PROOF THAT $x^2 + y^2 = 3$ HAS NO RATIONAL SOLUTIONS.

MATH 2106-D

Here, we follow a famous proof due to the very famous Fermat, known as the "prince of amateurs" due to the fact that his day job was as a lawyer. The method of infinite descent is a powerful tool in number theory, and a special kind of proof by contradiction. In particular, it aims to show that if you can find a solution to some equation, then you can always find a smaller solution to that equation, ad infinitum, and if you can guarantee that there's some finiteness property which can't be violated, this may yield an absurdity. For example, in the proof that $\sqrt{2}$ is irrational, any rational expression of $\sqrt{2}$ gives rise to a "smaller" fraction, where smaller means that the denominator and numerator are smaller numbers. Since given a positive integer n, you can't divide by 2 infinitely many times and keep getting integers, this doesn't make sense. In other words, we are using the *well-ordering principle*, which states that any (non-empty) subset of natural numbers has a *least* element.

Here, we will use a similar framework to explain why $x^2+y^2 = 3$ has no solutions with $x, y \in \mathbb{Q}$. In what follows, we will try to highlight the main structural points as we come across them. In general, when you are studying a new proof, or writing a proof, try to study the overall structure or main ideas of the proof first, as most proofs we will do boil down to a few "big" ideas, with smaller details in between. This is analogous to writing or reading an essay; when you write, you don't usually go from one sentence directly to the next in order, but think about the main structural points of the composition, like a skeleton of the essay, and then fill in the supporting details in between.

Suppose now for the sake of contradiction that there is a pair $(x, y) \in \mathbb{Q}^2$ with $x^2+y^2 = 3$. To use the a descent proof, we need to work with natural numbers, i.e., with positive integers, since there is no minimality property of $\mathbb{Q}$ like the well-ordering principle (e.g., you can keep dividing 100 by 2 as many times as you like and still keep getting rational numbers, although you leave the set of integers eventually).

Firstly, we will reduce to the case of positive numbers. If x or y is negative, then we can replace it by $-x$ or $-y$, respectively, and since the square of $-x$ or $-y$ is still x^2 or y^2, respectively, we get another solution in the set of positive rational numbers. Thus, assume WLOG that $x, y \geq 0$. If x or y is 0, say $y = 0$, then $x^2 = 3$ and $x \in \mathbb{Q}$, which says that $\sqrt{3}$ is rational. Exactly like in the proof that $\sqrt{2}$ is irrational, this is false, and so neither x nor y can be 0.

Thus, assume that $x, y > 0$. We reduce to the case of natural numbers as follows. By finding a common denominator, we can write x and y as (possibly non-reduced) fractions $x = a/c$, $y = b/c$, where $a, b, c \in \mathbb{N}$. Substituting in gives

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 3,$$

which yields

$$a^2 + b^2 = 3c^2. \tag{1}$$

Conversely, we can also take a solution to (1) and divide by c^2 to get a rational solution to $x^2 + y^2 = 3$. Thus, finding a solution to our original equation in the rationals is equivalent to solving $a^2 + b^2 = 3c^2$ in the natural numbers (there is a special word for when this works out this way; this polynomial in a, b, c is *homogenous*, meaning that all terms in it have the same degree).

Having reduced to this case, we are set up to try a proof by infinite descent. Suppose that $(a, b, c) \in \mathbb{N}^3$ solves (1). Then in particular $a^2 + b^2 \equiv 0 \pmod 3$. Note that $0^2 \equiv 0 \pmod 3$, $1^2 \equiv 1 \pmod 3$, and $2^2 \equiv 4 \equiv 1 \pmod 3$. Thus, if a and b aren't both divisible by 3, then $a^2 + b^2$ is congruent to $1 + 0$, $0 + 1$, or $1 + 1$, and hence is not congruent to 3. Thus, we must have $0 \equiv a \equiv b \pmod 3$. But then we can divide out by 3 to get $a = 3a'$, $b = 3b'$ for natural numbers a', b', so that

$$a^2 + b^2 = (3a')^2 + (3b')^2 = 9(a'^2 + b'^2) = 3c^2,$$

or

$$3(a'^2 + b'^2) = c^2.$$

Thus, $3|c^2$, and by the calculation above, $3|c$, and so we can write $c = 3c'$ for a natural number c'. But then

$$3(a'^2 + b'^2) = (3c')^2 = 9c'^2,$$

and so

$$a'^2 + b'^2 + 3c'^2.$$

In short, we have taken a solution (a, b, c) to (1) in the natural numbers, and showed that given such a solution, we can *always* find a smaller solution (a', b', c') still inside of $\mathbb{N}^3$, that is, a new solution with $a' < a$, $b' < b$, and $c' < c$. But, this is absurd, as repeating this process indefinitely implies that there are infinitely many natural numbers which are smaller than a given natural number, say a, which is false. By way of contradiction, this completes the proof.