PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Contributions to the Theory of Diophantine Equations. II. the Diophantine Equation y ^{2} = x^{3} + k

A. Baker

Phil. Trans. R. Soc. Lond. A 1968 **263**, 193-208
doi: 10.1098/rsta.1968.0011

CONTRIBUTIONS TO THE THEORY OF DIOPHANTINE EQUATIONS
II. THE DIOPHANTINE EQUATION $y^2 = x^3 + k$

By A. BAKER
Trinity College, Cambridge

(*Communicated by H. Davenport, F.R.S.—Received 24 August 1967*)

CONTENTS

This paper is a sequel to Part I (Baker 1968) in which an effective algorithm was established for solving in integers x, y any Diophantine equation of the type $f(x, y) = m$, where f denotes an irreducible binary form with integer coefficients and degree at least 3. Here the algorithm is utilized to obtain an explicit bound, free from unknown constants, for the size of all the solutions of the equation. As a consequence of the cubic case of the result, it is proved that, for any integer $k \neq 0$, all integers x, y satisfying the equation of the title have absolute values at most $\exp\{(10^{10}|k|)^{10^4}\}$.

1. Introduction

The problem of finding the totality of integers whose cubes differ by a given integer from a square has interested mathematicians for several centuries. According to Dickson's *History of the theory of numbers* researches on the subject can be traced back at least as far as Bachet (1621), and numerous contributions to the general theory can be found in the works of Fermat, Euler, V. A. Lebesgue, Pepin, Jonquières and many others. More especially, during the past fifty or so years, the equation of the title has been extensively investigated by Mordell (1913, 1914, 1922, 1923, 1963, 1964 and see, in particular, 1947: *A chapter in the theory of numbers*), Nagell (1929, 1930), Delaunay (1929),† Ljunggren (1942, 1963) and Hemer (1952, 1954),‡ and a complete set of solutions in integers has now been obtained for large classes of values of k; these include, for example, all k satisfying $0 < |k| \leqslant 100$, except for 20 special cases.‖ The methods of solution vary widely according to the specific k under discussion, but they usually involve a combination of congruence techniques, together with a detailed study of the arithmetic of certain underlying number fields. In addition, the argument often utilizes the well known connexion between the equation of the title and equations of the kind

$$f(x, y) = m, \tag{1}$$

† See also Delone [Delaunay] & Faddeev (1940).
‡ See also Skolem (1938), Marshall Hall (1953).
‖ An extensive theory has also been developed in connexion with rational solutions; cf. Cassels (1950, 1966), Selmer (1956).

where f denotes an irreducible binary form with integer coefficients and degree at least 3, and m denotes a fixed integer. In particular Mordell (1922, 1923)† has employed this feature, together with the famous theorem of Thue (1909), to show that, for any $k \neq 0$, the equation

$$y^2 = x^3 + k \tag{2}$$

has only a finite number of solutions in integers x, y. No general algorithm, however, has hitherto been established which would enable one to find all the solutions of (2) for any prescribed k.

In a recent paper (Baker 1968)‡ a new proof of the finiteness of the number of solutions of (1) was given, which, in contrast to Thue's original proof, proceeds by an argument that is effective and provides therefore a process for determining all solutions of the equation in integers x, y. Moreover, it was remarked that, in consequence of this result, one could now obtain an effective algorithm for the complete solution of (2) in integers x, y, and it is the purpose of the present paper to supply the details of the demonstration. The precise result that will be established is as follows.

THEOREM 1. *For any integer $k \neq 0$ all solutions of (2) in integers x, y satisfy*

$$\max(|x|, |y|) < \exp\{(10^{10}|k|)^{10^4}\}.$$

Although some care has been taken to obtain numerical constants reasonably close to the best that can be acquired with the present method of proof, there is, nevertheless, little doubt that the numbers on the right of the above inequality can be reduced to a certain extent by means of minor refinements. In particular it will be seen that several of the numbers occurring in our estimates have been freely rounded off in order that the final conclusion should assume a simple form, and so some obvious improvements are immediately obtainable. Furthermore, although at first glance it may appear that the magnitude of the bound furnished by theorem 1 precludes any possibility of practically computing the complete list of solutions of (2) for a given relatively small value of k, the methods used in the proof of the theorem, together with some additional techniques relating to continued fractions, would seem in fact to make the computation feasible, though possibly long. The rate of increase of the bound given by theorem 1 with respect to k is also worth noting; the degree of precision is perhaps best illustrated by expressing the assertion in the form

$$|x^3 - y^2| > 10^{-10}(\log x)^{10^{-4}},$$

the range of validity of this inequality extending to all positive integers x, y with $x^3 \neq y^2$.

The first stage in the proof of theorem 1 rests on the theory of the reduction of binary cubic forms which finds its genesis in Hermite's famous memoir of 1848; the exposition of the present paper will follow the modified approach developed by Davenport (1945) for another purpose, which is slightly simpler and leads to more precise numerical constants. By combining this theory of reduction with the techniques of Mordell (1913), there will be established (see § 2) a quantitative formulation of the connexion mentioned earlier between the solutions of (2) and those of certain equations of the type (1); it will remain then only to apply the work of **B**. In the argument of the latter paper, however, there occurred various constants which were said to be effectively computable but for which, in fact, no explicit

† See also Thue (1917), Landau & Ostrowski (1920), Siegel (1926).

‡ The paper will be referred to as **B**.

values were specified. The detailed calculation of these constants occupies the main part of the present work, and the ultimate theorem that will be established is as follows.

THEOREM 2. *Suppose that $f(x, y)$ is an irreducible binary form with degree $n \geqslant 3$ and with integer coefficients having absolute values at most $\mathscr{H}$. Suppose also that $\kappa > n+1$, and let m denote any positive integer. Then all solutions of (1) in integers x, y satisfy*

$$\max(|x|, |y|) < \exp\{n^{\nu^2}\mathscr{H}^{\nu n^3} + (\log m)^{\kappa}\},$$

where

$$\nu = 32n\kappa^2/(\kappa - n - 1).$$

It will be assumed that the reader is familiar with the work of **B**, and only a minimal amount of the discussion of that paper will be repeated here. In order to obtain the conclusion in the form enunciated above, however, it has been necessary to modify the previous argument to some extent, and in particular it has proved advantageous to re-define one of the basic parameters. Nevertheless, it will be seen that the primary exposition of **B** is not substantially altered. Preliminary to the proof of theorem 2, certain auxiliary results will be required concerning the units of algebraic number fields, and § 3 is devoted to an account of their derivation.

If $\log m < \mathscr{H}$ then clearly the best value (or substantially the best) to assign to κ in theorem 2 is $2n+2$, and one deduces easily that all solutions of (1) in integers x, y satisfy

$$\max(|x|, |y|) < \exp\{(n\mathscr{H})^{(10n)^5}\}.$$

As indicated in the earlier context, some diminution in the values of the constants is certainly possible here, and, in fact, in the proof of theorem 1, a slightly sharper form of this result has been employed. But the best possible choice for the parameters occurring in the derivation of theorem 2 will inevitably vary a little according to the particular application one has in mind, and it may well be profitable to re-work the proof to a certain degree if, for example, one has some additional information concerning the binary form f.

