We will prove the following famous theorem of Fermat. The proof is a classic example of the *infinite descent* method.

Theorem 1 *There exists no triple (x, y, z) of positive integers such that*

$$x^4 + y^4 = z^2. \qquad (1)$$

An immediate corollary is the case $n = 4$ of Fermat's Last Theorem, the only case for which Fermat is known to have actually written down a complete proof :

Corollary 2 *There exists no triple (x, y, z) of positive integers such that*

$$x^4 + y^4 = z^4. \qquad (2)$$

PROOF OF COROLLARY : If we substitute $w := z^2$, then (2) reduces to (1).

The first step in the proof of Theorem 1 is a result that goes back to Pythagoras. You shouldn't have any difficulty understanding why.

Proposition 3 *Let (x, y, z) be a triple of relatively prime positive integers. Then*

$$x^2 + y^2 = z^2 \qquad (3)$$

if and only if there exists a pair (a, b) of relatively prime positive integers such that either

$$x = a^2 - b^2, \qquad y = 2ab, \qquad z = a^2 + b^2 \qquad (4)$$

or

$$x = 2ab, \qquad y = a^2 - b^2, \qquad z = a^2 + b^2. \qquad (5)$$

NOTE : A triple (x, y, z) of positive integers satisfying (3) is called a *Pythagorean triple*. This is because, according to Pythagoras' theorem, these triples are in 1-1 correspondence with all right-angled triangles whose side lengths are integers.

PROOF OF PROPOSITION : If the triple (x, y, z) satisfies either (4) or (5), then a direct and easy computation shows that (3) is also satisfied. Now suppose that x, y, z are relatively prime and that (3) is satisfied.

If x and y were both odd, then we'd have $x^2 \equiv y^2 \equiv 1 \pmod 4$, implying $z^2 \equiv 2 \pmod 4$, which is impossible. Hence at least one of x or y is even. In fact, exactly one of them is even, since if both were, then so would be z, contradicting the assumption that x, y, z are relatively prime.

Case I: y is even and x is odd.

Then z is odd, so both $z + x$ and $z - x$ are even. We can rewrite (3) as

$$(z + x)(z - x) = y^2. \tag{6}$$

Let $d = \gcd(z + x, z - x)$. We claim that $d = 2$. Since both terms are even, we know that $d \geq 2$ and d is even. Now $d|z + x$ and $d|z - x$ so $d|2x$ and $d|2z$. Hence $\frac{d}{2}$ divides both x and z. By (3), it also divides y. That is, $\frac{d}{2}$ is a common divisor of x, y, z. Since these numbers are relatively prime, we must have $\frac{d}{2} = 1$, as required.

Now from (6) and the fact that $\gcd(z + x, z - x) = 2$, the Fundamental Theorem of Arithmetic immediately implies that there exist relatively prime positive integers a, b such that

$$y = 2ab, \qquad z + x = 2a^2, \qquad z - x = 2b^2,$$

from which (4) follows.

Case II: y is odd and x is even.

Just repeat the above argument, interchanging the roles of x and y. One deduces that equations of the form (5) are satisfied. This completes the proof of the proposition.

Proof of Theorem 1 (Fermat) : Let (x, y, z) be a hypothetical solution to (1), with $d = \gcd(x, y, z)$. Then $(x/d, y/d, z/d^2)$ is also a solution in relatively prime integers, so it suffices to prove that (1) has no solution in relatively prime integers. The proof is by the method of *infinite descent*. We assume that a solution (x, y, z) in relatively prime integers exists, and thereby construct another solution (x', y', z'), also in relatively prime integers, with $z' < z$. Since amongst all solutions, there must exist one with z minimal, we obtain a contradiction.

So let (x, y, z) be a relatively prime triple which satisfies (1). Then the triple (x^2, y^2, z) is relatively prime and satisfies (3). Assuming, without loss of generality, that x is odd and y even, Proposition 3 implies that there exist relatively prime integres a, b such that

$$x^2 = a^2 - b^2, \qquad y^2 = 2ab, \qquad z = a^2 + b^2. \tag{7}$$

Claim : b is even. For suppose b odd. Since x is odd, this would mean a is even, and hence that $x^2 \equiv -1 \pmod 4$, which is impossible.

Now (x, b, a) is a Pythagorean triple with b even, so by Proposition 3 again, there exist relatively prime integers c, d such that

$$x = c^2 - d^2, \qquad b = 2cd, \qquad a = c^2 + d^2. \tag{8}$$

Substituting (8) into (7) we get

$$y^2 = 2ab = 4cd(c^2 + d^2). \tag{9}$$

But c and d are relatively prime, hence both are relatively prime to $c^2 + d^2$. Since, by (9), the product of all three is a perfect square, it follows that each is a perfect square : that is, there exist relatively prime integers e, f, g such that

$$c = e^2, \qquad d = f^2, \qquad c^2 + d^2 = g^2.$$

But then the triple (e, f, g) also satisfies (1). Finally, by (8) and (7) we have that

$$g \leq g^2 = a \leq a^2 < z,$$

which completes the proof.