Rend. Lincei Mat. Appl. 26 (2015), 263–289
DOI 10.4171/RLM/706

Number Theory — *The Skolem–Abouzaïd theorem in the singular case*, by Boris Bartolome, communicated on 13 March 2015.

Abstract. — Let $F(X, Y) \in \mathbb{Q}[X, Y]$ be a $\mathbb{Q}$-irreducible polynomial. In 1929, Skolem ([13]) proved a result allowing explicit bounding of the solutions of $F(X, Y) = 0$ such that $\gcd(X, Y) = d$ in terms of the coefficients of F and d. In 2008, Abouzaïd [1] generalized this result by working with arbitrary algebraic numbers and by obtaining an asymptotic relation between the heights of the coordinates and their logarithmic gcd. However, he imposed the condition that $(0, 0)$ be a non-singular point of the plane curve $F(X, Y) = 0$. In this paper, we remove this constraint[1].

Key words: Skolem–Abouzaïd, Puiseaux series, lgcd, heights

Mathematics Subject Classification (primary; secondary): 11G50; 11D41, 11G30

1. Introduction

Let $F(X, Y) \in \mathbb{Q}[X, Y]$ be a $\mathbb{Q}$-irreducible polynomial. In 1929 Skolem [13] proved the following beautiful theorem:

Theorem 1.1 (Skolem). *Assume that*

$$F(0, 0) = 0. \tag{1}$$

Then for every non-zero integer d, the equation $F(X, Y) = 0$ has only finitely many solutions in integers $(X, Y) \in \mathbb{Z}^2$ with $\gcd(X, Y) = d$.

In the same year, Siegel obtained his celebrated finiteness theorem for integral solutions of Diophantine equations: equation $F(X, Y) = 0$ has finitely many solutions in integers unless the corresponding plane curve is of genus 0 and has at most 2 points at infinity. While Siegel's result is, certainly, deeper and more powerful than Theorem 1.1, the latter has one important advantage. Siegel's theorem is known to be non-effective: it does not give any bound for the size of integral solutions. On the contrary, Skolem's method allows one to bound the solutions explicitly in terms of the coefficients of the polynomial F and the integer d. Indeed, such a bound was obtained by Walsh [14]; see also [9].

In 2008, Abouzaïd [1] gave a far-going generalization of Skolem's theorem. He extended it in two directions.

[1] Presented by U. Zannier.

First, he studied solutions not only in rational integers, but in arbitrary algebraic numbers. To accomplish this, he introduced the notion of *logarithmic gcd* of two algebraic numbers α and β, which coincides with the logarithm of the usual gcd when $\alpha, \beta \in \mathbb{Z}$.

Second, he not only bounded the solution in terms of the logarithmic gcd, but obtained a sort of asymptotic relation between the heights of the coordinates and their logarithmic gcd.

Let us state Abouzaïd's principal result (see [1, Theorem 1.3]). In the sequel we assume that $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ is an absolutely irreducible polynomial, and use the notation

$$m = \deg_X F, \quad n = \deg_Y F, \quad M = \max\{m, n\}. \tag{2}$$

We denote by $\mathrm{h}(\alpha)$ the absolute logarithmic height of $\alpha \in \overline{\mathbb{Q}}$ and by $\mathrm{lgcd}(\alpha, \beta)$ the logarithmic gcd of $\alpha, \beta \in \mathbb{Q}$. We also denote by $\mathrm{h}_p(F)$ the projective height of the polynomial F. For all definitions, see Subsection 2.1.

THEOREM 1.2 (Abouzaïd). *Assume that* $(0, 0)$ *is a non-singular point of the plane curve* $F(X, Y) = 0$. *Let* ε *satisfy* $0 < \varepsilon < 1$. *Then for any solution* $(\alpha, \beta) \in \overline{\mathbb{Q}}^2$ *of* $F(X, Y) = 0$, *we have either*

$$\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \leq 56M^8\varepsilon^{-2}\mathrm{h}_p(F) + 420M^{10}\varepsilon^{-2}\log(4M),$$

or

$$\begin{aligned}\max\{&|\mathrm{h}(\alpha) - n\,\mathrm{lgcd}(\alpha, \beta)|, |\mathrm{h}(\beta) - m\,\mathrm{lgcd}(\alpha, \beta)|\} \\ &\leq \varepsilon \max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} + 742M^7\varepsilon^{-1}\mathrm{h}_p(F) + 5762M^9\varepsilon^{-1}\log(2m + 2n).\end{aligned}$$

Informally speaking,

$$\frac{\mathrm{h}(\alpha)}{n} \sim \frac{\mathrm{h}(\beta)}{m} \sim \mathrm{lgcd}(\alpha, \beta) \tag{3}$$

as $\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \to \infty$.

Unfortunately, Abouzaïd's assumption is slightly more restrictive than Skolem's (1): he assumes not only that the point $(0, 0)$ belongs to the plane curve $F(X, Y) = 0$, but also that $(0, 0)$ is a non-singular point on this curve.

Denote by r the "order of vanishing" of $F(X, Y)$ at the point $(0, 0)$:

$$r = \min\left\{ i + j : \frac{\partial^{i+j} F}{\partial^i X \partial^j Y}(0, 0) \neq 0 \right\}. \tag{4}$$

Clearly, $r > 0$ if and only if $F(0, 0) = 0$ and $r = 1$ if and only $(0, 0)$ is a non-singular point of the plane curve $F(X, Y) = 0$.

We can now state our principal result.

THEOREM 1.3. *Let $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ be an absolutely irreducible polynomial satisfying $F(0, 0) = 0$. Let ε satisfy $0 < \varepsilon < 1$. Then, for any $\alpha, \beta \in \overline{\mathbb{Q}}$ such that $F(\alpha, \beta) = 0$, we have either:*

$$\mathrm{h}(\alpha) \leq 200\varepsilon^{-2} mn^6 (\mathrm{h}_p(F) + 5)$$

or

$$\left| \frac{\mathrm{lgcd}(\alpha, \beta)}{r} - \frac{\mathrm{h}(\alpha)}{n} \right| \leq \frac{1}{r} (\varepsilon \mathrm{h}(\alpha) + 4000\varepsilon^{-1} n^4 (\mathrm{h}_p(F) + \log(mn) + 1) + 30n^2 m(\mathrm{h}_p(F) + \log(nm))).$$

By symmetry, the same kind of bound holds true for the difference $\frac{\mathrm{lgcd}(\alpha,\beta)}{r} - \frac{\mathrm{h}(\beta)}{m}$. Informally speaking,

$$\frac{\mathrm{h}(\alpha)}{n} \sim \frac{\mathrm{h}(\beta)}{m} \sim \frac{\mathrm{lgcd}(\alpha, \beta)}{r} \tag{5}$$

as $\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \to \infty$.

Validity of (5) was stated without proof by Abouzaïd, see the end of Section 1 in [1] (Abouzaïd's definition of r looks different, but it can be easily shown that it is equivalent to ours). The referee pointed us to an unpublished work of Habegger [8] from 2007, where he confirms Abouzaïd's conjecture; moreover, his bounds are sharper than ours. We would like to remark that Habegger's method is quite different and uses his sharp quantitative version of the quasi-equivalence of heights. On the contrary, our paper follows closely the methods of [1] wherever possible; in particular, like in [1], our main tool is Puiseux expansions. While we admit that Habegger's approach is more "industrial" and gives better quantitative results, we feel that Abouzaïd's initial argument is quite enlightening and, perhaps, more natural from certain points of view.

As indicated above, our argument follows, in principle, Abouzaïd's pattern. However, we had to substantially refine his proof at certain points, to accommodate it for the more general set-up of Theorem 1.3. For instance, our Proposition 5.1 comparing the logarithmic gcd with certain "partial height" is considerably more involved than its prototype from [1].

PLAN OF THE ARTICLE. Section 2 and 3 are preliminary: we compile therein some definitions and results from different sources, which will be used in the article. In Section 4 we establish the "Main Lemma", which is the heart of the proof of Theorem 1.3. In Section 5 we complete the proof of Theorem 1.3 using the "Main Lemma".

ACKNOWLEDGMENTS. I am grateful to Yuri Bilu for having pointed my attention to this problem and for an emulating exchange on this topic. I am also thankful to the referee for her/his helpful suggestions and for pointing out the unpublished result from Philip Habbeger.

2. Heights

In this section we recall definitions and collect various results about absolute values and heights.

We normalize the absolute values on number fields so that they extend standard absolute values on $\mathbb{Q}$: if $v \mid p$ (non-Archimedean) then $|p|_v = p^{-1}$ and if $v \mid \infty$ (Archimedean) then $|2015|_v = 2015$.

2.1. Heights and lgcd of algebraic numbers

Let $\mathbb{K}$ be a number field, $d = [\mathbb{K} : \mathbb{Q}]$ and $d_v = [\mathbb{K}_v : \mathbb{Q}_v]$. The *height* of an algebraic number $\alpha \in \mathbb{K}$ is defined as

$$\mathrm{h}(\alpha) = \frac{1}{d} \sum_{v \in M_{\mathbb{K}}} d_v \log^+ |\alpha|_v.$$

where $M_{\mathbb{K}}$ is the set of places (normalized absolute values) of the number field $\mathbb{K}$ and $\log^+ = \max\{\log, 0\}$. It is well-known that the height does not depend on the particular choice of $\mathbb{K}$, but only on the number α itself. It is equally well-known that $\mathrm{h}(\alpha) = \mathrm{h}(\alpha^{-1})$, so that

$$\mathrm{h}(\alpha) = \frac{1}{d} \sum_{v \in M_{\mathbb{K}}} -d_v \log^- |\alpha|_v = \sum_{v \in M_{\mathbb{K}}} \mathrm{h}_v(\alpha),$$

where $\log^- = \min\{\log, 0\}$ and

$$\mathrm{h}_v(\alpha) = -\frac{d_v}{d} \log^- |\alpha|_v.$$

The quantities $\mathrm{h}_v(\alpha)$ can be viewed as "local heights". Clearly, $\mathrm{h}_v(\alpha) \geq 0$ for any v and α.

We define the *logarithmic gcd* of two algebraic numbers α and β, not both 0, as

$$\mathrm{lgcd}(\alpha, \beta) = \sum_{v \in M_K} \min\{\mathrm{h}_v(\alpha), \mathrm{h}_v(\beta)\},$$

where $\mathbb{K}$ is a number field containing both α and β. It again depends only α and β, not on $\mathbb{K}$. A simple verification shows that for $\alpha, \beta \in \mathbb{Z}$ we have $\mathrm{lgcd}(\alpha, \beta) = \log \gcd(\alpha, \beta)$.

