Pythagorean Triples

Abstract

Let $\triangle ABC$ be a triangle, and set $a := |BC|$, $b := |AC|$, $c := |AB|$. The *Pythagorean Theorem* (and its converse) state that $\triangle ABC$ is a right triangle with right angle at $\angle C$ if and only if $a^2 + b^2 = c^2$. In this session, we shall explore the associated *Diophantine equation*, meaning we seek all solutions (a, b, c) to $a^2 + b^2 = c^2$ over the positive integers.

Positive integer solutions to $a^2 + b^2 = c^2$ are called *Pythagorean triples*, and our primary goal is to explore different methods to provide a complete characterization of all Pythagorean triples. These include elementary techniques in number theory, geometric methods, and application of properties of complex numbers.

Background needed: Prerequisites include basic algebra and some elementary number theory. We also will be using many ideas from geometry, including familiarity with equations for certain curves in the plane and expressing lines in the plane relative to a point on the line and the line's slope.

0 Warmup

As prerequisites for this session, it will help to answer the following first. You do *not* need to know these answers already, and many questions will be revisited later in the worksheet.
Exercises:

0.1 What is the *Pythagorean Theorem*?

0.2 Let a, b be integers. What does it mean for a and b to be *relatively prime* or *coprime*? (*Notation:* $\gcd(a, b) = 1$.)

Say we have finitely many integers $a_1, a_2, \dots, a_n$. What does it mean for all n positive integers to be relatively prime? (*Notation:* $\gcd(a_1, a_2, \dots, a_n) = 1$.)

What does it mean for the set $\{a_1, a_2, \dots, a_n\}$ to be *pairwise relatively prime* or *pairwise coprime*? Can you give an example of three positive integers a, b, c that are relatively prime but not pairwise relatively prime?

0.3 Let L be a line in the plane, where L is not parallel to the y-axis. What is the *slope* of L? Can you provide an equation for L using the slope of L?

0.4 What is an equation in the plane to represent a circle? From your equation, how can we detect the center, (h,k), and the radius r?

0.5 What is a *complex number*? In particular, what does i denote in the context of the complex numbers? How do we add, subtract, and multiply complex numbers?

0.6 Let m be a positive integer, and let a, b be any integers. What does it mean to say that *a is congruent to b modulo m*, denoted $a \equiv b \pmod{m}$?

1 An Introduction to Pythagorean Triples

Over the real numbers, the equation $a^2 + b^2 = c^2$ has infinitely many solutions (a,b,c).[1] In *number theory*, an important subject of interest is studying *Diophantine equations*, where

[1] Explicitly, for any arbitrary $a, b \in \mathbb{R}$, select $c := \sqrt{a^2+b^2}$.

we are limiting our attention to solutions over the integers (or occasionally the rational numbers).

Definition 1.1. For the Diophantine equation

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

any solution (a, b, c), where a, b, and c are all positive integers, is called a *Pythagorean triple*.

Example 1.2. The following are examples of Pythagorean triples:

(a) $(3, 4, 5)$ is a Pythagorean triple because $3^2 + 4^2 = 5^2$.

(b) $(8, 15, 17)$ is a Pythagorean triple because $8^2 + 15^2 = 17^2$.

(c) $(9, 12, 15)$ is a Pythagorean triple because $9^2 + 12^2 = 15^2$.

Note that Examples #1(a) and #3(c) are both Pythagorean triples, but they are not essentially different examples because the latter is an integer multiple of the former. To take this into account, we introduce the following definition:

Definition 1.3. Let (a, b, c) be a Pythagorean triple, meaning these are positive integers with $a^2 + b^2 = c^2$. Then (a, b, c) is a *primitive Pythagorean triple* if and only if $\gcd(a, b, c) = 1$.

That is, (a, b, c) is a primitive Pythagorean triple if it is a Pythagorean triple, and there is no common factor of a, b, and c greater than 1.

