POLYNOMIAL EQUATIONS MODULO PRIME NUMBERS

ARNAUD BODIN, PIERRE DÈBES, AND SALAH NAJIB

ABSTRACT. We consider polynomial equations, or systems of polynomial equations, with integer coefficients, modulo prime numbers p. We offer an elementary approach based on a counting method. The outcome is a weak form of the Lang-Weil lower bound for the number of solutions modulo p, only differing from Lang-Weil by an asymptotic p^{ε} multiplicative factor. Our second contribution is a reduction lemma to the case of a single equation which we use to extend our results to systems of equations. We show further how to use this reduction to prove the full Lang-Weil estimate for varieties, assuming it for hypersurfaces, in a version using a variant of the classical degree in the error term.

1. INTRODUCTION AND MAIN RESULTS

Let $F(x_1, \dots, x_r)$ be a nonconstant polynomial in one or several variables and with integer coefficients. For which prime numbers p the equation:

$$F(x_1, \dots, x_r) = 0 \bmod p$$

has integer solutions? and for such primes p, what is the size of the set of solutions? These are the questions that we consider, for such an equation, and more generally for a system of several such polynomial equations. In geometric terms, the problem is to count the number of rational points over finite fields $\mathbb{F}_p$ on the zero set $Z(F \bmod p)$, or, for a system, on the zero set of an ideal generated by several polynomials, regarded modulo p. A classical and deep achievement in this perspective is the

Lang-Weil estimate [10]. *Given nonnegative integers d, r, h, there is a positive constant $A(r,h)$ such that for every finite field $\mathbb{F}_q$ of cardinality $q = p^{\beta}$ with p prime and $\beta \geqslant 1$, and every prime ideal $I \subset \mathbb{F}_q[x_1, \dots, x_r]$ such that the affine variety $V = Z(I) \subset \mathbb{A}^r$ is geometrically irreducible*[1]*, of dimension* $\dim(V) = d$ *and of degree* $\deg(V) = h$*, we have:*

$$|\operatorname{card}(V(\mathbb{F}_q)) - q^d| \leqslant (h-1)(h-2)\, q^{d-\frac{1}{2}} + A(r,h)\, q^{d-1}. \tag{1}$$

Here $\dim(V)$ is the dimension of V and $\deg(V)$ is its degree, i.e. the number of intersection points of V with $\dim(V)$ hyperplanes in general position. For a single equation $F(x_1, \dots, x_r) = 0$, i.e. when V is a hypersurface, $\dim(V) = r-1$ and $\deg(V) = \deg(F)$.

We offer two main contributions to this topic with some applications.

Assume $F \in \mathbb{Z}[x_1, \dots, x_r]$ is nonconstant (but not necessarily irreducible). For every prime number p, denote by $c_p(F)$ the number of points $\underline{\omega} \in \mathbb{F}_p^r$ such that $(F \bmod p)(\underline{\omega}) = 0 \bmod p$. We will use the following bounds for $c_p(F)$ as landmarks.

Date: August 8, 2022.

2020 *Mathematics Subject Classification.* Primary 11D45, 11T06; Sec. 11D79, 11L20, 14G15.

Key words and phrases. polynomial equations, reduction modulo a prime, Lang-Weil inequalities.

Acknowledgment. This work was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01) and by the ANR project "LISA" (ANR-17-CE40–0023-01). The first author thanks the University of Vienna for his visit at the Wolfgang Pauli Institute.

[1] i.e. irreducible after scalar extension to $\overline{\mathbb{F}_q}$.

An upper bound is easily provided by the Zippel-Schwartz lemma, which is a several variable generalization of the fact that over a field, a one variable nonzero polynomial has no more roots than its degree; see Section 2.1 for a reminder.

Zippel-Schwartz upper bound. *For all primes p we have $c_p(F) \leqslant \deg(F)\, p^{r-1}$.*

This upper bound will be sufficient for our purposes. For other variants, we refer to [8] and [14].

Finding a lower bound is a deeper issue. Recall that it is not even clear a priori that $c_p(F) \neq 0$ for infinitely many p – this is a theorem of Schur [12] – and that it may well happen that $c_p(F) = 0$ for infinitely many p [2]: take $F = x^2y^2 + 1$. As detailed in Section 2.5, the *Lang-Weil estimate* (as stated above) leads to the following:

Lang-Weil lower bound. Assume $F \in \mathbb{Z}[x_1, \dots, x_r]$ is nonconstant. *For every $\varepsilon > 0$, there exist infinitely many primes p such that*

$$c_p(F) \geqslant (1-\varepsilon)\, p^{r-1}.$$

A *first contribution* of this paper is an elementary approach to the lower bound issue, which leads to the following weak but still meaningful form of the *Lang-Weil lower bound*, in the arbitrary dimension context. We start below with the case of hypersurfaces before giving the result in the general case of systems (Corollary 1.4).

Denote the set of prime numbers by $\mathcal{P}$.

Theorem 1.1. *Assume $F \in \mathbb{Z}[x_1, \dots, x_r]$ is nonconstant. Then the series $\sum_{p \in \mathcal{P}} \frac{c_p(F)}{p^r}$ is divergent. Consequently, for every $\varepsilon > 0$, we have:*

$$c_p(F) \geqslant p^{r-1-\varepsilon}.$$

for infinitely many $p \in \mathcal{P}$.

From the *Zippel-Schwartz upper bound*, the series $\sum_{p \in \mathcal{P}} c_p(F)/p^{r+\varepsilon}$ is convergent (for every $\varepsilon > 0$). Thus r is the largest exponent for which the series $\sum_{p \in \mathcal{P}} c_p(F)/p^r$ is divergent.

Our approach to Theorem 1.1 rests on combinatoric and analytic considerations going back to a method of Ekedahl [5] and Poonen [11] (already used in [1]), and on the Zippel-Schwartz lemma. Though weaker than the *Lang-Weil lower bound*, the more elementarily obtained Theorem 1.1 gives the right order of magnitude p^{r-1} for $c_p(F)$, up to a multiplicative factor $p^{-\varepsilon}$, for infinitely many $p \in \mathcal{P}$.

Remark 1.2. There is an abundant literature on the 1-dimensional case of the *Lang-Weil estimate*, which include refined bounds, elementary approaches, notably by Stepanov-Schmidt-Bombieri, Voloch, Heath-Brown, Corvaja-Zannier. We refer to the general texts [16, Chapter 6] and [15] for more on this topic and more references. Our bounds are valid in higher dimension but do not compete with these results in the curve case.

A *second contribution* of this paper is a reduction lemma to a single equation for a system of several polynomial equations, i.e. in geometric terms, from the case of a general affine variety to that of a hypersurface. The notation $c_p(I)$ used below for an ideal $I \subset \mathbb{Z}[x_1, \dots, x_r]$ generalizes $c_p(F)$: for every $p \in \mathcal{P}$, $c_p(I)$ is the number of points $\underline{\omega} \in \mathbb{F}_p^r$ such that $(P \bmod p)(\underline{\omega}) = 0 \bmod p$ for every $P \in I$; that is: $c_p(I) = \mathrm{card}(Z(I \bmod p)(\mathbb{F}_p))$ [3].

[2] but only in the case that F is reducible in $\overline{\mathbb{Q}}[x_1, \dots, x_r]$, as pointed out in Remark 2.5.

[3] that is: the cardinality of the set of $\mathbb{F}_p$-rational points on the Zariski-closed subset $Z(I \bmod p) \subset \mathbb{A}^r_{\mathbb{F}_p}$.

Lemma 1.3. *Let $I \subset \mathbb{Z}[x_1,\ldots,x_r]$ be a prime ideal such that $I \cap \mathbb{Z} = \{0\}$. Set $V = Z(I) \subset \mathbb{A}^r$ and $d = \dim(V)$. Then there is an irreducible polynomial $F \in \mathbb{Z}[T_1,\ldots,T_d,Y]$ and a constant B depending on I such that, for all primes p, we have:*

$$|c_p(I) - c_p(F)| \leqslant B\, p^{d-1}.$$

The classical approach to Lang-Weil goes by induction, on the dimension of V, using Chow varieties [10]. With Lemma 1.3 we can work instead with the number of defining equations of V, reducing to the case it is one, i.e. V is an hypersurface $H : F(\underline{t}, y) = 0 \subset \mathbb{A}^{d+1}$. Other approaches proceed as we do and construct hypersurfaces $H \subset \mathbb{A}^{d+1}$ from general affine varieties $V \subset \mathbb{A}^r$. But while these use generic linear projections $\mathbb{A}^r \to \mathbb{A}^{d+1}$ and try to optimize them to birationally map V to a good hypersurface H, we directly construct a specific hypersurface H that *locally represents* V, in the sense of Definition 3.1. Furthermore, our construction is performed over rings. See Lemmas 3.3–3.4, which rest on the Noether normalization lemma and the primitive element theorem and do not use Chow varieties.

We give *two applications*. The first one extends Theorem 1.1 to systems of equations.

Corollary 1.4. *Let $I \subset \mathbb{Z}[x_1,\ldots,x_r]$ be an ideal such that $I \cap \mathbb{Z} = \{0\}$ (not necessarily prime). Then the series $\sum_{p\in\mathcal{P}} \frac{c_p(I)}{p^{d+1}}$ is divergent.*

That is: Theorem 1.1 holds with $c_p(I)$ and $d+1$ replacing $c_p(F)$ and r. This first application includes further a generalization of the *Zippel-Schwartz upper bound* for $c_p(I)$ with $\deg(F)$ replaced by some constant M depending on I (Lemma 3.9(a)).

The second application is a proof, assuming the case of hypersurfaces, of the *Lang-Weil estimate* itself, with the following difference concerning the error term. Instead of the degree $\deg(V)$, we introduce the *hypersurface degree* $\mathrm{hdeg}(V)$ of a d-dimensional variety V as the smallest degree of some polynomial $F \in \mathbb{Q}[T_1,\ldots,T_d,Y]$ locally representing V as a hypersurface over $\mathbb{Z}[c^{-1}]$ for some nonzero $c \in \mathbb{Z}$ (Definition 3.6).

