

THERE IS NO LARGEST PRIME NUMBER

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

In earlier classes we proved the following handy facts:

Lemma. *Let a, b, c be integers. If $a|b$ and $a|c$, then a divides any linear combination of b and c . In other words, $a|ub + vc$ for all $u, v \in \mathbb{Z}$.*

Lemma. *If a, b are positive integers and if $a|b$, then $a \leq b$.*

We will need these facts to prove the following important theorem (from Sept. 14):

Theorem. *There is no largest prime number.*

Remark. Since every non-empty finite set of integers has a maximum, this result shows that the set of primes cannot be finite. In other words, *there are an infinite number of primes.*

Proof. (By contradiction) Suppose that P is the largest prime number. Let $N = P! + 1$. By the Fundamental Theorem of Arithmetic, N is the product of primes. Let q be a prime that occurs in the prime factorization of N . So q is a divisor of $N = P! + 1$.

Since q is a prime number, $q \leq P$ because P is the largest prime. Now $P! = 1 \cdot 2 \cdot 3 \cdots P$, so every positive integer less than or equal to P is a divisor of $P!$. In particular q divides $P!$.

Now we are in a very strange situation: $q|P! + 1$ and $q|P!$. This implies that q divides the linear combination $1 \cdot (P! + 1) + (-1) \cdot P! = 1$. Thus $q|1$. This means $q \leq 1$ which is a contradiction since primes are greater than 1. \square

Here is a concise version of the proof:

Proof. Suppose P is the largest prime number, and let $N = P! + 1$. Let q be a prime divisor of N . Observe that $q|P!$ since $q \leq P$. Thus q divides $N - P! = 1$. Contradiction. \square

One strategy for learning proofs is to learn concise versions, and test yourself to see if you can justify each step.

DR. WAYNE AITKEN, CAL. STATE, SAN MARCOS, CA 92096, USA
E-mail address: waitken@csusm.edu