Example 1.4. The following are examples—and nonexamples—of primitive Pythagorean triples:

(a) $(3, 4, 5)$ is a primitive Pythagorean triple because $3^2+4^2 = 9+16 = 25 = 5^2$, and $\gcd(3, 4, 5) = 1$.

(b) $(8, 15, 17)$ is a primitive Pythagorean triple because $8^2 + 15^2 = 64 + 225 = 289 = 17^2$, and $\gcd(8, 15, 17) = 1$.

(c) $(9, 12, 15)$ is a Pythagorean triple, because $9^2 + 12^2 = 81 + 144 = 225 = 15^2$. However, it is not primitive, because $\gcd(9, 12, 15) = 3 > 1$.

Exercises:

1.1 In the following, we shall explore examples and computations regarding Pythagorean triples.

   (a) Prove that $(5, 12, 13)$ is a Pythagorean triple. Is it a primitive Pythagorean triple?

(b) Prove that $(14, 48, 50)$ is a Pythagorean triple. Is it a primitive Pythagorean triple?

(c) Prove that $(9, 40, 41)$ is a Pythagorean triple. Is it a primitive Pythagorean triple?

(d) Can you produce other examples of Pythagorean triples and primitive Pythagorean triples other than those in Examples 1.2 and 1.4 and Exercise #1.1(a)–1.1(c)?

1.2 If (a, b, c) is a Pythagorean triple, then for any positive integer k, (ka, kb, kc) is also a Pythagorean triple.

For example, note that from Example 1(a) $(3, 4, 5)$ is a Pythagorean triple. For $k := 3$, we also have that $(3k, 4k, 5k) = (9, 12, 15)$ is a Pythagorean triple by Example 3(c).

1.3 Let (a, b, c) be a Pythagorean triple. If $d := \gcd(a, b, c)$, then

$$\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) \tag{1.2}$$

is a primitive Pythagorean triple

1.4 Let s is any positive integer, and show that $(2s+1, 2s^2+2s, 2s^2+2s+1)$ is a Pythagorean triple. That is, verify that

$$(2s+1)^2 + (2s^2+2s)^2 = (2s^2+2s+1)^2.$$

and these elements are relatively prime. (To see it is primitive, note that the second and third terms are consecutive and thus relatively prime.)

Since every odd positive integer is of the form $2s+1$, conclude that every odd positive integer is the length of a leg in a primitive Pythagorean triple. Further, since $2s^2+2s$ and $2s^2+2s+1$ are consecutive, this means there are infinitely many Pythagorean triples of the form (a, b, c), where b and c are consecutive integers. (Note that $(3, 4, 5)$, $(5, 12, 13)$, and and $(7, 24, 25)$ are all examples, for $s = 1$, $s = 2$, and $s = 3$, respectively.)

1.5 Let $\triangle ABC$ be a triangle as in the the abstract. The Pythagorean Theorem states that if $\angle C$ is a right angle, then $a^2 + b^2 = c^2$. Can you prove the Pythagorean Theorem?

For reference and additional information specific to the Pythagorean Theorem, see, for example, the Mathologer videos [7] and [6].

2 Properties of Primitive Pythagorean Triples

Before deriving the formula that lists every primitive Pythagorean triple, we first seek to better understand the basic structure of any primitive solution to $a^2 + b^2 = c^2$. The exercises in this section will use basic principles from number theory, including properties of *modular arithmetic* that was mentioned above in Exercise #0.6. Our goal is to establish some basic properties of any primitive Pythagorean triple, such as whether we can have a solution where both a and b are odd.

Exercises:

2.1 First, a definition:

Definition 2.1. Let a, b be integers. Then a *divides* b (or equivalent, a is a *divisor* of b, b is a *multiple* of a), if and only if there exists an integer a' such that $aa' = b$.

Notation: If a divides b, this is denoted $a \mid b$. If a does not divide b, that is denoted $a \nmid b$.

