RAD HRVATSKE AKADEMIJE ZNANOSTI I UMJETNOSTI
MATEMATIČKE ZNANOSTI

A. Jurasić

Four squares from three real polynomials

Manuscript accepted for publication

This is a preliminary PDF of the author-produced manuscript that has been peer-reviewed and accepted for publication. It has not been copy-edited, proofread, or finalized by Rad HAZU Production staff.

FOUR SQUARES FROM THREE REAL POLYNOMIALS

ANA JURASIĆ

ABSTRACT. We construct three nonconstant polynomials $a, b, c \in \mathbb{R}[X]$ such that

$$ab + 1, \qquad ac + 1, \qquad bc + 1, \qquad abc + 1$$

are all squares in $\mathbb{R}[X]$. The entries in the construction are quadratic, so the construction has the smallest possible positive degrees. By composition with nonconstant polynomials, this gives infinitely many examples over $\mathbb{R}[X]$ with all entries nonconstant.

1. INTRODUCTION

A Diophantine m-tuple is classically a set of m distinct positive integers for which the product of any two distinct elements, increased by 1, is a square. Polynomial analogues and $D(n)$-variants have a substantial literature. Early polynomial versions were studied by Jones [8]. Foundational work on polynomial variants includes [2, 3, 4, 5, 6, 9], and a recent general reference is [1]. The present note concerns a related, but stronger, condition for triples: besides requiring the three pairwise products plus 1 to be squares, we also require the product of all three entries plus 1 to be a square.

DEFINITION 1.1. *A set $\{a, b, c\} \subset \mathbb{R}[X]$ of three nonzero polynomials is called a* four-square polynomial triple *if there exist $r, s, t, u \in \mathbb{R}[X]$, such that*

$$ab + 1 = r^2, \qquad ac + 1 = s^2, \qquad bc + 1 = t^2, \qquad abc + 1 = u^2. \tag{1.1}$$

The corresponding problem for positive integers asks for $a, b, c > 1$ satisfying the four square conditions in (1.1). Dujella and Szalay [7] proved that there are infinitely many such triples of positive integers. Their construction lies inside regular Diophantine triples.

2020 *Mathematics Subject Classification.* 11D09,11C08.

Key words and phrases. Diophantine m-tuples, polynomial Diophantine tuples, squares in polynomial rings.

If we were to allow $a = 0$ in Definition 1.1, the four conditions in (1.1) would reduce to the single condition that $bc+1$ is a square. If one entry equals 1, say $a = 1$, then the four conditions reduce to the three distinct conditions that $b+1$, $c+1$, and $bc+1$ are squares. For example, for every integer $k \geq 2$, the set $\{1, k^2-1, (k+1)^2-1\}$ satisfies the four-square conditions in (1.1). Moreover, for every nonconstant $k \in \mathbb{Z}[X]$, the same formula gives a four-square polynomial triple in the sense of Definition 1.1. Therefore, as we explain in Section 2, the natural polynomial question is whether all three entries can be distinct nonconstant polynomials. We answer this question affirmatively over $\mathbb{R}[X]$: we construct three distinct quadratic polynomials satisfying (1.1).

2. Elementary restrictions

As in the classical case, it is natural to assume that at least one element of a four-square polynomial triple is nonconstant. Also, analogously as in classical case, we cannot have two equal polynomials in such a set. In this section we record the other three simple restrictions. The first concerns the possible constant entries in a four-square polynomial triple having at least one nonconstant entry. Although Definition 1.1 requires all three entries to be nonzero, in the following auxiliary lemma we consider arbitrary polynomial solutions of the four equations in (1.1), allowing zero entries.

Lemma 2.1. *Let $a, b, c \in \mathbb{R}[X]$ satisfy the equations in* (1.1)*, without assuming that a, b, c are nonzero. Suppose that one entry, say a, belongs to $\mathbb{R} \setminus \{0, 1\}$. Then, if b and c are both nonzero, they are both constant; if one of b and c is nonconstant, the other one is equal to zero.*

In particular, if $\{a, b, c\}$ is a four-square polynomial triple in the sense of Definition 1.1, then all three entries are constant.

Proof. From $bc + 1 = t^2$ and $abc + 1 = u^2$, we obtain

$$u^2 - at^2 = 1 - a.$$

Since $a \notin \{0, 1\}$,

$$(u - t\sqrt{a})(u + t\sqrt{a}) = 1 - a$$

is a factorization of a nonzero constant in $\mathbb{C}[X]$. Thus both factors are units in $\mathbb{C}[X]$, hence constants. Therefore u and t are constant, so $bc = t^2 - 1$ is constant.

