PYTHAGOREAN TRIPLES, COMPLEX NUMBERS, ABELIAN GROUPS AND PRIME NUMBERS

AMNON YEKUTIELI

Abstract. It is well-known that pythagorean triples can be represented by points of the unit circle with rational coordinates. These points form an abelian group, and we describe its structure. This structural description yields, almost immediately, an enumeration of the normalized pythagorean triples with a given hypotenuse, and also to an effective method for producing all such triples. This effective method seems to be new.

This paper is intended for the general mathematical audience, including undergraduate mathematics students, and therefore it contains plenty of background material, some history and several examples and exercises.

Contents

1. Pythagorean Triples

A *pythagorean triple* is a triple (a, b, c) of positive integers satisfying the equation

$$a^2 + b^2 = c^2. \tag{1.1}$$

The reason for the name is, of course, because of the Pythagoras Theorem, which says that the sides of a right angled triangle, with base a, height b and hypotenuse c, satisfy this equation. See Figure 1.

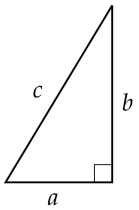

Figure 1. Right angled triangle, with base a, height b and hypotenuse c.

Date: 28 January 2021.

We say that two triples (a, b, c) and (a', b', c') are *equivalent* if the corresponding triangles are similar. Numerically this means that there is a positive number r, such that

$$(a', b', c') = (r \cdot a, r \cdot b, r \cdot c)$$

or

$$(a', b', c') = (r \cdot b, r \cdot a, r \cdot c).$$

See Figure 2. Clearly the number r is rational.

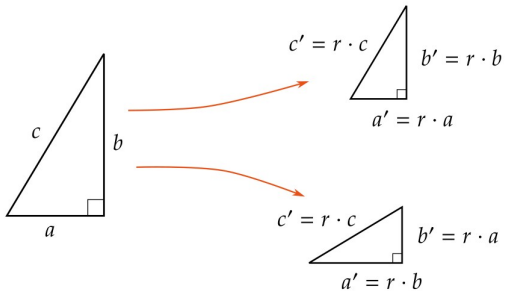

FIGURE 2. Similar right angled triangles.

Definition 1.2. We say that a pythagorean triple (a, b, c) is *normalized* if the greatest common divisor of these three numbers is 1, and $a \leq b$.

It is easy to see that every pythagorean triple (a, b, c) is equivalent to exactly one normalized triple (a', b', c'). For this reason we shall be mostly interested in normalized pythagorean triples.

Exercise 1.3. Let (a, b, c) be a normalized pythagorean triple. Show that c is odd, and $a < b$.

Here is an interesting question:

Question 1.4. Are there infinitely many normalized pythagorean triples?

The answer is *yes*. This fact was already known to the ancient Greeks. There is a formula attributed to Euclid for presenting all pythagorean triples, and it proves that there are infinitely many normalized triples. This formula is somewhat clumsy, and I will not display it. It can be found in many sources, including [Tk, Chapter 3], or online at [Wi1] or [Wo]. Later we will give a geometric argument showing that there are infinitely many normalized pythagorean triples. As explained in Remark 2.7, this geometric argument secretly relies on Euclid's formula.

Definition 1.5. Let us denote by PT the set of all normalized pythagorean triples, and for each integer $c > 1$ let PT_c be the set of normalized pythagorean triples with hypotenuse c.

Thus we obtain a partition $\mathrm{PT} = \coprod_{c>1} \mathrm{PT}_c$. A restatement of Question 1.4 is this: Is the set PT infinite? The next obvious question is:

Question 1.6. For which c is the set PT_c nonempty?

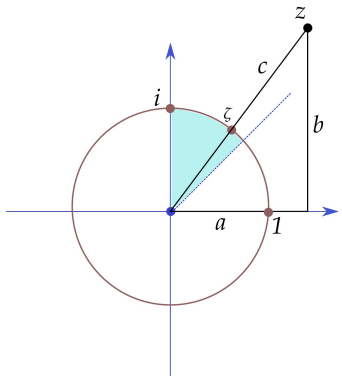

FIGURE 3. The number ζ in the second octant of the unit circle.

Exercise 1.3 shows that $\mathrm{PT}_c = \varnothing$ if c is even. Next is a quantitative variant of Question 1.6.

Question 1.7. What is the size of the set PT_c ?

The answer to this question was found in the 19th century, by Gauss. We will see it later in the article, in Corollary 5.8. An even more interesting question is the next one.

Question 1.8. Given c, is there an *effective* way to find the elements of PT_c ?

An effective method will be presented below, in Theorem 5.3.

2. From Pythagorean Triples to the Rational Unit Circle

It was observed a long time ago that pythagorean triples can be encoded as *complex numbers on the unit circle*.

