PRIME-POWER DIOPHANTINE TUPLES

ANDREJ DUJELLA

Dedicated to the memory of my dear friend and coauthor Florian Luca

ABSTRACT. A positive $D(n)$-m-tuple is a set $A = \{a_1, \dots, a_m\}$ of distinct positive integers such that $a_i a_j + n$ is a square for every $i \neq j$. In 2005, Dujella and Luca obtained an absolute bound for the cardinality of a $D(p)$- or $D(-p)$-tuple of positive integers, uniformly in the prime p. We extend the underlying gap argument to prime powers. An explicit toric elimination certificate, proved by elementary linear algebra, replaces the unsaturated homogeneous elimination step and is valid modulo every prime power. Explicit degree and height bounds for this eliminant yield a uniform gap principle. Combined with the general bound for bounded $|n|$, this shows that every positive reduced $D(\pm p^r)$-tuple (i.e. tuple with elements not divisible by p) has less than 2^{121} elements, independently of p and r. Thus, every positive $D(\pm p)$-tuple has at most 2^{121} elements, positive $D(\pm p^2)$-tuples have less than 2^{122} elements, and the maximal cardinality of a positive $D(\pm p^r)$-tuple is $O(r)$ uniformly in p. In particular, this answers Problem 5.6 of [7].

1. INTRODUCTION

Let n be a nonzero integer. A $D(n)$-m-tuple is a set $A = \{a_1, \dots, a_m\}$ of distinct nonzero integers such that $a_i a_j + n$ is a square for every $i \neq j$. If elements of a $D(n)$-m-tuple are positive integers, we call such set a positive $D(n)$-m-tuple. Diophantus found a $D(256)$-quadruple $\{1, 33, 68, 105\}$ while the first $D(1)$-quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat (see Sections 1.1 and 1.2 of [6]).

Let M_n^+ denote the supremum of the cardinalities of positive $D(n)$-tuples. By an elementary argument, Brown [3] proved that $M_n^+ = 3$ if $n \equiv 2 \pmod 4$. In particular, $M_2^+ = 3$ and $M_{-2}^+ = 3$. Other known values of M_n^+ (obtained by much more involved methods, in particular, Baker's method on linear forms in logarithms of algebraic numbers) are: $M_1^+ = 4$ (by He, Togbé, and Ziegler [9]), $M_4^+ = 4$ (by Bliznac Trebješanin and Filipin [1]), and $M_{-1}^+ = 3$ (by Bonciocat, Cipu, Mignotte [2]); their result also implies $M_{-4}^+ = 3$, since all elements of a $D(-4)$-quadruple are even.

Dujella and Luca [8] obtained the uniform estimate $M_p^+, M_{-p}^+ < 3 \cdot 2^{168}$ for primes p, together with a bound depending only on the number of prime divisors in the squarefree setting. For general n, Yip [10] proved the asymptotic estimate

$$M_n^+ \leq (2 + o(1)) \log |n| \qquad (|n| \to \infty).$$

In this paper, for prime powers we seek a bound independent of the size of the prime, despite the repeated prime factor. Section 5.2.4 of [6] gives a concise exposition of the gap-principle strategy for prime parameters. The passage to prime powers requires concentration of the full p-power in one factor, a separate 2-adic analysis, and a replacement for the homogeneous elimination step. The latter is supplied below by an explicit toric certificate, which works on the locus where all tuple coordinates are units modulo p^r. If $n = \varepsilon p^r$, where p is prime and $\varepsilon \in \{\pm 1\}$, we call such a $D(n)$-tuple *reduced* if $p \nmid a$ for every $a \in A$.

Put

$$C_{\mathrm{red}} := 2^{121}.$$

2020 *Mathematics Subject Classification.* Primary 11D09; Secondary 11D45.

Key words and phrases. Diophantine tuples, property $D(n)$, prime powers, gap principle, elimination.

Theorem 1.1 (reduced prime powers)**.** *Let p be a prime, $r \geq 1$, and $\varepsilon \in \{\pm 1\}$. Every positive reduced $D(\varepsilon p^r)$-tuple has less than C_{red} elements. The bound is independent of p, r, and ε.*

Corollary 1.2 (prime parameters)**.** *Let p be a prime and $\varepsilon \in \{\pm 1\}$. Every positive $D(\varepsilon p)$-tuple has at most $C_{\mathrm{red}} = 2^{121}$ elements.*

Corollary 1.3 (prime squares)**.** *Let p be a prime and $\varepsilon \in \{\pm 1\}$. Every positive $D(\varepsilon p^2)$-tuple has less than $C_{\mathrm{red}} + 4 < 2^{122}$ elements. If arbitrary nonzero integer elements are allowed, every $D(p^2)$-tuple has less than $2C_{\mathrm{red}} + 8 < 2^{123}$ elements, whereas every $D(-p^2)$-tuple satisfies the same bound as in the positive case.*

More generally, for $r \geq 2$ we shall prove

$$M^{+}_{\varepsilon p^r} \leq C_{\mathrm{red}} + M^{+}_{\varepsilon p^{r-2}}. \tag{1}$$

Therefore,

$$M^{+}_{\varepsilon p^{2s}} \leq sC_{\mathrm{red}} + 4, \qquad M^{+}_{\varepsilon p^{2s+1}} \leq (s+1)C_{\mathrm{red}},$$

and hence $M^{+}_{\pm p^r} = O(r)$ with an absolute effective implied constant, uniformly in p.

