JOURNAL OF NUMBER THEORY 26, 96–116 (1987)

The Diophantine Equation $x^2 = 4q^{a/2} + 4q + 1$, with an Application to Coding Theory

NIKOS TZANAKIS

Department of Mathematics, University of Crete, Iraklion, Crete, Greece

AND

JOHN WOLFSKILL

Department of Mathematics, Michigan State University, East Lansing, Michigan 48824

Communicated by D. J. Lewis

Received April 14, 1986

All solutions in positive integers of the equation of the title are found, under the restriction that q be a prime power. A method of F. Beukers is used to show that q is bounded, apart from trivial solutions. The remaining q's are dealt with by congruence arguments and by a method using second-order recurrence sequences. An application is given toward the classification of certain $[n, k]$ codes over $GF(q)$.

1

The main object of this paper is the solution of the equation

$$x^2 = 4q^{a/2} + 4q + 1, \tag{1.1}$$

where x and a are positive integers, and q is a prime power. If a is even in (1.1), we are led to consider the equation

$$x^2 = 4q^m + 4q + 1, \tag{1.2}$$

and if a is odd and q is a square, upon replacing q by $\sqrt{q}$ we are led to

$$x^2 = 4q^m + 4q^2 + 1. \tag{1.3}$$

In (1.3) we may assume that m is odd, since if m is even then (1.3) reduces back to (1.2).

For any q, (1.2) has the trivial solution $m = 2$, $x = 2q + 1$; similarly, (1.3)

0022-314X/87 $3.00

has the trivial solution $m = 1$, $x = 2q + 1$. In this paper, we will prove the following theorem, confirming a conjecture of Calderbank [4]:

THEOREM 1.1. *Let q be a prime power, and x, m positive integers. The only non-trivial solutions to* (1.2) *are* $q = 3$, $(m, x) = (1, 5)$ *and* $(3, 11)$. *The only non-trivial solutions to* (1.3) *with m odd are* $q = 2$, $(m, x) = (1, 5)$, $(3, 7)$, *and* $(7, 23)$.

Equation (1.1) was derived by Calderbank in [4] as a necessary condition for the existence of certain codes. Knowing all the solutions of (1.1), one can list all possible parameter sets of the codes studied in [4]. We will make this application now. We quote Theorem 1.1 of [4]:

THEOREM (Calderbank). *Let C be an $[n, k]$ code over $GF(q)$ with exactly two non-zero weights w_1 and w_2, and with the property that the minimum weight in the dual code $C^\perp$ is at least* 4. *If $k = 2$ then $n = 2$, $w_1 = 1$, and $w_2 = 2$.*

(A) *If $k \geqslant 3$ and $q = 2$ then either*

(1) $n = 2^{k-1}$, $w_1 = 2^{k-2}$, *and* $w_2 = 2^{k-1}$, *or*

(2) $k = 4$, $n = 5$, $w_1 = 2$, *and* $w_2 = 4$.

(B) *If $k \geqslant 3$ and $q \neq 2$ then either*

(3) $k = 3$, $q = 2^m$, $n = 2^m + 2$, $w_1 = 2^m$, *and* $w_2 = 2^m + 2$,

(4) $k = 4$, $n = q^2 + 1$, $w_1 = (q-1)\,q$, *and* $w_2 = q^2$,

(5) $(q-1)n = u(q^{k/2} + 1)$, $w_1 = uq^{(k-2)/2}$, *and* $w_2 = (u+1)\,q^{(k-2)/2}$, *where u is a positive integer and* $(2u+3)^2 = 4q^{k/2} + 4q + 1$, *or*

(6) $2(q-1)\,n = (2u+1)\,q^{(k-1)/2} + (q-2) - u(u+1)/q$, $w_1 = uq^{(k-3)/2}$, *and* $w_2 = (u+1)\,q^{(k-3)/2}$, *where u is a positive integer and* $(2u + (2q+1))^2 = 4q^{(k+1)/2} + 4q + 1$.

(We refer the interested reader to [4] for an explanation of the coding theory terminology.)

Alternatives (5) and (6) of this theorem imply the existence of a solution to (1.1). Further, it is easy to see that trivial solutions of (1.1) correspond in (5) or (6) either to situation (4) or to degenerate situations ($k = 1$ or $u = 0$). Therefore, Theorem 1.1 and Calderbank's theorem imply

COROLLARY 1.2. *Let C be as in Calderbank's theorem. Only the following values of k, n, w_1, and w_2 are possible*:

(1) *For any q*: $k = 2$, $n = 2$, $w_1 = 1$, $w_2 = 2$
$k = 4$, $n = q^2 + 1$, $w_1 = (q-1)\,q$, $w_2 = q^2$.

In addition, for

(2) $q=2$: $n=2^{k-1}$, $w_1=2^{k-2}$, $w_2=2^{k-1}$.

(3) $q=3$: $k=5$, $n=11$, $w_1=6$, $w_2=9$
$k=6$, $n=56$, $w_1=1$, $w_2=2$.

(4) $q=4$: $k=6$, $n=78$, $w_1=56$, $w_2=64$
$k=7$, $n=430$, $w_1=320$, $w_2=352$.

(5) $q=2^m$: $k=3$, $n=2^m+2$, $w_1=2^m$, $w_2=2^m+2$.

Codes exist with each of these parameter sets, with the possible exception of the [430, 7] code over $GF(4)$, whose existence still is an open problem (see [2, 4]).

Remarks. 1. Equation (1.1) for $q=3$ (or, equivalently, Eq. (1.2) with $q=3$) has been solved by Bremner *et al.* [2], Bremner and Morton [3], and the authors [6], all by essentially different arguments. Equation (1.1) for $q=4$ (or, equivalently, (1.2) with $q=4$ and (1.3) with $q=2$) is one of those solved by Beukers in [1, p. 408]. Thus, the non-trivial solutions of (1.1) and their corresponding parameter sets already were known (see [2, 4]); what we do here is to show that all the other q's give rise only to trivial solutions.

2. Equation (1.1) has an additional application toward the classification of linear representations of partial quadrangles. We refer the interested reader to [4, 5].

3. Some progress toward the solution of (1.1) was made by the authors in [6], and we will need to refer to several of the results there. Of particular importance is the fact that in (1.2) or (1.3), m must be large if q is large (the precise statement of this is in Sect. 3). In [6] a method of Beukers [1], based on hypergeometric polynomials, was applied; these same polynomials are used here in a p-adic context, leading to an upper bound for q in (1.2) and (1.3), excluding trivial solutions. The remaining (finitely many) q's are treated on a case-by-case basis, sometimes involving a fair amount of computation. Congruence arguments are very effective for (1.2), but not (1.3); the latter is treated by factoring in the field $\mathbb{Q}(\sqrt{q})$, and applying the method developed in part II of [6].

