where (R_1,R_2) was defined in (3.9).

Then the measure of all the solutions of $(m_2,m_3)(R_1,R_2)\equiv 0 \bmod p^{N_2+N_3}$ is

$$p^{-H_2+V_1-(N_2+N_3)}.$$

But we have another expression for this measure, namely it is

$$p^{U_1+U_2-2(N_2+N_3)}$$

where U_1 and U_2 are defined above in (3.10).

Again this provides us with a smooth way to understand the value of H_2.

In conclusion we have:

Proposition 3.2.

$$Z_2(M_2, N) = \begin{cases} 0 & \textit{if } M_2 < V_1 - (U_1 + U_2) + N_1 + N_2 + N_3, \\ p^{V_1 - (N_1 + N_2 + N_3)} & \textit{otherwise}, \end{cases}$$

where V_1 *is defined in* (3.14) *and* U_1 *and* U_2 *are defined in* (3.10).

3.3. Calculating $Z_3(M_3, N)$. Similarly to the above we have

$$Z_3(M_3, N) = \begin{cases} 0 & \text{if } M_3 < N_1, \\ \overline{Z_3}(M_3 - N_1, N) & \text{if } N_1 \leqq M_3, \end{cases}$$

where $\overline{Z_3}(M_3, N) = 1$ if

$$(3.15) \qquad (0, 0, p^{M_3}) \begin{pmatrix} 0 & -a & p^{N_1} \\ -a & 0 & 0 \\ p^{N_1} & 0 & -a \end{pmatrix} \equiv 0 \bmod p^{N_2},$$

$$(3.16) \quad (0, 0, p^{M_3}) \begin{pmatrix} Dp^{N_1+N_2} & ac - p^{N_2}b & -cp^{N_1} \\ ac - p^{N_2}b & p^{N_1+N_2} & 0 \\ -cp^{N_1} & 0 & ac - p^{N_2}b \end{pmatrix} \equiv 0 \bmod p^{N_2+N_3}.$$

We can see directly from the conditions (3.15) and (3.16) that $\overline{Z_3}(M_3, N) = 1$ if and only if

$$M_3 \geqq N_2 - N_1, N_2 - v(a),$$

$$M_3 \geqq N_2 + N_3 - N_1 - v(c), N_2 + N_3 - v(ac - p^{N_2}b),$$

and equals 0 otherwise.

If we return now to our integral we see that it is equal to

$$(3.17) \qquad \sum_{M_1, \ldots, M_6, N_1, N_2, N_3 \in \mathbb{N}} p^{-M_1 s} \ldots p^{-M_6(s-5)} p^{-N_1(s-6)} p^{-N_2(s-7)} p^{-N_3(s-8)}$$

$$\int_{(a,b,c)} Z_1(M_1, N) Z_2(M_2, N) Z_3(M_3, N) \Big(\sum_M Z_1(M, N)(p^{-M} - p^{-(M+1)}) \Big)^3$$

$$Z_1(M_4, N) Z_2(M_5, N) Z_3(M_6, N) |da|\,|db|\,|dc|.$$

4. Integrating by parts: the bottom

To calculate the integral over the matrix for the centre, we shall need to know the value of

$$a_{A,B,\tilde{B},C,E,N_1,N_2} = \mu\left\{\begin{matrix} (a,b,c) \in \mathbb{Z}_p^3\colon v(a) = A, v(b) = B, v(\tilde{b}) = \tilde{B}, v(c) = C, \\ v\big(-\tilde{b}^3 - (cp^{N_1})^2 p^{N_1+N_2} + D\tilde{b}(p^{N_1+N_2})^2\big) = E \end{matrix}\right\}.$$

It will suffice to prove the following although our analysis provides precise information about the linear functions and inequalities involved:

