W. DALE BROWNAWELL

On the orders of zero of certain functions

Mémoires de la S. M. F. 2e série, tome 2 (1980), p. 5-20
<http://www.numdam.org/item?id=MSMF_1980_2_2__5_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 5-20

ON THE ORDERS OF ZERO OF CERTAIN FUNCTIONS

by

W. Dale BROWNAWELL♦

I. INTRODUCTION

This is a report on joint work with D. W. Masser into the possible order of vanishing of a certain class of analytic functions. A complete exposition of our most general result and its relation to the previous work of Ju. Nesterenko [4] is given in [1] . That paper was written expressly for the use of fellow practitioners of transcendence theory.

For this conference it seemed appropriate to present a variant of the proof of the main theorem of [1] , this time assuming familiarity with commutative algebra from the outset. The major change is the use here of the Hilbert characteristic function $H_a(\mathfrak{a},t)$ for inhomogeneous ideals $\mathfrak{a}$. In this way we avoid the technicalities involved in keeping track of the order of vanishing while homogenizing and dehomogenizing ideals. (These technicalities seem indispensable however for handling denominators in some of Masser's most recent work). Since we have not found a reference for the properties of $H_a(\mathfrak{a},t)$ in the literature (see [2,p. 157] however), we discuss them in a short appendix following the body of the proof.

We are concerned here with solutions of a fixed system of differential equations

♦ Research supported in part by the National Science Foundation.

(1) $$f_i' = F_i(f_1,\dots,f_n) \qquad (1 \leq i \leq n)$$

where $F_1,\dots,F_n$ are non-zero polynomials of total degree at most d. For a given set of initial values $\Theta = (\theta_1,\dots,\theta_n)$, we denote by $\bar{f}(z;\Theta)$ the corresponding solution of (1) analytic at the origin, i.e. the coordinates $f_1(z;\Theta),\dots,f_n(z;\Theta)$ satisfy (1) and $\bar{f}(0,\Theta) = \Theta$. In this paper we will deal with $M+1$ fixed such initial conditions given by $\Theta_0, \Theta_1,\dots,\Theta_M$.

Let $\mathfrak{a}$ be an ideal of $R = \mathbb{C}[X_1,\dots,X_n]$. For $0 \leq m \leq M$ we define

$$\operatorname{ord}_m \mathfrak{a} = \min_{\substack{P \in \mathfrak{a} \\ P \neq 0}} \operatorname{ord} P(\bar{f}(z;\Theta_m)),$$

where ord on the right hand side denotes the order of zero at the origin with the usual proviso that ord $0 = \infty$. Say $\mathfrak{a}$ is generated by $P_1,\dots,P_s$. Then clearly

$$\operatorname{ord}_m \mathfrak{a} = \min_i \operatorname{ord} P_i(\bar{f}(z;\Theta_m)).$$

If $\mathfrak{a}$ has rank r (we avoid the term "height" because of other associations in transcendence theory), we can suppose that the indices are chosen in such a way that $P_1,\dots,P_r$ have total degrees at most $D_1 \geq \dots \geq D_r$, respectively, whereas $P_{r+1},\dots,P_s$ have total degrees at most D_r. Let $T = D_1 \dots D_r$, and recall that $d \leq \max_i \deg F_i$. Then we can state our main result.

<u>Theorem</u> : <u>Assume that</u> $\operatorname{ord}_m \mathfrak{a}$ <u>is finite for</u> $0 \leq m \leq M$. <u>Then if</u> $r < n$ <u>and</u> $d > 1$, <u>we have</u>

$$\sum_{m=0}^{M} \operatorname{ord}_m \mathfrak{a} \leq (dT)^{2^{n-r}} + M(dT)^{2^{n-r-1}},$$

<u>while if</u> $r < n$ <u>and</u> $d = 1$, <u>we have</u>

$$\sum_{m=0}^{M} \operatorname{ord}_m \mathfrak{a} \leq (n-r+1)D_1^{n-r}T + (n-r)MTD_1^{n-r-1}.$$

<u>Finally if</u> $r = n$, <u>then</u>

$$\sum_{m=0}^{M} \operatorname{ord}_m \mathfrak{a} \leq T.$$

II. UNMIXING

Because we can estimate the degree of an ideal of the principal class (rank = minimal number of generators) through Proposition 4A, we would be very happy if $r = s$. Since that is not always the case, we show that for our purposes, it is always possible to replace $\mathfrak{a}$ by an ideal $\mathfrak{a}_r$ of rank r and generated by r polynomials of degrees at most $D_1, \ldots, D_r$, respectively, such that

$$\mathrm{ord}_m \mathfrak{a}_r = \mathrm{ord}_m \mathfrak{a} \qquad (0 \leqslant m \leqslant M).$$

For that the following general remark is useful.

