ACTA ARITHMETICA
XXXIII (1977)

Conspectus materiae tomi XXXIII, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

Effectively computable bounds for the solutions of certain diophantine equations

by

ALFRED J. VAN DER POORTEN (Kensington, NSW)

1. Introduction. It is the purpose of this note to establish the existence of effectively computable bounds for the size of the solutions of certain diophantine equations. Thereby, in principle, we obtain an algorithm for obtaining all solutions of these diophantine equations, since only boundedly many possibilities remain to be checked. In practice, the bounds one obtains are far too large for it to be feasible to actually check the remaining cases, and in this paper we make no attempt either to compute bounds or to optimise the bounds our proofs might produce.

Recently, Tijdeman [12] employing a refined form of an inequality of Baker on linear forms in logarithms [3] established the existence of an effectively computable bound for the solutions of Catalan's equation. Tijdeman's argument is completed by an earlier result of Baker on the so-called hyperelliptic equation [2] which itself depends on a generalisation of Baker's work on Thue's equation [1].

It is our principal object to prove a p-adic generalisation of Tijdeman's result on Catalan's equation. Accordingly it is shown that:

THEOREM 1. *Let S be a finite set of distinct positive prime integers, $S = \{p_1, \ldots, p_s\}$, and denote by (x, y) the* gcd *of integers x, y, and by $\{u, v\}$ the* lcm *of integers u, v. Then there is an effectively computable constant $C > 0$ depending only on the set S, such that all rational integer solutions $x > 1$, $y > 1$, $u > 1$, $v > 1$, $w_1, \ldots, w_s$, excluding the case $u = v = 2$, and assuming $(x, y) = 1$, of the equation*

$$x^u - y^v = (p_1^{w_1} \ldots p_s^{w_s})^{\{u,v\}}$$

are bounded by C.

We denote by K an algebraic number field with degree d, and by $\theta_1, \ldots, \theta_t$ algebraic integers of K which are non-units, and which belong to the finite set $T = \{\theta_1, \ldots, \theta_t\}$. If x, z are integers of K then $(x, z) = 1$ denotes that x and z are relatively prime; equivalently, the ideal generated by x and z is the ring of integers of K.

In order to deal with the case $u = v$ of Theorem 1 we prove the following result. It is considerably more general than is required for Theorem 1 but this generality has some intrinsic interest.

THEOREM 2. *Let α, β, and $\gamma \neq 0$ be integers of K. Then there is an effectively computable constant $C' > 0$ depending only on α, β, γ, the field K and the set T, such that if $u > 2$, $w_1 \geqslant 0, \ldots, w_t \geqslant 0$ be rational integers, and x, y, z be algebraic integers of K such that $(x, z) = (y, z) = 1$, satisfying the equation*

$$\alpha x^u - \beta y^u = \gamma z, \quad \text{where} \quad z = \theta_1^{w_1} \ldots \theta_t^{w_t},$$

then $u, w_1, \ldots, w_t$ and all conjugates of x, y, z are bounded by C'.

There are a number of interesting implications of this result; I am indebted to T. N. Shorey for bringing these to my attention. For example, denote by $P[Z]$ the greatest prime factor of the rational integer Z. Then we have the corollary.

COROLLARY. *Let a, b be non-zero rational integers and let m, n be positive integers satisfying $mn > 2(m, n)$. Then for $X, Y \in \mathbf{Z}$, (X, Y) bounded,*

$$P[aX^m + bY^n] \to \infty \quad \text{as} \quad \max(|X|, |Y|) \to \infty.$$

To see this, write $m/(m, n) = m'$, $n/(m, n) = n'$ and $u = m'n'(m, n)$. Then the theorem implies that if $x^{n'}, y^{m'} \in \mathbf{Z}$ and $ax^u + by^u$ is a rational integer composed of some nominated finite set S of rational primes, then $|x|, |y|$ are bounded by a constant depending only on S, m' and n'. The assertion of the corollary is then immediate, and, indeed it is sufficient to require only that m', n' be bounded in which case one even has

$$P[aX^m + bY^n] \to \infty \quad \text{as} \quad \max\big(|X|, |Y|, (m, n)\big) \to \infty.$$

As stated, the corollary is a result of Mahler [8]; it is however an easy matter to give an explicit lower bound for $P[aX^m + bY^n]$ in view of the effective nature of our argument, and this effective aspect of the result is new.

