Pythagorean Triples and Cauchy's Functional Equation

Andrew D Smith
University College Dublin

4 October 2025

1 Part 1: 10:00 - 11:00. Integer Solutions

1.1 Introduction: Two Problems

Pythagoras Theorem: Let a, b, c be the side lengths of a right-angled triangle, with c the longest side. Then

$$a^2 + b^2 = c^2 \tag{1}$$

A *Pythagorean triple* (a, b, c) is a solution of equation 1 in positive integers a, b, c.

Well-known Pythagorean triples are:

$$3^2 + 4^2 = 5^2$$
$$5^2 + 12^2 = 13^2$$
$$7^2 + 24^2 = 25^2$$
$$8^2 + 15^2 = 17^2$$

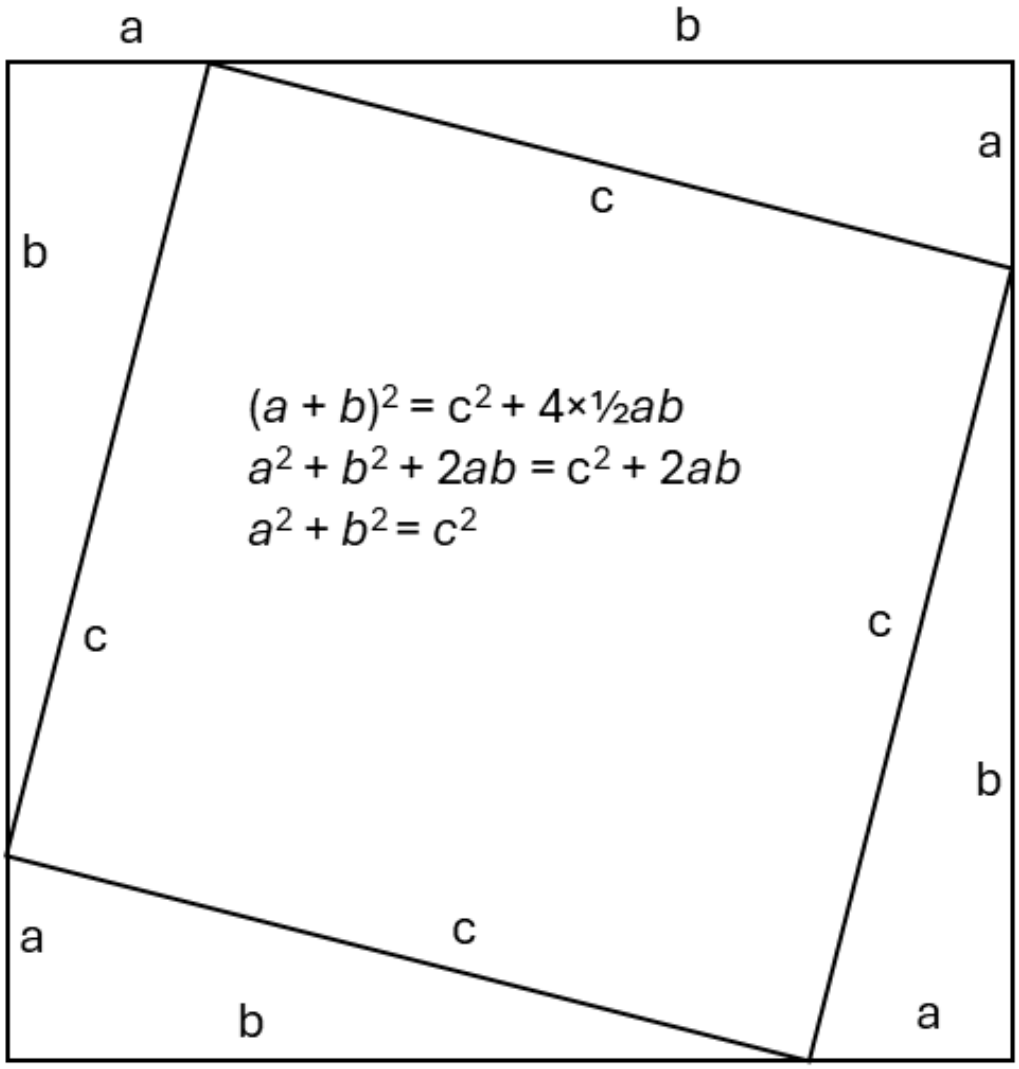
Find a formula to generate all Pythagorean triples.

