THE CONGRUENTIAL OBSTRUCTIONS TO A $D(n)$ PAIR OF TRIANGULAR NUMBERS ARE EXACTLY $n \equiv 2, 5 \pmod 9$

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. A $D(n)$ pair of triangular numbers is a pair (T_a, T_b) with T_aT_b+n a perfect square, where $T_a = a(a+1)/2$. Bagchi and Zhou-Zheng prove that no such pair exists when $n \equiv 2, 5 \pmod 9$, observe computationally that $n = 12, 17, 42$ also admit no pair with $a \leq 10^5$, conjecture that infinitely many such *sporadic* n exist, and assert that they "do not arise as a result of a congruential obstruction". The theorem they offer in support of that assertion is restricted to moduli m with $9 \nmid m$ — that is, it says nothing at exactly the moduli where their own obstruction lives. We remove the restriction at the prime 3: for every $n \not\equiv 2, 5 \pmod 9$ and every k, the congruence $T_aT_b + n \equiv c^2 \pmod{3^k}$ is solvable with distinct positive indices, by one explicit Hensel lift together with a five-case split on $n \bmod 27$. Hence solvability modulo every power of 3 holds if and only if $n \not\equiv 2, 5 \pmod 9$, the congruential obstructions to a triangular $D(n)$ pair are exactly those two classes, and the sporadic values $12, 17, 42$ carry no obstruction at any modulus. Read together with a recent preprint of Bliznac Trebješanin, which proves that no $D(12)$ pair exists at all, this exhibits $n = 12$ as a failure of the local-global principle for the equation. We also record a per-index obstruction with certified two-modulus sieves, which cut the admissible first indices for $n = 12, 17, 42$ to densities $91/675$, $1/15$ and $7/60$, and we note that the printed list of $n \leq 50$ without a pair omits $n = 50$, which the source's own theorem excludes. All theorems below are machine-checked in Lean 4; §7 says exactly what is checked and what is not, and §6 collects the numerical observations that lie outside the formal development.

1. INTRODUCTION

Following Diophantus and Fermat, a $D(n)$ *m-tuple* is a set of m positive integers such that the product of any two distinct elements, increased by n, is a perfect square; the classical case $n = 1$ culminated in the theorem of He, Togbé and Ziegler that no $D(1)$ quintuple exists [5], and the subject is surveyed in [3] with a running bibliography at [4]. Bagchi and Zhou-Zheng [1] restrict the elements to triangular numbers. We quote their definitions verbatim:

> "A $D(n)$ Diophantine m-tuple of rationals is a set of m positive rationals such that the product of any two distinct elements of the set is n less than a rational perfect square. If all rationals in the tuple are integers, then we say it is a $D(n)$ Diophantine m-tuple of integers."
>
> "The sum of the first n positive integers is known as the n-th triangular number, given by $T_n = n(n+1)/2$."
>
> "Throughout this paper, we will only consider Diophantine integer m-tuples consisting solely of triangular numbers, which we refer to as *triangular $D(n)$ tuples*."

For pairs, [1] reduces the question to a single Diophantine equation, again verbatim:

> "To find triangular pairs, we must find positive integer solutions (a, b, c) to the equation $a(a+1)/2 \cdot b(b+1)/2 + n = c^2$. Then, such a positive integer solution would correspond with the $D(n)$ pair (T_a, T_b), with $T_aT_b + n = c^2$."

The question that organises [1], and this paper, is: *for which n does a solution exist?* Three facts frame it.

First, a congruence removes two residue classes. [1] proves that no solution exists when $n \equiv 2, 5 \pmod 9$; we restate and reprove this in §3 in the slightly stronger form that the congruence already fails modulo 9.

Second, for a fixed first index the question is decidable. Setting $d = a(a+1)$, $x = 4c$ and $y = 2b+1$ turns $T_aT_b + n = c^2$ into the generalized Pell equation $x^2 - dy^2 = 16n - d$, whose solution classes have representatives inside an explicit box once a norm-one unit is known; $u = 2a+1+2\sqrt{a(a+1)}$ is such a unit, and the bounding theorem [1] quotes from [2] then gives an $O(a^{1/2})$ test deciding whether T_a lies in *any* $D(n)$ triangular pair, with the second index unbounded. This is the algorithm behind every numerical statement in [1] and in §6 below.

Third, some n outside the two obstructed classes still admit no pair in the searched range. [1] runs the test for $1 \le n \le 50$ and $1 \le a \le 10^5$, finds that $n = 12, 17, 42$ produce no pair although they are unobstructed, calls these values *sporadic*, writes that they "do not seem to follow any pattern", and conjectures that infinitely many sporadic n exist.

It then asserts more, and this is where the present paper begins. Verbatim:

> "One thing we can prove is that such n do not arise as a result of a congruential obstruction. In other words, we will prove the following:
>
> **Theorem.** Fix a positive integer n, and let m be a positive integer with $9 \nmid m$. Then, there exist positive integers a, b, c such that $T_aT_b + n = c^2 \pmod m$. In other words, the equation has solutions in $\mathbb{Z}/m\mathbb{Z}$."

The hypothesis $9 \nmid m$ is not incidental: it excludes precisely the moduli $9, 27, 81, \dots$ at which the obstruction of [1] itself lives. Its proof assembles $\mathbb{Z}/p^k\mathbb{Z}$ for $p > 3$ (pigeonhole for one solution modulo p, then multivariate Hensel at $t = 1$), $\mathbb{Z}/2^k\mathbb{Z}$ (the map $b \mapsto T_b$ is a bijection modulo 2^k) and $\mathbb{Z}/3\mathbb{Z}$, by the Chinese remainder theorem, and it stops there. The section closes with

> "Since we know solutions always exist modulo powers of a prime, apart from $p = 3$, it is curious that we do not find any solutions for some $n \neq 2, 5 \pmod 9$."