I am very much indebted to discussion with John Coates, in conversation with whom the idea of writing this note arose. The ideas of Alan Baker [1], [2], and Rob Tijdeman [12] are basic to this paper, and I was materially assisted by lectures given by Alan Baker at Cambridge University in Lent term, 1975. I am grateful for some helpful remarks of Cameron Stewart. This paper was written whilst the author was on study leave from the University of New South Wales, at the Department of Pure Mathematics and Mathematical Statistics of the University of Cambridge.

2. Preliminaries and remarks. Our proofs depend on the following two results, which refine results of Coates [6], and Baker [4] (see also Tijdeman [12], Theorem 2), and a result of Sprindžuk and Kotov [11].

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with degrees at most d and heights respectively at most $A_1, \ldots, A_n$ (all $A_j \geqslant 4$). Write

$$\Omega' = (\log A_1) \ldots (\log A_{n-1}), \quad A = A_n.$$

Denote by $\mathfrak{p}$ a prime ideal of the field $K = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ and suppose that $\mathfrak{p}$ divides the rational prime p; assume the usual normalisation of the valuation.

THEOREM A. *For some effectively computable number $C_p > 0$ depending only on p, n and d (and $\operatorname{ord}_{\mathfrak{p}} b_n$) the inequalities*

$$0 < |\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1|_{\mathfrak{p}} < \exp(-C_p \Omega' \log \Omega' \log A \log B)$$

have no solutions in rational integers $b_1, \ldots, b_n$ with absolute values at most B ($\geqslant 4$).

For a proof see [9], Theorem 1. One similarly shows that, [9], Theorem 2,

THEOREM B. *For some effectively computable number $C_\infty > 0$ depending only on n and d (and the determination of the logarithms) the inequalities*

$$0 < |b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n| < \exp(-C_\infty \Omega' \log \Omega' \log A \log B)$$

have no solutions in rational integers $b_1, \ldots, b_n$ with absolute values at most B ($\geqslant 4$).

Other than in Section 3 weaker results would suffice. In Section 5, Baker [3], and a p-adic equivalent would be sufficient, whilst in Section 3, Theorem B could of course be replaced by Tijdeman [12], Theorem 2.

In proving Theorem 1 our principal argument (Section 3) will show that if v is odd, and $u \neq v$ then the exponents u, v are bounded by an effectively computable constant. Subsequently (Section 5) we show, *inter alia*, that if $v = u$ then, similarly, u is so bounded, and (Section 6) that if $v = 2$ then u is again bounded. Thus our argument reduces the equation of Theorem 1 to finitely many equations of the shape $x^m - y^n = p_1^{w_1} \ldots p_s^{w_s}$ (and there is a similar reduction in the case of Theorem 2). To deal with these equations the following result suffices:

THEOREM C. *Let $\alpha_0 \neq 0$, $\alpha_0\alpha_1, \ldots, \alpha_0\alpha_n$ be integers of K and denote by f the polynomial $f(X) = \alpha_0(X - \alpha_1) \ldots (X - \alpha_n)$. We suppose that if the rational integer m satisfies $m > 2$ then f has at least 2 simple zeros and if $m = 2$ then f has at least 3 simple zeros. Then there is an effectively computable constant $C''' > 0$ depending only on the polynomial f, the field K, the set T, and the integer $m \geqslant 2$, such that if $w_1 \geqslant 0, \ldots, w_t \geqslant 0$ be rational integers, and x, y, z be algebraic integers of K such that $(x, z) = 1$, satis-*

fying the equation

$$y^m = a_0(x-\alpha_1 z)\dots(x-\alpha_n z), \quad \text{where} \quad z = \theta_1^{w_1}\dots\theta_t^{w_t},$$

then $w_1, \dots, w_t$ and all conjugates of x, y, z are bounded by C'''.

