1 Preliminaries: Definitions and Notation

Our ultimate goal is to prove the following:

Theorem 1.1. *Let a, b, and c be positive integers such that $a^2 + b^2 = c^2$. Further, assume that a, b, and c have no common divisor greater than* 1. *Then we have the following:*

- *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 can therefore assume without loss of generality that b is even.*
- *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.*
  - *We have*

$$a = r^2 - s^2 \tag{1.1}$$
$$b = 2rs \tag{1.2}$$
$$c = r^2 + s^2. \tag{1.3}$$

Every *positive solution to $a^2 + b^2 = c^2$, therefore, has the form $k(r^2 - s^2)$, $k(2rs)$, and $k(r^2 + s^2)$, where r, s are as above, and k is any positive integer.*

Definition 1.2. 1.1. The set of *natural numbers*, denoted $\mathbb{N}$, is the set $\mathbb{N} := \{1, 2, 3, 4, \cdots\}$.

1.2. The set of *integers*, denoted $\mathbb{Z}$, is the set $\mathbb{Z} := \{\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots\}$.

1.3. The set of *rational numbers*, denoted $\mathbb{Q}$, is the set

$$\mathbb{Q} := \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}.$$

That is, a number is rational if and only if it is expressible as a quotient of two integers, the denominator of which is nonzero.

1.4. Let $a, b \in \mathbb{Z}$. Then we say *a divides b*, denoted "$a \mid b$", if and only if there exists some $x \in \mathbb{Z}$ such that $ax = b$. Further, if a does *not* divide b, we shall write "$a \nmid b$".

1.5. If $a, b \in \mathbb{Z}$, then we say that $d \in \mathbb{Z}$ is a *common divisor of a and b* if and only if $d \mid a$ and $d \mid b$. More generally, if $a_1, a_2, \cdots, a_n \in \mathbb{Z}$, then d is a common divisor of $\{a_1, a_2, \cdots, a_n\}$ if and only if for all i with $1 \leq i \leq n$, $d \mid a_i$.

1.6. For integers $a, b \in \mathbb{Z}$, a *greatest common divisor* of a and b, denoted $\gcd(a, b)$ is a nonnegative integer d such that

- $d \mid a$ and $d \mid b$, and
- If $\ell \in \mathbb{Z}$ satisfies $\ell \mid a$ and $\ell \mid b$, then $\ell \mid d$.

More generally, for integers $a_1, a_2, \cdots, a_n \in \mathbb{Z}$, a greatest common divisor for $a_1, a_2, \cdots, a_n$ is a nonnegative integer d such that

- For all i such that $1 \leq i \leq n$, $d \mid a_i$, and
- If $\ell \in \mathbb{Z}$ is such that for all i with $1 \leq i \leq n$, then $\ell \mid a_i$, then we also have $\ell \mid d$.

That is, the greatest common divisor of integers a and b is a nonnegative integer d that *is* a common divisor of a and b and *divisible by* every common divisor of a and b.

Remark. The definition of the greatest common divisor of a and b with which you may be most familiar is the assertion that "$\gcd(a,b)$ is the greatest *of* the common divisors of a and b." In the case of the integers, it can be shown that these two notions are (nearly) equivalent, but the above formulation is frequently more useful.

1.7. If $a,b \in \mathbb{Z}$, then we shall say that a and b are *relatively prime* or *coprime* if and only if $\gcd(a,b) = 1$.

More generally, the integers $a_1, a_2, \cdots, a_n$ are *relatively prime* if and only if $\gcd(a_1, a_2, \cdots, a_n) = 1$. Further, we shall say that these integers are *pairwise relatively prime* if and only if for all i, j such that $1 \le i < j \le n$, $\gcd(a_i, a_j) = 1$.

