ACTA ARITHMETICA
XVI (1970)

An effective p-adic analogue of a theorem of Thue II
The greatest prime factor of a binary form

by

J. Coates (Cambridge)

I. Introduction. In part I of this paper [4] there appeared various numbers, which, it was asserted, could be effectively determined, but which in fact were not explicitly calculated. The purpose of the present paper is to derive appropriate values for these numbers, and thereby to obtain explicit statements of the principal results of [4]. As in [4], $f(x, y)$ will signify a binary form with integer coefficients and degree $n \geqslant 3$, irreducible over the rationals, and m will signify a non-zero integer. By $p_1, \ldots, p_s$ we shall denote a set of $s \geqslant 0$ prime numbers, and we shall use $\mathfrak{m}$ to denote the largest integer, comprised solely of powers of $p_1, \ldots, p_s$, which divides m. We denote by $\mathfrak{F}$ any number not less than the maximum of the absolute values of the coefficients of $f(x, y)$, and we suppose that $\mathfrak{F} \geqslant 2$. We write P for the maximum of $p_1, \ldots, p_s$; if no primes $p_1, \ldots, p_s$ are specified, we take $P = 2$. Finally, we signify by $\varkappa$ any number satisfying $\varkappa > n(s+1)+1$. Then we shall establish the following explicit form of Theorem 1 of [4].

THEOREM 1. *All solutions of the equation $f(x, y) = m$ in integers x, y, with $(x, y, p_1 \ldots p_s) = 1$, satisfy*

$$\max(|x|, |y|) < \exp\{2^{\nu^2} P^{26n^6\nu} \mathfrak{F}^{2n^3\nu} + (\log(|m|/\mathfrak{m}))^{\varkappa}\},$$

where $\nu = 64n(s+1)\varkappa^2/(\varkappa - n(s+1)-1)$.

It will be observed that when $s = 0$, that is when no primes $p_1, \ldots, p_s$ are specified, Theorem 1 reduces to a slightly weaker form of the main result of Baker's paper [2]. On the other hand, if m is comprised solely of powers of $p_1, \ldots, p_s$ so that $|m|/\mathfrak{m} = 1$, then Theorem 1 implies that all solutions of the equation $f(x, y) = m$ in integers x, y with $(x, y, p_1 \ldots p_s) = 1$, satisfy

$$\max(|x|, |y|) < \exp\{2^{\nu^2} P^{26n^6\nu} \mathfrak{F}^{2n^3\nu}\}. \tag{1}$$

The interest of this result lies in the fact that the number on the right does not depend on the exponents to which $p_1, \ldots, p_s$ divide m. In particular, it can be used to give the following explicit lower bound for the greatest prime factor of $f(x,y)$.

THEOREM 2. *If x, y are integers with $(x,y)=1$, then the greatest prime factor of $f(x,y)$ exceeds*

$$\left(\frac{\log\log X}{(10n)^8\log\mathfrak{F}}\right)^{1/4},$$

where $X=\max(|x|,|y|)$.

Theorem 2 is the first quantitative formulation of Mahler's theorem [5] asserting that the greatest prime factor of $f(x,y)$ tends to infinity with $\max(|x|,|y|)$. In order to deduce Theorem 2 from (1), we let $\mathfrak{P}$ be either 1 or the greatest prime factor of $f(x,y)$, according as $|f(x,y)|=1$ or $|f(x,y)|>1$, and we let $p_1,\ldots,p_s$ be the primes not exceeding $\mathfrak{P}$. We apply (1) with $\varkappa=2n(s+1)+2$; then $P\leqslant 2\mathfrak{P}$, $s+1\leqslant 2\mathfrak{P}$, $\nu\leqslant 10^4n^2\mathfrak{P}^2$, and so

$$X=\max(|x|,|y|)<\exp\{2^{10^8n^4\mathfrak{P}^4}(2\mathfrak{P})^{26\cdot 10^4n^8\mathfrak{P}^2}\mathfrak{F}^{2\cdot 10^4n^5\mathfrak{P}^2}\}$$
$$<\exp\exp\{\mathfrak{P}^4(10n)^8\log\mathfrak{F}\},$$

which is equivalent to the assertion of Theorem 2.

The main part of this paper involves the detailed estimation of the various unspecified constants appearing in the proof of Theorem 1 of [4]. It will be assumed that the reader is familiar with the work of [4], and only a minimal amount of the discussion of that paper will be repeated here. We also assume that the reader is familiar with § 4 of [2]. Finally, certain auxiliary results will be required concerning the S-units of an algebraic number field, and § II is devoted to an account of their derivation.

In conclusion, I wish to express my thanks to Dr. Baker for his advice on this work.

II. S-units of algebraic number fields. The purpose of this section is to construct S-units of an algebraic number field with the properties required in § V of [4].

The construction of these units will be based upon the following generalization of Minkowski's linear form theorem, due to Mahler [6]. Let Q be the field of rational numbers, let $p_1,\ldots,p_s$ be s prime numbers, and let Q_{p_i} be the completion of Q with respect to the valuation $|\ |_{p_i}$ defined by p_i.

LEMMA 1. *Let $L_{0h}(x)=\sum_{k=1}^{n}a_{0hk}x_k$ $(1\leqslant h\leqslant n)$ be n linear forms in n unknowns with real coefficients and non-vanishing determinant d, and let $L_{ih}(x)=\sum_{k=1}^{n}a_{ihk}x_k$ $(1\leqslant i\leqslant s,1\leqslant h\leqslant n_i)$ be finitely many linear forms in the same unknowns with integral p_i-adic coefficients. If λ_h $(1\leqslant h\leqslant n)$ are positive real numbers, and f_{ih} $(1\leqslant i\leqslant s,1\leqslant h\leqslant n_i)$ non-negative integers such that*

$$(2)\qquad \Big(\prod_{h=1}^{n}\lambda_h\Big)\Big(\prod_{i=1}^{s}\prod_{h=1}^{n_i}p_i^{-f_{ih}}\Big)\geqslant|d|,$$

then there exist rational integers $x_1,\ldots,x_n$, not all 0, satisfying

$$(3)\qquad |L_{0h}(x)|\leqslant\lambda_h\ (1\leqslant h\leqslant n),\qquad |L_{ih}(x)|_{p_i}\leqslant p_i^{-f_{ih}}\ (1\leqslant i\leqslant s,1\leqslant h\leqslant n_i).$$

