COUNTING POINTS OF SCHEMES OVER FINITE RINGS AND COUNTING REPRESENTATIONS OF ARITHMETIC LATTICES

AVRAHAM AIZENBUD AND NIR AVNI

ABSTRACT. We relate the singularities of a scheme X to the asymptotics of the number of points of X over finite rings. This gives a partial answer to a question of Mustata. We use this result to count representations of arithmetic lattices. More precisely, if Γ is an arithmetic lattice whose $\mathbb{Q}$-rank is greater than one, let $r_n(\Gamma)$ be the number of irreducible n-dimensional representations of Γ up to isomorphism. We prove that there is a constant C (in fact, any $C > 40$ suffices) such that $r_n(\Gamma) = O(n^C)$ for every such Γ. This answers a question of Larsen and Lubotzky.

CONTENTS

1. INTRODUCTION

1.1. **Main results.** This paper has two main results. The first is about counting points of schemes over finite rings. In the formulation of this result, we use the notions of local complete intersection and rational singularities, which we recall in §2.2.

Theorem A. *Let X be a scheme of finite type over $\mathbb{Z}$. Assume that the generic fiber $X_{\mathbb{Q}} := X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{Q}$ of X is reduced, absolutely irreducible, and a local complete intersection. The following conditions are equivalent:*

(1) For any m,

$$\lim_{p\to\infty} \frac{|X(\mathbb{Z}/p^m)|}{p^{m\cdot \dim X_{\mathbb{Q}}}} = 1.$$

2010 *Mathematics Subject Classification.* Primary 14G05, 14G10, 20G05, 20G30, Secondary: 14B05, 20F69.

Key words and phrases. Representation Growth, Igusa zeta function.

(2) *There is a finite set S of prime numbers and a constant C such that*

$$\left|\frac{|X(\mathbb{Z}/p^m)|}{p^{m\cdot\dim X_{\mathbb{Q}}}}-1\right|<Cp^{-1/2},$$

for any prime $p\notin S$ and any $m\in\mathbb{N}$.

(3) *There is a finite set S of prime numbers and a constant C such that*

$$\left|\frac{|X(\mathbb{Z}/p^m)|}{p^{m\cdot\dim X_{\mathbb{Q}}}}-\frac{|X(\mathbb{Z}/p)|}{p^{\dim X_{\mathbb{Q}}}}\right|<Cp^{-1},$$

for any prime $p\notin S$ and any $m\in\mathbb{N}$.

(4) *$X_{\mathbb{Q}}$ has rational singularities.*

In fact, we prove this theorem also for other rings, see Theorem 3.0.3.

We use Theorem A to prove our second main result, counting representations of arithmetic groups of high rank (for example $SL_d(\mathbb{Z})$ for $d\geq 3$):

Theorem B. *(see Theorem II) For any algebraic group scheme G whose generic fiber $G_{\mathbb{Q}}$ is simple, connected, simply connected, and of $\mathbb{Q}$-rank at least two, and every $C>40$,*

$$\left|\left\{\begin{array}{l}\text{Irreducible representations of } G(\mathbb{Z})\\ \text{of dimension } n\end{array}\right\}\right|=o\left(n^C\right).$$

Theorem B (and its generalization Theorem II below) give an affirmative answer to a question of Larsen and Lubotzky (see [LL08, §11]).

1.2. **Counting points.**

1.2.1. *Background and results.* Let X be a scheme of finite type over $\mathbb{Z}$. We will be interested in the number of $\mathbb{Z}/N$-points of X, as a function of N. If $s\in\mathbb{C}$ has sufficiently large real part, then the series

$$\mathfrak{P}_X(s)=\sum_{N=1}^{\infty}|X(\mathbb{Z}/N)|\cdot N^{-s} \tag{1}$$

(where $|X(\mathbb{Z}/1)|=1$) converges absolutely and defines a holomorphic function. The domain of absolute convergence of the series (1) has the form $\{s\mid\Re(s)>\alpha_X\}$. We call α_X the abscissa of convergence of $\mathfrak{P}_X$. We have

$$\alpha_X=\limsup_{n\to\infty}\frac{\log\left(|X(\mathbb{Z}/1)|+\cdots+|X(\mathbb{Z}/n)|\right)}{\log n}.$$

The Chinese Remainder Theorem implies a decomposition $\mathfrak{P}_X(s)=\prod_p\mathfrak{P}_{X,p}(s)$, where the product is over the set of prime numbers, and each local component is defined as

$$\mathfrak{P}_{X,p}(s)=\sum_{n=0}^{\infty}|X(\mathbb{Z}/p^n)|\cdot p^{-ns}.$$

The functions $\mathfrak{P}_{X,p}(s)$ were introduced by Borevich and Shafarevich, who conjectured that they are rational functions of p^{-s}. This conjecture was proved by Igusa and Meuser. For hypersurfaces, the function $\mathfrak{P}_{X,p}$ is studied via the following variant of it, called the Igusa zeta function:

$$\mathcal{Z}_{X,p}(s) := (1-p^s)\mathfrak{P}_{X,p}(s+\dim X_{\mathbb{Q}}+1)+p^s.$$

See [Mus, §1.3] for a definition of $\mathcal{Z}_{X,p}(s)$ as a p-adic integral.

du Sautoy and Grunewald studied more general p-adic integrals and defined the following Euler product:

$$\mathcal{Z}_X(s)=\prod_p \frac{\mathcal{Z}_{X,p}(s)}{\mathcal{Z}_{X,p}(\infty)}.$$

In [Mus], Mustata asks for relations between the analytic properties of $\mathcal{Z}_X(s)$ and algebro-geometric properties of X. A partial answer is given by the following corollary of Theorem A:

Theorem I. *(see §4.4) Let X be a scheme of finite type over $\mathbb{Z}$, whose generic fiber $X_{\mathbb{Q}}$ is reduced, absolutely irreducible, a local complete intersection, and has rational singularities. Then there is a finite set S of primes such that*

(1) For every $p \notin S$, either $\mathfrak{P}_{X,p}(s)=1$, or the abscissa of convergence of $\mathfrak{P}_{X,p}(s)$ is $\dim X_{\mathbb{Q}}$ and $\mathfrak{P}_{X,p}(s)$ has a simple pole at $\dim X_{\mathbb{Q}}$.

(2) Let $Y = X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec} S^{-1}\mathbb{Z}$. The abscissa of convergence of $\mathfrak{P}_Y(s)$ is $\dim X_{\mathbb{Q}}+1$. Moreover, if $\zeta(s)$ denotes the Riemann zeta function, then the function $\mathfrak{P}_Y(s)/\zeta(s-\dim X_{\mathbb{Q}})$ can be analytically continued to $\{s \mid \Re(s) > \dim X_{\mathbb{Q}}+1/2\}$. In particular, $\mathfrak{P}_Y(s)$ has meromorphic continuation to $\Re(s) > \dim X_{\mathbb{Q}}+1/2$, and the only pole of the continued function on the line $\Re(s)=\dim X_{\mathbb{Q}}+1$ is a simple pole at $\dim X_{\mathbb{Q}}+1$.

(3) Denote $H_Y(n) := n^{-\dim Y_Q}|Y(\mathbb{Z}/n)|$. The Cesàro mean

$$\lim_{N\to\infty}\frac{H_Y(1)+\cdots+H_Y(N)}{N}$$

exists and is a positive real number.

(4) If X is a hypersurface, then the abscissa of convergence of $\mathcal{Z}_Y(s)$ is 0 and the function $\mathcal{Z}_Y(s)/\zeta(s+1)$ can be analytically continued to $\{s \mid \Re(s) > -1/2\}$. In particular, $\mathcal{Z}_Y(s)$ has meromorphic continuation to $\Re(s) > -1/2$ with a simple pole at 0.

Remark 1.2.1.

- *If X itself is a local complete intersection, then we can take S to be empty (so $Y=X$); see §4.4.*
- *Contrary to (3), the sequence $H_Y(N)$ might not converge. This happens even for elliptic curves.*

1.2.2. *Sketch of the proof of Theorem A.* We sketch the proof of the implication (4) $\implies$ (3), since it contains most of the ideas in the proof. We first show that $|X(\mathbb{Z}/p^m)| = |X(\mathbb{F}_p[t]/t^m)|$, for all but finitely many primes p. Next, we consider the function $F(p,m) := H_X(p^m) = \frac{|X(\mathbb{Z}/p^m)|}{p^{m\cdot \dim X}}$. We show the following:

(a) For every p, the function $m \mapsto F(p,m)$ is bounded. This follows from [AA].
(b) Condition (3) holds for bounded m. To show this, we analyze the jet schemes $\mathrm{Jet}_n X$, which are schemes that satisfy $\mathrm{Jet}_n X(\mathbb{F}_p) \cong X(\mathbb{F}_p[t]/t^n)$. We apply the Lang–Weil bounds, and a theorem of Mustata claiming that, under our assumption, $\mathrm{Jet}_n X$ are irreducible.
(c) There is a formula for $F(p,m)$ involving simple expressions in m and p, as well as the number of $\mathbb{F}_p$-points on finitely many varieties. This is a consequence of motivic integration.

We deduce from (c) and (a) (and the Lang–Weil bounds) that there are finitely many $m_1, \dots, m_k$ such that, for all m, there is i such that $|F(m,p) - F(m_i,p)| = O(p^{-1})$. Applying (b), we get the result.

1.3. **Counting representations.** For a topological group Γ, let $r_n(\Gamma)$ be the number of isomorphism classes of irreducible, n-dimensional, complex, continuous representations of Γ. The sequence $r_n(\Gamma)$ is called the representation growth sequence of Γ. In general, $r_n(\Gamma)$ can be infinite, but we will only consider groups for which $r_n(\Gamma)$ is finite for any n.

The study of the representation growth sequence was introduced at [Jai06] and [LM04]. For more recent results, we refer the reader to [AA], [Avn11], [AKOV], [LL08], [LS05a], and the references therein.