2. ON THE REDUCTION OF BINARY CUBIC FORMS

It will be proved in § 6 that if $f(x, y)$ denotes an irreducible binary cubic form with integer coefficients having absolute values at most $\mathscr{H}$ then all solutions in integers x, y of

$$f(x, y) = 1$$

satisfy

$$\max(|x|, |y|) < \exp\{(10^5\mathscr{H})^{15\times 10^3}\}.$$

The result is employed in the present section to establish theorem 1.

Let k denote any integer other than 0 and suppose that x, y are integers satisfying (2). It can be assumed, without loss of generality, that $x > 0$, $y > 0$, for clearly, if $x < 0$, then $|x| \leqslant |k|^{\frac{1}{3}}$ and so theorem 1 is certainly valid. We denote by $f(X, Y)$ the binary cubic form

$$X^3 - 3xXY^2 - 2yY^3.$$

It will be observed immediately that, by virtue of (2), the discriminant $\mathscr{D}$ of f is given by $-108k$. We proceed now to prove that f can be reduced by an integral unimodular substitution to a binary cubic form f' in which each coefficient has absolute value at most $|\mathscr{D}|^{\frac{1}{2}}$. Two cases are distinguished according as $k < 0$ or $k > 0$.

(i) Suppose first that $k < 0$. Then the quadratic covariant of $f(X, Y)$, defined by

$$F(X, Y) = \frac{1}{4}\left\{\left(\frac{\partial^2 f}{\partial X\,\partial Y}\right)^2 - \frac{\partial^2 f}{\partial X^2}\frac{\partial^2 f}{\partial Y^2}\right\} = 9(xX^2+2yXY+x^2Y^2),$$

has positive discriminant $3\mathscr{D}$ and is thus positive definite. Hence there exists a substitution

$$X = pX'+qY', \quad Y = rX'+sY'$$

with integer coefficients p, q, r, s satisfying

$$ps-qr = \pm 1$$

which transforms $F(X, Y)$ into

$$F'(X', Y') = AX'^2+BX'Y'+CY'^2,$$

where A, B, C denote integers satisfying

$$0 \leqslant B \leqslant A \leqslant C.$$

Let $$f'(X', Y') = aX'^3+bX'^2Y'+cX'Y'^2+dY'^3$$

denote the corresponding transform of f. Then by the covariant property of F we have

$$F' = \frac{1}{4}\left\{\left(\frac{\partial^2 f'}{\partial X'\,\partial Y'}\right)^2 - \frac{\partial^2 f'}{\partial X'^2}\frac{\partial^2 f'}{\partial Y'^2}\right\},$$

whence $$A = b^2-3ac, \quad B = bc-9ad, \quad C = c^2-3bd.$$

Now since $$4AC-B^2 = 3\mathscr{D} > 0$$

and $B \leqslant (AC)^{\frac{1}{2}}$ we see that $AC \leqslant \mathscr{D}$. Further we have

$$2|bc|\,(AC)^{\frac{1}{2}} \leqslant Ac^2+Cb^2 = AC+Bbc \leqslant AC+|bc|\,(AC)^{\frac{1}{2}}$$

and thus $$|bc| \leqslant (AC)^{\frac{1}{2}} \leqslant \mathscr{D}^{\frac{1}{2}}.$$

Also it is clear that $$9|ad| = |bc-B| \leqslant 2\mathscr{D}^{\frac{1}{2}},$$

and the required bound for the absolute values of a, b, c, d follows immediately, provided that none of the latter is 0. The cases in which this condition does not hold are easily treated. If, for example, $d = 0$ then

$$A = b^2-3ac, \quad B = bc, \quad C = c^2$$

and since $A \neq 0$, $C \neq 0$ we have

$$|b| \leqslant B \leqslant \mathscr{D}^{\frac{1}{2}}, \quad |c| = C^{\frac{1}{2}} \leqslant \mathscr{D}^{\frac{1}{2}}.$$

Also $3ac \leqslant b^2$, and from $B \leqslant C$ we deduce that $|b| \leqslant |c|$ and thus $|a| \leqslant |c|$. This proves the assertion when $d = 0$, and the other cases follow similarly.

(ii) Suppose that $k > 0$. Then we have

$$f(X, Y) = (X+\theta Y)\,F(X, Y),$$

where θ is real and $F(X, Y)$ denotes a positive definite quadratic form. By a substitution of

the type specified in (i), $f(X, Y)$ can be transformed into

$$f'(X', Y') = (X' + \phi Y')\, F'(X', Y'),$$

where, on adopting the above notation for F', A, B, C now represent real numbers satisfying

$$-A \leqslant B \leqslant A \leqslant C$$

and $\phi \geqslant 0$. Clearly we have

$$a = A, \quad b = \phi A + B, \quad c = \phi B + C, \quad d = \phi C$$

and

$$-\mathscr{D} = (4AC - B^2)\,(A\phi^2 - B\phi + C)^2.$$

Now since

$$A\phi^2 - B\phi + C \geqslant A(\phi^2 - \phi) + C \geqslant C - \tfrac{1}{4}A \geqslant \tfrac{3}{4}C$$

and also

$$4AC - B^2 \geqslant 3AC$$

we see that $AC^3 \leqslant |\mathscr{D}|$. Thus, on noting that A is a positive integer, we obtain

$$C \leqslant (|\mathscr{D}|/A)^{\frac{1}{3}}, \quad |B| \leqslant A \leqslant |\mathscr{D}|^{\frac{1}{4}},$$

and, since $|\mathscr{D}| \geqslant 108$, it follows immediately that $A \leqslant \frac{1}{3}|\mathscr{D}|^{\frac{1}{2}}$ and $C \leqslant \frac{1}{2}|\mathscr{D}|^{\frac{1}{2}}$; moreover, in the latter inequality, $\frac{1}{2}$ can be replaced by $\frac{1}{3}$ unless $A < 3^3/|\mathscr{D}|^{\frac{1}{2}}$ (< 3). Now if $\phi \leqslant 2$ then obviously we have the required bounds for the absolute values of a, b, c, d. But the assertion holds also if $\phi > 2$, for then $\phi^2 - \phi > \frac{1}{2}\phi^2$ and thus

$$|\mathscr{D}| \geqslant 3AC(\tfrac{1}{2}A\phi^2 + C)^2;$$

in particular we see that $|\mathscr{D}| > 3(AC\phi)^2$ and so

$$|d| = C\phi \leqslant |\mathscr{D}|^{\frac{1}{2}};$$

further we have

$$|\mathscr{D}| \geqslant 3AC(A\phi + C)^2,$$

whence

$$\max(|b|, |c|) \leqslant A\phi + C \leqslant |\mathscr{D}|^{\frac{1}{2}}.$$

We now utilize the substitution derived above to prove theorem 1. It is necessary to distinguish two cases according as f' is or is not reducible.

(I) Suppose that f' is irreducible. On equating the coefficients of X^3 in the equation

$$f'(sX - qY, -rX + pY) = \pm f(X, Y) \tag{3}$$

we obtain

$$as^3 - bs^2r + csr^2 - dr^3 = \pm 1. \tag{4}$$

Hence by the result enunciated at the outset and the supposed irreducibility of f', we deduce immediately that

$$\max(|r|, |s|) < M,$$

where

$$M = \exp\{(10^5 |\mathscr{D}|^{\frac{1}{2}})^{15 \times 10^3}\}.$$

Further, on differentiating the identity

$$f(pX' + qY', rX' + sY') = f'(X', Y')$$

with respect to X', substituting $X' = s$, $Y' = -r$, and recalling that f includes no term in X^2Y, we see that

$$3p = 3as^2 - 2brs + cr^2.$$

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Hence we have

$$|p| \leqslant 2|\mathscr{D}|^{\frac{1}{2}} M^2,$$

and the same inequality is valid with p replaced by q. Now on equating the coefficients of XY^2 in (3) we obtain

$$3(drp^2 - asq^2) + 2pq(bs - cr) + brq^2 - csp^2 = \pm 3x,$$

and it follows easily that $3x \leqslant 12|\mathscr{D}|^{\frac{1}{2}} M(2|\mathscr{D}|^{\frac{1}{2}} M^2)^2$.

