Acta Math., 211 (2013), 315–382
DOI: 10.1007/s11511-013-0106-x

p-adic logarithmic forms and a problem of Erdős

by

Kunrui Yu

Hong Kong University of Science and Technology
Hong Kong, People's Republic of China

Dedicated to Prof. Gisbert Wüstholz on the occasion of his 61st birthday.

1. Introduction

1.1. Introduction and the main theorem

For any $m\in\mathbb{Z}$ let $P(m)$ denote the greatest prime divisor of m with the convention that $P(m)=1$ when $m\in\{1,0,-1\}$. By the problem of Erdős in the title of the present paper we mean his conjecture from 1965 that

$$\frac{P(2^n-1)}{n}\to\infty \quad \text{as } n\to\infty$$

(see Erdős [10]) and its far-reaching generalization to Lucas and Lehmer numbers. We briefly recall their definition in the sequel.

Let α and β be complex numbers such that $\alpha+\beta$ and $\alpha\beta$ are non-zero coprime rational integers and such that α/β is not a root of unity. The rational integers

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}$$

with $n>0$ are called *Lucas numbers*, see [15] published in 1876 and [16] published in 1878. The divisibility properties of numbers of such a form have been studied by Euler, Lagrange, Gauss, Dirichlet and others (see [9, Chapter XVII]).

Similarly, let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and such that α/β is not a root of unity. We define for $n>0$ the rational integers

$$\tilde{u}_n=\begin{cases}\dfrac{\alpha^n-\beta^n}{\alpha-\beta} & \text{for } n \text{ odd},\\[2mm] \dfrac{\alpha^n-\beta^n}{\alpha^2-\beta^2} & \text{for } n \text{ even},\end{cases}$$

known as *Lehmer numbers*. In 1930 Lehmer [13] extended the theory of Lucas numbers to this more general setting. Note that Lucas numbers are also Lehmer numbers up to a multiplicative factor $\alpha+\beta$ when n is even. For a detailed history of Lucas and Lehmer numbers we refer to [25].

The generalization of the conjecture of Erdős to Lucas numbers u_n and Lehmer numbers $\tilde{u}_n$ is that

$$\frac{P(u_n)}{n} \to \infty \quad \text{and} \quad \frac{P(\tilde{u}_n)}{n} \to \infty,$$

respectively, as $n \to \infty$.

Since the 1970s one of the big goals of Stewart has been to solve the problem of Erdős. Several partial results in this direction were obtained, see Stewart [23], [24] and especially Shorey and Stewart [22], where the lower bounds for $P(u_n)$ and $P(\tilde{u}_n)$ hold only for n belonging to a certain very restricted subset of natural numbers. They used p-adic logarithmic forms and had to rely on the work of van der Poorten [20] on lower bounds for logarithmic forms in the p-adic case. This work contains, as it turned out later, some inaccuracies, as were pointed out in Yu [34] and [39], and this made their proof not completely rigorous and it was necessary to revise van der Poorten's paper and to remove the inaccuracies so that their result in [22] could be fully justified. Also it became clear through their work that for getting progress especially toward the problem of Erdős the bounds for p-adic logarithmic forms had to be sharpened considerably.

In a sequence of papers (Yu [34]–[36]) on lower bounds for p-adic logarithmic forms the author was able to remove, with the help of the Vahlen–Capelli theorem and some p-adic devices, the problem in [20] and to sharpen the bounds substantially. Using the very subtle approach of Baker and Wüstholz in the Archimedean case in their 1993 paper [6], the author could then get a further significant refinement upon the results in [36] in analogy to their result. This was published in Yu [37] and [38] and used by Stewart and Yu [26] to deal with the *abc*-conjecture. Stimulated by the work of Matveev [18], [19] some further refinements were made possible in Yu [40] on the basis of the work of Loher and Masser [14] on counting points of bounded height. This was, as it turned out, crucial for attacking the problem of Erdős.

During Stewart's visit to the Hong Kong University of Science and Technology in 2005 we worked on improvements upon our result on the *abc*-conjecture in [26], using the new bound for p-adic logarithmic forms in [40]. In this discussion, he discovered a nice device, which we refer to as Stewart's device in the present paper and which we describe below. The problem came up how to estimate from above the $\mathfrak{p}$-adic order of numbers of the shape θ^b-1 with $\mathfrak{p}$ a prime ideal, lying above the rational prime p, θ a $\mathfrak{p}$-adic unit in K, and b a rational integer. The question can be transformed into, in the number field K, a problem of a p-adic logarithmic form with one term only. The best known result at the time in [40] was unfortunately insufficient to deal with the problem if one treated θ^b-1 directly. Stewart's idea was to transform the p-adic logarithmic form with one term into a p-adic logarithmic form with many terms and then to apply [40, Theorem 1]. This looks odd at the first glance but he was able to make it work. We briefly sketch the underlying idea. He artificially introduces $k-1$ prime numbers $p_2, ..., p_k$, prime to p (if $\theta=\alpha/\beta$ with α and β in the definition of Lucas or Lehmer numbers, then he requires $p_2, ..., p_k$ to be prime to $p\alpha\beta$), satisfying the following conditions:

(i) The numbers $\theta_1, p_2, ..., p_k$ with $\theta=\theta_1 p_2 ... p_k$ are multiplicatively independent. If $\theta=\alpha/\beta$, then this is the case indeed.

(ii) One chooses p_i as small as possible. In virtue of the prime number theorem with error term (see Rosser and Schoenfeld [21]), $\log p_k$ is basically of the size $\log k$.

(iii) The quantity k is chosen as $\log p/\log\log p$ multiplied by a very carefully determined constant.

When he applied [40, Theorem 1] to $\theta_1^b p_2^b ... p_k^b-1$ instead of θ^b-1 directly, he gained in the upper bound for the $\mathfrak{p}$-adic order of θ^b-1 a factor of the shape

$$\exp\left(-\frac{c\log p}{\log\log p}\right)$$

as needed. In retrospect, [40, Theorem 1] and Stewart's device along with his strategy were sufficient to solve the problem of Erdős in the case when α/β is rational, thereby establishing the conjecture of Erdős from 1965 (see §9 for details). After his visit to HKUST, he found out that the bottleneck for completely solving the problem of Erdős is the dependence on the parameter p in the estimates for p-adic logarithmic forms. According to [40], in the case when $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=2$ and $p\,(>2)$ is inert in $\mathbb{Q}(\alpha/\beta)$ the dependence is of size p^2. Stewart knew that if one could reduce p^2 to p, one would be able to solve the problem of Erdős completely. He was very excited and started to urge the author to try to get the improvement needed. The author knew that it would be a very tedious and demanding work. Nevertheless the author agreed to deliver the required improvement to help Stewart to solve the problem of Erdős. The present work is the result of the author's effort. On the basis of this work Stewart was able to pass through the bottleneck when $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=2$ and $p\,(>2)$ is inert in $\mathbb{Q}(\alpha/\beta)$, thereby solving the problem of Erdős also for the case when $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=2$, whence solving the problem completely (see [25]).

Since 2005 the author has re-examined [40] thoroughly and has achieved in the present paper, through very detailed work, three refinements upon [40]:

(1) The appeal to the Vahlen–Capelli theorem as in [40] and in [35]–[38] has been removed from the p-adic theory of logarithmic forms. It has the effect that a quadratic extension of the ground field (when $p>2$) can be avoided, whence it leads to a gain of

a factor 2^n in applications. Stewart has made substantial use of this refinement in [25]. The author is very confident that this refinement together with the streamlining of the proof carried through the present paper will have further value in the p-adic theory of logarithmic forms and in applications;

(2) The author has succeeded in establishing the relevant refinement in the dependence on the parameter p in the estimates for p-adic logarithmic forms. This is the key for getting the reduction of p^2 to p in the case when $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=2$ and $p\,(>2)$ is inert in $\mathbb{Q}(\alpha/\beta)$;

(3) As a by-product the author has got a nice improvement on the numerical constants in the theorems.

The refinements (1) and (2) will be explained in more detail after the statement of the main theorem in §1.1. The improvement (3) will be discussed at the end of §1.3.

Throughout this paper, [40] will be referred to frequently; for convenience, we shall refer to formulas, theorems, sections and so on in [40] by adjoining a ♣, e.g. (1.5)♣, §2♣ and Lemma 5.1♣.

We now start to state our main theorem. Let $\alpha_1, ..., \alpha_n$ be non-zero algebraic numbers and K be a number field containing $\alpha_1, ..., \alpha_n$ with $d=[K:\mathbb{Q}]$. Denote by $\mathfrak{p}$ a prime ideal of the ring $\mathcal{O}_K$ of algebraic integers in K, lying above the prime number p, by $e_{\mathfrak{p}}$ the ramification index of $\mathfrak{p}$, and by $f_{\mathfrak{p}}$ the residue class degree of $\mathfrak{p}$. For $\alpha\in K$, $\alpha\neq 0$, we write $\operatorname{ord}_{\mathfrak{p}}\alpha$ for the exponent to which $\mathfrak{p}$ divides the principal fractional ideal generated by α in K and we put $\operatorname{ord}_{\mathfrak{p}} 0=\infty$. An element α of K is said to be a $\mathfrak{p}$-*adic unit* if $\operatorname{ord}_{\mathfrak{p}}\alpha=0$; α is called a $\mathfrak{p}$-*adic integer* if $\operatorname{ord}_{\mathfrak{p}}\alpha\geqslant 0$. We shall estimate $\operatorname{ord}_{\mathfrak{p}}(\Xi-1)$ for

$$\Xi = \alpha_1^{b_1} ... \alpha_n^{b_n}, \tag{1.1}$$

with $b_1, ..., b_n$ being *rational integers* and $\Xi\neq 1$.

Write $K_{\mathfrak{p}}$ for the completion of K with respect to the exponential valuation $\operatorname{ord}_{\mathfrak{p}}$; and the completion of $\operatorname{ord}_{\mathfrak{p}}$ will be denoted again by $\operatorname{ord}_{\mathfrak{p}}$. Denote by $\overline{K}$ the residue class field of K at $\mathfrak{p}$. Now let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$ and $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}}_p$ with respect to the valuation of $\overline{\mathbb{Q}}_p$, which is the unique extension of the valuation $|\cdot|_p$ of $\mathbb{Q}_p$. Signify by $|\cdot|_p$ the valuation on $\mathbb{C}_p$, and by ord_p the exponential valuation on $\mathbb{C}_p$, with the convention that $\operatorname{ord}_p 0=\infty$. Then $|\gamma|_p=p^{-\operatorname{ord}_p\gamma}$ for all $\gamma\in\mathbb{C}_p$. There exists a $\mathbb{Q}$-isomorphism ψ from K into $\overline{\mathbb{Q}}_p$ such that $K_{\mathfrak{p}}$ is value-isomorphic to $\mathbb{Q}_p(\psi(K))$, whence we can identify $K_{\mathfrak{p}}$ with $\mathbb{Q}_p(\psi(K))$ (see Hasse [12, pp. 298–302]). This gives

$$\operatorname{ord}_{\mathfrak{p}}\gamma = e_{\mathfrak{p}} \operatorname{ord}_p \gamma \quad \text{for all } \gamma\in K_{\mathfrak{p}}.$$

Let $\varkappa$ be the rational integer determined by

$$p^{\varkappa-1}(p-1)\leqslant 2e_{\mathfrak{p}} < p^{\varkappa}(p-1). \tag{1.2}$$

If β is in $K_{\mathfrak{p}}$ and $\beta\equiv 1 \pmod{\mathfrak{p}}$, then the p-adic series $\beta^{p^{\varkappa}z}:=\exp(z\log\beta^{p^{\varkappa}})$ converges in the disk $\{z:|z|_p<p^{\vartheta}\}$ (ϑ will be given later by (2.1)) in $\mathbb{C}_p$ which contains strictly the unit disk (see [36, Lemma 1.1]).

One of the basic tools in the theory of logarithmic forms is the Kummer descent introduced by Baker and Stark [5]. For this one needs to choose a prime number q, which should be different from p in the p-adic case. The optimal choice for q is

$$q=\begin{cases} 2, & \text{if } p>2,\\ 3, & \text{if } p=2.\end{cases} \tag{1.3}$$

Let $\boldsymbol{\mu}(K)$ and $\boldsymbol{\mu}(K_{\mathfrak{p}})$ denote the groups of roots of unity in K and $K_{\mathfrak{p}}$, respectively, and let q^u and q^{μ} signify the order of the q-primary component of $\boldsymbol{\mu}(K)$ and $\boldsymbol{\mu}(K_{\mathfrak{p}})$, respectively. We fix a generator

$$\alpha_0=\zeta_{q^u} \tag{1.4}$$

of the q-primary component of $\boldsymbol{\mu}(K)$, where and in the sequel $\zeta_m=e^{2\pi i/m}$ for $m\in\mathbb{Z}_{>0}$. The classical Kummer theory requires that the field K contains ζ_q. This is certainly true if $q=2$ (i.e. $p>2$), since then $\zeta_q=-1$. Therefore we impose

$$\zeta_3\in K,\quad \text{if } q=3 \text{ (i.e. } p=2). \tag{1.5}$$

For a multiplicatively independent set $\mathfrak{a}=\{\alpha_1,...,\alpha_n\}$ of $\mathfrak{p}$-adic units in K we now introduce a quantity $\delta(\mathfrak{a})$. We apply the lattice saturation procedure described in §5$^{\clubsuit}$ as follows. From $\mathfrak{a}$ we introduce a *q-saturated* lattice $\mathbf{M}=\boldsymbol{\mathcal{M}}_K(\alpha_1,...,\alpha_n)\cap(\mathbb{Z}[1/q])^n$, where

$$\boldsymbol{\mathcal{M}}_K(\alpha_1,...,\alpha_n)=\left\{\left(\frac{s_1}{t},...,\frac{s_n}{t}\right): s_i\in\mathbb{Z},\ t\in\mathbb{Z}_{>0} \text{ and } {\alpha_1}^{s_1}...{\alpha_n}^{s_n}\in K^t\right\}$$

is the *Loher–Masser lattice*, see [14] (or §2$^{\clubsuit}$). We fix a basis $\{\boldsymbol{b}_1,...,\boldsymbol{b}_n\}$ of $\mathbf{M}$ and introduce a set of $\mathfrak{p}$-adic units $\{\vartheta_1,...,\vartheta_n\}$ in K corresponding to this basis (see §5$^{\clubsuit}$, replacing $\{\alpha_1',...,\alpha_r'\}$ by $\{\alpha_1,...,\alpha_n\}$ and $\{\theta_1,...,\theta_r\}$ by $\{\vartheta_1,...,\vartheta_n\}$). We remark that $\{\vartheta_1,...,\vartheta_n\}$ has the property that $\vartheta_i^{[\mathbf{M}:\mathbb{Z}^n]}$ $(1\leqslant i\leqslant n)$ is in the subgroup $\langle\alpha_0,\alpha_1,...,\alpha_n\rangle$ of K^* and that the Kummer condition

$$[K(\alpha_0^{1/q},\vartheta_1^{1/q},...,\vartheta_n^{1/q}):K]=q^{n+1}$$

is satisfied. Let $\bar{\alpha}_0,\bar{\vartheta}_1,...,\bar{\vartheta}_n$ be the images of $\alpha_0,\vartheta_1,...,\vartheta_n$ under the residue class map at $\mathfrak{p}$ from the ring of $\mathfrak{p}$-adic integers in K onto the residue class field $\overline{K}$ at $\mathfrak{p}$. The cardinality $|\langle\bar{\alpha}_0,\bar{\vartheta}_1,...,\bar{\vartheta}_n\rangle|$ of the subgroup $\langle\bar{\alpha}_0,\bar{\vartheta}_1,...,\bar{\vartheta}_n\rangle$ of the multiplicative group

$\overline{K}^*$ (of $\overline{K}$) depends on $\mathfrak{a}$ only; it is independent of the choice of basis $\{\boldsymbol{b}_1, ..., \boldsymbol{b}_n\}$ of $\mathbf{M}$ (see §5♣). Thus we can define an index $\delta(\mathfrak{a})$ by

$$\frac{p^{f_{\mathfrak{p}}}-1}{\delta(\mathfrak{a})} = \begin{cases} |\langle \bar{\alpha}_0, \bar{\vartheta}_1, ..., \bar{\vartheta}_n \rangle|, & \text{if } n \geqslant 2, \\ |\langle \bar{\alpha}_1 \rangle|, & \text{if } n=1. \end{cases} \tag{1.6}$$

It is clear that if $n \geqslant 2$ and the Kummer condition

$$[K(\alpha_0^{1/q}, \alpha_1^{1/q}, ..., \alpha_n^{1/q}) : K] = q^{n+1} \tag{1.7}$$

is satisfied then

$$\frac{p^{f_{\mathfrak{p}}}-1}{\delta(\mathfrak{a})} = |\langle \bar{\alpha}_0, \bar{\alpha}_1, ..., \bar{\alpha}_n \rangle|. \tag{1.8}$$

We now assume that $\alpha_1, ..., \alpha_n$ in (1.1) are multiplicatively independent $\mathfrak{p}$-adic units in K and write $\mathfrak{a}=\{\alpha_1, ..., \alpha_n\}$. For any $x>0$, let $\log^* x = \log\max\{x, e\}$. We introduce the terms

$$\begin{aligned} C_1(n,d,\mathfrak{p},\mathfrak{a}) &= c^{(1)}(a^{(1)})^n \frac{n^n(n+1)^{n+1}}{n!} \frac{d^{n+2}\log^* d}{q^u f_{\mathfrak{p}} \log p} \\ &\quad \times \max\left\{ \frac{p^{f_{\mathfrak{p}}}}{\delta(\mathfrak{a})(f_{\mathfrak{p}}\log p)^{n+1}}, \frac{e^n}{n^n} \right\} \max\{\log e^4(n+1)d, e_{\mathfrak{p}}, f_{\mathfrak{p}}\log p\}, \end{aligned} \tag{1.9}$$

$$\begin{aligned} C_2(n,d,\mathfrak{p},\mathfrak{a}) &= \frac{c^{(2)}}{p^{\varkappa}}(a^{(2)} e\, p^{\varkappa})^n \frac{(n+1)^{n+1}}{(n-1)!} \frac{d^{n+2}\log^* d}{q^u (f_{\mathfrak{p}}\log p)^3} \\ &\quad \times \max\left\{ \frac{p^{f_{\mathfrak{p}}}}{\delta(\mathfrak{a})}, \frac{e^n}{n^n}(f_{\mathfrak{p}}\log p)^{n+1} \right\} \max\{\log e^4(n+1)d, e_{\mathfrak{p}}, f_{\mathfrak{p}}\log p\}, \end{aligned} \tag{1.10}$$

$$G_1(n,d) = (n+1)(a_0^{(1)}n + a_1^{(1)} + \log(a_0^{(1)}n + a_2^{(1)}) + \log d), \tag{1.11}$$

$$G_2(n,d) = (n+1)(a_0^{(2)}n + a_1^{(2)} + \log(n+1) + \log d), \tag{1.12}$$

which will appear in the main theorem. The numerical values of $a^{(i)}$, $c^{(i)}$, $a_0^{(i)}$, $a_1^{(i)}$ $(i=1,2)$ and $a_2^{(1)}$ will be given in §1.3.

Throughout this paper we shall use the notation of heights introduced in [6, §2]. Thus let $h_0(\alpha)$ denote the absolute logarithmic Weil height of an algebraic number α with the minimal polynomial $a_0\prod_{j=1}^{\delta}(x-\alpha^{(j)})$ over $\mathbb{Z}$, where $a_0>0$. Then

$$h_0(\alpha) = \frac{1}{\delta}\left(\log a_0 + \sum_{j=1}^{\delta} \log\max\{1, |\alpha^{(j)}|\} \right).$$

We further introduce, for $i=1,2$,

$$h^{(i)} = \max\left\{ \log\left(\omega(d) \max_{1\leqslant j<n} \left(\frac{|b_n|}{h_0(\alpha_j)} + \frac{|b_j|}{h_0(\alpha_n)} \right) \right), \log B^{\circ}, G_i(n,d), (n+1) f_{\mathfrak{p}} \log p \right\}. \tag{1.13}$$

Here we note that $\alpha_1, ..., \alpha_n$ are not roots of unity, since they are multiplicatively independent, whence $h_0(\alpha_i)\neq 0$, $1\leqslant i\leqslant n$, and the terms B° and $\omega(d)$ are given by

$$B^\circ = \min_{\substack{1\leqslant j\leqslant n\\ b_j\neq 0}} |b_j| \tag{1.14}$$

and

$$\omega(d) = \begin{cases} \dfrac{1}{d\log^3 3d}, & \text{if } d>1,\\ \dfrac{\log 2\cdot\log 3}{\log 6}, & \text{if } d=1, \end{cases} \tag{1.15}$$

respectively. With the above notation we now state our main theorem.

MAIN THEOREM. *Assume that $n\geqslant 2$ and that (1.5) holds. Suppose further that $\alpha_1, ..., \alpha_n$ are multiplicatively independent elements of K, $b_1, ..., b_n$ are in $\mathbb{Z}$, not all zero, and that they satisfy*

$$\operatorname{ord}_{\mathfrak{p}} \alpha_j = 0 \qquad (1\leqslant j\leqslant n), \tag{1.16}$$

$$\operatorname{ord}_p b_n \leqslant \operatorname{ord}_p b_j \qquad (1\leqslant j\leqslant n). \tag{1.17}$$

Then we have

$$\operatorname{ord}_{\mathfrak{p}}(\Xi-1) < \min_{i=1,2}(C_i(n,d,\mathfrak{p},\mathfrak{a})h^{(i)})h_0(\alpha_1)\dots h_0(\alpha_n). \tag{1.18}$$

Comparing our main theorem with the main theorem$^\clubsuit$, we observe that (1.5)$^\clubsuit$ has been relaxed to (1.5). Namely, now we may simply take K as our ground field when $p>2$, whereas in [40] and in [36]–[38] if the first condition in (1.5)$^\clubsuit$, that is, $\operatorname{ord}_q(p^{f_\mathfrak{p}}-1)=1$ or $\zeta_4\in K$ when $q=2$ (i.e. $p>2$), does not hold, a quadratic extension of K obtained by adjoining ζ_4 to K is necessary. The underlying cause of this is that the author has succeeded in removing the appeal to the Vahlen–Capelli theorem as in [40] and in [35]–[38] from the theory of p-adic logarithmic forms. This is the first refinement.

Moreover, neglecting the difference between $p^{f_\mathfrak{p}}$ and $p^{f_\mathfrak{p}}-1$, the cardinality $|\overline{K}|=p^{f_\mathfrak{p}}$, as a factor in the upper bounds for $\operatorname{ord}_\mathfrak{p}(\Xi-1)$ in [35]–[38] and [40], has been reduced to the cardinality of a subgroup of $\overline{K}^*$, i.e., the quantity (1.6). This is the second refinement.

We now explain how we achieve the two refinements. Recall the definition of q^u and q^μ between (1.3) and (1.4). Set

$$G_0 = \frac{p^{f_\mathfrak{p}}-1}{q^u} \quad \text{and} \quad G_1 = \frac{p^{f_\mathfrak{p}}-1}{q^\mu}.$$

By Hasse [12, p. 220], we see that $q^u \mid (p^{f_\mathfrak{p}}-1)$ and $\mu = \mathrm{ord}_q(p^{f_\mathfrak{p}}-1)$, whence $\mu \geqslant u$. In [40], we use, in the Ith inductive step, $(8.1)^\clubsuit$ (iii), i.e.,

$$d_1\lambda_1+\ldots+d_r\lambda_r \equiv \varepsilon^{(I)} \pmod{G_1} \quad \text{for all } \boldsymbol{\lambda} \in \boldsymbol{\Lambda}^{(I)},$$

where $\boldsymbol{\Lambda}^{(I)}$ is a subset of $\mathbb{Z}^r$; accordingly, in the study of fractional points s/q (with $s \in \mathbb{Z}$ and $(s,q)=1$) for the Kummer descent, we demand the irreducibility of the polynomial $x^{q^{\mu-u+1}}-1$ over $K(\theta_1^{1/q}, ..., \theta_r^{1/q})$, for which we appeal to the Vahlen–Capelli theorem, whence we are forced to impose $(1.5)^\clubsuit$ on K. In contrast to [40], in the present paper, we use (iii) of (5.1), i.e.,

$$d_1\lambda_1+\ldots+d_r\lambda_r \equiv \varepsilon^{(I)} \pmod{G_0} \quad \text{for all } \boldsymbol{\lambda} \in \boldsymbol{\Lambda}^{(I)};$$

accordingly, in the Kummer descent, we demand the irreducibility of the polynomial $x^q-\alpha_0$ over K, which is, a priori, guaranteed by (1.4). Therefore we can avoid the Vahlen–Capelli theorem in the p-adic theory of logarithmic forms and relax $(1.5)^\clubsuit$ to (1.5). For more details, see the proof of Lemma 5.4; for the history of the introduction of the Vahlen–Capelli theorem into the p-adic theory of logarithmic forms, see [39]. Furthermore, to create $\boldsymbol{\Lambda}^{(I)}$ for $I=0$ (the initial inductive step), in the construction of auxiliary functions using Siegel's lemma, we classify the set

$$\left\{ \frac{d_1}{\delta(\mathfrak{a}')}\lambda_1+\ldots+\frac{d_r}{\delta(\mathfrak{a}')}\lambda_r : (\lambda_1, ..., \lambda_r) \in \boldsymbol{\Lambda}' \right\}$$

by the congruence relation modulo $G_0/\delta(\mathfrak{a}')$, where $\delta(\mathfrak{a}')=\gcd(G_0, d_1, ..., d_r)$ and $\boldsymbol{\Lambda}'$ is a certain finite subset of $\mathbb{Z}^r$. By Dirichlet's pigeonhole principle, there exist $\varepsilon_1 \in \mathbb{Z}$ and a subset $\boldsymbol{\Lambda}^{(0)} \subseteq \boldsymbol{\Lambda}'$ with cardinality $|\boldsymbol{\Lambda}^{(0)}| \geqslant |\boldsymbol{\Lambda}'|/(G_0/\delta(\mathfrak{a}'))$ such that

$$\frac{d_1}{\delta(\mathfrak{a}')}\lambda_1+\ldots+\frac{d_r}{\delta(\mathfrak{a}')}\lambda_r \equiv \varepsilon_1 \left(\mathrm{mod}\ \frac{G_0}{\delta(\mathfrak{a}')} \right) \quad \text{for all } (\lambda_1, ..., \lambda_r) \in \boldsymbol{\Lambda}^{(0)}.$$

Thus $\boldsymbol{\Lambda}^{(0)}$ is created and (5.1) (iii) for $I=0$ is satisfied with $\varepsilon^{(0)} := \delta(\mathfrak{a}')\varepsilon_1$ (see (4.19) (iii)). Now the quantity $G_0/\delta(\mathfrak{a}')$ comes into play through Siegel's lemma (here we use [6, Lemma 1]) and $\delta(\mathfrak{a}')$ is switched into $\delta(\mathfrak{a})$ (see (1.6)) by the basic hypothesis in §2. Finally $p^{f_\mathfrak{p}}/\delta(\mathfrak{a})$ appears as a factor of the upper bound for $\mathrm{ord}_\mathfrak{p}(\Xi-1)$ in our main theorem, in place of $p^{f_\mathfrak{p}}$ in the main theorem$^\clubsuit$. For more details, see §4. Note that some difficulty in the estimation from below arises due to the introduction of $\delta(\mathfrak{a}')$ and $\delta(\mathfrak{a})$. We overcome this difficulty by taking the first maximum in (3.4) (see, for instance, the proof of (3.23)); consequently, we take the first maximum in (1.9) and (1.10), which appear in our main theorem.

1.2. Variants for applications

Let $\mathfrak{a}=\{\alpha_1,\dots,\alpha_n\}$,

$$\Gamma=\langle\mathfrak{a}\rangle \quad\text{and}\quad r=\operatorname{rank}\Gamma. \tag{1.19}$$

If $r\geqslant 1$ we write $\mathfrak{b}$ for a multiplicatively independent subset of $\mathfrak{a}$ with cardinality $|\mathfrak{b}|=r$. For Theorems 1 and 2 below we define, for $\alpha\in K$,

$$h^{(n)}(\alpha)=\max\left\{h_0(\alpha),\frac{\max\{n,f_{\mathfrak{p}}\log p\}}{\varkappa_1(n+5)d}\right\}, \tag{1.20}$$

where the value of $\varkappa_1$ will be given in §1.3. Let

$$\Omega(\mathfrak{b})=\prod_{\alpha\in\mathfrak{b}}h_0(\alpha)\cdot\prod_{\alpha\in\mathfrak{a}\setminus\mathfrak{b}}h^{(n)}(\alpha),\qquad \Omega=\min_{\mathfrak{b}}\Omega(\mathfrak{b}) \tag{1.21}$$

and

$$C_1^*(n,d,\mathfrak{p},\mathfrak{b})=(n+1)C_1(n,d,\mathfrak{p},\mathfrak{b}), \tag{1.22}$$

where $C_1(n,d,\mathfrak{p},\mathfrak{b})$ is given by (1.9) with $\mathfrak{a}$ replaced by $\mathfrak{b}$. We note that here $\delta(\mathfrak{b})$ is defined by (1.6) with $\mathfrak{a}$ replaced by $\mathfrak{b}$. Let B be a real number satisfying

$$B\geqslant\max\{|b_1|,\dots,|b_n|,3\}. \tag{1.23}$$

Theorem 1. *Let $r\geqslant 1$. Suppose that (1.5) and (1.16) hold. If $\Xi\neq 1$, then*

$$\operatorname{ord}_{\mathfrak{p}}(\Xi-1)<C_1^*(n,d,\mathfrak{p},\mathfrak{b})\Omega\max\{\log B,f_{\mathfrak{p}}\log p\}, \tag{1.24}$$

where $\mathfrak{b}$ satisfies $\Omega(\mathfrak{b})=\Omega$. Furthermore, if $r=1$ then the right-hand side of (1.24) can be multiplied by $\frac{1}{2100}$.

For Theorem 2 below we define, for $\alpha\in K$,

$$h^{(n)}(\alpha)=\max\left\{h_0(\alpha),\frac{\max\{n/f_{\mathfrak{p}}\log p,1\}}{\varkappa_2 p^{\varkappa} d}\right\}, \tag{1.25}$$

where the value of $\varkappa_2$ will be given in §1.3. Define $\Omega(\mathfrak{b})$ and Ω by (1.21) with $h^{(n)}(\alpha)$ given by (1.25). Set

$$C_2^*(n,d,\mathfrak{p},\mathfrak{b})=(n+1)C_2(n,d,\mathfrak{p},\mathfrak{b}), \tag{1.26}$$

where $C_2(n,d,\mathfrak{p},\mathfrak{b})$ is given by (1.10) with $\mathfrak{a}$ replaced by $\mathfrak{b}$. Here, again, $\delta(\mathfrak{b})$ is defined by (1.6) with $\mathfrak{a}$ replaced by $\mathfrak{b}$. Let B satisfy (1.23).

Theorem 2. *Let $r\geqslant 1$. Suppose that (1.5) and (1.16) hold. If $\Xi\neq 1$, then*

$$\operatorname{ord}_{\mathfrak{p}}(\Xi-1)<C_2^*(n,d,\mathfrak{p},\mathfrak{b})\Omega\max\{\log B,f_{\mathfrak{p}}\log p\}, \tag{1.27}$$

where $\mathfrak{b}$ satisfies $\Omega(\mathfrak{b})=\Omega$. Furthermore, if $r=1$ then the right-hand side of (1.27) can be multiplied by $\frac{1}{4000}$.