Proposition 4.1. *There exists a finite partition $\bigcup\limits_{i \in S} \Theta_i$ of $\mathbb{R}^7$ defined by linear inequalities with coefficients in $\mathbb{Q}$ and for each $i \in S$, polynomials $P_i(X)$ and $Q_i(X)$ and linear function $\alpha_i(\boldsymbol{x})$ and $\beta_i(\boldsymbol{x})$ such that if $\boldsymbol{\Delta} = (A, B, \tilde{B}, C, E, N_1, N_2) \in \mathbb{N}^7 \cap \Theta_i$ then*

$$a_{\boldsymbol{\Delta}} = a_{A,B,\tilde{B},C,E,N_1,N_2} = P_i(p)p^{\alpha_I(\boldsymbol{\Delta})} + Q_i(p)|E(\mathbb{F}_p)|p^{\beta_I(\boldsymbol{\Delta})}.$$

Proof. Recall $\tilde{b} = ac - p^{N_2}b$. We can do this bit by parts by first fixing $\tilde{b}$ and c and calculating the measure of the corresponding a:

$$\mu\big((b/c + p^{N_2-C}\mathbb{Z}_p) \cap p^A\mathbb{Z}_p^*\big) = \begin{cases} 0 & \text{if } B \neq A + C \text{ and } N_2 - C > \min(A, B - C), \\ p^{-A}(1 - p^{-1}) & \text{if } B \neq A + C \text{ and } N_2 - C \leqq \min(A, B - C), \\ p^{C-N_2} & \text{if } B = A + C \text{ and } A + C < N_2, \\ p^{-A} & \text{if } B = A + C \text{ and } A + C < N_2. \end{cases}$$

Then

$$\mu\left\{\begin{matrix} (a,b,c) \in \mathbb{Z}_p^3\colon v(a) = A, v(b) = B, v(\tilde{b}) = \tilde{B}, v(c) = C, \\ v\big(-\tilde{b}^3 - (cp^{N_1})^2 p^{N_1+N_2} + D\tilde{b}(p^{N_1+N_2})^2\big) = E \end{matrix}\right\}$$
$$= \mu\big((b/c + p^{N_2-C}\mathbb{Z}_p) \cap p^A\mathbb{Z}_p^*\big)p^{N_2} \cdot \mu\left\{\begin{matrix} (\tilde{b}, c) \in \mathbb{Z}_p^2\colon v(\tilde{b}) = \tilde{B}, v(c) = C, \\ v\big(-\tilde{b}^3 - (cp^{N_1})^2 p^{N_1+N_2} + D\tilde{b}(p^{N_1+N_2})^2\big) = E \end{matrix}\right\}.$$

Hence it suffices to calculate the measure of

$$(4.1)\quad \mu\{(b,c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v\big(-b^3 - (cp^{N_1})^2 p^{N_1+N_2} + Db(p^{N_1+N_2})^2\big) = E\}$$

where now we write b for $\tilde{b}$ and B for $\tilde{B}$ to avoid too much notation.

The measure in (4.1) is the same as

$$p^{N_1}\mu\{(b,c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C + N_1, v\big(-b^3 - c^2p^{N_1+N_2} + Db(p^{N_1+N_2})^2\big) = E\}.$$

Let $N_1 + N_2 = N$.

We run over three cases: (1) $N \leqq B, C$; (2) $B < N$, $B \leqq C$; (3) $C < B, N$.

(1) $N \leqq B, C$. We make a transformation $b' = b/p^N$ and $c' = c/p^N$:

$$\mu\{(b,c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v(-b^3 - c^2p^N + Dbp^{2N}) = E\}$$
$$= p^{-2N}\mu\{(b',c') \in \mathbb{Z}_p^2\colon v(b') = B - N, v(c') = C - N, v(-b'^3 - c'^2 + Db') = E - 3N\}.$$

We need to calculate a value for

$$c_{B,C,E} = \mu\{(b,c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v(-b^3 - c^2 + Db) = E\}$$

(where we have replaced b', c' by b and c).

If we put

$$d_{B,C,E} = \mu\{(b,c) \in \mathbb{Z}_p^2\colon v(b) = B, v(c) = C, v(-b^3 - c^2 + Db) \geqq E\}$$

then $c_{B,C,E} = d_{B,C,E} - d_{B,C,E+1}$.

We shall suppose that $p \neq 2$.

