1 Contradiction, continued

Another famous proof by contradiction, originally set down by Euclid:

Theorem 1. *There are an infinite number of primes.*

Proof. We shall prove this by contradiction; let us assume to the contrary that there are only a finite number n of primes, and let us denote those primes by $p_1, p_2, p_3, \ldots, p_n$. Now, let $M = p_1p_2p_3 \cdots p_n + 1$. Note that the product of several positive integers must be a positive integer, so M must be an integer greater than 1; thus, M has at least one prime factor. Since the set $\{p_1, \ldots, p_n\}$ contains all primes, it thus must follow that some $p_i \mid M$. However, by the definition of divisibility, it is clear that $p_i \mid (-p_1p_2p_3 \cdots p_m)$, since $-p_1p_2p_3 \cdots p_m$ is the product of an integer with p_i. Thus, by additivity of divisibility, we know that $p_i \mid (M - p_1p_2p_3 \cdots p_m)$, but by the definition of M, this relation can be simplified to $p_i \mid 1$, which is impossible: the only positive divisor of 1 is 1, which is not prime, so it is not in fact possible for any p_i to divide M. □

There are many other proofs of the infinitude of primes, using other techniques (of particular interest is Fürstenberg's point-set topological proof), but this is often regarded as the "original" and "most elegant".

2 Counterexamples

A key concept set down in the previous proof was explicit construction. We claimed something was true (i.e. there were finitely many primes) and then gave it the lie with a very specific case (i.e. the product of all those primes plus one). When the defeat of our claim is premised on the claim's truth, as it was here, it serves us in a proof by contradiction. But a closely related concept is a specific example defeating a claim we are trying to prove. Such a specific case is called a *counterexample*, and it is a very useful exploratory tool.

Conjecture 1. *For any integer n, if $n \nmid a$ and $n \nmid b$, then $n \nmid ab$.*

This is called not a proposition or a theorem, but a *conjecture*, because we aren't sure if it's true or false yet. Before we set down to proving it, we might ask: is it even true? To test it out, we might try some triples of n, a, and b.

We might try $n = 2$, $a = 3$, and $b = 4$. But this isn't a counterexample, even though our consequence is false (that is, 2 *does* divide 12), because our premise is also false. Likewise, $n = 4$, $a = 3$, and $a = 5$ isn't a counterexample, because our consequence is true (indeed 4 doesn't divide 15). We might see if we can find a counterexample — a case where the premise of the above statement is true, but its consequence is false!

Note that a disproof of a statement does not show that the statement is universally false. There are many choices of n, a, and b for which the above statement is in fact true. However, it is not *universally* true, and cannot be asserted as such.

Likewise, here's a conjecture akin to a theorem we saw before:

Conjecture 2. *If we color the segments between the vertices of a regular pentagon red or blue, three vertices will be joined by a red triangle or a blue triangle.*

which we can demonstrate is not true by coloring the edges of the pentagon red and the pentagram blue.

Conjectures are, as a general rule, eventually settled one way or the other (there is a logical concept of "formal undecidability" which indicates certain exotic statments may be beyond truth assessment in a logical system, but you are fantastically unlikely to ever come across such a statement by accident). Conjectures can basically coem down one way or the other:

- If a proof of a conjecture is demonstrated, the conjecture is true and can be added to the canon.
- If a counterexample of a conjecture is demonstrated, the conjecture is false — but need not be discarded outright!

When a statement has been disproven, a good mathematician seeks to *salvage* it. For instance, the pentagon-coloring statement was false, but the same statement about a hexagon was true (and we proved it!). The divisibility problem above is false, but with the right conditions set on the value of n it might be true (it's true, for instance, when $n = 2$).

A number of statements we might think of as true on initial thought are false, as we can demonstrate:

Conjecture 3. *If x is real, then $\frac{x^2-x}{x-1} = x$.*

which is clearly denied by $x = 1$.

Conjecture 4. *For any real numbers a and b, $\sqrt{ab} = \sqrt{a}\sqrt{b}$.*

which is false when $a = -1$ and $b = -1$.

Note that both of these were statements with a kernel of truth, and can be salvaged:

Proposition 1. *If x is a real number not equal to 1, then $\frac{x^2-x}{x-1} = x$.*

Proposition 2. *For any positive real numbers a and b, $\sqrt{ab} = \sqrt{a}\sqrt{b}$.*

so the disprover's task is not just going around poking holes in things, but determining the nature of those holes and finding out how to work around them. For instance, the problem set asks you to identify and determine conditions to make the divisibility problem above true.