Frits Beukers suggested the key plan of attack used to bound q, and we acknowledge his help with many thanks. Also, we are grateful to Robert Calderbank for helpful discussions about the coding theory aspects of this work.

2

In this section we prove some elementary lemmas about Eq. (1.2) and (1.3).

LEMMA 2.1. *In* (1.2) $m = 1$ *is possible only for* $q = 3$.

Proof. If $m = 1$, we have $x^2 - 1 = 8q$. Let $s = \frac{1}{2}(x-1)$, so $s(s+1) = 2q$. If q is even then s must be one, implying $q = 1$, a contradiction. Hence q is odd, and so $s = 2$ and $q = s + 1 = 3$, as claimed.

From [6] we recall

LEMMA 2.2. *If* $m > 2$, *then* (1.2) *is impossible if* m *is even or if* q *is a square.*

(*This is Proposition* (A) *of the introduction of* [6]).

LEMMA 2.3. *In* (1.3) $m = 3$ *is possible only for* $q = 2$.

Proof. The equation is $x^2 - 1 = 4q^2(q+1)$. Let $s = \frac{1}{2}(x-1)$, so $s(s+1) = q^2(q+1)$. It must be that $q^2 | s$ or $q^2 | s+1$. In the first case, $s(s+1) \geqslant q^2(q^2+1) > q^2(q+1)$, a contradiction. In the second, $q^2(q+1) = s(s+1) \geqslant q^2(q^2-1)$, and so we have

$$q^2 - q - 2 \leqslant 0,$$

implying $q = 2$ as claimed.

LEMMA 2.4. *If* $m \geqslant 3$ *is odd and* q *is a square, then* (1.3) *has no solutions.*

Proof. From Lemma 2.3 we may assume $m \geqslant 5$. Let $q = r^2$, and let $s = x - 2r^m$, so $s(x + 2r^m) = 4r^4 + 1$. Note that $x > 2r^m$, so $s \geqslant 1$, and we have

$$4r^4 + 1 = s(x + 2r^m) \geqslant 4r^5,$$

which is obviously impossible.

3

In this section we use certain hypergeometric polynomials to bound q in (1.2) and (1.3). We write $q = p^f$, p a prime. The first step is to show that the exponent m must be fairly large.

LEMMA 3.1. (1) *In* (1.2), *if* $m \geqslant 3$ *is odd and* $q > 1000$, *then* $m \geqslant 51$.

(2) *In* (1.3), *if* $m \geqslant 5$ *is odd and* $q > 40$, *then* $m \geqslant 71$.

Proof. This result follows from Theorem I.1 of [6], which states that two solutions of an equation like (1.2) or (1.3) must have the exponents

very widely separated. Specifically, if the two exponents are n and n', with $n' > n$, this theorem states that

$$n' > \frac{13}{28} \cdot \frac{\log D}{\sqrt{\varepsilon}} \cdot (1 - 3\sqrt{\varepsilon}), \tag{3.1}$$

where $\varepsilon = D/q^n$, and $D = 4q + 1$ for (1.2) and $D = 4q^2 + 1$ for (1.3).

For (1.2), we apply (3.1) to the two solutions

$$(2q+1)^2 = 4q^2 + 4q + 1 \qquad \text{and} \qquad x^2 = 4q^m + 4q + 1$$

to obtain

$$m > \frac{13}{28} (\log 4q) \cdot \frac{q}{\sqrt{4q+1}} \cdot \left(1 - \frac{3\sqrt{4q+1}}{q}\right).$$

For $q > 1000$, one can check easily that this implies $m \geqslant 51$.

For (1.3), we apply (3.1) to the two solutions

$$(2q^2+1)^2 = 4q^4 + 4q^2 + 1 \qquad \text{and} \qquad x^2 = 4q^m + 4q^2 + 1$$

to obtain

$$m > \frac{13}{28} (\log 4q^2) \cdot \frac{q^2}{\sqrt{4q^2+1}} \cdot \left(1 - \frac{3\sqrt{4q^2+1}}{q^2}\right).$$

As before, one finds that $m \geqslant 71$ if $q > 40$.

We will use the usual hypergeometric function F, defined by the power series

$$F(a, b, c, z) = 1 + \frac{a \cdot b}{c \cdot 1} z + \frac{a(a+1) \cdot b(b+1)}{c(c+1) \cdot 1 \cdot 2} z^2 + \cdots.$$

Let G and H be the polynomials of degrees n_1 and n_2, respectively, defined by

$$G(z) = F(-n_2 - \tfrac{1}{2}, -n_1, -n, z) \quad \text{and} \quad H(z) = F(-n_1 + \tfrac{1}{2}, -n_2, -n, z).$$

Here $n = n_1 + n_2$ and n_1, n_2 are positive integers to be determined. From [1] we recall the identities

$$\begin{aligned} \binom{n}{n_2} G(z) &= \sum_{k=0}^{n_1} \binom{n_2 + \frac{1}{2}}{k} \binom{n-k}{n_2} (-z)^k \\ \binom{n}{n_2} H(z) &= \sum_{k=0}^{n_2} \binom{n_1 - \frac{1}{2}}{k} \binom{n-k}{n_1} (-z)^k. \end{aligned} \tag{3.2}$$

From (3.2) it follows that $\binom{n}{n_2} G(4z)$ and $\binom{n}{n_2} H(4z)$ are polynomials with integral coefficients (Lemma 3 of [1]). We will choose n_1 and n_2 so that $n_1 > n_2$. Hence, by (3.2),

$$\begin{aligned}
\binom{n}{n_2}|G(z)| &< \sum_{k=0}^{n_1} \binom{n_1}{k}\binom{n}{n_2}|z|^k = \binom{n}{n_2}(1+|z|)^{n_1} \\
\binom{n}{n_2}|H(z)| &< \sum_{k=0}^{n_2} \binom{n_1}{k}\binom{n-k}{n_1}|z|^k = \sum_{k=0}^{n_2} \binom{n_2}{k}\binom{n-k}{n_2}|z|^k \qquad (3.3)\\
&\leqslant \binom{n}{n_2}(1+|z|)^{n_2}.
\end{aligned}$$

From Lemma 1 of [1] we have

$$\binom{n}{n_2} G(4z) - \binom{n}{n_2}\sqrt{1-4z}\, H(4z) = (4z)^{n+1} \cdot \binom{n}{n_2} G(1)\, E(4z), \quad (3.4)$$

where $E(4z)$ is a power series in z (with no negative powers of z). Specifically, see [1, p. 390],

$$E(z) = \frac{F(n_2+1, n_1+\frac{1}{2}, n+2, z)}{F(n_2+1, n_1+\frac{1}{2}, n+2, 1)},$$

but we will not need the exact form of E. We will renotate (3.4) as

$$\binom{n}{n_2} G(4z) - \binom{n}{n_2}\sqrt{1-4z}\, H(4z) = z^{n+1} E_1(z). \quad (3.5)$$

Here $E_1(z)$ is some power series in z, and the important thing about it is that the coefficients are integers, by Lemma 3 of [1].