Cauchy's Functional Equation: Find all functions f such that, for all x and y:

$$f(x + y) = f(x) + f(y)$$

Such functions are called *additive*.

Graphical Demonstration of Pythagoras Theorem



1.2 Problems involving Pythagorean Triples

A *Diophantine* problem is an equation, or system of equations, to be solved in integers. For example finding Pythagorean triples is a Diophantine problem.

Easy Problem: Show that there are infinitely many Pythagorean triples.

Obvious Solution: $(a, b, c) = (3n, 4n, 5n)$ for positive integers n.

A Pythagorean triple (a, b, c) is *primitive* if there is no integer $d > 2$ which is a factor of a, b and c.

Remark 1: Pythagorean triples $(3n, 4n, 5n)$ are primitive only if $n = 1$.

Remark 2: If an integer $d > 2$ is a factor of two sides of a right-angled triangle, then it automatically divides the third side. Therefore, to show a Pythagorean triple is primitive, it is enough to check that any two sides have no common (prime) factor.

Harder Problem: Are there infinitely many primitive Pythagorean triples?

One Solution to Harder Problem: Notice that in the Pythagorean triples $3^2+4^2 = 5^2$, $5^2+12^2 = 13^2$ and $7^2+24^2 = 25^2$, the longer two sides differ by 1. Can we find infinitely many of these ?

If such triples exist, they are surely primitive. If an integer $d > 2$ is a factor of all the edge lengths, then both b and $c = b+1$ are multiples of d, which implies d is a factor of 1, a contradiction. Therefore there is no common factor of b and c.

Suppose then that $a^2 + b^2 = c^2$ with $c = b + 1$. Then, substituting for c:

$$a^2 + b^2 = (b + 1)^2 = b^2 + 2b + 1$$

Subtracting b^2 from each side:

$$a^2 = 2b + 1$$

In this case, $2b + 1$ must be a square number, and indeed an odd square number. Hence generate Pythagorean triples for all integers $m \geq 1$:

$$\begin{aligned} a &= 2m + 1 \\ 2b + 1 &= (2m + 1)^2 = 4m^2 + 4m + 1 \\ b &= 2m(m + 1) \\ c &= b + 1 = 2m^2 + 2m + 1 = m^2 + (m + 1)^2 \end{aligned}$$

A Claim implying Infinitely Many Primitive Triples: Suppose that m and n are integers with $m < n$, no common factor and not both odd. Then

$$\begin{aligned} a &= n^2 - m^2 \\ b &= 2mn \\ c &= m^2 + n^2 \end{aligned}$$

is a primitive Pythagorean triple.

Remark: This generalises the previous example by allowing general $n > m$ in place of $n = m + 1$.

Proof: It is easy to show that the algorithm produces Pythagorean triples, as

$$\begin{aligned} (m^2 + n^2)^2 &= m^2 + n^2 + 2m^2n^2 \\ &= m^2 + n^2 - 2m^2n^2 + 4m^2n^2 \\ &= (n^2 - m^2)^2 + (2mn)^2 \end{aligned}$$

To see that this is a primitive Pythagorean triple, suppose that a prime p is a factor both of $n^2 - m^2$ and of $m^2 + n^2$. That implies also that $2m^2 = (m^2 + n^2) - (n^2 - m^2)$ is a multiple of p, as is $2n^2 = (m^2 + n^2) + (n^2 - m^2)$. Since m^2 and n^2 have (by hypothesis) no common factor, the only possibility is $p = 2$. But that would apply $m^2 + n^2$ is a multiple of 2, contradicting that m and n are not both odd, nor both even.

