4 Topic: All Pythagorean triples

Recall first the discussion about Pythagorean triples in the textbook (pp. 107–109). At the end of the section "Early Solutions of the Pythagorean Equation" the textbook claims that "The converse problem of showing that any Pythagorean triple is necessarily of this form is much more difficult." Out goal in this project is to provide a proof to this "converse problem."

Specifically, the goal is to prove the following theorem.

Theorem 4.1. *Let (a, b, c) be a primitive Pythagorean triple. Then c is odd and exactly one of a and b is even. Assume that b is even. Then there exist relatively prime integers $m < n$, one even and one odd, such that*

$$a = n^2 - m^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

First, let me define terms. The abbreviation gcd stand for *greatest common divisor*. Recall that *relatively prime* for a, b means that $\gcd(a, b) = 1$, i.e., integers a and b have no common prime factors. We call the Pythagorean triple (i.e., three integers that satisfy $a^2+b^2 = c^2$) *primitive* if $\gcd(a, b, c) = 1$. If the Pythagorean triple is not primitive we can always divide a, b, c by the common factor and obtain a primitive triple. Hence if we are capable of producing *all* primitive Pythagorean triples, we know them all.

♢ **4.1.** First I ask you to prove the key fact that you will need to use in the proof of Theorem 4.1. You will need to use *the fundamental theorem of arithmetics* (recall its statement). Prove

Lemma 4.2. *If $xy = z^2$, where x and y are relatively prime integers, then both x and y are squares.*

♢ **4.2** (The general idea of the proof of Theorem 4.1 and hints)**.**

1. First assuming that (a, b, c) is a primitive Pythagorean triple, show that one of a and b must be even and one must be odd, and hence c must be odd. Just consider cases: a, b are both even, a, b are both odd, and conclude that it is not possible. It could be reasonable to start with characterizing squares of even and odd numbers. Without loss of generality assume that a, c are odd and $b = 2z$ is even.

2. Now observing that

$$c^2 - a^2 = (c - a)(c + a) = b^2 \Rightarrow \frac{(c-a)}{2}\frac{(c+a)}{2} = z^2,$$

   argue that $\frac{c-a}{2}$ and $\frac{c+a}{2}$ must be relatively prime integers, and hence, by Lemma 4.2, squares of some integers m and n (the formulas from the next hint can be useful here as well).

3. Finally, observing that

$$c = \frac{c-a}{2} + \frac{c+a}{2}, \quad a = \frac{c+a}{2} - \frac{c-a}{2}.$$

   obtain the required formulas and finish proving the theorem

♢ **4.3.** Put everything together in one coherent and detailed proof. Your submission should contain proofs of two results. First state and prove Lemma 4.2 and then state and prove Theorem 4.1. Make sure you include a proof for all the statements in the theorem.