So the sentence [1] advertises — that the sporadic n carry no congruential obstruction — is not established by the theorem it states, and [1] says as much.

Results. We complete the local analysis at the missing prime. Write $\mathbb{N}$ for the non-negative integers; throughout, $n \in \mathbb{N}$, which covers the positive n of [1].

(1) For every $n \not\equiv 2, 5 \pmod 9$ and every $k \ge 0$ there are positive integers $a \neq b$ and c with $T_aT_b + n \equiv c^2 \pmod{3^k}$ (Theorem 4.3). The proof is not a search: one explicit Hensel lift at 3 (Lemma 4.1) together with a five-case split on n mod 27, each case naming a pair of indices drawn from $T_1 = 1$, $T_2 = 3$, $T_4 = 10$, $T_7 = 28$, $T_{13} = 91$.

(2) Consequently solvability modulo every power of 3 holds *if and only if* $n \not\equiv 2, 5 \pmod 9$ (Theorem 4.4), the converse half being the theorem of [1]. Combined with the theorem of [1] quoted above, this determines the congruential obstructions completely: they are exactly the two classes already known (Corollary 4.6).

(3) In particular the sporadic values $n = 12, 17, 42$ are solvable modulo every power of 3 (Corollary 4.5), hence carry no congruential obstruction whatsoever. The natural first guess about the sporadic cases — that some modulus larger than 9 kills them — is therefore false, and false as a theorem rather than as a failed search.

Two further contributions are supporting rather than headline. §5 isolates a *per-index* obstruction — a residue A modulo m can be bad, in the sense that $A \cdot T_b + n \equiv c^2 \pmod m$ is insoluble, and then no a with $T_a \equiv A \pmod m$ occurs in any $D(n)$ pair — of which the opening observation of [1] is the case $m = 3$. Two moduli per sporadic value, verified rather than trusted, cut the admissible first indices to 182 of 1350 residue classes for $n = 12$, 70 of 1050 for $n = 17$, and 210 of 1800 for $n = 42$ (Theorems 5.4 and 5.5); this is an infinite statement obtained from a finite check. The obstruction itself is not new — its quadratic-residue form is Theorem 9 of [7] — but the sieve here is verified rather than asserted and comes with exact densities. There is no tension with the results above: a

per-index obstruction constrains a, not n. Finally, Proposition 3.3 records that the list of $n \le 50$ without a pair printed in [1] omits $n = 50$, which the theorem of [1] itself excludes.

Related work. The bibliography of [1] lists no paper that asks for which n a triangular $D(n)$ pair exists. Such a paper does exist, and it was posted first. Bliznac Trebješanin [7] studies the same equation $T_aT_b + n = c^2$ for arbitrary non-zero n; her second version, posted more than two months before [1], carries three results that bear on what follows. Her Theorem 6 is the obstruction $n \not\equiv 2, 5 \pmod 9$ — the theorem of [1], obtained independently and by a different argument, from the residue sets $c^2 \bmod 9 \in \{0, 1, 4, 7\}$ and $T_aT_b \bmod 9 \in \{0, 1, 3, 6\}$ rather than by the descent to $a \equiv b \equiv 1 \pmod 3$. Her Proposition 7 proves that *no* $D(12)$ pair of triangular numbers exists, and none for $n = -37$, by a descent inside a solution class; the same is asserted, with the proofs "omitted for brevity", for $n \in \{252, 487, -158, 42, 52\}$. Two of the three sporadic values of [1] are therefore settled there — $n = 12$ with a proof and $n = 42$ without one — and $n = 17$ is not. Her Theorem 9 is a quadratic-residue obstruction on the *index*, which reappears below as the second half of Theorem 5.2. Nothing in [7] concerns solvability modulo prime powers, so §4, which is this paper's headline, does not overlap it; §5 and §6 do, and say where.

Hamtat [6], listed in [4] as a 2025 preprint on Diophantine triples in triangular numbers, we were unable to obtain; we cite it exactly as [4] lists it and make no claim about its contents. A larger group of papers uses the phrase "triangular $D(n)$-tuple" for a *different* equation, in which $a_ia_j + n$ is required to be triangular rather than square [8, 9, 10, 11]. None of these does a local analysis of the equation $T_aT_b + n = c^2$.

2. Preliminaries

For $a \in \mathbb{N}$ put $T_a = a(a+1)/2$, so $T_0 = 0$, $T_1 = 1$, $T_2 = 3$, $T_4 = 10$, $T_7 = 28$, $T_{13} = 91$.

Definition 2.1. For $n, a, b, c \in \mathbb{N}$ write $\mathrm{Sol}(n; a, b, c)$ for the equation $T_aT_b + n = c^2$. A $D(n)$ *triangular pair* is a triple (a, b, c) with $a, b > 0$, $a \ne b$ and $\mathrm{Sol}(n; a, b, c)$.

The distinctness condition deserves a word, because [1] uses two readings. Its definition asks for a *set*, hence for distinct elements; its search predicate, quoted in §1, asks only for positive (a, b, c), and its own worked example for $n = 7$ is the "pair" (T_2, T_2), since $3 \cdot 3 + 7 = 4^2$. We keep both: **every nonexistence statement below is proved for** Sol, hence covers the weaker predicate and so both readings, and **every existence statement below produces** $a \ne b$, hence satisfies the stricter one.

