# Math 361

January 23, 2023

# Math 361

- https://people.reed.edu/~davidp/361/

# Pythagorean triples

A *Pythagorean triple* is a tuple $(x, y, z)$ of positive integers such that

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

# Pythagorean triples

A *Pythagorean triple* is a tuple $(x, y, z)$ of positive integers such that

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

It is *primitive* if $\gcd(x, y, z) = 1$.

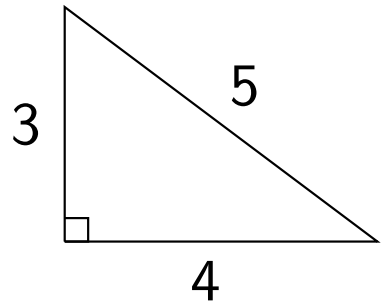
# Pythagorean triples

A *Pythagorean triple* is a tuple $(x, y, z)$ of positive integers such that

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

It is *primitive* if $\gcd(x, y, z) = 1$.

**Example.**




$$3^2 + 4^2 = 5^2$$

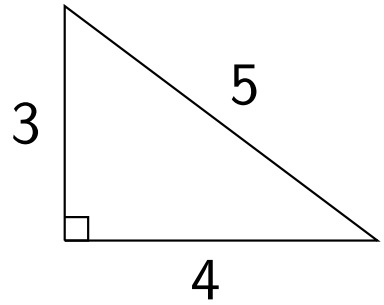
# Pythagorean triples

A *Pythagorean triple* is a tuple $(x, y, z)$ of positive integers such that

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

It is *primitive* if $\gcd(x, y, z) = 1$.

**Example.**




$$3^2 + 4^2 = 5^2$$

Problem. Find all primitive Pythagorean triples.

# Pythagorean triples

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

# Pythagorean triples

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

**First observations.**

1. If $(x, y, z)$ is a primitive Pythagorean triple, and $m$ is a positive integer, then $(mx, my, mz)$ is a Pythagorean triple. If $(x, y, z)$ is any Pythagorean triple, then canceling common factors yields a primitive Pythagorean triple.

# Pythagorean triples

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

**First observations.**

1. If $(x, y, z)$ is a primitive Pythagorean triple, and $m$ is a positive integer, then $(mx, my, mz)$ is a Pythagorean triple. If $(x, y, z)$ is any Pythagorean triple, then canceling common factors yields a primitive Pythagorean triple.

2. For a Pythagorean triple $(x, y, z)$, we have $\gcd(x, y, z) = 1$ if and only if $x, y, z$ are pairwise relatively prime.

# Pythagorean triples

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

**First observations.**

1. If $(x, y, z)$ is a primitive Pythagorean triple, and $m$ is a positive integer, then $(mx, my, mz)$ is a Pythagorean triple. If $(x, y, z)$ is any Pythagorean triple, then canceling common factors yields a primitive Pythagorean triple.

2. For a Pythagorean triple $(x, y, z)$, we have $\gcd(x, y, z) = 1$ if and only if $x, y, z$ are pairwise relatively prime.

3. If $(x, y, z)$ is a primitive Pythagorean theorem, then $z$ must be odd. (To see this, work modulo 4.)

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$.

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(i)$ is a field.

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(i)$ is a field. For instance,

$$\frac{1}{a + bi} =$$

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(i)$ is a field. For instance,

$$\frac{1}{a + bi} = \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi}$$

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(i)$ is a field. For instance,

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{1}{a^2+b^2}(a-bi)$$

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(i)$ is a field. For instance,

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{1}{a^2+b^2}(a-bi) = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \in \mathbb{Q}(i).$$

# Gaussian integers

**Problem.** Characterize Pythagorean triples.

Key idea: $x^2 + y^2 = (x + iy)(x - iy)$.

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(i)$ is a field. For instance,

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{1}{a^2+b^2}(a-bi) = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \in \mathbb{Q}(i).$$

*Gaussian integers:* $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.

# Factorization in $\mathbb{Z}[i]$

# Factorization in $\mathbb{Z}[i]$

1. Let $a, b \in \mathbb{Z}[i]$. Then $a$ *divides* $b$, written $a|b$, if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.

# Factorization in $\mathbb{Z}[i]$

1. Let $a, b \in \mathbb{Z}[i]$. Then $a$ *divides* $b$, written $a|b$, if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.
2. An element $u \in \mathbb{Z}[i]$ is a *unit* if $u|1$,

# Factorization in $\mathbb{Z}[i]$

1. Let $a, b \in \mathbb{Z}[i]$. Then $a$ *divides* $b$, written $a|b$, if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.
2. An element $u \in \mathbb{Z}[i]$ is a *unit* if $u|1$, i.e., if there exists $v \in \mathbb{Z}[i]$ such that $1 = uv$,

# Factorization in $\mathbb{Z}[i]$

1. Let $a, b \in \mathbb{Z}[i]$. Then $a$ *divides* $b$, written $a|b$, if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.
2. An element $u \in \mathbb{Z}[i]$ is a *unit* if $u|1$, i.e., if there exists $v \in \mathbb{Z}[i]$ such that $1 = uv$, i.e., if it is invertible in $\mathbb{Z}[i]$.

# Factorization in $\mathbb{Z}[i]$

1. Let $a, b \in \mathbb{Z}[i]$. Then $a$ *divides* $b$, written $a|b$, if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.
2. An element $u \in \mathbb{Z}[i]$ is a *unit* if $u|1$, i.e., if there exists $v \in \mathbb{Z}[i]$ such that $1 = uv$, i.e., if it is invertible in $\mathbb{Z}[i]$.
3. An element $p \in \mathbb{Z}[i]$ is *prime* if it is not 0 or a unit and whenever $p$ divides $ab$ for some $a, b \in \mathbb{Z}[i]$, then $p|a$ or $p|b$.

# Factorization in $\mathbb{Z}[i]$

1. Let $a, b \in \mathbb{Z}[i]$. Then $a$ *divides* $b$, written $a|b$, if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.
2. An element $u \in \mathbb{Z}[i]$ is a *unit* if $u|1$, i.e., if there exists $v \in \mathbb{Z}[i]$ such that $1 = uv$, i.e., if it is invertible in $\mathbb{Z}[i]$.
3. An element $p \in \mathbb{Z}[i]$ is *prime* if it is not 0 or a unit and whenever $p$ divides $ab$ for some $a, b \in \mathbb{Z}[i]$, then $p|a$ or $p|b$.

**Fact.** The ring $\mathbb{Z}[i]$ is a unique factorization domain (UFD).

# Factorization in $\mathbb{Z}[i]$

1. Let $a, b \in \mathbb{Z}[i]$. Then $a$ *divides* $b$, written $a|b$, if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.
2. An element $u \in \mathbb{Z}[i]$ is a *unit* if $u|1$, i.e., if there exists $v \in \mathbb{Z}[i]$ such that $1 = uv$, i.e., if it is invertible in $\mathbb{Z}[i]$.
3. An element $p \in \mathbb{Z}[i]$ is *prime* if it is not 0 or a unit and whenever $p$ divides $ab$ for some $a, b \in \mathbb{Z}[i]$, then $p|a$ or $p|b$.

**Fact.** The ring $\mathbb{Z}[i]$ is a unique factorization domain (UFD). That is, every nonzero element $a \in \mathbb{Z}[i]$ can be written uniquely, up to order, in the form

$$a = u \prod_{i=1}^{k} p_i^{e_i}$$

where $u$ is a unit, the $p_i$ are primes, and the $e_i$ are positive integers.

# Factorization in $\mathbb{Z}[i]$

**Examples (proofs to appear later).**

# Factorization in $\mathbb{Z}[i]$

**Examples (proofs to appear later).**

The units of $\mathbb{Z}[i]$ are

# Factorization in $\mathbb{Z}[i]$

**Examples (proofs to appear later).**

The units of $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$.

# Factorization in $\mathbb{Z}[i]$

**Examples (proofs to appear later).**

The units of $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$.

The elements $1 \pm i$ are prime.

# Factorization in $\mathbb{Z}[i]$

**Examples (proofs to appear later).**

The units of $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$.

The elements $1 \pm i$ are prime.

Although 2 is prime in $\mathbb{Z}$, it is not prime in $\mathbb{Z}[i]$. Its prime factorization in $\mathbb{Z}[i]$ is

$$2 = (1 + i)(1 - i).$$

# Back to Pythagorean triples

**Proposition.** Let $(x, y, z)$ be a primitive Pythagorean triple. Then

$$x + iy = uw^2$$

for some $u, w \in \mathbb{Z}[i]$ with $u$ a unit.

# Proof of proposition

$$x + iy = uw^2$$

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$.

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$. Suffices to show $p$ divides $x + iy$ an even number of times.

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$. Suffices to show $p$ divides $x + iy$ an even number of times. Considering the prime factorization of $z$:

$$z = v \prod_{i=1}^{k} p_i^{e_i}$$

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$. Suffices to show $p$ divides $x + iy$ an even number of times. Considering the prime factorization of $z$:

$$z = v \prod_{i=1}^{k} p_i^{e_i} \quad \Rightarrow \quad (x + iy)(x - iy) = z^2 =$$

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$. Suffices to show $p$ divides $x + iy$ an even number of times. Considering the prime factorization of $z$:

$$z = v \prod_{i=1}^{k} p_i^{e_i} \quad \Rightarrow \quad (x + iy)(x - iy) = z^2 = v^2 \prod_{i=1}^{k} p_i^{2e_i}.$$

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$. Suffices to show $p$ divides $x + iy$ an even number of times. Considering the prime factorization of $z$:

$$z = v \prod_{i=1}^{k} p_i^{e_i} \quad \Rightarrow \quad (x + iy)(x - iy) = z^2 = v^2 \prod_{i=1}^{k} p_i^{2e_i}.$$

Then $p|(x + iy) \Rightarrow$

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$. Suffices to show $p$ divides $x + iy$ an even number of times. Considering the prime factorization of $z$:

$$z = v \prod_{i=1}^{k} p_i^{e_i} \quad \Rightarrow \quad (x + iy)(x - iy) = z^2 = v^2 \prod_{i=1}^{k} p_i^{2e_i}.$$

Then $p|(x + iy) \Rightarrow p = p_i$ for some $i$.

# Proof of proposition

$$x + iy = uw^2$$

Let $p \in \mathbb{Z}[i]$ be prime and $p|(x + iy)$. Suffices to show $p$ divides $x + iy$ an even number of times. Considering the prime factorization of $z$:

$$z = v \prod_{i=1}^{k} p_i^{e_i} \quad \Rightarrow \quad (x + iy)(x - iy) = z^2 = v^2 \prod_{i=1}^{k} p_i^{2e_i}.$$

Then $p|(x + iy) \Rightarrow p = p_i$ for some $i$. Since $p_i = p$ appears an even number of times on the right, and $p$ is prime, it suffices to show $p \nmid (x - iy)$.

# Proof of proposition

For the sake of contradiction, suppose $p|(x + iy)$ and $p|(x - iy)$.

# Proof of proposition

For the sake of contradiction, suppose $p|(x+iy)$ and $p|(x-iy)$. Then $p$ divides both $z$ and $(x+iy)+(x-iy)=2x$ (in $\mathbb{Z}[i]$).

# Proof of proposition

For the sake of contradiction, suppose $p|(x + iy)$ and $p|(x - iy)$. Then $p$ divides both $z$ and $(x + iy) + (x - iy) = 2x$ (in $\mathbb{Z}[i]$). Since $(x, y, z)$ is primitive, $x$ and $z$ are relatively prime, i.e., they share no prime factors in $\mathbb{Z}$.

