MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 143
JULY 1978, PAGES 936-940

On a Method of Solving a Class of Diophantine Equations

By Charles M. Grinstead

Abstract. An elementary method for solving simultaneous Diophantine equations is given. This method will in general lead quickly to a solution-free region on the order of $1 < x < 10^{10^{50}}$. The method is illustrated by applying it to a set of Diophantine equations.

1. In the paper "The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$," [2], the authors, A. Baker and H. Davenport, applied a theorem of Baker to show that if any simultaneous solution of the two equations existed, it had the property that $x < 4^{10^{487}}$. They were then left with the problem of ruling out all x in the region $1 \leqslant x < 4^{10^{487}}$, except for the two known solutions, namely $x = 1$ and $x = 11$. They accomplished this by using a lemma from Diophantine approximation theory, and by calculating several real numbers to 600 decimal places. The purpose of this paper is to suggest an alternate method of completing the last part of the above proof, and to illustrate this method by applying it to a similar problem.

2. We begin by defining triangle, square, and centered hexagonal numbers as the numbers given by the formulas $x_n = \frac{1}{2}(n)(n-1)$, $y_n = n^2$, and $z_n = 1 + 3(n)(n-1)$, respectively. The centered hexagonal numbers arise geometrically by starting with one point, putting six points around the first point to form a hexagon, and continuing to build outward with 12 points, 18 points, and so on. The number of points in the nth arrangement is z_n.

The question was raised as to whether there are any integers besides 1 which are of all three of the above types (see [3]). We will show that 1 is the only simultaneous solution.

3. We will show that if any other solution exists, it must be less than $4^{10^{455}}$. To do this, we follow the proof in Baker and Davenport [2].

We wish to solve the following system of Diophantine equations:

$$k^2 + k = 2m^2, \qquad 3n^2 - 3n + 1 = m^2.$$

The set of solutions of the first equation form a second order linear recurrent sequence, with

$$m_l = \frac{(3 + 2\sqrt{2})^l - (3 - 2\sqrt{2})^l}{4\sqrt{2}}, \qquad l \geqslant 1.$$

The corresponding recurrent sequence is given by:

Received February 1, 1977; revised September 6, 1977.
AMS (MOS) subject classifications (1970). Primary 10B05.
Key words and phrases. Diophantine equations, linear recurrent sequences.

$$m_1 = 1, \qquad m_2 = 6, \qquad m_l = 6m_{l-1} - m_{l-2}, \qquad l \geqslant 3.$$

Similarly, the solutions of the second equation are given by:

$$m'_r = \frac{(2+\sqrt{3})^{2r-1} + (2-\sqrt{3})^{2r-1}}{4}, \qquad r \geqslant 1,$$

and

$$m'_1 = 1, \qquad m'_2 = 13, \qquad m'_r = 14m'_{r-1} - m'_{r-2}, \qquad r \geqslant 3.$$

We wish to find l and r such that $m_l = m'_r$. Letting this common value be m, we have:

$$4m = \frac{(3+2\sqrt{2})^l}{\sqrt{2}} - \frac{(3+2\sqrt{2})^{-l}}{\sqrt{2}} = (2+\sqrt{3})^{2r-1} + (2+\sqrt{3})^{-(2r-1)}.$$

Let $P = (3+2\sqrt{2})^l/\sqrt{2}$, and $Q = (2+\sqrt{3})^{2r-1}$. Then, we have:

$$P - \frac{1}{2}P^{-1} = Q + Q^{-1}.$$

Since $P^{-1} > 0$, $Q^{-1} > 0$, we have $P > Q$. Also,

$$P = Q + Q^{-1} + \frac{1}{2}P^{-1} < Q + \frac{3}{2}Q^{-1} < Q + \frac{3}{2},$$

so $Q > P - 3/2$.

We may suppose that $l \geqslant 3$, so $P \geqslant (3+2\sqrt{2})^3/\sqrt{2} > 125$. Therefore,

$$P - Q = \frac{1}{2}P^{-1} + Q^{-1} < \frac{1}{2}P^{-1} + \left(P - \frac{3}{2}\right)^{-1} < \frac{61}{40}P^{-1},$$

since $(P - 3/2)^{-1} < 41P^{-1}/40$. So,

$$0 < \log\frac{P}{Q} = -\log\left(1 - \frac{P-Q}{P}\right) < \left(\frac{61}{40}P^{-2}\right) + \left(\frac{61}{40}P^{-2}\right)^2$$

$$= \left(\frac{61}{40}P^{-2}\right)\left[1 + \frac{61}{40}P^{-2}\right] < \left(\frac{61}{40}P^{-2}\right)\left[1 + \frac{61}{40}\left(\frac{1}{125}\right)^2\right] < (1.526)P^{-2}.$$

If we substitute for P and Q in this last inequality, we obtain:

$$0 < (l)\log(3+2\sqrt{2}) - (2r-1)\log(2+\sqrt{3}) - \log(\sqrt{2})$$
$$< (1.526)P^{-2} < (3.052)(3+2\sqrt{2})^{-2l}.$$

We now state a theorem of Baker.

