A FIRST PROOF EXAMPLE: Classifying Primitive Pythagorean Triples

Any question of the form ‘Show that…’ or ‘Verify that…’ or ‘Justify…’ or ‘Demonstrate…’ is asking for a proof.

What is a proof?

A *proof* is a justification of a mathematical statement. When proving a particular statement, it is permissible at any time to make assertions of facts which are previously known, or which follow from previous steps in the proof, or which are assumed to be true by hypothesis. Proofs must always be written clearly, using complete sentences. In particular, correct spelling, grammar and punctuation is required, in addition to correct mathematical symbols, if any.

There is no absolute rule for determining how much justification is required for a particular step in a proof, since this depends partly on your level of experience as well as that of the intended reader. In general, it is not necessary to include detailed computations of college algebra since we assume that both you and the reader have previously mastered those skills. For example, if you know that $x(x-1)=6$, then you may immediately follow with ‘Therefore $x=-2$ or 3.’ In your rough work you may check the details of this computation, but such details are not expected in the final version of a proof at this level. The important things to include in a proof are all the logical steps.

It is one matter to say what is or is not a proof, and quite another matter (rather harder!) to explain how one produces a proof. (One evidence of this is the huge number of problems in number theory which remain unsolved to this day.) It is very helpful to study other people’s proofs, and to borrow their ideas. So do not be afraid to imitate a proof from class or from a textbook. In some courses we outline some basic strategies for trying to prove a statement—proof by contradiction, or by contrapositive; proof by induction, etc. One of the most helpful observations is to identify the key terms in the statement you are trying to prove, and to write down the precise definitions of these terms. Trying some numerical examples may also help to provide insight, even if they are not valid proofs by themselves. In any case, the final submitted proof will usually be obtained only after several stages of rough draft.

A Sample Proof

Recall that a *primitive Pythagorean triple* is a triple of pairwise relatively prime positive integers (x, y, z) such that $x^2+y^2=z^2$. The following theorem is given as an example of the writing style expected in proofs. A variant of this proof appears in Chapter 2 of the textbook.

Theorem. *Every primitive Pythagorean triple (x, y, z) is of the form*

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

for some relatively prime integers m and n where $m > n \geq 1$, and m and n are not both odd.

Proof. Let (x, y, z) be a primitive Pythagorean triple. Then x, y and z are not all even. Therefore one of x, y, z is even and the other two are odd. First we show (by contradiction) that z cannot be even.

We easily check that $n^2 \equiv 0$ or $1 \mod 4$ for every integer n, according as n is even or odd. If it is z that is even, with x and y odd, then we obtain $1+1 \equiv 0 \mod 4$, a contradiction. Therefore it must be either x or y that is even. We may assume that y is even, and x and z are odd; otherwise interchange x and y. Now the equation $x^2+y^2=z^2$ can be rewritten as

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

Note that each of the these quantities in parentheses is an integer. Moreover the integers $(z+x)/2$ and $(z-x)/2$ are relatively prime; for if d divides both $(z+x)/2$ and $(z-x)/2$, then d divides both their sum (z) and their difference (x). Now we have that the product of two relatively prime integers is a square. By considering prime factorizations, we see that both factors must be squares; that is, $(z+x)/2 = m^2$ and $(z-x)/2 = n^2$ for some positive integers m and n. Since these two factors are relatively prime, m and n must be relatively prime. Solving for x, y, z in terms of m and n gives $x = m^2-n^2$, $y = 2mn$, $z = m^2+n^2$. Also since x is odd, one of m and n is even and the other is odd. Finally, since x is positive, we obtain $m > n$. □

Note that the converse of this theorem is also true. Namely, if m and n are relatively prime positive integers of opposite parity (one even and the other odd), then we easily check that the positive integers $x = m^2-n^2$, $y = 2mn$, $z = m^2+n^2$ are pairwise relatively prime. Moreover, the identity

$$(m^2-n^2)^2 + (2mn)^2 = (m^2+n^2)^2$$

clearly holds.