Further, on equating the coefficients of Y^3 in (3) we get

$$aq^3 - bpq^2 + cp^2q - dp^3 = \pm 2y$$

and thus $2y \leqslant 4|\mathscr{D}|^{\frac{1}{2}} (2|\mathscr{D}|^{\frac{1}{2}} M^2)^3$.

Hence we see that $\max(x, y) < 16\mathscr{D}^2 M^6 < \exp\{(10^5 |\mathscr{D}|^{\frac{1}{2}})^{16\times 10^3}\}$,

and theorem 1 follows immediately on writing $|\mathscr{D}| = 108|k|$.

(II) Suppose that f' is reducible. Then there exist relatively prime integers u, v (possibly 1, 0 or 0, 1) such that

$$au^3 - bu^2v + cuv^2 - dv^3 = 0. \tag{5}$$

Without loss of generality we shall suppose that $v \neq 0$. Since obviously u and v each divide some non-zero coefficient a, b, c, d, we have

$$|u| \leqslant |\mathscr{D}|^{\frac{1}{2}}, \quad |v| \leqslant |\mathscr{D}|^{\frac{1}{2}}.$$

Now, as in (I), we see that r, s satisfy (4), and on multiplying (4) by v^3, (5) by r^3 and subtracting, we obtain

$$UV = \pm v^3,$$

where

$$U = vs - ur,$$

$$V = (au^2 - buv + cv^2) r^2 + (au - bv) vrs + av^2 s^2.$$

Since U, V divide v^3 we have

$$|U| \leqslant |\mathscr{D}|^{\frac{3}{2}}, \quad |V| \leqslant |\mathscr{D}|^{\frac{3}{2}}.$$

Further we note that V can be written in the form

$$(3au^2 - 2buv + cv^2) r^2 + (3au - bv) rU + aU^2,$$

and the coefficient of r^2 here cannot be 0, for otherwise $(vX' + uY')^2$ would divide $f'(X', Y')$ and so the discriminant $-108k$ of f' would vanish. Thus, if $r \neq 0$, we obtain

$$r^2 \leqslant |U|\{|r(3au - bv)| + |aU|\} + |V| \leqslant 6|r|\,|\mathscr{D}|^{\frac{5}{2}}$$

and hence

$$|r| \leqslant 6|\mathscr{D}|^{\frac{5}{2}}.$$

A similar inequality holds with r replaced by s, and so certainly

$$\max(|r|, |s|) < M,$$

where M is defined as in (I). The argument now proceeds as before.

3. On the units of algebraic number fields

Let α denote an algebraic integer of degree n and let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ denote the conjugates of α arranged so that $\alpha^{(1)}, \ldots, \alpha^{(s)}$ only are real and $\alpha^{(s+1)}, \ldots, \alpha^{(s+t)}$ are the complex conjugates of $\alpha^{(s+t+1)}, \ldots, \alpha^{(n)}$ respectively; thus it is implied that $n = s+2t$. Let K denote the algebraic number field generated by α over the rationals and let $\theta^{(1)}, \ldots, \theta^{(n)}$ denote the conjugates of any element θ of K corresponding to the conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$ of α. Further, let D denote any number which exceeds the absolute value of the discriminant of α, that is

$$\prod_{1 \leqslant i < j \leqslant n} |\alpha^{(i)} - \alpha^{(j)}|^2.$$

In this section we shall prove that there exist $r = s+t-1$ units $\eta_1, \ldots, \eta_r$ in K such that

$$|\log |\eta_k^{(j)}|| \leqslant \tfrac{1}{2} \log D \quad (1 \leqslant j, k \leqslant r, j \neq k) \tag{6}$$

and

$$r! \log D \leqslant \log |\eta_k^{(k)}| \leqslant 2(r!+1)\, D^{(n+1)/2} \log D \quad (1 \leqslant k \leqslant r). \tag{7}$$

Units with these properties will play a fundamental rôle in the subsequent work.

We note first that for any positive numbers $\lambda_1, \ldots, \lambda_r$ there exists an algebraic integer θ of K such that

$$\lambda_j / D^{\frac{1}{2}} \leqslant |\theta^{(j)}| \leqslant \lambda_j \quad (1 \leqslant j \leqslant r)$$

and

$$|\operatorname{norm} \theta| \leqslant D^{\frac{1}{2}}.$$

To verify this assertion we define λ_{r+1} as

$$D^{\frac{1}{2}} / (\lambda_1 \ldots \lambda_r) \quad \text{or} \quad D^{\frac{1}{2}} / (\lambda_1 \ldots \lambda_s \lambda_{s+1}^2 \ldots \lambda_r^2)^{\frac{1}{2}}$$

according as $t = 0$ or $t \neq 0$, and we observe that, by Minkowski's theorem on linear forms (see, for example, Cassels 1959, p. 73, theorem III) there exist rational integers $x_1, \ldots, x_n$, not all 0, such that

$$|\theta^{(j)}| \leqslant \lambda_j \quad (1 \leqslant j \leqslant s),$$

$$|\Re \theta^{(j)}| \leqslant \lambda_j / \sqrt{2}, \quad |\Im \theta^{(j)}| \leqslant \lambda_j / \sqrt{2} \quad (s+1 \leqslant j \leqslant s+t),$$

where

$$\theta = x_1 + x_2 \alpha + \ldots + x_n \alpha^{n-1};$$

the hypotheses of Minkowski's theorem are satisfied, for it is easily seen that the absolute value of the determinant of the linear forms on the left of these inequalities does not exceed $2^{-t} D^{\frac{1}{2}}$, and this is precisely the product of the constants on the right. Now the inequalities obviously imply that $|\theta^{(j)}| \leqslant \lambda_j$ $(1 \leqslant j \leqslant r+1)$, and so certainly

$$|\operatorname{norm} \theta| \leqslant D^{\frac{1}{2}}.$$

Since also

$$|\operatorname{norm} \theta| \geqslant 1$$

we see that

$$|\theta^{(j)}| \geqslant \lambda_j / (\lambda_1 \ldots \lambda_s \lambda_{s+1}^2 \ldots \lambda_{s+t}^2) = \lambda_j / D^{\frac{1}{2}},$$

and thus θ has all the required properties.

