MONOIDS CONNECTED WITH EULER'S DIOPHANTINE EQUATION

Aleksander Grytczuk

Abstract. In this paper we give a construction of infinite monoids generated by the integer solutions of Euler's Diophantine equation $x^2 + y^2 = z^n$, $n \geq 2$.

1. Introduction. It is well-known, by the classical result of Euler, that the Diophantine equation

$$x^2 + y^2 = z^n, \quad n \geq 2 \tag{1}$$

has infinitely many solutions in integers x, y, and z for any fixed positive integer $n \geq 2$. Moreover, all integer solutions of (1) in integers x, y, and z such that $(x, y) = 1$ are given by the following formula:

$$x = \frac{(r+is)^n + (r-is)^n}{2}, \quad y = \frac{(r+is)^n - (r-is)^n}{2i}, \quad z = r^2 + s^2, \tag{2}$$

where r and s are integers such that $(r, s) = 1$.
Let

$$S_n = \{\langle x, y, z\rangle \in \mathbb{Z}^3; \quad x^2 + y^2 = z^n; \quad n \geq 2\}. \tag{3}$$

Define the operation "$\circ$" on S_n as follows.
If $\alpha = \langle a, b, c\rangle \in S_n$ and $\beta = \langle u, v, w\rangle \in S_n$, then

$$\alpha \circ \beta = \langle a, b, c\rangle \circ \langle u, v, w\rangle = \langle au - bv, av + bu, cw\rangle = \gamma. \tag{4}$$

The following identity

$$(au - bv)^2 + (av + bu)^2 = (a^2 + b^2)(u^2 + v^2) \tag{5}$$

is well-known. Since $\alpha, \beta \in S_n$, then by (3) it follows that

$$a^2 + b^2 = c^n, \quad u^2 + v^2 = w^n. \tag{6}$$

From (5) and (6), we obtain

$$(au - bv)^2 + (av + bu)^2 = (cw)^n. \tag{7}$$

Now, by (7), it follows that the element $\gamma = \langle au - bv, av + bu, cw\rangle$ belongs to S_n. We prove that the set $\langle S_n; \circ\rangle$, where the operation "$\circ$" is define by (4) is a commutative monoid for any fixed positive integer $n \geq 2$. We note that in the case $n = 2$, the equation (1) reduces to the Pythagorean equation. In this case, B. Dawson [1] gave a construction of a Pythagorean ring. He defined two operations and an isomorphism $\Phi\colon P \to \mathbb{Z} \times \mathbb{Z}$, where $P = \{\langle x, y, z\rangle \in \mathbb{Z}^3;\ x^2 + y^2 = z^2\}$ and utilizing the elements of the set $P_n = \{\langle x, y, z\rangle \in P;\ z - y = n\}$. Moreover, in [2], it was proven that the set P_n, with respect to the particular operations "$\oplus$" and "$\circ$" is a commutative ring for any fixed integer n.

2. Results. We begin by proving the following theorem.

Theorem 1. The set $\langle S_n; \circ\rangle$, where the operation "$\circ$" is defined by (4) and S_n by (3), is a commutative monoid, for any positive integer $n \geq 2$.

Proof. Let $\alpha = \langle a, b, c\rangle \in S_n$, $\beta = \langle u, v, w\rangle \in S_n$, and $\gamma = \langle d, e, f\rangle \in S_n$. Then by (4), it follows that

$$\begin{aligned} L &= (\alpha \circ \beta) \circ \gamma = (\langle a, b, c\rangle \circ \langle u, v, w\rangle) \circ \langle d, e, f\rangle \\ &= \langle au - bv, av + bu, cw\rangle \circ \langle d, e, f\rangle. \end{aligned}$$

Putting $a_1 = au - bv$, $b_1 = av + bu$, and $c_1 = cw$ in the last equality and using (4), we obtain

$$L = \langle a_1, b_1, c_1\rangle \circ \langle d, e, f\rangle = \langle a_1 d - b_1 e, a_1 e + b_1 d, c_1 f\rangle.$$

In a similar way, we obtain

$$\begin{aligned} P &= \alpha \circ (\beta \circ \gamma) = \langle a, b, c\rangle \circ (\langle u, v, w\rangle \circ \langle d, e, f\rangle) \\ &= \langle a, b, c\rangle \circ \langle ud - ve, ue + vd, wf\rangle. \end{aligned}$$

Let $u_1 = ud - ve$, $v_1 = ue + vd$, and $w_1 = wf$. Then by (4) and the last equality, it follows that

$$P = \langle a, b, c\rangle \circ \langle u_1, v_1, w_1\rangle = \langle au_1 - bv_1, av_1 + bu_1, cw_1\rangle.$$

