PYTHAGOREAN TRIPLES

KEITH CONRAD

1. Introduction

A *Pythagorean triple* is a triple of positive integers (a, b, c) where $a^2 + b^2 = c^2$. Examples include $(3, 4, 5)$, $(5, 12, 13)$, and $(8, 15, 17)$. Below is an ancient Babylonian tablet listing 15 Pythagorean triples. It is called Plimpton 322 (George Arthur Plimpton donated it to Columbia University). For more information about it, see [1].

Plimpton 322

Some Pythagorean triples are scalar multiples of other triples: $(6, 8, 10)$ is twice $(3, 4, 5)$. We call a triple (a, b, c) *primitive* when the three integers have no common factor. For any triple (a, b, c), if d is the greatest common divisor of all three terms then $(a/d, b/d, c/d)$ is a primitive triple and the original triple is a scalar multiple of this, so finding all Pythagorean triples is basically the same as finding all primitive Pythagorean triples. Our goal is to describe the primitive Pythagorean triples.

We will be using different characterizations of primitive triples, as described in the following lemma.

Lemma 1.1. *For a Pythagorean triple (a, b, c), the following properties are equivalent:*

(1) *a, b, and c have no common factor, i.e., the triple is primitive,*
(2) *a, b, and c are pairwise relatively prime,*
(3) *two of a, b, and c are relatively prime.*

Proof. To show (1) implies (2), we prove the contrapositive. If (2) fails then two of a, b, and c have a common prime factor. Suppose a prime p divides a and b. Then $c^2 = a^2 + b^2$ is divisible by p, and since $p \mid c^2$ also $p \mid c$, so p is a common factor of a, b, and c. A similar argument works using a common prime factor of a and c or of b and c. Thus (1) fails.

It is easy to see that (2) implies (3) and (3) implies (1). □

Theorem 1.2. *If (a, b, c) is a primitive Pythagorean triple then one of a or b is even and the other is odd. Taking b to be even,*

$$\boxed{a = k^2 - \ell^2, \quad b = 2k\ell, \quad c = k^2 + \ell^2} \tag{1.1}$$

for integers k and ℓ with $k > \ell > 0$, $(k, \ell) = 1$, and $k \not\equiv \ell \bmod 2$. Conversely, for such integers k and ℓ the above formulas yield a primitive Pythagorean triple.

k	ℓ	a	b	c
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25

TABLE 1. Examples of Primitive Triples

Table 1 lists examples of k and ℓ for some primitive triples. Notice the triple $(8, 15, 17)$ occurs in the table as $(15, 8, 17)$ due to the convention in Theorem 1.2 that the middle term of the triple is even. Since $k \not\equiv \ell \bmod 2$, one of k and ℓ is even and the other is odd. The first two rows in Table 1 shows either k or ℓ can be even; it depends on the triple (a, b, c). How it depends on the triple will be seen at the end of Section 3.

Let's first check that the formula in Theorem 1.2 always yields primitive Pythagorean triples. For all k and ℓ in $\mathbf{Z}$, the formula

$$(k^2 - \ell^2)^2 + (2k\ell)^2 = (k^2 + \ell^2)^2$$

is true, so $(k^2 - \ell^2, 2k\ell, k^2 + \ell^2)$ is a Pythagorean triple when $k > \ell > 0$.[1] When $(k, \ell) = 1$ and $k \not\equiv \ell \bmod 2$, let's check $(k^2 - \ell^2, 2k\ell, k^2 + \ell^2)$ is a primitive triple. This follows (by Lemma 1.1) from showing $k^2 - \ell^2$ and $k^2 + \ell^2$ are relatively prime. If d is a (positive) common divisor of $k^2 - \ell^2$ and $k^2 + \ell^2$ then d divides their sum and difference, which are $2k^2$ and $2\ell^2$. Since $k^2 + \ell^2$ and $k^2 - \ell^2$ are odd, d is odd, so $d \mid k^2$ and $d \mid \ell^2$. Since k and ℓ are relatively prime, so are k^2 and ℓ^2, so $d = 1$.

If we relax any of the conditions on k and ℓ in Theorem 1.2 we won't get a primitive Pythagorean triple. For instance, taking $k = 3$ and $\ell = 1$ produces the triple $(8, 6, 10)$. The condition $k \not\equiv \ell \bmod 2$ is violated here.