Throughout the paper, fix an affine group scheme G over $\mathbb{Z}$ whose generic fiber $G_{\mathbb{Q}}$ is $\mathbb{Q}$-simple, connected, and simply connected. If k is a global field and T is a finite set of places of k containing all archimedean ones, we denote by $O_{k,T}$ the ring T-integers:

$$O_{k,T} = \{x \in k \mid \forall v \notin T \text{ we have } \|x\|_v \leq 1\}.$$

We will study the representation growth of the group $\Gamma = G(O_{k,T})$. The main theorem of [LM04] implies that, if Γ satisfies the congruence subgroup property (See Definition 4.3.1 below), then the sequence $r_n(\Gamma)$ is bounded by some polynomial in n. Examples of groups with the congruence subgroup property are $G(O_{k,T})$ assuming the $\mathbb{Q}$-rank of $G_{\mathbb{Q}}$ is greater than one. In order to capture the rate of polynomial growth of $r_n(\Gamma)$, we use the following definition:

Definition. *Let Γ be a topological group, and assume that the sequence $r_n(\Gamma)$ is bounded by a polynomial. The* representation zeta function *of Γ is the Dirichlet series*

$$\zeta_\Gamma(s) = \sum_{n=1}^{\infty} r_n(\Gamma) n^{-s}. \tag{2}$$

Denote the abscissa of convergence of ζ_Γ by $\alpha(\Gamma)$.

As before, we have:

$$\alpha(\Gamma) = \limsup_{n\to\infty} \frac{\log\left(r_1(\Gamma) + \cdots + r_n(\Gamma)\right)}{\log n}. \tag{3}$$

If $\Gamma = G(O_{k,T})$ as above, the lim sup in (3) is actually a limit and is a rational number (see [Avn11]).

The abscissa $\alpha(\Gamma)$ is related to the singularities of the varieties parameterizing homomorphisms from surface groups to G:

Definition. *Let $n \in \mathbb{Z}_{\geq 1}$ and let Σ_n be the closed surface of genus n. The* deformation variety *of Σ_n in G is the variety*

$$\mathrm{Def}_{G,n} = \mathrm{Hom}(\pi_1(\Sigma_n), G) = \{(g_1, h_1, \ldots, g_n, h_n) \in G \mid [g_1, h_1]\cdots[g_n, h_n] = 1\}.$$

We remark that $\mathrm{Def}_{G_{\mathbb{Q}},n}$ has rational singularities if $n \geq \mathcal{C}(G)$, where

$$\mathcal{C}(G) = \begin{cases} 12 & G \text{ is of type } A, B, D \\ 21 & G \text{ is of type } C \\ \lceil \frac{\dim(\mathfrak{g})\,\mathrm{rank}(\mathfrak{g})}{2(\dim(\mathfrak{g}) - 2\,\mathrm{rank}(\mathfrak{g}))} \rceil + 1 & G \text{ is exceptional and } \mathfrak{g} \text{ is a simple factor of } \mathrm{Lie}(G_{\overline{\mathbb{Q}}}) \end{cases}.$$

For the classical groups, this is proved in [AA, Theorem VIII]. For the exceptional groups, this follows from [AKOV2, Corollary 2.3] and [AA, Theorem IV]. Note that $\mathcal{C}(G)$ is bounded by 21 for any G.

The following is a generalization of Theorem B:

Theorem II (See §4.3)**.** *There is a finite set S of prime numbers such that, for every global field k of characteristic not in S and every finite set T of places of k containing all archimedean ones, if $G(O_{k,T})$ satisfies the congruence subgroup property and $\mathrm{Def}_{G_{\mathbb{Q}},n}$ has rational singularities, then $\alpha(G(O_{k,T})) \leq 2n - 2$.*

As a result, we get the following dichotomy for the representation growth of an arithmetic group Γ in characteristic zero: either $r_n(\Gamma) = o(n^{747})$, or $r_n(\Gamma)$ is either infinite or grows super-polynomially in n (this happens if Γ does not satisfy the Congruence Subgroup Property—see [LM04]).

We will deduce Theorem II from the following adelic version, which is applicable also for low rank groups. In the following, if A is a ring, we denote its pro-finite completion by $\widehat{A}$.

Theorem III (See §4.2)**.** *There is a finite set S such that, for any global field k of characteristic not in S, any finite set T of places of k containing all archimedean places, and any natural number n, if $\mathrm{Def}_{G_{\mathbb{Q}},n}$ has rational singularities, then $\alpha\left(G(\widehat{O_{k,T}})\right) \leq 2n - 2$.*

From Theorem III and Theorem 2.5.1 below, we deduce the following statement about finite groups like $G(\mathbb{Z}/N\mathbb{Z})$, generalizing [AA, Corollary XI]:

Corollary IV. *There is a finite set S of primes such that, for any ring of integers $O_{k,T}$ of any global field k of characteristic not in S, there is a constant C such that the following holds. For any non-trivial ideal I of $O_{k,T}$, any natural number $n \geq 3$ such that $\mathrm{Def}_{G_{\mathbb{Q}},n-1}$ has rational singularities, and any $g \in G(O_{k,T}/I)$,*

$$\mathrm{Prob}\left([g_1,h_1]\cdots[g_n,h_n]=g\right) < \frac{C}{|G(O_{k,T}/I)|},$$

where $g_1, h_1, \ldots, g_n, h_n$ are uniformly distributed random elements of $G(O_{k,T}/I)$.

We deduce Theorem III from the following one:

Theorem V (See §4.1)**.** *For every $n \geq 2$ such that $\mathrm{Def}_{G_{\mathbb{Q}},n}$ has rational singularities, there is a finite set S of prime numbers and an integer C such that, for any $p \notin S$ and any unramified extension F of either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$, we have*

$$\zeta_{G(O_F)}(2n-2)-1 \leq C|O_F/I_F|^{-1},$$

where O_F is the ring of integers of F and I_F is its maximal ideal.

In order to prove Theorem V, we use the Frobenius formula (Theorem 2.5.1 below) that relates $\zeta_{G(O_F/I_F^m)}(2n)$ to the sizes of $\mathrm{Def}_{G,n}(O_F/I_F^m)$. These sizes, in turn, are related to the singularities of $\mathrm{Def}_{G,n}$ by Theorem A (or, more precisely, by Theorem 3.0.3).

Remark. *Consider the following statements:*

(1) $\alpha(G(O)) < 2n-2$.
(2) $\alpha(G(O_v)) < 2n-2$ *for any valuation v of O.*
(3) $\mathrm{Def}_{G,n}$ *has rational singularities.*
(4) $\alpha(G(O)) \leq 2n-2$.

Then (1) $\implies$ (2) $\iff$ (3) $\implies$ (4).

The implication (1) $\implies$ (2) *follows easily from the observation that, using the map $G(O) \to G(O_v)$, we get that $r_n(G(O_v)) \leq r_n(G(O))$. The equivalence* (2) $\iff$ (3) *is proved in* [AA]. *In this paper, we prove* (3) $\implies$ (4).

Remark. *The assumption that G is defined over $\mathbb{Z}$ can be weakened to assuming that G is defined over the ring of T-integers in a number field. Indeed, if $G \subset \mathrm{GL}_{O_{k,T}}$ is defined over $O_{k,T}$, let $\mathcal{G}$ be the Zariski closure of G in GL_{O_k}. The theorems above applied to the restriction of scalars $\mathrm{Res}_{O_k/\mathbb{Z}}\mathcal{G}$ imply the theorems for G.*

1.4. **Structure of the paper.** In §2 we give the necessary preliminaries for the paper. In §2.2-§2.3 we review the relevant algebraic geometry. In §2.4 we review the results of [AA]. In §2.5 we recall a theorem of Frobenius on representations of finite groups. In §2.6 we review relevant parts from the theory of motivic integration.

In §3 we prove (a generalization of) Theorem A. In §3.1,§3.3, and §3.4, we review the tools we use for the proof. The proof itself is given in §3.2, §3.5, §3.6, and §3.7.

In §4 we prove Theorems I, II, III, and V. As mentioned above, these imply Theorem B and Corollary IV.

1.5. **Acknowledgements.** We thank Vladimir Hinich for useful discussions. Part of this paper was written during the program 'Multiplicity Problems in Harmonic Analysis' held at the Hausdorff Institute (2012-2014). A.A. was partially supported by ISF grant 687/13, NSF grant DMS-1100943, and a Minerva foundation grant. N.A. was partially supported by NSF grants DMS-0901638 and DMS-1303205. Both of us were partially supported by BSF grant 2012247.

2. Preliminaries

2.1. **Conventions.** Throughout this article we use the following conventions:

- Let $X \to S$ and $Y \to S$ be S-schemes. We denote $X \times_S Y$ by X_Y. If $Y = \operatorname{Spec} R$ is affine, we write X_R instead of $X_{\operatorname{Spec} R}$.
- If p is a prime number and $q = p^n$ is a power of p, we denote the unique degree-n unramified extension of $\mathbb{Q}_p$ by $\mathbb{Q}_q$, its ring of integers by $\mathbb{Z}_q$, and the maximal ideal of $\mathbb{Z}_q$ by $\mathfrak{m}_q$.
- For a set S of prime numbers, let
$$\mathcal{P}_S = \{p^n \mid p \text{ is a prime number not in } S \text{ and } n \in \mathbb{Z}_{\geq 1}\}$$
be the set of sizes of finite fields of characteristics not in S.
- If $X \to S$ is a smooth map of relative dimension d, let $\Omega^d_{X/S}$ denote the line bundle of relative top differential forms.

2.2. **Singularities.** In this section, we review the notions of resolution of singularities, rational singularities, and complete intersections. For more detailed overview, we refer the reader to [AA, Appendix B].

