# CONGRUENCE OBSTRUCTIONS FOR $D(z)$-QUADRUPLES IN $\mathbb{Z}[\sqrt{-2}]$

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $\omega = \sqrt{-2}$. A $D(z)$-$m$-tuple in $\mathbb{Z}[\omega]$ is a set of $m$ nonzero elements whose pairwise products, increased by $z$, are all squares. Dujella and Soldo determined the $z$ for which a $D(z)$-quadruple exists, up to three congruence classes and the three individual values $z \in \{-1, 1 \pm 2\omega\}$; for $z = -1$ they record the conjecture that none exists. Both non-existence statements in that classification follow from a congruence argument. We show that the method is exhausted. If $z$ is a difference of two squares of $\mathbb{Z}[\omega]$ — by a theorem of Dujella and Franušić, exactly when $z$ avoids the two classes already excluded — then for *every* modulus $m \geq 1$ there are four distinct nonzero elements of $\mathbb{Z}[\omega]$ all six of whose pairwise products, increased by $z$, are squares modulo $m$. Consequently no congruence argument at any modulus can prove that no $D(-1)$-quadruple exists, and none can settle any remaining case of the classification negatively. A congruence can still obstruct the extension of a *fixed* triple, and we exhibit an infinite family of such triples at $z = -1$: for $b \in \mathbb{Z}$ the set $T_b = \{-2,\ b^2-1-b\omega,\ b^2-1+b\omega\}$ is a $D(-1)$-triple whenever $b \neq 0$, and whenever $8 \nmid b$ it lies in no $D(-1)$-quadruple, by a single reduction modulo 16. Two of its three entries are not rational integers. All statements are formally verified in Lean 4, apart from two small steps that are identified in the text as done by hand.

## 1. Introduction

Let $R$ be a commutative ring with identity and $z \in R$. Following the classical terminology, a finite set $\{a_1, \ldots, a_m\} \subset R \setminus \{0\}$ is a *$D(z)$-$m$-tuple* if $a_i a_j + z$ is a square in $R$ for all $1 \leq i < j \leq m$. Fermat's set $\{1, 3, 8, 120\}$ is a $D(1)$-quadruple in $\mathbb{Z}$.

This paper concerns $R = \mathbb{Z}[\omega]$ with $\omega = \sqrt{-2}$, the ring of integers of $\mathbb{Q}(\sqrt{-2})$. For $x = p + q\omega$ we write $\mathrm{N}(x) = x\bar{x} = p^2 + 2q^2$. The existence question in this ring was opened by Abu Muriefah and Al-Rashed [1] and brought close to a complete answer by Dujella and Soldo [10], whose classification we shall refer to throughout.

> **Theorem A** ([10, Theorem 1.1], as quoted in [11]; we write $\omega$ for $\sqrt{-2}$). *Let $z \in \mathbb{Z}[\omega]$. If $z$ is of the form $z = a + (2b+1)\omega$ or $z = 4a + (4b+2)\omega$, $a, b \in \mathbb{Z}$, then there does not exist a $D(z)$-quadruple in $\mathbb{Z}[\omega]$. If $z$ is not of one of these two forms, then there exists at least one $D(z)$-quadruple, except possibly if $z$ has one of the forms*
>
> $$z = 24a + 2 + (12b+6)\omega, \quad z = 24a + 5 + (12b+6)\omega, \quad z = 48a + 44 + (24b+12)\omega, \quad a, b \in \mathbb{Z},$$
>
> *or if $z \in \{-1, 1 \pm 2\omega\}$.*

Soldo [14] settled a large part of the three exceptional congruence classes, and Dujella and Soldo [11, Theorem 1.7] have recently shown that each of the residue classes modulo 11 left open by [14] contains infinitely many $z$ admitting a $D(z)$-quadruple. What is left after [11] is (i) the individual values $z \in \{-1, 1 \pm 2\omega\}$ and (ii) the individual pairs $(a, b)$ for which the constructions have so far produced nothing: thirteen of them for the class $24a+5+(12b+6)\omega$ and nineteen for $24a+2+(12b+6)\omega$, listed up to the conjugation $(a, b) \mapsto (a, -b-1)$ in [11, Tables 1 and 2]; the third class is not tabulated separately there, its values being the image of the second under $z \mapsto -2z$. The tables carry the explicit warning that they "should therefore be understood only as a record of the limitations of this particular regular search. They do not assert non-existence of $D(z)$-quadruples." Characterizing the $z \in \mathbb{Z}[\omega]$ that admit a $D(z)$-quadruple is Problem 1.8 of Dujella's open-problem list [7].

The sharpest of the open cases is $z = -1$. Dujella and Soldo write [11, Section 5]: "At present, no example of a $D(-1)$-quadruple in $\mathbb{Z}[\omega]$ is known to us. In addition, extensive computer searches have failed to find such an example, which supports the conjecture that no $D(-1)$-quadruple exists in this

ring." For the two remaining values $1 \pm 2\omega$ they record that their search also found no quadruple but that triples do exist, for instance $\{-2, 1, 1 \pm 2\omega\}$; and, since $1 \pm 2\omega = -1 \cdot (1 \mp \omega)^2$, a $D(-1)$-quadruple would produce $D(1 \pm 2\omega)$-quadruples, though the converse does not follow.

**The method, and its limit.** Both non-existence statements of Theorem A follow from a congruence argument (Section 4): one reduces modulo a fixed $m$ and shows that four residues cannot satisfy the six conditions simultaneously. The same device, at $m = 4$, is what [11, Section 5] uses to prove that its infinite family of $D(1 + 2\omega)$-triples $S_n = \{1, n^2 - 1 - 2\omega, n^2 + 2n - 2\omega\}$ extends to no quadruple. It is therefore natural to ask whether a larger modulus settles $z = -1$.

Our main result says that no modulus does, and identifies exactly why. Call $z$ *obstructed at* $m$ if there is no quadruple of residues modulo $m$ satisfying all six conditions (Definition 3.2); obstruction at some $m$ implies non-existence of a $D(z)$-quadruple in the whole ring. The obstruction is governed by a single equation: a residue is compatible with itself exactly when $z$ is a difference of two squares modulo $m$, and if $z = t^2 - r^2$ holds already in $\mathbb{Z}[\omega]$ then translating $r$ by multiples of $m$ produces four genuinely distinct nonzero elements that satisfy every condition at once. This is Theorem 6.1:

> *If $r^2 + z = t^2$ for some $r, t \in \mathbb{Z}[\omega]$, then for every integer $m \geq 1$ there are four pairwise distinct nonzero $a_1, a_2, a_3, a_4 \in \mathbb{Z}[\omega]$ such that $a_i a_j + z$ is congruent modulo $m$ to a square of $\mathbb{Z}[\omega]$, for all $1 \leq i < j \leq 4$.*

By a theorem of Dujella and Franušić [8, Theorem 1], which [11] itself invokes, the elements of $\mathbb{Z}[\omega]$ representable as a difference of two squares are precisely those *outside* the two classes of Theorem A. So the dichotomy is exact: the two classes Theorem A excludes are obstructed — the first already modulo 2, the second modulo 4 — and no other $z$ is obstructed at any modulus whatsoever. In particular $z = -1$, $z = 1 \pm 2\omega$ and all three exceptional congruence classes are obstruction-free (Proposition 6.3), so the conjecture of [11] is unreachable by congruences, and so is a negative answer for any remaining entry of its tables.