1.8. Assume that $a,b,n \in \mathbb{Z}$. Then *a is congruent to b modulo n*, denoted $a \equiv b \pmod{n}$, if and only if $n \mid a-b$. The following notation is equivalent: $a \equiv b \mod n$, $a \equiv b\ (n)$, etc. (Where the modulus m is implicit, we may simply write $a \equiv b$.) If a is *not* congruent to b modulo n, then we shall write $a \not\equiv b \pmod{n}$, $a \not\equiv b \mod n$, or $a \not\equiv b\ (n)$.

1.9. An integer $p \in \mathbb{Z}$ is a *prime number* if and only if

- $p \neq 0$ *and* $p \neq \pm 1$, and
- If $p = ab$, where $a,b \in \mathbb{Z}$, then $a = \pm 1$ or $b = \pm 1$.

Remark. Note that under this definition, negative integers (such as -3, -17, or -101, *are* considered prime.

1.10. Let $n > 1$ be a positive integer. Then the set $S \subseteq \mathbb{Z}$ is a *complete residue system modulo n* if and only if for all $a \in \mathbb{Z}$, there exists a *unique* $s \in S$ such that $a \equiv s \pmod{n}$. Equivalently, S is a complete residue system modulo n if and only if $S = \{s_1, s_2, \ldots, s_n\}$, and for all distinct $1 \le i < j \le n$, $s_i \not\equiv s_j \pmod{n}$.

1.11. Let a,b be real numbers. Then an *integer linear combination of a and b* is any expression of the form $ax+by$, where $x,y \in \mathbb{Z}$. More generally, if $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, then an *integer linear combination of* $a_1, a_2, \ldots, a_n$ is any expression of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n,$$

where $x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

2 Numerical Problems with Divisibility and Modular Arithmetic

Intuitively, a is congruent to b modulo n if and only if a and b have the same remainders when divided by n. Some examples:

$$1 \equiv 5 \pmod{4}, \quad -1 \equiv 3 \pmod{4}, \quad 0 \equiv 100 \pmod{25}.$$

In particular, note the following: for fixed $n \in \mathbb{Z}$, congruence modulo n is an *equivalence relation*. Further, modular arithmetic behaves nicely with respect to addition, subtraction, and multiplication. (For example, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bc \pmod{n}$.)

2.1. Find, with justification, all solutions to the following congruences:

(a) $4x \equiv 1 \pmod{7}$

(b) $4x \equiv 1 \pmod{9}$

(c) $4x \equiv 1 \pmod{10}$

(d) $10x \equiv 15 \pmod{25}$

2.2. Compute the following:

(a) $\gcd(12, 18)$

(b) $\gcd(36, 100)$

(c) $\gcd(12, 18, 30)$

(d) For $n \in \mathbb{Z}$, $n \neq 0$, find $\gcd(n, 0)$.

(e) $\gcd(0, 0)$

(f) $\gcd(3759923, 3759924)$
Hint: It may be easier to consider a more general case. What is $\gcd(n, n+1)$? Does it depend upon n?

(g) $\gcd(105076758, 46756518)$

2.3. Find, with justification, all solutions to the following congruences:

(a) $x^2 \equiv 1 \pmod{3}$.

(b) $x^2 \equiv 1 \pmod{5}$.

(c) $x^2 \equiv 1 \pmod{13}$.

(d) $x^2 \equiv -1 \pmod{13}$.

(e) $x^2 \equiv 1 \pmod{15}$.
Note: How do the solutions to this compare to those of #2.3a and #2.3b?)

(f) $x^7 \equiv x \pmod{7}$.

2.4. (a) Find examples of $a, b, c \in \mathbb{N}$ such that $a \mid bc$, but $a \nmid b$ and $a \nmid c$. (Equivalently, $bc \equiv 0 \pmod{a}$, but $b \not\equiv 0 \pmod{a}$ and $c \not\equiv 0 \pmod{a}$.)

(b) Find examples of $a, b, c \in \mathbb{N}$ such that $a|c$ and $b|c$, but $ab \nmid c$.

2.5. Find solutions to the following simultaneous system of congruences, or prove that no solutions are possible.

(a) $x \equiv 1 \pmod{3}$ and $x \equiv 2 \pmod{4}$.

