MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 151
JULY 1980, PAGES 991–1002

# Elliptic Curves of Conductor 11

By M. K. Agrawal, J. H. Coates, D. C. Hunt and A. J. van der Poorten

**Abstract.** We determine all elliptic curves defined over Q of conductor 11. Firstly, we reduce the problem to one of solving a diophantine equation, namely a certain Thue-Mahler equation. Then we apply recent sharp inequalities for linear forms in the logarithms of algebraic numbers to bound solutions of that equation. Finally, some straightforward computations yield all solutions of the diophantine equation. Our results are in accordance with the conjecture of Taniyama-Weil for conductor 11.

Taniyama and Weil have asked whether all elliptic curves defined over **Q** of a given conductor $N$ are parametrized by modular functions for the subgroup $\Gamma_0(N)$ of the modular group. The assertion that this question has a positive answer has become known as the Taniyama-Weil conjecture. While the general question seems shrouded in mystery and quite inaccessible at present, one can at least try to verify the conjecture for small numerical values of $N$. A considerable amount of work has already been done in this direction (cf. [4], [5], [19]–[24], [29]). However, the first nontrivial case of the conjecture, namely $N = 11$, has not previously been settled. The aim of this note is to determine all elliptic curves of conductor 11 defined over **Q** and so to verify the conjecture of Taniyama-Weil for $N = 11$.

It is well known that the problem of finding all elliptic curves defined over **Q** of a given conductor $N$ can be reduced to finding $S$-integral points on certain associated curves of genus 1; here $S$ is the set of primes dividing $N$.

For certain values of $N$, these diophantine equations can easily be solved by congruence techniques. However, this elementary approach does not work for $N = 11$, and we are forced to solve these equations by using some recent sharp inequalities for linear forms in the logarithms of algebraic numbers.

The body of this paper is, thus, given over to solving a diophantine equation by Baker's method. Whilst our computations are of course specific to the particular equation we solve, our methods are quite general.

As regards the elliptic curves, we employ the usual notation and terminology. For background and more detailed explanation we refer the reader to the surveys of Swinnerton-Dyer and Birch [31] and of Gelbart [12]; see also Mazur and Swinnerton-Dyer [18].

**1.** An elliptic curve $E$ over a field **K** has a nonsingular plane cubic model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

Received July 29, 1979; revised September 19, 1979.

1980 *Mathematics Subject Classification.* Primary 10F10, 10D12, 10B10, 10B16, 14K07, 12A30.

with the $a_i$ in $\mathbf{K}$. If the characteristic char $\mathbf{K}$ of $\mathbf{K}$ is not 2, we can replace $4(2y + a_1x + a_3)$ by $y$ and $4x$ by $x$ to obtain

$$y^2 = x^3 + b_2x^2 + 8b_4x + 16b_6 \tag{2}$$

with

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6.$$

When also char $\mathbf{K} \neq 3$, replacing $y$ by $4y$ and $x + b_2/3$ by $4x$ yields the familiar Weierstrass equation

$$y^2 = 4x^3 - g_2x - g_3$$

with

$$12g_2 = c_4 = b_2^2 - 24b_4, \quad 216g_3 = c_6 = -b_3^2 + 36b_2b_4 - 216b_6.$$

The curve (1) is nonsingular when its discriminant $\Delta$ does not vanish. Here $\Delta$ is given by

$$1728\Delta = c_4^3 - c_6^2 = (12)^3(g_2^3 - 27g_3^2),$$

or equivalently,

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where

$$4b_8 = b_2b_6 - b_4^2 \quad \text{or} \quad b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

These last equations define $\Delta$ in any characteristic. The $j$-invariant of the curve is $j = c_4^3/\Delta$. The model (1) for an elliptic curve $E$ over $\mathbf{K}$ is unique up to a coordinate transformation of the form

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t$$

with $r$, $s$, $t$, $u$ in $\mathbf{K}$, $u \neq 0$. For full details, see Tate [34].

When $\mathbf{K} = \mathbf{Q}$ (or more generally for the quotient field of any principal ideal domain) we can choose the model (1) with the $a_i$ in $\mathbf{Z}$ and the $p$-order of $\Delta$ minimal for each prime $p$. Supposing (1) is such a global minimal model, we reduce (1) modulo $p$ to obtain a curve $\overline{E_p}$ over the finite field $\mathbf{F}_p$. If the reduction $\overline{E_p}$ of $E$ mod $p$ is elliptic over $\mathbf{F}_p$, that is, if and only if $\Delta \not\equiv 0 \bmod p$, then $E$ is said to have good reduction at $p$. The bad reduction of $E$ is measured by the (geometric) conductor

$$N = \text{Cond } E = \prod_p p^{f_p},$$

where $f_p = 0$ if $p \nmid \Delta$ (so $f_p = 0$ for all but finitely many $p$), whilst $f_p = 1$ if the singularity is a node, and $f_p \geqslant 2$ if the singularity is a cusp (and $f_p \leqslant 2$ if $p > 3$; for details see Ogg [23]). The $f_p$, and hence Cond $E$, are invariant under isogeny (see, for example, Neumann [21]).

Three curves of conductor 11 defined over **Q** were already known, namely

(A) $y^2 - y = x^3 - x^2$, $\Delta = -11$,

(B) $y^2 - y = x^3 - x^2 - 10x - 20$, $\Delta = -11^5$,

(C) $y^2 - y = x^3 - x^2 - 7820x - 263580$, $\Delta = -11$.

