

PYTHAGOREAN QUADRUPLETS

EDRAY GOINS AND ALAIN TOGBE

ABSTRACT. We consider the multiplicative properties of integer quadruplets (a, b, c, d) satisfying $a^2 + b^2 + c^2 = d^2$ as a generalization of Pythagorean Triplets. In the process we present a group structure on the rational points on the unit sphere minus the poles and discuss a factorization result.

1. INTRODUCTION

It is easy to show that the Pythagorean Triplets – integers a, b, c satisfying $a^2 + b^2 = c^2$ – are closed under “multiplication;” that is, given two such triplets one generates a third through the operation

$$(1) \quad (a_1, b_1, c_1) \oplus (a_2, b_2, c_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1, c_1 c_2).$$

This operation induces an associative, commutative multiplicative structure on the Pythagorean Triplets; see for example [Dav99, pg. 116]. We are motivated to study a generalization to four variables, the so-called Pythagorean Quadruplets, where we consider integers a, b, c, d such that $a^2 + b^2 + c^2 = d^2$. Such quadruplets have a parametrization similar to the well-known triplets, as outlined in the

Proposition 1.1. *For each Pythagorean Quadruplet (a, b, c, d) there exist integers m, n, p, q such that*

$$(2) \quad a = m n p, \quad b = m n q, \quad c = \frac{m^2 - p^2 - q^2}{2} n, \quad d = \frac{m^2 + p^2 + q^2}{2} n.$$

Similar formulae are well-known for Pythagorean Triplets; see [Dav99, pgs. 151 - 154]. Some examples of such quadruplets are

$$(3) \quad \begin{array}{rcl} & 1^2 + 2^2 + 2^2 & = 3^2 \\ & 3^2 + 4^2 & = 5^2 \\ & 2^2 + 3^2 + 6^2 & = 7^2 \\ \\ & 1^2 + 4^2 + 8^2 & = 4^2 + 4^2 + 7^2 = 9^2 \\ & 2^2 + 6^2 + 9^2 & = 6^2 + 6^2 + 7^2 = 11^2 \\ & 5^2 + 12^2 & = 3^2 + 4^2 + 12^2 = 13^2 \\ & 2^2 + 5^2 + 14^2 & = 2^2 + 10^2 + 11^2 = 15^2 \\ \\ & 8^2 + 15^2 & = 1^2 + 12^2 + 12^2 = 8^2 + 9^2 + 12^2 = 17^2 \\ & 1^2 + 6^2 + 18^2 & = 6^2 + 6^2 + 17^2 = 6^2 + 10^2 + 15^2 = 19^2 \end{array}$$

1991 *Mathematics Subject Classification.* 11E25, 11E20.

Key words and phrases. Pythagorean Triplets, Ternary Quadratic Forms, Sums of Squares.

In this paper, we consider the associative, commutative operation

$$(4) \quad \begin{aligned} & (a_1, b_1, c_1, d_1) \oplus (a_2, b_2, c_2, d_2) \\ & = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1, c_1 d_2 + c_2 d_1, c_1 c_2 + d_1 d_2) \end{aligned}$$

and attempt to ask questions of factorization. Our main result may be stated as follows. Let $\tilde{P} = (a, b, c, d)$ be a Pythagorean Quadruplet, and denote n as the greatest common divisor of a, b, c, d ; then $\tilde{P}_0 = (\frac{a}{n}, \frac{b}{n}, \frac{c}{n}, \frac{d}{n})$ is also a Pythagorean Quadruplet, and we say that $h(\tilde{P}) = |d/n|$ is the height of \tilde{P} . Define $\{\tilde{P}\}$ as the collection of all scalar multiples of \tilde{P}_0 where we allow sign changes and permutations $a \leftrightarrow b, a \leftrightarrow c, b \leftrightarrow c$ as well; this ‘‘conjugacy class’’ corresponds to the identity $a^2 + b^2 + c^2 = d^2$. Then we prove the following

