JOURNAL OF NUMBER THEORY 17, 144–164 (1983)

On the Diophantine Equation $y^2 - D = 2^k$

NICHOLAS TZANAKIS

8 Solomou Street, Iraklion, Crete, Greece

Communicated by D. J. Lewis

Received May 18, 1981

The equation of the title is studied for $1 \leqslant D \leqslant 100$. It is shown that for such values of D the above equation is really interesting only if $D = 17, 41, 73, 89, 97$. Then, for these values of D, (i) necessary conditions are given for the solvability of the diophantine equations $y^2 = 2x^4 + D$ and $y^2 = 8x^4 + D$, and (ii) $y^2 - D = 2^k$ is solved.

In this paper we deal with the diphantine equation

$$y^2 - D = 2^k \tag{1}$$

where D is a positive integer $\leqslant 100$. The diophantine equation

$$y^2 + A = p^k, \tag{2}$$

where A is an integer and p is a prime, has attracted the interest of many authors since 1913, when Ramanujan proposed his well-known problem on $x^2 + 7 = 2^k$. For the history of (2) as well as for references see [1].

When A is positive, (2) is not very difficult, because, on factorizing both sides in the field $\mathbf{Q}[(-A)^{1/2}]$, there is no problem with the units. When, however, A is negative, as in (1), another unknown exponent appears besides k: The exponent of the unit in the right-hand side and a usual method such as the p-adic method, which is used directly when $A > 0$, cannot now be used, because it leads to an equation with two unknowns. Therefore a different method must be applied.

Our method is that of Cohn [2], as presented in [3], somewhat modified. The essential idea is to relate the solutions to values of a second order linear recurrence relation and, by examining the recurrence modulo various moduli, eliminate or bound the values of certain of the variables in the equation.

Among the values of D the only ones for which (1) is really interesting are $D = 17, 41, 73, 97, 89$, as we show in Section A. In Section B we make some preliminary remarks and in Sections C–G we give the complete

0022-314X/83 $3.00

solution of (1) for the above values of D, respectively (see the corollaries of the respective paragraphs).

It is worth noticing that in an unpublished work we applied succesfully the same method as that used in this paper to the diophantine equation

$$y^2 = 4 \cdot 3^k + 13$$

which arises from coding theory (see [4, 5]; its only solutions with $y > 0$ are $(k, y) = (1, 5), (2. 7), (3, 11)$).

A. Let D Be Even

Then, as it is easily verified, (1) leads to either a trivially soluble equation or to an equation of the same type with an odd and lesser value for D.

Suppose now that D is odd. If $D \equiv -1, \pm 3 \pmod 8$, then (1) is uninteresting. Indeed, for such values of D, k cannot be greater than 2, as it is seen if we consider (1) as a congruence mod 8.

Therefore only the case $D \equiv 1 \pmod 8$ remains. The values of D between 1 and 100, which are $\equiv 1 \pmod 8$ are 1, 9, 17, 25, 33, 41, 49, 57, 65, 73, 81, 89, 97.

If $D = 1, 9, 25, 49, 81$, the left-hand side of (1) factorizes in $\mathbf{Z}$ and our equation is trivially soluble. If $D = 33, 57$, then, by (1), $y^2 \equiv 2^k \pmod 3$, so that k must be even, $y^2 - 2^k = D$ and since the left-hand side factorizes in $\mathbf{Z}$, our equation is trivially soluble. If $D = 65$, then, by (1), $y^2 \equiv 2^k \pmod 5$ and k must be even. As before, no difficulty with (1).

Thus we conclude that the only interesting values of D between 1 and 100 in (1) are $D = 17, 41, 73, 89, 97$.

In what follows we give the complete solution of

$$y^2 - 2^k = p, \tag{3}$$

where $k \geqslant 1$ and p is one of the primes 17, 41, 73, 89, 97.

B. Some Preliminary Remarks

If $k = 4m + 1$, $m \geqslant 0$, set $x = 2^m$, $c = 1$ and if $k = 4m + 3$, $m \geqslant 0$, set $x = 2^m$, $c = 2$. Then (3) becomes

$$y^2 - 2c^2x^4 = p. \tag{4}$$

Equation (4) is interesting in itself and we study it in its general form in

which x need not be of the form 2^m (although c always takes the value 1 or 2). The left-hand side factorizes in $\mathbf{Q}(\theta)$, where $\theta = 2^{1/2}$.

The class number in this field is 1 and the fundamental unit is $\varepsilon = 1 + \theta$.

If we set $\tilde{\varepsilon} = 1 - \theta$, then $\varepsilon\tilde{\varepsilon} = -1$, $\varepsilon + \tilde{\varepsilon} = 2$, $\varepsilon - \tilde{\varepsilon} = 2\theta$. On the other hand, p has two different prime divisors in $\mathbf{Q}(\theta)$, namely $(a + b\theta)$ and $(a - b\theta)$, where a and b are any integers such that $\text{Norm}(a + b\theta) = p$ $(a^2 - 2b^2 = p \equiv 1 \pmod 8$, from which a is odd and b is even). Therefore, from (4), we easily deduce that

$$\begin{aligned} y + cx^2\theta &= \pm\varepsilon^r(a + b\theta) \quad \text{or} \\ &= \pm\varepsilon^r(a - b\theta), \end{aligned} \tag{5}$$

where r is an integer. The following gives values of a and b for each value of p:

p	17	41	73	89	97
a	5	7	9	11	15
b	2	2	2	4	8.

