ACTA ARITHMETICA
XLII (1983)

Multiplicative dependence in number fields

by

J. H. Loxton (New South Wales) and A. J. van der Poorten
(Macquarie)

1. Introduction. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero elements of an algebraic number field K of degree D over the rationals. Such numbers are said to be *multiplicatively dependent* if there are rational integers $b_1, b_2, \ldots, b_n$, not all zero, such that

$$\alpha_1^{b_1}\alpha_2^{b_2}\ldots\alpha_n^{b_n} = 1. \tag{1}$$

We shall show that the integers $b_1, \ldots, b_n$ in the relation (1) can be chosen to have absolute values relatively small in terms of n, D and the sizes of the algebraic numbers $\alpha_1, \ldots, \alpha_n$. In particular, we are interested in circumstances in which these bounds do not depend explicitly on the degree D.

Our interest in these results stems from their application to linear forms in the logarithms of algebraic numbers. Specifically, an estimate for the size of the exponents in the multiplicative relation (1) reduces the general problem on linear forms in logarithms to the case in which the algebraic numbers satisfy a certain independence relation. (Cf. [1], Section 8, or [7].) In his original work, Alan Baker obtained the required bound for the smallest multiplicative relation by adapting the transcendence argument used to produce lower bounds for linear forms in logarithms, whereas the method used in [7] is quite elementary.

Recently, Bijlsma and Cijsouw [4] have considered this problem under slightly different hypotheses. They note that if the exponents $b_1, \ldots, b_n$ in (1) are relatively prime, then there are D linear relations

$$b_1\log\sigma\alpha_1 + b_2\log\sigma\alpha_2 + \ldots + b_n\log\sigma\alpha_n = 0, \tag{2}$$

where σ runs through the D embeddings of K into the complex numbers and $\log\sigma\alpha_j$ denotes an appropriate value of the logarithm, the branch depending on both σ and j. Bijlsma and Cijsouw use a variant of Baker's method which allows them to deal with simultaneous linear forms in the logarithms of algebraic numbers. However, the complicated transcendence argument is not needed in this context. We shall obtain more precise

results by a comparatively elementary method from the geometry of numbers. In [7], we used a primitive version of the same idea in the course of obtaining explicit lower bounds for linear forms in logarithms. The more refined results of the present paper do not give any improvements in this direction. However, we speculate that a comparison of the results obtained by the two methods indicates that the current estimates for linear forms in logarithms are close to best possible.

We would like to thank Lex Bijlsma for some valuable comments on a preliminary draft of this paper. In particular, these remarks encouraged us to look for Theorem 2 and Example 2.

2. Heights and denominators. Let α be a non-zero element of an algebraic number field K of degree D over the rationals and let $f(x)$ be the characteristic polynomial of the Q-linear map $x \to \alpha x$ on K. If A_0 is the least common denominator of the coefficients of $f(x)$, we can write

$$A_0 f(x) = A_0 x^D + A_1 x^{D-1} + \ldots + A_D = A_0 \prod_{i=1}^{D} (x - \alpha^{(i)}),$$

where $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(D)}$ are the field conjugates of α and $A_0, A_1, \ldots, A_D$ are relatively prime integers. The absolute logarithmic height $h(\alpha)$ of α is given by

$$h(\alpha) = D^{-1} \log \Big(|A_0| \prod_{i=1}^{D} \max\{1, |\alpha^{(i)}|\} \Big),$$

and we define a normalised denominator for α by

$$d(\alpha) = D^{-1} \max\{\log |A_0|, \log |A_D|\}.$$

It will also be useful to define an archimedean analogue of $d(\alpha)$, namely

$$s(\alpha) = D^{-1} \max\Big\{ \sum_{i=1}^{D} \log^+ |\alpha^{(i)}|, \sum_{i=1}^{D} \log^+ |\alpha^{(i)}|^{-1} \Big\},$$

where $\log^+ x = \max\{0, \log x\}$.