Vélu [35] has shown that these three curves are isogenous over **Q**, and that, up to isomorphism, they are a full isogeny class. Conversely, it follows from results of Serre [27] that in the present case, $N = 11$, the Taniyama-Weil conjecture is equivalent to there being exactly one isogeny class of elliptic curves. (For further comment see Gelbart [12, pp. 254–255].) Thus the conjecture is equivalent to the following theorem which we prove in the remainder of the paper.

THEOREM. *The only elliptic curves of conductor* 11 *defined over* **Q** *are, up to isomorphism, the curves* (A), (B), (C) *above.*

**2.** As remarked above, the determination of all elliptic curves with given conductor can be reduced to a problem on solving diophantine equations. Various authors (Ogg [23], [25], Coghlan, Neumann [20], [19], [21]) have dealt with the cases $N = 2^a3^b$ and other cases involving only small primes by showing that the elliptic curves possess rational points of small order. Setzer [29], and Neumann [21], [22] deal with many cases of prime conductor by showing that for $p \neq 2, 3, 17$ there is an elliptic curve conductor $p$ defined over **Q** with a rational point of order 2 if and only if $p = u^2 + 64$ for some integer $u$. On the other hand, unless 3 divides the class numbers of both $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\sqrt{-p})$, for $p \equiv \pm 1 \bmod 8$ a curve of conductor $p$ must possess a rational point of order 2. Hence, for many $p$ there cannot be elliptic curves defined over **Q** with conductor $p$. When $p = 17$ or $p = u^2 + 64$ the curves of conductor $p$ can be displayed explicitly. Of course, all the results obtained are consistent with the Taniyama-Weil conjecture.

Setzer [29], and subsequently Bölling [5], consider the case where $E$ has no rational point of order 2 but has prime conductor $p$. Then the 2-division field $\mathbf{Q}(E_2)$ generated by the coordinates of the 2-division points of $E$ over **Q**, is a Galois extension of **Q** with Galois group $S_3$, and is unramified at all primes distinct from 2 and $p$. This yields only finitely many possibilities for $\mathbf{Q}(E_2)$ and yields elliptic curves $E(u, v)$, where $(u, v)$ is an integer solution of a diophantine equation $f(u, v) = \pm 2^e p^s$ for certain cubic forms $f$ (depending, as does $e$, only on $p$). Conversely, each solution $(u, v)$ of this Thue-Mahler equation determines an elliptic curve with good reduction at all primes distinct from 2 and $p$. One must then exclude those solutions with bad reduction at 2 or bad reduction of the wrong type at $p$. Since, conversely, each elliptic curve of conductor $p$ determines a solution of the diophantine equation, those curves that remain (if any remain) after the exclusion constitute the elliptic curves defined over **Q** of conductor $p$.

Earlier Agrawal and Coates had obtained the same diophantine equations by a much clumsier argument. Namely, elliptic curves of conductor $p$ give rise to a solution

of the diophantine equation $c_4^3 - c_6^2 = \pm(12)^3 p^r$. Using factorization techniques this equation can eventually be transformed into one or more Thue-Mahler equations.

Of course it is easier to show that a diophantine equation has no solutions (or, as in the present case, no solutions satisfying certain additional conditions) than it is to find all solutions when nontrivial solutions exist. Thus Bölling [5] has completed work of Setzer [29] and has found all primes $p \leqslant 401$ for which there are no elliptic curves defined over $\mathbf{Q}$ of conductor $p$. On the other hand, in those cases where there are curves without a rational 2-division point it has not proved possible to determine whether all solutions have been detected. However, we know (see Coates [7] or [30]) that a Thue-Mahler equation has at most finitely many solutions and that all solutions can in principle be effectively found by using Baker's method. In the present paper we actually carry out the necessary computations in the case $p = 11$.

3. Let $E$ be an elliptic curve over $\mathbf{Q}$ with conductor 11, and minimal model (1) with discriminant $\pm 11^r$. Setzer [29] (or see [5]) shows that the 2-division field $\mathbf{Q}(E_2)$ contains a subfield $\mathbf{K}$ cubic over $\mathbf{Q}$, with discriminant $D = \pm 11$ or $\pm 44$. A table of cubic fields (see for example [1]) shows that $D = -44$ is the only possibility, and that $\mathbf{K}$ is generated over $\mathbf{Q}$ by a zero of

$$x^3 - x^2 + x + 1. \tag{3}$$

Let $1, \omega, \mu$ be an integral basis of $\mathbf{K}$. Explicitly, if $\omega$ is a zero of the polynomial $x^3 + bx^2 + acx + a^2 d$ (with $a, b, c, d$ rational integers) and $\mathbf{K} = \mathbf{Q}(\omega)$, then $\mu$ defined by $\omega^2 = -ac - b\omega + a\mu$ will do (this yields a Voronoi basis; see [9]). After a translation, if necessary, there is no loss of generality in supposing that $(\theta, 0)$ with $\theta = u\omega + v\mu$, and $u, v$ rational integers, is a 2-division point of $E$. Setzer shows that

$$N_{\mathbf{K}/\mathbf{Q}}(u\omega + v\mu) = au^3 + bu^2 v + cuv^2 + dv^3 = 2^3 11^s, \tag{4}$$

where $2s + 1 = r$; we can of course take $a = c = d = 1, b = -1$.