Now put

$$u_n = \frac{\varepsilon^n - \tilde{\varepsilon}^n}{\varepsilon - \tilde{\varepsilon}}.$$

Then,

$$u_0 = 0, \qquad u_1 = 1, \qquad u_{n+2} = 2u_{n+1} + u_n, \qquad u_{-n} = (-1)^{n+1} u_n. \tag{6}$$

The first case of (5) gives $\eta(y + cx^2\theta) = \varepsilon^r(a + b\theta)$ and $\eta(y - cx^2\theta) = \tilde{\varepsilon}^r(a - b\theta)$, $\eta = \pm 1$, from which

$$\begin{aligned} \pm cx^2(\varepsilon - \tilde{\varepsilon}) &= a(\varepsilon^r + \tilde{\varepsilon}^r) + \frac{b}{2}(\varepsilon - \tilde{\varepsilon})(\varepsilon^r + \tilde{\varepsilon}^r) \\ &= \frac{a}{2}(\varepsilon + \tilde{\varepsilon})(\varepsilon^r - \tilde{\varepsilon}^r) + \frac{b}{2}(\varepsilon - \tilde{\varepsilon})(\varepsilon^r + \tilde{\varepsilon}^r). \end{aligned}$$

Then,

$$\begin{aligned} \pm 2cx^2(\varepsilon - \tilde{\varepsilon}) &= (a + b)(\varepsilon^{r+1} - \tilde{\varepsilon}^{r+1}) + (a - b)\,\varepsilon\tilde{\varepsilon}(\varepsilon^{r-1} - \tilde{\varepsilon}^{r-1}) \\ &= (a + b)(\varepsilon^{r+1} - \tilde{\varepsilon}^{r+1}) - (a - b)(\varepsilon^{r-1} - \tilde{\varepsilon}^{r-1}). \end{aligned}$$

Dividing by $\varepsilon - \tilde{\varepsilon}$ we find

$$\pm 2cx^2 = (a + b)\,u_{r+1} - (a - b)\,u_{r-1}. \tag{7}$$

The second case of (5) gives in an analogous way

$$\pm 2cx^2 = (a-b)\,u_{r+1} - (a+b)\,u_{r-1}. \tag{7'}$$

Now let us write in general

$$w_n = (a+b)\,u_{n+1} - (a-b)\,u_{n-1} \tag{8}$$

$$z_n = (a-b)\,u_{n+1} - (a+b)\,u_{n-1}. \tag{8'}$$

In view of (6) we have

$$w_0 = 2b, \quad w_1 = 2(a+b), \quad w_{n+2} = 2w_{n+1} + w_n, \quad w_{-n} = (-1)^{n+1} z_n, \tag{9}$$

$$z_0 = -2b, \quad z_1 = 2(a-b), \quad z_{n+2} = 2z_{n+1} + z_n, \quad z_{-n} = (-1)^{n+1} w_n. \tag{9'}$$

Note that w_0, w_1 and z_1, z_2 are positive. Therefore, by induction, $w_n > 0$ for every $n \geqslant 0$ and $z_n > 0$ for every $n \geqslant 1$.

Now, by (7) and (7') and in view of the above notations, we have

$$2cx^2 = \pm w_r \qquad \text{or} \qquad 2cx^2 = \pm z_r.$$

However, it suffices to take only the upper sign. Indeed, consider the relation $2cx^2 = -w_r$. Then $r < 0$, since otherwise $-w_r < 0$. Put $r = -s$, $s > 0$. Then, $2cx^2 = -w_{-s} = -(-1)^{s+1} z_s = (-1)^s z_s$. Since $z_s > 0$, s must be even and $2cx^2 = z_s$.

Now consider the relation $2cx^2 = -z_r$. Then, $r \leqslant 0$, since otherwise $-z_r < 0$. Put $r = -s$, $s \geqslant 0$. Then, $2cx^2 = -z_r = -z_{-s} = -(-1)^{s+1} w_s = (-1)^s w_s$. Since $w_s > 0$, s must be even and $2cx^2 = w_s$. Thus (4) leads to either of the following equations:

$$2cx^2 = w_r. \tag{10}$$

$$2cx^2 = z_r. \tag{10'}$$

Now we prove two useful relations. An easy calculation shows that

$$(-1)^m (\varepsilon^{n+2m} - \tilde{\varepsilon}^{n+2m}) = \varepsilon^n - \tilde{\varepsilon}^n + (-1)^m (\varepsilon^{n+m} + \tilde{\varepsilon}^{n+m})(\varepsilon^m - \tilde{\varepsilon}^m).$$

Then, dividing by $\varepsilon - \tilde{\varepsilon}$, we have

$$(-1)^m u_{n+2m} = u_n + (-1)^m (\varepsilon^{n+m} + \tilde{\varepsilon}^{n+m})\, u_m,$$

where, clearly, $(-1)^m (\varepsilon^{n+m} + \tilde{\varepsilon}^{n+m})$ is a rational integer. Thus,

$$u_{n+2m} \equiv (-1)^m u_n \pmod{u_m}.$$

We can now easily prove by induction the relation

$$u_{n+2mt} \equiv (-1)^{mt} u_n \pmod{u_m}$$

and using the recursive formulae (8) and (8′), we find the useful congruences

$$w_{n+2mt} \equiv (-1)^{mt} w_n \pmod{u_m}. \tag{11}$$

$$z_{n+2mt} \equiv (-1)^{mt} z_n \pmod{u_m}. \tag{11′}$$

Now we are ready to examine each case of (4) (and consequently of (3)) separately.