Starting from a normalized pythagorean triple (a, b, c), we pass to the complex number

$$z := a + b \cdot \boldsymbol{i}, \tag{2.1}$$

which has absolute value $|z| = \sqrt{a^2 + b^2} = c$. Next we introduce the complex number

$$\zeta = s + t \cdot \boldsymbol{i} := \frac{z}{|z|} = \frac{a}{c} + \frac{b}{c} \cdot \boldsymbol{i}. \tag{2.2}$$

The number ζ has rational coordinates, and it is on the unit circle, in the second octant. See Figure 3. We can recover the number z, and thus the normalized pythagorean triple (a, b, c), by clearing the denominators from the pair of rational numbers $(s, t) = (\frac{a}{c}, \frac{b}{c})$.

Actually, there are 8 different points on the unit circle that encode the same pythagorean triple:

$$\pm\zeta,\ \pm\boldsymbol{i}\cdot\zeta,\ \pm\bar{\zeta},\ \pm\boldsymbol{i}\cdot\bar{\zeta}. \tag{2.3}$$

See Figure 4. These points can be obtained from ζ as follows. Let Γ be the group of symmetries of the circle generated by the two operations $\zeta \mapsto \boldsymbol{i}\cdot\zeta$ and $\zeta \mapsto \bar{\zeta}$. This is a nonabelian group of order 8 (a dihedral group), and we shall call it the *group of pythagorean symmetries of the circle*. The points in (2.3) are the orbit of the point ζ under the action of the group Γ.

Definition 2.4. Given a complex number $\zeta = s + t\cdot\boldsymbol{i}$ on the unit circle, with rational coordinates (s, t), and which does not belong to $\{\pm 1, \pm\boldsymbol{i}\}$, let us denote by $\mathrm{pt}(\zeta)$ the unique normalized pythagorean triple (a, b, c) that ζ encodes.

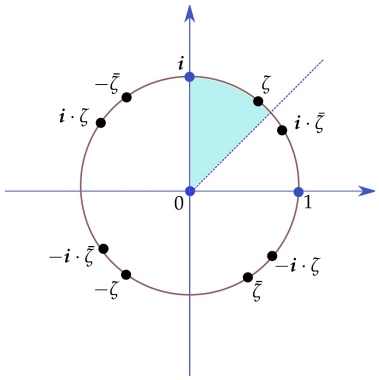

FIGURE 4. The number ζ in the second octant, and its orbit under the action of the group Γ of pythagorean symmetries of the circle.

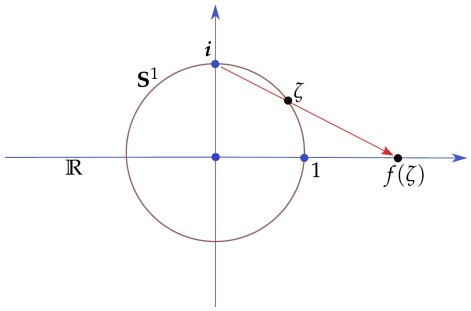

FIGURE 5. The stereographic projection with focus at $\boldsymbol{i}$.

In other words, given ζ, we first move it to the second octant by an element of the group Γ. For ζ in the second octant we have $\mathrm{pt}(\zeta) = (a, b, c)$ as in formula (2.2).

The function pt is a surjection from the set of points on the unit circle with rational coordinates, excluding the four special points $\{\pm 1, \pm \boldsymbol{i}\}$, to the set PT of normalized pythagorean triples. The fibers of the function pt are the orbits of the group Γ, and each fiber has cardinality 8.

Let's summarize what we have established so far:

Proposition 2.5. *The following assertions are equivalent*:

(i) *There are infinitely many normalized pythagorean triples.*
(ii) *There are infinitely many points on the unit circle with rational coordinates.*

Here is a geometric proof of assertion (ii) in the proposition above. Let us denote the unit circle by $\mathbf{S}^1$. The stereographic projection with focus at $\boldsymbol{i}$ is the bijective function $f : \mathbf{S}^1 - \{\boldsymbol{i}\} \to \mathbb{R}$, which sends the point $\zeta \in \mathbf{S}^1 - \{\boldsymbol{i}\}$ to the unique point $f(\zeta) \in \mathbb{R}$ that lies on the straight line connecting $\boldsymbol{i}$ and ζ. See Figure 5.

Exercise 2.6. Show that the point $\zeta \in \mathbf{S}^1 - \{\boldsymbol{i}\}$ has rational coordinates iff the number $f(\zeta) \in \mathbb{R}$ is rational. (Hint: Use similar triangles.)

Since there are infinitely many rational numbers, we are done. This answers Question 1.4 positively.

Remark 2.7. Here is an algebro-geometric explanation why the stereographic projection f sends rational points to rational points. This remark can be safely ignored by readers not familiar with the theory of schemes.

Consider the affine plane over $\mathbb{Q}$, which is the affine scheme $\mathbf{A}^2_{\mathbb{Q}} = \mathrm{Spec}(\mathbb{Q}[s,t])$. Let $X \subseteq \mathbf{A}^2_{\mathbb{Q}}$ be the closed subscheme whose ideal is generated by the polynomial $s^2 + t^2 - 1$. The set $X(\mathbb{R})$ of $\mathbb{R}$-valued points of X is the circle $\mathbf{S}^1$, and the set $X(\mathbb{Q})$ is precisely the set of points in $\mathbf{S}^1$ with rational coordinates.

