J. Pure Appl. Algebra 212 (2008) (1) 271–274

Parametrization of Pythagorean triples by a single triple of polynomials

Sophie Frisch and Leonid Vaserstein

Abstract. It is well known that Pythagorean triples can be parametrized by two triples of polynomials with integer coefficients. We show that no single triple of polynomials with integer coefficients in any number of variables is sufficient, but that there exists a parametrization of Pythagorean triples by a single triple of integer-valued polynomials.

The second author has recently studied polynomial parametrizations of solutions of Diophantine equations [8], and the first author has wondered if it were possible in some cases to parametrize by a k-tuple of integer-valued polynomials a solution set that is not parametrizable by a k-tuple of polynomials with integer coefficients [6]. Pythagorean triples provide an example that this is indeed so.

We call a triple of integers $(x, y, z) \in \mathbb{Z}^3$ satisfying

$$x^2 + y^2 = z^2$$

a Pythagorean triple, and, if $x, y, z > 0$, a positive Pythagorean triple.

It is well known that every Pythagorean triple is either of the form

$$\bigl(c(a^2 - b^2),\ 2cab,\ c(a^2 + b^2)\bigr)$$

or of the form

$$\bigl(2cab,\ c(a^2 - b^2),\ c(a^2 + b^2)\bigr)$$

2000 Math. Subj. Classification: primary 11D09, secondary 11D85, 11C08, 13F20.

with $a, b, c \in \mathbb{Z}$, see for instance [7].

To make precise our usage of the term polynomial parametrization, consider a set $S \subseteq \mathbb{Z}^k$. Let $f_1, \ldots, f_k$ be a k-tuple of polynomials either in the ring of polynomials with integer coefficients in n variables, $\mathbb{Z}[x_1, \ldots, x_n]$, or in

$$\mathrm{Int}(\mathbb{Z}^n) = \{f \in \mathbb{Q}[x_1, \ldots, x_n] \mid \forall a \in \mathbb{Z}^n \ f(a) \in \mathbb{Z}\},$$

the ring of integer-valued polynomials in n variables, for some n. In either case $F = (f_1, \ldots, f_k)$ defines a function $F\colon \mathbb{Z}^n \to \mathbb{Z}^k$. If S is the image of this function, $S = F(\mathbb{Z}^n)$, we say that $(f_1, \ldots, f_k)$ parametrizes S. We call this a parametrization of S by a single k-tuple of polynomials.

If $S \subseteq \mathbb{Z}^k$ is the union of the images of finitely many k-tuples of polynomials $F_i = (f_{i1}, \ldots, f_{ik})$, $S = \bigcup_{i=1}^{m} F_i(\mathbb{Z}^n)$, we call this a parametrization of S by a finite number of k-tuples of polynomials, and we distinguish between parametrizations by polynomials with integer coefficients, meaning $F_i \in (\mathbb{Z}[x_1, \ldots, x_n])^k$ for all i, and by integer-valued polynomials, meaning $F_i \in (\mathrm{Int}(\mathbb{Z}^n))^k$. Unless explicitly specified otherwise, we are using integer parameters, that is, we let all variables of all polynomials range through the integers.

We will give a parametrization of the set of Pythagorean triples by a single triple of integer-valued polynomials in 4 variables, that is, by (f_1, f_2, f_3) with $f_i \in \mathbb{Q}[x, y, z, w]$ such that $f_i(x, y, z, w) \in \mathbb{Z}$ whenever $x, y, z, w \in \mathbb{Z}$. First we will show that it is not possible to parametrize Pythagorean triples by a single triple of polynomials with integer coefficients in any number of variables.

Note, however, that every set of k-tuples of integers that is parametrizable by a single k-tuple of integer-valued polynomials is parametrizable by a finite number of k-tuples of polynomials with integer coefficients [6].