2. Preliminary lower bounds

Write $N = p^r$. The following elementary reduction will be used repeatedly.

Lemma 2.1. *Let $A = \{a_1 < a_2 < \cdots\}$ be a positive reduced $D(\varepsilon N)$-tuple. If $\varepsilon = 1$, then $a_3 > N^{1/4}$, so at most two elements fail the lower bound $a > N^{1/4}$. If $\varepsilon = -1$, then $a_2 > N^{1/2}$, so at most one element fails the stronger lower bound $a > N^{1/2}$.*

Proof. Suppose first that $\varepsilon = 1$, and write

$$a_1a_3 + N = x_{13}^2, \qquad a_2a_3 + N = x_{23}^2.$$

Then $x_{23} > x_{13} > \sqrt{N}$, and therefore

$$a_3(a_2 - a_1) = x_{23}^2 - x_{13}^2 = (x_{23} - x_{13})(x_{23} + x_{13}) > 2\sqrt{N}.$$

Since $a_2 - a_1 < a_3$, this gives $a_3 > N^{1/4}$.

Now let $\varepsilon = -1$. Reducedness rules out $x_{12} = 0$ in $a_1a_2 - N = x_{12}^2$, because $a_1a_2 = N$ would force a factor p in one of a_1, a_2. Thus

$$a_1a_2 = N + x_{12}^2 > N,$$

and hence $a_2^2 > a_1a_2 > N$. ☐

3. The prime-power factorization

Write

$$N = p^r, \qquad n = \varepsilon N.$$

Let $a < b < c$ be elements of a reduced $D(\varepsilon N)$-tuple and write

$$ab + \varepsilon N = x^2, \qquad ac + \varepsilon N = z^2, \qquad bc + \varepsilon N = y^2,$$

with $x, y, z \geq 0$. Put

$$P = abc, \qquad S = a + b + c,$$

and define, as in Section 5.2.4 of [6],

$$e = \varepsilon NS + 2P - 2xyz, \qquad \bar{e} = \varepsilon NS + 2P + 2xyz. \tag{2}$$

A direct computation gives

$$e\bar{e} = N^2(c - a - b + 2x)(c - a - b - 2x). \tag{3}$$

The common value in (3) is zero exactly in the regular cases

$$c = a + b \pm 2x. \tag{4}$$

For $D(N)$ only the plus sign can give $c > b$, while both signs may occur for $D(-N)$.

Lemma 3.1. *Assume that the triple is not regular.*

(1) *If p is odd, then exactly one of $e, \bar{e}$ is divisible by N^2.*
(2) *If $p = 2$ and $r \geq 3$, then*

$$\{v_2(e), v_2(\bar{e})\} = \{2, 2r - 2\}.$$

In particular, exactly one of $e, \bar{e}$ is divisible by $N^2/4$.

Proof. If p is odd, then $\bar{e} - e = 4xyz$. Since the tuple is reduced, $p \nmid xyz$, and hence e and $\bar{e}$ cannot both be divisible by p. Equation (3) implies that the whole factor $N^2 = p^{2r}$ divides exactly one of them.

Let $p = 2$ and $r \geq 3$. The elements a, b, c and the square roots x, y, z are odd. Hence $4 \mid e$ and $4 \mid \bar{e}$, while

$$v_2(\bar{e} - e) = v_2(4xyz) = 2.$$

Moreover $c - a - b$ and x are odd, so $(c - a - b)^2 - 4x^2$ is odd. Taking 2-adic valuations in (3) gives $v_2(e) + v_2(\bar{e}) = 2r$. The smaller valuation is exactly 2, which proves the statement. □

Put

$$\eta = \begin{cases} 1, & p \text{ odd}, \\ 4, & p = 2. \end{cases}$$

For $p = 2$ this notation will only be used when $r \geq 3$. Note that the cases $N = 2, 4$ are solved by the results mentioned in Introduction. For a nonregular triple, we say that it lies in the *e-branch* if $N^2/\eta \mid e$, and in the *$\bar{e}$-branch* otherwise. By Lemma 3.1, these are the only two possibilities and exactly one occurs.

4. The easy branch

Let

$$\mathcal{R} = (c - a - b)^2 - 4x^2 = a^2 + b^2 + c^2 - 2ab - 2ac - 2bc - 4\varepsilon N.$$

Then $e\bar{e} = N^2\mathcal{R}$, and, since $a, b < c$,

$$|\mathcal{R}| < 9c^2 + 4N. \tag{5}$$

Lemma 4.1. *Assume that $N > 2^{2^{117}}$, the triple is nonregular, and $N^2/\eta \mid e$. Assume also $a > N^{1/4}$ if $\varepsilon = 1$, and $a > N^{1/2}$ if $\varepsilon = -1$. Then*

$$c > N^{1/8}b.$$

Proof. Suppose first that $\varepsilon = 1$. Since $xyz > P$, we have $\bar{e} > 4P$. From $|e| \geq N^2/\eta$, (3), and (5),

