View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 16, 212–234 (1983)

# Two-Weight Ternary Codes and the Equation $y^2 = 4 \times 3^a + 13$

A. BREMNER

*Emmanuel College, Cambridge CB2 3AP, England*

R. CALDERBANK

*Bell Telephone Laboratories, Murray Hill, New Jersey 07974*

P. HANLON, P. MORTON, AND J. WOLFSKILL

*Department of Mathematics, California Institute of Technology, Pasadena, California 91125*

*Communicated by D. J. Lewis*

Received April 8, 1981

This paper determines the parameters of all two-weight ternary codes $C$ with the property that the minimum weight in the dual code $C^{\perp}$ is at least 4. This yields a characterization of uniformly packed ternary $[n, k, 4]$ codes. The proof rests on finding all integer solutions of the equation $y^2 = 4 \times 3^a + 13$.

## 1. INTRODUCTION

In 1948 Nagell [14] answered a question of Ramanujan [15] by showing that the only integral values of $a$ for which the Diophantine equation

$$y^2 = 2^a - 7 \tag{1}$$

has a solution, are $a = 3, 4, 5, 7, 15$. This equation turns up in the proof given in [13] that there does not exist a nontrivial binary 2-error correcting code which is perfect. (For the basic definitions of coding theory see Section 2 and [13].)

In this paper we show that the solutions of a similar Diophantine equation can be used to classify certain kinds of 2-weight ternary codes. We prove

THEOREM A. *Let $C$ be an $[n, k]$ code over $\mathbb{F}_3$ with exactly two nonzero*



0022-314X/83 $3.00

Copyright © 1983 by Academic Press, Inc.
All rights of reproduction in any form reserved.

*weights $\omega_1$ and $\omega_2$, where $k > 1$ and the minimum weight in the dual code $C^\perp$ is at least 4. Then*

(1) *if $k$ is even, we have*

$$4n = 1 - u(u+1) + 3^{k/2}(2u+1), \quad \omega_1 = u3^{(k-2)/2}, \quad \omega_2 = (u+1)3^{(k-2)/2},$$

*where $u \geqslant 1$ is a solution of*

$$(2u+3)^2 = 4 \times 3^{k/2} + 13;$$

(2) *if $k$ is odd,*

$$4n = 1 - \tfrac{1}{3}u(u+1) + 3^{(k-1)/2}(2u+1),$$
$$\omega_1 = u3^{(k-3)/2}, \qquad \omega_2 = (u+1)3^{(k-3)/2},$$

*where $u \geqslant 1$ is a solution of*

$$(2u+7)^2 = 4 \times 3^{(k+1)/2} + 13.$$

This theorem is proved by exploiting the connection between 2-weight $[n, k]$ codes over the finite field $\mathbb{F}_q$ and 2-parameter difference sets in $\mathbb{F}_q^k$. This connection is contained in a theorem of Goethals and van Tilborg [5]. Also, Camion [1] relates the parameters of the code to the parameters of a certain difference set arising from a generator matrix for the code. In Section 3 we deduce these same relations using only elementary linear algebra. Then in Section 4 we derive the formulas contained in Theorem A for the parameters of the code.

In Section 5 we complete the determination of the codes of Theorem A by finding all solutions of

$$y^2 = 4 \times 3^\alpha + 13. \tag{2}$$

We prove the following theorem, using only elementary algebraic number theory.

THEOREM B. *The only positive integer solutions $(\alpha, y)$ of* (2) *are* $(\alpha, y) = (1, 5), (2, 7), (3, 11)$.

Combining Theorems A and B we obtain

THEOREM C. *Let $C$ be an $[n, k]$ code over $\mathbb{F}_3$ with two nonzero weights $\omega_1$ and $\omega_2$. If $k > 1$ and the minimum weight in $C^\perp$ is at least four, then either*

(1) $k = 2$, $n = 2$, $\omega_1 = 1$, $\omega_2 = 2$, *or*

(2) $k = 4$, $n = 10$, $\omega_1 = 6$, $\omega_2 = 9$, *or*

(3) $k = 6$, $n = 56$, $\omega_1 = 36$, $\omega_2 = 45$, *or*

(4) $k = 5$, $n = 11$, $\omega_1 = 6$, $\omega_2 = 9$.

Furthermore, there exist codes with each of the above sets of parameters. (See [2, 9] and our discussion in Section 2.) As we remark in Section 2, Theorem C also yields a characterization of uniformly packed $[n, k, 4]$ codes over $\mathbb{F}_3$.

In [21] the second author has proved an analogue of Theorem A for codes over an arbitrary finite field $\mathbb{F}_q$. The existence of codes in the general case is related to the solutions of the equation

$$y^2 = 4q^\alpha + 4q + 1.$$

## 2. Orientation: Perfect Codes and Uniformly Packed Codes

For the convenience of the reader we start with several basic definitions. An $[n, k]$ code $C$ over the finite field $\mathbb{F}_q$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$, whose elements are called codewords. The weight $\mathrm{wt}(x)$ of a vector $x$ in $\mathbb{F}_q^n$ is defined to be the number of its nonzero entries. This gives rise to the distance function $\delta(x, y) = \mathrm{wt}(x - y)$. In particular, the minimum distance between codewords is the minimum weight among all nonzero codewords. We say that an $[n, k]$ code $C$ is an $e$-error correcting code if the minimum nonzero weight among codewords of $C$ is $d$, and $e = [(d-1)/2]$. Then $C$ is called an $[n, k, d]$ code.

If $C$ is an $e$-error correcting code, then any two spheres of radius $e$ (defined with respect to the distance function $\delta$) centered at distinct codewords must be disjoint. If the union of all such spheres exhausts $\mathbb{F}_q^n$, then $C$ is said to be perfect. An alternate characterization has been given by MacWilliams [12, 13], in terms of the dual code of $C$: this is the code $C^\perp$ consisting of all vectors of $\mathbb{F}_q^n$ having inner-product zero with all words in $C$. In terms of $C^\perp$ we have

Theorem 1. *Let $C$ be an $e$-error correcting code. Then $C$ is perfect if and only if there are exactly $e$ nonzero weights in the dual code $C^\perp$.*

For example, if $G_{11}$ is the perfect $[11, 6, 5]$ ternary Golay code (see [6, 7, 13]), then $G_{11}^\perp \subseteq G_{11}$ and the nonzero weights in $G_{11}^\perp$ are 6 and 9.

All perfect $[n, k]$ codes have been classified by Tietäväinen [19] and van Lint [10]. A related notion is that of a uniformly packed code, introduced by

Semakov *et al.* [18], and defined as follows. Let $B(x, i)$ be the number of codewords at distance $i$ from $x$.

DEFINITION. An $e$-error correcting code $C$ in $\mathbb{F}_q^n$ is said to be uniformly packed with parameters $\lambda$, $\mu$, satisfying the inequality

$$\lambda < (n-e)(q-1)/(e+1), \tag{3}$$

if for $x$ in $\mathbb{F}_q^n$ we have:

(1) if $\min_{c \in C} \{\delta(x, c)\} = e$, then $B(x, e+1) = \lambda$,

(2) if $\min_{c \in C} \{\delta(x, c)\} \geqslant e+1$, then $B(x, e+1) = \mu$.