Definition 2.2.1. *Let X be an algebraic variety defined over a field k. A* resolution of singularities *of X is a proper map $p : \tilde{X} \to X$ such that $\tilde{X}$ is smooth, p is birational, and the restriction of p to $p^{-1}(X^{sm})$ is an isomorphism.*

Definition 2.2.2 (cf. [KKMS73, I §3, page 50-51])**.** *Let X be an algebraic variety defined over a field k of characteristic 0.*

(1) We say that X has rational singularities *if, for any (equivalently, for some) resolution of singularities $p : \tilde{X} \to X$, the natural morphism $\mathcal{O}_X \to Rp_*(\mathcal{O}_{\tilde{X}})$ is an isomorphism.*

(2) A (usually singular) point $x \in X(k)$ is a rational singularity *if there is a Zariski neighborhood $U \subset X$ of x that has rational singularities.*

Definition 2.2.3. *Let X be a scheme of finite type over a ring R.*

(1) X is called a complete intersection *if there is an affine and smooth map $Y \to \operatorname{Spec} R$, a closed embedding $X \to Y$, commuting with the structure maps, and regular functions $f_1, \ldots, f_c \in O_Y(Y)$ such that the ideal of X in Y is generated by the f_i and each f_i is not a zero divisor in $O_Y(Y)/(f_1, \ldots, f_{i-1})$.*

(2) *X is called a* local complete intersection *if there is an open cover U_i of X such that each U_i is a complete intersection.*

2.3. **Jet schemes and Mustata's theorem.** In this section we recall the definition of jet schemes and quote one of our main tools, Mustata's theorem (see [Mus01]), which relates rational singularities and irreducibility of jet schemes. We will use repeatedly the following simple lemma:

Lemma 2.3.1. *Suppose that $Z \to T \to S$ and $X \to S$ are morphisms of schemes. Then* $\mathrm{Hom}_T(Z, X_T) \cong \mathrm{Hom}_S(Z, X)$.

We move on to define jet schemes.

Notation 2.3.2. *For a scheme Y, denote $Y^{[m]} = Y \times_{\mathrm{Spec}\,\mathbb{Z}} \mathrm{Spec}\,\mathbb{Z}[t]/t^{m+1}$.*

The projection $Y^{[m]} \to Y$ is finite and (locally) free. For every scheme S, the assignment $Y \mapsto Y^{[m]}$ gives rise to a functor between (Sch_S) and $(\mathrm{Sch}_{S^{[m]}})$.

Notation 2.3.3. *Let $X \to S$ be an affine morphism of finite type. Let $\mathscr{J}_m(X/S)$ be the restriction of scalars of $X^{[m]}$ along the map $S^{[m]} \to S$, i.e., the functor $\mathscr{J}_m(X/S) : (\mathrm{Sch}_S) \to (\mathrm{Set})$ given by*

$$\mathscr{J}_m(X/S)(Z) = \mathrm{Hom}_{S^{[m]}}(Z^{[m]}, X^{[m]}) \cong \mathrm{Hom}_S(Z^{[m]}, X).$$

From [BLR90, §7.6], we get

Theorem-Definition 2.3.4. *The functor $\mathscr{J}_m(X/S)$ is representable by a scheme of finite type over S. We call the representing scheme the m-th relative jet scheme of $X \to S$ and denote it by* $\mathrm{Jet}_m(X/S)$.

Let $X \to S$ be a morphism as above. For any morphisms $Z \to T \to S$ of schemes, we have a canonical bijections

$$\mathrm{Hom}_T(Z, \mathrm{Jet}_m(X_T/T)) \cong \mathrm{Hom}_T(Z^{[m]}, X_T) \cong \mathrm{Hom}_S(Z^{[m]}, X) \cong$$

$$\cong \mathrm{Hom}_S(Z, \mathrm{Jet}_m(X/S)) \cong \mathrm{Hom}_T(Z, \mathrm{Jet}_m(X/S)_T),$$

which is functorial in Z, and, therefore, defines an isomorphism $\mathrm{Jet}_m(X_T/T) \cong \mathrm{Jet}_m(X/S)_T$.

The following is Mustata's theorem:

Theorem 2.3.5 ([Mus01])**.** *Let X be an irreducible local complete intersection variety defined over a field k of characteristic 0. Then the following are equivalent:*

(1) *X has rational singularities.*
(2) *All the jet schemes* $\mathrm{Jet}_m(X/k)$ *are irreducible.*

2.4. **Rational singularities and integration.** In this section we review a result of [AA]. Recall that a measure m on a p-adic analytic manifold[1] is Schwartz if it is compactly supported and every point has a neighborhood U and a diffeomorphism $\varphi : U \to \mathbb{Z}_p^n$ such that $\varphi_* m$ is a scalar multiple of the Haar measure.

Theorem 2.4.1. *Let $\varphi : X \to Y$ be a map between smooth algebraic varieties defined over a non-archimedean local field F of characteristic zero, and let $x \in X(F)$. Assume that φ is flat at x, and x is a rational singularity of $\varphi^{-1}(\varphi(x))$. Then, there is a neighborhood $U \subset X(F)$ of x such that, for any Schwartz measure m on U, the measure $\varphi_*(m)$ has continuous density, i.e., can be written as a product of a Schwartz measure and a continuous function.*

2.5. **Frobenius formula.** We will use the following theorem of Frobenius:

Theorem 2.5.1 (Frobenius)**.** *Let Γ be a finite group, and let $n \geq 1$ be an integer. Then*

$$\left|\left\{(x_1, y_1, \ldots, x_n, y_n) \in \Gamma^{2n} \mid [x_1, y_1] \cdots [x_n, y_n] = 1\right\}\right| = |\Gamma|^{2n-1} \sum_{\pi \in \mathrm{Irr}(\Gamma)} \frac{1}{(\dim \pi)^{2n-2}},$$

where $\mathrm{Irr}(\Gamma)$ *denotes the set of isomorphism classes of irreducible representations of* Γ.

2.6. **Definable Integrals.** In this section, we recall the setting of definable p-adic integrals and state a uniformity result about p-adic integrals, which is a special case of [HK06, Theorem 1.3].

2.6.1. *The Denef–Pas language.* Let $L_\emptyset$ be the first-order language with:

- Three sorts, denoted by VF, RF, and VG, and called the valued field sort, the residue field sort, and the valuation group sort, respectively.
- Five constants, $0_{\mathrm{VF}}, 1_{\mathrm{VF}} \in \mathrm{VF}$, $0_{\mathrm{RF}}, 1_{\mathrm{RF}} \in \mathrm{RF}$, and $0_{\mathrm{VG}}, \infty_{\mathrm{VG}} \in \mathrm{VG}$.
- Seven functions, $+_{\mathrm{VF}} : \mathrm{VF} \times \mathrm{VF} \to \mathrm{VF}$, $\cdot_{\mathrm{VF}} : \mathrm{VF} \times \mathrm{VF} \to \mathrm{VF}$, $+_{\mathrm{RF}} : \mathrm{RF} \times \mathrm{RF} \to \mathrm{RF}$, $\cdot_{\mathrm{RF}} : \mathrm{RF} \times \mathrm{RF} \to \mathrm{RF}$, $+_{\mathrm{VG}} : \mathrm{VG} \times \mathrm{VG} \to \mathrm{VG}$, $\mathrm{val} : \mathrm{VF} \to \mathrm{VG}$, and $\mathrm{ac} : \mathrm{VF} \smallsetminus \{0_{\mathrm{VF}}\} \to \mathrm{RF}$.
- One binary relation, $<$, on VG.

2.6.2. *Structures.* Suppose that F is a field with a non-archimedean valuation v. Denote $O = \{x \in F \mid v(x) \geq 0\}$ and $\mathfrak{m} = \{x \in F \mid v(x) > 0\}$. Assume that the short exact sequence

$$1 \to O^\times/(1+\mathfrak{m}) \to F^\times/(1+\mathfrak{m}) \to F^\times/O^\times \to 1 \tag{4}$$

splits, and let $\sigma : F^\times/(1+\mathfrak{m}) \to O^\times/(1+\mathfrak{m})$ be such a splitting. An important example is the case where F is a non-archimedean local field. In this case, any uniformizer gives a splitting of (4).

From this data, we construct a structure for $L_\emptyset$ as follows: the sort VF is interpreted as F, the sort RF is interpreted as the residue field of F, and the sort VG is interpreted

[1] A p-adic manifold is a Hausdorff space X with a sheaf of functions that is locally isomorphic to the space $\mathbb{Z}_p^N$ together with the sheaf of functions that are locally given by convergent power series; see [Ser64].

as $\mathbb{Z}\cup\{\infty\}$. The function val is interpreted as the valuation v and the function ac is interpreted as the composition

$$F^\times \to F^\times/(1+\mathfrak{m}) \xrightarrow{\sigma} O^\times/(1+\mathfrak{m}) = \mathrm{RF}(F)\smallsetminus\{0\}\,.$$

The interpretation of the constants, relation, and the rest of the functions is clear. From this point on, when we write a valued field, we mean a valued field together with a splitting as above, and we consider it as a structure of the Denef–Pas language.

2.6.3. *Quantifier-free definable functions.* Suppose that $\mathfrak{S}$ is a structure for L. If $\varphi=\varphi(x_1,\dots,x_n,y_1,\dots,y_m,z_1,\dots,z_k)$ is a formula in L, where the variables x_i are of VF sort, the variables y_i are of RF sort, and the variables z_i are of VG sort, we denote

$$\varphi(\mathfrak{S})=\left\{(a_i,b_i,c_i)\in \mathrm{VF}(\mathfrak{S})^n\times\mathrm{RF}(\mathfrak{S})^m\times\mathrm{VG}(\mathfrak{S})^k \mid \varphi(a_i,b_i,c_i) \text{ holds in } \mathfrak{S}\right\}.$$

Definition 2.6.1.

(1) *We say that two formulas $\phi(x)$ and $\psi(x)$ are* equivalent *if, for every Henselian valued field F, we have $\phi(F)=\psi(F)$. An equivalence class of formulas is called a* definable set*. If X is a definable set and F is a Henselian valued field, we write $X(F)=\phi(F)$, for any $\phi\in X$.*

(2) *We say that a formula in L is* quantifier-free *if there are no quantifiers in it. A definable set is called quantifier-free, if there is a quantifier-free formula representing it.*

(3) *Suppose that X,Y are definable sets on variables x,y respectively (x and y are tuples of variables of the three sorts of L). A quantifier-free definable set Γ on the tuple of variables (x,y) is called a* quantifier-free definable function *if, for any Henselian valued field F, the set $\Gamma(F)$ is the graph of a function between $X(F)$ and $Y(F)$, which we also denote by $\Gamma(F)$.*

Example 2.6.2.

