COPRIME VALUES OF POLYNOMIALS IN SEVERAL VARIABLES

ARNAUD BODIN AND PIERRE DÈBES

Dedicated to Moshe Jarden on the occasion of his 80th birthday

Abstract. Given two polynomials $P(\underline{x})$, $Q(\underline{x})$ in one or more variables and with integer coefficients, how does the property that they are coprime relate to their values $P(\underline{n}), Q(\underline{n})$ at integer points $\underline{n}$ being coprime? We show that the set of all $\gcd(P(\underline{n}), Q(\underline{n}))$ is stable under gcd and under lcm. A notable consequence is a result of Schinzel: if in addition P and Q have no fixed prime divisor (i.e., no prime dividing all values $P(\underline{n})$, $Q(\underline{n})$), then P and Q assume coprime values at "many" integer points. Conversely we show that if "sufficiently many" integer points yield values that are coprime (or of small gcd) then the original polynomials must be coprime. Another noteworthy consequence of this paper is a version "over the ring" of Hilbert's irreducibility theorem.

Let $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be $s \geqslant 2$ polynomials in $r \geqslant 1$ variables $\underline{x} = (x_1, \dots, x_r)$. For $\underline{n} = (n_1, \dots, n_r) \in \mathbb{Z}^r$, we consider the corresponding values $P_i(\underline{n})$. Is there a connection between (a) $P_1(\underline{x}), \dots, P_s(\underline{x})$ being coprime as polynomials and (b) "many" of the values $P_1(\underline{n}), \dots, P_s(\underline{n})$ being coprime as integers? Answers exist in both directions.

Suppose that the polynomials $P_1(\underline{x}), \dots, P_s(\underline{x})$ are coprime and their values have no *fixed divisors*, i.e., no prime number p divides all $P_i(\underline{n})$ (for all i, and all $\underline{n}$). Then it is true that for some $\underline{n} \in \mathbb{Z}^r$, the integers $P_1(\underline{n}), \dots, P_s(\underline{n})$ are coprime: coprime polynomials assume coprime values. This is proved by Schinzel in [10]; Ekedahl [4] and Poonen [9] even give, in the special case $s = 2$, a formula for the density of the good $\underline{n}$; see Section 1.3 below, and also [1] where Schinzel's result is extended to other rings than $\mathbb{Z}$, including all UFDs and all Dedekind domains.

Here we put forward a more general property of polynomials that implies Schinzel's coprime conclusion. Set $d_{\underline{n}} = \gcd(P_1(\underline{n}), \dots, P_s(\underline{n}))$, for $\underline{n} \in \mathbb{Z}^r$, the gcd of the values. We show, even without the fixed divisor assumption, that the set $\mathcal{D}$ of all these $d_{\underline{n}}$ is stable under gcd and lcm, i.e., is a lattice for the divisibility (Theorem 1.1); the quick proof that it yields Schinzel's theorem is in Section 1.2. This generalizes previous results in one variable [2].

Regarding the Ekedahl–Poonen formula, we extend it to the case of $s \geqslant 2$ polynomials and to the situation that *several* families of such polynomials are given (Section 1.3). We can then show a version "over the ring $\mathbb{Z}$" of Hilbert's Irreducibility Theorem (Theorem 1.7).

In the reverse direction, it is not true that if $P_1(\underline{n}), \dots, P_s(\underline{n})$ are coprime at one integer point $\underline{n}$ (or even at infinitely many) then the polynomials $P_1(\underline{x}), \dots, P_s(\underline{x})$ are coprime. However we show that the coprimality of $P_1(\underline{x}), \dots, P_s(\underline{x})$ does hold if "sufficiently many" $\underline{n}$, in a density sense, can be found such that $P_1(\underline{n}), \dots, P_s(\underline{n})$ are coprime (Theorem 1.9).

Date: September 4, 2022.

2010 *Mathematics Subject Classification.* Primary 12E05 ; Sec. 11A05.

Key words and phrases. coprime polynomials, coprime integers, gcd.

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 Hilbertian specialization property has always been a central topic in Field Arithmetic. Through his work, Moshe Jarden has constantly promoted both the area and this subtopic. The celebrated "Fried-Jarden book", *the* Field Arithmetic reference, has been quite influential to both authors. With this paper, we are happy to contribute to the Israel Journal of Mathematics special volume dedicated to Moshe Jarden and to offer him as a final application a version "over the ring" of Hilbert's irreducibility theorem.

1. Presentation

Throughout the paper, we adhere to the following notation. Given $s \geqslant 2$ nonzero polynomials $P_1(\underline{x}), \dots, P_s(\underline{x})$ in $\mathbb{Z}[\underline{x}]$ (where $\underline{x} = (x_1, \dots, x_r)$ with $r \geqslant 1$), we say that they are *coprime* (over the field $\mathbb{Q}$) if no polynomial $D(\underline{x}) \in \mathbb{Q}[\underline{x}]$ with $\deg D > 0$ divides each of $P_1(\underline{x}), \dots, P_s(\underline{x})$. In the definition of $d_{\underline{n}} = \gcd(P_1(\underline{n}), \dots, P_s(\underline{n}))$ ($\underline{n} \in \mathbb{Z}^r$), we include the case where $P_1(\underline{n}) = \dots = P_s(\underline{n}) = 0$ by defining $\gcd(0, \dots, 0) = 0$. Finally we set $\mathcal{D} = \left\{ d_{\underline{n}} \mid \underline{n} \in \mathbb{Z}^r \right\}$.

1.1. The stability result.

Theorem 1.1. *If $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ are $s \geqslant 2$ nonzero coprime polynomials, then the set $\mathcal{D} = \left\{ d_{\underline{n}} \mid \underline{n} \in \mathbb{Z}^r \right\}$ is stable under gcd and lcm.*

That is: if $d, d' \in \mathcal{D}$ then $\gcd(d, d') \in \mathcal{D}$ and $\operatorname{lcm}(d, d') \in \mathcal{D}$. This is a generalization of the one variable case ($r = 1$) done with S. Najib [2].

Example 1.2. Let $P(x, y) = x^2 - y^3$, $Q(x, y) = x(y+2)+1$. Let $d_{m,n} = \gcd(P(m, n), Q(m, n))$ and $\mathcal{D} = \{d_{m,n}\}_{m,n \in \mathbb{Z}}$. For instance $P(5, 1) = 24$, $Q(5, 1) = 16$, hence $d_{5,1} = \gcd(24, 16) = 8$. For $(m, n) = (1, -3)$, $d_{m,n} = 28$. The gcd of 8 and 28 is 4, and 4 is an element of $\mathcal{D}$: $d_{5,5} = 4$. Experimentation yields an infinite set:

$$\mathcal{D} = \{1, 2, 4, 7, 8, 14, 16, 23, 28, 29, 32, 37, 41, 46, 47, 49, 53, 56, 58, 59, 61, 64, 67, 74, 79, 82, 83, 89, 92, 94, 97, 98, \dots\}$$

1.2. Consequences.

The following two corollaries are quick consequences of Theorem 1.1. The first one is what we refer to as Schinzel's result in our introduction.

Corollary 1.3. *Let $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be $s \geqslant 2$ nonzero coprime polynomials. Suppose that there is no prime number p that divides $P_i(\underline{n})$ for each $i = 1, \dots, s$ and every $\underline{n} \in \mathbb{Z}^r$. Then there exists $\underline{n}_0 \in \mathbb{Z}^r$ such that $P_1(\underline{n}_0), \dots, P_s(\underline{n}_0)$ are coprime integers.*

Moreover, the set of such $\underline{n}_0$ will be shown to be Zariski-dense in $\mathbb{Z}^r$ (Corollary 4.2), and even of positive density (as discussed in §1.3 below and shown in §6).

Proof of Corollary 1.3 assuming Theorem 1.1. The set $\mathcal{D} \subset \mathbb{N}$ is not necessarily finite (for $r \geqslant 2$). Let $\{d_{i_j}\}_{j \in \mathbb{N}}$ be an enumeration of $\mathcal{D}^\star = \mathcal{D} \setminus \{0\}$ and set $\delta_j = \gcd(d_{i_0}, \dots, d_{i_j})$. The sequence $(\delta_j)_{j \in \mathbb{N}}$ is a decreasing sequence of positive integers, hence is ultimately constant equal to some value $d^\star \in \mathbb{N}$, and $d^\star = \gcd(\mathcal{D}^\star) = \min(\mathcal{D}^\star)$.
By Theorem 1.1, $\mathcal{D}$ is stable by gcd; so is $\mathcal{D}^\star$. Using $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$, we have $\delta_j \in \mathcal{D}^\star$, for every $j \in \mathbb{N}$. It follows that $d^\star \in \mathcal{D}^\star$. The no fixed divisor assumption yields $d^\star = 1$. Hence $1 \in \mathcal{D}^\star$, thus giving the conclusion. □

Corollary 1.4. *Let $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be $s \geqslant 2$ nonzero polynomials with no common zero in $\mathbb{C}^r$. Then $\mathcal{D}$ is a finite subset of $\mathbb{Z}$ stable under gcd and lcm. In particular, the smallest positive element $d^\star$ of $\mathcal{D}$ is a common divisor of all elements of $\mathcal{D}$ and the largest positive element $\mu^\star$ of $\mathcal{D}$ is a common multiple of all elements of $\mathcal{D}$.*

Proof. Hilbert's Nullstellensatz provides polynomials $A_1(\underline{x}), \dots, A_s(\underline{x}) \in \mathbb{Q}[x]$ such that $\sum_{i=1}^s A_i(\underline{x})P_i(\underline{x}) = 1$. Clearing the denominators yields polynomials $B_1(\underline{x}), \dots, B_s(\underline{x}) \in \mathbb{Z}[x]$ and $\Delta \in \mathbb{Z}$, $\Delta \neq 0$, such that $\sum_{i=1}^s B_i(\underline{x})P_i(\underline{x}) = \Delta$. It readily follows that every element $d_{\underline{n}} \in \mathcal{D}$ divides Δ. Hence $\mathcal{D}$ is finite. The rest is given by Theorem 1.1. □

1.3. **Ekedahl–Poonen formula.** Given $s \geqslant 2$ nonzero coprime polynomials $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ as in Theorem 1.1, this formula provides another refinement of Corollary 1.3: it computes the density of integer points where the values are coprime. Specifically let

$$\mathcal{R} = \big\{\underline{n} \in \mathbb{Z}^r \mid P_1(\underline{n}), \dots, P_s(\underline{n}) \text{ are coprime}\big\}.$$

The *density* $\mu(\mathcal{S})$ of a subset $\mathcal{S}$ of points with non-negative integer coordinates is defined as follows. For $B > 0$, set $\mathbb{B} = [\![0, B-1]\!]^r$, where $[\![0, B-1]\!]$ is the set of integers from 0 to $B-1$. Then

$$\mu(\mathcal{S}) = \lim_{B \to +\infty} \frac{\#(\mathcal{S} \cap \mathbb{B})}{\#\mathbb{B}}.$$

The sets we consider are subsets of $\mathbb{Z}^r$ and our results are about their density within the r-dimensional quadrant $[0, +\infty[^r$. For simplicity of notation, we extend the definition of μ to subsets $S \subset \mathbb{Z}^r$ by setting: $\mu(S) = \mu(S \cap ([0, +\infty[^r))$. Remark 1.6 explains that, in addition to giving the density of $\mathcal{R}$, Theorem 1.5 shows that $\mathcal{R}$ is equidistributed among all r-dimensional quadrants.

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

Theorem 1.5 (Ekedahl–Poonen density formula)**.** *Let $\underline{x} = (x_1, \dots, x_r)$ ($r \geqslant 1$). Let $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ ($s \geqslant 2$) be nonzero coprime polynomials. We have:*

$$\mu(\mathcal{R}) = \prod_{p \in \mathcal{P}} \left(1 - \frac{c_p}{p^r}\right)$$

where $c_p = \#\big\{\underline{n} \in (\mathbb{Z}/p\mathbb{Z})^r \mid P_1(\underline{n}) = 0 \pmod p, \dots, P_s(\underline{n}) = 0 \pmod p\big\}$.

If we assume, as in Corollary 1.3, that there is no prime p dividing all values $P_1(\underline{n}), \dots, P_s(\underline{n})$ ($\underline{n} \in \mathbb{Z}^r$), we obtain that $\mathcal{R}$ *is of positive density*: all terms in the product from Theorem 1.5 are positive, and the product is convergent if $r \geqslant 2$ and finite if $r = 1$ (as shown in Section 2.3).

