BERTINI THEOREMS OVER FINITE FIELDS

BJORN POONEN

Abstract. Let X be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 0$ over $\mathbf{F}_q$. Then there exist homogeneous polynomials f over $\mathbf{F}_q$ for which the intersection of X and the hypersurface $f = 0$ is smooth. In fact, the set of such f has a positive density, equal to $\zeta_X(m+1)^{-1}$, where $\zeta_X(s) = Z_X(q^{-s})$ is the zeta function of X. An analogue for regular quasiprojective schemes over $\mathbf{Z}$ is proved, assuming the *abc* conjecture and another conjecture.

1. Introduction

The classical Bertini theorems say that if a subscheme $X \subseteq \mathbf{P}^n$ has a certain property, then for a sufficiently general hyperplane $H \subset \mathbf{P}^n$, $H \cap X$ has the property too. For instance, if X is a quasiprojective subscheme of $\mathbf{P}^n$ that is smooth of dimension $m \geq 0$ over a field k, and U is the set of points u in the dual projective space $\check{\mathbf{P}}^n$ corresponding to hyperplanes $H \subset \mathbf{P}^n_{\kappa(u)}$ such that $H \cap X$ is smooth of dimension $m-1$ over the residue field $\kappa(u)$ of u, then U contains a dense open subset of $\check{\mathbf{P}}^n$. If k is infinite, then $U \cap \check{\mathbf{P}}^n(k)$ is nonempty, and hence one can find H over k. But if k is finite, then it can happen that the finitely many hyperplanes H over k all fail to give a smooth intersection $H \cap X$. See Theorem 3.1.

N. M. Katz [Kat99] asked whether the Bertini theorem over finite fields can be salvaged by allowing hypersurfaces of unbounded degree in place of hyperplanes. (In fact he asked for a little more; see Section 3 for details.) We answer the question affirmatively below. O. Gabber [Gab01, Corollary 1.6] has independently proved the existence of good hypersurfaces of any sufficiently large degree divisible by the characteristic of k.

Let $\mathbf{F}_q$ be a finite field of $q = p^a$ elements. Let $S = \mathbf{F}_q[x_0, \ldots, x_n]$ be the homogeneous coordinate ring of $\mathbf{P}^n$, let $S_d \subset S$ be the $\mathbf{F}_q$-subspace of homogeneous polynomials of degree d, and let $S_{\text{homog}} = \bigcup_{d=0}^{\infty} S_d$. For each $f \in S_d$, let H_f be the subscheme $\operatorname{Proj}(S/(f)) \subseteq \mathbf{P}^n$. Typically (but not always), H_f is a hypersurface of dimension $n-1$ defined by the equation $f = 0$. Define the *density* of a subset $\mathcal{P} \subseteq S_{\text{homog}}$ by

$$\mu(\mathcal{P}) := \lim_{d \to \infty} \frac{\#(\mathcal{P} \cap S_d)}{\# S_d},$$

if the limit exists. For a scheme X of finite type over $\mathbf{F}_q$, define the zeta function [Wei49]

$$\zeta_X(s) = Z_X(q^{-s}) := \prod_{\text{closed } P \in X} \left(1 - q^{-s \deg P}\right)^{-1} = \exp\left(\sum_{r=1}^{\infty} \frac{\# X(\mathbf{F}_{q^r})}{r} q^{-rs}\right).$$

Date: August 31, 2004.

1991 *Mathematics Subject Classification.* Primary 14J70; Secondary 11M38, 11M41, 14G40, 14N05.

This research was supported by NSF grant DMS-9801104 and a Packard Fellowship. Part of the research was done while the author was enjoying the hospitality of the Université de Paris-Sud. This article has been published in *Annals of Math.* **160** (2004), no. 3, 1099–1127.

Theorem 1.1 (Bertini over finite fields)**.** *Let X be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 0$ over $\mathbf{F}_q$. Define*

$$\mathcal{P} := \{\, f \in S_{\text{homog}} : H_f \cap X \text{ is smooth of dimension } m-1 \,\}.$$

Then $\mu(\mathcal{P}) = \zeta_X(m+1)^{-1}$.

Remarks.

(1) The empty scheme is smooth of any dimension, including -1. Later (for instance, in Theorem 1.3), we will similarly use the convention that if P is a point not on a scheme X, then for any r, the scheme X is automatically smooth of dimension r at P.
(2) In this paper, $\cap$ denotes scheme-theoretic intersection (when applied to schemes).
(3) If $n \geq 2$, the density is unchanged if we insist also that H_f be a geometrically integral hypersurface of dimension $n-1$. This follows from the easy Proposition 2.7.
(4) The case $n = 1$, $X = \mathbf{A}^1$, is a well known polynomial analogue of the fact that the set of squarefree integers has density $\zeta(2)^{-1} = 6/\pi^2$. See Section 5 for a conjectural common generalization.
(5) The density is independent of the choice of embedding $X \hookrightarrow \mathbf{P}^n$!
(6) By [Dwo60], ζ_X is a rational function of q^{-s}, so $\zeta_X(m+1)^{-1} \in \mathbf{Q}$.

The overall plan of the proof is to start with all homogeneous polynomials of degree d, and then for each closed point $P \in X$ to sieve out the polynomials f for which $H_f \cap X$ is singular at P. The condition that P be singular on $H_f \cap X$ amounts to $m+1$ linear conditions on the Taylor coefficients of a dehomogenization of f at P, and these linear conditions are over the residue field of P. Therefore one expects that the probability that $H_f \cap X$ is nonsingular at P will be $1 - q^{-(m+1)\deg P}$. Assuming that these conditions at different P are independent, the probability that $H_f \cap X$ is nonsingular everywhere should be

$$\prod_{\text{closed } P \in X} \left(1 - q^{-(m+1)\deg P}\right) = \zeta_X(m+1)^{-1}.$$

Unfortunately, the independence assumption and the individual singularity probability estimates break down once $\deg P$ becomes large relative to d. Therefore we must approximate our answer by truncating the product after finitely many terms, say those corresponding to P of degree $< r$. The main difficulty of the proof, as with many sieve proofs, is in bounding the error of the approximation, i.e., in showing that when $d \gg r \gg 1$, the number of polynomials of degree d sieved out by conditions at the infinitely many P of degree $\geq r$ is negligible.

In fact we will prove Theorem 1.1 as a special case of the following, which is more versatile in applications. The effect of T below is to prescribe the first few terms of the Taylor expansions of the dehomogenizations of f at finitely many closed points.

Theorem 1.2 (Bertini with Taylor conditions)**.** *Let X be a quasiprojective subscheme of $\mathbf{P}^n$ over $\mathbf{F}_q$. Let Z be a finite subscheme of $\mathbf{P}^n$, and assume that $U := X - (Z \cap X)$ is smooth of dimension $m \geq 0$. Fix a subset $T \subseteq H^0(Z, \mathcal{O}_Z)$. Given $f \in S_d$, let $f|_Z$ be the element of $H^0(Z, \mathcal{O}_Z)$ that on each connected component Z_i equals the restriction of $x_j^{-d} f$ to Z_i, where $j = j(i)$ is the smallest $j \in \{0, 1 \ldots, n\}$ such that the coordinate x_j is invertible on Z_i. Define*

$$\mathcal{P} := \{\, f \in S_{\text{homog}} : H_f \cap U \text{ is smooth of dimension } m-1, \text{ and } f|_Z \in T \,\}.$$

Then

$$\mu(\mathcal{P}) = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \, \zeta_U(m+1)^{-1}.$$

Using a formalism analogous to that of Lemma 20 of [PS99], we can deduce the following even stronger version, which allows us to impose *infinitely* many local conditions, provided that the conditions at most points are no more stringent than the condition that the hypersurface intersect a given finite set of varieties smoothly.

Theorem 1.3 (Infinitely many local conditions). *For each closed point P of $\mathbf{P}^n$ over $\mathbf{F}_q$, let μ_P be normalized Haar measure on the completed local ring $\hat{\mathcal{O}}_P$ as an additive compact group, and let U_P be a subset of $\hat{\mathcal{O}}_P$ whose boundary ∂U_P has measure zero. Also for each P, fix a nonvanishing coordinate x_j, and for $f \in S_d$ let $f|_P$ be the image of $x_j^{-d} f$ in $\hat{\mathcal{O}}_P$. Assume that there exist smooth quasiprojective subschemes $X_1, \dots, X_u$ of $\mathbf{P}^n$ of dimensions $m_i = \dim X_i$ over $\mathbf{F}_q$ such that for all but finitely many P, U_P contains $f|_P$ whenever $f \in S_{\mathrm{homog}}$ is such that $H_f \cap X_i$ is smooth of dimension $m_i - 1$ at P for all i. Define*

$$\mathcal{P} := \{\, f \in S_{\mathrm{homog}} : f|_P \in U_P \text{ for all closed points } P \in \mathbf{P}^n \,\}.$$

Then $\mu(\mathcal{P}) = \displaystyle\prod_{\text{closed } P \in \mathbf{P}^n} \mu_P(U_P).$

Remark. Implicit in Theorem 1.3 is the claim that the product $\prod_P \mu_P(U_P)$ always converges, and in particular that its value is zero if and only if $\mu_P(U_P) = 0$ for some closed point P.

The proofs of Theorems 1.1, 1.2, and 1.3 are contained in Section 2. But the reader at this point is encouraged to jump to Section 3 for applications, and to glance at Section 5, which shows that the *abc* conjecture and another conjecture imply analogues of our main theorems for regular quasiprojective schemes over $\operatorname{Spec} \mathbf{Z}$. The *abc* conjecture is needed to apply a multivariable generalization [Poo03] of A. Granville's result [Gra98] about squarefree values of polynomials. For some open questions, see Sections 4 and 5.7, and also Conjecture 5.2.

The author hopes that the technique of Section 2 will prove useful in removing the condition "assume that the ground field k is infinite" from other theorems in the literature.

2. Bertini over finite fields: the closed point sieve

Sections 2.1, 2.2, and 2.3 are devoted to the proofs of Lemmas 2.2, 2.4, and 2.6, which are the main results needed in Section 2.4 to prove Theorems 1.1, 1.2, and 1.3.

2.1. **Singular points of low degree.** Let $A = \mathbf{F}_q[x_1, \dots, x_n]$ be the ring of regular functions on the subset $\mathbf{A}^n := \{x_0 \neq 0\} \subseteq \mathbf{P}^n$, and identify S_d with the set of dehomogenizations $A_{\le d} = \{\, f \in A : \deg f \le d \,\}$, where $\deg f$ denotes total degree.

Lemma 2.1. *If Y is a finite subscheme of $\mathbf{P}^n$ over a field k, then the map*

$$\phi_d : S_d = H^0(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(d)) \to H^0(Y, \mathcal{O}_Y(d))$$

is surjective for $d \ge \dim H^0(Y, \mathcal{O}_Y) - 1$.

Proof. Let $\mathcal{I}_Y$ be the ideal sheaf of $Y \subseteq \mathbf{P}^n$. Then $\operatorname{coker}(\phi_d)$ is contained in $H^1(\mathbf{P}^n, \mathcal{I}_Y(d))$, which vanishes for $d \gg 1$ by Theorem III.5.2b of [Har77]. Thus ϕ_d is surjective for $d \gg 1$.

Enlarging $\mathbf{F}_q$ if necessary, we can perform a linear change of variable to assume $Y \subseteq \mathbf{A}^n := \{x_0 \neq 0\}$. Dehomogenize by setting $x_0 = 1$, so that ϕ_d is identified with a map from $A_{\le d}$

to $B := H^0(Y, \mathcal{O}_Y)$. Let $b = \dim B$. For $i \geq -1$, let B_i be the image of $A_{\leq i}$ in B. Then $0 = B_{-1} \subseteq B_0 \subseteq B_1 \subseteq \dots$, so $B_j = B_{j+1}$ for some $j \in [-1, b-1]$. Then

$$B_{j+2} = B_{j+1} + \sum_{i=1}^{n} x_i B_{j+1} = B_j + \sum_{i=1}^{n} x_i B_j = B_{j+1}.$$

Similarly $B_j = B_{j+1} = B_{j+2} = \dots$, and these eventually equal B by the previous paragraph. Hence ϕ_d is surjective for $d \geq j$, and in particular for $d \geq b-1$. □

If U is a scheme of finite type over $\mathbf{F}_q$, let $U_{<r}$ be the set of closed points of U of degree $< r$. Similarly define $U_{>r}$.