All three of $h(\alpha)$, $d(\alpha)$ and $s(\alpha)$ are independent of the field K in which we happen to work. Further, $h(\alpha^{-1}) = h(\alpha)$, with obvious analogues for $d(\alpha)$ and $s(\alpha)$. Indeed, we can rewrite $h(\alpha)$ as

$$h(\alpha) = D^{-1} \Big(\log |A_0| + \sum_{i=1}^{D} \log^+ |\alpha^{(i)}| \Big) = D^{-1} \sum_{v} \log^+ |\alpha|_v.$$

In the final sum, v runs through all the valuations of K, both archimedean and non-archimedean, normalised so that the product formula,

$$\sum_{v} \log |\alpha|_v = 0,$$

holds for all non-zero elements α of K. The claim that $h(\alpha^{-1}) = h(\alpha)$ now follows immediately. We can also remark that

$$\log |A_0| = \sum_{v} \log^+ |\alpha|_v, \quad \log |A_D| = \sum_{v} \log^+ |\alpha^{-1}|_v,$$

where now the sums are restricted to the non-archimedean valuations of K. (Further details on these matters can be found in [2], Section 3.1.)

Let α be a non-zero element of K. We shall use the fundamental inequality of transcendence theory, namely

$$\log |A_0| + \log |N_{K/Q}\alpha| = \log |A_0| + \sum_{i=1}^{D} \log |\alpha^{(i)}| \geqslant 0, \tag{3}$$

which follows immediately from the product formula. Thus, should this inequality not hold for some α in K, we may conclude that $\alpha = 0$.

We shall also require the following observations on a question of Lehmer. There is a positive constant $\lambda(D)$, depending only on D, such that if α is a nonzero algebraic integer of degree D and $h(\alpha) < \lambda(D)/D$, then α must be a root of unity. (This follows by a simple compactness argument.) By a recent sharpening by Cantor of a result of Dobrowolski [6], we can take $\lambda(D) = (2-\varepsilon)(\log\log D/\log D)^3$ for any $\varepsilon > 0$, providing D is sufficiently large relative to ε. The example $\alpha = 2^{1/D}$ shows that $\lambda(D)$ cannot exceed $\log 2$.

3. Simultaneous linear relations. We shall prove three theorems, assuming progressively less about the sizes of the numbers $\alpha_1, \ldots, \alpha_n$ and their logarithms. Firstly, we suppose that we are given the complete set of conjugate linear relations (2). Part (A) of the theorem below is a sharpening of the result of Bijlsma and Cijsouw [4]; in particular, the dependence on all the parameters is now totally explicit. A simpler result is obtained by setting the parameter E equal to e ($= 2.71828\ldots$). The improvement brought about by the correct value of E seems to occur whenever we can use the fact that an algebraic number has conjugates close to 1. In part (B) of the theorem, the data are grouped in a different way. The proof contains a curious maximisation problem which, in the simplest case, comes down to the following: Maximise $|(z_1-1)(z_2-1)|$, where z_1, z_2 are complex numbers in the sector $\{z : |z| \leqslant 1, |\arg z| \leqslant \varphi\}$ subject to $|z_1 z_2| \geqslant \tau$. We would like to thank Esther Szekeres for help in unravelling the intricacies of this pleasant little problem. Finally, part (C) illustrates the extent to which the argument simplifies if $\alpha_1, \ldots, \alpha_n$ are units.

THEOREM 1. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero algebraic numbers belonging to an algebraic number field K of degree D over the rationals. Suppose that*

there are rational integers $b_1, b_2, \dots, b_n$ not all zero such that

$$b_1\log a_1^{(i)} + b_2\log a_2^{(i)} + \dots + b_n\log a_n^{(i)} = 0 \quad (1 \leqslant i \leqslant D),$$

for some determination of the logarithms $\log a_j^{(i)}$ which may depend on both i and j.

(A) *Define*

$$E = \min_{1\leqslant j\leqslant n} \max\{e,\ d(a_j)\log 2 / \max_{1\leqslant i\leqslant D} |\log a_j^{(i)}|\}$$

and

$$V_j = \max\{d(a_j),\ (e/\log 2)\max_{1\leqslant i\leqslant D} |\log a_j^{(i)}|\}/\log(E/\log E) \quad (1 \leqslant j \leqslant n).$$

Then there are integers $q_1, q_2, \dots, q_n$, not all zero, such that

$$q_1\log a_1^{(i)} + q_2\log a_2^{(i)} + \dots + q_n\log a_n^{(i)} = 0 \quad (1 \leqslant i \leqslant D) \tag{4}$$

and

$$|q_k| \leqslant (n-1)! \prod_{j\neq k} V_j \quad (1 \leqslant k \leqslant n). \tag{5}$$

(B) *Let $\varphi_0 = 0.313518639\dots$ be the smallest positive root of the equation $4\cos^2\varphi\log(2\cos\varphi) + \log(2-2\cos\varphi) = 0$. Choose φ such that $0 < \varphi < \varphi_0$ and let $\tau = (2\cos\varphi)^{1/2}$ and*

$$V_j = \max\{h(a_j)/\log\tau,\ \varphi^{-1}\max_{1\leqslant i\leqslant D} |\operatorname{im}\log a_j^{(i)}|\} \quad (1 \leqslant j \leqslant n).$$

Then, once again, there are integers q_j satisfying (4) and (5).

