JOURNAL OF NUMBER THEORY 23, 219–237 (1986)

# On the Diophantine Equation $y^2 = 4q^n + 4q + 1$

NIKOS TZANAKIS

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

AND

JOHN WOLFSKILL

*Department of Mathematics, Michigan State University, East Lansing, Michigan 48823*

*Communicated by D. J. Lewis*

Received May 23, 1984; revised September 18, 1984

It is known that a certain class of $[n, k]$ codes over $GF(q)$ is related to the diophantine equation $y^2 = 4q^n + 4q + 1$ (*). In Parts I and II of this paper, two different, and in a certain sense complementary, methods of approach to (*) are discussed and some results concerning (*) are given as applications. A typical result is that the only solutions to (*) are $(y, n) = (5, 1)$, $(7, 2)$, $(11, 3)$ when $q = 3$ and $(y, n) = (2q + 1, 2)$ when $q = 3^f$, $f \geqslant 2$. 

## 0. INTRODUCTION

In [6] R. Calderbank relates a certain class of $[n, k]$ codes over $GF(q)$, where $q \neq 2$ is a prime power, to the diophantine equation $y^2 = 4q^{a/2} + 4q + 1$. In this paper, we restrict our attention to the case in which $a$ is even. Renotating, we have

$$y^2 = 4q^n + 4q + 1. \tag{0.1}$$

Calderbank conjectured that his equation has only trivial solutions if $q \neq 2$, 3, or 4. Restricted to (0.1), his conjecture takes the following form:

CONJECTURE (R. Calderbank). *If $q \neq 3$ is a prime power, then the only solution to* (0.1) *is* $(\pm y, n) = (2q + 1, 2)$.

Throughout the paper we will refer to this as "Calderbank's conjecture."



0022-314X/86 $3.00

In general, let $P[a]$ denote the greatest prime dividing the integer $a$. Then, by Theorem 11 of Schinzel [7],

$$\liminf_{y \to \infty} \frac{P[y^2-(4q+1)]}{\log\log y} \geqslant c \tag{0.2}$$

where $c = 2/7$ or $4/7$ according as $4q+1$ is or is not a perfect square. This means that if $[q]$ is bounded, then (0.1) has only a finite number of solutions $(y, n, q)$. However, (0.2) cannot furnish us a practical method for finding the complete solution of (0.1), even in the case that $q$ is a fixed integer $>1$.

A much more practical method is that of Beukers [1, 2]. Beukers' ideas are applied in Part I of this paper to prove that if $q>200$ is a power of a prime $>2$, then (0.1) has at most one solution $(y, n)$ with $n \geqslant 3$ (Theorem I.3). A more precise result is proved when $q$ is a power of 3 (Theorem I.4). This result combined with Theorem II.1 proves that Calderbank's conjecture is true if $q$ is a power of 3 (Corollary 1(ii) to Theorem II.1).

We would like to emphasize the difference of the methods applied in Parts I and II. These methods are complementary and it seems that neither of them alone could prove the validity of Calderbank's conjecture for $q$ a power of 3.

We sketch briefly the method applied in Part I (Beukers' method): There are two key results. One of them is Theorem I.1, which says that any two solutions to (0.1) are widely separated. In particular, since we have the solution $(y, n) = (2q+1, 2)$, one finds that if $n \geqslant 3$, then $n$ must be fairly large ($n \to \infty$ with $q$; see the Corollary to Theorem I.1). The other key result is Theorem I.2, which says that if $p^n$, $n$ odd, is very close to a rational square with small denominator, then one can bound effectively further occurrences $p^{n'}$ with $n' > n$.

In Part II some results are proved for special values of $q$, which, as it seems, cannot be proved by the method of Part I. For example, compare Theorem I.3 when $q = 307$ with the Corollary to Theorem II.3. Note also that although (0.1) is also interesting in the general case, in which $q$ is not necessarily a prime power, the results of Part I do not give any information. On the other hand, the ideas of Part II are applied irrespective of whether $q$ is or is not a prime power (but always for a specified value of $q$). A non-trivial example is given for $q = 21$ (Theorem II.2 and its Corollary).

The method of Part II is that of [9] properly modified and extended. We sketch it in brief: If $q$ is an integer $>1$, not a perfect square, we put

$$q = dQ^2, \qquad d \quad \text{square-free} > 1.$$

In view of the Proposition at the end of this Introduction, we may suppose $n$ odd. On putting

$$n = 4h + 2j + 1, \qquad j \in \{0, 1\}, \tag{0.3}$$

(0.1) is transformed into

$$y^2 - d(2d^jQ)^2 (Q^jq^h)^4 = 4q + 1 \tag{0.4}$$

which is a particular case of

$$y^2 - dx^2 = s, \qquad (x, y) = 1 \tag{0.5}$$

with $s$ odd $> 1$ and $(d, s) = 1$. In Section 1 we express $x$ in (0.5) as $2^\delta x = \pm w_r$, where $\delta = 0$ or 1, according as $d \equiv 2$, 3 or 1 (mod 4) and $w_r$, $r \in \mathbf{Z}$ is a term of a second order recurrence sequence. Then, by (0.4)

$$2^{\delta+1} d^jQ(Q^jq^h)^2 = \pm w_r. \tag{0.6}$$

Working with various moduli and making use of some relations that are proved in Section 2, we can show that a relation of the form

$$2^{\delta+1} d^jQX^2 = \pm w_r \tag{0.7}$$

is either impossible, or that if $X$ is divisible by a specified power of a prime divisor of $q$, it must also be divisible by another prime, not dividing $q$. In the first case (0.6) is impossible, while in the second case we get an upper bound for $h$ in (0.6) and then, by (0.3), an upper bound of $n$. In the examples of the application of this method presented in Section 3, the upper bound of $n$ is either 3 or 5. In various other examples (unpublished) the upper bounds of $n$ were of an analogous size.

Finally, for a general $q$, not necessarily a power of a prime, one can easily prove the following useful

PROPOSITION. (A) *If either $n$ is even or $q$ is a square, then* (0.1) *has no solution with $n > 2$.*

(B) *Suppose that at least one of the following conditions is satisfied:*

(i) $4q + 1 \equiv 0 \pmod p$ for some prime $p \equiv 3 \pmod 4$.

(ii) $q \equiv -1 \pmod p$ for some prime $p$ satisfying $(p/7) = -1$.

(iii) $q \equiv 4$ or $7 \pmod 9$ and $q^2 - q + 1 \equiv 0 \pmod p$ for some prime $p \equiv \pm 2 \pmod 5$.

Then (0.1) has no solution $(y, n)$ with $n$ odd.

