MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 212
OCTOBER 1995, PAGES 1717–1731

48 MORE SOLUTIONS OF MARTIN DAVIS'S QUATERNARY QUARTIC EQUATION

DANIEL SHANKS AND SAMUEL S. WAGSTAFF, JR.

Dedicated to D. H. Lehmer and Julia Robinson

ABSTRACT. We find 48 more solutions to a Diophantine equation investigated by Martin Davis. Before our work, only two solutions were known. Construction of the new solutions required the factorization of several large integers. Because the equation relates to Hilbert's Tenth Problem it is desirable to know if it has only finitely many solutions. An elaborate argument is given for the conjecture that the equation has infinitely many solutions in integers.

1. INTRODUCTION

Martin Davis [1] introduced the equation

$$9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2 \tag{1}$$

with the catchy name "one equation to rule them all", and proved that if it had no solution in nonnegative integers other than the trivial

$$u = r = 1, \qquad v = s = 0, \tag{2}$$

then Hilbert's tenth problem would be unsolvable. Herrmann proved [2] the existence of a nontrivial solution, but he did not compute it explicitly. That was done by Shanks [3, p.68] who gave it as

$$\begin{aligned} u &= 525692038369576, \quad v = 1556327039191013, \\ r &= 2484616164142152, \quad s = 1381783865776981. \end{aligned} \tag{3}$$

At this point, Julia Robinson (as indicated in [3]), extended Davis's theorem by stating that if (1) had only finitely many solutions, then Hilbert's tenth problem would be unsolvable.

Shortly after this, Matiyasevich did prove it unsolvable by a different method. His new book [4] gives an exposition of the whole field. On page 36, he asks, as an open question, whether (1) does, or does not, have infinitely many solutions.

Received by the editor August 22, 1994.
1991 *Mathematics Subject Classification.* Primary 11D25; Secondary 11D09, 11Y05.
Key words and phrases. Hilbert's Tenth Problem, Diophantine equations, quadratic forms, factoring integers.
Some of the computing reported in this work was performed on a MasPar computer at Purdue University, which was supported in part by NSF Infrastructure Grant CDA-9015696.

We do what we can with that question later, but first we wish to show the existence of more solutions as in our title.

2. The Herrmann-Shanks solution

Herrmann begins with the Pell-like

$$9(A_n)^2 - 7(B_n)^2 = 2 \tag{4}$$

and obtains all positive A_n and B_n that satisfy (4). Beginning with the trivial solution (2), he gives

$$A_0 = 1, \qquad B_0 = 1 \tag{5}$$

and the simple recursions

$$A_{n+1} = 8A_n + 7B_n, \qquad B_{n+1} = 9A_n + 8B_n. \tag{6}$$

The two sequences grow exponentially like

$$(8 + 3\sqrt{7})^n$$

and give all positive solutions of (4).

Let us list n, A_n, and B_n (mod 7):

n	0	1	2	3	4	5	6
A_n	1	1	1	1	1	1	1
B_n	1	3	5	0	2	4	6

For a given n in (4) the question now is whether

$$A_n = u^2 + 7v^2, \qquad B_n = r^2 + 7s^2 \tag{7}$$

both have solutions. Let z be a positive integer. The criterion for odd z such that

$$z = x^2 + 7y^2 \tag{8}$$

is classical: such x and y exist if, and only if, *all* prime-power divisors P of z, that is:

$$P = p^k \parallel z,$$

satisfy

$$P \equiv 0, 1, 2, \text{ or } 4 \pmod 7. \tag{9}$$

Since a product π of P satisfying (9) again satisfies

$$\pi \equiv 0, 1, 2, \text{ or } 4 \pmod 7,$$

it follows from our table that if

$$n \equiv 1, 2, \text{ or } 6 \pmod 7, \tag{10}$$

B_n *cannot* satisfy (7). So those n, given by (10), *cannot* give us a solution of (1).

By further sieving discussed below, and massive computation, Herrmann first suspected, and then proved, that the 32-digit numbers A_{26} and B_{26} (with $26 \equiv 5 \pmod 7$) were both prime. This was his nonconstructive existence theorem for a nontrivial solution of (1).

In [3], QUPAPR (Quadratic Partitions of Primes) is one of the "five number-theoretic algorithms" of the title. It computes, very efficiently, x, y, and m in

$$p = (x^2 + Ny^2)/m \tag{11}$$

for any prime p for which

$$\left(\frac{-N}{p}\right) = +1, \tag{12}$$

and where m is minimal, and therefore $m = 1$ if that is possible. Then two examples are given. The remarkable prime $p = 26437680473689$ satisfies (12) for all N from 1 to 150, and so the solutions x, y, and m are listed for all these N. Second, for $p = A_{26}$, B_{26}, $N = 7$, and $m = 1$, the solution (3) is given. The amusing point is made that it is much faster to compute the *explicit* solution (3) than to do the lengthy primality tests for A_{26}, B_{26}, and thereby only obtain an existence theorem.