C. Let $p = 17$

By (9) and (9′),

$$\begin{aligned} w_0 &= 4, \qquad w_1 = 14, \qquad w_{n+2} = 2w_{n+1} + w_n; \\ z_0 &= -4, \qquad z_1 = 6, \qquad z_{n+2} = 2z_{n+1} + z_n. \end{aligned} \tag{12}$$

First consider (10). If $c = 2$, then

$$(2x)^2 = w_r \tag{13}$$

and for x even we have $w_r \equiv 0 \pmod{16}$. From (12), by taking residues mod 16, we find a periodic sequence of order 8 given by

$n \equiv$	0	1	2	3	4	5	6	7	mod 8,
$w_n \equiv$	4	−2	0	−2	−4	6	8	6	mod 16,

and by taking residues mod 3, we find a periodic sequence of order 8, given by

$n \equiv$	0	1	2	3	4	5	6	7	mod 8,
$w_n \equiv$	1	−1	−1	0	−1	1	1	0	mod 3.

In view of these tables,

$$w_r \equiv 0 \pmod{16} \to r \equiv 2 \pmod{8} \to w_r \equiv -1 \pmod{3}.$$

Thus (13) is impossible if x is even. If $c = 1$, then (10) becomes

$$2x^2 = w_r \tag{14}$$

and for $x \equiv 0 \pmod{8}$ we must have $w_r \equiv 0 \pmod{128}$. Table I, which has

TABLE I

The Residues mod 128 of the w_n's and z_n's
Form a Periodic Sequence of Order 64

n	w_n	z_n	n	w_n	z_n
mod 64	mod 128	mod 128	mod 64	mod 128	mod 128
0	4	−4	33	−50	−58
1	14	6	34	−32	−56
2	32	8	35	14	−42
3	−50	22	36	−4	−12
4	60	52	37	6	62
5	−58	−2	38	8	−16
6	−56	48	39	22	30
7	−42	−34	40	52	44
8	−12	−20	41	−2	−10
9	62	54	42	48	24
10	−16	−40	43	−34	38
11	30	−26	44	−20	−28
12	44	36	45	54	−18
13	−10	46	46	−40	64
14	24	0	47	−26	−18
15	38	46	48	36	28
16	−28	−36	49	46	38
17	−18	−26	50	0	−24
18	64	40	51	46	−10
19	−18	54	52	−36	−44
20	28	20	53	−26	30
21	38	−34	54	40	16
22	−24	−48	55	54	62
23	−10	−2	56	20	12
24	−44	−52	57	−34	−42
25	30	22	58	−48	56
26	16	−8	59	−2	−58
27	62	6	60	−52	−60
28	12	4	61	22	−50
29	−42	14	62	−8	−32
30	56	32	63	6	14
31	−58	−50			
32	−60	60			

been constructed with the aid of (9) and (9′), shows that by taking residues mod 128 of the w_n's (as well as of the z_n's) we find a periodic sequence of order 64.

We now note that

$$u_{32} = \frac{\varepsilon^{32} - \tilde{\varepsilon}^{32}}{\varepsilon - \tilde{\varepsilon}} = \frac{\varepsilon^{16} - \tilde{\varepsilon}^{16}}{\varepsilon - \tilde{\varepsilon}} (\varepsilon^{16} + \tilde{\varepsilon}^{16}) = u_{16}(\varepsilon^{16} + \tilde{\varepsilon}^{16}).$$

Since $\varepsilon^{16} = (1+\theta)^{16} = 665857 + 470832\theta$, we have $u_{32} \equiv 0 \pmod{665857}$. In Table II, which has been constructed with the aid of (9) and (9′), we find the residues mod 665857 of some of the w_n's $(1 \leqslant n \leqslant 50)$ and of the z_n's $(1 \leqslant n \leqslant 14)$. (We need only the residues of w_{50} and z_{14}; in fact, the residues of the w_n's and z_n's form a periodic sequence of order 64, but we do not need this here.)

Now, in view of Tables I and II and relation (11), we have

$$w_r \equiv 0 \pmod{128} \to r \equiv 50 \pmod{64} \to w_r \equiv w_{50} \pmod{u_{32}}$$
$$\to w_r \equiv w_{50} \pmod{665857}$$

and

$$(2x)^2 = 2w_r \equiv 2w_{50} \equiv 2 \cdot 315009 = 9^2 \cdot 2 \cdot 3889 \pmod{665857}.$$

TABLE II

	w_n	z_n		w_n
n	mod 665857	mod 665857	n	mod 665857
1	14	6	26	304
2	32	8	27	−126
3	78	22	28	52
4	188	52	29	−22
5	454	126	30	8
6	1096	304	31	−6
7	2646	734	32	−4
8	6388	1772	33	−14
9	15422	4278	34	−32
10	37232	10328	35	−78
11	89886	24934	36	−188
12	217004	60196	37	−454
13	−141963	145326	38	−1096
14	−66922	−315009	39	−2646
15	−275807		40	−6388
16	47321		41	−15422
17	−181165		42	−37232
18	−315009		43	−89886
19	−145326		44	−217004
20	60196		45	141963
21	−24934		46	66922
22	10328		47	275807
23	−4278		48	−47321
24	1772		49	181165
25	−734		50	315009

However, a simple calculation shows that $(\frac{2 \cdot 3889}{665857}) = -1$, so that the last congruence is impossible. Thus (14) is impossible if $x \equiv 0 \pmod 8$.