Remark 1.6. It follows from the formula for $\mu(\mathcal{R})$ that the density of $\mathcal{R}$ would be the same if computed w.r.t to any other r-dimensional quadrant, instead of $[0, +\infty[^r$: indeed the number c_p of solutions of $P_1(\underline{n}) = \cdots = P_s(\underline{n}) = 0 \pmod p$ in a box of width p is independent of the choice of the box. This also shows that for the density defined by $\tilde{\mu}(\mathcal{R}) = \lim_{B \to +\infty} \frac{\#(\mathcal{R} \cap \mathbb{B})}{\#\mathbb{B}}$ with this time $\mathbb{B} = [\![-B, B]\!]^r$, then $\tilde{\mu}(\mathcal{R}) = \mu(\mathcal{R})$.

We provide a proof of the Ekedahl–Poonen formula in Section 6. It follows Poonen's proof with some adjustments. In particular we consider the general case $s \geqslant 2$ (and not just $s = 2$). We also consider in Section 6.7 the more general situation that *several* families of coprime polynomials $\{P_{1i}(\underline{x})\}_i$, $\{P_{2i}(\underline{x})\}_i, \dots,$ $\{P_{\ell i}(\underline{x})\}_i$ are given and one looks for the density of the set of points $\underline{n} \in \mathbb{Z}^r$ such that, for each $j = 1, \dots, \ell$, the integers $P_{j1}(\underline{n}), P_{j2}(\underline{n}), \dots$ are coprime (Proposition 6.3). This generalization will be used to prove the case of *several* polynomials in the following result.

1.4. **A version over the ring of Hilbert's Irreducibility Theorem.**

Theorem 1.7. *Let $\underline{y} = (y_1, \dots, y_n)$ be $n \geqslant 1$ new variables. Let $P_1(\underline{x}, \underline{y}), \dots, P_\ell(\underline{x}, \underline{y})$ be $\ell \geqslant 1$ polynomials, irreducible in $\mathbb{Z}[\underline{x}, \underline{y}]$, of degree $\geqslant 1$ in $\underline{y}$. Assume there is no prime p such that $\prod_{j=1}^{\ell} P_j(\underline{n}, \underline{y}) \equiv 0 \pmod p$ for every $\underline{n} \in \mathbb{Z}^r$. Then the set of all $\underline{n} \in \mathbb{Z}^k$ such that $P_1(\underline{n}, \underline{y}), \dots, P_\ell(\underline{n}, \underline{y})$ are irreducible in $\mathbb{Z}[\underline{y}]$ is Zariski-dense, and even of positive $\tilde{\mu}$-density.*

Here, for "many" $\underline{n} \in \mathbb{Z}^r$, the specialized polynomials $P_1(\underline{n}, \underline{y}), \dots, P_\ell(\underline{n}, \underline{y})$ are irreducible in $\mathbb{Z}[\underline{y}]$, and not only in $\mathbb{Q}[\underline{y}]$ as Hilbert's Irreducibility Theorem would conclude: we have the additional conclusion that each polynomial $P_j(\underline{n}, \underline{y})$ is primitive, i.e., its coefficients are coprime integers. The assumption on the product $\prod_{j=1}^{\ell} P_j$ is clearly necessary and non void: for $P(x, y) = (x^2 - x)y + (x^2 - x + 2)$, we have $P(n, y) \equiv 0 \pmod 2$ and so $P(n, y)$ is divisible by 2 in $\mathbb{Z}[y]$, for every $n \in \mathbb{Z}$.
Theorem 1.7 compares to Theorem 1.6 from [1] (joint with Najib and König). The latter considers more general rings (UFDs or Dedekind domains, with a product formula), but does not have the density conclusion provided here in the special case of the ring of integers. The density approach also allows a quick proof of Theorem 1.7 assuming Theorem 1.5. The argument below is for $\ell = 1$; a reduction to this case is explained in Section 6.7.

Proof. Set $P = P_1$ and let $\mathcal{H}_P$ be the subset of $\mathbb{Z}^r$ of all $\underline{n}$ such that $P(\underline{n}, \underline{y})$ is irreducible in $\mathbb{Q}[\underline{y}]$. From Theorem 1 of [11, §13] (a result of S.D. Cohen), $\mathcal{H}_P$ is of density $\tilde{\mu}(\mathcal{H}_\mathcal{P}) = 1$ (with $\tilde{\mu}$ the density from Remark 1.6). Denote the coefficients of P, viewed as a polynomial in $\underline{y}$, by $P_1(\underline{x}), \dots, P_s(\underline{x})$ and consider the set $\mathcal{R}$ from Section 1.3 of all $\underline{n} \in \mathbb{Z}^r$ such that $P_1(\underline{n}), \dots, P_s(\underline{n})$ are coprime. The assumption of Theorem 1.7 corresponds to $P_1(\underline{x}), \dots, P_s(\underline{x})$ having no fixed divisor. From Theorem 1.5 and Remark 1.6, we have $\tilde{\mu}(\mathcal{R}) > 0$. It follows that $H = \mathcal{H}_P \cap \mathcal{R}$ is of positive $\tilde{\mu}$-density, thus proving the result since for every $\underline{n} \in H$, the polynomial $P(\underline{n}, \underline{y})$ is irreducible in $\mathbb{Z}[\underline{y}]$. ☐

1.5. **A criterion for coprimality.** In our introduction, we raised this reverse question: to what extent existence of coprime values forces the coprimality of the polynomials? For one variable polynomials we have this coprimality criterion involving the gcd in $\mathbb{Z}$ of some values. Define the *normalized height* of a degree d polynomial $P(x) = a_d x^d + \cdots + a_0$ by $H(P) = \max_{i=0,\dots,d-1} \left| \frac{a_i}{a_d} \right|$.

Proposition 1.8 ([2, Proposition 5.1])**.** *Let $P_1, \dots, P_s \in \mathbb{Z}[x]$ be $s \geqslant 2$ nonzero polynomials and H the minimum of the normalized heights $H(P_1), \dots, H(P_s)$. Then $P_1, \dots, P_s$ are coprime if and only if there exists $n \geqslant 2H + 3$ such that* $\gcd(P_1(n), \dots, P_s(n)) \leqslant \sqrt{n}$.

In particular if $P_1(n), \dots, P_s(n)$ are coprime (as integers) for some sufficiently large n then $P_1(x), \dots, P_s(x)$ are coprime (as polynomials). We wish to generalize this result to polynomials in several variables. But the following example proves that evaluation at one point, however big it is, may not give information on the coprimality of the polynomials: with $P(x, y) = (x - y)x$ and $Q(x, y) = (x - y)y$, we have $\gcd(P(n+1, n), Q(n+1, n)) = 1$, and so infinitely many points $(n + 1, n)$ where the gcd is small, despite the polynomials not being coprime.
The following result however ensures that if the gcd $d_{\underline{n}}$ is small for "sufficiently many" $\underline{n}$, in a stronger density sense, then the polynomials are coprime.

Theorem 1.9. *Let $P_1(\underline{x}), \ldots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be $s \geqslant 2$ nonzero polynomials in r variables. Let $\ell = \max(\deg P_1, \ldots, \deg P_s)$ and S be a nonempty finite set of $\mathbb{Z}$. Let $k > 0$. If*

$$\pi_k := \frac{\#\left\{\underline{n} \in S^r \mid d_{\underline{n}} \leqslant k\right\}}{\#S^r} > \frac{(2k+1)\ell}{\#S}$$

then $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime polynomials.

For $k = 1$, we have $\pi_1 := \frac{\#\left\{\underline{n} \in S^r | d_{\underline{n}} \leqslant 1\right\}}{\#S^r}$. Theorem 1.9 states that if $\pi_1 > \frac{3\ell}{\#S}$ then $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime polynomials; and clearly this also implies that $P_1(\underline{x}), \ldots, P_s(\underline{x})$ have no fixed prime divisor. This criterion is of interest because of the Ekedahl–Poonen density formula. If polynomials $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime and have no fixed prime divisor, then π_1 must be positive for sufficiently large S, and so up to taking S large enough, the criterion will indeed reach the coprimality conclusion.

Example 1.10. Let $P(x, y), Q(x, y) \in \mathbb{Z}[x, y]$ be two nonzero polynomials of degree $\leqslant \ell := 10$. Let $S = \{1, 2, \ldots, 100\}$ with $\#S = 100$. If for more than 30% of $(m, n) \in S^2$, we have $d_{m,n} = 1$ (i.e., $P(m, n)$ and $Q(m, n)$ coprime) or $d_{m,n} = 0$ (i.e., $P(m, n) = Q(m, n) = 0$), then we have $\pi_1 > \frac{30}{100}$, and so, from Theorem 1.9, $P(x, y)$ and $Q(x, y)$ are coprime polynomials.

Proof of Theorem 1.9. It relies on the Zippel–Schwartz lemma which is usually stated as a probability result, but in fact is an enumerative result.

Zippel–Schwartz lemma. *Let $P(x_1, \ldots, x_r)$ be a nonzero polynomial of degree ℓ over a field K. Let S be a nonempty finite set of K. Then*

$$\frac{\#\left\{(x_1, \ldots, x_r) \in S^r \mid P(x_1, \ldots, x_r) = 0\right\}}{\#S^r} \leqslant \frac{\ell}{\#S}.$$

Let $D(\underline{x}) = \gcd(P_1(\underline{x}), \ldots, P_s(\underline{x}))$. Then $\deg D \leqslant \ell$. Note further that $D(\underline{n})$ divides $d_{\underline{n}} = \gcd(P_1(\underline{n}), \ldots, P_s(\underline{n}))$, so that $|D(\underline{n})| \leqslant d_{\underline{n}}$. Now assume, by contradiction, that D is a non constant polynomial. We use the Zippel–Schwartz lemma to bound the number of solutions to the equations $D(\underline{n}) = j$. Specifically we have:

$$\begin{aligned}
\pi_k = \frac{\#\left\{\underline{n} \in S^r \mid d_{\underline{n}} \leqslant k\right\}}{\#S^r} &\leqslant \frac{\#\left\{\underline{n} \in S^r \mid |D(\underline{n})| \leqslant k\right\}}{\#S^r} \\
&\leqslant \sum_{j=-k}^{k} \frac{\#\left\{\underline{n} \in S^r \mid D(\underline{n}) = j\right\}}{\#S^r} \leqslant (2k+1)\frac{\ell}{\#S}
\end{aligned}$$

□

The paper is organized as follows. In Section 2, we focus on the case of polynomials in one variable. In Section 3, we present a tool of frequent use in the paper about how coprimality is preserved by specialization, in the vein of the Bertini–Noether and Ostrowski theorems for irreducibility (Proposition 3.1). Section 4 is devoted to a technical lemma, used in Section 5 for the proof of Theorem 1.1. We end in Section 6 with a proof of the Ekedahl–Poonen formula in the case of several polynomials.

2. The one variable case

The case of one variable polynomials plays a central role: first, some of the general results can be interestingly improved; secondly, most results in several variables will follow by reduction from the one variable case.

2.1. **Stability by gcd and lcm.**

Theorem 2.1 ([2, Prop. 3.2 and 3.3]). *Let $P_1(x), \dots, P_s(x) \in \mathbb{Z}[x]$ be nonzero coprime polynomials. Set $d_n = \gcd(P_1(n), \dots, P_s(n))$ $(n \in \mathbb{Z})$. Then the set $\mathcal{D} = \{d_n \mid n \in \mathbb{Z}\}$ is stable under gcd and lcm. Moreover there is a nonzero $\delta \in \mathbb{Z}$ that is a common multiple to all d_n and such that the sequence $(d_n)_{n\in\mathbb{Z}}$ is periodic of period δ. Hence $\mathcal{D}$ is a finite set.*

As $P_1(x), \dots, P_s(x)$ are coprime, note that it cannot happen that $P_1(n) = \dots = P_s(n) = 0$. The periodicity result is specific to the one variable case (see [2, §2.5]); δ can be taken to be any nonzero element of the ideal $\langle P_1, \dots, P_s\rangle \cap \mathbb{Z} \subset \mathbb{Z}[\underline{x}]$. For two polynomials $P(x)$ and $Q(x)$, δ can be chosen as the resultant of P and Q. More generally, as the polynomials $P_1(x), \dots, P_s(x)$ are coprime in $\mathbb{Q}[x]$, one can write a Bézout identity:

$$A_1(x)P_1(x) + \cdots + A_s(x)P_s(x) = 1$$

for some $A_1(x), \dots, A_s(x) \in \mathbb{Q}[x]$. Then δ can be taken to be the right-hand side of the identity obtained by clearing the denominators of the coefficients of the $A_i(x)$: for some $B_1(x), \dots, B_s(x) \in \mathbb{Z}[x]$, we have $B_1(x)P_1(x) + \cdots + B_s(x)P_s(x) = \delta \in \mathbb{Z}$.