One proves (A) by factoring $y^2-4q^n$, and (B) by showing that $4q^n+4q+1$ is a quadratic non-residue modulo $p$. To prove (iii), first note that if $q\equiv 4$ or 7 mod 9 and $n\equiv 1$ or 3 mod 6, then $4q^n+4q+1$ is divisible by 3 but not by 9, so cannot be a square. Finally, if $n\equiv 5 \bmod 6$, then $4q^n+4q+1$ is a quadratic non-residue modulo $p$. With the aid of this Proposition, Calderbank's conjecture can be verified when $q<307$ (only the values $q=27, 73, 127$ are not covered by the Proposition; they can be dealt with by individual congruence arguments). The case $q=307$, as previously was noted, is settled by the Corollary to Theorem II.3.

*Remark.* By Theorem 2 of [8], $X$ in (0.7) is effectively bounded, which means that, in view of (0.6), $h$ and $n$ are effectively bounded. However, the general method of [8] cannot, at present, offer a realistic method for finding all solutions to (0.1).

## PART I. BEUKERS'S METHOD APPLIED TO (0.1)

In what follows, by log we always mean natural logarithm.

LEMMA 1. *If $d\neq 1$ is a positive square-free integer* $\equiv 1 \pmod 4$ *and*

$$\frac{A+B\cdot d^{1/2}}{2}=\left(\frac{p+qB\cdot d^{1/2}}{2}\right)^a$$

*for some integers $A, B, p, q, a, B$ odd $>0$, $a\geqslant 2$, then $a=2$ and $|pq|=1$.*

The proof is very simple, analogous to the proof of Lemma 7 of [1].

THEOREM I.1. *Let $p$ be a prime and $D\equiv 1 \pmod 4$, $D\geqslant 13$ not a square, relatively prime to $p$. If $A^2-D=4p^n$, $A'^2-D=4p^{n'}$ with $n'>n>0$ and $\varepsilon=D/p^n<1/9$, then*

$$n'>\frac{13}{28}(\log D)\,\varepsilon^{-1/2}(1-3\cdot\varepsilon^{1/2}).$$

*More generally, the same inequality holds if $p$ is replaced by $p^f$.*

*Proof.* Write $D=B^2d$ with $d$ square-free ($B>0$). We have

$$\frac{A+B\cdot d^{1/2}}{2}\cdot\frac{A-B\cdot d^{1/2}}{2}=p^n$$

where the two factors on the left are relatively prime because $(D,p)=1$. Let $F=\mathbf{Q}(d^{1/2})$. The relation $A^2-B^2d=4p^n$, $n>0$, implies that if $p$ is an odd

prime, then $(d/p) = 1$ and if $p = 2$ then $d \equiv 1 \bmod 8$. Thus, in $F(p)$ splits into two different prime ideals, so we have the ideal equation

$$\left(\frac{A + B \cdot d^{1/2}}{2}\right) = \mathfrak{P}^n \tag{1.1}$$

where $\mathfrak{P}$ is an ideal of norm $p$. Let $e$ be the least positive integer such that $\mathfrak{P}^e$ is a principal ideal of the order $R = \mathbf{Z}[1, B(1 + d^{1/2})/2]$. Put

$$\mathfrak{P}^e = \left(\frac{\alpha + \beta \cdot d^{1/2}}{2}\right) = (\sigma) \tag{1.2}$$

where $\alpha, \beta$ are relatively prime rational integers and $B \mid \beta$. Clearly, $e \mid n$ and in view of (1.1) and (1.2)

$$\frac{A + B \cdot d^{1/2}}{2} = \pm \theta^r \cdot \sigma^{n/e} \tag{1.3}$$

where $\theta$ is a fundamental unit in $R$ and $r \in \mathbf{Z}$. Considering the conjugate relation of (1.3) and subtracting it from (1.3) gives

$$B \cdot d^{1/2} = |\theta^r \sigma^{n/e} - \tilde{\theta}^r \cdot \tilde{\sigma}^{n/e}|$$

where $\tilde{}$ denotes conjugation. Now

$$|\theta^r \sigma^{n/e}| \geqslant \tfrac{1}{2}(|A| - Bd^{1/2}) = \tfrac{1}{2}[(4p^n + D)^{1/2} - D^{1/2}] > p^{n/2}(1 - \tfrac{1}{2}\varepsilon^{1/2}).$$

Thus

$$\left|\left(\frac{\tilde{\theta}}{\theta}\right)^r \left(\frac{\tilde{\sigma}}{\sigma}\right)^{n/\varepsilon} - 1\right| = Bd^{1/2}|\theta^{-r}\sigma^{-n/e}| < \varepsilon^{1/2}(1 + \varepsilon^{1/2}) < \frac{4}{3}\varepsilon^{1/2}$$

as $\varepsilon < 1/9$. Put $x = (\tilde{\theta}/\theta)^r(\tilde{\sigma}/\sigma)^{n/e}$. Since, in general, $|\delta| < 1/2$ implies $|\log(1 - \delta)| < |\delta|(1 + |\delta|)$, it follows that

$$\left|-r \log\left|\frac{\theta}{\tilde{\theta}}\right| + \frac{n}{e} \log\left|\frac{\tilde{\sigma}}{\sigma}\right|\right|$$

$$= |\log|x|| < \varepsilon^{1/2}(1 + \varepsilon^{1/2})\left(1 + \frac{4}{3}\varepsilon^{1/2}\right) < \varepsilon^{1/2}(1 + 3\varepsilon^{1/2}). \tag{1.4}$$

Now work with $A'^2 - D = p^{n'}$ the same way to obtain

$$\left|-r' \log\left|\frac{\theta}{\tilde{\theta}}\right| + \frac{n'}{e} \log\left|\frac{\tilde{\sigma}}{\sigma}\right|\right| < \varepsilon'^{1/2}(1 + 3\varepsilon'^{1/2}) < \varepsilon^{1/2}(1 + 3\varepsilon^{1/2}) \tag{1.5}$$

where $\varepsilon' = D/p^{n'}$ and $r'$ is some rational integer. Now put $u = |\log|\theta/\tilde{\theta}|\,|$ and eliminate $\log|\tilde{\sigma}/\sigma|$ in (1.4) and (1.5) to get

$$|-rn' + r'n| < \frac{2n'}{u}\varepsilon^{1/2}(1 + 3\varepsilon^{1/2}). \tag{1.6}$$

We claim that $r/n \neq r'/n'$. Indeed, the contrary implies $r = ar_1$, $n/e = an_1/e$ and $r' = br_1$, $n'/e = bn_1/e$, where $(r_1, n_1/e) = 1$ and $a$, $b$ are positive integers. Thus

$$\frac{A + B\cdot d^{1/2}}{2} = \pm(\theta^{r_1}\sigma^{n_1/e})^a \qquad \text{and} \qquad \frac{\pm A' + B\cdot d^{1/2}}{2} = \pm(\theta^{r_1}\sigma^{n_1/e})^b \tag{1.7}$$

where $\mathfrak{P}^{n'} = ((\pm A' + Bd^{1/2})/2)$. This relation together with (1.1) and the fact that $n' > n$ shows that $a \neq b$. On the other hand, by Lemma 1, $a, b \in \{1, 2\}$, so that one among $a$, $b$ equals 1 and the other equals 2. Then, by (1.7) and Lemma 1, either $\pm A$ or $\pm A'$ is 1, clearly impossible. Hence $r/n \neq r'/n'$ and so $|-rn' + r'n| \geqslant 1$. Then, by (1.6),

$$n' > \frac{u}{2}\varepsilon^{-1/2}(1 + 3\varepsilon^{1/2})^{-1} > \frac{u}{2}\varepsilon^{-1/2}(1 - 3\varepsilon^{1/2}). \tag{1.8}$$