We stress what this does and does not assert. It does not produce a $D(z)$-quadruple, and it does not say that one exists. For most $z$ outside the two classes a quadruple is already known, and there the statement is empty of interest; its content lies exactly where existence is open, that is at $z \in \{-1, 1 \pm 2\omega\}$ and at the individual values of [11, Tables 1 and 2].

**Fixing a triple.** A congruence argument can still succeed if some of the four elements are held fixed — that is the shape of the $S_n$ argument of [11]. There is a clean criterion for when it cannot: if one member $a$ of a triple satisfies $a^2 + z$ a square, then the residue of $a$ extends the triple modulo every $m$ (Proposition 6.6 (iv)). At $z = -1$ this covers every triple containing $\pm 1$, since $(\pm 1)^2 - 1 = 0$; that is precisely why the published families $\{1, b, c\}$ of [15, 16, 9] are invisible to congruences. Each of those papers first proves that the third element is a rational integer and then imports the corresponding statement over $\mathbb{Z}$ — for the $b$ at hand, or, since [2], in the form that $\mathbb{Z}$ contains no $D(-1)$-quadruple at all.

Our second result is an infinite family at $z = -1$ that avoids $\pm 1$ and is therefore visible. For $b \in \mathbb{Z}$ put

$$x_b = b^2 - 1 - b\omega, \qquad \bar{x}_b = b^2 - 1 + b\omega, \qquad T_b = \{-2,\ x_b,\ \bar{x}_b\}.$$

Theorem 7.2 states that $T_b$ is a $D(-1)$-triple for every $b \neq 0$ and that for every $b$ with $8 \nmid b$ it extends to no $D(-1)$-quadruple. The proof is one reduction modulo 16; it uses no Pell theory and no input from the $\mathbb{Z}$ case. The triples are regular in the sense of [11, Section 2], with $r = -b^2$, so they are that paper's own construction applied to a conjugate pair at $z = -1$; and two of the three entries have imaginary part $\mp b \neq 0$, so no member of the family is a set of rational integers.

Neither the object nor the method is unprecedented, and it is worth saying exactly what is not. A single congruence applied to a fixed triple is the argument of [11, Section 5] for $S_n$, whose entries are likewise not all rational; what is added here is that the device reaches $z = -1$, where that paper proves nothing. Non-extendable $D(-1)$-triples in $\mathbb{Z}[\omega]$ are known as well: [15] treats $\{1, b, c\}$ for $b \in \{2, 5, 10, 17\}$ in $\mathbb{Z}[\sqrt{-t}\,]$ with $t \notin \{1, 4, 9, 16\}$, [16] treats $b \in \{26, 37, 50\}$ with $t \notin \{1, 4, 9, 25, 36, 49\}$, and [9, 13] treat further shapes; $t = 2$ falls under all of them. Tuples with irrational entries are not

new either: [4] multiplies the $D(1)$-quadruples of $\mathbb{Z}$ by $i$ and obtains infinitely many $D(-1)$-quadruples in $\mathbb{Z}[i]$, and [3] bounds the length of a $D(\pm1)$-tuple in the ring of integers of an imaginary quadratic field with no restriction on the entries.

What we have not found — in [6, 7, 5], in the papers cited here, or in a full-text search of an arXiv corpus — is a published *non-extendable* $D(-1)$-triple in $\mathbb{Z}[\sqrt{-t}\,]$ with an entry outside $\mathbb{Z}$, or a proof of non-extendability at $z=-1$ that does not import the corresponding statement over $\mathbb{Z}$. Both are outcomes of a search and are to be read as "not found". Nor is $T_b$ a rescaling of the $\{1,b,c\}$ families: [11, Lemma 2.1] scales a $D(z)$-quadruple by $\xi$ into a $D(z\xi^2)$-quadruple, and the same one-line computation applies to a triple, so at $z=-1$ the scaling preserves $z$ only for the units $\xi=\pm1$, while $\pm T_b$ never has the form $\{1,b,c\}$.

The hypothesis $8 \nmid b$ is not an artefact of the modulus chosen: at $b=8$ neither the modulus-8 nor the modulus-16 test finds an obstruction (Proposition 7.3), and a search outside the formal development found no obstruction at any prime power $\le 200$ for $b \in \{8,16,24,32,40,64\}$. Whether those $T_b$ extend is left open.

**Plan.** Section 2 fixes notation and records the finite test for squareness in $\mathbb{Z}[\omega]$ on which every negative statement here rests. Section 3 sets up reduction modulo an arbitrary $m$ and the two search predicates. Section 4 proves the non-existence half of Theorem A for all $a,b$. Section 5 records the difference-of-two-squares characterization with explicit witnesses. Section 6 contains the main theorem and its controls, Section 7 the family $T_b$, and Section 8 the computations reproducing [11] together with the box searches in the three open cells. Section 9 describes the formal verification.

## 2. Preliminaries

Throughout, $\omega=\sqrt{-2}$ and $\mathbb{Z}[\omega]=\{p+q\omega : p,q\in\mathbb{Z}\}$, a commutative ring with $\omega^2=-2$; for $x=p+q\omega$ we write $\operatorname{Re}x=p$, $\operatorname{Im}x=q$ and $\mathrm{N}(x)=p^2+2q^2$, so that N is multiplicative and non-negative. An element $x$ is a *square* if $x=y^2$ for some $y\in\mathbb{Z}[\omega]$. A *$D(z)$-$m$-tuple* is a set of $m$ pairwise distinct nonzero elements whose pairwise products, increased by $z$, are all squares; the cases $m=3,4$ are called triples and quadruples. For $B\in\mathbb{N}$ let $\square_B=\{p+q\omega : |p|,|q|\le B\}$, a set of $(2B+1)^2$ elements.

Squareness is an existential over an infinite ring, and the ring has no square-root function. The following elementary reduction is what makes every negative statement in this paper a theorem rather than an unrefuted guess.