Example 2.2. Theorem 2.1 is false for non coprime polynomials. Let $P(x) = 5(x^2-1)(x-1)$ and $Q(x) = (x^2-1)x^2$. Then $\mathcal{D}$ is an infinite set (because $d_n = \gcd(P(n), Q(n)) \geqslant |n^2-1|$ tends to infinity as $n \to +\infty$). The set $\mathcal{D}$ is not stable by gcd: for instance $d_2 = 3 \in \mathcal{D}$ and $d_6 = 8 \in \mathcal{D}$, but $1 \notin \mathcal{D}$ (by contradiction, suppose that for some $n \in \mathbb{Z}$ we have $d_n = 1$, then $|n^2 - 1| = 1$, so $n = 0$, but for $n = 0$, $P(n) = 5$, $Q(n) = 0$ and $d_n = 5$). Neither $\mathcal{D}$ is stable by lcm: $5 \in \mathcal{D}$, $8 \in \mathcal{D}$ but $40 \notin \mathcal{D}$ (for $|n| < 7$ we have $d_n \neq 40$ and for $|n| \geqslant 7$, $d_n \geqslant |n^2 - 1| > 40$).

2.2. **Proof of Theorem 2.1.** Everything in Theorem 2.1 is proved in [2], except the stability under lcm that was left to the reader (after the proof for the gcd was given). For completeness we detail it here.

Let d_{n_1} and d_{n_2} be two elements of $\mathcal{D}$ and let $m(n_1, n_2)$ be their lcm. The goal is to prove that $m(n_1, n_2)$ is an element of $\mathcal{D}$. The integer $m(n_1, n_2)$ can be factorized:

$$m(n_1, n_2) = \prod_{i\in I} p_i^{\alpha_i}$$

where, for each $i \in I$, p_i is a prime divisor of δ (see Theorem 2.1) and $\alpha_i \in \mathbb{N}$ (maybe $\alpha_i = 0$ for some $i \in I$).

Fix $i \in I$. As $p_i^{\alpha_i}$ divides $m(n_1, n_2)$, then $p_i^{\alpha_i}$ divides d_{n_1} or divides d_{n_2}; say that $p_i^{\alpha_i}$ divides d_{m_i} with m_i equals n_1 or n_2.

The Chinese Remainder Theorem provides an integer n, such that

$$n = m_i \pmod{p_i^{\alpha_i+1}} \quad \text{for each } i \in I.$$

By definition, $p_i^{\alpha_i}$ divides d_{n_1} or d_{n_2}, so $p_i^{\alpha_i}$ divides all integers $P_1(n_1), \dots, P_s(n_1)$, or divides all integers $P_1(n_2), \dots, P_s(n_2)$, so that $p_i^{\alpha_i}$ divides all $P_1(m_i), \dots, P_s(m_i)$. As for each $j = 1, \dots, s$, $P_j(n) = P_j(m_i) \pmod{p_i^{\alpha_i}}$, we obtain that $p_i^{\alpha_i}$ also divides $P_1(n), \dots, P_s(n)$. Whence $p_i^{\alpha_i}$ divides d_n for each $i \in I$.

On the other hand $p_i^{\alpha_i+1}$ does not divide d_{n_1} nor d_{n_2}. In particular $p_i^{\alpha_i+1}$ does not divide d_{m_i}. Hence there exists $j_0 \in \{1, \dots, s\}$ such that $p_i^{\alpha_i+1}$ does not divide $P_{j_0}(m_i)$. As $P_{j_0}(n) = P_{j_0}(m_i) \pmod{p_i^{\alpha_i+1}}$, then $p_i^{\alpha_i+1}$ does not divide $P_{j_0}(n)$. Hence $p_i^{\alpha_i+1}$ does not divide d_n.

We have proved that $p_i^{\alpha_i}$ is the greatest power of p_i dividing d_n, for every $i \in I$. As d_n divides δ, each prime factor of d_n is one of the p_i with $i \in I$. Conclude that $m(n_1, n_2) = d_n$.

2.3. **Ekedahl–Poonen density formula in one variable.** One main question is to decide if $d_n = 1$ for some value $n \in \mathbb{Z}$. In Section 1.3, we discussed the Ekedahl–Poonen density formula for any number r of variables. For $r = 1$, it is an exact formula.

Proposition 2.3. *Let $P_1(x), \dots, P_s(x) \in \mathbb{Z}[x]$ be nonzero coprime polynomials. Let $\delta \in \mathbb{Z}$ be a positive period of $(d_n)_{n\in\mathbb{Z}}$. The number of $n \in \mathbb{Z}$ with $0 \leqslant n < \delta$ such that $d_n = 1$ is*

$$\delta \prod_{p|\delta} \left(1 - \frac{c_p}{p}\right)$$

where c_p is the number of $n \in \mathbb{Z}/p\mathbb{Z}$ such that $P_i(n) = 0 \pmod p$ for each $i = 1, \dots, s$.

Note that, *in the one variable case, $c_p = 0$ for all sufficiently large primes p.* Namely let δ be a nonzero element of the ideal $\langle P_1, \dots, P_s\rangle \cap \mathbb{Z} \subset \mathbb{Z}[\underline{x}]$. Thus δ is of the form $\delta = B_1(x)P_1(x) + \cdots + B_s(x)P_s(x)$ for some $B_1, \dots, B_s \in \mathbb{Z}[\underline{x}]$. Clearly, if p does not divide δ, then p does not divide $\gcd(P_1(n), \dots, P_s(n))$ for any $n \in \mathbb{Z}$, hence $c_p = 0$.

The *proof of Proposition 2.3 assuming Theorem 1.5* easily follows. For $r = 1$, the density formula from Theorem 1.5 is a finite product: $\mu(\mathcal{R}) = \prod_{p|\delta}\left(1 - \frac{c_p}{p}\right)$. As the sequence $(d_n)_{n\in\mathbb{Z}}$ is periodic of period δ (Theorem 2.1), the claimed exact formula follows, for δ equal to the specific element of $\mathbb{Z}$ introduced above, or equal to any positive period.

Example 2.4. For two polynomials we recover a formula of [5]: *If $P(x), Q(x) \in \mathbb{Z}[x]$ are two monic coprime polynomials with a square-free resultant R, then*

$$\#\left\{n \in [\![0, R-1]\!] \mid d_n = 1\right\} = \prod_{p|R}(p-1).$$

In fact, for two polynomials, the integer δ can be chosen to be R. And if R is square-free, then $c_p = 1$ for all $p|R$ (see [5, proof of Theorem 6]).

3. A Bertini–Noether–Ostrowski property for coprimality

Proposition 3.1 below is of frequent use in this paper. It explains how coprimality of polynomials is preserved by specialization. It is obtained in Section 3.3 as a special case of Proposition 3.2, which is an analog for coprimality of the Bertini–Noether theorem for irreducibility of polynomials (e.g. [6, Prop.9.4.3]). This more general result is stated and proved in Section 3.2. Section 3.4 shows another standard special case concerned with reduction modulo p (Corollary 3.4), which will be used later in the proof of Corollary 6.1.

3.1. Specialization and coprimality.

Proposition 3.1. *Let k be an infinite field and $P_1(\underline{a}, \underline{x}), \dots, P_s(\underline{a}, \underline{x}) \in k[\underline{a}, \underline{x}]$ be polynomials in the variables $\underline{a} = (a_1, \dots, a_m)$ and $\underline{x} = (x_1, \dots, x_r)$ (with $s \geqslant 2$, $m \geqslant 1$, $r \geqslant 1$). The following conditions are equivalent:*

- (i) *The gcd of $P_1(\underline{a}, \underline{x}), \dots, P_s(\underline{a}, \underline{x}) \in k[\underline{a}, \underline{x}]$ is in $k[\underline{a}]$.*
- (ii) *The polynomials $P_1(\underline{a}, \underline{x}), \dots, P_s(\underline{a}, \underline{x}) \in k[\underline{a}, \underline{x}]$ are coprime in $k(\underline{a})[\underline{x}]$.*
- (iii) *There exists a proper Zariski-closed subset Z of k^m such that for all $\underline{a}^\star \in k^m \setminus Z$, the polynomials $P_1(\underline{a}^\star, \underline{x}), \dots, P_s(\underline{a}^\star, \underline{x})$ are coprime in $k[\underline{x}]$.*
- (iv) *There exists a Zariski-dense subset Y of k^m such that for all $\underline{a}^\star \in Y$, the polynomials $P_1(\underline{a}^\star, \underline{x}), \dots, P_s(\underline{a}^\star, \underline{x})$ are coprime in $k[\underline{x}]$.*

3.2. **Coprimality and reduction.** Given an integral domain Z and an ideal $\mathfrak{p} \subset Z$, we denote by $\overline{z}^{\mathfrak{p}}$ the coset of an element $z \in Z$ modulo $\mathfrak{p}$; we use the same notation for the induced reduction morphisms, e.g. on polynomial rings over Z. If $\mathfrak{p} \subset Z$ is a prime ideal, we write $k^{\mathfrak{p}}$ for the fraction field of the integral domain $Z/\mathfrak{p}$.

Proposition 3.2. *Let Z be a Unique Factorization Domain (UFD) with fraction field Q, let $\underline{x} = (x_1, \ldots, x_r)$ be $r \geqslant 1$ variables and let $P_1(\underline{x}), \ldots, P_s(\underline{x}) \in Z[\underline{x}]$ be $s \geqslant 2$ nonzero polynomials. Suppose also given a Zariski-dense subset $\mathcal{P} \subset \operatorname{Spec} Z$ [1]. Then the following five conditions are equivalent:*

(i) *The gcd in $Z[\underline{x}]$ of $P_1(\underline{x}), \ldots, P_s(\underline{x})$ is in Z.*
(ii) *$P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime in $Q[\underline{x}]$.*
(iii) *There is a nonzero element $R_0 \in Z$ with this property: for every prime ideal $\mathfrak{p} \subset Z$ such that $\overline{R_0}^{\mathfrak{p}} \neq 0$, the polynomials $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(\underline{x})$ are coprime in $k^{\mathfrak{p}}[\underline{x}]$.*
(iv) *For every nonzero element $R \in Z$, there exists a prime ideal $\mathfrak{p} \in \mathcal{P}$ such that $\overline{R}^{\mathfrak{p}} \neq 0$ and the polynomials $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(\underline{x})$ are coprime in $k^{\mathfrak{p}}[\underline{x}]$.*
(v) *For every nonzero element $R \in Z$, there exists a maximal ideal $\mathfrak{p} \subset Z$ such that $\overline{R}^{\mathfrak{p}} \neq 0$ and the polynomials $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(\underline{x})$ are coprime in $k^{\mathfrak{p}}[\underline{x}]$.*

Proof of Proposition 3.2. (ii) $\implies$ (i). Assume on the contrary that the gcd, say $D(\underline{x}) \in Z[\underline{x}]$, of $P_1(\underline{x}), \ldots, P_s(\underline{x})$ is not in Z. Then $D(\underline{x})$ is of degree $\geqslant 1$ (so not a unit of $Q[\underline{x}]$) and is a common divisor of $P_1(\underline{x}), \ldots, P_s(\underline{x})$ in $Q[\underline{x}]$. This contradicts (ii).

(i) $\implies$ (ii). Assume on the contrary that $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are not coprime in $Q[\underline{x}]$, i.e., a nonconstant polynomial $D(\underline{x}) \in Q[\underline{x}]$ divides all $P_i(\underline{x})$ in $Q[\underline{x}]$. We may assume that D is in $Z[\underline{x}]$, and even, using that $Z[\underline{x}]$ is a UFD, that D is irreducible in $Z[\underline{x}]$. Write $P_i(\underline{x}) = D(\underline{x})P_i'(\underline{x})$ with $P_i' \in Q[\underline{x}]$, $i = 1, \ldots, s$. Clearing the denominators, one obtains polynomial equalities in $Z[\underline{x}]$: $q_i P_i(\underline{x}) = D(\underline{x})\tilde{P}_i'(\underline{x})$, with $\tilde{P}_i' \in Z[\underline{x}]$ and $q_i \in Z$, $q_i \neq 0$, $i = 1, \ldots, s$. It follows that q_i divides $\tilde{P}_i'$ in $Z[\underline{x}]$, $i = 1, \ldots, s$, and so that D is a common divisor in $Z[\underline{x}]$ of all the $P_i(\underline{x})$. This contradicts (i).