Theorem 1.2. *Let \tilde{P} be a Pythagorean Quadruplet with $h(\tilde{P}) > 3$. Then there exist \tilde{P}_1, \tilde{P}_2 with $h(\tilde{P}_1), h(\tilde{P}_2) < h(\tilde{P})$ such that $\{\tilde{P}\} = \{\tilde{P}_1 \oplus \tilde{P}_2\}$.*

As an example, consider the identity $3^2 + 4^2 = 5^2$. Viewed as a Pythagorean Quadruplet, we have the factorization

$$(5) \quad \{(0, 3, 4, 5)\} = \{(0, 4, 3, 5)\} = \{(2, 2, 1, 3) \oplus (2, 2, 1, 3)\}.$$

In a sense the identity $3^2 + 4^2 = 5^2$ is ‘‘generated’’ by the identity $1^2 + 2^2 + 2^2 = 3^2$.

Our proof relies on the mapping

$$(6) \quad (a, b, c, d) \mapsto \frac{a + ib}{c + d}$$

where the multiplicative properties of the complex numbers induce the multiplicative properties of the Pythagorean Quadruplets. Most of the paper is concerned with the rational points on the unit sphere which have an induced group structure coming from stereographic projection.

2. MULTIPLICATION ON THE UNIT SPHERE

Ultimately we wish to study Pythagorean Quadruplets (a, b, c, d) , but we note that through the map

$$(7) \quad (a, b, c, d) \mapsto \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) \quad \text{where} \quad \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 + \left(\frac{c}{d}\right)^2 = 1$$

it suffices to consider rational points on the unit sphere. To this end, we begin with a discussion of the real points.

Recall that the unit sphere $S^2(\mathbb{R}) = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1\}$ is isomorphic with the extended complex numbers under the ‘‘stereographic projection’’ map $(x_1, x_2, x_3) \mapsto (x_1 + ix_2)/(1 + x_3)$. (See [Con78, pgs. 8-9] for details. Our formulas are different in that we map the north pole $(0, 0, 1) \mapsto 0$ and the south pole $(0, 0, -1) \mapsto \infty$.) The multiplicative structure of the complex numbers induces a corresponding structure on the unit sphere.

Theorem 2.1. *Denote the ‘‘poleless’’ unit sphere by*

$$(8) \quad S^{2,\times}(\mathbb{R}) = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1, x_3 \neq \pm 1\}$$

and define the operation $\oplus : S^{2,\times}(\mathbb{R}) \times S^{2,\times}(\mathbb{R}) \rightarrow S^{2,\times}(\mathbb{R})$ as

$$(9) \quad (x_1, x_2, x_3) \oplus (y_1, y_2, y_3) = \left(\frac{x_1 y_1 - x_2 y_2}{1 + x_3 y_3}, \frac{x_1 y_2 + x_2 y_1}{1 + x_3 y_3}, \frac{x_3 + y_3}{1 + x_3 y_3} \right).$$

This makes $S^{2,\times}(\mathbb{R})$ into a commutative group, where the identity is $\mathcal{O} = (1, 0, 0)$ and the inverse of a point $P = (x_1, x_2, x_3)$ is $[-1]P = (x_1, -x_2, -x_3)$.

The reader should keep in mind that although these formulas may seem a bit odd, the underlying structure is closely tied to that of the complex numbers. This construction is equivalent to $S^{2,\times}(\mathbb{R}) \cong \mathbb{C}^\times$ with stereographic projection the group isomorphism.