(C) *Finally, suppose that $a_1, a_2, \dots, a_n$ are units. Then there are integers q_j satisfying (4) with*

$$|q_k| \leqslant (n-1)!(\log 2)^{-(n-1)} \prod_{j\neq k} \max_{1\leqslant i\leqslant D} |\log a_j^{(i)}| \quad (1 \leqslant k \leqslant n).$$

Proof. (A) Let k be an integer with $1 \leqslant k \leqslant n$. Recalling that the volume of the convex body $\{(y_1, \dots, y_m)\colon \sum |y_j| \leqslant 1\}$ in R^m is $2^m/m!$, we apply Minkowski's convex body theorem, as in [5], page 73, and see that there are integers $q_1, \dots, q_n$ not all zero, such that

$$\sum_{j\neq k} V_j|q_j - b_jq_k/b_k| < 1 \quad \text{and} \quad |q_k| \leqslant (n-1)!\prod_{j\neq k} V_j.$$

Set $a = a_1^{q_1}a_2^{q_2}\dots a_n^{q_n}$ and fix $\log a^{(i)} = \sum q_j\log a_j^{(i)}$. Then, for each i,

$$\begin{aligned}|\log a^{(i)}| &= \Big|\sum_{j=1}^n q_j\log a_j^{(i)}\Big| = \Big|\sum_{j=1}^n (q_j - b_jq_k/b_k)\log a_j^{(i)}\Big| \\ &\leqslant \sum_{j=1}^n V_j|q_j - b_jq_k/b_k| \max_{1\leqslant i\leqslant D} |\log a_j^{(i)}|/V_j \\ &< E^{-1}\log 2\cdot\log(E/\log E).\end{aligned}$$

In particular, $|\log a^{(i)}| < \log 2$. But $|(e^w-1)/w| \leqslant (e^{|w|}-1)/|w| < 1/\log 2$ for $|w| < \log 2$, so

$$|a^{(i)} - 1| < |\log a^{(i)}|/\log 2 < E^{-1}\log(E/\log E). \tag{6}$$

On the other hand, we have for each valuation v of K,

$$\log|a|_v = \sum_{j=1}^n q_j\log|a_j|_v = \sum_{j=1}^n (q_j - b_jq_k/b_k)\log|a_j|_v,$$

so we have

$$\log^+|a|_v \leqslant \sum_{j=1}^n |q_j - b_jq_k/b_k|\log^+|a_j|_v, \tag{7}$$

and a similar inequality for $\log^+|a^{-1}|_v$. Summing over the non-archimedean valuations and dividing by D yields

$$d(a) \leqslant \sum_{j=1}^n |q_j - b_jq_k/b_k|\, d(a_j) = \sum_{j=1}^n V_j|q_j - b_jq_k/b_k|\, d(a_j)/V_j < \log(E/\log E).$$

Now suppose that $a \neq 1$. If, as in Section 2, we denote by A_0 the least common denominator of the coefficients of the characteristic polynomial of $a-1$ over K, then

$$\log|A_0| = \sum_v \log^+|a-1|_v = \sum_v \log^+|a|_v \leqslant Dd(a) < D\log(E/\log E),$$

where v runs through the non-archimedean valuations of K. With (6), this gives

$$D^{-1}\big(\log|A_0| + \log|N_{K/Q}(a-1)|\big) < \log(E/\log E) + \log\big(E^{-1}\log(E/\log E)\big) \leqslant 0.$$

Thus, by the fundamental inequality (3), we conclude that $a = 1$. It follows that $\log a^{(i)}$ is an integral multiple of $2\pi i$, though as already remarked $|\log a^{(i)}| < \log 2$. Consequently, $\log a^{(i)} = 0$, giving the required set of conjugate linear relations (4). Moreover, there is no loss of generality in supposing that no $n-1$ of the a_j, with the given determinations of the $\log a_j^{(i)}$, satisfy the hypotheses of the theorem, or that the integers $q_1, \dots, q_n$ above are relatively prime. These conditions fix the q_j and, since the choice of k was arbitrary, we obtain the required bound (5) for each k.