THEOREM 3.2. *Let q be a power of a prime, x an integer, and $m \geqslant 3$ an odd integer such that $x^2 = 4q^m + 4q + 1$. Then $q < 1020$.*

Proof. We may assume $q > 1000$; write $q = p^f$, p a prime. We use $\mathbb{Q}_p$ to denote the usual p-adic completion of $\mathbb{Q}$, and $\mathbb{Z}_p$ to denote the p-adic integers. The p-adic valuation will be denoted by $\|\cdot\|_p$.

Set $z = -q$ in (3.5). Certainly the left side of (3.5) converges in $\mathbb{Q}_p$ for $z = -q$, since G and H are polynomials, and $\sqrt{1-4z}$ always converges if $\|z\|_p < 1$. Hence $E_1(-q)$ is some number in $\mathbb{Q}_p$, and therefore in $\mathbb{Z}_p$, since the power series for E_1 has integral coefficients. Therefore, (3.5) implies that

$$\left\| \binom{n}{n_2} G(-4q) - \binom{n}{n_2}\sqrt{1+4q}\, H(-4q) \right\|_p \leqslant \|q^{n+1}\|_p = q^{-(n+1)}. \quad (3.6)$$

Next, from the diophantine equation we have

$$1+4q=x^2\left(1-\frac{4q^m}{x^2}\right).$$

We may replace x by $-x$ if necessary, so that $x\equiv 1 \bmod p$. Then

$$\sqrt{1+4q}=x\sqrt{1-\frac{4q^m}{x^2}}=x+q^m\cdot\zeta \tag{3.7}$$

for some $\zeta\in\mathbb{Z}_p$, since x is a p-adic unit. From (3.6) and (3.7),

$$\|\lambda-x\eta-q^m\eta\zeta\|_p\leqslant q^{-(n+1)},$$

where $\lambda=\binom{n}{n_2}G(-4q)$ and $\eta=\binom{n}{n_2}H(-4q)$; both are ordinary integers. Now, by the triangle inequality in $\mathbb{Q}_p$,

$$\begin{aligned}\|\lambda-x\eta\|_p&\leqslant\max\{\|\lambda-x\eta-q^m\eta\zeta\|_p,\ \|q^m\eta\zeta\|_p\}\\&\leqslant\max\{q^{-(n+1)},\ q^{-m}\}.\end{aligned}$$

Thus $\|\lambda-x\eta\|_p\leqslant q^{-t}$, where $t=\min\{m,\ n+1\}$. Let $K=\lambda-x\eta$; then $K\in\mathbb{Z}$, so

$$q^t|K, \tag{3.8}$$

from the definition of the p-adic valuation.

Now let $a=1$ or 3, chosen so that $m\equiv a \bmod 4$, and set

$$n_1=\frac{3(m-a)}{4}+b \qquad \text{and} \qquad n_2=\frac{m-a}{4}+b,$$

where $b=0$ or 1, to be chosen so that $K\neq 0$. Note that $n_1>n_2$ since $m>a$ obviously by Lemma 3.1. For $i=0, 1$ let G_i and H_i be the G and H for $b=i$. If $K=0$ for both, then

$$G_0(-4q)\,H_1(-4q)-G_1(-4q)\,H_0(-4q)=0,$$

which contradicts Lemma 4 of [1]. Thus we may assume $K\neq 0$, so $|K|\geqslant q^t$, by (3.8). We use (3.3) to get an upper bound on K. Since $|x|<2q^{m/2}+1$,

$$|K|<\binom{n}{n_2}[(1+4q)^{n_1}+(2q^{m/2}+1)(1+4q)^{n_2}]. \tag{3.9}$$

Note that $m/2 + n_2 - n_1 = \frac{1}{2}a > 0$, so the second term has the higher power of q. Since $q > 1000$ and $n_1 > n_2$, (3.9) implies

$$|K| < 2\binom{n}{n_2} \cdot \left(\frac{4001}{1000}\right)^{n_1} \cdot q^{m/2+n_2}. \tag{3.10}$$

It remains to find an upper bound for $\binom{n}{n_2}$. If k is a positive integer, it is easy to see by induction that

$$\binom{4k}{k} \leqslant \frac{27}{64} \cdot \left(\frac{4}{3^{3/4}}\right)^{4k}.$$

From this it follows that

$$\binom{4k+2}{k+1} = \frac{(4k+2)(4k+1)}{(k+1)(3k+1)} \cdot \binom{4k}{k} < \frac{16}{3} \cdot \frac{27}{64} \cdot \left(\frac{4}{3^{3/4}}\right)^{4k}$$
$$= \frac{27\sqrt{3}}{64} \cdot \left(\frac{4}{3^{3/4}}\right)^{4k+2}.$$

If $b = 0$ then $n = 4n_2$ and so $\binom{n}{n_2}$ has the form $\binom{4k}{k}$ above; if $b = 1$ it has the form $\binom{4k+2}{k+1}$. Hence, by (3.8) and (3.10),

$$q^{t-m/2-n_2} < \frac{27\sqrt{3}}{32} \cdot \left(\frac{4}{3^{3/4}}\right)^{n} \cdot \left(\frac{4001}{1000}\right)^{n_1}. \tag{3.11}$$

Depending on the values of a and b, there are four cases that can occur. Since $t = \min\{m, n+1\}$ and $n + 1 = m - a + 2b + 1$, we see that

$$t = m \qquad \text{if} \quad b = 1, \quad \text{or} \quad (b = 0 \quad \text{and} \quad a = 1);$$
$$t = m - 2 \qquad \text{if} \quad b = 0 \quad \text{and} \quad a = 3.$$

If in (3.11) $t = m$, then

$$q < \left(\frac{27\sqrt{3}}{32}\right)^{4/(m+a-4b)} \cdot \left(\frac{4}{3^{3/4}}\right)^{(4m-4a+8b)/(m+a-4b)}$$
$$\cdot \left(\frac{4001}{1000}\right)^{(3m-3a+4b)/(m+a-4b)}$$

The worst bound results from the largest b ($b = 1$), the smallest a ($a = 1$), and the smallest m ($m = 51$, by Lemma 3.1). If in (3.11), $t = m - 2$, then

$$q < \left(\frac{27\sqrt{3}}{32}\right)^{4/(m-5)} \cdot \left(\frac{4}{3^{3/4}}\right)^{(4m-12)/(m-5)} \cdot \left(\frac{4001}{1000}\right)^{(3m-9)/(m-5)}.$$

Again, $m=51$ provides the worst bound. In both cases one finds that $q<1020$, as claimed.