Now let $\mathbb{K}$ be a number field and S be a set of places of $\mathbb{K}$. We define the *S-height* by

$$\mathrm{h}_S(\alpha) = \sum_{v \in S} \mathrm{h}_v(\alpha).$$

Similarly we define lgcd_S. We shall frequently use the inequality $\mathrm{lgcd}_S(\alpha, \beta) \leq \mathrm{h}_S(\alpha) \leq \mathrm{h}(\alpha)$ without special reference.

2.2. *Affine and projective heights of polynomials*

We define the projective and the affine height of a vector $\underline{a} = (a_1, \ldots, a_m) \in \overline{\mathbb{Q}}^m$ with algebraic entries, by

$$\mathrm{h}_p(\underline{a}) = \frac{1}{d} \sum_{v \in M_{\mathbb{K}}} d_v \log \max_{1 \le k \le m} |a_k|_v \quad (\underline{a} \neq \underline{0}),$$

$$\mathrm{h}_a(\underline{a}) = \frac{1}{d} \sum_{v \in M_{\mathbb{K}}} d_v \log^+ \max_{1 \le k \le m} |a_k|_v.$$

Here, $\mathbb{K}$ is a number field containing $a_1, \ldots, a_m$, and d, d_v are defined as in the previous subsection. We notice that the height of an algebraic number defined in the previous subsection corresponds to the affine height of a one-dimensional vector.

We define the projective and affine height of a polynomial as the corresponding heights of the vector of its non-zero coefficients. If F is a non-zero polynomial, then, for $\alpha \in \overline{\mathbb{Q}}^*$ we have $\mathrm{h}_p(\alpha F) = \mathrm{h}_p(F)$. Also, $\mathrm{h}_p(F) \le \mathrm{h}_a(F)$, with $\mathrm{h}_p(F) = \mathrm{h}_a(F)$ if F has a coefficient equal to 1.

In [11, Lemma 4], Schmidt proves the following lemma:

LEMMA 2.1. *Let $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ be a polynomial with algebraic coefficients, such that $m = \deg_X F$ and $n = \deg_Y F$. Let $R_F(X) = \mathrm{Res}_Y(F, F'_Y)$ be the resultant of F and its derivative polynomial with respect to Y. Then:*

$$\mathrm{h}_p(R_F) \le (2n-1)\mathrm{h}_p(F) + (2n-1)\log((m+1)(n+1)\sqrt{n}). \tag{6}$$

It is well-known that the height of a root of a polynomial is bounded in terms of the height of the polynomial itself. The following lemma can be found in [3, Proposition 3.6]:

LEMMA 2.2. *Let $F(X)$ be a polynomial of degree m with algebraic coefficients. Let α be a root of F. Then, $\mathrm{h}(\alpha) \le \mathrm{h}_p(F) + \log 2$.*

We want to generalize this to a system of two algebraic equations in two variables.

LEMMA 2.3. *Let $F_1(X, Y)$ and $F_2(X, Y)$ be polynomials with algebraic coefficients, having no common factor. Put:*

$$m_i = \deg_X F_i, \quad n_i = \deg_Y F_i \quad (i = 1, 2).$$

Let α, β be algebraic numbers satisfying $F_1(\alpha, \beta) = F_2(\alpha, \beta) = 0$. Then

$$\mathrm{h}(\alpha) \le n_1\mathrm{h}_p(F_2) + n_2\mathrm{h}_p(F_1) + (m_1n_2 + m_2n_1) + (n_1 + n_2)\log(n_1 + n_2) + \log 2.$$

PROOF. Since F_1 and F_2 have no common factor, their Y-divisor $R(X)$ is a non-zero polynomial, and $R(\alpha) = 0$. [1, Proposition 2.4] gives the estimate

$$\mathrm{h}_p(R) \leq n_1 \mathrm{h}_p(F_2) + n_2 \mathrm{h}_p(F_1) + (m_1 n_2 + m_2 n_1) + (n_1 + n_2)\log(n_1 + n_2).$$

Combining this with Lemma 2.2, the result follows. □

We will also use [1, Proposition 2.5]:

LEMMA 2.4. *Let $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ be a polynomial with $m = \deg_X F$ and $n = \deg_Y F$ and let α, β be two algebraic numbers. Then*

1. *We have* $\mathrm{h}(F(\alpha, \beta)) \leq \mathrm{h}_a(F) + m\mathrm{h}(\alpha) + n\mathrm{h}(\beta) + \log((m+1)(n+1))$.
2. *If $F(\alpha, \beta) = 0$ with $F(\alpha, Y)$ not vanishing identically, then:*

$$\mathrm{h}(\beta) \leq \mathrm{h}_p(F) + m\mathrm{h}(\alpha) + n + \log(m+1).$$

2.3. *Coefficients versus roots*

In this subsection we establish some simple relations between coefficients and roots of a polynomial over a field with absolute value, needed in the proof of our main result. It will be convenient to use the notion of *v-Mahler measure* of a polynomial.

Let $\mathbb{K}$ be a field with absolute value v and $f(X) \in \mathbb{K}[X]$ a polynomial of degree n. Let $\beta_1, \ldots, \beta_n \in \overline{\mathbb{K}}$ be the roots of f:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 = a_n (X - \beta_1) \ldots (X - \beta_n).$$

Define the v-Mahler measure of f by

$$M_v(f) = |a_n|_v \prod_{i=1}^{n} \max\{1, |\beta_i|_v\},$$

where we extend v somehow to $\overline{\mathbb{K}}$. (Clearly, $M_v(f)$ does not depend on the particular extension of v.) It is well-known that $|f|_v = M_v(f)$ for non-archimedean v ("Gauss lemma") and $M_v(f) \leq (n+1)|f|_v$ for archimedean v (Mahler).

LEMMA 2.5. *Let $\beta_1, \ldots, \beta_{\ell+1}$ be $\ell + 1$ distinct roots of $f(X)$, where $0 \leq \ell \leq n - 1$. Then*

$$\max\{|\beta_1|_v, \ldots, |\beta_{\ell+1}|_v\} \geq c_v(n) \frac{|a_\ell|_v}{|f|_v},$$

where $c_v(n) = 1$ for non-archimedean v and $c_v(n) = (n+1)^{-1} 2^{-n}$ for archimedean v.

PROOF. We have

$$a_\ell = \pm a_n \sum_{1 \le i_1 < \cdots < i_{n-\ell} \le n} \beta_{i_1} \dots \beta_{i_{n-\ell}}, \tag{7}$$

where $\beta_1, \dots, \beta_n$ are all roots of $f(X)$ in $\overline{\mathbb{K}}$ counted with multiplicities. Observe that each term in the sum above contains one of the roots $\beta_1, \dots, \beta_{\ell+1}$, and the product of the other roots together with a_n is v-bounded by $M_v(f)$. Hence, denoting $\mu = \max\{|\beta_1|_v, \dots, |\beta_{\ell+1}|_v\}$, we obtain $|a_\ell|_v \le \mu M_v(f)$ in the non-archimedean case and $|a_\ell|_v \le \binom{n}{\ell} \mu M_v(f)$ in the archimedean case. Since $\binom{n}{\ell} \le 2^n$, the result follows. □

2.4. *Siegel's "Absolute" Lemma*

In this section we give a version of the Absolute Siegel's Lemma due to David and Philippon [3], adapted for our purposes.

We start from a slightly modified definition of the projective height of a non-zero vector $\underline{a} = (a_1, \dots, a_n) \in \overline{\mathbb{Q}}^n$. As before, we fix a number field $\mathbb{K}$ containing $a_1, \dots, a_n$ and set $d = [\mathbb{K} : \mathbb{Q}]$, $d_v = [\mathbb{K}_v : \mathbb{Q}_v]$ for $v \in M_{\mathbb{K}}$.

Now we define

$$\mathrm{h}_s(\underline{a}) = \sum_{v \in M_{\mathbb{K}}} \frac{d_v}{d} \log \|\underline{a}\|_v,$$

where

$$\|\underline{a}\|_v = \begin{cases} \max\{|a_1|_v, \dots, |a_n|_v\}, & v < \infty, \\ (|a_1|_v^2 + \cdots + |a_n|_v^2)^{1/2}, & v \mid \infty. \end{cases}$$

This definition is the same as for $\mathrm{h}_p(\underline{a})$, except that for the archimedean places the sup-norm is replaced by the euclidean norm. We have clearly $\mathrm{h}_s(\lambda \underline{a}) = \mathrm{h}_s(\underline{a})$ for $\lambda \in \overline{\mathbb{Q}}^\times$, and

$$\mathrm{h}_p(\underline{a}) \le \mathrm{h}_s(\underline{a}) \le \mathrm{h}_p(\underline{a}) + \frac{1}{2} \log n. \tag{8}$$

Now let us define the height of a linear subspace of $\overline{\mathbb{Q}}^n$. If W is a 1-dimensional subspace of $\overline{\mathbb{Q}}^n$ then we set

$$\mathrm{h}_s(W) := \mathrm{h}_s(\underline{w}),$$

where $\underline{w}$ is an arbitrary non-zero vector from W. Clearly, $\mathrm{h}_s(W)$ does not depend on the particular choice of the vector $\underline{w}$.

To extend this to subspaces of arbitrary dimension, we use Grassmann spaces. Recall that the mth Grassmann space $\bigwedge^m \overline{\mathbb{Q}}^n$ is of dimension $\binom{n}{m}$, and has a standard basis consisting of the vectors

$$e_{i_1} \wedge \cdots \wedge e_{i_m}, \quad (1 \le i_1 < \cdots < i_m \le n),$$

where $e_1, \dots, e_n$ is the standard basis of $\overline{\mathbb{Q}}^n$. If W is an m-dimensional subspace of $\overline{\mathbb{Q}}^n$ then $\bigwedge^m W$ is a 1-dimensional subspace of $\bigwedge^m \overline{\mathbb{Q}}^n$, and we simply define

$$\mathrm{h}_s(W) := \mathrm{h}_s\Big(\bigwedge^m W\Big).$$

Finally, we set $\mathrm{h}_s(W) = 0$ for the zero subspace $W = \{\underline{0}\}$.