<u>Lemma 1</u> : <u>Let $P_1, \ldots, P_s$ be polynomials and let $\vartheta_1, \ldots, \vartheta_k$ be ideals such that for each</u> $1 \leqslant \kappa \leqslant k$, <u>not all of</u> $P_1, \ldots, P_s$ <u>lie in</u> ϑ_κ. <u>Then for some integer</u>, $1 \leqslant \lambda \leqslant ks$,

$$P_1 + \lambda P_2 + \ldots + \lambda^{s-1} P_s \notin \bigcup_{\kappa=1}^{k} \vartheta_k .$$

<u>Proof</u> : If each of the $Q_\lambda = P_1 + \lambda P_2 + \ldots + \lambda^{s-1} P_s$ $(1 \leqslant \lambda \leqslant ks)$ lies in some ϑ, then by the Box Principle, at least s of the Q_λ lie in the same ϑ. Inverting the corresponding Vandermonde determinant shows then that $P_1, \ldots, P_s$ all lie in that same ϑ as well. This contradiction establishes the lemma.

For a vector $\Theta = (\theta_1, \ldots, \theta_n)$ of $\mathbb{C}^n$ we denote by $\mathfrak{M}(\Theta)$ the corresponding maximal ideal $(x_1 - \theta_1, \ldots, x_n - \theta_n)$. For brevity we write $\mathfrak{M}_0, \ldots, \mathfrak{M}_M$ instead of $\mathfrak{M}(\Theta_0), \ldots, \mathfrak{M}(\Theta_M)$, respectively. For $0 \leqslant m \leqslant M$ we write $\mathfrak{a}^{(m)}$ for the contracted extension

$$\mathfrak{a}^{(m)} = \mathfrak{a}_m \cap R ,$$

where $\mathfrak{a}_m$ denotes the extension of $\mathfrak{a}$ to the localization of $R = \mathbb{C}[x_1, \ldots, x_n]$ at $\mathfrak{M}_m$. Further we write $\mathfrak{a}^*$ for the contracted extension with respect to the multiplicative set $S = R \setminus \bigcup_{m=0}^{M} \mathfrak{M}_m$, i.e. $\mathfrak{a}^* = (\mathfrak{a} \otimes_R R_S) \cap R$. We see that $\mathfrak{a}^*$ is also obtained by deleting from a primary decomposition of $\mathfrak{a}$ components not lying in any $\mathfrak{M}_m$ $(0 \leqslant m \leqslant M)$, just as $\mathfrak{a}^{(m)}$ is obtained on deleting components not in $\mathfrak{M}_m$. Therefore

$$\mathfrak{a}^* = \bigcap_{m=0}^{M} \mathfrak{a}^{(m)} . \tag{2}$$

Since every element of $\mathfrak{a}^{(m)}$ is the quotient of an element of $\mathfrak{a}$ by an element outside $\mathfrak{M}_m$, we see that $\mathrm{ord}_m \mathfrak{a}^{(m)} = \mathrm{ord}_m \mathfrak{a}$. Therefore from $\mathfrak{a} \subseteq \mathfrak{a}^* \subseteq \mathfrak{a}^{(m)}$ we deduce that

$$\mathrm{ord}_m \mathfrak{a} = \mathrm{ord}_m \mathfrak{a}^* = \mathrm{ord}_m \mathfrak{a}^{(m)} \qquad (0 \leq m \leq M) \tag{3}$$

