COMPLETE n-SETS OF INTEGER TRIPLES, AND IMPROVED BOUNDS FOR $n_1(k)$

KOREA SUPERINTELLIGENCE LABS

Abstract. For a nonzero integer n, a $D(n)$-set is a set of distinct nonzero integers whose pairwise products, increased by n, are all perfect squares. Adžaga, Dujella, Kreso and Tadić asked, for each k, how small in absolute value a nonzero integer $n_1(k)$ can be when some triple of nonzero integers is a $D(n)$-set for k distinct values of n, one of them $n_1(k)$, and gave a table of upper bounds for $5 \leq k \leq 20$. Their bounds come from points on the elliptic curve induced by a triple, so each row exhibits some of the admissible n for its triple. We instead determine, for a fixed triple, *all* of them: the set of admissible n is the image of an explicit finite divisor enumeration, and sweeping that enumeration proves completeness rather than mere existence. This improves eight of the sixteen published rows, among them $|n_1(5)| \leq 4$ and $|n_1(6)| \leq 4$ in place of 36 and 215, $|n_1(7)| \leq 144$, $|n_1(8)| \leq 2304$, $|n_1(10)| \leq 103684$ and $|n_1(18)| \leq 493214400$. All sixteen rows are reproduced; the other eight are matched but not improved. Two of the improvements need no new triple: the triples printed on the rows $k = 16$ and $k = 18$ are $D(n)$-sets for 17 and for 19 values of n respectively. We also show that each of the seven published Diophantine triples that are $D(n)$-sets for four values of n carries exactly four and no more, and we add two further such triples, $\{20, 1980, 637602\}$ and $\{140, 204, 77913732\}$. All statements are formally verified in Lean 4.

1. Introduction

Following the classical terminology, for a nonzero integer n a set of distinct nonzero integers $\{a_1, \ldots, a_m\}$ is a *Diophantine m-tuple with the property $D(n)$*, or a *$D(n)$-set*, if $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$; see [1, Introduction]. A $D(1)$-set is a Diophantine m-tuple, Fermat's being $\{1, 3, 8, 120\}$.

Fix instead a triple $T = \{a, b, c\}$ of distinct nonzero integers and ask for how many *different* n it is a $D(n)$-set. Without further normalisation that number is unbounded, and [1, Section 4] explains why: if the elliptic curve $y^2 = (x + ab)(x + ac)(x + bc)$ induced by T has positive rank, one may pick m points $R_1, \ldots, R_m \in 2E(\mathbb{Q})$, choose $z \in \mathbb{Z} \setminus \{0\}$ with $z^2 x(R_i) \in \mathbb{Z}$ for all i, and then $\{az, bz, cz\}$ is a $D(z^2 x(R_i))$-set for every i. The values of n so produced grow with m, and the interesting question is how small the smallest of them can be kept. That is Question 1 of [1], which we quote verbatim.

Question 1.1 ([1, Question 1])**.** For a given positive integer k, what can be said about the smallest in absolute value nonzero integer $n_1(k)$ for which there exists a triple $\{a, b, c\}$ of nonzero integers and a set N of integers of size k containing $n_1(k)$ such that $\{a, b, c\}$ is a $D(n)$-set for all $n \in N$?

For $k \leq 4$ one has $n_1(k) = 1$, since Diophantine triples are known that are $D(n)$-sets for three further values of n [1, Section 3]. For $5 \leq k \leq 20$ the source answers Question 1.1 with the table of upper bounds reproduced as Table 2 below, obtained by the point-generating procedure just described; its stated motivation is the first row, "[o]ur initial motivation for Question 1 was to see how close to 1 we can get with $n_1(5)$. We can show that $|n_1(5)| \leq 36$" [1, Section 4]. The same authors record, in [1, Section 4] and again in [2], that they suspect $|n_1(5)| > 1$, on the basis of an unsuccessful computer search.

The source also records what shape the answer might have. Its triples are chosen to induce curves of moderate rank r with generators of small height, and the usual arguments [7, 8] suggest that $|n_1(k)|$ grows like $k^{(r+2)/r}$ — an estimate that [1, Section 4] points out ignores the heights of the generators, which conjecturally grow with the rank. Nothing below bears on that asymptotic; the improvements are to the individual rows.

We are aware of no improvement of these bounds since [1] appeared. The table is reprinted with identical entries in the survey talk [3]; the bound $|n_1(5)| \le 36$ is repeated in [2]; and the later survey [4] treats the same circle of questions without reproducing the table. The one place in this literature we have not been able to read is the section on $D(n)$-triples for several values of n in the monograph [5, Section 5.4.1].