(1) *Let $X\subset\mathbb{A}^N_{\mathbb{Z}}$ be an affine scheme over $\operatorname{Spec}\mathbb{Z}$. Choose a generating set $\{p_1,\dots,p_M\}\subset\mathbb{Z}[x_1,\dots,x_N]$ for the ideal of polynomials vanishing on X, and let X_{VF} be the equivalence class of the formula*

$$(p_1(x_1,\dots,x_N)=0)\wedge\cdots(p_M(x_1,\dots,x_N)=0)\,,$$

where $x_1,\dots,x_N$ are of the VF *sort. For any valued field F, we have $X_{\mathrm{VF}}(F)=X(F)$. Similarly, there is also a quantifier-free definable set, denoted by X_{RF}, such that $X_{RF}(F)=X(k)$, for all Henselian valued fields F with residue field k.*

(2) *Let $f:X\to Y\to\operatorname{Spec}\mathbb{Z}$ be morphisms of schemes. Then there is a quantifier-free definable function $f_{\mathrm{VF}}:X_{\mathrm{VF}}\to Y_{\mathrm{VF}}$ such that, for every Henselian valued field F, the function $f_{\mathrm{VF}}(F):X_{\mathrm{VF}}(F)\to Y_{\mathrm{VF}}(F)$ coincides with the restriction of f to F points.*

(3) *If X is an algebraic variety and p is a regular function on X, the formula $y=\mathrm{val}(p(x))$ gives rise to a quantifier-free definable function from X_{VF} to* VG*.*

The following theorem follows from [HK06, Theorem 1.3]:

Theorem 2.6.3. *Let $X \to \operatorname{Spec}\mathbb{Z}$ be an affine and smooth morphism of relative dimension d, let $\omega \in \Gamma(X, \Omega^d_{X/\operatorname{Spec}\mathbb{Z}})$, and let $f_1, f_2 : X_{\mathrm{VF}} \to \mathrm{VG}$ be quantifier-free definable functions. Then there are*

(1) A constant M.
(2) A finite set S of prime numbers.
(3) (Finite or infinite) arithmetic progressions $I_1, \dots, I_M \subset \mathbb{Z}$.
(4) Polynomials $g_1, \dots, g_M \in \mathbb{Q}[x, y]$ such that $g_j(x, y)$ is positive on $I_j \times \mathbb{R}_{>1}$.
(5) Reduced affine schemes $V_1, \dots, V_M$ of finite type over $\mathbb{Z}$ which are smooth over $\operatorname{Spec}\mathbb{Z}[S^{-1}]$ such that $(V_i)_{\mathbb{Q}}$ are non-empty and irreducible.
(6) Rational numbers $\alpha_1, \dots, \alpha_M, \beta_1, \dots, \beta_M$.
(7) Positive integers $a_{j,k}$ for $j = 1, \dots, M$ and $k = 1, \dots, M_j$.

such that, if F is a local field with residue field $\mathbb{F}_q$ of characteristic not in S, $m \in \mathbb{Z}$, and $|\omega|_F$ denotes the measure on $X(F)$ corresponding to ω, then

$$\int_{\{x \in X(O_F) \mid f_1(x) = m\}} q^{-f_2(x)} |\omega|_F = \sum_{j=1}^{M} 1_{I_j}(m) |V_j(\mathbb{F}_q)| \frac{g_j(m, q) q^{\alpha_j m + \beta_j}}{\prod_{k=1}^{M_j} (1 - q^{-a_{jk}})}, \tag{5}$$

assuming the integral converges.

3. Rational singularities and points over finite local rings

In this section, we study the number of points of schemes over finite rings. For this, we introduce the following notation:

Definition 3.0.1. *Let X be a scheme of finite type over $\mathbb{Z}$ and let A be a finite ring. If $X_{\mathbb{Q}}$ is nonempty, define $h_X(A) = \frac{|X(A)|}{|A|^{\dim X_{\mathbb{Q}}}}$. If $X_{\mathbb{Q}}$ is empty, let $h_X(A) = 0$.*

We will mostly consider the finite rings $\mathbb{Z}_q/\mathfrak{m}_q^m$ and $\mathbb{F}_q[t]/t^m$. The following proposition relates the counting functions for these rings.

Proposition 3.0.2. *(see §3.2) Let X be a scheme of finite type over $\mathbb{Z}$. There is a finite set S of prime numbers such that $h_X(\mathbb{Z}_q/\mathfrak{m}_q^m) = h_X(\mathbb{F}_q[t]/t^m)$, for any $q \in \mathcal{P}_S$ and any $m \in \mathbb{N}$.*

The main result of this section is the following theorem that generalizes Theorem A:

Theorem 3.0.3. *Let X be a scheme of finite type over $\mathbb{Z}$ such that $X_{\mathbb{Q}}$ is equi-dimensional and a local complete intersection. The following are equivalent:*

(i) For any m, $\lim_{p\to\infty} h_X(\mathbb{Z}/p^m) = \lim_{p\to\infty} h_X(\mathbb{F}_p[t]/t^m) = 1$.
(ii) There is a finite set S of prime numbers and a constant C such that $|h_X(\mathbb{Z}_q/\mathfrak{m}_q^m) - 1| = |h_X(\mathbb{F}_q[t]/t^m) - 1| < Cq^{-1/2}$, for any $q \in \mathcal{P}_S$ and $m \in \mathbb{N}$.
(iii) $X_{\overline{\mathbb{Q}}}$ is irreducible and there is a finite set S of prime numbers and a constant C such that $|h_X(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_X(\mathbb{F}_q)| = |h_X(\mathbb{F}_q[t]/t^m) - h_X(\mathbb{F}_q)| < Cq^{-1}$, for any $q \in \mathcal{P}_S$ and $m \in \mathbb{N}$.

(iv) $X_{\overline{\mathbb{Q}}}$ *is reduced, irreducible, and has rational singularities.*

The proof of the Theorem 3.0.3 proves also that, if X itself is local complete intersection, then (iv) implies:

(v) $X_{\overline{\mathbb{Q}}}$ is irreducible and for any prime power q, the sequence $n \mapsto h_X(\mathbb{Z}_q/\mathfrak{m}_q^n)$ is bounded.

We conjecture that this implication is true without this additional assumption. Moreover, we conjecture that (i)-(v) are also equivalent to

(vi) $X_{\overline{\mathbb{Q}}}$ is irreducible and there is a finite set S of prime numbers such that, for any prime p not in S, the sequence $n \mapsto h_X(\mathbb{Z}/p^n)$ is bounded.

Remark 3.0.4. *One can weaken Condition* (ii) *by replacing the set* $\mathcal{P}_S$ *by any sequence* $p_n^{m_n}$ *of prime powers such that the* p_n *are distinct and any integral polynomial splits over some finite field of size* $p_n^{m_m}$*. For example, one can take the sequence of primes that are congruent to 1 modulo* n*.*

3.1. **Counting points and integrals.**

Proposition 3.1.1. *Let* F *be a local field,* O *its ring of integers, and* $\mathfrak{m}$ *its maximal ideal. Suppose that* $Y \to \operatorname{Spec} O$ *is a smooth map of schemes of (pure) relative dimension* d*. For any* m*, denote the map* $Y(O) \to Y(O/\mathfrak{m}^m)$ *by* r_m*. There is a unique Schwartz measure* μ *on* $Y(O)$ *such that, for every* m *and* $y_0 \in Y(O/\mathfrak{m}^m)$*,*

$$\mu(r_m^{-1}(y_0)) = |O/\mathfrak{m}|^{-dm}$$

The Proposition follows from the following standard lemma:

Lemma 3.1.2. *Let* $F, O, \mathfrak{m}, Y, d,$ *and* r_m *be as in Proposition 3.1.1. Assume that there is an invertible section* ω *of* $\Omega^d_{Y/\operatorname{Spec} O}$*. Then, for every* $y_0 \in Y(O/\mathfrak{m}^m)$*,*

$$\int_{r_m^{-1}(y_0)} |\omega| = |O/\mathfrak{m}|^{-dm}$$

Proof. If $U \subset Y$ is open and $y_0 \in U(O/\mathfrak{m}^m)$, then $r_m^{-1}(y_0) \subset U$. Hence, we can assume that Y is affine and there is an étale map $\pi : U \to \mathbb{A}^d_O$. Since π is étale, we get that π induces a bijection between $r_m^{-1}(y_0)$ and some ball B of radius $|O/\mathfrak{m}^m|^{-1}$ in O^d. Let $\eta = dx_1 \wedge \cdots \wedge dx_d \in \Omega^d(\mathbb{A}^d_O/\operatorname{Spec} O)$. Then $\pi^*\eta = J\omega$, for some regular function J. Since the map is étale, J is invertible. Hence, for every $p \in Y(O)$, we have $|J(p)| = 1$. Hence, $\int_{r_m^{-1}(y_0)} |\omega| = \int_B |\eta| = |O/\mathfrak{m}|^{-dm}$. □

Corollary 3.1.3. *Let* Z *be a scheme of finite type over* $\mathbb{Z}$ *and assume that* $Z_{\mathbb{Q}}$ *is affine. Then there are* $M, S, I_j, g_j, V_j, \alpha_j, \beta_j, M_j, a_{j,k}$ *as in Theorem 2.6.3 such that, for any* $q \in \mathcal{P}_S$ *and any* $m \geq 0$*,*

$$h_Z(\mathbb{Z}_q/\mathfrak{m}_q^m) = h_Z(\mathbb{F}_q[t]/t^m) = \sum_{j=1}^{M} 1_{I_j}(m)|V_j(\mathbb{F}_q)|\frac{g_j(m,q)q^{\alpha_j m+\beta_j}}{\prod_{k=1}^{M_j}(1-q^{-a_{jk}})}. \tag{6}$$

Proof. If $Z_{\mathbb{Q}}$ is empty, the claim is clear. Otherwise, let S_0 be a finite set of primes and let $f_1 \dots f_l \in S_0^{-1}\mathbb{Z}[x_1, \dots, x_N]$ be polynomials such that $Z_{S_0^{-1}\mathbb{Z}}$ is the scheme defined by $f_1 = \dots = f_l = 0$ in $\mathbb{A}^N_{S_0^{-1}\mathbb{Z}}$. Let F be a local field of characteristic not in S, O be its ring of integers and $\mathfrak{m}$ be its maximal ideal. By Lemma 3.1.2 we have:

$$|Z(O/\mathfrak{m}^m)| = |O/\mathfrak{m}|^{Nm} \int_{\{x \in O^N | \min_j(\mathrm{val}(f_j(x))) \geq m\}} |dx_1 \wedge \dots \wedge dx_N| =$$
$$= |O/\mathfrak{m}|^{Nm} \sum_{n \geq m} \int_{\{x \in O^N | \min_j(\mathrm{val}(f_j(x))) = n\}} |dx_1 \wedge \dots \wedge dx_N|.$$

The claim now follows from Theorem 2.6.3. □

3.2. **Proof of Proposition 3.0.2.** We will use the following simple lemma.