Prove that if a, b, d are integers such that $d \mid a$ and $d \mid b$, then $d \mid (a+b)$ and $d \mid (a-b)$.

For example, if a and b are both even, meaning both are divisible by 2, $a+b$ and $a-b$ are also both even, too.

2.2 Prove that if (a, b, c) is any Pythagorean triple, then it is of the form (da', db', dc') for some unique positive integer d, and a unique primitive Pythagorean triple (a', b', c').

That is, any Pythagorean triple (a, b, c) is some multiple of a primitive Pythagorean triple, and both the scaling multiple and the primitive Pythagorean triple are uniquely determined by (a, b, c).

2.3 For a Pythagorean triple, the following are equivalent:

(a) a, b, and c are pairwise relatively prime.
That is, $\gcd(a, b) = \gcd(b, c) = \gcd(a, c) = 1$, all simultaneously.

(b) At least one particular pair among a, b, and c is relatively prime.
That is, either $\gcd(a, b) = 1$, $\gcd(b, c) = 1$, or $\gcd(a, c) = 1$.

(c) (a, b, c) is a primitive Pythagorean triple.
That is, $\gcd(a, b, c) = 1$.

2.4 Again, we first introduce a definition:

Definition 2.2. Let a, b, m be integers. Then *a is congruent to b modulo m* (or *mod m*) if and only if $m \mid a - b$.

Notation: a is congruent to b modulo m is denoted $a \equiv b \pmod{m}$. If a is not congruent

Equivalently: $a \equiv b \pmod{m}$ if and only if (1) m is a divisor of $a - b$, (2) $a - b$ is a multiple of m, or (3) a and b have the same remainders upon being divided by m. (This answers Exercise #0.6 from the warmup.)

Assume (a, b, c) is a primitive Pythagorean triple. Then $a \not\equiv b \pmod{2}$, and $c \equiv 1 \pmod{2}$. That is, one of a and b is odd, the other is even, and c is odd.

2.5 Let a, b, c be positive integers. If $\gcd(a, b) = 1$ and $ab = c^2$, then a and b are both perfect squares.

Remark. This can be generalized to higher powers of c. More generally, if a, b, c, k are a positive integers, $k \geq 2$, $\gcd(a, b) = 1$, and $ab = c^k$, then a and b are both perfect kth powers.

3 Solving for All Primitive Pythagorean Triples: An Algebraic Approach

In this section, we shall present a standard solution for all Pythagorean triples using results from elementary number theory. Our approach will be along the lines of that in [8], [4] and [5], [9]. Similar (though incomplete) approaches are also found in [2] and others.

Specifically, our goal is to prove the following:

Theorem 3.1 (Complete Characterization of Primitive Pythagorean Triples)**.** *Let* (a, b, c) *be a primitive Pythagorean triple. Then we have the following:*

(a) *Precisely one of a and b is even, and the other is odd. Since $a^2 + b^2 = c^2$ if and only if $b^2 + a^2 = c^2$, we therefore assume without loss of generality that b is even.*

(b) *Assuming, as above, that b is even, there exist positive integers $r > s$ such that*

- *The integers r and s have no common divisor greater than 1,*
- *Precisely one of r and s is even, and the other is odd,*
- *and*

$$a = r^2 - s^2 \tag{3.1}$$
$$b = 2rs \tag{3.2}$$
$$c = r^2 + s^2. \tag{3.3}$$

One can verify by algebra that if a, b, c are defined as in Theorem 3.1, then we do indeed have that $a^2 + b^2 = c^2$.

From the theorem, we obtain the following immediate corollary:

Corollary 3.1(a) (Complete Characterization of All Pythagorean Triples)**.** *Let (a, b, c) be any Pythagorean triple. Then there exist positive integers $r > s$ as in Theorem 3.1 such that*

- *The integers r and s have no common divisor greater than 1.*
- *Precisely one of r and s is even, and the other is odd.*

and a positive integer k such that

$$a := k(r^2 - s^2) \tag{3.4}$$
$$b := k(2rs) \tag{3.5}$$
$$c := k(r^2 + s^2), \tag{3.6}$$

or the formulas for a and b in (3.4) and (3.5) are interchanged.