Now we get a lower bound for $u = |\log|\theta/\tilde{\theta}|\,| = 2|\log|\theta|\,| = 2|\log|\tilde{\theta}|\,|$ (since $\theta\tilde{\theta} = \pm 1$). Let $\theta = (\zeta + \eta d^{1/2})/2$ with $B|\eta$. We have $\frac{1}{2}(|\zeta| + |\eta|d^{1/2}) = |\theta|$ or $|\tilde{\theta}|$ according as $\zeta n$ is $>0$ or $<0$. In either case

$$u = 2\cdot\log\left(\frac{1}{2}(|\zeta| + |\eta|\cdot d^{1/2})\right) \geqslant 2\log\frac{(D-4)^{1/2} + D^{1/2}}{2} \geqslant \frac{13}{14}\log D,$$

since $D \geqslant 13$. This, combined with (1.8), proves the inequality in the statement of the theorem. Finally, if $p$ is replaced by $p^f$, the same proof applies, with $n$ and $n'$ replaced by $fn$ and $fn'$. But $f$ divides out in (1.6), leading to the same inequality (1.8).

COROLLARY. *Let $q > 200$ be a power of a prime and suppose that $y^2 = 4q^n + 4q + 1$ with $n$ odd $\geqslant 3$. Then*

$$n > \frac{2}{15}q^{1/2}\log 4q.$$

*In particular, $n \geqslant 13$.*

*Proof.* Apply Theorem I.1 with the two solutions

$$(2q+1)^2 = 4q^2 + D, \qquad y^2 = 4q^n + D, \qquad D = 4q + 1.$$

Here $\varepsilon = (4q+1)\,q^{-2} < 1/9$; therefore

$$n > \frac{13}{28}(\log 4q)\,q(4q+1)^{-1/2}\left[1 - \frac{3}{q}(4q+1)^{1/2}\right]$$

$$= (q^{1/2}\log 4q)\left[\frac{13}{28}\left(\frac{q}{4q+1}\right)^{1/2}\left(1 - \frac{3}{q}(4q+1)^{1/2}\right)\right]$$

and the factor in the square brackets is $>2/15$. This completes the proof.

In what follows we need some properties of the hypergeometric functions. A hypergeometric function $F(\alpha, \beta, \gamma, z)$ is defined by the series

$$1 + \frac{\alpha\cdot\beta}{1\cdot\gamma}z + \frac{\alpha(\alpha+1)\,\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)}z^2 + \cdots$$

which converges for $|z|<1$ and for $z=1$ if $\gamma - \alpha - \beta > 0$. The following properties are needed (see [1]). Let $n_1, n_2 > 0$ be integers with $n_2 > n_1$ and put $n = n_1 + n_2$. Define $G(z) = F(-n_2 - 1/2,\ -n_1,\ -n,\ z)$, $H(z) = F(-n_1 + 1/2,\ -n_2,\ -n,\ z)$. Then

1. $G(z)$, $H(z)$ are polynomials of degrees $n_1$ and $n_2$, respectively, and, moreover, $\binom{n}{n_1}G(4z)$, $\binom{n}{n_1}H(4z)$ have integral coefficients.
2. $|G(z) - H(z)\cdot(1-z)^{1/2}| < G(1)\cdot|z|^{n+1}$ for $|z|<1$.
3. $G(1) < G(z) < G(0) = 1$ for $0 < z < 1$.
4. $\binom{n}{n_1}G(1) = \prod_{m=1}^{n_1}(1 - 1/2m) < \frac{1}{2}$ $\quad (n_1 \geqslant 1)$.
5. If $G^*(z)$ is the polynomial resulting from $G(z)$ when $n_1, n_2$ are replaced by $n_1+1$, $n_2+1$, respectively, and $H^*(z)$ is defined analogously, then

$$G^*(z)\cdot H(z) - G(z)\cdot H^*(z) = c\cdot z^{n+1}$$

for some non-zero constant $c$.

In the proof of Theorem I.2 we shall refer to these properties.

THEOREM I.2. *Let $p>0$ be an integer, not a square ($p$ does not have to be prime). Assume $x^2 + D = a^2 w$, where $w$ is an odd power of $p$ and $a$ is a positive integer. Let $r$, $s$ be positive integers such that*

$$a^2 w \geqslant |D|^{2+s/r}\cdot 4^{1+s/r}$$

*and define $v$ by*

$$w^v = 9a^2(81a^2 w/4)^{r/s}.$$

*Let $N > w$ be an odd power of $p$ and $y$ any integer. Then*

$$\left|\frac{y}{2N^{1/2}} - 1\right| > \frac{8}{2187a^5w^{3+v/2}}\left(\frac{81a^2w}{4}\right)^{1/s} N^{-(1+v)/2}.$$

*Proof.* Let $H(z)$, $G(z)$ be defined as before ($n_1$, $n_2$ will be determined later, so that $n_2 > n_1 > 0$). Note that $|D/a^2w| < 1$. Define $A$, $B$ by

$$\binom{n}{n_1} G\left(\frac{D}{a^2w}\right) = \frac{A}{(4a^2w)^{n_1}}, \qquad \binom{n}{n_1} H\left(\frac{D}{a^2w}\right) = \frac{B}{(4a^2w)^{n_2}}$$

so that, by property 1, $A, B \in \mathbf{Z}$.