Lemma 2.2 (Singularities of low degree)**.** *Let notation and hypotheses be as in Theorem 1.2, and define*

$$\mathcal{P}_r := \{\, f \in S_{\text{homog}} : H_f \cap U \text{ is smooth of dimension } m-1 \text{ at all } P \in U_{<r}, \text{ and } f|_Z \in T \,\}.$$

Then

$$\mu(\mathcal{P}_r) = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \prod_{P \in U_{<r}} \left(1 - q^{-(m+1)\deg P}\right).$$

Proof. Let $U_{<r} = \{P_1, \dots, P_s\}$. Let $\mathfrak{m}_i$ be the ideal sheaf of P_i on U, let Y_i be the closed subscheme of U corresponding to the ideal sheaf $\mathfrak{m}_i^2 \subseteq \mathcal{O}_U$, and let $Y = \bigcup Y_i$. Then $H_f \cap U$ is singular at P_i (more precisely, not smooth of dimension $m-1$ at P_i) if and only if the restriction of f to a section of $\mathcal{O}_{Y_i}(d)$ is zero. Hence $\mathcal{P}_r \cap S_d$ is the inverse image of

$$T \times \prod_{i=1}^{s} \left(H^0(Y_i, \mathcal{O}_{Y_i}) - \{0\}\right)$$

under the $\mathbf{F}_q$-linear composition

$$\phi_d : S_d = H^0(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(d)) \to H^0(Y \cup Z, \mathcal{O}_{Y \cup Z}(d)) \simeq H^0(Z, \mathcal{O}_Z) \times \prod_{i=1}^{s} H^0(Y_i, \mathcal{O}_{Y_i}),$$

where the last isomorphism is the (noncanonical) untwisting, component by component, by division by the d-th powers of various coordinates, as in the definition of $f|_Z$. Applying Lemma 2.1 to $Y \cup Z$ shows that ϕ_d is surjective for $d \gg 1$, so

$$\mu(\mathcal{P}_r) = \lim_{d \to \infty} \frac{\#\left[T \times \prod_{i=1}^{s} \left(H^0(Y_i, \mathcal{O}_{Y_i}) - \{0\}\right)\right]}{\#\left[H^0(Z, \mathcal{O}_Z) \times \prod_{i=1}^{s} H^0(Y_i, \mathcal{O}_{Y_i})\right]} = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \prod_{i=1}^{s} \left(1 - q^{-(m+1)\deg P_i}\right),$$

since $H^0(Y_i, \mathcal{O}_{Y_i})$ has a two-step filtration whose quotients $\mathcal{O}_{U,P_i}/\mathfrak{m}_{U,P_i}$ and $\mathfrak{m}_{U,P_i}/\mathfrak{m}_{U,P_i}^2$ are vector spaces of dimensions 1 and m respectively over the residue field of P_i. □

2.2. **Singular points of medium degree.**

Lemma 2.3. *Let U be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 0$ over $\mathbf{F}_q$. If $P \in U$ is a closed point of degree e, where $e \leq d/(m+1)$, then the fraction of $f \in S_d$ such that $H_f \cap U$ is not smooth of dimension $m-1$ at P equals $q^{-(m+1)e}$.*

Proof. Let $\mathfrak{m}$ be the ideal sheaf of P on U, and let Y be the closed subscheme of U corresponding to $\mathfrak{m}^2$. The $f \in S_d$ to be counted are those in the kernel of $\phi_d : H^0(\mathbf{P}^n, \mathcal{O}(d)) \to H^0(Y, \mathcal{O}_Y(d))$. We have $\dim H^0(Y, \mathcal{O}_Y(d)) = \dim H^0(Y, \mathcal{O}_Y) = (m+1)e \leq d$, so ϕ_d is surjective by Lemma 2.1, and the $\mathbf{F}_q$-codimension of $\ker \phi_d$ equals $(m+1)e$. □

Define the upper and lower densities $\overline{\mu}(\mathcal{P})$, $\underline{\mu}(\mathcal{P})$ of a subset $\mathcal{P} \subseteq S$ as $\mu(\mathcal{P})$ was defined, but using lim sup and lim inf in place of lim.

Lemma 2.4 (Singularities of medium degree)**.** *Let U be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 0$ over $\mathbf{F}_q$. Define*

$$\mathcal{Q}_r^{\text{medium}} := \bigcup_{d \geq 0} \{\, f \in S_d : \textit{ there exists } P \in U \textit{ with } r \leq \deg P \leq \frac{d}{m+1} \\ \textit{such that } H_f \cap U \textit{ is not smooth of dimension } m-1 \textit{ at } P \,\}.$$

Then $\lim_{r \to \infty} \overline{\mu}(\mathcal{Q}_r^{\text{medium}}) = 0$.

Proof. Using Lemma 2.3 and the crude bound $\# U(\mathbf{F}_{q^e}) \leq c q^{em}$ for some $c > 0$ depending only on U [LW54], we obtain

$$\begin{aligned} \frac{\#(\mathcal{Q}_r^{\text{medium}} \cap S_d)}{\# S_d} &\leq \sum_{e=r}^{\lfloor d/(m+1) \rfloor} (\text{number of points of degree } e \text{ in } U)\ q^{-(m+1)e} \\ &\leq \sum_{e=r}^{\lfloor d/(m+1) \rfloor} \# U(\mathbf{F}_{q^e}) q^{-(m+1)e} \\ &\leq \sum_{e=r}^{\infty} c q^{em} q^{-(m+1)e}, \\ &= \frac{c q^{-r}}{1 - q^{-1}}. \end{aligned}$$

Hence $\overline{\mu}(\mathcal{Q}_r^{\text{medium}}) \leq c q^{-r}/(1 - q^{-1})$, which tends to zero as $r \to \infty$. $\square$

2.3. **Singular points of high degree.**

Lemma 2.5. *Let P be a closed point of degree e in $\mathbf{A}^n$ over $\mathbf{F}_q$. Then the fraction of $f \in A_{\leq d}$ that vanish at P is at most $q^{-\min(d+1,e)}$.*

Proof. Let $\mathrm{ev}_P : A_{\leq d} \to \mathbf{F}_{q^e}$ be the evaluation-at-P map. The proof of Lemma 2.1 shows that $\dim_{\mathbf{F}_q} \mathrm{ev}_P(A_{\leq d})$ strictly increases with d until it reaches e, so $\dim_{\mathbf{F}_q} \mathrm{ev}_P(A_{\leq d}) \geq \min(d+1, e)$. Equivalently, the codimension of $\ker(\mathrm{ev}_P)$ in $A_{\leq d}$ is at least $\min(d+1, e)$. $\square$

Lemma 2.6 (Singularities of high degree)**.** *Let U be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 0$ over $\mathbf{F}_q$. Define*

$$\mathcal{Q}^{\text{high}} := \bigcup_{d \geq 0} \{\, f \in S_d : \exists P \in U_{>d/(m+1)} \textit{ such that } H_f \cap U \textit{ is not smooth of dimension } m-1 \textit{ at } P \,\}.$$

Then $\overline{\mu}(\mathcal{Q}^{\text{high}}) = 0$.

Proof. If the lemma holds for U and for V, it holds for $U \cup V$, so we may assume $U \subseteq \mathbf{A}^n$ is affine.

Given a closed point $u \in U$, choose a system of local parameters $t_1, \ldots, t_n \in A$ at u on $\mathbf{A}^n$ such that $t_{m+1} = t_{m+2} = \cdots = t_n = 0$ defines U locally at u. Then $dt_1, \ldots, dt_n$ are a $\mathcal{O}_{\mathbf{A}^n,u}$-basis for the stalk $\Omega^1_{\mathbf{A}^n/\mathbf{F}_q,u}$. Let $\partial_1, \ldots, \partial_n$ be the dual basis of the stalk $\mathcal{T}_{\mathbf{A}^n/\mathbf{F}_q,u}$ of the tangent sheaf. Choose $s \in A$ with $s(u) \neq 0$ to clear denominators so that $D_i := s\partial_i$ gives a global derivation $A \to A$ for $i = 1, \ldots, n$. Then there is a neighborhood N_u of u in

$\mathbf{A}^n$ such that $N_u \cap \{t_{m+1} = t_{m+2} = \cdots = t_n = 0\} = N_u \cap U$, $\Omega^1_{N_u/\mathbf{F}_q} = \oplus_{i=1}^n \mathcal{O}_{N_u} dt_i$, and $s \in \mathcal{O}(N_u)^*$. We may cover U with finitely many N_u, so by the first sentence of this proof, we may reduce to the case where $U \subseteq N_u$ for a single u. For $f \in A_{\le d}$, $H_f \cap U$ *fails* to be smooth of dimension $m-1$ at a point $P \in U$ if and only if $f(P) = (D_1 f)(P) = \cdots = (D_m f)(P) = 0$.

Now for the trick. Let $\tau = \max_i(\deg t_i)$, $\gamma = \lfloor (d-\tau)/p \rfloor$, and $\eta = \lfloor d/p \rfloor$. If $f_0 \in A_{\le d}$, $g_1 \in A_{\le \gamma}$, ..., $g_m \in A_{\le \gamma}$, and $h \in A_{\le \eta}$ are selected uniformly and independently at random, then the distribution of

$$f := f_0 + g_1^p t_1 + \cdots + g_m^p t_m + h^p$$

is uniform over $A_{\le d}$. We will bound the probability that an f constructed in this way has a point $P \in U_{>d/(m+1)}$ where $f(P) = (D_1 f)(P) = \cdots = (D_m f)(P) = 0$. By writing f in this way, we partially decouple the $D_i f$ from each other: $D_i f = (D_i f_0) + g_i^p s$ for $i = 1, \ldots, m$. We will select $f_0, g_1, \ldots, g_m, h$ one at a time. For $0 \le i \le m$, define

$$W_i := U \cap \{D_1 f = \cdots = D_i f = 0\}.$$

Claim 1: For $0 \le i \le m-1$, conditioned on a choice of $f_0, g_1, \ldots, g_i$ for which $\dim(W_i) \le m-i$, the probability that $\dim(W_{i+1}) \le m-i-1$ is $1 - o(1)$ as $d \to \infty$. (The function of d represented by the $o(1)$ depends on U and the D_i.)

Proof of Claim 1: Let V_1, ..., V_ℓ be the $(m-i)$-dimensional $\mathbf{F}_q$-irreducible components of $(W_i)_{\text{red}}$. By Bézout's theorem [Ful84, p. 10],

$$\ell \le (\deg \overline{U})(\deg D_1 f) \ldots (\deg D_i f) = O(d^i)$$

as $d \to \infty$, where $\overline{U}$ is the projective closure of U. Since $\dim V_k \ge 1$, there exists a coordinate x_j depending on k such that the projection $x_j(V_k)$ has dimension 1. We need to bound the set

$$G_k^{\text{bad}} := \{\, g_{i+1} \in A_{\le \gamma} : D_{i+1} f = (D_{i+1} f_0) + g_{i+1}^p s \text{ vanishes identically on } V_k \,\}.$$

If $g, g' \in G_k^{\text{bad}}$, then by taking the difference and multiplying by s^{-1}, we see that $g - g'$ vanishes on V_k. Hence if G_k^{bad} is nonempty, it is a coset of the subspace of functions in $A_{\le \gamma}$ vanishing on V_k. The codimension of that subspace, or equivalently the dimension of the image of $A_{\le \gamma}$ in the regular functions on V_k, exceeds $\gamma + 1$, since a nonzero polynomial in x_j alone does not vanish on V_k. Thus the probability that $D_{i+1} f$ vanishes on some V_k is at most $\ell q^{-\gamma-1} = O(d^i q^{-(d-\tau)/p}) = o(1)$ as $d \to \infty$. This proves Claim 1.

Claim 2: Conditioned on a choice of $f_0, g_1, \ldots, g_m$ for which W_m is finite, $\operatorname{Prob}(H_f \cap W_m \cap U_{>d/(m+1)} = \emptyset) = 1 - o(1)$ as $d \to \infty$.