Proof. By hypothesis, the a_{ihk} are p_i-adic integers, and hence there exist rational integers a'_{ihk} such that $|a_{ihk}-a'_{ihk}|_{p_i}\leqslant p_i^{-f_{ih}}$. Hence, in order to establish the assertion of the lemma, it suffices to prove that there exist integers $x_1,\ldots,x_n$, not all 0, satisfying

$$(4)\qquad |L_{0h}(x)|\leqslant\lambda_h\ (1\leqslant h\leqslant n),\qquad |L'_{ih}(x)|_{p_i}\leqslant p_i^{-f_{ih}}\ (1\leqslant i\leqslant s,1\leqslant h\leqslant n_i),$$

where $L'_{ih}(x)=\sum_{k=1}^{n}a'_{ihk}x_k$. We introduce new unknowns X_{ih} $(1\leqslant i\leqslant s,1\leqslant h\leqslant n_i)$, and new linear forms $L''_{ih}(x,X)=L'_{ih}(x)+p_i^{f_{ih}}X_{ih}$. Then it is clear that (4) will be valid if we can prove that there exist integers x_k, X_{ih}, not all 0, satisfying

$$|L_{0h}(x)|\leqslant\lambda_h\ (1\leqslant h\leqslant n),\qquad |L''_{ih}(x,X)|<1\ (1\leqslant i\leqslant s,1\leqslant h\leqslant n_i).$$

Note that, for such integers x_k, X_{ih}, not all of $x_1,\ldots,x_n$ can be 0. To prove the existence of integers x_k, X_{ih} satisfying this last inequality, we observe that the linear forms $L_{0h}(x), L''_{ih}(x,X)$ have real coefficients and determinant equal to $d\prod_{i=1}^{s}\prod_{h=1}^{n_i}p_i^{f_{ih}}$, and so, by virtue of (2), the assertion follows from Minkowski's linear form theorem (cf. [3]). This completes the proof of Lemma 1.

Let α denote an algebraic integer of degree $n\geqslant 3$, and let $\alpha^{(j)}$ $(1\leqslant j\leqslant n)$ denote the conjugates of α, arranged so that $\alpha^{(1)},\ldots,\alpha^{(r)}$ are real, and $\alpha^{(r+1)},\ldots,\alpha^{(\nu_0)}$ are the complex conjugates of $\alpha^{(\nu_0+1)},\ldots,\alpha^{(n)}$, respectively. Let $\mathfrak{K}$ be the algebraic number field obtained by adjoining α to Q, and let $\theta^{(j)}$ be the conjugate of an element θ of $\mathfrak{K}$ corresponding to the conjugate $\alpha^{(j)}$ of α. By $|\ |_{\mathfrak{N}_{0j}}$ $(1\leqslant j\leqslant\nu_0)$ we signify the valuations of $\mathfrak{K}$ extending the ordinary absolute value of Q, and by $|\ |_{\mathfrak{N}_{ij}}$ $(1\leqslant i\leqslant s, 1\leqslant j\leqslant\nu_i)$ the valuations of $\mathfrak{K}$ extending the valuations $|\ |_{p_i}$ $(1\leqslant i\leqslant s)$ of Q. We denote the set of valuations $|\ |_{\mathfrak{N}_{ij}}$ $(0\leqslant i\leqslant s,1\leqslant j\leqslant\nu_i)$ by S, and let $\varrho=\sum_{i=0}^{s}\nu_i$ be the number of elements of S. We recall that an S-unit is, by definition, an element of $\mathfrak{K}$ whose valuation is equal to 1 for all valuations of $\mathfrak{K}$ not in S. In the following, we shall prove that for each valuation $|\ |_{\mathfrak{R}_{hk}}$ in S, except $|\ |_{\mathfrak{R}_{0\nu_0}}$, there exists an S-unit η_{hk} satisfying the inequalities

$$\left|\log|\eta_{hk}|_{\mathfrak{R}_{ij}}\right| \leqslant \tfrac{1}{2}\log D \quad \text{for all } \mathfrak{R}_{ij} \neq \mathfrak{R}_{hk}, \tag{5}$$

$$(\varrho-1)!\log D \leqslant \log|\eta_{hk}|_{\mathfrak{R}_{hk}} \leqslant \varrho!\, D^{(n+1)/2}\log(DP), \tag{6}$$

where P is the maximum of 2 and $p_1, \ldots, p_s$, and D is any number not less than the discriminant of α, that is $\prod_{1\leqslant i<j\leqslant n}|\alpha^{(i)}-\alpha^{(j)}|^2$.

Now let λ_j $(1\leqslant j\leqslant \nu_0-1)$ be arbitrary positive numbers, and f_{ij} $(1\leqslant i\leqslant s, 1\leqslant j\leqslant \nu_i)$ arbitrary non-negative integers. Then, if n_{ij} denotes the degree of the completion of $\mathfrak{K}$ at $|\ |_{\mathfrak{R}_{ij}}$ over the corresponding completion of Q, we put

$$\lambda_{\nu_0} = \left\{\frac{D^{1/2}\prod_{i=1}^{s}\prod_{j=1}^{\nu_i} p_i^{n_{ij}f_{ij}}}{\prod_{j=1}^{\nu_0-1}\lambda_j^{n_{0j}}}\right\}^{1/n_{0\nu_0}},$$

so that

$$\Big(\prod_{j=1}^{\nu_0}\lambda_j^{n_{0j}}\Big)\Big(\prod_{i=1}^{s}\prod_{j=1}^{\nu_i} p_i^{-n_{ij}f_{ij}}\Big) = D^{1/2}. \tag{7}$$

