Math 310
September 25, 2020 Lecture

Steven G. Krantz

September 12, 2020

Figure: This is your instructor.

Aristotelian logic dictates that every sensible statement has a truth value: TRUE or FALSE. If we can demonstrate that a statement A could not possibly be false, then it must be true. On the other hand, if we can demonstrate that A could not be true, then it must be false. Here is a dramatic example of this principle. In order to present it, we shall assume for the moment that you are familiar with the system $\mathbb{Q}$ of rational numbers. These are numbers that may be written as the quotient of two integers (without dividing by zero, of course).

Theorem: [Pythagoras] *There is no rational number x with the property that $x^2 = 2$.*

Proof: In symbols, our assertion may be written

$$\sim \big(\exists x, (x \in \mathbb{Q} \wedge x^2 = 2)\big).$$

Seeking a contradiction, we assume the statement to be false. Then what we are assuming is that

$$\exists x, (x \in \mathbb{Q} \wedge x^2 = 2). \qquad (*)$$

Since x is rational, we may write $x = p/q$, where p and q are integers.

We may as well suppose that both p and q are positive and nonzero. After reducing the fraction, we may assume that it is in lowest terms—so p and q have no common factors.

Now our hypothesis asserts that

$$x^2 = 2$$

or

$$\left(\frac{p}{q}\right)^2 = 2.$$

We may write this out as

$$p^2 = 2q^2. \tag{$**$}$$

Observe that this equation asserts that p^2 is an even number. But then p must be an even number (p cannot be odd, for that would imply that p^2 is odd). So $p = 2r$ for some natural number r.

Substituting this assertion into equation $(**)$ now yields that

$$(2r)^2 = 2q^2.$$

Simplifying, we may rewrite our equation as

$$2r^2 = q^2.$$

This new equation asserts that q^2 is even. But then q itself must be even.

We have proven that both p and q are even. But that means that they have a common factor of 2. This contradicts our starting assumption that p and q have no common factor.

Let us pause to ascertain what we have established: the assumption that a rational square root x of 2 exists, and that it has been written in lowest terms as $x = p/q$, leads to the conclusion that p and q have a common factor and hence are *not* in lowest terms. What does this entail for our logical system?

We cannot allow a statement of the form $C = A \wedge \sim A$ (in the present context the statement A is "$x = p/q$ in lowest terms"). For such a statement C must be false.

But if x exists, then the statement C is true. No statement (such as A) can have two truth values. In other words, the statement C must be false. The only possible conclusion is that x does not exist. That is what we wished to establish. □

Remark: In practice, we do not include the last three paragraphs in a proof by contradiction. We provide them now because this is our first exposure to such a proof, and we want to make the reasoning absolutely clear. The point is that the assertions A and $\sim A$ cannot both be true. An assumption that leads to this eventuality cannot be valid. That is the essence of proof by contradiction.

Historically, this last theorem was extremely important. Prior to Pythagoras ($\sim$300 B.C.E.), the ancient Greeks (following Eudoxus) believed that all numbers (at least all numbers that arise in real life) are rational. However, by the Pythagorean theorem, the length of the diagonal of a unit square is a number whose square is 2. And our theorem asserts that such a number cannot be rational. We now know that there are many nonrational, or irrational, numbers. In fact, in a later lecture, we shall learn that, in a certain sense to be made precise, "most" numbers are irrational.

Here is a second example of a proof by contradiction:

Theorem: [Dirichlet] *Suppose that $n + 1$ pieces of mail are delivered to n mailboxes. Then some mailbox contains at least two pieces of mail.*

Proof: Seeking a contradiction, we suppose that the assertion is false. Then each mailbox contains either zero or one piece of mail. But then the total amount of mail in all the mailboxes cannot exceed

$$\underbrace{1+1+\cdots+1}_{n \text{ times}}.$$

In other words, there are at most n pieces of mail. That conclusion contradicts the fact that there are $n+1$ pieces of mail. We conclude that some mailbox contains at least two pieces of mail. □

The last theorem, due to Gustav Lejeune Dirichlet (1805–1859), was classically known as the *Dirichletscher Schubfachschluss*. This German name translates to “Dirichlet’s drawer shutting principle.” Today, at least in this country, it is more commonly known as “the pigeonhole principle.” Since pigeonholes are no longer a common artifact of everyday life, we have illustrated the idea using mailboxes.

Example: Draw the unit interval I in the real line. Now pick 11 points at random from that interval (imagine throwing darts at the interval, or dropping ink drops on the interval). Then some pair of the points has distance not greater than 0.1 inch apart. To see this, write

$$I = [0, 0.1] \cup [0.1, 0.2] \cup \cdots [0.8, 0.9] \cup [0.9, 1].$$

Here we have used standard interval notation. Think of each of these subintervals as a mailbox. We are delivering 11 letters (that is, the randomly selected points) to these ten mailboxes. By the pigeonhole principle, some mailbox must receive two letters.

We conclude that some subinterval of I, having length .1, contains two of the randomly selected points. Thus, their distance does not exceed 0.1 inch.

Example: We shall prove by contradiction that there are infinitely many prime numbers (this is an ancient result of Euclid).

Recall that a prime number is a whole number, or integer, greater than 1 which has no divisors except for 1 and itself. The first several primes are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots .$$

A natural number which is not prime is called *composite*. A composite number will have nontrivial factors. For example, $18 = 2 \cdot 3 \cdot 3$. In particular, a composite number will always be divisible by a smaller prime.

Now, seeking a contradiction, let us suppose that there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$. Define

$$P = (p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k) + 1 .$$

What can we say about the number P?

If we divide P by p_1, then p_1 goes evenly into the product, and there is a remainder of 1. If we divide P by p_2, then p_2 goes evenly into the product, and there is a remainder of 1. And so it goes for the rest of the p_j. Now P is either prime or composite. But we just checked every known prime—p_1, p_2, $\ldots$, p_k—and verified that none of them is a divisor of P. So P cannot be composite. We conclude that P is prime.

But this is a contradiction, because P is a prime that is evidently larger than each of the p_j. We had an exhaustive list of the primes, and now we have created one more. That is a contradiction. We conclude that there are infinitely many primes. □

Example: We shall show that there are no positive integer solutions to the equation $x^2 - y^2 = 1$. [Such an equation—a polynomial equation for which we seek integer solutions—is called a *diophantine equation*. This in honor of the ancient Greek mathematician Diophantus ($\sim$ 200 C.E.–$\sim$ 284 C.E.).]

Seeking a contradiction, we suppose that our diophantine equation *does* have integer solutions x, y. We write

$$1 = x^2 - y^2 = (x - y) \cdot (x + y) \,.$$

Thus either both $x - y = 1$ and $x + y = 1$ or else $x - y = -1$ and $x + y = -1$. In the first case, we can add the two equations to solve them and find that $x = 1$, $y = 0$. This contradicts the assumption that both x and y are positive. In the second case, we again can add the two equations and find that $x = -1$, $y = 0$. Again, we contradict the assumption that x and y are positive.

Either case leads to a contradiction. We conclude that the diophantine equation *cannot* have a solution. □

Example: We shall show that the sum of a rational number and an irrational number is always irrational.

Seeking a contradiction, we assume the contrary. So let q be a rational number and α an irrational number such that $q + \alpha$ is rational. So there is a rational number p with

$$q + \alpha = p \, .$$

But then we have

$$\alpha = p - q \, .$$

Surely the difference of two rational numbers is rational, so we have an irrational number equaling a rational number. That is a contradiction.