$$4abc < \bar{e} \leq \eta|\mathcal{R}| < \eta(9c^2 + 4N).$$

If $c^2 \leq N$, then the right-hand side is $< 13\eta N$, while $\bar{e} > NS > 3N^{5/4}$, a contradiction. Hence $c^2 > N$, and $4abc < 13\eta c^2$. Therefore

$$c > \frac{4ab}{13\eta} > N^{1/8}b.$$

Now let $\varepsilon = -1$. Since $ab, ac, bc > N$, we have $x < \sqrt{ab}$, $z < \sqrt{ac}$ and $y < \sqrt{bc}$, and hence $xyz < P$. Put $\Delta_0 = P - xyz > 0$. We have

$$P^2 - (xyz)^2 = NPS - N^2(ab + ac + bc) + N^3 < NPS,$$

so $\Delta_0 < NS$ and

$$|e| = |2\Delta_0 - NS| < NS. \tag{6}$$

The divisibility assumption gives $S > N/\eta$, hence

$$c > \frac{N}{3\eta}. \tag{7}$$

If $b \le N^{7/8}/(3\eta)$, this already gives $c > N^{1/8}b$.

Assume $b > N^{7/8}/(3\eta)$. Since $a > N^{1/2}$, we have $ab > N^{11/8}/(3\eta)$. Put

$$u = \frac{N}{ab}, \qquad v = \frac{N}{ac}, \qquad w = \frac{N}{bc}, \qquad \rho = u + v + w.$$

Then $\rho < 9\eta N^{-3/8}$ and

$$\frac{xyz}{P} = \sqrt{(1-u)(1-v)(1-w)} \ge 1 - \rho.$$

Since $NS/P = \rho$, we have

$$\frac{\bar{e}}{P} = -\rho + 2 + 2\frac{xyz}{P} \ge 4 - 3\rho > 1.$$

Thus $\bar{e} > P$. By (7), $c^2 > N$, so

$$abc < \bar{e} \le \eta|\mathcal{R}| < 13\eta c^2.$$

Therefore,

$$c > \frac{ab}{13\eta} > \frac{N^{1/2}}{13\eta} b > N^{1/8}b.$$

$\square$

5. The hard branch and full-modulus congruences

We now suppose that the large prime-power divisor occurs in $\bar{e}$ for all triples under consideration. For odd p, $N^2 \mid \bar{e}$ gives

$$xyz \equiv -abc \pmod{N}. \tag{8}$$

For $p = 2$, $r \ge 3$, Lemma 3.1 gives $v_2(\bar{e}) = 2r - 2$. Put $h = N/2$. Since $\bar{e}/2$ is divisible by N,

$$xyz + abc + \varepsilon h(a + b + c) \equiv 0 \pmod{N}.$$

The sum $a + b + c$ is odd and $h \equiv -h \pmod{N}$, so

$$xyz \equiv -abc + h \pmod{N}. \tag{9}$$

The term h disappears when two such triple congruences are multiplied.

Lemma 5.1. *Let $a < b < c < d$ belong to a reduced $D(\varepsilon N)$-tuple and write*

$$\begin{aligned} ab + \varepsilon N &= x_1^2, \quad ac + \varepsilon N = x_2^2, \quad bc + \varepsilon N = x_3^2, \\ ad + \varepsilon N &= x_4^2, \quad bd + \varepsilon N = x_5^2, \quad cd + \varepsilon N = x_6^2. \end{aligned}$$

Assume that every triple among a, b, c, d is in the $\bar{e}$-branch. Then

$$x_1x_6 \equiv x_2x_5 \equiv x_3x_4 \pmod{N}. \tag{10}$$

Proof. For odd p this is Lemma 3.1 of [8], with the same proof in $\mathbb{Z}/N\mathbb{Z}$. All elements being cancelled are units modulo N.

For $p = 2$, multiply (9) for (a, b, c) and (a, b, d). The right-hand side is

$$(-abc + h)(-abd + h) = a^2b^2cd - hab(c + d) + h^2 \equiv a^2b^2cd \pmod{N},$$

because $c + d$ is even and $h^2 \equiv 0 \pmod{N}$. Cancelling the unit $x_1^2 \equiv ab \pmod{N}$ gives $x_2x_3x_4x_5 \equiv abcd \pmod{N}$. The triples (a, b, c) and (a, c, d) give $x_1x_3x_4x_6 \equiv abcd \pmod{N}$. Cancelling x_3x_4 yields the first congruence in (10). The rest follows by permutation. $\square$

Define positive integers

$$\lambda_1 = \frac{\varepsilon(x_1x_6 - x_2x_5)}{N},$$
$$\lambda_2 = \frac{\varepsilon(x_1x_6 - x_3x_4)}{N}, \tag{11}$$
$$\lambda_3 = \frac{\varepsilon(x_2x_5 - x_3x_4)}{N}.$$

The exact identities are

$$(d-a)(c-b) = \lambda_1(x_1x_6 + x_2x_5),$$
$$(d-b)(c-a) = \lambda_2(x_1x_6 + x_3x_4), \tag{12}$$
$$(d-c)(b-a) = \lambda_3(x_2x_5 + x_3x_4).$$

If $\varepsilon = 1$, then, for example,

$$d^2 > (d-a)(c-b) = \lambda_1(x_1x_6 + x_2x_5) > 2\lambda_1\sqrt{abcd} > \lambda_1 a^2.$$

Hence

$$d > \sqrt{\lambda_i}\, a \qquad (i = 1,2,3), \tag{13}$$

and the arguments for λ_2 and λ_3 are identical. For the negative sign one needs the following observation.