To make this more explicit, pick a basis $\underline{w}_1, \dots, \underline{w}_m$ of W. Then $\bigwedge^m W$ is generated by $\underline{w}_1 \wedge \cdots \wedge \underline{w}_m$, and we have

$$\mathrm{h}_s(W) = \mathrm{h}_s(\underline{w}_1 \wedge \cdots \wedge \underline{w}_m). \tag{9}$$

This allows one to estimate the height of a subspace generated by a finite set of vectors in terms of heights of generators.

PROPOSITION 2.6. *Let W be a subspace of $\overline{\mathbb{Q}}^n$ generated by vectors $\underline{w}_1, \dots, \underline{w}_m \in \overline{\mathbb{Q}}^n$. Then*

$$\mathrm{h}_s(W) \le \mathrm{h}_s(\underline{w}_1) + \cdots + \mathrm{h}_s(\underline{w}_m).$$

PROOF. Selecting among $\underline{w}_1, \dots, \underline{w}_m$ a maximal linearly independent subset, we may assume that $\underline{w}_1, \dots, \underline{w}_m$ is a basis of W. Then we have (9). It remains to observe that for any place v we have

$$\|\underline{w}_1 \wedge \cdots \wedge \underline{w}_m\|_v \le \|\underline{w}_1\|_v \dots \|\underline{w}_m\|_v.$$

For non-archimedean v this is obvious, and for archimedean v this is the classical Hadamard's inequality. □

We denote by $(\underline{x} \cdot \underline{y})$ the standard inner product on $\overline{\mathbb{Q}}^n$:

$$(\underline{x} \cdot \underline{y}) = x_1 y_1 + \cdots + x_n y_n.$$

Let $W^\perp$ denote the orthogonal complement to W with respect to this product. It is well-known that the coordinates of $\bigwedge^m W$ (where $m = \dim W$) in the standard basis of $\bigwedge^m \overline{\mathbb{Q}}^n$ are the same (up to a scalar multiple) as the coordinates of $\bigwedge^{n-m} W^\perp$ in the standard basis of $\bigwedge^{n-m} \overline{\mathbb{Q}}^n$. In particular,

$$\mathrm{h}_s(W) = \mathrm{h}_s(W^\perp). \tag{10}$$

We use this to estimate the height of the subpace defined by a system of linear equations.

PROPOSITION 2.7. *Let $L_1, \dots, L_m$ be non-zero linear forms on $\overline{\mathbb{Q}}^n$, and let W be the subspace of $\overline{\mathbb{Q}}^n$ defined by $L_1(\underline{x}) = \cdots = L_m(\underline{x}) = 0$. Then*

$$\mathrm{h}_s(W) \le \mathrm{h}_p(L_1) + \cdots + \mathrm{h}_p(L_m) + \frac{m}{2} \log n. \tag{11}$$

PROOF. Let $\underline{a}_1, \dots, \underline{a}_m$ be vectors in $\overline{\mathbb{Q}}^n$ such that $L_i(\underline{x}) = (\underline{x} \cdot \underline{a}_i)$. Then

$$\mathrm{h}_p(L_i) = \mathrm{h}_p(\underline{a}_i) \quad (i = 1, \dots, m). \tag{12}$$

The space $W^\perp$ is generated by $\underline{a}_1, \dots, \underline{a}_m$. Applying to it Proposition 2.6 and using (8), we obtain

$$\mathrm{h}_s(W^\perp) \le \mathrm{h}_s(\underline{a}_1) + \cdots + \mathrm{h}_s(\underline{a}_m) \le \mathrm{h}_p(\underline{a}_1) + \cdots + \mathrm{h}_p(\underline{a}_m) + \frac{m}{2} \log n.$$

Together with (10) and (12), this gives (11). □

REMARK 2.8. It is not difficult to slightly refine (11), replacing $\log n$ by $\log m$ in the right-hand side, but this would not lead to any substantial improvement of our results.

In [3, Lemma 4.7] the following version of "absolute Siegel's lemma" is given.

PROPOSITION 2.9. *Let W be an ℓ-dimensional subspace of $\overline{\mathbb{Q}}^n$ and $\varepsilon > 0$. Then, there is a non-zero vector $\underline{x} \in W$, satisfying:*

$$\mathrm{h}_p(\underline{x}) \le \frac{\mathrm{h}_s(W)}{\ell} + \frac{1}{2\ell} \sum_{i=1}^{\ell-1} \sum_{k=1}^{i} \frac{1}{k} + \varepsilon.$$

COROLLARY 2.10. *Let $L_1, \dots, L_m$ be non-zero linear forms in n variables with algebraic coefficients. Then, there exists a non-zero vector $\underline{x} \in \overline{\mathbb{Q}}^n$ such that $L_1(\underline{x}) = \cdots = L_m(\underline{x}) = 0$ and*

$$\mathrm{h}_p(\underline{x}) \le \frac{1}{n-m} (\mathrm{h}_p(L_1) + \cdots + \mathrm{h}_p(L_m)) + \frac{1}{2} \frac{n}{n-m} \log n. \tag{13}$$

PROOF. We apply Proposition 2.9 with W the subspace defined by $L_1(\underline{x}) = \cdots = L_m(\underline{x}) = 0$. Denoting $\ell = \dim W$, we have clearly $n - m \le r \le n$ and

$$\frac{1}{2\ell} \sum_{i=1}^{\ell-1} \sum_{k=1}^{i} \frac{1}{k} < \frac{1}{2} \log \ell \le \frac{1}{2} \log n.$$

Hence there exists a non-zero $\underline{x} \in W$ satisfying

$$\mathrm{h}_p(\underline{x}) \le \frac{1}{n-m} \mathrm{h}_s(W) + \frac{1}{2} \log n.$$

Using (11), we find

$$\mathrm{h}_p(\underline{x}) \le \frac{1}{n-m} (\mathrm{h}_p(L_1) + \cdots + \mathrm{h}_p(L_m)) + \frac{1}{2} \frac{m}{n-m} \log n + \frac{1}{2} \log n,$$

which is (13). □

3. Power series

In this section we recall various results about power series, used in our proof.

3.1. Puiseux Expansions

Let $\mathbb{K}$ be a field of characteristic 0, and $\mathbb{K}((x))$ the field of formal power series over $\mathbb{K}$. It is well-known that an extension of $\mathbb{K}((x))$ of degree n is a subfield of a field of the form $\mathbb{L}((x^{1/e}))$, where e is a positive integer (the ramification index), $\mathbb{L}$ is a finite extension of $\mathbb{K}$, and

$$[\mathbb{L} : \mathbb{K}], \quad e \leq n.$$

This fact (quoted sometimes as the "Theorem of Puiseux") has the following consequence: if we fix an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, then the algebraic closure of $\mathbb{K}((x))$ can be given by

$$\overline{\mathbb{K}((x))} = \bigcup_{e=1}^{\infty} \bigcup_{\substack{\mathbb{K} \subset \mathbb{L} \subset \overline{\mathbb{K}} \\ [\mathbb{L}:\mathbb{K}] < \infty}} \mathbb{L}((x^{1/e})),$$

where the interior union is over all subfields $\mathbb{L}$ of $\overline{\mathbb{K}}$ finite over $\mathbb{K}$.

Another immediate consequence of the "Theorem of Puiseux" is the following statement:

Proposition 3.1. *Let*

$$F(X, Y) = f_n(X) Y^n + \cdots + f_0(X) \in \mathbb{K}[X, Y]$$

be a polynomial of Y-degree n. Then there exists a finite extension $\mathbb{L}$ of $\mathbb{K}$, positive integers $e_1, \ldots, e_n$, all not exceeding n, and series $y_i \in \mathbb{L}((x^{1/e_i}))$ such that

$$F(x, Y) = f_n(x)(Y - y_1) \cdots (Y - y_n). \tag{14}$$

Write the series $y_1, \ldots, y_n$ as

$$y_i = \sum_{k=\kappa_i}^{\infty} a_{ik} x^{k/e_i}$$

with $a_{i\kappa_i} \neq 0$. It is well-known and easy to show that

$$|\kappa_i| \leq \deg_X F \quad (i = 1, \ldots, n).$$

This inequality will be used throughout the article without special notice.

We want to link the numbers e_i and κ_i with the "order of vanishing" at $(0, 0)$, introduced in (4).

PROPOSITION 3.2. *Let $F(X, Y) \in \mathbb{K}[X, Y]$ and $y_1, \ldots, y_n$ be as above, and assume that $F(0, Y)$ is not identically 0. Then the quantity r, introduced in (4), satisfies*

$$r = \sum_{\kappa_i > 0} \min\{1, \kappa_i/e_i\}, \tag{15}$$

where the sum extends only to those i for which $\kappa_i > 0$.

PROOF. We denote by v_x the standard additive valuation on $\mathbb{K}((x))$, normalized to have $v_x(x) = 1$. This v_x extends in a unique way to the algebraic closure $\overline{\mathbb{K}((x))}$; precisely, for

$$y(x) = \sum_{k=\kappa}^{\infty} a_k x^{k/e} \in \overline{\mathbb{K}((x))} \quad (a_\kappa \neq 0)$$

we have $v_x(y) = \kappa/e$. Furthermore, for

$$G(x, Y) = g_s(x) Y^s + \cdots + g_0(x) \in \overline{\mathbb{K}((x))}[Y]$$

we set $v_x(G) = \min\{v_x(g_0), \ldots, v_x(g_s)\}$. Gauss' lemma asserts that for $G_1, G_2 \in \overline{\mathbb{K}((x))}[Y]$, we have $v_x(G_1 G_2) = v_x(G_1) + v_x(G_2)$.

Since $F(0, Y)$ is not identically 0, we have $v_x(F(x, Y)) = 0$. Applying Gauss' lemma to (14), we obtain

$$v_x(f_0(x)) + \sum \min\{0, \kappa_i/e_i\} = 0.$$

Hence, setting $\tilde{f}_0 = x^{-v_x(f_0(x))} f_0(x)$, we may re-write (14) as

$$F(x, Y) = \prod_{\kappa_i > 0} (Y - y_i) \cdot \tilde{f}_0(x) \prod_{\kappa_i \leq 0} (x^{-\kappa_i/e_i} Y - x^{-\kappa_i/e_i} y_i). \tag{16}$$

Now set $G(x, Y) = F(x, xY)$. Then clearly $r = v_x(G)$. Applying Gauss' Lemma to the decomposition

$$G(x, Y) = \prod_{\kappa_i > 0} (xY - y_i) \cdot \tilde{f}_0(x) \prod_{\kappa_i \leq 0} (x^{1-\kappa_i/e_i} Y - x^{-\kappa_i/e_i} y_i),$$

we obtain (15). □

Here is one more useful property.