What is proved here. A point search on the induced curve produces *some* admissible n for a given triple. We observe that for a fixed triple the set of *all* admissible n is finite and directly computable, by a divisor enumeration rather than by a search for points: if $ab + n = x^2$ and $ac + n = y^2$ with $x, y \ge 0$, then

$$(x-y)(x+y) = a(b-c), \qquad \text{hence} \qquad (x-y)^2 \le |a(b-c)|, \tag{1}$$

so every admissible n arises from a divisor $u = x - y$ of $a(b-c)$ with $|u| \le \sqrt{|a(b-c)|}$, through $n = \left(\frac{1}{2}(u + a(b-c)/u)\right)^2 - ab$. Sweeping the interval $|u| \le \lceil \sqrt{|a(b-c)|}\, \rceil$ therefore decides the whole question for that triple, and what one obtains is an equality: the triple is a $D(n)$-set for exactly the listed n and for no others (Section 3). Applied to triples that the source itself prints, and to scalings of one Diophantine triple that it does not use, this improves eight of the sixteen rows of Table 2.

k	[1]	here	factor	witnessing triple
5	36	4	9.00	$\{30, 1056, 65520\}$
6	215	4	53.75	$\{30, 1056, 65520\}$
7	900	144	6.25	$\{180, 6336, 393120\}$
8	7740	2304	3.36	$\{720, 25344, 1572480\}$
10	129600	103684	1.25	$\{4830, 170016, 10548720\}$
17	371289600	123303600	3.01	$\{185640, 592200, 911400\}$
18	4438929600	493214400	9.00	$\{371280, 1184400, 1822800\}$
19	18193190400	4438929600	4.10	$\{1113840, 3553200, 5468400\}$

TABLE 1. The eight improved upper bounds for $|n_1(k)|$ (Theorems 5.1–5.4); the last column is the triple carrying the bound. The triples on the rows $k = 17$ and $k = 19$ are those [1] itself prints on its rows $k = 16$ and $k = 18$, and the one on the row $k = 18$ is the former doubled.

Three features of Table 1 deserve emphasis.

First, the row $k = 5$ is the one Question 1.1 was raised for. The triple $\{30, 1056, 65520\}$ is a $D(4)$-set, since

$$30 \cdot 1056 + 4 = 178^2, \qquad 30 \cdot 65520 + 4 = 1402^2, \qquad 1056 \cdot 65520 + 4 = 8318^2,$$

and it is a $D(n)$-set for exactly six values of n, so it settles $k = 5$ and $k = 6$ at once. If the suspicion $|n_1(5)| > 1$ of [1, 2] is correct, the remaining gap at $k = 5$ is $2 \le |n_1(5)| \le 4$.

Second, two of the eight improvements use no new triple at all. The triple $\{185640, 592200, 911400\}$ on the row $k = 16$ of Table 2 is a $D(n)$-set for exactly 17 values of n, and $\{1113840, 3553200, 5468400\}$ on the row $k = 18$ for exactly 19. The published table therefore states less than its own data support: a point search reports the n it finds, and the enumeration (1) finds the rest.

Third, the eight rows $k = 9$, $k = 11, \ldots, 16$ and $k = 20$ are *not* improved here. For each of them the best value our search produced equals the published one, which is an independent confirmation of half the table.

Alongside the table we treat the other list of [1, Section 3]: Diophantine triples that are $D(n)$-sets for $n_1 = 1 < n_2 < n_3 < n_4$. Six are printed there, and a seventh, $\{15, 528, 32760\}$, is added in [2, 3, 4], the last of these recording "[b]y a computer search, we found 7 example of triples $\{a, b, c\}$ which are $D(n)$-sets for $n_1 = 1 < n_2 < n_3 < n_4$". We show that each of those seven carries exactly four values of n — a fifth does not exist — and we exhibit two more such triples, $\{20, 1980, 637602\}$ and $\{140, 204, 77913732\}$, taking that list from seven to nine (Section 6). This bears on the remark of [1, Section 3] that "[w]e have been able to find several such examples, but we do not know whether there exists infinitely many such triples"; it does not answer it.

Every statement of this paper has been formally verified in Lean 4; see Section 9.

2. Preliminaries

Throughout, a, b, c, n, x, y, u, v denote integers.

Definition 2.1. Let $n \neq 0$. A triple $\{a, b, c\}$ of pairwise distinct nonzero integers is a $D(n)$-*set* if $ab+n$, $ac+n$ and $bc+n$ are all perfect squares in $\mathbb{Z}$. For such a triple $T = \{a, b, c\}$ put

$$\mathcal{N}(T) = \{\, n \in \mathbb{Z} \setminus \{0\} \ : \ T \text{ is a } D(n)\text{-set} \,\},$$

the n-*set* of T.

We follow the source in allowing n of either sign and in requiring only that the entries be nonzero and pairwise distinct; in particular T need not consist of positive integers, and a $D(n)$-set in the sense of Definition 2.1 need not be a Diophantine triple. Every triple appearing below happens to consist of positive integers.