Lemma 3.2.1. *Let $X = U_1 \cup U_2$ be an open cover of a scheme. Then, for any finite local ring A, we have*

- $|X(A)| = |U_1(A)| + |U_2(A)| - |U_1 \cap U_2(A)|$.
- $|X(A)| \geq |U_1(A)|$.

We also need the following well known fact:

Lemma 3.2.2. *(cf. [Har77, Ex. II.4.3]) Let X be a separated scheme, and let $U_1, U_2 \subset X$ be open affine subschemes. Then $U_1 \cap U_2$ is affine.*

Proof of Proposition 3.0.2. We will show that there is a set S of prime numbers such that $|X(\mathbb{Z}_q/\mathfrak{m}_q^m)| = |X(\mathbb{F}_q[t]/t^m)|$, for all $q \in \mathcal{P}_S$ and all m. We prove this claim in the following cases:

Case 1 X is affine.
The claim follows from Corollary 3.1.3.

Case 2 X is separated.
The proof is by induction on the minimal size of an affine cover of X. The base is the affine case dicussed above. For the transition, let $X = \bigcup_1^n U_i$ be an affine cover and assume that we proved the claim for schemes that can be covered by less then n affine open subschemes. Let $U = \bigcup_2^n U_i$. By induction and Lemma 3.2.2, we know the statement for $U_1, U, U \cap U_1$. Thus Lemma 3.2.1 implies the assertion.

Case 3 The general case.
The proof is by induction on the minimal size of an affine cover of X by separated schemes. The base is the previous case. The transition is analogous to the proof in the previous case.

□

3.3. **Lang–Weil estimates.** We start with the following notation.

Notation 3.3.1. *Suppose that X is a scheme of finite type over* $\operatorname{Spec}\mathbb{Z}$ *and that k is a field. We denote the number of irreducible components of $X_{\overline{k}}$ that are defined over k and have dimension* $\dim X_k$ *by $c_X(k)$. If q is a prime power, we also write $c_X(q)$ instead of $c_X(\mathbb{F}_q)$.*

Theorem 3.3.2 (Lang–Weil (cf. [LW54]))**.** *Let X be a scheme of finite type over* $\operatorname{Spec}\mathbb{Z}$*. Let $d = \dim X_{\mathbb{Q}}$. There is a finite set S of prime numbers and a constant C such that, for any $q \in \mathcal{P}_S$,*

$$\left|\frac{|X(\mathbb{F}_q)|}{q^d} - c_X(q)\right| < Cq^{-\frac{1}{2}}.$$

3.4. **Irreducible components modulo p.** In this subsection, we prove the following

Proposition 3.4.1. *Suppose that X is a scheme of finite type over* $\operatorname{Spec}\mathbb{Z}$*. Assume that $X_{\mathbb{Q}}$ is irreducible. Then*

(1) For almost all prime numbers p, we have $c_X(\overline{\mathbb{F}_p}) = c_X(\overline{\mathbb{Q}})$.
(2) There are infinitely many prime numbers p such that $c_X(p) = c_X(\overline{\mathbb{Q}})$.

In order to prove the proposition, we recall the following notions and facts:

Definition 3.4.2. *Let S be an irreducible scheme with generic point η, let s be a closed point of S, and let $\varphi : X \to S$ be a morphism of finite type. Define a relation $\mathfrak{R}_{S,s}$ between the set of irreducible components of $X_\eta := \varphi^{-1}(\eta)$ and the set of irreducible components of $X_s := \varphi^{-1}(s)$ by $(Y_1, Y_2) \in \mathfrak{R}_{S,s}$ if $Y_2 \subset \overline{Y_1}$.*

Theorem 3.4.3. *(cf.* [Gro66, Proposition 9.7.8]*) Let S be an irreducible scheme with generic point η and let $\varphi : X \to S$ be a morphism of finite type. Assume that all irreducible components of X_η are absolutely irreducible. There is an open set $U \subset S$ such that, for any closed point $s \in U$,*

(1) All irreducible components of X_s are absolutely irreducible.
(2) The relation $\mathfrak{R}_{\eta,s}$ is the graph of a bijection.

Let $X \to \operatorname{Spec}\mathbb{Z}$ be a scheme of finite type. Let $L/\mathbb{Q}$ be a Galois extension such that all irreducible components of $X \times \operatorname{Spec} L$ are absolutely irreducible, and let O be the ring of integers of L. The group $\operatorname{Gal}(L/\mathbb{Q})$ acts on the set of irreducible components of $X \times \operatorname{Spec} L$. For any prime ideal $\mathfrak{p}$ of O with residue field $k_\mathfrak{p}$, consider the decomposition group $D_\mathfrak{p} = \{\sigma \in \operatorname{Gal}(L/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$, and the homomorphism $\Phi_\mathfrak{p} : D_\mathfrak{p} \to \operatorname{Gal}(k_\mathfrak{p}/\mathbb{F}_p)$. The group $\operatorname{Gal}(k_\mathfrak{p}/\mathbb{F}_p)$ acts on the set of irreducible components of $X_{k_\mathfrak{p}}$. The following is obvious

Proposition 3.4.4. *Under the assumptions above, for any $(Y_1, Y_2) \in \mathfrak{R}_{(0),\mathfrak{p}}$ and $\sigma \in D_\mathfrak{p}$, we have $(\sigma \cdot Y_1, \Phi_\mathfrak{p}(\sigma) \cdot Y_2) \in \mathfrak{R}_{(0),\mathfrak{p}}$.*

Proposition 3.4.4, Theorem 3.4.3, and Chebotarev's density theorem imply Proposition 3.4.1.

Corollary 3.4.5. *Let X be a scheme of finite type over $\operatorname{Spec}\mathbb{Z}$, and let $U \subset X$ be an open dense subscheme. There is finite set S of prime numbers and a constant C such that $h_X(\mathbb{F}_q) - h_U(\mathbb{F}_q) < Cq^{-1}$ for any $q \in \mathcal{P}_S$.*

Proof. Let $Z = X \smallsetminus U$. We have $\dim Z_{\mathbb{Q}} < \dim X_{\mathbb{Q}} = \dim U_{\mathbb{Q}}$. Letting $C = c_Z(\overline{\mathbb{Q}})$, the Lang–Weil estimates and Proposition 3.4.1(1) imply that there is a finite set of primes S such that

$$h_X(\mathbb{F}_q) - h_U(\mathbb{F}_q) = \frac{|Z(\mathbb{F}_q)|}{q^{\dim X_{\mathbb{Q}}}} < Cq^{-1}$$

for every $q \in \mathcal{P}_S$. □

3.5. **Proof of the implication** (iii) $\implies$ (ii)**.** It is enough to show that there is a finite set S' of prime numbers and a constant C' such that $|h_X(\mathbb{F}_q) - 1| < C'q^{-1/2}$ for all $q \in \mathcal{P}_{S'}$. By the assumption and Proposition 3.4.1(1), there is a finite set T of prime numbers such that $c_X(q) = 1$ for all $q \in \mathcal{P}_T$. The Lang-Weil estimates imply the result.

3.6. **Proof of the implication** (i) $\implies$ (iv)**.** Let $m \in \mathbb{N}$ and $X^{(m)} = \operatorname{Jet}_m(X/\operatorname{Spec}\mathbb{Z})$. There is a finite set S of prime numbers such that $X_{\mathbb{F}_p}$ is a local complete intersection and $\dim X^{(m)}_{\mathbb{F}_p} = \dim X^{(m)}_{\mathbb{Q}}$ for all $p \notin S$. By Proposition 3.4.1(1), we can enlarge S and assume, in addition, that $c_{X^{(m)}}(\overline{\mathbb{F}_p}) = c_{X^{(m)}}(\overline{\mathbb{Q}})$ for all $p \notin S$. By the Lang–Weil estimates, we get that

$$\left| \frac{h_X(\mathbb{F}_p[t]/t^m)}{p^{\dim X^{(m)}_{\mathbb{F}_q} - m\dim X_{\mathbb{Q}}}} - c_{X^{(m)}}(p) \right| = \left| \frac{|X^{(m)}(\mathbb{F}_p)|}{p^{\dim X^{(m)}_{\mathbb{F}_p}}} - c_{X^{(m)}}(p) \right| \underset{p\to\infty}{\longrightarrow} 0,$$

By Proposition 3.4.1(2), there are infinitely many primes p such that $c_{X^{(m)}}(p) = c_{X^{(m)}}(\overline{\mathbb{Q}})$. Taking the limit over those and using the assumption (i), we get that $p^{m\dim X_{\mathbb{Q}} - \dim X^{(m)}_{\mathbb{F}_q}} \to c_{X^{(m)}}(\overline{\mathbb{Q}})$, which implies that $\dim X^{(m)}_{\mathbb{Q}} = m\dim X_{\mathbb{Q}}$ and that $c_{X^{(m)}}(\overline{\mathbb{Q}}) = 1$. If $X_{\mathbb{Q}}$ were not reduced, then there would be a non-empty open set of points whose tangent space has dimension greater than $\dim X_{\mathbb{Q}}$, so $\dim X^{(2)}_{\mathbb{Q}} = \dim TX_{\mathbb{Q}}$ would be larger than $2\dim X_{\mathbb{Q}}$, a contradiction. Hence, $X_{\mathbb{Q}}$ is reduced. Since X is a local complete intersection, each irreducible component of $X^{(m)}_{\mathbb{Q}}$ has dimension at least $m \cdot \dim X_{\mathbb{Q}}$. Thus, $X^{(m)}_{\mathbb{Q}}$ is absolutely irreducible. By Mustata's theorem, X has rational singularities.