Proof. Given two points $(x_1, x_2, x_3), (y_1, y_2, y_3) \in S^{2,\times}(\mathbb{R})$ we define the expression $(x_1, x_2, x_3) \oplus (y_1, y_2, y_3) = (z_1, z_2, z_3)$ based on the product

$$(10) \quad \frac{x_1 + i x_2}{1 + x_3} \frac{y_1 + i y_2}{1 + y_3} = \frac{z_1 + i z_2}{1 + z_3} \quad \text{where} \quad (z_1, z_2, z_3) \in S^2(\mathbb{R}).$$

Noting that

$$(11) \quad \left| \frac{z_1 + i z_2}{1 + z_3} \right|^2 = \frac{z_1^2 + z_2^2}{(1 + z_3)^2} = \frac{1 - z_3^2}{(1 + z_3)^2} = \frac{1 - z_3}{1 + z_3},$$

we may take norms of both sides to aid in solving for z_3 :

$$(12) \quad \frac{1 - x_3}{1 + x_3} \frac{1 - y_3}{1 + y_3} = \frac{1 - z_3}{1 + z_3} \implies z_3 = \frac{x_3 + y_3}{1 + x_3 y_3};$$

(showing in particular that $z_3 \neq \pm 1$) while considering real and imaginary parts to aid in solving for z_1 and z_2 :

$$(13) \quad z_1 = \frac{x_1 y_1 - x_2 y_2}{1 + x_3 y_3} \quad \text{and} \quad z_2 = \frac{x_1 y_2 + x_2 y_1}{1 + x_3 y_3}.$$

The statements about \oplus being associative and commutative follow from associativity and commutativity of multiplication on the complex numbers. The point $(1, 0, 0) \mapsto 1$ under stereographic projection, and

$$(14) \quad (x_1, -x_2, -x_3) \mapsto \frac{x_1 - i x_2}{1 - x_3} = \frac{x_1^2 + x_2^2}{x_1 + i x_2} \frac{1 + x_3}{1 - x_3^2} = \left(\frac{x_1 + i x_2}{1 + x_3} \right)^{-1}$$

thereby verifying the statements about the identity and the inverse. \square

3. FACTORIZATION ON THE RATIONAL UNIT SPHERE

The formulas in Theorem 2.1 are rational, so $S^{2,\times}(k) = S^{2,\times}(\mathbb{R}) \cap k^3$ is a subgroup for any subfield k of \mathbb{R} . In particular, we focus on the case when $k = \mathbb{Q}$, where we have the rational part of the ‘‘poleless’’ unit sphere:

$$(15) \quad S^{2,\times}(\mathbb{Q}) = \{(x_1, x_2, x_3) \in \mathbb{Q}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1, x_3 \neq \pm 1\}.$$

For example, both $(0, \frac{4}{5}, \frac{3}{5})$ and $(\frac{2}{11}, \frac{6}{11}, \frac{9}{11})$ are such rational points, and in fact

$$(16) \quad \begin{aligned} \left(0, \frac{4}{5}, \frac{3}{5}\right) &= \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right) \oplus \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right), \\ \left(\frac{2}{11}, \frac{6}{11}, \frac{9}{11}\right) &= \left(\frac{2}{3}, \frac{1}{3}, \frac{2}{3}\right) \oplus \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right). \end{aligned}$$

This motivates the concept of ‘‘factorization’’ but first we need a way to measure when one point is ‘‘larger’’ than another.

Definition 3.1. Write $P = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) \in S^{2,\times}(\mathbb{Q})$ with a, b, c, d integers having no common factors. We define $h(P) = |d|$ as the height of P . Write $P = P_1 \oplus P_2$ with $P_1, P_2 \in S^{2,\times}(\mathbb{Q})$. We say that P is reducible if $h(P_1), h(P_2) < h(P)$; and irreducible if no such P_1, P_2 exist.

As $S^{2,\times}(\mathbb{Q})$ is a group, we can always find P_2 such that $P = P_1 \oplus P_2$ given P and P_1 . The importance of reducibility is in bounding the heights of P_1 and P_2 .

Proposition 3.2. Write $P = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$ as in 3.1.

1. $h(P)$ is odd.
2. If $h(P) \leq 3$ then P is irreducible.
3. If $h(P) > 3$ and $c + d$ is a multiple of 4 then P is reducible.