Remark 3.3. (a) The equivalence (i) $\Leftrightarrow$ (ii) has this close variant:

$P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime polynomials in $Z[\underline{x}]$ if and only if the equivalent conditions (i), (ii) *hold <u>and</u> the coefficients of $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime in Z.*

Indeed, if $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime in $Z[\underline{x}]$, they are coprime in $Q[\underline{x}]$ (by (i) $\Rightarrow$ (ii)), and obviously, the coefficients of $P_1(\underline{x}), \ldots, P_s(\underline{x})$ must be coprime in Z. Conversely, if $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime in $Q[\underline{x}]$ and their coefficients are coprime in Z, then their gcd in $Z[\underline{x}]$ is in Z (by (ii) $\Rightarrow$ (i)), so must necessarily be 1.

(iii) $\implies$ (iv). For a given nonzero element $R \in Z$, let $\mathfrak{p} \in \mathcal{P}$ be a prime ideal such that $\overline{RR_0}^{\mathfrak{p}} \neq 0$, where $R_0 \in Z$ is the nonzero element given by (iii); such a $\mathfrak{p}$ exists as $\mathcal{P}$ is assumed to be Zariski-dense. Then $\overline{R}^{\mathfrak{p}} \neq 0$ and $\overline{R_0}^{\mathfrak{p}} \neq 0$, and by (iii), the latter gives that $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(\underline{x})$ are coprime in $k^{\mathfrak{p}}[\underline{x}]$.

(iv) $\implies$ (i). Assume that the gcd, say $D(\underline{x}) \in Z[\underline{x}]$, of $P_1(\underline{x}), \ldots, P_s(\underline{x})$ is a polynomial of degree $\geqslant 1$. Let $R \in Z$ be a nonzero coefficient of a monomial of degree $\geqslant 1$ of $D(\underline{x})$.

[1] The subset $\mathcal{P} \subset \operatorname{Spec} Z$ only appears in condition (iv) below. The assumption that $\mathcal{P}$ is Zariski-dense means that for every nonzero element $R \in Z$, there is a prime ideal $\mathfrak{p} \in \mathcal{P}$ such that $\overline{R}^{\mathfrak{p}} \neq 0$. This is clearly necessary for (iv) to hold. In fact (iv) reformulates as saying that, with $\mathcal{C} \subset \operatorname{Spec} Z$ the set of primes $\mathfrak{p}$ such that $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(\underline{x})$ are coprime in $k^{\mathfrak{p}}[\underline{x}]$, the set $\mathcal{C} \cap \mathcal{P}$ is Zariski-dense in $\operatorname{Spec} Z$. In the same vein, condition (iii) means that $\mathcal{C}$ contains a nonempty Zariski-open subset of $\operatorname{Spec} Z$.

Then for every prime ideal $\mathfrak{p} \in \mathcal{P}$ such that $\overline{R}^{\mathfrak{p}} \neq 0$, the reduced polynomial $\overline{D}^{\mathfrak{p}}(\underline{x})$ is of degree $\geqslant 1$ and is a common divisor of $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(\underline{x})$ in $k^{\mathfrak{p}}[\underline{x}]$. This contradicts (iv).

(ii) $\implies$ (iii). We proceed by induction on the number of variables $r \geqslant 1$.
1st case: $r = 1$, i.e. $\underline{x}$ is a single variable x. The assumption (ii) that the polynomials $P_1(x), \ldots, P_s(x)$ are coprime in the Principal Ideal Domain (PID) $Q[x]$ provides a Bézout identity, which after clearing the denominators, is of this form:

$$\sum_{i=1}^{s} A_i(x)P_i(x) = R_0$$

with $A_1, \ldots, A_s \in Z[x]$ and $R_0 \in Z, R_0 \neq 0$.
Clearly then, for every prime ideal $\mathfrak{p} \subset Z$ such that $\overline{R_0}^{\mathfrak{p}} \neq 0$, the reduced polynomials $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(x)$ satisfy a Bézout identity in the PID $k^{\mathfrak{p}}[x]$, hence are coprime in $k^{\mathfrak{p}}[x]$.

2nd case: $r \geqslant 2$. Let $\underline{x} = (x_1, \ldots, x_{r-1}, x_r)$ and assume that (ii) $\Rightarrow$ (iii) is true for polynomials in the $r-1$ variables $(x_1, \ldots, x_{r-1})$. We will apply the induction hypothesis to the set of all coefficients $P_{i,j}(x_1, \ldots, x_{r-1})$ of the polynomials $P_i(x_1, \ldots, x_r)$ viewed as polynomials in x_r.
The polynomials $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are supposed to be coprime in $Q[x_1, \ldots, x_r]$. Thus, by the already proven implication (i) $\Rightarrow$ (ii) (applied with Z being $Q[x_1, \ldots, x_{r-1}]$), they are coprime in $Q(x_1, \ldots, x_{r-1})[x_r]$, and their coefficients $P_{i,j}(x_1, \ldots, x_{r-1})$ are coprime in $Q[x_1, \ldots, x_{r-1}]$. The former condition provides a Bézout identity, which after clearing the denominators, is of this form:

$$\sum_{i=1}^{s} A_i(\underline{x})P_i(\underline{x}) = \Delta(x_1, \ldots, x_{r-1})$$

with $A_1, \ldots, A_s \in Z[\underline{x}]$ and $\Delta \in Z[x_1, \ldots, x_{r-1}]$, $\Delta \neq 0$. Let $R_1 \in Z$ be a nonzero coefficient of a monomial of Δ. For every prime ideal $\mathfrak{p} \subset I$ such that $\overline{R_1}^{\mathfrak{p}} \neq 0$, the polynomial $\overline{\Delta}^{\mathfrak{p}}(\underline{x})$ is nonzero in $k^{\mathfrak{p}}[x_1, \ldots, x_{r-1}]$, and so, the polynomials $\overline{P_1}^{\mathfrak{p}}(\underline{x}), \ldots, \overline{P_s}^{\mathfrak{p}}(\underline{x})$ are coprime in $k^{\mathfrak{p}}(x_1, \ldots, x_{r-1})[x_r]$.
Furthermore, as the coefficients $P_{i,j}(x_1, \ldots, x_{r-1})$ are coprime in $Q[x_1, \ldots, x_{r-1}]$, the induction hypothesis provides a nonzero element $R_2 \in Z$ such that for every prime ideal $\mathfrak{p} \subset I$ such that $\overline{R_2}^{\mathfrak{p}} \neq 0$, the polynomials $\overline{P_{i,j}}^{\mathfrak{p}}(x_1, \ldots, x_{r-1})$ are coprime in $k^{\mathfrak{p}}[x_1, \ldots, x_{r-1}]$.
Using the already proven implication (ii) $\Rightarrow$ (i) (more exactly its variant from Remark 3.3), it follows that the element $R_0 = R_1R_2$ satisfies the requested conclusion (iii).

Equivalence of (v) *with all other conditions.* This follows from the fact that (v) is the special case of (iv) for which $\mathcal{P}$ is the set of all maximal ideals of Z. This subset $\mathcal{P} \subset \operatorname{Spec} Z$ is indeed Zariski-dense: as Z is an integral domain, the nilradical $\mathrm{nil}(Z)$ (consisting of all nilpotent elements of Z) is $\{0\}$. But $\mathrm{nil}(Z)$ is classically the intersection of all maximal ideals of Z. Thus if $R \in Z$, $R \neq 0$, there is a prime ideal $\mathfrak{p} \in \mathcal{P}$ such that $\overline{R}^{\mathfrak{p}} \neq 0$ (which is the definition of $\mathcal{P}$ being Zariski-dense in $\operatorname{Spec} Z$). □

3.3. **Proof of Proposition 3.1.** Proposition 3.1 corresponds to the special case of Proposition 3.2 for which $Z = k[\underline{a}]$ is a polynomial ring in $m \geqslant 1$ variables $\underline{a} = (a_1, \ldots, a_m)$ over a field k. Equivalence (i) $\Leftrightarrow$ (ii) from Proposition 3.2 exactly yields equivalence (i) $\Leftrightarrow$ (ii) from Proposition 3.1 in this special case; the field k need not be infinite here.

Assume now that k is infinite and take for $\mathcal{P}$ the set of maximal ideals of the form $\langle \underline{a}-\underline{a}^\star\rangle = \langle a_1-a_1^\star,\dots,a_r-a_r^\star\rangle$ with $\underline{a}^\star \in k^m$. With k infinite, the subset $\mathcal{P} = \mathbb{A}^n(k)$ is indeed Zariski-dense. Condition (iv) from Proposition 3.2 then yields condition (iv) from Proposition 3.1. Finally note that condition (iii) from Proposition 3.2 implies condition (iii) from Proposition 3.1, which itself implies condition (iv) from Proposition 3.2, and so all three conditions are equivalent, thus ending the proof of Proposition 3.1.

3.4. **The Ostrowski corollary.** For $Z = \mathbb{Z}$, Proposition 3.2 yields the following result, which is the coprimality analog of the Ostrowski theorem for irreducibility.

Corollary 3.4. *Let $P_1(\underline{x}),\dots,P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be $s \geqslant 2$ nonzero polynomials. The following four conditions are equivalent.*

(i) *The gcd of the polynomials $P_1(\underline{x}),\dots,P_s(\underline{x})$ is in $\mathbb{Z}$.*
(ii) *The polynomials $P_1(\underline{x}),\dots,P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ are coprime in $\mathbb{Q}[\underline{x}]$.*
(iii) *For all but finitely many primes $p \in \mathbb{Z}$, $\overline{P_1}^p(\underline{x}),\dots,\overline{P_s}^p(\underline{x})$ are coprime in $\mathbb{Z}/p\mathbb{Z}[\underline{x}]$.*
(iv) *For infinitely many primes $p \in \mathbb{Z}$, $\overline{P_1}^p(\underline{x}),\dots,\overline{P_s}^p(\underline{x})$ are coprime in $\mathbb{Z}/p\mathbb{Z}[\underline{x}]$.*

Example 3.5. How big should a prime number p be to guarantee that two polynomials in $\mathbb{Z}[\underline{x}]$ that are coprime in $\mathbb{Q}[\underline{x}]$ remain coprime modulo p? In the one variable case, it suffices that the prime p does not divide the resultant of the two polynomials (which can be quite large). Here is an example in two variables. Let $P(x,y) = x^3y-3x^3-2x+3y+2$ and $Q(x,y) = y(2x-11)$. These polynomials are coprime in $\mathbb{Z}[x,y]$. For $p = 5$, the gcd of P and Q modulo 5 is $x+2$. For $p = 271$, the gcd of P and Q modulo 271 is $x+130$. Experimentation shows that for other values of p, P and Q are coprime modulo p.

4. Further tools

We prove some more tools needed to establish the stability result in the next section.

Lemma 4.1. *Let $P_1(\underline{x}),\dots,P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be nonzero coprime polynomials in $r \geqslant 2$ variables. Suppose that $P_i(\underline{0}) \neq 0$ for at least one $i \in \{1,\dots,s\}$. Then the polynomials $P_1(t\underline{a}),\dots,P_s(t\underline{a})$ are coprime in $\mathbb{Q}[\underline{a},t]$. Consequently there is a proper Zariski-closed subset $Z \subset \mathbb{Z}^r$ such that, for all $\underline{a}^\star \in \mathbb{Z}^r \setminus Z$, the polynomials $P_1(t\underline{a}^\star),\dots,P_s(t\underline{a}^\star)$ are coprime in $\mathbb{Q}[t]$.*

This is false if $P_1,\dots,P_s$ vanish simultaneously at $\underline{0}$. For instance, with $P(x,y) = x$ and $Q(x,y) = y$, then $P(at,bt) = at$ and $Q(at,bt) = bt$ are not coprime, for any $(a,b) \in \mathbb{Z}^2$.