In the next two sections we will show in *two ways*, one algebraic and the other geometric, that every primitive Pythagorean triple (a, b, c) arises in the form given by Theorem 1.2: using unique factorization in $\mathbf{Z}$ and using intersections of lines and circles. Then we will put the parametric formula in Theorem 1.2 to work and see some generalizations.

2. Proof of Theorem 1.2 by algebra

To show that one of a and b is odd and the other is even, suppose a and b are both odd. Then $a^2 \equiv b^2 \equiv 1 \bmod 4$, so $c^2 = a^2 + b^2 \equiv 2 \bmod 4$. However, 2 mod 4 is not a

[1]Euclid, in Lemma 1 to Prop. 29 in Book X of his *Elements*, says a geometric formula equivalent to $(a, b, c) = (mn, (m^2 - n^2)/2, (m^2 + n^2)/2)$, where $m \equiv n \bmod 2$, produces Pythagorean triples. This is (1.1) with $m = k + \ell$ and $n = k - \ell$. See http://aleph0.clarku.edu/~djoyce/elements/bookX/propX29.html for a conversion of Euclid's geometric Lemma 1 to an algebraic formula. Euclid did not claim his formula gives all primitive triples. Who showed it does? See https://hsm.stackexchange.com/questions/14778.

square. Thus a or b is even. If both a and b are even the triple (a, b, c) is not primitive, a contradiction. That shows one of a or b is odd and the other is even, so $c^2 = a^2 + b^2$ is odd.

Taking b to be the even choice among a and b (swap their order if necessary), rewrite $a^2 + b^2 = c^2$ as

$$b^2 = c^2 - a^2 = (c + a)(c - a).$$

Both a and c are odd, so $c + a$ and $c - a$ are even. Dividing by 4,

$$\left(\frac{b}{2}\right)^2 = \frac{c+a}{2}\frac{c-a}{2}. \tag{2.1}$$

The two integers on the right, $(c+a)/2$ and $(c-a)/2$, are relatively prime: if d is a common divisor then it divides their sum and difference, which are c and a, and those are relatively prime, so $d = 1$. Since $c > a > 0$, both factors on the right side of (2.1) are *positive*. Now we'll use the following lemma, which is a consequence of unique factorization in $\mathbf{Z}$.

Lemma 2.1. *If $xy = z^2$ where $x, y, z \in \mathbf{Z}^+$ and $(x, y) = 1$, then x and y are both squares.*

Proof. The result is clear when x or y is 1, so let $x, y > 1$. Write them both in terms of their prime factorizations:

$$x = p_1^{e_1} \cdots p_k^{e_k}, \quad y = q_1^{f_1} \cdots q_\ell^{f_\ell}$$

for distinct primes $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ and positive exponents e_i and f_j. No p_i and q_j are equal since $(x, y) = 1$.

We have

$$xy = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_\ell^{f_\ell} = z^2.$$

In z^2, each prime factor of z has even multiplicity, so the e_i's and f_j's are even by unique factorization, say $e_i = 2e_i'$ and $f_j = 2f_j'$. Then

$$x = (p_1^{e_1'} \cdots p_k^{e_k'})^2, \quad y = (q_1^{f_1'} \cdots q_\ell^{f_\ell'})^2,$$

so x and y are both squares. □

Applying the lemma to $x = (c + a)/2$,$y = (c - a)/2$, and $z = b/2$ in (2.1),

$$\frac{c+a}{2} = k^2, \quad \frac{c-a}{2} = \ell^2 \tag{2.2}$$

for some k and ℓ in $\mathbf{Z}^+$. We noted already that $(c+a)/2$ and $(c-a)/2$ are relatively prime, so k and ℓ are relatively prime. Adding and subtracting the equations in (2.2),

$$\boxed{c = k^2 + \ell^2}, \quad \boxed{a = k^2 - \ell^2},$$

so

$$\left(\frac{b}{2}\right)^2 = k^2\ell^2 \Longrightarrow b^2 = 4k^2\ell^2 \Longrightarrow \boxed{b = 2k\ell},$$

the last step holding because b, k, and ℓ are positive.

It remains to show $k \not\equiv \ell \bmod 2$. If $k \equiv \ell \bmod 2$, then k and ℓ are both even or both odd. Since k and ℓ are relatively prime, they are not both even. If they were both odd then $k^2 + \ell^2$, $2k\ell$, and $k^2 - \ell^2$ would all be even, contradicting primitivity of (a, b, c). Thus $k \not\equiv \ell \bmod 2$.

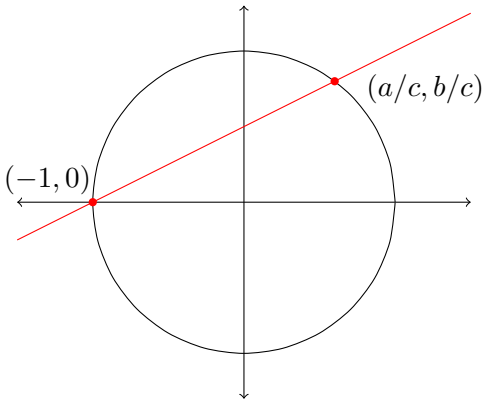
3. Proof of Theorem 1.2 by geometry

Pythagorean triples are connected to points on the unit circle: if $a^2 + b^2 = c^2$ then $(a/c)^2 + (b/c)^2 = 1$. So we get a rational point $(a/c, b/c)$ on the unit circle $x^2 + y^2 = 1$.

For a primitive Pythagorean triple (a, b, c), the first paragraph of the previous proof shows we can take a odd and b even. Having done that, draw the line through $(-1, 0)$ and $(a/c, b/c)$ as in the figure below. Its slope is

$$m = \frac{b/c}{1 + a/c} = \frac{b}{a + c}$$

and the line passes through $(-1, 0)$, so the equation of the line is $y = m(x + 1)$.



Substituting the equation for the line into the equation for the unit circle gives us an equation whose roots are the x-coordinates of the two points on both the line and the circle:

$$1 = x^2 + y^2 = x^2 + (m(x + 1))^2 = (1 + m^2)x^2 + 2m^2x + m^2,$$

so

$$(1 + m^2)x^2 + 2m^2x + m^2 - 1 = 0. \tag{3.1}$$

Since $(-1, 0)$ and $(a/c, b/c)$ lie on both the line and the circle, the two roots of (3.1) are -1 and a/c. The sum of the roots is $-2m^2/(1 + m^2)$, so

$$-1 + \frac{a}{c} = -\frac{2m^2}{1 + m^2}.$$

Thus

$$\frac{a}{c} = 1 - \frac{2m^2}{1 + m^2} = \frac{1 - m^2}{1 + m^2}.$$

Since $(a/c, b/c)$ is on the line $y = m(x + 1)$,

$$\frac{b}{c} = m\left(\frac{a}{c} + 1\right) = m\left(\frac{1 - m^2}{1 + m^2} + 1\right) = \frac{2m}{1 + m^2}.$$

Since m is the slope of a line connecting $(-1, 0)$ to a point on the unit circle in the first quadrant, $0 < m < 1$. Write $m = b/(a + c)$ in reduced form as $m = \ell/k$ with relatively prime k and ℓ in $\mathbf{Z}^+$. Since $m < 1$, $k > \ell$. Formulas for the reduced fractions a/c and b/c in terms of m are

$$\frac{a}{c} = \frac{1 - (\ell/k)^2}{1 + (\ell/k)^2} = \frac{k^2 - \ell^2}{k^2 + \ell^2} \tag{3.2}$$

and

$$\frac{b}{c} = \frac{2(\ell/k)^2}{1+(\ell/k)^2} = \frac{2k\ell}{k^2+\ell^2}. \tag{3.3}$$

By definition, k and ℓ are relatively prime. Let's check that $k \not\equiv \ell \bmod 2$. If $k \equiv \ell \bmod 2$ then k and ℓ are both even or both odd, and they are not both even since they are relatively prime. So k and ℓ are odd. Then the fraction $2k\ell/(k^2+\ell^2)$ in (3.3) has an even numerator and denominator, so it simplifies further:

$$\frac{2k\ell}{k^2+\ell^2} = \frac{k\ell}{(k^2+\ell^2)/2}.$$

The numerator on the right is odd, so the numerator of the reduced form of this fraction (divide numerator and denominator by their greatest common factor) is odd. The reduced form is b/c by (3.3), so b is odd. But b is even by hypothesis, so we have a contradiction. Thus k and ℓ are not both odd, so $k \not\equiv \ell \bmod 2$.

From the end of Section 1, the three numbers $k^2-\ell^2$, $2k\ell$, and $k^2+\ell^2$ form a Pythagorean triple and the first and third numbers are relatively prime, so the triple is primitive by Lemma 1.1. Therefore the fractions on the right in (3.2) and (3.3) are in reduced form. The fractions a/c and b/c are also in reduced form since the triple (a,b,c) is primitive, so the (positive) numerators and denominators match:

$$a = k^2-\ell^2, \quad b = 2k\ell, \quad c = k^2+\ell^2.$$

This concludes the geometric proof of Theorem 1.2.

Remark 3.1. While this derivation was motivated by geometry, the calculations were pure algebra and we could formulate them without any reference to a picture. That is, if we have numbers x and y where $x^2+y^2=1$ and $x \neq -1$, we can (without motivation) define the number m by declaring it to fit the condition $y = m(x+1)$, namely define $m = y/(x+1)$. Substituting $m(x+1)$ for y in $x^2+y^2=1$ tells us

$$x^2 + m^2(x+1)^2 = 1,$$

and expanding the square gives

$$0 = (1+m^2)x^2 + 2m^2x + (m^2-1) = (1+m^2)(x+1)\left(x + \frac{m^2-1}{1+m^2}\right),$$

so from $x \neq -1$ we have $x = (1-m^2)/(1+m^2)$ and $y = m(x+1) = 2m/(1+m^2)$.

One nice consequence of our geometric derivation of the formula for primitive Pythagorean triples (a,b,c) is that it tells us which of k or ℓ will be even. The formula

$$m = \frac{b}{a+c} = \frac{\ell}{k}$$

says that ℓ/k is the reduced form fraction for $b/(a+c)$. We know either ℓ or k is even. We will have k even when $a+c$ is divisible by a higher power of 2 than b is, and ℓ is even when b is divisible by a higher power of 2 than $a+c$ is. For instance, in the triple $(3,4,5)$, $a+c=8$ and $b=4$, so k is even. (Here $k=2$ and $\ell=1$.) The triple $(5,12,13)$ has $a+c = 18 = 2\cdot 9$ and $b = 12 = 2^2\cdot 3$, so ℓ is even. (Here $k=3$ and $\ell=2$.)

4. Applications

Using the parametric formula for primitive Pythagorean triples, we can address questions concerning relations among the sides of a primitive right triangle.

The famous triples $(3, 4, 5)$, and $(5, 12, 13)$, have consecutive terms. What are all the Pythagorean triples (a, b, c) with a pair of consecutive terms (either a and b, or b and c)? Such a triple is primitive since consecutive integers are relatively prime.

First suppose a and b (the two legs) are consecutive. That $a - b = \pm 1$ means

$$(k^2 - \ell^2) - 2k\ell = \pm 1.$$

This can be rewritten as

$$(k - \ell)^2 - 2\ell^2 = \pm 1,$$

where $k - \ell$ is positive and odd and ℓ is positive. Conversely, if we have a solution to $x^2 - 2y^2 = \pm 1$ in $\mathbf{Z}^+$, then necessarily x is odd and $(x, y) = 1$. Let $k = x + y$ and $\ell = y$, so $k > \ell > 0$, $(k, \ell) = 1$, and $k \not\equiv \ell \bmod 2$. Thus $(k^2 - \ell^2, 2k\ell, k^2 + \ell^2)$ is a primitive triple, so finding Pythagorean triples whose legs differ by 1 is *the same* as finding positive integer solutions to the Pell equation $x^2 - 2y^2 = \pm 1$. Some examples are in Table 2.

x	y	k	ℓ	a	b	c
1	1	2	1	3	4	5
3	2	5	2	21	20	29
7	5	12	5	119	120	169
17	12	29	12	697	696	985
41	29	70	29	4059	4060	5741

Table 2. Consecutive Legs

Even if two legs in a primitive triple don't differ by 1, the formula for their difference is still $(k-\ell)^2 - 2\ell^2$, so the possible differences between legs in a primitive triple are precisely the odd values of $x^2 - 2y^2$ for positive integers x and y. Not every odd number can arise in this way, *e.g.*, the equation $x^2 - 2y^2 = 5$ has no integral solution (why?), so no primitive Pythagorean triple has its legs differing by 5.

When a leg and hypotenuse differ by 1, the story is much simpler. The hypotenuse is odd, so it must differ by 1 from the even leg. The difference is

$$k^2 + \ell^2 - 2k\ell = (k - \ell)^2,$$

which is an odd square. This is 1 only if $k = \ell + 1$ (recall $k > \ell$ by convention), leading to the triple $(2\ell + 1, 2\ell^2 + 2\ell, 2\ell^2 + 2\ell + 1)$. The first four examples are in Table 3.

ℓ	$2\ell + 1$	$2\ell^2 + 2\ell$	$2\ell^2 + 2\ell + 1$
1	3	4	5
2	5	12	13
3	7	24	25
4	9	40	41

Table 3. Consecutive Leg and Hypotenuse

Now we look at a connection between Pythagorean triples and pairs of reducible quadratic polynomials, taken from [2]. Here "reducible" means integral coefficients. While

$$x^2 + 4x + 3 = (x+1)(x+3) \text{ and } x^2 + 4x - 3 \text{ is irreducible,}$$

we have

$$x^2 + 5x + 6 = (x+2)(x+3) \text{ and } x^2 + 5x - 6 = (x-1)(x+6).$$

Are there more examples like the second one, where integral polynomials $x^2 + mx + n$ and $x^2 + mx - n$ both factor? Here m and n are nonzero.

If we ask what happens when the sign of m changes, the answer is not interesting. Indeed, if $x^2 + mx + n = (x - r_1)(x - r_2)$ then $x^2 - mx + n = (x + r_1)(x + r_2)$, so either both of these factor (with integral coefficients) or both don't. Therefore in our question on $x^2 + mx \pm n$, we may assume $m > 0$. Since the issue is about sign changes on n, we may take $n > 0$ also.

By the quadratic formula, the roots of $x^2 + mx \pm n$ are $\dfrac{-m \pm \sqrt{m^2 \pm 4n}}{2}$, which are integers exactly when $m^2 \pm 4n = \square$. (Note $m^2 \pm 4n \equiv m \bmod 2$, so the numerator is even when the discriminant is a perfect square.) So we can factor $x^2 + mx + n$ and $x^2 + mx - n$ if and only if

$$m^2 - 4n = d^2, \quad m^2 + 4n = e^2, \quad d \text{ and } e \in \mathbf{Z}.$$

Then $d^2 + e^2 = 2m^2$, so $d \equiv e \bmod 2$. Solving,

$$m^2 = \frac{d^2 + e^2}{2} = \left(\frac{e+d}{2}\right)^2 + \left(\frac{e-d}{2}\right)^2.$$

Thus we have a Pythagorean triple (without a specified even term)

$$\left(\frac{e-d}{2}, \frac{e+d}{2}, m\right), \quad \frac{e-d}{2} < \frac{e+d}{2} < m.$$

As an exercise, show this Pythagorean triple is primitive if and only if $(m, n) = 1$.

There is a one-to-one correspondence

$$\text{Pythagorean triples } (a,b,c) \text{ with } a < b < c \longleftrightarrow \text{reducible } x^2 + mx \pm n,$$

given by

$$(a,b,c) \mapsto x^2 + cx \pm \frac{ab}{2}, \quad x^2 + mx \pm n \mapsto \left(\frac{e-d}{2}, \frac{e+d}{2}, m\right),$$

with $m^2 - 4n = d^2$ and $m^2 + 4n = e^2$. The table below shows some corresponding Pythagorean triples and reducible $x^2 + mx \pm n$. In particular, the example $x^2 + 5x \pm 6$ corresponds to the $(3,4,5)$ triple and thus is the simplest example.

a	b	c	m	n	$x^2 + mx + n$	$x^2 + mx - n$
3	4	5	5	6	$(x+2)(x+3)$	$(x-1)(x+6)$
5	12	13	13	30	$(x+3)(x+10)$	$(x-2)(x+15)$
8	15	17	17	60	$(x+5)(x+12)$	$(x-3)(x+20)$
20	21	29	29	210	$(x+14)(x+15)$	$(x-6)(x+35)$

Using the formula for primitive Pythagorean triples, we can now write a formula for all the reducible pairs of polynomials $x^2 + mx \pm n$ where $(m, n) = 1$:

$$x^2 + (k^2 + \ell^2)x \pm k\ell(k^2 - \ell^2),$$

where $k > \ell > 0$, $(k, \ell) = 1$, and $k \not\equiv \ell \bmod 2$. As an exercise, work out the factorization of this polynomial explicitly in terms of k and ℓ.