1.3. Numerical values

We consider the following cases:

(I) $p=3$, including sub-cases (I.1) $d>1$ and (I.2) $d=1$;

(II) $p=5$ with $e_{\mathfrak{p}}\geqslant 2$;

(III) $p\geqslant 5$ with $e_{\mathfrak{p}}=1$, including sub-cases (III.1) $d>1$ and (III.2) $d=1$;

(IV) $p\geqslant 7$ with $e_{\mathfrak{p}}\geqslant 2$;

(V) $p=2$.

We give the values of $a^{(i)}$, $\varkappa_i$, $a_0^{(i)}$ $(i=1,2)$ by (1.28) and (1.29), the values of $c^{(i)}$, $a_1^{(i)}$ $(i=1,2)$ by (1.30) and the values of $a_2^{(1)}$ by (1.31) below:

$$(a^{(1)},\varkappa_1,a_0^{(1)})=\begin{cases}(14,18,2+\log 14), & \text{in cases (I), (II) and (IV)},\\ \left(7\dfrac{p-1}{p-2},9\dfrac{p-1}{p-2},2+\log 7\right), & \text{in case (III)},\\ (26,34,2+\log 26), & \text{in case (V)}.\end{cases} \tag{1.28}$$

$$(a^{(2)},\varkappa_2)=\begin{cases}(7,25), & \text{if } p>2,\\ (13,48), & \text{if } p=2.\end{cases}\quad a_0^{(2)}=\begin{cases}2+\log 21, & \text{in case (I)},\\ 2+\log 35, & \text{in case (II)},\\ 2+\log 7, & \text{in cases (III) and (IV)},\\ 2+\log 52, & \text{in case (V)}.\end{cases} \tag{1.29}$$

$$(c^{(1)},a_1^{(1)},c^{(2)},a_1^{(2)})=\begin{cases}(939,4.03,1438,1.94), & \text{in case (I.1)},\\ (636,4.79,648,2.76), & \text{in case (I.2)},\\ (505,3.44,690,0.71), & \text{in case (II)},\\ \left(1794,4.71,495\dfrac{p-1}{p-2},1.99\right), & \text{in case (III.1)},\\ \left(1790,5.84,557\dfrac{p-1}{p-2},3.32\right), & \text{in case (III.2)},\\ (2680,5.12,2418,3.58), & \text{in case (IV)},\\ (206,2.52,406,1.48), & \text{in case (V)},\end{cases} \tag{1.30}$$

$$a_2^{(1)}=\begin{cases}a_1^{(1)}, & \text{in cases (I.2) and (III.2)},\\ a_1^{(1)}+\log 2, & \text{in the remaining cases}.\end{cases} \tag{1.31}$$

According to the definition of cases (I)–(V), (1.36)♣ and (1.37)♣ give

$$a^{(1)}=\begin{cases}16, & \text{in cases (I), (II) and (IV)},\\ 8\dfrac{p-1}{p-2}, & \text{in case (III)},\\ 32, & \text{in case (V)},\end{cases} \tag{1.32}$$

and

$$a^{(2)} = \begin{cases} 8, & \text{if } p > 2, \\ 16, & \text{if } p = 2. \end{cases} \tag{1.33}$$

Comparing (1.9) and (1.10) with (1.6)♣ and (1.7)♣, and (1.28) and (1.29) with (1.32) and (1.33), one can see the numerical refinements.

1.4. Outline of the paper

Obviously the main theorem is equivalent to the following two theorems.

THEOREM I. *Under the hypotheses of the main theorem, we have*

$$\operatorname{ord}_{\mathfrak{p}}(\Xi-1) < C_1(n,d,\mathfrak{p},\mathfrak{a}) h_0(\alpha_1) \dots h_0(\alpha_n) h^{(1)}.$$

THEOREM II. *Under the hypotheses of the main theorem, we have*

$$\operatorname{ord}_{\mathfrak{p}}(\Xi-1) < C_2(n,d,\mathfrak{p},\mathfrak{a}) h_0(\alpha_1) \dots h_0(\alpha_n) h^{(1)}.$$

In §§2–7 below, we give a proof of Theorem I.

Then we deduce Theorem 1 from Theorem I in §8. We have also carefully worked out a proof of Theorem II, which implies Theorem 2 and which is obtained following the same line of argumentation as in Part II of [40] and utilizing the three refinements upon [40] explained in §1.1. In order to reduce the size of the present paper, we have skipped the proofs of Theorems II and 2. We remark further that one can deduce from Theorem I (resp. Theorem II) a theorem, which is an improvement upon Theorem 2♣ (resp. Theorem 4♣), following the argumentation in §12♣. Finally, in §9 we give further remarks on the solution of the problem of Erdős, in order to be more streamlined with respect to the p-adic theory of logarithmic forms.

2. Basic hypothesis

From now on till the end of this paper, we always assume (1.5). Let $\varkappa$ be defined by (1.2), q by (1.3), u and α_0 by (1.4). Set ϑ and θ to be

$$\vartheta = \begin{cases} \dfrac{p-2}{p-1}, & \text{if } p \geqslant 5 \text{ with } e_{\mathfrak{p}} = 1, \\ \dfrac{p^{\varkappa}}{2e_{\mathfrak{p}}}, & \text{otherwise} \end{cases} \qquad \text{and} \quad \theta = \left(1+\frac{1}{2n}10^{-26}\right)^{-1} \vartheta. \tag{2.1}$$

Put

$$c_2 = \begin{cases} \frac{7}{4}, & \text{if } p>2,\\ \frac{13}{9}, & \text{if } p=2. \end{cases} \tag{2.2}$$

Let $\alpha_1, ..., \alpha_n$ and $b_1, ..., b_n$ be given as in the main theorem. Define

$$l_0 = \frac{2\pi i}{q^u}, \quad l_j = \log|\alpha_j| + i \arg \alpha_j, \quad \arg \alpha_j \in (-\pi, \pi] \quad (1 \leqslant j \leqslant n), \tag{2.3}$$

and

$$L = b_1 z_1 + ... + b_n z_n. \tag{2.4}$$

Our *basic hypothesis* is that there exist linear forms $L_0, L_1, ..., L_r$ in $z_0, z_1, ..., z_n$ with coefficients in $\mathbb{Z}$ and positive real numbers $\sigma_1, ..., \sigma_r$ having the following properties:

(i) $L_0 = z_0$; $L_0, L_1, ..., L_r$ are linearly independent; and

$$L = B_0 L_0 + B_1 L_1 + ... + B_r L_r \tag{2.5}$$

for some rationals $B_0, B_1, ..., B_r$, with $B_r \neq 0$.

(ii) We have

$$h_0(\alpha'_i) \leqslant \sigma_i \quad (1 \leqslant i \leqslant r) \tag{2.6}$$

for

$$\alpha'_i = e^{l'_i} \quad \text{with } l'_i = L_i(l_0, ..., l_n) \quad (0 \leqslant i \leqslant r), \tag{2.7}$$

and

$$\sum_{j=1}^{n} \left| \frac{\partial L_i}{\partial z_j} \right| h_0(\alpha_j) \leqslant \sigma_i \quad (1 \leqslant i \leqslant r). \tag{2.8}$$

(iii) $\sigma_1, ..., \sigma_r$ satisfy

$$\sigma_1 ... \sigma_r \leqslant \psi_1(r) h_0(\alpha_1) ... h_0(\alpha_n), \tag{2.9}$$

where

$$\psi_1(r) = \left(e c_2 q \frac{p^{\varkappa}}{e_{\mathfrak{p}} \theta} (n+1) d \right)^{n-r} \frac{\max\{p^{f_{\mathfrak{p}}}/\delta(\mathfrak{a})(f_{\mathfrak{p}} \log p)^{n+1}, e^n/n^n\}}{\max\{p^{f_{\mathfrak{p}}}/\delta(\mathfrak{a}')(f_{\mathfrak{p}} \log p)^{r+1}, e^r/r^r\}}, \tag{2.10}$$

with $\mathfrak{a}' = \{\alpha'_1, ..., \alpha'_r\}$.

Note that (2.8) will be used for the estimation of $|\gamma_j|$ (see (4.23)) and $|\gamma_j^{(I)}|$ (see (5.6)) from above. For more details see p. 220♣, line 9.

We note that $l'_0 = l_0$, $\alpha'_0 = \alpha_0$ and that $\alpha'_1, ..., \alpha'_r$ are *multiplicatively independent*, since $l'_0, l'_1, ..., l'_r$ are linearly independent. Further, we see that $\alpha'_1, ..., \alpha'_r$ are in K and

$$\operatorname{ord}_{\mathfrak{p}} \alpha'_i = 0 \quad (1 \leqslant i \leqslant r). \tag{2.11}$$

Thus $\delta(\mathfrak{a}')$ is well defined in the sense of (1.6). For $r = n$, a set of linear forms and a set of positive real numbers as above exist, e.g., $L_i = z_i$ $(0 \leqslant i \leqslant n)$ and $\sigma_i = h_0(\alpha_i)$ $(1 \leqslant i \leqslant n)$. We now take r as the *least* integer for which two such sets exist.

LEMMA 2.1. *If* $r=1$, *then Theorem* I *holds.*

Before proving Lemma 2.1, we remark that [35, Lemma 1.4] can be restated as follows. Suppose that α is a $\mathfrak{p}$-adic unit in a number field K of degree d and $b\in\mathbb{Z}\setminus\{0\}$. If $\alpha^b\neq 1$, then

$$\operatorname{ord}_{\mathfrak{p}}(\alpha^b-1)\leqslant\frac{d}{f_{\mathfrak{p}}\log p}\left(\log 2|b|+|\langle\bar{\alpha}\rangle|\left(1+\frac{1}{p-1}\right)e_{\mathfrak{p}}h_0(\alpha)\right),$$

where $|\langle\bar{\alpha}\rangle|$ denotes the cardinality of $\langle\bar{\alpha}\rangle$ as a subgroup of $\overline{K}^*$.

Proof. Note that $B_1\neq 0$. Write $B_1=p_1/q_1$, with $p_1,q_1\in\mathbb{Z}$, $(p_1,q_1)=1$ and $q_1>0$. By (2.5), we have

$$q_1L=q_1B_0z_0+p_1L_1.$$

Thus $q_1B_0\in\mathbb{Z}$ and $p_1|b_j$ $(1\leqslant j\leqslant n)$, whence $|p_1|\leqslant B^\circ$. Now

$$\begin{aligned}\operatorname{ord}_{\mathfrak{p}}(\Xi-1)&\leqslant\operatorname{ord}_{\mathfrak{p}}((\alpha_1^{b_1}\dots\alpha_n^{b_n})^{q_1q^u}-1)=\operatorname{ord}_{\mathfrak{p}}((\alpha_1')^{p_1q^u}-1)\\&\leqslant\frac{d}{f_{\mathfrak{p}}\log p}(\log 2q^uB^\circ+2|\langle\bar{\alpha}_1'\rangle|e_{\mathfrak{p}}h_0(\alpha_1')),\end{aligned}$$

where the second inequality is obtained by the above restated [35, Lemma 1.4]. Note that $\log 2q^uB^\circ\leqslant 2h^{(1)}$ by (1.13). Now, by applying [14, Theorem 3] for a lower bound of $h_0(\alpha_1)\dots h_0(\alpha_n)$, and by (2.6), (2.9) and (2.10), observing that $|\langle\bar{\alpha}_1'\rangle|<p^{f_{\mathfrak{p}}}/\delta(\mathfrak{a}')$ (by (1.6)), Theorem I follows. □

By Lemma 2.1, we may assume that $r\geqslant 2$ in our basic hypothesis from now on to the end of §7.

Proposition 3.1♣ will be applied to a polynomial $\mathcal{P}(Y_0,\dots,Y_r)$ with differential operators $\partial_1,\dots,\partial_{r-1}$ replaced by a new set as follows. We write

$$\partial_j^*=\frac{1}{B_r}\sum_{i=1}^{r-1}\left(b_n\frac{\partial L_i}{\partial z_j}-b_j\frac{\partial L_i}{\partial z_n}\right)\partial_i\quad(1\leqslant j<n).\tag{2.12}$$

Now the linear independence of $L_0,\dots,L_r$ implies that the matrix of coefficients of $\partial_1,\dots,\partial_{r-1}$ has rank $r-1$. It follows that this matrix has a non-singular square submatrix of order $r-1$. Let S_{n-1} be the symmetric group on $\{1,\dots,n-1\}$. Without loss of generality, we may assume that

$$\operatorname{ord}_p\det\left(b_n\frac{\partial L_i}{\partial z_j}-b_j\frac{\partial L_i}{\partial z_n}\right)_{1\leqslant i,j<r}=\min_{\tau\in S_{n-1}}\operatorname{ord}_p\det\left(b_n\frac{\partial L_i}{\partial z_{\tau(j)}}-b_{\tau(j)}\frac{\partial L_i}{\partial z_n}\right)_{1\leqslant i,j<r}.\tag{2.13}$$

Thus $\partial_1^*,\dots,\partial_{r-1}^*$ are linearly independent over $\mathbb{Q}$, and Proposition 3.1♣ holds with $\partial_1^*,\dots,\partial_{r-1}^*$ in place of $\partial_1,\dots,\partial_{r-1}$. Furthermore, ∂_j^* $(r\leqslant j<n)$ are linear combinations

of $\partial_1^*, ..., \partial_{r-1}^*$ with coefficients in $\mathbb{Q}\cap\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers. Note that the asterisked operators can be written in the form

$$\partial_j^* = \sum_{i=1}^{r} \left(b_n \frac{\partial L_i}{\partial z_j} - b_j \frac{\partial L_i}{\partial z_n} \right) Y_i \frac{\partial}{\partial Y_i}. \tag{2.14}$$

In §§3–7 below, we assume that the lattice saturation procedure described in §5♣ has been applied to the set $\{\alpha_1', ..., \alpha_r'\}$ in the basic hypothesis of this section.

3. Choices of parameters and numerical preparation for §§4–7

3.1. Choices of parameters

We introduce the parameters D_j, $j=-1,0,1,...,r$, for our auxiliary function (in §4 below), and S and T for the range of zeros and the multiplicity of zeros.

Let h be given by (1.13) for $i=1$ with $G_1(n,d)$ replaced by $g_0=g_0(r,d):=G_1(r,d)$ and $(n+1)f_{\mathfrak{p}} \log p$ replaced by $(r+1)f_{\mathfrak{p}} \log p$. Let q be given by (1.3), u by (1.4), ν by (5.4)♣, c_2 by (2.2) and c_0, c_1, c_3 and c_4 be given by Table 3.1 (in §3.3 below). Put

$$S = \frac{c_3 q (r+1) d (h+\nu \log q)}{f_{\mathfrak{p}} \log p}, \tag{3.1}$$

$$\gamma = \frac{q^\nu h \max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}} \log p\}}{(h+\nu \log q)(\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}} \log p\}+\nu \log q)}, \tag{3.2}$$

where $g_1=g_1(r,d)=\log e^4(r+1)d$ (see also (3.16) in §3.3). Note that γ, as a function of ν, increases for $\nu \geqslant 0$, since $h \geqslant g_0 = G_1(r,d) > 39$ (by (1.11) and $r \geqslant 2$) and $g_1 > 5$. So

$$1 \leqslant \gamma \leqslant q^\nu. \tag{3.3}$$

Set

$$\begin{aligned} D = {} & \frac{\gamma}{q^{\nu+u}} (1+\varepsilon) \left(2 + \frac{1}{g_2}\right) c_0 c_1 c_4 \left(c_2 q \frac{p^{\varkappa}}{e_{\mathfrak{p}} \theta}\right)^r \frac{r^r (r+1)^r}{r!} \\ & \times \max\left\{ \frac{p^{f_{\mathfrak{p}}}}{\delta(\mathfrak{a}')(f_{\mathfrak{p}} \log p)^r}, \frac{e^r}{r^r} f_{\mathfrak{p}} \log p \right\} \\ & \times d^{r+1} (\log^* d) \sigma_1 \ldots \sigma_r (\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}} \log p\} + \nu \log q), \end{aligned} \tag{3.4}$$

where ε and g_2 will be given by (3.16), $\varkappa$ by (1.2), θ by (2.1), and r, $\mathfrak{a}'=\{\alpha_1', ..., \alpha_r'\}$,

$\delta(\mathfrak{a}')$ and $\sigma_1, ..., \sigma_r$ are those in the basic hypothesis (see §2),

$$T=\frac{q(r+1)D}{c_1\theta\, e_{\mathfrak{p}} f_{\mathfrak{p}} \log p}, \tag{3.5}$$

$$\widetilde{D}_{-1}=h+\nu\log q-1, \qquad D_{-1}=\lfloor \widetilde{D}_{-1}\rfloor, \tag{3.6}$$

$$\widetilde{D}_0=\frac{1}{c_1c_4}\frac{1}{(D_{-1}+1)}\frac{SD}{d}\frac{1}{\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q}, \qquad D_0=\lfloor \widetilde{D}_0\rfloor, \tag{3.7}$$

$$D_i=\frac{D}{c_1c_2rp^{\varkappa}d\sigma_i}, \quad 1\leqslant i\leqslant r. \tag{3.8}$$

3.2. Proposition 3.1

Set

$$U=\frac{q^{r+1}}{e_{\mathfrak{p}} f_{\mathfrak{p}}\log p}SD. \tag{3.9}$$

PROPOSITION 3.1. *Under the hypotheses of Theorem I, we have*

$$\mathrm{ord}_p(\Xi-1)<U.$$

In §§4–7, we shall prove Proposition 3.1.

LEMMA 3.2. *Proposition 3.1 implies Theorem I.*

Proof. On noting (2.1), (3.1), (3.2) and (3.4), Proposition 3.1 gives

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}(\Xi-1)<\frac{f_0}{1+10^{-26}}\left(c_2q^2\frac{p^{\varkappa}}{e_{\mathfrak{p}}\theta}\right)^r\frac{r^r(r+1)^{r+1}}{r!}\frac{d^{r+2}\log^* d}{q^u f_{\mathfrak{p}}\log p}&\\ \times\max\left\{\frac{p^{f_{\mathfrak{p}}}}{\delta(\mathfrak{a}')(f_{\mathfrak{p}}\log p)^{r+1}},\frac{e^r}{r^r}\right\}\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}\sigma_1\dots\sigma_r h,&\end{aligned} \tag{3.10}$$

where

$$f_0=(1+10^{-26})(1+\varepsilon)\left(2+\frac{1}{g_2}\right)c_0c_1c_3c_4q^2. \tag{3.11}$$

Recall $a^{(1)}$ and $c^{(1)}$ given in §1.3. By Table 3.2 below, we have $f_0\leqslant c^{(1)}$. From (1.2), (1.3), (2.1) and (2.2) we get

$$\left(\frac{c_2q^2p^{\varkappa}}{e_{\mathfrak{p}}\theta}\right)^n<(1+10^{-26}){a^{(1)}}^n.$$

On applying (2.9) and (2.10) and observing that

$$\frac{r^r}{r!}\leqslant\frac{2^{r-n}n^n}{n!},$$

Theorem I follows from (3.10). □

Case	c_0	c_1	c_3	c_4	c_5			g_9	
					$r=2$	$r\in[3,7]$	$r\geqslant 8$	$r=2$	$r\geqslant 3$
(I.1)	2.66	1.449	1.4647	20.74	0.5377	0.55	0.56	1.1062	1.0666
(I.2)	1.9	1.4494	1.3852	20.8	0.538	0.551	0.56	$\frac{107}{103}$	$\frac{107}{103}$
(II)	2.74	1.4372	0.8412	19	0.53	0.54	0.55	1.109 02	1.067 94
(III.1)	2.78	1.4341	2.992	18.7	0.528	0.536	0.55	1.1096	1.069 93
(III.2)	2.6	1.432	3.26	18.2757	0.5267	0.534	0.55	$\frac{107}{103}$	$\frac{107}{103}$
(IV)	3	1.4441	3.849	20	0.5345	0.543	0.56	1.101 34	1.064 22
(V)	2.5	2.5347	0.4757	3.765	0.753	0.78	0.827	1.107 45	1.0658

Table 3.1. We have $g_9=\frac{107}{103}$ for $r\geqslant 8$ in all cases.

3.3. Numerical preparation for §§4–7

Here we make a detour. The reader may skip this subsection and continue to §4. We shall prepare most inequalities, which are needed in the theoretical argumentation in §§4–7, and the validity of which is reduced to numerical verifications in each of the cases (I)–(V) (see §1.3), using PARI/GP CALCULATOR V. 2.3.0 (shortened as PARI/GP). We hope, in this way, we can make the proof in §§4–7 neater and verifiable from the very bottom.

We keep the notation introduced in §1, §2 and §5♣. The values of c_0, c_1, c_3, c_4 and c_5 are given in Table 3.1 above. The definition of g_9 is given in (3.16).

Let c_2 be given by (2.2), and

$$a^*=\begin{cases} 7, & \text{in cases (I), (II) and (IV),}\\ \frac{7}{2}, & \text{in case (III),}\\ \frac{26}{3}, & \text{in case (V).}\end{cases} \tag{3.12}$$

Set

$$\eta=1-\frac{c_5}{r+1} \quad\text{and}\quad \varrho=\begin{cases} 58, & \text{if } d\geqslant 2,\\ 17, & \text{if } d=1.\end{cases} \tag{3.13}$$

Recall that $\varkappa$ is defined by (1.2), ϑ and θ by (2.1), and w_K is the number of roots of unity in K. Note that θ satisfies

$$\check{\theta}\leqslant\theta\leqslant\hat{\vartheta}, \tag{3.14}$$

where $\check{\theta}=\check{\vartheta}/(1+10^{-26})$, and $\check{\vartheta}$ and $\hat{\vartheta}$ are given by Table 3.2 below.

We shall need

$$\frac{d}{e_{\mathfrak{p}}}\geqslant q^{u-1}(q-1), \tag{3.15}$$

which is a consequence of the fact that p is unramified in $\mathbb{Q}(\zeta_{q^u})$.

We now define g_j $(0\leqslant j\leqslant 12)$, g_{61}, g_{91}, ε, i^* and i_1 by the following set of formulas:

$$
\begin{aligned}
g_0 &= g_0(r,d) = G_1(r,d), \quad \text{where } G_1(n,d) \text{ is defined by (1.11)},\\
g_1 &= \log e^4(r+1)d,\\
i^* &= \begin{cases} \dfrac{3g_1}{\log q\eta^{r+1}}+1, & \text{if } 2\leqslant r\leqslant 7,\\ \dfrac{3g_1}{\log qe^{-c_5}}+1, & \text{if } r\geqslant 8,\end{cases}\\
g_2 &= \begin{cases} \dfrac{c_3q(r+1)g_0e_{\mathfrak{p}}}{\log p}, & \text{in cases (I), (II) and (V)},\\ c_3q(r+1)^2d, & \text{in cases (III) and (IV)},\end{cases}\\
g_3 &= \frac{2}{\varrho}c_0c_1c_4(a^*)^r\frac{r^r(r+1)^r}{(r!)^2}g_1f_{\mathfrak{p}}\log p,\\
g_4 &= \frac{q(r+1)}{c_1\hat{\vartheta}}\frac{g_3}{f_{\mathfrak{p}}\log p}\cdot\begin{cases} 1, & \text{in cases (I.2) and (III)},\\ g_1^{-1}, & \text{otherwise},\end{cases}\\
1+\varepsilon &= \left(1+\frac{r+1}{2g_4}\right)^r,\\
i_1 &= \left\lfloor \frac{\log c_5(r+1)^{-1}g_4}{\log \eta^{-(r+1)}}\right\rfloor, \qquad\qquad (3.16)\\
g_5 &= \frac{c_3}{c_1c_4}\frac{q(r+1)g_3}{g_1f_{\mathfrak{p}}\log p},\\
g_{61} &= 2c_0c_1^{1-r}c_4\left(\frac{q}{\hat{\vartheta}}\right)^r\frac{(r+1)^re^r}{r!\,r^r}f_{\mathfrak{p}}\log p\cdot\frac{q-1}{q}g_1\cdot\begin{cases} g_3^{r-1}, & \text{in cases (I.2) and (III)},\\ \left(\dfrac{g_3}{g_1}\right)^{r-1}, & \text{otherwise},\end{cases}\\
g_6 &= \varrho\left(1+\frac{1}{g_5}\right)\left(1+\frac{1}{g_{61}}\right)\frac{1}{c_1^{r+1}c_2^rc_4p^{\varkappa r}w_K}\frac{r!e^r}{r^{2r}},\\
g_7 &= \frac{c_3q(r+1)g_0g_3}{f_{\mathfrak{p}}\log p},\\
g_8 &= \frac{1}{g_7}\left(\log g_7+g_1+\max\left\{\log\frac{g_6d}{e^{g_1}},0\right\}\right)+\frac{r}{c_3q(r+1)^2}\frac{\log g_3}{g_3},\\
g_{91} &= \begin{cases} 1+\dfrac{1+3\log\log 3d}{g_0}, & \text{if } d\geqslant 2,\\ 1+\dfrac{1}{g_0}\left(1+\log\dfrac{\log 6}{\log 2\cdot\log 3}\right), & \text{if } d=1,\end{cases}\\
g_9 &= \max\left\{g_{91},\tfrac{107}{103}\right\},\\
g_{10} &= \exp(-1+10^{-15})\frac{r-1}{q(r+1)c_2p^{\varkappa}}\cdot\begin{cases} g_0^{-1}\log p, & \text{in case (I.2)},\\ \dfrac{1}{r+1}, & \text{otherwise},\end{cases}
\end{aligned}
$$

$$g_{11}=\frac{4}{\varrho}qec_0c_1c_3c_4(a^*)^r\,\frac{(r+1)^{r+1}(r-1)^{r-1}}{(r!)^2}\,g_0g_1,$$

$$g_{12}=\begin{cases}\dfrac{g_1}{2g_7}+\dfrac{1}{g_{11}}, & \text{if } d\geqslant 2,\\ 0, & \text{if } d=1.\end{cases}$$

Now we show how to get the upper bound for g_9 in Table 3.1 by an example: case (I.1) with $r=2$. By considering d as a continuous variable with $d\geqslant 2$ and analyzing $\partial g_{91}/\partial d$ and $\partial^2 g_{91}/\partial d^2$, we see that

$$g_{91}(2,d)\leqslant g_{91}(2,4113)\leqslant 1.1062,$$

whence $g_9(2,d)\leqslant 1.1062$.

Let c_0 be given by Table 3.1, $g_9=g_9(r,d)$ in (3.16) and set

$$c_{01}=\frac{c_0(\log^* d)p^{f_\mathfrak{p}}}{p^{f_\mathfrak{p}}-1}, \tag{3.17}$$

$$c_{02}=c_0(\log^* d)\cdot\begin{cases}\frac{3}{2}, & \text{in case (I.2)},\\ 1, & \text{otherwise},\end{cases} \tag{3.18}$$

$$c_{03}=c_{03}(r,d,\mathfrak{p})=\frac{g_9(r,d)}{c_{01}-1}. \tag{3.19}$$

It is readily verified that

$$c_{03}\leqslant \hat{c}_{03}, \tag{3.20}$$

where $\hat{c}_{03}=\hat{c}_{03}(r)$ is given by

$$\hat{c}_{03}(r)=\begin{cases}\max\left\{\dfrac{g_9(r,2)}{c_0\frac{9}{8}-1},\dfrac{g_9(r,3)}{\frac{27}{26}c_0\log 3-1},\dfrac{g_9(r,4)}{c_0\log 4-1}\right\}, & \text{in case (I.1)},\\ \dfrac{\frac{107}{103}}{\frac{3}{2}c_0-1}, & \text{in case (I.2)},\\ \max\left\{\dfrac{g_9(r,2)}{\frac{5}{4}c_0-1},\dfrac{g_9(r,3)}{\frac{5}{4}c_0\log 3-1},\dfrac{g_9(r,4)}{c_0\log 4-1}\right\}, & \text{in case (II)},\\ \max\left\{\dfrac{g_9(r,2)}{c_0-1},\dfrac{g_9(r,3)}{c_0\log 3-1}\right\}, & \text{in cases (III.1) and (IV)},\\ \dfrac{g_9(r,1)}{c_0-1}, & \text{in case (III.2)},\\ \max\left\{\dfrac{g_9(r,2)}{\frac{4}{3}c_0-1},\dfrac{g_9(r,4)}{c_0\log 4-1}\right\}, & \text{in case (V)}.\end{cases} \tag{3.21}$$

Case	$p\geqslant$	$d\geqslant$	$e_{\mathfrak{p}}\geqslant$	$f_{\mathfrak{p}}\geqslant$	$p^{\varkappa}\geqslant$	$e_{\mathfrak{p}}\check{\vartheta}$	$\hat{\vartheta}$	$\frac{e_{\mathfrak{p}}}{d}\leqslant$	$w_K\geqslant$	$f_0\leqslant$
(I.1)	3^*	2	1	1	3	$\frac{3}{2}$	$\frac{3}{2}$	1	2	939
(I.2)	3^*	1^*	1^*	1^*	3^*	$\frac{3}{2}^*$	$\frac{3}{2}^*$	1^*	2^*	636
(II)	5^*	2	2	1	5	$\frac{5}{2}$	$\frac{5}{4}$	1	2	505
(III.1)	5	2	1^*	1	1^*	$\frac{3}{4}$	1	$\frac{1}{2}$	2	1794
(III.2)	5	1^*	1^*	1^*	1^*	$\frac{3}{4}$	1	1^*	2^*	1790
(IV)	7	2	2	1	1	$\frac{1}{2}$	$\frac{7}{6}$	1	2	2680
(V)	2^*	2	1	2	4	2	2	$\frac{1}{2}$	6	206

Table 3.2. Here $*$ means the exact equality

(Note that d is even in case (V) by (1.5).) In the computation, we shall use that

$$\hat{c}_{03}(r)\leqslant\hat{c}_{03}(3)\ \ (3\leqslant r\leqslant 7)\quad\text{and}\quad \hat{c}_{03}(r)\leqslant\hat{c}_{03}(8)\ \ (r\geqslant 8).$$

It can be verified that Table 3.2 above is true, where the values of $e_{\mathfrak{p}}\check{\vartheta}$ and $\hat{\vartheta}$ make (3.14) valid, and the column of f_0 is obtained by direct computation according to its definition (3.11), using the rest of Table 3.2.