Remark. *There do not exist $f, g, h \in \mathbb{Z}[x_1, \ldots, x_n]$ for any n such that (f, g, h) parametrizes the set of Pythagorean triples.*

Proof. Suppose (f, g, h) parametrizes the Pythagorean triples. As $\mathbb{Z}[\underline{x}]$ is a unique factorization domain, there exists $d = \gcd(g, h)$ (unique up to sign), which also divides f, since $f^2 + g^2 = h^2$. Let $\varphi = f/d$, $\psi = g/d$ and $\theta = h/d$.

Then

$$\varphi^2 = \theta^2 - \psi^2 = (\theta + \psi)(\theta - \psi)$$

and $\gcd((\theta + \psi), (\theta - \psi))$ is either 1 or 2, but it can't be 2, because there exist Pythagorean triples with odd first coordinate such as $(3, 4, 5)$. Since $(\theta + \psi)$ and $(\theta - \psi)$ are co-prime and their product is a square, $(\theta + \psi)$ and $(\theta - \psi)$ are either both squares, or both (-1) times a square, and we can get rid of the latter alternative by retro-actively changing the sign of the polynomial d, if necessary.

So there exist polynomials s and t with $(\theta+\psi)=s^2$ and $(\theta-\psi)=t^2$, and therefore

$$\theta=\frac{s^2+t^2}{2} \quad \text{and} \quad \psi=\frac{s^2-t^2}{2}.$$

Since $s^2-t^2=(s+t)(s-t)$ is divisible by 2, it is actually divisible by 4, so that ψ is divisible by 2, which contradicts the existence of Pythagorean triples with odd second coordinate such as $(4,3,5)$. $\square$

In a way, it was the unique factorization property of $\mathbb{Z}[\underline{x}]$ that prevented us from finding a triple of polynomials in $\mathbb{Z}[\underline{x}]$ parametrizing Pythagorean triples. Before we construct a parametrization of Pythagorean triples by a triple of integer-valued polynomials, we remark in passing that $\mathrm{Int}(\mathbb{Z}^n)$ does not enjoy unique factorization into irreducibles. An example of non-unique factorization into irreducibles in $\mathrm{Int}(\mathbb{Z})$ is given by

$$x(x-1)\dots(x-k+1)=k!\binom{x}{k}.$$

The lefthand side is a product of k irreducibles, while the righthand side, after factorization of $k!$ in $\mathbb{Z}$, becomes a product of far more irreducibles (for large k). (See [4] for integer-valued polynomials in general, and [1, 3, 5] for factorization properties.)

Theorem. *There exist $f,g,h\in\mathrm{Int}(\mathbb{Z}^4)$ such that (f,g,h) parametrizes the set of Pythagorean triples (as the variables range through $\mathbb{Z}$) namely,*

$$\Bigg(\frac{(2x-xw)((y+zw)^2-(z-yw)^2)}{2},$$

$$(2x-xw)(y+zw)(z-yw),$$

$$\frac{(2x-xw)((y+zw)^2+(z-yw)^2)}{2}\Bigg).$$

Proof. Every Pythagorean triple (x,y,z) with $\gcd(x,y,z)=1$ and $z>0$ is either of the form

$$T_1(a,b)=(a^2-b^2,\ 2ab,\ a^2+b^2),$$

or of the form

$$T_2(a,b)=(2ab,\ a^2-b^2,\ a^2+b^2),$$

with $a,b\in\mathbb{Z}$. Since

$$2\,T_2(a,b)=T_1(a+b,\ a-b),$$

every Pythagorean triple with $\gcd(x,y,z)=1$ and $z>0$ is of the form $cT_1(a,b)/2$ with $c\in\{1,2\}$ and $a,b\in\mathbb{Z}$. Let

$$T(a,b,c)=\left(\frac{c(a^2-b^2)}{2},\ cab,\ \frac{c(a^2+b^2)}{2}\right).$$

Then every Pythagorean triple is of the form $T(a,b,c)$ with $a,b,c\in\mathbb{Z}$. Also, every triple $T(a,b,c)$ with $a,b,c\in\mathbb{Z}$ is a rational solution of $x^2+y^2=z^2$.

So, the set of Pythagorean triples is precisely the set of integer triples in the range of the function $T\colon\mathbb{Z}^3\to\mathbb{Q}^3$.

