BAREKENG: Journal of Mathematics and Its Applications
March 2023 Volume 17 Issue 1 Page 0475–0480
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol17iss1pp0475-0480

ALTERNATIVE PROOF OF THE INFINITUDE PRIMES AND PRIME PROPERTIES

Dinni Rahma Oktaviani [1*], Muhammad Habiburrohman[2], Fiki Syaban Nugroho[3]

[1,3]Department of Mathematics, Faculty,of Science and Technology, UIN Walisongo Semarang
Prof. Hamka St., Semarang, 50185, Indonesia
[2]Department of Machine Technique, Faculty, of Science and Technology, Universitas Ivet
Pawayitan Luhur IV St., Semarang, 50235, Indonesia

*Corresponding author's e-mail: * **dinni@walisongo.ac.id***

ABSTRACT

Prime numbers are one kind of number that have many uses, one of which is cryptography. The uniqueness of prime numbers in their divisors and distributions causes prime numbers to be widely used in digital security systems. In number theory, one of the famous theorems is Euclid's theorem. Euclid's theorem says about infinitely of prime numbers. Many alternative proofs have been given by a mathematician to find new theories or approximations of prime properties. The construction of proof gives new ideas about the properties of a prime number. So, in this study, we will give an alternative proof of Euclid's theorem and investigate the properties of prime in distribution

Article History:

Received: 14th November 2022
Revised: 3rd February 2023
Accepted: 13th February 2023

Keywords:

Prime;
Infinity Prime Number;
Alternative Proof;
Prime Properties

How to cite this article:

D. R. Oktaviani, M. Habiburrohman and F. S. Nugroho., "ALTERNATIVE PROOF OF THE INFINITUDE PRIMES AND PRIME PROPERTIES," *BAREKENG: J. Math. & App.*, vol. 17, iss. 1, pp. 0475-0480, March 2023.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article • Open Access

1. INTRODUCTION

A prime number is a positive integer that only has two factors i.e., one and itself [17]. There are many benefits of a prime number. A prime number has shown its existence in nature. Cicadas of type Brood X spend most of their time hiding, only reappearing to mate every 13 or 17 years. In other words, cicada's cycle is prime number. This cycle minimizes interaction between predators and cicadas [15]. Prime numbers are also used n cryptography. Known as RSA, this system is based on basic number theory concepts, and its security lies in the inability to factor a number that is the product of two large primes, each more than 200 digits long. [9]. An asymmetric key-based Cryptographic Algorithm using Four Prime numbers (ACAFP) is a cryptographic algorithm that adopts the theory that four prime numbers are difficult to destroy and can increase the effectiveness of communication security [6]. Improving the security of data access or currency transactions electronic improvement can use a combination of two methods, namely digital face and the product of two prime numbers [10]. Modification Additive Generator Fibonacci (AGF) by using prime numbers as an iterative equation module that describes the operation of the generator to be implemented in hardware that allows providing high performance [13].

In addition to the factor properties of prime numbers, the distributional property of prime numbers has many uses [11]. Hence the distributional property has been researched a lot. The irregular distribution of prime numbers has multiple uses [12]. The distance between adjacent prime numbers statistically follows the Poisson distribution [20]. The distribution of prime numbers can be modeled by the differential-difference equation [14], and support vector domain description [5]. Combinatorics of the new class exhibits the same properties as the distribution of prime numbers, and the probability distribution of the combinatorial pairs of the nth primes is derived together with the probability of the prime count function (x) [4]. Besides researching the distribution of prime numbers, mathematicians also examine the sum of n prime numbers [2] and the exponential sums [16]. Bourgain estimated that the number of primes proportional to the digit specified in base 2 is an indeterminate absolute constant [8]. Cathy establishes the generalizability of these results n any basis and gives an explicit value that can be accepted for the proportion depending on [18].

Various special types of primes are defined, such as Luhn Prime numbers and Beurling's generalized prime number [7]. Prime numbers can be formed in a number of ways. Eratosthenes sieve and Sundaram sieve are two algorithms that can be used to generate prime numbers from random or sequentially generated random numbers [1]. Prime numbers can also be formed by inserting several digits between the numbers that make up the prime numbers with certain patterns [19]. And Baibekov, S., & Altynbek, S. is also developing a new method for distributing prime number [3].

Many researchers discuss the distribution and formation of a prime number. In this research, we will give the properties of prime numbers about the distribution by divisibility concept. But before that, we will give the alternative proof of infinity prime numbers in the hope that the construction can form prime numbers again.