<u>Proposition 2</u> : <u>If in addition to the hypotheses of the Main Theorem we have</u>

$$0 < \mathrm{ord}_m \mathfrak{a} \qquad (0 \leq m \leq M) \ ,$$

<u>then there are polynomials</u> $Q_1,\dots,Q_r$ <u>in</u> $\mathfrak{a}$ <u>with</u> $\deg Q_1 \leq D_1,\dots,\deg Q_r \leq D_r$ <u>such that the ideal</u> $\mathfrak{a}_r = (Q_1,\dots,Q_r)$ <u>satisfies</u>

$$\mathrm{rank}\, \mathfrak{a}_r = r \ ,$$

$$\mathrm{ord}_m \mathfrak{a}_r = \mathrm{ord}_m \mathfrak{a} \qquad (0 \leq m \leq M),$$

<u>and</u>

$$\deg \mathfrak{a}_r^* \leq D_1 \dots D_r = T \ .$$

<u>Proof</u> : Since $\mathrm{ord}_m \mathfrak{a}$ is assumed to be finite for each m, the polynomials P such that $\mathrm{ord}_m P > \mathrm{ord}_m \mathfrak{a}$ form an ideal which we denote $\mathfrak{b}_m$. By Lemma 1 we can select $\lambda \in \mathbb{Z}$ such that

$$Q_1 = P_1 + \lambda P_2 + \dots + \lambda^{s-1} P_s \notin \bigcup_{m=0}^{M} \mathfrak{b}_m .$$

Set $\mathfrak{a}_1 = (Q_1)$. Then $\mathrm{rank}\, \mathfrak{a}_1 = 1$ and $\mathrm{ord}_m \mathfrak{a}_1 = \mathrm{ord}_m \mathfrak{a}$, $0 \leq m \leq M$. Now $\mathfrak{a}_1^*$ is principal with generator obtained from Q_1 by deleting all factors not in any $\mathfrak{M}_m$, $0 \leq m \leq M$. Since $\mathrm{ord}_m \mathfrak{a}_1^* = \mathrm{ord}_m \mathfrak{a}_1 > 0$, Q_1 is not constant and $\mathrm{rank}\, \mathfrak{a}_1^* = 1$. We deduce from Proposition 4A of the appendix that

$$\deg \mathfrak{a}_1^* \leq D_1 \ ,$$

which is what was claimed for $r = 1$.

For $r > 1$ we choose polynomials $Q_2,\ldots,Q_r$ inductively of the form

$$(4) \qquad Q_i = P_i + \lambda_i P_{i+1} + \ldots + \lambda_i^{s-i} P_s$$

such that the ideals $\mathfrak{a}_i = (Q_1,\ldots,Q_i)$ satisfy

$$\text{rank } \mathfrak{a}_i = i, \ \deg \mathfrak{a}_i^* \leq D_1 \ldots D_i .$$

Moreover the form of selection given in (4) guarantees that for $1 \leq i \leq r$

$$\text{ord}_m \mathfrak{a}_i = \text{ord}_m \mathfrak{a} \qquad (0 \leq m \leq M)$$

The selection has already been made for $i = 1$, and now we show how to find Q_{i+1} with the desired properties once $\mathfrak{a}_i$ has been obtained $(i < r)$.

Fix a prime component $\mathfrak{p}$ of $\mathfrak{a}_i$ of rank i (necessarily so by the Cohen-Macauley Theorem [5-II, p.310]). If $P_{i+1},\ldots,P_s$ all lay in $\mathfrak{p}$, Then we see inductively from (4) that so do $P_i, P_{i-1},\ldots,P_1$. Thus $\mathfrak{a}$ would be contained in $\mathfrak{p}$ and rank $\mathfrak{a} \leq i$, contrary to our assumption that rank $\mathfrak{a} = r$. Thus at least one of $P_{i+1},\ldots,P_s$ does not lie in $\mathfrak{p}$. So by Lemma 1, there is a Q_{i+1} of the form (4) not in any prime component of $\mathfrak{a}_i$, i.e. $\mathfrak{a}_i : Q_{i+1} = \mathfrak{a}_i$. Therefore by Proposition 4A of the appendix, for $\mathfrak{a}_{i+1} = (\mathfrak{a}_i, Q_{i+1})$ we have rank $\mathfrak{a}_{i+1} = i+1$ and $\deg \mathfrak{a}_{i+1} \leq (\deg \mathfrak{a}_i) D_{i+1}$, which establishes Proposition 2.

III. <u>THE CASE n = r.</u>

To deal with this case we require a fundamental result concerning exponents of ideals.