Conversely, given an integer solution $(u, v)$ of (4), with $(u, v, 11) = 1$, let $g(x)$ be the minimal polynomial of $\theta$. Explicitly

$$g(x) = x^3 + (bu - cv)x^2 + (acu^2 + (3ad - bc)uv + bdv^2)x + (a^2 du^3 + (2abd - ac^2)u^2 v + (b^2 d - 2acd)uv^2 - ad^2 v^3),$$

which in the present case becomes

$$g(x) = x^3 - (u + v)x^2 + (u^2 + 4uv - v^2)x + (u^3 - 3u^2 v - u^2 v - v^3). \tag{5}$$

Then $y^2 = g(x)$ is an elliptic curve given by a model of the shape (2), with discriminant $\Delta = 2^4(\pm 2^3 11^s)^2 \cdot -44 = -2^{12} 11^{2s+1}$. It remains to determine whether we have a curve of conductor 11.

It is easy to see that the equation (4) with $a = c = d = 1, b = -1$ implies both $u$ and $v$ even. Henceforth, we write $u = 2u', v = 2v'$ and suppress the dash. Then a translation replacing $x$ by $x - 2(u' + v')$ yields the model

$$y^2 = x^3 + 4(u + v)x^2 + 8u(u + 3v)x + 16(u^3 + u^2 v + uv^2 - v^3). \tag{6}$$

But the equations of Section 2 show that in order that the curve have good reduction of 2 it is necessary and sufficient that (in order that we can move from (2) to (1)) $b_2$, $b_6$ be squares mod 4 and $b_2b_6 - b_4^2 \equiv 0 \bmod 4$. Here these conditions are that $4(u + v)$ and $u^3 + u^2v + uv^2 - v^3$ be squares mod 4 and $u^2(3u - v)(u + v) \equiv 0 \bmod 4$, which is $u(u + v) \equiv 0 \bmod 2$. Since, plainly, $(u, v) = 1$ (recall, this is $(u', v') = 1$) it is necessary and sufficient that $u - v \equiv 1 \bmod 4$, and $u \equiv 0 \bmod 2$. Next, we see that (6) is $y^2 \equiv (x + (u - 5v))(x - 4(u - 8v))^2 \bmod 11$. Hence, (6) has additive reduction at 11 if and only if $u \equiv 3v \bmod 11$. Summing up:

PROPOSITION. *Each elliptic curve $E = E(u, v)$ defined over* **Q** *of conductor* 11 *is determined by an integer solution $(u, v)$ with $(u, v, 11) = 1$ of the Thue-Mahler equation*

$$u^3 - u^2v + uv^2 + v^3 = \pm 11^s,$$

*where $s$ is a nonnegative integer. Moreover, each solution of this equation in integers $u, v$ with $(u, v, 11) = 1$ gives rise to an elliptic curve $E(u, v)$ defined over* **Q**, *and $E(u, v)$ has conductor* 11 *if and only if $u \equiv 0 \bmod 2$, $u - v \equiv 1 \bmod 4$, and $u \not\equiv 3v \bmod 11$.*

4. Write

$$p(x) = x^3 + x^2 + x - 1, \tag{7}$$

and let $\epsilon$ in **R**, $\delta$ and $\bar{\delta}$ denote its zeros in **C**. In $\mathbf{K} = \mathbf{Q}(\epsilon)$ we have $11 = (1 + 2\epsilon)(2 + \epsilon^2)^2$ (recall that $p(x)$ has discriminant $-44$) and $\epsilon$ is a fundamental unit. We have

$$f(u, v) = u^3 - u^2v + uv^2 + v^3 = (u + \epsilon v)(u + \delta v)(u + \bar{\delta} v) = \pm 11^s,$$

which implies

$$u + \epsilon v = \pm \epsilon^{b_0}(1 + 2\epsilon)^{b_1}(2 + \epsilon^2)^{b_2} \tag{8}$$

with $b_1 + b_2 = s$, $b_1, b_2 \geqslant 0$ and $b_0, b_1, b_2$ in **Z**.

By the identity

$$(\delta - \bar{\delta})(u + \epsilon v) + (\bar{\delta} - \epsilon)(u + \delta v) + (\epsilon - \delta)(u + \bar{\delta} v) = 0,$$

we have

$$1 - \frac{\epsilon - \delta}{\epsilon - \bar{\delta}} \frac{(u + \bar{\delta} v)}{(u + \delta v)} = \frac{\delta - \bar{\delta}}{\epsilon - \bar{\delta}} \frac{(u + \epsilon v)}{(u + \delta v)},$$

which becomes by virtue of (8) and its conjugate equations,

$$1 - \gamma_2^{-1}\gamma_0^{h_0}\gamma_1^{h_1} = \left(\frac{\delta - \bar{\delta}}{\epsilon - \bar{\delta}}\right)\left(\frac{\epsilon}{\delta}\right)^{h_0}\left(\frac{2 + \delta^2}{2 + \epsilon^2}\right)^{h_1}, \tag{9}$$

where $\gamma_2 = (\epsilon - \bar{\delta})/(\epsilon - \delta)$, $\gamma_1 = (2 + \delta^2)/(2 + \bar{\delta}^2)$, $\gamma_0 = \bar{\delta}/\delta$ and $h_0 = b_0$, $h_1 = 2b_1 - b_2$. We shall write $H = \max(|h_0|, |h_1|)$.