Let $X' \subseteq X$ be the open subscheme defined by the nonvanishing of the polynomial $t - 1$. Let $f : X' \to \mathbf{A}^1_{\mathbb{Q}} = \mathrm{Spec}(\mathbb{Q}[s])$ be the map of affine $\mathbb{Q}$-schemes whose formula is $f^*(s) := s/(1-t)$. On $\mathbb{R}$-valued points the function

$$f : X'(\mathbb{R}) = \mathbf{S}^1 - \{\boldsymbol{i}\} \to \mathbf{A}^1(\mathbb{R}) = \mathbb{R}$$

is the stereographic projection. It turns out that f is an isomorphism of $\mathbb{Q}$-schemes, and the formula for its inverse $g : \mathbf{A}^1_{\mathbb{Q}} \to X'$ involves the classical expressions of Euclid. See [Wi1]. Since $f : X' \to \mathbf{A}^1_{\mathbb{Q}}$ is an isomorphism of $\mathbb{Q}$-schemes, it induces a bijection $f : X'(\mathbb{Q}) \to \mathbf{A}^1(\mathbb{Q}) \cong \mathbb{Q}$.

3. The Rational Unit Circle as an Abelian Group

Previously we used the notation $\mathbf{S}^1$ for the unit circle. We will now switch to another notation, which is is better suited for our purposes. From now on we shall write

$$G(\mathbb{R}) := \mathbf{S}^1 = \{\zeta \in \mathbb{C} \mid |\zeta| = 1\}. \tag{3.1}$$

Note that the set $G(\mathbb{R})$ is a group whose operation is complex multiplication, because $|\zeta_1 \cdot \zeta_2| = |\zeta_1| \cdot |\zeta_2|$ and $|\zeta^{-1}| = |\zeta|^{-1}$.

Let $G(\mathbb{Q})$ be the subset of $G(\mathbb{R})$ consisting of points with rational coordinates; namely

$$G(\mathbb{Q}) = \{\zeta = s + t \cdot \boldsymbol{i} \mid s, t \in \mathbb{Q},\ s^2 + t^2 = 1\}. \tag{3.2}$$

Exercise 3.3. Prove that $G(\mathbb{Q})$ is a subgroup of $G(\mathbb{R})$. (Hint: Inspect the formulas for multiplication and inversion of complex numbers.)

In Remark 3.6 we explain what lies behind this choice of new notation.

Recall that to answer Question 1.4, namely to show there are infinitely many normalized pythagorean triples, it suffices to prove that the abelian group $G(\mathbb{Q})$ is infinite. This is by Proposition 2.5.

We first identify all the elements of finite order in the group $G(\mathbb{Q})$. These are the roots of 1, namely the elements $\zeta \in G(\mathbb{Q})$ satisfying $\zeta^n = 1$ for some positive integer n. Algebraic number theory tells us that there are just four of them: $1, \boldsymbol{i}, -1, -\boldsymbol{i}$. See [Ar, Section 11.2] or [Tk, Section 5.2]. (All the results from algebraic number theory that we need can be found in these books.)

This means that if we take any element $\zeta \in G(\mathbb{Q}) - \{\pm 1, \pm\boldsymbol{i}\}$, the cyclic subgroup that ζ generates, namely the set $\{\zeta^n \mid n \in \mathbb{Z}\} \subseteq G(\mathbb{Q})$, will be infinite!

Let us consider the familiar normalized pythagorean triple $(3, 4, 5)$. The corresponding element in $G(\mathbb{Q})$, by formulas (2.1) and (2.2), is

$$\zeta := \tfrac{3}{5} + \tfrac{4}{5} \cdot \boldsymbol{i}, \tag{3.4}$$

and it does not belong to $\{\pm 1, \pm\boldsymbol{i}\}$. So this element ζ has infinite order in the group $G(\mathbb{Q})$.

This provides us with a second way to answer Question 1.4 affirmatively. But we also get, almost for free, a whole list of new normalized pythagorean triples! See the first positive powers of ζ, and the corresponding triples, in Figure 6. The reader is encouraged

n	ζ^n	$\mathrm{pt}(\zeta^n) = (a_n, b_n, c_n)$
1	$\frac{3}{5} + \frac{4}{5} \cdot \boldsymbol{i}$	$(3, 4, 5)$
2	$-\frac{7}{25} + \frac{24}{25} \cdot \boldsymbol{i}$	$(7, 24, 25)$
3	$-\frac{117}{125} + \frac{44}{125} \cdot \boldsymbol{i}$	$(44, 117, 125)$
4	$-\frac{527}{625} - \frac{336}{625} \cdot \boldsymbol{i}$	$(336, 527, 625)$

FIGURE 6. A list of normalized pythagorean triples.

to verify that these are indeed pythagorean triples. It is clear that they are normalized, since the numbers a_n and b_n are not divisible by 5.