Using a more general form of Lemma 1.3 (namely Lemma 3.4), we prove the following statement, assuming the case of hypersurfaces (which is well-known; see e.g. [2]).

Corollary 1.5. *The* Lang-Weil estimate *holds with the condition* $\deg(V) = h$ *replaced by the condition* $\mathrm{hdeg}(V) = h$. [4]

If V is a hypersurface, then it follows from the definitions that $\mathrm{hdeg}(V) \leqslant \deg(V)$, but it is not clear to us how degree and hypersurface degree compare in general. The hypersurface degree seems however a more intrinsic notion than the usual degree (Remark 3.7).

Structure of the paper. Section 2 is devoted to the case of one polynomial equation. Theorem 1.1 is proved. Section 3 is concerned with the case of systems of polynomial equations: Lemma 3.4, which generalizes Lemma 1.3, is proved; then we deduce Corollary 1.4 and Corollary 1.5; a final illustration is given in Section 3.5.

2. One polynomial equation

This section is aimed at proving Theorem 1.1. The proof is divided into three stages which correspond to Sections §2.2–2.4. The preliminary Section 2.1 is a reminder on the Zippel-Schwartz lemma. Our proposed approach is elementary. As a comparison, we explain in the final Section 2.5 how to use the *Lang-Weil estimate*, first to obtain the *Lang-Weil lower bound*, and then in Remark 2.4, how to re-obtain Theorem 1.1.

[4] Corollary 1.5 is explicitly restated in Section 3, when it is proved.

2.1. **Zippel-Schwartz lemma.** This lemma is usually stated as a probability result; here we give a more arithmetic version of the statement and of the proof.

Theorem 2.1 (Zippel-Schwartz lemma). *Let $F(x_1,\dots,x_r)$ be a nonzero polynomial of degree d over a field K. Let S be a non-empty finite set of K. Then*

$$\operatorname{card}\{(a_1,\dots,a_r)\in S^r \mid F(a_1,\dots,a_r)=0\}\leqslant d\operatorname{card}(S)^{r-1}.$$

Applying this lemma with $K=\mathbb{Q}$ and $S=[\![0,p-1]\!]$ immediately yields the *Zippel-Schwartz upper bound* from Section 1.

Proof of Zippel-Schwartz lemma. The proof is by induction on the number r of variables. For $r=1$, the result is clear: a nonzero polynomial $F(x_1)$ of degree d has at most d roots in K. Suppose that the Zippel-Schwartz lemma is true for polynomials in $r-1$ variables. Let $F(x_1,\dots,x_r)$ be a nonzero polynomial of degree d. One may assume that the variable x_r actually appears in F and write F as a polynomial of degree $\delta\geqslant 1$ in this variable:

$$F(x_1,\dots,x_r)=f_\delta(x_1,\dots,x_{r-1})x_r^\delta+\dots+f_0(x_1,\dots,x_{r-1}).$$

Below we count the r-tuples $(a_1,\dots,a_r)\in S^r$ such that $F(a_1,\dots,a_r)=0$. Set $s=\operatorname{card}(S)$.

- If $f_\delta(a_1,\dots,a_{r-1})\neq 0$, then $F(a_1,\dots,a_{r-1},x_r)\in K[x_r]$ is a nonzero one variable polynomial of degree δ. There are at most s^{r-1} choices for $(a_1,\dots,a_{r-1})\in S^{r-1}$ and δ choices for a_r. Whence a subtotal of δs^{r-1} possibilities.
- If $f_\delta(a_1,\dots,a_{r-1})=0$, apply the induction hypothesis to the $r-1$-variable polynomial $f_\delta(x_1,\dots,x_{r-1})$, which is of degree $\leqslant d-\delta$. This yields at most $(d-\delta)s^{r-2}$ choices for $(a_1,\dots,a_{r-1})$ and s for a_r. Whence a subtotal of $(d-\delta)s^{r-1}$ possibilities.
- The sum of these two subtotals is the Zippel-Schwartz bound ds^{r-1}.

□

2.2. **A set of density** 0. The first stage of the proof of Theorem 1.1 is Lemma 2.2 below. Fix a nonconstant polynomial $F\in\mathbb{Z}[\underline{x}]$. For $p\in\mathcal{P}$, consider the sets:

$$\mathcal{Q}_p=\{\underline{x}\in\mathbb{Z}^r \mid F(\underline{x})=0 \bmod p\},$$
$$\mathcal{R}_p=\mathbb{Z}^r\setminus\mathcal{Q}_p=\{\underline{x}\in\mathbb{Z}^r \mid F(\underline{x})\neq 0 \bmod p\}`$$

We have:

$$c_p(F)=\operatorname{card}(\mathcal{Q}_p\cap[\![0,p-1]\!]^r).$$

Let $\mathcal{R}$ be the set of all $\underline{x}\in\mathbb{Z}^r$ such that no prime divides $F(\underline{x})$, that is:

$$\mathcal{R}=\bigcap_{p\in\mathcal{P}}\mathcal{R}_p=\{\underline{x}\in\mathbb{Z}^r \mid F(\underline{x})=\pm 1\}.$$

Recall that a *fixed prime divisor* of a polynomial $F(\underline{x})$ is a prime number q that divides $F(\underline{x})$ for all $\underline{x}\in\mathbb{Z}^r$. A nonzero polynomial has only finitely many fixed prime divisors (since they should all divide any nonzero value) and may have none.

Denote by $\mathcal{F}=\{q_1,\dots,q_m\}$ the set of fixed prime divisors of F. Let $\tilde{\mathcal{R}}$ be the the set of all $\underline{x}\in\mathbb{Z}^r$ such that $q_1,\dots,q_m$ are the only possible prime divisors of $F(\underline{x})$, that is:

$$\tilde{\mathcal{R}}=\bigcap_{p\in\mathcal{P}\setminus\mathcal{F}}\mathcal{R}_p$$

The *density* $\mu(\mathcal{S})$ of a subset $\mathcal{S}\subset\mathbb{Z}^r$ is defined as following limit, if it exists:

$$\mu(\mathcal{S})=\lim_{B\to+\infty}\frac{\operatorname{card}(\mathcal{S}\cap[\![0,B-1]\!]^r)}{B^r}.$$

Lemma 2.2. *We have $\mu(\mathcal{R}) = 0$ and $\mu(\tilde{\mathcal{R}}) = 0$.*

Proof. Density of $\mathcal{R}$. Denote by d the degree of $F(\underline{x})$. By the Zippel-Schwartz lemma applied to $(F(\underline{x}) = 1)$, we have:

$$\frac{\operatorname{card}(F(\underline{x}) = 1) \cap [\![0, B-1]\!]^r}{B^r} \leqslant \frac{d}{B} \xrightarrow[B\to+\infty]{} 0.$$

The same is true for $(F(\underline{x}) = -1)$. Hence $\mu(\mathcal{R}) = 0$.

Density of $\tilde{\mathcal{R}}$. We show below that the intersection of $\tilde{\mathcal{R}}$ with $[\![0, B-1]\!]^r$ is contained in the union of a relatively small number of sets $(F(\underline{x}) = q_1^{\alpha_1} \cdots q_m^{\alpha_m})$.

- Upper bound of $|F(\underline{x})|$ on $[\![0, B-1]\!]^r$. Let $F(\underline{x}) = \sum_{\underline{i}} a_{\underline{i}} \underline{x}^{\underline{i}}$. Let $H = \max |a_{\underline{i}}|$ and $d = \deg(F)$. Then
$$|F(\underline{x})| \leqslant \sum_{\underline{i}} |a_{\underline{i}}||\underline{x}^{\underline{i}}| \leqslant \sum_{\underline{i}} HB^d \leqslant (d+1)^r HB^d.$$
- Upper bound for the exponents α_i. Let $\underline{x} \in \tilde{\mathcal{R}} \cap [\![0, B-1]\!]^r$ and $F(\underline{x}) = q_1^{\alpha_1} \cdots q_m^{\alpha_m}$. As $q_i \geqslant 2$ and $F(\underline{x}) \leqslant (d+1)^r HB^d$ then $2^{\alpha_i} \leqslant (d+1)^r HB^d$, whence, for each $i = 1, \ldots, m$:
$$\alpha_i \leqslant \ln_2\left((d+1)^r HB^d\right)$$
and so
$$\alpha_i \leqslant d \ln_2(B) + c$$
where c is a constant depending only on r, d and H.
- Upper bound for $\operatorname{card}(\tilde{\mathcal{R}} \cap [\![0, B-1]\!]^r)$. An element $\underline{x}$ in $\tilde{\mathcal{R}} \cap [\![0, B-1]\!]^r$ is a solution of an equation $(F(\underline{x}) = q_1^{\alpha_1} \cdots q_m^{\alpha_m})$. Each set has at most dB^{r-1} elements by the Zippel-Schwartz lemma, and there are at most $(d \ln_2(B) + c)^m$ such equations. Thus we have:
$$\frac{\operatorname{card}(\tilde{\mathcal{R}} \cap [\![0, B-1]\!]^r)}{B^r} \leqslant \frac{(d \ln_2(B) + c)^m d}{B} \xrightarrow[B\to+\infty]{} 0.$$
Hence $\mu(\tilde{\mathcal{R}}) = 0$.

□

2.3. **Second stage of the proof of Theorem 1.1.** We prove the density formula from Lemma 2.3 below, by adjusting a method going back to Ekedahl and Poonen [11], [5].
For $M \geqslant 0$, let $\tilde{\mathcal{R}}_{\leqslant M}$ be the set of all $\underline{x} \in \mathbb{Z}^r$ such that the only prime divisors of $F(\underline{x})$ are $> M$ or are in the set $\mathcal{F}$ of fixed prime divisors, that is:

$$\tilde{\mathcal{R}}_{\leqslant M} = \bigcap_{\substack{p \in \mathcal{P} \setminus \mathcal{F} \\ p \leqslant M}} \mathcal{R}_p.$$

We simply denote $c_p(F)$ by c_p.