If b and c are both nonzero, then bc is a nonzero constant, so b and c are constants. If one of b and c is nonconstant, then $bc \in \mathbb{R}$ forces the other one to be equal to zero. Finally, in a four-square polynomial triple all entries are nonzero by Definition 1.1, so in that case b and c must both be constant. $\square$

The constants 0 and 1 are exceptional at the level of the equations in *(1.1)*. For any $k \in \mathbb{R}[X]$,

$$\{0,\ k^2-1,\ (k+1)^2-1\} \text{ and } \{1,\ k^2-1,\ (k+1)^2-1\}$$

satisfy the four equations in (1.1), since

$$(k^2-1)((k+1)^2-1)+1=(k^2+k-1)^2.$$

The first choice is not a four-square polynomial triple in the sense of Definition 1.1, because it contains a zero entry. If k is nonconstant, then the second choice is a four-square polynomial triple. Thus, by Lemma 2.1, in a four-square polynomial triple having at least one nonconstant entry, the only possible constant entry is 1.

LEMMA 2.2. *Let $\{a,b,c\} \subset \mathbb{R}[X]$ be a four-square polynomial triple whose three entries are nonconstant. Then $\deg a$, $\deg b$, and $\deg c$ are all even. Moreover, the leading coefficients of a,b,c are positive real numbers.*

PROOF. Since $ab+1$, $ac+1$, and $bc+1$ are nonconstant squares,

$$\deg a+\deg b \equiv \deg a+\deg c \equiv \deg b+\deg c \equiv 0 \pmod 2.$$

Thus, all three degrees have the same parity. Since $abc+1$ is also a nonconstant square, $\deg a+\deg b+\deg c$ is even. The common parity is therefore even.

Let A,B,C be the leading coefficients of a,b,c, respectively. The leading coefficients of $ab+1$, $ac+1$, $bc+1$, and $abc+1$ must be positive. Hence, $AB>0$, $AC>0$, $BC>0$, and $ABC>0$. It follows that A,B,C are all positive. □

We also note why the equation used by Dujella and Szalay [7] in their integer construction,

$$x^2-4xy+y^2=1 \tag{2.1}$$

does not immediately yield a polynomial construction. The direct polynomial analogue of this equation has no nonconstant solutions.

LEMMA 2.3. *If $x,y \in \mathbb{R}[X]$ satisfy* (2.1)*, then x and y are constant.*

PROOF. From (2.1), we have

$$\big(x-(2+\sqrt{3})y\big)\big(x-(2-\sqrt{3})y\big)=1.$$

Both factors are units in $\mathbb{R}[X]$, so they are constant. Solving the resulting two linear equations gives that x and y are constant. □

3. A minimal-degree construction

We first establish a simple criterion that will be used in the construction.

Lemma 3.1. *Let $u, v, D \in \mathbb{R}$ with $u \neq v$, and let $D > 0$. Then*

$$1 + D(Y - u)(Y - v)$$

is a square of a linear polynomial in Y if and only if

$$D = \frac{4}{(v-u)^2}.$$

For this value of D,

$$1 + \frac{4(Y-u)(Y-v)}{(v-u)^2} = \left(\frac{2Y - u - v}{v - u}\right)^2. \tag{3.1}$$

Proof. The discriminant of the polynomial

$$D(Y-u)(Y-v) + 1 = DY^2 - D(u+v)Y + Duv + 1$$

is

$$D^2(u+v)^2 - 4D(Duv+1) = D\big(D(u-v)^2 - 4\big).$$

Since $D > 0$, this discriminant vanishes exactly when $D = 4/(u-v)^2$. The identity (3.1) follows by substitution. □

We now give the construction. Let $Y = X^2$ and look for polynomials from $\mathbb{R}[X]$ of the form

$$a = A(X^2 - \alpha), \qquad b = B(X^2 - \beta), \qquad c = C(X^2 - \gamma), \tag{3.2}$$

where $A, B, C \neq 0$ and α, β, γ are distinct. The idea is to choose the parameters so that the first three square conditions in *(1.1)* hold automatically, while the fourth condition reduces to a square. Since $Y = X^2$, we have

$$\begin{aligned} ab + 1 &= 1 + AB(Y-\alpha)(Y-\beta), \\ ac + 1 &= 1 + AC(Y-\alpha)(Y-\gamma), \\ bc + 1 &= 1 + BC(Y-\beta)(Y-\gamma). \end{aligned}$$

We now apply Lemma 3.1 to these three expressions. Thus, the first three square conditions are satisfied if we impose

$$AB = \frac{4}{(\beta-\alpha)^2}, \qquad AC = \frac{4}{(\gamma-\alpha)^2}, \qquad BC = \frac{4}{(\gamma-\beta)^2}. \tag{3.3}$$

A convenient compatible choice is

$$A = \frac{2(\gamma-\beta)}{(\beta-\alpha)(\gamma-\alpha)}, \qquad B = \frac{2(\gamma-\alpha)}{(\beta-\alpha)(\gamma-\beta)}, \qquad C = \frac{2(\beta-\alpha)}{(\gamma-\alpha)(\gamma-\beta)}. \tag{3.4}$$

Set

$$\Delta = (\beta-\alpha)(\gamma-\alpha)(\gamma-\beta). \tag{3.5}$$

Then, equations in (3.4) also give

$$ABC = \frac{8}{\Delta}. \tag{3.6}$$

The only remaining condition is the fourth square condition $abc + 1 \in \mathbb{R}[X]^2$.

By (3.6),

$$abc + 1 = \frac{8}{\Delta}(Y - \alpha)(Y - \beta)(Y - \gamma) + 1. \tag{3.7}$$

We now choose α, β, γ so that

$$(Y - \alpha)(Y - \beta)(Y - \gamma) = Y(Y - 1)^2 - d, \tag{3.8}$$

for some nonzero constant d. Indeed, after a substitution $Y = X^2$,

$$Y(Y-1)^2 = X^2(X^2-1)^2 = \big(X(X^2-1)\big)^2$$

is already a square in $\mathbb{R}[X]$. Substituting (3.8) into (3.7), and taking

$$\Delta = 8d, \tag{3.9}$$

gives

$$abc + 1 = \frac{8}{\Delta}\big(Y(Y-1)^2 - d\big) + 1 = \frac{8}{\Delta}Y(Y-1)^2. \tag{3.10}$$

The problem is now reduced to finding a cubic polynomial

$$f(Y) = Y^3 - 2Y^2 + Y - d, \tag{3.11}$$

whose roots α, β, γ satisfy (3.9). The discriminant of the polynomial (3.11) is

$$\operatorname{disc}(f) = d(4 - 27d). \tag{3.12}$$

On the other hand, since f is monic, $\operatorname{disc}(f) = \Delta^2$. Hence, by (3.9) and (3.12), we get $d(4 - 27d) = 64d^2$. Since $d \neq 0$ by assumption, this yields $d = \frac{4}{91}$. In (3.11), now we have

$$f(Y) = Y^3 - 2Y^2 + Y - \frac{4}{91}. \tag{3.13}$$

The discriminant of f is

$$\operatorname{disc}(f) = \frac{1024}{8281} = \left(\frac{32}{91}\right)^2 > 0,$$

so f has three distinct real roots. Label them so that

$$\alpha < \beta < \gamma.$$

Then $\Delta > 0$ by (3.5). Since $\Delta^2 = \operatorname{disc}(f) = \left(\frac{32}{91}\right)^2$, we obtain

$$\Delta = \frac{32}{91} = 8d. \tag{3.14}$$

THEOREM 3.2. *The polynomials a, b, c defined by (3.2) form a four-square polynomial triple in $\mathbb{R}[X]$. More precisely,*

$$ab + 1 = \left(\frac{2X^2 - \alpha - \beta}{\beta - \alpha} \right)^2, \tag{3.15}$$

$$ac + 1 = \left(\frac{2X^2 - \alpha - \gamma}{\gamma - \alpha} \right)^2, \tag{3.16}$$

$$bc + 1 = \left(\frac{2X^2 - \beta - \gamma}{\gamma - \beta} \right)^2, \tag{3.17}$$

$$abc + 1 = \left(\frac{\sqrt{91}}{2} X(X^2 - 1) \right)^2. \tag{3.18}$$

In particular, a, b, c are different nonconstant polynomials. Their degrees are minimal among all four-square polynomial triples over $\mathbb{R}[X]$ with nonconstant entries.

PROOF. The numbers A, B, C are positive because $\alpha < \beta < \gamma$, and therefore a, b, c are nonconstant polynomials in $\mathbb{R}[X]$. They are pairwise distinct: if, for example, $A(X^2 - \alpha) = B(X^2 - \beta)$, then comparison of coefficients gives $A = B$ and $\alpha = \beta$, a contradiction. The identities (3.15), (3.16), and (3.17) follow from Lemma 3.1, equivalently from (3.1) and (3.3), after substituting $Y = X^2$. The equation (3.18) follows from (3.10) and (3.14). The last assertion follows from Lemma 2.2: in any example with all entries nonconstant, all three degrees are positive even integers, hence at least 2. □

REMARK 3.3. For reference, the roots of the polynomial (3.13) are

$$\alpha \approx 0.0485571496, \qquad \beta \approx 0.7594142315, \qquad \gamma \approx 1.1920286189.$$

The corresponding leading coefficients of the polynomials a, b and c are

$$A \approx 1.0644452464, \qquad B \approx 7.4365598181, \qquad C \approx 2.8739949355.$$

The exact form of the triple $\{a, b, c\}$ is the root-based one in (3.2).

4. INFINITELY MANY EXAMPLES

Now, it is easy to generate infinitely many four-square polynomial triples.

PROPOSITION 4.1. *Let $\{a, b, c\} \subset \mathbb{R}[X]$ be a four-square polynomial triple whose three entries are nonconstant. If $h \in \mathbb{R}[X]$ is nonconstant, then*

$$\{a \circ h,\ b \circ h,\ c \circ h\}$$

is again a four-square polynomial triple with three nonconstant entries.

PROOF. Substituting $X \mapsto h(X)$ in (1.1) gives

$$a(h)b(h)+1=r(h)^2, \qquad a(h)c(h)+1=s(h)^2,$$
$$b(h)c(h)+1=t(h)^2, \qquad a(h)b(h)c(h)+1=u(h)^2.$$

A composition of two nonconstant polynomials is nonconstant, so the three entries remain nonconstant. The substitution homomorphism $p(X) \mapsto p(h(X))$ is injective, because h is nonconstant. Hence, distinct entries remain distinct. $\square$

COROLLARY 4.2. *There are infinitely many four-square polynomial triples in $\mathbb{R}[X]$ with all entries nonconstant.*

PROOF. Apply Proposition 4.1 to the triple from Theorem 3.2, with $h_m(X) = X^m$, $m = 1, 2, 3, \ldots$. The degree of polynomials in the resulting triple is $2m$, so these triples are distinct for infinitely many m. $\square$

5. Final remarks

We described a construction over $\mathbb{R}[X]$. The present construction does not yield a solution over $\mathbb{Z}[X]$ or $\mathbb{Q}[X]$, because the coefficients in (3.2) are defined from the real roots of the cubic polynomial (3.13). Moreover, no evident coefficient rescaling preserves equations of the form “product plus 1 is a square”. Determining whether an analogue with all entries nonconstant exists over $\mathbb{Q}[X]$ or $\mathbb{Z}[X]$ remains a separate arithmetic question.

ACKNOWLEDGEMENTS.

This work was supported by the Croatian Science Foundation Grant No. IP-2022-10-5008. A. J. was also supported by the European Union – NextGenerationEU, project number uniri-iz-25-62-ALGEBRA. During the exploratory phase of this research, the author utilized GPT-5.5 Pro to investigate examples and candidate constructions. All mathematical results were independently verified by the author, who takes full responsibility for the mathematical correctness of these results.

References

[1] A. Dujella, *Diophantine m-tuples and elliptic curves*, Developments in Mathematics, vol. 79, Springer, Cham, 2024.

[2] A. Dujella and C. Fuchs, *Complete solution of the polynomial version of a problem of Diophantus*, *J. Number Theory* **106** (2004), 326–344.

[3] A. Dujella, C. Fuchs and R. F. Tichy, *Diophantine m-tuples for linear polynomials*, *Period. Math. Hungar.* **45** (2002), 21–33.

[4] A. Dujella, C. Fuchs and G. Walsh, *Diophantine m-tuples for linear polynomials. II. Equal degrees*, *J. Number Theory* **120** (2006), 213–228.

[5] A. Dujella and A. Jurasić, *On the size of sets in a polynomial variant of a problem of Diophantus*, *Int. J. Number Theory* **6** (2010), 1449–1471.

[6] A. Dujella and A. Jurasić, *Some Diophantine triples and quadruples for quadratic polynomials*, *J. Comb. Number Theory* **3** (2011), no. 2, 123–141.
[7] A. Dujella and L. Szalay, *Four squares from three numbers*, preprint, arXiv:2506.14013, 2025.
[8] B. W. Jones, *A variation on a problem of Davenport and Diophantus*, *Quart. J. Math. Oxford Ser. (2)* **27** (1976), 349–353.
[9] A. Jurasić, *Diophantine m-tuples for quadratic polynomials*, *Glas. Mat. Ser. III* **46** (2011), no. 2, 283–309.

Četiri potpuna kvadrata dobivena od triju realnih polinoma

Ana Jurasić

Sažetak. U radu je prikazana konstrukcija triju nekonstantnih polinoma $a, b, c \in \mathbb{R}[X]$ takvih da su

$$ab + 1, \qquad ac + 1, \qquad bc + 1, \qquad abc + 1$$

potpuni kvadrati u prstenu $\mathbb{R}[X]$. Polinomi u konstrukciji drugog su stupnja, što je najmanji mogući pozitivni stupanj. Komponiranjem s nekonstantnim polinomima dobiva se beskonačno mnogo takvih primjera u $\mathbb{R}[X]$, pri čemu su svi uključeni polinomi nekonstantni.

Ana Jurasić
Faculty of Mathematics
University of Rijeka
Radmile Matejčić 2
51000 Rijeka
Croatia
E-mail: `ajurasic@math.uniri.hr`