Lemma 2.2. *For every $a \in \mathbb{N}$ one has $2T_a = a(a+1)$. If $m, P \in \mathbb{N}$ with $2m \mid P$, then $T_a \equiv T_{a \bmod P} \pmod m$ for every a. In particular $T_a \bmod m$ depends only on $a \bmod 2m$.*

Proof. The first identity is the statement that $a(a+1)$ is even. For the second, $T_{a+2mq} = T_a + m\big(2aq + q(2mq+1)\big)$, which follows from the first identity applied to both sides; taking $q = \lfloor a/P \rfloor$ and $P = 2ms$ gives the congruence. □

Lemma 2.2 is what makes every congruence condition on the equation a *finite* condition: modulo m, the values T_b run over a set determined by $b \bmod 2m$ and the squares c^2 over a set determined by $c \bmod m$.

3. The obstruction modulo 9

We restate the theorem of [1] in the form the next section needs, namely as the insolubility of a congruence rather than of an equation.

Proposition 3.1 ([1], Section 3; independently [7], Theorem 6)**.** *Let $n \equiv 2$ or $5 \pmod 9$. Then for all $a, b, c \in \mathbb{N}$,*

$$T_aT_b + n \not\equiv c^2 \pmod 9.$$

In particular the equation $T_aT_b + n = c^2$ has no solution at all, so no $D(9k+2)$ or $D(9k+5)$ pair of triangular numbers exists.

Proof sketch. The mathematics is that of [1]: if $n \equiv 2 \pmod 3$ then $3 \nmid T_a$ and $3 \nmid T_b$ forces $a \equiv b \equiv 1 \pmod 3$, whence $T_a \equiv T_b \equiv 1 \pmod 9$ and $T_aT_b + n \equiv 1 + n \equiv 3, 6 \pmod 9$, neither of which is a quadratic residue. We run the same arithmetic as one finite check, after clearing the denominator so that no division by 2 modulo 9 is needed: by Lemma 2.2, $4T_aT_b = a(a+1) \cdot b(b+1)$, so a solution of the congruence would give

$$x(x+1) \cdot y(y+1) + 4r \equiv 4z^2 \pmod 9, \qquad r \in \{2, 5\},$$

with x, y, z the residues of a, b, c. For each of the two values of r and each of the $9^3 = 729$ triples (x, y, z) in $(\mathbb{Z}/9\mathbb{Z})^3$ — 1458 evaluations in all — the two sides differ. (In the formal proof the case split on r is made by the same decision procedure, which therefore scans all 9^4 quadruples (r, x, y, z) and discards the seven values of r that fail the hypothesis.) This is the only exhaustive computation on which Proposition 3.1, and the reverse implication of Theorem 4.4, rest. □

The following four facts fix the shape of Proposition 3.1; the first is the example printed in [1], the second and third show that the modulus 9 can be neither raised from nor lowered to 3, and the fourth records that the sporadic values are outside its scope.

Proposition 3.2. (1) $\{1, 3, 120\} = \{T_1, T_2, T_{15}\}$ *is a* $D(1)$ *triangular triple:* $1 \cdot 3 + 1 = 2^2$, $1 \cdot 120 + 1 = 11^2$, $3 \cdot 120 + 1 = 19^2$.

(2) *The hypothesis cannot be weakened to* $n \equiv 2 \pmod 3$*: for* $n = 8$ *one has* $T_1T_7 + 8 = 1 \cdot 28 + 8 = 6^2$*, a* $D(8)$ *triangular pair, and* $8 \equiv 2 \pmod 3$.

(3) *The modulus cannot be lowered to* 3*: for* $n = 2$ *one has* $T_1T_1 + 2 = 3 \equiv 0^2 \pmod 3$*, so the obstruction is invisible at the prime itself.*

(4) $2 \bmod 9 = 2$*, while* $12 \bmod 9 = 3$*,* $17 \bmod 9 = 8$ *and* $42 \bmod 9 = 6$*: the hypothesis is satisfiable, and the three sporadic values of* [1] *do not satisfy it.*

3.1. **A correction to the printed list.**

Proposition 3.3. *No* $D(50)$ *pair of triangular numbers exists.*

Proof. $50 \equiv 5 \pmod 9$; apply Proposition 3.1. □

This is a corollary of the theorem of [1], but it does not appear in the data printed there. [1] reports, of the run $1 \le n \le 50$ with $1 \le a \le 10^5$, that "Thirty-six such n produced a $D(n)$ pair in the range" and that "For fourteen such n, no integer solutions (x, y) in the range were found. They are: $n = 2, 5, 11, 12, 14, 17, 20, 23, 29, 32, 38, 41, 42, 47$". The value $n = 50$ is absent from that list, although Proposition 3.3 excludes it; accordingly the list has fifteen entries and the count should read thirty-five. An independent rerun of the same experiment, described in §6, returns exactly those fifteen values. Nothing else in [1] depends on the count, and the sporadic set $\{12, 17, 42\}$ is unchanged, 50 being an obstructed rather than a sporadic value.

4. Local solvability at the prime 3

This section removes the hypothesis $9 \nmid m$ from the theorem of [1] at the prime 3. Everything rests on one lift.