That is, every Pythagorean triple is a positive integer multiple of a primitive Pythagorean triple, and all primitive Pythagorean triples are of the form in Theorem 3.1.

As with Theorem 3.1, we can immediately verify that a, b, c as defined in Corollary 3.1(a) do form a Pythagorean triple.

Since a general Pythagorean triple need not have that $a \not\equiv b \pmod 2$, it is more cumbersome to describe the condition of b being "more even" than a without loss of generality. This accounts for the idea of potentially having to interchange the formulas for a and b in (3.4)–(3.5).

Remark. If s is a positive integer, then $s+1$ will be relatively prime to s and of opposite parity. The formula in Theorem 3.1 will produce the Pythagorean triple in Exercise #1.4.

Exercises:

3.1 Fill in the following table. (Here, “PT?” and “PPT?” ask you to determine, respectively, whether (a,b,c) is a Pythagorean triple (PT) or a primitive Pythagorean triple (PPT), respectively. Further, “$r \not\equiv s \pmod 2$?” asks whether r and s are opposite parity, and “$\gcd(r,s)$?” asks whether they are relatively prime.)

Do you notice? Do you have any conjectures? Can you prove them?

r	s	$r \not\equiv s \pmod 2$?	$\gcd(r,s) = 1$?	$a := r^2 - s^2$	$b := 2rs$	$c := r^2 + s^2$	PT?	PPT?
2	1	YES	YES	3	4	5	YES	YES
3	1	NO	YES	8	6	10	YES	NO
3	2	YES	YES	5	12	13	YES	YES
4	1	YES	YES	15	8	17	YES	YES
4	2							
4	3							
5	1							
5	2							
5	3							
5	4							
6	1							
6	2							
6	3							
6	4							
6	5							

3.2 Let (a,b,c) be a primitive Pythagorean triple such that, by Exercise #2.4, we may assume without loss of generality that $\underline{b \text{ is even}}$. Then

$$\left(\frac{b}{2}\right)^2 = \frac{c+a}{2} \cdot \frac{c-a}{2}. \tag{3.7}$$

Further, $\frac{b}{2}$, $\frac{c+a}{2}$, and $\frac{c-a}{2}$ are all positive integers, and

$$\gcd\left(\frac{c+a}{2}, \frac{c-a}{2}\right) = 1. \tag{3.8}$$

Hint: Start from $a^2 + b^2 = c^2$, and solve for b^2. Since b is even, divide both sides of the resulting equation by 4. We have that a, c must both be odd, so the factors on the right-hand side of (3.7) must both be integers.

To prove (3.8), recall that since (a, b, c) is a primitive Pythagorean triple with b even, a, b, c are pairwise relatively prime, and a, c are both odd. If d is a common divisor of $\frac{c+a}{2}$ and $\frac{c-a}{2}$, what can we deduce from the result of Exercise #2.1?

3.3 Let (a, b, c) be a primitive Pythagorean triple where b is even, as in Exercise #3.2. Prove that there exist positive integers $r > s$ such that

$$r^2 = \frac{c+a}{2}, \tag{3.9}$$
$$s^2 = \frac{c-a}{2}. \tag{3.10}$$

3.4 Complete the proofs of Theorem 3.1 and Corollary 3.1(a).

3.5 **Challenging:** Let $\mathbb{R}[x]$ denote the set of all polynomials in x with real coefficients. Say that the polynomial triple $(f(x), g(x), h(x))$ in $\mathbb{R}[x]$ is a *primitive polynomial Pythagorean triple* if $\gcd(f(x), g(x), h(x)) = 1$ and

$$\left[f(x)\right]^2 + \left[g(x)\right]^2 = [h(x)]^2. \tag{3.11}$$

Note: This result appears as Theorem 5.1 in [4]. Things are a bit trickier for polynomials with coefficients over the complex numbers $\mathbb{C}$, since we have, for example, $1^2 + i^2 = 0$.