Lemma 5.2. *Assume $\varepsilon = -1$, every one of the four triples contained in $\{a,b,c,d\}$ lies in the $\bar{e}$-branch, and $N > 2^{2^{117}}$. Then either*

$$c > N^{1/16}a,$$

or (13) *holds for $i = 1,2,3$.*

Proof. Apply the $\bar{e}$-branch to the sorted triple $a < b < c$. If $\bar{e} < 0$, then $|\bar{e}| \geq N^2/\eta$ gives $S > N/\eta$. Also $2(P + xyz) < NS < 3Nc$, hence $ab < 3N/2$, and therefore

$$\frac{c}{a} > \frac{N/(3\eta)}{\sqrt{3N/2}} > N^{1/16}.$$

Suppose $\bar{e} > 0$. Since $\bar{e} < 4P$ and $\bar{e} \geq N^2/\eta$,

$$abc > \frac{N^2}{4\eta}.$$

If $ab \leq N^{5/4}$, then $c > N^{3/4}/(4\eta)$ and $a \leq N^{5/8}$, so again $c > N^{1/16}a$.

It remains to consider $ab > N^{5/4}$. Every pair uv among a,b,c,d then satisfies $uv > N^{5/4}$ and

$$\sqrt{uv - N} > \sqrt{uv}\sqrt{1 - N^{-1/4}}.$$

Hence

$$x_1x_6 + x_2x_5 > 2(1 - N^{-1/4})\sqrt{abcd} > \sqrt{abcd}.$$

The first identity in (12) gives

$$d^2 > (d-a)(c-b) > \lambda_1\sqrt{abcd} > \lambda_1 a^2.$$

The arguments for λ_2 and λ_3 are identical. ☐

We shall also need the polynomial congruence attached to a quadruple. By (10) and (12),

$$(d-a)^2(c-b)^2 \equiv 4\lambda_1^2(x_1x_6)^2 \equiv 4\lambda_1^2 abcd \pmod{N}.$$

The analogous congruences for λ_2 and λ_3, multiplied together, give

$$\Delta(a,b,c,d)^2 \equiv 64\Lambda(abcd)^3 \pmod{N}, \qquad \Lambda = (\lambda_1\lambda_2\lambda_3)^2, \tag{14}$$

where

$$\Delta(a,b,c,d) = (d-c)(d-b)(d-a)(c-b)(c-a)(b-a).$$

6. A toric elimination lemma

The five homogeneous equations in the elimination step have fixed coordinate base points. We therefore work explicitly on the torus, where every tuple coordinate is a unit modulo N. This gives the congruence modulo N without any division by an integer content.

Let $b_1, \dots, b_5$ be a *labelled* quintuple of pairwise distinct elements. For each i, arrange the four elements b_j, $j \neq i$, increasingly before defining the three positive parameters $\lambda_{1,i}, \lambda_{2,i}, \lambda_{3,i}$ by (11), and put

$$\Lambda_i = (\lambda_{1,i}\lambda_{2,i}\lambda_{3,i})^2, \qquad T_i = 64\Lambda_i.$$

Both Λ_i and the square of the Vandermonde product of the four retained elements are unchanged by a permutation of those four elements. Thus (14) gives

$$\Delta_i(b)^2 \equiv T_i \left(\prod_{j\neq i} b_j\right)^3 \pmod N, \tag{15}$$

where

$$\Delta_i(X) = \prod_{\substack{j<k \\ j,k\neq i}} (X_k - X_j).$$

All b_j are units modulo N. Dehomogenize at the labelled coordinate b_5 by putting, in $\mathbb{Z}/N\mathbb{Z}$,

$$t_j = b_j b_5^{-1} \quad (1 \le j \le 4), \qquad t_5 = 1.$$

After division of (15) by b_5^{12}, we obtain

$$A_i(t) \equiv T_i B_i(t) \pmod N, \tag{16}$$

where

$$A_i(t) = \Delta_i(t)^2, \qquad B_i(t) = \left(\prod_{j\neq i} t_j\right)^3.$$

Here $\deg A_i, \deg B_i \le 12$ and every $B_i(t)$ is a unit modulo N. For an integral polynomial F, let $h(F)$ denote the sum of the absolute values of its coefficients.

Lemma 6.1 (toric eliminant). *Let*

$$D_0 = 24^4 = 331776.$$

There exists a nonconstant polynomial

$$Q(T_1, \dots, T_5) \in \mathbb{Z}[T_1, \dots, T_5]$$

with

$$1 \le q := \deg Q \le 5D_0 < 2^{21}, \tag{17}$$

and polynomials

$$G_i \in \mathbb{Z}[t_1, \dots, t_4, T_1, \dots, T_5] \qquad (1 \le i \le 5)$$

such that

$$(t_1t_2t_3t_4)^{12D_0} Q(T) = \sum_{i=1}^{5} G_i(t,T)\big(A_i(t) - T_iB_i(t)\big). \tag{18}$$