Lemma 4.2. (1) *If $E \leqq \min\{B, 2C\}$ then $d_{B,C,E} = p^{-C}p^{-B}(1-p^{-1})^2$.*

(2) *If $B \neq 0$ and $\min\{B, 2C\} < E$ then $d_{B,C,E} = 0$ unless $B = 2C$ when $d_{B,C,E} = p^{-E}p^{-C}(1-p^{-1})$.*

(3) *If $B = 0$ then if $1 \leqq E \leqq 2C$ we have $d_{0,C,E} = 2p^{-E}p^{-C}(1-p^{-1})$.*

(4) *If $B = 0$ then $d_{0,0,E} = p^{E-1}d_{0,0,1} = p^{E-1}\big(|E(\mathbb{F}_p)| - 1\big)$.*

Proof. (1) is clear. When $B \neq 2C$, (2) follows since we can't get any solutions. (3) forces the value of $b = \pm 1 \bmod p^E$. The remaining cases depend on the following quantitative version of Hensel's lemma applied to the non-singular curve $E = Y^2 + X^3 - DX$:

Lemma 4.3. *Let $E \geqq 1$, $p \neq 2$. Let $(b,c) \in \mathbb{Z}/p^E\mathbb{Z}$ with $-b^3 - c^2 + Db = 0 \bmod p^E$. Then there exist exactly p elements $(b_1, c_1) \in \mathbb{Z}/p^{E+1}\mathbb{Z}$ with $b \equiv b_1, c \equiv c_1 \bmod p^E$ and $-b_1^3 - c_1^2 + Db_1 = 0 \bmod p^{E+1}$.*

Proof. Put $b_1 = b + \beta p^E$ and $c_1 = c + \gamma p^E$. We are required to count how many pairs $(\beta, \gamma) \in \{0, \dots, p-1\}^2$ there are satisfying:

$$-b_1^3 - c_1^2 + Db_1 = 0 \bmod p^{E+1}. \tag{4.2}$$

We know that $-b^3 - c^2 + Db = tp^E$ for some t. Hence expanding the equation (4.2) and pulling out the common power of p^E we have to solve:

$$t + \beta(D - 3b^2) - 2\gamma c = 0 \bmod p.$$

If $c = 0 \bmod p$ then $b(D - b^2) = 0 \bmod p$ which implies that $D - 3b^2 \neq 0 \bmod p$ (assuming $p \neq 2$). Hence we get exactly p lifts to solutions (b_1, c_1). This completes Lemma 4.3.

This lemma implies that whenever $E > B, C, 0$ then $d_{B,C,E+1} = p^{-1}d_{B,C,E}$.

If $B = 2C < E$ ($B = 2C = E$ is already covered) then $d_{2C,C,E} = p^{-E+(2C+1)}d_{2C,C,2C+1}$.

If $C > 0$ then $d_{2C,C,2C+1} = p^{-C}p^{-(2C+1)}(1-p^{-1})$ since once c is determined this forces the value of $b \bmod p^{2C+1}$.

If $B = 0$ then $d_{0,0,E} = p^{E-1}d_{0,0,1} = p^{E-1}(|E(\mathbb{F}_p)| - 1)$. This completes the proof of Lemma 4.2.

Hence we can determine $d_{B,C,E}$ once we know $|E(\mathbb{F}_p)|$.

(Note that although $E = Y^2 + X^3 - DX$ is non-singular, it does not have normal crossings with the varieties $X = 0$ and $Y = 0$. We can see the normal crossing issue here in a difference between $d_{B+1,C,E+1}$ and $d_{B,C+1,E+1}$ and their relationship to $d_{B,C,E}$. Namely $d_{B,C+1,E+1} = p^{-2}d_{B,C,E}$ whilst for example $d_{2C+2,C+1,E+1} = p^{-2}d_{2C,C,E}$.)

(2) $B < N$, $B \leqq C$. Using a transformation $b' = p^N/b$ and $c' = c/b$ it will suffice by the same analysis as in case 1 to calculate a value for

$$d_{B,C,E} = \mu\{(b,c) \in \mathbb{Z}_p^2 \colon v(b) = B, v(c) = C, v(-1^3 - c^2b + Db^2) \geqq E\}$$

in the case that $B \geqq 1$ and $C \geqq 0$.