The next result bounds q in Eq. (1.3). The details are very similar to those in Theorem 3.2, so we will be more brief with the proof.

THEOREM 3.3. *Let q be a prime power, x an integer, and $m \geqslant 5$ an odd integer, such that $x^2 = 4q^m + 4q^2 + 1$. Then $q < 40$.*

Proof. Write $q = p^f$, as before. We may assume $q > 40$, and we have $m \geqslant 71$ by Lemma 3.1. Set $z = -q^2$ in (3.5) to get

$$\binom{n}{n_2} G(-4q^2) - \binom{n}{n_2} \sqrt{1+4q^2}\, H(-4q^2) = (-q^2)^{n+1} \cdot E_1(-q^2),$$

with $E_1(-q^2) \in \mathbb{Z}_p$. Choosing the sign of x appropriately, we have

$$\sqrt{1+4q^2} = \sqrt{x^2 - 4q^m} = x + q^m \cdot \zeta$$

for some $\zeta \in \mathbb{Z}_p$. Let $K = \binom{n}{n_2} G(-4q^2) - xH(-4q^2) \in \mathbb{Z}$. We have

$$q^t | K, \qquad \text{where} \quad t = \min\{m, 2n+2\}. \tag{3.12}$$

Let $a = 1, 3, 5,$ or 7, chosen so that $m \equiv a \bmod 8$. Set

$$n_1 = \frac{3(m-a)}{8} + b \qquad \text{and} \qquad n_2 = \frac{m-a}{8} + b,$$

where $b = 0$ or 1, chosen as before so that $K \neq 0$. Hence, by (3.12),

$$|K| \geqslant q^t. \tag{3.13}$$

From (3.3) it follows that

$$|K| < \binom{n}{n_2}[(1+4q^2)^{n_1} + (2q^{m/2}+1)(1+4q^2)^{n_2}].$$

The second term has the higher power of q, and the binomial coefficient $\binom{n}{n_2}$ has the form $\binom{4k}{k}$ or $\binom{4k+2}{k+1}$, so estimating as before we have

$$|K| < \frac{27\sqrt{3}}{32} \cdot \left(\frac{4}{3^{3/4}}\right)^n \cdot \left(\frac{6401}{1600}\right)^{n_1} \cdot q^{2n_2 + m/2}.$$

This, combined with (3.13), shows that

$$q^{t - 2n_2 - m/2} < \frac{27\sqrt{3}}{32} \cdot \left(\frac{4}{3^{3/4}}\right)^n \cdot \left(\frac{6401}{1600}\right)^{n_1} = \alpha \cdot \beta^n \cdot \gamma^{n_1}, \text{ say.}$$

We rewrite this as

$$q < \alpha^{1/(t-2n_2-m/2)} \cdot \beta^{n/(t-2n_2-m/2)} \cdot \gamma^{n_1/(t-2n_2-m/2)}. \tag{3.14}$$

It is straightforward to check that in all 8 cases (4 values of a and 2 of b), (3.14) implies $q < 40$. This completes the proof.

4

In this section we complete the treatment of Eq. (1.2). We are of course interested only in non-trivial solutions, so we exclude the case $m = 2$. We also exclude $q = 3$, since in this case (1.2) already has been solved, as was mentioned in Section 1. Applying Lemmas 2.1, 2.2 and Theorem 3.2, what remains to be considered are the cases in which all of the following hold:

$$\begin{aligned} &m \geqslant 3 \text{ is odd} \\ &q \text{ is not a square} \\ &q < 1020. \end{aligned} \tag{4.1}$$

We will show that (1.2) is unsolvable under these restrictions by considering the equation separately for each q satisfying (4.1). Fortunately, the vast majority of these q's can be eliminated systematically by simple congruence arguments. Proposition (B) of the introduction in [6] allows one to eliminate q if any of the following happen:

$$\pi | 4q + 1 \qquad \text{for a prime } \pi \equiv 3 \bmod 4 \tag{4.2}$$

$$\pi | q + 1 \qquad \text{for a prime } \pi \equiv 3, 5, \text{ or } 6 \bmod 7 \tag{4.3}$$

$$q \equiv 4 \text{ or } 7 \bmod 9 \quad \text{and} \quad \pi | q^2 - q + 1 \qquad \text{for a prime } \pi \equiv 2 \text{ or } 3 \bmod 5. \tag{4.4}$$

Note that

(4.2) applies if $q \equiv 2 \bmod 3$

(4.3) applies if $q \equiv 2, 4, 5 \bmod 7$ or $q \equiv 4 \bmod 5$

(4.4) applies if $q \equiv 4, 7 \bmod 9$ and ($q \equiv 3 \bmod 7$ or $q \equiv 2, 3, 4 \bmod 5$).

In particular, all odd powers of 2 and 5 are eliminated by (4.2); $q = 7$ is eliminated by (4.4), but $q = 7^3 = 343$ remains. In [6] it is proved that (1.2) has only the trivial solution for $q = 3^f$, $f > 1$. Thus, except for $q = 343$, we may assume that $2, 3, 5, 7 \nmid q$. For such a q to survive conditions (4.2)–(4.4), it must lie in one of 13 residue classes mod $315 = 9 \cdot 5 \cdot 7$—specifically,

$$q \equiv 1, 73, 76, 106, 118, 127, 136, 181, 211, 253, 262, 286, 307 \bmod 315. \tag{4.5}$$

The odd powers of primes $q < 1020$ satisfying (4.5) are (with 343)

$$q = 73, 127, 181, 211, 307, 343, 421, 433, 577, 601, 631, 757, 811, 883, 937. \tag{4.6}$$

The case $q = 307$ was settled in [6] (there are no non-trivial solutions). Some of the q's in (4.6) can be eliminated by (4.2), (4.3), (4.4), as summarized in the table.

q	181	211	577	811	883	937
Condition	(4.3)	(4.4)	(4.3)	(4.2)	(4.3)	(4.2)
π	13	73	17	11	13	23

We are left with 8 possible q's,

$$q = 73, 127, 343, 421, 433, 601, 631, 757.$$

These will be treated individually by ad hoc congruence arguments. The general strategy is to show that m odd implies $4q^m + 4q + 1$ is a quadratic non-residue modulo a certain prime. Depending on q, it is necessary to consider various cases, usually depending on the residue class of m mod 6.