Now $T(a,b,c)\in\mathbb{Z}^3$ if and only if $c\equiv 0 \bmod 2$ or $a\equiv b \bmod 2$. Triples $(a,b,c)\in\mathbb{Z}^3$ satisfying this condition can be parametrized by (for instance)

$$(y+zw,\ z-yw,\ 2x-xw).$$

Indeed, if w is even then $c\equiv 0 \bmod 2$, if w is odd then $a\equiv b \bmod 2$, and all (a,b,c) satisfying either congruence actually occur for some $(x,y,z,w)\in\mathbb{Z}^4$, as can be seen by setting $w=0$ or $w=1$.

Therefore, substituting $y+zw$ for a, $z-yw$ for b, and $2x-xw$ for c in $T(a,b,c)$ yields a parametrization of the set of Pythagorean triples by a triple of integer-valued polynomials. $\square$

Remark. *The set of positive Pythagorean triples is parametrized by*

$$\left(\frac{(x+(1-w)^2x)((y+(1+w)z)^2-y^2)}{2},\right.$$

$$(x+(1-w)^2x)(y+(1+w)z)y,$$

$$\left.\frac{(x+(1-w)^2x)((y+(1+w)z)^2+y^2)}{2}\right).$$

where x,y,z range through the positive integers and w through the non-negative integers. From this formula, a parametrization of positive Pythagorean triples with integer parameters can be obtained (using the 4-square theorem) by replacing w by $w_1^2+w_2^2+w_3^2+w_4^2$ and x, y, z by $x_1^2+x_2^2+x_3^2+x_4^2+1$, $y_1^2+y_2^2+y_3^2+y_4^2+1$, and $z_1^2+z_2^2+z_3^2+z_4^2+1$, respectively.

Proof. As in the proof of the theorem above, the positive Pythagorean triples are precisely the triples with positive integer coordinates in the range of the function $T\colon\mathbb{Z}^3\to\mathbb{Q}^3$. Now $T(a,b,c)$ is a positive triple if and only if a,b,c are positive integers with $a > b$ and either $c \equiv 0 \bmod 2$ or $a \equiv b \bmod 2$. Such triples (a, b, c) are parametrized by (for instance)

$$(y + (1 + w)z,\ y,\ x + (1 - w)^2 x)$$

with $x, y, z > 0$ and $w \geq 0$. Therefore substituting $y + (1 + w)z$ for a, y for b and $x + (1 - w)^2 x$ for c in $T(a, b, c)$ gives a parametrization of positive Pythagorean triples where w ranges through non-negative integers and x, y, z through positive integers. The 4-square theorem allows us to convert this to a parametrization with 16 integer parameters. □

References

[1] D. F. Anderson, P.-J. Cahen, S. Chapman, and W. W. Smith, *Some factorization properties of the ring of integer-valued polynomials*, in Anderson and Dobbs [2], 125–142.

[2] D. F. Anderson and D. Dobbs, eds., *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, vol. 171 of Lecture Notes in pure and applied mathematics, Dekker, 1995.

[3] P.-J. Cahen and J.-L. Chabert, *Elasticity for integral-valued polynomials*, J. Pure Appl. Algebra 103 (1995), 303–311.

[4] P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials*, vol. 48 of Mathematical Surveys and Monographs, Amer. Math. Soc., 1997.

[5] S. Chapman and B. A. McClain, *Irreducible polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra 293 (2005), 595–610.

[6] S. Frisch, *Remarks on polynomial parametrization of sets of integer points*, to appear in Comm. Algebra.

[7] E. Hlawka and J. Schoissengeier, *Zahlentheorie. Eine Einführung*, Manz, Vienna, 1979.

[8] L. Vaserstein, *Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups*, to appear in Ann. of Math.

S.F.
Institut für Mathematik C
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria
`frisch@blah.math.tu-graz.ac.at`

L.V.
Department of mathematics
Pennsylvania State University
University Park, PA 16802
U.S.A.
`vstein@math.psu.edu`