(B) As before, the application of Minkowski's theorem yields

$$|\operatorname{im}\log a^{(i)}| < \varphi,$$

and, by way of (7),

$$d(a) < \log\tau, \quad s(a) < \log\tau.$$

Now consider the problem of maximising the quantity $M = \prod |z_i - 1|^2$ for complex numbers $z_1, \ldots, z_D$ satisfying

$$|\arg z_i| \leqslant \varphi, \quad \prod_i \max\{1, |z_i|\} \leqslant \tau^D, \quad \prod_i \max\{1, |z_i|^{-1}\} \leqslant \tau^D.$$

At the maximum, $|\arg z_i| = \varphi$ for each i and the second and third constraints hold with equality whenever any z_i is outside (respectively, inside) the unit circle. By elementary calculus, the z_i outside the unit circle all satisfy $|z_i| = r$, say, and the z_i inside the unit circle, if any, satisfy $|z_i| = s^{-1}$. There are four configurations to consider.

First case. Suppose that there are k points at $re^{i\varphi}$ and $D-k$ points at $s^{-1}e^{i\varphi}$ with $r > 1$, $s > 1$ and $0 < k < D$. The constraints on the variables become $r^k = s^{D-k} = \tau^D$ and we require the maximum of

$$\begin{aligned} M &= (1 + r^2 - 2r\cos\varphi)^k (1 + s^{-2} - 2s^{-1}\cos\varphi)^{D-k} \\ &= (1 + r^2 - 2r\cos\varphi)^k (1 + s^2 - 2s\cos\varphi)^{D-k} \tau^{-2D}. \end{aligned}$$

Since r and s now play exactly the same role, the extreme choice is $k = \frac{1}{2}D$ and $r = s = \tau^2$, giving

$$M = (1 + \tau^4 - 2\tau^2\cos\varphi)^D \tau^{-2D} = \tau^{-2D}.$$

Second case. Suppose that there are D points at $re^{i\varphi}$ with $r > 1$. Then $r = \tau = (2\cos\varphi)^{1/2}$ and

$$M = \left(1 + 2\cos\varphi - (2\cos\varphi)^{3/2}\right)^D < \tau^{-2D},$$

because of the choice of φ.

Third case. Suppose that there are k points at $re^{i\varphi}$ and $D-k$ points at $e^{i\varphi}$ with $r > 1$ and $0 < k < D$. From the choice of φ, $(2\cos\varphi - 1)^{-1} < \tau = (2\cos\varphi)^{1/2}$, so we can move one of the points from $e^{i\varphi}$ to $s^{-1}e^{i\varphi}$ with $s > (2\cos\varphi - 1)^{-1} > 1$, thereby increasing M. Consequently, this case cannot give the maximum.

Fourth (and most interesting) case. Suppose that there are k points at $re^{i\varphi}$, l points at $s^{-1}e^{i\varphi}$ and $D-k-l$ points at $e^{i\varphi}$ with $r > 1$, $s > 1$, $k > 0$, $l > 0$ and $k + l < D$. We must now maximise

$$M = (1 + r^2 - 2r\cos\varphi)^k (1 + s^2 - 2s\cos\varphi)^l (2 - 2\cos\varphi)^{D-k-l} \tau^{-2D}$$

subject to the constraints $r^k = s^l = \tau^D$. As before, we can suppose that $r = s$ and $k = l$ and maximise

$$M = (1 + r^2 - 2r\cos\varphi)^{2k} (2 - 2\cos\varphi)^{D-2k} \tau^{-2D}$$

subject to $r^k = \tau^D$. We suppose for the moment that k is a continuous variable. Then the maximum is a stationary point and the method of

Lagrange multipliers leads to the equations

$$\begin{aligned} (2r - 2\cos\varphi)(1 + r^2 - 2r\cos\varphi)^{-1} &= \lambda r^{-1}, \\ \log(1 + r^2 - 2r\cos\varphi) - \log(2 - 2\cos\varphi) &= \lambda \log r. \end{aligned}$$