Computing the complex zeros of $p(x)$ (on a Hewlett Packard HP67) yields

$$\epsilon = 0.543\ 689\ 013\ \ldots, \quad \delta = -0.771\ 844\ 506\ \ldots \pm i \cdot 1.115\ 142\ 508\ \ldots$$

and $|\delta/\epsilon| = 2.4944\ldots$, $|(2+\delta^2)/(2+\epsilon^2)| = 0.9535\ldots$, $|(\delta-\bar{\delta})/(\epsilon-\bar{\delta})| = 1.2932\ldots$. We shall (easily) see below that $h_1 \geqslant -1$; and since obviously $|1-\gamma_2^{-1}\gamma_0^{h_0}\gamma_1^{h_1}| \leqslant 2$, since the $\gamma_i$ lie on the unit circle, we deduce that we only have two cases: (I) $H = h_0 \geqslant h_1$ and (II) $H = h_1 \geqslant |h_0|$. For case (II) we shall require the 11-adic zeros of $p(x)$. Writing, formally, $\theta^2 = -11$, we find (again on the HP67)

$$\epsilon' = 5 + 7.11 + 2.11^2 + 7.11^3 + 2.11^4 + \cdots,$$

$$\delta' = 8 + 5\theta + 1.11 + 2.11\theta + 4.11^2 + \cdots$$

(the third zero being $\bar{\delta}'$ with $\theta$ replaced by $\bar{\theta} = -\theta$). Since clearly $\mathrm{ord}_{11}(1-\gamma_2^{-1}\gamma_0^{h_0}\gamma_1^{h_1}) \geqslant 0$ (we suppress the necessary dashes), whilst $\mathrm{ord}_{11}(\epsilon/\delta) = 0$, $\mathrm{ord}_{11}((2+\delta^2)/(2+\epsilon^2)) = \frac{1}{2}$, and $\mathrm{ord}_{11}((\delta-\bar{\delta})/(\epsilon-\bar{\delta})) = \frac{1}{2}$, we deduce that $h_1 \geqslant -1$.

It is a mechanical matter to determine all solutions of (9), and/or its 11-adic equivalent, with $H$ small. In fact, all solutions of $f(u, v) = \pm 1$ are already provided in [9]. The solutions with $H \leqslant 20$ are

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $h_0 = 0$ | $b_1 = b_2 = 0$ | $s = 0$ | $u = 1$ | $v = 0$ | and | $u = -1$ | $v = 0$ |
| $h_0 = 1$ | $b_1 = b_2 = 0$ | $s = 0$ | $u = 0$ | $v = 1$ | and | $u = 0$ | $v = -1$ |
| $h_0 = 4$ | $b_1 = b_2 = 0$ | $s = 0$ | $u = -1$ | $v = 2$ | and | $u = 1$ | $v = -2$ |
| $h_0 = 17$ | $b_1 = b_2 = 0$ | $s = 0$ | $u = 56$ | $v = -103$ | and | $u = -56$ | $v = 103$ |
| $h_0 = 0$ | $b_1 = 1, b_2 = 0$ | $s = 1$ | $u = 1$ | $v = 2$ | and | $u = -1$ | $v = -2$ |
| $h_0 = 3$ | $b_1 = 0, b_2 = 1$ | $s = 1$ | $u = 2$ | $v = -3$ | and | $u = -2$ | $v = 3$ |
| $h_0 = 1$ | $b_1 = 2, b_2 = 0$ | $s = 2$ | $u = 4$ | $v = -3$ | and | $u = -4$ | $v = 3$. |

Of these 14 solutions all but 4 give rise to elliptic curves with bad reduction at 2, and $u = 2, v = -3$ gives rise to a curve with additive reduction at 11. Hence, we obtain 3 curves of conductor 11. We list the curves obtained according to the formulas of Section 3, the transformation required to bring them to a minimal form, and the corresponding minimal models.

(A) $u = 0 \quad v = -1 \quad y^2 = x^3 + 2x^2 - 4x + 8 \quad x = 4x' - 2, \quad y = 4(2y' - 1)$

$y^2 - y = x^3 - x^2$

(C) $u = -56 \quad v = 103 \quad y^2 = x^3 - 94x^2 - 122180x - 13146104$

$x = 4x' + 30, \quad y = 4(2y' - 1) \quad y^2 - y = x^3 - x^2 - 7820x - 263580$

(B) $u = -4 \quad v = 3 \quad y^2 = x^3 + 2x^2 - 164x - 1592$

$x = 4x' - 2, \quad y = 4(2y' - 1) \quad y^2 - y = x^3 - x^2 - 10x - 20$

Thus, we have found the three known rational elliptic curves of conductor 11. To prove the theorem of Section 1 it now suffices to show that the equation (9), and/or its 11-adic analogue, has no solution with $H > 20$.

5. Firstly, we remark that the quantities $\gamma_0$, $\gamma_1$ and $\gamma_2$ are not multiplicatively independent. Indeed

$$(\delta - \bar{\delta})^2 = -(1-\epsilon)^2\epsilon^{-4}(1+2\epsilon), \quad (1-\epsilon)^3 = 2\epsilon(2\epsilon - 1) = 2\epsilon^5,$$

so

$$\gamma_2^6 = \left(\frac{\epsilon - \bar{\delta}}{\epsilon - \delta}\right)^6 = \left(\frac{1-\delta}{1-\bar{\delta}}\right)^6 \left(\frac{\delta}{\bar{\delta}}\right)^{-12} \left(\frac{1+2\delta}{1+2\bar{\delta}}\right)^3 = \left(\frac{\delta}{\bar{\delta}}\right)^{-2} \left(\frac{2+\delta^2}{2+\bar{\delta}^2}\right)^{-6} = \gamma_0^2\gamma_1^{-6}.$$

(It was a salutary lesson for the authors that we failed to notice this relation until it became apparent in our attempts to simultaneously approximate quotients of 11-adic logarithms.)