Definition 2.2. For $k \geq 1$ call $n \in \mathbb{Z} \setminus \{0\}$ *attainable at level* k if there are a triple $\{a, b, c\}$ of nonzero integers and a set $N \subset \mathbb{Z}$ with $|N| = k$ and $n \in N$ such that $\{a, b, c\}$ is a $D(m)$-set for every $m \in N$. As in Question 1.1, $n_1(k)$ denotes an attainable n of least absolute value, and for $B \geq 0$ we write $|n_1(k)| \leq B$ for the assertion that some n attainable at level k satisfies $|n| \leq B$.

The set of absolute values of attainable n is a set of positive integers, so it has a least element as soon as it is nonempty, and $n_1(k)$ is well defined for every k for which some triple is a $D(n)$-set for k values of n; Proposition 4.1 supplies such a triple for each $k \leq 20$. The statement "$|n_1(k)| \leq B$" in the sense of Definition 2.2 is exactly what each row of Table 2 asserts, and it is the form in which all bounds below are proved: it does not require naming the minimiser. Note also that $|n_1(k)| \leq B$ implies $|n_1(k')| \leq B$ for $k' \leq k$, since a subset of N of size k' containing n serves.

Remark 2.3 (scaling; [1, Section 4]). If $\{a, b, c\}$ is a $D(n)$-set and $z \neq 0$, then $\{za, zb, zc\}$ is a $D(z^2n)$-set, because $(za)(zb) + z^2n = z^2(ab + n)$ and likewise for the other two products. Hence $z^2\,\mathcal{N}(T) \subseteq \mathcal{N}(zT)$ for every $z \neq 0$. The inclusion is in general strict, and that is what makes scaling useful here: the scaled triple can acquire values of n that are not z^2 times anything in $\mathcal{N}(T)$. For instance $\mathcal{N}(\{15, 528, 32760\})$ has four elements while $\mathcal{N}(\{30, 1056, 65520\})$ has six, of which only four are 4 times an element of the former (Theorem 5.1).

3. The n-set of a triple is a divisor enumeration

This section records the elementary mechanism behind every computation in the paper. Its first step is the identity used in [1, Section 3, Remark] for one parametrized family of triples — "$r - t \mid b(c - a)$", "[f]rom $d = r - t$ we can find n" — applied here to arbitrary fixed triples, and in particular to the triples of Table 2, where the source used a search for curve points instead.

Lemma 3.1. *Let a, b, c, n be integers such that $ab + n$ and $ac + n$ are perfect squares. Then there are integers $x, y \geq 0$ with*

$$(x - y)(x + y) = a(b - c) \qquad \textit{and} \qquad n = x^2 - ab.$$

Proof. Write $ab + n = r^2$ and $ac + n = s^2$ and set $x = |r|$, $y = |s|$. Then $x^2 - y^2 = (ab + n) - (ac + n) = a(b - c)$ and $n = x^2 - ab$. ☐

Fix now a triple $\{a, b, c\}$ with $a \neq 0$ and $b \neq c$, and put $M = a(b - c) \neq 0$. If $n \in \mathcal{N}(\{a, b, c\})$, apply Lemma 3.1 and set $u = x - y$ and $v = x + y$. Then $uv = M \neq 0$, so $u \neq 0$ and $v \neq 0$; since $x, y \geq 0$ we have $v = x + y \geq 0$, hence $v > 0$, and $|u| = |x - y| \leq x + y = v$. Thus $u \mid M$ with $v = M/u > 0$ and $|u| \leq M/u$, the sum $u + v = 2x$ is even, and

$$u^2 = |u|\,|u| \leq |u|\,v = |M|, \qquad n = x^2 - ab = \Big(\frac{u + M/u}{2}\Big)^2 - ab.$$

Thus n is determined by u, and u ranges over an explicit finite interval. Write $\nu(u) = \bigl(\frac{1}{2}(u+M/u)\bigr)^2 - ab$ for the value so produced.

Proposition 3.2 (exhaustiveness)**.** *Let $a \neq 0$ and $b \neq c$, put $M = a(b-c)$, let K be a nonnegative integer with $|M| \leq K^2$, and let L be a finite list of integers. Suppose that*

(i) *for every integer u with $|u| \leq K$, at least one of the following holds: $u = 0$; $u \nmid M$; $M/u \leq 0$; $M/u < |u|$; $u + M/u$ is odd; $\nu(u) = 0$; $\nu(u) \in L$; or $bc + \nu(u)$ is not a perfect square;*
(ii) *$\{a, b, c\}$ is a $D(n)$-set for every $n \in L$.*

Then $\mathcal{N}(\{a, b, c\}) = L$ as sets; that is, for every integer n, the triple $\{a, b, c\}$ is a $D(n)$-set if and only if $n \in L$.