By definition

$$G(z) = \sum_{k=0}^{n_1} \binom{n_2 + 1/2}{k}\binom{n_1}{k}\binom{n}{k}^{-1}(-z)^k. \tag{1.9}$$

Now $n = n_1 + n_2 > 2n_1$ implies $\binom{n}{k} > 2^k\binom{n_1}{k}$; therefore

$$\begin{aligned} |G(z)| &< \sum_{k=0}^{n_1} \binom{n_2 + 1/2}{k}\left(\frac{|z|}{2}\right)^k < \sum_{k=0}^{n_2+1} \binom{n_2+1}{k}\left(\frac{|z|}{2}\right)^k \\ &= \left(1 + \frac{|z|}{2}\right)^{n_2+1}. \end{aligned} \tag{1.10}$$

From (1.9) it is clear that $G(z) > 0$ if $z < 0$. If $0 < z < 1$ then, by properties 3 and 4, $G(z) > 0$. Thus $A > 0$. Applying now property 2 for $z = D/a^2w$ and multiplying by $\binom{n}{n_1}$ we get

$$\left|1 - \frac{xB}{aAw^{1/2}} \cdot \frac{1}{(4a^2w)^{n_2 - n_1}}\right| < \frac{1}{2} \cdot \frac{|D|^{n+1}}{A} \cdot \frac{4^{n_1}}{(a^2w)^{n_2+1}}.$$

Let $|-1 + y/2N^{1/2}| = \varepsilon$. Adding, we see that

$$K = \left|\frac{y}{2N^{1/2}} - \frac{xB}{aAw^{1/2}} \cdot \frac{1}{(4a^2w)^{n_2-n_1}}\right| < \varepsilon + \frac{1}{2} \cdot \frac{|D|^{n+1}}{A} \cdot \frac{4^{n_1}}{(a^2w)^{n_2+1}}. \tag{1.11}$$

Define the positive integer $\lambda$ by the relation

$$w^{\lambda - 1} < (N/w)^{1/2} \leqslant w^{\lambda}$$

(note that each term is a power of $p$ with non-negative integral exponent). Now we choose $n_1$ so that

$$\frac{r}{s}\lambda \leqslant n_1 \leqslant \frac{r}{s}\lambda + \frac{2s-1}{s} \tag{1.12}$$

and we set

$$n_2 = n_1 + \lambda > n_1, \qquad n = n_1 + n_2 = 2n_1 + \lambda.$$

Note that (1.12) is satisfied by two (consecutive) values of $n_1$ and the polynomials $G$ and $H$ corresponding to the greater value of $n_1$ are $G^*$ and $H^*$, respectively (cf. property 5). If for both values of $n_1$ the corresponding $K$'s in (1.11) are zero, then it is easy to see that $(G \cdot H^* - G^* \cdot H)(D/a^2 w) = 0$ and this contradicts property 5. Thus, we can select $n_1$ so that $K \neq 0$. Now $aAw^{1/2}(4a^2w)^{n_2 - n_1} = aAw^{1/2}(4a^2w)^{\lambda} = 2N^{1/2} \cdot$ integer, by the definition of $\lambda$. Hence $K \geqslant (aAw^{1/2})^{-1}(4a^2w)^{-\lambda}$ and, in view of (1.11),

$$1 < \varepsilon aAw^{1/2}(4a^2w)^{\lambda} + \tfrac{1}{2}aw^{1/2}|D|^{n+1} \cdot 4^{n_2}(a^2w)^{-n_1 - 1}. \tag{1.13}$$

The second term in the right-hand side is $(|D|/2aw^{1/2}) \cdot |D|^{2n_1 + \lambda} \cdot 4^{n_1 + \lambda}(a^2w)^{-n_1}$ and in view of (1.12) this is

$$\leqslant \frac{|D|}{2aw^{1/2}} \left( \frac{|D|^{2 + s/r} \cdot 4^{1 + s/r}}{a^2 w} \right)^{n_1} \leqslant \frac{|D|}{2aw^{1/2}}$$

by the hypotheses of the theorem. Also, $aw^{1/2} > 2|D|$, so the second term in the right-hand side of (1.13) must be $< 1/4$. Hence

$$\frac{3}{4} < \varepsilon aAw^{1/2}(4a^2w)^{\lambda} = \varepsilon aw^{1/2}(4a^2w)^{n_2} \cdot \binom{n}{n_1} \cdot G\left(\frac{D}{a^2w}\right).$$

On the other hand, by (1.10)

$$\binom{n}{n_1} G\left(\frac{D}{a^2w}\right) < 2^{n-1}\left(1 + \frac{D}{2a^2w}\right)^{n_2 + 1} < 2^{n-1}\left(\frac{9}{8}\right)^{n_2 + 1} \leqslant \frac{1}{2}\left(\frac{9}{4}\right)^{n}$$

so that we have

$$\frac{3}{4} < \varepsilon aw^{1/2}(4a^2w)^{n_2} \cdot \frac{1}{2}\left(\frac{9}{4}\right)^{n} = \frac{\varepsilon aw^{1/2}}{2} \cdot (4a^2w)^{n_1 + \lambda}\left(\frac{9}{4}\right)^{2n_1 + \lambda}$$

$$< \frac{1}{2}\varepsilon aw^{1/2}(4a^2w)^{(2s-1)/s} \cdot \left(\frac{9}{4}\right)^{(4s-2)/s}\left[(4a^2w)^{1 + r/s} \cdot \left(\frac{9}{4}\right)^{1 + 2r/s}\right]^{\lambda}$$

in view of (1.12). The quantity in the square brackets is $9a^2w \cdot w^{r/s}(81a^2/4)^{r/s} = w^{1+\nu}$, by the definition of $\nu$. So, $\frac{3}{2} < \varepsilon aw^{1/2}(81a^2w/4)^{(2s-1)/s} \cdot w^{\lambda(1+\nu)} < \varepsilon aw^{1/2}(6561a^4w^2/16)(81a^2w/4)^{-1/s}(Nw)^{(1+\nu)/2}$ by the definition of $\lambda$. Hence,

$$\frac{8}{2187}\, a^{-5} w^{-5/2}(81a^2w/4)^{1/s} < \varepsilon(Nw)^{(1+\nu)/2},$$

i.e.,

$$\left|\frac{y}{2N^{1/2}}-1\right|=\varepsilon>\frac{8}{2187}\,a^{-5}w^{-3-v/2}(81a^2w/4)^{1/s}N^{-(1+v)/2},$$

which completes the proof of the theorem.

THEOREM I.3. *Let $p$ be a prime and $q=p^f>200$. Then the diophantine equation $y^2=4q^n+4q+1$, $y>0$, $n\geqslant 3$ can have at most one solution.*

*Proof.* By the Proposition of the Introduction we may suppose that $f, n$ are odd. Now we suppose that there are two solutions and derive a contradiction.