2. RESEARCH METHODS

The research method relies on the literature on integer systems, divisibility, and prime number. We first searched the properties of divisibility integer, prime properties, and previous Euclid's theorem proof. So, we can get the alternative proof of the Infinitude prime number that is different from the previous proof. We also investigate the properties of prime numbers about their distribution.

3. RESULTS AND DISCUSSION

An integer $p \geq 2$ is prime number if and only if its divisors are only 1 and itself. The other is composite. Euclid's theorem says that there are infinitely many prime numbers Proof of theorem using contradiction. Assume there is finitely many prime numbers, $p_1 = 2, p_2 = 3, \ldots, p_n$. Construct $N = p_1 p_2 \cdots p_n + 1$. Since $p_1 = 2$, then $N \geq 2$. So, N have a prime divisor p. The prime divisor must one of $p_1, p_2, \cdots, p_n$ because the assumptions. But note the equation

$$N = p_i (p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n) + 1$$

with $0 \leq 1 < p_i$ then N can't divide by p_i.

If it is a contradiction, then the assumption is false. It should be infinitely many prime numbers (Proven). By using the properties of prime numbers and divisibility, we construct constructions different from those presented by Euclid.

The alternative proof. Suppose there are finitely many prime numbers, such that $p_1 = 2,\ p_2 = 3, \ldots,\ p_n$. Let $N = p_1 p_2 \cdots p_{i-1} p_{i-2} \cdots p_n + pi.\ \ i \in \{1,2,\ldots,n\}$
Since $p_1 = 2$, then $N \geq 2$. Consider N have prime divisor p. The prime is must be one of $p_1, p_2, \ldots, p_n$ as from the assumption that many prime numbers is finite.
Without loss of generality, we have $p_k \mid N$, with $p_k \in \{p_1, p_2, \ldots, p_n\}$ implies there are integer m such that $N = p_k . m$
Write

$$N = p_k . m = p_1 p_2 \cdots p_{i-1} p_{i-2} \cdots p_n + pi$$

then

$$m = \frac{p_1 p_2 \cdots p_{i-1} p_{i-2} \cdots p_n + pi}{p_k} = \frac{p_1 p_2 \cdots p_{i-1} p_{i-2} \cdots p_n}{p_k} + \frac{pi}{p_k}$$

If $i = k$, then $p_k \mid p_1 p_2 \cdots p_{i-1} p_{i-2} \cdots p_n$(contradiction)
If $i \neq k$, then $p_k \mid p_i$(contradiction).
It means that must be there are other prime number of $\{p_1, p_2, \ldots, p_n\}$ be divisor of N.

The construction of the alternative proof does not always be prime numbers, but sure gives different prime factor.

Example 1. The sum of 2.3.5+7=37 is prime, but 2.3.5.7+11=221 is composite because 221 is product of 13 and 17 (13 and 17 is the different prime factor).

The pattern or distribution of prime numbers seems random. But with the patterns, we formulate some properties of the distribution of prime numbers as follows. The properties are proved by divisibility properties and the definition of a prime number.

Theorem 1. *There are no five consecutive odd number are all prime.*
Proof. Let $k, k+2, k+4, k+6, k+8$ are five consecutive odd number. By using division algorithm, we have five cases, there are:
1. If $k = 0\ mod\ 5$, the proof is done, because k is composite.
   a. Take $k = 5$, then $k + 4$ is 9.
   b. Take $k = a5$ where a is integer, $a \neq 1$, then k is composite, since that 5 is positive divisor of k, besides of 1and k.
2. If $k \equiv 1(mod\ 5)$, then $k + 4 \equiv 1 + 4(mod\ 5)$ or $k + 4 \equiv 0(mod\ 5)$. So $k + 4$ is composite by case (1)
3. If $k \equiv 2(mod\ 5)$, then $k + 8 \equiv 2 + 8(mod\ 5)$ or $k + 8 \equiv 0(mod\ 5)$. So $k + 8$ is composite by case (1)
4. If $k \equiv 3(mod\ 5)$, then $k + 2 \equiv 3 + 2(mod\ 5)$ or $k + 2 \equiv 0(mod\ 5)$. So $k + 2$ is composite by case (1)
5. If $k \equiv 4(mod\ 5)$, then $k + 6 \equiv 4 + 6(mod\ 5)$ or $k + 6 \equiv 0(mod\ 5)$. So $k + 6$ is composite by case (1)

Theorem 2. *For integer $n > 3$, there are no three consecutive odd number are all prime.*
Proof. Let $k, k+2, k+4$ are three consecutive odd number. By using division algorithm, we have three cases, there are:
1. If $k \equiv 0(mod\ 3)$, then $k = 3a$ with integer a and $a \neq 1$, clear that k has positive factor is 3, different with k and 1. So, k is composite.
2. If $k \equiv 1\ (mod\ 3)$, then $k + 2 \equiv 1 + 2\ (mod\ 3)$ or $k + 2 \equiv 0\ (mod\ 3)$. So $k + 2$ is composite by case (1).
3. If $k \equiv 2\ (mod\ 3)$, then $k + 4 \equiv 2 + 4\ (mod\ 3)$ or $k + 4 = 0\ (mod\ 3)$. So $k + 4$ is composite by case (1).