Proof. The inclusion $L \subseteq \mathcal{N}(\{a, b, c\})$ is (ii). Conversely let $n \in \mathcal{N}(\{a, b, c\})$, so $n \neq 0$ and $ab + n$, $ac + n$, $bc + n$ are squares. The paragraph above produces u with $u \neq 0$, $u \mid M$, $M/u > 0$, $M/u \geq |u|$, $u + M/u$ even and $\nu(u) = n$; and $u^2 \leq |M| \leq K^2$ gives $|u| \leq K$. So u is one of the integers considered in (i), and the first five alternatives there fail for it. Of the remaining three, $\nu(u) = 0$ is excluded by $n \neq 0$ and "$bc + \nu(u)$ is not a square" by the hypothesis on n. Hence $\nu(u) = n$ lies in L. □

Corollary 3.3. *In the situation of Proposition 3.2, if N is any finite set of integers such that $\{a, b, c\}$ is a $D(m)$-set for all $m \in N$, then $|N| \leq |L|$.*

Proof. $N \subseteq \mathcal{N}(\{a, b, c\}) = L$. □

Proposition 3.2 is what turns "at least k values of n" into "exactly k", and it is the only place where a computation of any size occurs: condition (i) is a check at each of the $2K + 1$ integers of the interval $[-K, K]$, each check being one division with remainder, a few comparisons and at most one square test. Condition (ii) is $3|L|$ square tests. The values of K needed below range from 41 to 1460557; the eighteen complete n-sets proved in this paper together require 5 220 742 such checks.

Remark 3.4. Both conditions need a decision procedure for "is this integer a perfect square?". We use one that certifies its own answers: a candidate root $r \geq 0$ is produced by a binary search of fixed depth, and the answer is accepted only on the evidence $r^2 = x$ (a square, with witness r) or $r^2 < x < (r+1)^2$ (not a square, by an interval argument). Nothing is assumed about the search itself, so an incorrect candidate can only cause a check to fail, never cause a false statement to be accepted.

4. The published table, re-derived

k	$\lvert n_1(k)\rvert \leq$	rk	$\{a, b, c\}$	k	$\lvert n_1(k)\rvert \leq$	rk	$\{a, b, c\}$
5	36	3	$\{6, 48, 720\}$	13	4932144	5	$\{37128, 118440, 182280\}$
6	215	3	$\{28, 168, 1848\}$	14	7706475	5	$\{46410, 148050, 227850\}$
7	900	4	$\{380, 1400, 3240\}$	15	30825900	5	$\{92820, 296100, 455700\}$
8	7740	3	$\{168, 1008, 11088\}$	16	123303600	5	$\{185640, 592200, 911400\}$
9	32400	4	$\{2280, 8400, 19440\}$	17	371289600	5	$\{59400, 108360, 223200\}$
10	129600	4	$\{4560, 16800, 38880\}$	18	4438929600	5	$\{1113840, 3553200, 5468400\}$
11	215991	5	$\{9120, 22770, 30960\}$	19	18193190400	5	$\{415800, 758520, 1562400\}$
12	863964	5	$\{18240, 45540, 61920\}$	20	18193190400	5	$\{415800, 758520, 1562400\}$

Table 2. The table of [1, Section 4], reproduced; "rk" is the rank of the induced elliptic curve as printed there. All sixteen rows are re-derived in Proposition 4.1. The two triples in italics carry more values of n than their row records (Theorem 5.4).

The source prints, for each row, the bound and the triple, but not the set N realising them. We recovered a set N for each row by the enumeration of Section 3 and then verified the row from it.

Proposition 4.1. *Every row of Table 2 holds: for each k with $5 \le k \le 20$, the triple listed on the row k is a $D(n)$-set for at least k distinct nonzero integers n, one of which has absolute value equal to the bound printed on that row. Consequently $|n_1(k)|$ is at most the printed bound, for each of the sixteen values of k.*

Proof. For each row an explicit list L_k of k or more integers is exhibited, and each $n \in L_k$ is checked to satisfy the three square conditions for the row's triple, by producing the three roots (Remark 3.4); the entries of L_k are pairwise distinct and nonzero. The element of L_k of least absolute value equals, in absolute value, the printed bound. The lists are those computed by the enumeration of Section 3 and are recorded in the formal development. □

Remark 4.2. The enumeration gives more than Proposition 4.1 needs, although only part of the surplus is inside the formal development. For each of the sixteen triples we computed the *complete* n-set, and in every row its element of least absolute value has exactly the absolute value printed by [1]; so no row of Table 2 can be improved by keeping its triple and looking harder for small n, and each published bound is optimal for its published triple. For fourteen of the sixteen rows that last sentence is a computation reported here as a computation, and no statement of this paper rests on it; completeness is verified only for the two triples used in Theorem 5.4. What is verified for all sixteen is the containment recorded in Proposition 4.1.