Lemma 4.1 (Hensel at 3)**.** *Let* v *be an integer with* $v \equiv 1 \pmod 3$*. Then for every* $k \ge 0$ *there is an integer* z *with* $3^{k+1} \mid z^2 - v$*. Consequently, if* $v \in \mathbb{N}$ *satisfies* $v \equiv 1 \pmod 3$ *then* v *is a square modulo* 3^k *for every* k*.*

Proof. Write $v = 3u + 1$ and induct, the base case being $z = 1$, for which $z^2 - v = -3u$. Given $z^2 - v = 3^{k+1}s$, take $z' = z(1 + 3^{k+1}s)$. Substituting $z^2 = 3u + 1 + 3^{k+1}s$ gives the identity

$$z'^2 - v = 3^{k+2} \cdot s\big(1 + 2u + 3 \cdot 3^k s + 3u \cdot 3^k s + 3(3^k)^2 s^2\big),$$

which is a polynomial identity in u, s and 3^k. The lift is explicit and no appeal to a general Hensel lemma is made; this matters for the verification of §7, since the standard library statement available to us is for the p-adic integers rather than for $\mathbb{Z}/p^k\mathbb{Z}$. □

Corollary 4.2. *If $v \in \mathbb{N}$ satisfies $v \equiv 9 \pmod{27}$ then v is a square modulo 3^k for every k.*

Proof. Write $v = 9w$; then $w \equiv 1 \pmod 3$, so $w \equiv c_0^2$ modulo 3^k by Lemma 4.1 and $v \equiv (3c_0)^2$ modulo 3^k. □

Theorem 4.3. *Let $n \in \mathbb{N}$ with $n \not\equiv 2 \pmod 9$ and $n \not\equiv 5 \pmod 9$. Then for every $k \geq 0$ there exist positive integers $a \neq b$ and $c \in \mathbb{N}$ with*

$$T_a T_b + n \equiv c^2 \pmod{3^k}.$$

Proof. The residues of n not excluded by the hypothesis are covered by the five cases

$$n \equiv 0\ (3), \quad n \equiv 1\ (3), \quad n \equiv 8\ (27), \quad n \equiv 17\ (27), \quad n \equiv 26\ (27),$$

since $n \equiv 2 \pmod 3$ splits modulo 9 into $n \equiv 2, 5, 8$, of which the first two are excluded, and $n \equiv 8 \pmod 9$ splits modulo 27 into $8, 17, 26$. In each case we name two distinct positive indices and apply Lemma 4.1 or Corollary 4.2 to the resulting value:

class of n	(a, b)	$T_a T_b + n$	reason
$n \equiv 0\ (3)$	$(1, 4)$	$10 + n \equiv 1\ (3)$	Lemma 4.1
$n \equiv 1\ (3)$	$(1, 2)$	$3 + n \equiv 1\ (3)$	Lemma 4.1
$n \equiv 8\ (27)$	$(1, 7)$	$28 + n \equiv 9\ (27)$	Corollary 4.2
$n \equiv 17\ (27)$	$(4, 13)$	$910 + n \equiv 9\ (27)$	Corollary 4.2
$n \equiv 26\ (27)$	$(1, 4)$	$10 + n \equiv 9\ (27)$	Corollary 4.2

Here $T_1 T_4 = 10$, $T_1 T_2 = 3$, $T_1 T_7 = 28$ and $T_4 T_{13} = 10 \cdot 91 = 910$, and in every row the two indices are distinct and positive. □

The case $n \equiv 2 \pmod 3$ is the delicate one and explains the shape of the table. There a solution modulo 9 must have $3 \nmid T_a$ and $3 \nmid T_b$, since otherwise the value is $\equiv n \equiv 2 \pmod 3$, a non-residue; so $a \equiv b \equiv 1 \pmod 3$, hence $T_a \equiv T_b \equiv 1 \pmod 9$ and the value is $\equiv 1 + n \pmod 9$. For the three classes $n \equiv 2, 5, 8 \pmod 9$ that is 3, 6, 0, and only the last is a square modulo 9 — which is Proposition 3.1 again, and leaves only $n \equiv 8 \pmod 9$. The value is then divisible by 9, and the three sub-cases modulo 27 choose indices for which it is exactly 9 times a unit congruent to 1 modulo 3; that this is always possible comes from $T_a \bmod 27 \in \{1, 10\}$ for the indices used. For example, for $n = 17$ the witness is $(a, b) = (4, 13)$, where $10 \cdot 91 + 17 = 927 = 9 \cdot 103$ and $103 \equiv 1 \pmod 3$.

Theorem 4.4. *For $n \in \mathbb{N}$, the congruence $T_a T_b + n \equiv c^2 \pmod{3^k}$ is solvable with a, b positive and distinct for every $k \geq 0$ if and only if $n \not\equiv 2, 5 \pmod 9$.*

Proof. The implication from right to left is Theorem 4.3. Conversely, taking $k = 2$ turns a solution into a solution modulo 9, which Proposition 3.1 forbids when $n \equiv 2, 5 \pmod 9$. □

Corollary 4.5. *For each $n \in \{12, 17, 42\}$ and each $k \geq 0$ there are positive integers $a \neq b$ and c with $T_a T_b + n \equiv c^2 \pmod{3^k}$.*

Proof. $12 \equiv 3$, $17 \equiv 8$ and $42 \equiv 6$ modulo 9; apply Theorem 4.3. □

Combining Theorem 4.3 with the theorem of [1] quoted in §1 settles the question for every modulus at once.