Theorem 3. *Let p prime, $p = 3n + 1$ with integer n then there is integer m such that $p = 6m + 1$.*
Proof. Let $p = 3n + 1$ prime with integer n then p odd. Since p odd, then $p - 1$ even. Note $p - 1 = 3n$ is even implies that n even. As n even then there is integer m such that $n = 2m$. So,

$$p = 3n + 1 = 3(2m) + 1 = 6m + 1.$$

Theorem 4. *For $n > 1$, there are no prime p such that $p = n^3 + 1$.*
Proof: We have $n^3 + 1 = (n + 1)(n^2 - n + 1), n^3 + 1$ is not prime if one of the factors is equal to 1 and the other factor is equal to $n^3 + 1$. It's clear that $(n + 1) > 1$, then we have $n + 1 = n^3 + 1$. For $n > 1$, is impossible if $n + 1 = n^3 + 1$. So, it is true that there are no prime with form $n^3 + 1$, for $n > 1$.

Theorem 5. *For integer a and b, $a > b$, there are no prime p such that $a^4 - b^4 = p$.*
Proof: For $a > b$, let $n = a^4 - b^4 = (a - b)(a + b)(a^2 + b^2)$. From the quation we have $a + b$ as factor of $a^4 - b^4$, furthermore $a + b$ is not 1 and n.

Theorem 6. *If p and $p^2 + 8$ is prime then $p^3 + 4$ is also prime.*
Proof: Consider the previous theorem, if $p > 3$ prime, then p have $6k + 1$ or $6k + 5$ form with integer k. For $p = 6k + 1$ then $p^2 + 8 = (6k + 1)^2 + 8 = 36k^2 + 12k + 9$, and if $p = 6k + 5$ then $p^2 + 8 = (6k + 5)^2 + 8 = 36k^2 + 60k + 33$. Furthermore 3 is the factor of $p = 6k + 1$ and $p = 6k + 5$, such that $p^2 + 8$ is not prime for $p > 3$. From the condition, p must be prime and $p^2 + 8$ is also prime, then the p that have the condition is only $p = 3$. If $p = 3$ then $p^2 + 8 = 17$. Hence $p^3 + 4 = 31$.

Theorem 7. *For each odd prime p is the form of p either $4k + 1$ or $4k + 3$, for any non-negative integer k.*
Proof: By using division algorithm, for any integer a, we can write a as $a = bq + r, 0 \leq r < b$ or equivalent with $a = 4q + r, r = 0,1,2,3$
Since $a = 4q + r, r = 0,1,2,3$, we have four cases, there are

1. $r = 0, a = 4q = 2(2q)$, integer even.
2. $r = 1, a = 4q + 1 = 2(2q) + 1$, integer odd.
3. $r = 2, a = 4q + 2 = 2(2q + 1) = 2m$, integer even.
4. $r = 3, a = 4q + 3 = 2(2q + 1) + 1 = 2m + 1$, integer odd.

Hence, any odd prime p have the form either $4k + 1$ or $4k + 3$ for any non-negative integer k.

Theorem 8. *There is no arithmetic progression with the form $a, a + b, a + 2b, \ldots$ that consist only prime number.*
Proof: Let $p = a + nb$ by division algorithm, with prime p. If $n_k = n + kp$ for $k = 1,2,3 \ldots$ then the n-th of arithmetic progression is n_k, we have

$$\begin{aligned} a + n_k b &= a + (n + kp)b \\ &= (a + nb) + kpb \\ &= p + kbp \\ &= p(1 + kb) \end{aligned}$$

Hence p is factor of a+$n_k b$, then $a + n_k b$ is not prime. So, no arithmetic progression consists of only prime numbers.