5. Eight improved bounds

All the improvements at $k \le 10$ come from a single Diophantine triple that does not occur in [1], namely $\{15, 528, 32760\}$, which is a $D(n)$-set for exactly $n = 1$, 66609, 5369841 and 15984081 (Theorem 6.1); it is the seventh entry of the list of [2, 3, 4]. Scaling it by z produces a triple that is a $D(z^2)$-set, and for suitable z the scaled triple picks up enough further values of n to reach level k while keeping z^2 as its smallest $|n|$ (Remark 2.3). This is why the bounds $4 = 2^2$, $144 = 12^2$, $2304 = 48^2$ and $103684 = 322^2$ below are perfect squares.

Theorem 5.1. *The triple $\{30, 1056, 65520\} = 2 \cdot \{15, 528, 32760\}$ is a $D(n)$-set for exactly the six integers*

$$n \in \{\, 4,\ 266436,\ 15248601,\ 21479364,\ 63936324,\ 1037903409 \,\}$$

and for no other n. Consequently

$$|n_1(5)| \le 4 \qquad \textit{and} \qquad |n_1(6)| \le 4,$$

improving the bounds 36 *and* 215 *of* [1, Section 4] *by factors* 9.00 *and* 53.75*. The same triple does not settle $k = 7$.*

Proof. Here $a = 30$, $b = 1056$, $c = 65520$, $M = a(b - c) = -1933920$ and $K = 1391$ satisfies $|M| \le K^2 = 1934881$. The six listed values are checked directly to satisfy the three square conditions, and condition (i) of Proposition 3.2 is verified at each of the 2783 integers u with $|u| \le 1391$; the proposition then gives the equality. The two bounds follow by taking N to be the whole six-element set, respectively any five-element subset containing 4, in Definition 2.2. The last assertion is Corollary 3.3: no set N of seven values of n can work for this triple, since $|\mathcal{N}| = 6$. □

Theorem 5.2. *The triples $12 \cdot \{15, 528, 32760\}$ and $48 \cdot \{15, 528, 32760\}$ have the complete n-sets*

$$\mathcal{N}(\{180, 6336, 393120\}) = \{\, 144,\ 9591696,\ 548949636,\ 773257104,\ 2301707664,\ 37364522724,\ 41893990009 \,\},$$

$$\mathcal{N}(\{720, 25344, 1572480\}) = \{\, 2304,\ 153467136,\ 1359720961,\ 8783194176,\ 12372113664,\ 36827322624,\ 597832363584,\ 670303840144 \,\},$$

of sizes 7 *and* 8*. Consequently*

$$|n_1(7)| \le 144 \qquad \textit{and} \qquad |n_1(8)| \le 2304,$$

improving the bounds 900 *and* 7740 *of* [1, Section 4] *by factors* 6.25 *and* 3.36*.*

Proof. As in Theorem 5.1, with $K = 8344$ (so $2K + 1 = 16689$ checks) for the first triple, where $M = -69621120$, and $K = 33376$ (so 66753 checks) for the second, where $M = -1113937920$. □

Theorem 5.3. *The triple* $322 \cdot \{15, 528, 32760\} = \{4830, 170016, 10548720\}$ *has the complete* n*-set*

$$\{\,103684,\ 6906287556,\ 14183357769,\ 45669944644,\ 304950219876,\\ 395258986521,\ 556766594244,\ 845074737796,\ 1657293454404,\ 26903494264689\,\},$$

of size 10*. Consequently* $|n_1(10)| \le 103684$*, improving the bound* 129600 *of* [1, Section 4] *by a factor* 1.25*.*

Proof. As above, with $M = -50129140320$ and $K = 223896$, so that 447793 integers u are checked. □

The three remaining improvements concern the upper end of the table, and two of them use the source's own triples.

Theorem 5.4. *The three triples*

$$P_{16} = \{185640, 592200, 911400\}, \qquad 2P_{16} = \{371280, 1184400, 1822800\},\\ P_{18} = \{1113840, 3553200, 5468400\}$$

are $D(n)$*-sets for exactly* 17*, exactly* 18 *and exactly* 19 *values of* n *respectively, namely*

$$\begin{aligned}\mathcal{N}(P_{16}) = \{ &-123303600,\ 49233073600,\ -62968449600,\ -69039035100,\\ &-88899406400,\ -100814229936,\ -103564615959,\ -105476439600,\\ &-107608910400,\ -109500033600,\ 400810054225,\ 608089740496,\\ &1700918654400,\ 2970720824400,\ 3616338278736,\ 5119243819600,\\ &12301311153600\,\},\\ \mathcal{N}(2P_{16}) = {} &4 \cdot \mathcal{N}(P_{16}) \,\cup\, \{2495601459225\},\\ \mathcal{N}(P_{18}) = \{ &-4438929600,\ 1772390649600,\ -2266864185600,\ -2485405263600,\\ &-3200378630400,\ -3629312277696,\ -3728326174524,\ -3797151825600,\\ &-3873920774400,\ -3942001209600,\ 6883913587600,\ 14429161952100,\\ &21891230657856,\ 22460413133025,\ 61233071558400,\ 106945949678400,\\ &130188178034496,\ 184292777505600,\ 442847201529600\,\}.\end{aligned}$$