Therefore, as there is no common prime factor, the triple is a primitive Pythagorean triple.

Harder Question: Can all primitive Pythagorean triples be represented as $n^2 - m^2, 2mn, m^2 + n^2$?

To answer this, we need some more number theory. But before we do that, let us look at Cauchy's functional equation.

1.3 Cauchy's Functional Equations

1. Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{Z}$.

2. Find all functions $f : \mathbb{Q} \to \mathbb{Q}$ such that $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{Q}$.

3. (The endomorphism problem). Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all $x, y \in \mathbb{Z}$

$\mathbb{Z}$ is the set of integers (negative, zero or positive). $\mathbb{Q}$ is the set of *rational numbers*, that is, the set of numbers that can be expressed as an integer numerator, divided by an integer (non-zero) denominator.

The $\mathbb{Q}$ stands for *quotient* while $\mathbb{Z}$ stands for *Zahl*, which is number in German.

Solution to Cauchy's Equation over $\mathbb{Z}$.

The question is to find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x+y) = f(x) + f(y)$ for all integers x, y.

I **claim** there is some $c \in \mathbb{Z}$ such that $f(x) = cx$ for all $x \in \mathbb{Z}_{>0}$. That is clearly sufficient to solve the functional equation, but is it necessary?

To show that $f(x)$ is necessarily a linear function, let us suppose the opposite and derive a contradiction.

Let us suppose f satisfies Cauchy's functional equation, and define $c = f(1)$. Now consider the smallest positive integer for which applying f is not the same as multiplying by c. That smallest counterexample (if it exists) cannot be 1, as $f(1) = c \cdot 1$, so must be at least 2. Let us call that smallest counterexample $x+1$, so that $f(x+1) \neq c(x+1)$. As $x+1$ is the smallest counterexample, then x is not a counterexample and $f(x) = cx$. But now Cauchy's functional equation implies $f(x+1) = cx + c = x(x+1)$ contradicting the assumption that$f(x+1) \neq c(x+1)$. As there is no smallest counterexample, there can be no counterexample at all, and so $f(x) = cx$ for all positive integers x.

Now it remains to sweep up zero and negative numbers.

Putting $y = 0$ gives $f(x) = f(x) + f(0)$, implying $f(0) = 0$.

Putting $y = -x$ for$x > 0$ gives $f(0) = f(x) + f(-x)$ so $f(-x) = -f(x) = -cx$

This proves that all solutions $f : \mathbb{Z} \to \mathbb{Z}$ of Cauchy's functional equation are the linear functions $f(x) = cx$.

Solution to Cauchy's Equation over $\mathbb{Q}$.

