American Math. Monthly, Vol 113, No. 10, December 2006.

A NEW PROOF OF EUCLID'S THEOREM

FILIP SAIDAK

A prime number is an integer greater than 1 that is divisible only by 1 and itself. Mathematicians have been studying primes and their properties for over twenty-three centuries. One of the very first results concerning these numbers was presumably proved by Euclid of Alexandria, sometime before 300 B.C. In Book IX of his legendary *Elements* (see [2]) we find Proposition 20, which states:

Proposition. *There are infinitely many prime numbers.*

Euclid's proof (modernized). Assume to the contrary that the set P of all prime numbers is finite, say $P = \{p_1, p_2, \cdots, p_k\}$ for a positive integer k. If $Q := (p_1 p_2 \cdots p_k) + 1$, then $\gcd(Q, p_i) = 1$ for $i = 1, 2, \cdots k$. Therefore Q has to have a prime factor different from all existing primes. That is a contradiction. ■

Today many proofs of Euclid's theorem are known. It may come as a surprise that the following almost trivial argument has not been given before:

New proof. Let n be an arbitrary positive integer greater than 1. Since n and $n+1$ are consecutive integers, they must be coprime. Hence the number $N_2 = n(n+1)$ must have at least two different prime factors. Similarly, since the integers $n(n+1)$ and $n(n+1)+1$ are consecutive, and therefore coprime, the number $N_3 = n(n+1)[n(n+1)+1]$ must have at least three different prime factors. This process can be continued indefinitely, so the number of primes must be infinite. ■

Analysis. The proof just given is conceptually even simpler than the original proof due to Euclid, since it does not use Eudoxus's method of "reductio ad absurdum," proof by contradiction. And unlike most other proofs of the theorem, it does not require Proposition 30 of *Elements* (sometimes called "Euclid's Lemma") that states: if p is a prime and $p|ab$, then either $p|a$ or $p|b$. Moreover, our proof is constructive, and it gives integers with an arbitrary number of prime factors.

Remarks. In Ribenboim [4, pp.3–11] and Narkiewicz [3, pp.1–10] one finds at least a dozen different proofs of the classical theorem of Euclid, and many other variations of the arguments listed in [1], [3], and [4] have been published over the years (in chronological order) by: Goldbach (1730), Euler (1737 and 1762), Kummer (1878), Perott (1881), Stieltjes (1890), Thue (1897), Brocard (1915), Pólya (1921), Erdős (1938), Bellman (1947), Fürstenberg (1955), Barnes (1976), Washington (1980), and others. Goldbach's proof (see [4], p.4), which uses pairwise coprimality of Fermat numbers, seems to be closest in spirit to the argument we have presented.

ACKNOWLEDGMENTS. Personal and virtual conversations with Professors Paulo Ribenboim (Queen's University) and Eduard Kostolansky (Bratislava) are gratefully acknowledged. I would also like to thank Professor Władyslaw Narkiewicz (Wroclaw) for bringing to my attention Hermite's very simple proof concerning $n! + 1$.

References

[1] M. Aigner and G. M. & Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin, 1999

[2] T. L. Heath, *The Thirteen Books of Euclid's Elements*, vol. 2, University Press, Cambridge, 1908; 2nd ed. reprinted by Dover, New York, 1956.

[3] W. Narkiewicz, *The Development of Prime Number Theory*, Springer-Verlag, New York, 2000

[4] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996