We assert that the following inequalities for $r(\geqslant 2)$, d and $\mathfrak{p}$,

$$f_j=f_j(r,d,\mathfrak{p})\geqslant 0\quad(1\leqslant j\leqslant 30)\tag{3.22}$$

hold for all cases (I)–(V), where f_j $(1\leqslant r\leqslant 30)$ are defined as follows. (The inequality $f_j\geqslant 0$ will be referred to as (3.22) (j).) In fact, we have tried very hard to make, in each case, a nearly optimal choice of c_0, c_1, c_3, c_4 and c_5, such that f_0 (see (3.11)) is as small as possible, subject to condition (3.22). We let

$$\begin{aligned}f_1=2c_5q\left(1-\frac{1}{2g_2}\right)&-c_1\left(g_{12}+\left(1+\frac{1}{2(c_{02}-1)}\right)g_8\right)\\&-\frac{1}{c_2}\left(q+\frac{1}{2(c_{02}-1)}\left(1+\frac{1}{2g_2+1}\right)\right)\\&-\frac{1}{c_3}\left(\frac{1}{e_{\mathfrak{p}}\theta}(g_9\hat{\eta}+\hat{c}_{03})+\left(1+\frac{1}{c_{02}-1}\right)g_{10}\right)\\&-\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\left(1+\frac{1}{c_{02}-1}+\left(\theta+\frac{1}{p-1}\right)\frac{e_{\mathfrak{p}}}{d}\right),\end{aligned}$$

where and in the sequel, c_0, c_1, c_3, c_4 and c_5 are given by Table 3.1, c_2 by (2.2), q by (1.3), g_j $(0\leqslant j\leqslant 12)$ and i_1 by (3.16), c_{02} by (3.18), $\hat{c}_{03}$ by (3.21), θ by (2.1), $e_{\mathfrak{p}}\check{\vartheta}$ and $\hat{\vartheta}$ by Table 3.2, and

$$\hat{\eta}=\begin{cases}\eta, & \text{if } 2\leqslant r\leqslant 7,\\ 1, & \text{if } r\geqslant 8,\end{cases}$$

with η given by (3.13),

$$f_2=((q\eta)^r-1)\frac{q}{c_2}-\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\left(\frac{q\log q}{(q-1)g_1}+\begin{cases}0, & \text{if } p>2,\\ \dfrac{5\log q}{3\log q\eta^{r+1}}, & \text{if } p=2\end{cases}\right),$$

where $(q\eta)^r$ is replaced by $q^r e^{-c_5}$ when $r\geqslant 8$,

$$\begin{aligned}f_3=f_1+2c_5q\left(q-2+\frac{1}{2g_2}\right)+\frac{g_9}{c_3e_{\mathfrak{p}}\theta}(\hat{\eta}-\eta^{r+2})\\ -\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\left(\frac{\log q}{(q-1)g_1}+\begin{cases}0, & \text{if } p>2,\\ \dfrac{5\log q}{3\log q\eta^{r+1}}, & \text{if } p=2\end{cases}\right),\end{aligned}$$

where η^{r+2} is replaced by e^{-c_5} when $r\geqslant 8$,

$$\begin{aligned}f_4=2c_5q(q-1)\left(\eta-\frac{r+1}{c_5g_2g_4}\right)-c_1\left(g_{12}+\left(1+\frac{1}{2(c_{02}-1)}\right)g_8\right)\\ -\frac{1}{c_2}\left(\frac{1}{2(c_{02}-1)}\left(1+\frac{1}{2g_2+1}\right)+q\begin{cases}\frac{7}{8}, & \text{if } p>2,\\ \frac{13}{16}, & \text{if } p=2\end{cases}\right)\\ -\frac{1}{c_3}\left(\frac{1}{e_{\mathfrak{p}}\theta}\left(g_9\frac{r+1}{c_5g_4}+\hat{c}_{03}\right)+\left(1+\frac{1}{c_{02}-1}\right)g_{10}\right)\\ -\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\left(1+\frac{1}{c_{02}-1}+\left(\theta+\frac{1}{p-1}\right)\frac{e_{\mathfrak{p}}}{d}+\begin{cases}\dfrac{\log q\eta^{r+1}}{g_1}, & \text{if } p>2,\\ \dfrac{5\log q}{3\log q\eta^{r+1}}, & \text{if } p=2\end{cases}\right),\end{aligned}$$

where $\log q\eta^{r+1}$ is replaced by $\log qe^{-c_5}$ when $p>2$ and $r\geqslant 8$,

$$f_5=\begin{cases}c_1-4c_5\eta^r-\dfrac{2}{q^r\eta g_4}\left(\dfrac{r+1}{g_2}+\dfrac{1}{qc_3e_{\mathfrak{p}}\check{\theta}}\right), & \text{if } p>2,\\ c_1-6c_5\eta^r-\dfrac{1}{q^rg_4}\left(\dfrac{r+1}{\eta g_2}+\dfrac{1}{qc_3e_{\mathfrak{p}}\check{\theta}}\right), & \text{if } p=2,\end{cases}$$

$$f_6=2-\left(\frac{1}{g_2}+\frac{1}{qc_3e_{\mathfrak{p}}\check{\theta}(r+1)}\right),$$

$$f_7=\begin{cases} 2c_5-\left(2-\dfrac{c_5}{r+1}\right)\left(\dfrac{r+1}{q^r g_2}+\dfrac{1}{q^{r+1}c_3e_{\mathfrak{p}}\breve{\theta}}\right), & \text{if } p>2,\\ 1-\dfrac{1}{q^r g_2}-\dfrac{1}{q^{r+1}(r+1)c_3e_{\mathfrak{p}}\breve{\theta}}, & \text{if } p=2,\end{cases}$$

where $2-c_5/(r+1)$ is replaced by 2 when $r\geqslant 8$,

$$f_8=\begin{cases} 2c_5-\dfrac{\hat{\eta}}{q^{r+1}c_3e_{\mathfrak{p}}\breve{\theta}}, & \text{if } p>2,\\ 1-\dfrac{\hat{\eta}}{q^{r+1}(r+1)c_3e_{\mathfrak{p}}\breve{\theta}}, & \text{if } p=2,\end{cases}$$

$$f_9=\left(\begin{cases}\frac78, & \text{if } p>2,\\ \frac{13}{16}, & \text{if } p=2\end{cases}\right)-\frac{1}{(e^4(r+1)d)^3}-\left(1+\frac{1}{g_5}\right)\frac{c_2}{c_4}\frac{\log q}{q\log q\eta^{r+1}}\begin{cases}3, & \text{if } p>2,\\ \frac43, & \text{if } p=2,\end{cases}$$

$$f_{10}=\left(\begin{cases}\frac78, & \text{if } p>2,\\ \frac{13}{16}, & \text{if } p=2\end{cases}\right)-\frac{1}{(q\eta^{r+1})^{i_1}}-\left(1+\frac{1}{g_5}\right)\frac{c_2}{c_4}\frac{\log q}{q}\frac{i_1}{g_1}\begin{cases}1, & \text{if } p>2,\\ \frac49, & \text{if } p=2,\end{cases}$$

where i_1 is replaced by 10 when $r\geqslant 8$,

$$f_{11}=2c_5\eta-\frac{\log q}{\log q\eta}\left(\frac{1}{c_2}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{1}{g_1q}\right),$$

$$f_{12}=2c_5\eta^2-\frac{\log q}{\log q\eta}\left(\frac{1}{c_2}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{1}{g_1q^2}\right) \qquad (\text{for } r\geqslant 3),$$

$$f_{13}=2c_5\eta^3-\frac{\log q}{\log q\eta}\left(\frac{1}{c_2}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{1}{g_1q^3}\right) \qquad (\text{for } r\geqslant 4),$$

$$f_{14}=2c_5\eta^{r-1}-\frac{\log q}{\log q\eta}\left(\frac{1}{c_2}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{1}{g_1q^4}\right\} \qquad (\text{for } 5\leqslant r\leqslant 7),$$

$$f_{15}=2c_5\left(\begin{cases}\eta^{r+1}, & \text{if } p>2,\\ e^{-c_5}, & \text{if } p=2\end{cases}\right)-\left(\frac{1}{c_2}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{1}{g_1q^4}\right) \qquad (\text{for } r\geqslant 8),$$

$$f_{16}=2c_5\eta^r-\frac{\log q}{\log q\eta}\left(\frac{1}{c_2}\left(\begin{cases}\frac78, & \text{if } p>2,\\ \frac{13}{16}, & \text{if } p=2\end{cases}\right)+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{1}{g_1q^r}\right),$$

where η^r is replaced by e^{-c_5} when $r\geqslant 8$,

$$f_{17}=2c_5(q-1)\log q\eta-\frac{1}{c_2}\frac{\log q}{(q\eta^{r+1})^{i_1}}-\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{\log q}{g_1q\eta},$$

$$f_{18}=e^3-\frac{2}{(r+1)d}-\frac{c_3g_0}{(g_0-1)f_{\mathfrak{p}}\log p}\begin{cases}q^2, & \text{if } p>2,\\ q^{13/6}, & \text{if } p=2\end{cases}$$

$$f_{19}=e^3-\frac{2q}{(r+1)d}-\frac{c_3qg_0}{(g_0-1)f_{\mathfrak{p}}\log p},$$

$$f_{20}=q-\frac{1}{\eta^{r+1}}-\frac{1}{g_2},$$

$$f_{21}=\begin{cases}\dfrac{r-1}{c_1c_2}\dfrac{g_3}{p^{\varkappa}}-e, & \text{in cases (I.2) and (III)},\\ \dfrac{p-1}{2p}\dfrac{r-1}{c_1c_2}\dfrac{g_3}{g_1}-e, & \text{otherwise},\end{cases}$$

$$f_{22}=\frac{g_0}{r+1}-\log\frac{c_5g_4}{r+1},$$

$$f_{23}=\frac{c_5g_4\eta^{r+1}}{r+1}-e,$$

$$f_{24}=1-\frac{\log g_0}{g_0}-\frac{2}{r+1},$$

$$f_{25}=2c_5-\frac{(r+1)q}{g_2g_4}-\frac{1}{c_3e_{\mathfrak{p}}\check{\theta}}\frac{1}{g_4},$$

$$f_{26}=\frac{g_0}{r+1}-\log\left(3q^{r+2}\frac{c_3(r+1)d}{f_{\mathfrak{p}}\log p}\right),$$

$$f_{27}=2c_5\eta^r-\frac{r+1}{q^rg_2g_4\eta}+\left(1-\frac{2}{\eta}\right)\frac{1}{q^{r+1}c_3e_{\mathfrak{p}}\check{\theta}\,g_4}\quad\text{(for } p=2 \text{ only)},$$

where η^r is replaced by e^{-c_5} and $1-2/\eta$ is replaced by $-2/\eta$ when $r\geqslant 8$,

$$f_{28}=2c_5\left(1-\frac{1}{g_2}\right)q\eta-\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{\log q}{g_1},$$

$$f_{29}=(q\eta^{r+1})^{i_1}-q,$$

$$f_{30}=\frac{q^2\eta}{3}\left(1-\frac{1}{g_2}\right)-\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{e_{\mathfrak{p}}}{d}\hat{\vartheta}.$$

We now prove (3.22). Observe that each f_j $(1\leqslant j\leqslant 30)$, as a function of r, increases monotonically for $r\geqslant 8$. (Here we use the fact that, as functions of r, η^{r+1} increases and η^r decreases, and both tend to e^{-c_5} as $r\to\infty$.) Thus (3.22) with $r=8$ implies (3.22) for $r>8$, and it suffices to verify (3.22) for $r=2,3,...,8$.

Let

$$\delta=\frac{1}{c_4}\left(1+\frac{1}{g_5}\right).$$

We estimate the following terms $F_j(e_{\mathfrak{p}}\theta)$ appearing in f_j $(j=1,3,4)$, where

$$F_j(x)=\frac{\beta_j}{x}+\frac{\delta}{d}x,$$

with

$$\beta_1 = \frac{1}{c_3}(g_9\hat{\eta}+\hat{c}_{03}),$$
$$\beta_3 = \frac{1}{c_3}\left(\hat{c}_{03}+g_9\begin{cases}\eta^{r+2}, & \text{if } 2\leqslant r\leqslant 7,\\ e^{-c_5}, & \text{if } r\geqslant 8\end{cases}\right),$$
$$\beta_4 = \frac{1}{c_3}\left(g_9\frac{r+1}{c_5 g_4}+\hat{c}_{03}\right).$$

Thus, by the fact that $F_j''(x)>0$ for $x>0$ $(j=1,3,4)$, we have

$$F_j(e_\mathfrak{p}\theta)\leqslant \max\{F_j(e_\mathfrak{p}\check{\theta}), F_j(e_\mathfrak{p}\hat{\vartheta})\}, \quad j=1,3,4.$$

In f_j $(j=1,3,4)$, for cases (III) and (IV), we replace $F_j(e_\mathfrak{p}\theta)$ by the above upper bound; for cases (I), (II) and (V), we replace $F_j(e_\mathfrak{p}\theta)$ by

$$\frac{\beta_j}{e_\mathfrak{p}\check{\theta}}+\delta\left(\frac{e_\mathfrak{p}}{d}\right)\hat{\vartheta}.$$

We denote by $\tilde{f}_j$ $(j=1,3,4)$ the resulting function. Thus $f_j\geqslant\tilde{f}_j$ $(j=1,3,4)$.

In f_j $(1\leqslant j\leqslant 30$, with $j\neq 1,3,4)$, $\tilde{f}_1$, $\tilde{f}_3$ and $\tilde{f}_4$, we now apply the values

$$e_\mathfrak{p}\check{\theta}=\frac{e_\mathfrak{p}\check{\vartheta}}{1+10^{-26}}$$

and $\hat{\vartheta}$ given by Table 3.2; furthermore, we replace g_9 by its upper bound in Table 3.1, p, d, $e_\mathfrak{p}$, $f_\mathfrak{p}$, $p^{\varkappa}$ and w_K by their lower bounds in Table 3.2, and $e_\mathfrak{p}/d$ by its upper bound in Table 3.2. Now we are ready to run PARI/GP, separately in each of the cases (I)–(V), for computing f_j $(1\leqslant j\leqslant 30,\ j\neq 1,3,4)$, $\tilde{f}_1$, $\tilde{f}_3$ and $\tilde{f}_4$ for $r=2,3,...,8$. We conclude that, in each case,

$$f_j(r,d,\mathfrak{p})\geqslant 0 \quad (r=2,3,...,8), \quad 1\leqslant j\leqslant 30,\ j\neq 1,3,4,$$
$$\tilde{f}_j(r,d,\mathfrak{p})\geqslant 0 \quad (r=2,3,...,8), \quad j=1,3,4.$$

This completes the proof of (3.22).

Recall (3.16). It is readily seen that the following inequalities (3.23), (3.25)–(3.33) hold. We now list (3.23)–(3.33) and prove part of them, when it is necessary.

$$S\geqslant g_2, \quad D\geqslant g_3, \quad \frac{SD}{d}\geqslant g_7 \quad\text{and}\quad \frac{2SD}{rd^2\sigma_i}\geqslant g_{11}\ \ (1\leqslant i\leqslant r). \tag{3.23}$$

Proof. We prove $D\geqslant g_3$. The other three inequalities can be proved similarly. Note that $w_K\geqslant q^u$ and $c_2qp^{\varkappa}/e_{\mathfrak{p}}\theta\geqslant a^*$, by (1.2)–(1.4), (2.1), (2.2) and (3.12). Applying [14, Theorem 3], and using (2.6) and (5.4)$^\clubsuit$, we obtain

$$d^{r+1}(\log^* d)\sigma_1 \dots \sigma_r \geqslant \frac{1}{\varrho}\frac{r^r}{r!e^r}q^\nu w_K, \tag{3.24}$$

where ϱ is given by (3.13). Now $D\geqslant g_3$ follows at once. Observe that we have replaced the first maximum in (3.4) by $(e^r/r^r)f_{\mathfrak{p}}\log p$ to obtain the lower bound g_3 of D. □

$$T\geqslant g_4 \quad \text{and} \quad \binom{[T]+r}{r}\leqslant(1+\varepsilon)\frac{T^r}{r!}, \tag{3.25}$$

$$\widetilde{D}_0\geqslant g_5 \quad \text{and} \quad D_0+1\leqslant\left(1+\frac{1}{g_5}\right)\widetilde{D}_0, \tag{3.26}$$

$$(D_{-1}+1)(D_0+1)\frac{q^\nu D_1\dots D_r}{G_0/\delta(\mathfrak{a}')}\geqslant c_{01}(2S+1)\binom{[T]+r}{r}, \tag{3.27}$$

where $G_0=G/q^u$ with $G=p^{f_{\mathfrak{p}}}-1$, $\mathfrak{a}'=\{\alpha_1',\dots,\alpha_r'\}$ and $\delta(\mathfrak{a}')$ are those in the basic hypothesis (see §2), and c_{01} is given by (3.17).

$$(D_{-1}+1)(D_0+1)(q^\nu D_1\dots D_r+1)\leqslant g_6SD^{r+1}\leqslant\exp\left(g_8\frac{SD}{d}\right). \tag{3.28}$$

Proof. By (3.4), (3.8) and (3.16), we have $q^\nu D_1\dots D_r\geqslant g_{61}$. Now (3.7), (3.8), (3.24) and (3.26) yield the first inequality of (3.28). Note that

$$g_6SD^{r+1}=\frac{g_6d}{e^{g_1}}e^{g_1}\frac{SD}{d}D^r \quad \text{and} \quad \frac{r\log D}{SD/d}\leqslant\frac{r}{c_3q(r+1)^2}\frac{\log D}{D}.$$

Now on applying (3.23), the second inequality of (3.28) follows. □

$$p^{\varkappa}S\sum_{i=1}^r D_i\sigma_i\leqslant\frac{1}{c_1c_2}\frac{SD}{d}, \tag{3.29}$$

$$T(\widetilde{D}_{-1}+1)=T(h+\nu\log q)=\frac{1}{c_1c_3e_{\mathfrak{p}}\theta}\frac{SD}{d}, \tag{3.30}$$

$$\log\left(e\left(2+\frac{S}{D_{-1}+1}\begin{cases} q, & \text{if } p>2, \\ q^{7/6}, & \text{if } p=2\end{cases}\right)\right)\leqslant g_1, \tag{3.31}$$

$$\log\left(e\left(2q+\frac{S}{D_{-1}+1}\right)\right)\leqslant g_1. \tag{3.32}$$

Proof. Formulas (3.31) and (3.32) are consequences of (3.22) (18) and (3.22) (19), respectively. □

$$x\log\left(\frac{1}{e^h}+\frac{(r-1)D}{c_1c_2\,p^{\varkappa}}\frac{1}{x}\right)\leqslant g_{10}\frac{1}{c_1c_3}\frac{SD}{d}\quad \text{for } x\geqslant 1. \tag{3.33}$$

Proof. Recall that $h\geqslant g_0=G_1(r,d)>39$ (by (1.11) and $r\geqslant 2$). By (3.22) (21), we see that $(r-1)D/c_1c_2p^{\varkappa}\geqslant f_{21}+e\geqslant e$. The proof of [37, (9.31)] also works here, which gives

$$\text{left-hand side of (3.33)}\leqslant\frac{e^{-1+\delta}(r-1)D}{c_1c_2p^{\varkappa}},$$

where $\delta\in(0,1)$ satisfies $\delta=e^{-(h+1-\delta)}<e^{-h}<10^{-15}$. Using the fact that

$$\frac{S}{d}\geqslant\begin{cases}\dfrac{c_3q(r+1)g_0}{\log p}, & \text{in case (I.2)},\\ c_3q(r+1)^2, & \text{otherwise},\end{cases}$$

(3.33) follows. □

4. The construction of auxiliary functions

Recall (1.4). By Hasse [12, p. 220], we have $q^u\,|\,(p^{f_{\mathfrak{p}}}-1)$. Put

$$G=p^{f_{\mathfrak{p}}}-1\quad\text{and}\quad G_0=\frac{G}{q^u}. \tag{4.1}$$

Choose and fix ζ, a Gth primitive root of unity in $K_{\mathfrak{p}}$, such that

$$\zeta^{G_0}=\alpha_0. \tag{4.2}$$

Fix $\xi\in\mathbb{C}_p$ satisfying

$$\xi^q=\zeta. \tag{4.3}$$

Thus $\xi^{G_0}\in\mathbb{C}_p$ is a qth root of α_0. We fix

$$\alpha_0^{1/q}:=\xi^{G_0}. \tag{4.4}$$

Furthermore, we have

$$\zeta^{G_0/q}=\alpha_0^{1/q}\quad\text{if } q\,|\,G_0. \tag{4.5}$$

Recall $\alpha'_1,...,\alpha'_r$ in the basic hypothesis (see §2) and $\theta_1,...,\theta_r$ in §5♣. By (1.16), (2.11) and (5.10)♣, there exist rational integers $\tilde a_j$, $\tilde a'_j$ and $\tilde d_j$ such that

$$\begin{aligned}\alpha_j&\equiv\zeta^{\tilde a_j}\ (\mathrm{mod}\ \mathfrak{p})\quad(1\leqslant j\leqslant n),\\ \alpha'_j&\equiv\zeta^{\tilde a'_j}\ (\mathrm{mod}\ \mathfrak{p})\quad(1\leqslant j\leqslant r),\\ \theta_j&\equiv\zeta^{\tilde d_j}\ (\mathrm{mod}\ \mathfrak{p})\quad(1\leqslant j\leqslant r).\end{aligned} \tag{4.6}$$

Now [36, Lemma 1.1] implies that

$$\begin{aligned} \operatorname{ord}_p(\alpha_j^{p^{\varkappa}}\zeta^{a_j}-1) &> \theta+\frac{1}{p-1} \quad (1\leqslant j\leqslant n),\\ \operatorname{ord}_p((\alpha_j')^{p^{\varkappa}}\zeta^{a_j'}-1) &> \theta+\frac{1}{p-1} \quad (1\leqslant j\leqslant r),\\ \operatorname{ord}_p(\theta_j^{p^{\varkappa}}\zeta^{d_j}-1) &> \theta+\frac{1}{p-1} \quad (1\leqslant j\leqslant r), \end{aligned} \tag{4.7}$$

where $a_j=-\tilde{a}_j p^{\varkappa}$, $a_j'=-\tilde{a}_j' p^{\varkappa}$, $d_j=-\tilde{d}_j p^{\varkappa}$, $\varkappa$ is given by (1.2) and θ by (2.1).

Recall that $r\geqslant 2$ and

$$|\langle\bar{\alpha}_0,\bar{\theta}_1,...,\bar{\theta}_r\rangle|=\frac{p^{f_{\mathfrak{p}}}-1}{\delta(\mathfrak{a}')}$$

(see (1.6), §2 and §5♣). By (4.2) and (4.6), we have

$$|\langle\bar{\alpha}_0,\bar{\theta}_1,...,\bar{\theta}_r\rangle|=|\langle\zeta^{G_0},\zeta^{\tilde{d}_1},...,\zeta^{\tilde{d}_r}\rangle|=|\langle\zeta^{\gcd(G_0,\tilde{d}_1,...,\tilde{d}_r)}\rangle|=\frac{p^{f_{\mathfrak{p}}}-1}{\gcd(G_0,\tilde{d}_1,...,\tilde{d}_r)}. \tag{4.8}$$

Obviously, $\gcd(G_0,\tilde{d}_1,...,\tilde{d}_r)=\gcd(G_0,d_1,...,d_r)$. Thus

$$\delta(\mathfrak{a}')=\gcd(G_0,d_1,...,d_r). \tag{4.9}$$

We have noted in §1.1 that there exists a $\mathbb{Q}$-isomorphism ψ from K into $\overline{\mathbb{Q}}_p\subseteq\mathbb{C}_p$ such that $K_{\mathfrak{p}}$ is value-isomorphic to $\mathbb{Q}_p(\psi(K))$, whence we can identify $K_{\mathfrak{p}}$ with $\mathbb{Q}_p(\psi(K))$. Henceforth we embed $K_{\mathfrak{p}}$ into $\mathbb{C}_p$ in this fashion.

For the basic properties of the p-adic exponential function exp and logarithmic function log, see, e.g., [34, §1.1].

Let $L_i(z_0,...,z_n)$ and α_i' $(1\leqslant i\leqslant r)$ be as specified in the basic hypothesis in §2. Then

$$\exp(L_i(0,\log\alpha_1^{p^{\varkappa}}\zeta^{a_1},...,\log\alpha_n^{p^{\varkappa}}\zeta^{a_n}))=(\alpha_i')^{p^{\varkappa}}\zeta^{a_i'},\quad 1\leqslant i\leqslant r, \tag{4.10}$$

(this is just (7.5)♣). Here and in (4.11) below exp and log signify the p-adic exponential and logarithmic functions. Henceforth for all $z\in\mathbb{C}_p$ with $\operatorname{ord}_p z\geqslant-\theta$, we define

$$((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^z=\exp(z\log(\alpha_i')^{p^{\varkappa}}\zeta^{a_i'}) \quad\text{and}\quad (\theta_i^{p^{\varkappa}}\zeta^{d_i})^z=\exp(z\log\theta_i^{p^{\varkappa}}\zeta^{d_i}). \tag{4.11}$$

Observe that the functions in (4.11) have supernormality θ in the sense that

$$((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{p^{-\theta}z} \quad\text{and}\quad (\theta_i^{p^{\varkappa}}\zeta^{d_i})^{p^{-\theta}z}$$

are p-adic normal functions by (4.7). (The concepts of p-adic normal series and functions are due to Mahler [17], see also Adams [1] and [34].) We define $(\theta_i^{p^{\varkappa}}\zeta^{d_i})^{1/q}$ by (4.11) with

$z=1/q$, and we fix a choice of qth roots of $\theta_1, ..., \theta_r$ in $\mathbb{C}_p$, denoted by $\theta_1^{1/q}, ..., \theta_r^{1/q}$, such that

$$(\theta_i^{p^{\varkappa}}\zeta^{d_i})^{1/q} = (\theta_i^{1/q})^{p^{\varkappa}}\xi^{d_i}, \quad 1 \leqslant i \leqslant r, \tag{4.12}$$

where ξ has been fixed, satisfying (4.3). We remark that, taking $\theta_0^{1/q}$ as $\alpha_0^{1/q}$ in (4.4), and $\theta_i^{1/q}$ $(1 \leqslant i \leqslant r)$ as in (4.12), then (5.11)$^♣$ still holds.

We shall use the notation introduced in Baker and Wüstholz [6, §12]:

$$\Delta(z;k) = \frac{(z+1)\dots(z+k)}{k!} \text{ for } k \in \mathbb{Z}_{>0} \quad \text{and} \quad \Delta(z;0)=1,$$

$$\Pi(z_1, ..., z_{r-1}; t_1, ..., t_{r-1}) = \prod_{i=1}^{r-1} \Delta(z_i;t_i) \quad (t_1, ..., t_{r-1} \in \mathbb{N}\,(:=\mathbb{Z}_{\geqslant 0})),$$

and

$$\Theta(z;k,l,m) = \frac{1}{m!}\left(\frac{d}{dz}\right)^m \Delta(z;k)^l \quad (l,m \in \mathbb{N}).$$

For the functions Π with $T'=t_1+...+t_{r-1} \geqslant 1$ we have

$$|\Pi| \leqslant e^{T'}\left(1+\frac{|z_1|+...+|z_{r-1}|}{T'}\right)^{T'}.$$

By the argument in Tijdeman [27, p. 200], we see that [36, Lemma 1.3] and the first assertion of [27, Lemma T1] remain valid for $x \leqslant 0$.

Recall the matrices $\widetilde{\boldsymbol{\mathcal{B}}}$ and $\boldsymbol{\mathcal{B}}$ in §5$^♣$, and that $\boldsymbol{b}_1, ..., \boldsymbol{b}_r$, the rows of $\boldsymbol{\mathcal{B}}$, form a basis for the lattice $\mathbf{M}$. For every $(\lambda_1, ..., \lambda_r) \in \mathbb{Z}^r$, $(\mu_1, ..., \mu_r) := (\lambda_1, ..., \lambda_r)\boldsymbol{\mathcal{B}}$ is in $\mathbf{M}$. We fix

$$\mu_0 = \lambda_1 b_{10} + ... + \lambda_r b_{r0}, \tag{4.13}$$

so that

$$(\mu_0, \mu_1, ..., \mu_r) = (0, \lambda_1, ..., \lambda_r)\widetilde{\mathcal{B}} \tag{4.14}$$

is in $\widetilde{\mathbf{M}}$. On defining for all $s \in \mathbb{Z}$, with the usual exponential function,

$$(\alpha_i')^{\mu_i s} = \exp(\mu_i s\, l_i') \quad (0 \leqslant i \leqslant r), \tag{4.15}$$

where l_i' is given by (2.7), we see that (4.14) yields

$$\prod_{i=1}^{r} \theta_i^{\lambda_i s} = \prod_{i=0}^{r} (\alpha_i')^{\mu_i s}. \tag{4.16}$$

We also write for $\boldsymbol{\mu} \in \mathbf{M}$ and $\boldsymbol{\lambda} = \boldsymbol{\mu}\mathcal{B}^{-1} = \boldsymbol{\mu}\mathcal{V}$ (see (5.15)$^♣$),

$$\mu_i' = q^{\nu}\mu_i\,(0 \leqslant i \leqslant r) \quad \text{and} \quad \lambda_i' = q^{\nu}\lambda_i\,(1 \leqslant i \leqslant r), \tag{4.17}$$

where μ_0 is given by (4.13). Thus $\mu_i'\in\mathbb{Z}$ $(0\leqslant i\leqslant r)$ by (5.4)♣.

We quote Lemma 7.1♣ as our Lemma 4.1 below, where

$$((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{\mu_i s/q} \quad \text{and} \quad (\theta_i^{p^{\varkappa}}\zeta^{d_i})^{\lambda_i s/q}$$

are given by the p-adic functions in (4.11) at $z=\mu_i s/q$ and $z=\lambda_i s/q$, respectively.

Lemma 4.1. *For all $\boldsymbol{\mu}\in\mathbf{M}$ and $s\in\mathbb{Z}$, we have*

$$\prod_{i=1}^{r}((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{\mu_i s/q}=\prod_{i=1}^{r}(\theta_i^{p^{\varkappa}}\zeta^{d_i})^{\lambda_i s/q},$$

where $\boldsymbol{\lambda}=(\lambda_1,...,\lambda_r)\in\mathbb{Z}^r$ is determined by $\boldsymbol{\lambda}=\boldsymbol{\mu}\mathcal{B}^{-1}=\boldsymbol{\mu}\mathcal{V}$.