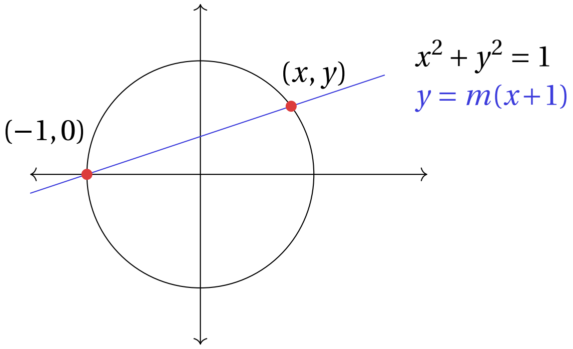

Figure 4.1: Rational points (x, y) in the first quadrant of the unit circle $x^2 + y^2 = 1$.

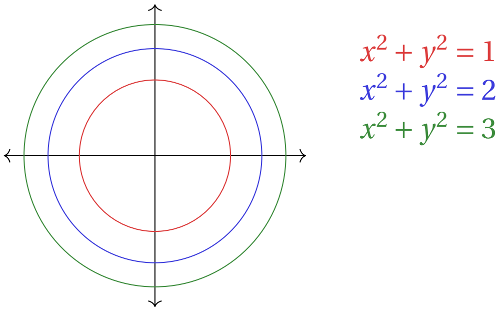

Figure 4.2: Graphs of three circles in the plane.

4 Geometry and Pythagorean Triples

Though we have already provided a complete solution for how to represent all primitive Pythagorean triples, we now reconsider the question from another vantage point. Using geometry, we shall connect primitive Pythagorean triples to rational points on the unit circle $x^2 + y^2 = 1$. This geometric approach, taken from [11], [4], and [5], is versatile, allowing insight into a range of Diophantine equations.
Exercises: In what follows, it will help to reference Figures 4.1 and 4.2.

4.1 Consider the curve in the plane given by $x^2 + y^2 = 1$. Produce an example of a rational point on this curve. (The points $(\pm 1, 0)$ and $(0, \pm 1)$ are "trivial" in this case, so produce a nontrivial rational point.)

4.2 Consider the curve in the plane given by $x^2 + y^2 = 2$. Can you find a rational point on this circle? What about a rational point other than $(\pm 1, \pm 1)$?

4.3 Consider the curve in the plane given by $x^2 + y^2 = 3$.

4.4 Show that for every rational point on $x^2+y^2 = 1$, there is a corresponding triple (a, b, c) of integers (not necessarily positive!) such that $a^2 + b^2 = c^2$. Is there a *unique* such triple for every rational point (x, y) satisfying $x^2 + y^2 = 1$? A nontrivial one? Why or why not?

4.5 Consider the unit circle $x^2 + y^2 = 1$, as well as the line of slope m through the point $(-1, 0)$, which lies on this circle. See Figure 4.1.

(a) Verify that an equation for the line of slope m passing through the point $(-1, 0)$ is $y = m(x + 1)$.

(b) Fix a slope $m \in \mathbb{R}$, and consider the point (x, y) where the line $y = m(x + 1)$ intersects the unit circle $x^2 + y^2 = 1$. Find the coordinates for (x, y) with respect to m.

(c) Show that if the slope m is rational, then the point of intersection (x, y) is a rational point on the unit circle.

(d) Prove that if (x, y) is a rational point on the unit circle, $(x, y) \neq (-1, 0)$, and m is the slope of the unique line through $(-1, 0)$ and (x, y), then m is rational.