Corollary 4.6. *Assume the theorem of [1] for moduli m with $9 \nmid m$. Then for every $m \geq 1$ and every $n \not\equiv 2, 5 \pmod 9$ the congruence $T_a T_b + n \equiv c^2 \pmod m$ has a solution in positive integers; and for $n \equiv 2, 5 \pmod 9$ it has none already for $m = 9$. Thus the congruential obstructions to a $D(n)$ triangular pair are exactly the two classes $n \equiv 2, 5 \pmod 9$, and the sporadic values $n = 12, 17, 42$ carry none at any modulus.*

Proof. Write $m = 3^k m'$ with $3 \nmid m'$. Theorem 4.3 solves the congruence modulo 3^k and the theorem of [1] solves it modulo m', since $9 \nmid m'$; combine the two solutions by the Chinese remainder theorem. (Distinctness of the two indices is claimed only in Theorem 4.3, not here.) The second assertion is Proposition 3.1. □

Corollary 4.6 is the only statement in this paper whose proof uses a result we have not verified ourselves: the theorem of [1] is quoted, not reproved. Theorems 4.3 and 4.4 and Corollary 4.5 are independent of it.

Remark 4.7. Corollary 4.6 and [7, Proposition 7] together exhibit a failure of the local-global principle for this equation. For $n = 12$ the congruence $T_aT_b + 12 \equiv c^2 \pmod m$ is solvable in positive integers for every modulus m, while by that proposition no $D(12)$ pair of triangular numbers exists. That is the shape Corollary 4.6 forces on any genuinely sporadic value, and $n = 12$ is the first for which both halves are theorems. Both halves are quoted rather than verified here — the first uses the theorem of [1] for $9 \nmid m$, the second is [7, Proposition 7] — and nothing below depends on this remark.

The next two facts confine Theorem 4.4 from both sides.

Proposition 4.8. (1) *The equivalence is not the vacuous one "solvable for every n": for $n = 2$ solvability modulo every power of 3 fails, there being already no solution modulo 9.*
(2) *The hypothesis of Lemma 4.1 is not decorative: $2 \equiv 2 \pmod 3$ is a non-residue, so no c has $c^2 \equiv 2 \pmod 3$, whereas $4 \equiv 1 \pmod 3$ is a square modulo $3^5 = 243$ by the lemma.*

5. A per-index obstruction, and how thin the admissible indices are

The results of §4 say that no congruence in n can explain the sporadic values. A congruence in the *index* is a different matter, and [1] already uses one. The proof of its Theorem on $n \equiv 2, 5 \pmod 9$ opens with the observation, verbatim: "Note that $3 \mid T_a$ if and only if $a \equiv 0, 2 \pmod 3$. Thus, if either $a \equiv 0, 2 \pmod 3$ or $b \equiv 0, 2 \pmod 3$, then modulo 3 the equation becomes $2 \equiv c^2 \pmod 3$, which is impossible. Hence, we may assume that $a, b \equiv 1 \pmod 3$." This generalises.

Definition 5.1. For $n, m, A \in \mathbb{N}$ with $m > 0$, say that A is *bad for n modulo m* if

$$A \cdot T_t + n \not\equiv c^2 \pmod m \quad \text{for all } t < 2m \text{ and all } c < m.$$

By Lemma 2.2 this is a finite condition that decides the corresponding infinite one, and the values $t < 2m$, $c < m$ exhaust the relevant residues.

Theorem 5.2. *Let $m > 0$ and let a be such that $T_a \bmod m$ is bad for n modulo m. Then there are no b, c whatsoever with $T_aT_b + n = c^2$; that is, T_a lies in no $D(n)$ triangular pair, with the second index unbounded. In particular, if $p \mid T_a$ and n is not a square modulo p, then T_a lies in no $D(n)$ triangular pair.*

Proof. Reduce a hypothetical solution modulo m: $T_a \equiv T_a \bmod m$, $T_b \equiv T_{b \bmod 2m}$ by Lemma 2.2, and $c \equiv c \bmod m$, so the pair $(t, c') = (b \bmod 2m,\ c \bmod m)$ realises the forbidden congruence. For the second statement, $p \mid T_a$ gives $T_a \bmod p = 0$ and the condition of Definition 5.1 becomes "n is not a square modulo p". □

The second statement is not new. For odd p one has $p \mid T_a$ if and only if $p \mid a(a+1)$, so it says that a triangular number T_a can lie in a $D(n)$ pair only if every odd prime divisor of $a(a+1)$ divides n or has n as a quadratic residue — which is Theorem 9 of [7], proved there by the same reduction of the Pell equation modulo p. What the rest of this section adds is that the general form, Theorem 5.2, gives *certified* sieves with exact densities.

Lemma 5.3. *$T_a \equiv 1 \pmod 3$ if $a \equiv 1 \pmod 3$, and $T_a \equiv 0 \pmod 3$ otherwise. Consequently, if $n \equiv 2 \pmod 3$ and $T_aT_b + n = c^2$ with $a, b, c \in \mathbb{N}$, then $a \equiv b \equiv 1 \pmod 3$.*

Proof. The first claim is the case $m = 3$, $P = 6$ of Lemma 2.2 together with the six values $T_0, \dots, T_5$ modulo 3. For the second, 0 is bad for n modulo 3 when $n \equiv 2 \pmod 3$ — one checks the three residues $c < 3$ — so Theorem 5.2 applies to any index with $T_a \equiv 0$, and the equation is symmetric in a and b. □