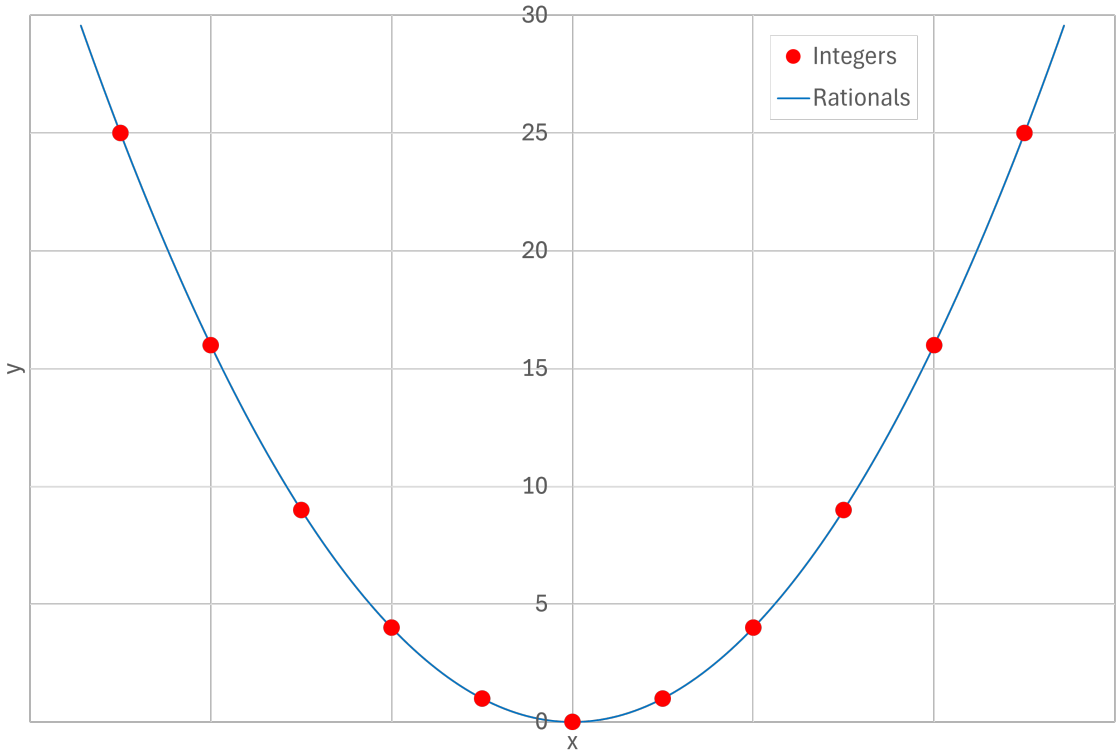
I claim that if $f : \mathbb{Q} \to \mathbb{Q}$ satisfies Cauchy's functional equation, then $f(x) = cx$ for some $c \in \mathbb{Q}$ and all $x \in \mathbb{Q}$.

The proof is similar to the proof over $\mathbb{Z}$. Show that for all $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$

$$f\left(\frac{p}{q}\right) = pf\left(\frac{1}{q}\right)$$

Then set $p = q$ with $c = f(1)$ to complete the proof.

Graph of $y = x^2$ for various Number Sets:



1.4 Integers, Primes and Factors

You might see $\mathbb{N}$ for the *natural numbers*, sometimes $\{0, 1, 2, 3 \ldots\}$ or $\{1, 2, 3 \ldots\}$ but there is no agreement on whether $\mathbb{N}$ includes zero. If you use $\mathbb{N}$ (not recommended) be sure to state clearly whether you mean $\mathbb{Z}_{>0}$ or $\mathbb{Z}_{\geq 0}$.

Given two positive integers x and y, we say that x is a *factor* of y if there exists another positive integer z such that $y = xz$. A *prime* number is a positive integer which has exactly two factors: 1 and itself. The number 1 (a *unit*) is not considered a prime number. Positive integers that are not 1 and not primes are *composite*.

Two positive integers x and y are *co-prime* or *relatively prime* if they have no common factor besides 1.

Fundamental Theorem of Arithmetic:

1. Every integer $n \geq 2$ is a product of one or more (not necessarily distinct) prime numbers.

2. The prime factorisation is essentially unique, ie two different factorisations contain the same primes, raised to the same powers, but perhaps in a different order.

Proof of 1. Suppose the opposite holds, and there exists a positive integer n which is not a product of primes. Take the smallest such n.

Then either n is prime, or it is not.

If n is prime then it is a product of the one prime, itself.

If n is composite, then it has a prime factor $p > 1$. As n is the smallest positive integer not a product of primes, then the integer n/p is a product of primes. But then $n = p \times n/p$ is a product of primes, a contradiction.

Proof of 2. Not provided here. Most solutions use Bézout's identity and Euclid's lemma. Look them up on Wikipedia.

1.5 Describing all Primitive Triples

Claim: The formula $(n^2 - m^2, 2mn, m^2 + n^2)$ for relatively prime $m < n$ generates all Pythagorean triples.

Proof: First note that if (a, b, c) is a primitive Pythagorean triple, then one of (a, b) is even, and the other odd.

It is clear they cannot both be even, as that would contradict the triple being primitive.

To see why a and b cannot both be odd, we notice that squares of any integer must be either multiple of 4, or one more than a multiple of 4 (why?). Therefore the sum of two odd squares leaves a remainder of 2 on division by 4, and cannot be a square. Thus, one of a, b must be odd, the other even.

Without loss of generality, let us suppose that a is odd and b is even, which implies c is also odd. The Pythagorean equation then becomes:

$$\left(\frac{b}{2}\right)^2 = \frac{c^2 - a^2}{4} = \left(\frac{c-a}{2}\right)\left(\frac{c+a}{2}\right) \tag{2}$$

Now, it cannot be the case that $\frac{c-a}{2}$, $\frac{c+a}{2}$ have a common

prime factor, because, if they did, then c and a would both be multiples of that prime factor, contradicting (a, bc) being a primitive triple.

Now factorise $\frac{b}{2}$ into a product of primes using the fundamental theorem of arithmetic. Squaring that product, all primes are raised to an even power. As the two factors on the right hand side have no common prime factor, and as the left hand size is a perfect square, then every prime on the right hand side is also raised to an even power. This implies that the factors on the right-hand side must also be perfect squares. Let us then write:

$$m^2 = \frac{c-a}{2}; n^2 = \frac{c+a}{2}$$

This finally gives the representation $a = n^2 - m^2$, $c = m^2 + n^2$ and so $b = 2mn$, proving the claim.

Question: Can all Pythagorean triples (not necessarily primitive) be represented as $n^2 - m^2, 2mn, m^2 + n^2$ for some integers m, n?

Answer: No. Counter-example $(9, 12, 15)$.

1.6 Related Problem: Squares in Arithmetic Progression

Show there are infinitely many relatively-prime positive integer triples (x, y, z) such that x^2, y^2, z^2 is an arithmetic progression.

Hint: As $z^2 - x^2 = 2(y^2 - x^2)$ so x, z are of the same *parity* (both odd or both even) so we can write $x = b - a$ and $z = a + b$. Now reduce this to a problem of Pythagorean triples.

1.7 Just for Completeness: Real Numbers

$\mathbb{R}$ is the set of *real numbers* that is, the set of rational numbers and limits of rational numbers. Adding limits is a common idea in mathematical analysis, called *completing* a (metric) space.

For example, a right angled triangle with side lengths 1, 1 and $\sqrt{2}$. All these edge lengths are real numbers. But $\sqrt{2}$ is not a rational number. It is an irrational number. The same is true of $\pi = 3.14159265...$ (proofs of irrationality not included here).

It is possible to approximate $\sqrt{2}$ arbitrarily closely with rational numbers. For example, let $a_0 = 2$ and, for $n \in \mathbb{Z}_{\geq 0}$ define

$$a_{n+1} = \frac{a_n}{2} + \frac{1}{a_n}$$

It is easy to see that the sequence $(a_n : n \geq 0)$ are all rational numbers. Numerical calculations appear to converge to a limit (this is called iteration):

n	0	1	2	3	4	5
a_n	2	1.5	1.416666667	1.414215686	1.414213562	1.414213562

The limit should satisfy:

$$a = \frac{a}{2} + \frac{1}{a}$$

Subtracting $\frac{a}{2}$ from each side gives

$$\frac{a}{2} = \frac{1}{a}$$

Multiplying each side by $2a$ gives $a^2 = 2$, so $a = \sqrt{2}$ given that $a > 0$. This iteration is the algorithm most computer chips use to calculate $\sqrt{2}$.

More than this, it is possible to approximate *any* real number arbitrarily closely with rational numbers. In mathematical terms, the rational numbers $\mathbb{Q}$ are *dense* in the real numbers $\mathbb{R}$. There is no interval of the real numbers, of length > 0, which does not contain a rational number.

The integers $\mathbb{Z}$ are not dense in $\mathbb{R}$. That is because we cannot approximate real numbers arbitrarily closely with integers. The closest integer to π is 3, and we can get no closer.

Pythagorean triples in $\mathbb{R}$ are not interesting. We can pick any $a, b > 0$ and write $c = \sqrt{a^2 + b^2}$.

2 11:30-12:30 Solutions in $\mathbb{Z}\left[\sqrt{2}\right]$

2.1 The Ring $\mathbb{Z}$

Algebraists say the set $\mathbb{Z}$ of integers is a *ring* because:

- It is closed under addition and subtraction.
- It has an additive identity, 0.
- It is closed under multiplication.
- It has a multiplicative identity, 1.

The sets $\mathbb{Q}$, $\mathbb{R}$ are also rings, but they are special kinds of rings which are also closed under division (except by 0).

The set $\mathbb{Z}_{>0}$ is not a ring, because it is not closed under subtraction.

Algebraists can construct more general rings (not considered here) which are not subsets of $\mathbb{R}$, but where addition and multiplication follow certain rules (axioms).

Question: How many theorems involving $\mathbb{Z}$ apply to rings in general?

2.2 The Ring $\mathbb{Z}\left[\sqrt{2}\right]$

Consider the set: $\mathbb{Z}\left[\sqrt{2}\right] \subset \mathbb{R}$, defined as:

$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{u + v\sqrt{2} : u \in \mathbb{Z}, v \in \mathbb{Z}\right\}$$

Algebraic Properties of $\mathbb{Z}\left[\sqrt{2}\right]$
Some properties in common with $\mathbb{Z}$:

- Contains 0 and 1
- Closed under addition:

$$u + v\sqrt{2} + w + x\sqrt{2} = u + v + (v + x)\sqrt{2}$$

- Closed under multiplication:

$$(u + v\sqrt{2})(w + x\sqrt{2}) = uw + 2vx + (ux + vw)\sqrt{2}$$

So $\mathbb{Z}\left[\sqrt{2}\right]$ is also a *ring*.
But there are also some differences from $\mathbb{Z}$:

- $\mathbb{Z}\left[\sqrt{2}\right]$ has many *units*, that is elements $u \in \mathbb{Z}\left[\sqrt{2}\right]$ such that $u^{-1} \in \mathbb{Z}\left[\sqrt{2}\right]$. Examples:

$$\begin{array}{cc} \sqrt{2}-1 & \sqrt{2}+1 \\ 1-\sqrt{2} & -1-\sqrt{2} \\ \pm(\sqrt{2}-1)^n & \pm(\sqrt{2}+1)^n \end{array}$$

- In contrast, the only units in $\mathbb{Z}$ are ± 1.

Topological Property The set $\mathbb{Z}\left[\sqrt{2}\right]$ is dense in $\mathbb{R}$.
Why? Take a real number x and a positive integer k.
Then there is an integer n, depending on k, such that:

$$n \leq \left(\sqrt{2}+1\right)^k x < n+1$$

It follows that:

$$\left(\sqrt{2}-1\right)^k n \leq x < \left(\sqrt{2}-1\right)^k (n+1)$$

Both the left hand side and the right hand side are elements of $\mathbb{Z}\left[\sqrt{2}\right]$. By making k large (so in general n also becomes large) we can find elements of $\mathbb{Q}\left[\sqrt{2}\right]$ as close as we wish to any real x.

2.3 Some Simple Questions in $\mathbb{Z}\left[\sqrt{2}\right]$

1. Distinctness: If $u+v\sqrt{2} = w+x\sqrt{2}$ for $u, v, w, x \in \mathbb{Z}$, does it follow that $u = w$ and $v = x$?

2. How can we tell if $u+v\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$ is a square number in $\mathbb{Z}\left[\sqrt{2}\right]$?

3. Is $\pi \in \mathbb{Z}\left[\sqrt{2}\right]$?

An informal description of the distinctness criterion is as follows. Suppose we have a million numbers written in an array with 1000 rows and 1000 columns. In column u and row v write the number$u+v\sqrt{2}$. Are all those million numbers different, or could the same number appear more than once?