PROPOSITION 3.3. *In the set-up of Proposition 3.2, assume that $\kappa_i > 0$ for exactly ℓ indexes $i \in \{1, \ldots, n\}$. Then $f_k(0) = 0$ for $k < \ell$, but $f_\ell(0) \neq 0$.*

PROOF. Re-write (16) as

$$F(x, Y) = \prod_{\kappa_i>0}(Y - y_i) \prod_{\kappa_i=0}(Y - y_i) \cdot \tilde{f}_0(x) \prod_{\kappa_i<0}(x^{-\kappa_i/e_i} Y - x^{-\kappa_i/e_i} y_i).$$

Substituting $x = 0$, every factor in the first product becomes Y, every factor in the second product becomes $Y - a_{i0}$, with $a_{i0} \neq 0$, and every factor in the third product (including $\tilde{f}_0(0)$) becomes constant. Whence the result. □

3.2. Eisenstein's theorem

In this subsection, we recall the quantitative Eisentsein's theorem due to work from Dwork, Robba, Schmidt and Van der Poorten [6, 7, 11], as given in [3]. It will be convenient to use the notion of $M_{\mathbb{K}}$-divisor.

An $M_{\mathbb{K}}$-divisor is an infinite vector $(A_v)_{v \in M_{\mathbb{K}}}$ of positive real numbers, each A_v being associated to one $v \in M_{\mathbb{K}}$, such that for all but finitely many $v \in M_{\mathbb{K}}$ we have $A_v = 1$. An $M_{\mathbb{K}}$-divisor is effective if for all $v \in M_{\mathbb{K}}$, $A_v \geq 1$.

We define the *height* of an $M_{\mathbb{K}}$-divisor $\mathscr{A} = (A_v)_{v \in M_{\mathbb{K}}}$ as

$$\mathrm{h}(\mathscr{A}) = \sum_{v \in M_{\mathbb{K}}} \frac{d_v}{d} \log A_v. \tag{17}$$

The following version of Eisenstein's theorem is from [3, Theorem 7.5].

THEOREM 3.4. *Let $F(X, Y)$ be a separable polynomial of degrees $m = \deg_X F$ and $n = \deg_Y F$. Further, let $y(x) = \sum_{k=\kappa}^{\infty} a_k x^{k/e} \in \mathbb{K}[[x^{1/e}]]$ be a power series satisfying $F(x, y(x)) = 0$. (Here we do not assume that $a_\kappa \neq 0$.) Then there exists an effective $M_{\mathbb{K}}$-divisor $\mathscr{A} = (A_v)_{v \in M_{\mathbb{K}}}$ such that:*

$$|a_k|_v \leq \max\{1, |a_{e\lfloor \kappa/e \rfloor}|_v\} A_v^{k/e - \lfloor \kappa/e \rfloor},$$

for any $v \in M_{\mathbb{K}}$ and any $k \geq \kappa$, and such that $\mathrm{h}(\mathscr{A}) \leq 4n\mathrm{h}_p(F) + 3n\log(nm) + 10en$.

Applying this theorem to the series of the form $a_1 x^{1/e} + a_2 x^{2/e} + \cdots$ (that is, with $a_k = 0$ for $k \leq 0$) and setting $\kappa = 0$, we obtain that:

COROLLARY 3.5. *Let $F(X, Y)$ be a separable polynomial of degrees $m = \deg_X F$ and $n = \deg_Y F$. Further, let $y(x) = \sum_{k=1}^{\infty} a_k x^{k/e} \in \mathbb{K}[[x^{1/e}]]$ be a power series satisfying $F(x, y(x)) = 0$. Then, there exists an effective $M_{\mathbb{K}}$-divisor $\mathscr{A} = (A_v)_{v \in M_{\mathbb{K}}}$ such that:*

$$|a_k|_v \leq A_v^{k/e} \quad (v \in M_{\mathbb{K}}, k = 1, 2, \ldots), \tag{18}$$

and such that

$$\mathrm{h}(\mathscr{A}) \leq 4n\mathrm{h}_p(F) + 3n\log(nm) + 10en. \tag{19}$$

The following lemma is a slightly modified version of Proposition 2.7 from [1]:

LEMMA 3.6. *Let $\mathbb{K}$ be a number field and let $y(x) = \sum_{k=1}^{\infty} a_k x^{k/e}$ be a series with coefficients in $\mathbb{K}$. Assume further that there exists an effective $M_{\mathbb{K}}$-divisor $\mathscr{A} = (A_v)_{v \in M_{\mathbb{K}}}$, such that for all $k \geq 1$ we have $|a_k|_v \leq A_v^{k/e}$. For $\ell \in \mathbb{N}$ write $y(x)^{\ell} = \sum_{k=1}^{\infty} a_k^{(\ell)} c^{k/e}$. Then, for any $v \in M_K$ and for all $k \geq 1$ we have:*

$$|a_k^{(\ell)}|_v \leq \begin{cases} 2^{\ell+k} A_v^{k/e}, & \text{if } v \mid \infty, \\ A_v^{k/e}, & \text{if } v < \infty. \end{cases} \tag{20}$$

In [1], a slightly sharper estimate, with $\binom{\ell+k-1}{k}$ instead of $2^{\ell+k}$ is given.

4. The "Main Lemma"

In this section we prove an auxiliary statement which is crucial for the proof of Theorem 1.3. It can be viewed as a version of the famous Theorem of Sprindzhuk, see [4, 2]. In fact, our argument is an adaptation of that from [2]. We follow [1, Sections 3.1–3.3] with some changes.

4.1. Statement of the Main Lemma

In this section $\mathbb{K}$ is a number field, $F(X, Y) \in \mathbb{K}[X, Y]$ an absolutely irreducible polynomial of degrees $m = \deg_X F$ and $n = \deg_Y F$, and $\alpha, \beta \in \mathbb{K}^{\times}$ satisfy $F(\alpha, \beta) = 0$. Furthermore, everywhere in this section except Subsection 4.6

$$y(x) = \sum_{k=1}^{\infty} a_k x^k \in \mathbb{K}[[x]]$$

is a power series satisfying $F(x, y(x)) = 0$; in particular, $F(0, 0) = 0$.

We consider the following finite subset of M_K:

$$T = \{v \in M_{\mathbb{K}} : |\alpha|_v < 1 \text{ and } y(x) \text{ converges } v\text{-adically to } \beta \text{ at } x = \alpha\}.$$

LEMMA 4.1 ("Main Lemma"). *Let ε satisfy $0 < \varepsilon \leq 1$. Then we have either*

$$\mathrm{h}(\alpha) \leq 200\varepsilon^{-2} mn^4 (\mathrm{h}_p(F) + 5), \tag{21}$$

or

$$\left| \frac{\mathrm{h}(\alpha)}{n} - \mathrm{h}_T(\alpha) \right| \leq \varepsilon n \mathrm{h}(\alpha) + 200\varepsilon^{-1} n^2 (\mathrm{h}_p(F) + \log(mn) + 10). \tag{22}$$

4.2. Preparations

The proof of the "Main Lemma" requires some preparation. First of all, recall that, according to Eisenstein's Theorem as given in Corollary 3.5, there exists

an effective $M_{\mathbb{K}}$-divisor $\mathscr{A} = (A_v)_{v \in M_{\mathbb{K}}}$ such that both (18) and (19) hold with $e = 1$:

$$|a_k|_v \le A_v^k \quad (v \in M_{\mathbb{K}},\ k = 1, 2, \ldots),$$
$$\mathrm{h}(\mathscr{A}) \le 4n\mathrm{h}_p(F) + 3n\log(nm) + 10n.$$

We fix this $\mathscr{A}$ until the end of the section.

Next, we need to construct an "auxiliary polynomial".

PROPOSITION 4.2 (Auxiliary polynomial). *Let δ be a real number $0 < \delta \le 1/2$ and let N be a positive integer. There exists a non-zero polynomial $G(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ satisfying* $\deg_X G \le N$, $\deg_Y G \le n - 1$,

$$v_x(G(x, y(x))) \ge (1 - \delta)Nn, \tag{23}$$

$$\mathrm{h}_p(G) \le \delta^{-1} nN(\mathrm{h}(\mathscr{A}) + 3). \tag{24}$$

PROOF. It is quite analogous to the proof of Proposition 3.1 in [1]. Condition (23) is equivalent to a system of $(1 - \delta)Nn$ linear equations in the $n(N + 1)$ coefficients of G. Each coefficient of each linear equation is a coefficient of x^k, for $k \le Nn$, one of the series $y(x)^\ell$ for $\ell = 0, \ldots, n - 1$.

Using (18) and Lemma 3.6, we estimate the height of every equation as $nN\mathrm{h}(\mathscr{A}) + (Nn + n)\log 2$. Corollary 2.10 implies now that we can find a non-zero solution of our system of height at most

$$\delta^{-1}(nN\mathrm{h}(\mathscr{A}) + (Nn + n)\log 2) + \frac{1}{2}\delta^{-1}\log(nN).$$

This is smaller than the right-hand side of (24). □

4.3. Upper Bound

Now we can obtain an upper bound for $\mathrm{h}_T(\alpha)$ in terms of $\mathrm{h}(\alpha)$.

PROPOSITION 4.3 (Upper bound for $\mathrm{h}_T(\alpha)$). *Let δ satisfy $0 < \delta \le 1/2$. Then we have either*

$$\mathrm{h}(\alpha) \le 10\delta^{-2} mn^4(\mathrm{h}_p(F) + 5), \tag{25}$$

or

$$n\mathrm{h}_T(\alpha) \le (1 + 4\delta)\mathrm{h}(\alpha) + 8\delta^{-1} n(\mathrm{h}(\mathscr{A}) + 10) + \mathrm{h}_p(F). \tag{26}$$

PROOF. Fix a positive integer N, to be specified later, and let $G(X, Y)$ be the auxiliary polynomial introduced in Proposition 4.2. Extending the field $\mathbb{K}$, we may assume that $G(X, Y) \in \mathbb{K}[X, Y]$. We may also assume that G has a coeffi-

cient equal to 1; in particular, $|G|_v \geq 1$ for all $v \in M_{\mathbb{K}}$, where we denote by $|G|_v$ the maximum of v-adic norms of coefficients of G.