Lemma 2.3. *We have:*

$$\mu(\tilde{\mathcal{R}}_{\leqslant M}) = \prod_{\substack{p \in \mathcal{P} \setminus \mathcal{F} \\ p \leqslant M}} \left(1 - \frac{c_p}{p^r}\right).$$

Proof. First we compute the density of $\mathcal{Q}_p$ and $\mathcal{R}_p$ for any fixed prime $p \in \mathcal{P}$. Note that p divides $F(x_1, \ldots, x_r)$ with $(x_1, \ldots, x_r) \in \mathbb{Z}^r$ if and only if p divides $F(x_1+k_1p, \ldots, x_r+k_rp)$ for any $(k_1, \ldots, k_r) \in \mathbb{Z}^r$. Hence $\mathcal{Q}_p$ is invariant by any translation of vector in $(p\mathbb{Z})^r$. Hence, as a function of B, the cardinality $\operatorname{card}(\mathcal{Q}_p \cap [\![0, B-1]\!]^r)$ is asymptotic to $c_p \cdot \left(\frac{B}{p}\right)^r$ as $B \to \infty$. Thus we obtain:

$$\mu(\mathcal{Q}_p) = \lim_{B\to+\infty} \frac{\operatorname{card}(\mathcal{Q}_p \cap [\![0, B-1]\!]^r)}{B^r} = \frac{c_p}{p^r} \qquad \text{and} \qquad \mu(\mathcal{R}_p) = 1 - \frac{c_p}{p^r}. \tag{2}$$

Note further that if p is a fixed prime divisor then $\mu(\mathcal{Q}_p) = 1$ and $\mu(\mathcal{R}_p) = 0$.

Next fix $M \geqslant 0$ and let $\{p_1, \ldots, p_\ell\} = (\mathcal{P} \setminus \mathcal{F}) \cap [\![0, M]\!]$ be the set of primes $\leqslant M$ that are not fixed prime divisors, and let N be the product of these primes. The Chinese Remainder Theorem gives an isomorphism from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z}$, which we extend to the dimension r by:

$$\underline{x} \in (\mathbb{Z}/N\mathbb{Z})^r \longmapsto (\underline{x_1}, \ldots, \underline{x_\ell}) \in (\mathbb{Z}/p_1\mathbb{Z})^r \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^r,$$

where $\underline{x_j}$ is $\underline{x}$ modulo p_j. We have the following equivalences:

$$\begin{aligned} & \underline{x} \in \tilde{\mathcal{R}}_{\leqslant M} \cap [\![0, N-1]\!]^r \\ \iff \quad & \forall j \in \{1, \ldots, \ell\} \qquad F(\underline{x}) \neq 0 \bmod p_j \\ \iff \quad & \forall j \in \{1, \ldots, \ell\} \qquad F(\underline{x_j}) \neq 0 \bmod p_j \\ \iff \quad & \forall j \in \{1, \ldots, \ell\} \quad \underline{x_j} \in \mathcal{R}_{p_j} \cap [\![0, p_j - 1]\!]^r. \end{aligned}$$

Recall that $\mathcal{R}_p = \mathbb{Z}^r \setminus \mathcal{Q}_p$ so that $\operatorname{card}(\mathcal{R}_p \cap [\![0, p-1]\!]^r) = p^r - c_p$. Whence:

$$\operatorname{card}(\tilde{\mathcal{R}}_{\leqslant M} \cap [\![0, N-1]\!]^r) = \prod_{j=1}^{\ell} (p_j^r - c_{p_j}).$$

This provides the announced density of $\tilde{\mathcal{R}}_{\leqslant M}$:

$$\mu(\tilde{\mathcal{R}}_{\leqslant M}) = \lim_{B\to+\infty} \frac{\operatorname{card}(\tilde{\mathcal{R}}_{\leqslant M} \cap [\![0, B-1]\!]^r)}{B^r} = \lim_{B\to+\infty} \frac{\left(\frac{B}{N}\right)^r \prod_{j=1}^{\ell} (p_j^r - c_{p_j})}{B^r} = \prod_{j=1}^{\ell} \left(1 - \frac{c_{p_j}}{p_j^r}\right).$$

□

2.4. **End of proof of Theorem 1.1.** Setting $\mathcal{Q}_{>M} = \bigcup_{p>M} \mathcal{Q}_p$ and using (2), we obtain:

$$\mu(\mathcal{Q}_{>M}) = \mu\left(\bigcup_{p>M} \mathcal{Q}_p\right) \leqslant \sum_{p>M} \mu(\mathcal{Q}_p) \leqslant \sum_{p>M} \frac{c_p}{p^r}.$$

By contradiction, assume that the series $\sum_{p\in\mathcal{P}} \frac{c_p}{p^r}$ converges. Then we deduce from the previous inequalities:

$$\mu(\mathcal{Q}_{>M}) \xrightarrow[M\to+\infty]{} 0 \tag{3}$$

On the one hand $\tilde{\mathcal{R}} \subset \tilde{\mathcal{R}}_{\leqslant M}$. On the other hand $\tilde{\mathcal{R}}_{\leqslant M} \setminus \tilde{\mathcal{R}} \subset \mathcal{Q}_{>M}$: indeed if $\underline{x} \in \tilde{\mathcal{R}}_{\leqslant M} \setminus \tilde{\mathcal{R}}$ then $F(\underline{x})$ has only prime divisors $> M$, so that $\underline{x} \in \mathcal{Q}_p$ for some $p > M$.
Consider the decomposition:

$$\tilde{\mathcal{R}}_{\leqslant M} = \tilde{\mathcal{R}} \cup (\tilde{\mathcal{R}}_{\leqslant M} \setminus \tilde{\mathcal{R}}) \subset \tilde{\mathcal{R}} \cup \mathcal{Q}_{>M}.$$

It yields the inequalities:

$$\mu(\tilde{\mathcal{R}}) \leqslant \mu(\tilde{\mathcal{R}}_{\leqslant M}) \leqslant \mu(\tilde{\mathcal{R}}) + \mu(\mathcal{Q}_{>M}).$$

As, by (3), $\mu(\mathcal{Q}_{>M}) \xrightarrow[M\to+\infty]{} 0$, we obtain

$$\mu(\tilde{\mathcal{R}}_{\leqslant M}) \xrightarrow[M\to+\infty]{} \mu(\tilde{\mathcal{R}}). \tag{4}$$

As $\mu(\tilde{\mathcal{R}}_{\leqslant M}) = \prod_{p\leqslant M, p\in\mathcal{P}\setminus\mathcal{F}} \left(1 - \frac{c_p}{p^r}\right)$ by Lemma 2.3, then

$$\mu(\tilde{\mathcal{R}}) = \prod_{p\in\mathcal{P}\setminus\mathcal{F}} \left(1 - \frac{c_p}{p^r}\right) > 0.$$

The density is indeed positive: the series $\sum_{p\in\mathcal{P}} \frac{c_p}{p^r}$ converges and any factor of this infinite product is nonzero because $c_p = p^r$ if and only if p is a fixed prime divisor (which is ruled out by $p \notin \mathcal{F}$). This gives a contradiction with $\mu(\tilde{\mathcal{R}}) = 0$ (Lemma 2.2).
The second part of Theorem 1.1 is an immediate consequence of the first one.

2.5. **The Lang-Weil approach.** As a comparison with our approach, we explain how to use the *Lang-Weil estimate* to deduce the *Lang-Weil lower bound* (both as stated in Section 1). The argument, in addition to the *Lang-Weil estimate*, uses the Chebotarev density theorem and the Ostrowski theorem; recall however that the resulting bound is better than that of Theorem 1.1. Remark 2.4 completes the argument to obtain the full Theorem 1.1, i.e. the divergence of the series $\sum_{p\in\mathcal{P}} c_p(F)/p^r$, but at the cost of using the Lagarias-Odlyzko effective form of the Chebotarev theorem.

Alternate proof of the Lang-Weil lower bound. Let $F \in \mathbb{Z}[\underline{x}]$ be a nonconstant polynomial in $r \geqslant 1$ variables. Let $P \in \overline{\mathbb{Q}}[\underline{x}]$ be an irreducible factor of F in the UFD $\overline{\mathbb{Q}}[\underline{x}]$. Let K be a number field containing all coefficients of P, and $\beta \in \mathcal{O}_K$, $\beta \neq 0$, such that $\tilde{P} = \beta P \in \mathcal{O}_K[\underline{x}]$ (with $\mathcal{O}_K$ the ring of integers of K). It follows from the Chebotarev density theorem that the set S_K of primes p that are totally split in K is of density $\gamma \geqslant 1/n_K!$, where $n_K = [K:\mathbb{Q}]$. In particular, S_K is infinite. Remove from S_K the finite set of primes p for which β is in a prime ideal $\mathfrak{p}$ of K above p. Denote the resulting set by S'_K. For every prime $p \in S'_K$, select a prime $\mathfrak{p}$ of K above p. By definition of S_K, we have $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$. By the Ostrowski theorem, for all but finitely many $p \in S'_K$, the reduced polynomial $(\tilde{P} \bmod \mathfrak{p}) \in \mathbb{F}_p[\underline{x}]$ is irreducible in $\overline{\mathbb{F}_p}[\underline{x}]$. Denote the set of those p by S''_K. For $p \in S''_K$, denote the number of r-tuples $\underline{\omega} \in \mathbb{F}_p^r$ such that $(\tilde{P} \bmod \mathfrak{p})(\underline{\omega}) = 0$ by $n_{\mathfrak{p}}(\tilde{P})$. By the *Lang-Weil estimate*, we have $n_{\mathfrak{p}}(\tilde{P}) = p^{r-1} + O(p^{r-3/2})$, and clearly we have $c_p(F) \geqslant n_{\mathfrak{p}}(\tilde{P})$. The *Lang-Weil lower bound* from Section 1 follows (for every $p \in S''_K$). □