<u>Lemma 3</u> : <u>If</u> $\mathfrak{q}$ <u>is a primary ideal of length</u> ℓ <u>and exponent</u> e, <u>then</u> $e \leq \ell$.

<u>Proof</u> : Say that $\mathfrak{q}$ is $\mathfrak{p}$-primary. Then $\mathfrak{p}^e \subseteq \mathfrak{q}$, and e is the least positive power of $\mathfrak{p}$ lying in $\mathfrak{q}$. If $e = 1$, then $\mathfrak{p} = \mathfrak{q}$ and there is nothing to show. If $e \geq 2$, the ideals $\mathfrak{q}_i = \mathfrak{q} : \mathfrak{p}^i$ $(0 \leq i \leq e)$ are $\mathfrak{p}$ -primary [5-I, p.154] . Since $\mathfrak{p}^{e-1}\mathfrak{p} = \mathfrak{p}^e \subseteq \mathfrak{q}$, $\mathfrak{p} \subset \mathfrak{q}_{e-1}$, and so $\mathfrak{p} = \mathfrak{q}_{e-1}$. Thus we obtain e primary ideals

$$\mathfrak{q} = \mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subsetneq \cdots \subseteq \mathfrak{q}_{e-1} = \mathfrak{p}$$

If we can show that these inclusions are strict, then the lemma will follow. But $\mathfrak{p}\mathfrak{q}_{k+1} \subseteq \mathfrak{q}_k$ $(0 \leq k < e-1)$. So if some $\mathfrak{q}_k = \mathfrak{q}_{k+1}$, then $\mathfrak{p}\mathfrak{q}_{k+2} \subseteq \mathfrak{q}_{k+1} = \mathfrak{q}_k$. Therefore $\mathfrak{p}^{k+1}\mathfrak{q}_{k+2} \subseteq \mathfrak{p}^k\mathfrak{q}_k \subseteq \mathfrak{q}$ and $\mathfrak{q}_{k+2} \subseteq \mathfrak{q}_{k+1}$. Consequently $\mathfrak{q}_k = \mathfrak{q}_{k+1} = \mathfrak{q}_{k+2}$. Repeating the argument shows that

$$\mathfrak{q}_k = \mathfrak{q}_{k+1} = \dots = \mathfrak{q}_{e-1} .$$

Thus $\mathfrak{p} = \mathfrak{q} : \mathfrak{p}^k$ and $\mathfrak{p}^{k+1} \subseteq \mathfrak{q}$. By the definition of e, $e \leq k+1$. But $k+1 \leq e-1$ by assumption. This contradiction shows that the inclusions are strict and establishes the lemma.

<u>Proposition 4</u> : <u>Let $\mathfrak{q}$ be primary of rank n such that</u> $\text{ord}_m \mathfrak{q}$ <u>is positive but finite for some</u> $0 \leq m \leq M$. <u>Then</u> $\mathfrak{M}_m$ <u>is the associated prime ideal of $\mathfrak{q}$ and</u>

$$\text{ord}_m \mathfrak{q} \leq \deg \mathfrak{q}.$$

<u>Proof</u> : Since $\text{ord}_m \mathfrak{q} > 0$, we have $\mathfrak{q} \subseteq \mathfrak{M}_m$. Because rank $\mathfrak{q} = n$, $\mathfrak{M}_m$ is the associated prime. Let e be the exponent of $\mathfrak{q}$. Then

$$\mathfrak{M}_m^e \subseteq \mathfrak{q} \subseteq \mathfrak{M}_m.$$

Since for any ideals $\mathfrak{k}, \mathfrak{L}$

$$\text{ord}_m(\mathfrak{k} \cap \mathfrak{L}) \leq \text{ord}_m(\mathfrak{k}\mathfrak{L}) = \text{ord}_m \mathfrak{k} + \text{ord}_m \mathfrak{L},$$

we see that

$$\text{ord}_m \mathfrak{q} \leq e \ \text{ord}_m \mathfrak{M}_m.$$

From Proposition 2A of the appendix and Lemma 4 we see that

$$e \leq \text{length}\ \mathfrak{q} \leq \deg \mathfrak{q}.$$

If $\Theta_m = (\theta_1, \dots, \theta_n)$, then $\text{ord}_m \mathfrak{M}_m = \min_i \text{ord}_m(f_i(z;\Theta_m) - \theta_i)$, and so if $\text{ord}_m \mathfrak{M}_m > 1$, then each $f_i'(z;\Theta_m)$ vanishes at the origin. Now differentiation of (1) leads to the relations

$$f_i''(z;\,\Theta_m) = \sum_{j=1}^{n} \frac{\partial F_i}{\partial x_j}\bigg|_{\bar{f}(z;\,\Theta_m)} f_j'(z;\,\Theta_m) \qquad (1 \leq i \leq n).$$