The series $z(x) = G(x, y(x)) \in \mathbb{K}[[x]]$ can be written as

$$z(x) = \sum_{k=\eta}^{\infty} b_k x^k$$

with $\eta \geq (1-\delta)Nn \geq \frac{1}{2}Nn$ (recall that $\delta \leq 1/2$). Again using (18) and Lemma 3.6, we estimate the coefficients b_k as follows: for $v < \infty$ we have $|b_k|_v \leq |G|_v A_v^k$, and for $v \mid \infty$ we have $|b_k|_v \leq n(N+1)2^{k+n-1}|G|_v A_v^k$. Since for $k \geq \eta \geq \frac{1}{2}Nn$ we have $n(N+1)2^{k+n-1} \leq 8^k$, we obtain the estimate

$$|b_k| \leq \begin{cases} |G|_v A_v^k, & v < \infty, \\ |G|_v (8A_v)^k, & v \mid \infty. \end{cases} \quad (v \in M_k,\ k \geq \eta). \tag{27}$$

Now we distinguish two cases.

CASE 1: $G(\alpha, \beta) = 0$. In this case we have $F(\alpha, \beta) = G(\alpha, \beta) = 0$. We want to apply Lemma 2.3; for this, we have to verify that polynomials F and G do not have a common factor. This is indeed the case, because F is absolutely irreducible, and $\deg_Y G < \deg_Y F$.

Lemma 2.3, combined with (24) and (19), gives

$$\begin{aligned} \mathrm{h}(\alpha) &\leq n\mathrm{h}_p(G) + (n-1)\mathrm{h}_p F + (m(n-1) + Nn) \\ &\quad + (2n-1)\log(2n-1) + \log 2 \\ &\leq \delta^{-1} Nn^2(\mathrm{h}(\mathscr{A}) + 6) + (n-1)(\mathrm{h}_p(F) + m) \\ &\leq 5\delta^{-1} Nn^3(\mathrm{h}_p(F) + 5) + mn. \end{aligned} \tag{28}$$

Below, after specifying N, we will see that this is sharper than (25).

CASE 2: $G(\alpha, \beta) = \gamma \neq 0$. To treat this case it will be convenient to use, instead of the set T, a slightly smaller subset $\tilde{T}$, consisting of $v \in T$ satisfying

$$|\alpha|_v < \begin{cases} A_v^{-1}, & v < \infty, \\ (16A_v)^{-1}, & v \mid \infty. \end{cases}$$

We have clearly

$$0 \leq \mathrm{h}_T(\alpha) - \mathrm{h}_{\tilde{T}}(\alpha) \leq \mathrm{h}(\mathscr{A}) + \log 16, \tag{29}$$

and (27) implies the estimate

$$|b_k \alpha^k|_v < \begin{cases} |G|_v A_v^\eta |\alpha|_v^\eta, & v < \infty, \\ |G|_v (8A_v)^\eta |\alpha|_v^\eta \cdot (1/2)^{k-\eta}, & v \mid \infty. \end{cases} \quad (v \in \tilde{T},\ k \geq \eta). \tag{30}$$

Recall that for $v \in T$, the series $y(x)$ converges v-adically to β at $x = \alpha$. Hence the same holds true for $v \in \tilde{T}$. It follows that, for $v \in \tilde{T}$, the series $z(x) = G(x, y(x))$ converges v-adically to[2] $G(\alpha, \beta) = \gamma$.

Using (30), we can estimate $|\gamma|_v$ for $v \in \tilde{T}$:

$$|\gamma|_v < \begin{cases} |G|_v A_v^{\eta} |\alpha|_v^{\eta}, & v < \infty, \\ 2|G|_v (8A_v)^{\eta} |\alpha|_v^{\eta}, & v \mid \infty. \end{cases} \qquad (v \in \tilde{T},\ k \geq \eta).$$

Using this and remembering that $|G|_v \geq 1$ for all v, we obtain the following lower estimate for $\mathrm{h}(\gamma)$:

$$\begin{aligned} \mathrm{h}(\gamma) &\geq \mathrm{h}_{\tilde{T}}(\gamma) \\ &\geq \eta \mathrm{h}_{\tilde{T}}(\alpha) - \mathrm{h}_p(G) - \eta \mathrm{h}(\mathscr{A}) - \eta \log 16 - \log 2 \\ &\geq Nn(1-\delta)\mathrm{h}_{\tilde{T}}(\alpha) - 2\delta^{-1} nN(\mathrm{h}(\mathscr{A}) + 6). \end{aligned}$$

Combining this with (29), we obtain

$$\mathrm{h}(\gamma) \geq Nn(1-\delta)\mathrm{h}_T(\alpha) - 3\delta^{-1} nN(\mathrm{h}(\mathscr{A}) + 6). \tag{31}$$

On the other hand, using Lemma 2.4 it is easy to bound $\mathrm{h}(\gamma)$ from above. Indeed, part 2 of this lemma implies that

$$\mathrm{h}(\beta) \leq \mathrm{h}_p(F) + m\mathrm{h}(\alpha) + n + \log(m+1),$$

and part 1 implies that

$$\mathrm{h}(\gamma) \leq \mathrm{h}_a(G) + N\mathrm{h}(\alpha) + (n-1)\mathrm{h}(\beta) + \log((N+1)n).$$

Since G has a coefficient equal to 1, we have $\mathrm{h}_a(G) = \mathrm{h}_p(G) \leq \delta^{-1} nN(\mathrm{h}(\mathscr{A}) + 3)$. Hence

$$\begin{aligned} \mathrm{h}(\gamma) &\leq \mathrm{h}_p(G) + N\mathrm{h}(\alpha) + (n-1)(\mathrm{h}_p(F) + m\mathrm{h}(\alpha) + n + \log(m+1)) + \log((N+1)n) \\ &\leq (N+mn)\mathrm{h}(\alpha) + \delta^{-1} nN(\mathrm{h}(\mathscr{A}) + 4) + n\mathrm{h}_p(F) + n^2 + n\log(m+1). \end{aligned}$$

Combining this with (31) and dividing by N, we obtain

$$\begin{aligned} n(1-\delta)\mathrm{h}_T(\alpha) \leq \Big(1 + \frac{mn}{N}\Big)\mathrm{h}(\alpha) + 4\delta^{-1} n(\mathrm{h}(\mathscr{A}) + 6) \\ + N^{-1}(n\mathrm{h}_p(F) + n^2 + n\log(m+1)). \end{aligned} \tag{32}$$

[2] For archimedean v to make this conclusion we need absolute convergence of $y(x)$ at $x = \alpha$, which is obvious for $v \in \tilde{T}$.

COMPLETING THE PROOF OF PROPOSITION 4.3. Now it is the time to specify N: we set $N = \lceil \delta^{-1} mn \rceil$. With this choice of N, inequality (28) is indeed sharper than (25), and inequality (32) implies the following:

$$n(1-\delta)\mathrm{h}_T(\alpha) \le (1+\delta)\mathrm{h}(\alpha) + 4\delta^{-1}n(\mathrm{h}(\mathscr{A}) + 10) + \delta \mathrm{h}_p(F).$$

Since $\delta \le 1/2$, this is sharper than (26). □

4.4. Lower Bound

Our next objective is a lower bound for $\mathrm{h}_T(\alpha)$. We will see that it easily follows from the upper bound.

PROPOSITION 4.4 (Lower bound for $\mathrm{h}_T(\alpha)$). *Let δ satisfy $0 < \delta \le 1/2$. Then we have either* (25) *or*

$$n\mathrm{h}_T(\alpha) \ge (1 - 4n\delta)\mathrm{h}(\alpha) - 9\delta^{-1}n^2(\mathrm{h}(\mathscr{A}) + 10) - n\mathrm{h}_p(F). \tag{33}$$

PROOF. Remark first of all that we may assume that the polynomial $F(\alpha, Y)$ is of degree n and separable. Indeed, if this is not the case, then $R_F(\alpha) = 0$, where $R_F(X)$ is the Y-resultant of $F(X, Y)$ and its Y-derivative $F'_Y(X, Y)$. In this case, the joint application of Lemmas 2.1 and 2.2 gives

$$\mathrm{h}(\alpha) \le 2n\mathrm{h}_p(F) + 2n\log((m+1)(n+1)\sqrt{n}) + \log 2,$$

sharper than (25).

Thus, $F(\alpha, Y)$ has n distinct roots in $\overline{\mathbb{Q}}$, one of which is β; we denote them $\beta_1 = \beta, \beta_2, \ldots, \beta_n$. Extending the field $\mathbb{K}$, we may assume that $\beta_1, \ldots, \beta_n \in \mathbb{K}$.

Set $S = \{v \in M_{\mathbb{K}} : |\alpha|_v < 1\}$. For $i = 1, \ldots, n$ we let T_i be the set of $v \in S$ such that $y(x)$ converges v-adically to β_i at $x = \alpha$; in particular, $T_1 = T$. The sets $T_1, \ldots, T_n$ are clearly disjoint, and we have

$$S \supset T_1 \cup \cdots \cup T_n \supset \tilde{S}, \tag{34}$$

where $\tilde{S}$ consists of $v \in S$ for which $|\alpha|_v < A_v^{-1}$. The left inclusion in (34) is trivial, and to prove the right one just observes that for every $v \in \tilde{S}$, the series $y(x)$ absolutely converges v-adically at $x = \alpha$, and, since $F(x, y(x)) = 0$, the sum must be a root of $F(\alpha, Y)$.