We first establish the existence of an algebraic integer θ in K satisfying

$$\begin{aligned} \lambda_j D^{-1/2} &\leqslant |\theta|_{\mathfrak{R}_{0j}} \leqslant \lambda_j \quad (1\leqslant j\leqslant \nu_0),\\ p_i^{-f_{ij}} D^{-1/2} &\leqslant |\theta|_{\mathfrak{R}_{ij}} \leqslant p_i^{-f_{ij}} \quad (1\leqslant i\leqslant s,\ 1\leqslant j\leqslant \nu_i). \end{aligned} \tag{8}$$

To prove this, we let $\theta = \sum_{k=1}^{n} x_k\alpha^{k-1}$, where $x_1, \ldots, x_n$ are unknown integers. We define n linear forms $L_{0j}(x)$ $(1\leqslant j\leqslant n)$ with real coefficients by

$$L_{0j}(x) = \theta^{(j)} \quad (1\leqslant j\leqslant \tau),$$

$$L_{0j}(x) = \mathscr{R}\theta^{(j)} \quad (\tau+1\leqslant j\leqslant \nu_0), \qquad L_{0j}(x) = \mathscr{I}\theta^{(j)} \quad (\nu_0+1\leqslant j\leqslant n),$$

where $\mathscr{R}\theta^{(j)}, \mathscr{I}\theta^{(j)}$ denote the real and imaginary part of $\theta^{(j)}$. Further, for each suffix i we have $n = \sum_{j=1}^{\nu_i} n_{ij}$, and so we can define n linear forms

$$L_{ijk}(x) = \sum_{l=1}^{n} x_l a_{ijkl} \quad (1\leqslant j\leqslant \nu_i,\ 1\leqslant k\leqslant n_{ij}),$$

with integral p_i-adic coefficients, where the a_{ijkl} are given by

$$\alpha^{l-1} = \sum_{k=1}^{n_{ij}} a_{ijkl}\,\omega_{ijk},$$

where $\omega_{ij1}, \ldots, \omega_{ijn_{ij}}$ denote an integral basis (cf. [8], p. 104) of the completion of $\mathfrak{K}$ at $|\ |_{\mathfrak{R}_{ij}}$ over Q_{p_i}. We now apply Lemma 1 to these linear forms, and conclude that there exist integers $x_1, \ldots, x_n$, not all 0, such that

$$|L_{0j}(x)| \leqslant \lambda_j \quad (1\leqslant j\leqslant \tau),$$

$$|L_{0j}(x)| \leqslant \lambda_j/\sqrt{2} \quad (\tau+1\leqslant j\leqslant \nu_0), \qquad |L_{0j}(x)| \leqslant \lambda_{j-\nu_0+\tau}/\sqrt{2} \quad (\nu_0+1\leqslant j\leqslant n),$$

$$|L_{ijk}(x)|_{p_i} \leqslant p_i^{-f_{ij}} \quad (1\leqslant i\leqslant s,\ 1\leqslant j\leqslant \nu_i,\ 1\leqslant k\leqslant n_{ij}).$$

This is valid, since by (7) the product of the numbers appearing as upper bounds in these inequalities is equal to $D^{1/2}2^{-(\nu_0-\tau)}$, and this is greater than or equal to the absolute value of the determinant of the n real linear forms. We conclude that, for this choice of $x_1, \ldots, x_n$, we have $|\theta|_{\mathfrak{R}_{0j}} \leqslant \lambda_j$ $(1\leqslant j\leqslant \nu_0)$ and

$$|\theta|_{\mathfrak{R}_{ij}} = \Big|\sum_{k=1}^{n_{ij}} L_{ijk}(x)\,\omega_{ijk}\Big|_{\mathfrak{R}_{ij}} \leqslant \max_k |L_{ijk}(x)|_{p_i} \leqslant p_i^{-f_{ij}} \quad (1\leqslant i\leqslant s,\ 1\leqslant j\leqslant \nu_i),$$

so that θ satisfies the upper bounds required by (8). But, as θ is a non-zero algebraic integer,

$$\prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta|_{\mathfrak{R}_{ij}}^{n_{ij}} \geqslant 1,$$

whence these upper bounds, together with (7), clearly imply the lower estimates given in (8). This completes the proof of the existence of an algebraic integer θ satisfying (8).

We now establish the existence of the S-units η_{hk}, by making appropriate choices for the λ_j and the f_{ij}. First assume that $h = 0$, and define

$$\lambda_j = 1 \quad (1\leqslant j\leqslant \nu_0-1,\ j\neq k), \qquad \lambda_k = D^{((\varrho-1)!+1)l},$$

$$f_{ij} = 0 \quad (1\leqslant i\leqslant s,\ 1\leqslant j\leqslant \nu_i),$$

where l denotes any positive integer. Let θ_{0kl} be the algebraic integer satisfying (8) with this choice of parameters. Since by (8)

$$\prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta_{0kl}|_{\mathfrak{R}_{ij}}^{n_{ij}} \leqslant D^{1/2},$$

it is clear that among the numbers θ_{0kl}, with $1\leqslant l\leqslant [D^{1/2}]^{n+1}+1$, there is at least one pair

$$\theta_{0kl'} = \sum_{j=1}^{n} x_j'\alpha^{j-1}, \qquad \theta_{0kl''} = \sum_{j=1}^{n} x_j''\alpha^{j-1},$$

with $l' > l''$, and at least one positive integer N, such that

$$\prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta_{0kl'}|_{\mathfrak{P}_{ij}}^{n_{ij}} = \prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta_{0kl''}|_{\mathfrak{P}_{ij}}^{n_{ij}} = N,$$

and $x_j' \equiv x_j'' \pmod N$ $(1 \leqslant j \leqslant n)$. We then define $\eta_{0k} = \theta_{0kl'}/\theta_{0kl''}$. Thus

$$\prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\eta_{0k}|_{\mathfrak{P}_{ij}}^{n_{ij}} = 1, \tag{9}$$

and as

$$\prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta_{0kl''}|_{\mathfrak{P}_{ij}}^{n_{ij}} = |\mathrm{Norm}\,\theta_{0kl''}|\prod_{i=1}^{s}|\mathrm{Norm}\,\theta_{0kl''}|_{p_i} = N,$$

it is plain that $N/\theta_{0kl''}$ has valuation at most 1 for every valuation of $\mathfrak{K}$ not in S. Since $(\theta_{0kl'}-\theta_{0kl''})/N$ is an algebraic integer, it follows that