Thus, the critical radius, r_0 say, is determined by

$$(8) \qquad \frac{2r(r - \cos\varphi)}{1 + r^2 - 2r\cos\varphi} = \frac{\log(1 + r^2 - 2r\cos\varphi)/(2 - 2\cos\varphi)}{\log r} \qquad (= \lambda)$$

and the corresponding maximum value of M is

$$M_0 = \tau^{2D(\lambda - 1)} (2 - 2\cos\varphi)^D.$$

Now, the graphs of the left and right sides of (8) cross at r_0 which is the maximum of the right side; the value of the left side is greater than, or less than, that of the right side, according as $1 < r < r_0$ or $r > r_0$. From the choice of φ, the latter possibility applies when $r = 2\cos\varphi$, so $r_0 \leqslant 2\cos\varphi$. On the other hand, from the choice of τ, $r_0 = \tau^{D/k} > 2\cos\varphi$, since $k < \frac{1}{2}D$. So this case cannot give the maximum under the prevailing conditions on φ and τ. As will be seen, the hypotheses of the theorem have been chosen to give a tidy value of τ. It would be possible to analyse the situation for larger angles φ, adjusting τ appropriately, but this would not significantly improve the theorem.

Summing up, we have shown that under the stated conditions, the quantity M satisfies $M \leqslant \tau^{-2D}$. From the remarks at the beginning of this part of the proof, we can apply the above analysis to $N(\alpha - 1) = \prod(\alpha^{(i)} - 1)$ and we see that $|N(\alpha - 1)| < \tau^{-D}$. However, $N(\alpha - 1)$ is a rational number with denominator at most τ^D, so we find again that $\alpha = 1$. Since $|\arg \alpha^{(i)}| < \varphi$, this implies that $\log \alpha^{(i)} = 0$ for each i and so yields the required result as in part (A).

(C) Already with

$$V_j = \max_{1 \leqslant i \leqslant D} |\log a_j^{(i)}| / \log 2 \qquad (1 \leqslant j \leqslant n),$$

we obtain $|\alpha^{(i)} - 1| < 1$ for each i. Since α is an algebraic integer (in fact, a unit), this yields $\alpha = 1$ immediately and we can complete the argument as before.

4. A single linear relation. It is perhaps unnatural to assume that all the branches $\log a_j^{(i)}$ are given for all the conjugates of the a_j. In practice, we will only have information about one linear relation

$$b_1 \log a_1 + b_2 \log a_2 + \ldots + b_n \log a_n = 0.$$

Although this implies the complete set of conjugate linear relations (2) for suitable determinations of the logarithms, we must expect some of the

$\log a_j^{(i)}$ to be large. (Cf. the example in Section 6.) Under these circumstances, the following theorem may be sharper than Theorem 1. The case $n = 2$ of the theorem includes the Lemma 2.11 of Bijlsma [3], obtained by Gel'fond's method. Bijlsma has used this result to prove a refined measure of simultaneous approximation for the numbers α, β and α^β.

THEOREM 2. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero algebraic numbers belonging to an algebraic number field K of degree D over the rationals. Suppose that there are rational integers $b_1, b_2, \ldots, b_n$, not all zero, such that*

$$b_1\log\alpha_1 + b_2\log\alpha_2 + \ldots + b_n\log\alpha_n = 0,$$

for some determinations of the logarithms. Define

$$E = \min_{1\leqslant j\leqslant n} \max\{e, Dh(\alpha_j)\log 2/2^D|\log\alpha_j|\}$$

and

$$V_j = \max\{Dh(\alpha_j), 2^D e|\log\alpha_j|/\log 2\}/\log(E/\log E) \quad (1\leqslant j\leqslant n).$$

Then there are integers $q_1, q_2, \ldots, q_n$, not all zero, such that

$$q_1\log\alpha_1 + q_2\log\alpha_2 + \ldots + q_n\log\alpha_n = 0$$

and

$$|q_k| \leqslant (n-1)!\prod_{j\neq k} V_j \quad (1\leqslant k\leqslant n).$$

Proof. We construct $\alpha = \alpha_1^{q_1}\alpha_2^{q_2}\ldots\alpha_n^{q_n}$ as in the proof of Theorem 1 and, as before, we obtain

$$|\alpha - 1| < 2^{-D}E^{-1}\log(E/\log E)$$

and, from (7),

$$h(\alpha) < D^{-1}\log(E/\log E).$$

For the conjugates $\alpha^{(i)}$ other than α, we have the trivial inequality

$$|\alpha^{(i)} - 1| \leqslant 2\max\{1, |\alpha^{(i)}|\}.$$

Now, with v running through the non-archimedean valuations of K,

$$\sum_v \log^+|\alpha-1|_v + \log|N_{K/\mathbb{Q}}(\alpha-1)|$$

$$\leqslant \sum_v \log^+|\alpha|_v + \log|\alpha-1| + D\log 2 + \sum_{i=1}^{D}\log^+|\alpha^{(i)}|$$

$$= \log|\alpha-1| + D\log 2 + Dh(\alpha) \leqslant 0,$$

from the previous estimates. Thus, $\alpha = 1$ and the conclusion follows as in Theorem 1.