Goethals and van Tilborg have shown that perfect codes are exactly the codes which satisfy this definition with $\lambda = (n-e)(q-1)/(e+1)$. They have also proved the following analogue of Theorem 1 (see [5]).

THEOREM 2. *Let $C$ be an $e$-error correcting code. Then $C$ is uniformly packed if and only if there are exactly $e+1$ nonzero weights in the dual code $C^\perp$.*

To obtain an example, let $G_{10}^\perp$ be the code gotten from $G_{11}^\perp$ by taking all codewords with 0 as the entry in a fixed coordinate position, and then deleting that coordinate position. The code $G_{10}^\perp$ is a [10, 4] code with 2 nonzero weights 6 and 9. The dual code $G_{10}$ is a [10, 6, 4] code, and by Theorem 2, $G_{10}$ is a uniformly packed 1-error correcting code. Another example of a uniformly packed 1-error correcting code was discovered independently by Delsarte [2] and by Hill [9]. The dual code is a (56, 6) code with nonzero weights 36 and 45.

By Theorem 2, all $[n, k, 4]$ codes over $\mathbb{F}_3$ which are uniformly packed must have dual codes whose parameters are given by Theorem C (Section 1). We do not see any way of obtaining this characterization without finding all solutions of (2).

We conclude this section by pointing out the connection between 2-weight codes and certain geometric configurations in projective space. Let $C$ be an $[n, k]$ code and let $M$ be a $k \times n$ matrix over $\mathbb{F}_q$ whose row space is $C$. Such an $M$ is called a generator matrix for $C$. Also, let $O(C)$ denote the set of $n$ 1-dimensional subspaces of $\mathbb{F}_q^k$ generated by the $n$ columns of $M$. Then $O(C)$ consists of points in $PG(k-1, q)$, $(k-1)$-dimensional projective space over $\mathbb{F}_q$.

The following result is due to Goethals and van Tilborg.

THEOREM 3. *Let $C$ be an $[n, k]$ code over $\mathbb{F}_q$. Then $C$ has exactly two nonzero weights if and only if*

(1) *any point $Q$ of $PG(k-1,q)$ on $O(C)$ is collinear with a fixed number $E_1$ of pairs of points of $O(C)$; and*

(2) *any point $Q$ of $PG(k-1,q)$ not on $O(C)$ is collinear with a fixed number $E_2$ of pairs of points of $O(C)$.*

This theorem is also an easy consequence of the results presented in Section 3. We remark that when $C = G_{10}^{\perp}$, the set $O(C)$ is an elliptic quadric in $PG(3,3)$ (see [9]). Games [4] refers to these geometries as caps with constant elimination number.

## 3. Necessary Conditions for Existence

Let $C$ be an $[n,k]$ code over $\mathbb{F}_3$ with exactly two nonzero weights $\omega_1$ and $\omega_2$, where $\omega_1 < \omega_2$. Throughout this section we shall suppose that the minimum weight in the dual code $C^{\perp}$ is at least four. Under this assumption we shall deduce certain necessary conditions which must be satisfied by the parameters $n$, $k$, $\omega_1$, $\omega_2$ of the code. (See Eqs. (8)–(13).)

To begin with, if $M$ is a $k \times n$ generator matrix for $C$, then any two columns of $M$ are linearly independent, since a dependence would give rise to a vector of weight two in $C^{\perp}$. Let

$$\Omega = \{\pm g;\ g \text{ is a column of } M\} \tag{4}$$

and let $\tilde{M}$ be the $k \times 2n$ matrix with column set $\Omega$. Matrix $\tilde{M}$ is a generator matrix for a $[2n,k]$ code $\tilde{C}$ with two nonzero weights $2\omega_1$ and $2\omega_2$. Let $m_1,\ldots,m_k$ be the rows of $\tilde{M}$, and let $G = \mathbb{F}_3^k$. We regard $G$ as an additive group of column vectors.

The column vector $h = (h_1,\ldots,h_k)^t$ in $G$ corresponds to the codeword $c(h) = \sum_{i=1}^{k} h_i m_i$ in $\tilde{C}$. We order the elements $g_1,\ldots,g_{3^k}$ of $G$ so that $g_1 = \mathbf{0}$ and

$$\begin{aligned} \mathrm{wt}(c(g_j)) &= 2\omega_1, \qquad \text{if} \quad 2 \leqslant j \leqslant A_1 + 1, \\ &= 2\omega_2, \qquad \text{if} \quad A_1 + 2 \leqslant j \leqslant 1 + A_1 + A_2 = 3^k, \end{aligned} \tag{5}$$

where $A_i$ is the number of codewords of weight $\omega_i$, $i = 1, 2$.

We now consider the $3^k \times 3^k$ integral matrix $B = [b_{ij}]$ defined by

$$\begin{aligned} b_{ij} &= 1, \qquad \text{if} \quad g_i - g_j \in \Omega, \\ &= 0, \qquad \text{otherwise.} \end{aligned}$$

The necessary conditions we derive for the existence of the code $C$ will follow from considering the minimal polynomial of $B$ on the orthogonal space (over $\mathbb{C}$) of the $3^k$-dimensional vector $(1, 1,\ldots, 1)^t$.

We first compute $B^2$ in terms of the numbers

$$E(g) = \text{cardinality}\{(h_1, h_2);\ h_1, h_2 \in \Omega \text{ and } h_1 + h_2 = g\}.$$

LEMMA 1. *The $ij$th entry of $B^2$ is $E(g_i - g_j)$.*

*Proof.* The $ij$th entry of $B^2$ is equal to the number of $g_k$ for which $g_i - g_k = h_1$ and $g_k - g_j = h_2$ are simultaneously in $\Omega$. Since $g_i - g_j = h_1 + h_2$, this number is easily seen to coincide with $E(g_i - g_j)$.

We next compute the eigenvectors of $B$. Let $\xi = e^{2\pi i/3}$ be a primitive cube root of unity and define the column vector $v_g$ by setting

$$(v_g)_i = \xi^{(g, g_i)}, \qquad 1 \leqslant i \leqslant 3^k, \quad g \in G,$$

where $(g, h)$ denotes the usual inner product on $G$.

LEMMA 2. *The vector $v_g$ is an eigenvector of $B$ with eigenvalue* $2n - \frac{3}{2}\text{wt}(c(g))$.

*Proof.* We have

$$(Bv_g)_i = \sum_{\substack{j \\ g_i - g_j \in \Omega}} \xi^{(g_j, g)} = \xi^{(g_i, g)} \sum_{\substack{j \\ g_i - g_j \in \Omega}} \xi^{(g_j - g_i, g)}$$

$$= (v_g)_i \sum_{h \in \Omega} \xi^{(h, g)} \qquad \text{for} \quad 1 \leqslant i \leqslant 3^k.$$

Now the components of the codeword $c(g)$ are the numbers $(h, g)$, for $h \in \Omega$, and so

$$\text{wt}(c(g)) = \text{cardinality}\{h \in \Omega;\ (h, g) \neq 0\}.$$

It follows that

$$\sum_{h \in \Omega} \xi^{(h, g)} = \sum_{\substack{h \in \Omega \\ (h, g) = 0}} \xi^{(h, g)} + \sum_{\substack{h \in \Omega \\ (h, g) \neq 0}} \xi^{(h, g)}$$

$$= 2n - \text{wt}(c(g)) + \tfrac{1}{2}\text{wt}(c(g))(\xi + \xi^{-1}) = 2n - \tfrac{3}{2}\text{wt}(c(g)),$$

and this proves the lemma.