Since $B \geqq 1$ the following lemma is clear:

Lemma 4.4. *$d_{B,C,E} = 0$ unless $E = 0$ in which case $d_{B,C,E} = p^{-B-C}(1-p^{-1})^2$.*

(3) $C < B, N$. Using a transformation $b' = b/c$ and $c' = p^N/c$ it will suffice to calculate for $B, C > 0$:

$$d_{B,C,E} = \mu\{(b,c) \in \mathbb{Z}_p^2 \colon v(b) = B, v(c) = C, v(-b^3 - c + Dbc^2) \geqq E\}.$$

Lemma 4.5. *Suppose $B, C > 0$. Then*

(1) *if $E \leqq \min\{3B, C\}$ then $d_{B,C,E} = p^{-C-B}(1-p^{-1})^2$;*

(2) *if $3B \neq C$ and $\min\{3B, C\} < E$ then $d_{B,C,E} = 0$;*

(3) *if $3B = C$ then $d_{B,3B,E} = p^{-E-B}(1-p^{-1})$.*

Proof. (1) and (2) are clear. (3) follows from the quantitative version of Hensel's Lemma for the non-singular curve $-X^3 - Y + DXY^2$:

Lemma 4.6. *Let $E \geqq 1$, $p \neq 2$. Let $(b,c) \in \mathbb{Z}/p^E\mathbb{Z}$ with $-b^3 - c + Dbc^2 = 0 \bmod p^E$. Then there exist exactly p elements $(b_1, c_1) \in \mathbb{Z}/p^{E+1}\mathbb{Z}$ with $b \equiv b_1, c \equiv c_1 \bmod p^E$ and $-b_1^3 - c_1 + Dbc_1^2 = 0 \bmod p^{E+1}$.*

Proof. Put $b_1 = b + \beta p^E$ and $c_1 = c + \gamma p^E$. We are required to count how many pairs $(\beta, \gamma) \in \{0, \ldots, p-1\}^2$ there are satisfying:

$$-b_1^3 - c_1 + Dbc_1^2 = 0 \bmod p^{E+1}. \qquad (4.3)$$

We know that $-b^3 - c + Dbc^2 = tp^E$ for some t. Hence expanding the equation (4.3) and pulling out the common power of p^E we have to solve:

$$t + \beta(Dc^2 - 3b^2) - 2\gamma(-1 + 2Dbc) = 0 \bmod p.$$

If $Dc^2 - 3b^2 = 0$ then $2Dbc^2/3 - c = c(2Dbc/3 - 1) = 0$. So $2Dbc - 1 \neq 0$ assuming $p \neq 2$. Hence we get exactly p lifts to solutions (b_1, c_1). This completes the proof of Lemma 4.6.

This lemma implies that whenever $E > B, C, 1$ then $d_{B,C,E+1} = p^{-1} d_{B,C,E}$.

If $E \leqq \min\{3B, C\}$ then $d_{B,C,E} = p^{-C} p^{-B} (1 - p^{-1})^2$.

If $3B \neq C$ and $\min\{3B, C\} < E$ then $d_{B,C,E} = 0$.

So the only interesting case is $d_{B,3B,E}$. Our lemma implies that

$$d_{B,3B,E} = p^{-E+(3B+1)} d_{B,3B,3B+1} = p^{-E+(3B+1)} p^{-B} p^{-(3B+1)} (1 - p^{-1}) = p^{-E-B}(1 - p^{-1}).$$

Remark 1. Note that the case distinction in (1), (2) and (3) reflects a blow-up of the variety $-b^3 - c^2 n + Dbn^2$ at the singular point $(0, 0, 0)$. Each case distinction represents the image of the variety in the three separate charts that define the blow-up.

The above analysis suffices to prove Proposition 4.1.