Remark 2.4 (Alternate proof of Theorem 1.1). Being more precise on the Chebotarev theorem, the same argument leads to the stronger conclusion of Theorem 1.1 that the series $\sum_{p\in\mathcal{P}} c_p(F)/p^r$ diverges. Indeed, the smaller series $\sum_{p\in S''_K} n_{\mathfrak{p}}(\tilde{P})/p^r$ is of the same nature as $\sum_{p\in S''_K} 1/p$ (by the *Lang-Weil estimate*); and we claim that

$$\sum_{p\in S_K,\, p\leqslant n} \frac{1}{p} \sim \gamma \log\log(n) \qquad \text{when } n \to +\infty \tag{5}$$

Proof of the claim. We adjust an argument showing that the sum of inverse of primes $\leqslant n$ is asymptotic to $\log\log n$ when $n \to +\infty$. For every integer $n \geqslant 0$, denote by $\pi_K(n)$ the number of primes $p \leqslant n$ that are in S_K. From the Chebotarev theorem, the definition of the density and the prime number theorem, we have $\pi_K(n) \simeq \gamma n/\log n$ when $n \to +\infty$. From the effective form of Chebotarev proved by Lagarias-Odlyzko [9] (and improved in [13]), we have $\pi_K(n) = \frac{n}{\log n}\left(\gamma + O(\frac{1}{\log n})\right)$. Claim (5) is the outcome of these evaluations:

$$\begin{aligned}
\sum_{p\in S_K, p\leqslant n} \frac{1}{p} &= \sum_{k=1}^{n} \frac{\pi_K(k)-\pi_K(k-1)}{k} = \sum_{k=1}^{n} \frac{\pi_K(k)}{k} - \sum_{k=0}^{n-1} \frac{\pi_K(k)}{k+1} \\
&= \frac{\pi_K(n)}{n} + \sum_{k=1}^{n-1} \frac{\pi_K(k)}{k(k+1)} = \frac{\pi_K(n)}{n} + \sum_{k=1}^{n-1} \frac{\pi_K(k)}{k^2} - \sum_{k=1}^{n-1} \frac{\pi_K(k)}{k^2(k+1)} \\
&= \sum_{k=3}^{n-1} \frac{\pi_K(k)}{k^2} + O(1) = \sum_{k=3}^{n-1} \left[\frac{\gamma}{k\log k} + O\left(\frac{1}{k(\log k)^2}\right)\right] + O(1) \\
&= \gamma \log\log n + O(1)
\end{aligned}$$

where we bound $\sum_{k=3}^{n-1} \frac{1}{k\log k}$ by $\int_2^{n-1} \frac{\mathrm{d}x}{x\log x}$ and $\int_3^{n} \frac{\mathrm{d}x}{x\log x}$ in the last step. □

Remark 2.5. If $F \in \mathbb{Z}[\underline{x}]$ is irreducible in $\overline{\mathbb{Q}}[\underline{x}]$, then the *Lang-Weil estimate* gives that $c_p(F) > 0$ *for all but finitely many* $p \in \mathcal{P}$. Thus polynomials $F \in \mathbb{Z}[\underline{x}]$ like $F = x^2y^2 + 1$ for which $c_p(F) = 0$ for infinitely many $p \in \mathcal{P}$ are necessarily reducible in $\overline{\mathbb{Q}}[\underline{x}]$.

3. Systems of polynomial equations

This section is devoted to *systems* of polynomial equations. Our reduction to the situation of one equation is explained in Sections 3.1–3.2. The goal is Lemma 3.4, which generalizes Lemma 1.3 from Section 1. Its applications, Corollary 1.5 and Corollary 1.4, are then proved in Section 3.3 and Section 3.4. Section 3.5 is a final illustration.

3.1. Representing varieties as hypersurfaces.

Fix the following for the whole subsection and the next one. Let R be an integral domain and let K be its fraction field. Let $\underline{x} = (x_1, \dots, x_r)$ be an r-tuple of indeterminates with $r \geqslant 1$. Let $I \subset R[\underline{x}]$ be a prime ideal such that $I \cap R = \{0\}$; this condition guarantees that I remains prime and of the same height if base changed to K. Let $A = R[\underline{x}]/I$ be the quotient ring and $V = Z(I) \subset \mathbb{A}^r$ be the associated affine variety. Let L be the fraction field of A. Let $d = \dim(V) \geqslant 0$ be the dimension of V; it is also the Krull dimension of A and the transcendence degree of the extension L/K. Let $T_1, \dots, T_d, Y$ be $d+1$ new indeterminates and set $\underline{T} = (T_1, \dots, T_d)$.

Definition 3.1. A polynomial $F \in R[\underline{T}, Y]$, monic and separable in Y, irreducible in $K[\underline{T}, Y]$ and of degree $\delta = \deg_Y(F) \geqslant 1$, is said to *locally represent the affine variety V as a hypersurface over R* if there exist:

- a d-tuple $\underline{t} = (t_1, \dots, t_d) \in A^d$ and an element $\alpha \in A$ such that $F(\underline{t}, \alpha) = 0$, and
- a nonzero polynomial $\Delta \in R[\underline{t}]$ satisfying $\Delta(\underline{t}) \neq 0$,

such that:

(*) $A[\Delta(\underline{t})^{-1}]$ *is a* $R[\underline{t}, \Delta(\underline{t})^{-1}, \alpha]$*-module generated by finitely many purely inseparable elements over* $K(\underline{t}, \alpha)$.

Note that $L = \mathrm{Frac}(A[\Delta(\underline{t})^{-1}])$ is a finite extension of $K(\underline{t})$; both fields have transcendence degree d, which forces $t_1, \dots, t_d$ to be algebraically independent over K. In particular $\Delta(\underline{t}) \neq 0$ follows from $\Delta \neq 0$ and we can lighten the notation by writing Δ^{-1} for $\Delta(\underline{t})^{-1}$.

Remark 3.2 (about the phrase *"locally represented by a hypersurface"*). Instead of "*locally*", we say "*above the Zariski-open subset* $\mathbb{A}^d \setminus Z(\Delta)$" when we want to be more specific. Below we explain the geometric hypersurface representation idea behind Definition 3.1.
Assume that R is of characteristic 0. So there are no inseparables and (*) rewrites as

$$A[\Delta^{-1}] = R[\underline{t}, \Delta^{-1}, \alpha] = R[\underline{t}, \Delta^{-1}] + R[\underline{t}, \Delta^{-1}]\,\alpha + \cdots + R[\underline{t}, \Delta^{-1}]\,\alpha^{\delta-1}. \tag{6}$$

It follows next from F being irreducible in $K[\underline{T}, Y]$ and monic that F is irreducible in $R[\underline{T}, Y]$ and that $R[\underline{t}, \Delta^{-1}, \alpha]$ is isomorphic to the coordinate ring $R[\underline{T}, \Delta^{-1}][Y]/(F)$ of the hypersurface $Z(F) \subset \mathbb{A}^{d+1}$, above the open subset $\mathbb{A}^d \setminus Z(\Delta)$. Definition 3.1 geometrically means that

(**) *there is a finite morphism* $V \to \mathbb{A}^d$ (given by the inclusion $R[\underline{t}] \subset A$) *such that, above the open subset* $\mathbb{A}^d \setminus Z(\Delta)$*, the variety* V *is isomorphic to the* hypersurface $Z(F)$.

With no assumption on the characteristic of R, there is a finite purely inseparable morphism $V \to W$ such that W has property (**).

Lemma 3.3. *Assume that* R *is integrally closed. Then there exists* $c \in R$, $c \neq 0$, *such that the affine variety* $V \subset \mathbb{A}^r$ *can be locally represented as a hypersurface over the ring* $R[c^{-1}]$.

Lemma 3.3 can be viewed as an improved version, over rings, of the classical fact that every variety V over a field K of characteristic 0 is birational to a hypersurface.

Proof of Lemma 3.3. The R-algebra A being of finite type, the Noether normalization lemma (e.g. [4, Cor.13.18]) may be applied to provide:

- an element $c \in R$, $c \neq 0$,
- a d-tuple $\underline{t} = (t_1, \ldots, t_d)$ of elements of $R[c^{-1}]$, algebraically independent over K,
- m elements $\theta_1, \ldots, \theta_m \in A[c^{-1}]$ ($m \geqslant 1$),

such that:

$$A[c^{-1}] = R[c^{-1}][\underline{t}]\,\theta_1 + \cdots + R[c^{-1}][\underline{t}]\,\theta_m. \tag{7}$$

Consider the field extension:

$$L/K(\underline{t}) = K(\underline{t}, \theta_1, \ldots, \theta_m)/K(\underline{t}).$$

The ring $A[c^{-1}]$ being a $R[c^{-1}][\underline{t}]$-module of finite type, the elements $\theta_1, \ldots, \theta_m$ are integral over $R[c^{-1}][\underline{t}]$; in particular, the extension $L/K(\underline{t})$ is finite.
Let $p \geqslant 0$ be the characteristic of R. For each $i = 1, \ldots, m$, let p^{k_i} be the minimal exponent such that $\widetilde{\theta}_i = \theta_i^{p^{k_i}}$ is separable over $K(\underline{t})$, with the convention that $p^{k_i} = 1$ if $p = 0$. With

$$\widetilde{A} = R[\underline{t}, \widetilde{\theta}_1, \ldots, \widetilde{\theta}_m] \qquad \text{and} \qquad \widetilde{L} = K(\underline{t}, \widetilde{\theta}_1, \ldots, \widetilde{\theta}_m),$$

(***) *the ring* $A[c^{-1}]$ *is the* $\widetilde{A}[c^{-1}]$*-module generated by* $\theta_1, \ldots, \theta_m$*, which are purely inseparable over* $\widetilde{L}$.