Clearly,

$$0 \le \mathrm{h}(\alpha) - \mathrm{h}_{\tilde{S}}(\alpha) = \mathrm{h}_S(\alpha) - \mathrm{h}_{\tilde{S}}(\alpha) \le \mathrm{h}(\mathscr{A}).$$

It follows that

$$\mathrm{h}_{T_1}(\alpha) + \cdots + \mathrm{h}_{T_n}(\alpha) \ge \mathrm{h}_{\tilde{S}}(\alpha) \ge \mathrm{h}(\alpha) - \mathrm{h}(\mathscr{A}).$$

Now observe that the upper bound (26) holds true with T replaced by any T_i:

$$n\mathrm{h}_{T_i}(\alpha) \le (1 + 4\delta)\mathrm{h}(\alpha) + 8\delta^{-1}n(\mathrm{h}(\mathscr{A}) + 10) + \mathrm{h}_p(F) \quad (i = 1, \ldots, n).$$

The last two inequalities imply that

$$n\mathrm{h}_T(\alpha) = n\mathrm{h}_{T_1}(\alpha) \geq n(\mathrm{h}(\alpha) - \mathrm{h}(\mathscr{A})) - (n-1)((1+4\delta)\mathrm{h}(\alpha) + 8\delta^{-1}n(\mathrm{h}(\mathscr{A}) + 10) + \mathrm{h}_p(F)),$$

which easily transforms into (33). □

4.5. *Proof of the "Main Lemma"*

Using Propositions 4.3 and 4.4 with $\delta = \varepsilon/4$ and dividing by n, we obtain that either (21) holds, or

$$\left|\mathrm{h}_T(\alpha) - \frac{\mathrm{h}(\alpha)}{n}\right| \leq \varepsilon\mathrm{h}(\alpha) + 40\varepsilon^{-1}n(\mathrm{h}(\mathscr{A}) + 10) + \mathrm{h}_p(F).$$

Combining this with (19), we obtain (22). □

4.6. *"Ramified Main Lemma"*

We will actually need a slightly more general statement, allowing ramification in the series $y(x)$. The set-up is as before, except that now we consider the series

$$y(x) = \sum_{k=1}^{\infty} a_k x^{k/e} \in \mathbb{K}[[x^{1/e}]]$$

satisfying $F(x, y(x)) = 0$. We fix an e-th root $\alpha^{1/e}$ and we will assume that it belongs to $\mathbb{K}$. We will now say that the series $y(x)$ converges v-adically to β at α if the series $y(x^e)$ converges v-adically to β at $\alpha^{1/e}$. (Of course, this depends on the particular choice of the root $\alpha^{1/e}$.) We again define T as the set of all $v \in S$ for which $y(x)$ converges v-adically to β at α.

LEMMA 4.5 ("Ramified Main Lemma"). *Let ε satisfy $0 < \varepsilon \leq 1$. Then we have either*

$$\mathrm{h}(\alpha) \leq 200\varepsilon^{-2}me^2n^4(\mathrm{h}_p(F) + 5), \tag{35}$$

or

$$\left|\frac{\mathrm{h}(\alpha)}{n} - \mathrm{h}_T(\alpha)\right| \leq \varepsilon\mathrm{h}(\alpha) + 200\varepsilon^{-1}en^2(\mathrm{h}_p(F) + 2\log(mn) + 10). \tag{36}$$

PROOF. The proof is by reduction to the unramified case. Apply Lemma 4.1 to the polynomial $F(X^e, Y)$, the series $y(x^e)$ and the number $\alpha^{1/e}$. We obtain that either

$$\mathrm{h}(\alpha^{1/e}) \leq 200\varepsilon^{-2}men^6(\mathrm{h}_p(F) + 5),$$

or

$$|\mathrm{h}(\alpha^{1/e}) - n\mathrm{h}_T(\alpha^{1/e})| \le \varepsilon \mathrm{h}(\alpha^{1/e}) + 200\varepsilon^{-1}n^4(\mathrm{h}_p(F) + \log(men) + 10).$$

These estimates easily transform into (35) and (36), respectively, using that

$$\mathrm{h}(\alpha^{1/e}) = e^{-1}\mathrm{h}(\alpha), \quad \mathrm{h}_T(\alpha^{1/e}) = e^{-1}\mathrm{h}_T(\alpha), \quad e \le n. \qquad \square$$

5. Proof of the Main Theorem

In this section we prove Theorem 1.3. First of all, we investigate the relation between $\mathrm{h}_T(\alpha)$ and $\mathrm{lgcd}_T(\alpha, \beta)$, where T is defined as in Section 4.

5.1. *Comparing* $\mathrm{h}_T(\alpha)$ *and* $\mathrm{lgcd}_T(\alpha, \beta)$

In this subsection we retain the set-up of Subsection 4.1, except that we allow ramification in the series $y(x)$, as we did in Subsection 4.6. Thus, in this subsection:

- $\mathbb{K}$ is a number field;
- $F(X, Y) \in \mathbb{K}[X, Y]$ is an absolutely irreducible polynomial;
- $\alpha, \beta \in \mathbb{K}$ satisfy $F(\alpha, \beta) = 0$;
- $y(x) = \sum_{k=1}^{\infty} a_k x^{k/e} \in \mathbb{K}[[x^{1/e}]]$ satisfies $F(x, y(x)) = 0$;
- $T \subset M_{\mathbb{K}}$ is the set of all $v \in M_{\mathbb{K}}$ such that $|\alpha|_v < 1$ and $y(x)$ converges v-adically at α to β.

The v-adic convergence is understood in the same sense as in Subsection 4.6: we fix an e-th root $\alpha^{1/e}$, assume that it belongs to $\mathbb{K}$ and define v-adic convergence of $y(x)$ to β at α as v-adic convergence of $y(x^e)$ to β at $\alpha^{1/e}$.

Let κ be the smallest k such that $a_k \ne 0$; by the assumption, $\kappa > 0$. Then we have $v_x(y) = \kappa/e$ and

$$y(x) = \sum_{k=\kappa}^{\infty} a_k x^{k/e}$$

with $a_\kappa \ne 0$. In this subsection we prove that $\mathrm{lgcd}_T(\alpha, \beta)$ can be approximated by $\min\{1, \kappa/e\}\mathrm{h}_T(\alpha)$.

Proposition 5.1. *In the above set-up we have*

$$|\mathrm{lgcd}_T(\alpha, \beta) - \min\{\kappa/e, 1\}\mathrm{h}_T(\alpha)| \le 30n\kappa \mathrm{h}_p(F) + 30n\kappa \log(nm) + 15en. \tag{37}$$

This statement corresponds to Proposition 3.6 in [1]. Our proof is, however, much more involved, in particular because Abouzaïd did not need the lower estimate.

PROOF. Let $\mathscr{A} = (A_v)_{v \in M_{\mathbb{K}}}$ be the $M_{\mathbb{K}}$-divisor from Corollary 3.5. For the reader's convenience, we reproduce here (18) and (19):

$$|a_k|_v \le A_v^{k/e} \quad (v \in M_{\mathbb{K}},\, k \ge 1),$$
$$\mathrm{h}(\mathscr{A}) \le 4n\mathrm{h}_p(F) + 3n\log(nm) + 10en.$$

As we already did several times in Section 4, it will be convenient to replace T by a smaller subset. Thus, let $\tilde{T}$ consist of $v \in T$ satisfying

$$|\alpha|_v < \begin{cases} A_v^{-\kappa-1} \min\{1, |a_\kappa|_v\}^e, & v < \infty, \\ (1/4)^e A_v^{-\kappa-1} \min\{1, |a_\kappa|_v\}^e, & v < \infty. \end{cases} \tag{38}$$

(Attention: this is not the same $\tilde{T}$ as in Subsection 4.3!) Clearly,

$$0 \le \mathrm{h}_T(\alpha) - \mathrm{h}_{\tilde{T}}(\alpha) \le (\kappa+1)\mathrm{h}(\mathscr{A}) + e\mathrm{h}_{T\setminus\tilde{T}}(a_\kappa).$$

Using (18) we estimate $\mathrm{h}(a_\kappa) \le (\kappa/e)\mathrm{h}(\mathscr{A})$. We obtain

$$0 \le \mathrm{h}_T(\alpha) - \mathrm{h}_{\tilde{T}}(\alpha) \le (\kappa+1)\mathrm{h}(\mathscr{A}) \le 3\kappa\mathrm{h}(\mathscr{A}) + e\log 4, \tag{39}$$

where for the latter estimate we use $\kappa \ge 1$. In particular,

$$0 \le \mathrm{lgcd}_T(\alpha,\beta) - \mathrm{lgcd}_{\tilde{T}}(\alpha,\beta) \le 3\kappa\mathrm{h}(\mathscr{A}) + e\log 4. \tag{40}$$

After this preparation, we can now proceed with the proof. For every $v \in \tilde{T}$ we want to obtain an estimate of the form $c_v|\alpha|_v^{\kappa/e} \le |\beta|_v \le c_v'|\alpha|_v^{\kappa/e}$, where c_v and c_v' are some quantities not depending on α.

Upper estimate for $|\beta|_v$. This is easy. It follows from (38) that

$$|\alpha|_v < \begin{cases} A_v^{-1}, & v < \infty, \\ (4^e A_v)^{-1}, & v < \infty. \end{cases}$$

From this and (18) we deduce that

$$|a_k\alpha^{k/e}|_v < \begin{cases} A_v^{\kappa/e}|\alpha|_v^{\kappa/e}, & v < \infty, \\ A_v^{\kappa/e}|\alpha|_v^{\kappa/e} \cdot (1/4)^{k-\kappa}, & v \mid \infty \end{cases} \quad (k \ge \kappa). \tag{41}$$

Hence

$$|\beta|_v < \begin{cases} A_v^{\kappa/e}|\alpha|_v^{\kappa/e}, & v < \infty, \\ 2A_v^{\kappa/e}|\alpha|_v^{\kappa/e}, & v \mid \infty. \end{cases}$$

Lower estimate for $|\beta|_v$. The lower estimate is slightly more subtle. First, we bound the difference $\beta - a_\kappa\alpha^{\kappa/e}$ from above using (38).

Similarly to (41), we have

$$|a_k\alpha^{k/e}|_v < \begin{cases} A_v^{(\kappa+1)/e}|\alpha|_v^{(\kappa+1)/e}, & v < \infty, \\ A_v^{(\kappa+1)/e}|\alpha|_v^{(\kappa+1)/e} \cdot (1/4)^{(k-\kappa-1)/e}, & v \mid \infty \end{cases} \qquad (k \geq \kappa+1).$$

Hence, presenting $\beta - a_\kappa\alpha^{\kappa/e}$ as the v-adic sum of the series

$$y(x) - a_\kappa x^{\kappa/e} = \sum_{k=\kappa+1}^{\infty} a_k x^{k/e}$$

at $x = \alpha$, we obtain the estimate

$$|\beta - a_\kappa\alpha^{\kappa/e}|_v < \begin{cases} A_v^{(\kappa+1)/e}|\alpha|_v^{(\kappa+1)/e}, & v < \infty, \\ 2A_v^{(\kappa+1)/e}|\alpha|_v^{(\kappa+1)/e}, & v \mid \infty. \end{cases}$$

Combining this with (38), we find

$$|\beta - a_\kappa\alpha^{\kappa/e}|_v < \begin{cases} \min\{|a_\kappa|_v, 1\}|\alpha|_v^{\kappa/e}, & v < \infty, \\ (1/2)\min\{|a_\kappa|_v, 1\}|\alpha|_v^{\kappa/e}, & v \mid \infty. \end{cases}$$

Hence

$$|\beta|_v \geq \begin{cases} \min\{|a_\kappa|_v, 1\}|\alpha|_v^{\kappa/e}, & v < \infty, \\ (1/2)\min\{|a_\kappa|_v, 1\}|\alpha|_v^{\kappa/e}, & v \mid \infty, \end{cases}$$

the lower estimate we were seeking.

