ON EUCLID’S AND EULER’S PROOF THAT THE NUMBER OF PRIMES IS INFINITE AND SOME APPLICATIONS

ALI H. HAKAMI

Department of Mathematics
Faculty of Science
Jazan University
P. O. Box 277
Jazan, 45142
Saudi Arabia
e-mail: aalhakami@jazanu.edu.sa

Abstract

Euclid’s theorem is a fundamental statement in number theory that asserts that there are infinitely many prime numbers. In this paper, we shall give a new analytic technique to prove this well known theorem. Also, we shall use Euclid’s proof to show some facts.

1. Introduction

There are several proofs for the following well known theorem:

Theorem 1. The number of primes is infinite. That is, there is no end to the sequence of primes 2, 3, 5, 7, 11, 13, ….

2010 Mathematics Subject Classification: Primary 01A05, 11A41, 11A51; Secondary 11A07, 11A05, 11A25.

Keywords and phrases: prime, infinite of prime (IP), Euclid’s theorem, Euclid’s proof, Euler's proof of IP.

Received June 17, 2013

© 2013 Scientific Advances Publishers
Theorem 1 first appears in the works of Euclid [1], which has the advantage of depending on little beyond the definition of the primes. Another proof for Theorem 1, by the Swiss mathematician Leonhard Euler [7], relies on the fundamental theorem of arithmetic, see, for example, [8], that every integer has a unique prime factorization. We shall give these two proofs in the next section. Hillel [5] introduced a proof for Theorem 1 by using point-set topology and Pinasco [3] by using inclusion-exclusion principle, the number of positive integers less than or equal to \( x \) that are divisible by one of the smallest \( N \) primes \( p_1, \ldots, p_N \).

Whang [4] has recently published his proof for Theorem 1 by contradiction with the de Polignac’s formula
\[
\sum_{\text{prime } p} p^{\nu(p)} = \pi_1 \times \pi_2 \times \pi_3 \times \cdots
\]
where \( k \) is any positive integer and \( f(p, k) = \lfloor k/p \rfloor + \lfloor k/p^2 \rfloor + \cdots \). Theorem 1 can be also proved by using Euler’s totient function \( \phi \) (see, for example, [6]). In this proof, one need the following property: For \( n \geq 3 \), \( \phi(n) \) is an even integer. Lastly, one can proof Theorem 1 by using the irrationality of \( \pi \). He need to amply the following formula, which was also discovered by Euler primes:

\[
\frac{\pi}{4} = \frac{3}{4} \times \frac{5}{4} \times \frac{7}{8} \times \frac{11}{12} \times \frac{13}{16} \times \frac{17}{20} \times \frac{19}{24} \times \frac{23}{28} \times \frac{29}{32} \times \cdots
\]

2. Euclid’s and Euler’s Proof That the Number of Primes is Infinite

Euclid’s proof of Theorem 1. We assume there are only the primes \( p_1, p_2, \ldots, p_k \) and no more. Consider the number

\[
Q = p_1 p_2 \cdots p_k + 1.
\]

Now is either prime or else has a prime factor. If \( Q \) is prime, we have a contradiction, since \( p_1, p_2, \ldots, p_k \) are supposed to be all primes. But any prime factor of \( Q \) must be different from all of \( p_1, p_2, \ldots, p_k \), since it is easy to see that none of the \( ps \) can divided \( Q \). This again contradictions the assumption that \( p_1, p_2, \ldots, p_k \) comprise all the primes.
It is often erroneously reported the Euclid proved this result by contradiction, beginning with the assumption that the set initially considered contains all prime numbers, or that it contains precisely the smallest primes, rather than any arbitrary finite set of primes (see [2]). Although the proof as a whole is not by contradiction, in that it does not begin by assuming that only finitely many primes exist, there is a prove by contradiction within it, that is the proof that none of the initially considered primes can divide the number called \( Q \) above.

**Euler’s proof of Theorem 1.** Euler gave a more sophisticated proof of Theorem 1. Again, we assume \( p_1, p_2, \ldots, p_k \) are all the primes. Then if \( n \) is any positive integer, we may choose \( r \) big enough so that all the terms \( 1, 1/2, 1/3, \ldots, 1/n \) appear when we multiply out the product

\[
\left( 1 + \frac{1}{p_1} \right) \left( 1 + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \cdots \right) \left( 1 + \frac{1}{p_2} \right) \left( 1 + \frac{1}{p_2^2} + \frac{1}{p_2^3} + \cdots \right) \cdots \left( 1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \cdots + \frac{1}{p_k^r} \right).
\]

In fact increasing \( r \) merely adds in more terms. For example, we get \( 1/12 \) by choosing \( 1/2^2 \) from the first factor, \( 1/3 \) from the second, and \( 1 \) from all the others (assuming that \( p_1 = 2 \) and \( p_2 = 3 \)).