3. More solutions

The new book [4] renewed interest in the problem and the open question. With a little sieving, discussed below, A_n, B_n looked promising for $n = 33$ and 35. In the quarter century since Herrmann's paper, algorithms for primality and factorization have improved enormously. Since much of this progress is associated with the journal *Mathematics of Computation* and the Cunningham Project, the present authors can claim a minor role, since one of us is an editor of the journal and the other is the manager of the project. One of us asked the other to please factor A_{33}, B_{33}, A_{35}, B_{35}. The whole table of factors of A_n, B_n, from $n = 1$ to 35 was produced at once and is exhibited in the Appendix below.

Note first that A_{26} and B_{26} are confirmed to be prime. Now examine A_{33} and B_{33} and reduce them and their prime factors modulo 7. We have

$$\begin{aligned} A_{33} &\equiv 1 \equiv 4 \cdot 1 \cdot 2 \pmod 7, \\ B_{33} &\equiv 4 \equiv 1 \cdot 4 \cdot 1 \pmod 7. \end{aligned} \tag{13}$$

All prime factors here are expressible as

$$p = x^2 + 7y^2$$

and, for the first two prime factors of A_{33} we have

$$1607 = 40^2 + 7 \cdot 1^2, \qquad 243402458839 = 179208^2 + 7 \cdot 173735^2.$$

Then, the two products

$$(40 + \sqrt{-7})(179208 \pm 173735\sqrt{-7})$$

are

$$5952175 + 7128608\sqrt{-7}, \qquad 8384465 - 6770192\sqrt{-7},$$

and give the product of these first two prime factors by two representations, namely

$$(5952175^2 + 7 \cdot 7128608^2) = (8384465^2 + 7 \cdot 6770192^2).$$

Then, continuation with the third prime factor gives us four distinct representations:

$$A_{33} = u^2 + 7v^2.$$

Likewise, we obtain four for

$$B_{33} = r^2 + 7s^2.$$

So, $n = 33$ gives us 16 solutions of (1). There is no real value in listing these 16 sets of big numbers u, v, r, and s since their only known purpose is visibility.

Similarly for $n = 35$, we have

$$\begin{aligned} A_{35} &\equiv 1 \equiv 1 \cdot 1 && \pmod 7, \\ B_{35} &\equiv 1 \equiv 2 \cdot 2 \cdot 4 \cdot 4 \cdot 1 && \pmod 7 \end{aligned} \tag{14}$$

and therefore 32 more solutions of (1). Then, and this is the easy part,

$$16 + 32 = 48. \tag{15}$$

4. The conjecture

The "Open Question" whether (1) has infinitely many solutions may be very difficult. It is even possible that it is undecidable. We have been sensitized to that possibility by our earlier collaboration [5, 6] on the problem of Euclid's Primes. Freeman Dyson suggested that the conjecture in [5] may be undecidable.

We give our best judgement of the question concerning (1) and embody that in our

Conjecture 1. *Equation* (1) *has infinitely many solutions in integers.*

The fact that we so easily obtained 48 new solutions of (1) is *not* evidence for Conjecture 1. The number of decimals in A_n and B_n is approximately

$$n \log_{10}(8 + 3\sqrt{7}) = 1.202n,$$

and for $n = 33$ or 35 factorization is now easy. But one would not have to increase n too much before even the NSA could not factor A_n and B_n. The difficulty of factoring very large numbers creates the possibility that our conjecture may be undecidable.

Consider the positive integers z given by (8). Let the number of such integers $\leq Z$ be $B_7(Z)$. Then, by a variation of a theorem of Landau [7] one has

$$B_7(Z) \sim \frac{b_7 Z}{\sqrt{\log Z}}, \tag{16}$$

where

$$b_7 = 0.543539641. \tag{17}$$

For comparison, let $B_3(Z)$ be the number of positive integers $z \leq Z$ of the form

$$z = x^2 + 3y^2.$$

Then one has

$$B_3(Z) \sim \frac{0.638909405\ Z}{\sqrt{\log Z}}. \tag{18}$$

The function-theoretic source of (16) comes from the distribution of primes into

(19)
$$\begin{aligned} &p \text{ primes, where } p \equiv 1, 2, \text{ or } 4 \pmod 7 \\ &\text{and} \\ &q \text{ primes, where } q \equiv 3, 5, \text{ or } 6 \pmod 7. \end{aligned}$$

The denominator $\sqrt{\log Z}$ comes from the fact that the p and q primes are equinumerous as they go to infinity, while the constant b_7 is based upon the details of their distribution. Whereas in (18), we have two types of primes:

$$p \equiv 1 \pmod 3, \qquad q \equiv 2 \pmod 3.$$

These are also equinumerous, but they have a detailed distribution distinct from those in (19). So $\sqrt{\log Z}$ remains the same, while the constant is different. We will need this distinction presently.