(b) $x \equiv 2 \pmod{5}$ and $x \equiv 1 \pmod{7}$.

(c) $x \equiv 1 \pmod{6}$ and $x \equiv 8 \pmod{14}$.

(d) $x \equiv 5 \pmod{99}$ and $x \equiv 8 \pmod{103}$.

(e) $x \equiv 1 \pmod{11}$, $x \equiv 2 \pmod{13}$, and $x \equiv 3 \pmod{17}$.

3 Proofs with Divisibility and Modular Arithmetic

3.1. Prove that if $a, b \in \mathbb{Z}$ are both positive, and $a \mid b$, then $a \leq b$. As a corollary, prove that if $a, b \in \mathbb{Z}$, and we have both $a \mid b$ and $b \mid a$, then $a = \pm b$.

Note: As a corollary, this proves that *if* a greatest common divisor exists, then it must be unique. If all the integers are zero, then the gcd must also be zero, making it uniquely determined. If not all the given integers are zero, then consider two putatively-different gcds d and d'. Since d is a common divisor and d' is a gcd, $d \mid d'$. Similarly, $d' \mid d$. Assuming, by convention, that $d, d' \geq 0$, since both must be positive, we have $d = d'$.

3.2. Prove that for all $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

3.3. Prove that $\gcd(a, b) > 0$ if and only if there exists a prime $p \in \mathbb{Z}$ such that $p \mid a$ and $p \mid b$ *and* at least one of a and b is nonzero. (To prove this, you may assume the following proposition: for each $n \in \mathbb{Z}$, $n \neq \pm 1$, there exists at least one prime $p > 0$ such that $p \mid n$.)

3.4. Prove or disprove, with justification: there exists a set of positive integers $a_1, a_2, \cdots, a_n$ which is relatively prime but *not* pairwise relatively prime.

3.5. It is often taken as an axiom for the set of integers that their positive elements are *well-ordered*. That is:

For all *nonempty* subsets $S \subseteq \mathbb{N}$, there exists an $\ell \in S$ such that for all $s \in S, s \le \ell$.

Equivalently, every nonempty set of positive integers must have a smallest element. (For the reals, compare this to the set $\{x \in \mathbb{R} : x > 0\}$, which has no smallest element.) Prove that the well-ordering of $\mathbb{N}$ implies the principle of mathematical induction. That is, if P is any statement defined for all $n \in \mathbb{N}$ such that

- $P(1)$ is true, and
- For all $k \in \mathbb{N}$, *if* $P(k)$ is true, *then* $P(k+1)$ is true,

then $P(n)$ is true for all $n \in \mathbb{N}$. (*Hint:* Consider the set $S' := \mathbb{N} \setminus \{n \in \mathbb{N} : P(n) \text{ is true}\}$; that is, $S' = \{n \in \mathbb{N} : P(n) \text{ is false}\}$. If $P(n)$ *is* true for all $n \in \mathbb{N}$, then that is equivalent to saying $S' = \varnothing$. Proceed as proof-by-contradiction: assume $S' \neq \varnothing$. If ℓ is the smallest element of S', then what can we say about $\ell - 1$?)

3.6. If $a, b, m \in \mathbb{Z}$ with $m \neq 0$ and $a \equiv b \pmod{m}$, then $\gcd(a,m) = \gcd(b,m)$.

3.7. *Euclid's Algorithm*: assume that $a, b \in \mathbb{Z}$ with $b \neq 0$. If each $q_i, r_i \in \mathbb{Z}$ are such that

$$\begin{aligned}
a &= bq_1 + r_1, && \text{where } 0 < r_1 < |b| \\
b &= r_1 q_2 + r_2, && \text{where } 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, && \text{where } 0 < r_3 < r_2 \\
\vdots \quad & \quad \vdots && \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, && \text{where } 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n, && \text{where } 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1},
\end{aligned}$$

then $\gcd(a,b) = r_n$. (*Hint:* By the first line, $a \equiv r_1 \pmod{b}$.)