Proof of Claim 2: The Bézout theorem argument in the proof of Claim 1 shows that $\#W_m = O(d^m)$. For a given point $P \in W_m$, the set H^{bad} of $h \in A_{\le \eta}$ for which H_f passes through P is either $\emptyset$ or a coset of $\ker(\mathrm{ev}_P : A_{\le \eta} \to \kappa(P))$, where $\kappa(P)$ is the residue field of P. If moreover $\deg P > d/(m+1)$, then Lemma 2.5 implies $\#H^{\text{bad}}/\#A_{\le \eta} \le q^{-\nu}$ where $\nu = \min(\eta + 1, d/(m+1))$. Hence

$$\operatorname{Prob}(H_f \cap W_m \cap U_{>d/(m+1)} \ne \emptyset) \le \#W_m q^{-\nu} = O(d^m q^{-\nu}) = o(1)$$

as $d \to \infty$, since ν eventually grows linearly in d. This proves Claim 2.

End of proof of Lemma 2.6: Choose $f \in S_d$ uniformly at random. Claims 1 and 2 show that with probability $\prod_{i=0}^{m-1}(1 - o(1)) \cdot (1 - o(1)) = 1 - o(1)$ as $d \to \infty$, $\dim W_i = m - i$

for $i = 0, 1, \ldots, m$ and $H_f \cap W_m \cap U_{>d/(m+1)} = \emptyset$. But $H_f \cap W_m$ is the subvariety of U cut out by the equations $f(P) = (D_1 f)(P) = \cdots = (D_m f)(P) = 0$, so $H_f \cap W_m \cap U_{>d/(m+1)}$ is exactly the set of points of $H_f \cap U$ of degree $> d/(m+1)$ where $H_f \cap U$ is not smooth of dimension $m-1$. $\square$

2.4. **Proofs of theorems over finite fields.**

Proof of Theorem 1.2. As mentioned in the proof of Lemma 2.4, the number of closed points of degree r in U is $O(q^{rm})$; this guarantees that the product defining $\zeta_U(s)^{-1}$ converges at $s = m+1$. By Lemma 2.2,

$$\lim_{r\to\infty} \mu(\mathcal{P}_r) = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)}\, \zeta_U(m+1)^{-1}.$$

On the other hand, the definitions imply $\mathcal{P} \subseteq \mathcal{P}_r \subseteq \mathcal{P} \cup \mathcal{Q}_r^{\text{medium}} \cup \mathcal{Q}^{\text{high}}$, so $\overline{\mu}(\mathcal{P})$ and $\underline{\mu}(\mathcal{P})$ each differ from $\mu(\mathcal{P}_r)$ by at most $\overline{\mu}(\mathcal{Q}_r^{\text{medium}}) + \overline{\mu}(\mathcal{Q}^{\text{high}})$. Applying Lemmas 2.4 and 2.6 and letting r tend to ∞, we obtain

$$\mu(\mathcal{P}) = \lim_{r\to\infty} \mu(\mathcal{P}_r) = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)}\, \zeta_U(m+1)^{-1}.$$

$\square$

Proof of Theorem 1.1. Take $Z = \emptyset$ and $T = \{0\}$ in Theorem 1.2. $\square$

Proof of Theorem 1.3. The existence of $X_1, \ldots, X_u$ and Lemmas 2.4 and 2.6 let us approximate $\mathcal{P}$ by the set $\mathcal{P}_r$ defined only by the conditions at closed points P of degree less than r, for large r. For each $P \in \mathbf{P}^n_{<r}$, the hypothesis $\mu_P(\partial U_P) = 0$ lets us approximate U_P by a union of cosets of an ideal I_P of finite index in $\hat{\mathcal{O}}_P$. (The details are completely analogous to those in the proof of Lemma 20 of [PS99].) Finally, Lemma 2.1 implies that for $d \gg 1$, the images of $f \in S_d$ in $\prod_{P \in \mathbf{P}^n_{<r}} \hat{\mathcal{O}}_P / I_P$ are equidistributed. $\square$

Finally let us show that the densities in our theorems do not change if in the definition of density we consider only f for which H_f is geometrically integral, at least for $n \geq 2$.

Proposition 2.7. *Suppose $n \geq 2$. Let $\mathcal{R}$ be the set of $f \in S_{\text{homog}}$ for which H_f fails to be a geometrically integral hypersurface of dimension $n-1$. Then $\mu(\mathcal{R}) = 0$.*

Proof. We have $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$ where $\mathcal{R}_1$ is the set of $f \in S_{\text{homog}}$ that factor nontrivially over $\mathbf{F}_q$, and $\mathcal{R}_2$ is the set of $f \in S_{\text{homog}}$ of the form $N_{\mathbf{F}_{q^e}/\mathbf{F}_q}(g)$ for some homogeneous polynomial $g \in \mathbf{F}_{q^e}[x_0, \ldots, x_n]$ and $e \geq 2$. (Note: if our base field were an arbitrary perfect field, an irreducible polynomial that is not absolutely irreducible would be a constant times a norm, but the constant is unnecessary here, since $N_{\mathbf{F}_{q^e}/\mathbf{F}_q} : \mathbf{F}_{q^e} \to \mathbf{F}_q$ is surjective.)

We have

$$\frac{\#(\mathcal{R}_1 \cap S_d)}{\#S_d} \leq \frac{1}{\#S_d} \sum_{i=1}^{\lfloor d/2 \rfloor} (\#S_i)(\#S_{d-i}) = \sum_{i=1}^{\lfloor d/2 \rfloor} q^{-N_i},$$

where

$$N_i = \binom{n+d}{n} - \binom{n+i}{n} - \binom{n+d-i}{n}.$$

For $1 \le i \le d/2 - 1$,

$$\begin{aligned} N_{i+1} - N_i &= \left[\binom{n+d-i}{n} - \binom{n+d-i-1}{n}\right] - \left[\binom{n+i+1}{n} - \binom{n+i}{n}\right] \\ &= \binom{n+d-i-1}{n-1} - \binom{n+i}{n-1} \\ &> 0. \end{aligned}$$

Similarly, for $d \gg n$,

$$N_1 = \binom{n+d-1}{n-1} - \binom{n+1}{n} \ge \binom{n+d-1}{1} - \binom{n+1}{1} = d-2.$$

Thus

$$\frac{\#(\mathcal{R}_1 \cap S_d)}{\#S_d} \le \sum_{i=1}^{\lfloor d/2 \rfloor} q^{-N_i} \le \sum_{i=1}^{\lfloor d/2 \rfloor} q^{2-d} \le dq^{2-d},$$

which tends to zero as $d \to \infty$.

The number of $f \in S_d$ that are norms of homogeneous polynomials of degree d/e over $\mathbf{F}_{q^e}$ is at most $(q^e)^{\binom{d/e+n}{n}}$. Therefore

$$\frac{\#(\mathcal{R}_2 \cap S_d)}{\#S_d} \le \sum_{e|d, e>1} q^{-M_e}$$

where $M_e = \binom{d+n}{n} - e\binom{d/e+n}{n}$. For $2 \le e \le d$,

$$\begin{aligned} \frac{e\binom{d/e+n}{n}}{\binom{d+n}{n}} &= \frac{e\left(\frac{d}{e}+n\right)\left(\frac{d}{e}+n-1\right)\cdots\left(\frac{d}{e}+1\right)}{(d+n)(d+n-1)\cdots(d+1)} \\ &\le \frac{e\left(\frac{d}{e}+n\right)\left(\frac{d}{e}+n-1\right)}{(d+n)(d+n-1)} \\ &\le \frac{e\left(\frac{d}{e}+n\right)^2}{d^2} \\ &= \frac{1}{e} + \frac{2n}{d} + \frac{en^2}{d^2} \\ &\le \frac{1}{2} + \frac{2n^2}{d} + \frac{dn^2}{d^2} \\ &\le 2/3, \end{aligned}$$

once $d \ge 18n^2$. Hence in this case, $M_e \ge \frac{1}{3}\binom{d+n}{n} \ge d^2/6$ for large d, so

$$\frac{\#(\mathcal{R}_2 \cap S_d)}{\#S_d} \le \sum_{e|d, e>1} q^{-M_e} \le dq^{-d^2/6},$$

which tends to zero as $d \to \infty$. $\square$

Another proof of Proposition 2.7 is given in Section 3.2, but that proof is valid only for $n \ge 3$.

3. Applications

3.1. **Counterexamples to Bertini.** Ironically, we can use our hypersurface Bertini theorem to construct counterexamples to the original hyperplane Bertini theorem! More generally, we can show that hypersurfaces of bounded degree do not suffice to yield a smooth intersection.

Theorem 3.1 (Anti-Bertini theorem)**.** *Given a finite field $\mathbf{F}_q$ and integers $n \geq 2$, $d \geq 1$, there exists a smooth projective geometrically integral hypersurface X in $\mathbf{P}^n$ over $\mathbf{F}_q$ such that for each $f \in S_1 \cup \cdots \cup S_d$, $H_f \cap X$ fails to be smooth of dimension $n-2$.*

Proof. Let $H^{(1)}, \ldots, H^{(\ell)}$ be a list of the H_f arising from $f \in S_1 \cup \cdots \cup S_d$. For $i = 1, \ldots, \ell$ in turn, choose a closed point $P_i \in H^{(i)}$ distinct from P_j for $j < i$. Using a T as in Theorem 1.2, we can express the condition that a hypersurface in $\mathbf{P}^n$ be smooth of dimension $n-1$ at P_i and have tangent space at P_i equal to that of $H^{(i)}$ whenever the latter is smooth of dimension $n-1$ at P_i. Theorem 1.2 (with Proposition 2.7) implies that there exists a smooth projective geometrically integral hypersurface $X \subseteq \mathbf{P}^n$ satisfying these conditions. Then for each i, $X \cap H^{(i)}$ fails to be smooth of dimension $n-2$ at P_i. □

Remark. Katz [Kat99, p. 621] remarks that if X is the hypersurface

$$\sum_{i=1}^{n+1} (X_i Y_i^q - X_i^q Y_i) = 0$$

in $\mathbf{P}^{2n+1}$ over $\mathbf{F}_q$ with homogeneous coordinates $X_1, \ldots, X_{n+1}, Y_1, \ldots, Y_{n+1}$, then $H \cap X$ is singular for every hyperplane H in $\mathbf{P}^{2n+1}$ over $\mathbf{F}_q$.

3.2. **Singularities of positive dimension.** Let X be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 0$ over $\mathbf{F}_q$. Given $f \in S_{\mathrm{homog}}$, let $(H_f \cap X)_{\mathrm{sing}}$ be the closed subset of points where $H_f \cap X$ is not smooth of dimension $m-1$.

Although Theorem 1.1 shows that for a nonempty smooth quasiprojective subscheme $X \subseteq \mathbf{P}^n$ of dimension $m \geq 0$, there is a positive probability that $(H_f \cap X)_{\mathrm{sing}} \neq \emptyset$, we now show that the probability that $\dim(H_f \cap X)_{\mathrm{sing}} \geq 1$ is zero.

Theorem 3.2. *Let X be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 0$ over $\mathbf{F}_q$. Define*

$$\mathcal{S} := \{\, f \in S_{\mathrm{homog}} : \dim(H_f \cap X)_{\mathrm{sing}} \geq 1 \,\}.$$

Then $\mu(\mathcal{S}) = 0$.

Proof. This is a corollary of Lemma 2.6 with $U = X$, since $\mathcal{S} \subseteq \mathcal{Q}^{\mathrm{high}}$. □

Remark. If $f \in S_{\mathrm{homog}}$ is such that H_f is not geometrically integral of dimension $n-1$, then $\dim(H_f)_{\mathrm{sing}} \geq n-2$. Hence Theorem 3.2 with $X = \mathbf{P}^n$ gives a new proof of Proposition 2.7, at least when $n \geq 3$.

3.3. **Space-filling curves.** We next use Theorem 1.2 to answer affirmatively all the open questions in [Kat99]. In their strongest forms, these are

> *Question 10:* Given a smooth projective geometrically connected variety X of dimension $m \geq 2$ over $\mathbf{F}_q$, and a finite extension E of $\mathbf{F}_q$, is there always a closed subscheme Y in X, $Y \neq X$, such that $Y(E) = X(E)$ and such that Y is smooth and geometrically connected over $\mathbf{F}_q$?