Let us interpret (16) by saying the probability of (8) is

(20)
$$\frac{b_7}{\sqrt{\log z}}.$$

Our B_n range over all residue classes (mod 7) like all positive integers z, and are divisible by some p primes and some q primes.

Let us *tentatively*, subject to correction later, assume the probability of

(21)
$$B_n = r^2 + 7s^2$$

to be

$$\frac{b_7}{\sqrt{\log B_n}} \approx \frac{b_7}{\sqrt{n \log(8 + 3\sqrt{7})}}.$$

That equals

(22)
$$\frac{0.327}{\sqrt{n}}.$$

Now $A_n \equiv 1 \pmod 7$ always, and let us assume with sufficient accuracy, that the probability of

(23)
$$A_n = u^2 + 7v^2$$

is twice that of (22), and let us assume, as seems to be true, that (21) and (23) are independent events. Then the probability that n gives us a solution is

$$\frac{0.213}{n}.$$

So the number of $n \leq N$ that yield solutions is

(24)
$$0.213(\log N + \gamma),$$

i.e., it goes to infinity.

But the *number* of solutions goes to infinity much faster. The second case, $n = 26$, is freakish in that it gives only one solution. Usually we have 2^m solutions, and on the average, m will increase with n.

This is evidence for our conjecture. But wait; we must make the correction mentioned above. It is in fact, the most interesting part of the paper.

5. The intricate balance

Before we launch into that, we must correct two errors in [2, p. 209]. In his (6.6) Herrmann states that the primitive period of (A_n, B_n) mod P for any prime $P > 3$ is a divisor of

$$P - \left(\frac{P}{7}\right).$$

That is an error, typographical or otherwise; it should read

$$P - \left(\frac{7}{P}\right).$$

His $(P/7) = (-7/P)$ is the character for $Q(\sqrt{-7})$ as in (19) whereas the character for $Q(\sqrt{7})$, which is $(7/P)$, is appropriate for (4). For example, for $P = 31$, the primitive period is 15 which divides $30 = 31 - (7/31)$ and not $32 = 31 - (31/7)$. Note, in our factor table, 31 divides B_7 and then B_{22}, and $22 - 7 = 15$.

Secondly, in "the first case" at the bottom of page 209, he suggests there may be q primes that never divide A_n or B_n. There are no such q primes, for if P is a q prime, then

$$P - \left(\frac{7}{P}\right) = q \pm 1$$

according as $q = 4k \pm 1$. In either case $q \pm 1$ is twice an odd number. But if the primitive period is $2(2n_0 + 1)$, then $q | A_{n_0}$ as in Herrmann's (6.1). And if the primitive period is $(2n_0 + 1)$, then $q | B_{n_0}$ as in his (6.2).

Let us examine which primes divide which A_n or B_n, and which primes divide neither. First, 2, 3 and 7 are special, since they occur in (1). One finds

2 never divides A_n or B_n,
3 divides A_n for all $n = 3k + 1$,
7 divides B_n for all $n = 7k + 3$.

There are simple rules for 3^k and 7^k to be divisors, but we can skip them for brevity.

For any q prime there is a positive n_0 which we call its *pioneer*. Then, as in [2, pp. 209, 210 as corrected], q divides A_n, or B_n, but not both, for all

$$n = (2n_0 + 1)k + n_0. \tag{25}$$

The odd number $(2n_0 + 1)$ we call q's *period*. To determine the period, and therefore the pioneer of any $q > 3$, one finds

$$2n_0 + 1 = (q \pm 1)/2m, \tag{26}$$

where m is some divisor, necessarily odd, of $(q \pm 1)$, and where we select ± 1 according as

$$q = 4k \pm 1. \tag{27}$$

Frequently, $m = 1$. Once we compute the pioneer n_0 of q from the *first* zero of A_n or B_n (mod q), then, of course,

$$m = (q \pm 1)/2(2n_0 + 1).$$

For those frequent q where $m = 1$, we have

$$n_0 \approx \tfrac{1}{4}q, \tag{28}$$

an important point since, as we shall see, the n_0 for p primes will always be smaller.