Recall D_i $(1\leqslant i\leqslant r)$ defined by (3.8) and $q^{\nu}D_1\,...\,D_r\geqslant g_{61}$ (see the proof of (3.28)). Let

$$\mathbf{C}=\{\boldsymbol{x}\in\mathbb{R}^r: 0\leqslant x_i\leqslant D_i, 1\leqslant i\leqslant r\} \quad \text{and} \quad m=[q^{\nu}D_1\,...\,D_r]. \tag{4.18}$$

It may be of some interest to note that $q^{\nu}D_1\,...\,D_r\geqslant g_{61}>5\cdot 10^5$, computed by running PARI/GP. Thus $m\geqslant 5\cdot 10^5$. By Lemma 5.1♣, we see that $\mathbf{M}\cap(\mathbf{C}-\boldsymbol{x}^{(0)})$ $(\boldsymbol{x}^{(0)}:=\boldsymbol{x}_0)$ contains $m+1$ distinct points

$$\mathbf{0}, \quad \boldsymbol{\mu}_1=\boldsymbol{x}_1-\boldsymbol{x}_0, \quad ..., \quad \boldsymbol{\mu}_m=\boldsymbol{x}_m-\boldsymbol{x}_0.$$

Let $d_1,...,d_r$ be given by (4.7), G and G_0 by (4.1), and consider $\{\mathbf{0},\boldsymbol{\mu}_1,...,\boldsymbol{\mu}_m\}\mathcal{V}\subseteq\mathbb{Z}^r$ (recalling $\boldsymbol{\mathcal{V}}=\boldsymbol{\mathcal{B}}^{-1}$, see (5.15)♣). We classify the set

$$\left\{\frac{d_1}{\delta(\mathfrak{a}')}\lambda_1+...+\frac{d_r}{\delta(\mathfrak{a}')}\lambda_r:(\lambda_1,...,\lambda_r)\in\{\mathbf{0},\boldsymbol{\mu}_1,...,\boldsymbol{\mu}_m\}\mathcal{V}\right\}$$

by the congruence relation modulo $G_0/\delta(\mathfrak{a}')$, where $\delta(\mathfrak{a}')=(G_0,d_1,...,d_r)$ (see(4.9)). By Dirichlet's pigeonhole principle, there exist a subset $\boldsymbol{\Lambda}^{(0)}\subseteq\{\mathbf{0},\boldsymbol{\mu}_1,...,\boldsymbol{\mu}_m\}\mathcal{V}\subseteq\mathbb{Z}^r$ with cardinality $|\boldsymbol{\Lambda}^{(0)}|\geqslant(m+1)/(G_0/\delta(\mathfrak{a}'))$ and $\varepsilon_1\in\mathbb{Z}$ such that

$$\frac{d_1}{\delta(\mathfrak{a}')}\lambda_1+...+\frac{d_r}{\delta(\mathfrak{a}')}\lambda_r\equiv\varepsilon_1\left(\operatorname{mod}\frac{G_0}{\delta(\mathfrak{a}')}\right) \quad \text{for all } (\lambda_1,...,\lambda_r)\in\boldsymbol{\Lambda}^{(0)}.$$

Observe that $\boldsymbol{\Lambda}^{(0)}\subseteq\{\mathbf{0},\boldsymbol{\mu}_1,...,\boldsymbol{\mu}_m\}\mathcal{V}\subseteq\mathbb{Z}^r$ has the following properties:

(i) $\mathbf{M}^{(0)}:=\boldsymbol{\Lambda}^{(0)}\mathcal{B}\subseteq\mathbf{M}\cap(\mathbf{C}-\boldsymbol{x}^{(0)})$;

(ii) $q^{\nu}D_1\,...\,D_r/(G_0/\delta(\mathfrak{a}'))<|\mathbf{M}^{(0)}|=|\boldsymbol{\Lambda}^{(0)}|\leqslant q^{\nu}D_1\,...\,D_r+1$; (4.19)

(iii) $d_1\lambda_1+...+d_r\lambda_r\equiv\varepsilon^{(0)}\ (\operatorname{mod}\ G_0)$ for all $\boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(0)}$, where $\varepsilon^{(0)}:=\delta(\mathfrak{a}')\varepsilon_1$.

Fix a point $\boldsymbol{\lambda}^{(0)}=(\lambda_1^{(0)},...,\lambda_r^{(0)})$ of $\boldsymbol{\Lambda}^{(0)}$. Then

$$d_1(\lambda_1-\lambda_1^{(0)})+...+d_r(\lambda_r-\lambda_r^{(0)})\equiv 0 \pmod{G_0} \quad \text{for all } \boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(0)}. \tag{4.20}$$

Write $\hat{\boldsymbol{\lambda}}=(\lambda_{-1},\lambda_0,\boldsymbol{\lambda})=(\lambda_{-1},\lambda_0,\lambda_1,...,\lambda_r)$ and define, with D_{-1} and D_0 given by (3.6) and (3.7),

$$\hat{\boldsymbol{\Lambda}}^{(0)}=\{\hat{\boldsymbol{\lambda}}\in\mathbb{Z}^{r+2}:0\leqslant\lambda_i\leqslant D_i\ (i=-1,0) \text{ and } \boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(0)}\}. \tag{4.21}$$

We shall construct a rational function $P=P(Y_0,...,Y_r)$ of the form

$$P=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}}\varrho(\hat{\boldsymbol{\lambda}})(\Delta(Y_0+\lambda_{-1};D_{-1}+1))^{\lambda_0+1}Y_1^{\mu_1'-(\mu_1^{(0)})'}...\,Y_r^{\mu_r'-(\mu_r^{(0)})'} \tag{4.22}$$

with coefficients $\varrho(\hat{\boldsymbol{\lambda}})$ in $\mathcal{O}_K$, where $(\mu_1^{(0)},...,\mu_r^{(0)})=\boldsymbol{\lambda}^{(0)}\mathcal{B}$ with $\boldsymbol{\lambda}^{(0)}\in\boldsymbol{\Lambda}^{(0)}$ in (4.20), $(\mu_1,...,\mu_r)=\boldsymbol{\lambda}\mathcal{B}$ for each $\boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(0)}$, and $\mu_i'=q^\nu\mu_i$ and $(\mu_i^{(0)})'=q^\nu\mu_i^{(0)}$ $(1\leqslant i\leqslant r)$ (see (4.17)).

Denote by $\partial_1^*,...,\partial_{n-1}^*$ the differential operators specified in (2.12) (see also (2.14)) and put $\partial_0^*=\partial/\partial Y_0$. Then we have

$$\partial_j^*Y_1^{\mu_1'-(\mu_1^{(0)})'}...\,Y_r^{\mu_r'-(\mu_r^{(0)})'}=\gamma_jY_1^{\mu_1'-(\mu_1^{(0)})'}...\,Y_r^{\mu_r'-(\mu_r^{(0)})'} \quad (1\leqslant j<n),$$

where

$$\gamma_j=q^\nu\sum_{i=1}^r\left(b_n\frac{\partial L_i}{\partial z_j}-b_j\frac{\partial L_i}{\partial z_n}\right)(\mu_i-\mu_i^{(0)}) \quad (1\leqslant j<n), \tag{4.23}$$

and γ_j $(1\leqslant j<n)$ are rational integers by (5.4)♣.

For $\boldsymbol{t}=(t_0,...,t_{r-1})\in\mathbb{N}^r$, write $|\boldsymbol{t}|=t_0+...+t_{r-1}$ and put

$$\Pi(\boldsymbol{t})=\Pi(\gamma_1,...,\gamma_{r-1};t_1,...,t_{r-1})=\Delta(\gamma_1;t_1)\,...\,\Delta(\gamma_{r-1};t_{r-1}),$$
$$\Theta(Y_0;\boldsymbol{t})=v(D_{-1}+1)^{t_0}\Theta(Y_0+\lambda_{-1};D_{-1}+1,\lambda_0+1,t_0),$$

where

$$v(k)=\operatorname{lcm}(1,2,...,k) \quad \text{for } k\in\mathbb{Z}_{>0}.$$

We record (see Rosser and Schoenfeld [21, p. 71, (3.35)])

$$\log v(k)<1.03883k<\tfrac{107}{103}k. \tag{4.24}$$

We introduce further rational functions $Q(\boldsymbol{t})=Q(Y_0,...,Y_r;\boldsymbol{t})$ by

$$Q(\boldsymbol{t})=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}}\varrho(\hat{\boldsymbol{\lambda}})\Pi(\boldsymbol{t})\Theta(Y_0;\boldsymbol{t})Y_1^{\mu_1'-(\mu_1^{(0)})'}...\,Y_r^{\mu_r'-(\mu_r^{(0)})'}. \tag{4.25}$$

As indicated in §1.1, we use the notation of heights introduced in [6, §2]. Now we apply Siegel's lemma—here we use [6, Lemma 1], which is a consequence of Bombieri and Vaaler [7, Theorem 9], to prove the following lemma, where

$$\boldsymbol{\varrho}=(\varrho(\hat{\boldsymbol{\lambda}}):\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)})\in\mathbb{P}^N \quad \text{with } N=|\hat{\boldsymbol{\Lambda}}^{(0)}|,$$

c_{02} is given by (3.18) and $\hat{c}_{03}$ by (3.21). Recall S and T given by (3.1) and (3.5).

Lemma 4.2. *There exist $\boldsymbol{\varrho}(\hat{\boldsymbol{\lambda}})\in\mathcal{O}_K$, $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}$, not all zero, with*

$$\begin{aligned} h_0(\boldsymbol{\varrho})\leqslant \frac{SD}{d}\Bigg(g_{12}+\frac{1}{c_{02}-1}\Bigg(\frac{1}{2}g_8+\frac{1}{2}\Bigg(1+\frac{1}{2g_2+1}\Bigg)\frac{1}{c_1c_2} \\ +g_{10}\frac{1}{c_1c_3}+\Bigg(1+\frac{1}{g_5}\Bigg)\frac{1}{c_1c_4}\Bigg)+\frac{\hat{c}_{03}}{e_{\mathfrak{p}}\theta}\frac{1}{c_1c_3}\Bigg), \end{aligned} \tag{4.26}$$

such that

$$Q(s,((\alpha_1')^{p^{\varkappa}}\zeta^{a_1'})^{s/q^{\nu}},...,((\alpha_r')^{p^{\varkappa}}\zeta^{a_r'})^{s/q^{\nu}};\boldsymbol{t})=0 \tag{4.27}$$

for all $s\in\mathbb{Z}$ with $|s|\leqslant S$ and $\boldsymbol{t}\in\mathbb{N}^r$ with $|\boldsymbol{t}|\leqslant T$.

In the sequel, s always denotes a rational integer and $\boldsymbol{t}$ is always in $\mathbb{N}^r$. The expressions "$s\in\mathbb{Z}$" and "$\boldsymbol{t}\in\mathbb{N}^r$" will be omitted.

Proof. If $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}$ then, by (4.20), there exists $w_1(\hat{\boldsymbol{\lambda}})\in\mathbb{Z}$ such that

$$d_1(\lambda_1-\lambda_1^{(0)})+...+d_r(\lambda_r-\lambda_r^{(0)})=w_1(\hat{\boldsymbol{\lambda}})G_0.$$

Thus for each $\hat{\boldsymbol{\lambda}}=(\lambda_{-1},\lambda_0,\boldsymbol{\lambda})\in\hat{\boldsymbol{\Lambda}}^{(0)}$, $\boldsymbol{\mu}=\boldsymbol{\lambda}\mathcal{B}$, we have, by Lemma 4.1, (4.2), $\alpha_0'=\theta_0=\alpha_0$ (see §5♣) and (4.16),

$$\begin{aligned} \prod_{i=1}^r(((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{s/q^{\nu}})^{\mu_i'-(\mu_i^{(0)})'} &= \prod_{i=1}^r((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{(\mu_i-\mu_i^{(0)})s} \\ &= \prod_{i=1}^r(\theta_i^{p^{\varkappa}}\zeta^{d_i})^{(\lambda_i-\lambda_i^{(0)})s} \\ &= \theta_0^{w_1(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^r\theta_i^{(\lambda_i-\lambda_i^{(0)})p^{\varkappa}s} \\ &= (\alpha_0')^{w(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^r(\alpha_i')^{(\mu_i-\mu_i^{(0)})p^{\varkappa}s}\in\mathbb{Q}(\theta_0,\theta_1,...,\theta_r), \end{aligned} \tag{4.28}$$

where $w(\hat{\boldsymbol{\lambda}})=w_1(\hat{\boldsymbol{\lambda}})+(\mu_0-\mu_0^{(0)})p^{\varkappa}\in q^{-\nu}\mathbb{Z}$ with μ_0 and $\mu_0^{(0)}$ determined by $\boldsymbol{\lambda}$ and $\boldsymbol{\lambda}^{(0)}$ through (4.13). Thus it suffices to construct $\varrho(\hat{\boldsymbol{\lambda}})\in\mathcal{O}_K$, $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}$, not all zero, such that

$$\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}}\varrho(\hat{\boldsymbol{\lambda}})\Pi(\boldsymbol{t})\Theta(s;\boldsymbol{t})(\alpha_0')^{w(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^r(\alpha_i')^{(\mu_i-\mu_i^{(0)})p^{\varkappa}s}=0 \tag{4.29}$$

for all $|s|\leqslant S$ and $|\boldsymbol{t}|\leqslant T$.

Here (4.29) is a system of

$$M\leqslant(2S+1)\binom{[T]+r}{r}$$

homogeneous linear equations in $N=|\hat{\boldsymbol{\Lambda}}^{(0)}|$ unknowns $\varrho(\hat{\boldsymbol{\lambda}})$, $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}$, with coefficients in $E=\mathbb{Q}(\theta_0,\theta_1,\dots,\theta_r)\subseteq K$. Note that (4.19) and (3.27) imply that

$$N>\frac{(D_{-1}+1)(D_0+1)q^{\nu}D_1\dots D_r}{G_0/\delta(\mathfrak{a}')}\geqslant c_{01}M. \tag{4.30}$$

By applying [6, Lemma 1] and following the lines of argumentation in the proof of Lemma 7.2♣, we can determine $\varrho(\hat{\boldsymbol{\lambda}})\in\mathcal{O}_E$, $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)}$, not all zero, and Lemma 4.2 follows. We omit the details here. □

5. The first main inductive argument

In order to state and prove the first and second main inductive argument in the sequel, we have to introduce further notation. Let $I\in\mathbb{N}$. Suppose that $\boldsymbol{x}^{(I)}\in\mathbb{R}^r$, $\varepsilon^{(I)}\in\mathbb{Z}$ and $\boldsymbol{\Lambda}^{(I)}(\subseteq\mathbb{Z}^r)$ satisfy the following properties:

$$\begin{aligned}&\text{(i) } \mathbf{M}^{(I)}:=\boldsymbol{\Lambda}^{(I)}\mathcal{B}\subseteq\mathbf{M}\cap(q^{-I}\mathbf{C}-\boldsymbol{x}^{(I)});\\ &\text{(ii) } 1\leqslant|\mathbf{M}^{(I)}|=|\boldsymbol{\Lambda}^{(I)}|\leqslant q^{\nu}D_1\dots D_r+1;\\ &\text{(iii) } d_1\lambda_1+\dots+d_r\lambda_r\equiv\varepsilon^{(I)}\ (\mathrm{mod}\ G_0)\text{ for all }\boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(I)}.\end{aligned} \tag{5.1}$$

Fix a point $\boldsymbol{\lambda}^{(I)}=(\lambda_1^{(I)},\dots,\lambda_r^{(I)})\in\boldsymbol{\Lambda}^{(I)}$. Then

$$d_1(\lambda_1-\lambda_1^{(I)})+\dots+d_r(\lambda_r-\lambda_r^{(I)})\equiv 0\ (\mathrm{mod}\ G_0)\quad\text{for all }\boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(I)}. \tag{5.2}$$

Define

$$\hat{\boldsymbol{\Lambda}}^{(I)}=\{\hat{\boldsymbol{\lambda}}=(\lambda_{-1},\lambda_0,\boldsymbol{\lambda})\in\mathbb{Z}^{r+2}:0\leqslant\lambda_i\leqslant D_i\ (i=-1,0)\text{ and }\boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(I)}\}. \tag{5.3}$$

We shall construct $\boldsymbol{\Lambda}^{(I)}$, $\boldsymbol{x}^{(I)}$, $\boldsymbol{\varepsilon}^{(I)}$ and $\varrho^{(I)}(\hat{\boldsymbol{\lambda}})\in\mathcal{O}_K$, $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}$, in the first main inductive argument below.

We introduce $Q^{(I)}(\boldsymbol{t})=Q^{(I)}(Y_0,\dots,Y_r;\boldsymbol{t})$ by

$$Q^{(I)}(\boldsymbol{t})=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}}\varrho^{(I)}(\hat{\boldsymbol{\lambda}})\Pi^{(I)}(\boldsymbol{t})\Theta(q^{-I}Y_0;\boldsymbol{t})Y_1^{\mu_1'-\mu_1^{(I)\prime}}\dots Y_r^{\mu_r'-\mu_r^{(I)\prime}}, \tag{5.4}$$

where

$$\Pi^{(I)}(\boldsymbol{t})=\Pi(\gamma_1^{(I)},...,\gamma_{r-1}^{(I)};t_1,...,t_{r-1})=\Delta(\gamma_1^{(I)};t_1)...\Delta(\gamma_{r-1}^{(I)};t_{r-1}) \tag{5.5}$$

with

$$\gamma_j^{(I)}=q^\nu\sum_{i=1}^{r}\left(b_n\frac{\partial L_i}{\partial z_j}-b_j\frac{\partial L_i}{\partial z_n}\right)(\mu_i-\mu_i^{(I)}) \quad (1\leqslant j<n), \tag{5.6}$$

$(\mu_1,...,\mu_r)=\boldsymbol{\lambda}\mathcal{B}$ for each $\boldsymbol{\lambda}\in\boldsymbol{\Lambda}^{(I)}$, $(\mu_1^{(I)},...,\mu_r^{(I)})=\boldsymbol{\lambda}^{(I)}\mathcal{B}$ with $\boldsymbol{\lambda}^{(I)}\in\boldsymbol{\Lambda}^{(I)}$ in (5.2), $\mu_i'=q^\nu\mu_i$ and $(\mu_i^{(I)})'=q^\nu\mu_i^{(I)}$ $(1\leqslant i\leqslant r)$.

We now define the linear forms

$$M_i=L_i-\frac{1}{b_n}\frac{\partial L_i}{\partial z_n}L \quad (1\leqslant i\leqslant r), \tag{5.7}$$

where L_i $(1\leqslant i\leqslant r)$ are the linear forms in the basic hypothesis (see §2) and

$$L=b_1z_1+...+b_nz_n.$$

Then

$$b_nM_i=b_n\left(\frac{\partial L_i}{\partial z_0}\right)z_0+\sum_{j=1}^{n-1}\left(b_n\frac{\partial L_i}{\partial z_j}-b_j\frac{\partial L_i}{\partial z_n}\right)z_j \quad (1\leqslant i\leqslant r).$$

For $z_0,z_1,...,z_n$ in $\mathbb{C}_p$ with $\operatorname{ord}_p z_0\geqslant 0$ and $\operatorname{ord}_p z_j>1/(p-1)$ $(1\leqslant j\leqslant n)$, we define the p-adic functions (here $e^{L_i}=\exp(L_i)$ and $e^{M_i}=\exp(M_i)$),

$$\varphi^{(I)}(z_0,...,z_n;\boldsymbol{t})=Q^{(I)}(z_0,e^{L_1(0,z_1,...,z_n)},...,e^{L_r(0,z_1,...,z_n)};\boldsymbol{t}), \tag{5.8}$$

$$f^{(I)}(z_0,...,z_{n-1};\boldsymbol{t})=Q^{(I)}(z_0,e^{M_1(0,z_1,...,z_{n-1})},...,e^{M_r(0,z_1,...,z_{n-1})};\boldsymbol{t}). \tag{5.9}$$

We put, for $z\in\mathbb{C}_p$ with $\operatorname{ord}_p z\geqslant 0$,

$$\varphi^{(I)}(z;\boldsymbol{t})=\varphi^{(I)}(z,zq^{-\nu}\log\alpha_1^{p^\varkappa}\zeta^{a_1},...,zq^{-\nu}\log\alpha_n^{p^\varkappa}\zeta^{a_n};\boldsymbol{t}), \tag{5.10}$$

$$f^{(I)}(z;\boldsymbol{t})=f^{(I)}(z,zq^{-\nu}\log\alpha_1^{p^\varkappa}\zeta^{a_1},...,zq^{-\nu}\log\alpha_{n-1}^{p^\varkappa}\zeta^{a_{n-1}};\boldsymbol{t}). \tag{5.11}$$

By (4.10), we have, for $z\in\mathbb{C}_p$ with $\operatorname{ord}_p z\geqslant 0$,

$$\varphi^{(I)}(z;\boldsymbol{t})=Q^{(I)}(z,((\alpha_1')^{p^\varkappa}\zeta^{a_1'})^{z/q^\nu},...,((\alpha_r')^{p^\varkappa}\zeta^{a_r'})^{z/q^\nu};\boldsymbol{t}). \tag{5.12}$$

Recall η given by (3.13), S by (3.1), T by (3.5). Define $S^{(I)}$, $T^{(I)}$, I^*, I_1 and I_0 by

$$S^{(I)}=\eta^{-(r+1)I}, \quad T^{(I)}=\eta^{(r+1)I}T, \tag{5.13}$$

$$I^*=\frac{3(\max\{g_1,e_\mathfrak{p},f_\mathfrak{p}\log p\}+\nu\log q)}{\log(q\eta^{r+1})}+1, \tag{5.14}$$

$$T^{(I_1+1)}\frac{c_5}{r+1}<1\leqslant T^{(I_1)}\frac{c_5}{r+1}, \tag{5.15}$$

$$I_0=\min\{I^*,I_1\}. \tag{5.16}$$

Note that (5.15) means that I_1 is the farthest depth of descent one can reach by the classical small inductive steps (see the proofs of Lemmas 5.2–5.4 below), using [37, Lemmas 2.1 and 2.2] with $M\geqslant 1$. I^* in (5.14) indicates the depth of descent determined by the multiplicity estimates in §3♣. In the next two formulas we set

$$a=\begin{cases}1, & \text{if } p>2,\\ \frac{4}{9}, & \text{if } p=2.\end{cases}$$

Observe that (3.22) (9) and (5.14) imply that

$$\frac{1}{(q\eta^{r+1})^I}+a\left(1+\frac{1}{g_5}\right)\frac{c_2}{c_4}\frac{\log q}{q}\frac{I}{\max\{g_1,e_{\mathfrak p},f_{\mathfrak p}\log p\}+\nu\log q}\leqslant 1 \tag{5.17}$$

for $0\leqslant I\leqslant I^*-1$. Note that $I_1\geqslant i_1$ (see (3.16)) and $i_1\geqslant 10$ when $r\geqslant 8$, where the latter can be verified by running PARI/GP. Now, by (3.22) (9), (3.22) (10) and (5.14), $I_1\geqslant i_1$ imply that if $I^*>I_1$ then

$$\frac{1}{(q\eta^{r+1})^I}+a\left(1+\frac{1}{g_5}\right)\frac{c_2}{c_4}\frac{\log q}{q}\frac{I}{\max\{g_1,e_{\mathfrak p},f_{\mathfrak p}\log p\}+\nu\log q}\leqslant\begin{cases}\frac{7}{8}, & \text{if } p>2,\\ \frac{13}{16}, & \text{if } p=2,\end{cases} \tag{5.18}$$

for $I_1\leqslant I\leqslant I^*-1$.

The first main inductive argument. Suppose that Proposition 3.1 is false, i.e.,

$$\operatorname{ord}_p(\Xi-1)\geqslant U \tag{5.19}$$

for some $\alpha_1,...,\alpha_n$ and $b_1,...,b_n$ in the main theorem. Then for every $I\in\mathbb{Z}$ with $0\leqslant I\leqslant I_0$ there exist $\mathbf{\Lambda}^{(I)}\subseteq\mathbb{Z}^r$, $\boldsymbol{x}^{(I)}\in\mathbb{R}^r$, $\varepsilon^{(I)}\in\mathbb{Z}$ satisfying (5.1) and $\varrho^{(I)}(\hat{\boldsymbol\lambda})\in\mathcal{O}_K$, $\hat{\boldsymbol\lambda}\in\hat{\mathbf{\Lambda}}^{(I)}$, not all zero, satisfying (4.26) with $\boldsymbol\varrho$ replaced by $\boldsymbol\varrho^{(I)}$, such that

$$\varphi^{(I)}(s;\boldsymbol t)=0\quad\text{for all } |s|\leqslant qS^{(I)} \text{ and } |\boldsymbol t|\leqslant\eta T^{(I)}. \tag{5.20}$$

In the remainder of this section, and in §6 and §7, we always keep (5.19).

LEMMA 5.1. *Suppose that $\varrho^{(I)}(\hat{\boldsymbol\lambda})\in\mathcal{O}_K$, $\hat{\boldsymbol\lambda}\in\hat{\mathbf{\Lambda}}^{(I)}$, are not all zero, and set*

$$\Delta^{(I)}=\min_{\hat{\boldsymbol\lambda}\in\hat{\mathbf{\Lambda}}^{(I)}}\operatorname{ord}_p\varrho^{(I)}(\hat{\boldsymbol\lambda}). \tag{5.21}$$

Then for all $y\in\mathbb{Q}\cap\mathbb{Z}_p$ and $|\boldsymbol t|\leqslant T$ we have

$$\operatorname{ord}_p(f^{(I)}(y;\boldsymbol t)-\varphi^{(I)}(y;\boldsymbol t))\geqslant U-\operatorname{ord}_p b_n+\Delta^{(I)}.$$

Proof. This is similar to the proof of [37, Lemma 11.1]. We omit the details here. □

We now define $\varrho^{(0)}(\hat{\boldsymbol{\lambda}})$ to be $\varrho(\hat{\boldsymbol{\lambda}})$ $(\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(0)})$ in Lemma 4.2, $\gamma_j^{(0)}$ to be γ_j $(1\leqslant j<n)$ in (4.23) and $\Pi^{(0)}(\boldsymbol{t})$ to be $\Pi(\boldsymbol{t})$ in Lemma 4.2. Thus Lemma 4.2 gives

$$\varphi^{(0)}(s;\boldsymbol{t})=0 \quad \text{for all } |s|\leqslant S^{(0)} \text{ and } |\boldsymbol{t}|\leqslant T^{(0)}. \tag{5.22}$$

LEMMA 5.2. *Suppose $I=0$ or I is in $\mathbb{Z}$ with $1\leqslant I\leqslant I_0-1$, for which the first main inductive argument holds. Then for $J=1,...,r$ we have*

$$\varphi^{(I)}(s;\boldsymbol{t})=0 \quad \textit{for all } |s|\leqslant q^J S^{(I)} \textit{ and } |\boldsymbol{t}|\leqslant \eta^J T^{(I)}. \tag{5.23}$$

Proof. By (5.6), (5.7), (5.9) and (5.11),

$$f^{(I)}(z;\boldsymbol{t})=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}}\varrho^{(I)}(\hat{\boldsymbol{\lambda}})\Pi^{(I)}(\boldsymbol{t})\Theta(q^{-I}z;\boldsymbol{t})\prod_{j=1}^{n-1}(\alpha_j^{p^{\varkappa}}\zeta^{a_j})^{z\gamma_j^{(I)}/b_n q^{\nu}}. \tag{5.24}$$

We remark that (8.26)♣ with $f_b^{(I)}$ replaced by $f^{(I)}$ holds.

Note that (5.23) holds for $J=0$ when $I=0$ by (5.22), and for $J=1$ when $I\geqslant 1$ by (5.20). Assume that (5.23) holds for $J=k$ with $0\leqslant k\leqslant r$ when $I=0$, and with $1\leqslant k\leqslant r$ when $I\geqslant 1$. We shall prove (5.23) for $J=k+1$ with $k<r$ and include the case $k=r$ for later use.

Similarly to [37, §11], we see that, by (5.21) and (5.24),

$$F^{(I)}(z;\boldsymbol{t}):=p^{(D_{-1}+1)(D_0+1)(\theta+1/(p-1))-\Delta^{(I)}}f^{(I)}(p^{-\theta}z;\boldsymbol{t}) \quad (|\boldsymbol{t}|\leqslant\eta^{k+1}T^{(I)}) \tag{5.25}$$

are p-adic normal functions. Obviously

$$\frac{1}{m!}\left(\frac{d}{dz}\right)^m F^{(I)}(sp^{\theta};\boldsymbol{t})=p^{(D_{-1}+1)(D_0+1)(\theta+1/(p-1))-\Delta^{(I)}-m\theta}\frac{1}{m!}\left(\frac{d}{dz}\right)^m f^{(I)}(s;\boldsymbol{t}). \tag{5.26}$$

We now apply [37, Lemma 2.1] to each function in (5.25), taking

$$R=[q^k S^{(I)}] \quad \text{and} \quad M=\left[\eta^k T^{(I)}\frac{c_5}{r+1}\right]. \tag{5.27}$$

(Note that $M\geqslant 1$, since $I\leqslant I_0-1\leqslant I_1-1$ and $k\leqslant r$). By (5.26), (8.26)♣ with $f_b^{(I)}$ replaced by $f^{(I)}$, and (5.23) with $J=k$ and Lemma 5.1, we see that [37, (2.3)] holds for each $F^{(I)}(z;\boldsymbol{t})$ in (5.25) whenever

$$\begin{aligned}U+(D_{-1}+1)(D_0+1)\left(\theta+\frac{1}{p-1}\right)&\\ \geqslant (M+1)(2R+1)\theta+\frac{(M+1)\max\{h+\nu\log q,\log(2R+1)\}}{\log p}&.\end{aligned} \tag{5.28}$$

We now verify (5.28). By (5.15), we see that (8.31)$^\clubsuit$ holds. Further (3.23) and (5.27) give (8.32)$^\clubsuit$. Thus we have, on noting (3.5) and (3.9),

$$\frac{\eta^k}{q^r}\left(2q^k-\frac{1}{g_2}\right)\frac{c_5}{c_1}U<(M+1)(2R+1)\theta\leqslant\frac{\eta^k+\eta^{r+1}}{q^r}\left(2q^k+\frac{1}{g_2}\right)\frac{c_5}{c_1}U. \tag{5.29}$$

Now (3.1), (3.22) (26) and (5.27) yield

$$\log(2R+1)\leqslant\log 3q^r S^{(I)}\leqslant\eta^{-(r+1)I}(h+\nu\log q) \tag{5.30}$$

for all $I\geqslant 0$ (here we extend the definition of R in (5.27) for all $I\geqslant 0$). Now, by (8.31)$^\clubsuit$, (3.1), (3.5), (3.9) and (5.30) we obtain

$$\frac{(M+1)\max\{h+\nu\log q,\log(2R+1)\}}{\log p}\leqslant\frac{1}{c_3e_{\mathfrak{p}}\theta}\frac{\eta^k+\eta^{r+1}}{(r+1)q^{r+1}}\frac{c_5}{c_1}U. \tag{5.31}$$

Denote by $A(k)$ the sum of the extreme right-hand sides of (5.29) and (5.31), multiplied by q^rc_1/c_5U, and consider k as a continuous variable on the interval $0\leqslant k\leqslant r$. Then

$$\frac{1}{(q\eta)^k}\frac{dA(k)}{dk}>2\log q\eta+(\log\eta)\left(\frac{1}{g_2}+\frac{1}{qc_3e_{\mathfrak{p}}\check{\theta}(r+1)}\right)\geqslant 2\log q\eta^2>0,$$

where the second inequality follows from (3.22) (6). Thus (5.28) follows from the inequality $U\geqslant A(r)c_5U/c_1q^r$, which is implied by

$$c_1\geqslant c_5(\eta^r+\eta^{r+1})\left(2+\frac{1}{q^rg_2}+\frac{1}{c_3e_{\mathfrak{p}}\check{\theta}q^{r+1}(r+1)}\right).$$

The above inequality is a consequence of (3.22) (5) and (3.22) (7). This proves (5.28). Thus we can apply [37, Lemma 2.1] to each of the functions in (5.25), and by (5.28), (5.29) and Lemma 5.1 we obtain

$$\operatorname{ord}_p\varphi^{(I)}\left(\frac{s}{q};\boldsymbol{t}\right)+(D_{-1}+1)(D_0+1)\left(\theta+\frac{1}{p-1}\right)-\Delta^{(I)}>2c_5\eta^k\left(q^k-\frac{1}{2g_2}\right)\frac{U}{c_1q^r} \tag{5.32}$$

for all $s\in\mathbb{Z}$ and $|\boldsymbol{t}|\leqslant\eta^{k+1}T^{(I)}$.

We now assume $k<r$ and prove (5.23) for $J=k+1$. Suppose that it were false, i.e., there exist s and $\boldsymbol{t}$ such that

$$\varphi^{(I)}(s;\boldsymbol{t})\neq 0,\quad\text{with } |s|\leqslant q^{k+1}S^{(I)} \text{ and } |\boldsymbol{t}|\leqslant\eta^{k+1}T^{(I)}. \tag{5.33}$$

We proceed to get a contradiction. In the remainder of the proof, we fix these s and $\boldsymbol{t}$.