Given an odd integer $d = 2m + 1$, we can always find a point $P \in S^{2,\times}(\mathbb{Q})$ such that $h(P) = |d|$. This is equivalent to expressing $d^2 = 8\frac{m^2+m}{2} + 1 = a^2 + b^2 + c^2$ as the sum of three integral squares, a result which was known to Legendre; see [Dav99, pg. 127] and [Gau86, article 291].

Proof. Since P is a point on the unit sphere, $a^2 + b^2 + c^2 = d^2$. Assume that $h(P) = |d|$ is even so that $a^2 + b^2 + c^2$ is a multiple of 4. This happens only when a, b, c are even as well, which contradicts the assumption that a, b, c, d are coprime. Hence, $h(P)$ must be odd.

Now assume that P is reducible with $h(P) \leq 3$. From the definitions, if $h(P) = 1$, then P is irreducible; from the above result, $h(P) = 2$ is not possible, so $h(P) = 3$. Then there exist P_1, P_2 each of height 1 such that $P = P_1 \oplus P_2$. The only points of height 1 are $(\pm 1, 0, 0)$ and $(0, \pm 1, 0)$ – corresponding to ± 1 and $\pm i$ under stereographic projection – and these points are closed under \oplus so P must be of height 1 as well, a contradiction.

Finally assume that $d > 3$ and $c + d = 4n$. Since $(a + b)^2 = 2ab + 4n(d - c)$, the sum $a + b = 2m$ is even as well. Define $P_1 = \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right) \in S^{2,\times}(\mathbb{Q})$ and

$$(17) \quad P_2 = P \oplus [-1]P_1 = \left(\frac{m}{d-n}, \frac{m-a}{d-n}, \frac{3n-d}{d-n}\right).$$

Then $P = P_1 \oplus P_2$ and $h(P) = d > 3 = h(P_1)$ so it remains to show that $h(P_2) < d$ as well. Clearly $|c| < \sqrt{a^2 + b^2 + c^2} = d$ so $0 < n < d/2$; that is, $\frac{3n-d}{d-n} \neq \pm 1$ so that $P_2 \in S^{2,\times}(\mathbb{Q})$ and $h(P_2) \leq d - n < d$ as desired. \square

The condition that $c + d$ be a multiple of 4 is a bit strong. In fact, there are irreducible points P where $h(P) > 3$; take for example $\left(\frac{2}{7}, \frac{3}{7}, \frac{6}{7}\right)$. To remedy this, we consider instead a “conjugacy class” which can always be factored.

Definition 3.3. Let $P = (x_1, x_2, x_3) \in S^{2,\times}(\mathbb{Q})$. Denote the conjugacy class of P as the set

$$(18) \quad \{P\} = \{(\pm x_{\sigma(1)}, \pm x_{\sigma(2)}, \pm x_{\sigma(3)}) \mid \sigma \in \text{Sym}(3)\} \cap S^{1,\times}(\mathbb{Q}).$$

We say that $\{P\}$ is reducible if there is a representative $P_0 \in \{P\}$ such that P_0 is reducible; and irreducible if no such P_0 exists.

For instance, while $\left(\frac{2}{7}, \frac{3}{7}, \frac{6}{7}\right)$ is irreducible as a point, $\left\{\left(\frac{2}{7}, \frac{3}{7}, \frac{6}{7}\right)\right\}$ is reducible as a conjugacy class:

$$(19) \quad \left\{\left(\frac{2}{7}, \frac{3}{7}, \frac{6}{7}\right)\right\} = \left\{\left(\frac{2}{7}, \frac{6}{7}, -\frac{3}{7}\right)\right\} = \left\{\left(\frac{2}{3}, \frac{1}{3}, -\frac{2}{3}\right) \oplus \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right)\right\}.$$

This motivates the main result of this section.