Now let k denote any integer satisfying $1 \leqslant k \leqslant r$, and for each $l = 1, 2, \ldots$ let θ_{kl} denote the element θ of K corresponding as above to the set of positive numbers

$$\lambda_j = D \quad (1 \leqslant j \leqslant r, j \neq k), \quad \lambda_k = D^{(r!+1)l}.$$

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

By virtue of the inequality

$$|\text{norm}\,\theta_{kl}| \leqslant D^{\frac{1}{2}},$$

we see that among the numbers θ_{kl} with $1 \leqslant l \leqslant [D^{\frac{1}{2}}]^{n+1}+1$ there is at least one pair $\theta_{kl'}$ and $\theta_{kl''}$ with $l' > l''$ such that the norms of $\theta_{kl'}$ and $\theta_{kl''}$ have the same absolute value, say N, and, further, the corresponding integers x'_j and x''_j satisfy

$$x'_j \equiv x''_j \pmod{N} \quad (1 \leqslant j \leqslant n).$$

On writing $\eta_k = \theta_{kl'}/\theta_{kl''}$ we see that norm $\eta_k = \pm 1$, and since both

$$\phi = (\theta_{kl'} - \theta_{kl''})/N \quad \text{and} \quad N/\theta_{kl''}$$

are algebraic integers in K, we deduce that also

$$\eta_k = 1 + N\phi/\theta_{kl''}$$

is an algebraic integer in K. Hence η_k is a unit in K, and it remains only to verify (6) and (7). But now (6) is clear, for if $j \neq k$, then $\log|\theta^{(j)}_{kl'}|$ and $\log|\theta^{(j)}_{kl''}|$ each lie between $\frac{1}{2}\log D$ and $\log D$, and (7) is valid since obviously

$$\log|\theta^{(k)}_{kl'}| - \log|\theta^{(k)}_{kl''}|$$

is not less than $\{(r!+1)(l'-l'') - \frac{1}{2}\}\log D,$

and cannot exceed $(r!+1)\,l'\log D.$

This completes the proof of the initial assertion.

4. On the logarithms of algebraic numbers

Henceforth it will be assumed that the reader is familiar with the work of **B**. The object of the present section is to prove that a suitable value for the number C specified in theorem 4 of **B** is given by

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

where $$B = \max(4, A', A_1, \ldots, A_{n-1})$$

and $$\rho = 8n\kappa(\kappa+n+1)/(\kappa-n-1).$$

To obtain the conclusion in this form several modifications to the arguments of §§ 3, 4 and 5 of **B** have been introduced. Nevertheless, the basic structure of the exposition remains essentially unaltered, and it will suffice therefore to give an account only of those points in the discussion which differ from their counterparts given previously, or which require a more detailed consideration.

The definitions given in § 3 of **B** remain unchanged, except that we now specify h by the equations

$$k = [H^{\zeta}], \quad h = [k^{\frac{1}{4}\epsilon}],$$

and we suppose that $\delta \leqslant 1$. It is assumed that (10) of **B** holds, where C is given by (8), and we proceed to prove that H is then sufficiently large for the validity of the subsequent argument. It will be noted immediately that ρ, as defined above, can be expressed alternatively as $4(\epsilon\zeta)^{-1}$ and so, since $H > C$, we have

$$h > k^{\frac{1}{4}\epsilon} - 1 > \tfrac{2}{3}H^{\frac{1}{4}\epsilon\zeta} - 1 > \tfrac{1}{2}H^{\frac{1}{4}\epsilon\zeta}.$$

Thus we see that $h > \frac{1}{2}C^{1/\rho}$, whence $h > (2\rho g)^2$, (9)

and also $h > 2^{\frac{1}{2}\rho+2} n\delta^{-1} D \log(dB)$ (10)

(where $D = d^n$, as in **B**). Frequent allusion to (9) and (10) (and more especially to the latter inequality) will be made throughout the later discussion.

The narrative which follows is partitioned to correspond to the lemmas and the final deduction as given in **B**.

Lemma 1. Unchanged.

Lemma 2. A slightly stronger form of the result is established in which l extends over the range $1 \leqslant l \leqslant Dh$ in place of $1 \leqslant l \leqslant h$.

First, we note that a suitable choice for c_1 is $2B$. Further we observe that the new value for U can be taken as $(2B)^{nLDh}(2A)^{L_n Dh}(2LH^g)^k$.

Since now $M \leqslant D^2(k+1)^{n-1}h$, the inequality $N > 2M$ will be satisfied provided that $k^\epsilon > 2^n D^2 h$, and this condition is certainly valid for we have $k^\epsilon > h^4$ and† $\rho > 46n(n+1)$. By virtue of the latter inequality we see that $h > 2^{100}$, whence $h^{\frac{1}{2}} > 2\log(4h)$ and thus, by (9),

$$e^{\frac{1}{2}h} > (4h)^{h^{\frac{1}{2}}} > (4h)^{2\rho g} > (2k)^{2g/\zeta} > H^{g+1},$$

in confirmation of (19) of **B**. The bound $NU \leqslant e^{hk}$ follows from (18) and (19) of **B**, on noting that, by (10) and the inequality $L \leqslant kh^{-4}$, we have

$$k^n < e^{\frac{1}{8}hk}, \quad 2Dk^{1-n\epsilon} < \tfrac{1}{8}k, \quad nDL\log(4B) < \tfrac{1}{8}k.$$

A suitable choice for c_3 is clearly given by $(4dB)^2$. Also we observe that

$$|\log\alpha_j| \leqslant \{(\log|\alpha_j|)^2 + \pi^2\}^{\frac{1}{2}} \leqslant 4\log(dB) \quad (1 \leqslant j \leqslant n).$$

Thus we can take c_4 as $(4dB)^n$, and we have then $c_4^{k+LDh} < e^{\frac{1}{2}hk}$. To confirm the final assertion we note that $c_3^D < e^h$ and so (15) of **B** holds provided only that $H > 8\delta^{-1}h^2k$; and the latter condition is satisfied since $H \geqslant k^{1/\zeta} \geqslant h^\rho$ and $\zeta < \frac{1}{3}$.

Lemma 3. It is shown that suitable values for c_5 and c_6 are given by $(dB)^{6n}$ and $2(dB)^{2n}$ respectively.

The value for c_5 is easily verified for, by virtue of the bound for $|\log\alpha_n|$ noted above, c_7 and c_8 can be taken as $(dB)^6$ and $4\log(dB)$ respectively, and obviously both k^n and c_8^k do not exceed $e^{\frac{1}{4}hk}$.

To confirm the value for c_6 we note first that c_9 can be taken as $(dB)^{2(n-1)}$, whence by (18) of **B** and the inequality $k^n < e^{\frac{1}{8}hk}$, we see that an appropriate choice for c_{10} is $(dB)^{2n}$. Further it is clear that c_{11} can be defined as $c_3c_4 = (4dB)^{n+2}$. Since

$$Ll \leqslant hk^{(1/\zeta)-\frac{1}{2}\epsilon} \leqslant H^{1-1/\rho} \quad \text{and} \quad H > C$$

we have then $c_{11}^{Ll}\, e^{hk-\delta H} < e^{-\frac{3}{4}\delta H}$, and the subsequent deduction arising from this inequality is easily verified. A suitable value for c_{12} is B^{n-1}, and, since $A^{L_n} < e^L < B^L$, we see that c_{13} can be taken as B^n. Further, an appropriate choice for c_{15} is obviously $4\log(dB)$. To calculate c_{14} we note first that

$$|\alpha_j - 1| = |e^{\log\alpha_j} - 1| \leqslant |\log\alpha_j|\, e^{|\log\alpha_j|} \leqslant |\log\alpha_j|\,(dB)^4,$$

and, secondly, that each conjugate of $\alpha_j - 1$ has absolute value at most $2\,dB$. Also, in view

† For a given n, the smallest value assumed by ρ is $8(3+2\sqrt{2})\,n(n+1)$, the value being attained when $\kappa = (1+\sqrt{2})\,(n+1)$.

of the hypothesis of theorem 4, we have $\alpha_j \neq 1$ and so $|\text{norm}\,(\alpha_j - 1)| \geqslant B^{-1}$; this gives $|\log \alpha_j| \geqslant (2dB)^{-d-4}$, whence c_{14} can be defined as $(2dB)^{d+4}$. We observe next that $e^h > c_{14}$, $c_{10} > c_{13}$ and thus an appropriate choice for c_{16} is $c_{10} = (dB)^{2n}$. To complete the discussion of lemma 3 it suffices now to verify that $2\,e^{2Dhk}$, c_{16}^{DLl} and c_{15}^{k} are all less than $e^{\frac{1}{8}\delta H}$, and this follows easily on noting again that $Ll \leqslant H^{1-1/\rho}$, $hk \leqslant H^{\frac{1}{2}}$ and $H > C$.