> *Question 13:* Given a closed subscheme $X \subseteq \mathbf{P}^n$ over $\mathbf{F}_q$ that is smooth and geometrically connected of dimension m, and a point $P \in X(\mathbf{F}_q)$, is it true for all $d \gg 1$ that there exists a hypersurface $H \subseteq \mathbf{P}^n$ of degree d such that P lies on H and $H \cap X$ is smooth of dimension $m-1$?

Both of these questions are answered by the following:

Theorem 3.3. *Let X be a smooth quasiprojective subscheme of $\mathbf{P}^n$ of dimension $m \geq 1$ over $\mathbf{F}_q$, and let $F \subset X$ be a finite set of closed points. Then there exists a smooth projective geometrically integral hypersurface $H \subset \mathbf{P}^n$ such that $H \cap X$ is smooth of dimension $m-1$ and contains F.*

Remarks.

(1) If $m \geq 2$ and if X in Theorem 3.3 is geometrically connected and projective in addition to being smooth, then $H \cap X$ will be geometrically connected and projective too. This follows from Corollary III.7.9 in [Har77].
(2) Recall that if a variety is geometrically connected and smooth, then it is geometrically integral.
(3) Question 10 and (partially) Question 13 were independently answered by Gabber [Gab01].

Proof of Theorem 3.3. Let $T_{P,X}$ be the Zariski tangent space of a point P on X. At each $P \in F$ choose a codimension 1 subspace $V_P \subset T_{P,\mathbf{P}^n}$ not equal to $T_{P,X}$. We will apply Theorem 1.3 with the following local conditions: for $P \in F$, U_P is the condition that the hypersurface H_f passes through P and $T_{P,H} = V_P$; for $P \notin F$, U_P is the condition that H_f and $H_f \cap X$ be smooth of dimensions $n-1$ and $m-1$, respectively, at P. Theorem 1.3 (with Proposition 2.7) implies the existence of a smooth projective geometrically integral hypersurface $H \subset \mathbf{P}^n$ satisfying these conditions. $\square$

Remark. If we did not insist in Theorem 3.3 that H be smooth, then in the proof, Theorem 1.2 would suffice in place of Theorem 1.3. This weakened version of Theorem 3.3 is already enough to imply Corollaries 3.4 and 3.5, and Theorem 3.7. Corollary 3.6 also follows from Theorem 1.2.

Corollary 3.4. *Let X be a smooth, projective, geometrically integral variety of dimension $m \geq 1$ over $\mathbf{F}_q$, let F be a finite set of closed points of X, and let y be an integer with $1 \leq y \leq m$. Then there exists a smooth, projective, geometrically integral subvariety $Y \subseteq X$ of dimension y such that $F \subset Y$.*

Proof. Use Theorem 3.3 with reverse induction on y. $\square$

Corollary 3.5 (Space-filling curves)**.** *Let X be a smooth, projective, geometrically integral variety of dimension $m \geq 1$ over $\mathbf{F}_q$, and let E be a finite extension of $\mathbf{F}_q$. Then there exists a smooth, projective, geometrically integral curve $Y \subseteq X$ such that $Y(E) = X(E)$.*

Proof. Apply Corollary 3.4 with $y = 1$ and F the set of closed points corresponding to $X(E)$. $\square$

In a similar way, we prove the following:

Corollary 3.6 (Space-avoiding varieties)**.** *Let X be a smooth, projective, geometrically integral variety of dimension m over $\mathbf{F}_q$, and let ℓ and y be integers with $\ell \geq 1$ and $1 \leq y < m$. Then there exists a smooth, projective, geometrically integral subvariety $Y \subseteq X$ of dimension y such that Y has no points of degree less than ℓ.*

Proof. Repeat the arguments used in the proof of Theorem 3.3 and Corollary 3.4, but in the first application of Theorem 1.3, instead force the hypersurface to avoid the finitely many points of X of degree less than ℓ. $\square$

3.4. **Albanese varieties.** For a smooth, projective, geometrically integral variety X over a field, let $\operatorname{Alb} X$ be its Albanese variety. As pointed out in [Kat99], a positive answer to Question 13 implies that every positive dimensional abelian variety A over $\mathbf{F}_q$ contains a smooth, projective, geometrically integral curve Y such that the natural map $\operatorname{Alb} Y \to A$ is surjective. We generalize this slightly in the next result, which strengthens Theorem 11 of [Kat99] in the finite field case.

Theorem 3.7. *Let X be a smooth, projective, geometrically integral variety of dimension $m \geq 1$ over $\mathbf{F}_q$. Then there exists a smooth, projective, geometrically integral curve $Y \subseteq X$ such that the natural map $\operatorname{Alb} Y \to \operatorname{Alb} X$ is surjective.*

Proof. Choose a prime ℓ not equal to the characteristic. Represent each ℓ-torsion point in $(\operatorname{Alb} X)(\overline{\mathbf{F}}_q)$ by a zero-cycle of degree zero on X, and let F be the finite set of closed points appearing in these. Use Corollary 3.4 to construct a smooth, projective, geometrically integral curve Y passing through all points of F. The image of $\operatorname{Alb} Y \to \operatorname{Alb} X$ is an abelian subvariety of $\operatorname{Alb} X$ containing all the ℓ-torsion points, so the image equals $\operatorname{Alb} X$. (The trick of using the ℓ-torsion points is due to Gabber [Kat99].) $\square$

Remarks.

(1) A slightly more general argument proves Theorem 3.7 over an arbitrary field k [Gab01, Proposition 2.4].
(2) It is also true that any abelian variety over a field k can be embedded as an abelian subvariety of the Jacobian of a smooth, projective, geometrically integral curve over k [Gab01].

3.5. **Plane curves.** The probability that a projective plane curve over $\mathbf{F}_q$ is nonsingular equals

$$\zeta_{\mathbf{P}^2}(3)^{-1} = (1 - q^{-1})(1 - q^{-2})(1 - q^{-3}).$$

(We interpret this probability as the density given by Theorem 1.1 for $X = \mathbf{P}^2$ in $\mathbf{P}^2$.) Theorem 1.3 with a simple local calculation shows that the probability that a projective plane curve over $\mathbf{F}_q$ has at worst nodes as singularities equals

$$\zeta_{\mathbf{P}^2}(4)^{-1} = (1 - q^{-2})(1 - q^{-3})(1 - q^{-4}).$$

For $\mathbf{F}_2$, these probabilities are $21/64$ and $315/512$.

Remark. Although Theorem 1.1 guarantees the existence of a smooth plane curve of degree d over $\mathbf{F}_q$ only when d is sufficiently large relative to q, in fact such a curve exists for every $d \geq 1$ and every finite field $\mathbf{F}_q$. Moreover, the corresponding statement for hypersurfaces of specified dimension and degree is true [KS99, §11.4.6]. In fact, for any field k and integers $n \geq 1$, $d \geq 3$ with (n, d) not equal to $(1, 3)$ or $(2, 4)$, there exists a smooth hypersurface X over k of degree d in $\mathbf{P}^{n+1}$ such that X has *no nontrivial automorphisms* over $\overline{k}$ [Poo00]. This last statement is false for $(1, 3)$; whether or not it holds for $(2, 4)$ is an open question.

4. An open question

In response to Theorem 1.1, Matt Baker has asked the following:

Question 4.1. Fix a smooth quasiprojective subscheme X of dimension m over $\mathbf{F}_q$. Does there exist an integer $n_0 > 0$ such that for $n \geq n_0$, if $\iota : X \to \mathbf{P}^n$ is an embedding such that no connected component of X is mapped by ι into a hyperplane in $\mathbf{P}^n$, then there exists a hyperplane $H \subseteq \mathbf{P}^n$ over $\mathbf{F}_q$ such that $H \cap \iota(X)$ is smooth of dimension $m-1$?

Theorem 1.1 proves that the answer is yes, if one allows only the embeddings ι obtained by composing a fixed initial embedding $X \to \mathbf{P}^n$ with d-uple embeddings $\mathbf{P}^n \to \mathbf{P}^N$. Nevertheless, we conjecture that for each X of positive dimension, the answer to Question 4.1 is no.

5. An arithmetic analogue

We formulate an analogue of Theorem 1.1 in which the smooth quasiprojective scheme X over $\mathbf{F}_q$ is replaced by a regular quasiprojective scheme X over $\operatorname{Spec} \mathbf{Z}$, and we seek hyperplane sections that are regular. The reason for using regularity instead of the stronger condition of being smooth over $\mathbf{Z}$ is discussed in Section 5.7.

Fix $n \in \mathbf{N} = \mathbf{Z}_{\geq 0}$. Redefine S as the homogeneous coordinate ring $\mathbf{Z}[x_0, \ldots, x_n]$ of $\mathbf{P}^n_{\mathbf{Z}}$, let $S_d \subset S$ be the $\mathbf{Z}$-submodule of homogeneous polynomials of degree d, and let $S_{\text{homog}} = \bigcup_{d=0}^{\infty} S_d$. If p is prime, let $S_{d,p}$ be the set of homogeneous polynomials in $\mathbf{F}_p[x_0, \ldots, x_n]$ of degree d. For each $f \in S_d$, let H_f be the subscheme $\operatorname{Proj}(S/(f)) \subseteq \mathbf{P}^n_{\mathbf{Z}}$. Similarly, for $f \in S_{d,p}$, let H_f be $\operatorname{Proj}(\mathbf{F}_p[x_0, \ldots, x_n]/(f)) \subseteq \mathbf{P}^n_{\mathbf{F}_p}$.

If $\mathcal{P}$ is a subset of $\mathbf{Z}^N$ for some $N \geq 1$, define the *upper density*

$$\overline{\mu}(\mathcal{P}) := \max_{\sigma} \limsup_{B_{\sigma(1)} \to \infty} \cdots \limsup_{B_{\sigma(N)} \to \infty} \frac{\#(\mathcal{P} \cap \text{Box})}{\#\text{Box}},$$

where σ ranges over permutations of $\{1, 2, \ldots, N\}$ and

$$\text{Box} = \{(x_1, \ldots, x_N) \in \mathbf{Z}^N : |x_i| \leq B_i \text{ for all } i\}.$$

(In other words, we take the lim sup only over growing boxes whose dimensions can be ordered so that each is very large relative to the previous dimensions.) Define *lower density* $\underline{\mu}(\mathcal{P})$ similarly using min and lim inf. Define upper and lower densities $\overline{\mu}_d$ and $\underline{\mu}_d$ of subsets of a fixed S_d by identifying S_d with $\mathbf{Z}^N$ using a $\mathbf{Z}$-basis of monomials. If $\mathcal{P} \subseteq S_{\text{homog}}$, define $\overline{\mu}(\mathcal{P}) = \limsup_{d \to \infty} \overline{\mu}_d(\mathcal{P} \cap S_d)$ and $\underline{\mu}(\mathcal{P}) = \liminf_{d \to \infty} \underline{\mu}_d(\mathcal{P} \cap S_d)$. Finally, if $\mathcal{P}$ is a subset of S_{homog}, define $\mu(\mathcal{P})$ as the common value of $\overline{\mu}(\mathcal{P})$ and $\underline{\mu}(\mathcal{P})$ if $\overline{\mu}(\mathcal{P}) = \underline{\mu}(\mathcal{P})$. The reason for choosing this definition is that it makes our proof work; aesthetically, we would have preferred to prove a stronger statement by defining density as the limit over arbitrary boxes in S_d with $\min\{d, B_1, \ldots, B_N\} \to \infty$; probably such a statement is also true but extremely difficult to prove.

For a scheme X of finite type over $\mathbf{Z}$, define the zeta function [Ser65, §1.3]

$$\zeta_X(s) := \prod_{\text{closed } P \in X} \left(1 - \#\kappa(P)^{-s}\right)^{-1},$$

where $\kappa(P)$ is the (finite) residue field of P. This generalizes the definition of Section 1, since a scheme of finite type over $\mathbf{F}_q$ can be viewed as a scheme of finite type over $\mathbf{Z}$. On the other hand, $\zeta_{\operatorname{Spec} \mathbf{Z}}(s)$ is the Riemann zeta function.

