THE EQUATIONS $3x^2-2 = y^2$ AND $8x^2-7 = z^2$

By A. BAKER *and* H. DAVENPORT

[Received 6 November 1968]

1. THE four numbers 1, 3, 8, 120 have the property that the product of any two, increased by 1, is a perfect square. Professor J. H. van Lint, in a lecture at Oberwolfach in March 1968, discussed the problem whether there is any other positive integer that can replace 120. Since then Professor van Lint has been good enough to send us a copy of a report† in which he gives references to the history of the problem, and also gives a proof that there is no such integer up to $10^{1700000}$.

An integer N which can replace 120 while preserving the property must have the form $N = x^2-1$, and the conditions are equivalent to the two equations

$$3x^2-2 = y^2, \qquad 8x^2-7 = z^2. \tag{1}$$

Thus the question is whether these simultaneous equations have any solution in positive integers, other than the solutions with $x = 1$ (corresponding to $N = 0$) and $x = 11$ (corresponding to $N = 120$). The object of the present note is to prove that there is no other solution.

It is well known that two equations of the form (1) can have only finitely many solutions in integers. One way of proving this is to apply a theorem of Siegel‡ to the equation

$$(3x^2-2)(8x^2-7) = t^2.$$

Another way is to express the solutions of the separate equations in (1) by powers of quadratic irrationals, as was done by Professor van Lint, and as we shall do in § 2. This leads to an inequality satisfied by a linear combination of the logarithms of three particular algebraic numbers, and to this we can apply a theorem of Gelfond.§ Both Siegel's theorem and Gelfond's theorem depend ultimately on Thue's theorem and its refinements, and are therefore not effective. That is, they offer no possibility of determining a number X such that there is no solution with $x > X$.

† J. H. van Lint, 'On a set of Diophantine equations', Report 68–WSK–03 of the Technological University Eindhoven, September 1968.

‡ C. L. Siegel (under the pseudonym 'X'), 'The integer solutions of the equation $y^2 = ax^n+bx^{n-1}+...+k$', *J. London Math. Soc.* 1 (1926) 66–8, or *Gesammelte Abhandlungen* I, 207–8.

§ A. O. Gelfond, *Transcendental and algebraic numbers* (Dover, New York 1960), p. 34, Theorem IV.

Quart. J. Math. Oxford (2), 20 (1969), 129–37.

3695.2.20 K

Some recent work of one of us (A. B.) results in an effective form of Gelfond's theorem, and this makes it possible to compute a number X with the property just stated. The latest paper† establishes a theorem which is completely explicit and is well adapted to the solution of particular problems, such as the present one. It is as follows:

THEOREM. *Suppose that $k \geqslant 2$, and that $\alpha_1,\ldots, \alpha_k$ are non-zero algebraic numbers, whose degrees do not exceed d and whose heights do not exceed A, where $d \geqslant 4$ and $A \geqslant 4$. If the rational integers $b_1,\ldots, b_k$ satisfy*

$$0 < |b_1 \log \alpha_1 + \ldots + b_k \log \alpha_k| < e^{-\delta H}, \tag{2}$$

where $0 < \delta \leqslant 1$ *and*

$$H = \max(|b_1|,\ldots, |b_k|), \tag{3}$$

then

$$H < (4^{k^2}\delta^{-1}d^{2k} \log A)^{(2k+1)^2}. \tag{4}$$

In this theorem the logarithms are supposed to have their principal values, but this is of no importance to us here, since we shall be concerned exclusively with positive algebraic numbers.

We apply the theorem to the present problem in § 2, and deduce that the positive integer m, in terms of which x is expressed by (6) below, satisfies

$$m < 10^{487}. \tag{5}$$

There remains the problem of covering this range without a prohibitive amount of computation, and this is the main theme of the present note. We treat the problem in § 3 by means of a simple lemma on Diophantine approximation.

The lemma leaves us with one serious computational problem, and for this we were fortunate in having the co-operation of the Atlas Computer Laboratory of the Science Research Council at Chilton, Berkshire. Mr. S. T. E. Muir, of that Laboratory, used a package originally developed by Mr. W. F. Lunnon, of Manchester University, to carry out multi-length arithmetic to an arbitrary precision. The numerical data found by the Laboratory are given in an appendix. The inequalities needed for the lemma are satisfied with an ample margin. But for the sake of interest, and for possible use in other problems, we explain briefly in § 5 the procedure which could have been followed if they had not been satisfied.