Theorem 3.4. *Let $P \in S^{2,\times}(\mathbb{Q})$.*

1. $h(P)$ is independent of the choice of representative of $\{P\}$.
2. If $h(P) \leq 3$ then $\{P\}$ is irreducible.
3. If $h(P) > 3$ then $\{P\}$ is reducible.

The conjugacy class $\{P\}$ is just a fancy way to say we don't care about the ordering or signs of the coordinates. The only points P with $h(P) = 1$ correspond to the class $\{(1, 0, 0)\}$ while the only points with $h(P) = 3$ correspond to $\{(\frac{1}{3}, \frac{2}{3}, \frac{2}{3})\}$. An equivalent way to say a class $\{P\}$ is reducible is to say there are rational points P_1 and P_2 each with height less than that of P such that $\{P\} = \{P_1 \oplus P_2\}$.

Proof. Write $P = (\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ as in 3.1 so that $h(P) = |d|$. Then $\{P\}$ simply consists of permutations and sign changes of the coordinates, and each representative $P_0 \in \{P\}$ has the same denominator d . Hence $h(P_0) = |d|$ as well.

If $h(P) \leq 3$ then $h(P_0) \leq 3$ for each representative P_0 . Each P_0 is irreducible by 3.2 so the statement follows.

Now assume that $h(P) > 3$. By Proposition 3.2, $d = 2m + 1$ is odd, and not all of a, b, c , are even so choose a representative $P_0 = (\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ with $c = 2n + 1$ odd as well. Note that $c + d = 2(m + n + 1)$ and $-c + d = 2(m + n) - 4n$ so choose the sign of c so that $c + d$ is a multiple of 4; this can be done because either $m + n$ or $m + n + 1$ is even. Then by Proposition 3.2, P_0 is reducible, so by definition $\{P\}$ is reducible. \square

4. FACTORIZATION OF PYTHAGOREAN QUADRUPLETS

We now consider the composition of maps

$$(20) \quad (a, b, c, d) \mapsto \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d} \right) \mapsto \frac{a + ib}{c + d}$$

to gain more information about the multiplicative nature of Pythagorean Quadruplets. For the sake of completeness, we show how to parametrize all such quadruplets.

Proposition 4.1. *For each Pythagorean Quadruplet (a, b, c, d) there exist integers m, n, p, q such that*

$$(21) \quad a = mnp, \quad b = mnq, \quad c = \frac{m^2 - p^2 - q^2}{2}n, \quad d = \frac{m^2 + p^2 + q^2}{2}n.$$

Proof. If $a = b = c = d = 0$ there is nothing to prove, so assume that $d \neq 0$. Then here exist relatively prime integers m, p, q such that $m(a + ib) = (c + d)(p + iq)$. Considering real and imaginary parts and using the fact that $a^2 + b^2 + c^2 = d^2$ we find that

$$(22) \quad \frac{a}{d} = \frac{2mp}{m^2 + p^2 + q^2}, \quad \frac{b}{d} = \frac{2mq}{m^2 + p^2 + q^2}, \quad \frac{c}{d} = \frac{m^2 - p^2 - q^2}{m^2 + p^2 + q^2};$$

the formulas follow. \square

Now that we know how to factor points on the rational unit sphere, we discuss factorizations of Pythagorean Quadruplets. We begin by discussing ‘‘conjugacy classes.’’

Definition 4.2. Let $\tilde{P} = (a, b, c, d)$ be a nontrivial Pythagorean Quadruplet i.e. integers such that $a^2 + b^2 + c^2 = d^2$ but $c^2 \neq d^2$. Denote the conjugacy class of \tilde{P} as the set

$$(23) \quad \{\tilde{P}\} = \left\{ (a', b', c', d') \in \mathbb{Z}^4 \mid d' \neq 0, \left(\frac{a'}{d'}, \frac{b'}{d'}, \frac{c'}{d'} \right) \in \{P\} \right\}.$$

where $P = (\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$. For any representative $\tilde{P}_0 \in \{\tilde{P}\}$ define the height $h(\tilde{P}_0)$ as the height of a representative $P_0 \in \{P\}$. We say that $\{\tilde{P}\}$ is reducible (irreducible, respectively) if $\{P\}$ is reducible (irreducible, respectively).