Exercise 3.5. Find a normalized pythagorean triple with hypotenuse $c = 3125$. (Later we will see that there is only one.)

Remark 3.6. Here is another bit of algebraic geometry, which is not required for understanding this paper (yet it did play a role in the discovery of the results).

The unit circle, which in Remark 2.7 was viewed as an affine scheme X, can also be viewed as an affine group scheme G over $\mathbb{Q}$, namely the group $G := \mathrm{SO}_2$. The equality $G(\mathbb{R}) = \mathbf{S}^1$ recovers the group structure of the circle. Looking at the situation this way, it is clear that $G(\mathbb{Q})$ is a subgroup of $G(\mathbb{R})$.

Remark 3.7. After giving a colloquium talk on this topic a few years ago, I was informed that the connection between pythagorean triples and the group $G(\mathbb{Q})$ was already observed by O. Tausski [Ts] in 1970. An inspection of that paper shows that such a connection was made; yet a full understanding of the situation seems to be absent from that paper. In particular, the paper [Ts] does not touch the question of enumeration of pythagorean triples (cf. Corollary 5.8), nor does it give an effective method for their computation (cf. Theorem 5.3 below). Even a list such as in Figure 6 does not appear in that paper.

4. Prime Numbers and the Abelian Group Structure

We have seen that the pythagorean triples are represented by the points of the unit circle with rational coordinates, that we now denote by $G(\mathbb{Q})$. The main result of this section is Theorem 4.15, which describes the structure of the abelian group $G(\mathbb{Q})$ in terms of prime numbers. Getting there requires a few steps, including an understanding of the irreducible elements of the *ring of Gauss integers*

$$\mathbb{Z}[\boldsymbol{i}] := \{m + n \cdot \boldsymbol{i} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{C}. \tag{4.1}$$

All facts we use here can be found in [Ar, Section 11.5] and [Tk, Section 5.4].

When we talk about *prime integers* we mean *positive* prime integers. Let's introduce some notation. The set of prime integers is denoted by P. It is partitioned into

$$P = P_1 \sqcup P_2 \sqcup P_3, \tag{4.2}$$

where

$$P_i := \big\{p \in P \mid p \equiv i \ (\mathrm{mod}\, 4)\big\}. \tag{4.3}$$

Explicitly, $P = \{2, 3, 5, \ldots\}$, $P_1 = \{5, 13, 17, \ldots\}$, $P_2 = \{2\}$ and $P_3 = \{3, 7, 11, \ldots\}$. It is known that the sets P_1 and P_3 are infinite, but this fact is not important for us.

Our first step is to study the prime numbers $p \in P_1$. It turns out that such a prime p can be written as a sum of two squares of integers:

$$p = m^2 + n^2. \tag{4.4}$$

Because p is odd, we must have $|m| \neq |n|$. Therefore, without loss of generality, we can assume that $0 < m < n$. Let us define the complex number

$$q := m + n \cdot \boldsymbol{i}. \tag{4.5}$$

Its conjugate is then

$$\bar{q} = m - n \cdot \boldsymbol{i}. \tag{4.6}$$

Their product is

$$q \cdot \bar{q} = (m + n \cdot \boldsymbol{i}) \cdot (m - n \cdot \boldsymbol{i}) = m^2 + n^2 = p. \tag{4.7}$$

We shall be interested in the quotient

$$\zeta_p := q/\bar{q} \in \mathbb{C}. \tag{4.8}$$

An easy calculation shows that ζ_p has rational coordinates and absolute value 1; thus $\zeta_p \in G(\mathbb{Q})$.

It might appear that the numbers q and $\bar{q}$ above depend on our choice of m and n. However, by the classification of the irreducible elements of the ring $\mathbb{Z}[\boldsymbol{i}]$, which we are going to recall below, it follows that there is exactly one irreducible divisor q of p in the ring $\mathbb{Z}[\boldsymbol{i}]$ that sits in the second octant, and this is the number q in formula (4.5).

Example 4.9. Take the prime $p = 5$. It satisfies $5 = 1^2 + 2^2$, so by our convention above we have $m = 1, n = 2$, $q = 1 + 2 \cdot \boldsymbol{i}$ and $\bar{q} = 1 - 2 \cdot \boldsymbol{i}$. The resulting element of $G(\mathbb{Q})$ is $\zeta_5 = q/\bar{q} = -\frac{3}{5} + \frac{4}{5} \cdot \boldsymbol{i}$.

Note that ζ_5 does not coincide with the number $\zeta = \frac{3}{5} + \frac{4}{5} \cdot \boldsymbol{i}$ from equation (3.4). However, they are in the same orbit under the action of the group Γ of pythagorean symmetries of the circle: $\zeta_5 = -\bar{\zeta}$. So they represent the same normalized pythagorean triple, which is $(3, 4, 5)$.