In virtue of (5.2) and similarly to the proof of formula (4.28), we see that for each $\hat{\boldsymbol{\lambda}}=(\lambda_{-1},\lambda_0,\boldsymbol{\lambda})\in\hat{\boldsymbol{\Lambda}}^{(I)}$, $\boldsymbol{\mu}=\boldsymbol{\lambda}\mathcal{B}$, there exists a rational integer $w_1^{(I)}(\hat{\boldsymbol{\lambda}})$, such that

$$d_1(\lambda_1-\lambda_1^{(I)})+\ldots+d_r(\lambda_r-\lambda_r^{(I)})=w_1^{(I)}(\hat{\boldsymbol{\lambda}})G_0$$

and

$$\begin{aligned}\prod_{i=1}^r(((\alpha_i')^{p^\varkappa}\zeta^{a_i'})^{s/q^\nu})^{\mu_i'-(\mu_i^{(I)})'}&=\prod_{i=1}^r((\alpha_i')^{p^\varkappa}\zeta^{a_i'})^{(\mu_i-\mu_i^{(I)})s}\\&=\prod_{i=1}^r(\theta_i^{p^\varkappa}\zeta^{d_i})^{(\lambda_i-\lambda_i^{(I)})s}\\&=\theta_0^{w_1^{(I)}(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^r\theta_i^{(\lambda_i-\lambda_i^{(I)})p^\varkappa s}\\&=(\alpha_0')^{w^{(I)}(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^r(\alpha_i')^{(\mu_i-\mu_i^{(I)})p^\varkappa s}\in\mathbb{Q}(\theta_0,\theta_1,\ldots,\theta_r),\end{aligned}\tag{5.34}$$

where $w^{(I)}(\hat{\boldsymbol{\lambda}})=w_1^{(I)}(\hat{\boldsymbol{\lambda}})+(\mu_0-\mu_0^{(I)})p^\varkappa\in q^{-\nu}\mathbb{Z}$ with μ_0 and $\mu_0^{(I)}$ determined by $\boldsymbol{\lambda}$ and $\boldsymbol{\lambda}^{(I)}$ through (4.13). Let

$$\delta_I=\begin{cases}0, & \text{if } I=0,\\ 1, & \text{if } I\geqslant 1.\end{cases}$$

Then, by [27, Lemma T1] if $I=0$ and [36, Lemma 1.3] if $I\geqslant 1$, we see that

$$q^{\delta_I(D_0+1)[(D_{-1}+1)I+\operatorname{ord}_q((D_{-1}+1)!)]}\Theta(q^{-I}s;\boldsymbol{t})\Pi^{(I)}(\boldsymbol{t})\in\mathbb{Z}.\tag{5.35}$$

By (5.34), we have $\operatorname{ord}_p\varphi^{(I)}(s;\boldsymbol{t})=\operatorname{ord}_p\varphi'$, where

$$\begin{aligned}\varphi'=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}}&\varrho^{(I)}(\hat{\boldsymbol{\lambda}})q^{\delta_I(D_0+1)[(D_{-1}+1)I+\operatorname{ord}_q((D_{-1}+1)!)]}\\&\times\Theta(q^{-I}s;\boldsymbol{t})\Pi^{(I)}(\boldsymbol{t})(\alpha_0')^{w^{(I)}(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^r(\alpha_i')^{(\mu_i-\mu_i^{(I)})p^\varkappa s}\end{aligned}\tag{5.36}$$

is in $\mathbb{Q}(\theta_0,\theta_1,\ldots,\theta_r)\subseteq K$ and is non-zero. Now let $|\cdot|_v$ be an absolute value on K normalized as in [6, §2], and let $|\cdot|_{v_0}$ be the one corresponding to $\mathfrak{p}$, whence

$$\operatorname{ord}_p\varphi'=\frac{1}{e_\mathfrak{p}f_\mathfrak{p}\log p}(-\log|\varphi'|_{v_0})=\frac{1}{e_\mathfrak{p}f_\mathfrak{p}\log p}\sum_{v\neq v_0}\log|\varphi'|_v,\tag{5.37}$$

by the product formula on K. We note that (8.42)$^\clubsuit$ with $\hat{\boldsymbol{\Lambda}}_b^{(I)}$ replaced by $\hat{\boldsymbol{\Lambda}}^{(I)}$, (8.43)$^\clubsuit$ with $\hat{\boldsymbol{\Lambda}}_b^{(I)}$ replaced by $\hat{\boldsymbol{\Lambda}}^{(I)}$ and $\Delta_b^{(I)}$ replaced by $\Delta^{(I)}$, (8.44)$^\clubsuit$ and (8.46)$^\clubsuit$ are valid in the current setting. By (1.13), (2.8), (3.33), (5.1), (5.5), (5.6) and the definition of g_{91} in (3.16), we see that (7.32)♣ with $\Pi(\boldsymbol{t})$ replaced by $\Pi^{(I)}(\boldsymbol{t})$ (i.e, γ_j replaced by $\gamma_j^{(I)}, 1\leqslant j<r$) is valid for $T'\geqslant 1$ and it holds trivially for $T'=0$. Using [35, Lemma 1.6], the fact that $q\eta^{r+1}>1$ and (3.22) (18), we obtain

$$\log|\Theta^{(I)}(q^{-I}s;\boldsymbol{t})|\leqslant\frac{107}{103}t_0(D_{-1}+1)\\ +\left(1+\frac{1}{g_5}\right)\frac{1}{c_1c_4}\frac{SD}{d}\left(1+\frac{\log q}{\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q}k_p\right)$$

for $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}$, with s and $\boldsymbol{t}$ as in (5.33), where

$$k_p=\begin{cases}k, & \text{if } p>2,\\ \max\{k-\frac{1}{6},0\}, & \text{if } p=2.\end{cases}$$

Thus we have

$$\log|\Theta(q^{-I}s;\boldsymbol{t})\Pi^{(I)}(\boldsymbol{t})|\leqslant\frac{SD}{d}\left[\left(\frac{g_9\eta^{k+1}}{e_{\mathfrak{p}}\theta}+g_{10}\right)\frac{1}{c_1c_3}+\left(1+\frac{1}{g_5}\right)\frac{1}{c_1c_4}\right.\\ \left.\times\left(1+\frac{\log q}{\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q}k_p\right)\right] \tag{5.38}$$

for $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}$, with s and $\boldsymbol{t}$ as in (5.33). We assert that

$$\frac{1}{c_2}\frac{q^{k+1}}{(q\eta^{r+1})^I}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{\log q}{\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q}\left(\delta_I\left(I+\frac{1}{q-1}\right)+k_p\right)\\ \leqslant\frac{1}{c_2}q^{k+1}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{k\log q}{\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q}. \tag{5.39}$$

Clearly (5.39) holds for $I=0$. If $I\geqslant 1$, then $k\geqslant 1$. On noting that $I\leqslant I_0-1\leqslant I^*-1$, (5.39) follows from (5.17).

By the above discussion and (4.26) (with $\boldsymbol{\varrho}$ replaced by $\boldsymbol{\varrho}^{(I)}$), and noting (3.9), we see that (5.33) implies that

$$\frac{c_1q^{r+1}}{U}\left(\operatorname{ord}_p\varphi^{(I)}(s;\boldsymbol{t})+(D_{-1}+1)(D_0+1)\left(\theta+\frac{1}{p-1}\right)-\Delta^{(I)}\right)\\ \leqslant c_1\left[g_{12}+\left(1+\frac{1}{2(c_{02}-1)}\right)g_8\right]+\frac{1}{c_2}\left[q^{k+1}+\frac{1}{2(c_{02}-1)}\left(1+\frac{1}{2g_2+1}\right)\right]\\ +\frac{1}{c_3}\left[\frac{1}{e_{\mathfrak{p}}\theta}(g_9\eta^{k+1}+\hat{c}_{03})+\left(1+\frac{1}{c_{02}-1}\right)g_{10}\right]\\ +\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\left[1+\frac{1}{c_{02}-1}+\frac{k\log q}{g_1}+\left(\theta+\frac{1}{p-1}\right)\frac{e_{\mathfrak{p}}}{d}\right]. \tag{5.40}$$

Write $\mathfrak{R}(k)$ for the right-hand side of (5.40). Observe that (5.32) and (5.40) give

$$\mathfrak{L}(k) := 2c_5 q\eta^k \left(q^k - \frac{1}{2g_2}\right) - \mathfrak{R}(k) < 0. \tag{5.41}$$

Now (3.22) (j), $j=11, ..., 15$, imply that $\mathfrak{L}'(x)>0$ for $0 \leqslant x \leqslant r-1$. Thus (5.41) yields $\mathfrak{L}(0)<0$. Recalling f_1 in (3.22) and $\hat{\eta} \geqslant \eta$, we get $f_1 \leqslant \mathfrak{L}(0) < 0$, contradicting (3.22) (1). This proves that (5.33) is impossible, whence (5.23) holds for $J=k+1$. The proof of Lemma 5.2 is thus complete. □

Lemma 5.3. *For every I as in Lemma 5.2 we have*

$$\varphi^{(I)}\left(\frac{s}{q}; \boldsymbol{t}\right) = 0 \quad \textit{for all } |s| \leqslant q([S^{(I+1)}]+1) \textit{ and } |\boldsymbol{t}| \leqslant T^{(I+1)}. \tag{5.42}$$

Proof. The proof follows the pattern of that of Lemma 8.3♣ and utilizes §3.3, especially (3.22) (1) and (3.22) (2). We omit the details here. □

Lemma 5.4. *For every I as in Lemma 5.2 there exist $\boldsymbol{\Lambda}^{(I+1)} \subseteq \mathbb{Z}^r$, $\boldsymbol{x}^{(I+1)} \in \mathbb{R}^r$, $\varepsilon^{(I+1)} \in \mathbb{Z}$ satisfying (5.1) with I replaced by $I+1$ and $\varrho^{(I+1)}(\hat{\boldsymbol{\lambda}}) \in \mathcal{O}_K$, $\hat{\boldsymbol{\lambda}} \in \hat{\boldsymbol{\Lambda}}^{(I+1)}$, not all zero, satisfying (4.26) with $\boldsymbol{\varrho}$ replaced by $\boldsymbol{\varrho}^{(I+1)}$, such that*

$$\varphi^{(I+1)}(s; \boldsymbol{t}) = 0 \quad \textit{for all } |s| \leqslant q([S^{(I+1)}]+1) \textit{ and } |\boldsymbol{t}| \leqslant \eta T^{(I+1)}. \tag{5.43}$$

Proof. Write the elements of $\boldsymbol{\Lambda}^{(I)}$ as $\boldsymbol{\iota}=(\iota_1, ..., \iota_r)$ and recall the fixed $\boldsymbol{\lambda}^{(I)} \in \boldsymbol{\Lambda}^{(I)}$ in (5.2). For every $\boldsymbol{\lambda}^*=(\lambda_1^*, ..., \lambda_r^*) \in \mathbb{Z}^r$ with $0 \leqslant \lambda_i^* < q$ $(i=1, ..., r)$, let

$$\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*) = \{\boldsymbol{\iota} \in \boldsymbol{\Lambda}^{(I)} : \boldsymbol{\iota} - \boldsymbol{\lambda}^{(I)} \equiv \boldsymbol{\lambda}^* \pmod{q}\}, \tag{5.44}$$

where the congruence signifies the system of r congruences for the corresponding coordinates. Thus for $\boldsymbol{\iota} \in \boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)$, there exists a unique $\boldsymbol{\lambda} \in \mathbb{Z}^r$, such that

$$\boldsymbol{\iota} - \boldsymbol{\lambda}^{(I)} = q\boldsymbol{\lambda} + \boldsymbol{\lambda}^*. \tag{5.45}$$

Writing ι_{-1} and ι_0 for λ_{-1} and λ_0, set $\hat{\boldsymbol{\Lambda}}^{(I)}(\boldsymbol{\lambda}^*) = \{\hat{\boldsymbol{\iota}} = (\iota_{-1}, \iota_0, \boldsymbol{\iota}) \in \hat{\boldsymbol{\Lambda}}^{(I)} : \boldsymbol{\iota} \in \boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)\}$. We decompose $\varphi^{(I)}(s/q; \boldsymbol{t})$ (see (5.12)) into the sum of q^r sub-sums indexed by $\boldsymbol{\lambda}^*$

$$\begin{aligned}\varphi_{\boldsymbol{\lambda}^*}^{(I)}\left(\frac{s}{q}; \boldsymbol{t}\right) := \sum_{\hat{\boldsymbol{\iota}} \in \hat{\boldsymbol{\Lambda}}^{(I)}(\boldsymbol{\lambda}^*)} & \varrho^{(I)}(\hat{\boldsymbol{\iota}}) \Pi^{(I)}(\boldsymbol{t}) \Theta(q^{-(I+1)} s; \boldsymbol{t}) \\ & \times \prod_{i=1}^{r} (((\alpha_i')^{p^{\varkappa}} \zeta^{a_i'})^{1/q^{\nu}})^{(\tau_i' - (\mu_i^{(I)})') s/q},\end{aligned}$$

where $\boldsymbol{\tau}=(\tau_1,...,\tau_r)=\boldsymbol{\iota}\mathcal{B}$, and $\tau_i'=q^\nu\tau_i$ $(1\leqslant i\leqslant r)$. For $\boldsymbol{\iota}\in\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)$, we have, by (5.2) and (5.45),

$$q\sum_{i=1}^r d_i\lambda_i+\sum_{i=1}^r d_i\lambda_i^*=\sum_{i=1}^r d_i(\iota_i-\lambda_i^{(I)})=g(\boldsymbol{\lambda},\boldsymbol{\lambda}^*)G_0$$

for some $g(\boldsymbol{\lambda},\boldsymbol{\lambda}^*)\in\mathbb{Z}$. Thus, Lemma 4.1 and (4.12) give

$$\begin{aligned}\prod_{i=1}^r((\alpha_i')^{p^\varkappa}\zeta^{a_i'})^{(\tau_i-\mu_i^{(I)})s/q}&=\prod_{i=1}^r(\theta_i^{p^\varkappa}\zeta^{d_i})^{(\iota_i-\lambda_i^{(I)})s/q}\\&=\prod_{i=1}^r((\theta_i^{1/q})^{p^\varkappa}\xi^{d_i})^{(q\lambda_i+\lambda_i^*)s}\\&=\biggl(\prod_{i=1}^r(\theta_i^{1/q})^{p^\varkappa s\lambda_i^*}\biggr)\biggl(\prod_{i=1}^r\theta_i^{p^\varkappa s\lambda_i}\biggr)\xi^{G_0g(\boldsymbol{\lambda},\boldsymbol{\lambda}^*)s}.\end{aligned}\tag{5.46}$$

Now, (5.46), (4.4) and $\alpha_0=\theta_0$ yield

$$\varphi_{\boldsymbol{\lambda}^*}^{(I)}\Bigl(\frac{s}{q};\boldsymbol{t}\Bigr)\in\biggl(\prod_{i=1}^r(\theta_i^{1/q})^{p^\varkappa s\lambda_i^*}\biggr)K(\theta_0^{1/q}).\tag{5.47}$$

From (5.11)♣ and $[K(\theta_0^{1/q}):K]=q$ (by $\theta_0=\alpha_0$ and (1.4)), we get

$$[K(\theta_0^{1/q})(\theta_1^{1/q},...,\theta_r^{1/q}):K(\theta_0^{1/q})]=q^r.\tag{5.48}$$

By (5.42), (5.47) and (5.48), we obtain, for every $\boldsymbol{\lambda}^*=(\lambda_1^*,...,\lambda_r^*)\in\mathbb{Z}^r$ with $0\leqslant\lambda_i^*<q$ $(1\leqslant i\leqslant r)$,

$$\varphi_{\boldsymbol{\lambda}^*}^{(I)}\Bigl(\frac{s}{q};\boldsymbol{t}\Bigr)=0\quad\text{for all } |s|\leqslant q([S^{(I+1)}]+1) \text{ with } (s,q)=1 \text{ and } |\boldsymbol{t}|\leqslant T^{(I+1)}.\tag{5.49}$$

There exists a $\boldsymbol{\lambda}^*$ as above, such that $\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)\neq\varnothing$ and $\varrho^{(I)}(\hat{\boldsymbol{\iota}})$, $\hat{\boldsymbol{\iota}}\in\hat{\boldsymbol{\Lambda}}^{(I)}(\boldsymbol{\lambda}^*)$, are not all zero. We fix this $\boldsymbol{\lambda}^*$ in the remainder of the proof of the current lemma. Using the second line of (5.46) and

$$q\sum_{i=1}^r d_i\lambda_i+\sum_{i=1}^r d_i\lambda_i^*=g(\boldsymbol{\lambda},\boldsymbol{\lambda}^*)G_0,$$

we obtain from (5.49) that

$$\sum_{\hat{\boldsymbol{\iota}}\in\hat{\boldsymbol{\Lambda}}^{(I)}(\boldsymbol{\lambda}^*)}\varrho^{(I)}(\hat{\boldsymbol{\iota}})\Pi^{(I)}(\boldsymbol{t})\Theta(q^{-(I+1)}s;\boldsymbol{t})\prod_{i=1}^r(\theta_i^{p^\varkappa}\zeta^{d_i})^{\lambda_i s}=0\tag{5.50}$$

for all $|s|\leqslant q([S^{(I+1)}]+1)$, with $(s,q)=1$, and $|\boldsymbol{t}|\leqslant T^{(I+1)}$.

From (5.45) and (5.2) we see that for $\boldsymbol{\iota}\in\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)$,

$$q\sum_{i=1}^{r} d_i\lambda_i+\sum_{i=1}^{r} d_i\lambda_i^*\equiv\sum_{i=1}^{r} d_i(\iota_i-\lambda_i^{(I)})\equiv 0 \pmod{G_0}. \tag{5.51}$$

Now we consider two cases: (i) $(q,G_0)=1$ and (ii) $q|G_0$.

(i) $(q,G_0)=1$. (5.51) implies that there exists a unique $\varepsilon'\in\mathbb{Z}$ (mod G_0) satisfying

$$q\varepsilon'+\sum_{i=1}^{r} d_i\lambda_i^*\equiv 0 \pmod{G_0}. \tag{5.52}$$

(ii) $q|G_0$. (5.51) and $q|G_0$ imply that $q|\sum_{i=1}^{r} d_i\lambda_i^*$ and

$$\sum_{i=1}^{r} d_i\lambda_i\equiv -\frac{1}{q}\sum_{i=1}^{r} d_i\lambda_i^*+b\frac{G_0}{q} \pmod{G_0} \tag{5.53}$$

for some $b\in\mathbb{Z}$ with $1\leqslant b\leqslant q$. Now we have a partition

$$\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)=\bigcup_{b=1}^{q}\boldsymbol{\Lambda}_b^{(I)}(\boldsymbol{\lambda}^*),$$

where

$$\boldsymbol{\Lambda}_b^{(I)}(\boldsymbol{\lambda}^*)=\{\boldsymbol{\iota}\in\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*):\boldsymbol{\lambda}=(\lambda_1,...,\lambda_r) \text{ in (5.45) satisfies (5.53)}\}. \tag{5.54}$$

The left-hand side of (5.50) is decomposed into a sum of q sub-sums, denoted by $\boldsymbol{\Sigma}_b$, over

$$\hat{\boldsymbol{\Lambda}}_b^{(I)}(\boldsymbol{\lambda}^*)=\{\hat{\boldsymbol{\iota}}=(\iota_{-1},\iota_0,\boldsymbol{\iota})\in\mathbb{Z}^{r+2}:0\leqslant\iota_i\leqslant D_i\ (i=-1,0) \text{ and } \boldsymbol{\iota}\in\boldsymbol{\Lambda}_b^{(I)}(\boldsymbol{\lambda}^*)\}$$

$(b=1,...,q)$. For $\hat{\boldsymbol{\iota}}\in\hat{\boldsymbol{\Lambda}}_b^{(I)}(\boldsymbol{\lambda}^*)$, (4.2), (4.5) and (5.53) give

$$\begin{aligned}\zeta^{q^{-1}(\sum_{i=1}^{r} d_i\lambda_i^*)s}\prod_{i=1}^{r}(\theta_i^{p^{\varkappa}}\zeta^{d_i})^{\lambda_i s}&=\biggl(\prod_{i=1}^{r}\theta_i^{p^{\varkappa}\lambda_i s}\biggr)\zeta^{b(G_0/q)s}\zeta^{g_1(\boldsymbol{\lambda},\boldsymbol{\lambda}^*)G_0 s}\\&=\biggl(\prod_{i=1}^{r}\theta_i^{p^{\varkappa}\lambda_i s}\biggr)\alpha_0^{g_1(\boldsymbol{\lambda},\boldsymbol{\lambda}^*)s}(\alpha_0^{1/q})^{sb}\end{aligned}$$

for some $g_1(\boldsymbol{\lambda},\boldsymbol{\lambda}^*)\in\mathbb{Z}$. Thus

$$\zeta^{q^{-1}(\sum_{i=1}^{r} d_i\lambda_i^*)s}\boldsymbol{\Sigma}_b\in(\alpha_0^{s/q})^b K.$$

Now (1.4) and $(s,q)=1$ imply that $[K(\alpha_0^{s/q}):K]=q$. Thus (5.50) implies, for $b=1,...,q$, $\boldsymbol{\Sigma}_b=0$ for s and $\boldsymbol{t}$ in (5.50). There exists a $b\in\{1,...,q\}$ such that $\boldsymbol{\Lambda}_b^{(I)}(\boldsymbol{\lambda}^*)\neq\varnothing$ and $\varrho^{(I)}(\hat{\boldsymbol{\iota}})$, $\hat{\boldsymbol{\iota}}\in\hat{\boldsymbol{\Lambda}}_b^{(I)}(\boldsymbol{\lambda}^*)$, are not all zero. Fix this b in the remainder of the proof of the current lemma and let

$$\varepsilon''=-\frac{1}{q}\sum_{i=1}^{r}d_i\lambda_i^*+b\frac{G_0}{q}. \tag{5.55}$$

Now we write out "$\boldsymbol{\Sigma}_b=0$ for s and $\boldsymbol{t}$ in (5.50)" as

$$\sum_{\hat{\boldsymbol{\iota}}\in\hat{\boldsymbol{\Lambda}}_b^{(I)}(\boldsymbol{\lambda}^*)}\varrho^{(I)}(\hat{\boldsymbol{\iota}})\Pi^{(I)}(\boldsymbol{t})\Theta(q^{-(I+1)}s;\boldsymbol{t})\prod_{i=1}^{r}(\theta_i^{p^{\varkappa}}\zeta^{d_i})^{\lambda_i s}=0 \tag{5.56}$$

for all $|s|\leqslant q([S^{(I+1)}]+1)$, with $(s,q)=1$, and $|\boldsymbol{t}|\leqslant T^{(I+1)}$.

We take

$$\boldsymbol{\Lambda}^{(I+1)}=\{\boldsymbol{\lambda}=q^{-1}(\boldsymbol{\iota}-\boldsymbol{\lambda}^{(I)}-\boldsymbol{\lambda}^*):\boldsymbol{\iota}\in\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)\} \tag{5.57}$$

if $(q,G_0)=1$, whereas if $q|G_0$, $\boldsymbol{\Lambda}^{(I)}(\boldsymbol{\lambda}^*)$ in (5.57) is replaced by $\boldsymbol{\Lambda}_b^{(I)}(\boldsymbol{\lambda}^*)$. Let

$$\boldsymbol{x}^{(I+1)}=q^{-1}(\boldsymbol{x}^{(I)}+\boldsymbol{\mu}^{(I)}+\boldsymbol{\mu}^*),\quad\text{where } \boldsymbol{\mu}^*=\boldsymbol{\lambda}^*\boldsymbol{\mathcal{B}}, \tag{5.58}$$

$$\varepsilon^{(I+1)}=\begin{cases}\varepsilon' \text{ in (5.52)}, & \text{if } (q,G_0)=1,\\ \varepsilon'' \text{ in (5.55)}, & \text{if } q\,|\,G_0.\end{cases} \tag{5.59}$$

Set $\mathbf{M}^{(I+1)}=\boldsymbol{\Lambda}^{(I+1)}\boldsymbol{\mathcal{B}}$. It is readily verified that $\boldsymbol{\Lambda}^{(I+1)}$, $\boldsymbol{x}^{(I+1)}$ and $\varepsilon^{(I+1)}$ satisfy (5.1) with I replaced by $I+1$. For each $\hat{\boldsymbol{\lambda}}=(\lambda_{-1},\lambda_0,\boldsymbol{\lambda})\in\hat{\boldsymbol{\Lambda}}^{(I+1)}$, on noting that $\lambda_{-1}=\iota_{-1}$ and $\lambda_0=\iota_0$, we define

$$\varrho^{(I+1)}(\hat{\boldsymbol{\lambda}}):=\varrho^{(I)}(\hat{\boldsymbol{\iota}}),$$

where $\boldsymbol{\lambda}$ and $\boldsymbol{\iota}$ are connected by (5.57). Obviously $\boldsymbol{\varrho}^{(I+1)}:=(\varrho^{(I+1)}(\hat{\boldsymbol{\lambda}}):\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I+1)})$ satisfies (4.26) with $\boldsymbol{\varrho}$ replaced by $\boldsymbol{\varrho}^{(I+1)}$. We now fix $\boldsymbol{\lambda}^{(I+1)}\in\boldsymbol{\Lambda}^{(I+1)}$. For $\boldsymbol{\iota}$ in (5.57), we have, by (5.5),

$$\Pi^{(I)}(\boldsymbol{t})=\Delta(\gamma_1^{(I)};t_1)\dots\Delta(\gamma_{r-1}^{(I)};t_{r-1}),$$

where, by (5.6) and (5.45), with $\boldsymbol{\tau}=\boldsymbol{\iota}\mathcal{B}$, $\boldsymbol{\mu}=\boldsymbol{\lambda}\mathcal{B}$, $\boldsymbol{\mu}^*=\boldsymbol{\lambda}^*\mathcal{B}$ and $\boldsymbol{\mu}^{(I+1)}=\boldsymbol{\lambda}^{(I+1)}\mathcal{B}$,

$$\gamma_j^{(I)}=q^{\nu}\sum_{i=1}^{r}\left(b_n\frac{\partial L_i}{\partial z_j}-b_j\frac{\partial L_i}{\partial z_n}\right)(\tau_i-\mu_i^{(I)})=q\gamma_j^{(I+1)}+\gamma_j^*\quad(1\leqslant j<r), \tag{5.60}$$

in which $\gamma_j^{(I+1)}$ is given by (5.6) with I replaced by $I+1$, and γ_j^* is given by the right-hand side of (5.6) with $\mu_i-\mu_i^{(I)}$ replaced by $q\mu_i^{(I+1)}+\mu_i^*$. Note that $\gamma_j^*\in\mathbb{Z}$ $(1\leqslant j<r)$. By (5.60) and [34, Lemma 2.6], we see that, for $1\leqslant j<r$, $\Delta(\gamma_j^{(I)};t_j)$ is a linear combination of

$\Delta(\gamma_j^{(I+1)};k)$, $k{=}0,...,t_j$, with the coefficient of $\Delta(\gamma_j^{(I+1)};t_j)$ non-zero. So $\Delta(\gamma_j^{(I+1)};t_j)$ is a linear combination of $\Delta(\gamma_j^{(I)};k)$, $k{=}0,...,t_j$. Thus (5.50) (when $(q,G_0){=}1$) and (5.56) (when $q|G_0$) imply that

$$\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I+1)}} \varrho^{(I+1)}(\hat{\boldsymbol{\lambda}})\Pi^{(I+1)}(\boldsymbol{t})\Theta(q^{-(I+1)}s;\boldsymbol{t})\prod_{i=1}^{r}(\theta_i^{p^{\varkappa}}\zeta^{d_i})^{(\lambda_i-\lambda_i^{(I+1)})s}=0 \tag{5.61}$$

for all $|s|\leqslant q([S^{(I+1)}]+1)$, with $(s,q){=}1$, and $|\boldsymbol{t}|\leqslant T^{(I+1)}$.

Now (5.61) gives, by Lemma 4.1,

$$\varphi^{(I+1)}(s;\boldsymbol{t})=0 \quad \text{for all } |s|\leqslant q([S^{(I+1)}]+1), \text{ with } (s,q)=1, \text{ and } |\boldsymbol{t}|\leqslant T^{(I+1)}. \tag{5.62}$$

In order to prove Lemma 5.4, it remains to verify (5.43) for s with $q|s$. We now apply [37, Lemma 2.2] to each function in (5.25) with I replaced by $I{+}1$ and with $|\boldsymbol{t}|\leqslant\eta T^{(I+1)}$, taking

$$R=q([S^{(I+1)}]+1) \quad \text{and} \quad M=\left[T^{(I+1)}\frac{c_5}{r+1}\right]. \tag{5.63}$$

(Note that $I\leqslant I_0-1\leqslant I_1-1$, so $M\geqslant[T^{(I_1)}c_5/(r+1)]\geqslant 1$.) By (5.26) with I replaced by $I{+}1$, (8.26)♣ with $f_b^{(I)}$ replaced by $f^{(I+1)}$, (5.62) and Lemma 5.1, we see that [37, (2.6)] holds for each $F^{(I+1)}(z;\boldsymbol{t})$ with $|\boldsymbol{t}|\leqslant\eta T^{(I+1)}$ whenever

$$\begin{aligned} U+(D_{-1}+1)(D_0+1)\left(\theta+\frac{1}{p-1}\right) \\ \geqslant 2\left(1-\frac{1}{q}\right)R(M+1)\theta+\frac{(2M+2)\max\{h+\nu\log q,\log 2R\}}{\log p}. \end{aligned} \tag{5.64}$$

By (3.22) (20), we have

$$\left|\frac{s}{q}\right|\leqslant[S^{(I+1)}]+1\leqslant qS^{(I)}.$$

This inequality and (5.63) imply that

$$qS^{(I+1)}<R\leqslant q^2S^{(I)} \quad \text{and} \quad \frac{c_5}{r+1}T^{(I+1)}<M+1\leqslant 2M\leqslant\frac{2c_5}{r+1}T^{(I+1)}. \tag{5.65}$$

The second inequality of (5.30) implies that

$$\eta^{(r+1)I}\log 2R\leqslant h+\nu\log q. \tag{5.66}$$

Now, (5.65), (5.66), $c_3{>}0.47$ (see Table 3.1) and $e_{\mathfrak{p}}\check{\theta}\geqslant 0.49$ (see Table 3.2) yield

$$\begin{aligned} \frac{c_1}{U}\cdot\text{right-hand side of (5.64)} &\leqslant 4c_5\eta^{r+1}\left(\frac{q-1}{q^{r-1}}+\frac{1}{q^{r+1}(r+1)c_3e_{\mathfrak{p}}\check{\theta}}\right) \\ &\leqslant 2c_5\eta^{r+1}\left(2+\frac{1}{q^{r+1}(r+1)c_3e_{\mathfrak{p}}\check{\theta}}\right)\leqslant c_1, \end{aligned}$$

where the third inequality follows from (3.22) (5) and (3.22) (8). The above inequality implies (5.64). Thus we can apply [37, Lemma 2.2] to each $F^{(I+1)}(z;\boldsymbol{t})$ with $|\boldsymbol{t}|\leqslant\eta T^{(I+1)}$. By (5.64), (5.65) and Lemma 5.1, we obtain

$$\operatorname{ord}_p \varphi^{(I+1)}(s;\boldsymbol{t})+(D_{-1}+1)(D_0+1)\left(\theta+\frac{1}{p-1}\right)-\Delta^{(I+1)}>\frac{2c_5(q-1)U}{c_1q^r} \tag{5.67}$$

for all $|s|\leqslant q([S^{(I+1)}]+1)$, with $q|s$, and $|\boldsymbol{t}|\leqslant\eta T^{(I+1)}$.