Consequently

$$|n_1(17)| \le 123303600, \qquad |n_1(18)| \le 493214400, \qquad |n_1(19)| \le 4438929600,$$

improving the bounds 371289600*,* 4438929600 *and* 18193190400 *of* [1, Section 4] *by factors* 3.01*,* 9.00 *and* 4.10*.*

Proof. Proposition 3.2 applied three times, with $K = 243427$, $K = 486853$ and $K = 1460557$ respectively, that is with 486855, 973707 and 2921115 integers u checked; here $M = -59256288000$, $M = -237025152000$ and $M = -2133226368000$. The three bounds follow from the displayed sets by Definition 2.2: the elements of least absolute value are -123303600, $-493214400 = 4 \cdot (-123303600)$ and -4438929600, and the sets have 17, 18 and 19 elements. □

Remark 5.5. P_{16} and P_{18} are the triples printed by [1, Section 4] on the rows $k = 16$ and $k = 18$ of Table 2, with the bounds 123303600 and 4438929600 — exactly the smallest $|n|$ of the sets displayed above. Since those sets have 17 and 19 elements, the rows $k = 17$ and $k = 19$ can be filled in with the same two triples and the same two numbers. The under-reporting is a feature of the method rather than an oversight: a search for points $R \in 2E(\mathbb{Q})$ with $z^2 x(R) \in \mathbb{Z}$ reports the points it finds, and there is no reason for it to find all of them. The intermediate row $k = 18$ is then reached by doubling: $2P_{16}$ carries 18 values of n, the 17 values $4 \cdot \mathcal{N}(P_{16})$ together with the odd value 2495601459225, which is therefore not four times anything.

Remark 5.6. The rows $k = 9$, $k = 11, \dots, 16$ and $k = 20$ of Table 2 are not improved here. For each of those eight values of k the searches described in Section 7 matched the published bound and produced nothing smaller, which is an independent check on half the table. The stubborn row is $k = 9$: the published bound 32400 is attained by the published triple, while the scaling sweep of Section 7 first reaches nine values of n at $z = 240$, with least $|n|$ equal to 57600. Beating that row needs a new seed rather than a longer sweep.

6. Triples that are $D(n)$-sets for four values of n

Section 3 of [1] lists six Diophantine triples that are $D(n)$-sets for $n_1 = 1 < n_2 < n_3 < n_4$; [2, 3, 4] list a seventh, $\{15, 528, 32760\}$. For each of the seven, the sources exhibit the four values; they do not assert that there is no fifth. The enumeration of Section 3 settles that.

Theorem 6.1. *Each of the seven published triples below is a $D(n)$-set for exactly the four listed values of n and for no other integer n:*

$\{a, b, c\}$	$\mathcal{N}(\{a, b, c\})$
$\{4, 12, 420\}$	1, 436, 3796, 40756
$\{10, 44, 21252\}$	1, 825841, 6921721, 112338361
$\{4, 420, 14280\}$	1, 14704, 950896, 47995504
$\{40, 60, 19404\}$	1, 19504, 3680161, 93158704
$\{78, 308, 7304220\}$	1, 242805865, 4770226465, 13336497750865
$\{4, 485112, 16479540\}$	1, 16964656, 2007609136, 63955397832496
$\{15, 528, 32760\}$	1, 66609, 5369841, 15984081

Proof. Seven applications of Proposition 3.2, with $K = 41$, 461, 236, 880, 23869, 7999 and 696 in the order of the table. $\square$

Theorem 6.2. *The triples* $\{20, 1980, 637602\}$ *and* $\{140, 204, 77913732\}$ *are Diophantine triples which are $D(n)$-sets for exactly four values of n each, namely*

$$\mathcal{N}(\{20, 1980, 637602\}) = \{\, 1,\ 327244681,\ 1328052649,\ 100997436001 \,\},$$
$$\mathcal{N}(\{140, 204, 77913732\}) = \{\, 1,\ 3216449236,\ 52716590641,\ 1517624007381076 \,\}.$$

Neither occurs in the lists of [1, 2, 3, 4, 6]*, which record seven such triples, so these two take that list of Diophantine triples that are $D(n)$-sets for four values of n from seven to nine. Moreover*

$$\mathcal{N}(\{160, 198, 64080\}) = \{\, 4,\ 257764,\ 14279409,\ 17058276,\ 1015091641 \,\},$$
$$\mathcal{N}(\{40, 3960, 1275204\}) = \{\, 4,\ 1279201,\ 1308978724,\ 5312210596,\ 403989744004 \,\},$$

each of size 5 *with least $|n|$ equal to* 4*, so that $|n_1(5)| \leq 4$ has three mutually independent witnesses: these two and the triple of Theorem 5.1.*