Before we go on to the surprising behavior of the p primes, let us make an application of the q-theory in (25) and (26). After a little sieving with small primes, it was observed that no q prime seemed to be a divisor for $n = 33$. Since $2 \cdot 33 + 1$ is prime, it follows that no q having a pioneer < 33 divides A_{33} or B_{33}. Therefore, if any q does divide, 33 must be its pioneer n_0. Then from (26), we have

$$q = 134(2t + 1) \mp 1,$$

where we have replaced the odd m by $(2t + 1)$. On a little HP42S calculator, it was quickly found that no

$$q = 268t + 133 \text{ or } 135 < 10,000$$

divides A_{33} or B_{33}, and this suggested that A_{33} and B_{33} may be q-free.

Likewise for A_{35} and B_{35} and

$$q = 284t + 141 \text{ or } 143 < 10,000.$$

That is why we went on to factor A_n and B_n for $n = 33$ and $n = 35$. Actually, as it turns out, Herrmann [2] had done something similar for $n = 26$ except that he tried both p and q primes as divisors.

Now we go to the startling behavior of the p primes. We write any $p > 2$ in terms of two nonnegative parameters s and t as

$$p = 2^s(8t + 4) \pm 1. \tag{29}$$

We call s the *variety* of p and, for clarity, we list the first three varieties:

s	p	density
0	$8t + 3$ or 5	1/2
1	$16t + 7$ or 9	1/4
2	$32t + 15$ or 17	1/8

One-half of the p, those in variety 0, have the forms $8t+3$ or 5. One-quarter of the p, those in variety 1, have the forms $16t + 7$ or 9, etc.

The first important fact is that *all* p in variety 0, namely $p = 11, 29, 37, 43, 53, \ldots,$ behave like 2: they never divide A_n or B_n since both contingencies contradict (4) modulo p. All p in varieties $s > 0$ are in six residue classes (mod 56), namely,

$$p \equiv 23, 25, 15, 9, 39, \text{ or } 1 \pmod{56}. \tag{30}$$

We may visualize these six residues as a cyclic subgroup in the cycle graph for 56 shown on [8, any edition, p.88]. Now *most* of the p primes in (30) also behave like 2, they never divide A_n or B_n!

Let us examine the first 30 examples of $p \equiv 9 \pmod{56}$ and $p \equiv 39 \pmod{56}$ in Table 1 listing their pioneers, if they have one. The table was computed on a HP42S, as before.

TABLE 1

$56t + 9$			$56t + 39$		
p		n_0	p		n_0
233	–	–	151	–	–
401	–	–	263	B	16
457	B	28	431	–	–
569	B	35	487	–	–
1129	–	–	599	B	37
1297	–	–	823	B	51
1409	–	–	991	–	–
1801	A	37	1103	–	–
1913	A	119	1327	–	–
2081	–	–	1439	–	–
2137	–	–	1607	A	33
2417	B	75	1663	–	–
2473	B	154	1831	B	114
2753	–	–	1999	–	–
3089	–	–	2111	–	–
3257	B	203	2447	A	25
3313	B	11	2503	–	–
3593	–	–	2671	–	–
3761	–	–	3119	–	–
3929	B	245	3343	–	–
4153	B	259	3511	–	–
4657	–	–	3623	A	226
4937	B	308	3847	–	–
4993	–	–	4127	–	–
5273	A	329	4463	–	–
5441	–	–	4519	–	–
6113	–	–	4799	–	–
6337	–	–	4967	–	–
6449	–	–	5023	–	–
6673	–	–	5303	A	25

The table is read this way:

$p = 233, 401, 1129, \ldots,$ and $p = 151, 431, 487, \ldots$ behave like 2; they never divide A_n or B_n. On the other hand

$$\begin{aligned} 457 &\text{ divides } B_n \text{ for } n = 57k + 28, \\ 1801 &\text{ divides } A_n \text{ for } n = 75k + 37, \\ 263 &\text{ divides } B_n \text{ for } n = 33k + 16, \\ 1607 &\text{ divides } A_n \text{ for } n = 67k + 33, \end{aligned}$$

etc., where, as before, the period equals $2n_0 + 1$ where n_0 is the pioneer.

Note that 1607 divides A_{33} as we previously observed. Likewise 569 divides B_{35}. The other four residues (mod 56) in (30) behave similarly to the two in Table 1 and are omitted for brevity.