Lemma 4. The assertion is modified slightly so that, when $J = 0$, the range for l reads $1 \leqslant l \leqslant Dh$. The conclusion remains valid in this case in view of the strengthened version of lemma 2.

The definitions introduced in the course of the proof remain unaltered except that R_0 is now taken as Dh instead of h and the radius of Γ is specified as $R_{K+1}h$ instead of $R_{K+1}\log k$.

The first inequality requiring verification occurs in (27) where it is asserted that

$$h < H^{\frac{1}{2}\{1-(n+1)\zeta\}};$$

this is obviously valid, for we have

$$\tfrac{1}{2}\{1-(n+1)\zeta\} = 4n\kappa/\rho$$

and $H \geqslant h^{\rho}$. Further, in order that the next displayed set of inequalities should hold, we require $H(8n)^k < e^{\frac{1}{4}\delta H}$, and this is again readily confirmed since $k \leqslant H^{\frac{1}{2}}$. Furthermore, the inequality $R_{K+1} \leqslant H$ occurring at the beginning of the next paragraph is valid, for obviously we have $hk^{\frac{1}{2}\epsilon-1} < 1$. It is then necessary to confirm that

$$R_K(S_{K+1}+1) < \tfrac{1}{8}\delta H/\log H;$$

by (27), this holds if

$$H^{\frac{1}{2}\{1-(n+1)\zeta\}} > 8h\,\delta^{-1}\log H.$$

But as above we see that the number on the left is at least $h^{4n\kappa}$, and, since $H \leqslant (4h)^{\rho}$, the number on the right is at most $8\rho h\delta^{-1}\log(4h)$; the inequality now follows easily from (10). The bound expressed by $|f(l)| > 2\,e^{-\frac{1}{8}\delta H}$ is verified by observations similar to those recorded at the end of the discussion of lemma 3.

In view of the change in the radius of Γ introduced earlier, we now have

$$\Theta \geqslant (\tfrac{1}{2}R_{K+1}h)^{R_K(S_{K+1}+1)} \quad \text{and} \quad \theta \leqslant e^{2hk}\,c_5^{LR_{K+1}h}.$$

Further, since $c_6 < c_5$, we see that the bound asserted for $\theta\,|f(l)|^{-1}$ is valid. Thus it remains only to consider the inequality (32). This now reads

$$\log 4 + (D+1)\{2hk + c_{17}LR_{K+1}h\} \geqslant R_K(S_{K+1}+1)\log(\tfrac{1}{2}h),$$

where $c_{17} = \log c_5$. When $K = 0$ we obtain

$$\log 4 + (D+1)(2hk + c_{17}k) \geqslant \tfrac{1}{2}Dhk\log(\tfrac{1}{2}h).$$

But on recalling that $c_5 = (dB)^{6n}$ it follows easily from (10) that the number on the left is at most $8Dhk$, and, since $\log(\frac{1}{2}h) > 2^5$, this is clearly incompatible with the number on the right. When $K > 0$ we obtain

$$\log 4 + (D+1)\{2hk + c_{17}k^{\frac{1}{2}\epsilon K+1}\} \geqslant 2^{-(K+2)}hk^{\frac{1}{2}\epsilon K+1}\log(\tfrac{1}{2}h).$$

Now $K < \tau - 1 < \frac{1}{2}\rho$ (since $n - 1 < \zeta^{-1}$) and, on noting again that $\log(\frac{1}{2}h) > 2^5$, it follows easily that the number on the right exceeds $2^{-\frac{1}{2}\rho+3}hk^{\frac{1}{2}\epsilon K+1}$. But we have $k^{\frac{1}{2}\epsilon} > h^2$ and, by (10),

$$h > 2^{\frac{1}{2}\rho-1}c_{17}D.$$

Hence the inequality is inconsistent also in the case when $K > 0$, and the discussion of lemma 4 is complete.

Lemma 5. A slightly sharper result is established in which $\log k$ on the right of (33) is replaced by 2^τ.

The integer Y specified in the proof is now defined as $[k/2^{\tau+1}]$, and the radius of the circle Γ is taken as Xh instead of $X \log k$. The first inequality requiring verification, namely $(8n)^{k+2}H < \mathrm{e}^{\frac{1}{4}\delta H}$, is easily seen to hold (cf. lemma 4). The lower bound for $|\Xi|$ now reads $(\frac{1}{2}Xh)^{X(Y+1)}$, and the upper bound for ξ is now given by $\mathrm{e}^{2hk} c_5^{LXh}$. Thus the two terms $\log k$ appearing in the upper bound for $|\phi(w)|$ must now be replaced by h. Further, we now have

$$2XY \log (2X) \leqslant 2\epsilon(\tau-1)\, k^{\frac{1}{2}\epsilon(\tau-1)+1} \log k.$$

But $2\epsilon(\tau-1) \leqslant 4\zeta^{-1}$, $\log k \leqslant \zeta \log H$ and

$$k^{\frac{1}{2}\epsilon(\tau-1)+1} \leqslant H^{\frac{1}{2}\{(n+1)\zeta+1\}} = H^{1-4n\kappa/\rho},$$

whence the number on the right does not exceed $\frac{1}{8}\delta H$ (again cf. lemma 4). Also, since $Lh \leqslant kh^{-3}$, we have

$$\tfrac{1}{2}(Y+1) > k/2^{\tau+2} > k/2^{\frac{1}{2}\rho+3} > Lh \log c_5,$$

and clearly

$$\tfrac{1}{2}X(Y+1) > 2hk + \log 2.$$

Thus we obtain

$$|\phi(w)| \leqslant (\tfrac{1}{16}h)^{-X(Y+1)} + \mathrm{e}^{-\frac{1}{8}\delta H};$$

and the number on the right is at most $h^{-\frac{1}{2}X(Y+1)}$, for it is easily seen that

$$X(Y+1) \log h < \tfrac{1}{8}\delta H.$$

For the last part we use the inequalities

$$j!\, 4^j \leqslant (4k^n)^{k^n} \leqslant \mathrm{e}^{k^{n+\frac{1}{2}}}.$$

Since, from (37) of **B**,

$$\tfrac{1}{4}X(Y+1) > k^{\frac{1}{2}\epsilon(\tau-1)+1}/2^{\tau+4} > k^{n+\frac{1}{2}},$$

we deduce easily that

$$|\phi_j(0)| < h^{-\frac{1}{4}X(Y+1)},$$

and the modified form of (33) follows by virtue of the estimate $\log h > 2^6$.