$$\eta_{0k} = 1 + \frac{N}{\theta_{0kl''}}\cdot\frac{(\theta_{0kl'}-\theta_{0kl''})}{N}$$

also has valuation at most 1 for every valuation of $\mathfrak{K}$ not in S. Hence, by virtue of (9) and the product formula for the valuations of $\mathfrak{K}$ (cf. [8], p. 158), we conclude that η_{0k} is an S-unit. The estimate (5) is an immediate consequence of (8), and the estimate (6) also follows from (8) by noting that $\log|\eta_{0k}|_{\mathfrak{P}_{0k}}$ is not less than

$$\{((\varrho-1)!+1)(l'-l'')-\tfrac{1}{2}\}\log D \geqslant (\varrho-1)!\log D,$$

and cannot exceed

$$\{((\varrho-1)!+1)(l'-l'')+\tfrac{1}{2}\}\log D \leqslant \varrho!\, D^{(n+1)/2}\log(2D).$$

This completes the proof of the existence of the S-unit η_{0k}.

We next suppose that $h > 0$, and define

$$\lambda_j = 1 \ (1 \leqslant j \leqslant \nu_0 - 1), \qquad f_{hk} = \left[\frac{\log D}{\log p_h}((\varrho-1)!+1)+1\right]l,$$

with $f_{ij} = 0$ otherwise. Let θ_{hkl} be the algebraic integer satisfying (8) with this choice of parameters. Since by (8)

$$\prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta_{hkl}|_{\mathfrak{P}_{ij}}^{n_{ij}} \leqslant D^{1/2},$$

it is clear that among the numbers θ_{hkl}, with $1 \leqslant l \leqslant [D^{1/2}]^{n+1}+1$, there is at least one pair $\theta_{hkl'}, \theta_{hkl''}$ with $l' > l''$, and at least one positive integer N, such that

$$\prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta_{hkl'}|_{\mathfrak{P}_{ij}}^{n_{ij}} = \prod_{i=0}^{s}\prod_{j=1}^{\nu_i}|\theta_{hkl''}|_{\mathfrak{P}_{ij}}^{n_{ij}} = N,$$

and $x_j' \equiv x_j'' \pmod N$ $(1 \leqslant j \leqslant n)$. We then define $\eta_{hk} = \theta_{hkl'}/\theta_{hkl''}$. A similar argument to that given in the case $h = 0$ shows that η_{hk} is an S-unit, and thus it only remains to establish (5) and (6). The inequality (5) follows from (8), and it is also plain from (8) that $\log|\eta_{hk}|_{\mathfrak{P}_{hk}}$ is not less than

$$\{((\varrho-1)!+1)(l'-l'')-\tfrac{1}{2}\}\log D \geqslant (\varrho-1)!\log D,$$

and cannot exceed

$$\{((\varrho-1)!+1)(l'-l'')+\tfrac{1}{2}\}\log D + (l'-l'')\log P \leqslant \varrho!\, D^{(n+1)/2}\log(DP).$$

This completes the proof of the existence of the S-units η_{hk}.

III. On the logarithms of algebraic numbers. By arguments analogous to those employed in [2], we deduce easily that a suitable value for the number C appearing in Theorem 4 of [4] is given by

$$C^{1/\mu} = 8\max\{(\mu g)^2, 2^{\mu/2}n\delta^{-1}d^n\log(dB)\}, \tag{10}$$

where

$$B = \max\{4, p, A_1, \ldots, A_{n-1}\}, \qquad \mu = 8n\varkappa(\varkappa+n+1)/(\varkappa-n-1), \tag{11}$$

and where also it has been assumed that $\delta \leqslant 1$. This is the same as the value for C obtained in [2], except that the term A' occurring in the definition of C in [2] has been replaced by p ([1]). This latter term arises from the need to satisfy the inequality $|\xi|_p < p^{-\nu}$ (see § IV), and also the inequality $e^{-\frac{\delta}{8}H} < p^{-(\nu-2)X(Y+1)}$ occurring in the proof of Lemma 5 of [4].

The arguments confirming that H is sufficiently large for the validity of Lemmas 1 to 7 of [4], if the above value is taken for C, are slightly simpler than the corresponding arguments of [2], and so we omit them. However, it may be useful to record the following points. The values of the various constants appearing in Lemmas 1 to 7 can be assigned as follows:

$$c_1 = 2B, \quad c_2 = (2B)^{n-1}, \quad c_3 = (dB)^{2(n-1)}, \quad c_4 = (dB)^{2n},$$
$$c_5 = (2dB)^{2nd}, \quad c_6 = (dB)^{2n}, \quad c_7 = (dB)^{2nd}, \quad c_8 = 4nd\log(dB),$$
$$c_9 = 4d/2^{\varkappa}, \quad c_{10} = d/2^{\varkappa-2}, \quad c_{11} = (dB)^{2n}, \quad c_{12} = 2^{n+1}d\log c_{11}.$$

Again we have

$$h > \max\{(2\mu g)^2, 2^{\frac{1}{2}\mu+2}n\delta^{-1}d^n\log(dB)\}.$$

Also we have $H \geqslant h^{\mu}$, whence

$$H^{\frac{1}{2}(1-(n+1)\varrho)} > 16\delta^{-1}h\log H,$$

([1]) Note that our definition of d is slightly different from that given in [2].