3.8. Let $F_0 := 0$, $F_1 := 1$, and $F_n := F_{n-1} + F_{n-2}$ for all $n \ge 2$; that is, F_n is the nth Fibonacci number. Prove that any two consecutive Fibonacci numbers are relatively prime.

3.9. For this exercise, we shall assume the following proposition:

The Division Algorithm: for all $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \text{ where } 0 \le r < |b|.$$

(This can be deduced from the well-ordering of $\mathbb{N}$, which we shall also implicity assume; see Exercise #3.5 for the definition.)

Prove that the division algorithm and Euclid's Algorithm can be used to *produce* $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a,b)$. Generalize this to show that if $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ are not all zero, then one can *produce* $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ such that

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = \gcd(a_1, a_2, \ldots, a_n).$$

3.10. For fixed $a, b \in \mathbb{Z}$, characterize all $c \in \mathbb{Z}$ such that the equation

$$ax + by = c$$

has a solution with $x, y \in \mathbb{Z}$. (*Note:* the diophantine equation $ax + by = \gcd(a,b)$ is called *Bézout's identity*.) More generally, if $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, then for what $c \in \mathbb{Z}$ does the equation

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = c$$

have a solution with $x_1, x_2, \ldots, x_n \in \mathbb{Z}$?

3.11. Let $a,b \in \mathbb{Z}$ be such that $d := \gcd(a,b) \neq 0$. (Equivalently, at least one of a and b is nonzero.) Prove that if $a = a'd$ and $b = b'd$, then $\gcd(a',b') = 1$. Equivalently,

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1.$$

More generally, if $a_1, a_2, \ldots, a_n$ are not all zero, then we have

$$\gcd\left(\frac{a_1}{\gcd(a_1,a_2,\ldots,a_n)}, \frac{a_2}{\gcd(a_1,a_2,\ldots,a_n)}, \cdots, \frac{a_n}{\gcd(a_1,a_2,\ldots,a_n)}\right) = 1.$$

3.12. Fix $n \in \mathbb{Z}$ with $n > 1$. Let $a \in \{0,1,2,\ldots,n-1\}$, and consider the congruence

$$ax \equiv 1 \pmod{n}.$$

Characterize all a such that the above congruence has a solution $x \in \mathbb{Z}$. If $n = p$, a positive prime, then how many $a \in \{0,1,\ldots,p-1\}$ admit solutions to the congruence $ax \equiv 1 \pmod{p}$? What if $n > 1$ is not a prime?

3.13. (a) Assume $a,b,c \in \mathbb{Z}$, $a \mid bc$, and $\gcd(a,b) = 1$. Prove that $a \mid c$.

(b) Assume that $a,b,p \in \mathbb{Z}$, p is prime, and $p \mid ab$. Prove that $p \mid a$ or $p \mid b$.

(c) Assume that $a,b,c \in \mathbb{Z}$, $a \mid c$, $b \mid c$, and $\gcd(a,b) = 1$. Prove that $ab \mid c$. More generally, if $a_1,a_2,\ldots,a_n \in \mathbb{Z}$ are pairwise relatively prime and each $a_i \mid c$, then

$$a_1 a_2 \cdots a_n \mid c.$$

What if $a_1,a_2,\ldots,a_n$ are merely relatively prime and not *pairwise* relatively prime?

(d) Assume that $a,b \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $n > 1$. Prove that if $\gcd(a,n) = \gcd(b,n) = 1$, then $\gcd(ab,n) = 1$.

3.14. (a) Prove that if $\gcd(a,n) = 1$ and $ab \equiv 0 \pmod{n}$, then $b \equiv 0 \pmod{n}$. Further, prove that if $\gcd(a,n) = 1$, then $ab \equiv ac \pmod{n}$ implies $b \equiv c \pmod{n}$.

(b) Prove that if $\gcd(a,n) = 1$, then the sets

$$\{0,1,2,\ldots,n-1\} \text{ and } \{a\cdot 0, a\cdot 1, a\cdot 2, \ldots, a\cdot(n-1)\}$$

both consist of a complete set of residues modulo n.