3.7. **The implication** (iv) $\implies$ (iii)**.** If $X_{\mathbb{Q}}$ is empty, the claim is trivial. Hence, in the following, we will assume that $X_{\mathbb{Q}}$ is non-empty.

3.7.1. *The case of fixed m.*

Proposition 3.7.1. *Assume that X satisfies condition* (iv)*. Then, for any m, there is a finite set $S(m)$ of prime numbers and a constant $C(m)$ such that $|h_X(\mathbb{F}_q[t]/t^m) - h_X(\mathbb{F}_q)| < C(m)q^{-1}$ for all $q \in \mathcal{P}_{S(m)}$.*

Proof. Let $U \subset X$ be the smooth locus of the structure map $X \to \operatorname{Spec}\mathbb{Z}$. Since $X_{\mathbb{Q}}$ is reduced, $U_{\mathbb{Q}}$ is dense in $X_{\mathbb{Q}}$. It follows that there is a finite set S_1 of prime numbers such that $U_{\mathbb{F}_p}$ is a dense subvariety of $X_{\mathbb{F}_p}$, for all $p \notin S_1$. By enlarging S_1 if needed, we can assume that $\dim X_{\mathbb{F}_p} = \dim X_{\mathbb{Q}}$ for all $p \notin S_1$.

Denote $X^{(m)} = \operatorname{Jet}_m(X/\operatorname{Spec}\mathbb{Z})$ and $U^{(m)} = \operatorname{Jet}_m(U/\operatorname{Spec}\mathbb{Z})$. For any $p \notin S_1$ and any n, the natural projection $U^{(n+1)}_{\mathbb{F}_p} \to U^{(n)}_{\mathbb{F}_p}$ is an $\mathbb{A}^{\dim U_{\mathbb{Q}}}$-bundle. In particular, $|U^{(m)}(\mathbb{F}_q)| = |U(\mathbb{F}_q)| \cdot q^{(m-1)\dim U_{\mathbb{F}_q}}$. Hence,

$$h_U(\mathbb{F}_q[t]/t^m) = h_U(\mathbb{F}_q). \tag{7}$$

By Corollary 3.4.5, there is a finite set $S_2 \supset S_1$ of prime numbers and a constant C_2 such that

$$|h_X(\mathbb{F}_q) - h_U(\mathbb{F}_q)| < C_2 q^{-1} \quad q \in \mathcal{P}_{S_2}. \tag{8}$$

Since $X_{\mathbb{Q}}$ has rational singularities, Mustata's theorem implies that $U^{(m)}_{\mathbb{Q}}$ is dense in $X^{(m)}_{\mathbb{Q}}$. There is a finite set $S_3(m)$ of prime numbers such that $U^{(m)}_{\mathbb{F}_p}$ is dense in $X^{(m)}_{\mathbb{F}_p}$, for all $p \notin S_3(m)$. Applying Corollary 3.4.5, we get that there is a finite set $S_4(m) \supset S_3(m)$ of prime numbers and a constant C_4 such that

$$|h_X(\mathbb{F}_q[t]/t^m) - h_U(\mathbb{F}_q[t]/t^m)| = |h_{X^{(m)}}(\mathbb{F}_q) - h_{U^{(m)}}(\mathbb{F}_q)| < C_4 q^{-1} \quad q \in \mathcal{P}_{S_4(m)}. \tag{9}$$

The claim now follows from (7), (8), and (9).

□

3.7.2. (iv) $\implies$ (vi) *in the case where $X_{\mathbb{Q}}$ is a complete intersection.* Since $X_{\mathbb{Q}}$ is a complete intersection, there is a smooth algebraic variety $\overline{Y}$ over $\mathbb{Q}$, a closed embedding $X_{\mathbb{Q}} \to \overline{Y}$, and a regular map $\overline{\varphi} : \overline{Y} \to \mathbb{A}^N_{\mathbb{Q}}$, which is flat above 0, such that $X_{\mathbb{Q}} \cong \overline{\varphi}^{-1}(0)$. There is a finite set S of primes and a $\mathbb{Z}[S^{-1}]$-scheme Y of finite type and a regular map $\varphi : Y \to \mathbb{A}^N_{\mathbb{Z}[S^{-1}]}$ such that $Y_{\mathbb{Q}} = \overline{Y}$ and $\varphi_{\mathbb{Q}} = \overline{\varphi}$. After, possibly, enlarging S, we can assume that $Y_{\mathbb{Z}[S^{-1}]}$ is smooth over $\operatorname{Spec}\mathbb{Z}[S^{-1}]$, the restriction $\varphi_{\mathbb{Z}[S^{-1}]}$ is flat above 0, and the isomorphism $X_{\mathbb{Q}} \cong \overline{\varphi}^{-1}(0)$ extends to an isomorphism $X_{\mathbb{Z}[S^{-1}]} \cong \varphi^{-1}_{\mathbb{Z}[S^{-1}]}(0)$. It is enough to show, for any $p \notin S$, that $h_{\varphi^{-1}_{\mathbb{Z}[S^{-1}]}(0)}(\mathbb{Z}/p^m)$ is bounded uniformly in m.

Fix $p \notin S$. Let μ be the measure on $Y(\mathbb{Z}_p)$ given by Corollary 3.1.1. We have

$$\mu\left(\varphi^{-1}(p^m\mathbb{Z}_p^N)\right) = \mu\left(r_m^{-1}(\varphi^{-1}_{\mathbb{Z}/p^m}(0)(\mathbb{Z}/p^m))\right) = \sum_{x \in \varphi^{-1}_{\mathbb{Z}/p^m}(0)(\mathbb{Z}/p^m)} \mu\left(r_m^{-1}(x)\right) = p^{-m\dim Y_{\mathbb{Q}}} |\varphi^{-1}_{\mathbb{Z}/p^m}(0)(\mathbb{Z}/p^m)|.$$

By Theorem 2.4.1, there is a constant C such that, for any $m \in \mathbb{N}$,

$$\mu\left(\varphi^{-1}(p^m\mathbb{Z}_p^N)\right) = \varphi_*\mu\left(p^m\mathbb{Z}_p^N\right) < \frac{C}{p^{mN}}.$$

we get that

$$|X(\mathbb{Z}/p^m)| = |\varphi^{-1}_{\mathbb{Z}/p^m}(0)(\mathbb{Z}/p^m)| < C p^{\dim Y_{\mathbb{Q}} - N}.$$

Since $\dim Y_{\mathbb{Q}} - N = \dim X_{\mathbb{Q}}$, this implies the estimate we want.

3.7.3. (iv) $\implies$ (iii) *in the case where $X_{\mathbb{Q}}$ is a complete intersection.* Assume now that X is a complete intersection and satisfies (iv). Applying Corollary 3.1.3, we get $M, S, I_j, g_j, V_j, \alpha_j, \beta_j, M_j, a_{j,k}$ such that

$$h_X(\mathbb{Z}_q/\mathfrak{m}_q^m) = h_X(\mathbb{F}_q[t]/t^m) = \sum_{j=1}^{M} 1_{I_j}(m)|V_j(\mathbb{F}_q)|\frac{g_j(m,q)q^{\alpha_j m+\beta_j}}{\prod_{k=1}^{M_j}(1-q^{-a_{jk}})} \tag{10}$$

for all $q \in \mathcal{P}_S$ and m.

Define an equivalence relation on $\mathbb{N}$ by $m_1 \sim m_2$ iff $\forall j$ we have $m_1 \in I_j \Leftrightarrow m_2 \in I_j$. We will show that there is a constant C such that, for any $m_1 \sim m_2$, we have

$$|h_X(\mathbb{Z}_q/\mathfrak{m}_q^{m_1}) - h_X(\mathbb{Z}_q/\mathfrak{m}_q^{m_2})| < Cq^{-1}. \tag{11}$$

Property (iii) for X will follow by applying Proposition 3.7.1 to representatives of the finitely many equivalence classes of $\sim$.

If the equivalence class of m_1 and m_2 is finite then (11) follows from Proposition 3.7.1. Thus, we can assume that all I_j are infinite.

Lemma 3.7.2. *Let V be a scheme of finite type over* $\operatorname{Spec}\mathbb{Z}$ *whose generic fiber is non-empty, let $g(x,y)$ be a real polynomial, let $\alpha, \beta \in \mathbb{R}$, and let $a_1, \dots, a_n$ be negative integers, Set*

$$P(m,q) = |V(\mathbb{F}_q)| \cdot \frac{g(m,q)q^{\alpha m+\beta}}{\prod_1^n (1-q^{a_k})}.$$

Then the following claims hold:

1. *Assume that either*
   (a) *$\alpha > 0$ or*
   (b) *$\alpha = 0$ and g depends on m non-trivially (i.e. $\frac{\partial g}{\partial m} \neq 0$).*
   Then $\lim_{m\to\infty} P(m,p) = \pm\infty$ for infinitely many primes p.
2. *If $\alpha < 0$ then there is a constant D such that $|P(m,q)| < q^{-1}$ for $m > D$ and any prime power q.*

Proof.

(1) Under the assumptions, the limit $\lim_{m\to\infty} P(m,p)$ will be infinity if $V(\mathbb{F}_p) \neq \emptyset$. By the Lang–Weil bounds and Proposition 3.4.1(2), this happens for infinitely many primes.

(2) Suppose that the degree of g is d. Then there is a constant M such that $|g(m,q)| \leq Mm^d q^d$. In addition, There is a constant e such that $|V(\mathbb{F}_q)| < eq^e$ for all prime powers q. Hence, there is a constant C such that

$$|P(m,q)| \leq Cm^d q^{\alpha m+\beta+d+e}.$$

This implies the assertion.

□

By §3.7.2, after enlarging S, we have that

$$\sup_m h_X(\mathbb{F}_p[t]/t^m) = \sup_m h_X(\mathbb{Z}/p^m) < \infty,$$

for any prime $p \notin S$. Since each summand in the right hand side of (10) is non-negative, we get that, for each j and $p \notin S$,

$$\sup_m 1_{I_j}(m)|V_j(\mathbb{F}_q)|\frac{g_j(m,q)q^{\alpha_j m+\beta_j}}{\prod(1-q^{-a_{jk}})} < \infty. \tag{12}$$

For each j, Lemma 3.7.2 implies that either $\alpha_j < 0$ or $\alpha_j = 0$ and g_j is independent of m. Moreover, there is D such that

$$|V_j(\mathbb{F}_q)|\frac{g_j(m,q)q^{\alpha_j m+\beta_j}}{\prod(1-q^{-a_{jk}})} < q^{-1}, \tag{13}$$

if $\alpha_j < 0$ and $m > D$. Let $J_1 = \{j \mid \alpha_j < 0\}$.