Assume $y_1^2=4q^n+4q+1$ and $y_2^2=4q^{n'}+4q+1$ with $n'>n$ ($n'$ odd). We apply Theorem I.2 with $a=2$, $w=q^n$, $D=-(4q+1)$; so $|D|<801q/200$, as $q>200$. By the Corollary to Theorem I.1, $n>(2/15)\,q^{1/2}\log 4q$ and now a simple calculation shows that on applying Theorem I.2 we can take $(r, s)=(1, 6)$, so that $v<1/4$ and, consequently, for $N=q^{n'}$ we have

$$\frac{y_2}{2N^{1/2}}-1>\frac{1}{4}\cdot 3^{-19/3}w^{-71/24}\cdot N^{-5/8}. \tag{1.14}$$

Now

$$\frac{4q+1}{8N}=\frac{1}{2}\left(\frac{y_2}{2N^{1/2}}+1\right)\left(\frac{y_2}{2N^{1/2}}-1\right)>\frac{y_2}{2N^{1/2}}-1$$

and this combined with (1.14) implies

$$N^{3/8}<\frac{1}{2}\left(3^{19/3}\cdot w^{71/24}\cdot\frac{801}{200}q\right)<3^7\cdot q^{1+71n/24}.$$

Hence

$$\frac{3}{8}n'<\frac{7\log 3}{\log q}+1+\frac{71n}{24}<\frac{71n}{24}+\frac{5}{2}$$

since $q>200$. Thus

$$n'<\frac{71n}{9}+\frac{20}{3}<9n \tag{1.15}$$

since, by the Corollary to Theorem I.1, $n\geqslant 13$. But Theorem I.1 implies that

$$n'>\frac{13}{28}(\log(4q+1))\left(\frac{q^n}{4q+1}\right)^{1/2}\left[1-3\left(\frac{4q+1}{q^n}\right)^{1/2}\right]$$

and the right-hand side, as is easily seen, is $> \frac{3}{2}q^{(n-1)/2}$. Thus, in view of (1.15), $9n > \frac{3}{2}q^{(n-1)/2}$, which is a contradiction.

THEOREM I.4. *Let $q = 3^f$. Then $y^2 = 4q^n + 4q + 1$ is impossible if $f > 9$ and $n \geqslant 3$.*

*Proof.* By the Proposition of the Introduction, we may suppose that $f$ and $n$ are odd. Suppose that $f \geqslant 11$ and let $(y, n)$ be a solution of $y^2 = 4 \cdot 3^{nf} + 4 \cdot 3^f + 1$ with $y > 0$ and $n \geqslant 3$. We have $3788^2 - 37 = 3^{15}$; therefore we can apply Theorem I.2 with $a = 1$, $w = 3^{15}$, $D = -37$, $(r, s) = (2, 3)$, so that $v < 14/15$ and, consequently, for $N = 3^{nf}$ we have

$$\frac{y}{2 \cdot N^{1/2}} - 1 > \frac{1}{N^{29/30}} \cdot \frac{8}{2187 \cdot 3^{45+7}} \left(\frac{3^{19}}{4}\right)^{1/3}. \tag{1.16}$$

On the other hand

$$\frac{4 \cdot 3^f + 1}{8N} = \frac{y^2 - 4N}{8N} > \frac{y}{2N^{1/2}} - 1,$$

which combined with (1.16) implies $N^{1/30} < 3^{f + 152/3}$, i.e.,

$$(n - 30) \cdot f < 1520. \tag{1.17}$$

Now, by the Corollary to Theorem I.1, $n > (2/15)\, 3^{f/2} \log(4 \cdot 3^f)$ and since $f \geqslant 11$, this implies $n - 30 > 2f \cdot 3^{f/2}/15$, which contradicts (1.17).

## PART II. AN ALTERNATIVE APPROACH TO (0.1)

### 1. ON THE SOLUTION OF $y^2 - dx^2 = s$

Consider the diophantine equation

$$y^2 - dx^2 = s, \qquad (x, y) = 1 \tag{2.1}$$

where $d > 1$ is a square-free integer, $s$ is odd $> 1$ and $(d, s) = 1$. It is the purpose of this section to express $x$ as a term of a second order recurrence sequence.

We put $\theta = d^{1/2}$ and work in $\mathbf{Q}(\theta)$. For every $\alpha \in \mathbf{Q}(\theta)$ we denote by $\alpha'$ its algebraic conjugate. Let $D$ be the discriminant of this field. It is well known that $D = d$ or $4d$ according as $d \equiv 1$ or 2, 3 (mod 4). In view of the restrictions on $d$ and $s$, for every prime $p$ dividing $s$ we have $(p, 2D) = 1$ and from (2.1), $(d/p) = 1$, so that [5, Chap. 3, Sect. 8, Theorem 1] in $\mathbf{Q}(\theta)$ $p = \mathfrak{P}_1 \mathfrak{P}_2$, where $\mathfrak{P}_1 \neq \mathfrak{P}_2$ are prime ideals. These are called conjugate ideals.

Now we write (2.1) as $(y+\theta x)(y-\theta x)=s$, where the factors in the left-hand side are, clearly, relatively prime. Therefore, if $s=p_1\cdots p_m$ is the decomposition of $s$ into rational primes (the $p_i$'s are not necessarily distinct) and we put $p_i=\mathfrak{P}_{i1}\mathfrak{P}_{i2}$, then we have an ideal equation

$$(y+\theta x)=\mathfrak{A}, \qquad \mathfrak{A}\in A \tag{2.2}$$

where $A$ is the set of all ideals of the form $\mathfrak{P}_{1j_1}\cdots\mathfrak{P}_{mj_m}$, with $j_1,\ldots,j_m\in\{1,2\}$. But if $\mathfrak{A}\in A$, then its conjugate, say $\mathfrak{A}'$, which results on replacing the $\mathfrak{P}_{ij}$'s by their conjugates, is different from $\mathfrak{A}$ and also belongs to $A$. Therefore we can write $A=A_1\cup A_2$, where $A_1$ is a set of $2^{m-1}$ pairwise distinct and non-conjugate ideals $\mathfrak{A}$ and $A_2$ is the set of the ideals conjugate to those of $A_1$. Since from (2.2) $\mathfrak{A}$ is a principal ideal, it follows that we can find an algebraic integer $\sigma\in\mathbf{Q}(\theta)$ such that $\mathfrak{A}=(\sigma)$. Then, to different $\mathfrak{A}$'s correspond non-associate $\sigma$'s and also $\mathfrak{A}'=(\sigma')$. In conclusion, (2.2) is equivalent to

$$(y+\theta x)=(\sigma) \text{ or } (\sigma'), \qquad \sigma\in S \tag{2.3}$$

where $S$ is a complete system of pairwise non-conjugate and non-associate integers of $\mathbf{Q}(\theta)$ having norm equal to $s$.

Now consider $(y+\theta x)=(\sigma)$. If $\varepsilon$ is the fundamental unit in $\mathbf{Q}(\theta)$, then $y+\theta x=\pm\varepsilon^r\cdot\sigma$, $r\in\mathbf{Z}$ and subtracting from this its conjugate relation gives

$$2\theta x=\pm(\sigma\cdot\varepsilon^r-\sigma'\cdot\varepsilon'^r), \qquad r\in\mathbf{Z}. \tag{2.4}$$

If in (2.3) we consider $\sigma'$ instead of $\sigma$, then we get $2\theta x=\pm(\sigma'\cdot\varepsilon^r-\sigma\cdot\varepsilon'^r)$ and since $\varepsilon'=\pm\varepsilon^{-1}$, we find that $x=\pm(\sigma\varepsilon^{-r}-\sigma'\varepsilon'^{-r})$. Therefore, it suffices to consider (2.3) with $\sigma$ only.