Corollary 4.2. *Let $P_1(\underline{x}),\dots,P_s(\underline{x})$ be $s \geqslant 2$ nonzero coprime polynomials. If $d_{\underline{n}_0} = 1$ for some $\underline{n}_0 \in \mathbb{Z}^r$, then $d_{\underline{n}} = 1$ for every $\underline{n}$ in a Zariski-dense subset of $\mathbb{Z}^r$.*

Proof of Corollary 4.2. With no loss of generality, assume that $\underline{n}_0 = \underline{0}$. By Lemma 4.1, for all directions $\underline{a}^\star$ in a Zariski-open set of $\mathbb{Q}^r$, the one variable polynomials $P_1(t\underline{a}^\star),\dots,P_s(t\underline{a}^\star)$ are coprime. From Theorem 2.1, for each of these $\underline{a}^\star$, we have $\gcd_i P_i(k\underline{a}^\star) = \gcd_i P_i(\underline{0}) = 1$ for all k in some nonzero ideal $\delta\mathbb{Z} \subset \mathbb{Z}$. The set of all such $k\underline{a}^\star \in \mathbb{Z}^r$, with varying k and $a^\star$, form a Zariski-dense subset of $\mathbb{Z}^r$. □

Proof of Lemma 4.1. We prove the first part; the second part easily follows by combining it with Proposition 3.1. On the contrary, suppose that $P_i(t\underline{a}) = D(\underline{a},t)\cdot P_i'(\underline{a},t)$, $(i = 1,\dots,s)$ with $\deg D > 0$. If $\deg_t(D) = 0$, then setting $t = 1$ leads to a factorization $P_i(\underline{a}) = D(\underline{a},1)\cdot P_i'(\underline{a},1)$ where $\deg D(\underline{a},1) > 0$; changing the variable $\underline{a}$ to $\underline{x}$ proves that the polynomials $P_i(\underline{x})$ are not coprime.

Suppose next that $\deg_t D(\underline{a},t) > 0$. One may assume that $\deg_t D(a_1^\star, a_2, \dots, a_r, t) > 0$ for some $a_1^\star \in k$. For simplicity take $a_1^\star = 1$ (the general case only introduces some technicalities). Set $\underline{a}' = (1, a_2, \dots, a_r)$ and write the decomposition in $\mathbb{Q}[\underline{a}', t]$:

$$P_i(t\underline{a}') = D(\underline{a}', t) \cdot P_i'(\underline{a}', t) \quad (i = 1, \dots, s)$$

with $\deg D(\underline{a}', t) > 0$.
Set $\underline{x} = t\underline{a}'$, that is, $x_i = a_i t$ (and $x_1 = t$); hence $a_i = x_i/x_1$ (and $a_1 = 1$), $i = 1, \dots, r$. Using the change of variables $(\underline{a}', t) \mapsto \underline{x}$, we obtain:

$$P_i(\underline{x}) = D\left(\frac{\underline{x}}{x_1}, x_1\right) \cdot P_i'\left(\frac{\underline{x}}{x_1}, x_1\right) \quad (i = 1, \dots, s).$$

By hypothesis we have $P_{i_0}(\underline{0}) \neq 0$ for some $i_0 \in \{1, \dots, s\}$. This is equivalent to $t \not| P_{i_0}(t\underline{a}')$ and implies $t \not| D(\underline{a}', t)$ in $\mathbb{Q}[\underline{a}', t]$.
Write

$$D(\underline{a}', t) = \sum_{\underline{i}, j} \alpha_{\underline{i}, j} \underline{a}'^{\underline{i}} t^j \qquad \text{in } \mathbb{Q}[a_2, \dots, a_r, t].$$

As $a_1 = 1$, the multi-index $\underline{i}$ stands for $(0, i_2, \dots, i_r)$ and $|\underline{i}| = i_2 + \dots + i_r$. Then

$$\begin{aligned} D\left(\frac{\underline{x}}{x_1}, x_1\right) &= \sum_{\underline{i}, j} \alpha_{\underline{i}, j} \left(\frac{\underline{x}^{\underline{i}}}{x_1^{|\underline{i}|}}\right) x_1^j = \sum_{\underline{i}, j} \alpha_{\underline{i}, j} \underline{x}^{\underline{i}} x_1^{j - |\underline{i}|} \\ &= \frac{1}{x_1^d} \sum_{\underline{i}, j} \alpha_{\underline{i}, j} \underline{x}^{\underline{i}} x_1^{j - |\underline{i}| + d} = \frac{1}{x_1^d} \tilde{D}(\underline{x}) \end{aligned}$$

where $d \in \mathbb{Z}$, and $\tilde{D}(\underline{x}) \in \mathbb{Q}[\underline{x}]$ is not divisible by x_1. A similar computation yields $P_i'\left(\frac{\underline{x}}{x_1}, x_1\right) = \frac{1}{x_1^{d_i}} \tilde{P}_i'(\underline{x})$ with $d_i \in \mathbb{Z}$, and $\tilde{P}_i'(\underline{x}) \in \mathbb{Q}[\underline{x}]$ not divisible by x_1. This gives:

$$x_1^{d + d_i} P_i(\underline{x}) = \tilde{D}(\underline{x}) \tilde{P}_i'(\underline{x}) \quad (i = 1, \dots, s).$$

By definition $\tilde{D}(\underline{x})$ is not a monomial in x_1. Moreover $\tilde{D}(\underline{x})$ is a nonconstant polynomial. Assume on the contrary that $\tilde{D}(\underline{x})$ is constant. Then $\alpha_{\underline{i}, j} = 0$ for $(\underline{i}, j) \neq (\underline{0}, d)$. This implies $D(\underline{a}', t) = \alpha_{\underline{0}, d} t^d$, in contradiction with $t \not| D(\underline{a}', t)$ and $\deg D(\underline{a}', t) > 0$. Conclusion: $\tilde{D}(\underline{x})$ is a non trivial factor of each of the $P_i(\underline{x})$, hence $P_1(\underline{x}), \dots, P_s(\underline{x})$ are not coprime. □

We end by a generalization of Lemma 4.1. Let $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be a family of coprime polynomials in two or more variables ($r \geqslant 2$).

Lemma 4.3. *Let $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$ be nonzero coprime polynomials in $r \geqslant 2$ variables. Let $\underline{n} \in \mathbb{Z}^r$ such that $P_i(\underline{n}) \neq 0$ for at least one $i \in \{1, \dots, s\}$. Then the polynomials $P_1(u\underline{n} + t\underline{a}), \dots, P_s(u\underline{n} + t\underline{a})$ are coprime in $\mathbb{Q}[\underline{a}, u, t]$. Consequently there is a proper Zariski-closed set $Z \subset \mathbb{Z}^r$ such that for all $\underline{a}^\star \in \mathbb{Z}^r \setminus Z$, the polynomials $P_1(u\underline{n} + t\underline{a}^\star), \dots, P_s(u\underline{n} + t\underline{a}^\star)$ are coprime in $\mathbb{Q}[u, t]$.*

Proof. For every $u^\star \in \mathbb{Q}$, the polynomials $\tilde{P}_i(\underline{x}) := P_i(u^\star \underline{n} + \underline{x})$, $i = 1, \dots, s$, are coprime in $\mathbb{Q}[\underline{x}]$ (they are deduced from the $P_i(\underline{x})$ by a mere translation on the variables). As $P_i(\underline{n}) \neq 0$ for some i, then $\tilde{P}_i(\underline{0}) = P_i(u^\star \underline{n}) \neq 0$ for all but finitely many $u^\star \in \mathbb{Q}$. By Lemma 4.1, for such $u^\star$, the polynomials $\tilde{P}_1(t\underline{a}), \dots, \tilde{P}_s(t\underline{a})$ are coprime in $\mathbb{Q}[\underline{a}, t]$, hence so are the polynomials $P_1(u^\star \underline{n} + t\underline{a}), \dots, P_s(u^\star \underline{n} + t\underline{a})$. It follows from Proposition 3.1 that the polynomials $P_1(u\underline{n} + t\underline{a}), \dots, P_s(u\underline{n} + t\underline{a})$ are coprime in $\mathbb{Q}(u)[\underline{a}, t]$.

Assume next that their gcd in $\mathbb{Q}[u, \underline{a}, t]$ is a nonconstant polynomial $D(u) \in \mathbb{Q}[u]$. Thus we have $P_i(u\underline{n}+t\underline{a}) = D(u)P'_i(\underline{a}, u, t)$ for some $P'_i \in \mathbb{Q}[u, \underline{a}, t]$, $i = 1, \ldots, s$. Choose $t^\star = 1$ and $\underline{a}^\star(u) = -u\underline{n} + \underline{c}$, where $\underline{c}$ is a constant such that $P_i(\underline{c}) \neq 0$, for at least one $i \in \{1, \ldots, s\}$. For this choice, we have $P_i(u\underline{n} + t^\star \underline{a}^\star(u)) = P_i(\underline{c}) = D(u)P'_i(\underline{a}^\star(u), u, t^\star)$. As $P_i(\underline{c})$ is a nonzero constant, $D(u)$ is a constant polynomial.
By Remark 3.3(a), the polynomials $P_1(u\underline{n} + t\underline{a}), \ldots, P_s(u\underline{n} + t\underline{a})$ are coprime in $\mathbb{Q}[u][\underline{a}, t]$. This proves the first assertion of Lemma 4.3; the second one follows by combining it with Proposition 3.1. □

5. Proof of the stability

This section is devoted to the proof of Theorem 1.1.

Idea of the proof. Consider two coprime polynomials $P(x, y)$ and $Q(x, y)$ and the special case of two pairs (m, n_1) and (m, n_2) (with the same x-coordinate). We will find n_3 such that $\gcd(d_{m,n_1}, d_{m,n_2}) = d_{m,n_3}$. As $P(x, y)$ and $Q(x, y)$ are coprime and by Bézout, there exist $A(x), B(x), R(x) \in \mathbb{Z}[x]$ such that:

$$A(x)P(x, y) + B(x)Q(x, y) = R(x).$$

For all $m \in \mathbb{Z}$ but finitely many, we have $R(m) \neq 0$. For such m, $P(m, y)$ and $Q(m, y)$ are coprime (in $\mathbb{Q}[y]$). By the gcd stability result in one variable (Theorem 2.1), there exists n_3 such that $\gcd(d_{m,n_1}, d_{m,n_2}) = d_{m,n_3}$.

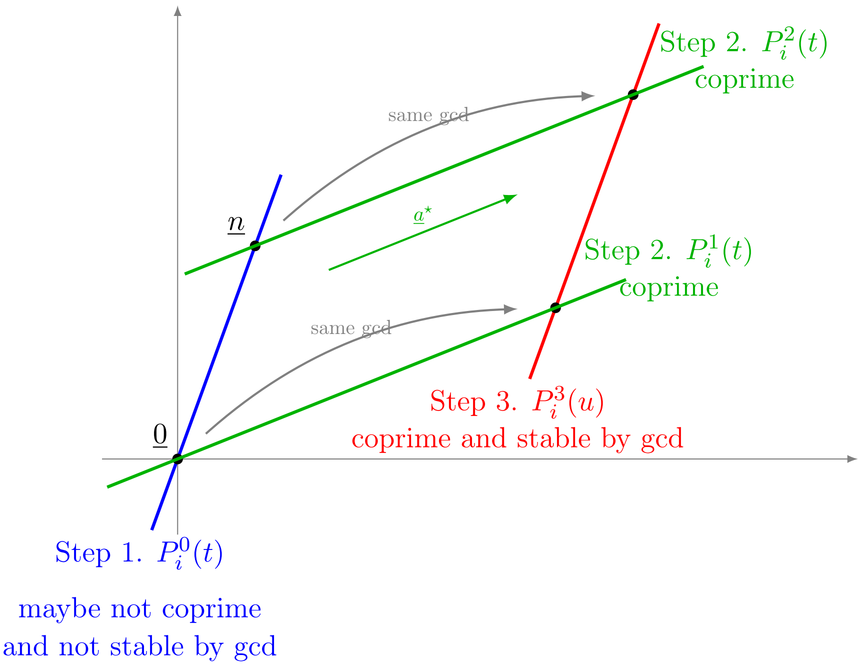
The proof extends this idea: we need (a) to deal with the case where $P(m, y)$ and $Q(m, y)$ are no longer coprime; (b) also consider pairs (m_1, n_1) and (m_2, n_2) with $m_1 \neq m_2$.

Step 1. Let $\underline{m} \in \mathbb{Z}^r$ and $\underline{n} \in \mathbb{Z}^r$. For simplicity, and with no loss of generality, we assume $\underline{m} = \underline{0}$. We may also assume that $P_i(\underline{0}) \neq 0$ for at least one $i \in \{1, \ldots, s\}$: otherwise $d_{\underline{0}} = 0$ so that we can directly conclude $\gcd(d_{\underline{0}}, d_{\underline{n}}) = d_{\underline{n}}$. We may also assume that $P_i(\underline{n}) \neq 0$ for at least one $i \in \{1, \ldots, s\}$. We reduce from several to one variables by restricting the polynomials on the line passing through $\underline{0}$ and $\underline{n}$. That is, we set:

$$P_i^0(t) = P_i(t\underline{n}), \qquad i = 1, \ldots, s.$$

Then $P_i^0(0) = P_i(\underline{0})$ and $P_i^0(1) = P_i(\underline{n})$. However the polynomials $P_1^0(t), \ldots, P_s^0(t)$ are not necessarily coprime. The following picture helps visualize the next steps of the proof.