and $k^{s/2} \geqslant c_8/c_9$; these inequalities are used in the discussion of Lemma 4. The contradiction at the end of § IV is established by means of

$$hk^{\frac{1}{2}s(\tau-1)+1-n} \geqslant c_{12}/c_{10}.$$

To estimate the value of the number C appearing in Theorem 3 of [4], we first note that, if $\alpha_1, \ldots, \alpha_n$ satisfy the condition (7) of [4], then one can take

$$C^{1/\mu} = 2^{1/2\mu+3} n\delta^{-1} d^n \log(dB). \tag{12}$$

This follows at once from the value of C given above and remarks of the kind occurring at the end of § 4 of [2]. It remains to obtain an appropriate value for C when the condition (5) of [4] is satisfied in place of (7). Following the discussion of § III of [4], we see that, provided $H \geqslant 2\delta^{-1}\log \Xi$, we can apply Theorem 3 with $\alpha_1, \ldots, \alpha_n$ replaced by $\alpha_1'', \ldots, \alpha_n''$, where $\alpha_j'' = (\alpha_j \pi^{-\sigma_j})^q$, δ replaced by $\delta/2$, and with $\varkappa$ replaced by $\varkappa' = \frac{1}{2}(\varkappa+n+1)$. We conclude from (12) that $H < \max\big(C'', (\log A'')^{\varkappa'}\big)$, where

$$A'' = A_n'', \qquad B'' = \max\{4, p, A_1'', \ldots, A_{n-1}''\},$$

$$\mu'' = 8n\varkappa'(\varkappa'+n+1)/(\varkappa'-n-1), \qquad C''^{1/\mu''} = 2^{1/2\mu''+4} n\delta^{-1} d^n \log(dB'').$$

Now clearly $\mu'' \leqslant 2\mu$. We shall prove below that

$$\log(dA_j'') \leqslant p^{25d^2} \max\{\log A_j, \log\Theta \log\Xi\} \quad (1 \leqslant j \leqslant n), \tag{13}$$

provided that $\Xi \geqslant 3$, and where $\Theta \geqslant 3$ now denotes any number exceeding the maximum of the absolute values of the conjugates of θ. It is also now assumed that θ is an algebraic integer. This gives

$$H < \max\big(C, (\log A'')^{\varkappa'}\big),$$

where

$$C^{1/2\mu} = 2^{\mu+4} n\delta^{-1} d^n p^{25d^2} \log B, \qquad \mu = 8n\varkappa(\varkappa+n+1)/(\varkappa-n-1) \tag{14}$$

and $B = \max(A_1, \ldots, A_{n-1}, \Theta^{\log\Xi})$. On distinguishing two cases according as $\log A \leqslant \log\Theta \log\Xi$ or $\log A > \log\Theta\log\Xi$, it is readily seen that the conclusion of Theorem 3 is valid with the value of C given by (14).

To establish (13), we recall that, by (5) of [4], we have $|\sigma_j| \leqslant \dfrac{d\log\Xi}{\log p}$ $(1 \leqslant j \leqslant n)$. Further by [8], p. 151, we see that

$$q \leqslant (N\mathfrak{p})^{(r+1)\operatorname{ord}_\mathfrak{p} p} \leqslant p^{21 d f_\mathfrak{p} \operatorname{ord}_\mathfrak{p} p} \leqslant p^{21d^2};$$

the last inequality is true by virtue of the fact that $f_\mathfrak{p} \operatorname{ord}_\mathfrak{p} p \leqslant d$. Furthermore, π is given by one of the elements of an integral basis $\omega_1, \ldots, \omega_d$ of $\mathfrak{p}$, and, if

$$D = \prod_{1 \leqslant i < j \leqslant d} |\theta^{(i)} - \theta^{(j)}|^2,$$

then one can take

$$\omega_j = c_{j1}\cdot 1/D + \ldots + c_{j,j-1}\theta^{j-2}/D + c_{jj}\theta^{j-1}/D \quad (1 \leqslant j \leqslant d),$$

where the c_{jk} are integers satisfying $0 \leqslant c_{jk} \leqslant pD$. For the ideal $\mathfrak{p}$ is a sublattice of the lattice with basis θ^{j-1}/D $(1 \leqslant j \leqslant d)$, and, on the other hand $pD\cdot\theta^{j-1}/D$ $(1 \leqslant j \leqslant d)$ belongs to $\mathfrak{p}$, whence the assertion follows by Minkowski's adaption argument (cf. [8], p. 144). Thus we have

$$|\pi^{(j)}| \leqslant p\Theta^d \leqslant p^{3d\log\Theta} \quad (1 \leqslant j \leqslant d).$$

If $\sigma_j > 0$, $b = |\pi^{(1)} \ldots \pi^{(d)}|$, and a_j denotes the leading coefficient of the minimal polynomials of α_j, then clearly the minimal polynomial of α_j'' divides the polynomial

$$a_j^{qd} b^{\sigma_j q d} \prod_{i=1}^{d} \big(x - \alpha_j^{(i)q}/\pi^{(i)\sigma_j q}\big).$$

Since $|a\alpha_j^{(i)}| \leqslant dA_j$ (cf. [1], p. 178), and $|b/\pi^{(i)}| \leqslant p^{3d^2\log\Theta}$, the inequality (13) follows at once. A similar argument establishes (13) when $\sigma_j \leqslant 0$.

IV. Proof of Theorem 1. We now use the results obtained in § II and § III to establish Theorem 1. It will be assumed that the reader is familiar with § V of [4], on which the discussion will be based.

In the following we shall suppose that the coefficient of x^n in $f(x, y)$ is equal to 1, and we shall establish a slightly different form of Theorem 1 involving $\varkappa' = \frac{1}{2}\big(\varkappa+n(s+1)+1\big)$ rather than $\varkappa$. We shall subsequently verify that this implies Theorem 1.

The number field $\mathfrak{K}$ appearing in § II of the present paper is now taken to be the number field $\mathfrak{K}$ of § V of [4], and in both cases S denotes the set of valuations of $\mathfrak{K}$ extending the valuations $|\ |, |\ |_{p_1}, \ldots, |\ |_{p_s}$ of Q. If we assume, as we may, that $|\ |_{\mathfrak{P}_\varrho}$ is the archimedean valuation denoted by $|\ |_{\mathfrak{P}_{0\nu_0}}$ in § II, then we can take $\eta_1, \ldots, \eta_{\varrho-1}$ to be the units η_{hk} whose existence was proven in § II.

We shall not specify C_1 explicitly, but shall instead employ (5) and (6) directly at the point where C_1 becomes significant. C_2 can obviously be taken as the number on the extreme right of (6). Further, as is remarked in § 5 of [2], a suitable choice for D is given by $n^{5n}\mathfrak{F}^{2n-2}$.