(e) Let $r, s \in \mathbb{Z}$, with $r \neq 0$ and $\gcd(r, s) = 1$, and set $m := \frac{s}{r}$. (Note the order of r and s in this fraction!) Compute the rational point $(x, y) \neq (-1, 0)$ that lies on the unit circle and the line through $(-1, 0)$ of slope m with respect to r and s.

Note: If (x, y) is a rational point in the first quadrant, then $0 < m < 1$, from which it follows that $r > s > 0$.

4.6 Let (a, b, c) be a primitive Pythagorean triple. From Exercise #2.4, precisely one of a and b is even, so now and for the remainder of this section, assume without loss of generality that b is even.

Consider the associated rational point $(x, y) := \left(\frac{a}{c}, \frac{b}{c}\right)$ on the unit circle. Then with r, s as in Exercise #4.5(e), show that we may assume $r > s > 0$ without loss of generality, and $r \not\equiv s \pmod 2$. That is, precisely one of r and s is odd, and the other is even.

Note: We already established in Exercise #2.4 that in a primitive Pythagorean triple, a, b must have opposite parity. Can you provide an independent proof here using the geometry?

4.7 Theorem 3.1 is true. Specifically, if (a,b,c) is a positive, primitive Pythagorean triple where b is even without loss of generality, then there exist positive integers $r > s$ with $\gcd(r,s) = 1$ and $r \not\equiv s \pmod 2$ such that

$$\begin{aligned} a &= r^2 - s^2 \\ b &= 2rs \\ c &= r^2 + s^2. \end{aligned}$$

4.8 **Challenging:** Consider rational points on the circle $x^2 + y^2 = 2$, the blue circle in Figure 4.2. From Exercise #4.2 (or otherwise), note that $(-1,-1)$ is such a rational point.

Prove that the rational points on the circle $x^2 + y^2 = 2$, other than $(-1,1)$ and $(-1,-1)$, are of the form

$$(x,y) = \left(\frac{1+2m-m^2}{m^2+1}, \frac{m^2+2m-1}{m^2+1}\right) \tag{4.1}$$

Note: This appears as Theorem 5.2 in [4]. I mark this as challenging primarily because it is likely to be time-consuming. If you solve this, can you completely characterize all integer solutions to the Diophantine equation $a^2 + b^2 = 2c^2$?

4.9 **Challenging:** Let d be a nonzero integer. Then the rational points on the hyperbola $x^2 - dy^2 = 1$ are given by

$$(x,y) = \left(\frac{1+dm^2}{1-dm^2}, \frac{2m}{1-dm^2}\right), \tag{4.2}$$

for each rational number m, as well as the point $(-1,0)$.

Note: This appears as an unnumbered theorem in [5]. Again, I mark this as challenging primarily because it is likely to be time-consuming. If you solve this, can you completely characterize all integer solutions to the Diophantine equation $a^2 - db^2 = c^2$?

This geometric approach has wide applicability beyond simply rational points on a single circle. One can use it to identify all rational points on other conics, such as *ellipses*, *parabolas*, and *hyperbolas*. Perhaps more important in the context of modern mathematics, this approach motivates the study of *elliptic curves*,[2] Elliptic curves are of great theoretical interest to mathematicians, including their role in the proof of *Fermat's Last Theorem* by Andrew Wiles and Richard Taylor. Elliptic curves have important real-world applications, too, including *elliptic curve cryptography* and *elliptic curve primality testing*.

Separately, note that *every* right triangle is arbitrarily close to being similar to a right triangle with integer side lengths. This result is due to [10], itself an exposition of "The Shapes and Sizes of Pythagorean Triangles" by P. Shui, *The Mathematical Gazette*, Vol. 67, No. 439 (March 1983), pp. 33–38.