We now return to the proof of Theorem 2.2. We combine the expressions for $Z_1(M_1, N)$, $Z_2(M_2, N)$, $Z_3(M_3, N)$, the analysis of $a_{A,B,\tilde{B},C,E,N_1,N_2}$ with equation (3.17). Together they imply that there exists a finite partition $\bigcup_{i \in S} \Theta_i$ of $\mathbb{R}^{14}$ defined by linear inequalities with coefficients in $\mathbb{Q}$ and for each $i \in S$, polynomials $P_i(X)$ and $Q_i(X)$ and linear function $\alpha_i(\boldsymbol{x})$, $\beta_i(\boldsymbol{x})$, $\gamma_i(\boldsymbol{x})$ and $\delta_i(\boldsymbol{x})$ such that for p coprime to $2D$, putting $\boldsymbol{\Lambda} = (A, B, \tilde{B}, C, E, M_1, \ldots, M_6, N_1, N_2, N_3)$,

$$\zeta^{\triangleleft}_{L(E),p}(s) = \sum_{i \in S} \sum_{\boldsymbol{\Lambda} \in \mathbb{N}^{14} \cap \Theta_i} P_i(p) p^{\alpha_i(\boldsymbol{\Lambda}) + \gamma_i(\boldsymbol{\Lambda})s} + Q_I(p) |E(\mathbb{F}_p)| p^{\beta_i(\boldsymbol{\Lambda}) + \delta_i(\boldsymbol{\Lambda})s}.$$

Proposition 2.3 implies then that there exist two rational functions $P_1(X, Y)$ and $P_2(X, Y) \in \mathbb{Q}(X, Y)$ such that for p coprime to $2D$:

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

Hence Theorem 2.2 is proved.

5. Motivic zeta functions

In this section we show how to use the zeta function of a group to canonically associate to the group a subring of the Grothendieck ring. In particular we show why the elliptic curve $E = y^2 + x^3 - Dx$ is canonically associated to $G(E)$.

Let us recall the definition of the Grothendieck ring $\mathscr{M}$ of algebraic varieties over a field k. This is the ring generated by symbols $[S]$, for each S an algebraic variety over k, with the relations

(1) $[S] = [S']$ if S is isomorphic to S';

(2) $[S] = [S \backslash S'] + [S']$ if S' is closed in S; and

(3) $[S \times S'] = [S][S']$.

We denote by $\mathbf{L} = [\mathbb{A}_k^1]$ the Lefschetz motive.

It is tempting given an expression (valid for almost all p)

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

where

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

to associate the subring of the Grothendieck ring generated by the varieties. But how canonical or unique is this? In general it is not unique. It is possible to have non-isomorphic varieties with the same number of points mod p. For example, suppose that calculating $\zeta^{\triangleleft}_{G(E),p}(s)$ by an alternative method we produce a formula of the form

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

where E' is another elliptic curve. Then it does not mean that E and E' are isomorphic—distinct varieties over $\mathbb{Q}$ may have the same number of points in $\mathbb{F}_p$. In fact this is the case if the elliptic curves E and E' are isogenous. Much deeper is the fact, due to Faltings [6], that if, for almost all primes p, $|E(\mathbb{F}_p)| = |E'(\mathbb{F}_p)|$ then E and E' are isogenous. Isogenous elliptic curves define the same Chow motive. Therefore even without appealing to the formalism of motivic zeta functions, we may deduce:

Theorem 5.1. *The Chow motive of E is canonically associated with $G(E)$.*

However by using recent work with Loeser [5] on the concept of a motivic zeta function we can in fact show that E is canonically associated to $G(E)$. In [5] we define a motivic zeta function associated to a $\mathbb{Z}$-Lie algebra. This is a power series with coefficients in the Grothendieck ring of algebraic varieties.