Theorem C is easily deduced from a result of Sprindžuk and Kotov [11] by, for example, the method described in Baker [2] and the obvious changes necessary for p-adic case. For completeness we mention an appropriate formulation of the required form of the Thue–Mahler theorem as proved [11] (see also Kotov [7]):

THEOREM D. *Let $\alpha_1, \dots, \alpha_n$, where $n \geqslant 3$, be distinct integers of K and denote by δ, where $\delta \neq 0$, an integer of K. Then there is an effectively computable constant $C'' > 0$ depending only on $\alpha_1, \dots, \alpha_n$, δ, the field K, and the set T, such that if $w_1 \geqslant 0, \dots, w_t \geqslant 0$ be rational integers, and x, y, z be algebraic integers of K such that $(x, z) = (y, z) = 1$, satisfying the equation*

$$(x-\alpha_1 y)\dots(x-\alpha_n y) = \delta z, \quad \text{where} \quad z = \theta_1^{w_1}\dots\theta_t^{w_t},$$

then $w_1, \dots, w_t$ and all conjugates of x, y, z are bounded by C''.

Theorem 1 generalises, and includes, a recent result of Tijdeman [12], Theorem 2 is new as regards the variable u, but otherwise our results represent only a mild generalisation of results of Coates [6]. There is an extensive related literature; we refer the reader to the surveys by Tijdeman [13], [14] and thence to the surveys and literature there mentioned. Regarding the Catalan equation, see Cassels [5] and Tijdeman [12].

3. A p-adic analogue of the equation of Catalan. For positive integers u, v denote by $\{u, v\}$ their lowest common multiple. We shall consider the diophantine equation

$$x^u - y^v = (p_1^{w_1}\dots p_s^{w_s})^{\{u,v\}} \tag{1}$$

in rational integers $x, y, u, v, w_1, \dots, w_s$ satisfying respectively $x > 1$, $y > 1$, $u > 1$, $v > 1$, where $p_1, \dots, p_s$ are distinct positive primes belonging to the finite set $S = \{p_1, \dots, p_s\}$. It is clear that the numbers $w_1, \dots, w_s$ are non-negative, and we shall suppose, as we plainly may without loss of generality, that u and v are prime numbers. It will be convenient to suppose for the first part of our argument that v is an odd prime. We shall write $z = p_1^{w_1}\dots p_s^{w_s}$ and observe that we may suppose without loss of generality that $(x, z) = 1$, $(y, z) = 1$, since it is evident that we may cancel out any factor that happens to be common to x, y and z. Finally, we write $\{u, v\} = uv' = u'v$ and remark that of course if $u \neq v$ then $u' = u$, $v' = v$ whilst if $u = v$ then $u' = 1$, $v' = 1$.

We have

$$\begin{aligned} y^v + z^{u'v} &= \big((y+z^{u'}) - z^{u'}\big)^v + z^{u'v} \\ &\equiv v(y+z^{u'})z^{u'(v-1)} - \tfrac{1}{2}v(v-1)(y+z^{u'})^2 z^{u'(v-2)} \pmod{(y+z^{u'})^3} \end{aligned} \tag{2}$$

and claim that therefore

$$\left(y+z^{u'}, \frac{y^v+z^{u'v}}{y+z^{u'}}\right) = 1 \text{ or } v. \tag{3}$$

To see this, observe that if a prime p is such that $p|z$ then $p \nmid y+z^{u'}$ because $(y, z) = 1$, whilst if $p \mid y+z^{u'}$ then (2) implies that if $p \mid (y^v+z^{u'v})/(y+z^{u'})$ then $p \mid vz^{u'(v-1)}$; hence necessarily the only prime which can divide both $y+z^{u'}$ and $(y^v+z^{u'v})/(y+z^{u'})$ is v. Moreover (2) implies that if $v \mid y+z^{u'}$ then we have

$$(y^v+z^{u'v})/(y+z^{u'}) \equiv vz^{u'(v-1)} \pmod{v^2},$$

and this confirms our claim (3).

Now since (1) implies that $x^u = (y+z^{u'})\cdot(y^v+z^{u'v})/(y+z^{u'})$ we can conclude that if $v \mid y+z^{u'}$ then $v^{u-1} \mid y+z^{u'}$, whilst if p is prime and $p \neq v$ then $p \mid y+z^{u'}$ implies that $p^u \mid y+z^{u'}$. It follows that there is a positive integer Y such that if y satisfies (1) then

$$y = v_0 Y^u - z^{u'} \tag{4}$$

where $v_0 = 1$ or v^{-1}. By a similar argument if follows that if x satisfies (1) then there is a positive integer X such that

$$x = u_0 X^v + z^{v'} \tag{5}$$

where $u_0 = 1$ or u^{-1}.