Now note, of the 60 p primes in the table only 20 divide A_n or B_n. We conjecture that this is the correct asymptotic ratio:

Conjecture 2. *Asymptotically speaking, one-third of the p primes in varieties $s > 0$ divide A_n or B_n. They comprise one-sixth of all p primes.*

We think this conjecture is provable and may well be an already known theorem. There exists considerable literature on related problems.

Now consider the pioneers and periods for the p primes that do divide A_n or B_n. Instead of rule (26) for q primes we now have

$$2n_0 + 1 = (p \mp 1)/2^{s+2}m. \tag{31}$$

Here m, as before, is an odd divisor of $(p \mp 1)$. There are two important changes in (31) relative to (26): first, the signs $\pm$ have been interchanged for the primes

$$p = 4k \pm 1. \tag{32}$$

Second, instead of 2 in the denominator, we now have 8 for p of variety 1, 16 for p of variety 2, etc.

We may expect m to be distributed in the same way for q and p primes. But the power of 2 causes a major change. We may weight the factor

$$1/2^{s+2}$$

for p primes of variety s by the density

$$1/2^{s+1}$$

of p primes of variety s to obtain an average value of the factor. It is

$$\sum_{s=1}^{\infty} \frac{1}{2^{2s+3}} \Big/ \sum_{s=1}^{\infty} \frac{1}{2^{s+1}} = \frac{1}{12}. \tag{33}$$

Instead of $\frac{1}{2}$ in (26), on the average we have $\frac{1}{12}$ in (31). Therefore, on the average, the periods and pioneers of p primes will be only $\frac{1}{6}$ of the periods and pioneers of q primes.

In the A_n and B_n we therefore have a remarkable and intricate balance of q and p divisors. Only 1/6 of the p primes are divisors, but n-wise, they have been squeezed to the left by a factor of 6 and therefore as $n \to \infty$, we should expect equinumerous p and q divisors. Is this not wondrous strange? We quote Hamlet in Act 1, Scene 5: "There are more things in heaven and earth, Horatio, than are dreamt of in your philosophy."

The result is that instead of (22) as the probability, we now expect

$$\frac{b}{\sqrt{n}} \tag{34}$$

as the probability of (21), where b is an unknown constant. We do not know it even crudely, let alone with the precision in (17). Then, likewise, we replace (24) with

$$c(\log N + \gamma) \tag{35}$$

for an unknown constant c.

We have no doubt that many investigators have given heuristic arguments for Conjecture 1, and we have been told about two of them: D. J. Newman and Don Zagier. But we know of no one who has incorporated into his argument the intricate balancing of the p and q divisors of A_n and B_n that we have discussed in this section. Yet that is clearly necessary since that is how A_n and B_n actually behave.

Reader, as an exercise, verify from our

$$1607 \mid A_{33} \text{ and } 569 \mid B_{35}$$

mentioned above, and (31), that 33 and 35 are their pioneers, they both are of variety 1, and while the first has $m = 3$ the second has $m = 1$. The second, instead of (28) has

$$n_0 \approx \tfrac{1}{16} p.$$

That is the point: the intricate balance (33).

In [8, third or fourth edition, p. 239 ff], there is a lengthy analysis as to what kind and how much evidence a proposition should have before we call it a conjecture. By those standards, we cannot claim that our Conjecture 1 is as convincing as, say, the twin-prime conjecture. We may even admit a slight doubt in the correctness of (35). Nonetheless, as a whole, we believe that the evidence favors Conjecture 1 and we think it is true.

We wish to be candid about (35). There is a phenomenon here that we may not have properly included in our analysis. In the theory for (16) each q prime is acting individually with its own period q. But the q divisors of A_n and B_n often work in gangs. For example,

$$q = 3, 5, \text{ and } 17$$

all divide A_n or B_n for $n = 3k + 1$. Thus, an A_n or B_n that is struck by a q, may like Julius Caesar, be struck several times. This overkill must mean that the q comprise, effectively a smaller set, and on occasion an A_n and B_n both escape without injury. We do not know whether this mechanism merely changes the constant c in (35) or whether the function of N there actually changes. But in either case, it does not seem like it can damage Conjecture 1 since, if anything, it will cause more solutions to occur.