Our next step is to study some properties of the ring $\mathbb{Z}[\boldsymbol{i}]$. It is known that this ring is a *principal ideal domain*, and therefore it is a *unique factorization domain*. Let U be the group of invertible elements of $\mathbb{Z}[\boldsymbol{i}]$, and let Q be a complete set of irreducible elements of $\mathbb{Z}[\boldsymbol{i}]$; to be precise, we choose one representative $q \in Q$ from every coset $U \cdot q$ of irreducible elements. Every nonzero element $z \in \mathbb{Z}[\boldsymbol{i}]$ has a unique factorization

$$z = u \cdot \prod_{i=1,\ldots,k} q_i^{e_i} \tag{4.10}$$

where $u \in U$, $k \geq 0$, $(q_1, \ldots, q_k)$ is a sequence of distinct elements of Q, and the multiplicities are $e_i \geq 1$. The uniqueness of the factorization (4.10) is up to a permutation of the sequence $(1, \ldots, k)$.

The group of invertible elements of $\mathbb{Z}[\boldsymbol{i}]$ is

$$U = \{1, \boldsymbol{i}, -1, -\boldsymbol{i}\}. \tag{4.11}$$

The irreducible elements of $\mathbb{Z}[\boldsymbol{i}]$ are of three types, according to the partition (4.2) of P.

- (P_1) For every prime integer $p \in P_1$, the numbers q and $\bar{q}$ from formulas (4.5) and (4.6) are irreducible in $\mathbb{Z}[\boldsymbol{i}]$, and they are not equivalent, namely $U \cdot q \neq U \cdot \bar{q}$.
- (P_2) The number $1 + \boldsymbol{i}$ is irreducible in $\mathbb{Z}[\boldsymbol{i}]$.
- (P_3) Every prime integer $p \in P_3$ is irreducible in $\mathbb{Z}[\boldsymbol{i}]$.

In the next definition we are going to select a particular set of representatives Q of the irreducible elements of $\mathbb{Z}[\boldsymbol{i}]$, according to the three types above.

Definition 4.12. Define the complete set of irreducible elements Q of $\mathbb{Z}[\boldsymbol{i}]$ to be

$$Q := Q_1 \sqcup \bar{Q}_1 \sqcup Q_2 \sqcup Q_3$$

where:

(1) For every $p \in P_1$, the element q from (4.5) associated to p belongs to Q_1, and the element $\bar{q}$ from (4.6) belongs to $\bar{Q}_1$. These are all the elements in $Q_1 \sqcup \bar{Q}_1$.
(2) $Q_2 := \{1 + \boldsymbol{i}\}$.
(3) $Q_3 := P_3$.

Note that the functions $p \mapsto q$ and $p \mapsto \bar{q}$, from formulas (4.5) and (4.6) respectively, are bijections $P_1 \xrightarrow{\simeq} Q_1$ and $P_1 \xrightarrow{\simeq} \bar{Q}_1$.

It will be important to know the absolute values of the elements of Q. An element $q \in Q_1$, and its conjugate $\bar{q} \in \bar{Q}_1$, have $|q| = |\bar{q}| = \sqrt{p}$, where $p = q \cdot \bar{q} \in P_1$. The element $q = 1 + \boldsymbol{i} \in Q_2$ has $|q| = \sqrt{2}$. And an element $q = p \in Q_3 = P_3$ has $|q| = p$.

The field of fractions of $\mathbb{Z}[\boldsymbol{i}]$ is

$$\mathbb{Q}[\boldsymbol{i}] := \{s + t \cdot \boldsymbol{i} \mid s, t \in \mathbb{Q}\} \subseteq \mathbb{C}. \tag{4.13}$$

Like (4.10), every nonzero element $z \in \mathbb{Q}[\boldsymbol{i}]$ has a unique factorization

$$z = u \cdot \prod_{i=1,\ldots,k} q_i^{e_i} \tag{4.14}$$

where $u \in U$, $k \geq 0$, $(q_1, \ldots, q_k)$ is a sequence of distinct elements of Q, but now the multiplicities e_i are nonzero integers.

As shown in formula (4.8), to each $p \in P_1$ we assign a number $\zeta_p \in G(\mathbb{Q})$. In this way we obtain a collection $\{\zeta_p\}_{p \in P_1}$ of elements of $G(\mathbb{Q})$.

Theorem 4.15. *The abelian group $G(\mathbb{Q})$ decomposes into a product*

$$G(\mathbb{Q}) = U \times F,$$

where $U = \{\pm 1, \pm \boldsymbol{i}\}$, and F is a free abelian group with basis the collection $\{\zeta_p\}_{p \in P_1}$.