Picture of the proof.



Step 2. By Lemma 4.1, for all $\underline{a}^\star \in \mathbb{Z}^r$ but in a proper Zariski-closed set, the polynomials $P_1(t\underline{a}^\star), \dots, P_s(t\underline{a}^\star)$ are coprime in $\mathbb{Q}[t]$. Moreover, again by Lemma 4.1 centered at $\underline{n}$, for all $\underline{a}^\star \in \mathbb{Z}^r$ but in a proper Zariski-closed set, the polynomials $P_1(\underline{n}+t\underline{a}^\star), \dots, P_s(\underline{n}+t\underline{a}^\star)$ are coprime in $\mathbb{Q}[t]$. Finally by Lemma 4.3, for all $\underline{a}^\star \in \mathbb{Z}^r$ but in a proper Zariski-closed set, the polynomials $P_1(u\underline{n}+t\underline{a}^\star), \dots, P_s(u\underline{n}+t\underline{a}^\star)$ are coprime in $\mathbb{Q}[u,t]$.
Pick $\underline{a}^\star \in \mathbb{Z}^r$ such that the following conditions are satisfied:

- $P_i^1(t) := P_i(t\underline{a}^\star)$, $i = 1, \dots, s$, are coprime in $\mathbb{Q}[t]$,
- $P_i^2(t) := P_i(\underline{n}+t\underline{a}^\star)$, $i = 1, \dots, s$, are coprime in $\mathbb{Q}[t]$,
- $P_i(u\underline{n}+t\underline{a}^\star)$, $i = 1, \dots, s$, are coprime in $\mathbb{Q}[u,t]$.

In the computations below, all gcds are computed with respect to the indices $i = 1, \dots, s$. By the one variable case for $P_1^1(t), \dots, P_s^1(t)$, the corresponding sequence of gcd is periodic, for some (nonzero) period $\delta_1 \in \mathbb{Z}$ (Theorem 2.1). This yields that for any $k \in \mathbb{Z}$, we have $\gcd P_i^1(0) = \gcd P_i^1(0 + k\delta_1)$, and so

$$d_{\underline{0}} = \gcd P_i(\underline{0}) = \gcd P_i(k\delta_1\underline{a}^\star).$$

We do the same for $P_i^2(t)$. For some period $\delta_2 \in \mathbb{Z}$, for any $k \in \mathbb{Z}$, we have $\gcd P_i^2(0) = \gcd P_i^2(0 + k\delta_2)$, and so

$$d_{\underline{n}} = \gcd P_i(\underline{n}) = \gcd P_i(\underline{n} + k\delta_2\underline{a}^\star).$$

We also have $P_1(u\underline{n}+t\underline{a}^\star), \dots, P_s(u\underline{n}+t\underline{a}^\star)$ coprime in $\mathbb{Q}[u,t]$. Thus, by Proposition 3.1, for all but finitely many $t^\star \in \mathbb{Q}$, the polynomials $P_1(u\underline{n}+t^\star\underline{a}^\star), \dots, P_s(u\underline{n}+t^\star\underline{a}^\star)$ are coprime in $\mathbb{Q}[u]$.

Step 3. Set $t^\star = k\delta_1\delta_2$ with $k \in \mathbb{Z}$ and $P_i^3(u) := P_i(u\underline{n}+t^\star\underline{a}^\star)$, $i = 1, \dots, s$. Pick k large enough to guarantee that $P_1^3(u), \dots, P_s^3(u)$ are coprime in $\mathbb{Q}[u]$ (Proposition 3.1).
Note that

$$\gcd P_i^3(0) = \gcd P_i(t^\star\underline{a}^\star) = \gcd P_i(k\delta_1\delta_2\underline{a}^\star) = \gcd P_i(\underline{0}) = d_{\underline{0}}$$

and

$$\gcd P_i^3(1) = \gcd P_i(\underline{n}+t^\star\underline{a}^\star) = \gcd P_i(\underline{n}+k\delta_1\delta_2\underline{a}^\star) = \gcd P_i(\underline{n}) = d_{\underline{n}}.$$

Now by the gcd stability (resp. lcm stability) assertion from Theorem 2.1, applied to the one variable coprime polynomials $P_1^3(u), \dots, P_s^3(u)$, there exists $\ell \in \mathbb{Z}$ such that

$$\gcd\left(\gcd P_i^3(0), \gcd P_i^3(1)\right) = \gcd P_i^3(\ell)$$

(resp. $\operatorname{lcm}\left(\gcd P_i^3(0), \gcd P_i^3(1)\right) = \gcd P_i^3(\ell)$). Setting $\underline{m} = \ell \underline{n} + t^\star \underline{a}^\star$, so $P_i^3(\ell) = P_i(\underline{m})$, we obtain

$$\gcd\left(d_{\underline{0}}, d_{\underline{n}}\right) = d_{\underline{m}}$$

(resp. $\operatorname{lcm}\left(d_{\underline{0}}, d_{\underline{n}}\right) = d_{\underline{m}}$), which proves the stability of $\mathcal{D}$ by gcd (resp. lcm).

6. Proof of the Ekedahl–Poonen formula

This section is mainly devoted to the proof of the Ekedahl–Poonen formula as stated in Theorem 1.5. While [9, Theorem 3.1] is valid over the rings $\mathbb{Z}$ and $\mathbb{F}_q[t]$, here we state and prove Theorem 1.5 over $\mathbb{Z}$ only, which enables simplifications. Another simplification is that our density is defined by squared boxes, while [9] allows rectangular ones. Another difference (minor for the proof, but important for the applications) is that we allow any $s \geqslant 2$ polynomials (instead of 2). Finally in Section 6.7, we generalize the formula to the situation of *several families* of coprime polynomials (Proposition 6.3), and then use this generalization to extend the proof of Theorem 1.7 given in Section 1.4 for one polynomial to several polynomials.

6.1. Sets.

As usual, fix $s \geqslant 2$ nonzero polynomials $P_1(\underline{x}), \dots, P_s(\underline{x}) \in \mathbb{Z}[\underline{x}]$. In the following, p is a prime number, and $\mathcal{P}$ the set of prime numbers.
For $p \in \mathcal{P}$, consider the set:

$$\mathcal{R}_p = \left\{\underline{n} \in \mathbb{Z}^r \mid p \text{ does not divide all } P_1(\underline{n}), \dots, P_s(\underline{n})\right\}.$$

Then, with $\mathcal{R}$ the set (introduced in Section 1.3) of all $\underline{n} \in \mathbb{Z}^r$ such that $P_1(\underline{n}), \dots, P_s(\underline{n})$ are coprime, we have:

$$\mathcal{R} = \bigcap_{p \in \mathcal{P}} \mathcal{R}_p = \left\{\underline{n} \in \mathbb{Z}^r \mid \gcd(P_1(\underline{n}), \dots, P_s(\underline{n})) = 1\right\}.$$

We will approximate $\mathcal{R}$ by sets $\mathcal{R}_{\leqslant M}$ defined by:

$$\mathcal{R}_{\leqslant M} = \bigcap_{p \leqslant M} \mathcal{R}_p = \left\{\underline{n} \in \mathbb{Z}^r \mid \text{ for every } p \leqslant M, p \text{ does not divide all } P_1(\underline{n}), \dots, P_s(\underline{n})\right\}.$$

We will also work with:

$$\mathcal{Q}_p = \mathbb{Z}^r \setminus \mathcal{R}_p = \left\{\underline{n} \in \mathbb{Z}^r \mid p \text{ divides } P_1(\underline{n}), \dots, P_s(\underline{n})\right\} = \left\{\underline{n} \in \mathbb{Z}^r \mid p \text{ divides } \gcd_{1 \leqslant i \leqslant s} P_i(\underline{n})\right\}.$$

and

$$\begin{aligned} \mathcal{Q}_{>M} = \bigcup_{p > M} \mathcal{Q}_p &= \left\{\underline{n} \in \mathbb{Z}^r \mid \text{ there exists } p > M, p \text{ divides } P_1(\underline{n}), \dots, P_s(\underline{n})\right\} \\ &= \left\{\underline{n} \in \mathbb{Z}^r \mid \text{ there exists } p > M \text{ such that } p \text{ divides } \gcd_{1 \leqslant i \leqslant s} P_i(\underline{n})\right\}. \end{aligned}$$

Here are the main steps of the proof:

- Compute the density of $\mathcal{Q}_p$ (and $\mathcal{R}_p$) in terms of c_p.
- Prove that this density is in $O(\frac{1}{p^2})$.
- Compute the density of $\mathcal{R}_{\leqslant M}$ from $\mathcal{R}_p$, using the Chinese Remainder Theorem.
- Prove that $\mu(\mathcal{R}_{\leqslant M}) \xrightarrow[M \to +\infty]{} \mu(\mathcal{R})$.

For $r = 1$, the last step is not necessary since, following notation of Section 2.3, for $M \geqslant \delta$, we have $\mathcal{R}_{\leqslant M} = \mathcal{R}$.

6.2. **Density of $\mathcal{Q}_p$ and $\mathcal{R}_p$.** By definition, $\underline{n} \in \mathcal{Q}_p$ if and only if $P_i(\underline{n}) = 0 \pmod p$ for each $i = 1, \ldots, s$. Hence

$$\#(\mathcal{Q}_p \cap [\![0, p-1]\!]^r) = c_p \tag{1}$$

In fact, p divides $P_i(n_1, \ldots, n_r)$ if and only if p divides $P_i(n_1 + k_1 p, \ldots, n_r + k_r p)$ for any $k_j \in \mathbb{Z}$. Hence $\mathcal{Q}_p$ is invariant by any translation of vector $(k_1 p, \ldots, k_r p)$ (with $k_j \in \mathbb{Z}$). Hence, as a function of B, the cardinality $\#(\mathcal{Q}_p \cap \mathbb{B})$ (with $\mathbb{B} = [\![0, B-1]\!]^r$) is asymptotic to $c_p \left(\frac{B}{p}\right)^r$ as $B \to \infty$ (this formula is exact if p divides B).
Then:

$$\mu(\mathcal{Q}_p) = \lim_{B \to +\infty} \frac{\#(\mathcal{Q}_p \cap \mathbb{B})}{\#\mathbb{B}} = \frac{c_p}{p^r} \tag{2}$$

As $\mathcal{R}_p = \mathbb{Z}^r \setminus \mathcal{Q}_p$ we also get:

$$\mu(\mathcal{R}_p) = 1 - \frac{c_p}{p^r} \tag{3}$$

6.3. **Bound for $\mathcal{Q}_p$.** We need to bound the number c_p of solutions in $(\mathbb{Z}/p\mathbb{Z})^r$ of the set of equations $P_i(\underline{n}) = 0 \pmod p$ $(i = 1, \ldots, s)$. If $r = 1$, we explained in Section 1.3 that $c_p = 0$ for all suitably large primes p. For $r \geqslant 2$, one can bound c_p using the Bézout theorem over $\mathbb{Z}/p\mathbb{Z}$. For $r = 2$, one can use for instance [12, Theorem 4.1]. For $r \geqslant 2$, we have this general version, by Lachaud–Rolland [8, Corollary 2.2]:

General Bézout theorem. *Let $r \geqslant 2$. We have $c_p \leqslant d^s \cdot p^m$, where m is the dimension of the zero-set of the polynomials $P_1(\underline{x}), \ldots, P_s(\underline{x})$, assumed to be of degree $\leqslant d$.*

Corollary 6.1. *For all sufficiently large p, we have $c_p \leqslant d^s \cdot p^{r-2}$. Consequently, we obtain $\mu(\mathcal{Q}_p) = O\left(\frac{1}{p^2}\right)$.*

