ANOTHER PROOF OF THE INFINITUDE OF PRIMES

KENT SLINKER

That there are an infinite number of primes is something that has been known since antiquity. Euclid's proof, accessible to even the beginning Mathematician, shows that no finite set of primes can be complete. It comes as no surprise that in the many ensuing years more proofs of this result have appeared in the pages of Mathematical journals, books, and recently websites devoted to Mathematics. Here we present another short elementary proof.

To facilitate our proof we introduce the following notation: Let $n = \prod_{i=1}^{k} p_i^2$ be the product of k distinct primes squared. Let $1 \leq j \leq k$, and define $r_j = \dfrac{n}{p_j^2}$. In other words, r_j is the product of k distinct primes squared except the j^{th}. Let $k_j = \sqrt{r_j}$ and observe $k_j \in \mathbb{N}$.

Theorem. *There exists an infinite number of primes.*

Proof. First note that $\{2, 3\}$ is a set of primes, hence there exists a prime which is not equal to 2. Now assume by way of contradiction that there are a finite number of primes contained in the set $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$. Set $n = \prod_{i=1}^{k} p_i^2$, and consider,

$$r_j - 1 = (k_j - 1)(k_j + 1)$$

where $p_j \neq 2$. We want to show that at least one of the factors $(k_j - 1)$ or $(k_j + 1)$ must contain a prime not in $\mathcal{P}$. Observe $r_j \equiv 0 \pmod{p}$ for every $p \in \mathcal{P}$ except p_j, hence neither of the factors $(k_j - 1)$ or $(k_j + 1)$ can be divisible by any $p \in \mathcal{P}$ except p_j, (else we have the contradiction $-1 \equiv 0 \pmod{p}$ for some $p \in \mathcal{P}$). So what remains to show is that at least one of the factors $(k_j - 1)$ or $(k_j + 1)$ is not divisible by p_j.

If just one of the pair $(k_j - 1)$ or $(k_j + 1)$ contain p_j as a factor, then the other must contain a prime not in $\mathcal{P}$ and we are done. Suppose then that both $(k_j - 1)$ and $(k_j + 1)$ contain p_j as a factor, this implies $GCD((k_j - 1), (k_j + 1)) \geq p_j$. But $GCD((k_j - 1), (k_j + 1))$ is at most 2 for all $k_j \in \mathbb{N}$, and we have assumed $p_j \neq 2$, hence there is at least one prime which is not in our set $\mathcal{P}$ supposed to be complete, which contradicts our original assumption. □

For Further Reading

Aigner, Martin and Ziegler, Gunter. *Proofs from the Book.* Springer 2010.

Bogomolny, Alexander. *Infinitude of Primes.*

http://www.cut-the-knot.org/proofs/primes.shtml

Dickson, L. *History of the Theory of Numbers.* Vol. 1, Carnegie Institute of Washington 1919.

Meštrović, Romeo. *Euclid's Theorem on the Infinitude of Primes: A Historical Survey of its Proofs.* http://arxiv.org/pdf/1202.3670v2