**Lemma 2.1** (Bounded search)**.** *Let $x\in\mathbb{Z}[\omega]$ and $B\in\mathbb{N}$ with $\mathrm{N}(x)\le B^4$. Then $x$ is a square if and only if $x=y^2$ for some $y\in\square_B$. Moreover, if $x=y^2$ with $y=p+q\omega$, then, writing $\nu=\sqrt{\mathrm{N}(x)}$,*

$$p^2=\frac{\nu+\operatorname{Re}x}{2},\qquad q^2=\frac{\nu-\operatorname{Re}x}{4},$$

*so that $x$ has at most the four square roots $\pm p\pm q\omega$ determined by these equations.*

*Proof.* If $y^2=x$ then $\mathrm{N}(y)^2=\mathrm{N}(x)\le(B^2)^2$, so $\mathrm{N}(y)\le B^2$; since $\mathrm{N}(y)=p^2+2q^2$ this bounds $|p|$ and $|q|$ by $B$ separately. For the second part, comparing coefficients in $y^2=x$ gives $p^2-2q^2=\operatorname{Re}x$, while $p^2+2q^2=\mathrm{N}(y)=\sqrt{\mathrm{N}(x)}=\nu$; adding and subtracting gives the two displayed identities. □

The hypothesis $\mathrm{N}(x)\le B^4$ cannot be dropped, and the second part of Lemma 2.1 turns the test for squareness into a constant-time computation, which is what the searches of Section 8 run; see Proposition 8.5.

## 3. Reduction modulo an arbitrary modulus

Fix $m\ge1$. Since $\mathbb{Z}[\omega]\cong\mathbb{Z}[X]/(X^2+2)$, the quotient $\mathbb{Z}[\omega]/m\mathbb{Z}[\omega]$ is the set $\mathcal{R}_m=(\mathbb{Z}/m)\times(\mathbb{Z}/m)$ of pairs, with componentwise addition and the product

$$(\alpha_1,\beta_1)\cdot(\alpha_2,\beta_2)=(\alpha_1\alpha_2-2\beta_1\beta_2,\ \alpha_1\beta_2+\beta_1\alpha_2). \tag{1}$$

Write $\rho_m : \mathbb{Z}[\omega] \to \mathcal{R}_m$, $\rho_m(p+q\omega) = (p \bmod m,\ q \bmod m)$, and let $\mathcal{S}_m = \{A \cdot A : A \in \mathcal{R}_m\}$ be the set of square residues.

**Lemma 3.1.** *$\rho_m$ is a ring homomorphism for the operations above, and if $x \in \mathbb{Z}[\omega]$ is a square then $\rho_m(x) \in \mathcal{S}_m$.*

*Proof.* Both statements are immediate from (1): the first by comparing coefficients, the second by applying the first to $x = y^2$. □

Only $m = 2, 4, 8, 16$ occur below. For those we use explicit lists of 2, 4, 8 and 24 residues, each certified *complete* — that is, containing every square residue — by evaluating $A \cdot A$ over all $m^2$ residues $A$. Completeness is the direction every non-existence statement below needs: a list larger than $\mathcal{S}_m$ can only make an obstruction harder to certify. At $m = 2$ and $m = 4$ the lists are moreover exactly $\mathcal{S}_m$. Modulo 2 this is immediate, since $(p+q\omega)^2 \equiv p^2$, so that $\mathcal{S}_2 = \{0, 1\}$; modulo 4 it is proved, and gives

$$\mathcal{S}_4 = \{0,\ 1,\ 2,\ 3 + 2\omega\},$$

which is the direct computation recorded in [11, Section 5]. Here the list is produced from the definition rather than assumed, and equality with the four residues named there is proved. At $m = 8, 16$ only completeness is certified, so the two *negative* outcomes reported at those moduli — Propositions 6.6 (i) and 7.3 (iii), which record that a search found no obstruction — are statements about the search as run against the certified lists. Nothing in this paper rests on them: that $z = -1$ is obstructed at no modulus at all is Corollary 6.2, which uses no list.

**Definition 3.2.** Let $z \in \mathbb{Z}[\omega]$ and $Z = \rho_m(z)$. We say $z$ is *obstructed at $m$* if there is no 4-tuple $(A_1, A_2, A_3, A_4) \in \mathcal{R}_m^4$ with $A_iA_j + Z \in \mathcal{S}_m$ for all $1 \le i < j \le 4$. Similarly, a triple $(a, b, c)$ of elements of $\mathbb{Z}[\omega]$ is *extension-obstructed at $m$* if no $D \in \mathcal{R}_m$ satisfies $\rho_m(a)D+Z,\ \rho_m(b)D+Z,\ \rho_m(c)D+Z \in \mathcal{S}_m$.

The residues $A_i$ are not required to be distinct or nonzero: distinctness and non-vanishing are conditions in $\mathbb{Z}[\omega]$, not modulo $m$. This is what makes the definition usable, and also what limits it.

**Proposition 3.3.** *Let $z \in \mathbb{Z}[\omega]$ and $m \ge 1$.*

1. *If $z$ is obstructed at $m$, then $\mathbb{Z}[\omega]$ contains no $D(z)$-quadruple.*
2. *If a triple $(a, b, c)$ is extension-obstructed at $m$, then no $d \in \mathbb{Z}[\omega]$ makes all of $ad + z$, $bd + z$, $cd + z$ squares; in particular $\{a, b, c\}$ lies in no $D(z)$-quadruple.*

*Proof.* For (i), a $D(z)$-quadruple $\{a_1, \dots, a_4\}$ has $a_ia_j + z$ a square for all six pairs, so by Lemma 3.1 the residues $A_i = \rho_m(a_i)$ satisfy $A_iA_j + Z \in \mathcal{S}_m$ for all six, contradicting the hypothesis. Part (ii) is the same argument with three of the four elements fixed. □

*Remark* 3.4. Deciding Definition 3.2 naively means quantifying over $\mathcal{R}_m^4$, that is $m^8$ cases. All searches below are instead run in neighbour-list form: for each $A_1$ one first computes the list of residues compatible with $A_1$ and quantifies only inside it. At $m = 4$ this is the difference between a computation we measured at 95 seconds and 7.7 gigabytes and one that takes seconds; at $m = 16$ it is what makes the search possible at all.

## 4. The two obstructed classes

The non-existence half of Theorem A is a statement about every $a, b \in \mathbb{Z}$. It is Lemma 2.3 of [10], which attributes it to [12, Proposition 5], where it is proved for every $d \equiv 2 \pmod 4$ in place of $-2$. Here both halves are instances of Proposition 3.3 (i).