Lemma 5.3 recovers the observation of [1]. With more moduli the same device becomes quantitative. For the three sporadic values we fix two moduli each and the following residue sets, obtained by enumeration and then verified:

$$\begin{aligned}
n = 12: &\quad B_{12,25} = \{0,1,5,6,10,11,15,16,20\}, \quad B_{12,27} = \{0,3,6,9,12,18,21\};\\
n = 17: &\quad B_{17,21} = \{0,3,6,7,9,12,14,15,18\}, \quad B_{17,25} = \{0,1,5,6,10,15,16,20,21\};\\
n = 42: &\quad B_{42,25} = \{0,1,5,6,10,15,16,20,21\},\\
&\quad B_{42,36} = \{0,4,6,8,9,12,15,16,18,20,24,27,28,32,33\}.
\end{aligned}$$

Theorem 5.4. *Every element of $B_{n,m}$ is bad for n modulo m, for each of the six pairs above. Consequently, if $T_aT_b + n = c^2$ with $n = 12$ then $T_a \bmod 25 \notin B_{12,25}$ and $T_a \bmod 27 \notin B_{12,27}$, and similarly for $n = 17$ (moduli $21, 25$) and $n = 42$ (moduli $25, 36$). Call an index a* admissible *for n when it passes both tests; then admissibility for $n = 12$, 17, 42 depends only on a modulo* 1350, 1050, 1800 *respectively.*

Proof sketch. Badness of a listed residue A is the exhaustive check of Definition 5.1, which compares $2m^2$ pairs (t, c): $9 \cdot 1250$ and $7 \cdot 1458$ evaluations for $n = 12$, $9 \cdot 882$ and $9 \cdot 1250$ for $n = 17$, $9 \cdot 1250$ and $15 \cdot 2592$ for $n = 42$; 90 774 evaluations in all. The lists themselves were produced by a search over small moduli: for each n and each m with $2 \le m \le 64$, enumerate the residues $A < m$ that are bad; then compare every set of at most four such moduli whose common period $\operatorname{lcm}_i(2m_i)$ is at most 2000, and keep one of least admissible density. In each of the three cases that minimum is attained by a pair, and by the pair named above. That search is not trusted: every listed residue is re-verified by the check above, and a residue wrongly included would be caught rather than believed. The consequence is Theorem 5.2 applied to both moduli. The period claim is Lemma 2.2 with $P = \operatorname{lcm}(2m_1, 2m_2)$, which is $1350 = 2 \cdot 27 \cdot 25$, $1050 = 2 \cdot 21 \cdot 25$ and $1800 = 2 \cdot 25 \cdot 36$ for the three pairs of moduli. □

Theorem 5.5. *Exactly* 182 *of the* 1350 *residue classes are admissible for $n = 12$, exactly* 70 *of* 1050 *for $n = 17$, and exactly* 210 *of* 1800 *for $n = 42$. The admissible indices therefore have densities*

$$\frac{91}{675} \approx 13.5\%, \qquad \frac{1}{15} \approx 6.7\%, \qquad \frac{7}{60} \approx 11.7\%.$$

Proof. Enumerate the $1350 + 1050 + 1800 = 4200$ residue classes and apply the two membership tests of Theorem 5.4 to each. This is an exhaustive computation, and it is the whole proof. □

Two remarks. First, $a = 1$ is inadmissible for all three values, since $T_1 = 1$ and 1 is bad modulo 25 in each case; for $n = 12$ this is the statement that $u^2 - 8c^2 = -95$ has no solution, which one sees modulo 25: the congruence forces $5 \mid u$ and $5 \mid c$, hence $25 \mid 95$. Second, the sieve does not prove the conjecture of [1] by accident — see Proposition 5.6(2) — and it is far from exhausting the method: taking all moduli $m \le 1000$ instead of two reduces the surviving fraction of indices $a \le 20\,000$ to about 2.1%, 0.6% and 3.1% respectively, after which it plateaus, as Theorem 4.4 says it must. That larger computation is not part of the verified development, its period being of order 10^5. For comparison, the condition of [7, Theorem 9] — which looks at every odd prime divisor of $a(a+1)$ rather than at two fixed moduli — leaves 6.9%, 1.9% and 12.2% of the indices $a \le 20\,000$, so the two-modulus sieve above is the weaker of the two for $n = 12$ and $n = 17$. Its point is not strength: it is that Theorems 5.4 and 5.5 are statements about *all* a, checked by the proof kernel, rather than counts over a range.

Proposition 5.6.
(1) *The residue* 7 *is* not *bad for $n = 12$ modulo* 25*: $7 \cdot T_1 + 12 = 19$ and $19 \equiv 12^2 \pmod{25}$. So the sets $B_{n,m}$ cannot be padded.*
(2) *Admissible indices exist: $a = 7$ for $n = 12$, $a = 16$ for $n = 17$, $a = 2$ for $n = 42$. So Theorem 5.4 does not vacuously prove that no pair exists.*
(3) *The device is genuinely about n: for $n = 1$ the residue* 1 *is not bad modulo* 25*, since $1 \cdot T_2 + 1 = 4 = 2^2$. So it is not an artefact rejecting every parameter.*

6. Computations outside the formal development

The statements of this section are numerical. They are **not** part of the machine-checked development of §7, for a specific reason: the $O(a^{1/2})$ test decides that T_a lies in no $D(n)$ pair only because every solution class of a generalized Pell equation has a representative inside an explicit box, and no bounding theorem of that kind is available to us in verified form. Positive answers are exact identities and are checked as such; negative answers rest on the bound. We record them as observations.