Distinctness Proof: Write the equation as:

$$u - w = (x - v)\sqrt{2}$$

If one side is non-zero, then both sides are non-zero, but that would imply

$$\sqrt{2} = \frac{u - w}{x - v}$$

contradicting the irrationality of $\sqrt{2}$. Therefore, $u + v\sqrt{2} = w + x\sqrt{2}$ for $u, v, w, x \in \mathbb{Z}$ only if $u = w$ and $v = x$.

Detecting Squares: When is $u + v\sqrt{2}$ a square in $\mathbb{Z}\left[\sqrt{2}\right]$?

Solution: If $u + v\sqrt{2} = (a + b\sqrt{2})^2$ then $u = a^2 + 2b^2$ and $v = 2ab$. It then follows that:

$$u^2 - 2v^2 = a^4 + 4a^2b^2 + 4b^4 - 8a^2b^2 = (a^2 - 2b^2)^2$$

In particular, the left-hand-side is a square number in $\mathbb{Z}$. It follows that

$$a^2 = \frac{1}{2}\left(u \pm \sqrt{u^2 - 2v^2}\right)$$
$$b^2 = \frac{1}{4}\left(u \mp \sqrt{u^2 - 2v^2}\right)$$

If any combination of $\pm$ gives square numbers on the left hand side, then $u + v\sqrt{2}$ is square in $\mathbb{Z}\left[\sqrt{2}\right]$.

It is MUCH harder (not included) to show that $\pi \notin \mathbb{Z}\left[\sqrt{2}\right]$.

2.4 Finding Pythagorean Triples in $\mathbb{Z}\left[\sqrt{2}\right]$

If we can choose $a, b, c \in \mathbb{Z}\left[\sqrt{2}\right]$, there are more Pythagorean triples. For example, the isosceles right-angled triangle:

$$1^2 + 1^2 = (\sqrt{2})^2$$

Armed with a squareness test, we find more by trial-and-error:

$$1^2 + (2\sqrt{2})^2 = 3^3$$
$$(2\sqrt{2} - 1)^2 + (4 + 4\sqrt{2})^2 = (7 + 2\sqrt{2})^2$$
$$(6\sqrt{2} - 3)^2 + (2\sqrt{2})^2 = (9 - 2\sqrt{2})^2$$

2.5 Functional Equations in $\mathbb{Z}\left[\sqrt{2}\right]$

1. Find all functions $f : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{Z}\left[\sqrt{2}\right]$ such that $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{Z}\left[\sqrt{2}\right]$.

2. Find all endomorphisms $f : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{Z}\left[\sqrt{2}\right]$ such that $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all $x, y \in \mathbb{Z}\left[\sqrt{2}\right]$.

Solution: For part 1, there must be $c, d \in \mathbb{Z}\left[\sqrt{2}\right]$ such that

$$f\left(u + v\sqrt{2}\right) = cu + dv$$

Then applying part 2 with $x = y = 1$ gives $c = c^2$, so $c = 0$ or $c = 1$. Applying part 2 with $x = y = \sqrt{2}$ gives $2c = d^2$.