The *abc* conjecture, formulated by D. Masser and J. Oesterlé in response to insights of R. C. Mason, L. Szpiro, and G. Frey, is the statement that for any $\epsilon > 0$, there exists a constant $C = C(\epsilon) > 0$ such that if a, b, c are coprime positive integers satisfying $a + b = c$, then $c < C(\prod_{p|abc} p)^{1+\epsilon}$.

For convenience, we say that a scheme X of finite type over $\mathbf{Z}$ is *regular of dimension* m if for every *closed* point P of X, the local ring $\mathcal{O}_{X,P}$ is regular of dimension m. For a scheme X of finite type over $\mathbf{Z}$, this is equivalent to the condition that $\mathcal{O}_{X,P}$ be regular for *all* $P \in X$ and all irreducible components of X have Krull dimension m. If X is smooth of relative dimension $m-1$ over $\operatorname{Spec} \mathbf{Z}$, then X is regular of dimension m, but the converse need not hold. The empty scheme is regular of every dimension.

Theorem 5.1 (Bertini for arithmetic schemes)**.** *Assume the abc conjecture and Conjecture 5.2 below. Let X be a quasiprojective subscheme of $\mathbf{P}^n_{\mathbf{Z}}$ that is regular of dimension $m \geq 0$. Define*

$$\mathcal{P} := \{\, f \in S_{\text{homog}} : H_f \cap X \text{ is regular of dimension } m-1 \,\}.$$

Then $\mu(\mathcal{P}) = \zeta_X(m+1)^{-1}$.

Remark. The case $X = \mathbf{P}^0_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}$ in $\mathbf{P}^0_{\mathbf{Z}}$ of Theorem 5.1 is the statement that the density of squarefree integers is $\zeta(2)^{-1}$, where ζ is the Riemann zeta function. The proof of Theorem 5.1 in general will involve questions about squarefree values of multivariable polynomials.

Given a scheme X, let $X_{\mathbf{Q}} = X \times \mathbf{Q}$, and let $X_p = X \times \mathbf{F}_p$ for each prime p.

Conjecture 5.2. *Let X be an integral quasiprojective subscheme of $\mathbf{P}^n_{\mathbf{Z}}$ that is smooth over $\mathbf{Z}$ of relative dimension r. There exists $c > 0$ such that if d and p are sufficiently large, then*

$$\frac{\#\{\, f \in S_{d,p} : \dim(H_f \cap X_p)_{\text{sing}} \geq 1 \,\}}{\# S_{d,p}} < \frac{c}{p^2}.$$

Heuristically one expects that Conjecture 5.2 is true even if c/p^2 is replaced by c/p^k for any fixed $k \geq 2$. On the other hand, for the application to Theorem 5.1, it would suffice to prove a weak form of Conjecture 5.2 with the upper bound c/p^2 replaced by any $\epsilon_p > 0$ such that $\sum_p \epsilon_p < \infty$. We used c/p^2 only to simplify the statement.

If d is sufficiently large relative to p, then Theorem 3.2 provides a suitable upper bound on the ratio in Conjecture 5.2. If p is sufficiently large relative to d, then one can derive a suitable upper bound from the Weil Conjectures. (In particular, the truth of Conjecture 5.2 is unchanged if we drop the assumption that d and p are sufficiently large.) The difficulty lies in the case where d is *comparable* to p.

See Section 5.4, for a proof of Conjecture 5.2 in the case where the closure of $X_{\mathbf{Q}}$ in $\mathbf{P}^n_{\mathbf{Q}}$ has at most isolated singularities.

5.1. **Singular points with small residue field.** We begin the proof of Theorem 5.1 with analogues of results in Section 2.1. If M is a finite abelian group, let $\operatorname{length}_{\mathbf{Z}} M$ be its length as a $\mathbf{Z}$-module.

Lemma 5.3. *If Y is a zero-dimensional closed subscheme of $\mathbf{P}^n_{\mathbf{Z}}$, then the map $\phi_d : S_d = H^0(\mathbf{P}^n_{\mathbf{Z}}, \mathcal{O}(d)) \to H^0(Y, \mathcal{O}_Y(d))$ is surjective for $d \geq \operatorname{length}_{\mathbf{Z}} H^0(Y, \mathcal{O}_Y) - 1$.*

Proof. Assume $d \geq \operatorname{length}_{\mathbf{Z}} H^0(Y, \mathcal{O}_Y) - 1$. The cokernel C of ϕ_d is finite, since it is a quotient of the finite group $H^0(Y, \mathcal{O}_Y(d))$. Moreover, C has trivial p-torsion for each prime p, by Lemma 2.1 applied to $Y_{\mathbf{F}_p}$ in $\mathbf{P}^n_{\mathbf{F}_p}$. Thus $C = 0$. Hence ϕ_d is surjective. □

Lemma 5.4. *If $\mathcal{P} \subseteq \mathbf{Z}^N$ is a union of c distinct cosets of a subgroup $G \subseteq \mathbf{Z}^N$ of index m, then $\mu(\mathcal{P}) = c/m$.*

Proof. Without loss of generality, we may replace G with its subgroup $(m\mathbf{Z})^N$ of finite index. The result follows, since any of the boxes in the definition of μ can be approximated by a box of dimensions that are multiples of m, with an error that becomes negligible compared with the number of lattice points in the box as the box dimensions tend to infinity. □

If X is a scheme of finite type over $\mathbf{Z}$, define $X_{<r}$ as the set of closed points P with $\#\kappa(P) < r$. (This conflicts with the corresponding definition before Lemma 2.2; forget that one.) Define $X_{\geq r}$ similarly. We say that X is regular of dimension m at a closed point P of $\mathbf{P}^n_{\mathbf{Z}}$ if either $P \notin X$ or $\mathcal{O}_{X,P}$ is a regular local ring of dimension m.

Lemma 5.5 (Small singularities)**.** *Let X be a quasiprojective subscheme of $\mathbf{P}^n_{\mathbf{Z}}$ that is regular of dimension $m \geq 0$. Define*

$$\mathcal{P}_r := \{\, f \in S_{\text{homog}} : H_f \cap X \text{ is regular of dimension } m-1 \text{ at all } P \in X_{<r} \,\}.$$

Then

$$\mu(\mathcal{P}_r) = \prod_{P \in X_{<r}} \left(1 - \#\kappa(P)^{-(m+1)}\right).$$

Proof. Given Lemmas 5.3 and 5.4, the proof is the same as that of Lemma 2.2 with $Z = \emptyset$. □

5.2. **Reductions.** Theorem 1 of [Ser65] shows that $\prod_{P \in X_{<r}} \left(1 - \#\kappa(P)^{-(m+1)}\right)$ converges to $\zeta_X(m+1)^{-1}$ as $r \to \infty$. Thus Theorem 5.1 follows from Lemma 5.5 and the following, whose proof will occupy the rest of Section 5.

Lemma 5.6 (Large singularities)**.** *Assume the abc conjecture and Conjecture 5.2. Let X be a quasiprojective subscheme of $\mathbf{P}^n_{\mathbf{Z}}$ that is regular of dimension $m \geq 0$. Define*

$$\mathcal{Q}_r^{\text{large}} := \{\, f \in S_{\text{homog}} : \text{there exists } P \in X_{\geq r} \text{ such that } H_f \cap X \text{ is not regular of dimension } m-1 \text{ at } P \,\}.$$

Then $\lim_{r\to\infty} \overline{\mu}(\mathcal{Q}_r^{\text{large}}) = 0$.

Lemma 5.6 holds for X if it holds for each subscheme in an open cover of X, since by quasicompactness any such open cover has a finite subcover. In particular, we may assume that X is connected. Since X is also regular, X is integral. If the image of $X \to \operatorname{Spec} \mathbf{Z}$ is a closed point (p), then X is smooth of dimension m over $\mathbf{F}_p$, and Lemma 5.6 for X follows from Lemmas 2.4 and 2.6. Thus from now on, we assume that X dominates $\operatorname{Spec} \mathbf{Z}$.

Since X is regular, its generic fiber $X_{\mathbf{Q}}$ is regular. Since $\mathbf{Q}$ is a perfect field, it follows that $X_{\mathbf{Q}}$ is smooth over $\mathbf{Q}$, of dimension $m-1$. By [EGA IV(4), 17.7.11(iii)], there exists an integer $t \geq 1$ such that $X \times \mathbf{Z}[1/t]$ is smooth of relative dimension $m-1$ over $\mathbf{Z}[1/t]$.

5.3. **Singular points of small residue characteristic.**

Lemma 5.7 (Singularities of small characteristic)**.** *Fix a nonzero prime $p \in \mathbf{Z}$. Let X be an integral quasiprojective subscheme of $\mathbf{P}^n_{\mathbf{Z}}$ that dominates $\operatorname{Spec} \mathbf{Z}$ and is regular of dimension $m \geq 0$. Define*

$$\mathcal{Q}_{p,r} := \{\, f \in S_{\text{homog}} : \text{ there exists } P \in X_p \text{ with } \#\kappa(P) \geq r \text{ such that } H_f \cap X \text{ is not regular of dimension } m-1 \text{ at } P \,\}.$$

Then $\lim_{r\to\infty} \overline{\mu}(\mathcal{Q}_{p,r}) = 0$.

Proof. We may assume that X_p is nonempty. Then, since X_p is cut out in X by a single equation $p = 0$, and since p is neither a unit nor a zerodivisor in $H^0(X, \mathcal{O}_X)$, $\dim X_p = m-1$.

Let

$$\mathcal{Q}^{\text{medium}}_{p,r} := \bigcup_{d\geq 0} \{\, f \in S_d : \text{ there exists } P \in X_p \text{ with } r \leq \#\kappa(P) \leq p^{d/(m+1)} \text{ such that } H_f \cap X \text{ is not regular of dimension } m-1 \text{ at } P \,\}$$

and

$$\mathcal{Q}^{\text{high}}_{p} := \bigcup_{d\geq 0} \{\, f \in S_d : \text{ there exists } P \in X_p \text{ with } \#\kappa(P) > p^{d/(m+1)} \text{ such that } H_f \cap X \text{ is not regular of dimension } m-1 \text{ at } P \,\}.$$

Since $\mathcal{Q}_{p,r} = \mathcal{Q}^{\text{medium}}_{p,r} \cup \mathcal{Q}^{\text{high}}_{p}$, it suffices to prove $\lim_{r\to\infty} \overline{\mu}(\mathcal{Q}^{\text{medium}}_{p,r}) = 0$ and $\overline{\mu}(\mathcal{Q}^{\text{high}}_{p}) = 0$. We will adapt the proofs of Lemmas 2.4 and 2.6.

If P is a closed point of X, let $\mathfrak{m}_{X,P} \subseteq \mathcal{O}_X$ be the ideal sheaf corresponding to P, and let Y_P be the closed subscheme of X corresponding to the ideal sheaf $\mathfrak{m}^2_{X,P}$. For fixed d, the set $\mathcal{Q}^{\text{medium}}_{p,r} \cap S_d$ is contained in the union over P with $r \leq \#\kappa(P) \leq p^{d/(m+1)}$ of the kernel of the restriction $\phi_P : S_d \to H^0(Y_P, \mathcal{O}(d))$. Since $H^0(Y_P, \mathcal{O}(d)) \simeq H^0(Y_P, \mathcal{O}_{Y_P})$ has length $(m+1)[\kappa(P) : \mathbf{F}_p] \leq d$ as a $\mathbf{Z}$-module, ϕ_P is surjective by Lemma 5.3, and Lemma 5.4 implies $\overline{\mu}(\ker \phi_P) = \#\kappa(P)^{-(m+1)}$. Thus

$$\overline{\mu}(\mathcal{Q}^{\text{medium}}_{p,r} \cap S_d) \leq \sum_P \overline{\mu}(\ker \phi_P) = \sum_P \#\kappa(P)^{-(m+1)}.$$

where the sum is over $P \in X_p$ with $r \leq \#\kappa(P) \leq p^{d/(m+1)}$. The crude form $\#X_p(\mathbf{F}_{p^e}) = O(p^{e(m-1)})$ of the bound in [LW54] implies that

$$\lim_{r\to\infty} \overline{\mu}(\mathcal{Q}^{\text{medium}}_{p,r}) = \lim_{r\to\infty} \lim_{d\to\infty} \overline{\mu}(\mathcal{Q}^{\text{medium}}_{p,r} \cap S_d) = 0.$$

Next we turn to $\mathcal{Q}^{\text{high}}_{p}$. Since we are free to pass to an open cover of X, we may assume that X is contained in the subset $\mathbf{A}^n_{\mathbf{Z}} := \{x_0 \neq 0\}$ of $\mathbf{P}^n_{\mathbf{Z}}$. Let $A = \mathbf{Z}[x_1, \ldots, x_n]$ be the ring of regular functions on $\mathbf{A}^n_{\mathbf{Z}}$. Identify S_d with the set of dehomogenizations $A_{\leq d} = \{\, f \in A : \deg f \leq d \,\}$, where $\deg f$ denotes total degree.