Remark 1. *The arithmetic progression consists infinity composite number.*

Theorem 9. *For all p prime with $p \leq \sqrt{n}$ such that $p \nmid n$ then n prime or n is product of 2 primes.*
Proof. This theorem says that for this condition n is prime or composite with product of two primes.
If n prime then done. If n composite, suppose that n is a product of more than two primes, write $n = p_1 p_2 p_3 \ldots p_k, k \geq 3$. Furthermore $p_1 p_2 p_3 \ldots p_k > \sqrt[3]{n}$, then $p_1 p_2 p_3 \ldots p_k > \sqrt[3]{n}\sqrt[3]{n}\sqrt[3]{n} = n$. So $p_1 p_2 p_3 \ldots p_k > n$ (contradiction), so n must be product of 2 primes.

In addition to the pattern of prime numbers, the nature of the distribution of prime numbers can also be seen from the boundaries of a prime number, such as the following properties.

Theorem 10. *Let integer $n, n > 2$, then there is prime p such that $n < p < n!$.*
Proof: For n>2 we have $n < n! - 1 < n!$, if $n! - 1$ prime then done.
If $n! - 1$ is not prime, then select prime factor $n! - 1$, such that $p < n! - 1$. Let $p \leq n$, then p is one of 1,2,3,…,n. So $p|n!$. Furthermore $p|n!$ and $p|(n! - 1)$, by using divisibility properties we have $p|(n! - (n! - 1)) = 1$. Hence, $p > n$.

Theorem 11. *For each integer $n \geq 2$, there is prime p such that $p < n < 2p$.*
Proof:
The proof will use Bertrand's Conjecture that for any positive integer $z > 1$, there are prime p such that $z \leq p < 2z$.
Case 1: Let n odd, since $n \geq 2$ then there is integer $k \geq 1$ such that $n = 2k + 1$. Note $p < (p + 1) < (2k + 1) = n \Rightarrow p < n$. Furthermore $2k < 2p \Rightarrow (2k + 1) \leq 2p \Rightarrow n \leq 2p$. We have $2k + 1$ odd, and $2p$ even, then we get conclusion is $n < 2p$. Hence, there is prime p such that $p < n < 2p$.
Case 2: Let n even. Implies that there is integer $k \geq 1$ such that $n = 2k$. $k < p < 2k = n \Rightarrow p < n$ (p prime). Furthermore $n = 2k < 2p \Rightarrow n < 2p$. So, we get $p < n < 2p$.

Theorem 12. *If n-th prime is p_n then $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$ for $n \geq 3$..*
Proof: Since p_n is prime, we have $p_{n+1} < 2p_n$. Furthermore $p_{n+3} < 2p_{n+2}$. Then $p_{n+3}^2 < 4p_{n+2}^2 < 4p_{n+2}(2p_{n+1}) = 8p_{n+2}p_{n+1}$. Let $p_5 = 11 \Rightarrow 8p_{n+2}p_{n+1} < p_5 p_{n+2} p_{n+1}$. Therefore $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$, if $n \geq 5$
If $n = 4$ then $p_7^2 = 289 < p_4 p_5 p_6 = 1001$.
If $n = 3$ then $p_6^2 = 169 < p_3 p_4 p_5 = 385$.
If $n = 2$ then $p_5^2 = 121 < p_2 p_3 p_4 = 105$. Hence, for $n \geq 3$ we have $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$

Theorem 13 *If the n-th prime is p_n then $p_n < p_1 + p_2 + p_3 \cdots + p_{n-1}$ for $n > 3$.*
Proof: Proof using contradiction
For $n = 4$, we get $7 < 2 + 3 + 5$
For $n = 5$, we have $11 < 2 + 3 + 5 + 7$
For $n = 6$, we have $13 < 2 + 3 + 5 + 7 + 11$
For $n = 7$, we have $17 < 2 + 3 + 5 + 7 + 11 + 13$
⋮
And so on.
Suppose there are $n > 3$ y such that $p_n \geq p_1 + p_2 + p_3 \cdots + p_{n-1}$. Take the smallest n have that satisfying the condition. Let the smallest integer $n = ka > 3$ that satisfying $p_k \geq p_1 + p_2 + p_3 \cdots + p_{k-1}$. Consider the condition, then we have $p_{k-1} < p_1 + p_2 + p_3 \cdots + p_{k-2}$.
As a consequence

$$\begin{aligned} p_k &\geq (p_1 + p_2 + p_3 \cdots + p_{k-2}) + p_{k-1} \\ &> p_{k-1} + p_{k-1} \\ &= 2p_{k-1} \end{aligned}$$

Then we get $p_k > 2p_{k-1} > p_{k-1} \Rightarrow p_k > p_{k-1}$. Then Consider Bertrand's conjecture, there is prime number between p_{k-1} and $2p_{k-1}$ (let p_s). Then $p_k > 2p_{k-1} > p_s > p_{k-1} \Rightarrow p_k > p_s > p_{k-1}$.
This is contradiction with p_{k-1} and p_k consecutive prime number.