Next consider (10′). If $c = 1$, then

$$2x^2 = z_r \tag{14′}$$

and for $x \equiv 0 \pmod 4$, we have $z_r \equiv 0 \pmod{16}$. By taking residues mod 16 we find a periodic sequence of order 8:

$$\begin{array}{lcccccccccc} n \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \mod 8, \\ z_n \equiv & -4 & 6 & 8 & 6 & 4 & -2 & 0 & -2 & \mod 16. \end{array}$$

By taking residues mod 3 we find a periodic sequence of order 8

$$\begin{array}{lcccccccccc} n \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \mod 8, \\ z_n \equiv & -1 & 0 & -1 & 1 & 1 & 0 & 1 & -1 & \mod 3. \end{array}$$

Therefore, $z_r \equiv 0 \pmod{16} \to r \equiv 6 \pmod 8 \to z_r \equiv 1 \pmod 3$ and (14′) is thus impossible if x is $\equiv 0 \pmod 4$.

If $c = 2$, then

$$(2x)^2 = z_r \tag{13′}$$

and for $x \equiv 0 \pmod 8$ we must have $z_r \equiv 0 \pmod{128}$. Using Tables I and II and relation (11′) we have,

$$\begin{aligned} z_r \equiv 0 \pmod{128} &\to r \equiv 14 \pmod{64} \to z_r \equiv z_{14} \pmod{u_{32}} \\ &\to z_r \equiv z_{14} \pmod{665857} \end{aligned}$$

and $(2x)^2 = z_r \equiv z_{14} \equiv -315009 = -9^2 \cdot 3889 \pmod{665857}$, which is impossible, since a simple calculation shows that $(\frac{-3889}{665857}) = -1$. Therefore (13′) is impossible if $x \equiv 0 \pmod 8$.

In this paragraph we have thus proved the following:

THEOREM. *The diophantine equations*

$$y^2 - 2x^4 = 17, \qquad y^2 - 8x^4 = 17$$

are impossible if $x \equiv 0 \pmod 8$.

COROLLARY. *The only solutions to the diophantine equation*

$$y^2 - 17 = 2^k$$

with $y > 0$ *are given by* $(k, y) = (3, 5), (5, 7), (6, 9), (9, 23)$.

Proof. If k is even, then $(y+2^{k/2})(y-2^{k/2})=17$, from which $y+2^{k/2}=17$ and $y-2^{k/2}=1$. These equations give $y=9$ and $k=3$. If k is odd, then as we have seen in Section B, $y^2-17=2^k$ is equivalent to either $y^2-2x^4=17$ or $y^2-8x^4=17$, where $x=2^m$ and $k=4m+1$ in the first case, while $k=4m+3$ in the second case.

In view of the theorem, $m\leqslant 2$, therefore $k\leqslant 11$ and the only odd values of k which are $\leqslant 11$ and such that 2^k+17 is a perfect square are $k=3, 5, 9$ with corresponding $y=5, 7, 23$, as was to be proved.

D. Let $p=41$

By (9) and (9′),

$$w_0=4, \qquad w_1=18, \qquad w_{n+2}=2w_{n+1}+w_n;$$
$$z_0=-4, \qquad z_1=10, \qquad z_{n+2}=2z_{n+1}+z_n.$$

First consider (10). If $c=2$, then

$$(2x)^2=w_r, \tag{15}$$

and for x even we must have $w_r\equiv 0 \pmod{16}$. On taking residues mod 16 and mod 3, respectively, we get a periodic sequence of order 8 as follows:

$n\equiv$	0	1	2	3	4	5	6	7	mod 8,
$w_n\equiv$	4	2	8	2	−4	−6	0	−6	mod 16,
$w_n\equiv$	1	0	1	−1	−1	0	−1	1	mod 3.

As is seen from the above, $w_r\equiv 0 \pmod{16}\rightarrow r\equiv 6 \pmod 8\rightarrow w_r\equiv -1 \pmod 3$ and (15) is therefore impossible if x is even.

If $c=1$, then (10) becomes

$$2x^2=w_r \tag{16}$$

and for $x\equiv 0 \pmod 8$ we must have $w_r\equiv 0 \pmod{64}$. On taking residues mod 64 we find a periodic sequence of order 32 as shown in Table III. From this table we see that $w_r\equiv 0 \pmod{64}\rightarrow r\equiv 22 \pmod{32}$ and then, in view of (11), $w_r\equiv w_{22} \pmod{u_{16}}$. Now, as we can easily see, $u_{16}\equiv 0 \pmod{577}$, and also making use of Table IV, we have

$$2x^2=w_r\equiv w_{22}\equiv -222 \pmod{577} \quad \text{or} \quad (2x)^2\equiv -4\cdot 111 \pmod{577}.$$

However, a simple calculation shows that $\left(\frac{-111}{577}\right)=-1$ and the last congruence is therefore impossible. Thus (16) is impossible if $x\equiv 0 \pmod 8$.