# Proof of proposition

For the sake of contradiction, suppose $p|(x+iy)$ and $p|(x-iy)$. Then $p$ divides both $z$ and $(x+iy)+(x-iy)=2x$ (in $\mathbb{Z}[i]$). Since $(x,y,z)$ is primitive, $x$ and $z$ are relatively prime, i.e., they share no prime factors in $\mathbb{Z}$. Since $z$ is odd, $2x$ and $z$ are relatively prime integers.

# Proof of proposition

For the sake of contradiction, suppose $p|(x+iy)$ and $p|(x-iy)$. Then $p$ divides both $z$ and $(x+iy)+(x-iy)=2x$ (in $\mathbb{Z}[i]$). Since $(x,y,z)$ is primitive, $x$ and $z$ are relatively prime, i.e., they share no prime factors in $\mathbb{Z}$. Since $z$ is odd, $2x$ and $z$ are relatively prime integers. By Math 113, there exists $m,n\in\mathbb{Z}$ such that

$$m(2x)+nz=\gcd(2x,z)=1.$$

# Proof of proposition

For the sake of contradiction, suppose $p|(x+iy)$ and $p|(x-iy)$. Then $p$ divides both $z$ and $(x+iy)+(x-iy)=2x$ (in $\mathbb{Z}[i]$). Since $(x,y,z)$ is primitive, $x$ and $z$ are relatively prime, i.e., they share no prime factors in $\mathbb{Z}$. Since $z$ is odd, $2x$ and $z$ are relatively prime integers. By Math 113, there exists $m,n\in\mathbb{Z}$ such that

$$m(2x)+nz=\gcd(2x,z)=1.$$

Thinking again about division in $\mathbb{Z}[i]$,

# Proof of proposition

For the sake of contradiction, suppose $p|(x+iy)$ and $p|(x-iy)$. Then $p$ divides both $z$ and $(x+iy)+(x-iy)=2x$ (in $\mathbb{Z}[i]$). Since $(x,y,z)$ is primitive, $x$ and $z$ are relatively prime, i.e., they share no prime factors in $\mathbb{Z}$. Since $z$ is odd, $2x$ and $z$ are relatively prime integers. By Math 113, there exists $m,n\in\mathbb{Z}$ such that

$$m(2x)+nz=\gcd(2x,z)=1.$$

Thinking again about division in $\mathbb{Z}[i]$, since $p|(2x)$ and $p|z$, it follows that $p|1$ in $\mathbb{Z}[i]$.

# Proof of proposition

For the sake of contradiction, suppose $p|(x+iy)$ and $p|(x-iy)$. Then $p$ divides both $z$ and $(x+iy)+(x-iy)=2x$ (in $\mathbb{Z}[i]$). Since $(x,y,z)$ is primitive, $x$ and $z$ are relatively prime, i.e., they share no prime factors in $\mathbb{Z}$. Since $z$ is odd, $2x$ and $z$ are relatively prime integers. By Math 113, there exists $m,n\in\mathbb{Z}$ such that

$$m(2x)+nz=\gcd(2x,z)=1.$$

Thinking again about division in $\mathbb{Z}[i]$, since $p|(2x)$ and $p|z$, it follows that $p|1$ in $\mathbb{Z}[i]$. Hence, $p$ is a unit, contradicting the assumption that $p$ is prime. This contradiction completes the proof. $\square$

# Characterization of Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

# Characterization of Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

*Proof.* We leave the check that the displayed triples are primitive if and only if $\gcd(m, n) = 1$ and have differing parity as an exercise.

# Characterization of Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

*Proof.* We leave the check that the displayed triples are primitive if and only if $\gcd(m, n) = 1$ and have differing parity as an exercise.

Easy check: the displayed triples are Pythagorean triples.