Assume (5.43) were false, i.e., there exist s and $\boldsymbol{t}$ such that

$$\varphi^{(I+1)}(s;\boldsymbol{t})\neq 0 \quad \text{for all } |s|\leqslant q([S^{(I+1)}]+1), \text{ with } q\,|\,s, \text{ and } |\boldsymbol{t}|\leqslant\eta T^{(I+1)}. \tag{5.68}$$

We proceed to deduce a contradiction. In the sequel, we fix these s and $\boldsymbol{t}$. Now, since $q|s$, we have, by [27, Lemma T1] if $I=0$ and by [36, Lemma 1.3] if $I\geqslant 1$,

$$q^{\delta_I(D_0+1)((D_{-1}+1)I+\operatorname{ord}_q((D_{-1}+1)!))}\Theta(q^{-(I+1)}s;\boldsymbol{t})\Pi^{(I+1)}(\boldsymbol{t})\in\mathbb{Z}. \tag{5.69}$$

Similarly to the proof of Lemma 5.2, we have $\operatorname{ord}_p\varphi^{(I+1)}(s;\boldsymbol{t})=\operatorname{ord}_p\varphi'''$, where

$$\begin{aligned}\varphi'''=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I+1)}}&\varrho^{(I+1)}(\hat{\boldsymbol{\lambda}})q^{\delta_I(D_0+1)((D_{-1}+1)I+\operatorname{ord}_q((D_{-1}+1)!))}\\ &\times\Theta(q^{-(I+1)}s;\boldsymbol{t})\Pi^{(I+1)}(\boldsymbol{t})(\alpha_0')^{w^{(I+1)}(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^{r}(\alpha_i')^{(\mu_i-\mu_i^{(I+1)})p^{\varkappa}s}\end{aligned}$$

(with $w^{(I+1)}(\hat{\boldsymbol{\lambda}})\in q^{-\nu}\mathbb{Z}$) is in K and non-zero. Let $|\cdot|_v$ be an absolute value on K normalized as in [6, §2], and $|\cdot|_{v_0}$ be the one corresponding to $\mathfrak{p}$. Then we have (5.37) with φ' replaced by φ'''. Following the same lines of argumentation as in the proof of Lemma 5.2, and utilizing (5.17), we see that (5.68) implies that

$$\begin{aligned}\frac{c_1q^{r+1}}{U}&\cdot\text{left-hand side of (5.67)}\\ &\leqslant c_1\left(g_{12}+\left(1+\frac{1}{2(c_{02}-1)}\right)g_8\right)\\ &\quad+\frac{1}{c_2}\left(q+\frac{1}{2(c_{02}-1)}\left(1+\frac{1}{2g_2+1}\right)\right)\\ &\quad+\frac{1}{c_3}\left(\frac{1}{e_{\mathfrak{p}}\theta}(g_9\eta^{r+2}+\hat{c}_{03})+\left(1+\frac{1}{c_{02}-1}\right)g_{10}\right)\\ &\quad+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\left(1+\frac{1}{c_{02}-1}+\frac{\log q}{(q-1)g_1}+\left(\theta+\frac{1}{p-1}\right)\frac{e_{\mathfrak{p}}}{d}\right)\end{aligned} \tag{5.70}$$

if $p>2$, whereas if $p=2$, the right-hand side of (5.70) is replaced by the sum of it and the term

$$\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{5}{3}\frac{\log q}{\log q\eta^{r+1}}.$$

Write $\mathfrak{R}_2$ for the right-hand side of (5.70). Then (5.67), (5.70) and the definition of f_3 in (3.22) give

$$f_3 = 2c_5 q(q-1) - \mathfrak{R}_2 < 0, \tag{5.71}$$

contradicting (3.22) (3). Thus (5.68) is impossible, whence Lemma 5.4 follows. □

By applying Lemma 5.2 with $I=0$ and $J=1$, and applying Lemma 5.4 with $I=0$, we see that the first main inductive argument is true for $I=0,1$. Now the first main inductive argument follows by induction on I, utilizing Lemma 5.4.

If $I^* \leqslant I_1$, we take $I=I_0=I^*$ in the first main inductive argument. In §6, starting from (5.20) with $I=I^*$, we shall carry out a group variety reduction and reach a contradiction to the minimal choice of r. This will prove Proposition 3.1 when $I^* \leqslant I_1$.

In the remainder of this section we prepare the proof of Proposition 3.1 when

$$I^* > I_1. \tag{5.72}$$

(We shall complete this proof in §7). The first main inductive argument with $I=I_0=I_1$ gives

$$\varphi^{(I_1)}(s;\boldsymbol{t}) = 0 \quad \text{for all } |s| \leqslant qS^{(I_1)} \text{ and } |\boldsymbol{t}| \leqslant \eta T^{(I_1)}. \tag{5.73}$$

Define $r_1 \in \mathbb{Z}$ by

$$1 \leqslant \eta^{r_1} T^{(I_1)} \frac{c_5}{r+1} < \frac{1}{\eta}. \tag{5.74}$$

Thus, by (5.15),

$$0 \leqslant r_1 \leqslant r. \tag{5.75}$$

Lemma 5.5. *If $I^* > I_1$, we have*

$$\varphi^{(I_1)}(s;\boldsymbol{t}) = 0 \quad \textit{for all } |s| \leqslant q^{r_1+1} S^{(I_1)} \textit{ and } |\boldsymbol{t}| \leqslant \eta^{r_1+1} T^{(I_1)}. \tag{5.76}$$

Proof. The proof follows the pattern of that of Lemma 8.5♣ and utilizes §3.3, especially (3.22) (j), $j=1,5,27$. We omit the details here. □

6. Group variety reduction ($I^* \leqslant I_1$)

Now $I^* \leqslant I_1$ implies $I_0 = I^*$. We write $I=I^*$ in this section. Then the first main inductive argument gives

$$\varphi^{(I)}(s;\boldsymbol{t}) = 0 \quad \text{for all } |s| \leqslant qS^{(I)} \text{ and } |\boldsymbol{t}| \leqslant \eta T^{(I)}. \tag{6.1}$$

Let

$$\delta_i = [q^{\nu-I} D_i], \quad 1 \leqslant i \leqslant r. \tag{6.2}$$

Recalling (5.4), (5.8), (5.10) and multiplying (9.1) by

$$\prod_{i=1}^{r}(((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{s/q^{\nu}})^{\delta_i},$$

we obtain

$$\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}}\varrho^{(I)}(\hat{\boldsymbol{\lambda}})\Pi^{(I)}(\boldsymbol{t})\Theta(q^{-I}s;\boldsymbol{t})\prod_{i=1}^{r}(((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{s/q^{\nu}})^{\mu_i'-(\mu_i^{(I)})'+\delta_i}=0 \tag{6.3}$$

for all $0\leqslant s\leqslant qS^{(I)}$ and $|\boldsymbol{t}|\leqslant\eta T^{(I)}$; here we recall (4.17) and that $\boldsymbol{\mu}=\boldsymbol{\lambda}\mathcal{B}$ and $\boldsymbol{\mu}^{(I)}=\boldsymbol{\lambda}^{(I)}\mathcal{B}$. Now we take

$$\mathcal{P}(Y_0,...,Y_r)=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}}\varrho^{(I)}(\hat{\boldsymbol{\lambda}})\Delta(q^{-I}Y_0+\lambda_{-1};D_{-1}+1)^{\lambda_0+1}\prod_{i=1}^{r}Y_i^{\mu_i'-(\mu_i^{(I)})'+\delta_i}. \tag{6.4}$$

Note that $\varrho^{(I)}(\hat{\boldsymbol{\lambda}})$, $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}$, are not all zero. So $\mathcal{P}(Y_0,...,Y_r)$ is a non-zero polynomial with degree in Y_i at most $\mathcal{D}_i$ $(0\leqslant i\leqslant r)$, where

$$\mathcal{D}_0=(D_{-1}+1)(D_0+1)\quad\text{and}\quad\mathcal{D}_i=2q^{\nu-I}D_i\ \ (1\leqslant i\leqslant r). \tag{6.5}$$

Take

$$\mathcal{S}=qS^{(I)},\quad\mathcal{T}=\eta T^{(I)}\quad\text{and}\quad\vartheta_i=((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{1/q^{\nu}}\ \ (1\leqslant i\leqslant r). \tag{6.6}$$

Observe that $\vartheta_1,...,\vartheta_r$ are multiplicatively independent, since so are $\alpha_1',...,\alpha_r'$ (see §2). Recall that $\partial_0^*=\partial_0=\partial/\partial Y_0$ and $\partial_1^*,...,\partial_{n-1}^*$ are the differential operators specified in §2, and that

$$\partial_j^*\prod_{i=1}^{r}Y_i^{\mu_i'-(\mu_i^{(I)})'+\delta_i}=\gamma_j\prod_{i=1}^{r}Y_i^{\mu_i'-(\mu_i^{(I)})'+\delta_i}\quad(1\leqslant j<n), \tag{6.7}$$

where γ_j is given by (see (4.17) and (5.6))

$$\gamma_j=\gamma_j^{(I)}+\sum_{i=1}^{r}\left(b_n\frac{\partial L_i}{\partial z_j}-b_j\frac{\partial L_i}{\partial z_n}\right)\delta_i\quad(1\leqslant j<n). \tag{6.8}$$

By [34, Lemma 2.6], we obtain from (6.3), (6.4) and (6.6)–(6.8)

$$(\partial_0^*)^{t_0}(\partial_1^*)^{t_1}...(\partial_{r-1}^*)^{t_{r-1}}\mathcal{P}(s,\vartheta_1^s,...,\vartheta_r^s)=0\quad\text{for all } 0\leqslant s\leqslant\mathcal{S}\text{ and }|\boldsymbol{t}|\leqslant\mathcal{T}. \tag{6.9}$$

Now Proposition 3.1♣ holds with $\partial_1^*,...,\partial_{r-1}^*$ in place of $\partial_1,...,\partial_{r-1}$ (see §2). Put

$$\mathcal{S}_0=\left\lfloor\frac{\mathcal{S}}{3}\right\rfloor,\quad\mathcal{S}_i=\left\lfloor\frac{2\mathcal{S}}{3r}\right\rfloor\ \ (1\leqslant i\leqslant r),\quad\mathcal{T}_i=\left\lfloor\frac{\mathcal{T}}{r+1}\right\rfloor\ \ (0\leqslant i\leqslant r). \tag{6.10}$$

Then $\mathcal{S}_0 \geqslant \mathcal{S}_1 = ... = \mathcal{S}_r$ since $r \geqslant 2$, $\mathcal{T}_0 = ... = \mathcal{T}_r$, $\mathcal{S}_0 + ... + \mathcal{S}_r \leqslant \mathcal{S}$ and $\mathcal{T}_0 + ... + \mathcal{T}_r \leqslant \mathcal{T}$.

We note that

$$q\eta^{2(r+1)} < 1, \tag{6.11}$$

since $q\eta^{2(r+1)} < qe^{-2c_5} < 1$, by the fact that $c_5 > \frac{1}{2}\log q$ (see Table 3.1). Recalling that $I = I^*$, we see that (5.14) and (6.11) imply that

$$\eta^{-(r+1)I} > (q\eta^{r+1})^I > \exp(3(\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}} \log p\} + \nu \log q)). \tag{6.12}$$

Now we prove

$$\mathcal{T}_r + r \leqslant \mathcal{D}_0, \tag{6.13}$$

which implies (3.2)$^{\clubsuit}$. By (3.26) and (6.5), we have

$$\frac{\mathcal{D}_0}{r} > \frac{(D_{-1}+1)\widetilde{D}_0}{r} > \frac{\widetilde{D}_0}{r} \geqslant \frac{g_5}{r} > 4,$$

where the third inequality follows from the definition of g_5 in (3.16), using PARI/GP. Further, by (3.1), (3.5), (3.7), (6.5), (6.6), (6.10), (6.12) and the definition of h in §3.1, we have

$$\frac{\mathcal{D}_\prime}{\mathcal{T}_\triangledown} > e\frac{c_3}{c_4}(r+1)g_0(e_{\mathfrak{p}}\check{\theta})(e^4(r+1)d)^2 > 4$$

(see Tables 3.1 and 3.2). This completes the proof of (6.13).

By (3.7), (3.8), (6.5), (6.12) and using that $d\sigma_i > 2/\log^3 3d$ if $d > 1$ (see Voutier [28]) and that $d\sigma_i \geqslant \log 2$ if $d = 1$, we obtain

$$\mathcal{D}_0 > \mathcal{D}_i \quad (1 \leqslant i \leqslant r). \tag{6.14}$$

Now we verify (3.1)$^{\clubsuit}$.

(i) $m = 0$. By (6.14), it suffices to show that $(\mathcal{S}_0+1)(\mathcal{T}_0+1) > \mathcal{D}_0$. By (3.5), (3.7), (3.26), (6.5), (6.6) and (6.10), we have

$$(\mathcal{S}_0+1)(\mathcal{T}_0+1) > \frac{1}{c_1}\frac{q^2\eta}{3\hat{\vartheta}}\frac{SD}{e_{\mathfrak{p}} f_{\mathfrak{p}} \log p}$$

and

$$\mathcal{D}_0 = (D_1+1)(D_0+1) \leqslant \left(1 + \frac{1}{g_5}\right)\frac{1}{c_1 c_4}\frac{SD}{d}\frac{1}{f_{\mathfrak{p}} \log p}.$$

Thus (3.1)$^{\clubsuit}$ with $m = 0$ follows from (3.22) (30).

(ii) $1 \leqslant m < r$. By (3.5), (3.7), (3.8), (3.26), (6.5), (6.6), (6.10) and $\eta^{m+1} \geqslant \eta^r \geqslant e^{-c_5}$ we have

$$(\mathcal{S}_m+1)\binom{\mathcal{T}_m+m+1}{m+1} > \frac{2qe^{-c_5}\eta^{(r+1)Im}}{(m+1)!\,3r}\left(\frac{q}{c_1\theta e_{\mathfrak{p}} f_{\mathfrak{p}} \log p}\right)^{m+1} SD^{m+1}$$

and for any $1\leqslant i_1<...<i_m\leqslant r$,

$$\mathcal{D}_0\mathcal{D}_{i_1}\dots\mathcal{D}_{i_m}\leqslant\left(1+\frac{1}{g_5}\right)\frac{1}{c_1c_4}\frac{SD^{m+1}(2q^{\nu-I})^m}{(c_1c_2rp^{\varkappa})^m(d^{m+1}\sigma_{i_1}\dots\sigma_{i_m})f_{\mathfrak{p}}\log p}.$$

Applying [14, Theorem 3] for a lower bound of $d^{m+1}\sigma_{i_1}\dots\sigma_{i_m}$ and using

$$(q\eta^{r+1})^{Im}>(e^4(r+1)d)^{2m}p^{f_{\mathfrak{p}}m}q^{3\nu m}$$

(see (6.12)), we obtain $(3.1)^{\clubsuit}$ with $1\leqslant m<r$.

(iii) $m=r$. By (3.4), (3.5), (3.7), (3.8), (3.26), (6.5), (6.6), (6.10) and

$$\max\left\{\frac{p^{f_{\mathfrak{p}}}}{\delta(\mathfrak{a}')(f_{\mathfrak{p}}\log p)^r},\frac{e^r}{r^r}f_{\mathfrak{p}}\log p\right\}\leqslant\frac{p^{f_{\mathfrak{p}}}}{(f_{\mathfrak{p}}\log p)^{r-1}},\tag{6.15}$$

we have

$$(\mathcal{S}_r+1)\binom{\mathcal{T}_r+r}{r}>\eta^{(r+1)I(r-1)}\frac{2qe^{-c_5}}{r!\,3r}\left(\frac{q}{c_1\theta e_{\mathfrak{p}}f_{\mathfrak{p}}\log p}\right)^rSD^r$$

and

$$\begin{aligned}\mathcal{D}_0\mathcal{D}_1\dots\mathcal{D}_m\leqslant(2q^{\nu-I})^rq^{-u}\left(1+\frac{1}{g_5}\right)(1+\varepsilon)\left(2+\frac{1}{g_2}\right)c_0\log^*d&\\ \times p^{f_{\mathfrak{p}}}f_{\mathfrak{p}}\log p\frac{(r+1)^r}{r!}\left(\frac{q}{c_1\theta e_{\mathfrak{p}}f_{\mathfrak{p}}\log p}\right)^rSD^r.&\end{aligned}$$

Now by $\eta^{-(r+1)I}>p^{3f_{\mathfrak{p}}}$ (see (6.12)) and

$$(q\eta^{r+1})^{Ir}>(e^4(r+1)d)^{3r}q^{3\nu r},$$

$(3.1)^{\clubsuit}$ with $m=r$ follows.

Having verified $(3.1)^{\clubsuit}$ and $(3.2)^{\clubsuit}$, we can now apply Proposition $3.1^{\clubsuit}$ with $a_i=\sigma_i$ $(1\leqslant i\leqslant r)$. Thus there exist an integer ϱ with $1\leqslant\varrho<r$ and a set of linearly independent linear forms $\mathcal{L}_1,\dots,\mathcal{L}_\varrho$ in $Z_1,\dots,Z_r$ over $\mathbb{Z}$ such that $B_1Z_1+\dots+B_rZ_r$ is in the module generated by $\mathcal{L}_1,\dots,\mathcal{L}_\varrho$ over $\mathbb{Q}$ and, on defining

$$\mathcal{R}_i=\sum_{j=1}^r\left|\frac{\partial\mathcal{L}_i}{\partial Z_j}\right|\sigma_j\quad(1\leqslant i\leqslant\varrho),\tag{6.16}$$

we have at least one of $(3.3)^{\clubsuit}$ and $(3.4)^{\clubsuit}$, whence $(3.4)^{\clubsuit}$ always holds, since $(3.3)^{\clubsuit}$ implies $(3.4)^{\clubsuit}$ by (6.10) and (6.13). Now

$$\mathcal{L}_i':=\mathcal{L}_i(L_1,\dots,L_r)\quad(1\leqslant i\leqslant\varrho)\tag{6.17}$$

are linear forms in $z_0, z_1, ..., z_n$ over $\mathbb{Z}$ having the following two properties:

(i) The $\varrho+1$ linear forms $\mathcal{L}'_0=z_0$, $\mathcal{L}'_1, ..., \mathcal{L}'_\varrho$ are linearly independent and

$$L=B_0\mathcal{L}'_0+B'_1\mathcal{L}'_1+...+B'_\varrho\mathcal{L}'_\varrho$$

for some rationals $B'_1, ..., B'_\varrho$, not all zero, since $\{\mathcal{L}_1, ..., \mathcal{L}_\varrho\}$ is a set of linearly independent linear forms in $Z_1, ..., Z_r$ over $\mathbb{Z}$ and $B_1Z_1+...+B_rZ_r$ is in the module generated by $\mathcal{L}_1, ..., \mathcal{L}_\varrho$ over $\mathbb{Q}$.

(ii) We have $h_0(\alpha''_i)\leqslant\mathcal{R}_i$ $(1\leqslant i\leqslant\varrho)$ for $\alpha''_i=e^{l''_i}$ with $l''_i=\mathcal{L}'_i(l_0, l_1, ..., l_n)$ $(1\leqslant i\leqslant\varrho)$, since $l''_i=\mathcal{L}_i(l'_1, ..., l'_r)$ (by (2.7) and (6.17)), whence, by (2.6), (2.7) and (6.16),

$$h_0(\alpha''_i)\leqslant\sum_{j=1}^{r}\left|\frac{\partial\mathcal{L}_i}{\partial Z_j}\right|h_0(\alpha'_j)\leqslant\mathcal{R}_i\quad(1\leqslant i\leqslant\varrho).$$

Further (2.8) and (6.16) give

$$\sum_{j=1}^{n}\left|\frac{\partial\mathcal{L}'_i}{\partial z_j}\right|h_0(\alpha_j)\leqslant\sum_{j=1}^{n}\sum_{k=1}^{r}\left|\frac{\partial\mathcal{L}_i}{\partial Z_k}\right|\left|\frac{\partial L_k}{\partial z_j}\right|h_0(\alpha_j)\leqslant\sum_{k=1}^{r}\left|\frac{\partial\mathcal{L}_i}{\partial Z_k}\right|\sigma_k=\mathcal{R}_i\quad(1\leqslant i\leqslant\varrho).$$

We note that the set $\mathfrak{a}''=\{\alpha''_1, ..., \alpha''_\varrho\}$ is multiplicatively independent, since $l_0, l''_1, ..., l''_\varrho$ are linearly independent. Further we see that $\alpha''_1, ..., \alpha''_\varrho$ are $\mathfrak{p}$-adic units in K. Thus $\delta(\mathfrak{a}'')$ is well defined in the sense of (1.6). Let $\psi_1(\varrho)$ be defined by (2.10) with r replaced by ϱ and $\mathfrak{a}'$ replaced by $\mathfrak{a}''$. We shall prove that (3.4)$^\clubsuit$ implies that

$$\mathcal{R}_1 ... \mathcal{R}_\varrho\leqslant\psi_1(\varrho)h_0(\alpha_1) ... h_0(\alpha_n),\tag{6.18}$$

whence the basic hypothesis in §2 holds with ϱ in place of r. By the minimal choice of r, we have a contradiction and this establishes Proposition 3.1 when $I^*\leqslant I_1$.

Now, by (3.4)$^\clubsuit$, (2.9), (2.10), (3.4), (3.5), (3.7), (3.8), (3.26), (6.5), (6.6), (6.10), $e^r\geqslant r^r/r!$, $\mathcal{C}(\varrho)\leqslant\varrho!\,r^\varrho$ (see §3$^\clubsuit$), $q\eta^\varrho(1-1/g_2)>1$ and (6.15) with r replaced by ϱ and $\mathfrak{a}'$ replaced by $\mathfrak{a}''$, in order to prove (6.18), it suffices to show that

$$\begin{aligned}\eta^{-(r+1)I}(q\eta^{r+1})^{I\varrho}\geqslant 1.5\frac{c_0}{q^u}(1+\varepsilon)\left(2+\frac{1}{g_2}\right)\left(1+\frac{1}{g_5}\right)&\\ \times(2eq^\nu)^\varrho r(r+1)^\varrho(\varrho+1)(\varrho!)^2(\log^* d)p^{f_\mathfrak{p}}f_\mathfrak{p}\log p.&\end{aligned}\tag{6.19}$$

It is readily verified that $(q\eta^{r+1})^{I\varrho}>(e^4(r+1)d)^{3\varrho}q^{3\nu\varrho}$ and $\eta^{-(r+1)I}>p^{3f_\mathfrak{p}}$ (see (6.12)) imply (6.19). This proves Proposition 3.1 when $I^*\leqslant I_1$.

7. The second main inductive argument

In this section we treat the case when

$$I^* > I_1 \tag{7.1}$$

and complete the proof of Proposition 3.1.

Recalling (5.15) (the definition of I_1) and (5.74) (the definition of r_1), we define

$$I_2 = \left\lfloor \frac{3(\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}} \log p\} + \nu \log q) - I_1 \log q \eta^{r+1}}{\log q} \right\rfloor + 1 \quad \text{and} \quad I_3 = I_1 + I_2. \tag{7.2}$$

The second main inductive argument. Under (7.1) and the hypothesis of the first main inductive argument, for every $I \in \mathbb{Z}$ with $I_1 \leqslant I \leqslant I_3$ there exist $\boldsymbol{\Lambda}^{(I)} \subseteq \mathbb{Z}^r$, $\boldsymbol{x}^{(I)} \in \mathbb{R}^r$, $\varepsilon^{(I)} \in \mathbb{Z}$ satisfying (5.1) and $\varrho^{(I)}(\hat{\boldsymbol{\lambda}}) \in \mathcal{O}_K$, $\hat{\boldsymbol{\lambda}} \in \hat{\boldsymbol{\Lambda}}^{(I)}$, not all zero, satisfying (4.26) with $\boldsymbol{\varrho}$ replaced by $\boldsymbol{\varrho}^{(I)}$, such that

$$\varphi^{(I)}(s; \boldsymbol{t}) = 0 \quad \text{for all } |s| \leqslant q[q^{r_1} S^{(I_1)}] \text{ and } |\boldsymbol{t}| \leqslant \eta^{r_1+1} T^{(I_1)}. \tag{7.3}$$

In this section we always keep (5.19).

We remark here that the proof given in [37, §2] is valid also for $M=0$. Therefore Lemmas 2.1 and 2.2 in [37] with $M=0$ are true, which are important for the proofs of Lemmas 7.1 and 7.2 below.

LEMMA 7.1. *Suppose that I is in $\mathbb{Z}$ with $I_1 \leqslant I \leqslant I_3 - 1$, for which the second main inductive argument holds. Then we have*

$$\varphi^{(I)}\left(\frac{s}{q}; \boldsymbol{t}\right) = 0 \quad \textit{for all } |s| \leqslant q[q^{r_1} S^{(I_1)}] \textit{ and } |\boldsymbol{t}| \leqslant \eta^{r_1+1} T^{(I_1)}. \tag{7.4}$$

Proof. The conclusion (7.4) for s with $q|s$ follows from (7.3). Now we consider s with $(s,q)=1$. Note that, by (5.74),

$$\eta^{r_1+1} T^{(I_1)} \frac{c_5}{r+1} < 1.$$

So we apply [37, Lemma 2.1], to each function in (5.25) with $|\boldsymbol{t}| \leqslant \eta^{r_1+1} T^{(I_1)}$, with

$$R = q[q^{r_1} S^{(I_1)}] \quad \text{and} \quad M = 0. \tag{7.5}$$

By Lemma 5.1, (7.3) and the definition of h in §3.1, which implies that $\operatorname{ord}_p b_n \leqslant h/\log p$, we see that [37, (2,3)] holds for each $F^{(I)}(z; \boldsymbol{t})$ in (5.25) with $|\boldsymbol{t}| \leqslant \eta^{r_1+1} T^{(I_1)}$ whenever

$$U + (D_{-1}+1)(D_0+1)\left(\theta + \frac{1}{p-1}\right) \geqslant (2R+1)\theta + \frac{h + \nu \log q}{\log p}. \tag{7.6}$$

By (3.5), (3.9), (3.23), (3.25), (5.74) and (7.5), we obtain

$$(2R+1)\theta \leqslant \frac{c_5}{r+1}\eta^{r_1}T^{(I_1)}(2R+1)\theta \leqslant \frac{c_5}{c_1}\frac{U}{q^r}\eta^{r_1}\left(2q^{r_1+1}+\frac{r+1}{c_5\eta^{r_1+1}g_2g_4}\right). \tag{7.7}$$

By (3.1), (3.5), (3.9) and (3.25), we have

$$\frac{h+\nu\log q}{\log p} \leqslant \frac{T}{g_4}\frac{h+\nu\log q}{\log p} \leqslant \frac{U}{q^{r+1}c_1c_3e_{\mathfrak{p}}\check{\theta}g_4}. \tag{7.8}$$

Thus

$$c_1 \geqslant 2c_5\eta^{r_1}q^{r_1+1-r}+\frac{1}{q^rg_4}\left(\frac{r+1}{\eta g_2}+\frac{1}{qc_3e_{\mathfrak{p}}\check{\theta}}\right),$$

which is by (5.75) a consequence of (3.22) (5), implies (7.6), and hence implies [37, (2.3)]. Further

$$\begin{aligned} 2\left(1-\frac{1}{q}\right)R\theta &> 2\left(1-\frac{1}{q}\right)R\theta\eta^{r_1+1}T^{(I_1)}\frac{c_5}{r+1} \\ &\geqslant 2c_5(q-1)\eta^{r_1+1}\left(q^{r_1}-\frac{r+1}{c_5\eta^{r_1+1}g_2g_4}\right)\frac{U}{c_1q^r}. \end{aligned} \tag{7.9}$$

We also have

$$\begin{aligned} (2R+1)\theta-2\left(1-\frac{1}{q}\right)R\theta &> 2R\theta\eta^{r_1+1}T^{(I_1)}\frac{c_5}{(r+1)q} \\ &> 2c_5\left(1-\frac{1}{g_2}\right)(q\eta)^{r_1+1}\frac{U}{c_1q^{r+1}} \\ &\geqslant \left(1+\frac{1}{g_5}\right)\frac{\log q}{c_4g_1}\frac{U}{c_1q^{r+1}}, \end{aligned} \tag{7.10}$$

where the third inequality follows from (3.22) (28).

Let $K'=K(\theta_0^{1/q},\theta_1^{1/q},...,\theta_r^{1/q})$ and recall (5.11)♣. By consecutively applying [11, Chapter III, (2.28) (c)] $r+1$ times, we see that $\mathfrak{p}\mathcal{O}_{K'}=\mathfrak{P}_1\mathfrak{P}_2\dots\mathfrak{P}_{q^{r_0}}$ for some r_0 with $0\leqslant r_0\leqslant r+1$, where $\mathfrak{P}_j$ are distinct prime ideals of $\mathcal{O}_{K'}$ with ramification index and residue class degree (over $\mathbb{Q}$)

$$e_{\mathfrak{P}_j}=e_{\mathfrak{p}} \quad \text{and} \quad f_{\mathfrak{P}_j}=q^{r+1-r_0}f_{\mathfrak{p}}, \quad j=1,...,q^{r_0}.$$

Denote by $|\cdot|_{v'}$ an absolute value on K' normalized as in [6, §2], and by $|\cdot|_{v'_j}$ the one corresponding to $\mathfrak{P}_j$, and let $K'_{\mathfrak{P}_j}$ be the completion of K' with respect to $|\cdot|_{v'_j}$. The embedding of $K_{\mathfrak{p}}$ into $\mathbb{C}_p$ (see §1.1) can be extended to an embedding of $K'_{\mathfrak{P}_j}$ into $\mathbb{C}_p$, and we define for $\beta\in K'_{\mathfrak{P}_j}$, with $\beta\neq 0$,

$$\operatorname{ord}_p^{(j)}\beta := \frac{1}{e_{\mathfrak{P}_j}f_{\mathfrak{P}_j}\log p}(-\log|\beta|_{v'_j}) = \frac{1}{q^{r+1-r_0}e_{\mathfrak{p}}f_{\mathfrak{p}}\log p}(-\log|\beta|_{v'_j}).$$

We have $\operatorname{ord}_p^{(j)}\varphi^{(I)}(s/q;\boldsymbol{t})=\operatorname{ord}_p\varphi^{(I)}(s/q;\boldsymbol{t})$ $(1\leqslant j\leqslant q^{r_0})$, since $\varphi^{(I)}(s/q;\boldsymbol{t})\in K_{\mathfrak{p}}(\subseteq K'_{\mathfrak{P}_j})$.