DEFINITION. If $(x, y)$ is a solution of (2.1) and $(y+\theta x)=(\sigma)$, where $\sigma$ is as in (2.3), then we say that the solution $(x, y)$ is generated by $\sigma$. If we replace $\sigma$ by any of its associates, then exactly the same solution $(x, y)$ of (2.1) will be generated.

Now we put

$$\varepsilon+\varepsilon'=E\in\mathbf{Z}, \qquad \varepsilon\varepsilon'=J=\pm1$$

and for every integer $n$,

$$u_n=(\varepsilon^n-\varepsilon'^n)/(\varepsilon-\varepsilon'), \qquad v_n=\varepsilon^n+\varepsilon'^n.$$

Then,

$$\begin{aligned} &u_0=0, \quad u_1=1, \quad u_{n+2}=Eu_{n+1}-Ju_n, \quad u_{-n}=-J^nu_n \\ &v_0=2, \quad v_1=E, \quad v_{n+2}=Ev_{n+1}-Jv_n, \quad v_{-n}=J^nv_n. \end{aligned} \tag{2.5}$$

(A) Let $d \equiv 2, 3 \pmod 4$. In this case we put

$$\varepsilon = e + f\theta, \qquad \sigma = a + b\theta, \qquad a, b, e, f \in \mathbf{Z}$$

so that

$$E = 2e, \qquad \theta = (\varepsilon - \varepsilon')/2f.$$

Then, from (2.4)

$$\begin{aligned} \pm(\varepsilon - \varepsilon')\, x/f &= \varepsilon^r(a + b\theta) - \varepsilon'^r(a - b\theta) = a(\varepsilon^r - \varepsilon'^r) + b\theta(\varepsilon^r + \varepsilon'^r) \\ &= \frac{a}{2e}(\varepsilon + \varepsilon')(\varepsilon^r - \varepsilon'^r) + \frac{b}{2f}(\varepsilon - \varepsilon')(\varepsilon^r + \varepsilon'^r) \\ &= \left(\frac{a}{2e} + \frac{b}{2f}\right)(\varepsilon^{r+1} - \varepsilon'^{r+1}) + \left(\frac{a}{2e} - \frac{b}{2f}\right) J(\varepsilon^{r-1} - \varepsilon'^{r-1}), \end{aligned}$$

i.e.,

$$\pm x = \frac{af + be}{2e} u_{r+1} + J\frac{af - be}{2e} u_{r-1}. \tag{2.6}$$

For every $n \in \mathbf{Z}$ we put

$$w_n = \frac{af + be}{2e} u_{n+1} + J\frac{af - be}{2e} u_{n-1} \tag{2.7}$$

where, in view of (2.5),

$$w_0 = b, \qquad w_1 = af + be, \qquad w_{n+2} = Ew_{n+1} - Jw_n. \tag{2.8}$$

Thus, (2.6) is equivalent to

$$x = \pm w_r, \qquad \text{for some } r \in \mathbf{Z}. \tag{2.9}$$

(B) Let $d \equiv 1 \pmod 4$. In this case the ring of integers in $\mathbf{Q}(\theta)$ is $\mathbf{Z}[\omega]$, where $\omega = (1 + \theta)/2$, $\omega' = 1 - \omega$ and we put

$$\varepsilon = e + f\omega, \qquad \sigma = a + b\omega, \qquad a, b, e, f \in \mathbf{Z}$$

so that

$$E = 2e + f, \qquad \theta = (\varepsilon - \varepsilon')/f.$$

Then, from (2.4)

$$\pm 2(\varepsilon-\varepsilon')\,x/f=\varepsilon^r(a+b\omega)-\varepsilon'^r(a+b\omega')=a(\varepsilon^r-\varepsilon'^r)+b(\omega\varepsilon^r-\omega'\varepsilon'^r)$$
$$=a(\varepsilon^r-\varepsilon'^r)+b[\omega(\varepsilon^r+2\varepsilon'^r)-(2\omega+\omega')\,\varepsilon'^r]$$
$$=a(\varepsilon^r-\varepsilon'^r)+b\frac{1+\theta}{2}(\varepsilon^r+2\varepsilon'^r)-b\frac{3+\theta}{2}\varepsilon'^r$$
$$=\left(a+\frac{b}{2}\right)(\varepsilon^r-\varepsilon'^r)+\frac{b}{2}\theta(\varepsilon^r+\varepsilon'^r)$$
$$=\frac{2a+b}{2(2e+f)}(\varepsilon+\varepsilon')(\varepsilon^r-\varepsilon'^r)+\frac{b}{2f}(\varepsilon-\varepsilon')(\varepsilon^r+\varepsilon'^r)$$
$$=\frac{af+be+bf}{(2e+f)f}(\varepsilon^{r+1}-\varepsilon'^{r+1})+J\frac{af-be}{(2e+f)f}(\varepsilon^{r-1}-\varepsilon'^{r-1}),$$

i.e.,

$$\pm 2x=\frac{af+be+bf}{2e+f}u_{r+1}+J\frac{af-be}{2e+f}u_{r-1}. \tag{2.6'}$$

If for every $n\in\mathbf{Z}$ we put

$$w_n=\frac{af+be+bf}{2e+f}u_{n+1}+J\frac{af-be}{2e+f}u_{n-1} \tag{2.7'}$$

we have

$$w_0=b, \qquad w_1=af+be+bf, \qquad w_{n+2}=Ew_{n+1}-Jw_n \tag{2.8'}$$

and (2.6′) is equivalent to

$$2x=\pm w_r \qquad \text{for some } r\in\mathbf{Z}. \tag{2.9'}$$

## 2. Some Useful Congruences

From the identity

$$\varepsilon^{n+2m}-\varepsilon'^{n+2m}=J^m(\varepsilon^n-\varepsilon'^n)+(\varepsilon^{n+m}+\varepsilon'^{n+m})(\varepsilon^m-\varepsilon'^m)$$

we get $u_{n+2m}\equiv J^m u_n \pmod{u_m}$ and then, inductively,

$$u_{n+2mt}\equiv J^{mt}u_n \qquad (\mathrm{mod}\ u_m).$$

The last relation together with (2.7) and (2.7′) implies

$$w_{n+2mt}\equiv J^{mt}w_n \qquad (\mathrm{mod}\ u_m). \tag{2.10}$$

Analogously, starting from the identity

$$\varepsilon^{n+2m} - \varepsilon'^{n+2m} = -J^m(\varepsilon^n - \varepsilon'^n) + (\varepsilon^{n+m} - \varepsilon'^{n+m})(\varepsilon^m + \varepsilon'^m)$$

we get

$$w_{n+2mt} \equiv (-1)^t J^{mt} w_n \pmod{v_m}. \tag{2.11}$$

## 3. Applications

THEOREM II.1. *Let $s$ be an odd number $>1$, prime to 3. Consider the diophantine equation*

$$y^2 - 4 \cdot 3^{2j+1} x^4 = s, \qquad j \in \{0, 1\}, (x, y) = 1. \tag{2.12}$$