By (13) and (10) we get that, for any $m > D$ and $q \in \mathcal{P}_S$,

$$\left| h_X(\mathbb{F}_q[t]/t^m) - \sum_{j\notin J_1} 1_{I_j}(m)|V_j(\mathbb{F}_q)|\frac{g_j(m,q)q^{\alpha_j m+\beta_j}}{\prod(1-q^{-a_{jk}})} \right| < |J_1|q^{-1}.$$

Note that the sum on the left hand side depends only on q and the equivalence class of m. Thus, if $m_1, m_2 > D$, $m_1 \sim m_2$, and $q \in \mathcal{P}_S$, then

$$|h_X(\mathbb{F}_q[t]/t^{m_1}) - h_X(\mathbb{F}_q[t]/t^{m_2})| < 2|J_1|q^{-1}.$$

This, together with proposition 3.7.1, implies (11).

3.7.4. (iv) $\implies$ (iii) *in general.* The proof is by induction on the size of the minimal open cover of $X_{\mathbb{Q}}$ by complete intersection varieties. The base is §3.7.3. For the transition, let $X_{\mathbb{Q}} = \bigcup_1^n X'_i$ be a minimal open cover of $X_{\mathbb{Q}}$ by complete intersection varieties and assume that we know the assertion for any Y such that $Y_{\mathbb{Q}}$ can be covered by less then n complete intersection varieties. We can choose complete intersection schemes X_i and a finite set of primes S_0 such that $X_{S_0^{-1}\mathbb{Z}} = \bigcup_1^n X_i$ is an open cover.

Let $U = \bigcup_2^n X_i$ and let $V \subset U \cap X_1$ be a complete intersection, open, and non-empty subscheme. By induction, we know that there is a finite set $S_1 \supset S_0$ of prime numbers and a constant C_1 such that, for any $q \in \mathcal{P}_{S_1}$ and $m \in \mathbb{N}$, we have:

- $|h_{X_1}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{X_1}(\mathbb{F}_q)| < C_1 q^{-1}$.
- $|h_U(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_U(\mathbb{F}_q)| < C_1 q^{-1}$.
- $|h_V(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_V(\mathbb{F}_q)| < C_1 q^{-1}$.

By Lemma 3.2.1,

$$\begin{aligned} &h_X(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_X(\mathbb{F}_q) = \\ &= \left(h_{X_1}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{X_1}(\mathbb{F}_q)\right) + \left(h_U(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_U(\mathbb{F}_q)\right) - \left(h_{X_1\cap U}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{X_1\cap U}(\mathbb{F}_q)\right), \end{aligned}$$

and so it is enough to prove that $|h_{X_1\cap U}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{X_1\cap U}(\mathbb{F}_q)| = O(q^{-1})$.

By Corollary 3.4.5, there exist a finite set $S \supset S_1$ of prime numbers and a constant C_2 such that, for any $q \in \mathcal{P}_S$ and $m \in \mathbb{N}$, we have:

- $|h_{X_1}(\mathbb{F}_q) - h_{X_1\cap U}(\mathbb{F}_q)| < C_2 q^{-1}$.
- $|h_{X_1\cap U}(\mathbb{F}_q) - h_V(\mathbb{F}_q)| < C_2 q^{-1}$.

Now,

$$h_{X_1\cap U}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{X_1\cap U}(\mathbb{F}_q) \le h_{X_1}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{X_1}(\mathbb{F}_q) + h_{X_1}(\mathbb{F}_q) - h_{X_1\cap U}(\mathbb{F}_q) < (C_1+C_2)q^{-1},$$

Similarly,

$$h_{X_1\cap U}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{X_1\cap U}(\mathbb{F}_q) \ge h_V(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_V(\mathbb{F}_q) + h_V(\mathbb{F}_q) - h_{X_1\cap U}(\mathbb{F}_q) > -(C_1+C_2)q^{-1}.$$

4. Zeta functions

4.1. **Representation zeta functions of compact p-adic groups and the proof of Theorem V.** By [AA, Corollary 4.1.4], the deformation variety $\mathrm{Def}_{G,n}$ is absolutely irreducible; by the assumptions, it has rational singularities. By Proposition 3.0.2 and Theorem 3.0.3, we can choose a finite set S of primes and a positive number C such that

- For any $q \in \mathcal{P}_S$ and any positive integer m,
  (a) $h_{\mathrm{Def}_{G,n}}(\mathbb{Z}_q/\mathfrak{m}_q^m) = h_{\mathrm{Def}_{G,2n}}(\mathbb{F}_q[t]/t^m)$.
  (b) $h_G(\mathbb{Z}_q/\mathfrak{m}_q^m) = h_G(\mathbb{F}_q[[t]]/t^m)$.
  (c) $|h_{\mathrm{Def}_{G,n}}(\mathbb{F}_q) - 1| < Cq^{\frac{1}{2}}$.
  (d) $|h_{\mathrm{Def}_{G,n}}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{\mathrm{Def}_{G,n}}(\mathbb{F}_q)| < Cq^{-1}$.
  (e) $|h_G(\mathbb{Z}_q/\mathfrak{m}_q^m) - 1| < Cq^{-\frac{1}{2}}$.
- G is smooth over $\mathrm{Spec}(S^{-1}\mathbb{Z})$.

There is a finite extension K of $\mathbb{Q}$ such that G_K is K-split. Hence, there is a simply connected semisimple group scheme H which is split over $\mathbb{Z}$ and an isomorphism $G_K \cong H_K$. Hence, for all but finitely many primes $\mathfrak{p}$ of O_K, we have $G_{O_K/\mathfrak{p}} \cong H_{O_K/\mathfrak{p}}$, so $G_{O_K/\mathfrak{p}}$ is semisimple and simply connected. Hence, after enlarging S, we can assume that $G_{\mathbb{F}_p}$ is simply connected and semisimple, for all $p \notin S$. In addition, (e) implies that, after a further enlargement of S, we can assume that, for any $q \in \mathcal{P}_S$,

(f) $h_G(\mathbb{Z}_q/\mathfrak{m}_q^m) > \frac{1}{2}$.

For any m,

$$\zeta_{G(\mathbb{Z}_q/\mathfrak{m}_q^m)}(2n-2) = \frac{|\mathrm{Def}_{G,n}(\mathbb{Z}_q/\mathfrak{m}_q^m)|}{|G^{2n-1}(\mathbb{Z}_q/\mathfrak{m}_q^m)|} = \frac{h_{\mathrm{Def}_{G,n}}(\mathbb{Z}_q/\mathfrak{m}_q^m)}{h_{G^{2n-1}}(\mathbb{Z}_q/\mathfrak{m}_q^m)} = \frac{h_{\mathrm{Def}_{G,n}}(\mathbb{Z}_q/\mathfrak{m}_q^m)}{h_{G^{2n-1}}(\mathbb{F}_q)}, \tag{14}$$

where the first equality follows from the Frobenius formula (Theorem 2.5.1), the second follows from the fact that $\dim \mathrm{Def}_{G_{\mathbb{Q}},n} = \dim G_{\mathbb{Q}}^{2n-1}$ ([AA, Corollary 4.1.4]), and the third follows from the fact that G is smooth over O and Hensel's lemma.

From [LS05b, Lemma 2.1], we get

(g) $|\zeta_{G(\mathbb{F}_q)}(2n-2) - 1| < Cq^{-1}$.

Fix $q \in \mathcal{P}_S$. Let O be either $\mathbb{Z}_q$ or $\mathbb{F}_q[[t]]$, and let $\mathfrak{m} \subset O$ be the maximal ideal. By (a), (b), and the Frobenius formula,

$$\zeta_{G(O/\mathfrak{m}^m)}(2n-2) = \frac{|\operatorname{Def}_{G,n}(O/\mathfrak{m}^m)|}{|G^{2n-1}(O/\mathfrak{m}^m)|} = \frac{|\operatorname{Def}_{G,n}(\mathbb{Z}_q/\mathfrak{m}_q^m)|}{|G^{2n-1}(\mathbb{Z}_q/\mathfrak{m}_q^m)|} = \zeta_{G(\mathbb{Z}_q/\mathfrak{m}_q^m)}(2n-2). \tag{15}$$

Thus, Equation (14) implies that

$$|\zeta_{G(O/\mathfrak{m}^m)}(2n-2)-1| \leq |\zeta_{G(\mathbb{Z}_q/\mathfrak{m}_q^m)}(2n-2) - \zeta_{G(\mathbb{F}_q)}(2n-2)| + |\zeta_{G(\mathbb{F}_q)}(2n-2)-1| = \\ = \frac{|h_{\operatorname{Def}_{G,n}}(\mathbb{Z}_q/\mathfrak{m}_q^m) - h_{\operatorname{Def}_{G,n}}(\mathbb{F}_q)|}{h_{G^{2n-1}}(\mathbb{F}_q)} + |\zeta_{G(\mathbb{F}_q)}(2n-2)-1|.$$

Using (d), (f), (g), we obtain that:

$$|\zeta_{G(O/\mathfrak{m}^m)}(2n-2)-1| \leq (2^{2n-1}+1)Cq^{-1}.$$

Since each continuous representation of a pro-finite group is locally constant, we get that the series defining $\zeta_{G(O)}(2n-2)$ equals the limit

$$\lim_{m\to\infty} \zeta_{G(O/\mathfrak{m}^m)}(2n-2),$$

and the result follows.

4.2. **Representation zeta functions of adelic groups and the proof of Theorem III.**

Proof of Theorem III. Theorem V implies that there is a finite set S of prime numbers and a positive integer D such that, for every $q \in \mathcal{P}_S$,

$$\zeta_{G(\mathbb{Z}_q)}(2n-2) - 1 = \zeta_{G(\mathbb{F}_q[[t]])}(2n-2) - 1 \leq Dq^{-1}. \tag{16}$$

Let $C > \max S$, let k be a global field of characteristic greater than C, let T be a finite set of places of k containing all archimedean ones, and let n be such that $\operatorname{Def}_{G_{\mathbb{Q}},n}$ has rational singularities. We will show that $\zeta_{G(\widehat{O_{k,T}})}(2n-2+\epsilon)$ converges, for every positive ϵ.