We now apply [37, Lemma 2.1] to each $F^{(I)}(z;\boldsymbol{t})$ in (5.25) with $|\boldsymbol{t}|\leqslant\eta^{r_1+1}T^{(I_1)}$, and by (7.6), (7.9), (7.10) and Lemma 5.1, we obtain, for all $s\in\mathbb{Z}$,

$$\begin{aligned}\sum_{j=1}^{q^{r_0}}&\operatorname{ord}_p^{(j)}\varphi^{(I)}\left(\frac{s}{q};\boldsymbol{t}\right)+q^{r_0}(D_{-1}+1)(D_0+1)\left(\theta+\frac{1}{p-1}\right)-q^{r_0}\Delta^{(I)}\\&=q^{r_0}\left(\operatorname{ord}_p\varphi^{(I)}\left(\frac{s}{q};\boldsymbol{t}\right)+(D_{-1}+1)(D_0+1)\left(\theta+\frac{1}{p-1}\right)-\Delta^{(I)}\right)\\&>\frac{U}{c_1q^{r+1-r_0}}\left(2c_5q(q-1)\eta^{r_1+1}\left(q^{r_1}-\frac{r+1}{c_5\eta^{r_1+1}g_2g_4}\right)+\left(1+\frac{1}{g_5}\right)\frac{1}{c_4}\frac{\log q}{g_1}\right).\end{aligned}\tag{7.11}$$

Now we prove (7.4) for s with $(s,q)=1$. Suppose (7.4) were false, i.e., there exist s and $\boldsymbol{t}$ such that

$$\varphi^{(I)}\left(\frac{s}{q};\boldsymbol{t}\right)\neq0,\quad\text{for } |s|\leqslant q[q^{r_1}S^{(I_1)}],\text{ with } (s,q)=1,\text{ and } |\boldsymbol{t}|\leqslant\eta^{r_1+1}T^{(I_1)}.\tag{7.12}$$

We proceed to deduce a contradiction. In the sequel, we fix these s and $\boldsymbol{t}$.

For each $\hat{\boldsymbol{\lambda}}=(\lambda_{-1},\lambda_0,\boldsymbol{\lambda})\in\hat{\boldsymbol{\Lambda}}^{(I)}$, $\boldsymbol{\mu}=\boldsymbol{\lambda}\mathcal{B}$, by Lemma 4.1, (4.3), (4.4), (4.12) and $\alpha_0=\theta_0$, we have, with $w_1^{(I)}(\hat{\boldsymbol{\lambda}})\in\mathbb{Z}$ occurring in (5.34),

$$\begin{aligned}\prod_{i=1}^{r}(((\alpha_i')^{p^{\varkappa}}\zeta^{a_i'})^{1/q^{\nu}})^{(\mu_i'-(\mu_i^{(I)})')s/q}&=\prod_{i=1}^{r}((\theta_i^{1/q})^{p^{\varkappa}}\xi^{d_i})^{(\lambda_i-\lambda_i^{(I)})s}\\&=(\theta_0^{1/q})^{w_1^{(I)}(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^{r}(\theta_i^{1/q})^{(\lambda_i-\lambda_i^{(I)})p^{\varkappa}s}\\&\in K(\theta_0^{1/q},\theta_1^{1/q},...,\theta_r^{1/q})=K'.\end{aligned}\tag{7.13}$$

By [36, Lemma 1.3], for $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}$,

$$q^{(D_0+1)((D_{-1}+1)(I+1)+\operatorname{ord}_q((D_{-1}+1)!))}\Theta(q^{-(I+1)}s;\boldsymbol{t})\Pi^{(I)}(\boldsymbol{t})\in\mathbb{Z}.$$

By (1.3), (7.12) and (7.13), we have

$$\operatorname{ord}_p^{(j)}\varphi^{(I)}\left(\frac{s}{q};\boldsymbol{t}\right)=\operatorname{ord}_p^{(j)}\varphi''\quad(j=1,...,q^{r_0}),\tag{7.14}$$

where

$$\begin{aligned}\varphi''=\sum_{\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I)}}&\varrho^{(I)}(\hat{\boldsymbol{\lambda}})q^{(D_0+1)((D_{-1}+1)(I+1)+\operatorname{ord}_q((D_{-1}+1)!))}\\&\times\Theta(q^{-(I+1)}s;\boldsymbol{t})\Pi^{(I)}(\boldsymbol{t})(\theta_0^{1/q})^{w_1^{(I)}(\hat{\boldsymbol{\lambda}})s}\prod_{i=1}^{r}(\theta_i^{1/q})^{(\lambda_i-\lambda_i^{(I)})p^{\varkappa}s}\end{aligned}\tag{7.15}$$

is in K' and is non-zero. Then, by the product formula on K', we have

$$q^{r+1-r_0} e_{\mathfrak{p}} f_{\mathfrak{p}} (\log p) \sum_{j=1}^{q^{r_0}} \operatorname{ord}_p^{(j)} \varphi'' = -\sum_{j=1}^{q^{r_0}} \log |\varphi''|_{v'_j} = {\sum}' \log |\varphi''|_{v'}, \tag{7.16}$$

where ${\sum}'$ signifies the summation over all $v' \neq v'_1, ..., v'_{q^{r_0}}$. For $\hat{\boldsymbol{\lambda}} = (\lambda_{-1}, \lambda_0, \boldsymbol{\lambda}) \in \hat{\boldsymbol{\Lambda}}^{(I)}$, $\boldsymbol{\mu} = \boldsymbol{\lambda}\mathcal{B}$, we have, by (1.4), (4.16) and (4.17), with $\alpha'_0 = \theta_0 = \alpha_0$, and (5.1),

$$\begin{aligned}
&\log \left| (\theta_0^{1/q})^{w_1^{(I)}(\hat{\boldsymbol{\lambda}})s} \prod_{i=1}^r (\theta_i^{1/q})^{(\lambda_i - \lambda_i^{(I)}) p^{\varkappa} s} \right|_{v'} \\
&\quad = \frac{1}{q^{\nu+1}} \log \left| \prod_{i=1}^r (\alpha'_i)^{(\mu'_i - (\mu_i^{(I)})') p^{\varkappa} s} \right|_{v'} \\
&\quad = \frac{1}{q^{\nu+1}} \log \left(\prod_{i=1}^r |(\alpha'_i)^{p^{\varkappa} s}|_{v'}^{\mu'_i + (x_i^{(I)})'} \prod_{i=1}^r |(\alpha'_i)^{p^{\varkappa} s}|_{v'}^{-((\mu_i^{(I)})' + (x_i^{(I)})')} \right) \\
&\quad \leqslant \frac{1}{q^{I+1}} \sum_{i=1}^r D_i \log \max\{1, |(\alpha'_i)^{p^{\varkappa} s}|_{v'}\} - \frac{1}{q} \sum_{i=1}^r (\mu_i^{(I)} + x_i^{(I)}) \log |(\alpha'_i)^{p^{\varkappa} s}|_{v'}.
\end{aligned}$$

Now $\log |(\alpha'_i)^{p^{\varkappa} s}|_{v'_j} = 0$ $(1 \leqslant j \leqslant q^{r_0})$ by (2.11). So ${\sum}' \log |(\alpha'_i)^{p^{\varkappa} s}|_{v'} = 0$ by the product formula on K'. Thus for s in (7.12), we have, by (2.6), (3.8) and (5.11)♣,

$${\sum}' \log \left| (\theta_0^{1/q})^{w_1^{(I)}(\hat{\boldsymbol{\lambda}})s} \prod_{i=1}^r (\theta_i^{1/q})^{(\lambda_i - \lambda_i^{(I)}) p^{\varkappa} s} \right|_{v'} \leqslant \frac{q^{r+1+r_1}}{q^{I-I_1} (q\eta^{r+1})^{I_1}} \frac{1}{c_1 c_2} SD.$$

Bearing in mind that s and $\boldsymbol{t}$ are as in (7.12), we obtain, by (3.22) (19) and (3.22) (29),

$$\begin{aligned}
\log \left(e \left(2 + \frac{q^{-(I+1)}|s|}{D_{-1}+1} \right) \right) &\leqslant \log \left(e \left(2 + \frac{q^{r_1} S}{(q\eta^{r+1})^{I_1} (D_{-1}+1)} \right) \right) \\
&\leqslant \log \left(e \left(2 + \frac{q^{r_1 - 1} S}{D_{-1}+1} \right) \right) \\
&\leqslant \log \left(e q^{r_1 - 1} \left(2q + \frac{c_3 q g_0}{(g_0 - 1) f_{\mathfrak{p}} \log p} (r+1) d \right) \right) \\
&\leqslant g_1 + (r_1 - 1) \log q.
\end{aligned}$$

By (3.1), (3.5), (3.6), (5.74), we get

$$\eta^{r_1+1} T^{(I_1)} (D_{-1}+1) \leqslant \frac{(r+1)SD}{d c_5 g_4 c_1 c_3 e_{\mathfrak{p}} \theta}.$$

Thus

$$\begin{aligned}
&\log |q^{(D_0+1)((D_{-1}+1)(I+1) + \operatorname{ord}_q((D_{-1}+1)!))} \Theta(q^{-(I+1)} s; \boldsymbol{t}) \Pi^{(I)}(\boldsymbol{t})| \\
&\quad \leqslant \left(\frac{g_9}{e_{\mathfrak{p}} \theta} \frac{r+1}{c_5 g_4} + g_{10} \right) \frac{1}{c_1 c_3} \frac{SD}{d} + \left(1 + \frac{1}{g_5} \right) \left(1 + \frac{(I + r_1 + 1/(q-1)) \log q}{\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}} \log p\} + \nu \log q} \right) \frac{1}{c_1 c_4} \frac{SD}{d}.
\end{aligned}$$

Following the same line of argumentation as in the proof of Lemmas 8.2♣ and 8.3♣, we see, by (7.11), that (7.12) implies that

$$\mathfrak{L}(r_1, I) < 0, \tag{7.17}$$

where

$$\begin{aligned}\mathfrak{L}(r_1, I) = 2c_5(q-1)(q\eta)^{r_1+1} - \frac{2q(q-1)(r+1)}{g_2 g_4} - c_1\left(g_{12} + \left(1 + \frac{1}{2(c_{02}-1)}\right)g_8\right) \\ - \frac{1}{c_2}\left(\frac{q^{r_1}}{q^{I-I_1}(q\eta^{r+1})^{I_1}} + \frac{1}{2(c_{02}-1)}\left(1 + \frac{1}{2g_2+1}\right)\right) \\ - \frac{1}{c_3}\left(\frac{1}{e_{\mathfrak{p}}\theta}\left(g_9\frac{r+1}{c_5 g_4} + \hat{c}_{03}\right) + \left(1 + \frac{1}{c_{02}-1}\right)g_{10}\right) \\ - \frac{1}{c_4}\left(1 + \frac{1}{g_5}\right)\left(1 + \frac{1}{c_{02}-1} + \left(\theta + \frac{1}{p-1}\right)\frac{e_{\mathfrak{p}}}{d}\right. \\ \left. + \frac{(I-1+r_1+1/(q-1))\log q}{\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}}\log p\} + \nu\log q}\right).\end{aligned}$$

By $I_1 \geqslant i_1$ (see (3.16) and (5.15)) and (3.22) (17), we see, on noting that $I_1 \leqslant I \leqslant I_3 - 1$ and $q\eta^{r_1+1} \geqslant q\eta^{r+1} > 1$, that $\partial\mathfrak{L}(x, I)/\partial x > 0$ for $0 \leqslant x \leqslant r$. Hence, (7.17) implies that

$$\mathfrak{L}(0, I) < 0. \tag{7.18}$$

Further, $d^2\mathfrak{L}(0, y)/dy^2 < 0$ for $I_1 \leqslant y \leqslant I_3 - 1$. Thus (7.18) gives

$$\min\{\mathfrak{L}(0, I_1), \mathfrak{L}(0, I_3-1)\} < 0, \tag{7.19}$$

since the left-hand side of (7.19) is the minimum of $\mathfrak{L}(0, y)$ on the interval $I_1 \leqslant y \leqslant I_3 - 1$. By (5.18) and (7.1), we have

$$\begin{aligned}\frac{1}{c_2}\frac{1}{(q\eta^{r+1})^{I_1}} + \frac{1}{c_4}\left(1 + \frac{1}{g_5}\right)\frac{(I_1 + 1/(q-1) - 1)\log q}{\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}}\log p\} + \nu\log q} \\ < \frac{1}{c_2}\frac{q}{(q\eta^{r+1})^{I_1}} + \frac{1}{c_4}\left(1 + \frac{1}{g_5}\right)\frac{I_1\log q}{\max\{g_1, e_{\mathfrak{p}}, f_{\mathfrak{p}}\log p\} + \nu\log q} \leqslant \frac{7q}{8c_2}\end{aligned}$$

if $p > 2$, whereas, if $p = 2$, $7q/8c_2$ in the extreme right-hand side is replaced by the expression

$$\frac{13q}{16c_2} + \frac{1}{c_4}\left(1 + \frac{1}{g_5}\right)\frac{5\log q}{3\log q\eta^{r+1}}.$$

Thus

$$f_4 < \mathfrak{L}(0, I_1), \tag{7.20}$$

where f_4 is given by (3.22). Now we treat $\mathfrak{L}(0,I_3-1)$. By (5.14), we have

$$(I^*-1)\log q\eta^{r+1} \leqslant 3(\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q) < I^*\log q\eta^{r+1}. \tag{7.21}$$

Thus, by (7.2),

$$\begin{aligned}\log q^{I_3-1-I_1}(q\eta^{r+1})^{I_1} &= (I_2-1)\log q+I_1\log q\eta^{r+1}\\ &> 3(\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q)-\log q\\ &\geqslant (I^*-1)\log q\eta^{r+1}-\log q.\end{aligned} \tag{7.22}$$

Further, by (7.1), (7.2) and (7.21),

$$\begin{aligned}(I_3-2)\log q &= (I_1-1)\log q+(I_2-1)\log q\\ &\leqslant (I_1-1)\log q+3(\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q)-I_1\log q\eta^{r+1}\\ &< (I_1-1)\log q+(I^*-I_1)\log q\eta^{r+1}\\ &= (I^*-1)\log q+(I^*-I_1)\log \eta^{r+1}\\ &\leqslant (I^*-1)\log q+\log \eta^{r+1}.\end{aligned} \tag{7.23}$$

So, by (5.18), (6.11), (7.22) and (7.23), we obtain

$$\begin{aligned}&\frac{1}{c_2}\frac{1}{q^{I_3-1-I_1}(q\eta^{r+1})^{I_1}}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{(I_3-2+1/(q-1))\log q}{\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q}\\ &\quad<\frac{1}{c_2}\frac{q}{(q\eta^{r+1})^{I^*-1}}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{(I^*-1)\log q+\log\eta^{r+1}+(\log q)/(q-1)}{\max\{g_1,e_{\mathfrak{p}},f_{\mathfrak{p}}\log p\}+\nu\log q}\\ &\quad\leqslant\frac{7}{8}\frac{q}{c_2}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{\log q\eta^{r+1}}{g_1},\end{aligned} \tag{7.24}$$

if $p>2$, whereas, if $p=2$, the extremely right-hand side of (7.24) is replaced by the expression

$$\frac{13}{16}\frac{q}{c_2}+\frac{1}{c_4}\left(1+\frac{1}{g_5}\right)\frac{5}{3}\,\frac{\log q}{\log q\eta^{r+1}}.$$

Now (7.24) implies that

$$f_4<\mathfrak{L}(0,I_3-1). \tag{7.25}$$

Summing up, (7.19), (7.20) and (7.25) give $f_4<0$, contradicting (3.22) (4). This proves that (7.12) is impossible, whence (7.4) holds and Lemma 7.1 follows. □

LEMMA 7.2. *For every I as in Lemma 7.1 there exist $\boldsymbol{\Lambda}^{(I+1)}\subseteq\mathbb{Z}^r$, $\boldsymbol{x}^{(I+1)}\in\mathbb{R}^r$, $\varepsilon^{(I+1)}\in\mathbb{Z}$ satisfying (5.1) with I replaced by $I+1$, and $\varrho^{(I+1)}(\hat{\boldsymbol{\lambda}})\in\mathcal{O}_K$, $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}^{(I+1)}$, not all zero, satisfying (4.26) with $\boldsymbol{\varrho}$ replaced by $\boldsymbol{\varrho}^{(I+1)}$, such that*

$$\varphi^{(I+1)}(s;\boldsymbol{t})=0\quad \textit{for all } |s|\leqslant q[q^{r_1}S^{(I_1)}] \textit{ and } |\boldsymbol{t}|\leqslant\eta^{r_1+1}T^{(I_1)}. \tag{7.26}$$

Proof. The proof follows the pattern of that of Lemma 9.2$^{\clubsuit}$ and Lemma 5.4, and utilizes §3.3. We omit the details here. □

By Lemma 5.5, the second main inductive argument is valid for $I=I_1$. Now the second main inductive argument follows by induction on I, utilizing Lemma 7.2.

Starting from (7.3) with $I=I_3$, we carry out a group variety reduction and reach a contradiction to the minimal choice of r in the basic hypothesis in §2 (this is very similar to §6 and §10$^{\clubsuit}$, so we omit the details here). This proves Proposition 3.1 when $I^*>I_1$. Recalling §6, the proof of Proposition 3.1 is now complete. By Lemma 3.2, Theorem I is established.

8. The proof of Theorem 1

We first deduce a special case of Theorem 1 from Theorem I. Recall (1.19)–(1.23).

LEMMA 8.1. *Suppose that $r=n\geqslant 1$. Then Theorem 1 holds.*

Proof. The condition $r=n$ implies that

$$\mathfrak{b}=\mathfrak{a} \quad \text{and} \quad \Omega=h_0(\alpha_1)\ldots h_0(\alpha_n).$$

Using (1.9), (1.22) and applying [14, Theorem 3] for a lower bound of Ω, we get

$$C_1^*(n,d,\mathfrak{p},\mathfrak{b})\Omega\geqslant\frac{d}{f_{\mathfrak{p}}\log p}\frac{c^{(1)}}{\varrho}(a^{(1)})^n\frac{n^n(n+1)^{n+2}}{(n!)^2}\log e^4(n+1)d, \tag{8.1}$$

where ϱ is given by (3.13). Thus

$$\frac{d}{f_{\mathfrak{p}}\log p}\log 2<C_1^*(n,d,\mathfrak{p},\mathfrak{b})\Omega\max\{\log B, f_{\mathfrak{p}}\log p\}\frac{1}{7900}. \tag{8.2}$$

We prove Lemma 8.1 for $n=1$ first. By the restated (in §2) [35, Lemma 1.4], we have

$$\operatorname{ord}_{\mathfrak{p}}(\Xi-1)\leqslant\frac{d}{f_{\mathfrak{p}}\log p}\left(\log 2B+|\langle\bar{\alpha}_1\rangle|\left(1+\frac{1}{p-1}\right)e_{\mathfrak{p}}h_0(\alpha_1)\right).$$

By (8.1), we get

$$\frac{d}{f_{\mathfrak{p}}\log p}\log B<\frac{1}{3950}C_1^*(1,d,\mathfrak{p},\{\alpha_1\})\Omega\max\{\log B, f_{\mathfrak{p}}\log p\}.$$

Further, using (1.6) and (3.15), we obtain

$$\frac{d}{f_{\mathfrak{p}}\log p}|\langle\bar{\alpha}_1\rangle|\left(1+\frac{1}{p-1}\right)e_{\mathfrak{p}}h_0(\alpha_1)<\frac{1}{28000}C_1^*(1,d,\mathfrak{p},\{\alpha_1\})\Omega\max\{\log B, f_{\mathfrak{p}}\log p\}.$$

Thus Lemma 8.1 for $n=1$ follows. We now prove Lemma 8.1 for $n\geqslant 2$. Without loss of generality, we may assume (1.17). Let

$$h_0(\alpha_k)=\max\{h_0(\alpha_1),...,h_0(\alpha_n)\}.$$

By [34, (2.6)], we have

$$\mathrm{ord}_{\mathfrak{p}}(\Xi-1)\leqslant\frac{d}{f_{\mathfrak{p}}\log p}(nBh_0(\alpha_k)+\log 2). \tag{8.3}$$

By (8.2) and (8.3), we may assume that

$$\frac{B}{\log B}>\left(1-\frac{1}{7900}\right)\frac{f_{\mathfrak{p}}\log p}{nd}C_1^*(n,d,\mathfrak{p},\mathfrak{b})\frac{\Omega}{h_0(\alpha_k)}. \tag{8.4}$$

Write W for the right-hand side of (8.4). Applying [14, Theorem 3] for a lower bound of $\Omega/h_0(\alpha_k)$, we obtain

$$W\geqslant\left(1-\frac{1}{7900}\right)\frac{c^{(1)}e}{\varrho}(a^{(1)})^n\frac{(n+1)^{n+2}(n-1)^{n-1}}{(n!)^2}d\log e^4(n+1)d. \tag{8.5}$$

Recalling $a^{(1)}$, $c^{(1)}$, $a_0^{(1)}$, $a_1^{(1)}$ and $a_2^{(1)}$ given in §1.3, we see that

$$\log W\geqslant a_0^{(1)}n+a_1^{(1)}+\log d\geqslant a_0^{(1)}n+a_2^{(1)}.$$

Thus (8.4) gives (see (1.11))

$$(n+1)\log B\geqslant(n+1)(\log W+\log\log W)\geqslant G_1(n,d).$$

This, together with (1.13)–(1.15) and Voutier [28, Corollary 1], yields

$$(n+1)\max\{\log B,f_{\mathfrak{p}}\log p\}\geqslant h^{(1)}.$$

Now, on noting (1.9) and (1.22), Theorem 1 follows from Theorem I when $r=n\geqslant 1$. □

Proof of Theorem 1. By Lemma 8.1, Theorem 1 holds for $r=n$ and we may assume that $r<n$.

In the remainder of the proof of Theorem 1, we assume that

$$h_0(\alpha_1)\leqslant...\leqslant h_0(\alpha_n). \tag{8.6}$$

Thus $h_0(\alpha_n)>0$, since $r\geqslant 1$. There exist $i_1,...,i_r$ in $\mathbb{Z}$ with $1\leqslant i_1<...<i_r\leqslant n$ such that

(i) $\mathfrak{b}:=\{\alpha_{i_1},...,\alpha_{i_r}\}$ is multiplicatively independent;

(ii) if $i_1>1$ then each α_i $(1\leqslant i<i_1)$ is a root of unity;

(iii) for $k=1,...,r-1$, α_i is multiplicatively dependent on $\{\alpha_{i_1},...,\alpha_{i_k}\}$ for all i with $i_k\leqslant i<i_{k+1}$.

Obviously

$$\Omega=\Omega(\mathfrak{b}) \quad \text{with } \mathfrak{b}:=\{\alpha_{i_1},...,\alpha_{i_r}\}. \tag{8.7}$$

By applying [14, Theorem 3] for a lower bound of $h_0(\alpha_{i_1})\dots h_0(\alpha_{i_r})$ and using the inequalities

$$\left(\frac{n}{\varkappa_1(n+5)}\right)^{n-r} \geqslant \frac{\varkappa_1^{r-n}(n+5)}{e^5 n} \quad \text{and} \quad \frac{\varkappa_1^r r^r}{r!e^r} \geqslant \frac{\varkappa_1}{e},$$

we get

$$\begin{aligned} &C_1^*(n,d,\mathfrak{p},\mathfrak{b})\Omega\max\{\log B, f_{\mathfrak{p}}\log p\}\frac{f_{\mathfrak{p}}\log p}{d\log 2} \\ &\quad \geqslant \frac{c^{(1)}\varkappa_1}{\varrho e^6\log 2}\left(\frac{a^{(1)}}{\varkappa_1}\right)^n \frac{e^n(n+1)^{n+2}(n+5)}{n!n}(\log e^4(n+1)d)f_{\mathfrak{p}}\log p>2100. \end{aligned} \tag{8.8}$$

By (8.3), with α_k replaced by α_n, (8.6) and (8.8), we may assume that

$$\frac{B}{\log B} > \left(1-\frac{1}{2100}\right)\frac{f_{\mathfrak{p}}\log p}{nd}C_1^*(n,d,\mathfrak{p},\mathfrak{b})\frac{\Omega}{h_0(\alpha_n)}. \tag{8.9}$$

We consider three cases:

(1) $i_r<n$. We apply [14, Theorem 3] for a lower bound of $h_0(\alpha_{i_1})\dots h_0(\alpha_{i_r})$.

(2) $i_r=n$ with $r\geqslant 2$. We apply [14, Theorem 3] for a lower bound of

$$h_0(\alpha_{i_1})\dots h_0(\alpha_{i_{r-1}}).$$

(3) $i_r=n$ with $r=1$. We use (3.15).

We see that, in all three cases, (8.9) implies that

$$\frac{B}{\log B} > 50\left(\frac{a^{(1)}}{\varkappa_1}e^2\right)^n d. \tag{8.10}$$

We now prove Theorem 1 by induction on n, using Lemma 8.1. Suppose that Theorem 1 holds for $n-1$ with $n\geqslant 2$. We proceed to prove that Theorem 1 holds for n. Note that (1.9) and (1.22) give

$$\frac{C_1^*(n,d,\mathfrak{p},\mathfrak{b})}{C_1^*(n-1,d,\mathfrak{p},\mathfrak{b})} \geqslant \frac{a^{(1)}(n+1)^{n+2}}{(n-1)^{n-1}n^2}\frac{d}{\max\{n, f_{\mathfrak{p}}\log p\}}. \tag{8.11}$$

Suppose now $i_1=1$ (we treat the case $i_1>1$ at the end of the proof). Let m be the largest integer such that $i_1=1,...,i_m=m$. So $1\leqslant m\leqslant r$. If $m<r$, then $i_m<m+1<i_{m+1}$; if $m=r$, then $m+1\leqslant n$. Thus α_{m+1} is multiplicatively dependent on $\{\alpha_1,...,\alpha_m\}$. There exist $j_1,...,j_t$ in $\mathbb{Z}$ with $1\leqslant j_1<...<j_t\leqslant m$ such that $\alpha_{j_1},...,\alpha_{j_t},\alpha_{m+1}$ are multiplicatively dependent and any t numbers from $\alpha_{j_1},...,\alpha_{j_t},\alpha_{m+1}$ are multiplicatively independent.

By [14, Corollary 3.2], there are non-zero rational integers $k_1, ..., k_t, k_{m+1}$ ($k_{m+1}>0$) such that $\alpha_{j_1}^{k_1} ... \alpha_{j_t}^{k_t} \alpha_{m+1}^{k_{m+1}} = 1$ and

$$\begin{aligned}\max\{|k_1|, ..., |k_t|, |k_{m+1}|\} &\leqslant \varrho\left(\frac{t!e^t}{t^t}\right) d^{t+1} (\log^* d) \frac{h_0(\alpha_{m+1})}{h_0(\alpha_{j_1})} \prod_{\tau=1}^{t} h_0(\alpha_{j_\tau}) \\ &\leqslant \begin{cases} \frac{1}{8} B d h^{(n)}(\alpha_{m+1}), & \text{if } m+1=n, \\ \frac{1}{8} B, & \text{if } m+1<n, \end{cases}\end{aligned} \tag{8.12}$$

where ϱ is given by (3.13) and the second inequality is deduced from (1.20), (1.21), (8.7) and (8.9) by applying [14, Theorem 3]. Set

$$\Omega'' = \prod_{\alpha \in \mathfrak{b}} h_0(\alpha) \cdot \prod_{\alpha \in \mathfrak{a}'' \setminus \mathfrak{b}} h^{(n-1)}(\alpha) \quad \text{with } \mathfrak{a}'' = \{\alpha_1, ..., \alpha_n\} \setminus \{\alpha_{m+1}\}. \tag{8.13}$$

We may assume that $\Xi^{k_{m+1}} - 1 \neq 0$, since otherwise $\mathrm{ord}_\mathfrak{p}(\Xi - 1) \leqslant (d/f_\mathfrak{p} \log p) \log 2$ and Theorem 1 holds trivially by (8.8). Now, by the inductive hypothesis and by (8.10) and (8.12), we obtain

$$\begin{aligned}\mathrm{ord}_\mathfrak{p}(\Xi - 1) &\leqslant \mathrm{ord}_\mathfrak{p}((\alpha_1^{b_1} ... \alpha_n^{b_n})^{k_{m+1}} - 1) \\ &= \mathrm{ord}_\mathfrak{p}\left(\prod_{\tau=1}^{t} \alpha_{j_\tau}^{b_{j_\tau} k_{m+1} - b_{m+1} k_\tau} \cdot \prod_{\substack{1 \leqslant i \leqslant n \\ i \notin \{j_1, ..., j_t, m+1\}}} \alpha_i^{b_i k_{m+1}} - 1\right) \\ &< C_1^*(n-1, d, \mathfrak{p}, \mathfrak{b}) \Omega'' \max\{\log(B^2 \exp((4e)^{-1} d h^{(n)}(\alpha_{m+1}))), f_\mathfrak{p} \log p\} \\ &\leqslant C_1^*(n-1, d, \mathfrak{p}, \mathfrak{b}) \Omega'' \max\{\log B, f_\mathfrak{p} \log p\} \left(2 + \frac{1}{4e} \frac{d h^{(n)}(\alpha_{m+1})}{\max\{n, f_\mathfrak{p} \log p\}}\right),\end{aligned} \tag{8.14}$$

where $C_1^*(n-1, d, \mathfrak{p}, \mathfrak{b})$ is replaced by $\frac{1}{2100} C_1^*(n-1, d, \mathfrak{p}, \mathfrak{b})$ when $r=1$. By (1.20), (1.21), (8.7) and (8.13), we have

$$\frac{\Omega}{\Omega''} \geqslant h^{(n)}(\alpha_{m+1}) \left(\frac{n+4}{n+5}\right)^{n-r-1} \geqslant h^{(n)}(\alpha_{m+1}) \left(\frac{n+4}{n+5}\right)^{n-2}. \tag{8.15}$$

It can be verified that

$$\frac{(n+1)^{n+2}}{(n-1)^{n-1} n^2} \left(\frac{n+4}{n+5}\right)^{n-2} \geqslant e(n+5) \tag{8.16}$$

for $n \geqslant 2$. By (1.20), (8.11) and (8.14)–(8.16) in order to prove Theorem 1 in the case when $i_1 = 1$, it suffices to show that

$$\frac{1}{\varkappa_1 (n+5)} \left(a^{(1)} e(n+5) - \frac{1}{4e}\right) \geqslant 2.$$

The above inequality follows from the definition of $a^{(1)}$ and $\varkappa_1$ in §1.3. Thus Theorem 1 is proved in the case when $i_1=1$.

Finally, if $i_1>1$, then α_1 is a root of unity. We may assume that $\Xi^{w_K}-1\neq 0$, since otherwise $\operatorname{ord}_{\mathfrak{p}}(\Xi-1)\leqslant(d/f_{\mathfrak{p}}\log p)\log 2$ and Theorem 1 follows from (8.8). Now

$$\operatorname{ord}_{\mathfrak{p}}(\Xi-1)\leqslant \operatorname{ord}_{\mathfrak{p}}(\Xi^{w_K}-1)=\operatorname{ord}_{\mathfrak{p}}(\alpha_2^{b_2 w_K}\dots\alpha_n^{b_n w_K}-1).$$

Note that Waldschmidt [29, p. 276] and (8.10) give $w_K\leqslant 4d\log\log 6d\leqslant B$, whence

$$|b_i w_K|\leqslant B^2 \quad (2\leqslant i\leqslant n).$$

Thus we can prove Theorem 1 similarly to the case when $i_1=1$. The proof of Theorem 1 is complete. □

9. Further remarks on the solution of the problem of Erdős

Our exposition here follows basically Stewart [25], with some modifications, in order to be more streamlined with respect to the p-adic theory of logarithmic forms. Especially, we shall analyze the role of [40] and the role of the present paper in the solution of this problem.