We now come to the main argument of § V of [4]. Recalling that $\sigma = s+1$ and $\varrho \leqslant n\sigma$, it is clear that an appropriate value for C_3 is $\frac{1}{2}(n\sigma)^2 C_2$. We do not specify C_4, but use a direct argument later. In order to determine C_5, we observe that, by virtue of (5) and (6), the same reasoning as given in § 5 of [2] shows that

$$|\Delta| \geqslant \tfrac{1}{2}\mathfrak{P}, \quad |\Delta_{jk}| \leqslant \big((\varrho-1)\log D\big)^{-1}\mathfrak{P},$$

where $\mathfrak{P} = \prod_{k=1}^{\varrho-1} \log|\eta_k|_{\mathfrak{N}_k}$; and Δ_{jk} denotes the cofactor of the element in the jth row and kth column of the determinant Δ. It is therefore plain that we can take $C_5 = \frac{1}{2}\log D$.

The most important part of the argument is to apply the explicit forms of Theorem 3 of [1] and Theorem 3 of [4] to establish the inequality

$$(15) \qquad H < \max\{C', (\log A)^{\varkappa'}\},$$

where $\varkappa' = \frac{1}{2}(\varkappa + n\sigma + 1)$, and

$$\mu' = 8n\sigma\varkappa'(\varkappa' + n\sigma + 1)/(\varkappa' - n\sigma - 1), \qquad A = (e^{(n\sigma)^3 C_2}|m|/\mathfrak{m})^{n^4},$$

$$C' = \{2^{\mu'}(n\sigma)^{4n\sigma}P^{25n^6}\mathfrak{F}C_2\}^{2\mu'}.$$

We proceed to do this by obtaining estimates for the various numbers occurring in these theorems.

We can evidently assume that $H > n^2\sigma\log P + C_3$. It follows that we can take C_6 to be 1. Suitable values for C_7 and C_8 are given by e^{3C_3} and $\dfrac{1}{2n\sigma}\log D$; for, since $\alpha_i^{(k)} - \alpha_i^{(j)}$ is an algebraic integer of degree at most n^2, we deduce from (4) of [4] that $|\alpha_i^{(k)} - \alpha_i^{(j)}|_{r_i}$ is at least $(2n\mathfrak{F})^{-n^2+1}$ or $(2n\mathfrak{F})^{-n^2}$ according as $i = 1$ or $i > 1$, whence

$$(16) \qquad \left|\frac{\alpha_i^{(k)} - \alpha_i^{(h)}}{\alpha_i^{(k)} - \alpha_i^{(j)}}\right|_{r_i} \leqslant (2n\mathfrak{F})^{n^2} < e^{C_3/2},$$

and the assertion follows. We also conclude from (16) that we can choose $C_{10} = C_{11} = e^{3C_3}$. Estimates for the heights of $\alpha_1, \ldots, \alpha_\varrho$ are provided by the following lemma.

LEMMA 2. *The height of α_g $(1 \leqslant g \leqslant \varrho - 1)$ is at most $e^{3n^2\sigma C_2}$, and the height of α_ϱ is at most $A = (e^{(n\sigma)^3 C_2}|m|/\mathfrak{m})^{n^4}$.*

Proof. Noting that each conjugate of $\alpha_g = \eta_{gi}^{(k)}/\eta_{gi}^{(h)}$ $(1 \leqslant g \leqslant \varrho - 1)$ in Ω_{r_l} $(1 \leqslant l \leqslant \sigma)$ has valuation at most e^{2C_2}, and that α_g has degree at most n^2, we conclude, by the same argument as that used to estimate the height of γ in [4], that α_g has height at most $2^{n^2}e^{2n^2\sigma C_2} < e^{3n^2\sigma C_2}$. This establishes the first assertion of the lemma. Next let K be the number field obtained by adjoining $\alpha_i^{(h)}, \alpha_i^{(j)}, \alpha_i^{(k)}$ to Q. It is clear that K has degree $d \leqslant n^3$, and that α_ϱ belongs to K. Hence the roots of the minimal polynomial of α_ϱ in Ω_{r_1} will be a subset of the field conjugates $\alpha_\varrho^{(1)}, \ldots, \alpha_\varrho^{(d)}$ of α_ϱ in Ω_{r_1}. Further, if we now write d' for the symbol d occurring in the estimation of the height of γ in § V of [4], and put

$$a = d'|\gamma_1^{(1)} \ldots \gamma_1^{(n)}|, \qquad b = \prod_{1 \leqslant j < l \leqslant n} |\alpha_1^{(j)} - \alpha_1^{(l)}|^2,$$

it is easily seen that $d'ab\alpha_\varrho$ is an algebraic integer. It follows that the minimal polynomial of α_ϱ divides the polynomial

$$(d'ab)^d \prod_{l=1}^{d} (x - \alpha_\varrho^{(l)}).$$

In addition, by (43) and (47) of [4], we have

$$\max\{|ad'|, |ad'\vartheta|\} \leqslant e^{2n\sigma C_3}\varphi^{2n\sigma}, \qquad \max\{b, |b\vartheta'|\} \leqslant (2n\mathfrak{F})^{n^2},$$

where ϑ, ϑ' denote arbitrary conjugates of $\gamma_i^{(k)}/\gamma_i^{(h)}$, $(\alpha_i^{(h)} - \alpha_i^{(j)})/(\alpha_i^{(k)} - \alpha_i^{(j)})$ in Ω_{r_1}. Hence the height A of α_ϱ satisfies the inequality

$$\log A \leqslant \log\left(2^{n^3}(2n\mathfrak{F})^{n^5}e^{2n^4\sigma C_3}\varphi^{2n^4\sigma}\right) \leqslant n^4\log(e^{(n\sigma)^3 C_2}|m|/\mathfrak{m}),$$

as required. This completes the proof of Lemma 2.

We can now apply Theorem 3 of [4] and Theorem 3 of [1] to obtain (15). The argument divides into two cases, according as $i > 1$ or $i = 1$. In both cases it is clear from the explicit values for C_7 and C_8 that we can assume $C_7\varphi^{n/(n-1)}e^{-\frac{C_8}{2}H} \leqslant 1$; for if this inequality does not hold, (15) is certainly valid.