Proof. Four applications of Proposition 3.2, with $K = 3566$, 104441, 3198 and 7131 respectively. That 1 belongs to the first two n-sets is the assertion that the triples are Diophantine; for instance $20 \cdot 1980 + 1 = 199^2$, $20 \cdot 637602 + 1 = 3571^2$ and $1980 \cdot 637602 + 1 = 35531^2$. The bound $|n_1(5)| \leq 4$ from either of the last two sets is Definition 2.2 applied to the whole five-element set. $\square$

Remark 6.3. Both five-element n-sets of Theorem 6.2 come from doubling a Diophantine triple, and in each case the doubled triple gains values that are not four times anything. One of the two seeds is itself new: $\{40, 3960, 1275204\} = 2 \cdot \{20, 1980, 637602\}$, with $\mathcal{N}(\{40, 3960, 1275204\}) = 4 \cdot \mathcal{N}(\{20, 1980, 637602\}) \cup \{1279201\}$, four values becoming five. The other is $\{160, 198, 64080\} = 2 \cdot \{80, 99, 32040\}$, where the seed carries the three values 1, 64441, 4264569 and the double carries five, the two extra ones being the odd numbers 14279409 and 1015091641. The triple of Theorem 5.1 behaves the same way, four values becoming six.

7. The searches

Two searches were run outside the formal development, to find the triples that Sections 5 and 6 then verify. Neither is used in the proof of any statement above; every triple they produced is verified from scratch by Proposition 3.2, and the reader who takes the triples on faith loses nothing.

The scaling sweep. For each of eleven small primitive triples — among them $\{15, 528, 32760\}$ and $\{221, 705, 1085\}$ — and each integer z with $1 \leq z \leq 12000$, the complete n-set of $z \cdot \{a, b, c\}$ was computed by the enumeration of Section 3, and for each k the least $|n|$ over all sets of size at least k was retained. This produced the eight improvements of Table 1 and nothing further; in particular it is the source of Remark 5.6. It also exposes how much of Table 2 rests on one seed: $\{221, 705, 1085\}$ scaled by $z = 168$, 210, 420, 840 and 5040 gives exactly the triples on the rows $k = 13$, 14, 15, 16 and 18 of [1], and $z = 1680$ gives $2P_{16}$, the triple used here for $k = 18$. (The rows $k = 17$, 19 and 20 use triples outside this family.) Total cost: about four minutes on one core.

The box search. The two new triples of Theorem 6.2 came from an exhaustive enumeration of a box. For each $n_0 \in \{\pm 1, \pm 2, \pm 3, \pm 4\}$ and each $a \leq 200$ the full list of $c \leq 10^8$ with $ac + n_0$ a square was formed, and every pair from that list was tested; this enumerates *every* triple $\{a, b, c\}$ of positive integers with min ≤ 200 and max $\leq 10^8$ that is a $D(n_0)$-set for some n_0 with $|n_0| \leq 4$. The run tested 12 911 983 triples in 77 seconds on one core. As a control it rediscovered all seven published triples of Theorem 6.1 without being given them.

Remark 7.1 (a measurement, not a theorem). The box search is an external computation, and the following three observations about it are outside the formal development of Section 9; they are recorded as measurements of that particular box and not as theorems. Inside the box just described: (i) exactly nine triples are $D(n)$-sets for four or more values of n with 1 among them — the seven of Theorem 6.1 and the two of Theorem 6.2; (ii) no triple at all whose least $|n|$ is 1, 2 or 3 is a $D(n)$-set for as many as four values of n, which is evidence for the suspicion $|n_1(5)| > 1$ of [1, 2] and in no way a proof of it; (iii) the largest n-set with least $|n|$ equal to 4 has six elements, attained by $\{30, 1056, 65520\}$, so that inside the box both the value 4 and the count 6 of Theorem 5.1 are optimal.

8. Controls

A development in which every check succeeds proves nothing about the checks. The following were verified alongside the results above.

Proposition 8.1. (i) (No vacuous bound.) *For every k, the assertion $|n_1(k)| \leq 0$ is false, since attainable integers are nonzero by definition.*

(ii) (The bound 4 is not an artefact.) *$\{30, 1056, 65520\}$ is not a $D(1)$-set — it is not a Diophantine triple — and is not a $D(n)$-set for $n = 2, 3, 5$ or -4.*

(iii) (Ceilings.) *No set of seven values of n works for $\{30, 1056, 65520\}$, and no set of eighteen works for P_{16}.*

(iv) (Every clause of Definition 2.1 bites.) *$\{1, 4, 9\}$ has all three products square, and fails to be a $D(0)$-set only because $n \neq 0$ is required; $\{4, 4, 10\}$ at $n = 9$ has $25, 49, 49$ and fails only on $a \neq b$; $\{0, 3, 8\}$ at $n = 1$ has $1, 1, 25$ and fails only on the entries being nonzero.*

(v) (The sweep rejects an incomplete answer.) *Deleting the value 1037903409 from the list of Theorem 5.1 makes condition (i) of Proposition 3.2 fail; with the full list it holds.*

(vi) (The interval is minimal.) *For $\{30, 1056, 65520\}$ the hypothesis $|M| \leq K^2$ fails at $K = 1390$, so $K = 1391$ is the least admissible choice.*

(vii) (Compatibility.) *$|n_1(5)| \leq 4$ implies $|n_1(5)| \leq 36$; the improvement is a strengthening of the published row in the published row's own terms.*

Item (v) is the load-bearing one. Without it, a sweep procedure that accepted everything would prove every completeness statement in this paper; the control exhibits an input on which it returns the opposite answer.

