Recall that a 3-tuple (a, b, c) of natural numbers is a *Pythagorean triple* provided that $a^2 + b^2 = c^2$. The purpose of this problem is to prove the following theorem: For any $(a, b, c) \in \mathbb{N}^3$, (a, b, c) is a Pythagorean triple if and only if there exist natural numbers m, n, k satisfying $m > n$ and $\gcd(m, n) = 1$ such that $c = (m^2 + n^2)k$ and either $a = (m^2 - n^2)k$ and $b = 2mnk$, or $a = 2mnk$ and $b = (m^2 - n^2)k$. (You will most likely need to use the Fundamental Theorem of Arithmetic, as stated in Chapter 11.)

(a) Prove the "if" direction of the theorem.
Suppose $m, n, k \in \mathbb{N}$ such that $m > n, gcd(m, n) = 1, c = k(m^2+n^2)$ and $a = k(m^2-n^2), b = 2mnk$ or $a = 2mnk, b = k(m^2-n^2)$. We must show that $a^2+b^2 = c^2$. Note that since addition of natural numbers is commutative, the choice we make for a and b can be swapped and not affect the proof. Therefore WLOG we assume that $a = k(m^2 - n^2)$, $b = 2mnk$. Note that since $m > n$, then $m^2 > n^2$, and thus we have $m^2 - n^2 > 0$, and thus makes the product of k and $m^2 - n^2$ a natural number. Therefore by algebraic manipulation we have:

$$\begin{aligned}
a^2 + b^2 &= k^2(m^2 - n^2)^2 + 4m^2n^2k^2 \\
&= k^2m^4 - 2k^2m^2n^2 + k^2n^4 + 4m^2n^2k^2 \\
&= k^2(m^4 - 2m^2n^2 + n^4 + 4m^2n^2) \\
&= k^2(m^2 + 2m^2n^2 + n^4) \\
&= k^2(m^2 + n^2)^2 \\
&= (k(m^2 + n^2))^2 \\
&= c^2.
\end{aligned}$$

The rest of the problem is for the "only if" direction. Suppose a, b, c is a Pythagorean triple. We must show there exists m, n with the desired properties. The proof will have two lemma. Main Lemma: if $\gcd(a, b, c) = 1$ then the conclusion holds. Secondary lemma: if the result holds whenever $\gcd(a, b, c) = 1$ then it also holds for all a, b, c.

(b) Prove the secondary lemma: Assume that the result is true whenever $\gcd(a, b, c) = 1$. Use this to prove that the result is true for all Pythagorean triples a, b, c.

Suppose $(a, b, c) \in \mathbb{N}^3, a^2 + b^2 = c^2$ and that for all $(x, y, z) \in \mathbb{N}^3$ if $gcd(a, b, c) = 1$, then the theorem holds. We must show there exists $m, n, k \in \mathbb{N}$ such that $m > n, gcd(m, n) = 1, c = k(m^2 + n^2)$ and $a = k(m^2 - n^2), b = 2mnk$ or $a = 2mnk, b = k(m^2 - n^2)$. Suppose $a \neq 2mnk, b \neq k(m^2 - n^2)$. We must show there exists $m, n, k \in \mathbb{N}$ such that $m > n, gcd(m, n) = 1, c = k(m^2 + n^2)$ and $a = k(m^2 - n^2), b = 2mnk$. Let l be given by $l = gcd(a, b, c)$. Therefore l divides a, b, c. Therefore by definition of divisibility $a = la', b = lb', c = lc'$. Thus by algebraic manipulation we have $l^2a'^2 + l^2b'^2 = l^2c'^2, a'^2 + b'^2 = c'^2$. Therefore (a', b', c') is a Pythagorean triple. Note that since $l = gcd(a, b, c)$, then there exists $x_1, x_2, x_3 \in \mathbb{Z}$ such that $x_1a + x_2b + x_3c = l$, therefore dividing out l to get a', b', c' yields $x_1a' + x_2b' + x_3c' = 1$, which by the definition of gcd means $gcd(a', b', c') = 1$. Therefore since $a'^2 + b'^2 = c'^2$ and $gcd(a', b', c') = 1$ then there exists $m, n, k' \in \mathbb{N}$ such that $m > n, gcd(m, n) = 1, c' = k'(m^2 + n^2), a' = k'(m^2 - n^2), b' = 2mnk'$. Let $k = lk'$. We claim that m, n, k satisfy the requirements. Since $a = la' = l = lk'(m^2 - n^2) = k(m^2 - n^2), b =$

$lb' = lk'2mn = k2mn, c = lc' = lk'(m^2 + n^2) = k(m^2 + n^2)$, and all of the other requirements are satisfied by m, n then the requirements have been satisfied.

The remaining parts of the problem are for proving the main lemma. So we assume $\gcd(a, b, c) = 1$, and prove that the desired m, n exist.