5. Multiplicative relations. Thirdly, we suppose we have a multiplicative relation (1). This is a slightly weaker condition than (2) because we cannot suppose that the exponents $b_1, \ldots, b_n$ are relatively prime. However, even if $b_1, \ldots, b_n$ are relatively prime, we now have no information about the branches $\log\alpha_j^{(i)}$ in any of the relations (2). Our construction does not give an element of the field K close to 1, so that we lose the parameter E in Theorem 2. In general, we cannot hope to remove the dependence on D from part (A) of the theorem, in view of the example in Section 6. Exceptionally, the totally real case in part (B) does lead to bounds independent of D because it is possible to control the branches of the logarithms in (2).

THEOREM 3. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero algebraic numbers in an algebraic number field K of degree D over the rationals. Let $w(K)$ denote the number of roots of unity in K and define $\lambda(D)$ as in Section 2. Suppose that there are rational integers $b_1, b_2, \ldots, b_n$, not all zero, such that*

$$\alpha_1^{b_1}\alpha_2^{b_2}\ldots\alpha_n^{b_n} = 1.$$

(A) *In general, there are integers $q_1, q_2, \ldots, q_n$, not all zero, such that*

$$\alpha_1^{q_1}\alpha_2^{q_2}\ldots\alpha_n^{q_n} = 1, \tag{9}$$

$$|q_k| \leqslant (n-1)!w(K)\prod_{j\neq k}\left(Dh(\alpha_j)/\lambda(D)\right) \quad (1\leqslant k\leqslant n).$$

(B) *If K is totally real, then there are integers $q_1, q_2, \ldots, q_n$ satisfying (9) as above and such that*

$$|q_k| \leqslant 2^{2n-1}(n-1)!\prod_{j\neq k}\left(h(\alpha_j)/\log 2\right) \quad (1\leqslant k\leqslant n).$$

(C) *Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are units and that K is almost real, that is K is a totally real field or an imaginary quadratic extension of a totally real field. Then there are integers $q_1, q_2, \ldots, q_n$ satisfying (9) as above and such that*

$$|q_k| \leqslant 2^{n-1}(n-1)!w(K)\prod_{j\neq k}\left(h(\alpha_j)/\log\varrho\right) \quad (1\leqslant k\leqslant n),$$

where $\varrho = \frac{1}{2}(1+5^{1/2})$.

Proof. (A) Set $V_j = Dh(\alpha_j)/\lambda(D)$ for $1\leqslant j\leqslant n$. We construct α as in the proof of Theorem 1 and, by way of (7), we obtain $h(\alpha) < \lambda(D)/D$. In particular, $d(\alpha) < \lambda(D)/D < \log 2/D$, so α is an algebraic integer, indeed a unit. From the definition of $\lambda(D)$, we conclude that α is a root of unity. So we have found integers $q_1, \ldots, q_n$, not all zero, such that $\alpha_1^{q_1}\ldots\alpha_n^{q_n}$ is a root of unity and

$$|q_k| \leqslant (n-1)!\prod_{j\neq k} V_j.$$

(The argument to show that this bound holds for all k is the same as in the proof of Theorem 1.) Part (A) of the theorem follows since the roots of unity in K form a cyclic group of order $w(K)$.

(B) Construct α as before, with $V_j = 4h(a_j)/\log 2$. Since K is totally real, the conjugates of α^2 are all positive. As in part (B) of Theorem 1, we wish to estimate $N_{K/\mathbb{Q}}(\alpha^2-1)$. This leads to the maximisation problem considered earlier with $\varphi = 0$ and $\tau = 2^{1/2}$. Since only the first case in the previous discussion is applicable, we conclude without any trouble that $N_{K/\mathbb{Q}}(\alpha^2-1) < \tau^{-D}$. This yields $\alpha = \pm 1$ and so proves part (B) of the theorem.