First, even if (4.4) does not apply completely, it can in part. To be precise, (4.4) is the union of the following two statements:

$$\text{If} \quad q \equiv 4, 7 \bmod 9 \quad \text{then} \quad m \equiv 5 \bmod 6. \tag{4.7}$$

$$\text{If} \quad q \equiv 3 \bmod 7 \quad \text{or} \quad q \equiv 2, 3, 4 \bmod 5 \quad \text{then} \quad m \not\equiv 5 \bmod 6. \tag{4.8}$$

These are easy to prove. For (4.7), if $m \equiv 1, 3 \bmod 6$ then $4q^m + 4q + 1$ is divisible by 3 but not by 9, so cannot be a square. For (4.8), $4q^m + 4q + 1$ will be a non-square mod 7 or mod π for some π for which q has order 6, if $m \equiv 5 \bmod 6$.

We are ready now to dispose of the 8 remaining q's. We denote $4q^m + 4q + 1$ by R.

q = 73. From (4.8), $m \not\equiv 5 \bmod 6$. 73 has order 3 mod 1801, so

$$R \equiv \begin{cases} 8q + 1 \bmod 1801 & \text{if} \quad m \equiv 1 \bmod 6 \\ 4q + 5 \bmod 1801 & \text{if} \quad m \equiv 3 \bmod 6. \end{cases}$$

However, the Legendre symbols $(\frac{8 \cdot 73 + 1}{1801})$ and $(\frac{4 \cdot 73 + 5}{1801})$ both equal -1.

q = 127. From (4.8), $m \not\equiv 5 \bmod 6$. 127 has orders 3 mod 5419 and

6 mod 13. If $m \equiv 1 \bmod 6$ then $R \equiv 8q+1 \bmod 5419$, and if $m \equiv 3 \bmod 6$ then $R \equiv 4q-3 \bmod 13$, but

$$\left(\frac{8q+1}{5419}\right) = \left(\frac{4q-3}{13}\right) = -1.$$

q = 343. From (4.8), $m \not\equiv 5 \bmod 6$. 343 has orders 3 mod 37 and 6 mod 117307. If $m \equiv 1 \bmod 6$ then $R \equiv 8q+1 \bmod 117307$, and if $m \equiv 3 \bmod 6$ then $R \equiv 4q+5 \bmod 37$, but

$$\left(\frac{8q+1}{117307}\right) = \left(\frac{4q+5}{37}\right) = -1.$$

q = 421. From (4.7), $m \equiv 5 \bmod 6$, so $m \equiv 5, 11 \bmod 12$. 421 has orders 4 mod 13 and 12 mod 37. If $m \equiv 5 \bmod 12$, $R \equiv 8q+1 \bmod 13$; and if $m \equiv 11 \bmod 12$, $R \equiv -4q^5 + 4q + 1 \bmod 37$. In both cases the appropriate Legendre symbol is -1.

q = 433. From (4.8), $m \not\equiv 5 \bmod 6$. 433 has order 6 mod 13 and mod 14389. If $m \equiv 1 \bmod 6$, $R \equiv 8q+1 \bmod 13$, and if $m \equiv 3 \bmod 6$, $R \equiv 4q-3 \bmod 14389$, both cases leading to the usual contradiction.

q = 601. $601 \equiv 13 \bmod 49$, so $7 | R$ and consequently $49 | R$ as well. This implies that $7 | m$, for mod 49,

$$R \equiv 4 \cdot (7 \cdot 2 - 1)^m + 4 \equiv 4 \sum_{j=0}^{m} \binom{m}{j} 2^j 7^j (-1)^{m-j} + 4$$

$$\equiv 4 \cdot (-1)^m + 56m \cdot (-1)^{m-1} + 4 \equiv 7m \qquad \text{since } m \text{ is odd.}$$

Hence $m \equiv 7, 21 \bmod 28$. But each case leads to a contradiction mod 29.

q = 631. 631 has orders 3 mod 307, 6 mod 331, and 12 mod 13. If $m \equiv 1 \bmod 6$, $R \equiv 8q+1 \bmod 307$ and this is a quadratic non-residue. If $m \equiv 3 \bmod 6$, $R \equiv 4q-3 \bmod 331$, again a non-square. If $m \equiv 5 \bmod 6$, $R \equiv \pm 4q^5 + 4q + 1 \bmod 13$ and both are non-squares.

q = 757. From (4.8), $m \equiv 1, 3 \bmod 6$. 757 has order 3 mod 14713 and this will rule out $m \equiv 1 \bmod 6$, so $m \equiv 3, 9, 15 \bmod 18$. The first two are impossible mod 19, so $m \equiv 15 \bmod 18$. If $m \equiv 1 \bmod 4$, then $R \equiv 17 \bmod 5$, a non-square, so it must be that $m \equiv 15 \bmod 36$. Finally, this leads to a contradiction mod 37.

5

In this section we complete the treatment of Eq. (1.3). As was stated in Section 1, we assume m is odd in (1.3)—otherwise, (1.3) reduces to (1.2).

We exclude the trivial solution $m = 1$, and we also exclude the case $q = 2$, as (1.3) already has been solved in this case (see Sect. 1). Applying Lemmas 2.3, 2.4 and Theorem 3.3, it remains to consider (1.3) under the restrictions

$$\begin{aligned} &m \geqslant 5 \quad \text{is} \quad \text{odd} \\ &q \quad \text{is} \quad \text{not} \quad \text{a} \quad \text{square} \\ &q \leqslant 37. \end{aligned} \tag{5.1}$$

The case $q = 8$ and 32 can be solved easily by known results. If $q = 8$, Eq. (1.3) takes the form

$$x^2 = 2^{3m+2} + 257,$$

which was solved by Beukers in [1, p. 408]. There are no solutions with $m \geqslant 5$ and odd. For $q = 32$, the equation is

$$x^2 = 2^{5m+2} + 4097.$$

We apply Corollary 2 to Theorem 1 of [1] to get

$$5m + 2 < 18 + \frac{2 \log 4097}{\log 2},$$

implying $m \leqslant 8$. From (5.1), the only possible m's are 5 and 7, neither of which gives a solution to (1.3).

The case $q = 37$ can be taken care of by slightly augmenting the results from Section 3.

THEOREM 5.1. *The equation* $x^2 = 4 \cdot 37^m + 5477$ *has no solutions with odd* $m \geqslant 5$.

Proof. Proceeding as in the proof of (2) of Lemma 3.1, one finds that $m \geqslant 63$. On the other hand, the proof of Theorem 3.3 shows that $m \leqslant 83$, for if $m \geqslant 85$, then in (3.14) it follows that $q < 37$. (Note that an upper bound for m can be obtained in this way for any $q \geqslant 27$. The reason for the barrier at 27 is that as $m \to \infty$, the right side of (3.14) approaches $\beta^2 \cdot \gamma^{3/2} \approx 24.6$. As q decreases, the upper bound increases, and it is immediately useful only for $q = 37$.)