We postpone discussion of the case $u = v$ until Section 5 below, and confine ourselves here to the case $u \neq v$. Then in view of (4) and (5) we may write (1) as

$$(u_0 X^v + z^v)^u - (v_0 Y^u - z^u)^v = z^{uv}. \tag{6}$$

We shall suppose that $u > v$, observing that in view of the symmetry of (6), the case $v > u$ will be similar. By $c, c', c_1, c_2, \dots$ we denote constants depending only on the set S, and by k, k' we denote absolute constants. As we aim to show that $v, u < c_1$ we may suppose that $u > c_2$. Our first object is to show that $v < u$ implies that

$$v < c(\log u)^\kappa. \tag{7}$$

Plainly, for $p \mid z$ we have that (1), (5) and (4) respectively imply that

$$\begin{aligned} |x^u y^{-v} - 1|_p &= |z^{uv} y^{-v}|_p = p^{-wuv}, \\ |xu_0^{-1} X^{-v} - 1|_p &= |z^v u_0^{-1} X^{-v}|_p = p^{-wv}, \\ |yv_0^{-1} Y^{-u} - 1|_p &= |z^u v_0^{-1} Y^{-u}|_p = p^{-wu}. \end{aligned}$$

(Note that if u, or v belongs to S and the corresponding w is non-zero then, necessarily $u_0 = 1$, or, respectively, $v_0 = 1$.) Hence it follows that

$$|u_0^u v_0^{-v}(X/Y)^{uv} - 1|_p \leqslant \max\{p^{-wv}, p^{-wu}, p^{-wuv}\} = p^{-wv}. \tag{8}$$

We firstly suppose that $X < Y$, and aim to show that X is not too small compared to Y. Hence we apply Theorem A to

$$\Lambda = u_0^u v_0^{-v}(X/Y)^{uv} - 1 \quad \text{with} \quad \Omega' = \log u \log v,\ A = Y,\ B = uv$$

and, assuming $\Lambda \neq 0$, we obtain that

$$|\Lambda|_p > \exp\bigl(-C_p(\log u)^4 \log Y\bigr), \tag{9}$$

for some constant C_p depending only on p, $p \in S$. Comparing (9) with (8) we see that

$$p^{wv} < \exp\bigl(C_p(\log u)^4 \log Y\bigr). \tag{10}$$

Taking the product of the inequalities (10) for all $p \in S$ we obtain that

$$z^v < Y^{C_S(\log u)^4}, \tag{11}$$

where $C_S = \sum_{p \in S} C_p$ depends only on the set S.

We remark that indeed $\Lambda \neq 0$; for if the contrary were the case then we should have

$$(x - z^v)^u = (y + z^u)^v,$$

so $(x - z^v)^u > y^v + z^{uv}$, which plainly contradicts $x^u - y^v = z^{uv}$.

As we aim to show that (7) is the case, we can suppose that

$$v > c_3(\log u)^4 \tag{12}$$

with, say, $c_3 > 3C_s$. Then (11) implies that

$$z < Y^{1/3}.$$

Hence

$$y = v_0 Y^u - z^u > Y^{3u/4} - Y^{u/3} > Y^{2u/3}. \tag{13}$$

Therefore equation (6) implies that

$$(u_0 X^v + z^v)^u > Y^{2uv/3} + z^{uv} > Y^{2uv/3}$$

so by (11) and (12)

$$u_0 X^v > Y^{2v/3} - z^v > Y^{v/2}. \tag{14}$$

We remark that in making our convenient estimates we make heavy use of our assumptions $u > c_2$ and (12).