(c) *Fermat's Little Theorem:* prove that if $p \in \mathbb{N}$ is prime, then for all $a \in \mathbb{Z}$ such that $p \nmid a$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

3.15. Let $a,b,m,n \in \mathbb{Z}$, with $m,n \geq 2$. Prove that if $\gcd(m,n) = 1$, then there is a solution to the simultaneous system of congruences

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

Can you generalize this to show that the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ \vdots\ &\ \ \vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a solution given suitable conditions on the moduli $m_1, m_2, \ldots, m_k$?

3.16. Assume that $a, b \in \mathbb{Z}$. Prove that $\gcd(a, b) = 1$ if and only if for all $m, n \in \mathbb{N}$, $\gcd(a^m, b^n) = 1$.

3.17. *Rational Root Theorem:* Let $p(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial all of whose coefficients are integers. That is,

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ and $a_n \neq 0$. Prove that if $q \in \mathbb{Q}$ is a root of p—that is, $p(q) = 0$—where $q = \frac{r}{s}$, $r, s \in \mathbb{Z}$, and $\gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$. In particular, if p is *monic* (meaning $a_n = 1$), then any rational root of p must be an integer.

3.18. Assume $x, y \in \mathbb{Z}$. Further, assume $a, b, c, d \in \mathbb{Z}$ satisfy $ad - bc = \pm 1$. Prove that $\gcd(x, y) = \gcd(ax + by, cx + dy)$. Can you generalize?

3.19. Let $n \in \mathbb{N}$ be a positive integer, and let S denote the sum of the base-ten digits of n. Prove that

$$n \equiv S \pmod 9.$$

Can you generalize? For example, what if S_b denotes the sum of the base-b digits of n?

3.20. Prove that if $n > 1$ is odd, then

$$n \mid 1^n + 2^n + 3^n + \cdots + (n-2)^n + (n-1)^n.$$

Are there counterexamples if $n > 2$ is even?

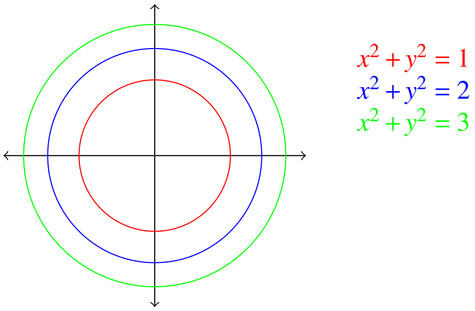
3.21. Find all solutions $p, q \in \mathbb{Z}$ such that $p, q > 0$, p, q are both primes, and

$$q^{p+q} + p^p(p+q)^p = (p^2 + q)^q.$$

4 Rational Points on Curves: Definitions and Examples

Definition 4.1. Let C be a subset of the plane, $\mathbb{R}^2$. Then a point $(x, y) \in C$ is called a *rational point* if and only if $x, y \in \mathbb{Q}$. More generally, if $C \subseteq \mathbb{R}^n$ and $\mathbf{x} := (x_1, x_2, \ldots, x_n) \in C$, then we say $\mathbf{x}$ is a rational point if and only if for all i, $x_i \in \mathbb{Q}$.

We shall consider rational points on circles in the plane whose center is the origin:



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 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?

5 Rational Points on Curves and Pythagorean Triples

Definition 5.1. We say that $(a,b,c) \in \mathbb{Z}^3$ is a *Pythagorean triple* if and only if $a^2 + b^2 = c^2$. Next, we say that (a,b,c) is a *nontrivial Pythagorean triple* if and only if (a,b,c) is a Pythagorean triple and none of a,b,c is zero. Further, we say that (a,b,c) is a *primitive Pythagorean triple* if and only if (a,b,c) is a Pythagorean triple and $\gcd(a,b,c) = 1$. Finally, we say that (a,b,c) is a *positive Pythagorean triple* if and only if it is a Pythagorean triple and $a,b,c > 0$.