THEOREM (BAKER [1]). *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 $d \geqslant 4$, $A \geqslant 4$. If the rational integers $b_1, \ldots, b_k$ satisfy*

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

where $0 < \delta \leqslant 1$, *and* $H = \max(|b_1|, \ldots, |b_k|)$, *then* $H < (4^{k^2}\delta^{-1}d^{2k}\log A)^{(2k+1)^2}$.

We apply this theorem to the last inequality, with $k = 3$, $\alpha_1 = 3 + 2\sqrt{2}$, $\alpha_2 = 2 + \sqrt{3}$, $\alpha_3 = \sqrt{2}$, $H = \max(l, 2r - 1) = 2r - 1$.

Since $P > Q$, we have $P^2 > Q^2$, so

$$\frac{(3 + 2\sqrt{2})^{2l}}{2} > (2 + \sqrt{3})^{4r+2} > e^{4r+2} > \frac{3}{2}e^{2r+1}.$$

Thus, $(3 + 2\sqrt{2})^{2l} > 3e^{2r+1} > (2.27)r^{2r+1}$, so

$$\frac{2.27}{(3 + 2\sqrt{2})^{2l}} < \frac{1}{e^{2r+1}},$$

so we may take $\delta = 1$.

The equations satisfied by α_1, α_2 and α_3 are:

$$\alpha_1^2 - 6\alpha_1 + 1 = 0, \quad \alpha_2^2 - 4\alpha_2 + 1 = 0 \quad \text{and} \quad \alpha_3^2 - 2 = 0.$$

Hence, the maximum height of α_1, α_2 and α_3 is $A = 6$. We also have $d = 4$.

The theorem then gives:

$$2r + 1 = H < (4^9 \circ 4^6 \circ \log 6)^{49} < 4^{735} \cdot (1.7918)^{49} < 10^{455}.$$

So, $m < Q/4 + 1 < (2 + \sqrt{3})^{10^{455}} < 4^{10^{455}}$.

4. In this section we will give the method which shows that 1 is the only solution in the range $m < 4^{10^{455}}$.

We wish to find l and r such that $m_l = m'_r$. With the aid of a computer, we are able to show that the statement $m_l = m'_r$ implies that $l \equiv 1 \pmod{p}$, for all primes $p < 1095$. Therefore, $l \equiv 1 \pmod{\Pi_{p<1095}p}$. Thus, either $l = 1$, or $l > \Pi_{p<1095}p > 10^{460}$. But if $l = 1$, then $m_l = 1$, and if $l > 10^{460}$, then $m_l > 5^{10^{460}} > 4^{10^{455}}$, so m_l is outside the range of solutions.

Given a prime $p < 1095$, we will assume that the statement $m_l = m'_r$ implies $l \equiv 1 \pmod{q}$ for all primes $q < p$. (We also assume that $l \equiv 1 \pmod{2^4 \cdot 3^2 \cdot 5^2}$, which can be shown by hand calculation.) Next, we define $L(q)$ as the length of the period of the linear recurrence defining $m_l \pmod{q}$. We generate a list of primes q, such that (1) $p \mid L(q)$, $p^2 \nmid L(q)$, (2) no prime larger than p divides $L(q)$, and (3) $L(q)$ has no multiple prime factors, except possibly 2^2, 2^3, 2^4, 3^2, or 5^2.

Now the two sequences $\{m_l\}$ and $\{m'_r\}$ are generated (mod q). We know that $m_l \equiv m'_r \pmod{q}$ for any solution m_l, and also, by induction, we know that $l \equiv 1 \pmod{L(q)/p}$. Thus, if we write the sequence $\{m_l\} \pmod{q}$, we have only p possible positions for solutions, namely those positions $\equiv 1 \pmod{L(q)/p}$. If any number in these positions does not occur in the sequence $\{m'_r\} \pmod{q}$, that position may be ruled out. If we have not ruled out all remaining positions except the first position (which will never be ruled out because $m_l = 1$ is a solution), then we record which positions have not been ruled out (mod p), and move to the next q on our list. As

soon as all positions except the first position have been ruled out, we know that $l \equiv 1 \pmod{p}$, and we go to the next prime greater than p. When this was done on a computer, in every case, l was shown to be 1 (mod p) by using at most eight q's. The actual program was written in Fortran IV by Ken Muntz, and was run on a Xerox Sigma 5 computer.