Lemma 6. A suitable value for c_{20} is $(dB)^{2nD}$. For clearly the absolute value of each conjugate of ω is at most $2(dB)^{2(n-1)T} A^{2|t_n|}$, whence c_{21} can be taken as $(dB)^{2n}$. Further, a suitable value for c_{22} is given by B^n. Thus, if $|W| < 1$, we have

$$|\omega| \leqslant |W|\, \mathrm{e} B^{nT} A^{|t_n|} \leqslant |W|\, c_{21}^T A^{|t_n|},$$

and the asserted value for c_{20} follows immediately.

Final deduction. By the bound for $|\log \alpha_n|$ given above, we see that a suitable value for c_{23} is $4n \log (dB)$. Since, by (11) of **B**,

$$|\gamma_1 \log \alpha_1 + \ldots + \gamma_{n-1} \log \alpha_{n-1}| \leqslant |\psi_r| + L\, \mathrm{e}^{-\delta H} \leqslant 8nL \log (dB),$$

we deduce that c_{24} can be taken as $16n \log (dB)$. To show that

$$|\phi_j(0) - \Psi_j| < \mathrm{e}^{-\frac{1}{2}\delta H}$$

we observe first that

$$(R+1)\, (c_{24} L)^R \leqslant (32n \log (dB))^R \leqslant h^R$$

and $hk < \frac{1}{4}\delta H$. Thus it suffices to verify that $R \log h < \frac{1}{4}\delta H$; but this certainly holds, for we

have $R \leqslant H^{\zeta n}$, $\zeta < 1/(n+1)$ and $H^{1/(n+1)} > 4\delta^{-1}\log h$. In accordance with the modified form of lemma 5, the term $\log k$ in (38) is now to be replaced by 2^τ.

The lower bound asserted for $|\psi_r - \psi_s|$ is at least $(dB)^{-2nDk}\,\mathrm{e}^{-k}$, since, by (18) of **B**, we have

$$2DL_n \log A < 4Dk^{1-n\epsilon} < k.$$

It follows easily that a suitable value for c_{25} is $4nD\log(dB)$. Clearly c_{26} and c_{27} can be taken as 2 and 3 respectively. On replacing $\log k$ in the inequality for $\log|p_r\Delta_r(\psi_r)|$ by 2^τ, and noting also that

$$\log(R+1) + R\log(c_{27}k) \leqslant 2k^n \log k \leqslant k^{n+1}/2^{\tau+2},$$

we see that the asserted upper bound for $\log|\Delta_r(\psi_r)|$ is valid, again with 2^τ in place of $\log k$. Thus the final conclusion holds if

$$k^{\frac{1}{2}\epsilon(\tau-1)+1}/2^{\tau+3} > c_{25}k^{n+1},$$

that is if

$$k^{\frac{1}{2}\{(1/\zeta)-(n+1)\}} > 2^{\tau+5}nD\log(dB).$$

But $\tau \leqslant \frac{1}{2}\rho + 1$ and the number on the left can be expressed as $k^{\epsilon n\kappa} \geqslant h^{4n\kappa}$. The validity of the inequality is now obvious, and the proof of the opening assertion is complete.

To conclude this section we observe that, by virtue of the result just established, an appropriate choice for the constant C specified in theorem 3 of **B** is given by

$$C^{1/\rho} = 2^{\frac{1}{2}\rho+5}n\delta^{-1}d^n\log(dB),$$

where B and ρ are defined as above, and where n must be replaced by $n+1$ if $\alpha_1, \ldots, \alpha_n$ are not all real (the substitution of $n+1$ for n applies to ρ but not to B). The assertion is easily verified by a study of section 2 of **B**. For suppose first that $\alpha_1, \ldots, \alpha_n$ are all real. Then the hypotheses of theorem 3 imply that (7) of **B** holds with $\alpha_1, \ldots, \alpha_n$ replaced by $|\alpha_1|, \ldots, |\alpha_n|$ respectively and with δ replaced by $\frac{1}{2}\delta$, provided only that $\mathrm{e}^{\frac{1}{2}\delta H} > 4|\alpha_n|^{-1}$. Further, by the arguments following the enunciation of theorem 4, we see that the hypotheses of the latter theorem will be satisfied with g defined as $2n$, with δ replaced by $\frac{1}{4}\delta$ and with the basic algebraic numbers given by some subset of $|\alpha_1|, \ldots, |\alpha_n|$, provided that now $\mathrm{e}^{\frac{1}{4}\delta H} > H^n > 2^n$ and that $|\log\alpha_j| \geqslant \mathrm{e}^{-\frac{1}{2}\delta H}$ for $j = 1, 2, \ldots, n$. Clearly if the above conditions are not satisfied then the desired conclusion is certainly valid. If, on the other hand, the conditions are satisfied then the conclusion follows immediately from theorem 4, on observing that, by virtue of the definition of g, the second term in the expression on the right of (8) is greater than the first. Note also that, throughout the above discussion, it has been assumed that $\delta \leqslant 1$, and, furthermore, implicit reference has been made to the fact that C increases monotonically with respect to n, and exceeds $(\log B)^\kappa$. A similar argument applies when $\alpha_1, \ldots, \alpha_n$ are not all real, the set now being enlarged by the addition of the algebraic number $\alpha_0 = -1$, which clearly does not affect the definitions of d or B.

5. Proof of theorem 2

We now utilize the results obtained in §3 and §4 to establish theorem 2. The discussion is based on §§6 and 7 of **B** with which the reader is again supposed to be familiar.

We note first that there is no loss of generality in assuming that the coefficient of x^n in $f(x, y)$ is ± 1, provided that one establishes, in this case, the stronger conclusion

$$\max(|x|, |y|) < \exp\{\tfrac{1}{2}n^{\nu^2}\mathscr{H}^{\nu n^2} + (\log m)^\kappa\}.$$

For it is clear that the absolute values of the coefficients in the binary form $F(X, Y)$ specified in §6 of **B** do not exceed $\mathscr{H}^n$, and, with the notation of that section, we have either $\log m > 2^{\nu/\kappa}\mathscr{H}^n$, whence, since

$$\nu/\kappa > (\kappa+n+1)/(\kappa-n-1) = \kappa'/(\kappa-\kappa'),$$

it follows that $M < m^2$ and $(\log M)^{\kappa'} < (\log m)^{\kappa}$, or $\log m \leqslant 2^{\nu/\kappa}\mathscr{H}^n$ and thus

$$(\log M)^{\kappa'} \leqslant (\log M)^{\kappa} < 2^{\nu+\kappa}\mathscr{H}^{n\kappa} < n^{2\nu}\mathscr{H}^{\nu n}.$$

The notation of §6 of **B** agrees with that given at the beginning of §3 (on writing $\alpha = \alpha^{(1)}$) and we suppose that $\eta_1, \ldots, \eta_r$ are units in K satisfying (6) and (7). We shall not specify C_1 explicitly, but shall instead employ (6) and (7) directly at the point in the argument where C_1 becomes significant. C_2 can obviously be taken as the number on the extreme right of (7) (D being used now in the sense of §3 and not of §4).