The same polynomial Q may be chosen so that

$$\log_2(h(Q)64^q) < 2^{116}. \tag{19}$$

Consequently every reduced labelled quintuple satisfying (16) *satisfies*

$$Q(64\Lambda_1, \dots, 64\Lambda_5) \equiv 0 \pmod{N}. \tag{20}$$

Proof. For $\alpha = (\alpha_1, \dots, \alpha_5)$ with $0 \le \alpha_i \le D_0$, define

$$F_\alpha(t) = \prod_{i=1}^{5} A_i(t)^{\alpha_i} B_i(t)^{D_0 - \alpha_i}.$$

For a fixed variable t_j, only the four factors indexed by $i \ne j$ involve t_j. In each such factor, the t_j-degree is at most

$$6\alpha_i + 3(D_0 - \alpha_i) \le 6D_0.$$

Hence

$$\deg_{t_j} F_\alpha \le 24D_0 \qquad (j = 1, \dots, 4).$$

Therefore, the coefficient vectors of all F_α lie in a vector space of dimension at most

$$M = (24D_0 + 1)^4.$$

There are $(D_0 + 1)^5$ such polynomials. Since $D_0 = 24^4$,

$$(24D_0 + 1)^4 < [24(D_0 + 1)]^4 = D_0(D_0 + 1)^4 < (D_0 + 1)^5.$$

Thus the family is linearly dependent.

Let ρ be the rank of its integer coefficient matrix. Choose ρ linearly independent columns and one further column in their span. Choose a nonzero $\rho \times \rho$ minor of the independent columns and use the corresponding signed maximal minors to obtain an integral relation

$$\sum_\alpha c_\alpha F_\alpha(t) = 0 \tag{21}$$

supported on at most $\rho + 1$ columns. Using these same coefficients, define

$$Q(T) = \sum_\alpha c_\alpha T_1^{\alpha_1} \cdots T_5^{\alpha_5}.$$

The monomials T^α are distinct, so $Q \ne 0$. Moreover Q is nonconstant: a constant relation would be supported only at $\alpha = (0, \dots, 0)$, whereas

$$F_{\mathbf{0}} = \prod_{i=1}^{5} B_i^{D_0} \ne 0.$$

This proves (17).

Put $S(t) = \prod_i B_i(t)^{D_0}$. Since

$$\prod_{i=1}^{5} B_i(t) = (t_1 t_2 t_3 t_4)^{12},$$

we have $S = (t_1 t_2 t_3 t_4)^{12D_0}$. For each α, $F_\alpha - ST^\alpha$ belongs to the ideal generated by the five polynomials $A_i - T_i B_i$. Indeed, this follows by replacing the factors one at a time and using $U^m - V^m = (U - V)(U^{m-1} + \cdots + V^{m-1})$. Summing with the coefficients c_α in (21) gives (18). Since $t_1 t_2 t_3 t_4$ is a unit modulo N, (20) follows.

It remains to bound the same maximal-minor relation. Each Δ_i is a product of six binomials, so

$$h(A_i) \le 2^{12}, \qquad h(B_i) = 1,$$

and therefore $h(F_\alpha) \le 2^{60D_0}$. The Euclidean norm of every coefficient column is at most its ℓ^1-norm, hence at most 2^{60D_0}. Hadamard's inequality gives

$$h(Q) \le (\rho + 1) 2^{60D_0 \rho}.$$

Furthermore,

$$\rho \le (24D_0 + 1)^4 < 2^{92}, \qquad q \le 5D_0.$$

Hence,

$$\begin{aligned}\log_2\big(h(Q)64^q\big) &\le \log_2(\rho+1) + 60D_0\rho + 6q\\ &< 92 + 60D_0(24D_0+1)^4 + 30D_0\\ &< 2^{116},\end{aligned}$$

where the last inequality is a direct integer calculation. This proves (19). □

7. From the toric eliminant to a uniform gap

Assume now

$$N > 2^{2^{117}}. \tag{22}$$

Let $q = \deg Q$ and put

$$\delta = \frac{1}{12q}, \qquad \gamma = \frac{\delta}{2} = \frac{1}{24q}.$$

Since $q < 2^{21}$,

$$\gamma > 2^{-26}. \tag{23}$$

Consider a labelled quintuple of pairwise distinct elements for which none of the ten determined triples lies in the e-branch. Thus all ten triples lie in the $\bar{e}$-branch, and each of the five four-element subsets satisfies Lemma 5.1. If one of the fifteen parameters $\lambda_{j,i}$ is at least N^δ, then after arranging the relevant quadruple increasingly, (13) gives a gap of exponent γ when $\varepsilon = 1$. When $\varepsilon = -1$, Lemma 5.2 gives either the same conclusion or the stronger $N^{1/16}$-gap. We may therefore suppose that all fifteen parameters satisfy

$$\lambda_{j,i} < N^\delta.$$

Then $\Lambda_i < N^{6\delta}$, and Lemma 6.1 gives

$$Q(64\Lambda_1, \dots, 64\Lambda_5) \equiv 0 \pmod N.$$

Moreover,

$$\begin{aligned}|Q(64\Lambda_1, \dots, 64\Lambda_5)| &\le h(Q)(64N^{6\delta})^q\\ &= h(Q)64^q N^{1/2}.\end{aligned}$$