5. Generalizations

Our two derivations of the parametric formula for primitive Pythagorean triples, one algebraic and the other geometric, are each worthwhile: they let us extend Theorem 1.2 in different directions.[2]

The algebraic proof of Theorem 1.2 carries over to Pythagorean triples of polynomials in $\mathbf{R}[T]$. These are polynomials $f(T), g(T)$, and $h(T)$ in $\mathbf{R}[T]$ that satisfy

$$f(T)^2 + g(T)^2 = h(T)^2.$$

One example of such a triple is $(T^2 - 1, 2T, T^2 + 1)$. Can we describe all polynomial Pythagorean triples?

There are two features of the Pythagorean triples of integers that play no role when we look at Pythagorean triples of polynomials:

(1) The special attention to positive solutions of $a^2 + b^2 = c^2$ is ignored. We allow any polynomial solutions to $f^2 + g^2 = h^2$ with the only restriction being that f, g, and h are all nonzero.
(2) The number 2 is an invertible constant in $\mathbf{R}[T]$, so the even/odd aspect that occurs for integral Pythagorean triples simply drops out of consideration. Being divisible by 2 is not important in $\mathbf{R}[T]$ since everything is divisible by 2: $f(T) = 2(f(T)/2)$ in $\mathbf{R}[T]$.

We will call a Pythagorean triple of polynomials (f, g, h) *primitive* if the terms in it are pairwise relatively prime. This is the same as any two of the polynomials being relatively prime, and is also the same as (f, g, h) not being a non-constant multiple of another triple (polynomial analogue of Lemma 1.1).

Theorem 5.1. *The primitive Pythagorean triples $(f(T), g(T), h(T))$ in $\mathbf{R}[T]$ are given by the formulas*

$$\boxed{f(T) = c(k(T)^2 - \ell(T)^2), \quad g(T) = \pm 2ck(T)\ell(T), \quad h = \pm c(k(T)^2 + \ell(T)^2)}$$

where $c \in \mathbf{R}^\times$ and $k(T)$ and $\ell(T)$ are relatively prime in $\mathbf{R}[T]$.

Proof. This is left as an exercise in adapting the techniques in the algebraic proof of Theorem 1.2. Note that if two polynomials are relatively prime and multiply to a squared polynomial, the two polynomials have to be squares *up to constant multiple*. This follows from unique factorization in $\mathbf{R}[T]$. □

The geometric proof of Theorem 1.2 gives us a non-trigonometric parametrization of the points on the unit circle: for each point (x_0, y_0) on the circle $x^2 + y^2 = 1$ other than $(-1, 0)$, has the form

$$x_0 = \frac{1 - m^2}{1 + m^2}, \quad y_0 = \frac{2m}{1 + m^2} \tag{5.1}$$

where $m = y_0/(x_0 + 1)$. The formulas in (5.1) for x_0 and y_0 arise by looking at the intersection points of the circle $x^2 + y^2 = 1$ and the line $y = m(x + 1)$, where the linear

[2]Other ways of getting the parametric formula use more advanced ideas: a proof based on factoring in the Gaussian integers is in Theorem 8.3 in https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf and a proof based on Hilbert's Theorem 90 from Galois theory is at the end of Section 4 of https://kconrad.math.uconn.edu/blurbs/galoistheory/linearchar.pdf.

equation describes the lines through $(-1,0)$ other than a vertical line. The correspondences

$$m \rightsquigarrow \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right), \quad (x,y) \rightsquigarrow m = \frac{y}{1+x}, \tag{5.2}$$

between real numbers m and points on the unit circle (x,y) other than $(-1,0)$ are inverses of each other, as the reader can check. Moreover, the formulas have arithmetic content: m is rational if and only if x_0 and y_0 are both rational since the formulas in (5.2) both have rational output if there is rational input. So (5.1) is well-suited to describe the rational points on $x^2+y^2=1$. See Table 4. Compare this to the trigonometric parametrization $(\cos\theta, \sin\theta)$, where nearly all rational points have messy corresponding angles θ.

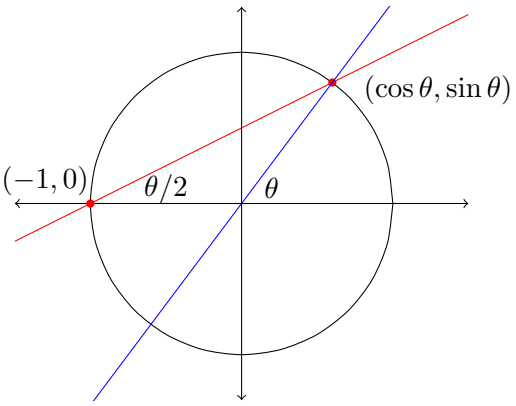
m	x	y
$1/2$	$3/5$	$4/5$
$1/3$	$4/5$	$3/5$
$2/5$	$21/29$	$20/29$
$7/9$	$16/65$	$63/65$

TABLE 4. Rational points from slopes on $x^2+y^2=1$

Comparing the rational parametrization of the unit circle in (5.1) and the trigonometric parametrization $(\cos\theta, \sin\theta)$, we can write (with some assistance from (5.2))

$$\cos\theta = \frac{1-m^2}{1+m^2}, \quad \sin\theta = \frac{2m}{1+m^2}, \quad m = \frac{\sin\theta}{1+\cos\theta}. \tag{5.3}$$

A point on the unit circle at angle θ relative to the origin and the positive x-axis makes an angle $\theta/2$ relative to the point $(-1,0)$ and the x-axis, as shown in the figure below. The slope of a line equals the tangent of the angle the line makes with the x-axis, so $\boxed{m = \tan(\theta/2)}$.



The formulas in (5.3) have a connection to calculus. In terms of the substitution $u = \tan(\theta/2)$, which is motivated by the formula for the slope m above, we can write

$$\cos\theta = \frac{1-u^2}{1+u^2}, \quad \sin\theta = \frac{2u}{1+u^2},$$

and

$$du = \sec^2\left(\frac{\theta}{2}\right)\frac{d\theta}{2} = \left(1+\tan^2\left(\frac{\theta}{2}\right)\right)\frac{d\theta}{2} = (1+u^2)\frac{d\theta}{2} \Longrightarrow d\theta = \frac{2}{1+u^2}\,du.$$

With these formulas, integrals of rational functions of $\cos\theta$ and $\sin\theta$ can be turned into integrals of rational functions of u. This method of integration is called a $\tan(\theta/2)$-substitution or a Weierstrass substitution.[3] It is based on having two different parametrizations of the unit circle, which allow us to express an integral involving one of the parameterizations (with trig functions) as an integral involving the other parametrization (with rational functions).

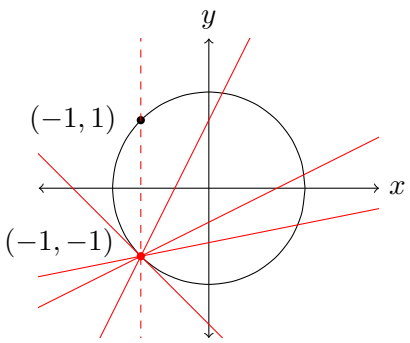
What we just did with rational points on the unit circle is not true just for that curve. If we take any smooth conic in the plane (a smooth curve of degree 2: an ellipse, hyperbola, or parabola) that is defined by an equation having rational coefficients and we know one rational point on the conic, then slopes of lines through that point let us parametrize all the other rational points on the conic. Here is an example of this idea using another circle.

Theorem 5.2. *The rational points on the circle $x^2 + y^2 = 2$ other than $(-1, 1)$ can be described by the formula*

$$\left(\frac{1 + 2m - m^2}{m^2 + 1}, \frac{m^2 + 2m - 1}{m^2 + 1}\right)$$

where $m \in \mathbf{Q}$. A rational point (x, y) other than $(-1, \pm 1)$ arises this way using $m = (y + 1)/(x + 1)$, and $(-1, -1)$ arises this way using $m = -1$.

Proof. The point $(-1, -1)$ lies on the circle. A non-vertical line through $(-1, -1)$ has the form $y = m(x + 1) - 1$. Any line through $(-1, -1)$ intersects the circle in a second point, except for the tangent line $y = -x - 2$ (where $m = -1$).



To find the second point of intersection, substitute the equation of the line into the equation $x^2 + y^2 = 2$ and solve for the two roots of the resulting quadratic in x: one root is 1, and we can find the other root by the same method as in the geometric proof of Theorem 1.2. This will give the x-coordinate formula above, and substituting this into $y = m(x + 1) - 1$ gives the y-coordinate. The only rational point on $x^2 + y^2 = 2$ that we don't find by this method is $(-1, 1)$, which is the second intersection point of the circle with the vertical line through $(-1, -1)$. This vertical line is not described by an equation of the form $y = m(x + 1) - 1$. The parameter value that gives the point $(-1, -1)$ itself is $m = -1$, which is the slope of the tangent line to $x^2 + y^2 = 2$ at $(-1, -1)$ (touching the point $(-1, -1)$ twice, in a sense). □

Remark 5.3. Since $x^2 + y^2 = 2$ if and only if $((x - y)/2)^2 + ((x + y)/2)^2 = 1$, the geometric proof of Theorem 1.2 yields $(x - y)/2 = (1 - m^2)/(1 + m^2)$ and $(x + y)/2 = 2m/(1 + m^2)$. Adding and subtracting these equations recovers the formulas for x and y in Theorem 5.2.

[3]See https://en.wikipedia.org/wiki/Weierstrass_substitution.

Armed with the description of the rational points on $x^2 + y^2 = 2$ in Theorem 5.2, we can get a description of the primitive integral solutions of $a^2 + b^2 = 2c^2$, where primitive means a, b, and c have no common factor (equivalently, this means any two of a, b, and c are relatively prime, *i.e.*, an analogue of Lemma 1.1 holds). In a primitive triple (a, b, c), a and b both must be odd, so $2c^2 \equiv 2 \bmod 8$, hence c is odd as well. For Pythagorean triples, the middle term was chosen to be the even one. The analogue of that here is that we take $c > 0$ and pick the signs on a and b so that $a \not\equiv b \bmod 4$. With these conventions, we have

$$a = k^2 + 2k\ell - \ell^2, \quad b = \ell^2 + 2k\ell - k^2, \quad c = k^2 + \ell^2$$

where $(k, \ell) = 1$, $k \not\equiv \ell \bmod 2$, and $k > 0$. Conversely, any triple defined by these formulas is a primitive solution to $a^2 + b^2 = 2c^2$ with $b \not\equiv a \bmod 4$.

k	ℓ	a	b	c
1	2	1	7	5
1	-2	-7	-1	5
1	4	-7	23	17
4	1	23	-7	29
2	5	-1	41	29

TABLE 5. Primitive Solutions to $a^2 + b^2 = 2c^2$

Integers satisfying $a^2 + b^2 = 2c^2$ are not the sides of a right triangle, but they have an arithmetic interpretation: since $c^2 = \frac{1}{2}(a^2 + b^2)$, c^2 is the average of a^2 and b^2. In other words, a^2, c^2, b^2 is an arithmetic progression of squares (taking $a^2 < b^2$). From Table 5, squaring the entries in the a, b, and c columns yield three such progressions: $1, 25, 49$ (common difference 24), $49, 289, 529$ (common difference 240), and $1, 841, 1681$ (common difference 840). There are infinitely many 3-term arithmetic progressions of squares in $\mathbf{Z}^+$, and we can find all of them from the parametrization of the rational points on $x^2 + y^2 = 2$ in Theorem 5.2.

What about 4-term arithmetic progressions of squares? That is a more complicated story. See https://kconrad.math.uconn.edu/blurbs/ugradnumthy/4squarearithprog.pdf.

REFERENCES

[1] W. Casselman, http://www.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html.
[2] J. L. Poet and D. L. Vestal, Jr., "Curious Consequences of a Miscopied Quadratic," College Math. J. **36** (2005), 273–277.