Let Ω be the sheaf of differentials $\Omega_{X_p/\mathbf{F}_p}$. For $P \in X_p$, define the dimension of the fiber

$$\phi(P) = \dim_{\kappa(P)} \, \Omega \underset{\mathcal{O}_{X_p}}{\otimes} \kappa(P).$$

Let $\mathfrak{m}_{X_p,P}$ be the maximal ideal of the local ring $\mathcal{O}_{X_p,P}$. If P is a closed point of X_p, the isomorphism

$$\Omega \underset{\mathcal{O}_{X_p}}{\otimes} \kappa(P) \simeq \frac{\mathfrak{m}_{X_p,P}}{\mathfrak{m}_{X_p,P}^2}$$

of Proposition II.8.7 of [Har77] shows that $\phi(P) = \dim_{\kappa(P)} \mathfrak{m}_{X_p,P}/\mathfrak{m}_{X_p,P}^2$; moreover

$$p\mathcal{O}_{X,P} \to \frac{\mathfrak{m}_{X,P}}{\mathfrak{m}_{X,P}^2} \to \frac{\mathfrak{m}_{X_p,P}}{\mathfrak{m}_{X_p,P}^2} \to 0$$

is exact. Since X is regular of dimension m, the middle term is a $\kappa(P)$-vector space of dimension m. But the module on the left is generated by one element. Hence $\phi(P)$ equals $m-1$ or m at each closed point P.

Let $Y = \{\, P \in X_p : \phi(P) \geq m \,\}$. By Exercise II.5.8(a) of [Har77], Y is a closed subset, and we give Y the structure of a reduced subscheme of X_p. Let $U = X_p - Y$. Thus for closed points $P \in X_p$,

$$\phi(P) = \begin{cases} m-1, & \text{if } P \in U \\ m, & \text{if } P \in Y. \end{cases}$$

If U is nonempty, then $\dim U = \dim X_p = m-1$, so U is smooth of dimension $m-1$ over $\mathbf{F}_p$, and $\Omega|_U$ is locally free. At a closed point $P \in U$, we can find $t_1, \ldots, t_n \in A$ such that $dt_1, \ldots, dt_{m-1}$ represent an $\mathcal{O}_{X_p,P}$-basis for the stalk Ω_P, and $dt_m, \ldots, dt_n$ represent a basis for the kernel of $\Omega_{\mathbf{A}^n/\mathbf{F}_p} \otimes \mathcal{O}_{X_p,P} \to \Omega_P$. Let $\partial_1, \ldots, \partial_n \in \mathcal{T}_{\mathbf{A}^n/\mathbf{F}_p,P}$ be the basis of derivations dual to $dt_1, \ldots, dt_n$. Choose $s \in A$ nonvanishing at P such that $s\partial_i$ extends to a global derivation $D_i : A \to A$ for $i = 1, 2, \ldots, m-1$. In some neighborhood V of P in $\mathbf{A}^n_{\mathbf{F}_p}$, $dt_1, \ldots, dt_n$ form a basis of $\Omega_{V/\mathbf{F}_p}$, and $dt_1, \ldots, dt_{m-1}$ form a basis of $\Omega_{U \cap V/\mathbf{F}_p}$, and $s \in \mathcal{O}(V)^*$. By compactness, we may pass to an open cover of X to assume $U \subseteq V$. If $H_f \cap X$ is not regular at a closed point $Q \in U$, then the image of f in $\mathfrak{m}_{U,Q}/\mathfrak{m}_{U,Q}^2$ must be zero, and it follows that $D_1 f, \ldots, D_{m-1} f, f$ all vanish at Q. The set of $f \in S_d$ such that there exists such a point in U can be bounded using the induction argument in the proof of Lemma 2.6.

It remains to bound the $f \in S_d$ such that $H_f \cap X$ is not regular at some closed point $P \in Y$. Since Y is reduced, and since the fibers of the coherent sheaf $\Omega \otimes \mathcal{O}_Y$ on Y all have dimension m, the sheaf is locally free by Exercise II.5.8(c) in [Har77]. By the same argument as in the preceding paragraph, we can pass to an open cover of X, and find $t_1, \ldots, t_n, s \in A$ such that $dt_1, \ldots, dt_n$ are a basis of the restriction of $\Omega_{\mathbf{A}^n/\mathbf{F}_p}$ to a neighborhood of Y in $\mathbf{A}^n_{\mathbf{F}_p}$, and $dt_1, \ldots, dt_m$ are an $\mathcal{O}_Y$-basis of $\Omega \otimes \mathcal{O}_Y$, and $s \in \mathcal{O}(Y)^*$ is such that if $\partial_1, \ldots, \partial_n$ is the dual basis to $dt_1, \ldots, dt_n$, then $s\partial_i$ extends to a derivation $D_i : A \to A$ for $i = 1, \ldots, m-1$. (We could also define D_i for $i = m$, but we already have enough.) We finish again by using the induction argument in the proof of Lemma 2.6. □

5.4. **Singular points of midsized residue characteristic.** While examining points of larger residue characteristic, we may delete the fibers above small primes of $\mathbf{Z}$. Hence in this section and the next, our lemmas will suppose that X is smooth over $\mathbf{Z}$.

Lemma 5.8 (Singularities of midsized characteristic)**.** *Assume Conjecture 5.2. Let X be an integral quasiprojective subscheme of $\mathbf{A}^n_{\mathbf{Z}}$ that dominates* $\operatorname{Spec} \mathbf{Z}$ *and is smooth over* $\mathbf{Z}$ *of* *relative dimension $m-1$. For $d, L, M \geq 1$, define*

$$\mathcal{Q}_{d,L<\cdot<M} := \{\, f \in S_d : \text{there exist } p \text{ satisfying } L < p < M \text{ and } P \in X_p \text{ such that } H_f \cap X \text{ is not regular of dimension } m-1 \text{ at } P \,\}.$$

Given $\epsilon > 0$, if d and L are sufficiently large, then $\overline{\mu}(\mathcal{Q}_{d,L<\cdot<M}) < \epsilon$.

Proof. If P is a closed point of degree at most $d/(m+1)$ over $\mathbf{F}_p$ where $L < p < M$, then the set of $f \in S_d$ such that $H_f \cap X$ is not regular of dimension $m-1$ at P has upper density $\#\kappa(P)^{-(m+1)}$, as in the argument for $\mathcal{Q}_{p,r}^{\text{medium}}$ in Lemma 5.7. The sum over $\#\kappa(P)^{-(m+1)}$ over all such P is small if L is sufficiently large: this follows from [LW54], as usual. By Conjecture 5.2, the upper density of the set of $f \in S_d$ such that there exists p with $L < p < M$ such that $\dim(H_f \cap X_p)_{\text{sing}} \geq 1$ is bounded by $\sum_{L<p<M} c/p^2$, which again is small if L is sufficiently large.

Let $\mathcal{E}_{d,p}$ be the set of $f \in S_d$ for which $(H_f \cap X_p)_{\text{sing}}$ is finite and $H_f \cap X$ fails to be regular of dimension $m-1$ at some closed point $P \in X_p$ of degree greater than $d/(m+1)$ over $\mathbf{F}_p$. It remains to show that if d and L are sufficiently large, $\sum_{L<p<M} \overline{\mu}(\mathcal{E}_{d,p})$ is small. Write $f = f_0 + pf_1$ where f_0 has coefficients in $\{0, 1, \ldots, p-1\}$. Once f_0 is fixed, $(H_f \cap X_p)_{\text{sing}}$ is determined, and in the case where it is finite, we let $P_1, \ldots, P_\ell$ be its closed points of degree greater than $d/(m+1)$ over $\mathbf{F}_p$. Now $H_f \cap X$ is not regular of dimension $m-1$ at P_i if and only if the image of f in $\mathcal{O}_{X,P_i}/\mathfrak{m}_{X,P_i}^2$ is zero; for fixed f_0, this is a condition only on the image of f_1 in $\mathcal{O}_{X_p,P_i}/\mathfrak{m}_{X_p,P_i}$. It follows from Lemma 2.5 that the fraction of f_1 for this holds is at most $p^{-\nu}$ where $\nu = d/(m+1)$. Thus $\overline{\mu}(\mathcal{E}_{d,p}) \leq \ell p^{-\nu}$. As usual, we may assume we have reduced to the case where $(H_f \cap X_p)_{\text{sing}}$ is cut out by $D_1 f, \ldots, D_{m-1} f, f$ for some derivations D_i, and hence by Bézout's Theorem, $\ell = O(d^m) = O(p^{\nu-2})$ as $d \to \infty$, so $\overline{\mu}(\mathcal{E}_{d,p}) = O(p^{-2})$. Hence $\sum_{L<p<M} \overline{\mu}(\mathcal{E}_{d,p})$ is small whenever d and L are large. ∎

The following lemma and its proof were suggested by the referee.

Lemma 5.9. *Conjecture 5.2 holds when the closure $\overline{X}_{\mathbf{Q}}$ of $X_{\mathbf{Q}}$ in $\mathbf{P}^n_{\mathbf{Q}}$ has at most isolated singularities.*

Proof. We use induction on n. Let $\overline{X}$ be the closure of X in $\mathbf{P}^n_{\mathbf{Z}}$. Since $\overline{X}_{\mathbf{Q}}$ has at most isolated singularities, a linear change of coordinates over $\mathbf{Q}$ makes $\overline{X}_{\mathbf{Q}} \cap \{x_0 = 0\}$ is smooth of dimension $r-1$. Since the statement of Conjecture 5.2 is unchanged by deleting fibers of $X \to \operatorname{Spec} \mathbf{Z}$ above small primes, we may assume that $\overline{X} \cap \{x_0 = 0\}$ is smooth over $\mathbf{Z}$ of relative dimension $r-1$. Next, we may enlarge X to assume that X is the smooth locus of $\overline{X} \to \operatorname{Spec} \mathbf{Z}$, since this only makes the desired conclusion harder to prove. The smooth $\mathbf{Z}$-scheme $\overline{X} \cap \{x_0 = 0\}$ is contained in the smooth locus X of the $\mathbf{Z}$-scheme $\overline{X}$, so $X \cap \{x_0 = 0\} = \overline{X} \cap \{x_0 = 0\}$.

If $f \in S_{d,p}$ is such that $\dim(H_f \cap X_p)_{\text{sing}} \geq 1$, then the closure of $(H_f \cap X_p)_{\text{sing}}$ intersects $\{x_0 = 0\}$. But $X \cap \{x_0 = 0\} = \overline{X} \cap \{x_0 = 0\}$, so $(H_f \cap X_p)_{\text{sing}}$ itself intersects $\{x_0 = 0\}$. Thus it suffices to prove

$$\frac{\#\{f \in S_{d,p} : (H_f \cap X_p)_{\text{sing}} \cap \{x_0 = 0\} \neq \emptyset\}}{\#S_{d,p}} < \frac{c}{p^2}.$$

For a closed point y of degree $\leq d/(r+1)$ of $X_p \cap \{x_0 = 0\}$, the probability that $y \in (H_f \cap X_p)_{\text{sing}}$ is $\#\kappa(y)^{-r-1}$ and the sum over such points is treated as in the proof of Lemma 5.8.