Since $37^3 \equiv -1 \bmod 31$, if $m \equiv 3 \bmod 6$ then $4 \cdot 37^m + 5477 \equiv 17 \bmod 31$, but $(\frac{17}{31}) = -1$. Similarly, $37^3 \equiv 1 \bmod 7$ and this rules out $m \equiv 5 \bmod 6$, so $m = 67$, 73, or 79. But $4 \cdot 37^m + 5477$ is a non-square mod 11 for the first two, and mod 17 for the last. Thus no solutions exist.

We are left with Eq. (1.3), where $m \geqslant 5$ is odd and $q = 3, 5, 7, 11,$

13, 17, 19, 23, 27, 29, or 31. For each of these q's, (1.3) will be treated by factoring in the field $\mathbb{Q}(\sqrt{q})$ and applying the method developed in [6, 7]. Accordingly, we will change the notation of (1.3) to fit that of [6]—the equation will be written as

$$y^2 - q(2q^j x^2)^2 = s, \tag{5.2}$$

where $m = 4k + 2j + 1$, $x = q^k$, $s = 4q^2 + 1$, and $j = 0$ or 1, depending on the residue class of m mod 4. Note that in (5.2) $q|x$, since $m \geqslant 5$. The general strategy is to express $2q^j x^2$ in (5.2) as a term of a second-order recurrence sequence (this is done in [6]) and to work with various moduli to show that in the recurrence sequence, x cannot be a power of q. The cases $q = 3$ and 27 can be treated quickly using a result from [6].

THEOREM 5.2. *The equation* $y^2 = 4q^m + 4q^2 + 1$, *with odd* $m \geqslant 5$, *is unsolvable if* $q = 3$ *or* 27.

Proof. For $q = 3$, the equation has the form (5.2) with $s = 37$. In the field $\mathbb{Q}(\sqrt{3})$, 37 factors as $(7 + 2\sqrt{3}) \cdot (7 - 2\sqrt{3})$. We will apply Theorem II.1 of [6]. We define sequences $\{u_n\}$ and $\{v_n\}$, both satisfying the recurrence $z_{n+2} = 4z_{n+1} - z_n$, by $u_0 = 0$, $u_1 = 1$, $v_0 = 2$, and $v_1 = 4$. The theorem says that there is exactly one integer $k \in [0, 17]$ such that

$$b_k = 7u_k + v_k \equiv 0 \bmod 18,$$

and one checks easily that in this case $k = 14$. Further, b_{14} is congruent to 2 mod 5 and 6 mod 17. Since

$$\left(\frac{\frac{1}{2}b_{14}}{17}\right) = \left(\frac{\frac{3}{2}b_{14}}{5}\right) = -1,$$

the same theorem shows that (5.2) is impossible if $3|x$. But we must have $3|x$, since $m \geqslant 5$; hence no solutions exist.

The proof is similar for $q = 27$. Here $s = 2917$ (a prime), and 2917 factors as $(55 + 6\sqrt{3}) \cdot (55 - 6\sqrt{3})$. In this case,

$$b_k = 55u_k + 3v_k \equiv 0 \bmod 18$$

for $k = 12$, and $b_{12} \equiv 1$ mod 5 and 27 mod 53. Since

$$\left(\frac{\frac{1}{2}b_{12}}{5}\right) = \left(\frac{\frac{3}{2}b_{12}}{53}\right) = -1,$$

no solutions exist, for the same reason.

For the remaining q's we need to set up some notation. We will work in

the field $\mathbb{Q}(\sqrt{q})$, and we denote as usual $\omega = \sqrt{q}$ if $q \equiv 2, 3 \bmod 4$ and $\omega = \frac{1}{2}(1+\sqrt{q})$ if $q \equiv 1 \bmod 4$. We denote the fundamental unit in $\mathbb{Q}(\sqrt{q})$ by $e+f\omega$, and we use $a+b\omega$ to denote a typical element of a complete system of pair-wise non-conjugate and non-associate elements of $\mathbb{Z}[\omega]$ having norm $s = 4q^2+1$. We define J by

$$J = \text{Norm}(e+f\omega) = \pm 1,$$

and we define E, w_0, w_1 by

$$E = 2e, \quad w_0 = b, \quad w_1 = af+be \qquad \text{if} \quad q \equiv 2, 3 \bmod 4$$

$$E = 2e+f, \quad w_0 = b, \quad w_1 = af+be+bf \qquad \text{if} \quad q \equiv 1 \bmod 4$$

We make use of the recurrence sequences $\{u_n\}$, $\{v_n\}$, $\{w_n\}$, all satisfying the recurrence

$$z_{n+2} = Ez_{n+1} - Jz_n,$$

where $\{u_n\}$ and $\{v_n\}$ have the initial values

$$u_0 = 0, \quad u_1 = 1, \quad v_0 = 2, \quad v_1 = E.$$

In part II of [6] it is shown that (5.2) implies that

$$2q^j x^2 = \pm w_r \qquad \text{if} \quad q \equiv 2, 3 \bmod 4, \tag{5.3}$$

or

$$4q^j x^2 = \pm w_r \qquad \text{if} \quad q \equiv 1 \bmod 4, \tag{5.4}$$

for some integer r. From [6] we recall the congruences

$$w_{r+2nt} \equiv J^{nt} w_r \bmod u_n \tag{5.5}$$

$$w_{r+2nt} \equiv (-1)^t J^{nt} w_r \bmod v_n. \tag{5.6}$$

Our general strategy is based on the fact that modulo any integer N, the sequence $\{w_r\}$ is periodic with period, say, $P(N)$. Consequently, if w_r is fixed mod N, r is fixed mod $P(N)$; in many cases, one can derive a contradiction from this modulo one of the u's or v's, using the relations (5.3)–(5.6).

For the values of q for which (1.3) has not yet been solved, we have Table I. In each case we have factored s into primes, and the collection of numbers $a+b\omega$ forms a complete set of pairwise non-conjugate, non-associate integers with norm s.

TABLE I

q	e	f	J	E	s	a	$b = w_0$	w_1
5	0	1	−1	1	101	9	4	13
7	8	3	1	16	197	15	2	61
11	10	3	1	20	$5 \cdot 97$	296	89	1778
						32	7	166
13	1	1	−1	3	677	25	4	33
17	3	2	−1	8	$13 \cdot 89$	233	148	1206
						37	−4	54
19	170	39	1	340	$5 \cdot 17^2$	951	218	74149
						39	−2	1181
23	24	5	1	48	$29 \cdot 73$	415	86	4139
						47	−2	187
29	2	1	−1	5	$5 \cdot 673$	156	67	357
						61	−4	49
31	1520	273	1	3040	$5 \cdot 769$	993	178	541649
						63	2	20239

In treating Eq. (5.2) for $q = 23$ and 31, it is necessary to use the fact that $x = q^k$ is a power of q. For the other q's, it is possible to show that (5.2) is unsolvable under the weaker condition that x merely be divisible by q.