We come now to the discussion of §7 of **B**, and we note first that a suitable value for C_3 is given by n^2C_2. Further we observe that the height of γ cannot exceed $(1+\mathrm{e}^{C_3}m^{1/n})^n$, and so an appropriate choice for C_4 is e^{2nC_3}. In order to define C_5 we use the fact that, by virtue of (6) and (7), the term given by the leading diagonal of Δ, namely

$$\mathscr{P} = \prod_{k=1}^{r} \log|\eta_k^{(k)}|,$$

exceeds the absolute values of each of the $(r!-1)$ remaining terms in the expansion of Δ by at least a factor $2r!$; thus we have

$$|\Delta| > \tfrac{1}{2}\mathscr{P}.$$

Also we see that the absolute value of each of the $(r-1)!$ terms in the expansion of any cofactor of Δ does not exceed the product of $r-1$ numbers from the set $\log|\eta_k^{(k)}|$ $(1 \leqslant k \leqslant r)$, and so, by (7), each cofactor has absolute value at most $(r\log D)^{-1}\mathscr{P}$. It follows easily that an appropriate choice for C_5 is $2(\log D)^{-1}$ (the original designation that $C_1, C_2, \ldots$ should each exceed 1 being disregarded here). On assuming that $H > C_3C_5$ (the condition to be discussed later), (44) of **B** implies that C_6 can be taken as 1, and it follows immediately that suitable values for C_7 and C_8 occurring in (46) of **B** are given by e^{C_3} and nC_5 respectively.

We have now to estimate the heights of $\alpha_1, \ldots, \alpha_{r+1}$, and for this purpose we make the preparatory observation that if α, β denote algebraic numbers with degrees at most d_1, d_2 respectively and with heights at most $\mathscr{H}$, then $\alpha+\beta$ and $\alpha\beta$ have degrees at most $d = d_1d_2$ and heights at most $(4d\mathscr{H}^4)^d$. This follows easily on noting that $\alpha+\beta$ and $\alpha\beta$ are zeros of polynomials of the kind specified in §6 of **B** (with d_1d_2 in place of d^2) and that

$$|1+\alpha^{(i)}+\beta^{(j)}| \leqslant (1+d_1+d_2)\,\mathscr{H}, \quad |1+\alpha^{(i)}\beta^{(j)}| \leqslant (1+d_1d_2)\,\mathscr{H}^2.$$

Now by (6) and (7) it is clear that η_k has height at most $(1+\mathrm{e}^{C_2})\,(1+D^{\frac{1}{2}})^{n-1}$, and this does not exceed e^{2C_2} if one assumes (as will be amply satisfied later) that $D \geqslant 10$. Thus a suitable value for C_9 is given by $\mathrm{e}^{10n^2C_2}$. Further, the height of

$$(\alpha^{(j)}-\alpha^{(l)})/(\alpha^{(k)}-\alpha^{(l)})$$

is at most $\mathscr{H}' = (2n\mathscr{H})^{16n^6}$, and if now we assume that $\mathscr{H}'$ does not exceed C_4, then appropriate choices for C_{10} and C_{11} will be given by $C_4(=\mathrm{e}^{2nC_3})$ and $25n^8$ respectively. Furthermore,

it is clear that both $|\alpha_{r+1}|$ and $|\alpha_{r+1}|^{-1}$ cannot be greater than $n^4\mathscr{H}'\,\mathrm{e}^{2C_3}$, and thus, if $\mathrm{e}^{C_3} > n^4\mathscr{H}'$, a suitable value for C_{12} is e^{3C_3}. Obviously one can then take $C_{13} = C_{12}$.

We observe next that the discriminant of α can be expressed as a Sylvester determinant of order $2n-1$ with elements given by the coefficients of $f(x,1)$ and its derivative with respect to x. On recalling that the leading coefficient in $f(x,1)$ is ± 1, we deduce easily that each of the $(2n-1)!$ terms in the expansion of the determinant has absolute value at most $n^n\mathscr{H}^{2n-2}$, and thus an appropriate choice for D is $n^{5n}\mathscr{H}^{2n-2}$. Since $r \leqslant n-1$ and clearly also $\log D \leqslant n^5\mathscr{H}^{\frac{1}{2}}$ we see that

$$n^{2n^2}\mathscr{H}^{n^2-1} < C_2 < n^{5n^2}\mathscr{H}^{n^2-\frac{1}{2}}.$$

Further we note that the conditions on $\mathscr{H}'$ specified above are satisfied since

$$C_2 > n^{18}\mathscr{H}^8 > n^{16}\log(2n\mathscr{H}) > \log(n^4\mathscr{H}')$$

and $C_4 > \mathrm{e}^{C_3} > \mathrm{e}^{C_2}$. Since also $C_8 = 2n(\log D)^{-1} < \frac{1}{2}$, it is now clear that, subject only to the condition

$$H > \max\{C_3 C_5, \log(C_7 C_{13})\}, \tag{11}$$

all the hypotheses of theorem 3 of **B** will be satisfied with A given by

$$\log A = 25n^8(2n^3C_2 + \log m),$$

with B (as defined in § 4) given by $\mathrm{e}^{10n^2C_2}$, with κ replaced by $\kappa' = \frac{1}{2}(\kappa+n+1)$, with n replaced by $r+1$, with $\delta = 1$ and with $d = n^6$. Thus by the result given at the end of § 4 we conclude that $H < M$, where

$$M = \max\{C', (\log A)^{\kappa'}\},$$

$$C' = \{2^{\frac{1}{2}\rho+5}n^{6n+1}\log(n^6B)\}^{\rho}$$

and

$$\rho = 8n\kappa'(\kappa'+n+1)/(\kappa'-n-1).$$

Now it is easily verified that $\rho < \nu$, where ν is defined in the enunciation of theorem 2, and thus we see that

$$C' \leqslant \{2^{\frac{1}{2}\nu+6}n^{6n+1}\log B\}^{\nu}.$$

Further we have

$$\log B = 10n^2C_2 \leqslant n^{5n^2+5}\mathscr{H}^{n^2-\frac{1}{2}},$$

whence it follows easily that $C' \leqslant C''$, where

$$C'' = \{2^{\frac{1}{2}\nu}n^{9n^2}\mathscr{H}^{n^2-\frac{1}{2}}\}^{\nu}$$

(C'' being used here in a different sense to that indicated in **B**). Furthermore, the number on the right of (11) is precisely $4n^2C_2$, and this is clearly less than M; thus if (11) does not hold then again we have the conclusion $H < M$.

For the final deduction we note that since

$$|\alpha^{(2)} - \alpha^{(1)}| > (2n\mathscr{H})^{-(2n)^2}$$

and both $|\alpha^{(1)}|$ and $|\alpha^{(2)}|$ do not exceed $n\mathscr{H}$, an appropriate choice for C_{14} is $(2n\mathscr{H})^{8n^2}$. Further, by (41) of **B** together with (6) and (7), we deduce that a suitable value for C_{15} is $\mathrm{e}^{2n^2C_2}$. Thus we conclude that

$$\max(|x|, |y|) < m^{1/n}(2n\mathscr{H})^{8n^2}\mathrm{e}^{2n^2C_2M}.$$

Now the number on the right certainly does not exceed $\mathrm{e}^{4n^2C_2M}$, and it remains therefore only to verify that

$$4n^2C_2M \leqslant \tfrac{1}{2}n^{\nu^2}\mathscr{H}^{\nu n^2} + (\log m)^{\kappa}.$$

But since $\nu > 32n^2$ we see that

$$4n^2C_2C'' \leqslant \{2^{\frac{1}{2}\nu}n^{10n^2}\mathscr{H}^{n^2}\}^\nu \leqslant \{(2n)^{\frac{1}{2}\nu}\mathscr{H}^{n^2}\}^\nu,$$

and so the assertion is assuredly valid if $C'' > (\log A)^\kappa$. On the other hand, if $C'' \leqslant (\log A)^{\kappa'}$, then clearly $\log m > C''^{1/(2\kappa')}$ and hence

$$\log A \leqslant 100n^{11}C_2 \log m \leqslant C''^{1/\nu} \log m \leqslant (\log m)^{1+2\kappa'/\nu}.$$

But this implies that

$$4n^2C_2 (\log A)^{\kappa'} \leqslant C''^{1/\nu}(\log A)^{\kappa'} \leqslant (\log m)^{\kappa'+2\kappa'(\kappa'+1)/\nu},$$

and it is readily confirmed that the exponent of $\log m$ on the extreme right does not exceed κ. Thus again the assertion is well-founded, and the proof of theorem 2 is complete.