Two boxes were used, and it matters which. Write $d = a(a+1)$ and $N = 16n - d$. The runs below scan the odd y up to $\sqrt{-N/a}$ when $N < 0$ and up to $\sqrt{N/(a+1)}$ when $N > 0$, plus a small constant margin against floating-point error: this is the classical bound on the fundamental solution of a solution class, instantiated at the norm-one unit $(2a+1, 2)$ of $x^2 - dy^2 = 1$. The second box is the one [1] quotes, $|y| \le \sqrt{|N|}\,(1+\sqrt{u})/(2\sqrt{d})$ with $u = 2a + 1 + 2\sqrt{d}$ ([2, Theorem 2.1]); it is the larger of the two for every (n, a) occurring below. Every run of the test reported here was carried out with both boxes, from two independently written implementations, and they agree on every answer.

Remark 6.1 (Reproduction and validation). We reimplemented the $O(a^{1/2})$ test in C from the textual description in [1], deliberately without consulting the SageMath repository named in its footnote, so that the reproduction is independent. Three checks were run before anything else. A direct box search finds 942 pairs with $1 \le a \le 300$ and $a \le b \le 3 \cdot 10^5$ for $n = 1$, the smallest being $T_1T_2 + 1 = 2^2$, $T_1T_5 + 1 = 4^2$, $T_1T_{15} + 1 = 11^2$. The worked example of [1] for $n = 7$ reproduces: $a = 1$ admits no partner $b \le 2 \cdot 10^8$. And on the 7 200 pairs (n, a) with $1 \le n \le 60$ and $1 \le a \le 120$ the fast test agrees with a direct scan over $b \le 2 \cdot 10^5$ in both directions — 1 070 positive answers verified as exact integer identities, 6 130 negative answers confirmed by the scan, no discrepancies. Rerunning the run $1 \le n \le 50$, $a \le 10^5$ of [1] returns 35 values of n with a pair and 15 without, the fifteen being the fourteen printed in [1] together with $n = 50$; this is the computational half of §3.1.

Remark 6.2 (The census, extended to $n \le 10^4$). Running the same test with the same box $a \le 10^5$ over all 7 778 values $n \le 10^4$ with $n \not\equiv 2, 5 \pmod 9$ leaves 942 values with no pair — 12.11% — beginning $12, 17, 42, 52, 62, 67, 87, 98, 102, 107, 132, 142, 150, 152, 192$ and ending at 9989. At $n \le 10^3$ the count is 90 of 778, or 11.6%, so the proportion is flat over a decade. This is the largest body of evidence we know of for the conjecture of [1]; [7, Proposition 7] settles a handful of individual n outright, which is far stronger for those values but says nothing about a density.

These values are moreover not patternless, contrary to the expectation recorded in [1], at least over the range computed. Let $k(n) = \#\{p \in \{3, 5, 7, 11, 13, 17, 19\} : n \text{ is not a square modulo } p\}$. Then:

$k(n)$	0	1	2	3	4	5	6	7
no pair found	0	7	73	226	339	224	65	8
values tested	214	879	2069	2326	1568	591	121	10
proportion	0%	0.8%	3.5%	9.7%	21.6%	37.9%	53.7%	80%

In particular not one of the 214 values that are squares modulo every one of $3, 5, 7, 11, 13, 17, 19$ is among them. Theorem 5.2 supplies the mechanism: each prime p with n a non-residue deletes every index a with $p \mid T_a$, a proportion $2/p$ of all indices, so the more such primes, the thinner the set of indices that could work. This is a bias in the indices, not a congruence in n, and it is therefore consistent with Corollary 4.6. We state it as an observation about the range computed and not as a theorem or a conjecture.

Remark 6.3 (The sporadic values, pushed to $a \le 10^7$). For each $n \in \{12, 17, 42\}$ and each $a \le 10^7$ — one hundred times the range of [1] — the test reports that T_a lies in no $D(n)$ triangular pair, the second index unbounded. Since a pair (T_a, T_b) with $a \le b$ has smaller index a, this says that both indices of any $D(12)$, $D(17)$ or $D(42)$ triangular pair exceed 10^7, so that both elements exceed $5 \cdot 10^{13}$. As a safety check, rerunning $a \le 10^6$ with the search bound tripled returns the same answer, so the constant in the bound is not load-bearing.

For two of the three values this is now a consistency check rather than evidence: [7, Proposition 7] proves that no $D(12)$ pair of triangular numbers exists at all, and asserts the same for $n = 42$ with

the proof omitted. For $n = 17$ we know of no such argument, and the run above is where the evidence stands.

7. Verification

Every numbered statement of §§2–5 except Corollary 4.6 and Remark 4.7 — that is, Lemmas 2.2, 4.1 and 5.3, Corollaries 4.2 and 4.5, Theorems 4.3, 4.4, 5.2, 5.4 and 5.5, and Propositions 3.1, 3.2, 3.3, 4.8 and 5.6 — has been machine-checked in Lean 4 [12] against Mathlib [13], in three files (objects and the obstruction modulo 9; the local analysis at 3; the per-index obstruction and the sieves). The development contains no `sorry` and, in particular, no appeal to compiled evaluation: the exhaustive computations quoted above — the 1458 residue comparisons behind Proposition 3.1, the 90 774 behind Theorem 5.4 and the 4 200 index tests behind Theorem 5.5 — are carried out by the proof kernel itself, so the axiom closure of every theorem is contained in propositional extensionality, quotient soundness and the axiom of choice. Three limitations should be stated plainly. Corollary 4.6 is a paper argument that quotes the theorem of [1] for moduli m with $9 \nmid m$; that theorem is not reproved here, and the results it is combined with (Theorems 4.3 and 4.4, Corollary 4.5) do not depend on it. Remark 4.7 quotes, in addition, [7, Proposition 7], which we have neither reproved nor refereed; nothing else in the paper uses it. And everything in §6 is outside the development, for the reason given there. Repository reference to be added at submission.