THEOREM 5.3. *The diophantine equations*

$$y^2 - 4qx^4 = 4q^2 + 1 \qquad \text{and} \qquad y^2 - 4q^3x^4 = 4q^2 + 1$$

are impossible if $q|x$, *for* $q = 5, 7, 11, 13, 17, 19,$ *or* 29.

An immediate consequence of this theorem is

COROLLARY 5.4. *The equation* $y^2 = 4q^m + 4q^2 + 1$ *has no solutions with odd* $m \geqslant 5$ *for the q's listed above.*

Proof of Corollary 5.4. We write, as before, $m = 4k + 2j + 1$, and $x = q^k$. Since $m \geqslant 5$, $k \geqslant 1$, so $q|x$. Depending on the value of j, the equation takes one of the two forms treated in the theorem. Thus no solutions exist.

Proof of Theorem 5.3. First, since $q|x$, we have $w_r \equiv 0 \bmod q^2$ in (5.3) or (5.4). We treat each q separately:

q = 5. In (5.4) we have $w_r \equiv 0 \bmod 5$ and mod 4. The first implies that $r \equiv 3 \bmod 5$, and the second that r is even. Hence $r \equiv 8, 18 \bmod 20$. If

$r \equiv 8 \bmod 20$, then $r \equiv 8, 28 \bmod 40$, and so $w_r \equiv \mp 3 \bmod 41$, and (5.4) becomes

$$4 \cdot 5^j x^2 \equiv \pm 3 \bmod 41.$$

But this is impossible since $(\frac{5}{41}) = +1$ and $(\frac{\pm 3}{41}) = -1$. So $r \equiv 18 \bmod 20$. Since $w_r \equiv 0 \bmod 25$, this implies that $r \equiv 58 \bmod 100$. Now apply (5.5): we get $w_r \equiv w_{58} \bmod u_{25}$, and $u_{25} = 75025$, which is divisible by 3001. Thus (5.4) implies that

$$4 \cdot 5^j x^2 = \pm w_r \equiv \pm w_{58} \equiv \mp 325 \bmod 3001;$$

but this is impossible since $(\frac{325}{3001}) = -1$ and $(\frac{5}{3001}) = +1$.

q = 7. In (5.3) we have $w_r \equiv 0 \bmod 7$ and $\bmod 2$. These imply that $r \equiv 4 \bmod 7$ and $r \equiv 0 \bmod 2$, so $r \equiv 4 \bmod 14$. Now (5.5) implies that $w_r \equiv w_4 \bmod u_7$. We have $u_7 = 7 \cdot 2350153$ and $w_4 = 247394$, so (5.3) implies

$$2 \cdot 7^j x^2 \equiv \pm 247394 \bmod 2350153,$$

which is impossible.

q = 11. Consider the first pair $(a, b) = (296, 89)$. One checks that $w_r \equiv 0 \bmod 2 \cdot 11$ implies $r \equiv 7 \bmod 22$, so by (5.6), $w_r \equiv \pm w_7 \bmod v_{11}$. Now $v_{11} = 4 \cdot 5 \cdot 9961203701989$ and $w_7 = 2 \cdot 56045954041$, so (5.3) implies an impossible congruence mod 9961203701989.

Now consider the second pair $(a, b) = (32, 7)$. In this case $r \equiv 5 \bmod 22$, so (5.6) implies that $w_r \equiv \pm w_5 \bmod v_{11}$. But $5 | v_{11}$ and $w_5 \equiv 1 \bmod 5$, so (5.3) says that

$$2 \cdot 11^j x^2 \equiv \pm 1 \bmod 5,$$

clearly impossible.

q = 13. In (5.4) we have w_r divisible by 13 and by 4; these imply that $r \equiv 20, 46 \bmod 52$. Applying (5.5), we see that $w_r \equiv w_{20}, w_{46} \bmod u_{13}$. Now $u_{13} = 13 \cdot 118717$ and $-w_{46} \equiv w_{20} \equiv 7124 \bmod 118717$. From these one sees that (5.4) leads to a contradiction mod 118717.

q = 17. Consider the first pair $(a, b) = (233, 148)$. In (5.4) we have $4 \cdot 17 | w_r$, and this forces $r \equiv 10 \bmod 34$, so by (5.5), $w_r \equiv \pm w_{10} \bmod u_{17}$. Now $u_{17} = 17 \cdot 20824391977457$ and $w_{10} = 16 \cdot 11430725403$; one finds that (5.4) leads to a contradiction mod 20824391977457.

For the second pair $(a, b) = (37, -4)$, one finds that $w_r \equiv \pm w_8 \bmod v_{17}$ in a similar way. We have $v_{17} = 4 \cdot 364909962777361$ and $w_8 = 4 \cdot 30752303$, and (5.4) leads to a contradiction mod 364909962777361.

q = 19. For the first pair $(a, b) = (951, 218)$, w_r even implies r even, which in turn implies $w_r \equiv \pm 3 \bmod 17$. Now (5.3) says that

$$2 \cdot 19^j x^2 \equiv \pm 3 \bmod 17,$$

an impossible congruence.

For the second pair $(a, b) = (39, -2)$, $19 | w_r$ implies $r \equiv 17 \bmod 19$, and so $w_r \equiv -1 \bmod 37$. Now (5.3) says that

$$2 \cdot 19^j x^2 \equiv \pm 1 \bmod 37,$$

and this forces $j = 1$. Finally, $w_r \equiv \pm 2, \pm 51, \pm 53 \bmod 113$, so

$$\pm 19x^2 \equiv 1, 31, 30 \bmod 113,$$

all of which are impossible.

q = 29. For the first pair $(a, b) = (156, 67)$, $w_r \equiv 2 \bmod 5$ for every r, and so (5.4) is impossible.

For the second pair $(a, b) = (61, -4)$, $4 \cdot 29 | w_r$ implies that $r \equiv 10, 68 \bmod 116$. The sequence $\{w_n\} \bmod 233$ is periodic with period 116, so one finds that $w_r \equiv \mp 41 \bmod 233$. Finally, (5.4) says that

$$4 \cdot 29^j x^2 \equiv \pm 41 \bmod 233,$$

which is impossible. This finishes the proof of Theorem 5.3.

Remark. From the proof, one can see that except for $q = 5$, we only needed w_r divisible by q and not q^2. From (5.3) and (5.4), we have $q | w_r$ for $j = 1$ regardless of x. This means that the second equation in the statement of the theorem (i.e., (5.2) with $j = 1$) is impossible for any x, not just those divisible by q.