In view of (11) and (14) we have

$$|x/(u_0 X^v) - 1| = |z^v/(u_0 X^v)| < \tfrac{1}{2} u^{-1} Y^{c_4(\log u)^4 - \frac{1}{2}v},$$
$$|y/(v_0 Y^u) - 1| = |z^u/(v_0 Y^u)| < \tfrac{1}{2} v^{-1} Y^{(c_5(\log u)^4 - v)u/v}$$

and by (13)

$$|x^u/y^v - 1| = |z^{uv}/y^v| < \tfrac{1}{2} Y^{(c_6(\log u) - \frac{1}{2}v)u}.$$

Recalling that if $|\alpha| < \frac{1}{2}$ then $|\log(1+\alpha)| < 2|\alpha|$ we obtain

$$|u \log x - u \log(u_0 X^v)| < Y^{c_4(\log u)^4 - \frac{1}{2}v},$$
$$|v \log y - v \log(v_0 Y^u)| < Y^{(c_5(\log u)^4 - v)u/v},$$
$$|u \log x - v \log y| < Y^{(c_6(\log u)^4 - \frac{1}{2}v)u},$$

whence

$$|u \log u_0 - v \log v_0 + uv \log(X/Y)| < Y^{-\frac{1}{2}(v - c_7(\log u)^4)}. \tag{15}$$

We now apply Theorem B to

$$\Lambda' = u \log u_0 - v \log v_0 + uv \log(X/Y) \quad \text{with} \quad \Omega' = \log u \log v,\ A = Y,\ B = uv$$

noting that $\Lambda' \neq 0$ since $\Lambda \neq 0$. We obtain that

$$|\Lambda'| > \exp\bigl(-C_\infty(\log u)^4 \log Y\bigr) \tag{16}$$

where C_∞ is an absolute constant. Comparing (15) with (16) we see that

$$v < c_8(\log u)^4$$

which is the assertion (7); we remark that we could actually have shown that $v < c_9(\log u)^3 \log\log u$.

To complete this part of our argument we observe that (6) implies that

$$(u_0 X^v/z^v)^u \leqslant (u_0 X^v/z^v + 1)^u - 1 = (v_0 Y^u/z^u - 1)^v < (v_0 Y^u/z^u)^v,$$

whence, in any event,

$$X \leqslant u_0^{-1/v} v_0^{1/u} Y < 2Y$$

and with very slight adjustments our proof above applies to the possibility $X > Y$.

Our second objective will be to show that indeed

$$u < c'(\log u)^{\kappa'} \tag{17}$$

and our argument will, in structure, follow the argument we have used above.

We obtain, as at (8), that on the one hand

$$|v_0^{-v}(x/Y^v)^u - 1|_p \leqslant p^{-wu}. \tag{18}$$

We suppose that $x < Y^v$. Indeed by (1) and (4)

$$(x/z^v)^u = (v_0 Y^u/z^u - 1)^v + 1 < v_0^v (Y^v/z^v)^u,$$

and as $v_0 \leqslant 1$ we invariably have $x < Y^v$. Then we may apply Theorem A to

$$\Lambda = v_0^{-v}(x/Y^v)^u - 1 \quad \text{with} \quad \Omega' = \log v,\ A = Y^v,\ B = u$$

and, assuming $\Lambda \neq 0$, we obtain that for each $p \in S$

$$|\Lambda|_p > \exp\left(-C_p(\log u)^3 v \log Y\right). \tag{19}$$

Comparing (19) with (18) we see that

$$p^{wu} < \exp\left(C_p(\log u)^3 v \log Y\right) \tag{20}$$

and taking the product of the inequalities (20) for all $p \in S$ we obtain that

$$z^u < Y^{C_S(\log u)^3 v}. \tag{21}$$

Hence, recalling (7), we see that $y = v_0 Y^u - z^u > Y^{u/2}$, so

$$|x^u/y^v - 1| = |z^{uv}/y^v| < \tfrac{1}{2} Y^{(c_{10}(\log u)^3 v - \frac{1}{2}u)v},$$

$$|y/(v_0 Y^u) - 1| = |z^u/(v_0 Y^u)| < \tfrac{1}{2} v^{-1} Y^{c_{11}(\log u)^3 v - u},$$

whence, as above at (15), we obtain that

$$|u \log(x/Y^v) - v \log v_0| < Y^{c_{12}(\log u)^3 v - u}. \tag{22}$$

We now apply Theorem B to

$$\Lambda' = u \log(x/Y^v) - v \log v_0, \quad \text{with} \quad \Omega' = \log v,\ A = Y^v,\ B = u$$

and, assuming $\Lambda' \neq 0$, we obtain that

$$|\Lambda'| > \exp\left(-C_\infty(\log u) v \log Y\right). \tag{23}$$

Comparing (23) with (22) we see that

$$u - c_{12}(\log u)^3 v < c_{13}(\log u)^2 v,$$

and recalling (7) we obtain

$$u < c'(\log u)^7 \tag{24}$$

which is (17) as required; we remark that we could actually have shown that $u < c''(\log u)^5 \log\log u$.