(c) Prove that c is odd and exactly one of a and b is odd.
Suppose $(a, b, c) \in \mathbb{N}^3, a^2 + b^2 = c^2, gcd(a, b, c) = 1$. We must show that c is odd and exactly one of a and b is odd. By definition we must show c is odd, and $a \equiv 1 \mod 2$ and $b \equiv 0 \mod 2$ or $a \equiv 0 \mod 2$ and $b \equiv 1 \mod 2$. Suppose $a \not\equiv 1 \mod 2, b \not\equiv 0 \mod 2$. We must show that c is odd, and $a \equiv 0 \mod 2, b \equiv 1 \mod 2$. By definition of not congruent, $a \equiv 0 \mod 2, b \equiv 1 \mod 2$. Therefore we must show c is odd. By definition of odd, we must show $c \equiv 1 \mod 2$. Note that since if $x \equiv 0 \mod 2$, then $x^2 \equiv 0^2 = 0 \mod 2$, and if $x \equiv 1 \mod 2$ then $x^2 \equiv 1^2 = 1 \mod 2$, then for $\mathbb{Z}/2\mathbb{Z}$ $x^2 \equiv x \mod 2$. Therefore $c^2 \equiv c \mod 2, a^2 + b^2 \equiv a + b \mod 2$. By algebraic manipulation we have:

$$\begin{aligned} c &\equiv a + b \\ &\equiv 1 + 0 \\ &= 1 \mod 2. \end{aligned}$$

(d) Without loss of generality assume that a is odd. Prove that $\gcd(c - a, c + a) = 2$.
Suppose $(a, b, c) \in \mathbb{N}^3, a^2+b^2 = c^2, gcd(a, b, c) = 1$, a is odd. We must show $\gcd(c-a, c+a) = 2$. Suppose for contradiction Note by the previous lemma c is odd. Since a is odd, then b is even. By the definition of even and odd, let $a = 2q-1, b = 2r, c = 2s-1$, where $q, r, s \in \mathbb{N}$. By the definition of gcd we must show there exists $x_1, x_2 \in \mathbb{Z}$ such that $(c+a)x_1+(c-a)x_2 = 2$. By the parity of a, c we must show that $2(s+q-1)x_1+2(s-q)x_2 = 2$. Dividing out by 2 we must show $(s+q-1)x_1+(s-q)x_2 = 1$. Suppose for contradiction that $(s+q-1)x_1+(s-q)x_2 > 1$. Let $k = gcd(s + q - 1, s - q)$. Then $k \mid c - a, k \mid c + a$. Therefore by algebraic manipulation

$$\begin{aligned} \frac{c-a}{k}\frac{c+a}{k} &= \frac{(c-a)(c+a)}{k^2} \\ &= \frac{c^2 - a^2}{k^2} \\ &= \frac{c^2}{k^2} - \frac{a^2}{k^2} \\ &= (\frac{c}{k})^2 - (\frac{a}{k})^2 \\ &= \frac{b^2}{k^2} \\ &= (\frac{b}{k})^2 \end{aligned}$$

Since k divides a, b, c, then $k \mid gcd(a, b, c)$. This is a contradiction as $k > 1$, and $gcd(a, b, c) = 1$. Therefore $gcd(c + a, c - a) = 2$.

(e) Show that the required integers m and n exist. Suppose $a, b, c \in \mathbb{N}, gcd(a, b, c) = 1, a^2 + b^2 = c^2, gcd(c+a, c-a) = 2$. We must show that there exists $m, n \in \mathbb{N}$ such that $m > n, gcd(m, n) = 1, a = m^2 - n^2, b = 2mn, c = m^2 + n^2$. Since $b^2 = c^2 - a^2$, then by algebraic manipulation

$$\begin{aligned} b^2 &= c^2 - a^2 \\ &= (c+a)(c-a) \\ b &= \frac{(c+a)(c-a)}{b} \\ \frac{b}{c+a} &= \frac{c-a}{b} \end{aligned}$$

Let $\frac{n}{m}$ be given by $\frac{n}{m} = \frac{b}{c+a}$ in lowest terms. Therefore $gcd(m, n) = 1$. Since $\frac{m}{n} = \frac{c+a}{b}, \frac{n}{m} = \frac{c-a}{b}$ then by algebraic manipulation we have

$$\begin{aligned} 2\frac{c}{b} &= \frac{m}{n} + \frac{n}{m} \\ &= \frac{m^2 + n^2}{nm} \\ \frac{c}{b} &= \frac{m^2 + n^2}{2nm} \\ 2\frac{a}{b} &= \frac{m}{n} - \frac{n}{m} \\ &= \frac{m^2 - n^2}{nm} \\ \frac{a}{b} &= \frac{m^2 - n^2}{2nm} \end{aligned}$$

Therefore $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$. We must show that $m > n$. Suppose for contradiction that $m \leq n$. Then $m^2 \leq n^2, m^2 - n^2 \leq 0$. This is a contradiction as $a = m^2 - n^2, a \in \mathbb{N}$. Therefore $m > n$. Thus the requirements have been satisifed.