It remains to count $f \in S_{d,p}$ such that $H_f \cap X_p$ is singular at a closed point y of degree $> d/(r+1)$ of $X_p \cap \{x_0 = 0\}$. Note that $(H_f \cap X_p)_{\text{sing}} \cap \{x_0 = 0\}$ is contained in the subscheme $\Sigma_f := (H_f \cap X_p \cap \{x_0 = 0\})_{\text{sing}}$. By the inductive hypothesis applied to $X \cap \{x_0 = 0\}$, we may restrict the count to the f for which $H_f \cap X_p \cap \{x_0 = 0\}$ is of pure dimension $r-2$ and Σ_f is finite. Then by Bézout, $\#\Sigma_f = O(d^r)$, where the implied constant depends only on X. If we write $f = f_0 + f_1 x_0 + f_2 x_0^2 + \dots$ with $f_i \in \mathbf{F}_p[x_1, \dots, x_n]$, then Σ_f depends only on f_0. For fixed f_0 and $y \in \Sigma_f = \Sigma_{f_0}$, whether or not $y \in (H_f \cap X_p)_{\text{sing}}$ depends only on the "value" of f_1 at y (which is in $\Gamma(y, \mathcal{O}(d-1)|_y)$), and at most one value corresponds to a singularity. The $\mathbf{F}_p$-vector space of possible values of f_1 at y has dimension $\geq \min(\deg(y), d)$, so if we restrict to y of degree $> d/(r+1)$, the probability that $y \in (H_f \cap X_p)_{\text{sing}}$ is at most $p^{-d/(r+1)}$. Thus, for fixed f_0, the probability that $H_f \cap X_p$ is singular at some such y is $O(d^r p^{-d/(r+1)})$, which is $O(p^{-2})$ for d large enough. Finally, the implied constant is independent of f_0, so the overall probability is again $O(p^{-2})$. □

5.5. **Singular points of large residue characteristic.** We continue to identify homogeneous polynomials in $x_0, \dots, x_n$ with their dehomogenizations obtained by setting x_0, when needed to consider them as functions on $\mathbf{A}^n_{\mathbf{Z}} \subseteq \mathbf{P}^n_{\mathbf{Z}}$.

Lemma 5.10. *Let X be an integral quasiprojective subscheme of $\mathbf{A}^n_{\mathbf{Z}}$ that dominates* $\operatorname{Spec} \mathbf{Z}$ *and is smooth over $\mathbf{Z}$ of relative dimension $m-1$. Fix $d \geq 1$. Let $f \in \mathbf{Z}[c_0, \dots, c_N][x_0, \dots, x_n]$ be the generic homogeneous polynomial in $x_0, \dots, x_n$ of total degree d, having the indeterminates $c_0, \dots, c_N$ as coefficients (so $N+1$ is the number of homogeneous monomials in $x_0, \dots, x_n$ of total degree d). Then there exists an integer $M > 0$ and a squarefree polynomial $R(c_0, \dots, c_N) \in \mathbf{Z}[c_0, \dots, c_N]$ such that if $\bar{f}$ is obtained from f by specializing the coefficients c_i to integers γ_i, and if $H_{\bar{f}} \cap X$ fails to be regular at a closed point in the fiber X_p for some prime $p \geq M$, then p^2 divides the value $R(\gamma_0, \dots, \gamma_N)$.*

Proof. By using a "d-uple embedding" of X (i.e., mapping $\mathbf{A}^n$ to $\mathbf{A}^N$ using all homogeneous monomials in $x_0, \dots, x_n$ of total degree d), we reduce to the case of intersecting X instead with an affine hyperplane $H_f \subset \mathbf{A}^n_{\mathbf{Z}}$ defined by (the dehomogenization of) $f = c_0 x_0 + \dots + c_n x_n$. Let $\mathbf{A}^{n+1} = \mathbf{A}^{n+1}_{\mathbf{Z}}$ be the affine space whose points correspond to such homogeneous linear forms. Thus $c_0, \dots, c_n$ are the coordinates on $\mathbf{A}^{n+1}$.

If X has relative dimension n over $\operatorname{Spec} \mathbf{Z}$ (so X is a nonempty open subset of $\mathbf{A}^n$), we may trivially take $R = c_0$ if $n = 0$ and $R = c_0 c_1$ if $n > 0$. Therefore we assume that the relative dimension is strictly less than n in what follows.

Let $\Sigma \subseteq X \times \mathbf{A}^{n+1}$ be the reduced closed subscheme of points (x, f) such that the variety $H_f \cap X$ over the residue field of (x, f) is not smooth of dimension $m-2$ at x. Then, because we have excluded the degenerate case of the previous paragraph, $\Sigma_{\mathbf{Q}}$ is the closure in $X_{\mathbf{Q}} \times \mathbf{A}^{n+1}_{\mathbf{Q}}$ of the inverse image under $X_{\mathbf{Q}} \times \mathbf{A}^{n+1}_{\mathbf{Q}} \dashrightarrow X_{\mathbf{Q}} \times \mathbf{P}^n_{\mathbf{Q}}$ of the *conormal variety* $CX \subseteq X_{\mathbf{Q}} \times \mathbf{P}^n_{\mathbf{Q}}$ as defined in [Kle86, I-2] (under slightly different hypotheses). Concretely, Σ is the subscheme of $X \times \mathbf{A}^{n+1}$ locally cut out by the equations $D_1 f = \cdots D_{m-1} f = f = 0$ where the D_i are defined locally on X as in the penultimate paragraph of the proof of Lemma 5.7.

Let I be the scheme-theoretic image of Σ under the projection $\pi : \Sigma \to \mathbf{A}^{n+1}$. Thus $I_{\mathbf{Q}} \subseteq \mathbf{A}^{n+1}_{\mathbf{Q}}$ is the cone over the *dual variety* $\check{X}$, defined as the scheme-theoretic image of the corresponding projection $CX \to \mathbf{P}^n_{\mathbf{Q}}$. By [Kle86, p. 168], we have $\dim CX = n-1$, so $\dim \check{X} \leq n-1$.

Case 1. $\dim \check{X} = n-1$.

Then $I_{\mathbf{Q}}$ is an integral hypersurface in $\mathbf{A}^n_{\mathbf{Q}}$, say given by the equation $R_0(c_0, \ldots, c_n) = 0$, where R_0 is an irreducible polynomial with content 1. After inverting a finite number of nonzero primes of $\mathbf{Z}$, we may assume that $R_0 = 0$ is also the equation defining I in $\mathbf{A}^n_{\mathbf{Z}}$. Choose M greater than all the inverted primes.

Since $\dim \check{X} = n-1$, the projection $C\check{X} \to \check{X}$ is a birational morphism. By duality (see the Monge-Segre-Wallace criterion on p. 169 of [Kle86]), $CX = C\check{X}$, so $CX \to \check{X}$ is a birational map. It follows that $\pi : \Sigma \to I$ is a birational morphism. Thus we may choose an open dense subset I' of I such that the birational morphism $\pi : \Sigma \to I$ induces an isomorphism $\Sigma' \to I'$, where $\Sigma' = \pi^{-1}(I')$. By Hilbert's Nullstellensatz, there exists $R_1 \in \mathbf{Z}[c_0, \ldots, c_n]$ such that R_1 vanishes on the closed subset $I - I'$ but not on I. We may assume that R_1 is squarefree. Define $R = R_0 R_1$. Then R is squarefree.

Suppose that $H_{\bar{f}} \cap X$ fails to be regular at a point $P \in X_p$ with $p \geq M$. Let γ be the closed point of $\mathbf{A}^{n+1}$ defined by $c_0 - \gamma_0 = \cdots = c_n - \gamma_n = p = 0$. Then the point (P, γ) of $X \times \mathbf{A}^{n+1}$ is in Σ. Hence $\gamma \in I$, so $R_0(\gamma_0, \ldots, \gamma_n)$ is divisible by p. If $\gamma \in I - I'$, then $R_1(\gamma_0, \ldots, \gamma_n)$ is divisible by p as well, so $R(\gamma_0, \ldots, \gamma_n)$ is divisible by p^2, as desired.

Therefore we assume from now on that $\gamma \in I'$, so $(P, \gamma) \in \Sigma'$. Let W be the inverse image of I' under the closed immersion $\operatorname{Spec} \mathbf{Z} \to \mathbf{A}^{n+1}$ defined by the ideal $(c_0 - \gamma_0, \ldots, c_n - \gamma_n)$. Let V be the inverse image of Σ' under the morphism $X \hookrightarrow X \times \mathbf{A}^{n+1}$ induced by the previous closed immersion. Thus we have a cube in which the top, bottom, front, and back faces are cartesian:

$$\begin{tikzcd}
V \arrow[rr] \arrow[dr] \arrow[dd] & & \Sigma' \arrow[dr] \arrow[dd] & \\
& X \arrow[rr] \arrow[dd] & & X \times \mathbf{A}^{n+1} \arrow[dd] \\
W \arrow[rr] \arrow[dr] & & I' \arrow[dr] & \\
& \operatorname{Spec} \mathbf{Z} \arrow[rr] & & \mathbf{A}^{n+1}
\end{tikzcd}$$

Near $(P, \gamma) \in X \times \mathbf{A}^{n+1}$ the functions $D_1 f, \cdots, D_{m-1} f, f$ cut out Σ (and hence also its open subset Σ') locally in $X \times \mathbf{A}^{n+1}$. Then $\mathcal{O}_{V,P} = \mathcal{O}_{X,P}/(D_1 \bar{f}, D_2 \bar{f}, \ldots, D_{m-1} \bar{f}, \bar{f})$. By assumption, $H_{\bar{f}} \cap X$ is not regular at P, so $\bar{f}$ maps to zero in $\mathcal{O}_{X,P}/\mathfrak{m}^2_{X,P}$. Now $\mathcal{O}_{X,P}$ is a regular local ring of dimension m, $D_i \bar{f} \in \mathfrak{m}_{X,P}$, and $\bar{f} \in \mathfrak{m}^2_{X,P}$, so the quotient $\mathcal{O}_{V,P}$ has length at least 2. Since $\Sigma' \to I'$ is an isomorphism, the cube shows that $V \to W$ is an isomorphism too. Hence the localization of W at p has length at least 2. On the other hand I' is an open subscheme of I, whose ideal is generated by $R_0(c_0, \ldots, c_n)$ (after some primes were inverted), so W is an open subscheme of $\mathbf{Z}/(R_0(\gamma_1, \ldots, \gamma_N))$. Thus $R_0(\gamma_0, \ldots, \gamma_n)$ is divisible by p^2 at least. Thus $R(\gamma_0, \ldots, \gamma_n)$ is divisible by p^2.

Case 2. $\dim \check{X} < n-1$.

Then $I_{\mathbf{Q}}$ is of codimension ≥ 2 in $\mathbf{A}^{n+1}_{\mathbf{Q}}$. Inverting finitely many primes if necessary, we can find a pair of distinct irreducible polynomials $R_1, R_2 \in \mathbf{Z}[c_0, \ldots, c_n]$ vanishing on I. Let $R = R_1 R_2$. As in Case 1, if $H_{\bar{f}} \cap X$ fails to be regular at $P \in X_p$ with $p \geq M$, then the values of R_1 and R_2 both vanish modulo p, so the value of R is divisible by p^2. $\square$

Because of Lemma 5.10, we would like to know that most values of a multivariable polynomial over $\mathbf{Z}$ are almost squarefree (that is, squarefree except for prime factors less than M). It is here that we need to assume the *abc* conjecture.

Theorem 5.11 (Almost squarefree values of polynomials)**.** *Assume the abc conjecture. Let $F \in \mathbf{Z}[x_1, \ldots, x_n]$ be squarefree. For $M > 0$, define*

$$\mathcal{S}_M := \{\, (a_1, \ldots, a_n) \in \mathbf{Z}^n \mid F(a_1, \ldots, a_n) \text{ is divisible by } p^2 \text{ for some prime } p \geq M \,\}.$$

Then $\overline{\mu}(\mathcal{S}_M) \to 0$ as $M \to \infty$.

Proof. The $n = 1$ case is in [Gra98]. The general case follows from Lemma 6.2 of [Poo03], in the same way that Corollary 3.3 there follows from Theorem 3.2 there. Lemma 6.2 there is proved there by reduction to the $n = 1$ case. $\square$

Remarks.