Proof. We begin by noting that $G(\mathbb{Q}) = \mathbb{Q}[\boldsymbol{i}] \cap G(\mathbb{R})$, or in other words

$$G(\mathbb{Q}) = \{z \in \mathbb{Q}[\boldsymbol{i}] \mid |z| = 1\}.$$

Take an element $z \in G(\mathbb{Q})$. Being a nonzero element of $\mathbb{Q}[\boldsymbol{i}]$, it has its unique factorization (4.14). It will be useful for us to alter the factorization (4.14), by inserting more factors from the set Q of irreducible elements, with multiplicities 0, and then to rearrange to product. The new factorization is this:

$$z = u \cdot (1 + \boldsymbol{i})^c \cdot r_1^{d_1} \cdots r_l^{d_l} \cdot (q_1^{e_1} \cdot \bar{q}_1^{e'_1}) \cdots (q_k^{e_k} \cdot \bar{q}_k^{e'_k}). \tag{4.16}$$

Here $u \in U$; $r_1, \ldots, r_l$ are distinct elements of Q_3; $q_1, \ldots, q_k$ are distinct elements of Q_1; and $\bar{q}_1, \ldots, \bar{q}_k \in \bar{Q}_1$ are the conjugates of the q_i, in the same order. The multiplicities $c, d_1, \ldots, d_l, e_1, \ldots, e_k, e'_1, \ldots, e'_k$ are allowed to be 0.

We now examine what the condition $|z| = 1$ imposes on the factorization (4.16). Recall that $|u| = 1$, $|1 + \boldsymbol{i}| = \sqrt{2}$, $|r_i| = r_i$, and $|q_i| = |\bar{q}_i| = \sqrt{p_i}$, where $p_i = q_i \cdot \bar{q}_i$. It is better to work with z^2. We get:

$$1 = |z^2| = 1 \cdot 2^c \cdot r_1^{2 \cdot d_1} \cdots r_l^{2 \cdot d_l} \cdot (p_1^{e_1} \cdot p_1^{e'_1}) \cdots (p_k^{e_k} \cdot p_k^{e'_k}). \tag{4.17}$$

Because the integer primes $2, r_1, \ldots, r_l, p_1, \ldots, p_k$ are all distinct, we conclude that $c = 0$, $d_i = 0$ and $e_i' = -e_i$. This means that in the product (4.16) we can erase all the factors that belong to $Q_2 \cup Q_3$, and also all the factors q_i and $\bar{q}_i$ that belong to $Q_1 \cup \bar{Q}_1$ whose multiplicities are $e_i = e_i' = 0$. Next, for every i such that $e_i \neq 0$ we have $q_i^{e_i} \cdot \bar{q}_i^{e_i'} = q_i^{e_i} \cdot \bar{q}_i^{-e_i} = \zeta_{p_i}^{e_i}$, see formula (4.8). Therefore, after renumbering the remaining factors in (4.16), and setting a new value for k, we obtain the factorization

$$z = u \cdot \zeta_{p_1}^{e_1} \cdots \zeta_{p_k}^{e_k} \tag{4.18}$$

with $u \in U$, $k \geq 0$, $p_1, \ldots, p_k$ distinct elements of P_1, and the multiplicities e_i are nonzero integers. The factorization (4.18) is unique up to a permutation of $(1, \ldots, k)$. This establishes the decomposition $G(\mathbb{Q}) = U \times F$. □

Remark 4.19. Theorem 4.15 is related to the easy form of Hilbert's Theorem 90, which says that every element $\zeta \in G(\mathbb{Q})$ satisfies $\zeta = z/\bar{z}$ for some $z \in \mathbb{Q}[\boldsymbol{i}]$. See [Wi2].

5. Back to Pythagorean Triples

Recall that $G(\mathbb{Q})$ is the group of points on the unit circle with rational coordinates, $U = \{\pm 1, \pm \boldsymbol{i}\} \subseteq G(\mathbb{Q})$, and for every point $\zeta \in G(\mathbb{Q}) - U$ we write $\mathrm{pt}(\zeta)$ for the corresponding normalized pythagorean triple. The set of integer primes congruent to 1 modulo 4 is denoted by P_1. For each $p \in P_1$ we assigned the element $\zeta_p \in G(\mathbb{Q})$, see (4.8).

Lemma 5.1. *Let k be a positive integer, let $p_1, \ldots, p_k$ be distinct primes in P_1, let $n_1, \ldots, n_k$ be nonzero integers, let $\epsilon_1, \ldots, \epsilon_k \in \{\pm 1\}$, and let*

$$(a, b, c) := \mathrm{pt}\big(\zeta_{p_1}^{\epsilon_1 \cdot n_1} \cdots \zeta_{p_k}^{\epsilon_k \cdot n_k}\big) \in \mathrm{PT}\,.$$

Then $c = p_1^{n_1} \cdots p_k^{n_k}$.