**Theorem 4.1** (Franušić; Dujella–Soldo)**.** *Let $a, b \in \mathbb{Z}$. There is no $D(z)$-quadruple in $\mathbb{Z}[\omega]$ for $z = a+(2b+1)\omega$, and none for $z = 4a+(4b+2)\omega$. More precisely, every $z$ with $\operatorname{Im} z$ odd is obstructed at $m = 2$, and every $z$ with $4 \mid \operatorname{Re} z$ and $\operatorname{Im} z \equiv 2 \pmod 4$ is obstructed at $m = 4$.*

*Proof.* For the first class, the search of Definition 3.2 at $m = 2$ over the four residues of $\mathcal{R}_2$ returns that no four residues are pairwise compatible when $Z$ has odd second coordinate; the conclusion follows from Proposition 3.3 (i). The content of that finite check is visible: by Lemma 3.1 and (1) a square has even imaginary part, so all six numbers $\operatorname{Im}(a_i a_j)$ would have to be odd, that is, the alternating form $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \mapsto \alpha_1\beta_2 + \beta_1\alpha_2$ on $\mathbb{F}_2^2$ would have to take the value 1 on all six pairs drawn from four vectors; but only the three nonzero vectors of $\mathbb{F}_2^2$ are pairwise so related. For the second class the same search at $m = 4$, over the 16 residues of $\mathcal{R}_4$, finds no compatible quadruple (indeed no compatible pair $A, A$), and Proposition 3.3 (i) applies again. Both parametrized statements follow: $2b + 1$ is odd, and $4a$, $4b + 2$ satisfy the divisibility conditions. □

The two moduli are the right ones. For the class $a + (2b + 1)\omega$ the obstruction is already visible over the four residues of $\mathcal{R}_2$, in the two-line form given in the proof. The second class genuinely needs modulus 4: modulo 2 such a $z$ is 0, and then the four zero residues satisfy all six conditions.

## 5. Differences of two squares

The two classes of Theorem 4.1 have a second description, which is the reason the congruence method stops exactly there.

**Proposition 5.1** (Dujella–Franušić)**.** *For $z \in \mathbb{Z}[\omega]$ the following are equivalent:*

(1) *there are $r, t \in \mathbb{Z}[\omega]$ with $r^2 + z = t^2$;*
(2) *$\operatorname{Im} z$ is even, and it is not the case that both $4 \mid \operatorname{Re} z$ and $\operatorname{Im} z \equiv 2 \pmod 4$.*

*Explicit witnesses for (i), in the three cases of (ii), are*

$$z = 2s + 1 + 2j\omega : \qquad z = \big(s + 1 + j\omega\big)^2 - \big(s + j\omega\big)^2, \tag{2}$$

$$z = 4k + 2 + 2j\omega : \qquad z = \big(j - k\omega\big)^2 - \big(j - (k+1)\omega\big)^2, \tag{3}$$

$$z = 4s + 4u\omega : \qquad z = \big(s + 1 + u\omega\big)^2 - \big(s - 1 + u\omega\big)^2. \tag{4}$$

*Proof.* (ii)⇒(i). Write $\operatorname{Im} z = 2j$. If $\operatorname{Re} z$ is odd, use (2). If $\operatorname{Re} z \equiv 2 \pmod 4$, use (3); this is the factorization $z = \omega \cdot (z/\omega)$ with both factors congruent to $\omega$ modulo 2. If $4 \mid \operatorname{Re} z$, then (ii) forces $4 \mid \operatorname{Im} z$, and (4) applies. Each of the three is a polynomial identity in $\mathbb{Z}[\omega]$.

(i)⇒(ii). For any $y \in \mathbb{Z}[\omega]$, $\operatorname{Im}(y^2) = 2 \operatorname{Re} y \operatorname{Im} y$ is even, so $r^2 + z = t^2$ forces $\operatorname{Im} z$ even. For the second condition, reduce $r^2 + z = t^2$ modulo 4: an exhaustive check of the $16 \times 16$ pairs $(\rho_4(r), \rho_4(t))$ shows that $R \cdot R + (0, 2) = T \cdot T$ has no solution in $\mathcal{R}_4$, which rules out every $z$ with $4 \mid \operatorname{Re} z$ and $\operatorname{Im} z \equiv 2 \pmod 4$. □

Proposition 5.1 is the case $d = -2$ of [8, Theorem 1], whose clause for $d \equiv 2 \pmod 4$ with $x^2 - dy^2 = \pm 2$ solvable — which holds for $d = -2$ with $(x, y) = (0, 1)$ — lists the representable elements as $2m + 1 + 2n\sqrt{d}$, $4m + 4n\sqrt{d}$, $4m + 2 + 4n\sqrt{d}$, $4m + 2 + (4n + 2)\sqrt{d}$ — exactly the complement of the two classes of Theorem A. The paper [11] cites that theorem for the same purpose. We have reproved it here because the result of the next section needs the *witness* $r$, not merely the existence statement.

## 6. No congruence obstruction outside the two classes

Write $x \equiv \square \pmod m$, for $x \in \mathbb{Z}[\omega]$ and $m \in \mathbb{Z}$, to mean that $x = y^2 + mc$ for some $y, c \in \mathbb{Z}[\omega]$. This is a statement inside $\mathbb{Z}[\omega]$, with no quotient ring in it, so a single formula quantifies over all moduli at once.

**Theorem 6.1.** *Let $z \in \mathbb{Z}[\omega]$ and suppose $r^2 + z = t^2$ for some $r, t \in \mathbb{Z}[\omega]$. Then for every integer $m \geq 1$ there exist $a_1, a_2, a_3, a_4 \in \mathbb{Z}[\omega]$, pairwise distinct and all nonzero, such that*

$$a_i a_j + z \;\equiv\; \square \pmod m \qquad \text{for all } 1 \leq i < j \leq 4.$$

*Explicitly one may take $a_i = r + m(K + i)$ for $i = 1, 2, 3, 4$, where $K = |\operatorname{Re} r| + 1$.*

*Proof.* For any $u, v \in \mathbb{Z}$,

$$\big(r+mu\big)\big(r+mv\big)+z \;=\; \big(r^2+z\big)+m\big((u+v)r+muv\big) \;=\; t^2+m\big((u+v)r+muv\big),$$

so every such product, increased by $z$, is congruent to the square $t^2$ modulo $m$. Taking $u, v \in \{K+1, K+2, K+3, K+4\}$ gives all six conditions at once. For distinctness and non-vanishing, note that $\operatorname{Re} a_i = \operatorname{Re} r + m(K+i)$. Since $m \geq 1$ and $K+i \geq K \geq |\operatorname{Re} r|+1$ we get $m(K+i) \geq K+i > |\operatorname{Re} r|$, so $\operatorname{Re} a_i > 0$ and $a_i \neq 0$; and $\operatorname{Re} a_i = \operatorname{Re} a_j$ forces $m(K+i) = m(K+j)$, hence $i = j$ because $m \neq 0$. □

The proof uses no computation whatsoever: it is one algebraic identity plus a bound. What the identity says is that a congruence argument sees only the diagonal. A residue $A$ is compatible with itself precisely when $A^2 + Z \in \mathcal{S}_m$, and if that happens for $A = \rho_m(r)$ then the constant 4-tuple $(A, A, A, A)$ already satisfies Definition 3.2; the content of Theorem 6.1 is that the constant tuple can be spread out into four honestly distinct nonzero elements of the ring, so that nothing is lost by the failure of the residues to be distinct.