Proof of Corollary 6.1. The polynomials $P_1(\underline{x}), \ldots, P_s(\underline{x})$ are coprime in $\mathbb{Z}[\underline{x}]$. By Corollary 3.4, they are coprime in $\mathbb{Q}[\underline{x}]$ and the polynomials $\overline{P_1}^p(\underline{x}), \ldots, \overline{P_s}^p(\underline{x})$ (reduced modulo p) are nonzero and coprime in $\mathbb{F}_p[\underline{x}]$ for all suitably large primes p. It follows that they are coprime in $\overline{\mathbb{F}_p}[\underline{x}]$ for the same primes p (this is explained for example in [3, §2.1]).
Fix such a prime p and consider the ideal $\mathcal{I} = \langle \overline{P_1}^p, \ldots, \overline{P_s}^p \rangle \subset \overline{\mathbb{F}_p}[\underline{x}]$. We estimate below the dimension of the zero-set $Z(\mathcal{I}) \subset \overline{\mathbb{F}_p}^r$ of $\mathcal{I}$ and then we will apply the general Bézout theorem. Classically this dimension is also the Krull dimension $\dim \overline{\mathbb{F}_p}[\underline{x}]/\mathcal{I}$ of the quotient ring $\overline{\mathbb{F}_p}[\underline{x}]/\mathcal{I}$ (e.g. [7, Proposition 1.7]).
By definition, $\dim \overline{\mathbb{F}_p}[\underline{x}]/\mathcal{I}$ is the supremum of the heights of minimal prime ideals of $\overline{\mathbb{F}_p}[\underline{x}]$ containing $\mathcal{I}$. We may assume that $\deg \overline{P_1}^p \geqslant 1$; otherwise $c_p = 0$. Then $\overline{P_1}^p$ has at least one irreducible factor $\Delta \in \overline{\mathbb{F}_p}[\underline{x}]$. Furthermore the prime ideal $\langle \Delta \rangle \subset \overline{\mathbb{F}_p}[\underline{x}]$ is not maximal (by Nullstellensatz and $r \geqslant 2$), but is contained in a maximal ideal. We deduce that $\mathrm{height}(\langle \Delta \rangle) \geqslant 1$, and, by [7, Theorem 1.8 A], that

$$\dim \overline{\mathbb{F}_p}[\underline{x}]/\mathcal{I} \leqslant \dim \overline{\mathbb{F}_p}[\underline{x}]/\langle \overline{P_1}^p \rangle \leqslant r - 1.$$

Assume that $\dim \overline{\mathbb{F}_p}[\underline{x}]/\mathcal{I} = r - 1$. Let $\mathfrak{p} \subset \overline{\mathbb{F}_p}[\underline{x}]$ be a minimal prime ideal containing $\mathcal{I}$; thus $\dim \overline{\mathbb{F}_p}[\underline{x}]/\mathfrak{p} = r - 1$, or, equivalently $\mathfrak{p}$ is of height 1. By Krull's Hauptidealsatz [7, Theorem 1.11 A & Proposition 1.13], the variety $Z(\mathfrak{p})$ is a hypersurface $Z(f)$, for some irreducible polynomial $f \in \overline{\mathbb{F}_p}[\underline{x}]$. But then it follows from $\langle f \rangle = \mathfrak{p} \supset \mathcal{I}$ that f divides each polynomial $\overline{P_i}^p$ in $\overline{\mathbb{F}_p}[\underline{x}]$, $i = 1, \ldots, s$, a contradiction. Conclude that $\dim \overline{\mathbb{F}_p}[\underline{x}]/\mathcal{I} \leqslant r - 2$.

The first assertion of Corollary 6.1 then readily follows from the General Bézout theorem, and the second one from this easy estimate:

$$\mu(\mathcal{Q}_p) = \frac{c_p}{p^r} \leqslant \frac{d^s \cdot p^{r-2}}{p^r} = \frac{d^s}{p^2} = O\left(\frac{1}{p^2}\right).$$

□

6.4. **The set $\mathcal{R}_{\leqslant M}$.** Let $M \geqslant 0$, let $\{p_1, \ldots, p_\ell\}$ be the set of primes $\leqslant M$ and 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

$$\underline{n} \in (\mathbb{Z}/N\mathbb{Z})^r \mapsto (\underline{n_1}, \ldots, \underline{n_\ell}) \in (\mathbb{Z}/p_1\mathbb{Z})^r \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^r,$$

where $\underline{n_j}$ is $\underline{n}$ modulo p_j. We have a 1-1 correspondence between the sets $\mathcal{R}_{\leqslant M}$ and $\mathcal{R}_{p_1} \times \cdots \times \mathcal{R}_{p_\ell}$. Namely:

$$\begin{aligned} & \underline{n} \in \mathcal{R}_{\leqslant M} \cap [\![0, N-1]\!]^r \\ \iff & \forall j \in \{1, \ldots, \ell\} \quad \exists i \in \{1, \ldots, s\} \qquad P_i(\underline{n}) \neq 0 \pmod{p_j} \\ \iff & \forall j \in \{1, \ldots, \ell\} \quad \exists i \in \{1, \ldots, s\} \qquad P_i(\underline{n_j}) \neq 0 \pmod{p_j} \\ \iff & \forall j \in \{1, \ldots, \ell\} \quad \underline{n_j} \in \mathcal{R}_{p_j} \cap [\![0, p_j - 1]\!]^r. \end{aligned}$$

Recall that $\mathcal{R}_p = \mathbb{Z}^r \setminus \mathcal{Q}_p$. Thus, with (1), we obtain:

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

Whence:

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

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

$$\mu(\mathcal{R}_{\leqslant M}) = \lim_{B\to+\infty} \frac{\#(\mathcal{R}_{\leqslant M} \cap \mathbb{B})}{\#\mathbb{B}} = \lim_{B\to+\infty} \frac{\left(\frac{B}{N}\right)^r \prod_{j=1}^{\ell}(p_j^r - c_{p_j})}{B^r} = \prod_{j=1}^{\ell} \left(1 - \frac{c_{p_j}}{p_j^r}\right).$$

Whence:

$$\mu(\mathcal{R}_{\leqslant M}) = \prod_{p \leqslant M} \left(1 - \frac{c_p}{p^r}\right) \tag{4}$$

6.5. **Limit of $\mu(\mathcal{Q}_{>M})$.**

Lemma 6.2. *We have:*

$$\mu(\mathcal{Q}_{>M}) \xrightarrow[M\to+\infty]{} 0 \tag{5}$$

The proof (here, for several polynomials) is similar to [9, Lemma 5.1] (for two polynomials) with some simplifications.

Proof. Fix $M > 0$ and $B \geqslant M$ and consider the decomposition:

$$\mathcal{Q}_{>M} = \mathcal{Q}_{>M, \leqslant B} \cup \mathcal{Q}_{>B},$$

where $\mathcal{Q}_{>M,\leqslant B} = \bigcup_{M<p\leqslant B} \mathcal{Q}_p$ and $\mathcal{Q}_{>B} = \bigcup_{p>B} \mathcal{Q}_p$. We will prove that each term has a relatively small cardinal compared to $B^r = \#\mathbb{B}$, where $\mathbb{B} = [\![0, B-1]\!]^r$.

Estimate for $\mathcal{Q}_{>M,\leqslant B}$.

From Corollary 6.1, we have $c_p = \#(\mathcal{Q}_p \cap [\![0,p-1]\!]^r) \leqslant d^s \cdot p^{r-2}$. This gives $\#(\mathcal{Q}_p \cap \mathbb{B}) \leqslant Cp^{r-2}\left(\frac{B}{p}\right)^r$ for some constant C (depending only on d and s). Thus we obtain:

$$\frac{\#(\mathcal{Q}_{>M} \cap \mathbb{B})}{\#\mathbb{B}} \leqslant \sum_{M<p\leqslant B} \frac{\#(\mathcal{Q}_p \cap \mathbb{B})}{\#\mathbb{B}} \leqslant \sum_{M<p\leqslant B} \frac{Cp^{r-2}\left(\frac{B}{p}\right)^r}{B^r} \leqslant C\sum_{p>M}\frac{1}{p^2} \tag{6}$$

The last term does not depend on B and tends to 0 as $M \to +\infty$.

Estimate for $\mathcal{Q}_{>B}$.

Preliminaries. Firstly, we may reduce to the case where each polynomial P_i is irreducible in $\mathbb{Z}[\underline{x}]$. Indeed assume $P_1 = Q \cdot R$ with $Q, R \in \mathbb{Z}[\underline{x}]$. If $p|P_1(\underline{n})$ then $p|Q(\underline{n})$ or $p|R(\underline{n})$. Hence $\mathcal{Q}_{>B}(QR, P_2, \ldots, P_s) \subset \mathcal{Q}_{>B}(Q, P_2, \ldots, P_s) \cup \mathcal{Q}_{>B}(R, P_2, \ldots, P_s)$. This reduction process will eventually replace the tuple $(P_1, \ldots, P_s)$ by several such tuples but with irreducible components, the number of these tuples only depending on d and s.

Secondly, we may also reduce to the case where one of the polynomials, say P_s, is a polynomial in $x_1, \ldots, x_{r-1}$ only. Namely, as $P_1, \ldots, P_s$ are coprime, we have a Bézout identity $\sum_{i=1}^s A_i(\underline{x})P_i(\underline{x}) = \Delta(x_1, \ldots, x_{r-1})$ with $A_i \in \mathbb{Z}[\underline{x}]$, $i = 1, \ldots, s$ and $\Delta \in \mathbb{Z}[x_1, \ldots, x_{r-1}]$, $\Delta \neq 0$. If $p|P_i(\underline{n})$ for $i = 1, \ldots, s$ then $p|\Delta(\underline{n})$. Hence $\mathcal{Q}_{>B}(P_1, \ldots, P_s) \subset \mathcal{Q}_{>B}(P_1, \ldots, P_{s-1}, \Delta)$ and $P_1, \ldots, P_{s-1}, \Delta$ are coprime polynomials (if some nonconstant polynomial R divides P_1, a polynomial where all the variables $x_1, \ldots, x_r$ occur, then $R = P_1$, up to some multiplicative constant, because P_1 is irreducible, but then R cannot divide Δ in the variables $x_1, \ldots, x_{r-1}$ only).

Thirdly, we may assume that the leading coefficient of $P_i(\underline{x})$, $i = 1, \ldots, s-1$, seen as a polynomial in x_r, is not divisible by the last polynomial $P_s(x_1, \ldots, x_{r-1})$. Indeed, write $P_i(\underline{x}) = P_i^0(x_1, \ldots, x_{r-1})x_r^{\delta_i} + \cdots \in \mathbb{Z}[x_1, \ldots, x_{r-1}][x_r]$. If $P_i^0 = Q_iP_s$, then $P_i' = P_i - Q_iP_sx_r^{\delta_i}$ is a polynomial with $\deg_{x_r}(P_i') < \deg_{x_r}(P_i)$. We proceed by induction on $\deg_{x_r}(P_i)$ until P_s does not divide P_i^0 (or $\deg_{x_r}(P_i) = 0$). Note that the set $\mathcal{Q}_p$ is preserved in this process ($p|P_i(\underline{n})$ and $P_s(\underline{n})$ iff p divides $(P_i - Q_iP_sx_r^{\delta_i})(\underline{n})$ and $P_s(\underline{n})$), and that one may have to apply the first reduction to the new polynomials, to get irreducible polynomials.

We prove below that

$$\frac{\#(\mathcal{Q}_{>B} \cap \mathbb{B})}{\#\mathbb{B}} \xrightarrow[B\to+\infty]{} 0 \tag{7}$$

Induction. The proof is by induction on the dimension r. For $r = 1$, a Bézout identity $\sum_{i=1}^s A_i(x)P_i(x) = \Delta$ (with $A_i \in \mathbb{Z}[x]$, $\Delta \in \mathbb{Z}$, $\Delta \neq 0$) implies that if $p|P_i(n)$ for every $i = 1, \ldots, s$, then $p|\Delta \in \mathbb{Z}$. Hence for $B > \Delta$, $\mathcal{Q}_{>B} = \varnothing$.

For $r \geqslant 1$, we introduce the three following subsets $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$ and work with the inclusion: $\mathcal{Q}_{>B} \cap \mathbb{B} \subset \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$.