6. Completion of proof of theorem 1

It remains only to prove the strengthened special case of theorem 2 enunciated at the beginning of § 2. By observations similar to those recorded at the beginning of § 5, it clearly suffices to assume that the coefficient of x^3 in $f(x, y)$ is ± 1, and thence to obtain the conclusion that all solutions in integers x, y of $f(x, y) = m$, where m denotes a positive integer not exceeding $\mathscr{H}^2$, satisfy

$$\max(|x|, |y|) < \exp\{(10^{14}\mathscr{H})^{5\times 10^3}\}.$$

Now by the arguments of § 5 we reach the inequality

$$\max(|x|, |y|) < e^{36C_2M},$$

where C_2 and M are defined as above with $n = 3$ and with κ representing any number > 4. But, by virtue of the supposition $m \leqslant \mathscr{H}^2$, it is clear that $M = C'$, and so we have now merely to verify that, for some κ,

$$36C_2C' < (10^{14}\mathscr{H})^{5\times 10^3}. \tag{12}$$

It is easily seen that ρ, as defined in § 5, assumes is smallest value when $\kappa' = (1+\sqrt{2})(n+1)$. Accordingly we take $\kappa = 4(1+2\sqrt{2})$, whence we have

$$\kappa' = 4(1+\sqrt{2}) \quad \text{and} \quad \rho = 96(3+2\sqrt{2}) < 560.$$

Noting now that

$$C' \leqslant \{2^{\frac{1}{2}\rho+6}3^{19}\log B\}^\rho,$$

that $\log B = 90C_2$ and that also $C_2 < 3^{45}\mathscr{H}^{\frac{17}{2}}$, it readily follows that the number on the left of (12) does not exceed

$$36(3^{45}\mathscr{H}^{\frac{17}{2}})\{2^{286}.3^{66}.10\mathscr{H}^{\frac{17}{2}}\}^{560}.$$

A simple calculation shows that the above expression is less than $(10^{14}\mathscr{H})^{5\times 10^3}$, and this completes the proof of theorem 1.

References

Bachet, C. G. 1621 *Diophanti Alexandrini*. Arith. lib. VI, 422–425. Lutetiae Parisiorum.

Baker, A. 1968 Contributions to the theory of Diophantine equations: I. On the representation of integers by binary forms. *Phil. Trans.* A **263**, 173. (Paper **B**.)

Cassels, J. W. S. 1950 The rational solutions of the Diophantine equation $Y^2 = X^3 - D$. *Acta Math.* **82**, 243–273.

Cassels, J. W. S. 1959 *An introduction to the geometry of numbers*. Berlin, Göttingen, Heidelberg: Springer.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Cassels, J. W. S. 1966 Diophantine equations with special reference to elliptic curves. *J. Lond. Math. Soc.* **41**, 193–291.

Davenport, H. 1945 The reduction of a binary cubic form. *J. Lond. Math. Soc.* **20**, (I) 14–22; (II) 139–147.

Delaunay, B. 1929 Ueber die Darstellung der Zahlen durch binäre kubische Formen von negativer Diskriminante. *Math. Z.* **31**, 1–26.

Delone [Delaunay], B. N. & Faddeev, D. K. 1940 *The theory of irrationalities of the third degree.* Moscow, Leningrad, 1964; Translations: *Math. Monographs* 10; American Math. Soc.

Dickson, L. E. 1920 *History of the theory of numbers.* II, ch. XX. Washington: Carnegie Inst.; reprinted 1952, New York: Chelsea.

Hall, Marshall, Jr. 1953 Some equations $y^2 = x^3 - k$ without integer solutions. *J. Lond. Math. Soc.* **28**, 379–383.

Hemer, O. 1952 *On the Diophantine equation* $y^2 - k = x^3$. Uppsala: Almqvist and Wiksells.

Hemer, O. 1954 Notes on the Diophantine equation $y^2 - k = x^3$. *Ark. Mat.* **3**, 67–77.

Hermite, Ch. 1848 Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indéterminées. *J. reine angew. Math.* **36**, 357–364; = *Oeuvres* I, 84–93.

Landau, E. & Ostrowski, A. 1920 On the Diophantine equation $ay^2 + by + c = dx^n$. *Proc. Lond. Math. Soc.* **19**, 276–280.

Ljunggren, W. 1942 Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante. *Acta Math.* **75**, 1–21.

Ljunggren, W. 1963 On the Diophantine equation $y^2 - k = x^3$. *Acta Arith.* **8**, 451–463.

Mordell, L. J. 1913 The Diophantine equation $y^2 - k = x^3$. *Proc. Lond. Math. Soc.* **13**, 60–80.

Mordell, L. J. 1914 Indeterminate equations of the third and fourth degrees. *Quart. J. pure appl. Math.* **45**, 170–186.

Mordell, L. J. 1922 Note on the integer solutions of the equation $Ey^2 = Ax^3 + Bx^2 + Cx + D$. *Messenger Math.* **51**, 169–171.

Mordell, L. J. 1923 On the integer solutions of the equation $ey^2 = ax^3 + bx^2 + cx + d$. *Proc. Lond. Math. Soc.* **21**, 415–419.

Mordell, L. J. 1947 *A chapter in the theory of numbers.* Cambridge University Press.

Mordell, L. J. 1963 The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, or fifty years after. *J. Lond. Math. Soc.* **38**, 454–458.

Mordell, L. J. 1964 The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. *Rend. Circ. Mat. Palermo* **8**, 1–8.

Nagell, T. 1929 *L'analyse indéterminée de degré supérieur.* Mém. des sciences math. fasc. 39: Gauthier-Villars.

Nagell, T. 1930 Einige Gleichungen von der Form $ay^2 + by + c = dx^3$. *Vid. Akad. Skrifter, Oslo* **1**, no. 7.

Selmer, E. S. 1956 The rational solutions of the diophantine equation $\eta^2 = \xi^3 - D$ for $|D| \leqslant 100$. *Math. Scand.* **4**, 281–286.

Siegel, C. L. 1926 (under the pseudonym X) The integer solutions of the equation

$$y^2 = ax^n + bx^{n-1} + \ldots + k.$$

J. Lond. Math. Soc. **1**, 66–68; = *Ges. Abhandlungen* **1**, 207–208.

Skolem, Th. 1938 *Diophantische Gleichungen. Ergebn. Math.* V, 4. Berlin: Springer; reprinted 1950, New York: Chelsea.

Thue, A. 1909 Über Annäherungswerte algebraischer Zahlen. *J. reine angew. Math.* **135**, 284–305.

Thue, A. 1917 Über die Unlösbarkeit der Gleichung $ax^2 + bx + c = dy^n$ in grossen ganzen Zahlen x und y. *Arch. Math. Naturvid. Kristiania*, B **34**, no. 16.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES