On the Infinitude of Primes of Certain Types

Abstract

Prime numbers and their patterns are a very important topic historically as well as in current times with applications to fields such as cryptography. In this paper, we give different proofs than those availiable in the literature of infinitude of primes of the type $4k+3$, $6k+5$, and $4k+1$. These are all special cases of the Dirichlet prime number theorem. We have used the technique of Saidak as well as divisibility properties to construct an expression different from that availiable in literature, to prove the infinitude of the primes of the form $4k+3$ and $6k+5$. The infinitude of primes of the type $3k+2$ is a corollary.

To prove that there are infinitely many primes of the type $4k+1$, we have showed that Fermat numbers for $n \geq 1$ are of the form $4k+1$ and any two of them are coprime. This along with a standard result in number theory has enabled us to prove that there are infinitely many primes of the type $4k+1$.

Mathematics Subject Classification[2020]: Primary 11A41

Keywords: Infinitude of primes, Dirichlet theorem, Fermat Number

1 Introduction

Prime numbers are one of the most important concepts in elementary number theory. Prime numbers can be considered as building blocks of integers. This is formally known as the Fundamental Theorem of Arithmetic. It says that every integer greater than 1 can, except for the order of factors, be represented as a product of primes in one and only one way. So the study of primes is essential. An obvious question is whether the number of primes is finite. The answer is negative. Several proofs of the infinitude of primes can be found in the literature. The subject is of great historical importance. It is relevant in modern times as properties of primes are greatly used in encryption algorithms. The properties of primes have been studied extensively in [4], [5]. The properties of whether there are infinitely many composite numbers of a certain type have been studied in [11].

More than 2000 years ago, Euclid proved that there were infinitely many primes by using the method of contradiction. Kummer's proof involved an elegant variation of Euclid's proof. In 1737, Euler proved the same by showing that the sum of reciprocals of primes diverges. In 1938, Paul Erdos gave an alternative proof of the same. There are many beautiful proofs of this classical theorem [3]. There is also a topological proof of the same by Furstenburg proved in 1955. A group theoretical proof involving Fermat's little theorem and Lagrange's theorem for finite groups to prove the infinitude of primes exists. One can also prove the infinitude of primes by constructing any infinite set of natural numbers such that any two numbers of the set are coprime. There is an elegant proof by Polya on these lines. For a few other proofs, you may refer to [2],[14] [7]. We see that the techniques used in each of the proofs are very different from one another. They involve creativity, imagination, mathematical rigour, and diverse thinking. One is never surprised if a very new proof of the infinitude of primes gets proved.

There are several questions that are considered regarding the distribution of primes. The Twin prime conjecture, which asserts there are infinitely many pairs of prime numbers that differ by exactly two, such as (3, 5), (11, 13), is one of them. Another one is the Goldbach conjecture, which states that every even integer greater than 2 is the sum of two prime numbers. Both these are long standing open problems. While studying patterns in primes, several different types of primes and their patterns have been studied. A few interesting ones are Fermat's primes, Fibonacci primes, Sophie Germaine primes, and Mersenne primes.

The question about prime numbers of a certain form is also very interesting. One of the most important results in this area is Dirichlet theorem on primes. [10]. The proof of this theorem is highly non-trivial. A few cases of the theorem have been proved using elementary number theory [8].

In this paper,using the idea from a proof of the infinitude of primes given by Saidak in 2006 [6], we give different proofs of a few cases of Dirichlet's Theorem, [1], [8], [10]. In particular, we give different proofs than those availiable in literature to show that there are infinitely many primes of the form $4k + 3$ and $6k + 5$. We also give a new proof to prove the infinitude of primes of the form $4k + 1$. This proof is a combination of ideas of Polya's proof [13] of the infinitude of primes and another result in number theory (Theorem 2.11 from [8]).

2 Special cases of Dirichlet prime number theorem

In this section, we use the technique in the proof by Saidak to prove that there are infinitely many primes of the type $4k + 3, 6k + 5$.
For the sake of completeness, let us begin by defining a prime number.

Definition 1 *An integer $p > 1$ is called a prime number, or a prime, in case there is no divisor d of p satisfying $1 < d < p$. If an integer $a > 1$ is not a prime, it is called a composite number.*

Thus, 2, 3, 5, and 7 are primes, but 4, 6, and 9 are composite. 1 is considered neither a prime nor a composite.
We now state the Dirichlet prime number theorem.

Theorem 2 *Dirichlet prime number theorem states that for any two positive co-prime integers a and d, there are infinitely many primes of the form $a + nd$, where n is also a positive integer [10].*

We now consider special cases of this theorem with $n = 4, a = 3; n = 4, a = 1; n = 3, a = 2; n = 6, a = 5$.
It follows from Dirichlet's theorem that there are infinitely many primes of the form $4k+3, 4k+1, 3k+2, 6k+5$. For more elementary proofs that the primes of the type $4k + 3, 4k + 1, 3k + 2, 6k + 5$ are infinite, one can refer to [9]. These proofs that are availiable in literature use the method of contradiction.
In this section, we have used the idea of an elegant proof by Saidak [6] to give new proofs of infinitude of primes of the type $4k + 3$ and $6k + 5$.
We begin our proof by proving the following lemma.

Lemma 3 *Let n be a positive integer of the form $4k + 3$ for some $k \in \mathbb{Z}$. Then n has at least one prime factor of the form $4k + 3$.*

Proof:
If all the prime factors of n are of the form $4k+1$, then the product of all such primes will be of the form $4l+1$. Thus n will be of the form $4l+1$. This is a contradiction. Thus n has at least one prime factor of the form $4k+3$ [8].
We now prove the main theorem.

Theorem 4 *There are infinitely many primes of the form* $4k+3$.

Proof: Let n be any number of the form $4k+3$. By lemma 3, n has at least one prime factor of the form $4k+3$. Consider the numbers $n,\ n+4,\ n+8$.
All the three numbers $n,\ n+4,\ n+8$ are of the form $4k+3$ and by lemma 3 each of them has atleast one prime factor of the form $4k+3$. Note that $(n,n+4) = (4k+3,4k+7) = (4k+3,4) = 1$. Similarly, $(n,n+8) = (4k+3,4k+11) = (4k+3,8) = 1$. Also $(n+4,n+8) = (4k+7,4k+11) = (4k+7,4)$=1.
All numbers $n, n+4, n+8$ are of the form $4k+3$, and they have different prime factors. Now $n \equiv 3 \pmod 4$, $n+4 \equiv 3 \pmod 4$ and $n+8 \equiv 3 \pmod 4$. Thus $N = n(n+4)(n+8) \equiv 3^3 \equiv 3 \pmod 4$. Now each of $n, n+4, n+8$ is of the form $4k+3$ and by lemma 3, each has atleast one prime divisor of the type $4k+3$. Also any two of them are coprime. Thus $N = n(n+4)(n+8)$ has at least 3 different prime divisors of the form $4k+3$. Moreover, N is of the form $4k+3$. Now consider the numbers $N, N+4, N+8$. By a similar argument $(N,N+4) = (N+4,N+8) = (N,N+8) = 1$. So all the divisors (>1) of $N, N+4, N+8$ are different and by lemma 3 each of $N+4$ and $N+8$ also has atleast one prime factor of the form $4k+3$. Also N has atleast 3 factors of the form $4k+3$ by construction.
Thus $N_1 = N(N+4)(N+8)$ has atleast $3+1+1$ different prime factors of the form $4k+3$. Similarly, $N_2 = N_1(N_1+4)(N_1+8)$ has at least 7 different prime factors of the form $4k+3$.
We can continue this process indefinitely, where we get different primes of the form $4k+3$ each time.
Thus, there are infinitely many primes of the form $4k+3$.
On similar lines, we now consider the case of primes of the type $6k+5$.

Lemma 5 *Let n be a positive integer of the form $6k+5$ for some $k \in \mathbb{N}$. Then n has at least one prime factor of the form $6k+5$.*

Proof: Firstly, note that no prime factor of n can be of the form $6k+3, k \geq 1$ as $6k+3$ is composite for $k \geq 1$. For $k=0$, we get a prime 3. But 3 does not divide $6k+5$ for any $k \geq 0$ as $6k+5 \equiv 2 \pmod 5$. If all the prime factors of n are of the form $6k+1$, then the product of all such primes will be of the form $6l+1$. Thus n will be of the form $6l+1$. This is a contradiction. Thus n has at least one prime factor of the form $6k+5$.

Theorem 6 *There are infinitely many primes of the form* $6k+5$.

Proof: Let n be any number of the form $6k+5$. So n has at least one prime factor of the form $6k+5$. Consider the numbers $n,\ n+6,\ n+12$. Consider the numbers $n,\ n+6,\ n+12$.
All the three numbers $n,\ n+6,\ n+12$ are of the form $6k+5$ and by lemma 5 each of them has atleast one prime factor of the form $6k+5$.
The proof is similar to the proof of Theorem 4, but we prove it here for completeness.
Note that $(n, n+6) = (6k+5, 6k+11) = (6k+5, 6) = 1$.
Similarly, $(n, n+12) = (6k+5, 6k+17) = (6k+5, 12) = 1$ and
$(n+6, n+12) = (6k+11, 6k+17) = (6k+11, 6) = 1$.
All numbers $n, n+6, n+12$ are of the form $6k+5$, and they have different prime factors. Now $n \equiv 5 \pmod 6$, $n+6 \equiv 5 \pmod 6$ and $n+12 \equiv 5 \pmod 6$. Thus $N = n(n+6)(n+12) \equiv 5^3 \equiv 5 \pmod 6$. Now each of $n, n+6, n+12$ is of the form $6k+5$ and by lemma 5, each has atleast one prime factor of the type $6k+5$. Also any two of them are coprime.
Thus $N = n(n+6)(n+12)$ has at least 3 different prime divisors of the form $6k+5$. Moreover, N is of the form $6k+5$. Now consider the numbers $N, N+6, N+12$.
By a similar argument $(N, N+6) = (N+6, N+12) = (N, N+12) = 1$.
So all the divisors (> 1) of $N, N+6, N+12$ are different and by lemma 5 each of $N+6$ and $N+12$ also has atleast one prime factor of the form $6k+5$. Also N has atleast 3 factors of the form $6k+5$ by construction.
Thus $N_1 = N(N+6)(N+12)$ has atleast $3+1+1$ different prime factors of the form $6k+5$. Similarly, $N_2 = N_1(N_1+6)(N_1+12)$ has at least 7 different prime factors of the form $6k+5$.
We can continue this process indefinitely, where we get different primes of the form $6k+5$ each time.
Thus, there are infinitely many primes of the form $6k+5$.

Corollary 7 *There are infinitely many primes of the form* $3k+2$.

Proof: Infinitude of primes of the form $3k+2$ follows from Theorem 6 as every prime of the form $6k+5$ is also of the form $3k+2$.

This can also be proved considering the numbers $n = 3k+2, n+3$, and $n+6$ and arguing similar to Theorem 4 and Theorem 6.
Now we move on to an application of Fermat's numbers to prove that there are infinitely many primes of the type $4k+1$.

3 An application of Fermat's Numbers

In this section, we use the notion of a Fermat number and a lemma in elementary number theory to prove that there are infinitely many primes of the type $4k+1$.

Definition 8 *A Fermat number is a positive integer of the form* $F_n = 2^{2^n} + 1$, *where* n *is a non-negative integer.*

The first few Fermat numbers are: 3, 5, 17, 257, 65537, 4294967297
Let us only consider the case F_n where $n \geq 1$.
It has been proved that the distinct Fermat numbers F_n, F_m are coprime. i.e. $(2^{2^n} + 1, 2^{2^m} + 1) = 1$. The infinitude of Fermat numbers and the fact that any two are coprime prove that there are infinitely many primes. This proof has been attributed to Polya. [13]

This is a very useful technique. If we are able to get any set of infinitely many natural numbers, such that any two of them are coprime, then it will proved that there are infinitely many primes.
We state below a result in elementary number theory, which shall be used to prove the infinitude of primes of the type $4k+1$.

Lemma 9 *Let* p *be a prime.* $x^2 + 1 \equiv 0 (\mathrm{mod}\ p)$ *has a solution in integers if and only if* $p = 2$ *or* $p \equiv 1 (\mathrm{mod}\ 4)$. *See Theorem 2.11 from [8].*

Theorem 10 *There are infinitely many primes of the form* $4k+1$.

Proof: Consider $F_n = 2^{2^n} + 1$. For each $n \in \mathbb{N}$, $F_n - 1$ is a perfect square as $F_n - 1 = (2^{2^{n-1}})^2$. Moreover for each $n \in \mathbb{N}$, F_n is of the form $4k+1$.
Let p be a prime dividing F_n. Note that $p = 2$ is not possible as F_n is odd. Also $(2^{2^{n-1}})^2 + 1 \equiv 0 (\mathrm{mod}\ p)$. Using lemma 9, we get $p \equiv 1 (\mathrm{mod}\ 4)$.

Since Fermat numbers are infinite and any two distinct are coprime [12], we get that there are infinitely many primes of the form $4k+1$.

4 Conclusion

In this paper, we have given proofs different from those availiable in literature of the infinitude of primes of the form $4k+3, 6k+5, 4k+1$. One can try to give proof of different cases of Dirichlet's prime number theorem. One can try to get different proofs of the fact that there exist infinitely many primes $\equiv 3 \pmod 8$ or $\equiv 5 \pmod 8$ or $\equiv 7 \pmod 8$ or $\equiv 9 \pmod{10}$ or some other cases of this type. It will also be an interesting problem to show that there are infinitely many primes which are not of a certain type. For eg: Show that there are infinitely many primes not of the type $ak+b$ where $(a,b)=1$ and $k \in \mathbb{N}$.
Acknowledgment: Authors are grateful to Prof. S. A. Katre, Bhaskaracharya Pratishthana, Pune, for fruitful discussions and encouragement.

References

[1] Gueron, S., & Tessler, R. (2002). Infinitely many primes in arithmetic progressions: the cyclotomic polynomial method. The Mathematical Gazette, 86(505), 110-114. (ISSN 0025-5572)

[2] Spencer, J., & Graham, R. (2009). The elementary proof of the prime number theorem. The Mathematical Intelligencer, 31(3). Print ISSN is 0343-6993, and its Online ISSN is 1866-7414.

[3] Nath, T. (2024). Some Proofs of Infinitude of Primes. Palestine Journal of Mathematics,58-61. 13. ISSN (Online): 2219-5688
$https://pjm.ppu.edu/sites/default/files/papers/PJM_13\%28Special\%20Issue\%20II\%29_2$

[4] Murty, M. R. (2002). Prime numbers and irreducible polynomials. The American mathematical monthly, 109(5), 452-458.
DOI: 10.1080/00029890.2002.11919872

[5] Curtis, M., & Tularam, G. A. (2011). The importance of numbers and the need to study primes: The prime questions. Journal of Mathematics and Statistics, 7(4), 262-269.
DOI: 10.3844/jmssp.2011.262.269 and ISSN: 1549-3644 (Online) / 1549-3652 (Print)

[6] Saidak, F. (2006). A New Proof of Euclid's Theorem. The American Mathematical Monthly, 113(10), 937–938. https://doi.org/10.1080/00029890.2006.11920383

[7] MacHale, D. (2013). 97.40 Infinitely many proofs that there are infinitely many primes. The Mathematical Gazette, 97(540), 495-498.
DOI: 10.1017/S0025557200000255

[8] I. Niven, H. S. Zuckerman and H. L. Montgomery, "An Introduction to the Theory of Numbers," 5th Edition, John Wiley & Sons, Inc., 1991.
ISBN-10: 0-471-62546-9 and ISBN-13: 978-0-471-62546-9.

[9] Burton, D. M. (2010). Elementary Number Theory (7th ed.). McGraw-Hill Education.
ISBN-13 978-007-305188-8 and ISBN-10 0-07-305188-8

[10] Ireland, K., & Rosen, M. (1990). A Classical Introduction to Modern Number Theory (2nd ed.). Graduate Texts in Mathematics, Vol. 84. Springer-Verlag, New York.
ISBN: 978-1-4757-2103-4 (Online/eBook)

[11] Lord N, MacHale D. Infinitely many composites. The Mathematical Gazette. 2024;108(571):20-26. doi:10.1017/mag.2024.4

[12] Aigner, M., & Ziegler, G. M. (2018). Proofs from THE BOOK (6th ed.). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-57265-8

[13] G. Polya and G. Szego, Aufgaben und Lehrsatze aus der Analysis, Springer, Berlin-Heidelberg, II, 1925. [Reprint: Dover, New York, 1945]; English translation: G. P´olya and G. Szeg˝o, Problems and Theorems in Analysis II, Springer-Verlag Berlin-Heidelberg-New York, 1976.
ISBN (Springer 1976 Edition): 978-3-540-07137-2 (Berlin-Heidelberg) / 978-0-387-07137-4 (New York).

[14] Bagni, G. T. (2004). Prime numbers are infinitely many: Four proofs from history to mathematics education. Mediterranean Journal for Research in Mathematics Education, 3(1-2), 21-36. ISSN: 1450-1104.