Now, by the formula for the sum of geometric progression

\[
1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^r} = \frac{1 - (p^{-1})^{r+1}}{1 - p^{-1}} < \frac{1}{1 - p^{-1}} = \frac{p}{1 - p^{-1}}.
\]

We see that for any \( n \), the sum

\[
1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n},
\]

cannot exceed

\[
\frac{p_1}{p_1 - 1}, \frac{p_2}{p_2 - 1}, \ldots, \frac{p_k}{p_k - 1}.
\]

But this contradicts the divergence of the harmonic series \( 1 + 1/2 + 1/3 + \cdots \). So, there is an infinite number of primes.
3. Theorem 1 and the Harmonic Series $1/p_1 + 1/p_2 + \cdots$

Our technique to prove Theorem 1 is to prove that the harmonic series $1/p_1 + 1/p_2 + \cdots$ is diverges. To this end, we need the following lemma:

**Lemma 1.** (i) For $k$, any positive integer

$$
\left(1 + \frac{1}{p}\right)\left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots + \frac{1}{p^{2k}}\right) = \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{2k+1}}\right).
$$

(ii) Let the $i$-th prime be $p_i$, and let $N$ be the set of all positive integers all of whose prime factors are $\leq p_k$. Then

$$
\left(1 + \frac{1}{p_1}\right)\left(1 + \frac{1}{p_2^2}\right)\cdots\left(1 + \frac{1}{p_i}\right)\sum_{n \in N} \frac{1}{n^2} = \sum_{n \in N} \frac{1}{n}.
$$

(iii) The limit

$$
\left(1 + \frac{1}{p_1}\right)\left(1 + \frac{1}{p_2}\right)\cdots\left(1 + \frac{1}{p_n}\right) \rightarrow \infty \text{ as } n \rightarrow \infty.
$$

(iv) If $C > 0$ ($C$ is constant), then $e^C > 1 + C$.

**Proof.** (i) Let $S(k)$ be represented by

$$
1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots + \frac{1}{p^{2k}}.
$$

Clearly,

$$
\left(1 + \frac{1}{p}\right)S(k) = S(k) + \left(\frac{1}{p} + \frac{1}{p^3} + \cdots + \frac{1}{p^{2k+1}}\right).
$$

If we take a limit $k \rightarrow \infty$ in the left hand side and the right hand side, we will get the following equality used in the following equality:

$$
\left(1 + \frac{1}{p}\right)\left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right)\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right).
$$
(ii) We observe that the fundamental theorem of arithmetic (see [8]) implies
\[ \sum_{n \in N} \frac{1}{n} = \prod_{i=1}^{k} \left( 1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots \right), \]
and
\[ \sum_{n \in N} \frac{1}{n^2} = \prod_{i=1}^{k} \left( 1 + \frac{1}{p_i^2} + \frac{1}{p_i^4} + \cdots \right). \]

Now (i) gives
\[ \left( 1 + \frac{1}{p_i} \right) \left( 1 + \frac{1}{p_i^2} + \frac{1}{p_i^4} + \cdots \right) = 1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots. \]

Multiplying these identities for \( i \) from 1 to \( k \), we get the statement of (ii).

(iii) The sequence \( s_k = \prod_{i=1}^{k} \left( 1 + \frac{1}{p_i} \right) \) is increasing. If it is bounded, then so is
\[ \left( 1 + \frac{1}{p_1} \right) \left( 1 + \frac{1}{p_2} \right) \cdots \left( 1 + \frac{1}{p_k} \right) \sum_{n \in N} \frac{1}{n^2} = \sum_{n \in N} \frac{1}{n}. \]

(since \( \sum_{n \in N} \frac{1}{n^2} \) is bounded by \( \sum_{n=1}^{\infty} \frac{1}{n^2} \) and the series \( \sum_{n=1}^{\infty} \frac{1}{n^2} \) is convergent). But this is not the case since for sufficiently large any \( k \), \( \sum_{n \in N} \frac{1}{n} \) is bigger than any partial sum of \( \sum_{n \in N} \frac{1}{n} \) and the harmonic series is divergent. Thus \( s_k \) is not bounded, that is, \( \lim_{k \to \infty} s_k = \infty \).