We now illustrate this method with an example. We will show that $l \equiv 1 \pmod{5}$. We assume that $l \equiv 1 \pmod{2^4 \cdot 3^2}$, which can be shown in a manner similar to what follows. The two values of q we will use are $q = 19$ and $q = 29$. We have $L(19) = 20$ and $L(29) = 10$. The sequence $\{m_l\}$ (mod 19) is:

$$\{1, 6, 16, 14, 11, 14, 16, 6, 1, 0, 18, 13, 3, 5, 8, 5, 3, 13, 18, 0\}.$$

Since we know that $l \equiv 1 \pmod{4}$, we need only look at every fourth term, starting with the first one. The sequence $\{m'_r\}$ (mod 19) is:

$$\{1, 13, 10, 13\}.$$

By comparing sequences, we see that $l \equiv 1, 9 \pmod{20}$ are the only two possible positions for solutions, so $l \equiv 1, 4 \pmod{5}$. We now rule out the possibility that $l = 4 \pmod{5}$. The sequence $\{m_l\}$ (mod 29) is:

$$\{1, 6, 6, 8, 0, 28, 23, 28, 0, 1\}.$$

The sequence $\{m'_r\}$ (mod 29) is:

$$\{1, 13, 7, 27, 23, 5, 18, 15, 18, 5, 23, 27, 7, 13, 1\}.$$

Since the number 0 is in the position 9 (mod 10) in the first sequence, and it does not occur in the second sequence, we have $l \equiv 1 \pmod{5}$.

5. We close by making a few remarks. First of all, if there had been more than one known solution of the problem, then we could split each recurrent sequence $\{m_l\}$ into several recurrent sequences of the form $\{m_{al+b}\}$ for $0 \leqslant b < a$, so that each sequence has at most one known solution, and then apply the method.

Secondly, there are two questions which one can ask about the generality of the method. One is whether the method will detect previously unknown solutions. The other is whether it will be possible to show $m_l = m'_r$ implies $l \equiv 1 \pmod{p}$ for all primes less than a certain large number (e.g. 1095), assuming all solutions are known.

The answers to both of these questions are heuristic ones. We believe that the bounds given by Baker's Theorem for solutions of these types of equations are too high, i.e. that the solutions of these types of equations do not approach the bounds. In the present problem, showing that $m_l = m'_r$ implies $l \equiv 1 \pmod{p}$ for primes less than 20 can be accomplished on a hand calculator in less than an hour. This shows that if a solution exists, it must be larger than $5^{(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19)} > 10^{10^{4.87}}$. So, if there is an unknown solution, and it is not "near" the upper bound given by Baker's Theorem, then we will quickly find that we will not be able to show that $m_l = m'_r$ implies $l \equiv 1 \pmod{p}$ for some small p. This failure will be fairly obvious, i.e. the same numbers, modulo certain small primes, will fail to be eliminated after

many trials. In this case it still remains to find the other solutions. So, we can assume that for many primes, q_j, we have shown that any solution must be $\equiv 1 \pmod{p}$, and for the primes p_i, $i = 1, \ldots, n$, we have shown that any solution must be $\equiv 1$ or $l_i \pmod{p_i}$. Then, given a sequence of values for the primes p_i (either 1 or l_i), there is at most one solution with the values, since two solutions with these same values would have to differ by $R = (\Pi_{i=1}^{n} p_i)(\Pi_j q_j)$, so at least one solution would have to be larger than R. The only supposed solution $< R$ would be easy to solve for, using congruences, and could then be checked.

To answer the second question, we first recall that we may assume there is only one solution (see above). Now, given a prime p, we assume that $m_l = m'_r$ implies $l \equiv 1 \pmod{q}$ for all $q < p$. If we take a prime s such that $p \| L(s)$, and p is the largest prime dividing $L(s)$, then we need only look at p terms in the sequence $\{m_l \pmod{s}: 1 \leqslant l \leqslant L(s)\}$. When s is large compared to p, most numbers (mod s) do not appear in this list, and the same can be said of the corresponding subsequence of $\{m'_r \pmod{s}\}$. So, on heuristic probabilistic grounds, the larger the value of s, the smaller the overlap. Recall also that the method is *cumulative,* so we do not have to eliminate all the subscripts with just one value of s. Furthermore, we need not show that $m_l = m'_r$ implies $l \equiv 1 \pmod{p}$ for *every* p less than a certain number. If we find that there is a prime t which will not work in this way, we could easily skip it and go on, taking care to eliminate all primes s with $t | L(s)$ from our lists. If t is relatively large, say $t > 100$, the number of s which we must eliminate will be very small.

Other methods of attack on this type of problem are given in [4] and [5].

The author would like to thank Ken Muntz for writing the computer program, and David Cantor and Ernst Straus for their advice.

Department of Mathematics
University of California
Los Angeles, California 90024

1. A. BAKER, "Linear forms in the logarithms of algebraic numbers," *Mathematika*, v. 15, 1968, pp. 204–216.

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

3. M. GARDNER, "On the patterns and the unusual properties of figurate numbers," *Sci. Amer.*, v. 231, no. 1, 1974, pp. 116–121.

4. P. KANAGASABAPATHY & T. PONNUDURAI, "The simultaneous diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$," *Quart. J. Math.*, v. 26, 1975, pp. 275–278.

5. GIOVANNI SANSONE, "Il sistema diofanteo $N + 1 = x^2$, $3N + 1 = y^2$, $8N + 1 = z^2$," *Ann. Mat. Pura Appl.* (4), v. 111, 1976, pp. 125–151.