*Case* (I). $H = h_0 \geqslant h_1$ and $H > 20$. We have by (9)

$$|1 - \gamma_0^{h_0}\gamma_1^{h_1}\gamma_2^{-1}| < (0.216 \times 2\pi)e^{-\Delta H}, \quad \text{with } \Delta > 0.9140\ldots. \tag{10}$$

Writing $\gamma_j = \exp(2\pi i\phi_j)$, $j = 0, 1, 2$, we obtain (since, say, $|\operatorname{Log}\alpha| < 2|1-\alpha|$ if $|1-\alpha| < \frac{1}{2}$)

$$\|h_0\phi_0 + h_1\phi_1 - \phi_2\| < e^{-\Delta H}, \tag{11}$$

where $\|\ \|$ denotes the distance to the nearest integer. Noting the cited relation, we similarly have

$$\|(6h_0 - 2)\phi_0 + (6h_1 + 6)\phi_1\| < 6e^{-\Delta H}. \tag{12}$$

*Case* (II). $H = h_1 \geqslant |h_0|$ and $H \geqslant 0$. We have by the 11-adic analogue of (9) and our earlier remarks

$$\operatorname{ord}_{11}(1 - \gamma_0^{h_0}\gamma_1^{h_1}\gamma_2^{-1}) = \tfrac{1}{2}(H+1). \tag{13}$$

Each of the $\gamma_i$ is of the shape $\gamma = (1 + c\theta)/(1 - c\theta)$ with $c$ an 11-adic integer. Hence, the 11-adic logarithms exist, indeed explicitly

$$\log\gamma = \log(1 + c\theta)/(1 - c\theta) = 2\theta\left(c - \frac{11c^3}{3} + \frac{11^2c^5}{5} - \frac{11^3c^7}{7} + \cdots\right). \tag{14}$$

We write $\chi = \log\gamma_0/\log\gamma_1$. In view of the relation we have (recalling that $\operatorname{ord}_p(1-x) = \operatorname{ord}_p \log x$ if $\operatorname{ord}_p(1-x) > 1/(p-1)$)

$$\operatorname{ord}_{11}((3h_0 - 1)\chi - (3h_1 + 3)) = \tfrac{1}{2}H. \tag{15}$$

6. Baker's inequalities for linear forms in the logarithms of algebraic numbers (see, for example, the first two chapters of [3]) yield the conclusion that (10) and, respectively, (13) have no solutions if $H$ is larger than some effectively computable constant. Explicitly, we employ the recent sharp inequalities of Loxton, Mignotte, van der Poorten and Waldschmidt [15]. These inequalities do not involve any principles additional to those described in [3]; rather they are the result of simultaneously introducing many known refinements to the known proof techniques. We state here only a weak partial result sufficient unto our present purpose:

Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers with $\mathbf{K} = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$, $[\mathbf{K}: \mathbf{Q}] = D$ and $[\mathbf{K}(\alpha_1^{1/2}, \ldots, \alpha_n^{1/2}): \mathbf{K}] = 2^n$. For an algebraic number $\alpha$ with defining polynomial $a_0X^d + \cdots + a_d$ write $\|\alpha\|^d = a_0\Pi \max(1, |\sigma\alpha|)$, where the product is over the $d$ automorphisms $\sigma$ of $\mathbf{Q}(\alpha)$ over $\mathbf{Q}$, and put $V_r = \max(|\log \alpha_r|, \mathrm{Log}\|\alpha_r\|)$, $1 \leqslant r \leqslant n$. Let $b_1, \ldots, b_n$ be rational integers not all zero with $B = \max|b_r|$. Finally, let $E = eD \min(V_r/|\log \alpha_r|)$. Write

$$\Lambda = 1 - \alpha_1^{b_1} \cdots \alpha_n^{b_n} \quad \text{or} \quad \Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$$

depending on which expression is more convenient in the application under investigation. The results with which we are concerned are of the following shape:

If $\Lambda \neq 0$ and $|\Lambda| < e^{-\delta B}$, some $\delta > 0$, then $B$ is bounded by a computable positive constant depending only on $\delta, n, D, V_1, \ldots, V_n$ (and $E$). Moreover, if $\rho$ is a prime ideal of $\mathbf{K}$ and $\rho|(\alpha_r - 1)$, $1 \leqslant r \leqslant n$, then similarly $\mathrm{ord}_\rho \Lambda > \delta B$ implies such a bound for $B$.

In each metric the bound obtainable is as follows: write $C = 2^n D b c^n d \Omega \delta^{-1}$ where $b$. $c$, $d$ are described below and $\Omega = V_1 V_2 \cdots V_n$. Then it is shown that $B < C(\mathrm{Log}\, EC)(\mathrm{Log}\, C)$. Let $b', c', d'$ be positive numbers which we may suppose to be no greater than 5, and put $x = 4(n+1)^2 D(\mathrm{Log}\, E)^{-1}$. Then we may take $b = b'x$, $c = c'x$ and $d = (n!)^{-1}d'$. To prevent overrough use of these remarks we add that some qualifications must be made if $E$ is very large, but $x \geqslant 1$ is always safe. Of course, a different definition to that given for $E$ applies in the $p$-adic case; the reader should simply replace $\mathrm{Log}\, E$ by 1 in the bounds given above. In the $p$-adic case one can actually obtain $B \log p$ is less than the cited bound (where $\rho$ divided the rational prime $p$). We emphasize again that the quoted results are weaker than those obtained in [15].