Moreover, it is easy to see that

$$cw_1 = cwf = c_1 f \tag{8}$$
$$a_1 d - b_1 e = (au - bv)d - (av + bu)e = a(ud - ve) - b(ue + vd) = av_1 + bu_1 \tag{9}$$
$$a_1 e + b_1 d = (au - bv)e + (av + bu)d = a(ue + vd) + b(ud - ve) = av_1 + bu_1. \tag{10}$$

From (8)–(10), it follows that $L = P$ and the associative law is satisfied. On the other hand, we have

$$\alpha \circ \beta = \langle a, b, c\rangle \circ \langle u, v, w\rangle = \langle au - bv, av + bu, cw\rangle = \beta \circ \alpha$$

and so the commutative law is satisfied. Finally, we remark that the element $e = \langle 1, 0, 1\rangle \in S_n$ and for every $\alpha \in S_n$ we have, by (4), that $\alpha \circ e = e \circ \alpha = \alpha$; therefore, the element $e = \langle 1, 0, 1\rangle$ is the identity element in the set S_n, and the proof of Theorem 1 is complete.

Remark. The set $\langle S_n; \circ\rangle$ is not a group, because α has an inverse in S_n if and only if $\alpha = \langle \pm 1, 0, \pm 1\rangle$ or $\langle 0, \pm 1, \pm 1\rangle$.

Now, we introduce a special set of matrices:

$$M_2^{(n)}(\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix};\ \det A = c^n;\ n \geq 2;\ a, b, c \in \mathbb{Z} \right\}. \tag{$*$}$$

We prove the following.

Theorem 2. Let $M_2^{(n)}(\mathbb{Z})$ be the set of all integral matrices defined by $(*)$ with the operation of matrix multiplication, denoted by "$\cdot$". Then the set $\langle S_n; \circ\rangle$ is isomorphic to the set $\langle M_2^{(n)}(\mathbb{Z}), \cdot\rangle$.

Proof. Let $\Phi\colon S_n \to M_2^{(n)}(\mathbb{Z})$ be the mapping defined as follows. If $\alpha = \langle a, b, c\rangle \in S_n$, then

$$\Phi(\alpha) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = A;\ \det A = c^n;\ n \geq 2. \tag{11}$$

First, we remark that the mapping Φ is bijective. Further, for $\alpha = \langle a, b, c\rangle \in S_n$ and $\beta = \langle u, v, w\rangle \in S_n$, we have

$$\Phi(\alpha \circ \beta) = \Phi(\langle a, b, c\rangle \circ \langle u, v, w\rangle) = \Phi(\langle au - bv, av + bu, cw\rangle).$$

From the last equality and (11), we obtain

$$\Phi(\alpha\circ\beta)=\begin{pmatrix} au-bv & av+bu \\ -(av+bu) & au-bv \end{pmatrix}=C,\ \det C=(cw)^n=(au-bv)^2+(av+bu)^2.$$

On the other hand, by (11), it follows that

$$\Phi(\alpha)=\Phi(\langle a,b,c\rangle)=A=\begin{pmatrix} a & b \\ -b & a \end{pmatrix},\ \det A=a^2+b^2=c^n \tag{12}$$

$$\Phi(\beta)=\Phi(\langle u,v,w\rangle)=B=\begin{pmatrix} u & v \\ -v & u \end{pmatrix},\ \det B=u^2+v^2=w^n. \tag{13}$$

By (12) and (13), it follows that

$$\Phi(\alpha)\cdot\Phi(\beta)=A\cdot B=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\cdot\begin{pmatrix} u & v \\ -v & u \end{pmatrix}=\begin{pmatrix} au-bv & av+bu \\ -(av+bu) & au-bv \end{pmatrix}. \tag{14}$$

For (14) and Cauchy's theorem on the product of determinants, we obtain

$$\det(A\cdot B)=\det A\cdot\det B=(a^2+b^2)(u^2+v^2)=(au-bv)^2+(av+bu)^2. \tag{15}$$

By (12), (13), and (15), it follows that $(cw)^n=(au-bv)^2+(av+bu)^2=\det C$ and consequently, we obtain $\Phi(\alpha\circ\beta)=\Phi(\alpha)\cdot\Phi(\beta)$, hence, $S_n\approx M_2^{(n)}(\mathbb{Z})$. The proof of Theorem 2 is complete.

References

1. B. Dawson, "A Ring of Pythagorean Triples," *Missouri Journal of Mathematical Sciences*, 6 (1994), 72–77.

2. A. Grytczuk, "Note on a Pythagorean Ring," *Missouri Journal of Mathematical Sciences*, 9 (1997), 83–89.

Aleksander Grytczuk
Institute of Mathematics
Department of Algebra and Number Theory
T. Kotarbiński Pedagogical University
65-069 Zielona Góra, Poland
email: grytal@omega.im.wsp.zgora.pl