5 Gaussian Integers and Pythagorean Triples

We conclude with yet another technique: using properties of a subset of the complex numbers. Applying the algebra of the Gaussian integers to prove Theorem 3.1 and Corollary 3.1(a) follows [4]. For a much richer animated visualization of connections between Gaussian integers and Pythagorean triples, as well as to rational points on the unit circle, I highly recommend [1].

The following are taken from "Modular Arithmetic and Gaussian Integers", the worksheet for the advanced group's session of November 5, 2022.

Definition 5.1. The *ring of Gaussian integers*, denoted $\mathbb{Z}[i]$, is the set $\{a+bi : a, b \in \mathbb{Z}\}$, where $i^2 = -1$.

For integers a, b, c, d, addition is defined pointwise: $(a+bi)+(c+di) := (a+c)+(b+d)i$. Multiplication is defined by $(a+bi)(c+di) := (ac-bd)+(ad+bc)i$.

Geometrically, we identify each point $a+bi$ of the Gaussian integers with the lattice point (a, b) in the plane. In this way, the Gaussian integers appear as points in the plane with integer x- and y-coordinates.

Remark. Every integer a is of the form $a+0i$. Therefore, every integer is also a Gaussian integer. (That is, $\mathbb{Z} \subseteq \mathbb{Z}[i]$.) The converse is false, though: $1+2i$ is a Gaussian integer, but $1+2i$ is not an integer.

Notation. Throughout, lower case Roman letters shall typically denote integers: a, b, c, etc. Lower case Greek letters shall denote Gaussian integers: α, β, γ, etc. In particular, π here shall denote a Gaussian integer and *not* the real number 3.14159265..., nor the prime-counting function.

[2] Note that an elliptic curve is *not* simply an ellipse. A general elliptic curve in the plane is something equivalent to (in a sense that can be made precise, but which is unimportant for our purposes) a curve of the form $y^2 = x^3 + ax + b$, where a, b are constants.

Definition 5.2. Let $\alpha = a + bi \in \mathbb{Z}[i]$, as in the notational convention above. Then the *conjugate* of α, denoted $\overline{\alpha}$ (or sometimes α^*), is defined by $\overline{\alpha} := a - bi$. The *norm* of α, denoted $N(\alpha)$, is defined by $N(\alpha) := a^2 + b^2$.

Geometrically, $\overline{\alpha}$ reflects α above the real axis. Further, $N(\alpha)$ represents the *square* of the distance between α and $0 = 0 + 0i$.

Remark. By the definitions above, for all $\alpha \in \mathbb{Z}[i]$, $N(\alpha) = \alpha \cdot \overline{\alpha}$. Moreover, $N(\alpha) = |\alpha|^2$, where $|\alpha|$ denotes the usual length of α. In particular, for every $\alpha \in \mathbb{Z}[i]$, $N(\alpha)$ is a nonnegative integer.

We shall also use the following to guide our intuition, though we state it without proof.

Proposition 5.3. *Let α, β be Gaussian integers. Consider the lines through α and the origin and through β and the origin, respectively, and the angles each line makes with the positive real axis. Then the product $\alpha\beta$ has length that is the product of the lengths of α and β. Further, its angle with the positive real axis is taken by adding the angles for α and β.*

That is, to multiply Gaussian integers, multiply their lengths*, then* add their angles.

In particular, if we *square* a Gaussian integer α, then α^2 will have length that is the square of the length of α, and its angle with the positive real axis will be double that of α itself.

Finally, we shall assert (without proof) that like the integers, the Gaussian integers have a version of the *Fundamental Theorem of Arithmetic*: if α is a Gaussian integer, and $\alpha \neq 0, \pm 1, \pm i$, then α is expressible as a product of elements that are primes—meaning prime *as Gaussian integers!*—and this prime factorization is unique up to the order of primes and the presence of factors of ± 1 or $\pm i$.