To complete our argument we observe that indeed $\Lambda \neq 0$, $\Lambda' \neq 0$ since otherwise we should have $x^u - v_0^v Y^{uv} = 0$ which contradicts $x^u < v_0^v Y^{uv}$ which we have already demonstrated above.

Since the equation (6) is not quite symmetric in u and v we should briefly consider the case $u < v$. We suppose that $v > c_{14}$ and note that, as shown above, $X < 2Y$. Then, simply by transposing u and v in the argument, we easily show that

$$u < c_{15}(\log v)^4. \tag{25}$$

Since by (1) and (5) we have

$$y^v = (u_0 Y^v + z^v)^u - z^{uv} < u_0^u X^{uv},$$

and $u_0 \leqslant 1$, we conclude that $y < X^u$. Now considering the expression

$$u_0^{-u}(y/X^u)^v - 1$$

leads, as above, to the required conclusion that

$$v < c'(\log v)^7. \tag{26}$$

Recalling that (24) is established under the assumption that $v < u$, similarly (26) under the assumption that $u < v$, we see that we have shown that if u, v are primes, $u \neq v$ and v odd, satisfying (1), then u and v are bounded by a constant depending only on the set $S = \{p_1, \ldots, p_s\}$. This reduces study of the equation (1) to the case $u = v$ (Theorem 2), the case $v = 2$ (Section 6) and to finitely many cases with u, v fixed. On applying Theorem C this completes the proof of Theorem 1 for the cases $u \neq v$ and $v \neq 2$.

4. The product formula. Let K be an algebraic number field with degree d, and denote by $N = N_{K/\boldsymbol{Q}}$ the field norm. If θ is any non-zero element of K then we have

$$\prod_p |N\theta|_p = 1, \tag{27}$$

where the product is over all valuations of $\boldsymbol{Q}$, including the archimedean valuation; equivalently the product is over all positive primes including the infinite prime. We have, for each p,

$$|N\theta|_p = \prod_{\mathfrak{p}|p} |\theta|_{\mathfrak{p}}^{n_{\mathfrak{p}}},$$

where the product is over the distinct prime ideals $\mathfrak{p}$ of K dividing p and $n_{\mathfrak{p}}$ is the degree of the completion of K at $\mathfrak{p}$ over the completion of $\boldsymbol{Q}$ at p (equivalently, for finite primes $\mathfrak{p}$, $n_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$ where $e_{\mathfrak{p}}$ is the exponent to which $\mathfrak{p}$ divides p and $f_{\mathfrak{p}}$ is given by $N\mathfrak{p} = p^{f_{\mathfrak{p}}}$); the primes dividing the infinite prime correspond to the distinct embeddings of K in $\boldsymbol{C}$. We will speak of the prime, and infinite (prime) valuations of K.

It follows that we have by virtue of (27),

$$\prod_{\mathfrak{p}} |\theta|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = |N\theta|^{-1} \tag{28}$$

where the product on the left is over all (finite) prime ideals of K. We have implicitly used this result in Section 3, and shall apply it explicitly below.

5. A p-adic analogue of the equation $ax^u - \beta y^u = \gamma$. We have omitted the case $u = v$ in our discussion in Section 3 above, and shall deal with it here as a special case of a considerably more general result. Incidentally, the special case $u = v$ of the equation (1) leads to a result which is trivial in the sense that it may be obtained by very much more elementary means. In particular it is inappropriate to apply the techniques of Section 3 to what is essentially a simpler problem.