By (19) and (22),

$$h(Q)64^q < 2^{2^{116}} < N^{1/2}.$$

Hence

$$Q(64\Lambda_1, \dots, 64\Lambda_5) = 0. \tag{24}$$

We now convert (24) into a polynomial condition in the five normalized tuple elements. For real variables in a region where the radicand is positive, write

$$s_\varepsilon(u,v) = \sqrt{uv+\varepsilon}.$$

For a quadruple (x,y,z,t) set

$$U = s_\varepsilon(x,y)s_\varepsilon(z,t), \qquad V = s_\varepsilon(x,z)s_\varepsilon(y,t), \qquad W = s_\varepsilon(x,t)s_\varepsilon(y,z),$$

and define

$$\mathcal{L}_\varepsilon(x,y,z,t) = \big((U-V)(U-W)(V-W)\big)^2. \tag{25}$$

The function $\mathcal{L}_\varepsilon$ is symmetric in its four arguments, because a permutation of the four vertices permutes the three partitions represented by U, V, W.

For $z = (z_1, \dots, z_5)$ define Φ_ε componentwise by

$$(\Phi_\varepsilon(z))_i = \mathcal{L}_\varepsilon(z_1, \dots, \widehat{z_i}, \dots, z_5), \qquad 1 \le i \le 5, \tag{26}$$

where the four displayed arguments are inserted in their inherited order. The symmetry makes that order irrelevant. For a normalized tuple $z_i = b_i/\sqrt{N}$, the i-th component is precisely Λ_i.

Lemma 7.1. *For each $\varepsilon \in \{\pm 1\}$,*

$$\det D\Phi_\varepsilon(2,3,4,5,6) \neq 0.$$

Consequently, for every nonzero polynomial $Q \in \mathbb{Z}[T_1,\dots,T_5]$, the real-analytic function $Q(64\Phi_\varepsilon(z))$ is not identically zero.

Proof. Exact rational interval arithmetic gives

$$\det D\Phi_+(2,3,4,5,6) \in [-1.22625271490038, -1.22625271490037] \cdot 10^{-31},$$

$$\det D\Phi_-(2,3,4,5,6) \in [2.9335784988635907, 2.9335784988635908] \cdot 10^{-29}.$$

Both intervals exclude zero. The deterministic certificate is described in Appendix A.

On a neighbourhood of $(2,3,4,5,6)$ all ten radicands are positive, so Φ_ε is real analytic. Since its Jacobian determinant is nonzero at that point, the inverse function theorem shows that its image contains a nonempty open subset of $\mathbb{R}^5$. A nonzero polynomial cannot vanish on a nonempty open subset of $\mathbb{R}^5$. Therefore $Q(64\Phi_\varepsilon(z))$ is not identically zero. $\square$

Let

$$K = \mathbb{Q}(z_1,\dots,z_5), \qquad L = K\big(s_{ij} : 1 \le i < j \le 5\big), \qquad s_{ij}^2 = z_i z_j + \varepsilon.$$

The extension L/K is multiquadratic, hence Galois, and $[L:K] \le 2^{10}$. Put

$$G_\varepsilon(z) = Q(64\Phi_\varepsilon(z)) \in L.$$

By Lemma 7.1, $G_\varepsilon \neq 0$. It is integral over $\mathbb{Z}[z_1,\dots,z_5]$, since every s_{ij} is integral over this ring. Define

$$R_{\varepsilon,0}(z) = \mathrm{Norm}_{L/K}(G_\varepsilon) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(G_\varepsilon). \tag{27}$$

This norm belongs to K and is integral over $\mathbb{Z}[z_1,\dots,z_5]$. Since the latter ring is integrally closed,

$$R_{\varepsilon,0} \in \mathbb{Z}[z_1,\dots,z_5].$$

It is nonzero because $G_\varepsilon \neq 0$. The identity automorphism occurs in the product (27). Therefore, after any specialization at which the radicals are defined,

$$G_\varepsilon(z) = 0 \quad \Longrightarrow \quad R_{\varepsilon,0}(z) = 0. \tag{28}$$

Each conjugate of G_ε is obtained by changing some signs of the radicals and has weighted degree at most $12q$, when both the variables z_i and the radicals s_{ij} are assigned weight 1. Thus

$$\deg R_{\varepsilon,0} \le 12q\,[L:K] \le 12q\,2^{10}. \tag{29}$$

Let us put

$$\mathcal{U}_\varepsilon(x,y,z) = x^2 + y^2 + z^2 - 2xy - 2xz - 2yz - 4\varepsilon.$$

This symmetric polynomial vanishes exactly when the corresponding normalized triple is regular. Multiply $R_{\varepsilon,0}$ by the ten diagonal factors $z_i - z_j$ and by the ten factors $\mathcal{U}_\varepsilon(z_i,z_j,z_k)$, $1 \le i < j < k \le 5$. The resulting nonzero polynomial R_ε has

$$\ell := \deg R_\varepsilon \le 12q\,2^{10} + 30 < 2^{35}. \tag{30}$$

We use the elementary polynomial nonvanishing lemma: if a nonzero polynomial in s variables has total degree d and a finite set $\mathcal{M}$ has more than d elements, then the polynomial does not vanish on all of $\mathcal{M}^s$ (compare Lemma 3.2 of [8]).