6. Sequel

While the foregoing was being typed, we continued with our computation and theory. We examined A_n and B_n for $36 \le n \le 200$, and quickly eliminated most of them, first, by using (10), and by sieving out those for which a q^{2k+1} factor had a small pioneer. Then we did a little trial-division factoring with small primes. On the few n that remained, elliptic curve factoring obtained a moderate q factor for most of them. Let us list examples since we wish to draw an inference later:

$$\begin{aligned} 121326659 &\mid A_{53}, & 74547793 &\mid B_{96}, \\ 13489347539 &\mid A_{54}, & 1098341 &\mid A_{189}, \\ 59061523 &\mid A_{68}, & 6402161 &\mid B_{194}. \end{aligned}$$

At this point, we were left with only $n = 81, 131, 153, 168, 173$, and 186 as those $n \leq 200$ possible for additional solutions. More elliptic factoring gave larger q factors, and

$$1128720907 \mid A_{173},$$
$$5097445601 \mid A_{186},$$
$$6584664031259 \mid A_{131},$$

left only

$$n = 81, 158, 168. \tag{36}$$

Now we pause for commentary. In these eliminations, it is clearly irrelevant whether q divides A_n or B_n, but we do not wish to deprive the reader of the criteria (mod 56) obtained by solving (4) modulo q:

TABLE 2: (mod 56)

3,	27,	19	$q \mid A_n$
5,	13,	45	$q \mid A_n$
17,	41,	33	$q \mid B_n$
31,	55,	47	$q \mid B_n$
11,	43,	51	$p \nmid A_n$ or B_n
37,	29,	53	$p \nmid A_n$ or B_n

In each line, the second entry is the cube of the first (mod 56), and the third is the fifth power of the first (mod 56). The first four triples are q primes and divide A_n or B_n as indicated. The last two triples are the p primes of variety 0, already discussed. All six triples comprise the alternate elements of the other six cyclic subgroups in the cycle graph for 56 previously mentioned [8, p.88].

Our second observation goes back to Conjecture 1. The *best* hope of disproving Conjecture 1 is to construct a *covering set*: that is, a moderate number of arithmetic progressions $n = a_i k + b_i$, with moderate coefficients a_i and b_i, that completely cover all $n >$ some N. But the large q listed above as divisors needed to eliminate $n = 54, 173, \ldots$ makes the existence of a covering set dubious.

Now we return to (36). A_{81} and B_{81} are 98 decimal digit composites. They cannot resist modern algorithms and computers but are not trivial: one must be appropriately equipped. By further elliptic curve factoring, we finally found a 20-digit p prime divisor of B_{81}. We call it p_{20}. Still more elliptic curve factoring on a faster machine, a MasPar ("massively parallel"), found nothing for B_{81} or A_{81}. At this point we know that the 78-digit B_{81}/p_{20} is a product of two p primes *or* two q primes.

But which? Is there an algorithm *faster* than factoring to make a determination? We know of none; it is an important question.

The 78-digit B_{81}/p_{20} was now treated by a different algorithm on the MasPar which was guaranteed to work in less than one hour. This algorithm [9] is known as ppmpqs. It is an advanced development of Pomerance's quadratic sieve. We spare you the details.

It did work and delivered $B_{81} = p_{20} \cdot q_{35} \cdot q_{44}$, where the subscripts on the q's give the number of decimal digits of the primes. They are q primes and $n = 81$ gives no solution of (1). For those who wish to see them, the factors

are

$$p_{20} = 74065332635371079447,$$
$$q_{35} = 12810478486228669448260507960524473,$$
$$q_{44} = 27954729044853253218766312116470987098157519.$$

Are we disappointed? Not really: we must admit a certain ambivalence. If $n = 81$ had worked, we would have to change our title and spoil the joke (15).

The two remaining candidates, $n = 158$ and 168, are beyond current techniques unless we are very lucky. We continue computations on them but must state that the prospects are not good. We are also continuing with some $n > 200$.

7. The rational case

For completeness, and though it may be too apparent to some readers, we will give a constructive proof of this

Theorem. *Equation* (1) *has infinitely many solutions in positive rational numbers.*

Proof. We need not venture beyond the trivial solution (2) where we had

$$u^2 + 7v^2 = 1, \qquad r^2 + 7s^2 = 1. \tag{37}$$

Let p be any p prime and write

$$p = a^2 + 7b^2. \tag{38}$$

Then, one easily verifies that

$$u = \frac{|a^2 - 7b^2|}{p}, \qquad v = \frac{2ab}{p} \tag{39}$$

satisfies (37). So, for example,

$$u = \tfrac{3}{11}, \quad v = \tfrac{4}{11}, \quad r = \tfrac{27}{29}, \quad s = \tfrac{4}{29}$$

is a solution of (1). And so forth.

Acknowledgment

We are pleased to acknowledge that David Rohrlich and Don Zagier read an earlier version of this paper carefully and found some minor errors.