Example 5.4. In the Gaussian integers, we have $2 = (1+i)(1-i) = -i(1+i)^2$. We have that $1+i$ and $1-i$ are both prime as Gaussian integers. These aren't essentially different, though, since $1-i = -i(1+i)$. Considering prime factorizations over the integers, this would be equivalent to noting that $15 = 3 \cdot 5 = (1) \cdot (-3) \cdot 5 = (-3) \cdot (-5)$.

Note also that while 2 is a prime number *as an integer*, 2 has a nontrivial factorization *as a Gaussian integer*. In a similar way, we can factor many integer primes within the Gaussian integers: $5 = (1+2i)(1-2i)$, $13 = (2+3i)(2-3i)$, $17 = (1+4i)(1-4i)$, etc.

Since the Gaussian integers have a counterpart to the Fundamental Theorem of Arithmetic, it also follows that we can meaningfully discuss divisibility, greatest common divisors, and related concepts within the context of the Gaussian integers. Because of our Gaussian *units* of $\pm 1, \pm i$, though, $\gcd(\alpha, \beta)$ is only defined up to unit multiple rather than as a uniquely defined Gaussian integer. That is, we can talk about *a* Gaussian integer gcd rather than *the* Gaussian integer gcd. This is basically because, unlike over the integers, we cannot neatly partition the Gaussian integers into zero, positive, and negative. (For example, should $-1 + 7i$ be positive or negative?)
Exercises:

5.1 Compute the following:

(a) $(2+i)^2$

(b) $(3+2i)^2$

(c) $(4+i)^2$

(d) $(3+4i)^2$

(e) Let c, d be integers. Compute $(c+di)^2$.

(f) Let c, d be positive integers with $c > d$. Then the real and imaginary coefficients of $(c+di)^2$ are legs in a Pythagorean triple.

5.2 Prove that for all $\alpha, \beta \in \mathbb{Z}[i]$, $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$.

5.3 Prove that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

5.4 Let (a, b, c) be a Pythagorean triple. Then $(a + bi)(a - bi) = c^2$.

5.5 Let (a, b, c) be a primitive Pythagorean triple. Then *over the Gaussian integers*, $\gcd(a + bi, a - bi) = 1$, in the sense that the only common divisors in the Gaussian integers of $a + bi$ and $a - bi$ are $\pm 1. \pm i$.

Note: A full development of the number theoretic properties of the Gaussian integers would require a long digression, so try to address this and other exercises without requiring full, rigorous proofs of everything.

5.6 Theorem 3.1 and Corollary 3.1(a) are true via this method.

References

[1] 3Blue1Brown. All possible pythagorean triples, visualized. https://www.youtube.com/watch?v=QJYmyhnaaek, May 26, 2017.

[2] blackpenredpen. finding all pythagorean triples (solutions to aˆ2+bˆ2=cˆ2). https://www.youtube.com/watch?v=n6vL2KiWrD4, July 8, 2018.

[3] Keith Conrad. The Gaussian integers. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf. online: retrieved November 4, 2022.

[4] Keith Conrad. Pythagorean triples. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pythagtriple.pdf. online: retrieved October 21, 2024.

[5] Keith Conrad. Pythagorean triples. https://kconrad.math.uconn.edu/ross2008/pythagtriple.pdf, August 4, 2008. online: retrieved October 21, 2024.

[6] Mathologer. Fibonacci = Pythagoras: Help save a beautiful discovery from oblivion. https://www.youtube.com/watch?v=94mV7Fmbx88, December 3, 2022.

[7] Mathologer. Visualising Pythagoras: ultimate proofs and crazy contortions. https://www.youtube.com/watch?v=p-0SOWbzUYI, February 25, 2018.

[8] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[9] Michael Penn. Number theory | primitive Pythagorean triples. https://www.youtube.com/watch?v=F3dR41ItmSg, August 28, 2019.

[10] Michael Penn. every right triangle is almost* Pythagorean. https://www.youtube.com/watch?v=e9mo0L0396s, October 6, 2024.

[11] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, 1992.