Let K be an algebraic number field with degree d and denote by $\theta_1, \ldots, \theta_t$ algebraic integers of K, which are non-units and which belong to the finite set $T = \{\theta_1, \ldots, \theta_t\}$. We denote by $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ a finite set of prime ideals of K satisfying the property that, if $|\theta|_\mathfrak{p} < 1$ for some θ in T and some valuation induced by a prime ideal $\mathfrak{p}$ of K then $\mathfrak{p}$ belongs to S. There is no loss of generality in supposing that K is a normal extension of Q and that the set T, and thence the set S, is invariant under automorphisms of K; this is so because the constants we obtain depend on K and the adjustments necessary may be assumed to be incorporated in the constants. We shall consider the equation

$$ax^u - \beta y^u = \gamma z, \tag{29}$$

where α, β, γ are integers of K, $\gamma \neq 0$, and

$$z = \theta_1^{w_1} \ldots \theta_t^{w_t}, \tag{30}$$

in rational integers $u > 2$, $w_1 \geqslant 0, \ldots, w_t \geqslant 0$ and algebraic integers x, y, z belonging to K and satisfying $(x, z) = (y, z) = 1$. We suppose that $x, y, z, u, w_1, \ldots, w_t$ satisfy (29) and (30) and the stated conditions, and denote by $c, c_1, c_2, \ldots$ positive constants depending only on α, β, γ, the field K, and the set T. After cancelling common factors, and if necessary adjusting the definition of z, we may suppose that $(\alpha, z) = 1$. As we propose to show that

$$u < c \log u \tag{31}$$

we may suppose that $u > c_1 \log u$.

We shall denote by X, Y the height of x, respectively y, and assume without loss of generality, as we may, that $X > Y$. For prime ideals $\mathfrak{p} \mid z$ (in S) we have, on writing

$$\Lambda = \beta/\alpha (y/x)^u - 1,$$

that

$$|\Lambda|_\mathfrak{p} = |\gamma z/\alpha x^u|_\mathfrak{p} \leqslant |z|_\mathfrak{p}. \tag{32}$$

Then, since $\Lambda \neq 0$, Theorem A implies that

$$|\Lambda|_\mathfrak{p} > X^{-c_2 \log u}, \tag{33}$$

whence we obtain that, on comparing the inequalities (32) and (33), and multiplying the resulting inequalities over all $\mathfrak{p}$ in S according to the product formula (28) of Section 4,

$$|Nz| < X^{c_3 \log u}. \tag{34}$$

Now because the elements of the set T are non-units of K (and because we may suppose that X is sufficiently large relative to some c), equation (34) implies that z, and each of its conjugates, is bounded according to

$$|z| < X^{c_4 \log u}. \tag{35}$$

To see this, we observe that $|N\theta|$ is a positive integer, greater than 1, for each θ in T, whence it follows that each w is bounded above by some $c_5 (\log X) \log u$, and the assertion (35) is an immediate consequence.

By, if necessary, considering an equation conjugate to (29), we may suppose that $|x|^{c_7} \geqslant X$, whence by (35) we have

$$|\Lambda| = |\gamma z/\alpha x^u| \leqslant \tfrac{1}{4} X^{c_6 \log u - c_7^{-1} u}, \text{ say.}$$

But for complex w, the inequality $|e^w - 1| < \frac{1}{4}$ implies that

$$|w - bi\pi| < 4 |e^w - 1|,$$

for some rational integer b. So on writing $w = \log \beta/\alpha + u \log y/x$ and

$$\Lambda' = w - b \log(-1),$$

we obtain that

$$|\Lambda'| \leqslant X^{c_6 \log u - c_7^{-1} u}; \tag{36}$$

we observe that we may suppose that $|b| \leqslant 2u$, say. We clearly have $\Lambda' \neq 0$, so Theorem B implies that

$$|\Lambda'| > X^{-c_8 \log u}, \tag{37}$$

and the two inequalities (36) and (37) together imply (31) as required.

This argument reduces the equation (29) to finitely many equations of the shape

$$\alpha x^m - \beta y^m = \gamma z,$$

and then Theorem D completes the proof of Theorem 2, and the proof of Theorem 1 for the cases $u = v$.