The extension $\widetilde{L}/K(\underline{t})$ is separable, hence has a primitive element α which classically can be taken of the form:

$$\alpha = \sum_{i=1}^{m} \alpha_i \widetilde{\theta}_i$$

with $\alpha_1, \ldots, \alpha_m \in R[\underline{t}]$. Thus $\alpha \in \widetilde{A}[c^{-1}]$ and is integral over the subring $R[c^{-1}][\underline{t}]$. Let

- $F(\underline{t}, Y)$ be the (monic) irreducible polynomial of α over $K(\underline{t})$, and
- $\Delta(\underline{t})$ be the discriminant of the $K(\underline{t})$-basis of $\widetilde{L}$:

$$1, \alpha, \ldots, \alpha^{\delta-1} \qquad \text{with } \delta = [\widetilde{L} : K(\underline{t})] = \deg_Y(F).$$

As $R[c^{-1}][\underline{t}]$ is integrally closed (as a consequence of R being so), we classically have that $F(\underline{t},Y) \in R[c^{-1}][\underline{t},Y]$, that $\Delta(\underline{t}) \in R[c^{-1}][\underline{t}]$ and is nonzero, and that

$$\Delta(\underline{t})\,\widetilde{\theta}_i \in R[c^{-1}][\underline{t},\alpha] \qquad i=1,\dots,m. \tag{8}$$

Conclude that $\widetilde{A}[c^{-1}][\Delta^{-1}] = R[c^{-1}][\underline{t},\Delta^{-1},\alpha]$ and that $A[c^{-1}][\Delta^{-1}]$ is a $R[c^{-1}][\underline{t},\Delta^{-1},\alpha]$-module generated by m elements, purely inseparable over $\widetilde{L} = K(\underline{t},\alpha)$. Note finally that as $t_1,\dots,t_d$ are algebraically independent over K, the polynomial $F(\underline{t},Y) \in K[\underline{t},Y]$ determines a polynomial $F \in K[\underline{T},Y]$ which is irreducible in $K[\underline{T},Y]$, monic, separable and of degree δ in Y. □

3.2. **A key lemma.** Retain the notation from Section 3.1. Let $\mathbb{F}$ be a finite field. Given a ring morphism $\rho : R \to \mathbb{F}$ and a polynomial P with coefficients in R, denote by P^ρ the polynomial obtained from P by applying the morphism ρ to all coefficients of P. We use similar notation for ideals of $R[\underline{x}]$.
Denote by $c_\rho(I)$ the number of $\mathbb{F}$-rational points on the Zariski-closed subset $Z(I^\rho) \subset \overline{\mathbb{F}}^r$:

$$c_\rho(I) = \operatorname{card}\big\{\underline{\omega} \in \mathbb{F}^r \mid P^\rho(\underline{\omega}) = 0 \text{ for every } P \in I\big\}.$$

Suppose given a polynomial $F \in R[\underline{T},Y]$ locally representing V as a hypersurface over R. Retain the notation from Definition 3.1 regarding $\underline{t}$, α and Δ. Since $\underline{t} \in A^d$, there exist polynomials $\varphi_1,\dots,\varphi_d \in R[\underline{x}]$ such that:

$$t_i = \varphi_i \bmod I = \varphi_i(\underline{x} \bmod I) \qquad i=1,\dots,d.$$

Set $\underline{\varphi} = (\varphi_1,\dots,\varphi_d)$ and consider the polynomial $f = \Delta(\underline{\varphi}) \in R[\underline{x}]$. For later use, note the following, which already shows that $f \notin I$:

$$(f \bmod I) = f(\underline{x} \bmod I) = \Delta(\underline{\varphi})(\underline{x} \bmod I) = \Delta(\underline{\varphi}(\underline{x} \bmod I)) = \Delta(\underline{t}) \neq 0. \tag{9}$$

Lemma 3.4. *Assume that V is locally represented by a hypersurface over R and retain the notation above. Let $\mathbb{F}$ be a finite field and $\rho : R \to \mathbb{F}$ be a ring morphism. Assume that both f^ρ and Δ^ρ are nonzero in $\mathbb{F}[\underline{x}]$. Then we have the following inequality:*

$$-\deg_Y(F)\, c_\rho(\Delta) \leqslant c_\rho(I) - c_\rho(F) \leqslant c_\rho(\langle I, f\rangle). \tag{10}$$

Remark 3.5 (Special case $d=0$). When $\dim(V) = d = 0$, the extension L/K is algebraic, there are no transcendentals $t_1,\dots,t_d$ but the result still holds with $\{t_1,\dots,t_d\}$ replaced by the empty set. The elements Δ and f are in R and are nonzero (and so $c_\rho(\Delta) = c_\rho(f) = 0$). Under the assumption that f^ρ and Δ^ρ are nonzero in $\mathbb{F}[\underline{x}]$, conclusion (10) reads: $c_\rho(I) = c_\rho(F)$. It is established below as the special case $d=0$ of the proof.

Proof. The proof divides into two parts. We preliminarily explain the strategy, which may somewhat be hidden by the necessary details leading to the claimed inequalities.

Strategy. The numbers $c_\rho(I)$, $c_\rho(F)$ are the cardinalities of the sets $Z(I^\rho)(\mathbb{F})$, $Z(F^\rho)(\mathbb{F})$. These in turn can be seen as follows. There is on one hand a 1-1 correspondence

$$Z(I^\rho)(\mathbb{F}) \to \operatorname{Mor}_\rho(A,\mathbb{F})$$

between $Z(I^\rho)(\mathbb{F})$ and the set $\operatorname{Mor}_\rho(A,\mathbb{F})$ of ring morphisms from A to $\mathbb{F}$ extending ρ; and on the other hand, there is a 1-1 correspondence

$$Z(F^\rho)(\mathbb{F}) \to \operatorname{Mor}_\rho(R[\underline{T},Y]/(F),\mathbb{F}).$$

We will show that, *up to inverting* Δ, first we have $\operatorname{Mor}_\rho(A,\mathbb{F}) = \operatorname{Mor}_\rho(R[\underline{t},\alpha],\mathbb{F})$ (as a consequence of A being generated as $R[\underline{t},\alpha]$-module by finitely many inseparables) and, second, $R[\underline{t},\alpha] \simeq R[\underline{T},Y]/(F)$ (as noticed in Remark 3.2). This indeed yields "$c_\rho(I) =$

$c_\rho(F)$ up to *some bound*" coming from the inversion of Δ and which the proof below makes precise.

1st part. *We construct a map $\Psi : Z(I^\rho)(\mathbb{F}) \to Z(F^\rho)(\mathbb{F})$, show that a certain restriction of Ψ is injective and deduce the upper bound part of Lemma 3.4.*

Suppose given an element $\underline{\omega} = (\omega_1, \ldots, \omega_r) \in Z(I^\rho)(\mathbb{F})$. The morphism $\rho : R \to \mathbb{F}$ uniquely extends to a morphism $\rho : A \to \mathbb{F}$ such that $\rho(\underline{x} \bmod I) = \underline{\omega}$. Consider the $(d+1)$-tuple $(\rho(t_1), \ldots, \rho(t_d), \rho(\alpha))$, which is in $\mathbb{F}^{d+1}$. This calculation shows that it lies in $Z(F^\rho)$:

$$F^\rho(\rho(t_1), \ldots, \rho(t_d), \rho(\alpha)) = \rho(F(t_1, \ldots, t_d, \alpha)) = \rho(0) = 0.$$

Denote the tuple $(\rho(t_1), \ldots, \rho(t_d), \rho(\alpha))$ by $(\tau_1, \ldots, \tau_d, \xi) = (\underline{\tau}, \xi)$ and consider the map

$$\Psi : Z(I^\rho)(\mathbb{F}) \to Z(F^\rho)(\mathbb{F})$$

that sends every r-tuple $\underline{\omega} \in Z(I^\rho)(\mathbb{F})$ to the $(d+1)$-tuple $(\underline{\tau}, \xi) \in Z(F^\rho)(\mathbb{F})$.

Using (9), we obtain:

$$\rho(\Delta(\underline{t})) = \rho(f(\underline{x} \bmod I)) = f^\rho(\rho(\underline{x} \bmod I)) = f^\rho(\underline{\omega}).$$

Consider the following Zariski-closed subset of $Z(I^\rho)$:

$$Z(\langle I^\rho, f^\rho \rangle) = \{\underline{\omega} \in Z(I^\rho) \mid f^\rho(\underline{\omega}) = 0\}^5$$

and denote its complement in $Z(I^\rho)(\mathbb{F})$ by $Z(I^\rho)(\mathbb{F})_{f^\rho \neq 0}$.

We claim that: *the restriction of Ψ to $Z(I^\rho)(\mathbb{F})_{f^\rho \neq 0}$ is injective.*

Namely, let $\underline{\omega}, \underline{\omega}' \in Z(I^\rho)(\mathbb{F})_{f^\rho \neq 0}$. They determine two morphisms $\rho, \rho' : A \to \mathbb{F}$ extending $\rho : R \to \mathbb{F}$ and such that $\rho(\underline{x} \bmod I) = \underline{\omega}$ and $\rho'(\underline{x} \bmod I) = \underline{\omega}'$. Assume that $\Psi(\underline{\omega}) = \Psi(\underline{\omega}')$. This means that $(\rho(t_1), \ldots, \rho(t_d), \rho(\alpha)) = (\rho'(t_1), \ldots, \rho'(t_d), \rho'(\alpha))$. Since $\rho(\Delta(\underline{t})) = f^\rho(\underline{\omega}) \neq 0$ and $\rho'(\Delta(\underline{t})) = f^\rho(\underline{\omega}') \neq 0$, ρ and ρ' can be extended to and coincide on $R[\underline{t}, \Delta^{-1}, \alpha]$. In particular, they coincide on $A[\Delta^{-1}]$ if R is of characteristic 0.