Note added in proof

Subsequently we completely factored $A_{158} = q_{30} \cdot q_{160}$, where the smaller q-prime is $q_{30} = 933819487673994667383468877843$. As of today, March 20, 1995, $n = 168$ has not been completed and we do not know if it gives solutions for (1). Don Zagier suggested that we might have better luck by going on to $200 < n \leq 300$ and specified eight candidates there. We were not optimistic: by (35), the number of "good" n in this interval is $c \log 3/2$, and though we do not know c, if it is anywhere near that in (24), the prospects were not good. And if there is a good n there, it would probably be impossible to factor both its A_n and B_n.

Nonetheless, we examined Zagier's candidates and eliminated them all:

q	(mod 56)	
18851295617977331	(19)	$\mid A_{210}$
3213542430409	(17)	$\mid B_{224}$
934465333248316483	(19)	$\mid A_{228}$
1183409	(17)	$\mid B_{243}$

q	(mod 56)	
25521018227	(19)	$\mid A_{270}$
6731903	(31)	$\mid B_{278}$
1907810341	(45)	$\mid A_{284}$
18421914172890751771	(3)	$\mid A_{299}$

We verified that all other n in $200 < n \leq 300$ are easily eliminated so the only candidate ≤ 300 remains 168.

The 48 new solutions, computed explicitly by QUPAPR, are available from us by e-mail. They had also been computed independently by John P. Robertson.

Appendix: Factorization of A_n and B_n for $1 \leq n \leq 35$

$A_1 = 3 \cdot 5$

$B_1 = 17$

$A_2 = 239$

$B_2 = 271$

$A_3 = 13 \cdot 293$

$B_3 = 7 \cdot 617$

$A_4 = 3 \cdot 3 \cdot 5 \cdot 19 \cdot 71$

$B_4 = 17 \cdot 4049$

$A_5 = 419 \cdot 2309$

$B_5 = 1097009$

$A_6 = 131 \cdot 117701$

$B_6 = 17483311$

$A_7 = 3 \cdot 5 \cdot 5 \cdot 239 \cdot 13709$

$B_7 = 17 \cdot 31 \cdot 271 \cdot 1951$

$A_8 = 101 \cdot 38775469$

$B_8 = 4440692161$

$A_9 = 911 \cdot 68513089$

$B_9 = 70772438609$

$A_{10} = 3 \cdot 5 \cdot 13 \cdot 293 \cdot 17410177$

$B_{10} = 7 \cdot 17 \cdot 41 \cdot 617 \cdot 374681$

$A_{11} = 139 \cdot 323471 \cdot 352589$

$B_{11} = 47 \cdot 1289 \cdot 3313 \cdot 89561$

$A_{12} = 239 \cdot 56599 \cdot 18677801$

$B_{12} = 271 \cdot 4751 \cdot 222510401$

$A_{13} = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 19 \cdot 71 \cdot 22110582149$

$B_{13} = 17 \cdot 4049 \cdot 159839 \cdot 414991$

$A_{14} = 59 \cdot 2957 \cdot 367837541873$

$B_{14} = 2765207 \cdot 26315036393$

$A_{15} = 61 \cdot 7193 \cdot 2330950146013$

$B_{15} = 109182559 \cdot 10621646561$

$A_{16} = 3 \cdot 5 \cdot 419 \cdot 2309 \cdot 7919 \cdot 9769 \cdot 14519$

$B_{16} = 17 \cdot 263 \cdot 1097009 \cdot 3768285047$

$A_{17} = 13 \cdot 239 \cdot 293 \cdot 349 \cdot 817646467189$

$B_{17} = 7 \cdot 271 \cdot 617 \cdot 4129 \cdot 60950142049$

$A_{18} = 4140124084452621921391$

$B_{18} = 73 \cdot 285937 \cdot 224901512375431$

$A_{19} = 3 \cdot 5 \cdot 131 \cdot 859 \cdot 1637 \cdot 117701 \cdot 202881431$

$B_{19} = 17 \cdot 12791 \cdot 17483311 \cdot 19679858951$

$A_{20} = 83 \cdot 609997 \cdot 20769906956429479$

$B_{20} = 2297 \cdot 4782487 \cdot 108541991056319$

$A_{21} = 1979 \cdot 11437 \cdot 19609 \cdot 37760737958617$

$B_{21} = 1031 \cdot 5591 \cdot 3296688492423667409$

$A_{22} = 3 \cdot 3 \cdot 5 \cdot 5 \cdot 19 \cdot 71 \cdot 239 \cdot 13709 \cdot 268577224977601$

$B_{22} = 17 \cdot 31 \cdot 89 \cdot 271 \cdot 1951 \cdot 4049 \cdot 3016231028009$