8. What remains

Three questions are left open, in increasing order of difficulty.

The first is quantitative and looks reachable. Remark 6.2 exhibits a correlation between having no pair in the searched range and being a quadratic non-residue at small primes, and Theorem 5.2 explains its mechanism. The natural statement is that for fixed n the set of admissible indices has density $\prod_{p:\,(n|p)=-1}(1 - 2/p)$, extended over the primes at which n is a non-residue; for non-square n those primes have density $1/2$, so $\sum 2/p$ diverges over them and the product is 0; the admissible indices would then have density zero for every non-square n. A theorem of that shape would go a long way towards explaining the sporadic phenomenon — though not, by itself, towards proving the conjecture of [1], since density zero is not emptiness. Its truncation to finitely many primes is already provable by the method of §5.

The second is a verification question with mathematical content. The negative half of the $O(a^{1/2})$ test rests on a bounding theorem for generalized Pell equations [2]; formalizing that bound would turn every observation of §6 into a theorem, and would be reusable wherever a Pell equation is decided by a finite scan.

The third is the conjecture of [1] itself. Corollary 4.6 closes off the easiest possible route to it — there is no congruence in n to be found — and Remark 6.2 says that the phenomenon it describes persists at a stable rate of about 12% across the decade from $n \le 10^3$ to $n \le 10^4$. Individual values are now within reach: [7, Proposition 7] settles $n = 12$ and $n = -37$ by a descent inside a solution class, and reports the same for five further values. That descent is carried out one n at a time, and the finite set of exceptional pairs it produces depends on n; how to run it uniformly over an infinite family of n, which is what the conjecture needs, we do not know.

References

[1] S. Bagchi and C. Zhou-Zheng, *Diophantine m-tuples of Triangular Numbers*, arXiv:2608.27697v1 [math.NT], 27 August 2026. The abstract page was consulted on 3 September 2026: v1 is the only version, and no journal version is recorded. All quotations above are from the e-print. Cited for the definitions, the algorithm of its Section 3, its Theorem on $n \equiv 2, 5 \pmod 9$, its Conjecture, its Theorem for moduli m with $9 \nmid m$ (its Section 3.1), and the run and printed list of its Section 3.

[2] B. Conrad, *Math 154. Generalized Pell equation*, course handout, Stanford University, 4 pp.; `https://math.stanford.edu/~conrad/154Page/handouts/genpell.pdf`, retrieved 3 September 2026; the file carries no printed date and was typeset on 26 July 2020, the date given for it in the bibliography of [1]. Its Theorem 2.1 is

the bounding theorem [1] quotes: for non-square $d > 0$, non-zero n and $u \in \mathbb{Z}[\sqrt{d}]^\times \setminus \{\pm 1\}$ with norm 1 and $u > 1$, every solution of $x^2 - dy^2 = n$ is equivalent to one with $|x| \le \sqrt{|n|}(1+\sqrt{u})/2$ and $|y| \le \sqrt{|n|}(1+\sqrt{u})/(2\sqrt{d})$.

[3] A. Dujella, *Diophantine m-tuples and Elliptic Curves*, Developments in Mathematics **79**, Springer, Cham, 2024, xi+335 pp.; DOI 10.1007/978-3-031-56724-7.

[4] A. Dujella, *Diophantine m-tuples* (running bibliography), `https://web.math.pmf.unizg.hr/~duje/ref.html`, consulted 3 September 2026. The source of the bibliographic data for [6, 7, 8, 9, 10, 11].

[5] B. He, A. Togbé and V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), no. 9, 6665–6709; DOI 10.1090/tran/7573. (The bibliography of [1] prints the year as 2018, which is the date of electronic publication; the issue is dated 2019, as Crossref and zbMATH record.)

[6] A. Hamtat, *Diophantine triples in triangular numbers*, preprint, 2025; listed in [4], which gives no venue and no identifier. We were unable to obtain a copy and make no claim about its contents.

[7] M. Bliznac Trebješanin, *On Diophantine pairs and triples of triangular numbers*, arXiv:2603.29565v2 [math.NT], 18 June 2026; also listed in [4] as a 2026 preprint. All numbered references above are to v2; v1 (31 March 2026) treats only $n = -1$ and contains none of the results cited here. No journal version is recorded on the abstract page, consulted 3 September 2026.

[8] A. Filipin and L. Szalay, *Triangular Diophantine tuples from* $\{1, 2\}$, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **27** (2023), 55–70.

[9] M. Jukić Bokun and I. Soldo, *Triangular $D(-1)$-tuples*, Bull. Math. Soc. Sci. Math. Roumanie, to appear.

[10] A. Filipin, A. Jurasić and L. Szalay, *Extensions of the Triangular $D(3)$-pair* $\{3, 6\}$, Math. Slovaca **75** (2025), 775–790.

[11] A. Filipin, Y. Fujita and A. Jurasić, *On the non-extendibility of Triangular $D(n)$-pairs* $\{n, 2n\}$ *with* $n = 2k^2 \pm k$, preprint, 2026; listed in [4].

[12] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.

[13] 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, 367–381; DOI 10.1145/3372885.3373824.