(C) An almost real field, K, is characterised by the property that complex conjugation maps K to itself and commutes with all the embeddings of K into the complex numbers. Hence, for α in K, the field conjugates of $|\alpha|^2$ are just the $|\alpha^{(i)}|^2$ with $1 \leqslant i \leqslant D$. We construct α as before, with $V_j = 2h(a_j)/\log\varrho$. By the preceding remarks, we find $h(|\alpha|^2) < \log\varrho$ and a modification of the argument sketched in (B) yields $N_{K/\mathbb{Q}}(|\alpha|^2-1) < 1$. From the additional hypotheses for this case, α is an algebraic integer, so $|\alpha^{(i)}|^2 = 1$ for each i and a theorem of Kronecker tells us that α is a root of unity. Part (C) of the theorem now follows.

6. Concluding remarks. The first example below shows that the dependence on the heights of the algebraic numbers in Theorem 3 is best possible. Comparing our results with those in Bijlsma and Cijsouw [4] then provides some circumstantial evidence that the current lower bounds for linear forms in the logarithms of algebraic numbers are also close to best possible in their dependence on the heights of the algebraic numbers involved. We also see that we cannot remove the dependence on the degree D in Theorems 2 and 3(A). The bounds in Theorem 1 manage to be independent of D because of a concealed dependence on D in the branches of the logarithms which are required to obtain the complete set of conjugate linear relations (2).

Example 1. Let $p_1 = 2$, $p_2 = 3, \ldots, p_{n-1}$ be the first $n-1$ primes and let $K = \mathbb{Q}(p_1^{1/s}, p_2^{1/s}, \ldots, p_{n-1}^{1/s})$, s being a positive integer. Thus $D = [K:\mathbb{Q}] = s^{n-1}$. Further, let u and v be relatively prime positive integers with, say, $u < v < 2u$. Set

$$(10) \qquad a_1 = p_1^{-u},\ a_2 = p_1^{v}p_2^{-u},\ \ldots,\ a_{n-1} = p_{n-2}^{v}p_{n-1}^{-u},\ a_n = p_{n-1}^{v}.$$

Then $a_1, a_2, \ldots, a_n$ are multiplicatively dependent and the minimal relation, $a_1^{b_1}a_2^{b_2}\ldots a_n^{b_n} = 1$ is given by $b_j = u^{j-1}v^{n-j}$. Next, set $\alpha_j = a_j^{1/s}$ for $1 \leqslant j \leqslant n$. Then $\alpha_1, \alpha_2, \ldots, \alpha_n$ are multiplicatively dependent elements of K having the same multiplicative relations as $a_1, a_2, \ldots, a_n$. For each j,

$$h(\alpha_j) = s^{-1}h(a_j) = s^{-1}\max\{u\log p_j, v\log p_{j-1}\} \leqslant A(n)s^{-1}u,$$

where $A(n)$ stands for a positive constant independent of s, u and v, but possibly depending on n. Thus

$$b_k = u^{k-1}v^{n-k} > A(n)D\prod_{j\neq k} h(a_j) \qquad (1 \leqslant k \leqslant n).$$

This example momentarily seems to contradict Theorem 1. However, if we use the notation $\alpha^{(l)}$ with $l = (l_1, \ldots, l_{n-1})$ to denote the conjugate of α in K obtained by sending $p_j^{1/s}$ to $p_j^{1/s}\exp(2\pi i l_j/s)$, then we can obtain the complete set of conjugate relations (2) with

$$\log\alpha_k^{(l)} = s^{-1}\log a_k + 2\pi i s^{-1}(l_{k-1}v - l_k u).$$

Since the l_j run from 0 to $s-1$, we have

$$\max_{(l)} |\log\alpha_k^{(l)}| \sim A(n)u$$

for large s, and all is well.

The second example shows that the dependence on the heights of the algebraic numbers in Theorems 1(A) and 2 is best possible and illustrates the role of the parameter E.