Recall the definition of $P(m)$ and the definition of Lucas numbers u_n and Lehmer numbers $\tilde{u}_n$ given in §1.1.

For any integer $n>0$ and any pair of complex numbers α and β, denote by

$$\Phi_n(\alpha,\beta)={\prod}'(\alpha-\zeta^j\beta) \tag{9.1}$$

the nth cyclotomic polynomial in α and β, where ζ is a primitive nth root of unity and $\prod'$ signifies that j runs through a reduced set of residues (mod n). From (9.1), we deduce that

$$\alpha^n-\beta^n=\prod_{d\mid n}\Phi_d(\alpha,\beta). \tag{9.2}$$

By [24], we see that $\Phi_n(\alpha,\beta)\in\mathbb{Z}$ for $n>2$ if $(\alpha+\beta)^2\in\mathbb{Z}$ and $\alpha\beta\in\mathbb{Z}$. Hence Lucas numbers u_n $(n>0)$ and Lehmer numbers $\tilde{u}_n$ $(n>0)$ are rational integers. From (9.2) and the fact that $\Phi_1(\alpha,\beta)=\alpha-\beta$ and $\Phi_2(\alpha,\beta)=\alpha+\beta$, we see that

$$P(u_n)\geqslant P(\Phi_n(\alpha,\beta)) \text{ and } P(\tilde{u}_n)\geqslant P(\Phi_n(\alpha,\beta)) \quad \text{for } n>2. \tag{9.3}$$

Let $\omega(m)$ denote the number of distinct prime divisors of $m\in\mathbb{Z}$ when $m\neq 0$.

Theorem. (Stewart [25, Theorem 1.1]) *Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero rational integers and α/β is not a root of unity. Then there exists a positive number C, which is effectively computable in terms of $\omega(\alpha\beta)$ and the discriminant of $\mathbb{Q}(\alpha/\beta)$, such that, for all $n>C$,*

$$P(\Phi_n(\alpha,\beta)) > n\exp\left(\frac{\log n}{104\log\log n}\right). \tag{9.4}$$

Clearly (9.3) and (9.4) prove the conjecture of Erdős from 1965 and its generalizations

$$\frac{P(u_n)}{n}\to\infty \text{ and } \frac{P(\tilde{u}_n)}{n}\to\infty, \text{ respectively,} \quad \text{as } n\to\infty, \tag{9.5}$$

to Lucas and Lehmer numbers.

Henceforth we shall always assume that

$$|\alpha|\geqslant|\beta|.$$

As pointed out in [25], we may assume, without loss of generality, that

$$\gcd((\alpha+\beta)^2,\alpha\beta)=1. \tag{9.6}$$

Denote by $\varphi(n)$ Euler's φ-function. By [25, Lemma 4.2], there exists an effectively computable positive number c_1 such that if $n>c_1$ then

$$\log|\Phi_n(\alpha,\beta)|\geqslant\tfrac{1}{2}\varphi(n)\log|\alpha|. \tag{9.7}$$

(Note that the proof of [25, Lemma 4.2] depends ultimately upon an estimate for a linear form in two logarithms of algebraic numbers due to Baker [2], [3]; see [25, §4] for details.) On the other hand,

$$\log|\Phi_n(\alpha,\beta)| = \sum_{p\mid\Phi_n(\alpha,\beta)} \operatorname{ord}_p\Phi_n(\alpha,\beta)\cdot\log p \quad \text{for } n>2. \tag{9.8}$$

Observe that α^2 and β^2 are in the ring $\mathcal{O}_{\mathbb{Q}(\alpha/\beta)}$ of algebraic integers in $\mathbb{Q}(\alpha/\beta)$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{Q}(\alpha/\beta)}$, lying above the prime number p. We now show two facts.

Fact 1. *If $n>2$ and $p|\Phi_n(\alpha,\beta)$, then* $\operatorname{ord}_\mathfrak{p}\alpha^2=\operatorname{ord}_\mathfrak{p}\beta^2=\operatorname{ord}_\mathfrak{p}(\alpha/\beta)=0$.

Proof. If n is even, then $\alpha^n-\beta^n\in\mathcal{O}_{\mathbb{Q}(\alpha/\beta)}$. From $p|\Phi_n(\alpha,\beta)$ and (9.2) we have $\mathfrak{p}|(\alpha^n-\beta^n)$. Assume that $\operatorname{ord}_\mathfrak{p}\alpha^2\neq0$, then we would have $\mathfrak{p}|\alpha^2$ and whence $\mathfrak{p}|\beta^2$, contradicting (9.6). Thus $\operatorname{ord}_\mathfrak{p}\alpha^2=0$. Similarly, we get $\operatorname{ord}_\mathfrak{p}\beta^2=0$.

If n is odd, then from $p|\Phi_n(\alpha,\beta)$ and (9.2) we have $\mathfrak{p}|(\alpha^{n+1}-\alpha\beta^n+\alpha^n\beta-\beta^{n+1})$ $(=\tilde{u}_n(\alpha^2-\beta^2)\in\mathcal{O}_{\mathbb{Q}(\alpha/\beta)})$. Assume that $\operatorname{ord}_\mathfrak{p}\alpha^2\neq0$, then we would have $\mathfrak{p}|\alpha^2$ and $\mathfrak{p}|\alpha\beta$ (since $\mathfrak{p}|(\alpha\beta)^2$) and whence $\mathfrak{p}|\beta^2$, contradicting (9.6). Thus $\operatorname{ord}_\mathfrak{p}\alpha^2=0$. Similarly we obtain $\operatorname{ord}_\mathfrak{p}(\beta^2)=0$.

Now $\operatorname{ord}_\mathfrak{p}(\alpha/\beta)=0$ follows from $2\operatorname{ord}_\mathfrak{p}(\alpha/\beta)=\operatorname{ord}_\mathfrak{p}(\alpha^2/\beta^2)=0$. This completes the proof of Fact 1. □

FACT 2. *If* $n>2$ *and* $p|\Phi_n(\alpha,\beta)$, *then* $\mathrm{ord}_p\,\Phi_n(\alpha,\beta)\leqslant\mathrm{ord}_{\mathfrak{p}}((\alpha/\beta)^n-1)$.

Proof. If n is even, then (9.2) and Fact 1 give

$$\mathrm{ord}_p\,\Phi_n(\alpha,\beta)\leqslant\mathrm{ord}_{\mathfrak{p}}(\alpha^n-\beta^n)=\mathrm{ord}_{\mathfrak{p}}\,\frac{\alpha^n-\beta^n}{\beta^n}=\mathrm{ord}_{\mathfrak{p}}\biggl(\biggl(\frac{\alpha}{\beta}\biggr)^n-1\biggr).$$

If n is odd, then (9.2) and Fact 1 give

$$\mathrm{ord}_p\,\Phi_n(\alpha,\beta)\leqslant\mathrm{ord}_{\mathfrak{p}}\,\frac{\alpha^n-\beta^n}{(\alpha-\beta)\beta^{n-1}}=\mathrm{ord}_{\mathfrak{p}}\,\frac{(\alpha/\beta)^n-1}{\alpha/\beta-1}\leqslant\mathrm{ord}_{\mathfrak{p}}\biggl(\biggl(\frac{\alpha}{\beta}\biggr)^n-1\biggr).$$

This completes the proof of Fact 2. □

By (9.7), (9.8) and Fact 2, we obtain, for $n>c_2=\max\{c_1,2\}$,

$$\tfrac{1}{2}\varphi(n)\log|\alpha|\leqslant\sum_{p|\Phi_n(\alpha,\beta)}\mathrm{ord}_{\mathfrak{p}}\biggl(\biggl(\frac{\alpha}{\beta}\biggr)^n-1\biggr)\log p. \tag{9.9}$$

The strategy to prove [25, Theorem 1.1] is to apply [25, Lemma 4.3] to (essentially) our inequality (9.9) and then to combine [25, Lemmas 2.1 and 2.3] to finish the proof. We see that [25, Lemma 4.3] is one of the core results of [25].

We now state [25, Lemma 4.3] and give some remarks on its proof. Suppose that α and β are complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero rational integers and such that α/β is not a root of unity and $|\alpha|\geqslant|\beta|$.

LEMMA. (Stewart [25, Lemma 4.3]) *Let* $n>1$ *be an integer*, p *be a prime with* $p\nmid\alpha\beta$ *and* $\mathfrak{p}$ *be a prime ideal of* $\mathcal{O}_{\mathbb{Q}(\alpha/\beta)}$, *lying above* p, *which does not ramify. There exists a positive number* C, *which is effectively computable in terms of* $\omega(\alpha\beta)$ *and the discriminant of* $\mathbb{Q}(\alpha/\beta)$, *such that if* $p>C$ *then*

$$\mathrm{ord}_{\mathfrak{p}}\biggl(\biggl(\frac{\alpha}{\beta}\biggr)^n-1\biggr)<p\exp\biggl(-\frac{\log p}{51.9\log\log p}\biggr)\log|\alpha|\log n. \tag{9.10}$$

We may assume henceforth, without loss of generality, that (9.6) is satisfied. Note that α/β is a zero of

$$\alpha\beta x^2-((\alpha+\beta)^2-2\alpha\beta)x+\alpha\beta\in\mathbb{Z}[x].$$

As such α/β is rational with the absolute logarithmic Weil height $h_0(\alpha/\beta)$ satisfying

$$\log 2\leqslant h_0\biggl(\frac{\alpha}{\beta}\biggr)=\frac{1}{2}h_0\biggl(\frac{\alpha^2}{\beta^2}\biggr)\leqslant\log|\alpha|,$$

or α/β is algebraic of degree 2 with

$$(\log 6)^{-3}<h_0\biggl(\frac{\alpha}{\beta}\biggr)=\frac{1}{2}\biggl(\log|\alpha\beta|+\log\biggl|\frac{\alpha}{\beta}\biggr|\biggr)=\log|\alpha|,$$

where the lower bound $(\log 6)^{-3}$ follows from [28, Corollary 1]. In the latter case, there exist $m\in\mathbb{Z}$ and $d\in\mathbb{Z}$, with $d\neq 1$ square-free, such that

$$(\alpha^2-\beta^2)^2=m^2d \quad \text{and} \quad \mathbb{Q}\left(\frac{\alpha}{\beta}\right)=\mathbb{Q}(\sqrt{d}). \tag{9.11}$$

Observe that if $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$ and $p>2$ is a prime, then p is ramified if and only if $p\mid d$. A prime $p>2$ with $p\nmid d$ splits completely in $\mathbb{Q}(\alpha/\beta)$ if the Legendre symbol (d/p) takes value 1 and is inert in $\mathbb{Q}(\alpha/\beta)$ otherwise (see [12, p. 498]).

We consider the following cases:

$$\begin{aligned} &\text{(i) } [\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=1;\\ &\text{(ii) } [\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=2, \text{ with sub-cases (ii.1) } (d/p)=1 \text{ and (ii.2) } (d/p)=-1; \end{aligned} \tag{9.12}$$

and assert that [40, Theorem 1] together with Stewart's device (see §1.1) is already sufficient for proving (9.10) with 51.9 replaced by 118.4 (or any number $>16e^2$) in case (i) and for proving (9.10) with 51.9 replaced by 236.8 (or any number $>32e^2$) in case (ii.1). However, [40] does not suffice to obtain any inequality of the quality (with respect to the dependence on p) as in (9.10) in case (ii.2).

Now we verify the above assertion. Recall that $\log^* x=\log\max\{x,e\}$ for any $x>0$. We first deduce from [40, Theorem 1] the following lemma.

Lemma 9.1. *Let K be a number field with $d=[K:\mathbb{Q}]$, $p\geqslant 5$ be a prime and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above p with ramification index $e_\mathfrak{p}=1$ and residue class degree $f_\mathfrak{p}$. We assume that*

$$\operatorname{ord}_2(p^{f_\mathfrak{p}}-1)=1 \quad or \quad \zeta_4\in K, \tag{9.13}$$

and suppose that $\alpha_1,...,\alpha_n$ are multiplicatively independent $\mathfrak{p}$-adic units in K, $b_1,...,b_n$ are rational integers, not all zero, and that B is a real number satisfying

$$B\geqslant \max\{|b_1|,...,|b_n|,3\}.$$

Then

$$\operatorname{ord}_\mathfrak{p}(\alpha_1^{b_1}...\alpha_n^{b_n}-1)<C_3(n,d,\mathfrak{p})h_0(\alpha_1)...h_0(\alpha_n)\log B,$$

where

$$C_3(n,d,\mathfrak{p})=359(n+1)^{3/2}\left(8e\frac{p-1}{p-2}\right)^n d^{n+2}(\log^* d)(\log e^4(n+1)d)\frac{p^{f_\mathfrak{p}}}{f_\mathfrak{p}\log p}\left(\frac{n}{f_\mathfrak{p}\log p}\right)^n.$$

Remark 9.2. Note that (9.13) is just $(1.5)^\clubsuit$ for the case $q=2$, i.e., $p>2$.

Proof. We apply [40, Theorem 1] for cases (III) and (IV) (see (1.35)♣). Note that for case (III), by (9.13), we have $d\geqslant 2$ and $u\geqslant 2$, and for case (IV) we have $u\geqslant 1$. Observe that

$$\begin{aligned}&\max\{\log e^4(n+1)d, e_{\mathfrak{p}}, f_{\mathfrak{p}}\log p\}\\&\qquad\leqslant(\log e^4(n+1)d)(f_{\mathfrak{p}}\log p)\max\{(f_{\mathfrak{p}}\log p)^{-1},(\log 2e^4d)^{-1}\}.\end{aligned}\tag{9.14}$$

By a formula for $\Gamma(x)$ given in Whittaker and Watson [30, p. 253], we see that

$$\frac{(n+1)^{n+2}}{n!}\leqslant\frac{1}{\sqrt{2\pi}}\,e^{n+1}(n+1)^{3/2}.\tag{9.15}$$

Now Lemma 9.1 follows from [40, Theorem 1] at once. □

We now discuss case (i). We may assume $p\nmid 6\alpha\beta$ and write $\mathfrak{p}=p\mathbb{Z}$. If $p\equiv 3 \pmod 4$, then $\operatorname{ord}_2(p^{f_{\mathfrak{p}}}-1)=1$. Thus we may work in $\mathbb{Q}$, using Lemma 9.1 with $K=\mathbb{Q}$ and, at the end, obtain (9.10) with 51.9 replaced by 59.2. We omit the details here. If $p\equiv 1 \pmod 4$, then in order to satisfy (9.13), we have to work in $K=\mathbb{Q}(\zeta_4)=\mathbb{Q}(\sqrt{-1})$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_K$ lying above $\mathfrak{p}=p\mathbb{Z}$. Then $e_{\mathfrak{P}}=f_{\mathfrak{P}}=1$, since $(-1/p)=1$. Our assumption $p\nmid 6\alpha\beta$ implies that $p\geqslant 5$ and $\operatorname{ord}_{\mathfrak{P}}(\alpha/\beta)=0$. Following [25], we introduce

$$k=\left\lfloor\frac{\log p}{118.35\log\log p}\right\rfloor$$

and see that $k\geqslant 2$ when $p>c_3$. For $j\geqslant 2$, let p_j be the $(j-1)$-th smallest prime such that

$$p_j\nmid p\alpha\beta.\tag{9.16}$$

We write

$$\frac{\alpha}{\beta}=\alpha_1p_2\ldots p_k\tag{9.17}$$

and obtain

$$\operatorname{ord}_{\mathfrak{p}}\left(\left(\frac{\alpha}{\beta}\right)^n-1\right)=\operatorname{ord}_{\mathfrak{P}}\left(\left(\frac{\alpha}{\beta}\right)^n-1\right)=\operatorname{ord}_{\mathfrak{P}}(\alpha_1^np_2^n\ldots p_k^n-1).\tag{9.18}$$

From (9.16), $p\nmid 6\alpha\beta$ and the fact that α/β is not a root of unity, we see that $\alpha_1,p_2,\ldots,p_k$ are multiplicatively independent $\mathfrak{P}$-adic units in K. An application of Lemma 9.1 to (9.18) gives

$$\operatorname{ord}_{\mathfrak{p}}\left(\left(\frac{\alpha}{\beta}\right)^n-1\right)<C_3(k,2,\mathfrak{P})h_0(\alpha_1)\log p_2\ldots\log p_k\cdot 2\log n.$$

Taking advantage of the fact that $f_{\mathfrak{P}}=1$, this ultimately leads to (9.10) with 51.9 replaced by 118.4 in case (i) (see [25] for more details).

We observe that along with the strategy of [25, §5] (namely to apply (9.10) with 51.9 replaced by 118.4 to our inequality (9.9) and then to combine [25, Lemmas 2.1 and 2.3] to finish the proof), Lemma 9.1, a consequence of [40, Theorem 1], together with Stewart's device yields (9.4) with 104 replaced by 237 in case (i), thereby proving the conjecture of Erdős from 1965.

We should emphasize here the following point. Recall that the second major improvement achieved in [40] (see p. 192♣), which is based on Loher and Masser [14], is that the product of absolute logarithmic Weil heights

$$h_0(\alpha_1)\dots h_0(\alpha_n)$$

appears in the main theorem of [40] (see (1.17)♣), in place of the product of the modified heights

$$h'(\alpha_1)\dots h'(\alpha_n) \quad \text{with } h'(\alpha_j)=\max\left\{h_0(\alpha_j), \frac{f_{\mathfrak{p}}\log p}{d}\right\}$$

in [37] and [38]. *It is this improvement which makes Stewart's device work.* By the way, we notice that the constant 118.4 can be replaced by 51.9 on the basis of the present paper.

Now we discuss case (ii.1). We may assume that

$$p\nmid 6d\alpha\beta \tag{9.19}$$

with d as in (9.11). Then $p\geqslant 5$ and from $(d/p)=1$ we deduce that $e_{\mathfrak{p}}=f_{\mathfrak{p}}=1$. If $p\equiv 3 \pmod 4$ then $\mathrm{ord}_2(p^{f_{\mathfrak{p}}}-1)=1$ and we can apply Lemma 9.1 with $K=\mathbb{Q}(\alpha/\beta)$ to obtain (9.10) with 51.9 replaced by 118.4. We omit the details here. If $p\equiv 1 \pmod 4$, then in order to satisfy (9.13), we have to work in $K=\mathbb{Q}(\alpha/\beta)(\zeta_4)$. We need only to consider the worst situation when $\zeta_4\notin\mathbb{Q}(\alpha/\beta)$ and $[K:\mathbb{Q}]=4$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_K$ lying above $\mathfrak{p}$. By the lemma in the appendix of [35], we have $e_{\mathfrak{P}}=e_{\mathfrak{p}}=1$ and $f_{\mathfrak{P}}=f_{\mathfrak{p}}=1$. Similar to our discussion in case (i), we introduce

$$k=\left\lfloor\frac{\log p}{236.7\log\log p}\right\rfloor$$

and keep (9.16) and (9.17), and we have (9.18) again. Observe that $\alpha_1, p_2, ..., p_k$ are multiplicatively independent $\mathfrak{P}$-adic units in K. An application of Lemma 9.1 with $K=\mathbb{Q}(\alpha/\beta)(\zeta_4)$ to (9.18) gives

$$\mathrm{ord}_{\mathfrak{p}}\left(\left(\frac{\alpha}{\beta}\right)^n-1\right)<C_3(k,4,\mathfrak{P})h_0(\alpha_1)(\log p_2)\dots(\log p_k)2\log n.$$

Taking advantage of the fact that $f_{\mathfrak{P}}=1$, this ultimately leads to (9.10) with 51.9 replaced by 236.8 in case (ii.1) (see [25] for more details).

Next, we discuss case (ii.2). We may assume (9.19) with d as in (9.11). Then $p\geqslant 5$ and from $(d/p)=-1$ we deduce that $e_{\mathfrak{p}}=1$ and $f_{\mathfrak{p}}=2$. In order to satisfy (9.13), we have to work in $K=\mathbb{Q}(\alpha/\beta)(\zeta_4)$, since now $\mathrm{ord}_2(p^{f_{\mathfrak{p}}}-1)\geqslant 3$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_K$ lying above $\mathfrak{p}$. By the lemma in the appendix of [35], we have $e_{\mathfrak{P}}=e_{\mathfrak{p}}=1$ and $f_{\mathfrak{P}}=f_{\mathfrak{p}}=2$. It is evident that [40, Theorem 1] (see Lemma 9.1) together with Stewart's device can just give an upper bound for $\mathrm{ord}_{\mathfrak{p}}((\alpha/\beta)^n-1)$ similar to (9.10), but with p^2 in place of p. Applied to (9.9), this cannot yield any lower bound for $P(\Phi_n(\alpha,\beta))$ that would give (9.5) in case (ii) where $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}]=2$.

Here the second refinement described in §1.1 *establishes the basis to overcome this serious problem.* While Stewart deduces for this purpose [25, Lemma 3.1] from our main theorem, we deduce Lemma 9.3 below, building on our Theorem 1 with $r=n$ (see (1.19)). Note that the deduction of Theorem 1 with $r=n$ from our main theorem utilizes the Liouville theorem (see the proof of Lemma 8.1), whence, generally speaking, Lemma 9.3 is sharper than [25, Lemma 3.1].

LEMMA 9.3. *Let K be a number field with $d=[K:\mathbb{Q}]$ and α_0 be given by* (1.4). *Let $p\geqslant 5$ be a prime and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above p with ramification index $e_{\mathfrak{p}}=1$ and residue class degree $f_{\mathfrak{p}}$. Suppose that $\alpha_1,...,\alpha_n$ are multiplicatively independent $\mathfrak{p}$-adic units in K, $b_1,...,b_n$ are rational integers, not all zero, and B is a real number satisfying*

$$B\geqslant\max\{|b_1|,...,|b_n|,5\}.$$

Then

$$\mathrm{ord}_{\mathfrak{p}}(\alpha_1^{b_1}...\alpha_n^{b_n}-1)<C_4(n,d,\mathfrak{p},\mathfrak{a})h_0(\alpha_1)...h_0(\alpha_n)\log B,$$

where

$$C_4(n,d,\mathfrak{p},\mathfrak{a})=376(n+1)^{3/2}\left(7e\frac{p-1}{p-2}\right)^n d^{n+2}(\log^* d)\log e^4(n+1)d \times\max\left\{\frac{p^{f_{\mathfrak{p}}}}{\delta(\mathfrak{a})}\left(\frac{n}{f_{\mathfrak{p}}\log p}\right)^n, e^n f_{\mathfrak{p}}\log p\right\}.$$

Remark 9.4. Observe that we do not assume (9.13). This is the benefit of the first refinement (see §1.1). Note also that (1.7) with $q=2$ implies that $\alpha_1,...,\alpha_n$ are multiplicatively independent.

Proof. We apply Theorem 1 with $r=n$ and we may take

$$c^{(1)}=1794\quad\text{and}\quad a^{(1)}=7\frac{p-1}{p-2},$$

since we are in case (III) of §1.3. Using (9.14), (9.15), $2^u\geqslant 2$ and

$$\max\{\log B, f_{\mathfrak{p}}\log p\}\leqslant\frac{f_{\mathfrak{p}}\log p}{\log 5}\log B,$$

Lemma 9.3 follows directly from Theorem 1 with $r=n$. □

Next, we reformulate [25, Lemma 2.2] for making applications more transparent.

LEMMA 9.5. *Let $d\neq 1$ be a square-free rational integer and $K=\mathbb{Q}(\sqrt{d})$. Let $\theta\in\mathcal{O}_K$ have degree 2 and let θ' denote the algebraic conjugate of θ over $\mathbb{Q}$. Suppose that p is a prime satisfying*

$$p\nmid 2dN(\theta) \quad \text{and} \quad \left(\frac{d}{p}\right)=-1,$$

where $N(\theta)=\theta\theta'$ denotes the norm of θ for $K/\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above p and $\overline{K}$ be the residue class field of K at $\mathfrak{p}$. Then the order of the residue class $\bar{\gamma}$ of $\gamma=\theta/\theta'$ in $\overline{K}^*$ divides $p+1$.

In [25] Stewart found the way, through his Lemmas 2.2 and 2.4, to apply successfully his Lemma 3.1, thereby proving his Lemma 4.3 for case (ii). We have carefully worked out a proof of his Lemma 4.3 for case (ii), where we use Lemma 9.3 in place of his Lemma 3.1 and Lemma 9.5 in place of his Lemma 2.2. In order to reduce the size of the present paper, we skip the proof. This completes our exposition.

Acknowledgments. This work was reported at the conference "Diophantine Geometry into the Millennium", Zürich, June 2-6, 2009, in honor of Prof. Gisbert Wüstholz. I would like to thank the Forschungsinstitut für Mathematik, ETH Zürich, for the invitation and hospitality. I would also like to express my sincere gratitude to the FIM at ETH-Zürich and Prof. Wüstholz for the hospitality and support during the period when a revised version of the paper was completed.

For the first refinement (see §1.1), I am in part indebted to a discussion with Prof. C. L. Stewart, during the ESI Vienna Workshop "Diophantine Approximation and Heights" in May 2006. I would like to express here my gratitude to Proff. D. W. Masser, H. P. Schlickewei and W. M. Schmidt, the organizers of the Workshop, for their invitation and to Erwin Schrödinger International Institute for Mathematical Physics for the support.

The research for this paper was done in part during visits to the University of Waterloo, Canada. I would like to express my gratitude to the University of Waterloo for the hospitality.

Most of the work in this paper was done at home since my retirement on July 1, 2006. I am very grateful to my wife Dehua Liu, son Jin Yu and daughter-in-law Yida Jiang for creating excellent working conditions, including computer environment.

References

[1] ADAMS, W. W., Transcendental numbers in the P-adic domain. *Amer. J. Math.*, 88 (1966), 279–308.

[2] BAKER, A., A sharpening of the bounds for linear forms in logarithms. *Acta Arith.*, 21 (1972), 117–129.
[3] — A sharpening of the bounds for linear forms in logarithms. II. *Acta Arith.*, 24 (1973), 33–36.
[4] — The theory of linear forms in logarithms, in *Transcendence Theory*: *Advances and Applications* (Cambridge, 1976), pp. 1–27. Academic Press, London, 1977.
[5] BAKER, A. & STARK, H. M., On a fundamental inequality in number theory. *Ann. of Math.*, 94 (1971), 190–199.
[6] BAKER, A. & WÜSTHOLZ, G., Logarithmic forms and group varieties. *J. Reine Angew. Math.*, 442 (1993), 19–62.
[7] BOMBIERI, E. & VAALER, J., On Siegel's lemma. *Invent. Math.*, 73 (1983), 11–32.
[8] — Addendum to: "On Siegel's lemma". *Invent. Math.*, 75 (1984), 377.
[9] DICKSON, L. E., *History of the Theory of Numbers.* Vol. I: *Divisibility and Primality.* Chelsea, New York, 1966.
[10] ERDŐS, P., Some recent advances and current problems in number theory, in *Lectures on Modern Mathematics*, Vol. III, pp. 196–244. Wiley, New York, 1965.
[11] FRÖHLICH, A. & TAYLOR, M. J., *Algebraic Number Theory.* Cambridge Studies in Advanced Mathematics, 27. Cambridge University Press, Cambridge, 1993.
[12] HASSE, H., *Number Theory.* Grundlehren der Mathematischen Wissenschaften, 229. Springer, Berlin–Heidelberg, 1980.
[13] LEHMER, D. H., An extended theory of Lucas' functions. *Ann. of Math.*, 31 (1930), 419–448.
[14] LOHER, T. & MASSER, D., Uniformly counting points of bounded height. *Acta Arith.*, 111 (2004), 277–297.
[15] LUCAS, E., Sur les rapports qui existent entre la théorie des nombres et le calcul intégral. *C. R. Acad. Sci. Paris*, 82 (1876), 1303–1305.
[16] — Theorie des fonctions numeriques simplement periodiques. *Amer. J. Math.*, 1 (1878), 184–240, 289–321.
[17] MAHLER, K., Über transzendente P-adische Zahlen. *Compos. Math.*, 2 (1935), 259–275.
[18] MATVEEV, E. M., An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. *Izv. Ross. Akad. Nauk Ser. Mat.*, 62 (1998), 81–136 (Russian); English translation in *Izv. Math.*, 62 (1998), 723–772.
[19] — An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.*, 64 (2000), 125–180 (Russian); English translation in *Izv. Math.*, 64 (2000), 1217–1269.
[20] VAN DER POORTEN, A. J., Linear forms in logarithms in the p-adic case, in *Transcendence Theory*: *Advances and Applications* (Cambridge, 1976), pp. 29–57. Academic Press, London, 1977.
[21] ROSSER, J. B. & SCHOENFELD, L., Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6 (1962), 64–94.
[22] SHOREY, T. N. & STEWART, C. L., On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. II. *J. London Math. Soc.*, 23 (1981), 17–23.
[23] STEWART, C. L., The greatest prime factor of a^n-b^n. *Acta Arith.*, 26 (1974/75), 427–433.
[24] — On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers. *Proc. London Math. Soc.*, 35 (1977), 425–447.
[25] — On divisors of Lucas and Lehmer numbers. *Acta Math.*, 211 (2013), 291–314.
[26] STEWART, C. L. & YU, K., On the *abc* conjecture. II. *Duke Math. J.*, 108 (2001), 169–181.
[27] TIJDEMAN, R., On the equation of Catalan. *Acta Arith.*, 29 (1976), 197–209.

[28] Voutier, P., An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74 (1996), 81–95.

[29] Waldschmidt, M., A lower bound for linear forms in logarithms. *Acta Arith.*, 37 (1980), 257–283.

[30] Whittaker, E. T. & Watson, G. N., *A Course of Modern Analysis*. Cambridge Mathematical Library. Cambridge Univ. Press, Cambridge, 1996.

[31] Wüstholz, G., A new approach to Baker's theorem on linear forms in logarithms. I, II, in *Diophantine Approximation and Transcendence Theory* (Bonn, 1985), Lecture Notes in Mathematics, 1290, pp. 189–202, 203–211. Springer, Berlin–Heidelberg, 1987.

[32] — A new approach to Baker's theorem on linear forms in logarithms. III, in *New Advances in Transcendence Theory* (Durham, 1986), pp. 399–410. Cambridge Univ. Press, Cambridge, 1988.

[33] — Multiplicity estimates on group varieties. *Ann. of Math.*, 129 (1989), 471–500.

[34] Yu, K., Linear forms in p-adic logarithms. *Acta Arith.*, 53 (1989), 107–186.

[35] — Linear forms in p-adic logarithms. II. *Compos. Math.*, 74 (1990), 15–113.

[36] — Linear forms in p-adic logarithms. III. *Compos. Math.*, 91 (1994), 241–276.

[37] — p-adic logarithmic forms and group varieties. I. *J. Reine Angew. Math.*, 502 (1998), 29–92.

[38] — p-adic logarithmic forms and group varieties. II. *Acta Arith.*, 89 (1999), 337–378.

[39] — Report on p-adic logarithmic forms, in *A Panorama of Number Theory or the View from Baker's Garden* (Zürich, 1999), pp. 11–25. Cambridge Univ. Press, Cambridge, 2002.

[40] — p-adic logarithmic forms and group varieties. III. *Forum Math.*, 19 (2007), 187–280.

Kunrui Yu
Department of Mathematics
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon
Hong Kong
People's Republic of China
makryu@ust.hk

Received June 3, 2011
Received in revised form November 8, 2012