For any non-archimedean place v, let O_v be the ring of integers of the completion k_v, and let $|v|$ be the size of the residue field of O_v. We have that $\zeta_{G(\widehat{O_{k,T}})}(s) = \prod_{v\notin T} \zeta_{G(O_v)}(s)$, by which we mean, in particular, that the left hand side converges absolutely if and only if each of the terms on the right hand side converges absolutely, and their product converges absolutely. By [AA, Theorem IV] and the assumptions, the series $\zeta_{G(O_v)}(2n-2)$ converges for every v. Thus, it is enough to prove that $\prod_{v\notin T'} \zeta_{G(O_v)}(2n-2+\epsilon)$ converges, for some finite set of places $T' \supset T$.

For almost all places v, we have

$$O_v \cong \mathbb{Z}_{|v|} \text{ or } O_v \cong \mathbb{F}_{|v|}[[t]]. \tag{17}$$

By [LM04, Proposition 4.6], there is a constant $\delta > 0$ such that, for almost all places v, the minimal dimension of a non-trivial representation of $G(O_v)$ is at least $|v|^{\delta}$. It follows that

$$\zeta_{G(O_v)}(2n-2+\epsilon) - 1 \leq |v|^{-\epsilon\delta} \left(\zeta_{G(O_v)}(2n-2) - 1\right). \tag{18}$$

Let $T' \supset T$ be a finite set of places such that (16), (17), and (18) hold for any $v \notin T'$. We have

$$\prod_{v\notin T'} \zeta_{G(O_v)}(2n-2+\epsilon) \leq \prod_{v\notin T'} \left(1 + D|v|^{-1-\epsilon\delta}\right) \leq \prod_{v\notin T'} \left(1 + |v|^{-1-\epsilon\delta}\right)^{D} \leq \prod_{v\notin T'} \left(1 - |v|^{-1-\epsilon\delta}\right)^{-D} \leq$$

$$\leq \left(\prod_{v \text{ non-archimedean}} \left(1 - |v|^{-1-\epsilon\delta}\right)^{-1} \right)^{D}.$$

The last product is the product expansion of the Dedekind zeta function of k at the point $1 + \epsilon\delta$, and it is well-known that it converges absolutely.

□

4.3. **Representation zeta functions of arithmetic groups and the proof of Theorem II.** Let us first recall the notion of the Congruence Subgroup Property.

Definition 4.3.1. *Let k be a global field, and let T be a finite set of places of k containing all archimedean ones. We say that $G(O_{k,T})$ has the* Congruence Subgroup Property *(CSP for short) if the canonical map*

$$\eta : \widehat{G(O_{k,T})} \to G\left(\widehat{O_{k,T}}\right)$$

has a finite kernel. Here, the domain of η is the pro-finite completion of $G(O_{k.T})$.

By our assumptions on G and the Strong Approximation Theorem ([PR94, Chapter 7]), the map η is always surjective. It is known that, if $\mathrm{rk}_k G_k \geq 2$, then $G(O_{k,T})$ satisfies CSP. More generally, a conjecture of Serre asserts that the group $G(O_{k,T})$ has CSP whenever $\sum_{v\in T} \mathrm{rk}_{k_v} G \geq 2$ and $\mathrm{rk}_{k_v} G \geq 1$ for any finite place $v \in T$. This conjecture is known in many cases; see, for example, [Rag04].

Theorem II follows from Theorem III and the following theorem

Theorem 4.3.2. *Let k be a global field and let T be a finite set of places of k containing all the archimedean ones. Assume that $G(O_{k,T})$ satisfies CSP, then $\alpha(G(O_{k,T})) = \alpha\left(G(\widehat{O_{k,T}})\right)$.*

Proof. If the characteristic of k is non-zero, the claim follows from [LL08, Theorem 3.3] and [LM04, Lemma 2.2]. If the characteristic of k is zero, the claim follows from [AKOV, Theorem 1.4]. □

4.4. **The Igusa zeta function and proof of Theorem I.** The following lemma is standard:

Lemma 4.4.1.

(1) *Let a_n be a sequence and assume that there is a constant $C > 0$ such that $\frac{1}{C} < a_n < C$ for $n > C$. Then the series $f(s) := \sum a_n p^{-ns}$ converges absolutely for $Re(s) > 0$ and diverges for $s = 0$.*

(2) *Suppose in addition that $f(s)$ coincides (in its domain of absolute convergence) with a rational function of p^{-s}, which we continue to denote by $f(s)$. Then 0 is a simple pole of $f(s)$ and all the poles on the imaginary axis are simple.*

(3) *Let $a_{n,p}$ be a sequence indexed by a positive integer n and a prime p, and let $\delta, C > 0$. Suppose that $|a_{n,p} - 1| < Cp^{-\delta}$. Let $Z(s) := \prod_p (1 + \sum_n a_{n,p} p^{-ns})$. Then:*
   (a) *$Z(s)$ converges absolutely for $Re(s) > 1$.*
   (b) *If $\zeta(s)$ denotes the Riemann zeta function, then $Z(s)/\zeta(s)$ can be analytically continued for $Re(s) > 1 - \delta$.*

Claim 1 of Theorem I follows from Lemma 4.4.1(1,2), Theorem A, and the rationality of $\mathfrak{P}_{X,p}(s)$. Claim 2 of Theorem I follows from Lemma 4.4.1(3) and Theorem A. Claim 3 of Theorem I follows from claim 2 and [dSG00, Theorem 4.20].

Finally, claim 4 of Theorem I follows from Lemma 4.4.1(3), Theorem A, and the fact that

$$\mathcal{Z}_{X,p}(s) = \sum_n \left(h_X(\mathbb{Z}/p^n) - \frac{h_X(\mathbb{Z}/p^{n+1})}{p} \right) p^{-n(s+1)}.$$

Remark 4.4.2. *In view of the comment just after Theorem 3.0.3 , Lemma 4.4.1 also implies that, if X is local complete intersection, then one can take S to be empty in Theorem I.*

References

[AA] Aizenbud, A.; Avni, N.; *Representation growth and rational singularities of the moduli space of local systems*. Arxiv 1307.0371, to appear in Inventiones Mathematicae.

[AKOV] Avni, N.; Klopsch, B.; Onn, U.; Voll, C.; *Arithmetic Groups, Base Change, and Representation Growth*. Arxiv 1110.6092.

[AKOV2] Avni, N.; Klopsch, B.; Onn, U.; Voll, C.; *Representation zeta functions of compact p-adic analytic groups and arithmetic groups*. Duke Math. J. 162 (2013), no. 1, 111–197.

[Avn11] Avni, N.; *Arithmetic groups have rational representation growth.* Ann. of Math. 174 (2011), 1009–1056.

[BLR90] Bosch, S.; Lütkebohmert, W.; Raynaud, M.; *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 21. Springer-Verlag, Berlin, 1990.

[dSG00] du Sautoy, M. P. F.; Grunewald, F.; *Analytic properties of zeta functions and subgroup growth.* Annals of Math. 152 (2000), 793–833.

[Gro66] Grothendieck A.; *Éléments de géométrie algébrique IV* Publications mathematiques de l' I.H.E.S., tome 28 (1966).

[Har77] Hartshorne, R.; *Algebraic geometry*, Springer-Verlag, New York (1977).

[HK06] Hrushovski, E.; Kazhdan. D.; *Integration in valued fields.* Algebraic geometry and number theory, volume 253 of Progr. Math., Birkhäuser Boston, Boston, MA, 2006.

[Jai06] Jaikin–Zapirain A.; *Zeta function of representations of compact p-adic analytic groups.* J. Amer. Math. Soc. 19 (2006), 91–118.

[KKMS73] Kempf, G.; Knudsen, F.; Mumford D.; Saint-Donat, B.; *Toroidal Embeddings I.* Springer Lecture Notes. no. 339 (1973)

[LL08] Larsen, M.; Lubotzky, A.; *Representation growth of linear groups.* J. Eur. Math. Soc. 10 (2008), 351–390.

[LM04] Lubotzky, A.; Martin, B.; *Polynomial representation growth and the congruence subgroup problem.* Israel J. Math. 144 (2004), 293–316.

[LS05a] Liebeck, M.W.; Shalev, A.; *Character degrees and random walks in finite groups of Lie type.* Proc. London Math. Soc. 90 (2005), 61–86.

[LS05b] Liebeck, M.W.; Shalev, A.; *Fuchsian groups, finite simple groups and representation varieties.* Inventiones Math. 159 (2005), 317–367.

[LW54] Lang, S.; Weil, A.; *Number of points of varieties in finite fields.* Amer. J. Math. 76 (1954), 819–827.

[Mus01] Mustaţă, M.; *Jet schemes of locally complete intersection canonical singularities.* Invent. Math. 145 (2001), no. 3, 397-424.

[Mus] Mustaţă, M.; Zeta functions in algebraic geometry. Lecture notes. Available at http://www.math.lsa.umich.edu/~mmustata/zeta_book.pdf.

[PR94] Platonov, V.; Rapinchuk, A.; *Algebraic groups and number theory.* Pure and Applied Mathematics, 139. Academic Press, Inc., Boston, MA, 1994.

[Rag04] Raghunathan, M.S.; *The congruence subgroup problem.* Proc. Indian Acad. Sci. Math. 114 (2004), no. 4, 299–308.

[Ser64] Serre, J.P. *Lie Algebras and Lie Groups.* Lecture Notes in Mathematics, **1500**. Springer-Verlag, New York, 1964.

Avraham Aizenbud, Faculty of Mathematics and Computer Science, Weizmann Institute of Science, Israel.

E-mail address: aizenr@gmail.com

URL: http://www.wisdom.weizmann.ac.il/~aizenr

Department of Mathematics, Northwestern University, Evanston, IL, USA.

E-mail address: avni.nir@gmail.com

URL: http://math.northwestern.edu/~nir