The rational prime 2 factors as $2 = (1+i)(1-i) = -i(1+i)^2$ in $\mathbb{Z}[i]$. Show that $1+i$ is prime in $\mathbb{Z}[i]$ and does not divide $a \pm bi$.

An odd rational prime may remain prime in the Gaussian integers, or it may factor as the product of two primes which are complex conjugates.

Now show that $a+bi$ and $a-bi$ are relatively prime in $\mathbb{Z}[i]$. Since their product is the square c^2, conclude by unique factorization that each is a square in $\mathbb{Z}[i]$ up to a unit.

Thus there exist integers m and n so that one of $\pm(a+bi) = (m+ni)^2$ or $\pm i(a+bi) = (m+ni)^2$ holds.

Examine these formulas to finish the proof. For example, if the unit is $+1$, then we have $a+bi = (m+ni)^2 = (m^2-n^2)+(2mn)i$ and equating real and imaginary parts gives the results $a = m^2-n^2$ and $b = 2mn$.

Project: Give a geometric proof of the classification of Pythagorean triples along the following lines.

Let C be the unit circle $x^2+y^2 = 1$ in the plane and let L be the line with slope t through the point $(1,0)$. Then L has equation $y = tx - t$ and intersects the circle C in two points, $Q = (1,0)$ and another point $P = (x,y)$. Take $y \geq 0$ to assume $t \leq 0$.

Note that if P has rational coordinates, then the slope t of the line L is also rational. Show that, conversely, if the slope t is rational, then the coordinates of the point P are rational.

Hint: Find the simultaneous solutions to the two equations $x^2+y^2 = 1$ and $y = tx - t$. Elimination of y leads to a quadratic in x. Since we know that $x = 1$ is one solution, it is easy to find the other solution by factorization.

Thus rational points $P = (a/c, b/c) \neq (1,0)$ on the circle are parametrized by rational numbers $t = m/n$. Use this information to classify reduced Pythagorean triples.