Regularity of Diophantine quadruples over $\mathbb{Q}(i)[X]$: an AI-assisted proof approach

Modular Curves and Applications of AI to Number Theory
Opatija, 2026

Sanda Bujačić Babić

Joint work with Ana Jurasić

Faculty of Mathematics, University of Rijeka

This work is supported by the Croatian Science Foundation under the project number HRZZ IP-2022-10-5008 and by the European Union-NextGeneration EU under the project number uniri-iz-25-62-ALGEBRA.

Definition

A set $\{a, b, c, d\}$ of four distinct nonzero polynomials in $\mathbb{Q}(i)[X]$ is a Diophantine quadruple if the product of any two distinct elements, increased by 1, is a square in $\mathbb{Q}(i)[X]$.

Thus, we write

$$ab+1 = r^2, \quad ac+1 = s^2, \quad bc+1 = t^2, \quad ad+1 = x^2, \quad bd+1 = y^2, \quad cd+1 = z^2, \quad (1)$$

for some $r, s, t, x, y, z \in \mathbb{Q}(i)[X]$.

- We assume that at most one polynomial of the Diophantine quadruple is constant.

A Diophantine quadruple $\{a, b, c, d\}$ is regular if $d = d_{\pm} = a + b + c + 2abc \pm 2rst$ or, equivalently,

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

Is every Diophantine quadruple over $\mathbb{Q}(i)[X]$ **regular**?

Every Diophantine quadruple is regular in:

Ring	Authors
$\mathbb{Z}[X]$	Dujella–Fuchs
$\mathbb{Z}[i][X]$	Filipin–Jurasić
$\mathbb{R}[X]$	Filipin–Jurasić

Irregular quadruples exist in $\mathbb{C}[X]$ (Dujella–Jurasić).

Theorem (B.B. & J.)

Every Diophantine quadruple in $\mathbb{Q}(i)[X]$ *is regular.*

Consequently, we answer the question whether every $D(4)$ quadruple in $\mathbb{Q}(i)[X]$ is regular.

All statements concern quadruples that contain at most one constant polynomial.

The Common Strategy

Common strategy is to

- find the system of simultaneous Pellian equations,
- find the intersection of the binary recurrent sequences,
- apply congruence relations and the gap principle.

We deal with the system of two Pellian equations

$$az^2 - cx^2 = a - c,$$
$$bz^2 - cy^2 = b - c$$

obtained by eliminating d from (1).

The Pellian equations lead to recurrence sequences $(v_m)_{m\geq 0}$ and $(w_n)_{n\geq 0}$

$$v_0 = z_0, \qquad v_1 = sz_0 + cx_0, \qquad v_{m+2} = 2sv_{m+1} - v_m,$$
$$w_0 = z_1, \qquad w_1 = tz_1 + cy_1, \qquad w_{n+2} = 2tw_{n+1} - w_n.$$

We determine a common term z of the two recurrence sequences:

$$z = v_m = w_n \text{ and get the extension } d = \frac{z^2 - 1}{c}.$$

Relations between degrees of polynomials

We introduce $\alpha = \deg a$, $\beta = \deg b$, $\gamma = \deg c$, with

$$0 \le \alpha \le \beta \le \gamma.$$

For $m, n \ge 1$,

$$\deg v_m = (m-1)\frac{\alpha+\gamma}{2} + \deg v_1,$$
$$\deg w_n = (n-1)\frac{\beta+\gamma}{2} + \deg w_1.$$

Let d_- denote the regular extension of a smaller degree. We prove

$$d_- = 0 \quad \text{or} \quad \deg d_- = \gamma - \alpha - \beta.$$

For all $m, n \geq 0$, we have

$$\begin{aligned} v_{2m} &\equiv z_0 && \pmod{c}, \\ v_{2m+1} &\equiv v_1 \equiv sz_0 && \pmod{c}, \\ w_{2n} &\equiv z_1 && \pmod{c}, \\ w_{2n+1} &\equiv w_1 \equiv tz_1 && \pmod{c}. \end{aligned}$$

Moreover

$$\begin{aligned} v_{2m} &\equiv z_0 + 2c\big(az_0m^2 + sx_0m\big) && \pmod{c^2}, \\ v_{2m+1} &\equiv sz_0 + c\big(2asz_0m(m+1) + x_0(2m+1)\big) && \pmod{c^2}, \\ w_{2n} &\equiv z_1 + 2c\big(bz_1n^2 + ty_1n\big) && \pmod{c^2}, \\ w_{2n+1} &\equiv tz_1 + c\big(2btz_1n(n+1) + y_1(2n+1)\big) && \pmod{c^2}. \end{aligned}$$

Possible initial terms

- We introduce a lemma that lists all possible initial terms and the necessary degree conditions.
- These are necessary conditions; not every listed case must occur.
- We examine all the cases, reducing some to others by changes of signs and shifts of indices, and show that **none yields an irregular quadruple**.

Possible initial terms

Lemma. If $v_m = w_n$ for some $m, n \geq 0$, then the initial terms z_0, z_1 and the degrees α, β, γ satisfy one of the following according to the parities of m and n.

1. $v_{2m} = w_{2n}$

(a) $z_0 = z_1 = \pm 1$;

(b) $z_0 = z_1 = \pm s, \quad \alpha = 0$;

(c) $z_0 = z_1 = \pm cr \pm st, \quad \alpha > 0,$
$\alpha + \beta \leq \gamma \leq 2\alpha + \beta.$

3. $v_{2m} = w_{2n+1}$

(a) $(z_0, z_1) = (\pm t, \pm 1),$
$\gamma \geq \alpha + 2\beta;$

(b) $(z_0, z_1) = (\pm s, \pm 1),$
$\alpha = 0, \quad \beta = \gamma;$

(c) $(z_0, z_1) = (\pm 1, \pm 1),$
$\alpha = 0, \quad \beta = \gamma;$

(d) $(z_0, z_1) = (\pm cr \pm st, \pm s),$
$\alpha \geq 0, \quad 2\alpha + \beta \leq \gamma \leq \alpha + 2\beta.$

Special case of 3(d): $(z_0, z_1) = (\pm s, \pm s)$, $\alpha = 0$, $\beta = \gamma$.

2. $v_{2m+1} = w_{2n}$

(a) $(z_0, z_1) = (\pm 1, \pm s), \ \gamma \geq 2\alpha + \beta;$

(b) $(z_0, z_1) = (\pm s, \pm 1), \ \alpha = 0, \ \beta \leq \gamma;$

(c) $(z_0, z_1) = (\pm t, \pm cr \pm st),$
$\alpha = \beta, \quad \gamma = 3\alpha.$

4. $v_{2m+1} = w_{2n+1}$

(a) $(z_0, z_1) = (\pm 1, \pm cr \pm st),$
$\gamma \leq 2\alpha + \beta;$

(b) $(z_0, z_1) = (\pm cr \pm st, \pm 1),$
$\gamma \leq \alpha + 2\beta;$

(c) $(z_0, z_1) = (\pm t, \pm s), \ \gamma \geq \alpha + 2\beta.$

Special cases of 4(a):

$(z_0, z_1) = (\pm 1, \pm 1), \quad \alpha \leq \beta = \gamma;$
$(z_0, z_1) = (\pm 1, \pm s), \quad \alpha = 0, \ \beta = \gamma.$

Special cases of 4(b):

$(z_0, z_1) = (\pm 1, \pm 1), \quad \alpha \leq \beta = \gamma;$
$(z_0, z_1) = (\pm s, \pm 1), \quad \alpha = 0, \ \beta = \gamma.$

Excluding irregular extensions

The proof of the main theorem combines:

- congruences modulo c and c^2;
- degree bounds for the initial terms and d_-;
- comparison of degrees and leading coefficients in $v_m = w_n$;
- comparison of coefficients in the resulting polynomial identities;
- coprimality and divisibility in $\mathbb{Q}(i)[X]$;
- integrality of the indices and square conditions in $\mathbb{Q}(i)$.

The direct application of these tools did not yield a contradiction in certain subcases of 2(a) and 4(a), where

$$\deg b = \deg s = \beta$$

allows cancellation of the leading terms.

Case 2(a): $v_{2m+1} = w_{2n},\ (z_0, z_1) = (\delta, \delta s),\ \delta \in \{\pm 1\}$

In the remaining subcase of 2(a), we have

$$\gamma = 2\beta - \alpha, \qquad \beta \geq 3\alpha > 0, \qquad \deg d_- = \beta - 2\alpha.$$

We consider the sign choice for which

$$d_- = a + b + c + 2abc - 2\delta rst.$$

ChatGPT 5.6 Sol proposed to set $M = m(m+1)$ and $K = 2m+1$. The recurrence congruences yield

$$2\delta aM + sK = 2\delta bn^2 + \delta n(a + b - d_-),$$
$$2\delta asM + K \equiv 2\delta bsn^2 + 2trn \pmod{c}.$$

The first congruence is an identity since all terms have degree less than γ.

The AI-suggested construction

Rearranging the first identity gives

$$L_1 := n(2n+1)b + an - nd_- - 2aM = \delta sK.$$

Hence $s \mid L_1$.
For the second congruence, put

$$D = 2\delta asM + K - 2\delta bsn^2 - 2trn, \qquad c \mid D.$$

Using $s^2 = ac + 1$ and the first identity gives

$$sD = c\delta Q_1, \qquad Q_1 := 2a^2M - 2an(n+1)b - n.$$

Writing $D = cE$, we obtain $sE = \delta Q_1$, hence $s \mid Q_1$.

Combine L_1 and Q_1 to eliminate the terms involving b.

Cancellation and contradiction

Since $s \mid L_1$ and $s \mid Q_1$, we have

$$s \mid R_1 := (2n+1)Q_1 + 2a(n+1)L_1.$$

The terms involving b cancel.

Now $s \mid R_1$ forces $R_1 = 0$, since every term has degree less than $\deg s = \beta$. Consequently,

$$2a\Big(a\big(n(n+1) - M\big) - n(n+1)d_-\Big) = n(2n+1).$$

$$a \mid n(2n+1), \qquad \deg a > 0, \qquad n \geq 1: \quad \text{a contradiction.}$$

The other sign choice admits an analogous cancellation.

Thank you for your attention!