Proposition 7.2. *Assume that $N > 2^{2^{117}}$. After the lower-bound reduction of Lemma 2.1, the ordered elements $a_1 < a_2 < \cdots < a_m$ of a positive reduced $D(\varepsilon N)$-tuple satisfy*

$$a_{i+\ell} > N^{\gamma} a_i \qquad (1 \le i \le m - \ell), \tag{31}$$

where $\ell < 2^{35}$ and $\gamma > 2^{-26}$.

Proof. Fix i and apply the nonvanishing lemma to

$$\mathcal{M} = \left\{ \frac{a_i}{\sqrt{N}}, \ldots, \frac{a_{i+\ell}}{\sqrt{N}} \right\}.$$

It gives a labelled point $(z_1, \ldots, z_5) \in \mathcal{M}^5$ such that $R_\varepsilon(z_1, \ldots, z_5) \neq 0$. The diagonal factors make these five entries pairwise distinct, and the symmetric regular factors ensure that none of the ten triples determined by them is regular.

If one of those ten triples lies in the e-branch, arrange that triple increasingly and apply Lemma 4.1. The resulting gap between two selected elements implies the required gap between the endpoints $a_i, a_{i+\ell}$ of the ambient block. Suppose therefore that none of the ten triples lies in the e-branch. Then all ten lie in the $\bar{e}$-branch. For each of the five four-element subsets, arrange its elements increasingly before applying Lemmas 5.1 and 5.2. If $\varepsilon = -1$, the latter lemma may already give a gap of exponent $1/16$. If some $\lambda_{j,i} \ge N^\delta$, then (13) or Lemma 5.2 gives a gap of exponent $\gamma = \delta/2$ between two selected elements, hence between the block endpoints.

Finally suppose that all fifteen parameters are less than N^δ. The labelled toric construction applies without reordering the five selected coordinates. Equation (24) gives $G_\varepsilon(z) = Q(64\Phi_\varepsilon(z)) = 0$, and (28) implies $R_{\varepsilon,0}(z) = 0$. This contradicts the chosen nonzero value of R_ε. Thus (31) holds. □

8. Proof of the main theorem and consequences

Proof of Theorem 1.1. First suppose $N \le 2^{2^{117}}$. It was proved in [5] that

$$M_n^+ \le 31 \quad (|n| \le 400), \qquad M_n^+ < 15.476 \log |n| \quad (|n| > 400),$$

where log denotes the natural logarithm. Thus, in the present range,

$$M_{\varepsilon N}^+ < 15.476\, 2^{117} \log 2 < 11 \cdot 2^{117} < 2^{121}$$

when $N > 400$, while the case $N \le 400$ is immediate.

Assume therefore that $N > 2^{2^{117}}$. By Lemma 2.1, after deleting at most two elements in the positive case, and at most one in the negative case, the lower bound $a > N^{1/4}$ holds for every remaining element. By the large-element estimate in [4] (see also [6, Proposition 5.2.1]), at most 21 elements exceed N^3. Hence, after deleting at most 23 elements, we may assume

$$N^{1/4} < a \le N^3$$

for every remaining element.

Let m_{rem} be the number of remaining elements. Iterating Proposition 7.2, gives

$$m_{\text{rem}} < \ell \left(1 + \frac{11}{4\gamma} \right).$$

Since $\ell < 2^{35}$ and $\gamma = 1/(24q)$ with $q < 2^{21}$, we have

$$\frac{11}{4\gamma} = 66q < 2^{28}.$$

Therefore $m_{\text{rem}} < 2^{64}$, and restoring the deleted elements gives $m < 2^{65} < 2^{121}$. □

Proof of Corollary 1.2. A positive $D(\varepsilon p)$-tuple contains at most one element divisible by p. Indeed, if $a = p\alpha$ and $b = p\beta$ were two such elements, then

$$ab + \varepsilon p = p(p\alpha\beta + \varepsilon)$$

would have p-adic valuation exactly 1, and hence could not be a square. The remaining subtuple is reduced. By Theorem 1.1 it contains at most $C_{\mathrm{red}} - 1$ elements, so the whole tuple has at most $C_{\mathrm{red}} = 2^{121}$ elements. □

We next prove recurrence (1). Split a positive $D(\varepsilon p^r)$-tuple into the elements divisible by p and those coprime to p. The latter subtuple is reduced. If $a = p\alpha$ and $b = p\beta$ belong to the divisible subtuple, then

$$p^2\alpha\beta + \varepsilon p^r = x^2.$$

Thus $p \mid x$, and division by p^2 gives

$$\alpha\beta + \varepsilon p^{r-2} = (x/p)^2.$$

Dividing every element of the divisible subtuple by p therefore produces a $D(\varepsilon p^{r-2})$-tuple, which proves (1).

For $r = 2$, the terminal tuple has property $D(1)$ or $D(-1)$. A positive $D(1)$-tuple has at most four elements by the result of He, Togbé and Ziegler [9], and a positive $D(-1)$-tuple has at most three elements by the result of Bonciocat, Cipu and Mignotte [2]. In particular, for either sign,

$$M^+_{\varepsilon p^2} < C_{\mathrm{red}} + 4 < 2^{122}.$$

This proves the positive part of Corollary 1.3.