- $\mathcal{S}_1 = \{\underline{n} \in \mathbb{B} \mid P_s(\underline{n}) = 0\}$. By the Zippel–Schwartz lemma, $\#\mathcal{S}_1/\#\mathbb{B}$ tends to 0 as $B \to +\infty$.
- $\mathcal{S}_2 = \{\underline{n} \in \mathbb{B} \mid \exists p > B, p|P_1^0(\underline{n}), \ldots, p|P_{s-1}^0(\underline{n}), p|P_s(\underline{n})\}$. By induction, $\#\mathcal{S}_2/\#\mathbb{B}$ tends to 0 as $B \to +\infty$.
- $\mathcal{S}_3 = \{\underline{n} \in \mathbb{B} \mid P_s(\underline{n}) \neq 0, \exists p > B, p|P_1(\underline{n}), \ldots, p|P_s(\underline{n}), p \nmid P_{i_0}^0(\underline{n})$ for some $1 \leqslant i_0 < s\}$. For all $\underline{n} \in \mathbb{B}$, $P_s(\underline{n}) = O(B^\gamma)$ with $\gamma = \deg(P_s)$. Fix $(n_1, \ldots, n_{r-1}) \in [\![0, B-1]\!]^{r-1}$ and consider a r-tuple $\underline{n} = (n_1, \ldots, n_{r-1}, n_r)$ in the set $\mathcal{S}_3$. For any sufficiently large B, there are at most γ possible primes $p > B$ such that p divides the nonzero integer $P_s(\underline{n})$. Pick such a prime p and let $i \in \{1, \ldots, s-1\}$ be an

index such that $p \nmid P_i^0(n_1, \dots, n_{r-1})$. Then write:

$$P_i(n_1, \dots, n_{r-1}, x) = P_i^0(n_1, \dots, n_{r-1}) x^{\delta_i} + \cdots$$

There are at most δ_i integers $x = n_r$ with $0 \leqslant n_r < p$, hence a fortiori with $0 \leqslant n_r < B$, such that $p | P_i(n_1, \dots, n_{r-1}, n_r)$. This shows that for each $(n_1, \dots, n_{r-1}) \in [\![0, B-1]\!]^{r-1}$, there are at most $C' = (s-1) \cdot \gamma \cdot \delta_1 \cdots \delta_{s-1}$ values of $n_r \in [\![0, B-1]\!]$ such that $(n_1, \dots, n_{r-1}, n_r) \in \mathcal{S}_3$. Hence $\#\mathcal{S}_3 / \#\mathbb{B} \leqslant \frac{B^{r-1} \cdot C'}{B^r} = \frac{C'}{B}$ and so $\#\mathcal{S}_3 / \#\mathbb{B}$ tends to 0 as $B \to +\infty$.

Conclusion. As $\mathcal{Q}_{>M} = \mathcal{Q}_{>M, \leqslant B} \cup \mathcal{Q}_{>B}$, then by (6):

$$\frac{\#\mathcal{Q}_{>M}}{\#\mathbb{B}} \leqslant \frac{\#(\mathcal{Q}_{>M,\leqslant B} \cap \mathbb{B})}{\#\mathbb{B}} + \frac{\#(\mathcal{Q}_{>B} \cap \mathbb{B})}{\#\mathbb{B}} \leqslant C \sum_{p>M} \frac{1}{p^2} + \frac{\#(\mathcal{Q}_{>B} \cap \mathbb{B})}{\#\mathbb{B}}.$$

By (7), the last term tends to 0 as $B \to +\infty$, and the first term tends to 0 as $M \to +\infty$. This indeed proves that $\mu(\mathcal{Q}_{>M}) \xrightarrow[M \to +\infty]{} 0$. □

6.6. **Limit of $\mathcal{R}_{\leqslant M}$.** We have $\mathcal{R} \subset \mathcal{R}_{\leqslant M}$. Note that $\mathcal{R}_{\leqslant M} \setminus \mathcal{R} \subset \mathcal{Q}_{>M}$: in fact $\mathcal{R}_{\leqslant M} \setminus \mathcal{R}$ is the set of $\underline{n}$ for which the primes p that divide all the $P_i(\underline{n})$ verify $p > M$, such $\underline{n}$ are in the union of the $\mathcal{Q}_p$, for $p > M$.
Consider the decomposition:

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

It yields the inequalities:

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

As, by Lemma 6.2, $\mu(\mathcal{Q}_{>M})$ tends to 0 as $M \to +\infty$, we obtain:

$$\mu(\mathcal{R}_{\leqslant M}) \xrightarrow[M \to +\infty]{} \mu(\mathcal{R}) \tag{8}$$

As $\mu(\mathcal{R}_{\leqslant M}) = \prod_{p \leqslant M} \left(1 - \frac{c_p}{p^r}\right)$ by (4), then

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

This infinite product is nonzero if no prime p divides all the values of $P_1(\underline{n}), \dots, P_s(\underline{n})$ for all $\underline{n} \in \mathbb{Z}^r$, i.e., if $c_p \neq p^r$ for all primes p.

6.7. **Generalization to several families of polynomials.** Consider $\ell \geqslant 1$ families $\mathcal{P}_j = \{P_{j1}(\underline{x}), \dots, P_{js_j}(\underline{x})\}$ of nonzero coprime polynomials in $\mathbb{Z}[\underline{x}]$, $j = 1, \dots, \ell$. For each $j = 1, \dots, \ell$, consider the set

$$\mathcal{R}(\mathcal{P}_j) = \{\underline{n} \in \mathbb{Z}^r \mid \gcd(P_{j1}(\underline{n}), \dots, P_{\ell s_\ell}(\underline{n})) = 1\}.$$

Our goal is to evaluate the set $\mathcal{R} = \bigcap_{j=1}^{\ell} \mathcal{R}(\mathcal{P}_j)$.

Proposition 6.3. *Let $\Pi = \mathcal{P}_1 \cdots \mathcal{P}_\ell \subset \mathbb{Z}[\underline{x}]$ be the set of all possible products $A_1 \cdots A_\ell$ with $A_j \in \mathcal{P}_j$ for $j = 1, \dots, \ell$. Then we have the following:*

(a) *The elements of Π are nonzero coprime polynomials (in $\mathbb{Q}[\underline{x}]$).*
(b) $\mathcal{R} = \mathcal{R}(\Pi)$.
(c) $\mu(\mathcal{R}) = \prod_{p \in \mathcal{P}} \left(1 - \frac{c_p}{p^r}\right)$ *where* $c_p = \#\big\{\underline{n} \in (\mathbb{Z}/p\mathbb{Z})^r \mid Q(\underline{n}) = 0 \pmod{p}, \forall Q \in \Pi\big\}$.

(d) *For every $p \in \mathcal{P}$, we have $c_p = p^r$ if and only if for every $\underline{n} \in \mathbb{Z}^r$, there exists $j \in \{1, \ldots, \ell\}$ such that the prime p divides all values $P_{j1}(\underline{n}), \ldots, P_{js_j}(\underline{n})$.*

Note that c_p can also be computed with the following formula:

$$c_p = \# \bigcup_{j=1}^{\ell} \left\{ \underline{n} \in (\mathbb{Z}/p\mathbb{Z})^r \mid P_{j1}(\underline{n}) = 0 \pmod p, \ldots, P_{js_j}(\underline{n}) = 0 \pmod p \right\}.$$

This equality follows from the relation $V(I \cdot J) = V(I) \cup V(J)$ for ideals and their varieties, applied to $\Pi = \mathcal{P}_1 \cdots \mathcal{P}_\ell$.

Proof. (a) Assume that some irreducible polynomial $D \in \mathbb{Q}[\underline{x}]$ divides all elements of Π. Then the product of all ideals $\langle \mathcal{P}_j \rangle \subset \mathbb{Q}[\underline{x}]$ ($j = 1, \ldots, \ell$), which is generated by the set Π, is contained in the ideal $\langle D \rangle \subset \mathbb{Q}[\underline{x}]$. As $\langle D \rangle$ is a prime ideal, we have $\langle \mathcal{P}_j \rangle \subset \langle D \rangle$ for some $j \in \{1, \ldots, \ell\}$. This contradicts $P_{j1}(\underline{x}), \ldots, P_{js_j}(\underline{x})$ being coprime.

(b) $\mathcal{R}(\Pi) \subset \mathcal{R}$: If $\underline{n} \notin \mathcal{R}$, i.e., $\underline{n} \notin \mathcal{R}(\mathcal{P}_j)$ for some $j \in \{1, \ldots, \ell\}$, then some prime p divides $P_{j1}(\underline{n}), \ldots, P_{js_\ell}(\underline{n})$. Clearly then, p divides all $Q(\underline{n})$ with $Q \in \Pi$, i.e., $\underline{n} \notin \mathcal{R}(\Pi)$.

$\mathcal{R}(\Pi) \supset \mathcal{R}$: Let $\underline{n} \notin \mathcal{R}(\Pi)$, i.e., some prime p divides all $Q(\underline{n})$ with $Q \in \Pi$. Observe that the ideal generated by all these $Q(\underline{n})$ is the product of the ideals $\langle P_{j1}(\underline{n}), \ldots, P_{js_j}(\underline{n}) \rangle \subset \mathbb{Z}$ with j ranging over $\{1, \ldots, s\}$. So this product is contained in $p\mathbb{Z}$. But then $p\mathbb{Z}$ must contain some ideal $\langle P_{j1}(\underline{n}), \ldots, P_{js_j}(\underline{n}) \rangle$; hence $\underline{n} \notin \mathcal{R}(\mathcal{P}_j)$ and so $\underline{n} \notin \mathcal{R}$.

(c) Follows from (b) and the Ekedahl–Poonen formula, for the case $\ell = 1$, with the polynomials in Π (Theorem 1.5).

(d) We have $c_p = p^r$ if and only if p divides all $Q(\underline{n})$ with $Q \in \Pi$ for every $\underline{n} \in \mathbb{Z}^r$. Arguing as in (b) above for each fixed $\underline{n} \in \mathbb{Z}^r$, we obtain that, for each $\underline{n}$, p divides $P_{j1}(\underline{n}), \ldots, P_{js_j}(\underline{n})$ for some $j \in \{1, \ldots, \ell\}$, which is the claimed condition. The converse is clear. □

Finally we can give the proof of Theorem 1.7 in the general case $\ell \geqslant 1$.

Proof of Theorem 1.7 ($\ell \geqslant 1$). Let $P_1(\underline{x}, \underline{y}), \ldots, P_\ell(\underline{x}, \underline{y})$ be as in the statement. The first point is based on the same result of Cohen used in the case $\ell = 1$. Specifically let $\mathcal{H}(P_1, \ldots, P_\ell)$ be the subset of $\mathbb{Z}^r$ of all $\underline{n}$ such that $P_1(\underline{n}, \underline{y}), \ldots, P_\ell(\underline{n}, \underline{y})$ are irreducible in $\mathbb{Q}[\underline{y}]$. From Theorem 1 of [11, §13], we have $\tilde{\mu}(\mathcal{H}(P_1, \ldots, P_\ell)) = 1$, with $\tilde{\mu}$ the density introduced in Remark 1.6.

For each $j = 1, \ldots, \ell$, denote by $\mathcal{P}_j \subset \mathbb{Q}[\underline{x}]$ the set of coefficients $P_{j1}(\underline{x}), \ldots, P_{js_j}(\underline{x})$ of P_j, viewed as a polynomial in $\underline{y}$; these polynomials are coprime. Using then the notation of Proposition 6.3, the set $\mathcal{R} \subset \mathbb{Z}^r$ is the subset of all $\underline{n}$ such that the polynomials $P_1(\underline{n}, \underline{y}), \ldots, P_\ell(\underline{n}, \underline{y})$ are primitive. Thus, for every $\underline{n} \in H = \mathcal{H}(P_1, \ldots, P_\ell) \cap \mathcal{R}$, the polynomials $P_1(\underline{n}, \underline{y}), \ldots, P_\ell(\underline{n}, \underline{y})$ are irreducible in $\mathbb{Z}[\underline{y}]$.

Observe that the assumption that there is no prime p such that $\prod_{j=1}^{\ell} P_j(\underline{n}, \underline{y}) \equiv 0 \pmod p$ for every $\underline{n} \in \mathbb{Z}^r$ forbids the equivalent conditions from Proposition 6.3(d) to happen. Thus, by Proposition 6.3(c), we have $\mu(\mathcal{R}) > 0$, and also $\tilde{\mu}(\mathcal{R}) > 0$ (as explained in Remark 1.6). Conclude that $\tilde{\mu}(H) > 0$ as well. □

References

[1] Arnaud Bodin, Pierre Dèbes, Joachim König, and Salah Najib. The Hilbert-Schinzel specialization property. *J. Reine Angew. Math.*, to appear, 2022.

[2] Arnaud Bodin, Pierre Dèbes, and Salah Najib. Prime and coprime values of polynomials. *Enseign. Math.*, 66(1-2):173–186, 2020.

[3] Arnaud Bodin, Pierre Dèbes, and Salah Najib. The Schinzel hypothesis for polynomials. *Trans. Amer. Math. Soc.*, 373(12):8339–8364, 2020.

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

[5] Péter E. Frenkel and József Pelikán. On the greatest common divisor of the value of two polynomials. *Amer. Math. Monthly*, 124(5):446–450, 2017.

[6] Michael D. Fried and Moshe Jarden. *Field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 3rd edition, 2008. Revised by Jarden. xxiv+792 pp.

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

[10] A. Schinzel. A property of polynomials with an application to Siegel's lemma. *Monatsh. Math.*, 137(3):239–251, 2002.

[11] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[12] Terence Tao. Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. *EMS Surv. Math. Sci.*, 1(1):1–46, 2014.

E-mail address: arnaud.bodin@univ-lille.fr
E-mail address: pierre.debes@univ-lille.fr

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