TABLE III

The Residues mod 64 of the w_n's and z_n's Form a Periodic Sequence of Order 32

n	w_n	z_n
mod 32	mod 64	mod 64
0	4	−4
1	18	10
2	−24	16
3	−30	−22
4	−20	−28
5	−6	−14
6	32	8
7	−6	2
8	20	12
9	−30	26
10	24	0
11	18	26
12	−4	−12
13	10	2
14	16	−8
15	−22	−14
16	−28	28
17	−14	−22
18	8	−16
19	2	10
20	12	4
21	26	18
22	0	−24
23	26	−30
24	−12	−20
25	2	−6
26	−8	32
27	−14	−6
28	28	20
29	−22	−30
30	−16	24
31	10	18

TABLE IV

n	w_n mod 577	z_n mod 577
1	18	10
2	40	16
3	98	42
4	236	100
5	−7	242
6	222	7
7	−140	256
8	−58	−58
9	−256	140
10	7	222
11	−242	
12	100	
13	−42	
14	16	
15	−10	
16	−4	
17	−18	
18	−40	
19	−98	
20	−236	
21	7	
22	−222	

Next consider (10′). If $c = 1$, then

$$2x^2 = z_r, \tag{16′}$$

and for $x \equiv 0 \pmod 4$ we must have $z_r \equiv 0 \pmod{16}$. However, in view of

$n \equiv$	0	1	2	3	4	5	6	7	mod 8,
$z_n \equiv$	−4	−6	0	−6	4	2	8	2	mod 16,
$z_n \equiv$	−1	1	1	0	1	−1	−1	0	mod 3,

we have $z_r \equiv 0 \pmod{16} \to r \equiv 2 \pmod 8 \to z_r \equiv 1 \pmod 3$. Thus (16′) is impossible if $x \equiv 0 \pmod 4$.

If $c = 2$, then (10′) becomes

$$(2x)^2 = z_r \tag{15′}$$

and for $x \equiv 0 \pmod 4$ we must have $z_r \equiv 0 \pmod{64}$. Table III shows then that $r \equiv 10 \pmod{32}$, and in view of (11'), $(2x)^2 \equiv z_r \equiv z_{10} \pmod{u_{16}}$. Since $u_{16} \equiv 0 \pmod{577}$ and $z_{10} \equiv 222 \pmod{577}$ (Table IV), we have

$$(2x)^2 \equiv 222 \pmod{577}$$

which is impossible since $(\frac{222}{577}) = -1$. Therefore (15') is impossible if $x \equiv 0 \pmod 4$.

We have thus proved the following:

THEOREM. *The diophantine equation*

$$y^2 = 2x^4 + 41$$

is imposible if $x \equiv 0 \pmod 8$, *while the diophantine equation*

$$y^2 = 8x^4 + 41$$

is impossible if $x \equiv 0 \pmod 4$.

COROLLARY. *The only solutions to the diophantine equation*

$$y^2 = 2^k + 41$$

with $y > 0$, *are given by* $(k, y) = (3, 7), (7, 13)$.

Proof. If k is even, then $(y + 2^{k/2})(y - 2^{k/2}) = 41$, which is, obviously impossible. If k is odd, then the same argument that was used in the proof of the corollary of Section C shows that $k \leqslant 11$. Now a simple calculation shows that the only admissible values for $k \leqslant 11$ are $k = 3, 7$ with, respectively $y = 7, 13$, as was to be proved.

E. LET $p = 73$.

By (9) and (9'),

$$w_0 = 4, \qquad w_1 = 22, \qquad w_{n+2} = 2w_{n+1} + w_n;$$
$$z_0 = -4, \qquad z_1 = 14, \qquad z_{n+2} = 2z_{n+1} + z_n.$$

First consider Eq. (10), $2cx^2 = w_r$. If x is even, then $w_r \equiv 0 \pmod 8$ and by taking residues of the w_n's mod 8 and mod 3, respectively, we find the following periodic sequences:

$$\begin{array}{rcccccccccl} n \equiv & 0 & 1 & 2 & 3 & & & & & & \mod 4 \\ w_n \equiv & 4 & -2 & 0 & -2 & & & & & & \mod 8 \\ n \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & & \mod 8, \\ w_n \equiv & 1 & 1 & 0 & 1 & -1 & -1 & 0 & -1 & & \mod 3. \end{array}$$

Thus, $w_r \equiv 0 \pmod 8 \to r \equiv 2 \pmod 4 \to r \equiv 2, 6 \pmod 8 \to w_r \equiv 0 \pmod 3$, which is impossible for $x \not\equiv 0 \pmod 3$.

Next consider Eq. (10′), $2cx^2 = z_r$. If x is even, then $z_r \equiv 0 \pmod 8$. As before,

$$\begin{array}{rcccccccccl} n \equiv & 0 & 1 & 2 & 3 & & & & & & \mod 4 \\ z_n \equiv & 4 & -2 & 0 & -2 & & & & & & \mod 8 \\ n \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & & \mod 8, \\ z_n \equiv & -1 & -1 & 0 & -1 & 1 & 1 & 0 & 1 & & \mod 3, \end{array}$$

which show that $z_r \equiv 0 \pmod 8 \to z_r \equiv 0 \pmod 3$, which is impossible for $x \not\equiv 0 \pmod 3$.