Example 5.2. Consider the following:

- Since $3^2 + 4^2 = 5^2$, $(3,4,5)$ is a Pythagorean triple. Further, it is a primitive Pythagorean triple. Other examples of primitive Pythagorean triples include $(5,12,13)$, $(8,15,17)$, and $(7,24,25)$
- Similarly, since $6^2 + 8^2 = 10^2$, $(6,8,10)$ is also a Pythagorean triple. However, $\gcd(6,8,10) = 2 > 1$, so $(6,8,10)$ is not a primitive. Note, however, that $(6,8,10) = (2\cdot 3, 2\cdot 4, 2\cdot 5)$, and $(3,4,5)$ is not only a Pythagorean triple but a *primitive* Pythagorean triple.
- For any $n \in \mathbb{N}$, $(n,0,n)$ is a Pythagorean triple, but it is clearly trivial: $n^2 + 0^2 = n^2$. If $n = \pm 1$, then $(n,0,n) = (\pm 1, 0, \pm 1)$ is trivial but primitive.

Our goal here is to consider rational points on the unit circle to give a complete characterization of all primitive Pythagorean triples. Since every Pythagorean triple is simple an integer multiple of a primitive Pythagorean triple,

5.1. Prove that if (a,b,c) is any nontrivial Pythagorean triple, then it is of the form (da', db', dc') for some unique $d \in \mathbb{N}$, and a unique primitive Pythagorean triple (a', b', c').

5.2. For a Pythagorean triple $(a,b,c) \in \mathbb{Z}^3$, the following are equivalent:

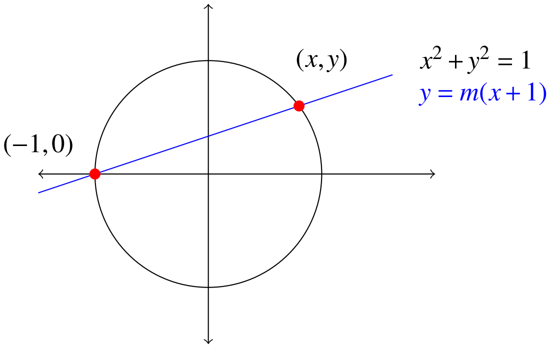
(a) a, b, and c are pairwise relatively prime.

(b) Some particular pair of a, b, and c is relatively prime.

(c) (a,b,c) is a primitive Pythagorean triple.

5.3. 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.

5.4. 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 below:



(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 $m := \frac{s}{r}$. 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.

5.5. Let (a,b,c) be a nontrivial positive, primitive Pythagorean triple. From Exercise #5.3, precisely one of a and b is even, so *now and hereafter, 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 #5.4e, 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.

5.6. Theorem 1.1 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

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

6 Possible Generalizations

It's worth noting that the results above have a number of generalizations worth exploring. These include some of the following:

- How many of the results from Section 3 hold in other number systems? For example, consider the set

  $$\mathbb{Z}[i] := \{a + bi : a,b \in \mathbb{Z}, i^2 = -1\}.$$

  Do we still have greatest common divisors? Primes? Euclid's Algorithm? What if we take the set $\mathbb{R}[x]$ of all polynomials in x with real coefficients rather than $\mathbb{Z}[i]$?

- Can we use this geometric method of identifying rational points on a curve to solve equations over the integers? For example, can we characterize all solutions to the equation $a^2 + b^2 = 2c^2$ by trying to parametrize the rational points on the circle $x^2 + y^2 = 2$? If so, what *are* all such solutions?

- We can consider the system of addition, subtraction, and multiplication mod n. What is its structure? Can we consider $\mathbb{Z}[i]$ modulo some complex number such as $5 - 2i$? Or $\mathbb{R}[x]$ modulo a polynomial like $x^2 + x + 1$?

- What other geometric methods might prove useful in seemingly-unrelated branches of mathematics like number theory?

Good luck with these problems!