Thus

$$\mathrm{ord}_{z=0} f_i''(z;\,\Theta_m) \geq \min_j \mathrm{ord}_{z=0} f_j'(z;\,\Theta_m) > 0 \qquad (1 \leq i \leq n).$$

This implies that $\mathrm{ord}_{z=0} f_i'(z;\,\Theta_m) = \infty$, $1 < i < n$. Then $\mathrm{ord}_m \mathfrak{M}_m = \infty$, a contradiction which completes the proof of the proposition.

<u>Proof of the case n = r.</u>

We may clearly assume that $\mathrm{ord}_m \mathfrak{A} > 0$ $(0 \leq m \leq M)$ simply by renumbering and taking M smaller if necessary. For if the analogous bound holds on the sum of the remaining $\mathrm{ord}_m \mathfrak{A}$, then the desired bound will hold on the full sum. We apply Proposition 2 to $\mathfrak{A}$ to obtain $\mathfrak{A}_n$. If $\mathfrak{A}_n^* = \mathfrak{q}_0 \cap \dots \cap \mathfrak{q}_N$ is the primary decomposition of $\mathfrak{A}_n^*$, then by the first half of Proposition 4, N = M, and we may take $\mathfrak{q}_m$ to be $\mathfrak{p}_m$-primary $(0 \leq m \leq M)$. By the second half of Propositions 3A and 4A of the appendix and by Proposition 4,

$$\begin{aligned} T \geq \deg \mathfrak{A}_n^* &= \sum_{m=0}^{M} \deg \mathfrak{q}_m \\ &\geq \sum_{m=0}^{M} \mathrm{ord}_m \mathfrak{q}_m = \sum_{m=0}^{M} \mathrm{ord}_m \mathfrak{A}, \end{aligned}$$

since $\mathrm{ord}_m \mathfrak{A} = \mathrm{ord}_m \mathfrak{A}_n = \mathrm{ord}_m \mathfrak{A}_n^{(m)} = \mathrm{ord}_m \mathfrak{q}_m$ $(0 \leq m \leq M)$. This proves the assertion of the theorem for r = n.

IV. <u>INCREASING THE LOCAL RANK</u>

In this section we develop a procedure which allows us to cope with ideals of rank less than n. We inductively produce polynomials $Q_{r+1},\dots,Q_n$ of predictably bounded degrees $D_{r+1},\dots,D_n$, respectively, through differentiation of the generators of $\mathfrak{A}_r$ such that for $r \leq i \leq n$ the ideals

$$\mathcal{L}_i = (\mathfrak{A}_r, Q_{r+1},\dots,Q_i) \tag{7}$$

satisfy

(8) $$\operatorname{rank} \mathcal{B}_i^{(m)} = i \qquad (0 \leq m \leq M)\ ,$$

(9) $$\deg \mathcal{B}_i^* \leq D_1 \ldots D_i$$

and

(10) $$\operatorname{ord}_m \mathcal{A} - W_{i-r-1} \leq \operatorname{ord}_m \mathcal{B}_i \neq \infty \qquad (0 \leq m \leq M)$$

where

$$W_k = \begin{cases} \sum_{j=o}^{k} d^{2^j-1} T^{2^j}, & \text{if } d > 1 \\ T \sum_{j=o}^{k} D_1^j, & \text{if } d = 1. \end{cases}$$

(Recall that d is our upper bound on the degree of the polynomials $F_1, \ldots, F_n$ in (1) and D_1 bounds the degree of all the generators of $\mathcal{A}$). As we shall see, W_{i-r-1} is a bound on the number of derivatives we may have to take to obtain $Q_{r+1}, \ldots, Q_i$. Because of its importance for the Main Theorem, we state the result for i = n as a proposition. Set

$$D_i = \begin{cases} (dT)^{2^{i-r-1}}, & \text{if } d > 1 \\ D_1, & \text{if } d = 1 \end{cases}$$