COMPLETING THE PROOF OF PROPOSITION 5.1. Thus, we proved that

$$c_v|\alpha|_v^{\kappa/e} \leq |\beta|_v \leq c_v'|\alpha|_v^{\kappa/e}, \tag{42}$$

with

$$c_v = \begin{cases} \min\{|a_\kappa|_v, 1\}, & v < \infty, \\ (1/2)\min\{|a_\kappa|_v, 1\}, & v \mid \infty, \end{cases}, \quad c_v' = \begin{cases} A_v^{\kappa/e}, & v < \infty, \\ 2A_v^{\kappa/e}, & v \mid \infty. \end{cases}$$

From (42) we deduce that for $v \in \tilde{T}$

$$c_v|\alpha|_v^{\min\{\kappa/e,1\}}\max\{|\alpha|_v, |\beta|_v\} \leq c_v'|\alpha|_v^{\min\{\kappa/e,1\}}.$$

(We use here the obvious inequality $c_v \leq 1 \leq c_v'$.) Hence

$$-(\kappa/e)\mathrm{h}(\mathscr{A}) - \log 2 \leq \mathrm{lgcd}_{\tilde{T}}(\alpha, \beta) - \min\{\kappa/e, 1\}\mathrm{h}_{\tilde{T}}(\alpha) \leq \mathrm{h}(a_\kappa) + \log 2.$$

Since $\mathrm{h}(a_\kappa) \leq (\kappa/e)\mathrm{h}(\mathscr{A})$, this implies

$$|\mathrm{lgcd}_{\tilde{T}}(\alpha, \beta) - \min\{\kappa/e, 1\}\mathrm{h}_{\tilde{T}}(\alpha)| \leq (\kappa/e)\mathrm{h}(\mathscr{A}) + \log 2,$$

which, together with (39) and (40) gives

$$|\mathrm{lgcd}_{\tilde{T}}(\alpha,\beta) - \min\{\kappa/e,1\}\mathrm{h}_{\tilde{T}}(\alpha)| \le 7\kappa\mathrm{h}(\mathscr{A}) + 4e.$$

Combining this with (18), we obtain (37). □

5.2. *Proving Theorem 1.3*

Now we are fully equipped for the proof of our main result. We want to show that, assuming

$$\mathrm{h}(\alpha) \ge 200\varepsilon^{-2}mn^6(\mathrm{h}_p(F)+5), \tag{43}$$

we have

$$\left|\frac{\mathrm{lgcd}(\alpha,\beta)}{r} - \frac{\mathrm{h}(\alpha)}{n}\right| \le \frac{1}{r}(\varepsilon\mathrm{h}(\alpha) + 4000\varepsilon^{-1}n^4(\mathrm{h}_p(F)+\log(mn)+1) + 30n^2m(\mathrm{h}_p(F)+\log(nm))). \tag{44}$$

Write $F(X,Y) = f_n(X)Y^n + \cdots + f_0(X)$. According to Proposition 3.1 we have

$$F(x,Y) = f_n(x)(Y-y_1)\dots(Y-y_n).$$

where

$$y_i = \sum_{k=\kappa_i}^{\infty} a_{ik}x^{k/e_i} \in \mathbb{K}((x^{1/e_i})) \quad (i=1,\dots,n).$$

We assume that $a_{i\kappa_i} \ne 0$ for $i=1,\dots,n$, so that $\kappa_i/e_i = v_x(y_i)$.

Denoting by ℓ the number of indexes i such that $\kappa_i > 0$, we may assume that $\kappa_1,\dots,\kappa_\ell > 0$ and $\kappa_{\ell+1},\dots,\kappa_n \le 0$. Propositions 3.2 implies that

$$r = \sum_{i=1}^{\ell} \min\{1,\kappa_i/e_i\}, \tag{45}$$

and Proposition 3.3 implies that $f_\ell(0) \ne 0$. We may normalize polynomial $F(X,Y)$ to have

$$f_\ell(0) = 1.$$

In particular, $|F|_v \ge 1$ for every $v \in M_{\mathbb{K}}$, where $|F|_v$ denotes the maximum of v-adic norms of the coefficients of F, and also $\mathrm{h}_p(F) = \mathrm{h}_a(F)$.

Set $E = \mathrm{lcm}(e_1,\dots,e_\ell)$ and fix an E-th root $\alpha^{1/E}$. This fixes uniquely the roots $\alpha^{1/e_1},\dots,\alpha^{1/e_\ell}$. Extending the field $\mathbb{K}$ we may assume that the coefficients of

the series $y_1, \dots, y_\ell$ belong to $\mathbb{K}$, and the same is true for $\alpha^{1/E}$ (and hence for $\alpha^{1/e_1}, \dots, \alpha^{1/e_\ell}$ as well). Having fixed the root $\alpha^{1/e_i} \in \mathbb{K}$, we may define v-adic convergence of y_i at α, see Subsection 4.6.

Extending further the field $\mathbb{K}$, we may assume that it contains all the roots of the polynomial $F(\alpha, Y)$. Hence, if one of the series $y_1, \dots, y_\ell$ converges v-adically at α (and if the convergence is absolute in the archimedean case), then the sum must belong to $\mathbb{K}$.

Consider the following subsets of $M_{\mathbb{K}}$:

$$S = \{v \in M_K : |\alpha|_v < 1\},$$
$$T_i = \{v \in S : \text{the series } y_i \text{ converges } v\text{-adically to } \beta \text{ at } \alpha\} \quad (i = 1, \dots, \ell).$$

(These sets are not the same T_i as in Subsection 4.4!)

We have clearly $\operatorname{lgcd}(\alpha, \beta) = \operatorname{lgcd}_S(\alpha, \beta)$. If we manage to show that the sets T_i are pairwise disjoint, and that $\mathrm{h}_{S\setminus(T_1\cup\cdots\cup T_\ell)}(\beta)$ is "negligible", then joint application of Lemma 4.5, Proposition 5.1 and identity (45) would prove Theorem 1.3. We will argue like this, only with the sets T_i replaced by slightly smaller subsets.

Let $\mathscr{A}_i = (A_{iv})_{v \in M_{\mathbb{K}}}$ be the $M_{\mathbb{K}}$-divisor for the series y_i given by Corollary 3.5. Define the $M_{\mathbb{K}}$-divisor $\mathscr{A} = (A_v)_{v \in M_{\mathbb{K}}}$ by

$$A_v = \max\{A_{1v}, \dots, A_{\ell v}\} \quad (v \in M_{\mathbb{K}}).$$

We have clearly

$$\begin{aligned} |a_{ki}|_v &\le A_v^{k/e} \quad (v \in M_{\mathbb{K}},\ 1 \le i \le \ell,\ k \ge \kappa_i), \\ \mathrm{h}(\mathscr{A}) &\le \mathrm{h}(\mathscr{A}_1) + \cdots + \mathrm{h}(\mathscr{A}_\ell) \\ &\le 4n^2 \mathrm{h}_p(F) + 3n^2 \log(nm) + 10n^3. \end{aligned} \tag{46}$$

Now let $\tilde{S}$ consist of $v \in S$ satisfying

$$|\alpha|_v < \begin{cases} |F|_v^{-n} A_v^{-1}, & v < \infty, \\ ((n+1)2^{n+3}|F|_v)^{-n} A_v^{-1}, & v \mid \infty, \end{cases} \tag{47}$$

and set $\tilde{T}_i = T_i \cap \tilde{S}$. (This is not the same $\tilde{S}$ that in Subsection 4.4!) Clearly,

$$\begin{aligned} 0 \le \operatorname{lgcd}(\alpha, \beta) - \operatorname{lgcd}_{\tilde{S}}(\alpha, \beta) &\le \mathrm{h}(\alpha) - \mathrm{h}_{\tilde{S}}(\alpha) \\ &= \mathrm{h}_{S\setminus\tilde{S}}(\alpha) \\ &\le \mathrm{h}(\mathscr{A}) + n\mathrm{h}_p(F) + \log((n+1)2^{n+3}) \\ &\le 5n^2 \mathrm{h}_p(F) + 3n^2 \log(nm) + 15n^3, \end{aligned} \tag{48}$$

$$\begin{aligned} 0 \le \operatorname{lgcd}_{T_i\setminus\tilde{T}_i}(\alpha, \beta) &\le \mathrm{h}_{S\setminus\tilde{S}}(\alpha) \\ &\le 5n^2 \mathrm{h}_p(F) + 3n^2 \log(nm) + 15n^3 \\ &\quad (i = 1, \dots, \ell). \end{aligned} \tag{49}$$

Here we used the equality $\mathrm{h}_p(F) = \mathrm{h}_a(F)$.

Mention also that for $v \in \tilde{S}$, we have $|\alpha|_v < A_v^{-1}$, which implies that the series $y_1, \dots, y_\ell$ converge v-adically at α in the completion $\mathbb{K}_v$, the convergence being absolute when v is archimedean. Hence, as we have seen above, the sum must belong to $\mathbb{K}$.