9. Verification

Every lemma, proposition, theorem and corollary above has been formally verified in Lean 4 against *Mathlib* [9]. The development contains no `sorry` and no hand-declared axiom, and consists of 75 theorems over the definitions of Section 2, which are transcribed from Question 1.1 without alteration. Repository reference to be added at submission. Of the 75, sixty-two are checked by Lean's kernel: sixty-one of them depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound` (ten on fewer), and one on no axioms at all. In particular *every* bound of the form $|n_1(k)| \le B$ — the sixteen rows of Proposition 4.1 and all eight improvements of Section 5 — is kernel-checked, as are Lemma 3.1, Proposition 3.2, Corollary 3.3 itself, and all of Proposition 8.1 except item (iii) for P_{16}.

The remaining thirteen statements are evaluated by compiled code (Lean's `native_decide`) rather than by the kernel, because their sweeps are the long ones: they are the completeness assertions $\mathcal{N}(T) = L$ for the seven triples $\{720, 25344, 1572480\}$, $\{4830, 170016, 10548720\}$, P_{16}, $2P_{16}$, P_{18}, $\{78, 308, 7304220\}$ and $\{140, 204, 77913732\}$ (that is, the second set of Theorem 5.2, Theorem 5.3, all three sets of Theorem 5.4, the fifth row of Theorem 6.1 and the second set of Theorem 6.2), together with the five instances of Corollary 3.3 at the first five of those triples — which inherit the delegation from the completeness statement each of them uses — and the assertion in Proposition 8.1 (iii) that P_{16} admits no set of eighteen values. The dividing line is the length of the interval $[-K, K]$: the kernel evaluates the sweep up to $K = 8344$, and beyond that the compiled evaluator is used. The bridge from the Boolean sweep to the mathematical statement, namely Proposition 3.2, is kernel-checked in all cases, so what is delegated is only the evaluation of an explicit Boolean function on an explicit interval of integers. Notably, no bound $|n_1(k)| \le B$ depends on that delegation: the eight improved bounds are proved directly from their lists of admissible n, and the completeness statements enter only where exactness is asserted.

The searches of Section 7 and the three measurements of Remark 7.1 lie outside the formal development; they were run in C and in Python and are reported here as searches, not as verified claims. Every numerical value quoted from [1] was recomputed from that paper's own definitions before being used, including all sixteen rows of Table 2 and all six triples of its Section 3 table.

References

[1] N. Adžaga, A. Dujella, D. Kreso and P. Tadić, *Triples which are $D(n)$-sets for several n's*, J. Number Theory **184** (2018), 330–341; arXiv:1703.10659. All section, question and table numbers cited here are those of the arXiv version v1, the only version there; the numbering of the typeset journal version was not checked against it.

[2] N. Adžaga, A. Dujella, D. Kreso and P. Tadić, *On Diophantine m-tuples and $D(n)$-sets*, RIMS Kôkyûroku **2092** (2018), 130–137.

[3] A. Dujella, *Triples which are $D(n)$-sets for several n's*, talk at RIMS, Kyoto, 2017, `https://web.math.pmf.unizg.hr/~duje/pdf/dujella-kyoto2017.pdf`, accessed 2 September 2026.

[4] A. Dujella, *Triples, quadruples and quintuples which are $D(n)$-sets for several n's*, in: Class Groups of Number Fields and Related Topics (K. Chakraborty, A. Hoque and P. P. Pandey, eds.), Springer, Singapore, 2024, pp. 77–92, DOI `10.1007/978-981-97-6911-7_5`.

[5] A. Dujella, *Diophantine m-tuples and Elliptic Curves*, Developments in Mathematics **79**, Springer, Cham, 2024, DOI `10.1007/978-3-031-56724-7`. Section 5.4.1, "$D(n)$-triples for several values of n", begins on p. 283 according to the book's table of contents; its text was not available to us.

[6] A. Dujella, *Sets with the property $D(n)$*, `https://web.math.pmf.unizg.hr/~duje/dn.html`, accessed 2 September 2026.

[7] N. Alon, O. Angel, I. Benjamini and E. Lubetzky, *Sums and products along sparse graphs*, Israel J. Math. **188** (2012), 353–384.

[8] A. Dujella and C. Elsholtz, *Sumsets being squares*, Acta Math. Hungar. **141** (2013), 353–357.

[9] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381.