We have thus proved the following:

THEOREM. *The diophantine equations*

$$y^2 = 2x^4 + 73, \qquad y^2 = 8x^4 + 73$$

are impossible if x is even and $\not\equiv 0 \pmod 3$.

COROLLARY. *The only solution to the diophantine equation*

$$y^2 = 2^k + 73$$

with positive y is given by $(k, y) = (3, 9)$.

Proof. Our equation is trivially impossible if k is even. When k is odd we apply the argument used in the proof of the corollary of Section C and we find that $k = 1$ or 3. Only the second value is admissible, which was to be proved.

F. LET $p = 97$

By (9) and (9′),

$$w_0 = 16, \qquad w_1 = 46, \qquad w_{n+2} = 2w_{n+1} + w_n;$$
$$z_0 = -16, \qquad z_1 = 14, \qquad z_{n+2} = 2z_{n+1} + z_n.$$

First consider (10). If $c = 1$, then

$$2x^2 = w_r, \tag{17}$$

and for $x \equiv 0 \pmod 4$ we must have $w_r \equiv 0 \pmod{16}$. Then in view of

$$\begin{array}{lllllllll} n \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \bmod 8, \\ w_n \equiv & 0 & -2 & -4 & 6 & 8 & 6 & 4 & -2 & \bmod 16, \\ w_n \equiv & 1 & 1 & 0 & 1 & -1 & -1 & 0 & -1 & \bmod 3, \end{array}$$

we have $w_r \equiv 0 \pmod{16} \to r \equiv 0 \pmod 8 \to w_r \equiv 1 \pmod 3$ and (17) is therefore impossible if $x \equiv 0 \pmod 4$.

If $c = 2$ then (10) becomes

$$(2x)^2 = w_r, \tag{18}$$

and for $x \equiv 0 \pmod 4$ we must have $w_r \equiv 0 \pmod{64}$ and then Table V shows that $r \equiv 24 \pmod{32}$. Now, in view of (11), $w_r \equiv w_{24} \pmod{u_{16}}$, while $u_{16} \equiv 0 \pmod{577}$. Thus, also making use of Table VI, we have

$$(2x)^2 = w_r \equiv w_{24} \equiv -123 \pmod{577}.$$

This congruence, however, is impossible, since $(\frac{-123}{577}) = -1$. Thus (18) is impossible if $x \equiv 0 \pmod 4$.

Next consider (10′). If $c = 2$, then

$$(2x)^2 = z_r, \tag{18′}$$

and for x even we must have $z_r \equiv 0 \pmod{16}$. However,

$$\begin{array}{lllllllll} n \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \bmod 8, \\ z_n \equiv & 0 & -2 & -4 & 6 & 8 & 6 & 4 & -2 & \bmod 16, \\ z_n \equiv & -1 & -1 & 0 & -1 & 1 & 1 & 0 & 1 & \bmod 3, \end{array}$$

show that $z_r \equiv 0 \pmod{16} \to r \equiv 0 \pmod 8 \to z_r \equiv -1 \pmod 3$, and (18′) is thus impossible if x is even.

If $c = 1$, then (10′) becomes

$$2x^2 = z_r, \tag{17′}$$

and for $x \equiv 0 \pmod 8$ we must have $z_r \equiv 0 \pmod{64}$. Then (Table V) $r \equiv 8$

TABLE V

The Residues mod 64 of the w_n's and z_n's Form a Periodic Sequence of Order 32

n	w_n	z_n
mod 32	mod 64	mod 64
0	16	−16
1	−18	14
2	−20	12
3	6	−26
4	−8	24
5	−10	22
6	−28	4
7	−2	30
8	32	0
9	−2	30
10	28	−4
11	−10	22
12	8	−24
13	6	−26
14	20	−12
15	−18	14
16	−16	16
17	14	−18
18	12	−20
19	−26	6
20	24	−8
21	22	−10
22	4	−28
23	30	−2
24	0	32
25	30	−2
26	−4	28
27	22	−10
28	−24	8
29	−26	6
30	−12	20
31	14	−18

(mod 32), and by (11′) $z_r \equiv z_8 \pmod{u_{16}}$. Since $u_{16} \equiv 0 \pmod{577}$ and $z_8 \equiv 123 \pmod{577}$ (Table VI), we have

$$(2x)^2 = 2z_r \equiv 2z_8 \equiv 2 \cdot 123 \pmod{577}.$$

This congruence is impossible, since $(2 \cdot 123/577) = -1$. Therefore (17′) is also impossible if $x \equiv 0 \pmod 8$.

TABLE VI

	w_n	z_n
n	mod 577	mod 577
1	46	14
2	108	12
3	262	38
4	55	88
5	−205	214
6	222	−61
7	239	92
8	123	123
9	−92	
10	−61	
11	−214	
12	88	
13	−38	
14	12	
15	−14	
16	−16	
17	−46	
18	−108	
19	−262	
20	−55	
21	205	
22	−222	
23	−239	
24	−123	

We have thus proved the following:

THEOREM. *The diophantine equation*

$$y^2 = 2x^4 + 97$$

is impossible if $x \equiv 0 \pmod 8$, *while the diophantine equation*

$$y^2 = 8x^4 + 97$$

is impossible if $x \equiv 0 \pmod 4$.