Let L be a Lie algebra over $\mathbb{Z}$. Let $\mathscr{X}^{\leqq}(k)$ (respectively $\mathscr{X}^{\triangleleft}(k)$) denote the class of $k[[t]]$-subalgebras (respectively ideals) of $L \otimes k[[t]]$ where k is a finite extension of $\mathbb{Q}$. Let $A_n(\mathscr{X}^*)(k)$ denote the set of subalgebras or ideals in $\mathscr{X}^*(k)$ of codimension n in $L \otimes k[[t]]$. It is shown in [5] why $A_n(\mathscr{X}^*)$ is a constructible set of the Grassmannian $\operatorname{Gr}(L \otimes k[[t]]/t^n L \otimes k[[t]])$ and hence $[A_n(\mathscr{X}^*)]$ defines an element of the Grothendieck ring. The motivic zeta function encodes the subalgebras or ideals of $L \otimes k[[t]]$ and is defined as follows:

$$P^*_{L\otimes\mathbb{Q}[[t]]}(T) = \sum_{n=0}^{\infty}[A_n(\mathscr{X}^*)]T^n \in \mathscr{M}[[T]].$$

Denote by $\mathscr{M}_{\mathrm{loc}}$ the ring $\mathscr{M}[\mathbf{L}^{-1}]$ obtained by localization and define by $\mathscr{M}[T]_{\mathrm{loc}}$ the subring of $\mathscr{M}_{\mathrm{loc}}[[T]]$ generated by $\mathscr{M}_{\mathrm{loc}}[T]$ and the series $(1-\mathbf{L}^aT^b)^{-1}$ with $a\in\mathbb{Z}$ and $b\in\mathbb{N}$. It was shown in [5] that the power series $P^*_{L\otimes\mathbb{Q}[[t]]}(T)$ is a rational function belonging to $\mathscr{M}[T]_{\mathrm{loc}}$. Let $\mathscr{L}$ be the subring of $\mathscr{M}$ generated by the Lefschetz motive $\mathbf{L}$.

We make the following:

Definition 5.2. The *space of varieties* $\mathscr{M}^{\leqq}(L)$ (*respectively* $\mathscr{M}^{\triangleleft}(L)$) *of* L *counting subalgebras* (*respectively ideals*) is defined to be the smallest $\mathscr{L}$-submodule of $\mathscr{M}$ containing the coefficients $[A_n(\mathscr{X}^*)]$.

The rationality of $P^*_{L\otimes\mathbb{Q}[[t]]}(T)$ implies that this module is in fact finitely generated.

In [5] it is shown that by "taking the trace of Frobenius" of the motivic zeta function of $P^*_{L\otimes\mathbb{Q}[[t]]}(T)$ that one can recover the local zeta functions $\zeta^*_{L\otimes\mathbb{Z}_p}(s)$ for almost all primes. Let us explain this in more detail. For any variety X over $\mathbb{Q}$, one can choose a model $\mathscr{X}$ of X over $\mathbb{Z}$, and consider the number of points $n_p(X)$ of the reduction of $\mathscr{X}$ modulo p, for p a prime number. Of course, for some prime numbers p, $n_p(X)$ may depend of the model $\mathscr{X}$, but, for a given X, the numbers $n_p(X)$ are well defined for almost all p. If we denote by $\mathscr{P}$ the set of all primes, the sequence $n_p(X)$ is well defined as an element of the ring $\mathbb{Z}^{\mathscr{P}\prime}$, where, for any ring R, we set $R^{\mathscr{P}\prime} := \prod_{p\in\mathscr{P}} R/\bigoplus_{p\in\mathscr{P}} R$. Moreover, counting points being additive for disjoint unions and multiplicative for products, the sequence $n_p(X)$ in $\mathbb{Z}^{\mathscr{P}\prime}$ only depends on the class of X in $\mathscr{M}$ and may be extended to a ring morphism $n\colon \mathscr{M}\to\mathbb{Z}^{\mathscr{P}\prime}$. Setting $n_p(\mathbf{L}^{-1}) = 1/p$, one may extend uniquely n to a ring morphism $n\colon \mathscr{M}_{\mathrm{loc}}\to\mathbb{Q}^{\mathscr{P}\prime}$.

What is the relationship then between $\mathscr{M}^*(L)$ and the varieties that we have to count points on mod p to calculate $\zeta^*_{L\otimes\mathbb{Z}_p}(s)$?