2. The general solution of each separate equation in (1) can be found by arguments that have been known since the eighteenth century.

† A. Baker, 'Linear forms in the logarithms of algebraic numbers', *Mathematika*, 15 (1968) 204–16. This contains references to earlier papers.

The first equation can be written as

$$(y+x\surd 3)(y-x\surd 3) = -2.$$

If we put $$y+x\surd 3 = (y_0+x_0\surd 3)(2+\surd 3)^m,$$

where $m \geqslant 0$, it is easily verified (by combining this equation with its conjugate) that x_0 is always positive but that y_0 is negative if m is large. Hence we can choose m so that $y_0 > 0$ but that if y_1 is defined by

$$y_0+x_0\surd 3 = (y_1+x_1\surd 3)(2+\surd 3)$$

then $y_1 < 0$. Since $y_1 = 2y_0-3x_0$, we have $y_0 < \frac{3}{2}x_0$. Hence

$$3x_0^2-2 = y_0^2 < \tfrac{9}{4}x_0^2,$$

whence $x_0 = 1$ and so $y_0 = 1$. Thus the general solution is given by

$$y+x\surd 3 = (1+\surd 3)(2+\surd 3)^m,$$

and accordingly

$$(2\surd 3)x = (1+\surd 3)(2+\surd 3)^m-(1-\surd 3)(2-\surd 3)^m, \qquad (6)$$

where $m = 0, 1, 2,\ldots$. The value $x = 1$ corresponds to $m = 0$, and the value $x = 11$ to $m = 2$.

The second equation can be written as

$$(z+x\surd 8)(z-x\surd 8) = -7.$$

Reasoning as before, with

$$z+x\surd 8 = (z_0+x_0\surd 8)(3+\surd 8)^n,$$

we find that $z_0 < \frac{8}{3}x_0$, whence

$$8x_0^2-7 = z_0^2 < \tfrac{64}{9}x_0^2,$$

so that $x_0 = 1$ or 2. If $x_0 = 1$ then $z_0 = 1$, and if $x_0 = 2$ then $z_0 = 5$. There are two classes of solutions, one given by

$$z+x\surd 8 = (1+\surd 8)(3+\surd 8)^n$$

and the other by

$$z+x\surd 8 = (5+2\surd 8)(3+\surd 8)^n.$$

The last formula can be simplified by noting that

$$5+2\surd 8 = (3+\surd 8)(-1+\surd 8).$$

The solutions of the second equation in (1) are therefore given by the alternative formulae

$$(2\surd 8)x = (1+\surd 8)(3+\surd 8)^n-(1-\surd 8)(3-\surd 8)^n, \qquad (7\,\mathrm{a})$$

where $n = 0, 1, 2,\ldots$, and

$$(2\surd 8)x = (-1+\surd 8)(3+\surd 8)^n-(-1-\surd 8)(3-\surd 8)^n, \qquad (7\,\mathrm{b})$$

where $n = 1, 2, \ldots$. The value $x = 1$ corresponds to $n = 0$ in (7a), and the value $x = 11$ to $n = 2$ in (7b).

We seek the common values of (6) and either (7a) or (7b). Consider first (6) and (7a). Here

$$2x = \frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^m + \frac{\sqrt{3}-1}{\sqrt{3}}(2+\sqrt{3})^{-m}$$

$$= \frac{1+\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^n + \frac{\sqrt{8}-1}{\sqrt{8}}(3+\sqrt{8})^{-n}.$$

If we put

$$P = \frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^m, \qquad Q = \frac{\sqrt{8}+1}{\sqrt{8}}(3+\sqrt{8})^n, \tag{8}$$

the last relation gives

$$P + \tfrac{2}{3}P^{-1} = Q + \tfrac{7}{8}Q^{-1}.$$

Since $\qquad P-Q > \tfrac{2}{3}Q^{-1} - \tfrac{2}{3}P^{-1} = \tfrac{2}{3}(P-Q)P^{-1}Q^{-1},$

and plainly $P > 1$, $Q > 1$, we must have $Q < P$. As we may suppose that $m \geqslant 3$, we have

$$P \geqslant \frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^3 > 80.$$

Also $Q > P - \frac{7}{8}Q^{-1} > P - \frac{7}{8}$. Hence

$$P - Q = \tfrac{7}{8}Q^{-1} - \tfrac{2}{3}P^{-1} < \tfrac{7}{8}(P-\tfrac{7}{8})^{-1} - \tfrac{2}{3}P^{-1} < \tfrac{1}{4}P^{-1}.$$

It follows that

$$0 < \log\frac{P}{Q} = -\log\left(1 - \frac{P-Q}{P}\right) < \tfrac{1}{4}P^{-2} + (\tfrac{1}{4}P^{-2})^2 < 0{\cdot}26P^{-2}.$$

Substituting from (8), we obtain

$$0 < m\log(2+\sqrt{3}) - n\log(3+\sqrt{8}) + \log\frac{(1+\sqrt{3})\sqrt{8}}{(1+\sqrt{8})\sqrt{3}}$$

$$< 0{\cdot}26P^{-2} < \frac{0{\cdot}11}{(2+\sqrt{3})^{2m}}. \tag{9}$$

We apply the theorem quoted in § 1 with $k = 3$ and

$$\alpha_1 = 2+\sqrt{3}, \qquad \alpha_2 = 3+\sqrt{8}, \qquad \alpha_3 = \frac{(1+\sqrt{3})\sqrt{8}}{(1+\sqrt{8})\sqrt{3}}.$$

We can take $\delta = 1$ (since $(2+\sqrt{3})^2 > e$) and $H = m$ since plainly $n < m$. The equations satisfied by α_1, α_2, α_3 are

$$\alpha_1^2 - 4\alpha_1 + 1 = 0, \qquad \alpha_2^2 - 6\alpha_2 + 1 = 0,$$

$$441\alpha_3^4 - 2016\alpha_3^3 + 2880\alpha_3^2 - 1536\alpha_3 + 256 = 0.$$

Hence the maximum height of α_1, α_2, α_3 is $A = 2880$. We also have $d = 4$. The theorem shows that

$$m < (4^9 \times 4^6 \times \log 2880)^{49} < (4^{15} \times 8)^{49} = 2^{1617} < 10^{487}.$$

If, in the foregoing argument, (7 a) is replaced by (7 b), the only difference is that α_3 is replaced by

$$\alpha_3' = \frac{(1+\sqrt{3})\sqrt{8}}{(\sqrt{8}-1)\sqrt{3}}.$$

Since this number satisfies the same equation as α_3 the conclusion remains valid in the second of the alternative cases.

We have now proved (5), and it remains to consider the range

$$2 < m < 10^{487}. \tag{10}$$

3. The inequality (9) implies, on division by $\log(3+\sqrt{8})$, that

$$|m\theta - n + \beta| < 0{\cdot}07C^{-m}, \tag{11}$$

where

$$\theta = \frac{\log(2+\sqrt{3})}{\log(3+\sqrt{8})}, \tag{12}$$

$$C = (2+\sqrt{3})^2 = 13{\cdot}928..., \tag{13}$$

$$\beta = \left(\log\frac{(1+\sqrt{3})\sqrt{8}}{(1+\sqrt{8})\sqrt{3}}\right)\Big/\log(3+\sqrt{8}). \tag{14 a}$$

In the alternative case, when (7 a) is replaced by (7 b), we have to replace β by

$$\beta' = \left(\log\frac{(1+\sqrt{3})\sqrt{8}}{(\sqrt{8}-1)\sqrt{3}}\right)\Big/\log(3+\sqrt{8}). \tag{14 b}$$

We prove a simple lemma, which is suggested by arguments that are well known in connection with non-homogeneous Diophantine approximation.

LEMMA. *Suppose that $K > 6$. For any positive integer M, let p and q be integers satisfying*

$$1 \leqslant q \leqslant KM, \qquad |\theta q - p| < 2(KM)^{-1}. \tag{15}$$

Then, if†

$$\|q\beta\| \geqslant 3K^{-1}, \tag{16}$$

there is no solution of (11) *in the range*

$$\frac{\log K^2M}{\log C} < m < M.$$

Remarks. (i) The result is independent of the particular values of

† $\|z\|$ denotes the distance of a real number z from the nearest integer.

θ, β, C; all that is supposed is that θ, β are real and $C > 1$. (ii) The factor 2 has been inserted in the second of the inequalities (15) to allow some margin in the application. The existence of p, q to satisfy (15), without the factor 2, follows from Dirichlet's theorem on Diophantine approximation, or alternatively by taking q to be the largest denominator of a convergent to the continued fraction for θ which does not exceed KM.

Proof. Write $q\theta = p+\phi$, where $|\phi| < 2(KM)^{-1}$. After multiplication by q, the inequality (11) implies that

$$|m(p+\phi)-nq+q\beta| < qC^{-m}. \tag{18}$$

Assuming that m satisfies (17), we have

$$m|\phi| < 2M(KM)^{-1} = 2K^{-1},$$

and

$$qC^{-m} \leqslant KMC^{-m} < K^{-1}.$$

Hence (18) implies that $\|q\beta\| < 3K^{-1}$, which contradicts (16). This proves the lemma.

To apply the lemma in our particular case, we take

$$M = 10^{487}, \qquad K = 10^{33}. \tag{19}$$

Let θ_0 be the value of θ correct to 1040 decimal places, so that

$$|\theta-\theta_0| < 10^{-1040}.$$

Let p/q be the last convergent to the continued fraction for θ_0 which satisfies $q \leqslant 10^{520}$. Then

$$|q\theta_0-p| < 10^{-520}.$$

We therefore have

$$|q\theta-p| \leqslant q|\theta-\theta_0|+|q\theta_0-p| < 10^{-520}+10^{-520}.$$

Hence the inequalities (15) are satisfied.

It follows from the lemma that provided

$$\|q\beta\| \geqslant 3\times 10^{-33} \quad \text{and} \quad \|q\beta'\| \geqslant 3\times 10^{-33} \tag{20}$$

there is no solution of (11), in either of its alternative forms, in the range

$$\frac{\log 10^{553}}{\log C} < m < 10^{487}.$$

The number on the left is less than 500.

The values of θ and q computed by the Atlas Computer Laboratory are given in the Appendix, and also the values of β, β' to 600 decimals for the verification of (20). In fact,

$$\|q\beta\| = 0{\cdot}422..., \qquad \|q\beta'\| = 0{\cdot}474...,$$

and consequently (20) holds with a big margin.

There remains now only the range

$$2 < m < 500, \tag{21}$$

and this will be treated in the next section.†

4. We treat the case (21) directly. From the first few decimals of θ_0 we find that the continued fraction for θ begins:

$$\theta = \frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{1+}\,\frac{1}{20+}\,\frac{1}{1+}\,\frac{1}{5+}\,\frac{1}{3+}\cdots.$$

The corresponding convergents are

$$\frac{1}{1},\ \frac{2}{3},\ \frac{3}{4},\ \frac{62}{83},\ \frac{65}{87},\ \frac{387}{518},\ \frac{1226}{1641}.$$

We easily find that

$$1641\theta - 1226 = -0{\cdot}000072\ldots.$$

The inequality (11), after multiplication by 1641, gives

$$|m(1226+\phi)-1641n+1641\beta| < (1641)(0{\cdot}07)(13{\cdot}9)^{-m}, \tag{22}$$

where $|\phi| < 0{\cdot}000073$. We have

$$|m\phi| < (500)(0{\cdot}000073) = 0{\cdot}0365.$$

From the first few digits of the computed values of β and β' we find that

$$1641\beta \equiv 0{\cdot}445\ldots, \qquad 1641\beta' \equiv 0{\cdot}402\ldots \pmod 1.$$

Hence (22) implies that

$$(1641)(0{\cdot}07)(13{\cdot}9)^{-m} > 0{\cdot}402 - 0{\cdot}0365 > 0{\cdot}36.$$

This gives $(13{\cdot}9)^m < 330$, which contradicts the supposition that $m \geqslant 3$.

5. We add a remark on the situation that would arise if the condition (16) of the lemma were not satisfied, that is, if

$$\|q\beta\| < 3K^{-1}.$$

Assuming that m satisfies (17), we could deduce from (18) that

$$|mp-nq+j| < 2K^{-1}+K^{-1}+3K^{-1} < 1,$$

where j denotes the integer nearest to $q\beta$. Hence $mp-nq+j = 0$, whence

$$mp \equiv -j \pmod q.$$

Although we can no longer conclude that there is no value for m in

† Alternatively we could quote Professor van Lint's result, mentioned in § 1, which amply suffices to exclude the range (21).

the range (17), we can say that there is at most one value to the modulus q, and this value is determined by the last congruence.

We know that $q \leqslant KM$. If $q > M$ there is at most one possible value for m in the range (17), and this value can be determined. Briefly, we may say that the present method fails only if $\|q\beta\|$ is exceptionally small *and* also q is exceptionally small relative to its upper bound.

APPENDIX. THE VALUES OF θ, q, β, β'.

$\theta =$ 0·74710 53797 84665 20012 01543 70987 43429 80788 38030 33805 98797 18301
35215 93101 65894 47558 71410 09083 24719 77026 94022 04272 36844 47074
12471 86614 61948 57047 19002 59494 92414 81632 70994 94874 69347 92496
91746 24447 67322 96759 75122 37578 13578 73124 15223 97375 42550 86341
28408 25852 32591 47071 00203 68677 30525 49839 41970 29261 92204 22891
43800 20286 28173 00021 25091 33330 75577 40328 56109 12631 96764 70569
72451 16785 94198 27261 53378 94148 84993 47452 47667 23032 11653 10130
86010 46320 29261 53811 64490 95474 32247 03604 38397 56356 47375 70168
28514 93764 33915 54651 84476 50745 31255 47734 79366 84695 75323 73773
98596 90872 05357 48632 71575 73345 15432 39157 21023 12872 93047 94800
33410 93254 62223 30771 97782 12679 72909 42929 67622 08492 21581 32178
26581 12367 25841 21769 17572 61976 36624 98418 60008 85792 47238 32628
32222 89486 91846 90299 07988 05903 31092 48415 65542 28419 93613 77973
67235 04025 57642 33030 84735 93059 68760 55579 10259 95202 20134 85601
51088 89303 73392 63441 53718 21337 47465 42915 64887 15496 76429 45982
14245 68497 89212 01339 47968 11799 75610 73086 64334 38232 94611 59189
14362 68415 65033 69402 08626 09575 88446 47642 92194 37848 30748 31024
40658 02911 72935 86428 ...

$q =$ 74766 56458 85928 21002 92900 19462 74193 99932 88435 51834 20544 67033
92527 99010 36030 14382 83128 15409 94079 49641 75823 72448 20294 43561
15091 97552 65496 09837 65725 70805 71781 03765 90201 82968 04828 89690
91216 09036 42656 74598 43126 05161 50601 13889 48311 34448 43630 77762
01995 69513 73885 70540 20065 08420 17453 43949 32542 08937 08733 92823
67336 28270 20008 54767 81468 64873 46464 28193 39455 78382 27505 86507
22688 57730 19978 42556 32569 44952 91835 82629 52538 66886 97685 22768
40839 96403 83429 92464 53386 46774 48258 60409 41197 29139 39485 18564
04207 26381 80339 63053 74225 67257 33135 04814

$\beta =$ 0·08680 37805 12726 74666 69179 85488 62043 09400 27562 31574 12877 44764
42664 28757 89578 98145 21965 19697 05574 28783 21749 69001 82663 24834
80663 05244 98911 19398 56491 59574 01089 34897 96813 75064 05999 88171
95279 65147 39498 28092 74652 90349 62678 25701 15528 75403 74101 03040
87505 54397 75699 60798 74511 12895 88873 67037 42711 63728 86192 87848
27564 19617 43926 14760 27387 41800 50878 86533 96430 95496 14099 31433
84419 17195 70143 71770 27723 87850 35938 79210 52022 24095 07526 40991
11866 20763 45290 13873 99973 88701 25650 86849 14626 33878 78815 95526
86078 33335 21371 61124 43499 21963 23097 54263 11308 07760 67047 34288
66526 08151 32771 13909 99186 93785 64542 32504 65508 56795 29420 92260
...

$\beta' =$ 0·50603 46008 68222 91804 14949 94047 61694 65628 61040 77955 89969 04661
15752 89767 64976 12579 10005 81725 98914 50295 80769 55476 17076 86182
64440 51854 36894 64016 85056 73685 91186 49665 28670 81998 20342 04331
79306 55575 31729 03499 56731 43626 36835 59411 11827 79697 77938 00624
88310 88665 22832 69977 09507 81708 41787 29625 06854 49359 59620 26853
77980 95960 87174 07966 08986 40846 21565 24301 23635 18841 20171 12637
74479 34127 22890 92792 34774 67846 08610 33345 64568 42402 89743 35718
12468 39950 19777 79282 86894 54616 98550 00504 56067 19130 72716 44096
07161 51424 88110 40061 26748 54614 33862 62064 40038 55624 13853 14742
97572 37308 03106 56198 80532 74986 10038 31627 21012 75755 46135 69439
...

Trinity College
Cambridge