Proof. Let's write $\zeta := \zeta_{p_1}^{\epsilon_1 \cdot n_1} \cdots \zeta_{p_k}^{\epsilon_k \cdot n_k}$. For every i define

$$\tilde{q}_i := \begin{cases} q_i & \text{if } \epsilon_i = 1 \\ \bar{q}_i & \text{if } \epsilon_i = -1. \end{cases}$$

Consider the numbers $c' := p_1^{n_1} \cdots p_k^{n_k}$ and $z := c' \cdot \zeta$. For every i we have

$$p_i^{n_i} \cdot \zeta_{p_i}^{\epsilon_i \cdot n_i} = (q_i \cdot \bar{q}_i)^{n_i} \cdot (q_i / \bar{q}_i)^{\epsilon_i \cdot n_i} = \tilde{q}_i^{\,2 \cdot n_i},$$

and therefore

$$z = \tilde{q}_1^{\,2 \cdot n_1} \cdots \tilde{q}_k^{\,2 \cdot n_k}. \tag{5.2}$$

We see that $z \in \mathbb{Z}[\boldsymbol{i}]$, so we can express it uniquely as $z = a' + b' \cdot \boldsymbol{i}$ with $a', b' \in \mathbb{Z}$. Since $\zeta \notin U$ and $z = c' \cdot \zeta$, it follows that $\bar{z} \neq z$ and $\bar{z} \neq -z$, and therefore a' and b' are nonzero. Moreover, $|z| = c'$. We conclude that (a', b', c') is a pythagorean triple.

We claim that the triple (a', b', c') is reduced, namely the greatest common divisor of these three numbers in $\mathbb{Z}$ is 1. The prime divisors of c' in $\mathbb{Z}$ are $p_1, \ldots, p_k$. Suppose some p_i divides both a' and b'. Then $a' = a'' \cdot p_i$ and $b' = b'' \cdot p_i$ for some $a'', b'' \in \mathbb{Z}$. This will give $z = p_i \cdot (a'' + b'' \cdot \boldsymbol{i})$ in $\mathbb{Z}[\boldsymbol{i}]$. But both irreducibles q_i and $\bar{q}_i$ divide p_i in $\mathbb{Z}[\boldsymbol{i}]$, and this implies that q_i and $\bar{q}_i$ both divide z. This is in contradiction to the decomposition (5.2) of z into irreducibles.

At this point we know that either (a', b', c') or (b', a', c') is a normalized pythagorean triple, and this is the triple $(a, b, c) = \mathrm{pt}(\zeta)$. In any case $c = c'$. □

Theorem 5.3. *Let c be an integer greater than 1, with prime decomposition*

$$c = p_1^{n_1} \cdots p_k^{n_k}$$

in $\mathbb{Z}$. Here $p_1, \ldots, p_k$ are distinct prime integers; $n_1, \ldots, n_k$ are positive integers; and k is a positive integer.

(1) *If $p_i \equiv 1 \pmod 4$ for every index i, then the function* pt *restricts to a bijection*

$$\text{pt} : \left\{ \zeta_{p_1}^{n_1} \cdot \zeta_{p_2}^{\epsilon_2 \cdot n_2} \cdots \zeta_{p_k}^{\epsilon_k \cdot n_k} \;\middle|\; \epsilon_2, \ldots, \epsilon_k \in \{\pm 1\} \right\} \xrightarrow{\simeq} \text{PT}_c \,.$$

Here ζ_{p_i} is the number defined in formula (4.8) for the prime p_i.

(2) *Otherwise, the set PT_c is empty.*

Proof. Consider the set $G(\mathbb{Q}) - U$, the complement of the subgroup U in the group $G(\mathbb{Q})$. We know that the function

$$\text{pt} : G(\mathbb{Q}) - U \to \text{PT} \tag{5.4}$$

is surjective, and its fibers are orbits of the group Γ of pythagorean symmetries. Thus, passing to the quotient set, we get a bijection

$$\text{pt} : \big(G(\mathbb{Q}) - U\big)/\Gamma \xrightarrow{\simeq} \text{PT}\,. \tag{5.5}$$

Let Γ_0 be the subgroup of Γ of order 2 generated by the complex conjugation $\gamma : z \mapsto \bar{z}$. Then $\Gamma = \Gamma_0 \ltimes U$, a semi-direct product. According to Theorem 4.15 there is a group decomposition $G(\mathbb{Q}) = U \times F$, where F is a free abelian group with basis the collection of elements $\{\zeta_p\}_{p \in P_1}$. The action of the group U on the set $G(\mathbb{Q}) - U$ is such that it induces a bijection

$$\big(G(\mathbb{Q}) - U\big)/U \xrightarrow{\simeq} F - \{1\}, \tag{5.6}$$

and this bijection respects the actions of Γ_0. Hence we can pass from the bijection (5.5) to the bijection

$$\text{pt} : \big(F - \{1\}\big)/\Gamma_0 \xrightarrow{\simeq} \text{PT}\,. \tag{5.7}$$

Now let us fix a positive integer k, distinct primes $p_1, \ldots, p_k$ in P_1, and positive integers $n_1, \ldots, n_k$. Consider the set

$$Z := \left\{ \zeta_{p_1}^{\epsilon_1 \cdot n_1} \cdots \zeta_{p_k}^{\epsilon_k \cdot n_k} \;\middle|\; \epsilon_1, \ldots, \epsilon_k \in \{\pm 1\} \right\}.$$