Applied to (10), noting the relation, the complex case certainly yields $H < 10^{15}$, and applied to (13), again noting the relation, the 11-adic case yields $H < 11^{15}$. We should remark that these bounds are not as sharp as possible and are quoted as convenient numbers only; the remainder of our proof is not sensitive to the precise size of the bounds. It now remains for us to close the gap between 20 and these respective upper bounds.

7. Our technique borrows from a suggestion of Ellison [10] which generalizes an idea of Baker and Davenport [2].

*Case* (I). We simultaneously rationally approximate $\phi_0, \phi_1$ obtaining

$$|\phi_i - p_i/q| < q^{-2/3}, \quad \text{with integers } p_0, p_1, q. \tag{16}$$

Write $r_i = q\phi_i - p_i$, $i = 0, 1$. Then

$$\|(h_0r_0 + h_1r_1) - q\phi_2 + (h_0p_0 + h_1p_1)\| < qe^{-\delta H}. \tag{17}$$

We notice that the relation implies $\|6q\phi_2\| < 8Hq^{-1/2}$ for $q$ satisfying (16). Hence, if $q$ is sufficiently large relative to the upper bound for $H$, then $\|q\phi_2\|$ is always (very nearly) an integer multiple of 1/6. (We noticed this phenomenon before we had found

the relation, but dismissed it as coincidence!) But with $q$ appropriately large and $\|q\phi_2\|$ not (very nearly) zero, the inequality (17) is impossible if $qe^{-\delta H}$ is noticeably less than 1/6. This yields a new, very much smaller, upper bound for $H$.

We computed

$$\phi_0 = 0.307\ 283\ 347\ 825\ 135\ 494\ 792\ 282\ 360\ 112\ 311\ 481\ 486\ 504\ 705$$
$$511\ 418\ 102\ 745\ 796\ 778\ \ldots,$$
$$\phi_1 = -0.288\ 055\ 833\ 808\ 469\ 053\ 321\ 695\ 954\ 512\ 194\ 607\ 473\ 252\ 968$$
$$601\ 753\ 438\ 867\ 670\ 338\ \ldots,$$
$$\phi_2 = 0.223\ 816\ 949\ 750\ 180\ 884\ 919\ 123\ 407\ 882\ 965\ 101\ 302\ 087\ 870$$
$$438\ 892\ 806\ 449\ 602\ 598\ \ldots,$$

and found an appropriate denominator $q$ satisfying (16)

$$q = 975\ 370\ 958\ 532\ 758\ 933\ 226\ 181\ 218\ 264\ 710\ 345\ 131$$
$$= 0.975\ 370 \times \cdots \times 10^{39}.$$

We checked $q\phi_2$ and found $\|q\phi_2\| = 0.500\ 000\ \ldots$ (with error $< 10^{-19}$). The relevant errors $r_0, r_1$ were of the following order:

$$r_0 = 1.3 \times \cdots \times 10^{-20}, \quad r_1 = 0.84 \times \cdots \times 10^{-20}.$$

Given that $H < 10^{15}$, (17) implies that $qe^{-\delta H} > 0.499\ \ldots$ which yields $H < 100$. This constitutes a striking improvement in the upper bound for $H$. The next appropriate denominator $q$ satisfying (16) we chose to be

$$q = 4\ 578\ 595;$$
$$\|q\varphi_2\| = 0.167\ \ldots, \quad r_0 = 0.646 \times \cdots \times 10^{-4}, \quad r_1 = 3.96 \times \cdots \times 10^{-4}.$$

Then (17) implies, given that $H < 100$, that $qe^{-\delta H} > 0.12\ \ldots$, which yields $H < 20$. Hence, we have closed the gap in Case (I).

*Case* (II). We rationally approximate $\chi$ so as to obtain two approximants

$$\text{ord}_{11}(q_i\chi - p_i) \geqslant s, \quad i = 1, 2 \text{ with integers } p_i, q_i \text{ such that} \tag{18}$$
$$p_1q_2 - p_2q_1 \neq 0, \tag{19}$$

and $11^s$ large relative to $|p_i|, q_i$, $i = 1, 2$. We write $r = q\chi - p$. Then

$$\text{ord}_{11}(r(3h_0 - 1) + (3h_0 - 1)p - (3h_1 + 3)q) = \tfrac{1}{2}H. \tag{20}$$

Hence, if $H \geqslant 2s$, then

$$\text{ord}_{11}((3h_0 - 1)p - (3h_1 + 3)q) \geqslant s. \tag{21}$$

But if $(3H - 1)|p| + (3H + 3)q < 11^s$, then (21) implies

$$(3h_0 - 1)p - (3h_1 + 3)q = 0.$$

This equation is impossible for both the approximants satisfying (19), so we obtain $H < 2s$. This yields a very much smaller upper bound for $H$.