*Keeping the notations of Section* 1, *we have the following results*:

(i) *For every $\sigma \in S$ there exists exactly one $k = k(\sigma) \in [0, 17]$ such that*

$$b_k = au_k + \tfrac{1}{2}bv_k \equiv 0 \pmod{18}.$$

(ii) *Let $P_1 = \{5, 17, 53\}$, $P_2 = \{13, 37, 73\}$. If there exists a $p \in P_1 \cup P_2$ such that $p \mid b_k$, then every solution $(x, y)$ of* (2.12) *generated by $\sigma$, such that $3 \mid x$, also satisfies $p \mid x$.*

(iii) *If there exists a $p \in P_1$ (resp. $p \in P_2$) such that $b_k \not\equiv 0 \pmod{p}$ and $((3^j b_k/2)/p) = -1$ (resp. $((b_k/2)/p) = -1$), then no solution $(x, y)$ of* (2.12) *generated by $\sigma$ exists, such that $3 \mid x$.*

*Proof.* Note that (2.12) is written $y^2 - 3(2 \cdot 3^j x^2)^2 = s$, which is of the form (2.1). We refer to Section 1, case A. Now

$$d = 3, \qquad e = 2, \qquad f = 1, \qquad E = 4, \qquad J = 1.$$

In view of the relations $(\varepsilon - \varepsilon')\, u_n = \varepsilon^n - \varepsilon'^n$, $v_n = \varepsilon^n + \varepsilon'^n$, we have $\varepsilon^n = u_n\theta + v_n/2$, so that

$$\begin{aligned}(a + b\theta)\, \varepsilon^n &= (\tfrac{1}{2}av_n + 3bu_n) + (au_n + \tfrac{1}{2}bv_n)\, \theta \\ &= (\text{by definition})\, a_n + b_n\theta.\end{aligned}$$

It is easily checked that the values of $b_n \pmod{18}$ form a periodic sequence with period 18 and the values of this period form a complete system of residues mod 18. This proves (i).

Now, since $\sigma$ and $\sigma_k = a_k + b_k\theta$ are associates, it follows that in the dis-

cussion of Section 1, case A, we can take $\sigma_k$ instead of $\sigma$ (cf. the Definition in Section 1). In view of (2.9),

$$2 \cdot 3^j x^2 = \pm w_r \tag{2.13}$$

where, by (2.8), $w_0 = b_k$, $w_1 = a_k + 2b_k$. As is easily seen, the values of $w_r$ (mod 18) form a periodic sequence of order 18, and the values of the period form a complete system of residues mod 18. Therefore, if $3 \mid x$, then by (2.13), $w_r \equiv 0 \pmod{18}$ and consequently $r \equiv 0 \pmod{18}$. But then from (2.10) and (2.11) we get, respectively,

$$2 \cdot 3^j x^2 = \pm w_r \equiv \pm w_0 = \pm b_k \qquad (\text{mod } u_9) \tag{2.14}$$

$$2 \cdot 3^j x^2 \equiv \pm b_k \qquad (\text{mod } v_9). \tag{2.14'}$$

Since $p \mid u_9$ for every $p \in P_1$ and $p \mid v_9$ for every $p \in P_2$, (2.14) and (2.14') clearly imply (ii) and (iii), respectively.

This completes the proof.

COROLLARY 1. (i) *The only solutions to* $y^2 = 4 \cdot 3^n + 13$ *are* $(\pm y, n) = (5, 1), (7, 2), (11, 3)$.

(ii) *Calderbank's conjecture is true for* $q = 3^f$.

*Proof.* By A of the Proposition in the Introduction and Theorem I.4 it suffices to consider only the values $q = 3, 3^3, 3^5, 3^7, 3^9$. Since $3^5 \equiv -1 \pmod{61}$, $3^9 \equiv -1 \pmod{19}$ and $(61/7) = (19/7) = -1$ it follows by B(ii) of the same Proposition that only the values $q = 3, 3^3, 3^7$ have to be considered. In the notation of Theorem II.1 we have the following table:

| $q$ | $a$ | $b$ | $k$ | $b_{k/2} \equiv r_k \pmod{p}$ |
|---|---|---|---|---|
| 3 | 4 | 1 | 7 | 18 (mod 37) |
| $3^3$ | 28 | 15 | 3 | 2 (mod 13) |
| $3^7$ | 107 | 30 | 12 | 2 (mod 13) |
| | 101 | 22 | 2 | 6 (mod 13) |

where $a$, $b$ correspond to all possible $\sigma = a + b \cdot 3^{1/2} \in S$ (cf. (2.3)). Since $(r_k/p) = -1$ in all cases above, (iii) of Theorem II.1 applies to show that the diophantine equation

$$y^2 - 4 \cdot 3^{2j+1} x^4 = 4 \cdot 3^m + 1, \qquad j \in \{0, 1\}, \qquad m \in \{1, 3, 7\}$$

with $(x, y) = 1$ and $3 \mid x$ is impossible. Now the proof follows at once.

*Remark.* $y^2 = 4 \cdot 3^n + 13$ has been solved previously by A. Bremner and P. Morton [3] and A. Bremner *et al.* [4]. Note that here we have, in fact, proved a more general result, namely that each of the diophantine equations $y^2 - 12x^4 = 13$ and $y^2 - 108x^4 = 13$ is impossible if $3 \mid x$.

Another example of an application of Theorem II.1, not related to Calderbank's conjecture, is given by the following result.

COROLLARY 2. *The only solutions of* $y^2 = 4 \cdot 3^n + 517$ *are* $(\pm y, n) = (23, 1), (25, 3), (29, 4)$.

*Proof.* If $n$ is even, then it is easily seen that $n = 4$. Therefore let $n = 4N + 2j + 1$, $j \in \{0, 1\}$, so that our equation becomes

$$y^2 - 4 \cdot 3^{2j+1}(3^N)^4 = 517$$

which is of the form (2.12). In the notation of Theorem II.1 we have $\sigma = 25 + 6 \cdot 3^{1/2}$ or $23 + 2 \cdot 3^{1/2}$ with $k = 12$ or 10, respectively. Since $53 \mid b_{12}$ and $13 \mid b_{10}$, (ii) of this Theorem applies to show that $N = 0$ and this completes the proof.

An interesting application of the method of Section 1 to (0.1) when $q$ is not a prime power is given by the following

THEOREM II.2. *The diophantine equation*

$$y^2 - 4 \cdot 21^{2j+1}x^4 = 85 \tag{2.15}$$

*is impossible if* $j = 0$ *and* $x \equiv 0 \pmod 9$ *or if* $j = 1$.