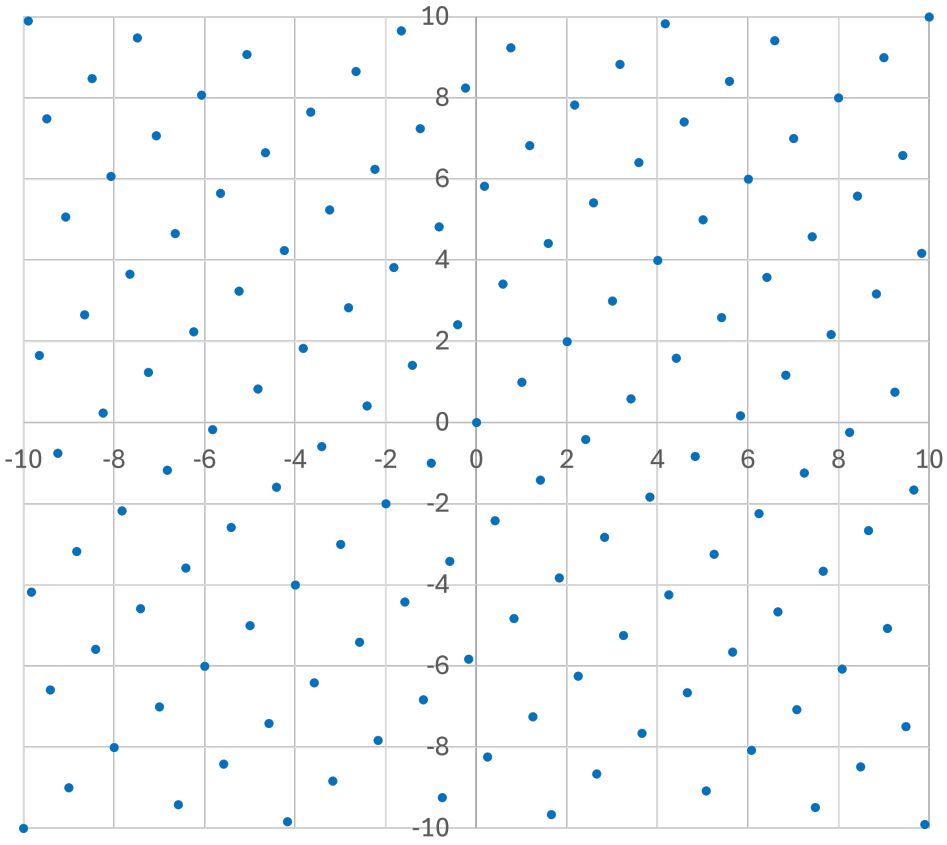
This leads to three endomorphisms (all of which work for general x, y):

Function	c	d
Zero	0	0
Identity	1	$\sqrt{2}$
Conjugate	1	$-\sqrt{2}$

Note that the conjugate function is *not* of the form $f(x) = cx$ for some $c \in \mathbb{Z}\left[\sqrt{2}\right]$. Conjugation is self-inverse (an involution).

The fact that conjugation is an endomorphism implies that if $x \in \mathbb{Z}\left[\sqrt{2}\right]$ satisfies an algebraic equation with integer coefficients, then so does the conjugate of x.

Graph of the Conjugate Function



2.6 Factorisation in $\mathbb{Z}[\sqrt{2}]$

- We say $x \in \mathbb{Z}\left[\sqrt{2}\right]$ is a factor of $y \in \mathbb{Z}\left[\sqrt{2}\right]$ if there is another $z \in \mathbb{Z}\left[\sqrt{2}\right]$ such that $y = xz$.
- What does it mean to say $p \in \mathbb{Z}\left[\sqrt{2}\right]$ is *prime*? Answer: only factors of p are
  - p
  - All units
  - p multiplied by any unit.
- Which primes $p \in \mathbb{Z}$ are also primes in $\mathbb{Z}\left[\sqrt{2}\right]$? Not $p = 2$, because $2 = \sqrt{2}^2$. And not $p = 7 = \left(3 - \sqrt{2}\right)\left(3 + \sqrt{2}\right)$ and not $17 = \left(5 - 2\sqrt{2}\right)\left(5 + 2\sqrt{2}\right)$. On the other hand it can be shown that 3, 5, 11, 13 are prime in $\mathbb{Z}\left[\sqrt{2}\right]$.
- Can every $n \in \mathbb{Z}\left[\sqrt{2}\right]$ be expressed as a product of primes? What goes wrong when you try to adapt the proof for $\mathbb{Z}$?
- Are prime factorisations unique? Yes, but hard to prove.
- Say $x, y \in \mathbb{Z}\left[\sqrt{2}\right]$ are *co-prime* if the only common factors of x and y are units. That allows the definition of primitive Pythagorean triples.

Interesting fact: It is not yet known in general for which positive (non-square) integers d the ring $\mathbb{Z}[\sqrt{d}]$ has unique factorisation into primes, or even if there are infinitely many such d.