GANIT *J. Bangladesh Math. Soc.* (ISSN 1606-3694) **37** (2017) 185-187

THE INFINITUDE OF PRIME NUMBERS REVISITED

Munibur Rahman Chowdhury
Retired Professor of Mathematics, University of Dhaka

Received 14.09.2017 Accepted 14.10.2017

ABSTRACT

We present here a proof of the infinitude of prime numbers based on the sequence $n! + k$, $k = 2, 3, \ldots, n$.

Keywords: Prime number, Infinitude.

Introduction

The fact that there exist infinitely many prime numbers have intrigued mathematicians since antiquity. The earliest known proof of this fact is found in Euclid's Elements, Book IX, Proposition 20. Euclid's statement of the proposition is as follows:

> Prime numbers are more than any assigned multitude of prime numbers.

In other words, if $p_1, p_2, \ldots, p_r$ are given (or known) mutually distinct prime numbers (however large may r be), there exist prime numbers besides these.

Euclid takes the product of the given prime numbers and adds 1 to it, getting the number

$a = p_1p_2 \ldots p_r + 1$. If a is a prime number, then we have found a prime number besides the given prime numbers. If not, then the least (positive) divisor greater than 1 of a is a prime number distinct from each of the given prime numbers. Indeed, in Proposition 31 of Book VII Euclid had proved that the least (positive) divisor greater than 1 of any composite number is necessarily a prime number.

Euclid's proof of the infinitude of prime numbers is exceptionally clever; mathematicians of all generations have admired Euclid's ingenuity. Moreover, Euclid's proof is constructive; beginning with only one prime number (say 2 or 3; these are the only pair of consecutive numbers each of which is prime) it allows us to find as many new prime numbers as we please. Regrettably, Euclid's constructive proof is often presented as an indirect (*reductio ad absurdum*) proof. The most recent example of this is found in Andrew Granville's article [2]. We quote him:

Proofs that there are infinitely many prime numbers typically rely on the theorem that every integer $q > 1$ has a prime factor.

Euclid used this to prove that there are infinitely many primes as follows. Suppose that $p_1, \ldots, p_k$ is a complete list of all the prime numbers. Now $q = p_1 \ldots p_k + 1$ is divisible by some prime p. But then $p = p_j$ for some j and so $q \equiv 1 \pmod{p}$, so that $(q, p) = 1$, a contradiction.

This distorted paraphrasing of Euclid's proof is, to say the least, lamentable.

Gaps in the Sequence of Prime Numbers

The sequence (arranged in ascending order) of prime numbers, though infinite, has gaps of any prescribed length. In other words: there are blocks of consecutive composite numbers whose length exceeds any given number N. Indeed, setting $n = N + 2$ every term of the sequence $n! + 2, n! + 3, \ldots, n! + n$ is a composite number (being divisible by 2, 3, …, n, respectively); so this is a block of $n - 1 = N + 1$ consecutive composite numbers whose length exceeds the given number N.

We show that this familiar sequence of $n - 1$ terms can be used to give a proof of infinitude of prime numbers quite distinct from other known proofs. To this end we prove the result below.

Theorem. For every natural number $n > 1$ and $k = 2, 3, \ldots, n$, the number $n! + k$ either has a prime factor $> n$, or k is a prime number greater $\frac{n}{2}$ and $n! + k$ is a power of k.

Proof. Every prime number $p \leq n$ which divides $n! + k$ $(2 \leq k \leq n)$ also divides $(n! + k) - n! = k$. Should p be less than k, then p also divides $\frac{n!}{k}$; hence p does not divide $\frac{n!}{k} + 1 = \frac{n! + k}{k}$. Therefore, the number $\frac{n! + k}{k}$, hence also the number $n! + k$, has a prime divisor $> n$.

In case, all prime factors of $n! + k$ are $\leq n$, it follows that then k itself is a prime number and it is the only prime factor of $n! + k$. So $n! + k = k^s$ holds for some integer $s \geq 2$. Then $\frac{n!}{k} = k^{s-1} - 1$. k does not divide $k^{s-1} - 1$; so k does not divide $\frac{n!}{k}$. Therefore $k > \frac{n}{2}$, for if k were $\leq \frac{n}{2}$ then $2k$ would appear as a factor of $\frac{n!}{k}$; so k would then divide $\frac{n!}{k}$. The theorem stands proved.

Consequences of our Theorem

Corollary 1. For every $n > 1$, every term of the sequence $n! + 2, \ldots, n! + n$ has a prime divisor which does not divide any other term of the sequence.

Proof. In case some term $n! + k$ has a prime divisor greater than n, then this divisor has the desired property (because the difference between any two terms of the sequence is less than n). Otherwise, k has the desired property.

Corollary 2. There are infinitely many prime numbers.

This is an immediate consequence of Corollary 1; for it guarantees the existence of $n - 1$ distinct prime number for every natural number $n > 1$.

Grundhöfer [3] proved that for $n > 5$ none of the numbers $n! + 2, \ldots, n! + n$ can be the power of a single prime number. So we have the result below.

Corollary 3. For every $n \geq 6$, each of the numbers $n! + 2$, $n! + 3$, …, $n! + n$, has more than one prime factor and at least one of them is greater than n.

Postscript. The word ‘Panopoly’ in the title of Granville’s delightful article should have been ‘Panoply’.

REFERENCES

[1] The Thirteen Books of Euclid’s *Elements*

Translated from the Text of Heiberg with Introduction and Commentary by Sir Thomas L. Heath, K.C.B., K.C.V.O., F.R.S., Sc.D. Camb., Hon. D.Sc. Oxford, Honorary Fellow of Trinity College, Cambridge, Dover Publication (Three Volumes), New York 1956 (First published in 1908 by Cambridge University Press).

[2] Granville, G., A Panopoly of Proofs that there are Infinitely Many Prime Numbers, Newsletter of London Mathematical Society 472, September 2017, 23-27.

[3] Grundhöfer, T., Über die Zahlen der From $n! + k$, Archiv der Mathematik. **33**, (1979) 361-363.