Let E_i ($i\in T$, T finite) be the subvarieties arising from the resolution of singularities of the polynomial $F_L(\boldsymbol{X})$ associated to a presentation of L that arose in proving the explicit expression for $\zeta^*_{L\otimes\mathbb{Z}_p}(s)$ in [4]. (Note that the polynomial $F_L(\boldsymbol{X})$ depends on a choice of presentation for L and we also have a choice in the resolution we take in general.) As proved in [5] the proof of the explicit formula in [4] translates into an explicit expression for $P^*_{L\otimes\mathbb{Q}[[t]]}(T)$ of the same form

$$P^*_{L\otimes\mathbb{Q}[[t]]}(T) = \sum_{I\subseteqq T}[E_I^\circ]W_I(\mathbf{L},T)$$

where $W_I(X,Y)\in\mathbb{Q}(X,Y)$ are rational functions, and $E_I = \bigcap_{i\in I} E_i$ and $E_I^\circ = E_I\setminus\bigcup_{j\in T\setminus I} E_j$. When $I=\emptyset$, we have $E_\emptyset = Y$. Note however that the definition of $P^*_{L\otimes\mathbb{Q}[[t]]}(T)$ is independent of any choices made in the calculation.

Hence $\mathscr{M}^*(L)$ is contained in the $\mathscr{L}$-submodule generated by the varieties E_i ($i\in T$) which arise from a resolution of singularities of the polynomial $F_L(\boldsymbol{X})$ defined from a presentation for L.

For the Lie algebra $L(E)$ one can follow the calculation above for $\zeta^{\triangleleft}_{L(E)\otimes\mathbb{Z}_p}(s)$ to show that it formally translates into the same result for the motivic zeta function of $L(E)$:

Theorem 5.3. $P^{\triangleleft}_{L(E)\otimes\mathbb{Q}[[t]]}(T) = P_1(\mathbf{L}, T) + [E]P_2(\mathbf{L}, T)$.

Corollary 5.4. *$\mathscr{M}^{\triangleleft}\big(L(E)\big)$ is the $\mathscr{L}$-submodule generated by $[E]$. The elliptic curve $[E]$ is canonically associated with $L(E)$ and hence $G(E)$.*

In [3] we analysed the subalgebras of index p^3 in $L(E)$ to show that $\zeta^{\leqq}_{L(E)\otimes\mathbb{Z}_p}(s)$ is also not finitely uniform. Although the conditions are little more complex, I would conjecture the following:

Conjecture 5.5. *There exist two rational functions $P_1(X, Y)$ and $P_2(X, Y) \in \mathbb{Q}(X, Y)$ such that for almost all primes p:*

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

and

$$P^{\leqq}_{L(E)\otimes\mathbb{Q}[[t]]}(T) = P_1(\mathbf{L}, T) + [E]P_2(\mathbf{L}, T).$$

Hence $\mathscr{M}^{\leqq}\big(L(E)\big)$ is the additive subgroup generated by $[E]$ and the Lefschetz motive $\mathbf{L}$.

The method of considering minors of matrices developed in section 3 certainly has some prospect for generalization. It seems likely that it will provide the key for example to determining for a general class two nilpotent group or Lie algebra a candidate for the smallest subring of the Grothendieck ring required to express the associated motivic zeta function counting ideals or normal subgroups. In other words, to count these ideals or normal subgroups can be reduced to counting points on the varieties from a resolution of singularities of the polynomial defined by a product of the minors of these matrices.

Also the method of constructing a presentation of a Lie algebra from the determinants of certain matrices seems also ripe for generalization. For example, suppose that we have a variety V defined as the solution set of a homogeneous polynomial $f(X_1, \dots, X_n) \in \mathbb{Z}[\boldsymbol{X}]$ of degree r. Suppose we can define an $r \times r$ matrix $\big(g_{ij}(\boldsymbol{X})\big)$ where $g_{ij}(\boldsymbol{X})$ are linear polynomials with coefficients in $\mathbb{Z}$ with the property that

$$f(X_1, \dots, X_n) = \det\big(g_{ij}(\boldsymbol{X})\big).$$

Define a Lie algebra

$$L(V) = \langle A_1, \dots, A_r, B_1, \dots, B_r, X_1, \dots, X_n \colon [A_i, B_j] = g_{ij}(\boldsymbol{X})\rangle$$

where all other commutators are zero. Then the analysis above suggests that $\mathscr{M}^{\triangleleft}\big(L(V)\big)$ should contain the variety $[V]$. However it is also likely to contain all the varieties defined by the various minors of $\big(g_{ij}(\boldsymbol{X})\big)$. The other point to bare in mind is of course that there is the possibility that cancelling of varieties might occur which could see the variety V disappear.