We present a more intuitive way to view this definition of conjugacy class. If $\tilde{P} = (a, b, c, d)$ and n is the greatest common divisor of a, b, c, d , set $\tilde{P}_0 = (\frac{a}{n}, \frac{b}{n}, \frac{c}{n}, \frac{d}{n})$. Then $\{\tilde{P}\}$ is the collection of all scalar multiples of \tilde{P}_0 where we allow sign changes and permutations $a \leftrightarrow b, a \leftrightarrow c, b \leftrightarrow c$ as well. For example, the Pythagorean Quadruplets with height either 3, 5, or 7 generate the classes $\{(1, 2, 2, 3)\}, \{(0, 3, 4, 5)\}$, and $\{(2, 3, 6, 7)\}$; a fact which corresponds to the identities $1^2 + 2^2 + 2^2 = 3^2$, $3^2 + 4^2 = 5^2$, and $2^2 + 3^2 + 6^2 = 7^2$.

We may now state the main result of the paper.

Theorem 4.3. Let $\tilde{P} = (a, b, c, d)$ be a nontrivial Pythagorean Quadruplet, and define the operation \oplus as

$$(24) \quad \begin{aligned} (a_1, b_1, c_1, d_1) \oplus (a_2, b_2, c_2, d_2) \\ = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1, c_1 d_2 + c_2 d_1, c_1 c_2 + d_1 d_2). \end{aligned}$$

1. This makes such quadruplets into a commutative monoid, with identity $\tilde{O} = (1, 0, 0, 1)$.
2. If $h(\tilde{P}) > 3$, there exist Pythagorean Quadruplets \tilde{P}_1, \tilde{P}_2 of height less than $h(\tilde{P})$ such that $\{\tilde{P}\} = \{\tilde{P}_1 \oplus \tilde{P}_2\}$. If $h(\tilde{P}) \leq 3$, then no such quadruplets exist.
3. $\{\tilde{P}\}$ is reducible if and only if $h(\tilde{P}) > 3$.

The operation \oplus may also be realized through the map defined by

$$(25) \quad \mu : \mathbb{Z}^4 \rightarrow \text{Mat}_4(\mathbb{Z}), \quad (a, b, c, d) \mapsto \begin{pmatrix} a & -b & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & d & c \\ 0 & 0 & c & d \end{pmatrix}.$$

Then $\mu(\tilde{P}_1 \oplus \tilde{P}_2) = \mu(\tilde{P}_1) \cdot \mu(\tilde{P}_2)$ is the product of the matrices, $\mu(\tilde{O})$ is the identity matrix, and the nontrivial Pythagorean Quadruplets correspond to the submonoid of the image defined by $\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \det \begin{pmatrix} d & c \\ c & d \end{pmatrix} \neq 0$.

Proof. The results follow directly from Theorems 2.1 and 3.4 via the mapping $(a, b, c, d) \mapsto (\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$. \square

REFERENCES

- [Con78] John B. Conway. *Functions of one complex variable*. Springer-Verlag, New York, second edition, 1978.
- [Dav99] J. H. Davenport. *The higher arithmetic*. Cambridge University Press, Cambridge, seventh edition, 1999. An introduction to the theory of numbers, Chapter VIII by J. H. Davenport.

- [Gau86] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

CALIFORNIA INSTITUTE OF TECHNOLOGY, MATHEMATICS 253-37, PASADENA, CA 91125
E-mail address: `goins@caltech.edu`

GREENVILLE COLLEGE, 315 E. COLLEGE AVENUE, P.O. BOX 159, GREENVILLE, IL 62246
E-mail address: `atogbe@greenville.edu`