(iv) Consider a function \( f(x) = e^x - 1 - x \). We have in \( f'(x) = e^x - 1 \geq 0 \) for \( x \geq 0 \). Thus \( f(x) \) is increasing for \( x \geq 0 \). Since \( f(0) = 0 \), we get that \( f(x) > 0 \) for any positive \( x \). \( \square \)
Our proof of Theorem 1. Use Lemma 1, (iii) and (iv), we have
\[
\phi^1/p_1 \phi^1/p_2 \cdots \phi^1/p_k = \phi^1/p_1 \phi^1/p_2 \cdots \phi^1/p_k \\
\geq \left( 1 + \frac{1}{p_1} \right) \left( 1 + \frac{1}{p_2} \right) \cdots \left( 1 + \frac{1}{p_k} \right).
\]

Thus, the sequence \( t_n = \frac{1}{p_1} + \cdots + \frac{1}{p_k} \) grows without bound. This means the number of primes is infinite.

4. Some Application

In this section, we shall adapt the proof of Euclid to show the following facts:

1. The \( n \)-th prime does not exceed \( 2^{2^{n-1}} \) for any positive integer \( n \).

2. For any positive integer \( x \), \( \pi(x) > \log_2 \log_2 x \) (here \( \pi(x) \) denotes the number of primes \( p \leq x \)).

3. There are infinitely many primes of the form \( p = 3n + 2, n \in \mathbb{N} \).

For (1), we need to use Euclid’s proof and generalized induction, so when \( n = 1 \), the first prime is \( p_1 = 2 \leq 2^{2^{n-1}} = 2^0 = 2 \). Suppose that \( p_j \leq 2^{2^{j-1}} \) for any \( 1 \leq j \leq n \), and any \( n \geq 1 \). We have to show that \( p_{n+1} \leq 2^{2^n} \). Reasoning as in Euclid’s proof, there is a prime \( p \neq p_1, p_2, \ldots, p_n \), which divides \( (p_1 \ldots p_n) + 1 \), i.e., \( p \leq (p_1 \ldots p_n) + 1 \), and then the \((n+1)\)th prime, which is smaller or equal than the prime \( p \), is such that

\[
P_{n+1} \leq \left( \prod_{j=1}^{n} p_j \right) + 1 \leq \left( \prod_{j=1}^{n} 2^{2^{j-1}} \right) + 1 = \left( 2^{\sum_{j=1}^{n} 2^j} \right) + 1, \]

using the induction hypothesis. For any integer \( m \geq 1 \) and any real number \( r \neq 1 \), we have that
\[
\sum_{j=0}^{m} r^j = 1 + r + r^2 + \cdots + r^m = \frac{1 - r^{m+1}}{1 - r},
\]
(which follows easily by multiplying by \((1 - r)\) on both sides). Then
\[
\sum_{j=1}^{n} 2^{j-1} = \sum_{j=0}^{n-1} 2^j = \frac{1 - 2^n}{1 - 2} = 2^n - 1.
\]
And replacing in the equation above, we have
\[
p_{n+1} \leq 2^{n-1} + 1 = \frac{1}{2} \left( 2^n \right) + 1 \leq 2^{2n},
\]
for any \(n \geq 1\).

For (2), using (1), we have that \(\pi\left(2^{2^{n-1}}\right) \geq n\) as the \(n\)-th prime is at most are \(2^{n-1}\). Let \(n\) be the unique integer such that
\[
2^{2^{n-1}} \leq x < 2^{2^n}.
\]
Then,
\[
\pi(x) \geq \pi\left(2^{2^{n-1}}\right) \geq n,
\]
and using the above condition, we have that
\[
2^{2^n} > x \iff 2^n > \log_2 x \iff n > \log_2 \log_2 x,
\]
which implies that \(\pi(x) > \log_2 \log_2 x\).

Finally for (3), we suppose that there are only finitely many primes \(p\) of the form \(p = 3n + 2\), say \(p_1, p_2, \ldots, p_n\). We consider the integer
\[
N_n = 3 \left( \prod_{j=1}^{n} p_j \right) - 1.
\]
We have to show that there is a prime \( p \) of the form \( 3n + 2 \) dividing \( N_n \). Suppose that all primes dividing \( N_n \) are of the form \( p = 3n + 1 \), i.e., \( N_n \) is a product of primes of the form \( 3n + 1 \). Then, as the set of those primes is closed under product, \( N_n \) would also be of the form \( 3n + 1 \), which is false as 
\[
N_n = 3(\prod_{i=1}^{n} p_i) - 1 = 3k - 1 = 3(k - 1) + 2.
\] There is then a prime \( p \) of the form \( 3n + 2 \) dividing \( N_n \). If \( p = p_i \) for some \( 1 \leq i \leq n \), then \( p \) divides \( (\prod_{i=1}^{n} p_i) - N_n = 1 \), which is impossible. This is a contradiction, and it is shows that there are infinitely many primes \( p \) of the form \( p = 3n + 2 \).

References