If arbitrary nonzero integer elements are allowed and $n = p^2 > 0$, split the tuple into its positive and negative elements. The positive elements and the absolute values of the negative elements are each positive $D(p^2)$-tuples. Hence the whole tuple has fewer than

$$2C_{\mathrm{red}} + 8 < 2^{123}$$

elements. If $n = -p^2$, mixed signs are impossible, because the product of oppositely signed elements minus p^2 is negative. After changing all signs if necessary, the tuple is positive, so the same positive bound applies.

Finally, iterating (1) and using Corollary 1.2 gives

$$M^+_{\varepsilon p^{2s}} \le sC_{\mathrm{red}} + 4, \qquad M^+_{\varepsilon p^{2s+1}} \le (s+1)C_{\mathrm{red}}.$$

Thus $M^+_{\pm p^r} = O(r)$ uniformly in p, with an explicit linear bound.

Remark 8.1. The five homogeneous equations used in the elimination step have fixed coordinate base points. In particular, every coordinate point of $\mathbb{P}^4$ is a common zero for every value of the five parameters. Hence an unsaturated homogeneous resultant cannot by itself produce the required nonzero eliminant. Lemma 6.1 instead works on the torus and supplies an integral monomial-saturated certificate, whose monomial factor is invertible for reduced tuples modulo p^r.

Remark 8.2. For completeness, Lemma 4.1 gives an independent proof of the negative-sign easy branch. This avoids relying on the displayed lower-bound estimate following equation (4) of [8], where the comparison between xyz and abc is not in the direction used in the printed inequality. The replacement is valid for all prime powers, including powers of 2.

Appendix A. A reproducible Jacobian certificate

For completeness we describe the certification used in Lemma 7.1. At the point $(2, 3, 4, 5, 6)$ every radicand $z_i z_j + \varepsilon$ is a positive integer. Fix a decimal precision P and use integer square roots to find rational endpoints

$$\frac{k}{10^P} \leq \sqrt{m} < \frac{k+1}{10^P}$$

for each required integer m. All subsequent additions, multiplications, divisions and derivatives are carried out with exact rational interval arithmetic. The determinant is evaluated as the sum of its 120 signed permutation terms. With $P = 90$ the program prints

```
sigma 1
 decimal enclosure: ('-0.000000000000000000000000000000122625271490038',
                     '-0.000000000000000000000000000000122625271490037')
 excludes zero: True
sigma -1
 decimal enclosure: ('0.000000000000000000000000000029335784988635907',
                     '0.000000000000000000000000000029335784988635908')
 excludes zero: True
```

which are precisely the enclosures stated in Lemma 7.1. The ancillary file `jacobian_certificate.py`, available on the author's web page, uses only Python's standard-library classes `Fraction` and `isqrt`, together with integer arithmetic. It was verified with Python 3.13.5 and can be run by

```
python3 jacobian_certificate.py
```

No floating-point assumption enters the nonvanishing assertion.

Acknowledgments

The author acknowledges support from the Croatian Science Foundation under the project no. IP-2022-10-5008 (TEBAG), the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", Grant No. PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027, and the European Union: NextGenerationEU through the National Recovery and Resilience Plan 2021–2026, Institutional grant of University of Zagreb Faculty of Science (IK IA 1.1.3. Impact4Math).

The author acknowledges the use of ChatGPT 5.6 Sol (OpenAI) in this work. In particular, discussions with ChatGPT concerning earlier manuscript versions of [8] and attempts to prove nonvanishing of the eliminant led to the toric elimination lemma (Lemma 6.1). The author is responsible for the proofs, verification of results and final presentation.

The author would like to thank Tomislav Pejković and Matija Kazalicki for their useful comments and suggestions.

References

[1] M. Bliznac Trebješanin and A. Filipin, Nonexistence of $D(4)$-quintuples, *J. Number Theory* 194 (2019), 170–217.

[2] N. C. Bonciocat, M. Cipu and M. Mignotte, There is no Diophantine $D(-1)$-quadruple, *J. Lond. Math. Soc. (2)* 105 (2022), no. 1, 63–99.

[3] E. Brown, Sets in which $xy + k$ is always a square, *Math. Comp.* 45 (1985), 613–620.

[4] A. Dujella, On the size of Diophantine m-tuples, *Math. Proc. Cambridge Philos. Soc.* 132 (2002), 23–33.

[5] A. Dujella, Bounds for the size of sets with the property $D(n)$, *Glas. Mat. Ser. III* 39(59) (2004), no. 2, 199–205.

[6] A. Dujella, *Diophantine m-tuples and Elliptic Curves*, Developments in Mathematics, vol. 79, Springer, Cham, 2024.

[7] A. Dujella, *Open problems on Diophantine m-tuples and elliptic curves*, online supplement, version dated 8 August 2026. `https://web.math.pmf.unizg.hr/~duje/pdf/open2.pdf`.

[8] A. Dujella and F. Luca, Diophantine m-tuples for primes, *Int. Math. Res. Not.* 2005, no. 47, 2913–2940.

[9] B. He, A. Togbé and V. Ziegler, There is no Diophantine quintuple, *Trans. Amer. Math. Soc.* 371 (2019), no. 9, 6665–6709.

[10] C. H. Yip, Improved upper bounds on Diophantine tuples with the property $D(n)$, *Bull. Aust. Math. Soc.* 111 (2025), no. 3, 428–432.