Assume that R is of characteristic $p > 0$. If θ is one from a finite list of purely inseparable elements (over $K(\underline{t}, \alpha)$) that generate $A[\Delta^{-1}]$ as $R[\underline{t}, \Delta^{-1}, \alpha]$-module, we have that $\theta^{p^k} \in R[\underline{t}, \Delta^{-1}, \alpha]$ for some integer $k \geqslant 0$. It follows that $\rho(\theta^{p^k}) = \rho'(\theta^{p^k})$ and so that $\rho(\theta) = \rho'(\theta)$ (since taking the p-th power is injective on the finite field $\mathbb{F}$). Conclude that ρ and ρ' coincide on $A[\Delta^{-1}]$ in the positive characteristic case as well.

In particular, in both cases, $\underline{\omega} = \rho(\underline{x} \bmod I) = \rho'(\underline{x} \bmod I) = \underline{\omega}'$, thus proving the claim.

We have $c_\rho(I) = \mathrm{card}(Z(I^\rho)(\mathbb{F}))$ and, by definition,

$$Z(I^\rho)(\mathbb{F}) = Z(I^\rho)(\mathbb{F})_{f^\rho \neq 0} \,\cup\, Z(\langle I^\rho, f^\rho \rangle)(\mathbb{F}). \tag{11}$$

Regarding the first term in the union, the proven injectivity conclusion gives

$$\mathrm{card}(Z(I^\rho)(\mathbb{F})_{f^\rho \neq 0}) \leqslant \mathrm{card}(Z(F^\rho)(\mathbb{F})) = c_\rho(F). \tag{12}$$

Regarding the second term, we have:

$$\mathrm{card}(Z(\langle I^\rho, f^\rho \rangle)(\mathbb{F})) = c_\rho(\langle I, f \rangle).$$

whence the upper bound part of Lemma 3.4.

2nd part. *We construct an injective map Φ from a Zariski-open subset of $Z(F^\rho)(\mathbb{F})$ to $Z(I^\rho)(\mathbb{F})$ and deduce the lower bound part of Lemma 3.4.*

Consider a $(d+1)$-tuple $(\tau_1, \ldots, \tau_d, \xi) \in \mathbb{F}^{d+1}$ such that

$$F^\rho(\tau_1, \ldots, \tau_d, \xi) = 0 \tag{13}$$

[5] In the special case $d = 0$, we have $Z(\langle I^\rho, f^\rho \rangle) = \emptyset$.

and

$$\Delta^\rho(\tau_1,\dots,\tau_d) \neq 0 \tag{14}$$

The morphism $\rho : R \to \mathbb{F}$ uniquely extends to a morphism

$$R[\underline{T},Y]/(F) \to \mathbb{F}$$

sending $\underline{T}$ to $\underline{\tau} = (\tau_1,\dots,\tau_d)$ and Y to ξ. As $t_1,\dots,t_d$ are algebraically independent and that the polynomial $F(\underline{T},Y) \in R[\underline{T},Y]$ is irreducible in $K[\underline{T},Y]$ and monic in Y, there is an isomorphism between the rings $R[\underline{T},Y]/(F)$ and $R[\underline{t},\alpha]$, sending $(\underline{T},Y)$ to $(\underline{t},\alpha)$ and equal to the identity on R. Furthermore, such an isomorphism is unique. This shows that there is a unique morphism

$$\sigma : R[\underline{t},\alpha] \to \mathbb{F}$$

extending $\rho : R \to \mathbb{F}$ and sending $(\underline{t},\alpha)$ to $(\underline{\tau},\xi)$. Due to (14), this morphism can be extended to a morphism $\sigma : R[\underline{t},\Delta(\underline{t})^{-1},\alpha] \to \mathbb{F}$.

From Definition 3.1, there exist finitely many elements $\theta_1,\dots,\theta_m \in A[\Delta^{-1}]$, purely inseparable over $K(\underline{t},\alpha)$, that generate $A[\Delta^{-1}]$ as a $R[\underline{t},\Delta^{-1},\alpha]$-module. The morphism $\sigma : R[\underline{t},\Delta(\underline{t})^{-1},\alpha] \to \mathbb{F}$ can be extended to $R[\underline{t},\Delta(\underline{t})^{-1},\alpha][\theta_1,\dots,\theta_m] = A[\Delta^{-1}]$ by extending it first to $R[\underline{t},\Delta(\underline{t})^{-1},\alpha][\theta_1]$, then to $R[\underline{t},\Delta(\underline{t})^{-1},\alpha][\theta_1,\theta_2]$, etc., thanks to the following classical statement:

(*) *Let $f : D \to C$ be a ring morphism between a domain D and a field C. Let ζ be algebraic over* Frac(D). *Assume that the irreducible polynomial P_ζ of ζ over* Frac(D) *is in $D[Y]$. Then the correspondence $\widetilde{f} \to \widetilde{f}(\zeta)$ between the set of extensions of f to a morphism $\widetilde{f} : D[\zeta] \to C$ and the set of roots lying in C of the polynomial $(P_\zeta)^f$ is bijective.*

(Merely note that in our situation, for each $i = 1,\dots,m$, the irreducible polynomial of θ_i is of the form $Y^{p^k} - \beta$ with $\beta = \theta_i^{p^k} \in R[\underline{t},\Delta(\underline{t})^{-1},\alpha]$ and $k \geqslant 0$, and that the equation $y^{p^k} - \sigma(\beta) = 0$ has a unique solution in the finite field $\mathbb{F}$.)

Furthermore, the resulting morphism $\sigma : A[\Delta^{-1}] \to \mathbb{F}$ that extends $\rho : R \to \mathbb{F}$ and sends $(\underline{t},\alpha)$ to $(\underline{\tau},\xi)$ is unique.

Set $\sigma(x_i \bmod I) = \omega_i$, $i = 1,\dots,r$ and $\underline{\omega} = (\omega_1,\dots,\omega_r)$. The following calculation shows that $\underline{\omega} \in Z(I^\rho)$: for $P \in I^\rho$, we have:

$$\begin{aligned} P^\rho(\underline{\omega}) &= P^\rho(\sigma(\underline{x} \bmod I)) = \sigma(P(\underline{x} \bmod I)) \\ &= \sigma(P(\underline{x}) \bmod I) = \sigma(0 \bmod I) = 0 \end{aligned}$$

Denote by $Z(F^\rho)(\mathbb{F})_{\Delta^\sigma \neq 0}$ the subset of $\mathbb{F}^{d+1}$ defined by conditions (13), (14) and by

$$\Phi : Z(F^\rho)(\mathbb{F})_{\Delta^\sigma \neq 0} \to Z(I^\rho)(\mathbb{F})$$

the map constructed above that sends every $(d+1)$-tuple $(\underline{\tau},\xi)$ to the r-tuple $\underline{\omega}$.

We claim that *the map Φ is injective*. Namely let $(\underline{\tau},\xi)$ and $(\underline{\tau}',\xi')$ be two tuples in $Z(F^\rho)(\mathbb{F})_{\Delta^\rho \neq 0}$. They determine two morphisms $\sigma,\sigma' : A \to \mathbb{F}$ such that $\sigma(\underline{t},\alpha) = (\underline{\tau},\xi)$ and $\sigma'(\underline{t},\alpha) = (\underline{\tau}',\xi')$. By construction, we have $\Phi(\underline{\tau},\xi) = \sigma(\underline{x} \bmod I)$ and $\Phi(\underline{\tau}',\xi') = \sigma'(\underline{x} \bmod I)$. If these two r-tuples are equal, then $\sigma = \sigma'$ and so $(\underline{\tau},\xi) = (\underline{\tau}',\xi')$.

Conclude that $\mathrm{card}(Z(I^\rho)(\mathbb{F})) \geqslant \mathrm{card}(Z(F^\rho)(\mathbb{F})_{\Delta^\rho \neq 0})$, and so that

$$c_\rho(I) \geqslant c_\rho(F) - c_\rho(\Delta)\deg_Y(F).^6 \tag{15}$$

□

[6] In the special case $d = 0$, condition (14) is void, $Z(F^\rho)(\mathbb{F})_{\Delta^\sigma \neq 0} = Z(F^\rho)(\mathbb{F})$ and $c_\rho(\Delta) = 0$.

3.3. **Proof of the Lang-Weil estimate assuming the case of hypersurfaces.** We retain the notation and assumptions from Sections 3.1–3.2.

Definition 3.6. The *hypersurface degree* of the d-dimensional affine variety $V \subset \mathbb{A}^r_R$ is defined to be the smallest degree of some polynomial $F \in K[\underline{T}, Y]$ such that for some nonzero $c \in R$, the polynomial F locally represents V as a hypersurface over $R[c^{-1}]$ (in the sense of Definition 3.1). We denote it by $\mathrm{hdeg}(V)$.

Remark 3.7.

(a) If R is integrally closed, we have $1 \leqslant \mathrm{hdeg}(V) < +\infty$ (Lemma 3.3). If V is itself a hypersurface, then $\mathrm{hdeg}(V) \leqslant \deg(V)$ where $\deg(V)$ is the usual degree, i.e. the degree of a polynomial defining the hypersurface V. This inequality is strict in general: for example, the hypersurface $V \subset \mathbb{A}^2$ of equation $Y^2+T^4-2T^2Y-T=0$ can be represented by the hypersurface of equation $Y^2-T=0$ and so $\mathrm{hdeg}(V) \leqslant 2 < \deg(V) = 4$.

(b) The hypersurface degree is more intrinsic than the usual degree (which depends on the embedding $V \subset \mathbb{A}^r$): if $V_1 \subset \mathbb{A}^{r_1}_R$ and $V_2 \subset \mathbb{A}^{r_2}_R$ are two d-dimensional affine varieties such that there exist two morphisms $\psi_i : V_i \to \mathbb{A}^d_R$, $i = 1, 2$, and two isomorphisms $\chi : V_1 \to V_2$ and $\lambda : \mathbb{A}^d_R \to \mathbb{A}^d_R$ satisfying $\psi_2 \circ \chi = \lambda \circ \psi_1$ above a Zariski-open subset $\mathbb{A}^d_R \setminus Z(\Delta)$ for some nonzero $\Delta \in R[\underline{T}]$, then $\mathrm{hdeg}(V_1) = \mathrm{hdeg}(V_2)$.