LEMMA 3. *If $J$ is the $3^k \times 3^k$ matrix with every entry 1, then $Jv_{g_1} = 3^k v_{g_1}$ and $Jv_{g_i} = \mathbf{0}$ if $i > 1$.*

*Proof.* This follows from the fact that the map $h \to \xi^{(h,g)}$ is a character of $G$, and

$$\sum_{h \in G} \xi^{(h,g)} = |G|, \quad \text{if} \quad g = g_1, \qquad = 0, \quad \text{otherwise.} \tag{6}$$

Note that the vectors $v_{g_i}$ are independent: for a relation of the form

$$\sum_{g \in G} a_g \xi^{(g,g_i)} = 0, \text{ for all } i,$$

implies by (6) that

$$|G|\, a_h = \sum_{g \in G} a_g \sum_i \xi^{(g-h,g_i)} = 0,$$

for all $h$ in $G$. Thus the matrix $S = [v_{g_1},..., v_{g_{3^k}}]$ is invertible, and

$$S^{-1} J S = \operatorname{diag}[3^k, 0,..., 0],$$

where $\operatorname{diag}[a_1,..., a_n]$ is a diagonal matrix with diagonal entries $a_1,..., a_n$. We have further by Lemma 2 and the labeling described in (5) that

$$S^{-1} B S = D = \begin{bmatrix} 2n & & 0 \\ & (2n - 3\omega_1) I_1 & \\ 0 & & (2n - 3\omega_2) I_2 \end{bmatrix},$$

where $I_j$ is the $A_j \times A_j$ identity matrix. Now

$$3^k (D - (2n - 3\omega_1) I)(D - (2n - 3\omega_2) I) = 9\omega_1 \omega_2 \operatorname{diag}[3^k, 0,..., 0].$$

Conjugating by $S$ we obtain

$$(B - (2n - 3\omega_1) I)(B - (2n - 3\omega_2) I) = (9\omega_1 \omega_2 / 3^k) J. \tag{7}$$

We now compare off-diagonal entries in (7). If $g \notin \Omega$ and $g \neq \mathbf{0}$, then by Lemma 1 we have

$$E(g) = 9\omega_1 \omega_2 / 3^k. \tag{8}$$

Thus $E(g) = E$ is constant for $g \notin \Omega$, $g \neq \mathbf{0}$. If $g \in \Omega$, then

$$E(g) - 4n + 3(\omega_1 + \omega_2) = 9\omega_1 \omega_2 / 3^k. \tag{9}$$

Recall that the minimum weight in the dual code $C^\perp$ is at least 4. It follows

that the only way to write $g = h_1 + h_2$ with $h_1, h_2 \in \Omega$ is to take $h_1 = h_2 = -g$. Hence if $g \in \Omega$, $E(g) = 1$. Note also that $E(\mathbf{0}) = 2n$.

From these facts and from Lemma 1 we deduce the equation

$$B^2 - B - E(J - B - I) - 2nI = 0,$$

or

$$B^2 - (1 - E)B + (E - 2n)I = EJ. \tag{10}$$

It is clear that (7) and (10) must coincide, so comparing the discriminants of the left-hand sides of these equations gives

$$9(\omega_2 - \omega_1)^2 = (1 - E)^2 + 4(2n - E). \tag{11}$$

We now appeal to a result of Delsarte [3, Corollary 2, p. 53], according to which $\omega_1 = u3^t$ and $\omega_2 = (u + 1)3^t$ for some integers $u, t$, $u \geqslant 1$. With this (8) becomes

$$E = u(u + 1)3^{2t}/3^{k-2}, \tag{12}$$

and from (9) and (11) we obtain

$$3^{2t+2} = 1 - 6E + E^2 + 8n = 1 - 6E + E^2 + 2\{1 + (2u + 1)3^{t+1} - E\},$$

or

$$3^{2t+2} = E^2 - 8E + 3 + (4u + 2)3^{t+1}. \tag{13}$$

In the next section we complete the proof of Theorem A by analysing (12) and (13).

We remark that the above discussion shows $\Omega$ to be a 2-parameter difference set in $\mathbb{F}_3^k$, assuming that $C$ is a two-weight code. Conversely, if $\Omega$ is known to be a 2-parameter difference set, then an equation of type (10) must hold, so that $B$ has two eigenvalues on the space orthogonal to $(1, 1, \ldots, 1)^t$; from this it follows that $C$ is a two-weight code (by Lemma 2).

## 4. The Proof of Theorem A

In this section we assume $k > 1$.

From (12) we have

$$E = u(u + 1)/3^\alpha, \tag{14}$$

where

$$a = k - 2 - 2t. \tag{15}$$

Putting this into (13) gives

$$3^{k-a} = (u(u+1)/3^a)^2 - 8(u(u+1)/3^a) + 3 + (4u+2)\,3^{(k-a)/2}. \tag{16}$$

We first discuss the cases $a = 0, 1$.

LEMMA 4. *If* $a = 0$, *then*

$$u = (-3 + \sqrt{4 \times 3^{k/2} + 13})/2. \tag{17}$$

*Proof.* If $a = 0$, then (16) becomes

$$3^k - (4u+2)\,3^{k/2} - 3 = u^2(u+1)^2 - 8u(u+1).$$

We subtract $4u$ from both sides and obtain

$$(3^{k/2}+1)(3^{k/2} - (4u+3)) = u(u+3)(u(u+3) - (4u+4)),$$

so that

$$\{(3^{k/2}+1) - u(u+3)\}\{(3^{k/2}+1) - (4u+4) + u(u+3)\} = 0.$$

If the second factor is zero, then

$$u = (1 \pm \sqrt{13 - 4 \times 3^{k/2}})/2.$$

Since $k > 0$ we have $k = 2$ and $u = 1, 0$. The first possibility is covered by (17) and the second is impossible. In any case we conclude that the first factor is zero and it follows that (17) holds.

LEMMA 5. *If* $a = 1$, *then*

$$u = (-7 + \sqrt{4 \times 3^{(k+1)/2} + 13})/2. \tag{18}$$

*Proof.* If $a = 1$, then (16) becomes

$$3^{k-1} - (4u+2)\,3^{(k-1)/2} - 3 = (u(u+1)/3)^2 - 8u(u+1)/3.$$

Multiplying through by 9 and subtracting $36u$ from both sides we obtain

$$\begin{aligned}(3^{(k+1)/2} + 3)&(3^{(k+1)/2} - 3(4u+3)) \\ &= (u+3)(u+4)((u+3)(u+4) - (12u+12)),\end{aligned}$$

and so

$$\{(3^{(k+1)/2} + 3) - (u+3)(u+4)\}$$
$$\times \{3^{(k+1)/2} + 3 - (12u + 12) + (u+3)(u+4)\} = 0.$$

If the second factor is zero, then

$$u = (5 \pm \sqrt{13 - 4 \times 3^{(k+1)/2}})/2;$$

but this is impossible since we are assuming $k > 1$. We conclude that the first factor is zero, and this implies (18).

The remainder of this section is devoted to proving that $a = 0$ or $a = 1$. Theorem A will then follow from Lemmas 4 and 5, Eqs. (9) and (15), and the fact that $\omega_1 = u3^t$, $\omega_2 = (u+1)3^t$.

Before continuing we note that the case $k = 2$ is included in Lemma 4. For $k = 2$ implies $a = -2t$ by (15). If $t > 0$, then by (14), $9 \mid E$; but this is impossible by (13). Thus $a = t = 0$. We shall henceforth assume $k > 2$.

LEMMA 6. *If $k > 2$, then $t > 0$ and $a \geqslant -1$.*

*Proof.* Suppose $k > 2$ and $t = 0$. Then by (14) we have $3 \mid u$ or $3 \mid (u+1)$, so $u \geqslant 2$. Now (13) gives

$$-24 \geqslant E^2 - 8E,$$

which is impossible since $x^2 - 8x + 24$ has imaginary roots. We conclude that $t \geqslant 1$. Again by (13) we see that $9 \nmid E$, and so $a \geqslant -1$ from (14) and (15).

We postpone discussion of the case $a = -1$. We shall assume $a \geqslant 2$ and derive a contradiction. In the later work we require the following estimate.

LEMMA 7. *If $a \geqslant 2$, then $(k-a)/2 \geqslant 2a + 1$.*

*Proof.* By (14) we have $3^a \mid u$ or $3^a \mid (u+1)$. Since

$$E \geqslant u \geqslant 3^a - 1 \geqslant 8,$$

equation (13) gives

$$3^{k-a} > (4u+2)3^{(k-a)/2} \geqslant (4 \times 3^a - 2)3^{(k-a)/2} > 3^{a+1}3^{(k-a)/2}, \qquad (19)$$

and so $(k-a)/2 \geqslant a + 2$.

Since $u = s3^a$ or $u = s3^a - 1$ for some integer $s$, we see from (16) that

$$3^{k-a} = s^2(s3^a \pm 1)^2 - 8s(s3^a \pm 1) + 3 + (4u+2)3^{(k-a)/2}.$$

Viewing this equation modulo $3^a$ gives

$$Q(s) = s^2 \mp 8s + 3 \equiv 0 \pmod{3^a}, \tag{20}$$

and modulo $3^{a+2}$ we have

$$Q(s) + s^2 3^a(\pm 2s - 8) \equiv 0 \pmod{3^{a+2}}. \tag{21}$$

By (20) we see that $3 \mid s$ or $s \equiv \pm 2 \pmod 9$. Therefore $s^2(\pm 2s - 8) \equiv 0 \pmod 9$ or $s^2(\pm 2s - 8) \equiv 2 \pmod 9$. If we let $Q(s) = \lambda 3^a$, then by (21), $\lambda \equiv 0$ or $7 \pmod 9$. Since the discriminant of $Q(s)$ is not a square we cannot have $\lambda = 0$. Furthermore, $Q(s) = (s \mp 4)^2 - 13 \geqslant -13$, and so $\lambda > 0$. Now if $\lambda = 7$, we obtain the impossible congruence

$$s^2 \mp 8s + 3 \equiv 0 \pmod 7,$$

so we conclude that $\lambda \geqslant 9$, and $Q(s) \geqslant 9 \times 3^a$.

We now claim that $s > 3^{(a+1)/2} + 3^{-a}$. If this is false, then

$$\begin{aligned} 9 \times 3^a - Q(s) &\geqslant 9 \times 3^a - \{(3^{(a+1)/2} + 3^{-a})^2 + 8(3^{(a+1)/2} + 3^{-a}) + 3\} \\ &> 6 \times 3^a - 9 \times 3^{(a+1)/2}. \end{aligned}$$

But $a \geqslant 2$, so that $Q(s) < 9 \times 3^a$. This contradiction proves our claim.

We next claim that

$$8u(u+1)/3^a \leqslant (4a+2)\, 3^{(k-a)/2};$$

for otherwise $4(u+1) > ((4u+2)/2u)\, 3^{(k+a)/2} > 2 \times 3^{(k+a)/2}$, and

$$(4u+2)\, 3^{(k-a)/2} > 2 \times 3^k - 2 \times 3^{(k-a)/2} > 3^k,$$

which is false by the first inequality in (19).

Therefore it follows from (16) that

$$3^{k-a} > ((u(u+1))/3^a)^2 \geqslant s^2(s\, 3^a - 1)^2.$$

Using $s > 3^{(a+1)/2} + 3^{-a}$, this gives

$$3^{k-a} > 3^{a+1} 3^{3a+1},$$

i.e., $k - a > 4a + 2$. This completes the proof.

We now return to equation (16). Multiplying through by $3^{2a}$ and rearranging we obtain

$$3^{2a}(3^{k-a} - (4u+2)\, 3^{(k-a)/2} - 3) = u^2(u+1)^2 - 8u(u+1)\, 3^a,$$

and subtracting $4u3^{2a}$ from both sides gives

$$3^{2a}(3^{(k-a)/2}+1)(3^{(k-a)/2}-(4u+3))$$
$$= u(u+3)\{u^2+3u-(4u+4)\}-(3^a-1)\{8u(u+1)+4u(3^a+1)\}. \quad (22)$$

Define the quartic polynomial $f_{k,a}(x)$ by

$$f_{k,a}(x) = x(x+3)(x(x+3)-(4x+4))-3^{2a}(3^{(k-a)/2}+1)(3^{(k-a)/2}-(4x+3))$$
$$-(3^a-1)(8x(x+1)+4x(3^a+1)). \quad (23)$$

We regard $k$ and $a$ as fixed and we let $x$ vary. We shall prove that $u$ is the unique root of $f_{k,a}(x)$ on the interval $[3^a-1, \infty)$. We then derive a contradiction by trapping $u(u+1)$ in an interval that does not contain an integral multiple of $2 \cdot 3^a$.

LEMMA 8. *If $a \geqslant 2$, then $f_{k,a}(x)$ is strictly increasing on the interval $[3^a-1, \infty)$.*

*Proof.* Differentiating (23) gives

$$f'_{k,a}(x) > 4x^3+6x^2-14x-12+(3^a-1)(16x+8+4(3^a+1)),$$

and since $x \geqslant 3^a-1$ we have

$$f'_{k,a}(x) > 4x^3+6x^2-14x-12-x(16x+8+4(x+2))$$
$$= 4x^3-14x^2-30x-12.$$

The right-hand side has a unique positive root, which is contained in the interval $(0, 6)$, so that $f'_{k,a}(x) > 0$ for $x \geqslant 3^a-1$ and $a \geqslant 2$.

It follows from (22) and Lemma 8 that $u$ is the unique root of $f_{k,a}(x)$ on $[3^a-1, \infty)$. Now let $x_1$ be the unique positive root of

$$x_1(x_1+3)+(3^a-1)\,2x_1 = 3^a(3^{(k-a)/2}+1)-2(3^a-1)^2 \times 3^a/(3^a-1), \quad (24)$$

and let $x_2$ be the unique positive root of

$$x_2(x_2+3)+(3^a-1)\,2x_2 = 3^a(3^{(k-a)/2}+1)-(3^a-1)^2\,2. \quad (25)$$

Since the right-hand sides of (24) and (25) are positive, by Lemma 7, and $x^2+(1+2\times 3^a)x$ is increasing for $x \geqslant 0$ and equal to 0 at $x=0$, the $x_i$ exist and are unique. Furthermore, $x_1 < x_2$ since the right side of (24) is smaller than the right side of (25).

LEMMA 9. *If* $a \geqslant 2$, *then*

$$3^a - 1 \leqslant x_1 < x_2 \leqslant \tfrac{1}{6} 3^{(k-a)/2}.$$

*Proof.* If $x_1 < 3^a - 1$, then (24) gives

$$(3^a - 1)(3^a + 2) + 2(3^a - 1)^2 > 3^a(3^{(k-a)/2} + 1) - 2 \times 3^a(3^a - 1),$$

and so $5 \times 3^{2a} > 3^a \times 3^{(k-a)/2}$. But this is impossible by Lemma 7. Thus $3^a - 1 \leqslant x_1$.

If $x_2 > \frac{1}{6} 3^{(k-a)/2}$, then by (25) we have

$$3^a 3^{(k-a)/2} > x_2^2 > \tfrac{1}{36} 3^{k-a},$$

and so $3^{(k-a)/2} < 36 \times 3^a$, which again contradicts Lemma 7. This completes the proof.

We shall prove that if $a \geqslant 2$, then $f_{k,a}(x_1) < 0$ and $f_{k,a}(x_2) > 0$. Then Lemma 9 implies $x_1 < u < x_2$. We begin by transforming (23) using the substitution

$$x(x+3) = 3^a(3^{(k-a)/2} + 1) - (3^a - 1)(2x + (3^a - 1)y). \tag{26}$$

Setting

$$g = 3^{2a}(3^{(k-a)/2} + 1)(3^{(k-a)/2} - (4x+3))$$

and

$$h = (3^a - 1)(8x^2 + 16x + 4x(3^a - 1)),$$

equation (23) becomes

$$\begin{aligned} f_{k,a}(x) = {} & \{3^a(3^{(k-a)/2} + 1) - (3^a - 1)(2x + (3^a - 1)y)\} \\ & \times \{3^a(3^{(k-a)/2} + 1) - (3^a - 1)(2x + (3^a - 1)y) - (4x+4)\} \\ & - g - h. \end{aligned}$$

Expanding, we obtain

$$\begin{aligned} f_{k,a}(x) = {} & 3^a(3^{(k-a)/2} + 1)\, 3^a(3^{(k-a)/2} + 1 - (4x+4)) \\ & + 3^a(3^{(k-a)/2} + 1)(3^a - 1)(4x+4) \\ & - 2 \times 3^a(3^a - 1)(3^{(k-a)/2} + 1)(2x + (3^a - 1)y) \\ & + (3^a - 1)^2 (2x + (3^a - 1)y)^2 \\ & + (3^a - 1)(2x + (3^a - 1)y)(4x+4) - g - h, \end{aligned}$$

whence

$$f_{k,a}(x) = (3^a - 1)\, 3^a(3^{(k-a)/2} + 1)(4 - 2(3^a - 1)\, y) + (3^a - 1)^2\, (2x + (3^a - 1)\, y)^2 + (3^a - 1)(2x + (3^a - 1)\, y)(4x + 4) - h.$$

We now substitute for $3^a(3^{(k-a)/2} + 1)$ from (26) and find after some simplification that

$$f_{k,a}(x) = (3^a - 1)(4x^2 + 4x) + (3^a - 1)^2 \times \{(4 - 2y)(x^2 + x) + 4 \times 3^a y - (3^a - 1)^2\, y^2\}. \tag{27}$$

LEMMA 10. *If $a \geqslant 2$, then $f_{k,a}(x_1) < 0$.*

*Proof.* If $x = x_1$, then by (24), $y = 2 \times 3^a/(3^a - 1)$. Using $4 - 2y = -4/(3^a - 1)$, we obtain from (27) that

$$f_{k,a}(x_1) = (3^a - 1)(8 \times 3^{2a} - (3^a - 1)\, 4 \times 3^{2a}).$$

Since $a \geqslant 2$ we do have $f_{k,a}(x_1) < 0$.

Note that $f_{k,a}(x_1) = 0$ if $a = 1$.

LEMMA 11. *If $a \geqslant 2$, then $f_{k,a}(x_2) > 0$.*

*Proof.* If $x = x_2$, then $y = 2$, so (27) gives

$$f_{k,a}(x_2) = (3^a - 1)\{4(x_2^2 + x_2) + 8 \times 3^a(3^a - 1) - 4(3^a - 1)^3\}.$$

We substitute for $x_2(x_2 + 1)$ using (25) and obtain

$$\begin{aligned} f_{k,a}(x_2) &= 4(3^a - 1)\{3^a(3^{(k-a)/2} + 1) - 2x_2\, 3^a - 2(3^a - 1)^2 \\ &\quad + 2 \times 3^a(3^a - 1) - (3^a - 1)^3\} \\ &> 4 \times 3^a(3^a - 1)(3^{(k-a)/2} - 2x_2 - (3^a - 1)^2) \\ &> 4 \times 3^a(3^a - 1)\{(\tfrac{1}{3} 3^{(k-a)/2} - 2x_2) + (\tfrac{2}{3} 3^{(k-a)/2} - 3^{2a})\}. \end{aligned}$$

The lemma now follows from Lemmas 9 and 7.

LEMMA 12. *If $k > 2$, then $a = -1$, 0, or 1.*

*Proof.* By Lemma 6 we have $a \geqslant -1$. Suppose $a \geqslant 2$. We have shown that $u$ is the unique root of $f_{k,a}(x)$ on the interval $[3^a - 1, \infty)$. By

Lemmas 9–11 we see that $x_1 < u < x_2$. Furthermore, by (24) and (25) we have

$$u(u+1) + 2u\,3^a = 3^a(3^{(k-a)/2} + 1) - (3^a - 1)^2\, y,$$

where $2 < y < 2 \times 3^a/(3^a - 1)$. Note that $u(u+1) + 2u\,3^a$ is divisible by $2 \times 3^a$, from (14). However, the interval $(3^a(3^{(k-a)/2} + 1) - 2 \times 3^a(3^a - 1),$ $3^a(3^{(k-a)/2} + 1) - 2(3^a - 1)^2)$ does not contain a multiple of $2 \times 3^a$. This is because the left end point is divisible by $2 \times 3^a$ and the length of the interval is $2(3^a - 1)$. Therefore $a < 2$.

We shall now prove $a \neq -1$. If $a = -1$, then (16) becomes

$$3^{k+1} = 9u^2(u+1)^2 - 24u(u+1) + 3 + (4u+2)\,3^{(k+1)/2}. \tag{28}$$

Define the polynomial $f_k(x)$ by

$$f_k(x) = 9x^2(x+1)^2 - 24x(x+1) + 3 + (4x+2)\,3^{(k+1)/2} - 3^{k+1}. \tag{29}$$

Differentiating with respect to $x$ we find that $f_k(x)$ is strictly increasing on the interval $[0, \infty)$, for $k \geqslant 3$. Now let $x_1$ be the positive root of

$$3x_1(x_1+1) = 3^{(k+1)/2} - (2x_1 - 1), \tag{30}$$

and let $x_2$ be the positive root of

$$3x_2(x_2+1) = 3^{(k+1)/2} - (2x_2 - 3). \tag{31}$$

LEMMA 13. *If $k > 2$, then $a = 0$ or 1.*

*Proof.* We suppose $a = -1$ and prove that $x_1 < u < x_2$. Since $f_k(x)$ is increasing it suffices to prove $f_k(x_1) < 0$ and $f_k(x_2) > 0$. Equations (29) and (30) give

$$f_k(x_1) = (3^{(k+1)/2} - (2x_1 - 1))^2 - 8(3^{(k+1)/2} - (2x_1 - 1)) + 3 + (4x_1 + 2)\,3^{(k+1)/2} - 3^{k+1},$$

which reduces to

$$f_k(x_1) = 4x_1(x_1 - 1) - 4(3^{(k+1)/2} - (2x_1 - 1)).$$

Now (30) implies $f_k(x_1) < 0$.

Similarly, equations (29) and (31) give

$$f_k(x_2) = 4x_2^2 + 4x_2 - 12.$$

If $f_k(x_2) \leqslant 0$, then $x_2 \leqslant (-1 + \sqrt{13})/2$, and from (31) we deduce that $9 > 3^{(k+1)/2}$. But $k > 2$, so this is impossible. Therefore $f_k(x_2) > 0$, and $x_1 < u < x_2$.

Finally, equations (30) and (31) give

$$3^{(k+1)/2} + 1 < u(3u + 5) < 3^{(k+1)/2} + 3,$$

which is impossible since $u(3u + 5)$ is even. Thus $a \neq -1$, and the lemma follows from Lemma 12.

This comples the proof of Theorem A.

## 5. Proof of Theorem B

To prove Theorem B we shall consider three cases. If we set $\alpha = 3n$, $3n + 1$, $3n + 2$, respectively in (2), we are led to consider the equations

$$y^2 = 4 \times 3^{3n} + 13, \tag{32}$$

$$y^2 = 12 \times 3^{3n} + 13, \tag{33}$$

$$y^2 = 36 \times 3^{3n} + 13. \tag{34}$$

To handle the first and third equations we shall work in an appropriate cubic extension of $\mathbb{Q}$; the discussion of (33) will take place in $\mathbb{Q}(\sqrt{13})$. (For an Hernate proof see [22].)

(a) We first consider (32). Set $x = 3^n$ and multiply through in (32) by $4^2$, to give

$$(4y)^2 = (4x)^3 + 16 \times 13 = \text{norm}(4x + 2\theta),$$

where the norm is from $K = \mathbb{Q}(\sqrt[3]{26})$ to $\mathbb{Q}$, and $\theta = \sqrt[3]{26}$. (For the details of the arithmetic in $K$, such as class number, fundamental unit, and integral basis, we refer to Selmer [17].) Working in $K$, write

$$(4x + 2\theta) = a\mathfrak{k}^2,$$

where $a$ is a square-free integral ideal. Since $(2) = \mathfrak{h}_2^3$ in $K$ ($\mathfrak{h}_a$ denotes a prime ideal of norm $a$), and since $\mathfrak{h}_2 \| \theta$ (exactly divides), we have that $\mathfrak{h}_2^4 \| (4x + 2\theta)$, so $\mathfrak{h}_2 \nmid a$. Moreover, if $\xi = (-1 + \sqrt{-3})/2$, and $\lambda$ is the number

$$\lambda = (4x + 2\xi\theta)(4x + 2\xi^2\theta) = 4(4x^2 - 2x\theta + \theta^2),$$

then

$$\lambda(4x + 2\theta) = \text{norm}(4x + 2\theta) = (4y)^2,$$

and

$$(4y)^2 = (\lambda)(4x + 2\theta) = (\lambda)\,\mathfrak{a}\mathfrak{k}^2.$$

This implies that $\mathfrak{a} \mid \lambda$. Since $\mathfrak{a} \mid (2x + \theta)$, it follows that $\mathfrak{a}$ divides

$$\tfrac{1}{4}\lambda + (2\theta - 2x)(2x + \theta) = 3\theta^2.$$

Now $(\theta) = \mathfrak{h}_2\mathfrak{h}_{13}$, so that $\mathfrak{a} \mid (3)\,\mathfrak{h}_3$. But $y$ is relatively prime to 39, so we must have $\mathfrak{a} = 1$.

Hence $(4x + 2\theta) = \mathfrak{k}^2$, which implies that $\mathfrak{k}$ is a principal ideal, since $K$ has class number 3 (by Selmer's tables). Consequently,

$$4x + 2\theta = \pm\eta^2 \qquad \text{or} \quad \pm\varepsilon\eta^2, \tag{35}$$

where $\varepsilon = 3 - \theta$ is the fundamental unit in $K$ and $\eta$ is an algebraic integer in $K$. We may ignore the minus signs since $y$, $\theta$, and $\varepsilon$ are all positive. Now the integers of $K$ have the form

$$\eta = (a - b\theta + c\theta^2)/3, \qquad a, b, c \in \mathbb{Z}, \quad a \equiv b \equiv c \pmod 3.$$

Using the fact that

$$\eta^2 = \frac{a^2 - 52bc}{9} + \frac{26c^2 - 2ab}{9}\,\theta + \frac{b^2 + 2ac}{9}\,\theta^2,$$

the two possibilities in (35) give rise to the following systems of equations, on equating coefficients of 1, $\theta$, $\theta^2$:

$$\begin{aligned} a^2 - 52bc &= 4 \times 3^{n+2}, \\ 26c^2 - 2ab &= 18, \\ b^2 - 2ac &= 0, \end{aligned} \tag{36}$$

$$\begin{aligned} 3a^2 - 156bc - 26b^2 - 52ac &= 4 \times 3^{n+2}, \\ 78c^2 - 6ab - a^2 + 52bc &= 18, \\ 3b^2 + 6ac - 26c^2 + 2ab &= 0. \end{aligned} \tag{37}$$

Equations (37) are easily seen to be contradictory. For the third and first equations imply, respectively, that $2 \mid b$ and $2 \mid a$. Then the last equation implies $2 \mid c$, which is impossible by the second relation.

We are thus left with (36). It is clear that $a = 2a_1$, $b = 2b_1$ with $a_1, b_1 \in \mathbb{Z}$. Putting in these values gives

$$\begin{aligned} a_1^2 - 26b_1c &= 3^{n+2}, \\ 13c^2 - 4a_1b_1 &= 9, \\ b_1^2 + a_1c &= 0, \end{aligned}$$

where $a_1b_1c \neq 0$. The last equation shows that any prime divisor of $a_1$ is a divisor of $b_1$, and so we have that $a_1 = 3^r$, $r \geqslant 0$, by the first equation. (We may assume $a > 0$ by multiplying $\eta$ by $-1$.) If $r = 0$, then $a_1 = 1$, $b_1^2 = -c$ and

$$0 = 13b_1^4 - 4b_1 - 9 = (b_1 - 1)(13b_1^3 + 13b_1^2 + 13b_1 + 9),$$

which has the unique integer solution $b_1 = 1$. Thus $a = 2$, $b = 2$, $c = -1$, and $n = 1$.

We now suppose that $r > 0$. Then $a_1 = 3a_2$, $b_1 = 3b_2$, $c = 3c_2$ with $a_2, b_2, c_2 \in \mathbb{Z}$, and the system becomes

$$\begin{aligned} a_2^2 - 26b_2c_2 &= 3^n, \\ 13c_2^2 - 4a_2b_2 &= 1, \\ b_2^2 + a_2c_2 &= 0. \end{aligned} \tag{38}$$

Here $a_2 = 3^{r-1}$. If $r = 1$, then $a_2 = 1$ and $13b_2^4 - 4b_2 - 1 = 0$, which is impossible. Thus $r > 1$ and $3 \nmid c_2$. The last equation in (38) now shows that $b_2$ is exactly divisible by $3^m$, where $m = (r-1)/2 > 0$, and the first equation gives that $n = m$, since the power of 3 dividing the left-hand side is $3^m$. Thus $a_2 = 3^{2n}$, $b_2 = 3^n b_3$, and eliminating $c_2 = -b_3^2$ from the equations leads to $13b_3^4 - 4 \times 3^{3n}b_3 - 1 = 0$. But this equation has no integer solutions for any $n > 0$, and so the case $r > 0$ does not occur.

Thus $n = 1$, $y = 11$ is the only positive solution of (32).

(b) To solve (34) we argue similarly. Multiply through by $36^2$, giving

$$(36y)^2 = \operatorname{norm}(36x + 6\theta),$$

where $x = 3^n$ and $\theta = \sqrt[3]{78}$. As in (a) we set

$$(36x + 6\theta) = \alpha \mathfrak{k}^2,$$

with $\alpha$ square-free. Since the prime divisors $\mathfrak{h}_2$ and $\mathfrak{h}_3$ of $(2) = \mathfrak{h}_2^3$ and $(3) = \mathfrak{h}_3^3$ divide $36x + 6\theta$ exactly to the fourth power, we have $(\alpha, \mathfrak{h}_2\mathfrak{h}_3) = 1$. It follows as before that $\alpha$ divides $\lambda = (6x + \xi\theta)(6x + \xi^2\theta) =$

$36x^2 - 6x\theta + \theta^2$, and so $\alpha$ divides $\lambda + (2\theta - 6x)(6x + \theta) = 3\theta^2$. Again this shows that $\alpha = 1$ and $(36x + 6\theta) = \mathfrak{k}^2$.

Now $K = \mathbb{Q}(\sqrt[3]{78})$ has class number 3 (see [17]), so we conclude that

$$36x + 6\theta = \eta_1^2 \qquad \text{or} \quad \varepsilon\eta_1^2, \tag{39}$$

where

$$\varepsilon = -2134079 + 841944\theta - 80154\theta^2$$

is the fundamental unit of $K$. (We shall not need the actual value of $\varepsilon$; see below.) An integral basis of $K$ is $1, \theta, \theta^2$, so the first possibility in (39) gives rise to the equation

$$36x + 6\theta = (a + b\theta + c\theta^2)^2 = a^2 + 156bc + (78c^2 + 2ab)\,\theta + (b^2 + 2ac)\,\theta^2.$$

Equating coefficients, we find that

$$\begin{aligned} a^2 + 156bc &= 4 \times 3^{n+2}, \\ 78c^2 + \quad 2ab &= 6, \\ b^2 + \quad 2ac &= 0. \end{aligned}$$

We may set $a = 2a_1$, $b = 2b_1$ with $a_1, b_1 \in \mathbb{Z}$, and the system becomes

$$\begin{aligned} a_1^2 + 78b_1c &= 3^{n+2}, \\ 39c^2 + \quad 4a_1b_1 &= 3, \\ b_1^2 + \quad a_1c &= 0. \end{aligned}$$

It is clear from these equations that $a_1 = 3^r$, $r > 0$, that $3 \mid b_1$ and that $3 \nmid c$. As before we have $b_1 = 3^m b_2$, where $3 \nmid b_2$ and $2m = r > 0$. The first equation then shows that $m + 1 = n + 2$, and combining the second and third equations gives

$$13b_2^4 + 4 \times 3^{3n+2}b_2 - 1 = 0.$$

Since this has no integral solutions for any $n \geqslant 0$, the first case in (39) is impossible.

Hence for any solution we must have

$$36x + 6\theta = \varepsilon\eta_1^2. \tag{40}$$

In particular, $n = 0$, $x = 1$, $y = 7$ is a solution, and so

$$36 + 6\theta = \varepsilon\eta_2^2, \tag{41}$$

for some integer $\eta_2$. If there is another solution, with $x = 3^n > 1$, then multiplying (40) and (41) gives

$$(6x + \theta)(6 + \theta) = \eta^2,$$

for some integer $\eta$ of $K$. Squaring and comparing coefficients yields

$$\begin{aligned} a^2 + 156bc &= 4 \times 3^{n+2}, \\ 78c^2 + 2ab &= 6 + 6 \times 3^n, \\ b^2 + 2ac &= 1. \end{aligned}$$

We set $a = 6a_1$ and $c = 3c_1$ with $a_1, c_1 \in \mathbb{Z}$ (note $3 \nmid b$), and obtain

$$\begin{aligned} a_1^2 + 13bc_1 &= 3^n, \\ 117c_1^2 + 2a_1 b &= 1 + 3^n, \\ b^2 + 36a_1 c_1 &= 1. \end{aligned}$$

It follows easily that $a_1$ and $b$ are odd, while $c_1$ is even. But then the second equation implies

$$2 \equiv 1 + 3^n \pmod 4,$$

so that $n$ is even. In that case $y^2 - 36 \times 3^{3n} = 13$ is a difference of squares, which only happens when $y = 7$ and $6 \times 3^{3n/2} = 6$, or $n = 0$.

Thus $n = 0$, $y = 7$ is the only solution of (34).

(c) To solve (33) we work in the quadratic field $Q(\sqrt{13})$, which has class number 1 and fundamental unit $\varepsilon = (3 + \sqrt{13})/2$. (We do not work in $K = \mathbb{Q}(\sqrt[3]{234})$,becuase the arithmetic in this field is too complicated. For instance, $K$ has class number 6, which is even.) We write (33) in the form

$$(y^2 - 13)/4 = 3x^3, \qquad x = 3^n.$$

Now $((y + \sqrt{13})/2,\ (y - \sqrt{13})/2) = ((y + \sqrt{13})/2, \sqrt{13}) = 1$, and $(3) = (4 + \sqrt{13})(4 - \sqrt{13})$, so on supposing that $y \equiv 1 \pmod 3$ (by changing $y$ to $-y$ if necessary) we have that

$$\pm(y + \sqrt{13})/2 = \varepsilon^i(4 + \sqrt{13})(a + b\omega)^3,$$

where $i = -1$, 0, or 1 and $\omega = \frac{1}{2}(1 + \sqrt{13})$. Absorbing the sign into the cube and multiplying out gives the equations

$$(y + \sqrt{13})/2 = \alpha\{(a^3 + \tfrac{3}{2}a^2 b + \tfrac{21}{2}ab^2 + 5b^2) + \sqrt{13}\,(\tfrac{3}{2}a^2 b + \tfrac{3}{2}ab^2 + 2b^3)\},$$