COROLLARY. *The only solution to the diophantine equation*

$$y^2 = 2^k + 97$$

with positive y *is given by* $(k, y) = (7, 15)$.

Proof. The proof is the same as those of the corollaries of the preceding sections.

G. Let $p = 89$

In this case the method which we applied in the preceding sections cannot be easily applied. The relations

$$2x^2 = w_r, \qquad (2x)^2 = z_r,$$

are impossible if $x \equiv 0 \pmod 4$ and $x \equiv 0 \pmod 2$, respectively. This can be proved as usual by taking the residues mod 16 and mod 3 of the w_n's and z_n's.

The relation

$$(2x)^2 = w_r$$

is impossible if $x \not\equiv 0 \pmod 5$. We prove this by taking the residues mod 5 of the w_n's. Now the relation

$$2x^2 = z_r \tag{19}$$

remains. If $x \equiv 0 \pmod{16}$, then $z_r \equiv 0 \pmod{512}$. Table VII shows the residues mod 512 of the z_n's (they form a periodic sequence of order 256). The table shows that $z_r \equiv 0 \pmod{512} \to r \equiv 196 \pmod{256}$, and in view of (11′),

$$z_r \equiv z_{196} \pmod{u_{128}}.$$

Then, we find (cf. Section C) that

$$u_{128} \equiv 0 \pmod{157258404803291863353217}$$

and we work mod 1572.... Table VIII shows the residues mod 1572... of the u_n's and we find

$$\begin{aligned} z_{196} &= 7u_{197} - 15u_{195} \equiv 7u_{59} - 15u_{61} \\ &\equiv -1090483523462416035524608 \pmod{1572...}. \end{aligned}$$

Then we have

$$(2x)^2 = 2z_r \equiv 2z_{196} \equiv -2 \cdot 1090... \pmod{1572...}. \tag{20}$$

A computation showed that

$$\left(\frac{-2.1090...}{1572...}\right) = 1$$

so that (19) is not, a priori, impossible.

TABLE VII

The Residues mod 512 of the z_n's Form a Periodic Sequence of Order 256

n	z_n	n	z_n	n	z_n	n	z_n	n	z_n
mod 256	mod 512	mod 256	mod 512	mod 256	mod 512	mod 256	mod 512	mod 256	mod 512
1	14	55	−82	109	−122	163	246	217	−66
2	20	56	−152	110	92	164	−64	218	36
3	54	57	126	111	62	165	118	219	6
4	128	58	100	112	216	166	172	220	48
5	−202	59	−186	113	−18	167	−50	221	102
6	236	60	240	114	180	168	72	222	252
7	−242	61	−218	115	−170	169	94	223	94
8	−248	62	−196	116	−160	170	−252	224	−72
9	−226	63	−98	117	22	171	102	225	−50
10	−188	64	120	118	−116	172	−48	226	−172
11	−90	65	142	119	−210	173	6	227	118
12	144	66	−108	120	−24	174	−36	228	64
13	198	67	−74	121	254	175	−66	229	246
14	28	68	256	122	−28	176	−168	230	44
15	254	69	−74	123	198	177	110	231	−178
16	24	70	108	124	−144	178	52	232	200
17	−210	71	142	125	−90	179	214	233	222
18	116	72	−120	126	188	180	−32	234	132
19	22	73	−98	127	−226	181	150	235	−26
20	160	74	196	128	248	182	−244	236	80
21	−170	75	−218	129	−242	183	174	237	134
22	−180	76	−240	130	−236	184	104	238	−164
23	−18	77	−186	131	−202	185	−130	239	−194
24	−216	78	−100	132	−128	186	−156	240	−40
25	62	79	126	133	54	187	70	241	238
26	−92	80	152	134	−20	188	−16	242	−76
27	−122	81	−82	135	14	189	38	243	86
28	176	82	−12	136	8	190	60	244	96
29	230	83	−106	137	30	191	158	245	−234
30	124	84	−224	138	68	192	−136	246	140
31	−34	85	−42	139	166	193	−114	247	46
32	56	86	204	140	−112	194	148	248	232
33	78	87	−146	141	−58	195	182	249	−2
34	212	88	−88	142	−228	196	0	250	228
35	−10	89	190	143	−2	197	182	251	−58
36	192	90	−220	144	−232	198	−148	252	112
37	−138	91	−250	145	46	199	−114	253	166
38	−84	92	−208	146	−140	200	136	254	−68
39	206	93	−154	147	−234	201	158	255	30
40	−184	94	−4	148	−96	202	−60	0	−8
41	−162	95	−162	149	86	203	38		
42	4	96	184	150	76	204	16		
43	−154	97	206	151	238	205	70		
44	208	98	84	152	40	206	156		
45	−250	99	−138	153	−194	207	−130		
46	220	100	−192	154	164	208	−104		
47	190	101	−10	155	134	209	174		
48	88	102	−212	156	−80	210	244		
49	−146	103	78	157	−26	211	150		
50	−204	104	−56	158	−132	212	32		
51	−42	105	−34	159	222	213	214		
52	224	106	−124	160	−200	214	−52		
53	−106	107	230	161	−178	215	110		
54	12	108	−176	162	−44	216	168		