PROPOSITION 5.2. *The sets $\tilde{T}_1, \dots, \tilde{T}_\ell$ pairwise disjoint. Furthermore, if $v \in \tilde{S}$ but $v \notin \tilde{T}_1 \cup \cdots \cup \tilde{T}_\ell$ then*

$$|\beta|_v \geq \begin{cases} |F|_v^{-1}, & v < \infty, \\ ((n+1)2^{n+2}|F|_v)^{-1}, & v \mid \infty. \end{cases} \tag{50}$$

PROOF. The polynomial

$$Q(Y) = (Y - y_1) \dots (Y - y_\ell) \in \mathbb{K}[[x^{1/E}]][Y].$$

divides $F(x, Y)$ in the ring $\mathbb{K}((x^{1/E}))[Y]$. By Gauss' Lemma, $Q(Y)$ divides $F(x, Y)$ in the ring $\mathbb{K}[[x^{1/E}]][Y]$ as well. Moreover, writing $F(x, Y) = Q(Y)U(Y)$ with

$$U(Y) = f_n(x)Y^{n-\ell} + u_{n-\ell-1}Y^{n-\ell-1} + \cdots + u_0 \in \mathbb{K}[[x^{1/E}]](Y),$$

the coefficients $u_0, \dots, u_{n-\ell-1}$ belong to the ring[3] $\mathbb{K}[x, y_1, \dots, y_\ell]$. Recall that for $v \in \tilde{S}$ the series $y_1, \dots, y_\ell$ converge v-adically at α in the field $\mathbb{K}$, the convergence being absolute when v is archimedean. Hence so do the coefficients of U.

Fix $v \in \tilde{S}$ and write

$$\begin{aligned} F(\alpha, Y) = (Y - y_1(\alpha)) \dots (Y - y_\ell(\alpha))(f_n(\alpha)Y^{n-\ell} \\ + u_{n-\ell-1}(\alpha)Y^{n-\ell-1} + \cdots + u_0(\alpha)), \end{aligned}$$

where $y_1(\alpha), \dots, y_\ell(\alpha) \in \mathbb{K}$ the v-adic sum of the corresponding series at α, and similarly for $u_{n-\ell-1}(\alpha), \dots, u_0(\alpha)$. We claim that $F(\alpha, Y)$ is a separable polynomial of degree n; indeed, if this is not the case, then, as we have seen in Subsection 4.4, our α must satisfy (44), which contradicts (43).

Now if $v \in T_i \cap T_j$ for $i \neq j$ then $\beta = y_i(\alpha) = y_j(\alpha)$, and $F(\alpha, Y)$ must have β as a double root, a contradiction. This proves disjointedness of the sets $\tilde{T}_i$.

Now assume that $v \in \tilde{S}$ but $v \notin \tilde{T}_1 \cup \cdots \cup \tilde{T}_\ell$. Then none of the sums $y_1(\alpha), \dots, y_\ell(\alpha)$ is equal to β; in other words $y_1(\alpha), \dots, y_\ell(\alpha), \beta$ are $\ell + 1$ distinct roots of the polynomial

$$P(Y) = F(\alpha, Y) = f_n(\alpha)Y^n + \cdots + f_0(\alpha).$$

[3] This is a consequence of the general algebraic property: let R be a commutative ring, R' a subring and $Q(Y), F(Y) \in R'[Y]$, the polynomial Q being monic; assume that $Q \mid F$ in $R[Y]$; then $Q \mid F$ in $R'[Y]$. Indeed, denoting by a the leading coefficient of F, the polynomial Q divides $G = F - aY^{\deg F - \deg Q}Q$ in $R[Y]$, and $\deg G < \deg F$, so by induction $Q \mid G$ in $R'[Y]$.

We are going to use Lemma 2.5. Since $f_\ell(0) = 1$ and

$$|\alpha|_v < \begin{cases} |F_v|^{-1}, & v < \infty, \\ (2|F|_v)^{-1}, & v \mid \infty, \end{cases}$$

we have

$$|f_\ell(\alpha)|_v \geq \begin{cases} 1, & v < \infty, \\ 1/2, & v \mid \infty, \end{cases} \quad |P|_v \leq \begin{cases} |F|_v, & v < \infty, \\ 2|F|_v, & v \mid \infty. \end{cases}$$

Now Lemma 2.5 implies that

$$\max\{|y_1(\alpha)|_v, \dots, |y_\ell(\alpha)|_v, |\beta|_v\} \geq \begin{cases} |F|_v^{-1}, & v < \infty, \\ ((n+1)2^{n+2}|F|_v)^{-1}, & v \mid \infty. \end{cases} \tag{51}$$

On the other hand, we may estimate $|y_i(\alpha)|_v$ from above using (46) and (47). In what follows we repeatedly use the inequality $e_i \leq n$. Since

$$|\alpha|_v < \begin{cases} A_v^{-1}, & v < \infty, \\ (2^{e_i}A_v)^{-1}, & v \mid \infty \end{cases} \quad (i = 1, \dots, \ell),$$

we have

$$|a_k\alpha^{k/e_i}|_v < \begin{cases} (A_v|\alpha|_v)^{1/e_i}, & v < \infty, \\ (A_v|\alpha|_v)^{1/e_i} \cdot (1/2)^{k-1}, & v \mid \infty \end{cases} \quad (k \geq 1,\ i = 1, \dots, \ell),$$

which implies

$$|y_i(\alpha)|_v < \begin{cases} (A_v|\alpha|_v)^{1/e_i}, & v < \infty, \\ 2(A_v|\alpha|_v)^{1/e_i}, & v \mid \infty \end{cases} \quad (i = 1, \dots, \ell).$$

Now since

$$|\alpha|_v < \begin{cases} |F|_v^{-e_i}A_v^{-1}, & v < \infty, \\ ((n+1)2^{n+3}|F|_v)^{-e_i}A_v^{-1}, & v \mid \infty \end{cases} \quad (i = 1, \dots, \ell),$$

we obtain finally

$$|y_i(\alpha)|_v < \begin{cases} |F|_v^{-1}, & v < \infty, \\ ((n+1)2^{n+2}|F|_v)^{-1}, & v \mid \infty \end{cases} \quad (i = 1, \dots, \ell).$$

Compared with (51), this implies (50). The proposition is proved. □

An immediate consequence of the second statement of Proposition 5.2 is the estimate

$$\operatorname{lgcd}_{\tilde{S}\setminus(\tilde{T}_1\cup\dots\cup\tilde{T}_\ell)} \leq \mathrm{h}_{\tilde{S}\setminus(\tilde{T}_1\cup\dots\cup\tilde{T}_\ell)}(\beta) \leq \mathrm{h}_p(F) + \log((n+1)2^{n+2}) \tag{52}$$

(we again use $\mathrm{h}_a(F) = \mathrm{h}_p(F)$).

Now we collect everything together to prove Theorem 1.3. According to Lemma 4.5, condition (43) implies that

$$\left|\frac{\mathrm{h}(\alpha)}{n} - \mathrm{h}_{T_i}(\alpha)\right| \leq \varepsilon \mathrm{h}(\alpha) + 200\varepsilon^{-1}n^3(\mathrm{h}_p(F) + 2\log(mn) + 10) \quad (i = 1, \ldots, \ell).$$

Combining this with Proposition 5.1 and estimate (49), we obtain

$$\left|\min\left\{\frac{\kappa_i}{e_i}, 1\right\}\frac{\mathrm{h}(\alpha)}{n} - \mathrm{lgcd}_{\tilde{T}_i}(\alpha, \beta)\right| \leq \varepsilon \mathrm{h}(\alpha) + 3000\varepsilon^{-1}n^3(\mathrm{h}_p(F) + \log(mn) + 1) + 30nm\mathrm{h}_p(F) + 30nm\log(nm). \quad (i = 1, \ldots, \ell).$$

Summing up, using (45) and the disjointedness of the sets $\tilde{T}_i$, we obtain

$$\left|r\frac{\mathrm{h}(\alpha)}{n} - \mathrm{lgcd}_{\tilde{T}_1 \cup \cdots \cup \tilde{T}_\ell}(\alpha, \beta)\right| \leq \varepsilon \mathrm{h}(\alpha) + 3000\varepsilon^{-1}n^4(\mathrm{h}_p(F) + \log(mn) + 1) + 30n^2m\mathrm{h}_p(F) + 30n^2m\log(nm).$$

Finally, combining this with (48) and (52), we obtain (44). □

References

[1] M. Abouzaïd, "*Heights and logarithmic gcd on algebraic curves*", Int. J. Number Th. 4, pp. 177–197 (2008).

[2] Y. Bilu - D. Masser, "*A quick proof of Sprindzhuk's decomposition theorem*", More sets, graphs and numbers, 25–32, Bolyai Soc. Math. Stud., 15, Springer, Berlin (2006).

[3] Y. Bilu - A. Borichev, "*Remarks on Eisenstein*", J. Aust. Math. Soc. 94, pp. 158–180 (2013).

[4] E. Bombieri, "*On Weil's "Théorème de Décomposition"*", American Journal of Mathematics 105, pp. 295–308 (1983).

[5] S. David - P. Philippon, "*Minorations des hauteurs normalisées des sous-variétés des tores*", Ann. Scuola Norm. Sup. Pisa Cl. Sci. 4, 28), no. 3, pp. 489–543 (1999).

[6] B. Dwork - P. Robba, "*On natural radii of p-adic convergence*", Trans. Amer. Math. Soc. 256, 199–213 (1979).

[7] B. M. Dwork - A. J. van der Poorten, "*The Eisenstein Constant*", Duke Math. J. 65(1), 23–43 (1992).

[8] P. Habegger, "*Heights and multiplicative relations on algebraic varieties*", PhD dissertation, Basel (2007).

[9] D. Poulakis, "*Integer points on rational curves with fixed gcd*", Publ. Math. Debrecen, 64, (3–4), pp. 369–379 (2004).

[10] W. M. Schmidt, "*Diophantine Approximations and Diophantine Equations*", Lecture Notes in Math. 1467, Springer-Verlag, Berlin-Heidelberg-New-York (1991).

[11] W. M. Schmidt, "*Eisenstein's theorem on power series expansions of algebraic functions*", Acta Arithmetica, 56, (2), pp. 161–179 (1990).

[12] C. L. Siegel, "*Uber einige Anwendungen Diophantischer Approximationen*", Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929) pp. 41–69; reprinted, Gesammelte Abhandlungen I, Springer, Berlin, pp. 209–266 (1966).

[13] T. Skolem, "*Lösung gewisser Gleichungssysteme in ganzen Zahlen oder ganzzahligen Polynomen mit beschrnktem gemeinschaftlichen Teiler*", Oslo Vid. Akar. Skr. I 12 (1929).

[14] P. G. Walsh, "*A quantitative version of Runge's theorem on diophantine equations*", Acta Arithmetica LXII.2, pp. 157–172 (1992).

Received 17 February 2015,
and in revised form 23 February 2015.

Enteleia Tech, La Cour
31320 Aureville, France
Boris.Bartolome@enteleia-tech.com