Math 403: Pythagorean Triples

We all are familiar with the Pythagorean Theorem, which states that the lengths a and b of the legs of a right triangle, together with the length c of the hypotenuse, satisfy the relation $a^2 + b^2 = c^2$. The triple (a, b, c) is a *Pythagorean Triple* iff a, b, and c satisfy the Pythagorean Theorem. A Pythagorean triple is *primitive* iff a, b, and c have no common integer divisor except 1. A pair of numbers p and q is *relatively prime* iff they have no common integer divisor except 1. Note that the converse of the Pythagorean Theorem is also true.

Throughout the discussion below, we need to specify the *parity* of an integer n, namely whether it is even ($n = 2j$ for some integer j) or odd ($n = 2k + 1$ for some integer k). We will let $\mathbb{N}$ be the set of natural numbers $\{1, 2, 3, \cdots\}$, and $\mathbb{Z}$ the set of integers $\{0, \pm 1, \pm 2, \cdots\}$.

1. Prove that p is odd iff p^2 is odd, and q^2 is even iff q is even. Hint: To show p^2 odd $\Longrightarrow$ p odd, consider $p^2 - 1$.
2. If $n \in \mathbb{Z}$, then n^2 divided by 4 leaves a remainder of 0 or 1. Hint: Do two cases based on parity.
3. Use the previous problem to prove that if (a, b, c) is a Pythagorean triple, then a and b cannot both be odd.
4. Show that

$$a = p^2 - q^2, \quad b = 2pq, \quad \text{and} \quad c = p^2 + q^2 \tag{1}$$

   is a Pythagorean triple for $p, q \in \mathbb{N}$.
5. If k is a prime integer divisor of x^2 for some $x \in \mathbb{N}$, prove that k is a prime integer divisor of x. Hint: Write x as a product of its prime divisors, say $x = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$, where the p_i are prime divisors of x of multiplicity d_i.
6. Show that the formulas in (1) define a primitive pythagorean triple with b even iff p and q are relatively prime and are of opposite parity. Hint: If p and q have the same parity, show that 2 divides a, b, c and that if a prime k divides p and q then k divides a, b, c also. For the converse, assume the restrictions on p and q, and suppose that a prime k divides a, b, and c. Show that k must be odd and divides both $2p^2$ and $2q^2$, and thus divides both p^2 and q^2, and then use the previous problem.
7. Show that all primitive Pythagorean triples with b even can be obtained from the formulas in (1). Hint: First determine the parity of a and c, and then explain why we can write

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

   Argue that $(c + a)/2$ must be a square, say p^2, and $(c - a)/2$ likewise must be a square, say q^2, using #5.

Math 403: Fermat's Last Theorem, $n = 4$

Note that Pythagorean triples are nontrivial integer solutions to $a^n + b^n = c^n$ for $n = 2$.

Fermat's Last Theorem: The equation $a^n + b^n = c^n$ has no solutions in non-zero integers a, b, c for integers $n \geq 3$.

In 1637 Pierre de Fermat wrote, in his copy of Claude-Gaspard Bachet's translation of the famous Arithmetica of Diophantus, "I have a truly marvellous proof of this proposition which this margin is too narrow to contain." The theorem was not proven, however, until Andrew Wiles published a full proof in 1995. We will prove Fermat's Last Theorem just for $n = 4$, that is: $a^4 + b^4 = c^4$ has no solutions in non-zero integers a, b, c. First we will prove the following lemma.

Lemma: If $x^4 + y^4 = z^2$ for some $x, y, z \in \mathbb{N}$, then there must exist other numbers $u, v, w \in \mathbb{N}$ such that $u^4 + v^4 = w^2$ with $w < z$.

8. Suppose $x^4 + y^4 = z^2$ for some $x, y, z \in \mathbb{N}$. Write down a related Pythagorean triple in terms of x, y, z.
9. If x, y, z all have a common prime factor k, explain why $z/k^2 \in \mathbb{N}$ and that x/k, y/k, z/k^2 prove the lemma. After this, assume x, y, z are all relatively prime in the rest of the problems below.
10. Point out why x^2 and y^2 cannot both be odd. Then let x^2 be odd and y^2 be even. What can you conclude about x and y? Since we have a Pythagorean triple, use p and q from #4 above to rewrite the triple in terms of p odd and q even.
11. Identify a Pythagorean triple using p, q, x. Since we already are using p and q, use r and s in place of p and q in #4 above to rewrite the triple in terms of r and s. Based on the parity of x, classify r and s.
12. Consider the product $p(q/2)$. Argue that both r and s must be perfect squares themselves, say $r = u^2$ and $s = v^2$. Finish the proof.
13. Explain why having proven the lemma we can prove the theorem. This kind of argument is known as the *method of infinite descent*.