4. CONCLUSIONS

The alternative proof of Euclid's theorem about the infinity of prime numbers uses divisibility properties with another construction of contradiction proves. But the construction is just saying that there are other prime factors. The construction does not always make a prime number. There are eleven properties of the prime distribution.

AKNOWLEDGEMENT

The author would like to thank all those who have provided support, especially the reviewers and my team research for the suggestion for improving our manuscript, also LP2M for the support of this research and the funding. And big thanks to the Barekeng journal's team, who were pleased to publish this manuscript.

REFERENCES

[1] Sukirman, *Logika dan Himpunan*. Yogyakarta: Hanggar Kreator, 2006.

[2] V. B. K. Olsen, V. B. K. Olsen, and W. Thrush, "Avian Insectivores Respond to 17-year Brood X Periodical Cicada Emergences Hypothesis : Avian insectivores show a positive numerical Discussion : This," in *University of Maryland Graduate Research Interaction Day*, 2007, no. Aprill.

[3] D. B. Ginting, "Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA (Rivest-Shamir-Adleman)," *Media Inform.*, vol. 9, no. 2, 2010.

[4] P. Chaudhury *et al.*, "ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm," in *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, 2017, pp. 332–337.

[5] G. Iovane, C. Bisogni, L. De Maio, and M. Nappi, "An encryption approach using information fusion techniques involving prime numbers and face biometrics," *IEEE Trans. Sustain. Comput.*, vol. 5, no. 2, pp. 260–267, 2018.

[6] V. Maksymovych, O. Harasymchuk, M. Karpinski, M. Shabatura, D. Jancarczyk, and K. Kajstura, "A new approach to the development of additive Fibonacci generators based on prime numbers," *Electronics*, vol. 10, no. 23, p. 2912, 2021.

[7] W. S. Kendal and B. Jørgensen, "A scale invariant distribution of the prime numbers," *Computation*, vol. 3, no. 4, pp. 528–540, 2015.

[8] S. Kristyan, "On the statistical distribution of prime numbers: A view from where the distribution of prime numbers are not erratic," in *AIP Conference Proceedings*, 2017, vol. 1863, no. 1, p. 560013.

[9] M. Wolf, "Nearest-neighbor-spacing distribution of prime numbers and quantum chaos," *Phys. Rev. E*, vol. 89, no. 2, p. 22922, 2014.

[10] S. H. Marshall and D. R. Smith, "Feedback, control, and the distribution of prime numbers," *Math. Mag.*, vol. 86, no. 3, pp. 189–203, 2013.

[11] M. El Boujnouni, "A study of prime numbers distribution based on support vector domain description," *J. Inf. Optim. Sci.*, vol. 42, no. 4, pp. 865–882, 2021.

[12] V. Barbarani, "Combinatorial Models of the Distribution of Prime Numbers," *Mathematics*, vol. 9, no. 11, p. 1224, 2021.

[13] C. Axler, "On the sum of the first $ n $ prime numbers," *J. Théorie des Nombres Bordeaux*, vol. 31, no. 2, pp. 293–311, 2019.

[14] Z. K. Rakhmonov and F. Z. Rakhmonov, "Sum of short exponential sums over prime numbers," in *Proceedings XII International Conference Algebra and Number Theory: Modern Problems and Application, dedicated to 80-th anniversary of Professor VN Latyshev TULA (2014)*, 2014, p. 148.

[15] G. Debruyne, J.-C. Schlage-Puchta, and J. Vindas, "Some examples in the theory of Beurling's generalized prime numbers," *arXiv Prepr. arXiv1505.04174*, 2015.

[16] C. Swaenepoel, "Prime numbers with a positive proportion of preassigned digits," *Proc. London Math. Soc.*, vol. 121, no. 1, pp. 83–151, 2020.

[17] O. Cira and F. Smarandache, "Luhn prime numbers," *Collect. Pap. V*, p. 37, 2014.

[18] D. Abdullah, R. Rahim, D. Apdilah, S. Efendi, T. Tulus, and S. Suwilo, "Prime numbers comparison using sieve of eratosthenes and Sieve of Sundaram Algorithm," in *Journal of Physics: Conference Series*, 2018, vol. 978, no. 1, p. 12123.

[19] I. J. Taneja, "Multiple Choice Patterns in Prime Numbers-III," RGMIA Research Report Collection, 20, 2017.

[20] S. Baibekov and S. Altynbek, "Development of new method for generating prime numbers," *Nat. Sci.*, vol. 7, no. 08, p. 416, 2015.