(1) These results assume the *abc* conjecture, but the special case where F factors into one-variable polynomials of degree ≤ 3 is known unconditionally [Hoo67]. Other unconditional results are contained in [GM91].
(2) Theorem 5.11 together with a simple sieve lets one show that the naive heuristic (multiplying probabilities for each prime p) correctly predicts the density of $(a_1, \ldots, a_n) \in \mathbf{Z}^n$ for which $F(a_1, \ldots, a_n)$ is squarefree, assuming the *abc* conjecture.

Lemma 5.12 (Singularities of large characteristic)**.** *Assume the abc conjecture. Let X be an integral quasiprojective subscheme of $\mathbf{A}^n_{\mathbf{Z}}$ that dominates* $\operatorname{Spec} \mathbf{Z}$ *and is smooth over* $\mathbf{Z}$ *of relative dimension $m - 1$. Define*

$$\mathcal{Q}_{d,\geq M} := \{\, f \in S_d : \text{there exists } p \geq M \text{ and } P \in X_p \text{ such that } H_f \cap X \text{ is not regular of dimension } m-1 \text{ at } P \,\}.$$

If d is sufficiently large, then $\lim_{M\to\infty} \overline{\mu}(\mathcal{Q}_{d,\geq M}) = 0$.

Proof. We may assume that d is large enough for Lemma 5.10. Apply Theorem 5.11 to the squarefree polynomial R provided by Lemma 5.10 for X. $\square$

5.6. **End of proof.** We are now ready to prove Theorem 5.1. Recall that in Section 5.2 we reduced to the problem of proving Lemma 5.6 in the case where X is an integral quasiprojective subscheme of $\mathbf{A}^n_{\mathbf{Z}}$ such that X dominates $\operatorname{Spec} \mathbf{Z}$ and is regular of dimension $m \geq 0$. In Lemma 5.6, d tends to infinity for each fixed r, and then r tends to infinity. We choose L depending on r, and M depending on r and d, such that $1 \ll L \ll r \ll d \ll M$. (The precise requirement implied by each $\ll$ is whatever is needed below for the applications of the lemmas below.) Then

$$\mathcal{Q}_r^{\text{large}} \cap S_d \subseteq \left(\bigcup_{p \leq L} (\mathcal{Q}_{p,r} \cap S_d) \right) \cup \mathcal{Q}_{d, L < \cdot < M} \cup \mathcal{Q}_{d,\geq M}, \tag{1}$$

and we will bound the upper density of each term on the right. Recall from the end of Section 5.2 that X has a subscheme of the form $X' = X \times \operatorname{Spec} \mathbf{Z}[1/t]$ that is smooth over $\mathbf{Z}$. We may assume $L > t$. By Lemma 5.7, $\lim_{r\to\infty} \overline{\mu}(\mathcal{Q}_{p,r}) = 0$ for each p, so $\overline{\mu}\left(\bigcup_{p\leq L} \mathcal{Q}_{p,r}\right)$ is small (by which we mean tending to zero) if r sufficiently large relative to L. By Lemma 5.8 applied to X', if L and d are sufficiently large, then $\overline{\mu}(\mathcal{Q}_{d,L<\cdot<M})$ is small. By Lemma 5.12 applied to X', if d is sufficiently large, and M is sufficiently large relative to d, then $\overline{\mu}(\mathcal{Q}_{d,\geq M})$

is small. Thus by (1), $\overline{\mu}(\mathcal{Q}_r^{\mathrm{large}})$ is small whenever r is large and d is sufficiently large relative to r. This completes the proof of Lemma 5.6 and hence of Theorem 5.1. ☐

Remark. Arithmetic analogues of Theorems 1.2 and 1.3, and of many of the applications in Section 3 can be proved as well.

5.7. **Regular versus smooth.** One might ask what happens in Theorem 5.1 if we ask for $H_f \cap X$ to be not only regular, but also smooth over $\mathbf{Z}$. We now show unconditionally that this requirement is so strict, that at most a density zero subset of polynomials f satisfies it, even if the original scheme X is smooth over $\mathbf{Z}$.

Theorem 5.13. *Let X be a nonempty quasiprojective subscheme of $\mathbf{P}^n_{\mathbf{Z}}$ that is smooth of relative dimension $m \geq 0$ over $\mathbf{Z}$. Define*

$$\mathcal{P}^{\mathrm{smooth}} := \{\, f \in S_{\mathrm{homog}} : H_f \cap X \textit{ is smooth of relative dimension } m-1 \textit{ over } \mathbf{Z}\,\}.$$

Then $\mu(\mathcal{P}^{\mathrm{smooth}}) = 0$.

Proof. Let

$$\mathcal{P}_r^{\mathrm{smooth}} := \{\, f \in S_{\mathrm{homog}} : H_f \cap X \text{ is smooth of relative dimension } m-1 \text{ over } \mathbf{Z} \text{ at all } P \in X_{<r}\,\}.$$

Suppose $P \in X_{<r}$ lies above the prime $(p) \in \operatorname{Spec} \mathbf{Z}$. Let Y be the closed subscheme of X_p corresponding to the ideal sheaf $\mathfrak{m}^2$ where $\mathfrak{m}$ is the ideal sheaf of functions on X_p vanishing at P. Then for $f \in S_d$, $H_f \cap X$ is smooth of relative dimension $m-1$ over $\mathbf{Z}$ at P if and only if the image of f in $H^0(Y, \mathcal{O}(d))$ is nonzero. Applying Lemma 5.3 to the union of such Y over all $P \in X_{<r}$, and using $\#H^0(Y, \mathcal{O}(d)) = \#\kappa(P)^{m+1}$, we find

$$\mu(\mathcal{P}_r^{\mathrm{smooth}}) = \prod_{P \in X_{<r}} \left(1 - \#\kappa(P)^{-(m+1)}\right).$$

Since $\dim X = m+1$, $\zeta_X(s)$ has a pole at $s = m+1$ and our product diverges to 0 as $r \to \infty$. (See Theorems 1 and 3(a) in [Ser65].) But $\mathcal{P}^{\mathrm{smooth}} \subseteq \mathcal{P}_r^{\mathrm{smooth}}$ for all r, so $\mu(\mathcal{P}^{\mathrm{smooth}}) = 0$. ☐

A density zero subset of S_{homog} can still be nonempty or even infinite. For example, if $X = \operatorname{Spec} \mathbf{Z}[1/2, x] \hookrightarrow \mathbf{P}^1_{\mathbf{Z}}$, then $\mathcal{P}^{\mathrm{smooth}} \cap S_d$ is infinite for infinitely many d: $H_f \cap X$ is smooth over $\mathbf{Z}$ whenever f is the homogenization of $(x-a)^{2^b} - 2$ for some $a, b \in \mathbf{Z}$ with $b \geq 0$.

On the other hand, N. Fakhruddin has given the following two examples in which $\mathcal{P}^{\mathrm{smooth}} \cap S_d$ is empty for all $d > 0$.

Example 5.14. Let X be the image of the 4-uple embedding $\mathbf{P}^1_{\mathbf{Z}} \to \mathbf{P}^4_{\mathbf{Z}}$. Then X is smooth over $\mathbf{Z}$. If $f \in \mathcal{P}^{\mathrm{smooth}} \cap S_d$ for some $d > 0$, then $H_f \cap X \simeq \coprod \operatorname{Spec} A_i$ where each A_i is the ring of integers of a number field K_i unramified above all finite primes of $\mathbf{Z}$, such that $\sum [K_i : \mathbf{Q}] = 4d$. The only absolutely unramified number field is $\mathbf{Q}$, so each A_i is $\mathbf{Z}$, and $H_f \cap X \simeq \coprod_{i=1}^{4d} \operatorname{Spec} \mathbf{Z}$. Then $4d = \#(H_f \cap X)(\mathbf{F}_2) \leq \#X(\mathbf{F}_2) = \#\mathbf{P}^1(\mathbf{F}_2) = 3$, a contradiction.

Example 5.15. Let X be the image of the 3-uple embedding $\mathbf{P}^2_{\mathbf{Z}} \to \mathbf{P}^9_{\mathbf{Z}}$. Then X is smooth over $\mathbf{Z}$. If $f \in \mathcal{P}^{\mathrm{smooth}} \cap S_d$ for some $d > 0$, then $H_f \cap X$ is isomorphic to a smooth proper geometrically connected curve in $\mathbf{P}^2_{\mathbf{Z}}$ of degree $3d$, hence of genus at least 1, so its Jacobian contradicts the main theorem of [Fon85].

Despite these counterexamples, P. Autissier has proved a positive result for a slightly different problem. An *arithmetic variety* of dimension m is an integral scheme X of dimension m that is projective and flat over $\mathbf{Z}$, such that $X_{\mathbf{Q}}$ is regular (of dimension $m-1$). If $\mathcal{O}_K$ is the ring of integers of a finite extension K of $\mathbf{Q}$, then an *arithmetic variety over* $\mathcal{O}_K$ is an $\mathcal{O}_K$-scheme X such that X is an arithmetic variety and whose generic fiber X_K is geometrically irreducible over K. The following is a part of Théorème 3.2.3 of [Aut01]:

> Let X be an arithmetic variety over $\mathcal{O}_K$ of dimension $m \geq 3$. Then there exists a finite extension L of K and a closed subscheme X' of $X_{\mathcal{O}_L}$ such that
> (1) The subscheme X' is an arithmetic variety over $\mathcal{O}_L$ of dimension $m-1$.
> (2) Whenever the fiber $X_{\mathfrak{p}}$ of X above $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ is smooth, the fiber $X'_{\mathfrak{p}'}$ of X' above $\mathfrak{p}'$ is smooth for all $\mathfrak{p}' \in \operatorname{Spec} \mathcal{O}_L$ lying above $\mathfrak{p}$.

Actually Autissier proves more, that one can also control the height of X'. (He uses the theory of heights developed by Bost, Gillet, and Soulé, generalizing Arakelov's theory.)

The most significant difference between Autissier's result and the phenomenon exhibited by Fakhruddin's examples is the finite extension of the base allowed in the former.

Acknowledgements

I thank Ernie Croot for a conversation at an early stage of this research (in 2000), David Eisenbud for conversations about Section 5.5, and Matt Baker, Brian Conrad, and Najmuddin Fakhruddin for some other comments. I thank Pascal Autissier and Ofer Gabber for sharing their (now published) preprints with me, and Jean-Pierre Jouanolou for sharing some unpublished notes about resultants and discriminants. Finally, I thank the referee for an extremely helpful report, which included among other things the statement and proof of Lemma 5.9.

References

[Aut01] Pascal Autissier, *Points entiers et théorèmes de Bertini arithmétiques*, Ann. Inst. Fourier (Grenoble) **51** (2001), no. 6, 1507–1523.

[Aut02] Pascal Autissier, *Corrigendum: "Integer points and arithmetical Bertini theorems" (French)*, Ann. Inst. Fourier (Grenoble) **52** (2002), no. 1, 303–304.

[Dwo60] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[EGA IV(4)] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 32, 361.

[Fon85] Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* **Z**, Invent. Math. **81** (1985), no. 3, 515–538.

[Ful84] William Fulton, *Introduction to intersection theory in algebraic geometry*, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1984.

[Gab01] O. Gabber, *On space filling curves and Albanese varieties*, Geom. Funct. Anal. **11** (2001), no. 6, 1192–1200.

[GM91] Fernando Gouvêa and Barry Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), no. 1, 1–23.

[Gra98] Andrew Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices (1998), no. 19, 991–1009.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hoo67] C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21–26.

[Kat99] Nicholas M. Katz, *Space filling curves over finite fields*, Math. Res. Lett. **6** (1999), no. 5-6, 613–624.

[Kat01] Nicholas M. Katz, *Corrections to: Space filling curves over finite fields*, Math. Res. Lett. **8** (2001), no. 5-6, 689–691.

[Kle86] Steven L. Kleiman, *Tangency and duality*, Proceedings of the 1984 Vancouver conference in algebraic geometry (Providence, RI), CMS Conf. Proc., vol. 6, Amer. Math. Soc., 1986, pp. 163–225.

[KS99] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society, Providence, RI, 1999.

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

[Poo00] Bjorn Poonen, *Varieties without extra automorphisms III: hypersurfaces*, preprint, 2 May 2000.

[Poo03] Bjorn Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J. **118** (2003), no. 2, 353–373.

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149.

[Ser65] Jean-Pierre Serre, *Zeta and L functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 82–92.

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu