J. Pure Appl. Algebra 216 (1) (2012) 184-191

Polynomial parametrization of Pythagorean quadruples, quintuples and sextuples.

Sophie Frisch (TU Graz) and Leonid Vaserstein (PSU)

Abstract. For $n = 4$ or 6, the Pythagorean n-tuples admit a parametrization by a single n-tuple of polynomials with integer coefficients (which is impossible for $n = 3$). For $n = 5$, there is an integer-valued polynomial Pythagorean 5-tuple which parametrizes Pythagorean 5-tuples (similar to the case $n = 3$). Pythagorean quadruples are closely related to (integer) Descartes quadruples, which we also parametrize by a Descartes quadruple of polynomials with integer coefficients.

Introduction

A Pythagorean triple is a triple of integers (x_1, x_2, x_3) satisfying $x_1^2 + x_2^2 = x_3^2$. More generally, for any integer $n \geq 3$, and any commutative ring A, a Pythagorean n-tuple over A is an n-tuple $(x_1, \dots, x_n) \in A^n$ such that

$$x_1^2 + \cdots + x_{n-1}^2 = x_n^2. \tag{1}$$

Whenever A is not specified, we will understand $A = \mathbb{Z}$. Likewise, "polynomial Pythagorean n-tuple" means a Pythagorean n-tuple over a ring of polynomials in finitely many indeterminates with coefficients in $\mathbb{Z}$.

Instead of studying (1) directly, it is often convenient to substitute $u = x_n + x_{n-1}$, $v = x_n - x_{n-1}$, and to consider the equation

$$x_1^2 + \cdots + x_{n-2}^2 = uv. \tag{2}$$

Over any ring A in which 2 is not a zero-divisor, this substitution and the reverse substitution

$$x_{n-1} = (u - v)/2, \qquad x_n = (u + v)/2, \tag{3}$$

establish a bijection between solutions $(x_1, \dots, x_n) \in A^n$ of (1) and solutions $(x_1, \dots, x_{n-2}, u, v) \in A^n$ with $u - v \in 2A$ of (2).

We recall the existing polynomial parametrizations of integer Pythagorean triples. It is well known that up to permutation of x_1 and x_2, every Pythagorean triple has the form

$$(x_1, x_2, x_3) = y_0(2y_1y_2, y_1^2 - y_2^2, y_1^2 + y_2^2) \tag{4}$$

with $y_i \in \mathbb{Z}$. In other words, the set of integer Pythagorean triples is the union of $f_1(\mathbb{Z}^3)$ and $f_2(\mathbb{Z}^3)$ where

$$f_1(y_0, y_1, y_2) = y_0(2y_1y_2, y_1^2 - y_2^2, y_1^2 + y_2^2)$$

and

$$f_2(y_0, y_1, y_2) = y_0(y_1^2 - y_2^2, 2y_1y_2, y_1^2 + y_2^2)$$

are two Pythagorean triples over the polynomial ring $\mathbb{Z}[y_0, y_1, y_2]$. We say that all Pythagorean triples are covered by two polynomial Pythagorean triples (in 3 parameters each).

It is easy to see that the intersection of $f_1(\mathbb{Z}^3)$ and $f_2(\mathbb{Z}^3)$ contains only the zero triple. We know that it is not possible to cover all Pythagorean triples by any one Pythagorean triple over $\mathbb{Z}[y_1, \ldots, y_m]$ for any m [7]. It is, however, possible, to cover all integer Pythagorean triples by a single Pythagorean triple over the ring of integer-valued polynomials in 4 indeterminates [7]. An integer-valued polynomial is a polynomial with rational coefficients which takes integer values whenever the variables take integer values.

The primitive Pythagorean triples (x_1, x_2, x_3) with positive x_3, are, up to switching x_1 and x_2, given by (4) with primitive $(y_1, y_2) \in \mathbb{Z}^2$ such that $y_1 + y_2$ is odd. The set of such pairs (y_1, y_2) admits a polynomial parametrization [15]. Thus, all primitive Pythagorean triples can be covered by 4 polynomial triples (in 95 parameters each, see [15], Example 14).

All positive Pythagorean triples are, up to switching of x_1 and x_2, given by (4) with integers $y_1 > y_2 > 0$, $y_0 > 0$. The set of such pairs admits a polynomial parametrization using the fact that every positive integer can be written as a sum of 4 squares plus 1. Thus, the positive Pythagorean triples can be covered by 2 polynomial Pythagorean triples in 12 parameters.

It is unknown whether the set of positive primitive Pythagorean triples can be parametrized by a finite set of polynomial Pythagorean triples.

1. Quadruples

After the short discussion of Pythagorean triples in the introduction, we now address the case $n = 4$, in other words, Pythagorean quadruples.

Pythagorean quadruples were described by Carmichael [1], Chpt. II, §10, as follows: up to permutation of x_1, x_2, x_3, every Pythagorean quadruple has the form

$$\begin{aligned}&(x_1, x_2, x_3, x_4) = f(y_0, y_1, y_2, y_3, y_4) =\\ &y_0(2y_1y_3 + 2y_2y_4,\ 2y_1y_4 - 2y_2y_3,\ y_1^2 + y_2^2 - y_3^2 - y_4^2,\ y_1^2 + y_2^2 + y_3^2 + y_4^2)\end{aligned} \tag{5}$$

with integer values for the parameters $y_0, \ldots, y_4$. Thus, all Pythagorean quadruples are covered by 6 polynomial Pythagorean quadruples (in 5 parameters). Considering the position of the odd entry, it is easy to see that at least 3 permutations of x_1, x_2, x_3 are needed. If one examines Carmichael's proof, one sees that three polynomial quadruples suffice, namely (x_1, x_2, x_3, x_4), (x_1, x_3, x_2, x_4) and (x_3, x_2, x_1, x_4).

We now show that a single polynomial Pythagorean quadruple covers all Pythagorean quadruples. Our proof does not make use of Carmichael's result (but rather provides a shorter proof of Carmichael's result as a byproduct). Nor do we use unique factorization in the ring of Gaussian integers $\mathbb{Z}[i]$ (which could be used to give an alternative proof).

Definition. An n-tuple $w = (w_1, \ldots, w_n) \in A^n$ is called **unimodular** if $w_1A + \cdots + w_nA = A$. In the case when $A = \mathbb{Z}$ this means that $\gcd(w_1, \ldots, w_n) = 1$, i.e., w is primitive.

Proposition 1. *The integer solutions of*

$$x_1^2 + x_2^2 = uv \tag{6}$$

are parametrized by the polynomial quadruple

$$(x_1, x_2, u, v) = y_0(y_1y_3 + y_2y_4,\ y_1y_4 - y_2y_3,\ y_1^2 + y_2^2,\ y_3^2 + y_4^2) \tag{7}$$

as the parameters vary through the integers. Also, y_0 can be restricted to odd integers.

Proof. We represent the integer solutions of (6) as Hermitian matrices

$$w = \begin{pmatrix} u & x_1 + ix_2 \\ x_1 - ix_2 & v \end{pmatrix} = \begin{pmatrix} u & x \\ \bar{x} & v \end{pmatrix}$$

of determinant 0 over the Gaussian integers $\mathbb{Z}[i]$.

The group $GL(2, \mathbb{Z}[i])$ acts on the Hermitian matrices as follows

$$w \to g^* w g \tag{8}$$

where $g \in GL(2, \mathbb{Z}[i])$ and $*$ means transposition composed with entry-wise action of complex conjugation. In particular, for an elementary matrix $g = E_{12}(\lambda)$ with $\lambda = \lambda_1 + \lambda_2 i$

$$\begin{pmatrix} 1 & 0 \\ \bar{\lambda} & 1 \end{pmatrix} \begin{pmatrix} u & x \\ \bar{x} & v \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u & (x_1 + \lambda_1 u) + (x_2 + \lambda_2 u)i \\ (x_1 + \lambda_1 u) - (x_2 + \lambda_2 u)i & v + (\lambda_1^2 + \lambda_2^2)u + 2(\lambda_1 x_1 + \lambda_2 x_2) \end{pmatrix}$$

Setting either $\lambda_1 = 0$ or $\lambda_2 = 0$, we see that we can add an arbitrary integer multiple of u to x_2, leaving u and x_1 unchanged, and we can add an arbitrary multiple of u to x_1, leaving u and x_2 unchanged.

Given any solution with $u \neq 0$, we can, by applying elementary matrices g in $GL(2, \mathbb{Z}[i])$, make $|x_1|, |x_2| \leq |u|/2$, and hence $|v| \leq |u|/2$. Using the nontrivial permutation matrix in $GL(2, \mathbb{Z}[i])$, we can switch u and v.

Therefore, by an argument of descent, the orbit under $GL(2, \mathbb{Z}[i])$ of any unimodular solution $w = (x_1, x_2, u, v)$ to (6) contains a solution with $v = 0$ (and hence $x_1 = x_2 = 0$) and $u = 1$ or -1. So we get

$$w = \begin{pmatrix} u & x_1 + x_2 i \\ x_1 - x_2 i & v \end{pmatrix} = g^* \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} g = \begin{pmatrix} \bar{a} \\ \bar{b} \end{pmatrix} c(a, b) \tag{9}$$

with $c = \pm 1$, where (a, b) is the first row of the matrix $g \in GL(2, \mathbb{Z}[i])$.

So every integer solution of (6) has the form

$$w = \begin{pmatrix} u & x_1 + x_2 i \\ x_1 - x_2 i & v \end{pmatrix} = \begin{pmatrix} \bar{a} \\ \bar{b} \end{pmatrix} c(a, b)$$

with $a, b \in \mathbb{Z}[i]$, $c \in \mathbb{Z}$. Conversely, every expression of this form is a solution to (6) – it is not necessary to restrict (a, b) to be primitive or c to be ± 1 or (sum of 2 squares)-free.

Writing $c = y_0$, $a = y_1 + y_2 i$ and $b = y_3 + y_4 i$, with indeterminates y_k, we obtain a polynomial solution

$$(u, v, x_1, x_2) = y_0(y_1^2 + y_2^2,\ y_3^2 + y_4^2,\ y_1 y_3 + y_2 y_4,\ y_1 y_4 - y_2 y_3)$$

to (6) which covers all integer solutions. If we replace (a, b) above by $(1 + i)(a, b)$, the solution is multiplied by 2. We can, therefore, restrict y_0 to odd integers. □

Theorem 1. *Let*

$$f(y_0, y_1, y_2, y_3, y_4) = y_0(2y_1 y_3 + 2y_2 y_4,\ 2y_1 y_4 - 2y_2 y_3,\ y_1^2 + y_2^2 - y_3^2 - y_4^2,\ y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

The polynomial Pythagorean quadruple

$$g = f(y_0/2,\ y_1,\ y_2,\ y_3,\ y_1 + y_2 + y_3 + 2z) \in \mathbb{Z}[y_0, y_1, y_2, y_3, z]$$

in 5 parameters covers all Pythagorean quadruples, i.e., the range of the function $g\colon \mathbb{Z}^5 \to \mathbb{Z}^4$ *consists of all Pythagorean quadruples.*

Proof. Applying (3) to Proposition 1, we see that every Pythagorean quadruple has the form

$$(x_1, x_2, x_3, x_4) = y_0(y_1y_3 + y_2y_4,\ y_1y_4 - y_2y_3,\ (y_1^2 + y_2^2 - y_3^2 - y_4^2)/2,\ (y_1^2 + y_2^2 + y_3^2 + y_4^2)/2)$$

where $y_i \in \mathbb{Z}$ and $y_0(y_1+y_2+y_3+y_4)$ is even. Since y_0 can be chosen odd, we may assume that $y_1+y_2+y_3+y_4$ is even. Writing $y_4 = y_1 + y_2 + y_3 + 2z$, we prove Theorem 1. □

To get Carmichael's result, note that x_4 is odd for any primitive Pythagorean quadruple (x_1, x_2, x_3, x_4) and that exactly one of x_1, x_2, x_3 is also odd. So we can make $x_3 + x_4$ even by switching, if necessary, x_3 with x_1 or x_2. Then $\gcd(x_1, x_2, u, v) = 2$ for the corresponding solution (x_1, x_2, u, v) of (6). Going back from (7) with $y_0 = 2$ to the Pythagorean quadruple, we obtain Carmichael's formulas.

Notice that these formulas with $y_0 = 1$ and primitive (y_1, y_2, y_3, y_4) do not necessarily give primitive solutions. Our proof shows that the necessary and sufficient condition for primitivity is the primitivity of $(a, b) = (y_1 + y_2 i, y_3 + y_4 i)$. The set of primitive pairs of Gaussian integers admits a polynomial parametrization by methods of [15], but this is beyond the scope of the present paper.

2. Sextuples

We discuss Pythagorean sextuples before quintuples because we will use sextuples in the proof of the parametrization of Pythagorean quintuples by a single quintuple of integer-valued polynomials in the next section.

Dickson [4], Section 106, attempted to describe all Pythagorean sextuples, i.e., all integer solutions to

$$x_1^2 + \ldots + x_5^2 = x_6^2 \tag{10}$$

He observed that every integer solution of (10) gives rise to an integer solution of

$$x_1^2 + \ldots + x_4^2 = uv, \tag{11}$$

He solves the equation (11), in a lengthy proof of some 6 pages, but then fails to address the question of the reverse substitution: how to return to Pythagorean sextuples from integer solutions of (11).

We will also start by parametrizing the integer solutions of (11), giving a short proof using quaternions.

Definition. The algebra of **Lipschitz quaternions** is the $\mathbb{Z}$-algebra L generated by two symbols i and j subject to the defining relations $i^2 = -1$, $j^2 = -1$, and $ji = -ij$. We set $k = ij$.

We recall a few facts about the algebra of Lipschitz quaternions. L is a free $\mathbb{Z}$-module with basis $1, i, j, k$ and a free $\mathbb{Z}[i]$-module with basis $1, j$. L can be represented as an algebra of 4×4 integer matrices or as an algebra of 2×2 matrices over $\mathbb{Z}[i]$ by identifying $w = a + bi + cj + dk$ with

$$M_4(w) = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \quad \text{or} \quad M_2(w) = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

respectively.

An involution on L is given by the $\mathbb{Z}$-algebra anti-isomorphism

$$a + bi + cj + dk \mapsto (a + bi + cj + dk)^* = a - bi - cj - dk.$$

In the 4×4 integer matrix representation this corresponds to transposition; and in the 2×2 Gaussian integer matrix representation, to transposition followed by complex conjugation.

Definition. The **norm** of $w = a + bi + cj + dk \in L$ is defined as

$$(a^2 + b^2 + c^2 + d^2)^2 = \det(M_4(w)) = (\det M_2(w))^2$$

and the **reduced norm** as

$$a^2 + b^2 + c^2 + d^2 = w^* w = \det M_2(w).$$

For a 2×2 matrix M over L we define the norm of M as the determinant of the 8×8 integer matrix obtained by replacing each matrix entry w by $M_4(w)$, and the reduced norm as the determinant of the 4×4 matrix over $\mathbb{Z}[i]$ obtained by replacing each matrix entry w by $M_2(w)$.

Remark. If w is a Hermitian 2×2 matrix over L, its entries commute and we can calculate the determinant in a naïve way, as

$$\det \begin{pmatrix} u & x_1 + x_2 i + x_3 j + x_4 k \\ x_1 - x_2 i - x_3 j - x_4 k & v \end{pmatrix} = uv - x_1^2 - x_2^2 - x_3^2 - x_4^2.$$

The reduced norm of w as defined above is the square of this determinant.

Proposition 2. *A parametrization of all integer solutions* $(x_1, x_2, x_3, x_4, u, v)$ *of*

$$x_1^2 + \ldots + x_4^2 = uv$$

in 9 *parameters is given by*

$$\begin{aligned} x_1 &= y_0(y_1 y_5 + y_2 y_6 + y_3 y_7 + y_4 y_8) \\ x_2 &= y_0(-y_1 y_6 + y_2 y_5 + y_3 y_8 - y_4 y_7) \\ x_3 &= y_0(-y_1 y_7 - y_2 y_8 + y_3 y_5 + y_4 y_6) \\ x_4 &= y_0(-y_1 y_8 + y_2 y_7 - y_3 y_6 + y_4 y_5) \\ u &= y_0(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ v &= y_0(y_5^2 + y_6^2 + y_7^2 + y_8^2), \end{aligned}$$

as the parameters $y_0, \ldots, y_8$ *range through the integers. Here* y_0 *may be restricted to* ± 1.

Proof. We identify integer solutions $w = (x_1, x_2, x_3, x_4, u, v)$ of $x_1^2 + \ldots + x_4^2 = uv$ with 2×2 Hermitian matrices over the algebra of Lipschitz quaternions L

$$w = \begin{pmatrix} u & x_1 + x_2 i + x_3 j + x_4 k \\ x_1 - x_2 i - x_3 j - x_4 k & v \end{pmatrix}$$

of reduced norm 0.

The group $GL(2, L)$ acts on the set of 2×2 Hermitian matrices over L of reduced norm 0 by $(g, w) \mapsto g^* w g$, for $g \in GL(2, L)$, where g^* results from g by application of the involution $*$ to each entry, followed by transposition.

Given any unimodular solution of (11) with $u \neq 0$, using an elementary matrix in $GL(2, L)$, we can make $|x_1|, |x_2|, |x_3|, |x_4| \leq |u|/2$, and hence $|v| \leq |u|$. The inequality is strict unless $|x_m| = |v|/2$ for $m = 1, 2, 3, 4$, in which case $|v| = 2$ by unimodularity. In this last case, using an elementary matrix, we can arrange $x_m = 1$ for $m = 1, 2, 3, 4$.

Using the nontrivial permutation matrix in $GL(2, L)$, we can switch u and v. Therefore, by induction on $|u|$, the orbit of any unimodular solution $w = (x_1, x_2, x_3, x_4, u, v)$ to (11) contains a solution with either $|u| = 1$ and $x_m = 0$ for $m = 1, 2, 3, 4$ or $|u| = 2$ and $x_m = 1$ for $m = 1, 2, 3, 4$.

So we get that either

$$w = g^* \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} g = \begin{pmatrix} a^* \\ b^* \end{pmatrix} c(a, b)$$

with $c = \pm 1$ where (a, b) is the first row of the matrix $g \in GL(2, L)$ or

$$w = \pm g^* \begin{pmatrix} 2 & 1 + i + j + k \\ 1 - i - j - k & 2 \end{pmatrix} g = \pm \begin{pmatrix} a^* \\ b^* \end{pmatrix} (a, b)$$

where $(a, b) = \pm(1 - i, 1 + j)g$ with $g \in GL(2, L)$, because

$$\begin{pmatrix} 2 & 1 + i + j + k \\ 1 - i - j - k & 2 \end{pmatrix} = (1 - i, 1 + j)^*(1 - i, 1 + j).$$

So every integer solution of (11) has the form

$$w = \begin{pmatrix} u & x_1 + x_2 i + x_3 j + x_4 k \\ x_1 - x_2 i - x_3 j - x_4 k & v \end{pmatrix} = \begin{pmatrix} a^* \\ b^* \end{pmatrix} c(a, b)$$

with $a, b \in L$ and $c \in \mathbb{Z}$. Here we need not restrict (a, b) to be primitive.

Writing $c = y_0, a = y_1 + y_2 i + y_3 j + y_4 k$ and $b = y_5 + y_6 i + y_7 j + y_8 k$ we obtain the desired parametrization of all solutions $w = (x_1, x_2, x_3, x_4, u, v)$ of (11).

If we replace (a, b) above by $d(a, b)$ with $d \in L$, the solution w is multiplied by $d^* d$, which is equivalent to replacing y_0 by $y_0 d^* d$. Since every nonnegative integer is of the form $d^* d$ (sum of 4 squares) we can restrict y_0 to be ± 1. □

Returning to Pythagorean n-tuples, the following polynomial Pythagorean sextuple is known:

$$(x_1, \ldots, x_6) = h(y_0, \ldots, y_8) \in \mathbb{Z}[y_0, \ldots, y_8]^6 \tag{12}$$

with

$$\begin{aligned}
x_1 &= 2y_0(y_1 y_5 + y_2 y_6 + y_3 y_7 + y_4 y_8) \\
x_2 &= 2y_0(-y_1 y_6 + y_2 y_5 + y_3 y_8 - y_4 y_7) \\
x_3 &= 2y_0(-y_1 y_7 - y_2 y_8 + y_3 y_5 + y_4 y_6) \\
x_4 &= 2y_0(-y_1 y_8 + y_2 y_7 - y_3 y_6 + y_4 y_4) \\
x_5 &= y_0(y_1^2 + y_2^2 + y_3^2 + y_4^2 - y_5^2 - y_6^2 - y_7^2 - y_8^2) \\
x_6 &= y_0(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2)
\end{aligned}$$

There are, however, integer Pythagorean sextuples such as $(1, 1, 1, 1, 0, 2)$ that do not arise from the above polynomial sextuple with integer parameters y_i. We now give a parametrization of all integer Pythagorean sextuples by a single polynomial Pythagorean sextuple in 9 parameters, or, by restricting the parameter y_0 to ± 1, a parametrization by two integer Pythagorean sextuples in 8 parameters each.

Theorem 2. *Let $h = h(y_0, \ldots, y_8) \in \mathbb{Z}[y_0, \ldots, y_8]^6$ be the polynomial Pythagorean sextuple (12) above. Then the polynomial Pythagorean sextuple in $\mathbb{Z}[y_0, \ldots, y_7, z]^6$*

$$g(y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7, z) = h(y_0/2, y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + 2z)$$

in 9 parameters covers all Pythagorean sextuples, i.e., the range of the function $g\colon \mathbb{Z}^9 \to \mathbb{Z}^6$ is precisely the set of all Pythagorean sextuples. Also, the parameter y_0 can be restricted to ± 1.

Proof. We obtain all Pythagorean sextuples from all solutions of (11) with $u-v$ even by by (3). Since we can take y_0 odd (even ± 1) in Proposition 2, we may assume that $y_1+\cdots+y_8$ is even. Writing $y_8 = y_1+\cdots+y_7+2z$, we obtain a Pythagorean sextuple over $\mathbb{Z}[y_0, \ldots, y_7, z]$ in 9 parameters which parametrizes all Pythagorean sextuples:

$$\begin{aligned}
x_1 &= y_0(y_1y_5 + y_2y_6 + y_3y_7 + y_4(y_1 + \cdots + y_7 + 2z)) \\
x_2 &= y_0(-y_1y_6 + y_2y_5 + y_3(y_1 + \cdots + y_7 + 2z) - y_4y_7) \\
x_3 &= y_0(-y_1y_7 - y_2(y_1 + \cdots + y_7 + 2z) + y_3y_5 + y_4y_6) \\
x_4 &= y_0(-y_1(y_1 + \cdots + y_7 + 2z) + y_2y_7 - y_3y_6 + y_4y_5) \\
x_5 &= y_0(y_1^2 + y_2^2 + y_3^2 + y_4^2 - y_5^2 - y_6^2 - y_7^2 - (y_1 + \cdots + y_7 + 2z)^2)/2 \\
x_6 &= y_0(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + (y_1 + \cdots + y_7 + 2z)^2)/2
\end{aligned} \tag{13}$$

□

Remark. The $\mathbb{Z}$-algebra L is a subring of the ring H of rational quaternions (or Hamilton quaternions). Adjoining to L the element $(1+i+j+k)/2$, we obtain a larger subring L' of H, called the ring of **Hurwitz quaternions**. This ring H has certain unique factorization properties (cf. [2]), which, however, we did not use. They could be used to give alternative proofs for the results in this section.

3. Quintuples

We now consider the case $n = 5$ of Pythagorean quintuples. We obtain Theorem 3 from Proposition 2 via Proposition 3.

Proposition 3. *A parametrization of all integer quintuples (x_1, x_2, x_3, u, v) satisfying*

$$x_1^2 + x_2^2 + x_3^2 = uv$$

by a quintuple of polynomials with integer coefficients in the 12 parameters y_0, z_0, z_1, z_2, z_3, z_4, z_{12}, z_{13}, z_{14}, z_{23}, z_{24}, z_{34} is given by

$$\begin{aligned}
x_1 &= y_0(y_1y_5 + y_2y_6 + y_3y_7 + y_4y_8) \\
x_2 &= y_0(-y_1y_6 + y_2y_5 + y_3y_8 - y_4y_7) \\
x_3 &= y_0(-y_1y_7 - y_2y_8 + y_3y_5 + y_4y_6) \\
u &= y_0(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\
v &= y_0(y_5^2 + y_6^2 + y_7^2 + y_8^2),
\end{aligned}$$

with

$$\begin{aligned}
&y_1 = z_0z_1, \quad y_2 = z_0z_2, \quad y_3 = z_0z_3, \quad y_4 = z_0z_4, \\
&y_5 = -z_{14}z_1 - z_{24}z_2 - z_{34}z_3 \\
&y_6 = z_{13}z_1 + z_{23}z_2 - z_{34}z_4 \\
&y_7 = -z_{12}z_1 + z_{23}z_3 + z_{24}z_4 \\
&y_8 = -z_{12}z_2 - z_{13}z_3 - z_{14}z_4.
\end{aligned}$$

Proof. To solve $x_1^2+x_2^2+x_3^2=uv$, we set $x_4=0$ in the general solution to $x_1^2+x_2^2+x_3^2+x_4^2=uv$ obtained in Proposition 2:

$$-y_1y_8+y_2y_7-y_3y_6+y_4y_5=0 \tag{14}$$

(The case $y_0=0$ only contributes the zero solution which we will not miss.)

The integer solutions of (14) can be parametrized by 11 parameters as follows.

First we write $(y_1,y_2,y_3,y_4)=z_0(z_1,z_2,z_3,z_4)$ with $z_i\in\mathbb{Z}$ and (z_1,z_2,z_3,z_4) unimodular such that

$$(z_1,z_2,z_3,z_4).(-y_8,y_7,-y_6,y_5)=0$$

(the case $y_1=y_2=y_3=y_4=0$ only contributes solutions $(0,0,0,0,v)$ which we will not miss).

By [14], Remark after Lemma 9.6, we can write

$$(-y_8,y_7,-y_6,y_5)=$$
$$z_{12}(z_2,-z_1,0,0)+z_{13}(z_3,0,-z_1,0)+z_{14}(z_4,0,0,-z_1)+z_{23}(0,z_3,-z_2,0)+z_{24}(0,z_4,0,-z_2)+z_{34}(0,0,z_4,-z_3).$$

This gives a parametrization of the integer solutions of (14) in the 11 parameters z_0, z_1, z_2, z_3, z_4, z_{12}, z_{13}, z_{14}, z_{23}, z_{24}, z_{34}.

Therefore all integer solutions of $x_1^2+x_2^2+x_3^2=uv$ are parametrized by a polynomial solution with 12 parameters including y_0. □

Another parametrization of $x_1^2+x_2^2+x_3^2=uv$ with 20 parameters can be obtained using [15], Proposition 3.4 with $k=8$. We now parametrize integer Pythagorean quintuples by a single Pythagorean quintuple over the ring of integer-valued polynomials in 14 variables. This can be used to construct a parametrization by a finite number of integer-coefficient polynomial Pythagorean quintuples [6]. Whether it is possible to parametrize integer Pythagorean quintuples by a single quintuple of integer-coefficient polynomials or not, we do not know.

Theorem 3. *A parametrization of all Pythagorean quintuples by a quintuple of integer-valued polynomials in the 14 variables $w_0,w_{12},w_{13},w_{14},w_{23},w_{24},w_{34},t_1,t_2,t_3,d_1,d_2,d_3,w_4$ is given by (f_1,f_2,f_3,f_5,f_6), where*

$$\begin{aligned}
f_1 &= 2y_0(y_1y_5+y_2y_6+y_3y_7+y_4y_8)\\
f_2 &= 2y_0(-y_1y_6+y_2y_5+y_3y_8-y_4y_7)\\
f_3 &= 2y_0(-y_1y_7-y_2y_8+y_3y_5+y_4y_6)\\
f_5 &= y_0(y_1^2+y_2^2+y_3^2+y_4^2-y_5^2-y_6^2-y_7^2-y_8^2)/2\\
f_6 &= y_0(y_1^2+y_2^2+y_3^2+y_4^2+y_5^2+y_6^2+y_7^2+y_8^2)/2
\end{aligned}$$

and

$$\begin{aligned}
&y_1=z_0z_1,\quad y_2=z_0z_2,\quad y_3=z_0z_3,\quad y_4=z_0z_4,\\
&y_5=-z_{14}z_1-z_{24}z_2-z_{34}z_3\\
&y_6=z_{13}z_1+z_{23}z_2-z_{34}z_4\\
&y_7=-z_{12}z_1+z_{23}z_3+z_{24}z_4\\
&y_8=-z_{12}z_2-z_{13}z_3-z_{14}z_4.
\end{aligned}$$

and further

$$
\begin{aligned}
z_0 =& w_0 + t_1w_0 + t_2w_0 - 2t_1t_2w_0 + t_3w_0 - 2t_1t_3w_0 - t_2t_3w_0 + 2t_1t_2t_3w_0 + t_1w_{12} - t_1t_2w_{12} - \\
&- t_1t_3w_{12} + t_2t_3w_{12} + t_2w_{13} - t_1t_2w_{13} + t_3w_{14} - t_1t_3w_{14} + t_1w_{23} + t_2w_{23} - 2t_1t_2w_{23} - \\
&- t_1t_3w_{23} - t_2t_3w_{23} + 2t_1t_2t_3w_{23} + t_1w_{24} - t_1t_2w_{24} + t_3w_{24} - 2t_1t_3w_{24} - t_2t_3w_{24} + \\
&+ 2t_1t_2t_3w_{24} + t_2w_{34} - t_1t_2w_{34} + t_3w_{34} - t_1t_3w_{34} - 2t_2t_3w_{34} + 2t_1t_2t_3w_{34} \\
z_1 =& 2d_1 + t_1t_2 + t_3 - 2t_1t_2t_3 + w_4 \\
z_2 =& 2d_2 + t_1 - t_1t_2 + t_3 - t_1t_3 - t_2t_3 + 2t_1t_2t_3 + w_4 \\
z_3 =& 2d_3 + t_2 + t_3 - t_1t_3 - 2t_2t_3 + 2t_1t_2t_3 + w_4 \\
z_4 =& w_4 \\
z_{12} =& w_{12} + t_1t_2w_{12} - t_1t_2t_3w_{12} + t_1t_2w_{14} - t_1t_2t_3w_{14} + t_1t_2w_{23} - t_1t_2t_3w_{23} + t_1t_2w_{34} - t_1t_2t_3w_{34} \\
z_{13} =& w_{13} + t_1t_3w_{13} - t_1t_2t_3w_{13} + t_1t_3w_{14} - t_1t_2t_3w_{14} + t_1t_3w_{23} - t_1t_2t_3w_{23} + t_1t_3w_{24} - t_1t_2t_3w_{24} \\
z_{14} =& w_{14} \\
z_{23} =& w_{23} \\
z_{24} =& t_1t_2t_3w_{12} + t_1t_2t_3w_{13} + w_{24} + t_1t_2t_3w_{24} + t_1t_2t_3w_{34} \\
z_{34} =& w_{34}
\end{aligned}
$$

Proof. To go from the solutions of $x_1^2 + x_2^2 + x_3^2 = uv$ parametrized in Proposition 3 to the solutions of $x_1^2 + x_2^2 + x_3^2 + x_4^2 = x_5^2$ we use (3), allowing only those u, v with $u \pm v$ even.

In our case, we need to parametrize those $z_0, \ldots, z_{34}$ that make $y_1 + y_2 + \ldots + y_8$ even, i.e., those $z_0, \ldots, z_{34}$ such that $E = z_0z_1 + z_0z_2 + z_0z_3 + z_0z_4 + -z_{14}z_1 - z_{24}z_2 - z_{34}z_3 - z_{13}z_1 - z_{23}z_2 + z_{34}z_4 - z_{12}z_1 + z_{23}z_3 + z_{24}z_4 - z_{12}z_2 - z_{13}z_3 - z_{14}z_4$ is even.

This is achieved by the following substitution, which, after simplification, gives the parametrization in the statement of the theorem.

$$
\begin{gathered}
\big(z_0, z_1, z_2, z_3, z_4, z_{12}, z_{13}, z_{14}, z_{23}, z_{24}, z_{34}\big) = \\
\big(w_0, w_4 + 2d_1, w_4 + 2d_2, w_4 + 2d_3, w_4, w_{12}, w_{13}, w_{14}, w_{23}, w_{24}, w_{34}\big)(1-t_1)(1-t_2)(1-t_3) + \\
\big(w_{14} + w_{24} + w_{34} + 2w_0, w_4 + 2d_1 + 1, w_4 + 2d_2 + 1, w_4 + 2d_3 + 1, w_4, w_{12}, w_{13}, w_{14}, w_{23}, w_{24}, w_{34}\big)(1-t_1)(1-t_2)t_3 + \\
\big(w_{13} + w_{23} + w_{34} + 2w_0, w_4 + 2d_1, w_4 + 2d_2, w_4 + 2d_3 + 1, w_4, w_{12}, w_{13}, w_{14}, w_{23}, w_{24}, w_{34}\big)(1-t_1)t_2(1-t_3) + \\
\big(w_{12} + w_{23} + w_{24} + 2w_0, w_4 + 2d_1, w_4 + 2d_2 + 1, w_4 + 2d_3, w_4, w_{12}, w_{13}, w_{14}, w_{23}, w_{24}, w_{34}\big)t_1(1-t_2)(1-t_3) + \\
\big(w_{12} + w_{13} + w_{14} + 2w_0, w_4 + 2d_1 + 1, w_4 + 2d_2, w_4 + 2d_3, w_4, w_{12}, w_{13}, w_{14}, w_{23}, w_{24}, w_{34}\big)(1-t_1)t_2t_3 + \\
\big(w_0, w_4 + 2d_1 + 1, w_4 + 2d_2 + 1, w_4 + 2d_3, w_4, w_{12}, w_{23} + w_{24} + w_{14} + 2w_{13}, w_{14}, w_{23}, w_{24}, w_{34}\big)t_1(1-t_2)t_3 + \\
\big(w_0, w_4 + 2d_1 + 1, w_4 + 2d_2, w_4 + 2d_3 + 1, w_4, w_{23} + w_{14} + w_{34} + 2w_{12}, w_{13}, w_{14}, w_{23}, w_{24}, w_{34}\big)t_1t_2(1-t_3) + \\
\big(w_0, w_4 + 2d_1, w_4 + 2d_2 + 1, w_4 + 2d_3 + 1, w_4, w_{12}, w_{13}, w_{14}, w_{23}, w_{12} + w_{13} + w_{34} + 2w_{24}, w_{34}\big)t_1t_2t_3
\end{gathered}
$$

□

4. Descartes quadruples

In 1643 Descartes [3] described a relationship between the radii of four mutually tangent circles (called a Descartes configuration), namely,

$$2(b_1^2 + b_2^2 + b_3^2 + b_4^2) = (b_1 + b_2 + b_3 + b_4)^2 \tag{15}$$

where b_i are the reciprocals of the radii. Others, including Steiner, Beecroft, and Soddy [13], rediscovered the result. We call an integer solution of (15) a Descartes quadruple.

Given one Descartes configuration, there is a geometric way to produce plenty of them creating an Apollonian packing. If the four initial curvatures b_i are integers, all curvatures in the packing are integers. There are several publications about integer Apollonian packings [8], [9], [10], [5],[12], [11]. A bijection between integer Pythagorean quadruples and integer Descartes quadruples can be found in [8], Lemma 2.1.

In this section we parametrize all integer solutions of (15) by a single polynomial solution in 5 parameters, using a bijection between integer Descartes quadruples and integer solutions of (6).

Given an integer solution (x_1, x_2, u, v) of (6),

$$b_1 = u + v - 2x_1 + x_2, \quad b_2 = u + x_2, \quad b_3 = v + x_2, \quad b_4 = -x_2 \tag{16}$$

is an integer solution of (15). Conversely, we can invert this linear transformation: given an integer solution (b_1, b_2, b_3, b_4) of (15), $b_1 + b_2 + b_3 + b_4$ is even and

$$x_1 = (-b_1 + b_2 + b_3 + b_4)/2, \quad x_2 = -b_4, \quad u = b_2 + b_4, \quad v = b_3 + b_4$$

is an integer solution of (6).

Theorem 4. *A parametrization of all integer solutions of*

$$2(b_1^2 + b_2^2 + b_3^2 + b_4^2) = (b_1 + b_2 + b_3 + b_4)^2 \tag{15}$$

in 5 parameters is given by

$$\begin{aligned}
b_1 &= y_0(y_1^2 + y_2^2 + y_3^2 + y_4^2 - 2y_1y_3 - 2y_2y_4 + y_1y_4 - y_2y_3), \\
b_2 &= y_0(y_1^2 + y_2^2 + y_1y_4 - y_2y_3), \\
b_3 &= y_0(y_3^2 + y_4^2 + y_1y_4 - y_2y_3), \\
b_4 &= y_0(-y_1y_4 - y_2y_3).
\end{aligned}$$

Proof. In the expression (16) of b_1, b_2, b_3, b_4 in terms of a solution x_1, x_2, u, v of (6) we have substituted the parametrization of all integer solutions of (6) from Proposition 1. □

References

[1] R.D. Carmichael, Diophantine Analysis, John Wiley & Sons, New York, 1915.

[2] John H. Conway and Derek A. Smith, On quaternions and octonions. Their geometry, arithmetic, and symmetry, Peters, 2003.

[3] René Descartes, Correspondance IV, in: C. Adam and P. Tannery (eds.) Œuvres de Descartes, Leopold Cert, Paris, 1901.

[4] Leonard Eugene Dickson, Algebras and their arithmetics. Dover Publications, New York 1960.

[5] Nicholas Eriksson and Jeffrey C. Lagarias, Apollonian circle packings: number theory. II. Spherical and hyperbolic packings, Ramanujan J. 14 (2007), no. 3, 437–469.

[6] Sophie Frisch, Remarks on polynomial parametrization of sets of integer points, Comm. Algebra 36 (2008), no. 3, 1110–1114.

[7] Sophie Frisch and Leonid Vaserstein, Parametrization of Pythagorean triples by a single triple of polynomials, J. Pure Appl. Algebra 212 (2008) 271–274.

[8] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks and C.R. Yan, Apollonian circle packings: Number theory, J. Number Theory 100 (2003) 1–45.

[9] Ronald L. Graham, Jeffrey C. Lagarias, Colin L. Mallows, Allan R. Wilks, and Catherine H. Yan, Apollonian circle packings: geometry and group theory. II. Super-Apollonian group and integral packings. Discrete Comput. Geom. 35 (2006), no. 1, 1–36.

[10] Ronald L. Graham, Jeffrey C. Lagarias, Colin L. Mallows, Allan R. Wilks and Catherine H. Yan, Apollonian circle packings: geometry and group theory. III. Higher dimensions. Discrete Comput. Geom. 35 (2006), no. 1, 37–72.

[11] J.C. Lagarias, C.L. Mallows and A.R. Wilks, Beyond the Descartes circle theorem, Amer. Math. Monthly 109 (4) (2002) 338–361.

[12] S. Northshield, On integral Apollonian circle packings. J. Number Theory 119 (2006), no. 2, 171–193.

[13] F. Soddy, The kiss precise, Nature, vol 137 no. 3477 (June 20 1936) p1021.

[14] L.N. Vaserstein and A.A. Suslin, Serre's problem on projective modules over polynomial rings and algebraic K-theory, Izv.Akad.Nauk, ser.mat. 40:5 (1976), 993-1054 = Math.USSR Izv. 10:5, 937-1001.

[15] L.N. Vaserstein, Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups, Annals of Math. 171 (2), 2010, 979–1009.