TABLE VIII

The Residues mod 157258404803291863335321 7 of the u_n's[a] Form a Periodic Sequence of Order 256

n	u_n	n	u_n
mod 256	mod 157258404803291863335321 7	mod 256	mod 157258404803291863335321 7
0	0	54	165 326 326 037 771 920 630
1	1	55	399 133 058 537 705 128 729
2	2	56	963 592 443 113 182 178 088
3	5	57	2 326 317 944 764 069 484 905
4	12	58	5 616 228 332 641 321 147 898
5	29	59	13 558 774 610 046 711 780 701
6	70	60	32 733 777 552 734 744 709 300
7	169	61	79 026 329 715 516 201 199 301
8	408	62	190 786 436 983 767 147 107 902
9	985	63	460 599 203 683 050 495 415 105
10	2 378	64	$-u_{63}$
11	5 741	65	$-u_{64}$
12	13 860	66	u_{62}
13	33 461	67	$-u_{61}$
14	80 782	68	u_{60}
15	195 025	69	$-u_{59}$
16	470 832	70	u_{58}
17	1 136 689	71	$-u_{57}$
18	2 744 210	72	u_{56}
19	6 625 109	73	$-u_{55}$
20	15 994 428	74	u_{54}
21	38 613 965	75	$-u_{53}$
22	93 222 358	76	u_{52}
23	225 058 681	77	$-u_{51}$
24	543 339 720	78	u_{50}
25	1 311 738 121	79	$-u_{49}$
26	3 166 815 962	80	u_{48}
27	7 645 370 045	81	$-u_{47}$
28	18 457 556 052	82	u_{46}
29	44 560 482 149	83	$-u_{45}$
30	107 578 520 350	84	u_{44}
31	259 717 522 849	85	$-u_{43}$
32	627 013 566 048	86	u_{42}
33	1 513 744 654 945	87	$-u_{41}$
34	3 654 502 875 938	88	u_{40}
35	8 822 750 406 821	89	$-u_{39}$
36	21 300 003 689 580	90	u_{38}
37	51 422 757 785 981	91	$-u_{37}$
38	124 145 519 261 542	92	u_{36}
39	299 713 796 309 065	etc.	
40	723 573 111 879 672		
41	1 746 860 020 068 409		
42	4 217 293 152 016 490		
43	10 181 446 324 101 389		
44	24 580 185 800 219 268		
45	59 341 817 924 539 925		
46	143 263 821 649 299 118		
47	345 869 461 223 138 161		
48	835 002 744 095 575 440		
49	2 015 874 949 414 289 041		
50	4 866 752 642 924 153 522		
51	11 749 380 235 262 596 085		
52	28 365 513 113 449 345 692		
53	68 480 406 462 161 287 469		

[a] Consequently the z_n's also.

However, John Brillhart factorized the number 1572... (this problem of factorization was proposed to him by Andrew Bremner; the author really feels greatly indebted to both for their interest) as follows:

$$1572... = 11777 \cdot 2393857 \cdot 55780318173953.$$

On the other hand

$$1090... = 2^{12} \cdot 266231328970316414923$$

and as a consequence of (20),

$$(2x)^2 \equiv -2^{13} \cdot 266231... \pmod{11777}. \tag{21}$$

But now, a simple computation shows that

$$\left(\frac{-2^{13} \cdot 266231...}{11777}\right) = \left(\frac{266231...}{11777}\right) = -1$$

and, therefore, (21) is impossible.

Thus, we have proved the following:

THEOREM. *The diophantine equation*

$$y^2 = 2x^4 + 89$$

is impossible if $x \equiv 0 \pmod{16}$, *while the diophantine equation*

$$y^2 = 8x^4 + 89$$

is impossible if x *is even and* $\not\equiv 0 \pmod 5$.

COROLLARY. *The only solutions to the diophantine equation*

$$y^2 = 2^k + 89$$

with $y > 0$ *are given by* $(k, y) = (5, 11), (13, 91)$.

Note added in proof. While this paper was in preparation for publication, the author's attention was drawn by [6], which settles the problem of $y^2 - D = 2^k$ for every D. The results of [6] do not cover the theorems of the present paper (but only their corollaries), and the method used there is by no means elementary.

REFERENCES

1. E. L. COHEN, The diophantine equation $x^2 + 11 = 3^k$ and related questions, *Math. Scand.* **38** (1976), 240–246.
2. J. H. E. COHN, Lucas and Fibonacci numbers and some diophantine equations, *Proc. Glasgow Math. Assoc.* **7** (1965), 24–28.
3. L. J. MORDELL, "Diophantine Equations," Chap. 8, Theorem 5, Academic Press, London/New York, 1969.
4. A. BREMNER, R. CALDERBANK, P. HANLON, P. MORTON, AND J. WOLFSKILL, Two-weight ternary codes and the equation $y^2 = 4 \cdot 3^n + 13$, *J. Number Theory* **16** (1983), 212–234.
5. A. BREMNER AND P. MORTON, The integer points on three related elliptic curves, *Math. Comp.* **39** (1982), 235–238.
6. F. BEUKERS, On the generalized Ramanujan–Nagell equation I, *Acta Arith.* **38** (1981), 389–410.