Original Research Article

On the Infinitude of Primes of certain types

Abstract

Prime numbers and their patterns is a very important topic historically as well as in current times, considering their applications to cryptography. In this paper, we give several different elementary and elegant proofs of the infinitude of primes of the type $4k+3, 3k+2$, $6k+5$, and $4k+1$. These are all special cases of the Dirichlet prime number theorem. We have used the techniques of Saidak, Fermat, and Polya to prove the results.

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

[6], [7]. At the other end, properties of highly composite numbers have been studied in [13].

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 [5], [4]. 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 [3], [14], [15] [9]. 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. [12]. The proof of this theorem is highly non-trivial. A few cases of the theorem have been proved using elementary number theory [10].

In this paper, we use the idea from a proof of the infinitude of primes given by Saidak in 2006 [8]. We give an alternate proof of a few cases of Dirichlet's Theorem.[1], [2], [10], [12]. We also prove that the proof of the infinitude of primes of the form $4k + 1$ follows as a corollary of Polya's proof of the infinitude of primes and another result in number theory.

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 coprime integers a and d, there are infinitely many primes of the form $a + nd$, where n is also a positive integer [12].*

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 [11] [10].

In this section, we have used the idea of an elegant proof by Saidak [8] to prove the 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 $4k+3$ [10].

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 $4k+3$. So n has at least one prime factor of the form $4k+3$. Consider the numbers $n,\ n+4,\ n+8$. Note that $(n, n+4) = (4k+3, 4k+7) = (4k+3, 4) = 1$. Similarly,
$(n, n+8) = (4k+3, 4k+11) = (4k+3, 8) = 1$.
$(n+4, n+8) = (4k+7, 4k+11) = (4k+7, 4)$=1.
All numbers $n, n+4, n+8$ are of the form $4k+3$, and they have different prime factors. 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.
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 can be of the form $6k+3, k \geq 1$. 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 $n,\ n+6,\ n+12$.

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,
$(n, n+12) = (6k+5, 6k+17) = (6k+5, 12) = 1$.
$(n+6, n+12) = (6k+11, 6k+17) = (6k+11, 6)$=1.
All numbers $n, n+6, n+12$ are of the form $6k+5$, and they have different prime

factors. 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 $(N, N+6) = (N+6, N+12) = (N+6, N+12) = 1$.
So all the divisors (> 1) of $N, N+6, N+12$ are different.
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 $6k+5$.

We now prove an easy corollary of the above result.

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 $3k+2$.

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

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.

This is a very useful technique. If we are able to get any set of infinitely many natural number, any two coprime, then it will prove 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. $x^2+1 \equiv 0 \pmod{p}$ has a solution in integers if and only if $p=2$ or $p \equiv 1 \pmod{4}$.*

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.
$(2^{2^{n-1}})^2 + 1 \equiv 0 \pmod{p}$.
Using lemma 9, we get $p \equiv 1 \pmod{4}$.

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

4 Conclusion

In this paper, we have given several alternative proofs of the infinitude of primes of certain types. One can try different cases of Dirichlet's theorems on similar lines. It will also be an interesting problem to show that there are infinitely many primes which are not of a certain type.

References

[1] Gauchman, Hillel. "A special case of Dirichlet's theorem on primes in an arithmetic progression." Mathematics Magazine 74.5 (2001): 397-399.

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

[3] Spencer, J., & Graham, R. (2009). The elementary proof of the prime number theorem. The Mathematical Intelligencer, 31(3).

[4] Nath, T. (2024). Some Proofs of Infinitude of Primes. Palestine Journal of Mathematics, 13.

[5] Tikekar, V. G. (2013). There are infinitely many primes. At Right Angles, 2(3), 5-8.

[6] Murty, M. R. (2002). Prime numbers and irreducible polynomials. The American mathematical monthly, 109(5), 452-458.

[7] 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.

[8] Saidak, Filip. "A New Proof of Euclid's Theorem." The American Mathematical Monthly 113 (2006): 937 - 938.

[9] MacHale, D. (2013). 97.40 Infinitely many proofs that there are infinitely many primes. The Mathematical Gazette, 97(540), 495-498.

[10] I. Niven, H. S. Zuckerman and H. L. Montgomery, "An Introduction to the Theory of Numbers," 5th Edition, Oxford University Press, Oxford, 1991.

[11] Burton, D. M. (2010). Elementary Number Theory (7th ed.). McGraw-Hill Education.

[12] L.C. Washington, Introduction to Cyclotomic Fields, Second

Edition, Graduate Texts in Mathematics 83, Springer, New York, 1997.

[13] https://www.cambridge.org/core/journals/mathematical-gazette/article/abs/infinitely-many-composites/A522BC5767166463A1B00FECE6B68BD4

[14] https://primes.utm.edu/notes/proofs/infinite/index.html

[15] 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.