This at least raises the interesting problem:

Problem. Let $f(X_1, \dots, X_n) \in \mathbb{Z}[\boldsymbol{X}]$ be a homogeneous polynomial. Does there exist an $r \times r$ matrix $\bigl(g_{ij}(\boldsymbol{X})\bigr)$ where $g_{ij}(\boldsymbol{X})$ are linear polynomials with coefficients in $\mathbb{Z}$ with the property that

$$f(X_1, \dots, X_n) = \det\bigl(g_{ij}(\boldsymbol{X})\bigr)?$$

Does there exist an $m \times m$ matrix $\bigl(g_{ij}(\boldsymbol{X}, Z)\bigr)$ where $g_{ij}(\boldsymbol{X}, Z)$ are linear polynomials with coefficients in $\mathbb{Z}$ with the property that

$$Z^{m-r} f(X_1, \dots, X_n) = \det\bigl(g_{ij}(\boldsymbol{X}, Z)\bigr)?$$

The second question allows us some more flexibility and we can define an associated Lie algebra:

$$L(f) = \langle A_1, \dots, A_m, B_1, \dots, B_m, X_1, \dots, X_n, Z \colon (A_i, B_j) = g_{ij}(\boldsymbol{X}, Z) \rangle.$$

Note that the elliptic curves we have considered of the form $E = y^2 + x^3 - Dx$ all have complex multiplication. If you would like an example of a nilpotent group which involves counting points mod p on an elliptic curve without complex multiplication, for example $E = y^2 + y + x^3 - x$, I would conjecture the following:

Conjecture 5.6. *Let G be the nilpotent group with presentation*:

$$G(E) = \left\langle \begin{matrix} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 \colon [x_1, x_4] = y_3, [x_1, x_5] = y_1, [x_1, x_6] = y_2, \\ [x_2, x_4] = y_1, [x_2, x_5] = y_3, [x_3, x_4] = y_2 y_3, [x_3, x_6] = y_1 \end{matrix} \right\rangle.$$

Then 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:

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

where E is the elliptic curve $E = y^2 + y + x^3 - x$ without complex multiplication.

Note that the associated Lie algebra has a presentation

$$L(E) = \left\langle \begin{matrix} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 \colon (x_1, x_4) = y_3, (x_1, x_5) = y_1, (x_1, x_6) = y_2, \\ (x_2, x_4) = y_1, (x_2, x_5) = y_3, (x_3, x_4) = y_2 + y_3, (x_3, x_6) = y_1 \end{matrix} \right\rangle$$

and

$$\det\bigl((x_i, x_{3+j})\bigr) = -(y_2^2 y_3 + y_2 y_3^2 + y_1^3 - y_1 y_3^2).$$

References

[1] *M. P. F. du Sautoy*, Zeta functions and counting finite p-groups, Electronic Research Announcements of the American Math. Soc. **5** (1999), 112–122.

[2] *M. P. F. du Sautoy*, Counting p-groups and nilpotent groups, Inst. Hautes Ét. Sci. Publ. Math. **92** (2000), 63–112.

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

[4] *M. P. F. du Sautoy* and *F. J. Grunewald*, Analytic properties of zeta functions and subgroup growth, Ann. Math. **152** (2000), 793–833.

[5] *M. P. F. du Sautoy* and *F. Loeser*, Motivic zeta functions of infinite dimensional Lie algebras, École Polytechnique preprint series 2000-12.

[6] *G. Faltings*, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 349–366.

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

Mathematical Institute, 24-29 St Giles, Oxford OX1 3LB
e-mail: dusautoy@maths.ox.ac.uk

Eingegangen 1. August 2000