**Corollary 6.2.** *Let $z \in \mathbb{Z}[\omega]$ satisfy the equivalent conditions of Proposition 5.1, that is, let $z$ lie outside the two classes of Theorem A. Then $z$ is obstructed at no modulus $m \geq 1$.*

*Proof.* Take $a_1, \ldots, a_4$ from Theorem 6.1 and set $A_i = \rho_m(a_i)$. From $a_i a_j + z = y^2 + mc$ we get $A_i A_j + Z = \rho_m(y)^2 \in \mathcal{S}_m$ by Lemma 3.1, so Definition 3.2 fails at $m$. □

**Proposition 6.3.** *Each of the following $z$ is a difference of two squares in $\mathbb{Z}[\omega]$, with the witness $(r, t)$ displayed, and hence, by Corollary 6.2, is obstructed at no modulus:*

| | | |
|---|---|---|
| $z = -1,$ | $r = 1,$ | $t = 0;$ |
| $z = 1 + 2\omega,$ | $r = \omega,$ | $t = 1 + \omega;$ |
| $z = 1 - 2\omega,$ | $r = \omega,$ | $t = 1 - \omega;$ |
| $z = 24a + 2 + (12b + 6)\omega,$ | $r = 6b + 3 - (6a + 1)\omega,$ | $t = 6b + 3 - 6a\,\omega;$ |
| $z = 24a + 5 + (12b + 6)\omega,$ | $r = 12a + 2 + (6b + 3)\omega,$ | $t = 12a + 3 + (6b + 3)\omega;$ |
| $z = 48a + 44 + (24b + 12)\omega,$ | $r = 12a + 10 + (6b + 3)\omega,$ | $t = 12a + 12 + (6b + 3)\omega,$ |

*the last three for all $a, b \in \mathbb{Z}$.*

*Proof.* Each line is a polynomial identity $r^2 + z = t^2$ in $\mathbb{Z}[\omega]$, checked by expanding both sides. □

**Corollary 6.4.** *For $z = -1$, for $z = 1 \pm 2\omega$, and for every $z$ in the three exceptional congruence classes of Theorem A, there is no modulus $m \geq 1$ at which $z$ is obstructed. Hence non-existence of a $D(z)$-quadruple for such a $z$ cannot be established by Proposition 3.3 (i) at any modulus; in particular the conjecture of* [11, Section 5] *that no $D(-1)$-quadruple exists in $\mathbb{Z}[\omega]$ is out of reach of that argument.*

*Remark* 6.5. The scope of Corollary 6.4 deserves a plain statement. For most $z$ outside the two classes of Theorem A a $D(z)$-quadruple is known to exist, and there the corollary is vacuous in effect. Its content is confined to the cases where existence is genuinely open: $z \in \{-1, 1 \pm 2\omega\}$, and the individual values of [11, Tables 1 and 2]. For those, it closes one route and says nothing about any other; in particular it gives no evidence for or against the conjecture of [11, Section 5]. What it does isolate is the role of the difference-of-two-squares condition: Problem 1.9 of [7] asks for a conjecture connecting the existence of $D(n)$-quadruples with representability of $n$ as a difference of two squares in an arbitrary commutative ring with identity, and Theorem 6.1 says that in $\mathbb{Z}[\omega]$ that condition is exactly what a congruence sees.

**Controls.** Theorem 6.1 is a non-existence statement about a method, so it is worth exhibiting that the method is neither vacuously weak nor vacuously strong.

**Proposition 6.6.** (1) *At $z = -1$ the four-residue search returns "not obstructed" for $m = 2, 4, 8, 16$; at $m = 2$ and $m = 4$, where the certified list is exactly $\mathcal{S}_m$, this says that $z = -1$ is not obstructed at the two moduli at which the classes of Theorem 4.1 are.*

(2) *At $z = \omega$ with $m = 2$, and at $z = 2\omega$ with $m = 4$, the same search returns "obstructed"; so Theorem 4.1 is not vacuous.*
(3) *Pairwise compatible* triples *of residues exist in both excluded classes, at $m = 2$ and at $m = 4$. Hence the obstruction of Theorem 4.1 sits exactly at length four, matching Theorem A and no more.*
(4) *If $a, b, c \in \mathbb{Z}[\omega]$ are such that $a^2 + z$, $ba + z$ and $ca + z$ are all squares, then $(a, b, c)$ is extension-obstructed at no modulus. In particular, at $z = -1$, no triple containing $1$ or $-1$ is extension-obstructed at any modulus.*

*Proof.* Items (i)–(iii) are finite evaluations: the search of Definition 3.2 at $m = 2, 4, 8, 16$, over $\mathcal{R}_m$ in the neighbour-list form of Remark 3.4, and three explicit compatible pairs in each of $\mathcal{R}_2$ and $\mathcal{R}_4$ for (iii). For (iv), the residue $\rho_m(a)$ itself satisfies the three conditions, by Lemma 3.1; the last sentence is the case $a = \pm 1$, $z = -1$, where $a^2 + z = 0$ is a square. □

*Remark* 6.7. The following computations were carried out outside the formal development and are reported as motivation only. For $q$ a prime power with $q \le 128$, let $C_q \subset \mathcal{R}_q$ be the complement of $\mathcal{S}_q - \mathcal{S}_q$. Then $C_q = \emptyset$ for every odd prime power $q \le 128$, while $|C_{2^k}|$ equals $2, 9, 36, 144, 576, 2304, 9216$ for $k = 1, \dots, 7$; in every case $C_{2^k}$ is the preimage of $C_4 = \{\text{Im odd}\} \cup \{2\omega\}$ under $\mathcal{R}_{2^k} \to \mathcal{R}_4$. Odd moduli never obstruct anything, since for odd $m$ the element 2 is invertible and $t = (1 + z)/2$, $r = (z - 1)/2$ solve $t^2 - r^2 = z$. A full search over every $z$ modulo $m$, for $m = 2, 4, 8$, found that the maximum size of a pairwise compatible tuple of residues is 3 exactly for $z \in C_m$ and unbounded otherwise. By the Chinese remainder theorem $\mathbb{Z}[\omega]/m\mathbb{Z}[\omega] \cong \prod_{p^k \| m} \mathbb{Z}[\omega]/p^k\mathbb{Z}[\omega]$ with squareness componentwise, so obstruction at $m$ is equivalent to obstruction at some prime power dividing $m$, and prime powers are all that need sweeping. Theorem 6.1 replaces this evidence with a proof.

## 7. An infinite family of non-extendable $D(-1)$-triples

By Proposition 6.6 (iv) a congruence proof at $z = -1$ must start from a triple avoiding $\pm 1$. We first recall the model for such an argument, from [11, Section 5], at $z = 1 + 2\omega$.

**Proposition 7.1** (Dujella–Soldo)**.** *For every $n \in \mathbb{Z}$ the set $S_n = \{1,\ n^2 - 1 - 2\omega,\ n^2 + 2n - 2\omega\}$ is a $D(1 + 2\omega)$-triple, with roots $n$, $n + 1$ and $n^2 + n - 1 - 2\omega$; and, writing $z = 1 + 2\omega$, for no $n \in \mathbb{Z}$ and no $d \in \mathbb{Z}[\omega]$ are $d + z$, $(n^2 - 1 - 2\omega)d + z$ and $(n^2 + 2n - 2\omega)d + z$ all squares. Moreover $1 \pm 2\omega = -1 \cdot (1 \mp \omega)^2$; and if $u, v$ are positive rational integers then $uv + 1 + 2\omega$ is not a square in $\mathbb{Z}[\omega]$, so no $D(1 + 2\omega)$-tuple contains two positive rational integers.*

*Proof.* The triple conditions are three polynomial identities. For the non-extendability, reduce modulo 4: the squares of $\mathcal{R}_4$ are exactly $\{0, 1, 2, 3 + 2\omega\}$, and over the 64 triples $(n, \operatorname{Re} d, \operatorname{Im} d)$ of residues modulo 4 the three conditions are never simultaneously satisfiable; Proposition 3.3 (ii) then applies. For the last statement, if $uv + 1 + 2\omega = (p + q\omega)^2$ with $u, v$ positive integers, comparing coefficients gives $pq = 1$ and $uv + 1 = p^2 - 2q^2 = -1$, which is impossible. □

At $z = -1$ nothing of this kind is proved in [11], which records only that no $D(-1)$-quadruple is known. Our family is the following. For $b \in \mathbb{Z}$ set

$$x_b = b^2 - 1 - b\omega, \qquad \bar{x}_b = b^2 - 1 + b\omega, \qquad T_b = \{-2,\ x_b,\ \bar{x}_b\}.$$

**Theorem 7.2.** *Let $b \in \mathbb{Z}$.*

(1) *If $b \neq 0$ then $T_b$ is a $D(-1)$-triple in $\mathbb{Z}[\omega]$, with the three square roots*

$$(-2)x_b - 1 = (1 + b\omega)^2, \qquad (-2)\bar{x}_b - 1 = (1 - b\omega)^2, \qquad x_b\bar{x}_b - 1 = (b^2)^2.$$

(2) *$T_b$ is regular in the sense of* [11, Section 2]*: with $r = -b^2$ one has $x_b\bar{x}_b - 1 = r^2$ and $x_b + \bar{x}_b + 2r = -2$.*
(3) *If $8 \nmid b$ then no $d \in \mathbb{Z}[\omega]$ makes all three of $(-2)d - 1$, $x_b d - 1$, $\bar{x}_b d - 1$ squares. Consequently $T_b$ is a $D(-1)$-triple which lies in no $D(-1)$-quadruple.*

*Proof.* (i) The three displayed identities are polynomial identities in $\mathbb{Z}[b]$: for instance $(-2)(b^2-1-b\omega)-1=-2b^2+1+2b\omega$ and $(1+b\omega)^2=1-2b^2+2b\omega$. The third is $x_b\bar{x}_b=\mathrm{N}(x_b)=(b^2-1)^2+2b^2=b^4+1$. For $b\neq 0$ the three entries are nonzero and pairwise distinct, since $\operatorname{Im} x_b=-b$ and $\operatorname{Im}\bar{x}_b=b$ are nonzero and distinct while $\operatorname{Im}(-2)=0$. Item (ii) is again a direct identity.

(iii) The residues of $x_b$ and $\bar{x}_b$ modulo 16 depend only on $B=b \bmod 16$: $\rho_{16}(x_b)=(B^2-1,-B)$ and $\rho_{16}(\bar{x}_b)=(B^2-1,B)$. The hypothesis $8\nmid b$ gives $B\notin\{0,8\}$, leaving 14 residues $B$. For each of these 14 values, an exhaustive check over all 256 residues $D\in\mathcal{R}_{16}$ shows that

$$(14,0)\cdot D+(15,0),\qquad (B^2-1,-B)\cdot D+(15,0),\qquad (B^2-1,B)\cdot D+(15,0)$$

are never all three in $\mathcal{S}_{16}$ — that is, $(-2,x_b,\bar{x}_b)$ is extension-obstructed at 16. Here $(14,0)=\rho_{16}(-2)$ and $(15,0)=\rho_{16}(-1)$. Proposition 3.3 (ii) gives the conclusion. The finite search is $14\times 256=3584$ cases, each the evaluation of three products in $\mathcal{R}_{16}$ and three membership tests in a 24-element list. □

Modulus 8 already handles every $b$ with $4\nmid b$; the residues $b\equiv 4 \pmod 8$ need 16, and a single check at 16 covers both. The proof is self-contained: no box search, no Pell equation, and no appeal to the corresponding question over $\mathbb{Z}$.

**Proposition 7.3.** (1) *$T_1=\{-2,-\omega,\omega\}$, $T_2=\{-2,3-2\omega,3+2\omega\}$ and $T_3=\{-2,8-3\omega,8+3\omega\}$.*

(2) *For $b\neq 0$ two of the three entries of $T_b$ have imaginary part $\mp b\neq 0$, so no member of the family is a set of rational integers.*

(3) *At $b=8$ the search behind Theorem 7.2 (iii) reports no obstruction either at $m=8$ or at $m=16$: modulo 16 the residue $D=3$ passes all three conditions for $T_8=\{-2,63-8\omega,63+8\omega\}$. So the hypothesis $8\nmid b$ is not an artefact of stopping at modulus 16.*

(4) *The $D(-1)$-triple $(1,2,5)$ of rational integers is extension-obstructed at no modulus: at $m=16$ the residue of 1 works, and by Proposition 6.6 (iv) the same holds at every $m$.*

*Proof.* (i) and (ii) are evaluation and inspection. (iii) and (iv) are finite evaluations of the search of Definition 3.2 at the stated moduli; for (iv) the general reason is Proposition 6.6 (iv) with $a=1$, since $1^2-1=0$, $2\cdot 1-1=1$ and $5\cdot 1-1=4$ are squares. □

*Remark* 7.4. Whether $T_b$ with $8\mid b$ extends to a $D(-1)$-quadruple is open. Two computations outside the formal development bear on it: a sweep of every prime power $q\le 200$ found no obstruction for $b\in\{8,16,24,32,40,64\}$, so no congruence proof built from those moduli exists; and a search over $|\operatorname{Re} d|,|\operatorname{Im} d|\le 3000$, about $3.6\cdot 10^7$ candidates, found no extension of $T_8$, $T_{16}$ or $T_{24}$. Those triples appear simply to be invisible to congruences.

*Remark* 7.5. The family was not found by search. A set of the shape $\{-2,x,\bar{x}\}$ with $x\neq\bar{x}$ is a $D(-1)$-triple exactly when $-2x-1$ and $\mathrm{N}(x)-1$ are squares, the third condition being the conjugate of the first. Writing $-2x-1=(\alpha+\gamma\omega)^2$ forces $\alpha$ odd and $x=-(\alpha^2-2\gamma^2+1)/2-\alpha\gamma\,\omega$, and then $\mathrm{N}(x)-1=\big((\alpha^2+2\gamma^2)^2+2(\alpha^2-2\gamma^2)-3\big)/4$. At $\alpha=1$ that expression collapses identically to $\gamma^4$, and $T_b$ is what remains.

## 8. Computations

This section records what has been verified computationally: first the reproduction of the constructions of [11], then searches in the three open cells. Nothing here is a non-existence theorem, and the searches are stated as what they are.

**Proposition 8.1.** *Let $z,u,v,r\in\mathbb{Z}[\omega]$ with $uv+z=r^2$. If moreover $u(u+4v+4r)+z=y^2$ for some $y\in\mathbb{Z}[\omega]$, then all six products of $\{u,\ v,\ u+v+2r,\ u+4v+4r\}$, increased by $z$, are squares, with roots $r$, $u+r$, $v+r$, $y$, $2v+r$ and $u+2v+3r$ respectively. Five of the six conditions use only $uv+z=r^2$.*

*In particular, for the first parametrization of* [11, Proposition 3.1] *— $e=1-\omega$, $v=2\omega$ and $r=-9+(-18s+20)\omega$ with $s\in\mathbb{Z}$ — the displayed set*

$$\big\{-108s^2+480s-393+(216s^2-438s+187)\omega,\ \ 2\omega,$$

$$-108s^2+480s-411+(216s^2-474s+229)\omega,$$
$$-108s^2+480s-429+(216s^2-510s+275)\omega\,\big\}$$

*is a $D(z)$-quadruple for* every $s\in\mathbb{Z}$, *where* $z=216s^2-312s+29+(216s^2-636s+426)\omega$ *lies in the class* $24a+5+(12b+6)\omega$ *with* $a=9s^2-13s+1$ *and* $b=18s^2-53s+35$.

*Proof.* The four derived roots are single linear combinations of $uv+z-r^2$; only the fourth condition needs the hypothesis $u(u+4v+4r)+z=y^2$, which is why the search of [11] reduces to the single equation $3z=(u+2r-y)(u+2r+y)$. For the parametrized family, the third and fourth displayed entries are checked to equal $u+v+2r$ and $u+4v+4r$, and both hypotheses hold, the second with

$$y=u+2r-e=-108s^2+480s-412+(216s^2-474s+228)\omega,$$

a root that [11] does not display and which we recovered by computation and then verified symbolically. Non-degeneracy is arithmetic: the real parts of the three entries other than $2\omega$ are congruent to $3,1,3$ modulo 4, hence never zero, and differ pairwise by 18, 36 and 18. □

**Proposition 8.2.** *Let* $z=29+114\omega$, *the entry* $(a,b)=(1,9)$ *of* [11, Table 1]. *Then* $\mathrm{N}(z)=26833$ *and* 26833 *is prime, and the four rows of* [11, Proposition 4.1] *check exactly:*

$$\begin{aligned}
e=1:\quad & S=e+f=1+3z=88+342\omega,\\
& T_1=S^2-16z=-226648+58368\omega=-8(57-7\omega)(513-65\omega);\\
e=3:\quad & S=e+f=3+z=32+114\omega,\\
& T_3=S^2-16z=-25432+5472\omega=-8(57-7\omega)(57-5\omega);\\
e=1+\omega:\quad & f=257+85\omega,\qquad S=e+f=258+86\omega,\\
& T_{1+\omega}=S^2-16z=51308+42552\omega=-4(1-6\omega)(9-2\omega)(213-86\omega);\\
e=1-\omega:\quad & f=-199+143\omega,\qquad S=e+f=-198+142\omega,\\
& T_{1-\omega}=S^2-16z=-1588-58056\omega=4(3-2\omega)(11-12\omega)(243+28\omega),
\end{aligned}$$

*where* $f=3z/e$, *so that* $ef=3z$ *in each row.*

*Proof.* Each line is an evaluation in $\mathbb{Z}[\omega]$; primality of 26833 is a direct verification. □

We emphasize what Proposition 8.2 does not include. The proof of [11, Proposition 4.1] concludes by enumerating the divisors $u\mid T_e$ in the norm-Euclidean ring $\mathbb{Z}[\omega]$; that enumeration is not verified here, so [11, Proposition 4.1] itself is not among the statements we assert. Only its displayed arithmetic is.

**Proposition 8.3.** *Let* $z\in\{-1,\,1+2\omega,\,1-2\omega\}$. *No four pairwise distinct elements of* $\square_{15}$ *are pairwise compatible for* $z$; *in particular no $D(z)$-quadruple has all four entries with* $|\operatorname{Re}|,|\operatorname{Im}|\le 15$. *Moreover the triple* $\{1,2,5\}$ *at* $z=-1$ *and the triples* $\{-2,1,1\pm2\omega\}$ *at* $z=1\pm2\omega$ *have no fourth element in* $\square_{400}$.

*Proof.* For the first statement, the compatibility graph on the 961 elements of $\square_{15}$ is computed for each of the three values of $z$ — an edge between $a\neq b$ whenever $ab+z$ is a square, decided by the four-candidate test of Lemma 2.1 — and is found to contain no 4-clique. For the second, the $801^2=641\,601$ elements of $\square_{400}$ are filtered by the three conditions imposed by the named triple, and the filter is empty in each case. In both shapes the bridge from the Boolean search to the statement about elements of $\mathbb{Z}[\omega]$ is proved separately, so only the evaluation is computational. □

*Remark* 8.4. Proposition 8.3 is a statement about a box and nothing more. The ring is infinite and non-existence of a $D(z)$-quadruple is not a finitely decidable question; the framing in [11, Section 4] is the same. Larger searches outside the formal development agree and go further: over the 40 400 nonzero elements with $|\operatorname{Re}|,|\operatorname{Im}|\le 100$ there are 18 378 edges and 6 996 triples at $z=-1$ and 30 584 edges and 11 700 triples at $z=1\pm2\omega$, with no quadruple in any case; and extending each of the three named triples over $|\operatorname{Re}|,|\operatorname{Im}|\le 10^4$, about $4\cdot10^8$ candidates each, produced no extension. The

graphs for $1+2\omega$ and $1-2\omega$ have identical statistics, as conjugation requires; that identity was used as a check on the search code. No comparison with the searches of [11] is intended: the one reported in its Section 4 runs over the exceptional congruence classes and looks only for quadruples of the regular shape, and the "extensive computer searches" at $z=-1$ of its Section 5 are reported without a range.

**Proposition 8.5.** (1) *The hypothesis* $\mathrm{N}(x)\le B^4$ *of Lemma 2.1 cannot be dropped:* 9 *is a square, its root* 3 *lies outside* $\square_1$*, and* $\mathrm{N}(9)=81>1$*.*

(2) $\{1,3,8,120\}$ *is a* $D(1)$*-quadruple and* $\{1,3,8,121\}$ *is not, the latter because* $1\cdot 121+1=122$ *is not a square in* $\mathbb{Z}[\omega]$ *— verified through Lemma 2.1 with* $B=12$*, since* $\mathrm{N}(122)=14884\le 20736$*.*

(3) $\{-3,-1,1,3\}$ *is a* $D(1)$*-quadruple all of whose entries lie in* $\square_{15}$*, and the graph of Proposition 8.3 does contain a* 4*-clique at* $z=1$ *on that same box; the extension filter of the same proposition, run on* $\{1,3,8\}$ *at* $z=1$ *over* $\square_{400}$*, is likewise not empty — it returns* 0 *and Fermat's* 120*. Hence the negative results of Proposition 8.3 are about those* $z$ *and not about* $\square_{15}$ *being too small to contain any quadruple, nor about either search being unable to report a positive.*

(4) $\{1,2,5\}$ *is a* $D(-1)$*-triple and* $\{-2,1,1\pm 2\omega\}$ *are* $D(1\pm 2\omega)$*-triples, so the three open cells are non-vacuous at length three.*

*Proof.* Each item is a finite verification; (ii) and (iii) use Lemma 2.1 to turn the negative square conditions into searches over explicit boxes. Note that $z=1$ is excluded by neither class of Theorem A, which is what (ii) and (iii) illustrate. □

## 9. Verification

Every lemma, proposition, theorem and corollary of this paper has been formally verified in Lean 4 against *Mathlib* [17], with the two exceptions recorded below; the development contains no `sorry`, and the ring $\mathbb{Z}[\omega]$ is Mathlib's `Zsqrtd (-2)`, which supplies the commutative ring structure, decidable equality, and the multiplicativity of the norm. Repository reference to be added at submission.

The results of Sections 3–7 are checked by Lean's kernel and depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`; several of them (Proposition 5.1, the identities of Proposition 6.3, and Theorem 7.2 (i)–(ii)) depend on fewer. In particular Theorem 6.1 carries no computation at all, and every finite search behind Theorems 4.1 and 7.2 and Propositions 5.1, 6.6 and 7.3 is executed by the kernel rather than by compiled code: the completeness of each of the four square lists ($m=2,4,8,16$, that is 4, 16, 64 and 256 cases), the residue searches at $m=2,4,8,16$ in the neighbour-list form of Remark 3.4, the 256 residue pairs behind the second obstruction half of Proposition 5.1, the 64 residue triples behind Proposition 7.1, and the $14\times 256=3584$ cases behind Theorem 7.2 (iii). Two steps are not themselves machine-checked. Corollary 6.2 translates the congruence formulation of Theorem 6.1 into Definition 3.2, and that translation — one application of Lemma 3.1 — was carried out by hand. And, as Section 3 says, the square lists at $m=8$ and $m=16$ are certified complete but not exact, so the two negative outcomes recorded at those moduli are statements about the search as run; no positive statement of the paper depends on them.

Section 8 is where compiled evaluation is used. The two searches of Proposition 8.3, six Boolean values in all, together with the two control evaluations of Proposition 8.5 (iii) — the 4-clique at $z=1$ inside $\square_{15}$, and the non-empty extension filter over $\square_{400}$ — are delegated to Lean's `native_decide`; the bridges from those Booleans to statements about elements of $\mathbb{Z}[\omega]$ are kernel-checked separately, so the delegation is confined to the evaluation of an explicit Boolean function on an explicit finite list. Everything else in that section — the parametrized quadruple of Proposition 8.1, the arithmetic of Proposition 8.2, and items (i), (ii) and (iv) of Proposition 8.5 — is kernel-checked.

The computations reported in Remarks 6.7, 7.4 and 8.4 are outside the formal development; they were run in C and Python and are recorded here as motivation and as evidence about the sharpness of the hypotheses, not as verified claims. Every numerical value quoted from [11] was reproduced from

that paper's own definitions before being used, including the quadruple of Proposition 8.1 at sample values of $s$, the norm and factorizations of Proposition 8.2, and the square set $\mathcal{S}_4$.

## References


[1] F. S. Abu Muriefah and A. Al-Rashed, *Some Diophantine quadruples in the ring* $\mathbb{Z}[\sqrt{-2}]$, Math. Commun. **9** (2004), 1–8.

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

[3] M. Cipu and Y. Fujita, *On the length of* $D(\pm 1)$*-tuples in imaginary quadratic rings*, Bull. Lond. Math. Soc. **56** (2024), 274–287.

[4] A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III **32** (1997), 1–10.

[5] A. Dujella, *Diophantine m-tuples and elliptic curves*, Developments in Mathematics, Springer, Cham, 2024.

[6] A. Dujella, *Diophantine m-tuples page*, `https://web.math.pmf.unizg.hr/~duje/dtuples.html`, accessed 28 August 2026.

[7] A. Dujella, *Open problems on Diophantine m-tuples and elliptic curves*, version of 24 August 2026, `https://web.math.pmf.unizg.hr/~duje/pdf/open2.pdf`.

[8] A. Dujella and Z. Franušić, *On differences of two squares in some quadratic fields*, Rocky Mountain J. Math. **37** (2007), 429–453.

[9] A. Dujella, M. Jukić Bokun and I. Soldo, *A Pellian equation with primes and applications to* $D(-1)$*-quadruples*, Bull. Malays. Math. Sci. Soc. **42** (2019), 2915–2926; arXiv:1706.01959.

[10] A. Dujella and I. Soldo, *Diophantine quadruples in* $\mathbb{Z}[\sqrt{-2}]$, An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. **18** (2010), 81–98.

[11] A. Dujella and I. Soldo, *Infinite families of Diophantine quadruples in* $\mathbb{Z}[\sqrt{-2}]$ *in the remaining exceptional congruence classes*, arXiv:2607.07838v1 (2026). All theorem, proposition, section and table numbers cited here are those of v1.

[12] Z. Franušić, *Diophantine quadruples in the ring* $\mathbb{Z}[\sqrt{2}]$, Math. Commun. **9** (2004), 141–148.

[13] M. Jukić Bokun and I. Soldo, *Extensions of* $D(-1)$*-pairs in some imaginary quadratic fields*, New York J. Math. **30** (2024), 745–755.

[14] I. Soldo, *On the existence of Diophantine quadruples in* $\mathbb{Z}[\sqrt{-2}]$, Miskolc Math. Notes **14** (2013), 265–277.

[15] I. Soldo, *On the extensibility of* $D(-1)$*-triples* $\{1, b, c\}$ *in the ring* $\mathbb{Z}[\sqrt{-t}]$*,* $t > 0$, Studia Sci. Math. Hungar. **50** (2013), 296–330.

[16] I. Soldo, $D(-1)$*-triples of the form* $\{1, b, c\}$ *in the ring* $\mathbb{Z}[\sqrt{-t}]$*,* $t > 0$, Bull. Malays. Math. Sci. Soc. **39** (2016), 1201–1224.

[17] 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.