# Characterization of Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

*Proof.* We leave the check that the displayed triples are primitive if and only if $\gcd(m, n) = 1$ and have differing parity as an exercise.

Easy check: the displayed triples are Pythagorean triples.

For the converse, suppose $(x, y, z)$ is a primitive Pythagorean triple.

# Characterization of Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

*Proof.* We leave the check that the displayed triples are primitive if and only if $\gcd(m, n) = 1$ and have differing parity as an exercise.

Easy check: the displayed triples are Pythagorean triples.

For the converse, suppose $(x, y, z)$ is a primitive Pythagorean triple. By the Proposition,

$$(x + iy)(x - iy) = x^2 + y^2 = z^2 \quad \Rightarrow \quad x + iy = uw^2$$

for some $u, w \in \mathbb{Z}[i]$ with $u$ a unit.

# Characterization of Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

*Proof.* We leave the check that the displayed triples are primitive if and only if $\gcd(m, n) = 1$ and have differing parity as an exercise.

Easy check: the displayed triples are Pythagorean triples.

For the converse, suppose $(x, y, z)$ is a primitive Pythagorean triple. By the Proposition,

$$(x + iy)(x - iy) = x^2 + y^2 = z^2 \quad \Rightarrow \quad x + iy = uw^2$$

for some $u, w \in \mathbb{Z}[i]$ with $u$ a unit. Write $w = m + ni$ with $m, n \in \mathbb{Z}$.

# Characterization of Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

*Proof.* We leave the check that the displayed triples are primitive if and only if $\gcd(m, n) = 1$ and have differing parity as an exercise.

Easy check: the displayed triples are Pythagorean triples.

For the converse, suppose $(x, y, z)$ is a primitive Pythagorean triple. By the Proposition,

$$(x + iy)(x - iy) = x^2 + y^2 = z^2 \quad \Rightarrow \quad x + iy = uw^2$$

for some $u, w \in \mathbb{Z}[i]$ with $u$ a unit. Write $w = m + ni$ with $m, n \in \mathbb{Z}$. It follows that

$$x + iy = u(m + in)^2 = u((m^2 - n^2) + 2mni).$$

# Characterization of Pythagorean triples

We have

$$x + iy = u(m + in)^2 = u((m^2 - n^2) + 2mni).$$

with $u \in \mathbb{Z}[i]$ a unit.

# Characterization of Pythagorean triples

We have

$$x + iy = u(m + in)^2 = u((m^2 - n^2) + 2mni).$$

with $u \in \mathbb{Z}[i]$ a unit. Hence $u \in \{\pm 1, \pm i\}$.

# Characterization of Pythagorean triples

We have

$$x + iy = u(m + in)^2 = u((m^2 - n^2) + 2mni).$$

with $u \in \mathbb{Z}[i]$ a unit. Hence $u \in \{\pm 1, \pm i\}$. The result then follows by comparing real and imaginary parts in the displayed equation.

# Characterization of Pythagorean triples

We have

$$x + iy = u(m + in)^2 = u((m^2 - n^2) + 2mni).$$

with $u \in \mathbb{Z}[i]$ a unit. Hence $u \in \{\pm 1, \pm i\}$. The result then follows by comparing real and imaginary parts in the displayed equation. For example, if $u = 1$,

$$x + iy = (m^2 - n^2) + 2mni,$$

and, hence, $x = m^2 + n^2$ and $y = 2mn$. $\square$

# Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

# Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

**Exercise.**

- Show that the Pythagorean triple $(9, 12, 15)$ does not have either of the forms in the Corollary.

# Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

**Exercise.**

- Show that the Pythagorean triple $(9, 12, 15)$ does not have either of the forms in the Corollary.
- What doesn't this contradict the Corollary?

# Pythagorean triples

**Corollary.** The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

**Exercise.**

- Show that the Pythagorean triple $(9, 12, 15)$ does not have either of the forms in the Corollary.
- What doesn't this contradict the Corollary?
- How can you modify the corollary so that it covers all Pythagorean triples?