*Proof.* We write (2.15) in the form $y^2 - 21(2 \cdot 21^j x^2)^2 = 85$, so that the results of Section 1, case B, can be applied. Now

$$d = 21, \qquad e = 2, \qquad f = 1, \qquad E = 5, \qquad J = 1$$

and the set $S$ in (2.3) has the two elements $9 + \omega$, $10 + 3\omega$ ($\omega = (1 + 21^{1/2})/2$). Therefore, by (2.8′), either

$$a = 9, \qquad b = 1, \qquad w_0 = 1, \qquad w_1 = 12 \tag{2.16}$$

or

$$a = 10, \qquad b = 3, \qquad w_0 = 3, \qquad w_1 = 19 \tag{2.17}$$

and in both cases (cf. (2.9′))

$$21^j(2x)^2 = \pm w_r \qquad \text{for some } r \in \mathbf{Z}. \tag{2.18}$$

Consider first (2.16). If $j = 1$, then $w_r \equiv 0 \pmod 7$. As is easily checked, the residues mod 7 of the $w_r$'s form a periodic sequence of order 14 and $w_r \equiv 0 \pmod 7 \Leftrightarrow r \equiv 6, 13 \pmod{14}$. Therefore, by (2.11) and (2.18),

$$21(2x)^2 = \pm w_r \equiv \pm w_6, \pm w_{13} \pmod{v_7}. \tag{2.19}$$

Now $v_7 = 5 \cdot 11593$. The first instance of (2.19) is impossible since $w_6 = 31129$ and $((\pm 21 \cdot 31129/11593) = -1$. The second instance of (2.19) is impossible since $w_{13} \equiv 2 \pmod 5$. If $j = 0$ and $x \equiv 0 \pmod 9$ then, by (2.18), $w_r \equiv 0 \pmod{27}$. The residues mod 27 of the $w_r$'s form a periodic sequence of order 27 and $w_r \equiv 0 \pmod{27} \Leftrightarrow r \equiv 7 \pmod{27}$. Therefore $r \equiv 7, 34 \pmod{54}$ and by (2.18) and (2.10)

$$(2x)^2 = \pm w_r \equiv \pm w_7, \pm w_{34} \pmod{u_{27}}. \tag{2.20}$$

Now $u_{27} = u_9(v_{18} + 1)$, $v_{18} + 1 = v_9^2 - 1$, $v_9 - 1 = 1330669$ and, consequently, (2.20) implies $(2x)^2 \equiv \pm w_7, \pm w_{34} \pmod{1330669}$. But an easy computation shows that $w_{34} \equiv -w_7 \equiv -149148 \pmod{1330669}$ and $(\pm 149148/1330669) = -1$, so that (2.20) is impossible.

Next consider (2.17). If $j = 1$, then $w_r \equiv 0 \pmod 7$ and, as before, we find $r \equiv 3, 10 \pmod{14}$. If $r \equiv 3 \pmod{14}$, then, by (2.18) and (2.10), $21(2x)^2 = \pm w_r \equiv \pm w_3 = \pm 21^2 \pmod{u_7}$ and this is impossible since $13 \mid u_7$ and $(\pm 21/13) = -1$. If $r \equiv 10 \pmod{14}$, then $21(2x)^2 \equiv \pm w_{10} \pmod{v_7}$, which is impossible since $5 \mid v_7$ and $w_{10} \equiv 2 \pmod 5$. Finally, we deal with the case $j = 0$ in (2.17) in the same way as the case $j = 0$ in (2.16), and this completes the proof.

COROLLARY. *The only solutions of* $y^2 = 4 \cdot 21^n + 85$ *are* $(\pm y, n) = (13, 1), (43, 2)$.

*Proof.* If $n$ is even, then clearly $n = 2$. If $n$ is odd, put $n = 4h + 2j + 1$, $j \in \{0, 1\}$ so that our equation becomes $y^2 - 4 \cdot 21^{2j+1}(21^h)^4 = 85$. By Theorem II.2, $j = 0$ and $h = 0$ or 1, i.e., $n \leqslant 5$ and a computation shows that the only acceptable value is $n = 1$.

Finally, we verify Calderbank's conjecture for $q = 307$. In fact, we prove more generally the following

THEOREM II.3. *The diophantine equation*

$$y^2 - 4 \cdot 307^{2j+1}x^4 = 1229, \qquad j \in \{0, 1\}, (x, y) = 1 \tag{2.21}$$

*is impossible.*

*Proof.* We write (2.21) in the form $y^2 - 307(2 \cdot 307^j x^2)^2 = 1229$ and we apply the results of Section 1, case A. Now

$$e = 88529282, \quad f = 5052633, \quad E = 177058564, \quad J = 1$$
$$a = 1227, \quad b = 10, \quad w_0 = 70, \quad w_1 = 12396630431$$
$$2 \cdot 307^j x^2 = \pm w_r. \tag{2.22}$$

Since $w_r$ is even $r$ is even too. Now we note that $233 \mid E$, so that by (2.8), if $m \equiv n \pmod 2$, then $w_m \equiv \pm w_n \pmod{233}$. Therefore $w_r \equiv \pm w_0 = \pm 70 \pmod{233}$ and, by (2.22), $307^j x^2 \equiv \pm 35 \pmod{233}$. This relation, however, is impossible, since $(\pm 307/233) = +1$ and $(35/233) = -1$.

COROLLARY. *The only solution to* $y^2 = 4 \cdot 307^n + 1229$ *is* $(\pm y, n) = (615, 2)$.

## REFERENCES


1. F. BEUKERS, On the generalized Ramanujan–Nagell equation, I, *Acta Arith.* **38** (1981), 389–410.
2. F. BEUKERS, On the generalized Ramanujan–Nagell equation, II, *Acta Arith.* **39** (1981), 113–123.
3. A. BREMNER AND P. MORTON, The integer points on three related elliptic curves, *Math. Comp.* **39** (1982), 235–238.
4. A. BREMNER *et al.*, Two-weight ternary codes and the equation $y^2 = 4 \cdot 3^n + 13$, *J. Number Theory* **16** (1983), 212–234.
5. Z. I. BOREVIČ AND I. R. ŠAFAREVIČ, "Number Theory," Academic Press, New York/London, 1973.
6. R. CALDERBANK, On uniformly packed $[n, n-k, 4]$ codes over $GF(q)$ and a clas of caps in $PG(k-1, q)$, *J. London Math. Soc.* (2) **26** (1982), 365–384.
7. A. SCHINZEL, On two theorems of Gelfond and some of their applications, *Acta Arith.* **13** (1967), 177–236.
8. T. N. SHOREY AND C. L. STEWART, On the diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, *Math. Scand.* **52** (1983), 24–36.
9. N. TZANAKIS, On the diophantine equation $y^2 - D = 2^k$, *J. Number Theory* **17** (1983), 144–164.