Our goal is to prove the following statement, which is Corollary 1.5 from Section 1.

Theorem 3.8. *Given nonnegative integers d, r and h, there is a positive constant $A(r,h)$ such that for every finite field $\mathbb{F}_q$ of cardinality $q = p^\beta$ with p prime and $\beta \geqslant 1$, and every prime ideal $I \subset \mathbb{F}_q[\underline{x}]$ such that the affine variety $V = Z(I) \subset \mathbb{A}^r$ is geometrically irreducible, of dimension $\dim(V) = d$ and of hypersurface degree $\mathrm{hdeg}(V) = h$, we have:*

$$|\operatorname{card}(V(\mathbb{F}_q)) - q^d| \leqslant (h-1)(h-2)\, q^{d-\frac{1}{2}} + A(r,h)\, q^{d-1}. \tag{16}$$

From Remark 3.7, the error term on the right-hand side is smaller, for hypersurfaces, than the one from the original *Lang-Weil estimate.*

Proof. Fix an ideal I as in the statement. The proof uses Sections 3.1–3.2. Retain the notation from there and take $R = K = \mathbb{F} = \mathbb{F}_q$. Lemma 3.3 may be applied. Pick a polynomial $F \in \mathbb{F}_q[\underline{T}, Y]$ such that the polynomial F locally represents V as a hypersurface and such that $\deg(F) = \mathrm{hdeg}(V)$. Apply Lemma 3.4 with $\rho : \mathbb{F} \to \mathbb{F}$ the identity (so both f^ρ and Δ^ρ are nonzero in $\mathbb{F}_q[\underline{x}]$). We obtain:

$$c_\rho(F) - \deg_Y(F)\, c_\rho(\Delta) \leqslant c_\rho(I) \leqslant c_\rho(F) + c_\rho(\langle I, f\rangle). \tag{17}$$

The assumption that V is geometrically irreducible means that the extension $L/\mathbb{F}_q$ is regular (i.e. $L \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$). It classically follows that $[L\overline{\mathbb{F}_q} : \overline{\mathbb{F}_q}(\underline{t})] = [L : \mathbb{F}_q(\underline{t})]$ and so that F is irreducible in $\overline{\mathbb{F}_q}[\underline{T}, Y]$ (e.g. [3, Prop.2.3.2]). Now resort to the paper [2], which covers the hypersurface case, to assert that there exists a constant $A_1(r,h)$ such that

$$|c_\rho(F) - q^d| \leqslant (h-1)(h-2)\, q^{d-\frac{1}{2}} + A_1(r,h)\, q^{d-1}. \tag{18}$$

To prove Theorem 3.8, it remains to prove that there exist positive constants $A_2(r,h)$ and $A_3(r,h)$ such that

$$(*)\ c_\rho(\langle I, f\rangle) \leqslant A_2(r,h)\, q^{d-1} \quad \text{and} \quad (**)\ c_\rho(\Delta) \leqslant A_3(r,h)\, q^{d-1}.$$

(**) follows from the Zippel-Schwartz lemma (Theorem 2.1): we have $c_\rho(\Delta) \leqslant \deg(\Delta)\, q^{d-1}$, and Δ is the discriminant of F w.r.t. the variable Y, so its degree can be bounded from above in terms of $\deg(F) = \operatorname{hdeg}(V) \leqslant h$.

For (*), consider a r-tuple $\underline{\omega}$ in $Z(\langle I, f\rangle)(\mathbb{F})$. By definition $f(\underline{\omega}) = \Delta(\underline{\varphi}(\underline{\omega})) = 0$. We obtain that

$$\operatorname{card}\left(\underline{\varphi}\,[Z(\langle I, f\rangle)(\mathbb{F}_q)]\right) \leqslant c_\rho(\Delta) \leqslant A_3(r,h)\, q^{d-1}.$$

View the d-tuple $\underline{\varphi} = (\varphi_1, \dots, \varphi_d) \in R[\underline{x}]^d$ (defined in §3.2) as a morphism $\underline{\varphi} : Z(I) \to \mathbb{A}^d$. It is induced by the ring morphism $R[\underline{t}] \to R[\underline{x} \bmod I]$ that maps each t_i to $\varphi_i(\underline{x} \bmod I)$, $i = 1, \dots, d$. As $R[\underline{x} \bmod I] = A$ is a $R[\underline{t}]$-module of finite type, this morphism is finite. Thus the fibers are of finite cardinality, and less than or equal to the generic degree $[L : K(\underline{t})] = \deg_Y(F)$. Whence

$$\operatorname{card}(Z(\langle I, f\rangle)(\mathbb{F})) \leqslant \deg_Y(F)\ \operatorname{card}(\underline{\varphi}(Z(\langle I, f\rangle)(\mathbb{F}))) \leqslant h\, A_3(r,h)\, q^{d-1}.$$

□

3.4. **Proof of Corollary 1.4.** We will deduce it from the following lemma.

Lemma 3.9. *Let $I \subset \mathbb{Z}[\underline{x}]$ be an ideal such that $I \cap \mathbb{Z} = \{0\}$. Set $A = \mathbb{Z}[\underline{x}]/I$, $V = Z(I)$ and $d = \dim(V)$. Then we have the following:*

(a) there is a constant $M = M(I)$ depending on I such that $c_p(I) \leqslant M\, p^d$ for all primes p.

(b) If the ideal I is prime, there is an irreducible polynomial $F \in \mathbb{Z}[T_1, \dots, T_d, Y]$ and a constant $B = B(I)$ depending on I such that, for all primes p, we have:

$$|c_p(I) - c_p(F)| \leqslant B\, p^{d-1}.$$

Lemma 3.9(b) is Lemma 1.3 from Section 1 and Lemma 3.9(a) is the generalization to ideals I of the *Zippel-Schwartz upper bound* (mentioned after Corollary 1.4).

Proof of Lemma 3.9. Observe first that, for any prime p, $c_p(I)$ remains the same if I is replaced by its radical $\sqrt{I}$. Hence assume that $I = \sqrt{I}$. Classically then, I can be written as the intersection of finitely many prime ideals J_k (e.g. [3, Thm1.1.11]). If the ideals J_k are *minimal* prime ideals, the Zariski-closed subsets $Z(J_k)$ are the irreducible components of $Z(I)$ and $d = \dim(V)$ is the supremum of the dimensions $\dim(Z(J_k))$. Thus

(*) *for proving (a), one may assume that I is a prime ideal and, for the general case, eventually multiply the constant C obtained in the prime case by the number, say ν, of irreducible components of $V = Z(I) \subset \mathbb{A}^r$.*

Preliminary part. Assume that I is a prime ideal. Retain the notation from Sections 3.1–3.2 and assume further that $R = \mathbb{Z}$. From Lemma 3.3, there exists a nonzero element $c \in \mathbb{Z}$, such that, over the ring $\mathbb{Z}[c^{-1}]$, the affine variety $V \subset \mathbb{A}^r$ can be represented as a hypersurface above a Zariski-open $\mathbb{A}^d \setminus Z(\Delta)$ (for some nonzero $\Delta \in \mathbb{Z}[\underline{t}]$). Denote as usual by $F \in \mathbb{Z}[c^{-1}][T_1, \dots, T_d, Y]$ a monic polynomial defining the hypersurface.
Apply Lemma 3.4 with $\mathbb{F} = \mathbb{F}_p$, $\rho : \mathbb{Z} \to \mathbb{F}_p$ the reduction morphism and p a prime such that c, f, Δ are nonzero modulo p; this only excludes finitely many p. Lemma 3.4 yields:

$$-\deg_Y(F)\, c_p(\Delta) \leqslant c_p(I) - c_p(F) \leqslant c_p(\langle I, f\rangle). \tag{19}$$

At this point, distinguish two cases:

1st case: $(f \bmod I)$ *is a unit of* $A[c^{-1}]$. Then, for every $\underline{\omega} \in Z(I \bmod p)(\mathbb{F}_p)$, the element $(f \bmod I)(\underline{\omega})$ is non-zero in $\mathbb{F}_p$ [7], and so the set $Z(\langle I, f\rangle \bmod p)(\mathbb{F}_p)$ is empty, i.e.

$$c_p(\langle I, f\rangle) = 0. \tag{20}$$

2nd case: $(f \bmod I)$ *is not a unit of* $A[c^{-1}]$. As $(f \bmod I)$ is non-zero in $A[c^{-1}]$ (as noted in (9)) and that $A[c^{-1}]$ is an integral domain, $(f \bmod I)$ is not either a zero divisor. Thus Krull's Hauptidealsatz [7, Theorem 1.11A] may be applied to conclude that every minimal prime ideal of $A[c^{-1}]$ containing $(f \bmod I)$ is of height 1. In particular, the Zariski-closed subset $Z(\langle I, f\rangle)$ is of dimension $\dim(V) - 1 = d - 1$.

Proof of (a). Let I be an ideal as in Lemma 3.9 (not necessarily prime). The proof goes by induction on $d = \dim(V)$.
Assume $d = 0$. Assume first that I is a prime ideal. Then I is maximal (as A/I being of Krull dimension $d = 0$ implies that A/I is a field). Fix a prime p. If $c_p(I) \neq 0$, then the ideal I is contained in the maximal ideal $I_{\underline{\omega}} \subset \mathbb{Z}[\underline{x}]$ annihilating some $\underline{\omega} \in \mathbb{F}_p^r$. Conclude that $I = I_{\underline{\omega}}$ and so that $c_p(I) = 1$. Thus $c_p(I)$ equals 0 or 1 for every prime p. One may take $M(I) = 1$, when I is prime, and $M(I) = \nu$ in the more general case (from (*) above).