Example 2. Choose distinct primes p_j, q_j $(1 \leqslant j \leqslant n-1)$ satisfying $X < p_j < 2X$ and $0 < p_j - q_j < C\log X$ for each j and for some positive constant C. (This is possible because $\pi(2x) - \pi(x) \gg x/\log x$.) Construct $a_1, \ldots, a_n$ by modifying (10) as follows. Set

$$a_1 = (p_1/q_1)^{-u}, \quad a_2 = (p_1/q_1)^{v}(p_2/q_2)^{-u}, \quad \ldots$$
$$\ldots, \quad a_{n-1} = (p_{n-2}/q_{n-2})^{v}(p_{n-1}/q_{n-1})^{-u}, \quad a_n = (p_{n-1}/q_{n-1})^{v},$$

with $u = X$, $v = X+1$ and X a large integer parameter. We can now apply Theorem 1(A) to the multiplicatively dependent numbers $a_1, \ldots, a_n$, taking $K = \mathbb{Q}$ and $D = 1$. (In this case, Theorem 1(A) and Theorem 2 are equivalent.) We find

$$\log a_j = O(u\log p_j/q_j) = O(\log X),$$

as $X \to \infty$, with an implied constant depending only on n, and

$$h(a_j) = d(a_j) = O(u\log p_j) = O(X\log X).$$

According to the prescriptions of Theorem 1(A),

$$E = \min_{1\leqslant j\leqslant n} d(a_j)\log 2/\log a_j > A(n)X,$$

where $A(n)$ stands for a positive constant depending only on n, and

$$V_j = d(a_j)/\log(E/\log E) = O(X).$$

As before, the minimal relation $b_1 \log a_1 + \ldots + b_n \log a_n = 0$ has coefficients $b_j = u^{j-1} v^{n-j}$, and these satisfy

$$b_k > A(n) \prod_{j \neq k} V_j,$$

justifying our earlier assertions.

References

[1] A. Baker, *The theory of linear forms in logarithms*, A. Baker and D. W. Masser (eds.), *Transcendence theory: advances and applications*, Academic Press, 1977, Chapter 1.

[2] D. Bertrand, *Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe*, Compositio Math. 37 (1978), pp. 21–50.

[3] A. Bijlsma, *Simultaneous approximations in transcendental number theory*, Math. Centrum Tracts, number 94, Amsterdam 1978.

[4] A. Bijlsma and P. L. Cijsouw, *Degree-free bounds for dependence relations*, J. Austral. Math. Soc. (A) 31 (1981), pp. 496–507.

[5] J. W. S. Cassels, *An introduction to the geometry of numbers*, Second edition, Springer Verlag, 1971.

[6] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), pp. 391–401.

[7] J. H. Loxton and A. J. van der Poorten, *Multiplicative relations in number fields*, Bull. Austral. Math. Soc. 16 (1977), pp. 83–106. *Corrigenda*, ibid. 17 (1977), pp. 151–155.

SCHOOL OF MATHEMATICS
UNIVERSITY OF NEW SOUTH WALES
Kensington, N.S.W., 2033, Australia

SCHOOL OF MATHEMATICS AND PHYSICS
MACQUARIE UNIVERSITY
North Ryde, N.S.W., 2113, Australia

Received on 19. 9. 1981
and in revised form on 24. 3. 1982 (1268)

ACTA ARITHMETICA
XLII (1983)

On the diophantine equation $y^2 + D^m = p^n$

by

Masao Toyoizumi (Tokyo)

1. Introduction. Let D be a positive square free integer greater than 1 and let $p \equiv 3 \pmod 4$ be a prime number not dividing D. Let further d be the order of a prime ideal divisor of (p) in the ideal class group of the quadratic field $Q(\sqrt{-D})$. In the present paper we consider the diophantine equation

$$y^2 + D^m = p^n \tag{1}$$

in positive integers y, m, n. The aim of this paper is to prove the following two theorems.

Theorem 1. *Assume $D \equiv 1, 2 \pmod 4$ and $p^d - D$ is a square. Then the equation (1) implies that $m = 1$ unless $(p, D) = (3, 2)$.*

Theorem 2. *The only positive integer solutions of the equation*

$$y^2 + 2^m = 3^n \tag{2}$$

are given by $(y, m, n) = (1, 1, 1), (5, 1, 3), (1, 3, 2), (7, 5, 4)$.

We shall complete the proof of the above theorems by using the techniques of [2].

2. Proof of some lemmas.

Lemma 1. *Let d and D be as in Theorem 1. Assume that s is a fixed positive integer and $D \not\equiv 0 \pmod 3$. If the equation*

$$y^2 + D^{2s+1} = p^n \tag{3}$$

has integer solutions for y and n, then the equation

$$y^2 + D^{2(s-1)+1} = p^n$$

has also integer solutions for y and n.

Proof. Since $p^d - D$ is a square, $-D$ is a quadratic residue modulo p. Then from the theory of quadratic fields, it follows that $(p) = PP'$, where P and P' are distinct conjugate prime ideals in the quadratic field $Q(\sqrt{-D})$.