THEOREM 5.4. *The equation* $y^2 = 4q^m + 4q^2 + 1$ *has no solutions with odd* $m \geq 5$, *if* $q = 23$ *or* 31.

Proof. We write the equation in the form (5.2), with $x = q^k$. Note that $k \geq 1$, since $m \geq 5$.

q = 23. Consider the first pair $(a, b) = (415, 86)$. From (5.3), w_r is even, and this implies r is even, so that $w_r \equiv 1 \bmod 5$. Now (5.3) implies that

$$2 \cdot 23^j x^2 \equiv \pm 1 \bmod 5,$$

which forces $j=1$, so we have $46x^2 = \pm w_r$. The values of $w_r \bmod 47$ are periodic with period 6:

$r \bmod 6$	0	1	2	3	4	5
$w_r \bmod 47$	−8	3	11	8	−3	−11

Since r is even, if $46x^2 = -w_r$, we have $x^2 \equiv -8, 11, -3 \bmod 47$, all of which are impossible. So $46x^2 = +w_r$. Now look at $w_r \bmod 11$:

$r \bmod 10$	0	1	2	3	4	5	6	7	8	9
$w_r \bmod 11$	−2	3	3	−2	0	2	−3	−3	2	0

Since x is a power of 23, $11 \nmid w_r$, so $r \equiv 0, 2, 6, 8 \bmod 10$. If $r \equiv 0, 2 \bmod 10$ then we get $46x^2 \equiv -2, 3 \bmod 11$, a contradiction. If $r \equiv 8 \bmod 10$ then, by (5.5), $w_r \equiv w_8 \bmod u_5$. Now $2351 | u_5$, and $w_8 \equiv -614 \bmod 2351$; one finds that the equation $46x^2 = w_r$ leads to a contradiction mod 2351. We are left with the possibility that $r \equiv 6 \bmod 10$. Looking at $w_r \bmod 3$, we have

$r \bmod 4$	0	1	2	3
$w_r \bmod 3$	−1	−1	1	1

Since $46x^2 = w_r$ and r is even, it must be that $r \equiv 2 \bmod 4$, so $r \equiv 6 \bmod 20$. Then, by (5.6), $w_r \equiv w_6 \bmod v_5$; but $1879 | v_5$ and $w_6 \equiv 506 \bmod 1879$, so one gets a contradiction mod 1879.

Now consider the second pair $(a, b) = (47, -2)$. As for the first pair, one finds that r is even, and $j = 0$ to avoid a contradiction mod 5. Thus (5.3) takes the form $2x^2 = \pm w_r$. The values of $w_r \bmod 11$ are

$r \bmod 10$	0	1	2	3	4	5	6	7	8	9
$w_r \bmod 11$	−4	0	4	5	5	4	0	−4	−5	−5

We have r even and $r \neq 6$, since $11 \nmid x$. Using the fact that $2x^2 = \pm w_r$, we have the possibilities

$$2x^2 = w_r, \qquad r \equiv 2, 4 \bmod 10 \tag{5.7}$$

$$2x^2 = -w_r, \qquad r \equiv 0, 8 \bmod 10. \tag{5.8}$$

If $r \equiv 2 \bmod 10$, then $w_r \equiv w_2 \bmod u_5$, by (5.5), Now $41 | u_5$ and $w_2 \equiv -1 \bmod 41$, so (5.7) implies $2x^2 \equiv -1 \bmod 41$, which is impossible

because x is a power of 23 (that is, no power of 23 is congruent to 20 mod 41). If $r \equiv 4 \bmod 10$ then $w_r \equiv w_4 \bmod u_5$, leading to a contradiction mod 2351 (which divides u_5). If $r \equiv 8 \bmod 10$ then $w_r \equiv w_8 \bmod u_5$, again leading to a contradiction mod 2351. Finally, assume $r \equiv 0 \bmod 10$. Since $23 | w_r$, we have $r \equiv 5 \bmod 23$, and so $r \equiv 120 \bmod 230$. The values of $w_r \bmod 229$ have period 230, and $w_{120} \equiv -91 \bmod 229$. Thus (5.8) implies that $2x^2 \equiv 91 \bmod 229$, a contradiction.

q = 31. Consider the first pair $(a, b) = (993, 178)$. In order to have $2 | w_r$, we need r even. The values of $w_r \bmod 5$ and mod 19 have period 4:

$r \bmod 4$	0	1	2	3
$w_r \bmod 5$	−2	−1	2	1
$w_r \bmod 19$	7	−3	−7	3

If $r \equiv 0 \bmod 4$, then (5.3) implies

$$2 \cdot 31^{j+2k} \equiv \pm(-2) \bmod 5,$$

which shows that the minus sign holds. Then, viewing the same equation mod 19, one sees that $j = 0$; since $31 \equiv -7 \bmod 19$, we have

$$2 \cdot 7^{2k} \equiv -7 \bmod 19,$$

which is impossible since the powers of 7 mod 19 are 1, 7, and 11. In the same way one can eliminate the case $r \equiv 2 \bmod 4$.

Now consider the second pair $(a, b) = (63, 2)$. One finds that w_r divisible by $2 \cdot 31$ implies $r \equiv 52 \bmod 62$. The values of $w_r \bmod 373$ have period $372 = 6 \cdot 62$, so we consider the six cases $r \equiv 52, 114, 176, 230, 300, 362 \bmod 372$. The cases $r \equiv 114, 176, 300$, and 362 all lead to impossible congruences mod 373. The cases $r = 52, 238$ lead to the congruences $31^{2k} \equiv \pm 48, \pm 170 \bmod 373$ (depending on the value of j), all of which are impossible. This completes the proof, and also completes the solution of Eq. (1.3).

REFERENCES

1. F. BEUKERS, On the generalized Ramanujan–Nagell equation I, *Acta Arith.* **38** (1981), 389–410.
2. A. BREMNER *et al.*, Two-weight ternary codes and the equation $y^2 = 4 \cdot 3^a + 13$, *J. Number Theory* **16** (1983), 212–234.
3. A. BREMNER AND P. MORTON, The integer points on three related elliptic curves, *Math. Comp.* **39** (1982), 235–238.

4. R. CALDERBANK, On uniformly packed $[n, n-k, 4]$ codes over $GF(q)$ and a class of caps in $PG(k-1, q)$, *J. London Math. Soc.* (2) **26** (1982), 365–384.
5. P. J. CAMERON, Partial quadrangles, *Quart. J. Math. Oxford* (2) **26** (1975), 61–73.
6. N. TZANAKIS AND J. WOLFSKILL, On the diophantine equation $y^2 = 4q^n + 4q + 1$, *J. Number Theory* **23** (1986), 219–237.
7. N. TZANAKIS, On the diophantine equation $y^2 - D = 2^k$, *J. Number Theory* **17** (1983), 144–164.

Printed in Belgium