We computed

$$\chi = 2 + 6.11 + 4.11^2 + 5.11^3 + \cdots$$

$$= 264\ 592\ 979\ 998\ 093\ 174\ 365\ 567\ 059\ 092\ 223\ 070\ 028\ 910\ 476\ \text{A40}$$

$$618\ 661\ 481\ \text{A48} \ldots$$

and found, with $s = 40$,

$$q_1 = 133\ 337\ 970\ 558\ 677\ 219\ 027 = 1.333\ 379 \times \cdots \times 10^{20},$$

$$p_1 = 722\ 999\ 016\ 021\ 217\ 320\ 198 = 7.229\ 990 \times \cdots \times 10^{20},$$

$$q_2 = 506\ 135\ 618\ 806\ 951\ 323\ 269 = 5.061\ 356 \times \cdots \times 10^{20},$$

$$p_2 = -649\ 904\ 906\ 666\ 545\ 995\ 857 = -6.499\ 049 \times \cdots \times 10^{20}.$$

By the underlying theory (19) is automatic (with $p_1q_2 - p_2q_1 = 11^{40}$), which yields $H < 80$ (even $H < 72$). Next, with $s = 6$, we found

$$q_1 = 73, \qquad p_1 = -965,$$

$$q_2 = 1802, \qquad p_2 = 447,$$

and $p_1q_2 - p_2q_1 = -11^6$. These approximants yield $H < 12$ which closes the gap in Case (II).

8. All computer calculations were performed within the UNIX operating system (Bell Laboratories) on the Australian Graduate School of Management PDP 11/70 computer. The simultaneous approximation algorithm was performed using the DC and BC systems within UNIX. DC is an arbitrary-precision integer package; BC is a simple language with which to program DC.

We employed an efficient simultaneous approximation algorithm due to Szekeres [32]. The principle of the Szekeres algorithm is sequential 'Farey bisection' of simplexes. It is not known whether the algorithm necessarily succeeds (though see Cusick [8]), but in practice it appears to provide plenty of good simultaneous approximations at reasonable speed. It is a fortuitous feature of Ellison's recipes [10] which we employ, that we require no guarantee that we are obtaining all best approximations; good approximations suffice. We required 562 steps of the algorithm to obtain the large denominator in Case (I); the smaller denominator appears at step 146. The solution $h_0 = 17$ was 'noticed' by the algorithm which produced a particularly good approximation at step 69 (with $q = 106\ 462$, but $\|q\phi_2\|$ very nearly zero). All calculations were performed to accuracy of 98 decimal places.

To perform the 11-adic calculations of Case (II) we initially used the 11-ary (base 11) facility of DC. Later we wrote a package of FORTRAN subroutines for arbitrary primes $p$ to perform $p$-adic addition, subtraction, multiplication, division, logarithm and exponential (the last to check the accuracy of the logarithm routine).

To obtain the 11-adic approximants we use an idea of Mahler [17, p. 63]. Explicitly, we truncate the 11-adic expansion of $\chi$ at term $s$ ($s = 40$) obtaining a rational integer $\chi^1 < 11^s$. (If $\chi = a_0 + a_1 11 + a_2 11^2 + \cdots$ then $\chi^1 = a_{s-1} 11^{s-1} + a_{s-2} 11^{s-2} + \cdots + a_1 11 + a_0$.) We then approximated the rational number $\chi^1/11^s$ by the continued fraction algorithm. If $r/q$ is a convergent, then

$$|\chi^1/11^s - r/q| < 1/q^2 \quad \text{and} \quad \chi^1/11^s - r/q = p/11^s q,$$

so

$$\operatorname{ord}_{11}(q\chi - p) \geqslant \operatorname{ord}_{11}(q\chi^1 - p) = \operatorname{ord}_{11}(11^s r) \geqslant s,$$

and $pq < 11^s$. Choosing $q_1, q_2$ as consecutive denominators implies $|p_1 q_2 - p_2 q_1| = 11^s$ as asserted.

Thus, we approximated the rational number

$$\chi^1/11^s = 0.885\ 804\ 116\ 510\ 898\ 324\ 820\ 924\ 074\ 001\ 525\ 676\ 118\ 468\ 587\ \ldots$$

and selected appropriate pairs of consecutive convergents. For discussion of rational approximation in the $p$-adic case we refer the reader to Mahler [16], [17], Schneider [26], and Bundschuh [6].

Department of Mathematics
Panjab University
Chandigarh, India

Département de Mathématique
Université de Paris-Sud, Centre d'Orsay
91405 Orsay Cedex, France

School of Mathematics
The University of New South Wales
P. O. Box 1
Kensington, N.S.W. 2033, Australia

School of Mathematics and Physics
Macquarie University
North Ryde, N. S. W. 2113, Australia

1. I. O. ANGELL, "A table of complex cubic fields," *Bull. London Math. Soc.*, v. 5, 1973, pp. 37–38; "A table of totally real cubic fields," *Math. Comp.*, v. 30, 1976, pp. 184–187.

2. A. BAKER & H. DAVENPORT, "The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$," *Quart. J. Math. Oxford Ser.* (2), v. 20, 1969, pp. 129–137.

3. A. BAKER & D. W. MASSER (Eds.), *Transcendence Theory: Advances and Applications*, Academic Press, New York, 1977.

4. B. J. BIRCH & W. KUYK (Eds.), *Modular Functions of One Variable*. IV, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975.

5. REINHARD BÖLLING, "Elliptische Kurven mit Primzahl führer," *Math. Nachr.*, v. 80, 1977, pp. 253–278.

6. P. BUNDSCHUH, "Fractions continues et indépendance algébrique en $p$-adique. Journées arithmétiques de Caen," *Astérisque*, 41–42, 1977, pp. 179–181.