for $\alpha = (1 + \sqrt{13})/2$, $4 + \sqrt{13}$, and $(25 + 7\sqrt{13})/2$. We thus get, respectively, on comparing coefficients of $\sqrt{13}$,

$$a^3 + 3a^2b + 12ab^2 + 7b^3 = 1 \qquad (i = -1), \tag{42i}$$

$$2a^3 + 15a^2b + 33ab^2 + 26b^3 = 1 \qquad (i = 0), \tag{42ii}$$

$$7a^3 + 48a^2b + 111ab^2 + 85b^3 = 1 \qquad (i = 1). \tag{42iii}$$

Equation (42ii) is clearly impossible, since it implies $a^2b + ab^2 \equiv 1 \pmod 2$. Moreover we know $\text{Norm}(a + b\omega) = \pm 3^n$, i.e., $a^2 + ab - 3b^2 = \pm 3^n$. Thus, if $n > 0$, we have

$$a(a + b) \equiv 0 \pmod 3.$$

But both (42i) and (42iii) imply that

$$a^3 + b^3 \equiv 1 \pmod 3,$$

and thus in each case $a \equiv 0 \pmod 3$. By (42i)–(42iii) this results in the congruences

$$7b^3 \equiv 1 \pmod 9 \qquad \text{resp.} \qquad 4b^3 \equiv 1 \pmod 9,$$

both of which are impossible ($\pm 1$ are the only cubes mod 9.)

Therefore we must have $n = 0$ and $y = 5$.

This completes the proof of Theorem B. Since the proof we have given is heavily dependent on the arithmetic in the fields $\mathbb{Q}(\sqrt[3]{26})$, $\mathbb{Q}(\sqrt[3]{78})$, $\mathbb{Q}(\sqrt{13})$, we would like to point out that an alternate (non-elementary) proof may be given, which with some modifications is applicable to any equation of the form $y^2 = ap^n + d$. For this proof we start with the equation in the form

$$(y^2 - 13)/4 = 3^n, \tag{43}$$

and find by an easy argument (as in case (c)) that

$$(y \pm \sqrt{13})/2 = \varepsilon^{-m}\pi^n, \tag{44}$$

where $\varepsilon = (3 + \sqrt{13})/2$, $\pi = (5 + \sqrt{13})/2$, and $m \geqslant 0$. (Note $\text{norm}\,\pi = \pi\pi' = 3$.) Conjugating (44) and subtracting, we have

$$\pm\sqrt{13} = \varepsilon^{-m}\pi^n - \varepsilon^m\pi'^n,$$

so that

$$\pm\sqrt{13}/\varepsilon^m\pi^n = \varepsilon^{-2m} - (\pi'/\pi)^n. \tag{45}$$

By (43), $m \log \varepsilon = n \log(\pi/\sqrt{13}) + c$, where $|c| \leqslant 2$, and so the left-hand side

of (45) is "small." One can now obtain an upper bound on $n$ by applying a result of Schinzel [16, Theorem 2], which gives explicit lower bounds for expressions of the form $\alpha^m - \beta^n$, with $\alpha, \beta$ algebraic. From this theorem it follows that $n < 10^{17}$. Further, for any possible $n$ in this range a little more argument shows that

$$\left| \frac{m}{n} - \frac{\log \pi/\pi'}{\log \varepsilon^2} \right| < \frac{27}{n 3^{n/2}}, \tag{46}$$

i.e., that $m/n$ is an excellent rational approximation to the real number

$$\theta = \frac{\log \pi/\pi'}{\log \varepsilon^2} = \log \frac{19 + 5\sqrt{13}}{6} \Big/ \log \frac{11 + 3\sqrt{13}}{2}.$$

Consideration of the continued fraction of $\theta$ (only the first 43 convergents are required) then shows that (46) cannot hold for any $n$ with $12 < n < 10^{17}$.

We are grateful to F. Beukers and A. Odlyzko for pointing out this method of proof to us, and to A. Odlyzko for his computations showing that Eq. (46) cannot hold for $12 < n < 10^{17}$. As we have remarked, this method of proof is nonelementary (due to its reliance on Schinzel's theorem), but depends less on happenstance than the arithmetic proof we have given above.

## REFERENCES

1. P. CAMION, "Difference Sets in Elementary Abelian Groups," Les Presses de l'Université de Montréal, Montréal, 1979.
2. P. DELSARTE, "Two-weight Linear Codes and Strongly Regular Graphs," Report R160, MBLE Res. Lab., Brussels, 1971.
3. P. DELSARTE, Weights of linear codes and strongly regular normed spaces, *Discrete Math.* **3** (1972), 47–64.
4. R. A. GAMES, "The Packing Problem for Finite Projective Geometries," Ph.D. Dissertation, Ohio State Univ., Columbus, 1980.
5. J. M. GOETHALS AND H. C. A. VAN TILBORG, Uniformly packed codes, *Philips Res. Rep.* **30** (1975), 9–36.
6. M. J. E. GOLAY, Notes on digital coding, *Proc. IEEE* **37** (1949), 657.
7. M. J. E. GOLAY, Anent codes, priorities, patents, etc., *Proc. IEEE* **64** (1976), 572.
8. R. W. HAMMING, Error detecting and error correcting codes, *Bell System Tech. J.* **29** (1950), 147–160.
9. R. HILL, Caps and codes, *Discrete Math.* **22** (2) (1978), 111–137.
10. J. H. VAN LINT, A survey of perfect codes, *Rocky Mountain J. Math.* **5** (1975), 199–224.
11. S. P. LLOYD, Binary block coding, *Bell System Tech. J.* **36** (1957), 517–535.
12. F. J. MACWILLIAMS, "Combinatorial Problems of Elementary Group Theory," Ph.D. Dissertation, Harvard University, Cambridge, Mass., 1962.
13. F. J. MACWILLIAMS AND N. J. A. SLOANE, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.

14. T. NAGELL, The diophantine equation $x^2 + 7 = 2^n$, *Nordisk. Mat. Tidskr.* **30** (1948), 62–64; *Ark. Mat.* **4** (1960), 185–187.
15. S. RAMANUJAN, "Collected Papers," p. 327, Chelsea, New York, 1962.
16. A. SCHINZEL, On two theorems of Gelfond and some of their applications, *Acta Arith.* **13** (1967), 177–236.
17. E. S. SELMER, Tables for the purely cubic field $K(\sqrt[3]{m})$, *Avh. Norske Vid.-Akad. Oslo I (N.S.)* **5** (1955).
18. N. V. SEMAKOV, V. A. ZINOVJEV, AND G. V. ZAITZEV, Uniformly packed codes, *Problemy Peredači Informacii* **7** (1971), 38–50.
19. A. TIETÄVÄINEN, A short proof for the non-existence of unknown perfect codes over $GF(q)$, $q > 2$, *Ann. Acad. Sci. Fenn. Ser. A I. Math.* **580** (1974), 1–6.
20. H. C. A. VAN TILBORG, "Uniformly Packed Codes," Ph. D. Dissertation, Tech. Univ. Eindhoven, 1976.
21. 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.
22. A. BREMNER AND P. MORTON, The integer points on three related elliptic curves, *Math. of Comp.* **39** (1982), 235–238.