6. A p-adic analogue of the equation $x^u - y^2 = 1$. We briefly consider the case omitted in Section 3, namely the case where v is even. Hence we consider the diophantine equation

$$x^u - y^2 = (p_1^{w_1} \ldots p_s^{w_s})^2, \tag{38}$$

in rational integers $x, y, u, w_1, \ldots, w_s$ satisfying respectively $x > 1$, $y > 1$, $u > 2$ where $p_1, \ldots, p_s$ are distinct positive primes belonging to the finite set $S = \{p_1, \ldots, p_s\}$. It is clear that the numbers $w_1, \ldots, w_s$ are non-negative, and that we may suppose that x, y are prime to

$$z = p_1^{w_1} \ldots p_s^{w_s}$$

since otherwise we could cancel any common factor. We shall show that u is bounded in terms of constants $c, c_1, c_2, \ldots$ depending only on the set S, and accordingly we assume that $x, y, u, w_1, \ldots, w_s$ is a solution of (38).

In the Gaussian field we have

$$x^u = (y+iz)(y-iz),$$

and, recalling that y is prime to z, we have $\gcd(y+iz, y-iz) = 1$ or 2 so that we have, say

$$y+iz = \lambda\alpha^u, \quad y-iz = \mu\beta^u$$

with $\alpha, \beta, \lambda, \mu \in \mathbf{Z}[i]$ and $|\lambda| \leqslant 2$, $|\mu| \leqslant 2$, say. On eliminating y we obtain

$$\lambda\alpha^u - \mu\beta^u = 2iz,$$

whence, by the argument of Section 5, $u < c\log u$, and u is bounded as required. Theorem D now completes the proof of Theorem 1 for the case $v = 2$.

The above argument is a p-adic generalisation of a very particular case of the recent result of Schinzel and Tijdeman [10] on the equation $y^u = P(x)$; whilst it seems clear that a p-adic generalisation of that result should not present new difficulties it would lead us too far afield to attempt to show this here.

References

[1] A. Baker, *Contributions to the theory of diophantine equations, I On the representation of integers by binary forms, II The Diophantine equation* $y^2 = x^3 + k$, Phil. Trans. Roy. Soc. Lond. Ser. A 263 (1968), pp. 173–208.

[2] — *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Phil. Soc. 65 (1969), pp. 439–444.

[3] — *A sharpening of the bounds for linear forms in logarithms*, Acta Arith. 21 (1972), pp. 117–129.

[4] — *A sharpening of the bounds for linear forms in logarithms III*, ibid. 27 (1975), pp. 247–252.

[5] J. W. S. Cassels, *On the equation* $a^x - b^y = 1$ *II*, Proc. Camb. Phil. Soc. 56 (1960), pp. 97–103.

[6] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), pp. 279–305; *II The greatest prime factor of binary form*, ibid. 16 (1970), pp. 399–412; *III The diophantine equation* $y^2 = x^3 + k$, ibid. 16 (1970), pp. 425–435.

[7] S. V. Kotov, *The Thue–Mahler equation in relative fields*, ibid. 27 (1975), pp. 293–315.

[8] K. Mahler, *On the greatest prime factor of* $ax^m + by^n$, Nieuw Arch. v. Wisk. (3) 1 (1953), pp. 113–122.

[9] A. J. van der Poorten, *On Baker's inequality for linear forms in logarithms*, Math. Proc. Camb. Phil. Soc. 80 (1976), pp. 233–248.

[10] A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. 31 (1976), pp. 199–204.

[11] V. G. Sprindžuk and S. V. Kotov, *An effective analysis of the Thue–Mahler equation in relative fields*, Dokl. Akad. Nauk. BSSR 17 (1973), pp. 393–395, 477.

[12] R. Tijdeman, *On the equation of Catalan*, Acta Arith. 29 (1976), pp. 197–209.

[13] — *Applications of the Gel'fond–Baker method to rational number theory*, Bolyai Janos Soc. Colloquium on Number Theory, Debrecen 1974, P. Turán ed., *Topics in Number Theory*, North Holland 1976, pp. 399–416.

[14] — *Hilbert's seventh problem: On the Gel'fond–Baker method and its applications*, F. E. Browder ed., *Mathematical developments arising from Hilbert Problems*, Proc. Symp. Pure Maths. 28, Amer. Math. Soc. 1976.

Received on 10. 6. 1975
and in revised form on 8. 4. 1976 (726)