Suppose first that $i > 1$. To obtain better estimates, we let K be, as in Lemma 2, the number field generated by $\alpha_i^{(h)}, \alpha_i^{(j)}, \alpha_i^{(k)}$ over Q; the remarks made in § V of [4] evidently continue to hold with this modified definition. In order to apply Theorem 3 of [4], we must construct an algebraic integer θ which generates K over Q. This can be done by first observing that there is at least one integer l, with $1 \leqslant l \leqslant n^2$, such that all of the numbers

$$\alpha_i^{(\lambda)} + l\alpha_i^{(\tau)} \qquad (1 \leqslant \lambda \leqslant n, 1 \leqslant \tau \leqslant n)$$

are distinct from $\alpha' = \alpha_i^{(h)} + l\alpha_i^{(j)}$, except when $\lambda = h, \tau = j$. For such a choice of l, it is well known (cf. [7], p. 126) that α' generates the field obtained by adjoining $\alpha_i^{(h)}, \alpha_i^{(j)}$ to Q. Repeating this argument with $\alpha', \alpha_i^{(k)}$ instead of $\alpha_i^{(h)}, \alpha_i^{(j)}$, we conclude that K is generated over Q by an algebraic integer θ with the maximum of the absolute values of its conjugates at most $n^5\mathfrak{F}$. It is now clear that we can apply Theorem 3 of [4], with the following values for the quantities appearing in the theorem

$$\varkappa' = \tfrac{1}{2}(\varkappa + n\sigma + 1), \quad \delta = 1/\sigma, \quad \Xi = e^{3C_3}, \quad \varrho \leqslant n\sigma, \quad d \leqslant n^3, \quad \Theta \leqslant n^5\mathfrak{F}.$$

Noting the upper bounds for $A_1, \ldots, A_{\varrho-1}, A$ given in Lemma 2, we see that (15) is an immediate consequence of Theorem 3 and the explicit value (14) for the number C appearing in it, which was derived in § III.

Suppose next that $i = 1$. Then we can plainly apply Theorem 3 of [1], with the following values for the quantities appearing in the theorem

$$\varkappa' = \tfrac{1}{2}(\varkappa + n\sigma + 1), \quad \delta = 1/\sigma, \quad A' = e^{3C_3}, \quad d \leqslant n^3;$$

recall also that $\varrho \leqslant n\sigma$ or $\varrho \leqslant n\sigma - 1$, according as $a_1, \ldots, a_\varrho$ are or are not all real. Again noting the upper bounds for $A_1, \ldots, A_{\varrho-1}$, A given in Lemma 2, we see that (15) follows directly from Theorem 3 and the explicit value for the number C appearing in it, which was derived in § 4 of [2]. This completes the proof of the inequality (15).

Having established (15), the rest of the proof follows easily. As in § V of [4], we have, assuming $H \geqslant 1$,

$$|\beta_i^{(j)}|_{r_i} \leqslant \varphi e^{C_3 + n\sigma C_2 H} < \varphi e^{(n\sigma)^2 C_2 H} \quad (1 \leqslant i \leqslant \sigma,\ 1 \leqslant j \leqslant n),$$

whence, by a similar argument to that used in deriving (16), we conclude that

$$\max(|x'|_{r_i}, |y'|_{r_i}) < 2(2n\mathfrak{F})^{n^2} \varphi e^{(n\sigma)^2 C_2 H} \quad (1 \leqslant i \leqslant \sigma).$$

Hence we have

$$\max(|x|, |y|) < \varphi^\sigma e^{(n\sigma)^3 C_2 H}. \tag{17}$$

We simply substitute the upper bound for H, given by (15), into this inequality.

Suppose first that $(\log A)^{\varkappa'} \leqslant C'$. In particular, this implies that $|m|/\mathfrak{m} \leqslant e^{C'}$, whence it follows from (15) and (17) that

$$\max(|x|, |y|) < e^{2(n\sigma)^3 C_2 C'}.$$

Defining $\nu' = 32 n\sigma\varkappa'^2/(\varkappa' - n\sigma - 1)$, and observing that $\nu' - 2\mu' \geqslant 1$, we deduce that

$$\log\max(|x|, |y|) < \{2^{\nu'/2}(4\sigma)^{4n\sigma} P^{25n^6} \mathfrak{F} C_2\}^{\nu'}.$$

Since C_2 is given by the number on the extreme right of (6), and $D = n^{5n}\mathfrak{F}^{2n-2}$, it is readily verified that

$$\mathfrak{F} C_2 \leqslant (n\sigma)^{n\sigma} n^{6n^2} \mathfrak{F}^{2n^2} P. \tag{18}$$

Hence, as $\nu'/2 \geqslant 64(n\sigma)^2$, we obtain

$$\log\max(|x|, |y|) < \tfrac{1}{2} 2^{\nu'^2} P^{26n^6\nu'} \mathfrak{F}^{2n^2\nu'}. \tag{19}$$

On the other hand, if $(\log A)^{\varkappa'} > C'$, then $e^{(n\sigma)^3 C_2} \leqslant |m|/\mathfrak{m}$, and we conclude from (15) and (17) that

$$\max(|x|, |y|) < \varphi^\sigma \exp\{(n\sigma)^3 C_2 (2n^4 \log(|m|/\mathfrak{m}))^{\varkappa'}\}.$$

Thus, noting that C_2 is bounded above by the number on the right of (18), we obtain

$$\log\max(|x|, |y|) < \Gamma' (\log(|m|/\mathfrak{m}))^{\varkappa'}, \tag{20}$$

where $\Gamma' = n^{5\varkappa'}(n\sigma)^{2n\sigma} n^{6n^2} \mathfrak{F}^{2n^2} P$.

