

Contradict or Construct?

The Mathematical Intelligencer encourages comments about the material in this issue. Letters to the editor should be sent to either of the editors-in-chief, Chandler Davis or Marjorie Senechal.

Hurrah for Michael Hardy and Catherine Woodgold! ["Prime Simplicity," *Intelligencer*, Fall 2009, 44–52.] They have provided another brilliant example of what the mathematician Lacroix once described as "the ease with which errors pass from book to book." (Lacroix was writing in 1797 about the way in which so many of his predecessors had misunderstood and disparaged the foundations of Leibniz's calculus.)

However, I think they overlook an essential point when they fail to deny that Euclid proves "the existence of infinitely many prime numbers." Euclid does not deal in infinities. He proves that, given any finite set of primes, there is another prime not in the set, and his proof is constructive: Form the product, add one, and factor the result into primes. There is of course at least one prime factor, and none of the prime factors are in the set that was given.

Whether a proof by contradiction is appropriate depends on what is being proved. Euclid does prove Proposition 9 of Book X (of which the irrationality of $\sqrt{2}$ is a consequence) by contradiction. This is appropriate because the statement to be proved says something is *impossible*, whereas the statement about primes (as Euclid formulated it) says something is *possible*. In Essay 5.2 of my book "Essays in Constructive Mathematics" I argue that a proof by contradiction deserves to be called constructive if it proves a construction is impossible by deducing a contradiction from it, and I prove both the irrationality of $\sqrt{2}$ and Sylow's theorem in group theory by this method.

Harold Edwards
New York University
New York
USA
e-mail: edwards@cims.nyu.edu