Proposition 5 : Given $\mathcal{A}_r$ of Proposition 2 with

$$W_{n-r-1} < \operatorname{ord}_m \mathcal{A}_r \neq \infty \qquad (0 \leq m \leq M),$$

there are then polynomials $Q_{r+1}, \ldots, Q_n$ with $\deg Q_i \leq D_i$ $(r < i \leq n)$ such that the following holds for $\mathcal{B}_n = (\mathcal{A}_r, Q_{r+1}, \ldots, Q_n)$:

$$\operatorname{rank} \mathcal{B}_n^{(m)} = n,\ \operatorname{ord}_m \mathcal{A}_r - W_{n-r-1} \leq \operatorname{ord}_m \mathcal{B}_n \qquad (0 \leq m \leq M)$$

and

$$\deg \mathcal{B}_n^* \leq D_1 \ldots D_n\ .$$

<u>Proof</u> : As mentioned above, the construction of the $\mathcal{B}_{r+1},\ldots,\mathcal{B}_n$ with the properties (8), (9), (10) is inductive. If we set $W_{-1} = 0$, we may consider $\mathcal{B}_r = \mathcal{A}_r$ to start it off. For the inductive step assume that (8), (9), (10) hold for some $\mathcal{B}_i$ of the form (7), $r \leq i < n$. Consider the derivation

$$\Delta = \sum_{j=1}^{n} F_j \frac{\partial}{\partial x_j}$$

defined on $R = \mathbb{C}[x_1,\ldots,x_n]$. Clearly if $P \in R$ has total degree G, then ΔP has total degree at most $G + d - 1$. Also if $\bar{f} = (f_1,\ldots,f_n)$ is an analytic solution of (1) then for any polynomial $P \in R$,

$$\Delta P(\bar{f}) = \frac{d}{dz} P(\bar{f}).$$

So if $\mathrm{ord}_m P > 1$, then $\mathrm{ord}_m \Delta P = \mathrm{ord}_m P - 1$ $(C \leq m \leq M)$. Since the ideals $\mathcal{B}_i^{(m)}$ have rank i and $\mathcal{B}_i$ is generated by i elements, $\mathcal{B}_i^{(m)}$ is unmixed by the Cohen-Macauley Theorem [5-II, p.310] . Therefore in particular all primary components of $\mathcal{B}_i^*$ have rank i. For the next few paragraphs we consider one fixed such component $\mathfrak{q}$ and its associated prime $\mathfrak{p}$.

From Lemma 3, Propositions 2A and 3A of the appendix, and our induction assumption, we deduce that

(11) $$e \leq \deg \mathcal{A}_i^* \leq D_1 \ldots D_i$$

for the exponent e of $\mathfrak{q}$. We claim that

(12) $$\Delta^e \mathcal{B}_i^* \not\subseteq \mathfrak{p}.$$

Since $\mathcal{B}_i^* \subseteq \mathfrak{p} \subseteq \mathfrak{m}_m$ for some $0 \leq m \leq M$, $\mathrm{ord}_m \mathfrak{p}$ is positive but bounded by $\mathrm{ord}_m \mathcal{B}_i^*$. Choose a polynomial $P \in \mathfrak{p}$ with $\mathrm{ord}_m P = \mathrm{ord}_m \mathfrak{p}$. Since

$$\mathrm{ord}_m \Delta P = \mathrm{ord}_m P - 1 < \mathrm{ord}_m \mathfrak{p},$$

ΔP does not lie in $\mathfrak{p}$. Let Q be a polynomial lying in every primary component $\mathfrak{q}' \neq \mathfrak{q}$ of $\mathcal{B}_i^*$ and not lying in $\mathfrak{p}$ — for example the product of elements from each $\mathfrak{q}' \setminus \mathfrak{p}$. From the definition of exponent we know that P^e lies in $\mathfrak{q}$. So $P^e Q$ lies in $\mathcal{B}_i^*$. Moreover since P lies in $\mathfrak{p}$,

$$\Delta^e (P^e Q) \equiv e!(\Delta P)^e Q \qquad (\mathrm{mod}\ \mathfrak{p}).$$