It is a subset of $F - \{1\}$, stable under the action of Γ_0. Indeed, the conjugation γ acts by $\epsilon_i \mapsto -\epsilon_i$. Hence, if we let $Z' \subseteq Z$ be the subset corresponding to $\epsilon_1 = 1$, the restricted function $\text{pt} : Z' \to \text{PT}$ is injective. Lemma 5.1 says that the image $\text{pt}(Z')$ is contained in PT_c, where $c := p_1^{n_1} \cdots p_k^{n_k}$. The same lemma says that for any element $\zeta \in F - \{1\}$ that does not belong to Z, $\text{pt}(\zeta)$ is not in PT_c. The conclusion is that the function $\text{pt} : Z' \to \text{PT}_c$ is bijective. This proves item (1) of the theorem.

As for item (2): Since only numbers $c = p_1^{n_1} \cdots p_k^{n_k}$ with $p_i \in P_1$ occur as hypotenuses in the image of the bijection (5.7), the subsets PT_c are empty for numbers c that are not of this kind. □

Corollary 5.8. *Let c be an integer > 1, with prime decomposition as in Theorem 5.3.*

(1) *If $p_i \equiv 1 \pmod 4$ for every index i, then the number of normalized pythagorean triples with hypotenuse c is 2^{k-1}.*

(2) *Otherwise, there are no normalized pythagorean triples with hypotenuse c.*

Proof. (1) The set

$$Z' = \left\{ \zeta_{p_1}^{n_1} \cdot \zeta_{p_2}^{\epsilon_2 \cdot n_2} \cdots \zeta_{p_k}^{\epsilon_k \cdot n_k} \;\middle|\; \epsilon_2, \ldots, \epsilon_k \in \{\pm 1\} \right\}$$

has cardinality 2^{k-1}, and item (1) of the theorem says that the function $\mathrm{pt} : Z' \to \mathrm{PT}_c$ is bijective.

(2) This is clear from item (2) of the theorem. □

We end the article with an example and an exercise.

Example 5.9. Take the number $c = 289$. Its prime factorization is $c = 17^2$, and $17 \in P_1$, so by Corollary 5.8 there is one normalized pythagorean triple with hypotenuse 289. We can say what it quite easily. First we express 17 as a sum of two squares: $17 = 1 + 16 = 1^2 + 4^2$. We get $m = 1$, $n = 4$, $q = 1 + 4 \cdot \boldsymbol{i}$, $\bar{q} = 1 - 4 \cdot \boldsymbol{i}$ and

$$\zeta_{17} = q/\bar{q} = q^2/(q \cdot \bar{q}) = (1 + 4 \cdot \boldsymbol{i}) \cdot (1 + 4 \cdot \boldsymbol{i}) \cdot \tfrac{1}{17} = -\tfrac{15}{17} + \tfrac{8}{17} \cdot \boldsymbol{i}.$$

Next we compute

$$\zeta_{17}^2 = \left(-\tfrac{15}{17} + \tfrac{8}{17} \cdot \boldsymbol{i}\right) \cdot \left(-\tfrac{15}{17} + \tfrac{8}{17} \cdot \boldsymbol{i}\right) = \tfrac{161}{289} - \tfrac{240}{289} \cdot \boldsymbol{i}.$$

This tells us that our normalized pythagorean triple is

$$\mathrm{pt}(\zeta_{17}^2) = (161, 240, 289).$$

We leave it to the reader to verify that this is really a pythagorean triple (this requires a calculator). Checking for normalization is easy: 17 does not divide 161 and 240.

Exercise 5.10. Find the two normalized pythagorean triples with hypotenuse 65.

Acknowledgments. I wish to thank Eitan Bachmat, Moshe Newman, Noam Zimhoni, Moshe Kamenski, Ramin Takloo-Bighash, Gal Alster, Dor Amzaleg and Steven Miller for their advice in preparing this article.

References

[Ar] M. Artin, "Algebra", Prentice-Hall, 1991.
[Tk] R. Takloo-Bighash, "A Pythagorean Introduction to Number Theory", Springer, 2018.
[Ts] O. Taussky, Sums of squares, *Amer. Math. Monthly* **77** (1970), 805-830.
[Wi1] Wikipedia entry "Pythagorean Triple", http://en.wikipedia.org/wiki/Pythagorean_triple.
[Wi2] Wikipedia entry "Hilbert's Theorem 90", https://en.wikipedia.org/wiki/Hilbert's_Theorem_90.
[Wo] Wolfram Mathworld entry "Pythagorean Triple", http://mathworld.wolfram.com/PythagoreanTriple.html.

Department of Mathematics, Ben Gurion University, Be'er Sheva 84105, Israel
Email address: amyekut@math.bgu.ac.il