The estimates (19) and (20) have been established under the hypothesis that the coefficient of x^n in $f(x, y)$ is equal to 1. We now show that these estimates imply the conclusion of Theorem 1, whether this hypothesis holds or not ([2]). We follow the argument given at the beginning of § V of [4]. Let $m^* = |a^{n-1}m/b^n|$, and let $\mathfrak{m}^*$ be the largest product of powers of $p_1, \ldots, p_s$ which divides m^*. Since b^n is comprised solely of powers of $p_1, \ldots, p_s$, it is clear that $m^*/\mathfrak{m}^*$ is equal to the quotient of $|a^{n-1}m|$ and the largest product of powers of $p_1, \ldots, p_s$ which divides $|a^{n-1}m|$. Hence

$$m^*/\mathfrak{m}^* \leqslant |a^{n-1}m|/\mathfrak{m} \leqslant \mathfrak{F}^{n-1}|m|/\mathfrak{m}.$$

Now apply the known results (19) and (20) to $F(X, Y)$. As the coefficients of $F(X, Y)$ have absolute value at most $\mathfrak{F}^n$, b has absolute value at most $\mathfrak{F}$, and $\nu' \leqslant \nu$, it follows that either

$$\max(|x|, |y|) \leqslant |b| \max\left(\left|\frac{X}{b}\right|, \left|\frac{Y}{b}\right|\right) < \exp\{2^{\nu^2} p^{26n^6\nu} \mathfrak{F}^{2n^3\nu}\},$$

in which case the conclusion of Theorem 1 is valid, or

$$\max(|x|, |y|) \leqslant |b| \max\left(\left|\frac{X}{b}\right|, \left|\frac{Y}{b}\right|\right) < \exp\{\tfrac{1}{2}\Gamma(\log(\mathfrak{F}^{n-1}|m|/\mathfrak{m}))^{\varkappa'}\},$$

where $\Gamma = n^{6\varkappa}(n\sigma)^{2n\sigma} n^{6n^2} \mathfrak{F}^{2n^3} P$. If, in the latter case, we have $|m|/\mathfrak{m} \leqslant \mathfrak{F}^{n-1}$, then Theorem 1 is plainly valid. On the other hand, if $|m|/\mathfrak{m} > \mathfrak{F}^{n-1}$, we obtain

$$\max(|x|, |y|) < \exp\{\Gamma(\log(|m|/\mathfrak{m}))^{\varkappa'}\}.$$

By considering the possibilities $(\log(|m|/\mathfrak{m}))^{\varkappa-\varkappa'} > \Gamma$, $(\log(|m|/\mathfrak{m}))^{\varkappa-\varkappa'} \leqslant \Gamma$ it is then readily verified that the assertion of Theorem 1 holds.

This completes the proof of Theorem 1.

([2]) It seems to have been assumed in the corresponding deduction on p. 205 of [2] that ν increases with $\varkappa$; this, however is true only when $\varkappa > 2(n+1)$. The argument at this point would be valid for all $\varkappa$ if an extra factor 2 were included in the definition of ν, but the extra factor can easily be avoided by observing that, if we replace m by $M = m|a|^{n-1}$ on p. 206 of [2], then the bound asserted on p. 207 is unaltered.

References

[1] A. Baker, *Contributions to the theory of Diophantine equations I. On the representation of integers by binary forms*, Phil. Trans. Royal Soc. London, Series A, 263 (1968), pp. 173–191.

[2] — *II. The Diophantine equation $y^2 = x^3 + k$*, Phil. Trans. Royal Soc. London, Series A, 263 (1968), pp. 193–208.

[3] J. W. S. Cassels, *An introduction to the geometry of numbers*, Berlin 1959.

[4] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), pp. 279–305.

[5] K. Mahler, *Zur Approximation algebraischer Zahlen I*, Math. Ann. 107 (19 3), pp. 691–730.

[6] — *Ueber die Approximation P-adischer Zahlen*, Jber. Deutsche Math. Ver., (1934), pp. 250–255.

[7] B. van der Waerden, *Modern Algebra*, New York 1953, revised English edition.

[8] H. Weyl, *Algebraic theory of numbers*, Ann. of Math. Studies 1 (Princeton, 1940).

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
Cambridge, England

Reçu par la Rédaction le 2. 5. 1969

ACTA ARITHMETICA
XVI (1970)

Dirichlet's theorem on diophantine approximation. II

by

H. Davenport † and W. M. Schmidt* (Boulder, Colo.)

1. Introduction. We shall be interested in simultaneous approximation to n real numbers $a_1, \ldots, a_n$. There are two forms of Dirichlet's theorem:

(a) *For any positive integer N there exist integers $x_1, \ldots, x_n, y$ not all zero, satisfying*

$$|a_1x_1 + \ldots + a_nx_n + y| < N^{-n}, \quad \max(|x_1|, \ldots, |x_n|) \leqslant N. \tag{1a}$$

(b) *For any positive integer N there exist integers $x_1, \ldots, x_n, y$, not all zero, with*

$$\max(|a_1y - x_1|, \ldots, |a_ny - x_n|) < N^{-1}, \quad |y| \leqslant N^n. \tag{1b}$$

For particular $a_1, \ldots, a_n$ we shall say that (a) can be improved if there exists a $\mu = \mu(a_1, \ldots, a_n) < 1$ such that, for every sufficiently large N, the inequalities (1a) may be replaced by

$$|a_1x_1 + \ldots + a_nx_n + y| < \mu N^{-n}, \quad \max(|x_1|, \ldots, |x_n|) < \mu N. \tag{2a}$$

We shall say that (b) can be improved if there exists a $\mu < 1$ such that, for every sufficiently large N, the inequalities (1b) may be replaced by

$$\max(|a_1y - x_1|, \ldots, |a_ny - x_n|) < \mu N^{-1}, \quad |y| < \mu N^n. \tag{2b}$$

One main theorem is as follows.

THEOREM 1. *For almost every n-tuple $(a_1, \ldots, a_n)$, neither form (a) nor form (b) of Dirichlet's theorem can be improved.*

In this theorem *almost every* is used in the sense of n-dimensional Lebesgue measure. This theorem was announced in the first paper [2] of this series. Khintchine [4] showed that for almost every $(a_1, \ldots, a_n)$ there exists a $\mu = \mu^*(a_1, \ldots, a_n)$ such that (1a) may not be replaced by (2a), and (1b) may not be replaced by (2b). Thus for almost all $(a_1, \ldots, a_n)$,

* The second author was partially supported by NSF-GP-6515.