$A_{23} = 283 \cdot 90523 \cdot 166163429041348698409$

$B_{23} = 751 \cdot 6427071295434060531533489$

$A_{24} = 13 \cdot 293 \cdot 1781079642040270801735 6769$

$B_{24} = 7 \cdot 7 \cdot 97 \cdot 617 \cdot 5838449 \cdot 4492789568611609$

$A_{25} = 3 \cdot 5 \cdot 101 \cdot 2447 \cdot 5303 \cdot 38775469 \cdot 1418347070473$

$B_{25} = 17 \cdot 17 \cdot 103 \cdot 5885911 \cdot 1575725681 \cdot 4440692161$

$A_{26} = 172314290896246141666470862182959$

$B_{26} = 1953860404516750611809786951 1631$

$A_{27} = 239 \cdot 419 \cdot 2309 \cdot 331319 \cdot 3395921 \cdot 1055589380119$

$B_{27} = 271 \cdot 1759 \cdot 819391 \cdot 1097009 \cdot 726725691727969$

$A_{28} = 3 \cdot 5 \cdot 797 \cdot 911 \cdot 68513089 \cdot 1544192927 \cdot 3798439531$

$B_{28} = 17 \cdot 457 \cdot 6841 \cdot 244303 \cdot 5400610351 \cdot 70772438609$

$A_{29} = 23599 \cdot 7701979 \cdot 383765424374738665389331$

$B_{29} = 1491991 \cdot 530112208103852649882477284 39$

$A_{30} = 31721 \cdot 350451882355835690304687365878 31$

$B_{30} = 174703 \cdot 242495520767 \cdot 29753867037674612351$

$A_{31} = 3 \cdot 3 \cdot 5 \cdot 13 \cdot 19 \cdot 71 \cdot 293 \cdot 1429849 \cdot 17410177 \cdot 3077938662617449$

$B_{31} = 7 \cdot 17 \cdot 41 \cdot 617 \cdot 2017 \cdot 4049 \cdot 374681 \cdot 2180869437222901153$

$A_{32} = 131 \cdot 239 \cdot 117701 \cdot 766218974495773238168467939 21$

$B_{32} = 271 \cdot 17483311 \cdot 325944191 \cdot 207318599897029599551$

$$A_{33} = 1607 \cdot 243402458839 \cdot 1150468961626556575073758 3$$

$$B_{33} = 407359 \cdot 45590256356873 \cdot 274750586941086808567$$

$$A_{34} = 3 \cdot 5 \cdot 139 \cdot 323471 \cdot 352589 \cdot 3590347 \cdot 84000649255208196451$$

$$B_{34} = 17 \cdot 47 \cdot 1289 \cdot 3313 \cdot 89561 \cdot 655223 \cdot 7840089809 \cdot 51802561303$$

$$A_{35} = 69206257 \cdot 16515714544563093108617538971911153$$

$$B_{35} = 569 \cdot 12497 \cdot 14767 \cdot 2313398660689 \cdot 5335242610482412601$$

BIBLIOGRAPHY

1. Martin Davis, *One equation to rule them all*, Trans. New York Acad. Sci. (II) **30** (1968), 766–773.
2. Oskar Herrmann, *A non-trivial solution of the diophantine equation* $9(x^2 + 7y^2)^2 - 7(u^2+7v^2)^2 = 2$, Computers in Number Theory, Academic Press, London, 1971, pp. 207–212.
3. Daniel Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics, University of Manitoba, Winnipeg, 1972, pp. 51–70.
4. Yuri Matiyasevich, *Hilbert's Tenth Problem*, M. I. T. Press, Cambridge, Mass., 1993.
5. Daniel Shanks, *Euclid's primes*, Bull. Inst. Combin. Appl. **1** (1991), 33–36.
6. Samuel S. Wagstaff, Jr., *Computing Euclid's primes*, Bull. Inst. Combin. Appl. **8** (1993), 23–32.
7. Daniel Shanks and Larry P. Schmid, *Variations on a theorem of Landau, Part* I, Math. Comp. **20** (1966), 551–569.
8. Daniel Shanks, *Solved and unsolved problems in number theory, 4th ed.*, Chelsea, New York, 1993.
9. B. Dixon and A. K. Lenstra, *Factoring integers using SIMD sieves*, Advances in Cryptology, Eurocrypt '93, Lecture Notes in Comput. Sci., vol. 765, Springer-Verlag, Berlin, 1994, pp. 28–39.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MARYLAND 20742

E-mail address: dns@math.umd.edu

DEPARTMENT OF COMPUTER SCIENCES, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907

E-mail address: ssw@cs.purdue.edu