On a conjecture of Ma

Florian Luca Pantelimon Stănică

March 6, 2006

Abstract

In this paper, we prove a result concerning a conjecture of Ma from diophantine equations, which is connected to an open problem on abelian difference sets of multiplier -1.

1 Introduction

A (v, k, λ) difference set D in a group G is called reversible if $\{d^{-1} \ : \ d \in D\} = D$. If D is an abelian difference set with multiplier -1, then there exists a translate of D that is reversible. Moreover, there are two classes of reversible abelian difference sets, namely, those that satisfy $v \neq 4(k - \lambda)$ and those for which $v = 4(k - \lambda)$. There is only one example in the first class, due to McFarland [11]. More details can be found in [5]. McFarland [11] proposed the following conjecture.

Conjecture 1.1 (McFarland Conjecture)**.** *If D is a reversible abelian (v, k, λ) difference set, then either $v = 4000$, $k = 775$, $\lambda = 150$, or $v = 4(k - \lambda)$.*

Investigating sub-difference sets of reversible difference sets, in [10], S.L. Ma proposed the following conjectures, which imply the previous conjecture of McFarland:

Conjecture 1.2. *Let p be an odd prime, $a \geq 0$ and $b, m, r \geq 1$. Then,*

(1) $Y = 2^{2a+2}p^{2m} - 2^{2a+2}p^{m+r} + 1$ *is a square if and only if $m = r$ (i.e., $Y = 1$);*

(2) $Z = 2^{2b+2}p^{2m} - 2^{b+2}p^{m+r} + 1$ *is a square if and only if $p = 5$, $b = 3$, $m = 1$, $r = 2$ (i.e., $Z = 2401$).*

Part (1) of Conjecture 1.2 was confirmed by Le and Xiang in [6]. Nothing is known about part (2) of the above conjecture. While we cannot prove the above conjecture, we are able to show the following result.

[1] 2000 *Mathematics Subject Classification*: 05B10, 11D45, 11D72.

Theorem 1.3. *Assume that $p > 2$ is a fixed odd prime. Then the diophantine equation*

$$x^2 = 2^{2b+2}p^{2m} - 2^{b+2}p^{m+r} + 1 \tag{1}$$

in positive integer unknowns $x, b, m, r \geq 1$ has at most $2^{50,000}$ solutions.

On a related note, we mention that in [1], Calderbank relates a certain class of $[n, k]$ codes over $GF(q)$, where $q \neq 2$ is a prime power, to the diophantine equation

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

He conjectured that (2), for $q \neq 3$ a prime power, has only the trivial solutions $(\pm x, n) = (2q+1, 2)$. This was proved in the affirmative by Tzanakis and Wolfskill [14, 15]. Of a similar type is the diophantine equation $x^2 = 4\,z^2\,y^{m+n} + \epsilon\,4\,y^n + 1$, $\epsilon = \pm 1$, which was studied by Luca [7], who proved that every solution of such an equation with $x > 1, y > 1$ and $m,\ n$ of the same parity must satisfy $z^2 = y^{n-m}$ and $x = 2y^n + \epsilon$. Moreover, in [8, 9], Luca found all solutions of $x^2 = 4q^m - 4q^n + 1$ and of $x^2 = p^a \pm p^b + 1$, respectively.

Acknowledgments. This paper was written during a visit of P. S. at the Mathematical Institute of the UNAM in Morelia in June 2004. He thanks this Institute for its hospitality. Research of F. L. was supported in part by grants SEP-CONACyT 37259-E and 37260-E and that of P. S. by a grant from the Vice-Chancellor's Office at his institution.

2 Preparations

We start by recalling a particular instance of a quantitative version of the Schmidt Subspace Theorem due to J.-H. Evertse [4].

Let $M_{\mathbb{Q}}$ be the set of all the places of $\mathbb{Q}$. For $x \in \mathbb{Q}^*$ and $v \in M_{\mathbb{Q}}$ we put $|x|_v = |x|$ if $v = \infty$ and $|x|_v = p^{-\mathrm{ord}_p(x)}$ if v corresponds to the prime number p, where $\mathrm{ord}_p(x)$ is the order at which p appears in the factorization of x. When $x = 0$, we set $\mathrm{ord}_p(x) = \infty$ and $|x|_v = 0$. Then the product formula

$$\prod_{v \in M_{\mathbf{Q}}} |x|_v = 1$$

holds for all $x \in \mathbb{Q}^*$. Let $N \geq 2$ be a positive integer and define the *height* $\mathcal{H}(\mathbf{x})$ of $\mathbf{x} = (x_1, \ldots, x_N) \in \mathbb{Q}^N$ as follows. For $v \in M_{\mathbb{Q}}$, write

$$\begin{aligned} |\mathbf{x}|_v &= \Big(\sum_{i=1}^{N} x_i^2\Big)^{1/2} && \text{if } v = \infty, \\ |\mathbf{x}|_v &= \max\{|x_1|_v, \ldots, |x_N|_v\} && \text{otherwise.} \end{aligned}$$

Then,

$$\mathcal{H}(\mathbf{x}) = \prod_{v \in M_{\mathbb{Q}}} |\mathbf{x}|_v.$$

For a linear form $L(\mathbf{x}) = \sum_{i=1}^N a_i x_i$ with $\mathbf{a} = (a_1, \dots, a_N) \in \mathbb{Q}^N$, we write $\mathcal{H}(L) = \mathcal{H}(\mathbf{a})$.

We now let $N \geq 2$ be a positive integer, $\mathcal{S}$ be a finite subset of $M_{\mathbb{Q}}$ of cardinality s containing the infinite place, and for every $v \in \mathcal{S}$, we let $L_{1,v}, \dots, L_{N,v}$ be N linearly independent linear forms in N indeterminates with coefficients in $\mathbb{Q}$ satisfying

$$\mathcal{H}(L_{i,v}) \leq H \qquad \text{for } i = 1, \dots, N \text{ and } v \in \mathcal{S}. \tag{3}$$

Theorem 2.1. (The Subspace Theorem.) *Let $0 < \delta < 1$ and consider the inequality*

$$\prod_{v \in \mathcal{S}} \prod_{i=1}^{N} \frac{|L_{i,v}(\mathbf{x})|_v}{|\mathbf{x}|_v} < \left(\prod_{v \in \mathcal{S}} |\det(L_{1,v}, \dots, L_{N,v})|_v \right) \mathcal{H}(\mathbf{x})^{-N-\delta}. \tag{4}$$

Then the following hold:

(i) There exist proper linear subspaces $T_1, \dots, T_{t_1}$ of $\mathbb{Q}^N$ with

$$t_1 \leq \left(2^{60N^2} \delta^{-7N} \right)^s, \tag{5}$$

such that every solution $\mathbf{x} \in \mathbb{Z}^N \backslash \{\mathbf{0}\}$ of inequality (4) satisfying the inequality $\mathcal{H}(\mathbf{x}) \geq H$ belongs to $T_1 \cup \cdots \cup T_{t_1}$.

(ii) There exist proper linear subspaces $T_1', \dots, T_{t_2}'$ of $\mathbb{Q}^N$ with

$$t_2 \leq (150N^4\delta^{-1})^{Ns+1}(2 + \log\log 2H), \tag{6}$$

such that every solution $\mathbf{x} \in \mathbb{Z}^N \backslash \{\mathbf{0}\}$ of inequality (4) satisfying the inequality $\mathcal{H}(\mathbf{x}) < H$ belongs to $T_1' \cup \cdots \cup T_{t_2}'$.

We shall apply Theorem 2.1 to the finite subset $\mathcal{S} = \{2, p, \infty\}$ of $M_{\mathbb{Q}}$ and certain systems of linear forms $L_{i,v}$ with $i = 1, \dots, N$, and $v \in \mathcal{S}$. In our case, the points $\mathbf{x}$ for which inequality (4) will hold will be in $(\mathbb{Z}^*)^N$. In particular, the inequality $|\mathbf{x}|_v \leq 1$ holds for all $v \in M_{\mathbb{Q}} \backslash \{\infty\}$ as well as the inequalities

$$N \leq \mathcal{H}(\mathbf{x}) \leq \prod_{v \in \mathcal{S}} |\mathbf{x}|_v \leq N \max\{|x_i| \ : \ i = 1, \dots, N\}. \tag{7}$$

Finally, our linear forms will have coefficients 0 and ±1 (hence, we may take $H = N$), and will satisfy

$$\det(L_{1,v}, \dots, L_{N,v}) = \pm 1 \qquad \text{for all } v \in \mathcal{S}. \tag{8}$$

Thus, $\mathcal{H}(\mathbf{x}) \geq N = H$ holds for all such points $\mathbf{x} \in \mathbb{Z}^*$. The following statement is a straightforward consequence of Theorem 2.1 above.

Corollary 2.2. *Assume that* (8) *is satisfied, that* $0 < \delta < 1$, *and consider the inequality*

$$\prod_{v\in\mathcal{S}}\prod_{i=1}^{N}|L_{i,v}(\mathbf{x})|_v < N^{-\delta}\left(\max\{|x_i| \ : \ i=1,\ldots,N\}\right)^{-\delta}. \tag{9}$$

Then, there exist proper linear subspaces $T_1,\ldots,T_{t_1}$ *of* $\mathbb{Q}^N$, *with*

$$t_1 \le \left(2^{60N^2}\delta^{-7N}\right)^s, \tag{10}$$

such that every solution $\mathbf{x}\in\mathbb{Z}^N\backslash\{\mathbf{0}\}$ *of inequality* (9) *belongs to* $T_1\cup\cdots\cup T_{t_1}$.

Recall that an $\mathcal{S}$-*unit* is a nonzero rational number x such that $|x|_v = 1$ for all $v\notin\mathcal{S}$. We need the following version of a theorem of Evertse [3] on $\mathcal{S}$-unit equations.

Theorem 2.3. *Let* $a_1,\ldots,a_N$ *be nonzero rational numbers. Then, the equation*

$$\sum_{i=1}^{N} a_i u_i = 1 \tag{11}$$

in $\mathcal{S}$-*unit unknowns* u_i *for* $i=1,\ldots,N$ *has at most* $(2^{35}N^2)^{N^3 s}$ *solutions such that* $\sum_{i\in I} a_i u_i \ne 0$ *for each nonempty subset* $I\subseteq\{1,\ldots,N\}$.

We are now ready to proceed with the proof of our result.

3 Proof

3.1 Elementary Results

We start with the following lemmas.

Lemma 3.1. *Assume that* (x,b,m,r) *is a solution of equation* (1). *Then* $r>m$ *and* $p^m < 2^b$.

Proof. Note that

$$x^2 = 2^{2b+2}p^{2m} - 2^{b+2}p^{m+r} + 1 < 2^{2b+2}p^{2m} - 2^{b+2}p^m + 1 = (2^{b+1}p^m-1)^2,$$

therefore $x < 2^{b+1}p^m - 1$. Moreover, since $x^2\equiv 1 \pmod{2p^m}$, it follows that $x\equiv \pm 1 \pmod{2p^m}$. Hence, in fact, $x \le 2^{b+1}p^m - 2p^m + 1$, therefore

$$\begin{aligned} 2^{2b+2}p^{2m} - 2^{b+2}p^{m+r} + 1 &\le \left(2^{b+1}p^m - (2p^m-1)\right)^2 \\ &= 2^{2b+2}p^{2m} - 2^{b+2}p^m(2p^m-1) + (2p^m-1)^2, \end{aligned}$$

leading to

$$2^{b+2}p^m(2p^m - p^r - 1) \le (2p^m-1)^2 < 4p^{2m}. \tag{12}$$

If $r \leq m$, then $2p^m - p^r - 1 \geq p^m - 1 > p^m/2$, and moreover $2^{b+2} \geq 8$ by our assumption $b \geq 1$. Therefore,

$$2^{b+2}p^m(2p^m - p^r - 1) > 4p^{2m}$$

contradicting (12). Hence, $r > m$. Now

$$(x-1)(x+1) = x^2 - 1 = 2^{b+2}p^{2m}(2^b - p^{r-m}), \tag{13}$$

and since $\gcd(x-1, x+1) = 2$, it follows that $2p^{2m} \mid x + \eta$ for some $\eta \in \{\pm 1\}$. Hence, $x - \eta \mid 2^{b+1}(2^b - p^{r-m})$. We therefore get that $2p^{2m} \leq x + 1$ and $x - 1 \leq 2^{b+1}(2^b - p^{r-m})$. Thus,

$$2p^{2m} \leq 2^{b+1}(2^b - p^{r-m}) + 2 = 2^{2b+1} - 2^{b+1}p^{r-m} + 2 \leq 2^{2b+1} - 10,$$

because $b \geq 1$, $r - m \geq 1$, and $p \geq 3$. The above inequality leads to $p^{2m} < 2^{2b} - 5 < 2^{2b}$, therefore $p^m < 2^b$. □

Lemma 3.2. *Let* (x, b, m, r) *be a solution of equation* (1). *Then,*

(i) m *is uniquely determined by* b *and* $r - m$*;*

(ii) r *is uniquely determined by* b *and* m.

Proof. (i) Assume that b and $r - m$ are fixed. Let $b = 2b_0 + \ell$, where $\ell \in \{0, 1\}$ and put $D = 2^\ell(2^b - p^{r-m})$. Equation (1) implies that

$$x^2 - D(2^{b_0}p^m)^2 = 1.$$

In particular, $(X, Y) = (x, 2^{b_0}p^m)$ is a solution of the Pell equation $X^2 - DY^2 = 1$. It is known that all such solutions are of the form (X_k, Y_k) for some positive integer k, where (X_1, Y_1) is the minimal solution and for $k \geq 1$, the positive integers X_k and Y_k can be computed using the formula

$$X_k + Y_k\sqrt{D} = (X_1 + Y_1\sqrt{D})^k.$$

Assume now that there exist positive integers $k_1 < k_2$, such that $Y_{k_1} = 2^{b_0}p^{m_1}$ and $Y_{k_2} = 2^{b_0}p^{m_2}$. Clearly, $m_1 < m_2$, and since $Y_{k_1} \mid Y_{k_2}$, it follows that $k_1 \mid k_2$. Since all prime factors of Y_{k_2} are also prime factors of Y_{k_1}, it follows that Y_{k_2} does not have *primitive divisors* in the terminology from [2]. The results from [2] show that this is possible only for $k_2 \in \{2, 3, 4, 6, 12\}$. Moreover, it is known that if k_2/k_1 is even, then Y_{k_2}/Y_{k_1} is also even, which is not our case because for us $Y_{k_2}/Y_{k_1} = p^{m_2 - m_1}$. It is now easy to see that the only possibilities are $k_2 = 3k_1$ and $k_1 \in \{1, 2, 4\}$. Since $Y_{3k_1} = Y_{k_1}(4X_{k_1}^2 - 1)$, we get $p^{m_2 - m_1} = 4X_{k_1}^2 - 1 = (2X_{k_1} - 1)(2X_{k_1} + 1)$. The two factors $2X_{k_1} - 1$ and $2X_{k_1} + 1$ are coprime, therefore the above equation leads to $2X_{k_1} - 1 = 1$. Thus, $X_{k_1} = 1$, which is impossible because $X_{k_1}^2 - DY_{k_1}^2 = 1$ and $Y_{k_1} > 1$.

(ii) Let (x, b, m, r) be a positive integer solution of equation (1). From equation (13), we conclude that either $2^{b+1}p^{2m}$ divides one of $x+1$ or $x-1$, or 2^{b+1} divides one of them and p^{2m} divides the other. In the first case, we get that $2^{b+1}p^{2m} \mid x+\eta$ for some $\eta \in \{\pm 1\}$, therefore $x-\eta \mid 2(2^b - p^{r-m})$. Thus, $2^{b+1}p^{2m} \le x+1$ but $x-1 \le 2(2^b - p^{r-m}) < 2^{b+1}$. We then get that

$$2^{b+1} \cdot 9 \le 2^{b+1}p^{2m} \le x+1 < 2^{b+1}+2,$$

which is impossible. Hence, we must be in the second case, so we may write

$$x-\eta = 2^{b+1}\lambda, \qquad x+\eta = 2p^{2m}\mu, \qquad \lambda\mu = 2^b - p^{r-m}, \tag{14}$$

where $\eta \in \{\pm 1\}$ and λ, μ are positive integers. From equation (14), we derive

$$p^{2m}\mu - 2^b\lambda = \eta. \tag{15}$$

We now note that $\lambda < p^m$. Indeed, since $x \le 2^{b+1}p^m - (2p^m - 1) \le 2^{b+1}p^m - 5$, we have that

$$2^{b+1}\lambda = x - \eta \le x + 1 \le 2^{b+1}p^m - 4 < 2^{b+1}p^m,$$

therefore

$$\lambda < p^m. \tag{16}$$

Assume now that m and b are fixed. Let $A = p^{2m}$, $B = 2^b$. Then all positive integer solutions (μ, λ) of equation (15) for a fixed value of $\eta \in \{\pm 1\}$ are of the form $\mu = \mu_0 + B\ell$, $\lambda = \lambda_0 + A\ell$, where $\ell \ge 0$ is a nonnegative integer and (μ_0, λ_0) is the minimal solution of equation $A\mu - B\lambda = \eta$. Since for us $\lambda < p^m = A$, it follows that our values for μ and λ are the minimal ones. Hence, both λ and μ are uniquely determined and since $2^b - p^{r-m} = \lambda\mu$, it follows that $r - m$ is uniquely determined, too. It remains to show that given m and b there is at most one value of $\eta \in \{\pm 1\}$ such that if (μ_0, λ_0) denotes the minimal solution of equation (15), then $\lambda_0\mu_0 = 2^b - p^{r-m}$. Well, assume that this is not so and let (μ_0, λ_0) be the minimal solution of equation (15) for $\eta = 1$. Then $(2^b - \mu_0, p^{2m} - \lambda_0)$ is the minimal solution of equation (15) for $\eta = -1$. We then get equations

$$\lambda_0\mu_0 = 2^b - p^{r-m} \qquad \text{and} \qquad (p^{2m} - \lambda_0)(2^b - \mu_0) = 2^b - p^{r'-m},$$

for some integers r and r' both exceeding m. Substracting the first equation from the second we get

$$p^{2m}2^b - p^{2m}\mu_0 - 2^b\lambda_0 = p^{r-m} - p^{r'-m},$$

which leads to the conclusion that $p \mid 2^b\lambda_0$, which is impossible. Hence, if m and b are fixed, then $\eta \in \{\pm 1\}$ as well as λ and μ (hence, r too) are uniquely determined. □

3.2 An application of $\mathcal{S}$-unit equations

We keep the previous notations. In particular, λ, μ and η will have the meaning of (14). Here, we prove the following result.

Lemma 3.3. *There are at most 2^{3159} solutions (x, b, m, r) of equation (1) having a fixed value of λ.*

Proof. Writing $x = 2^{b+1}\lambda + \eta$ and inserting this into equation (1) we get

$$2^{2b+2}\lambda^2 + 2^{b+2}\eta\lambda + 1 = 2^{2b+2}p^{2m} - 2^{b+2}p^{r+m} + 1,$$

or

$$2^b\lambda^2 + \eta\lambda + p^{r+m} - 2^b p^{2m} = 0. \tag{17}$$

When λ is a positive integer, the above equation (17) is a particular case of an $\mathcal{S}$-unit equation as it can be rewritten as

$$\lambda(-\eta 2^b) + \frac{1}{\lambda}(-\eta p^{r+m}) + \frac{1}{\lambda}(\eta 2^b p^{2m}) = 1, \tag{18}$$

and we can take

$$(a_1, a_2, a_3) = (\lambda, 1/\lambda, 1/\lambda) \quad \text{and} \quad (x_1, x_2, x_3) = (-\eta 2^b, -\eta p^{r+m}, \eta 2^b p^{2m}).$$

It is easy to see that equation (18) is nondegenerate. Indeed, if it is degenerate, then one of the relations $2^b\lambda = -\eta$, or $p^{r+m} = -\eta\lambda$, or $2^b p^{2m} = \eta\lambda$ holds. However, none of those relations is possible because b, m and r are positive and λ is coprime to $2p$. Hence, by Theorem 2.3, we get that equation (17) has at most

$$(2^{35} \cdot 3^2)^{3^4} < \left(2^{39}\right)^{81} = 2^{3159}$$

solutions b, m and r. □

3.3 The first application of the Subspace Theorem

Let $\varepsilon > 0$ be some small positive real number to be fixed later. Here, we prove the following result.

Proposition 3.4. *There are at most*

$$2^{720}\left(2\varepsilon^{-1}\right)^{42} \tag{19}$$

positive integer solutions (x, b, m, r) of equation (1) such that

$$(2 - \varepsilon)m \log p - \log\lambda \geq \varepsilon\, b \log 2. \tag{20}$$

Proof. Let $N = 2$, $\mathbf{x} = (x_1, x_2)$. Let also $L_{i,v}$ be the linear forms in $\mathbb{Q}^2$ for $i = 1,\ 2$, and $v \in \mathcal{S}$, given by $L_{1,\infty}(\mathbf{x}) = x_1 - x_2$, $L_{2,\infty}(\mathbf{x}) = x_1$, and $L_{i,v}(\mathbf{x}) = x_i$ for all $(i,v) \in \{1,2\} \times \{2,p\}$. It is clear that $L_{1,v}$ and $L_{2,v}$ satisfy condition (8) for all $v \in \mathcal{S}$. Let $\mathbf{x} = (2^b\lambda, p^m\mu) \in \mathbb{Z}^2$. Note that

$$|L_{1,\infty}(\mathbf{x})|_\infty |L_{2,\infty}(\mathbf{x})|_\infty = |p^{2m}\mu - 2^b\lambda|\, 2^b\lambda = 2^b\lambda,$$

and

$$\prod_{i=1}^{2} \prod_{v\in\{2,p\}} |L_{i,v}(\mathbf{x})|_v = |x_1|_2|x_1|_p|x_2|_2|x_2|_p = \frac{1}{2^b p^{2m}}.$$

Hence,

$$\prod_{i=1}^{2} \prod_{v\in\mathcal{S}} |L_{i,v}(\mathbf{x})|_v \leq \frac{\lambda}{p^{2m}}. \tag{21}$$

Assume that inequality (20) holds. Then

$$\log\left(\frac{p^{2m}}{\lambda}\right) = 2m\log p - \log\lambda \geq \varepsilon(b\log 2 + m\log p) = \varepsilon\log(2^b p^m),$$

therefore the inequality

$$\frac{p^{2m}}{\lambda} \geq (2^b p^m)^\varepsilon \tag{22}$$

holds. Since $2^b\lambda < 2^b p^m$ (see (16)), and

$$p^{2m}\mu = 2^b\lambda + \eta \leq 2^b\lambda + 1 \leq 2^b(p^m - 1) + 1 < 2^b p^m,$$

it follows that $2^b p^m > \max\{x_1, x_2\}$. Equations (21) and (22) now imply that the inequality

$$\prod_{i=1}^{2} \prod_{v\in\mathcal{S}} |L_{i,v}(\mathbf{x})|_v < (\max\{x_1, x_2\})^{-\varepsilon} \tag{23}$$

holds. Since $\max\{x_1, x_2\} \geq p > 2 = N$, it follows easily that the above inequality implies

$$\prod_{i=1}^{2} \prod_{v\in\mathcal{S}} |L_{i,v}(\mathbf{x})|_v < 2^{-\varepsilon/2}\,(\max\{x_1, x_2\})^{-\varepsilon/2}. \tag{24}$$

Corollary 2.2 now immediately tells us that there exist at most

$$t_1 \leq \left(2^{60\cdot 2^2}(2/\delta)^{7\cdot 2}\right)^3 = 2^{720}\left(2\varepsilon^{-1}\right)^{42}$$

finitely many proper subspaces of $\mathbb{Q}^2$ such that $\mathbf{x}$ belongs to one of those. In particular, there exist rational numbers $r_1, \ldots, r_{t_1}$ such that $x_1/x_2 = r_j$ for some $j \in \{1, \ldots, t_1\}$. This implies that $p^{2m}\mu/2^b\lambda = r_j$, and since λ and μ are odd, coprime (see equation (15)), and coprime to p, it follows that m, b, λ and μ are uniquely determined in terms of r_j. Since $\lambda\mu = 2^b - p^{r-m}$, it follows that r is also uniquely determined in terms of r_j. □

3.4 The second application of the Subspace Theorem

From now on, by Proposition 3.4, we may assume that $\varepsilon \in (0,1)$ is as small as we wish and that (x,b,m,r) is a positive solution of equation (1) with $(2-\varepsilon)m\log p - \log\lambda < \varepsilon b \log 2$. We assume that $\varepsilon < 1/10$.

We first make some observations about these solutions. Clearly,

$$p^{2m} < 2^{\frac{2\varepsilon b}{2-\varepsilon}} \lambda^{\frac{2}{2-\varepsilon}} < 2^{\frac{\varepsilon b}{1-\varepsilon}} \lambda^{\frac{1}{1-\varepsilon}}. \tag{25}$$

Furthermore,

$$2^b\lambda - 1 \le p^{2m}\mu < 2^{\frac{\varepsilon b}{1-\varepsilon}} \lambda^{\frac{\varepsilon}{1-\varepsilon}} (\lambda\mu) = 2^{\frac{\varepsilon b}{1-\varepsilon}} \lambda^{\frac{\varepsilon}{1-\varepsilon}} (2^b - p^{r-m}) < 2^b \cdot 2^{\frac{\varepsilon b}{1-\varepsilon}} \lambda^{\frac{\varepsilon}{1-\varepsilon}};$$

hence,

$$\lambda < 2 \cdot 2^{\frac{\varepsilon b}{1-\varepsilon}} \lambda^{\frac{\varepsilon}{1-\varepsilon}},$$

leading to

$$\lambda < 2^{\frac{1-\varepsilon}{1-2\varepsilon}} \cdot 2^{\frac{\varepsilon b}{1-2\varepsilon}}. \tag{26}$$

Inserting estimate (26) into estimate (25), we get

$$p^{2m} < 2^{\frac{1}{1-2\varepsilon}} \cdot 2^{\varepsilon b\left(\frac{1}{1-\varepsilon} + \frac{1}{(1-\varepsilon)(1-2\varepsilon)}\right)}, \tag{27}$$

therefore

$$\lambda p^{2m} < 2^{\frac{2-\varepsilon}{1-2\varepsilon}} \cdot 2^{\varepsilon b\left(\frac{1}{1-\varepsilon} + \frac{1}{1-2\varepsilon} + \frac{1}{(1-\varepsilon)(1-2\varepsilon)}\right)}.$$

Since

$$\frac{2-\varepsilon}{1-2\varepsilon} < 3 \qquad \text{and} \qquad \frac{1}{1-\varepsilon} + \frac{1}{1-2\varepsilon} + \frac{1}{(1-\varepsilon)(1-2\varepsilon)} < 4$$

when $\varepsilon < 1/10$, we get that in this case

$$\lambda p^{2m} < 8 \cdot 2^{4\varepsilon b}. \tag{28}$$

Furthermore, by inequality (27) and the fact that

$$\frac{1}{1-2\varepsilon} < 2 \qquad \text{and} \qquad \frac{1}{1-\varepsilon} + \frac{1}{(1-\varepsilon)(1-2\varepsilon)} < 3$$

for $\varepsilon < 1/10$, we also get that

$$p^{2m} < 4 \cdot 2^{3\varepsilon b}. \tag{29}$$

We now observe the approximation

$$\frac{1}{2^b\lambda + \eta} = \frac{1}{2^b\lambda\,(1+\eta/(2^b\lambda))} = \frac{1}{2^b\lambda} + O\left(\frac{1}{(2^b\lambda)^2}\right),$$

where the constant implied by the above O can be taken to be 2. Multiplying the above estimate by $2^b - p^{r-m}$, we get that

$$\Big|\frac{2^b - p^{r-m}}{2^b\lambda + \eta} - \frac{1}{\lambda} + \frac{p^{r-m}}{2^b\lambda}\Big| \le \frac{4}{2^b}. \tag{30}$$

We put $N = 3$ and let $L_{i,v}$ for $(i, v) \in \{1, 2, 3\} \times \mathcal{S}$ be the linear forms given by

$$L_{1,\infty}(\mathbf{x}) = x_1 - x_2 + x_3,$$

and $L_{j,v}(\mathbf{x}) = x_j$ for all other choices $(j, v) \in \{1, 2, 3\} \times \mathcal{S}\backslash\{(1, \infty)\}$. It is easy to see that the forms $L_{1,v}, L_{2,v}, L_{3,v}$ fulfill condition (8) for all $v \in \mathcal{S}$. Note that we may write

$$\frac{2^b - p^{r-m}}{2^b\lambda + \eta} = \frac{\lambda}{p^{2m}}. \tag{31}$$

Let $B = p^{2m}2^b\lambda$. We evaluate the double product appearing in the left hand side of inequality (4) for the vector $B\mathbf{x}$, where

$$x_1 = \frac{2^b - p^{r-m}}{2^b\lambda + \eta}, \qquad x_2 = \frac{1}{\lambda}, \qquad x_3 = \frac{p^{r-m}}{2^b\lambda}. \tag{32}$$

It is easy to see that $B\mathbf{x} \in \mathbb{Z}^N$. By estimate (30), we have

$$|L_{1,\infty}(B\mathbf{x})|_\infty \le \frac{4B}{2^b} = 4\lambda p^{2m}, \tag{33}$$

while

$$\prod_{v\in\{2,p\}} |L_{1,v}(B\mathbf{x})|_v = \prod_{v\in\{2,p\}} |Bx_1|_v = \prod_{v\in\{2,p\}} |2^b\lambda^2|_v = \frac{1}{2^b}. \tag{34}$$

For the remaining forms, we have

$$\prod_{j=2}^{3}\prod_{v\in\mathcal{S}} |L_{j,v}(B\mathbf{x})|_v = \prod_{v\in\mathcal{S}} \Big|\frac{B}{\lambda}\Big|_v \Big|\frac{p^{r-m}B}{2^b\lambda}\Big|_v = \prod_{v\in\mathcal{S}} |2^bp^{2m}|_v|p^{r+m}|_v = 1. \tag{35}$$

Multiplying estimates (33), (34) and (35) and using inequality (28), we get

$$\prod_{j=1}^{3}\prod_{v\in\mathcal{S}} |L_{j,v}(B\mathbf{x})|_v \le \frac{4\lambda p^{2m}}{2^b} < \frac{32}{(2^b)^{1-4\varepsilon}}.$$

Furthermore, since

$$\max\{Bx_1, Bx_2, Bx_3\} = \max\{2^b\lambda, 2^bp^{2m}, p^r\} = 2^bp^{2m} < 4 \cdot 2^{b(1+3\varepsilon)},$$

(see (29)), it follows that the above inequality implies that

$$\begin{aligned}\prod_{j=1}^{3}\prod_{v\in\mathcal{S}} |L_{j,v}(B\mathbf{x})|_v &< \frac{32}{(2^b)^{1-4\varepsilon}} < 32 \cdot 4^{\frac{1+3\varepsilon}{1-4\varepsilon}} \cdot (\max\{Bx_1, Bx_2, Bx_3\})^{-\frac{1-4\varepsilon}{1+3\varepsilon}} \\ &< 2^{10}\left(\max\{Bx_1, Bx_2, Bx_3\}\right)^{-2\delta}, \end{aligned} \tag{36}$$

where we set $\delta = \dfrac{(1-4\varepsilon)}{2(1+3\varepsilon)}$. In the last inequality above we used the fact that

$$\frac{1+3\varepsilon}{1-4\varepsilon} < 2.5$$

for $\varepsilon < 1/10$.

Let us suppose first that $\max\{Bx_1, Bx_2, Bx_3\} \le \left(3 \cdot 2^{10}\right)^{\delta^{-1}}$. Then $2^b < \max\{Bx_1, Bx_2, Bx_3\} < \left(3 \cdot 2^{10}\right)^{\delta^{-1}}$, therefore $b < 12\delta^{-1}$. Since $p^{r-m} < 2^b$, we get that $r - m < 12\delta^{-1}$, and, by Lemma 3.2, it follows that there are at most $(12\delta^{-1})^2$ such solutions (x, b, m, r). When $\max\{Bx_1, Bx_2, Bx_3\} > \left(3 \cdot 2^{10}\right)^{\delta^{-1}}$, then the above inequality (36) implies

$$\prod_{j=1}^{3} \prod_{v \in \mathcal{S}} |L_{j,v}(B\mathbf{x})|_v < 3^{-1} \left(\max\{Bx_1, Bx_2, Bx_3\}\right)^{-\delta},$$

and, by Corollary 2.2, it follows that all the solutions $\mathbf{x}$ of the above inequality belong to at most

$$t_1 \le \left(2^{60 \cdot 3^2} \delta^{-7 \cdot 3}\right)^3 = 2^{1620} \left(\frac{2(1+4\varepsilon)}{1-3\varepsilon}\right)^{63}$$

proper subspaces of $\mathbb{Q}^3$. We now take $\varepsilon = 1/11$. Then $\delta = 1/4$. By the above remarks and Proposition 3.4, it follows that except for at most

$$2^{720} \cdot 22^{42} + 48^2 < 2 \cdot 2^{720} \cdot (2^5)^{42} = 2^{931}$$

solutions (x, b, m, r) of equation (1), all the other ones have the property that (x_1, x_2, x_3) belongs to at most

$$2^{1620} \cdot (2^2)^{63} = 2^{1746}$$

proper subspaces of $\mathbb{Q}^3$. Let $c_1x_1 + c_2x_2 + c_3x_3 = 0$ be one of such subspaces. The proof of the Theorem 1.3 will be completed by the following lemma.

Lemma 3.5. *Let $\mathcal{T}$ be a proper subspace of $\mathbb{Q}^3$. Then there exist at most $2^{28,200}$ solutions (x_1, x_2, x_3) on $\mathcal{T}$ of the form*

$$(x_1, x_2, x_3) = \left(\frac{\lambda}{p^{2m}}, \frac{1}{\lambda}, \frac{p^{r-m}}{2^b \lambda}\right) \tag{37}$$

with some positive integer $\lambda > 1$, coprime to $2p$ and satisfying equation (17).

Proof. Let $c_1x_1 + c_2x_2 + c_3x_3 = 0$ be the defining equation of $\mathcal{T}$. If $c_1 = 0$, then $2^b c_2 + c_3 p^{r-m} = 0$. Clearly, $c_2c_3 \neq 0$ and now b and $r - m$ are uniquely determined. By Lemma 3.2, m is also uniquely determined. So, we may assume that $c_1 \neq 0$. In particular, we may take $c_1 = 1$. If $c_2 = 0$, we then get the equation $\lambda^2 2^b = -c_3 p^{r-m}$, and since λ is coprime to $2p$, it follows that λ, b, and $r - m$ are uniquely determined. By Lemma 3.2, m is also uniquely determined. Thus, we may assume that

$c_2 \neq 0$. If $c_3 = 0$, we then get $\lambda^2 = -c_2 p^{2m}$, which shows that λ and m are uniquely determined. Since λ and m are fixed, Lemma 3.3 shows that equation (17) has at most 2^{3159} solutions $(b, r+m)$. Hence, if $c_3 = 0$, then there are at most 2^{3159} solutions (λ, b, m, r). Assume now that $c_2 c_3 \neq 0$. By substituting the values of x_1, x_2 and x_3 given by (32) into the defining equation of $\mathcal{T}$, we obtain

$$\frac{2^b - p^{r-m}}{2^b\lambda + \eta} + c_2\frac{1}{\lambda} + c_3\frac{p^{r-m}}{2^b\lambda} = 0,$$

which is equivalent to

$$2^b\lambda((1+c_2)2^b + (c_3-1)p^{r-m}) = -\eta(c_2 2^b + c_3 p^{r-m}).$$

If $(1+c_2)2^b + (c_3-1)p^{r-m} = 0$, then also $c_2 2^b + c_3 p^{r-m} = 0$, which is impossible. Assume now that $(1+c_2)2^b + (c_3-1)p^{r-m} \neq 0$. Then,

$$2^b\lambda = -\eta\frac{c_2 2^b + c_3 p^{r-m}}{(1+c_2)2^b + (c_3-1)p^{r-m}}.$$

Inserting the above relation into (17), we get

$$\begin{aligned}\left(\frac{c_2 2^b + c_3 p^{r-m}}{(1+c_2)2^b + (c_3-1)p^{r-m}}\right)^2 & - \frac{c_2 2^b + c_3 p^{r-m}}{(1+c_2)2^b + (c_3-1)p^{r-m}} \\ & + 2^b(p^{r+m} - 2^b p^{2m}) = 0,\end{aligned}$$

which can be rewritten as

$$\begin{aligned}-c_2 2^{2b} & + (c_2 - c_3)2^b p^{r-m} + c_3 p^{2(r-m)} + (c_3-1)^2 2^b p^{3r-m} \\ & - (1+c_2)^2 2^{4b} p^{2m} + (1+c_2)(c_2 - 2c_3 + 3)2^{3b} p^{r+m} \\ & + (c_3-1)(2c_2 - c_3 + 3)2^{2b} p^{2r} = 0. \qquad (38)\end{aligned}$$

The above equation is an $\mathcal{S}$-unit equation in 7 indeterminates. If it is nondegenerate, it then has at most

$$(2^{35} \cdot 7^2)^{7^3 \cdot 3} < \left(2^{41}\right)^{1029} = 2^{42,189}$$

solutions, by Theorem 2.3. For each such solution, $2^{2b}/(2^b p^{r-m})$ is uniquely determined, and by Lemma 3.2, the solution (x, b, m, r) is uniquely determined as well. It thus remains to study the degenerate cases. Every degenerate instance induces a partition of the set with (at most) seven elements into disjoint subsets of cardinality at least 2. Thus, there are at most 3 such disjoint subsets, therefore the total number of such partitions does not exceed

$$7 \cdot (2^7)^3 < 2^3 \cdot 2^{21} = 2^{24}.$$

We now show that in each of these cases, (x, b, m, r) is uniquely determined. Let

$$(y_1, \ldots, y_7) = (2^{2b}, 2^b p^{r-m}, p^{2(r-m)}, 2^b p^{3r-m}, 2^{4b} p^{2m}, 2^{3b} p^{r+m}, 2^{2b} p^{2r}).$$

Note that since $c_2c_3 \neq 0$, it follows that y_1 and y_3 effectively occur. Since y_1 appears, it follows that there must be another variable which appears in the same equation with y_1, and therefore b is uniquely determined. If two of the first three unknowns, or two of the last four unknowns appear within the same nondegenerate equation, then $r - m$ is uniquely determined and, by Lemma 3.2, (x, b, m, r) is uniquely determined. Thus, it suffices to study the case in which each subequation has exactly two terms, one from the first group of 3 and one from the last group of 4. If y_1 and y_i for $i = 4, 5, 6, 7$ appear in the same equation, then $3r - m,\ 2m,\ r + m$, or $2r$ are uniquely determined, respectively. If y_3 and y_i for $i = 4, 5, 6, 7$ appear in the same equation, then $r+m,\ 4m-2r,\ 3m-r$, or $2m$ are uniquely determined, respectively. It is now easy to see that any pair consisting of an exponent from the first group and one from the second group being determined implies that both m and r are determined, with the exceptions when one of the subequations contains y_1 and y_5 and the other y_3 and y_7, or one of the equations contains y_1 and y_6 and the other contains y_3 and y_4. Assume that we are in the first instance. Then m is determined. Since the coefficient of y_7 is $(c_3 - 1)(2c_2 - c_3 + 1)$ is nonzero, it follows that $c_3 \neq 1$. Hence, y_4 appears. If it appears in the same subequation with y_1 (hence, also y_5) or with y_3 (hence, also y_7), we get immediately that r is also determined. If not, it must appear in a different equation involving at least one of y_2 or y_6, and it is easy to see that r is also determined. Assume that we are in the second instance. Then $r + m$ is determined. Since the coefficient of y_6 is $(1 + c_2)(c_2 - 2c_3 + 3)$ is nonzero, we get that $1 + c_2 \neq 0$. Hence, y_5 also appears with nonzero coefficient. If y_5 appears in the same equation as y_1 (hence, as y_6 also), we get that m is determined, therefore both r and m are determined, while if y_5 appears in the same equation as y_3 (hence, as y_4), then $2r - 4m$ is determined, therefore again both r and m are determined. Finally, if y_5 does not appear in any of the above two equations, then it must appear in an equation involving either y_2 or y_7. Hence, either $r - 3m$ or $2m - 2r$ are determined, therefore both r and m are determined. This completes the proof of the claim that every solution of equation (38) determines (x, b, m, r) uniquely. Since the function $(2^{35}(N^2))^{N^3 s}$ is subadditive in N for fixed s, it follows that the totality of solutions does not exceed

$$2^{24} \cdot 2^{42,189} < 2^{42,213}$$

which completes the proof of Lemma 3.5. □

To summarize, except for 2^{931} solutions (x, b, m, r) of equation (1), each solution has the property that the vector $\mathbf{x}$ shown at (37) lies on one of at most 2^{1746} proper subspaces of $\mathbb{Q}^3$, and each one of such subspaces contains no more than $2^{42,213}$ such points $\mathbf{x}$ by Lemma 3.5. Thus, the total number of solutions (x, b, m, r) of equation (1) does not exceed

$$2^{931} + 2^{1746} \cdot 2^{42,213} < 2^{50,000},$$

which completes the proof of Theorem 1.3.

4 Comments

The bound we found for the number of solutions does not depend on the fixed prime p. It is perhaps true that a refined version of our argument can be used to prove the following more general result. Let $\mathcal{S}$ be a fixed finite set of prime numbers of cardinality s. Then, the diophantine equation

$$x^2 = u^{2b+2}v^{2m} - u^{b+2}v^{m+r} + 1$$

in positive integers x, u, v, b, m, r with coprime $\mathcal{S}$-units $u > 1$ and $v > 1$ has only finitely many solutions. Moreover, the number of such solutions does not exceed a computable number depending only on s. We have not verified the details of such a result.

References

[1] 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.* **26** (1982), 365-384.

[2] R.D. Carmichael, 'On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$', *Ann. of Math.* **15** (1913), 30–70.

[3] J.-H. Evertse, 'The number of solutions of decomposable form equations', *Invent. Math.* **122** (1995), 559–601.

[4] J.-H. Evertse, 'An improvement of the Quantitative Subspace Theorem', *Compos. Math.* **101** (1996), 225–311.

[5] D. Jungnickel, 'Difference Sets', In J.Dinitz, D.R. Stinson (ed.) *Contemporary Design Theory, A Colection of Surveys.* Wiley-Interscience Series in Discrete Mathematics and Optimization (1992), 241–324.

[6] M. Le and Q. Xiang, 'A result on Ma's conjecture', *J. Combin. Theory Ser. A* **73** (1996), 181–184.

[7] F. Luca, 'On the equation $x^2 = 4y^{m+n} \pm 4y^n + 1$'. *Bull. Math. Soc. Sci. Math. Roumanie* **90** (1999), 231-235.

[8] F. Luca, 'On the Diophantine equation $x^2 = 4q^m - 4q^n + 1$', *Proc. Amer. Math. Soc.* **131** (2003), 1339-1345.

[9] F. Luca, 'The Diophantine equation $x^2 = p^a \pm p^b + 1$', *Acta Arith.* **112** (2004), 87-101.

[10] S.L. Ma, 'McFarland's conjecture on abelian difference sets with multiplier -1', *Designs, Codes and Cryptography* **1** (1992), 321–322.

[11] R.L. McFarland 'A family of difference sets in non-cyclic groups', *J. Combin. Theory Ser. A* **15** (1973), 1–10.

[12] W. M. Schmidt, *Diophantine Approximations*, Springer Verlag, LNM **785** (1980).

[13] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Springer Verlag, LNM **1467** (1991).

[14] N. Tzanakis, J. Wolfskill, 'On the Diophantine equation $y^2 = 4q^n + 4q + 1$', *J. Number Theory* **23** (1986), 219-237.

[15] N. Tzanakis, J. Wolfskill, 'The Diophantine equation $x^2 = 4q^{a/2}+4q+1$, with an application to coding theory', *J. Number Theory* **26** (1987), 96-116.

Affiliations:

(F.L.): Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México; fluca@matmor.unam.mx

(P.S.): Auburn University Montgomery, Department of Mathematics, P.O. Box 244023, Montgomery, AL 36124-4023, USA; pstanica@mail.aum.edu

Eingegangen am 13. Januar 2005