Assume that $d \geqslant 1$. Again assume first that I is a prime ideal and use the preliminary part. Let p be a prime number such that c, f and Δ are all nonzero modulo p. From display (19), combined with the Zippel-Schwartz lemma (Theorem 2.1), we have:

$$c_p(I) \leqslant \deg(F)\, p^d + c_p(\langle I, f\rangle). \tag{21}$$

Furthermore, either $c_p(\langle I, f\rangle) = 0$, or $Z(\langle I, f\rangle)$ is of dimension $d - 1$, in which case the induction hypothesis gives

$$c_p(\langle I, f\rangle) \leqslant M(\langle I, f\rangle)\, p^{d-1} \tag{22}$$

(where $M(\langle I, f\rangle)$ is the constant associated to the ideal $\langle I, f\rangle$ in the induction hypothesis). Displays (21), (22) finish the induction: taking (*) into account, one may take $M(I)$ any constant $\geqslant \nu \times (\deg(F) + M(\langle I, f\rangle))$, and $\geqslant c_p(I)/p^d$ for all the finitely many primes p excluded in the preliminary part.

Proof of (b). Here assume that $I \subset \mathbb{Z}[\underline{x}]$ is a prime ideal. The requested conclusion follows from the double inequality (19) from the preliminary part. Namely, from the already proven part (a), we have $c_p(\langle I, f\rangle) \leqslant M(\langle I, f\rangle)\, p^{d-1}$, and from the Zippel-Schwartz lemma, we have $c_p(\Delta) \leqslant \deg(\Delta)\, p^{d-1}$, both for all primes p. [8]
Note finally that for the polynomial F to have coefficients in $\mathbb{Z}$ as claimed, instead of $\mathbb{Z}[c^{-1}]$ as constructed, it suffices to multiply it by a suitably big power of c. This does not affect the required conclusion, except possibly for the finite list of prime divisors of c, for which we may still keep the conclusion valid by enlarging the constant B. □

Finally we can prove Corollary 1.4 from Section 1, which we restate:

Corollary 1.4. *The series* $\displaystyle\sum_{p \in \mathcal{P}} \frac{c_p(I)}{p^{d+1}}$ *is divergent.*

[7] With the notation from the proof of Lemma 3.4, $(f \bmod I)(\underline{\omega})$ is $\rho(f \bmod I)$, with $\rho : A \to \mathbb{F}_p$ the prolongation of $\rho : R \to \mathbb{F}$ defined there.

[8] In the special case $d = 0$, the polynomial Δ is a nonzero constant that remains nonzero modulo p, so $c_p(\Delta) = 0$ which is indeed $\leqslant A_2 \deg(\Delta)\, p^{0-1}$ for every p.

Proof. Rewrite the conclusion of Lemma 3.9(b) as

$$\left|\frac{c_p(I)}{p^{d+1}} - \frac{c_p(F)}{p^{d+1}}\right| \leqslant \frac{B}{p^2} \qquad \text{for all primes } p.$$

The requested conclusion follows from this conclusion, combined with the fact, already proved as Theorem 1.1, that the series $\sum_{p\in\mathcal{P}} \frac{c_p(F)}{p^{d+1}}$ is divergent. □

3.5. **Variety variants of the Ostrowski theorem and the Lang-Weil lower bound.**

This subsection shows how to use Lemma 3.3 to extend to varieties two further statements known for hypersurfaces. In the first one (Corollary 3.10) it is the Ostrowski theorem that is extended, in the second one (Corollary 3.12), it is the *Lang-Weil lower bound*.

Corollary 3.10. *Let k be a number field and $\mathcal{O}$ be its ring of integers. Let $I \subset \mathcal{O}[\underline{x}]$ be an ideal such that $I \cap \mathcal{O} = \{0\}$ and $I \otimes_{\mathcal{O}} \overline{k}$ is a prime ideal of $\overline{k}[\underline{x}]$. Then for all but finitely many prime ideals $\mathfrak{p} \subset \mathcal{O}$, the ideal $(I \bmod \mathfrak{p})$ generates a prime ideal of $(\overline{\mathcal{O}/\mathfrak{p}})[\underline{x}]$.*

Equivalently, for the same prime ideals $\mathfrak{p}$, the Zariski-closed subsets $Z(I \bmod \mathfrak{p})$ are geometrically irreducible varieties.

The classical Ostrowski theorem is the special case that I is generated by a single polynomial $F \in \mathcal{O}[\underline{x}]$, i.e. $V = Z(I)$ is a hypersurface. The presented generalization was known before (e.g. [6, Corollary 10.4.3]), and obtained, as we will present too, by reduction to the classical case. We include it here as a further self-contained illustration of our approach; the proof given in [6] uses some model theory.

Proof. Set $V = Z(I) \subset \mathbb{A}^r_{\mathcal{O}}$ and $d = \dim(V)$. From Lemma 3.3, there exist $c \in \mathcal{O}$, $c \neq 0$ and an irreducible polynomial $F \in \mathcal{O}[\underline{T}, Y]$ (with $\underline{T} = (T_1, \ldots, T_d)$), monic in Y such that the affine variety V can be locally represented as the hypersurface $Z(F) \subset \mathbb{A}^{d+1}_{\mathcal{O}}$ over the ring $\mathcal{O}[c^{-1}]$. As noted in Remark 3.2, there is a finite morphism $V \to \mathbb{A}^d$ such that,

(*) *above some open subset $\mathbb{A}^d \setminus Z(\Delta)$ with $\Delta \in \mathcal{O}[c^{-1}][\underline{T}]$, $\Delta \neq 0$, the affine variety V is isomorphic to the hypersurface $Z(F)$.*

The classical Ostrowski theorem asserts that for all but finitely many primes $\mathfrak{p} \subset \mathcal{O}$, the polynomial $(F \bmod \mathfrak{p})$ is irreducible in $\overline{k_{\mathfrak{p}}}[\underline{T}, Y]$, where $k_{\mathfrak{p}}$ is the finite field $\mathcal{O}/\mathfrak{p}$. Equivalently, $Z(F) \otimes_{\mathcal{O}} \overline{k_{\mathfrak{p}}}$ is irreducible. It follows from (*) that for all prime ideals $\mathfrak{p} \subset \mathcal{O}$ but in a finite list including those that divide c, the Zariski-closed subset $V \otimes_{\mathcal{O}} \overline{k_{\mathfrak{p}}}$ is irreducible as well, which is equivalent to $(I \bmod \mathfrak{p})$ generating a prime ideal of $\overline{k_{\mathfrak{p}}}[\underline{x}]$. □

Remark 3.11. We restricted to the Ostrowski version of the Bertini-Noether theorem for simplicity. The same argument yields a similar "variety version" of the full Bertini-Noether theorem (as in [6, Prop.10.4.2]). The ring $\mathcal{O}$ can be taken any integrally closed domain and k its fraction field. In the conclusion, "*for all but finitely many prime ideals $\mathfrak{p} \subset \mathcal{O}$*" should be replaced by "*for all prime ideals $\mathfrak{p} \subset \mathcal{O}$ but in a Zariski-closed subset of* $\operatorname{Spec} \mathcal{O}$".

Our final application is this generalization of the *Lang-Weil lower bound* from Section 1.

Corollary 3.12. *Let $I \subset \mathbb{Z}[\underline{x}]$ be an ideal such that $I \cap \mathbb{Z} = \{0\}$. Set $V = Z(I)$ and $d = \dim(V)$. Then for every $\varepsilon > 0$, there exist infinitely many primes p such that*

$$c_p(I) \geqslant (1-\varepsilon)\, p^d.$$

Proof. Combine the argument given in Section 2.5 in the case that V is a hypersurface with Lemma 1.3 to reduce to that situation. □

References

[1] Arnaud Bodin and Pierre Dèbes. Coprime values of polynomials in several variables. *Israel J. Math.* (to appear), 2022.

[2] Antonio Cafure and Guillermo Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields Appl.*, 12(2):155–185, 2006.

[3] Pierre Dèbes. Arithmétique des revêtements de la droite. *Notes de cours, Univ. Lille*, 2009.

[4] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[5] Torsten Ekedahl. An infinite version of the Chinese remainder theorem. *Comment. Math. Univ. St. Paul.*, 40(1):53–59, 1991.

[6] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.

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

[8] Gilles Lachaud and Robert Rolland. On the number of points of algebraic sets over finite fields. *J. Pure Appl. Algebra*, 219(11):5117–5136, 2015.

[9] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464, 1977.

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

[11] Bjorn Poonen. Squarefree values of multivariable polynomials. *Duke Math. J.*, 118(2):353–373, 2003.

[12] Issai Schur. Über die Existenz unendlich vieler Primzahlen in einiger speziellen arithmetischen progressionen. *S.-B. Berlin Math. Ges.*, 11:40–50, 1912.

[13] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[14] Jean-Pierre Serre. Lettre à M. Tsfasman. Number 198-200, pages 11, 351–353 (1992). 1991. Journées Arithmétiques, 1989 (Luminy, 1989).

[15] Igor E. Shparlinski. Points on varieties over finite fields in small boxes. In *SCHOLAR—a scientific celebration highlighting open lines of arithmetic research*, volume 655 of *Contemp. Math.*, pages 209–233. Amer. Math. Soc., Providence, RI, 2015.

[16] Serguei A. Stepanov. *Codes on algebraic curves*. Kluwer Academic/Plenum Publishers, New York, 1999.

Email address: `arnaud.bodin@univ-lille.fr`
Email address: `pierre.debes@univ-lille.fr`
Email address: `slhnajib@gmail.com`

Université de Lille, CNRS, Laboratoire Paul Painlevé, 59000 Lille, France

Université de Lille, CNRS, Laboratoire Paul Painlevé, 59000 Lille, France

Laboratoire multidisciplinaire de recherche et d'innovation, Faculté Polydisciplinaire de Khouribga, Université Sultan Moulay Slimane, BP 145, Hay Ezzaytoune, 25000 Khouribga, Maroc.