7. J. COATES, "An effective $p$-adic analogue of a theorem of Thue. I; II: The greatest prime factor of a binary form; III: The diophantine equation $y^2 = x^3 + k$," *Acta Arith.*, v. 15, 1969, pp. 279–305; v. 16, 1970, pp. 399–412, 425–435.

8. T. W. CUSICK, "The Szekeres multidimensional continued fraction," *Math. Comp.*, v. 31, 1977, pp. 280–317.

9. B. N. DELONE & D. K. FADDEEV, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R. I., 1964.

10. W. J. ELLISON, *Recipes for Solving Diophantine Problems by Baker's Method*, Publications mathématiques, Bordeaux, Ann. 1, Fasc. 1, 1972.

11. R. FRICKE, *Die elliptischen Funktionen und ihre Anwendungen.* II, Teubner, Leipzig, 1922.

12. STEPHEN GELBART, "Elliptic curves and automorphic representations," *Adv. in Math.*, v. 21, 1976, pp. 235–292.

13. GÉRARD LIGOZAT, "Courbes modulaires de genre 1," *Bull. Soc. Math. France*, Mémoire 43, 1975.

14. GÉRARD LIGOZAT, *Courbes Modulaires de Niveau* 11. *Modular Functions of One Variable.* V, Lecture Notes in Math., vol. 601, Springer-Verlag, Berlin and New York, 1977.

15. J. LOXTON, M. MIGNOTTE, A. J. VAN DER POORTEN & M. WALDSCHMIDT, "Linear forms in logarithms with rational coefficients." (In preparation.)

16. KURT MAHLER, "On a geometrical representation of $p$-adic numbers," *Ann. of Math.* (2), v. 41, 1940, pp. 8–56.

17. KURT MAHLER, *Lectures on Diophantine Approximations.* Part I: *p-Adic Numbers and Roth's Theorem*, Univ. of Notre Dame, 1961.

18. B. MAZUR & P. SWINNERTON-DYER, "Arithmetic of Weil curves," *Invent. Math.*, v. 25, 1974, pp. 1–61.

19. OLAF NEUMANN, "Zur Reduktion der elliptischen Kurven," *Math. Nachr.*, v. 46, 1970, pp. 285–310.

20. OLAF NEUMANN, "Die elliptischen Kurven mit den Führern $3.2^m$ und $9.2^m$," *Math. Nachr.*, v. 48, 1970, pp. 387–389.

21. OLAF NEUMANN, "Elliptische Kurven mit vorgeschriebenen Reduktionsverhalten. I," *Math. Nachr.*, v. 49, 1971, pp. 107–123.

22. OLAF NEUMANN, "Elliptische Kurven mit vorgeschriebenen Reduktionsverhalten. II," *Math. Nachr.*, v. 56, 1973, pp. 269–280.

23. A. P. OGG, "Abelian curves of 2-power conductor," *Proc. Cambridge Philos. Soc.*, v. 62, 1966, pp. 143–148.

24. A. P. OGG, "Elliptic curves and wild ramification," *Amer. J. Math.*, v. 89, 1967, pp. 1–21.

25. A. P. OGG, "Abelian curves of small conductor," *J. Reine Angew. Math.*, v. 226, 1967, pp. 204–215.

26. TH. SCHNEIDER, *Über p-adische Kettenbrüche*, Symposia Mathematica IV, Istituto Nazionale di Alta Mathematica, 1970, pp. 181–189.

27. J.-P. SERRE, *Abelian l-Adic Representations and Elliptic Curves*, Benjamin, New York, 1968.

28. J.-P. SERRE, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques," *Invent. Math.*, v. 15, 1972, pp. 259–331.

29. BENNETT SETZER, "Elliptic curves of prime conductor," *J. London Math. Soc.* (2), v. 10, 1975, pp. 367–378.

30. T. N. SHOREY, A. J. VAN DER POORTEN, R. TIJDEMAN & A. SCHINZEL, "Applications of the Gel'fond-Baker method to diophantine equations" in *Transcendence Theory: Advances and Applications*, Chapter 3, pp. 59–77 (Baker & Masser, Eds.), Academic Press, New York, 1977.

31. H. P. F. SWINNERTON-DYER & B. J. BIRCH, "Elliptic curves and modular functions," in *Modular Functions of One Variable.* IV, Chapter 2, pp. 2–32 (Birch & Kuyk, Eds.), Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975.

32. G. SZEKERES, "Multidimensional continued fractions," *Ann. Univ. Sci. Budapest, Eötvös Sect. Math.*, v. 13, 1970, pp. 113–140.

33. JOHN T. TATE, "The arithmetic of elliptic curves," *Invent. Math.*, v. 23, 1974, pp. 179–206.

34. J. TATE, "Algorithm for determining the type of a singular fibre in an elliptic pencil," in *Modular Functions of One Variable.* IV, Chapter 3, pp. 33–52 (Birch & Kuyk, Eds.), Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975.

35. JACQUES VÉLU, "Courbes elliptiques sur $Q$ ayant bonne réduction en dehors de $\{11\}$," *C. R. Acad. Sci. Paris Sér. A-B*, v. 273, 1971, pp. A73–A75.

36. A. WEIL, "Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen," *Math. Ann.*, v. 168, 1967, pp. 149–156.