A New Proof of the Infinitude of Primes

Bibekananda Maji

Bibekananda Maji is a PhD student at Harish-Chandra Research Institute, Allahabad. He is interested in number theory.

In this article, we will discuss some interesting proofs of the infinitude of prime numbers and provide a new way to construct an infinite sequence of pairwise relatively prime natural numbers.

1. Introduction

When we start to read basic number theory, the question of infinitude of primes comes first and we start with Euclid's (300 BC) proof. Over the next twenty-three centuries, many mathematicians have provided different proofs for this beautiful result. We will state a few preliminaries which will be used later in this article.

The greatest common divisor (gcd) of two integers a and b, when at least one of them is not zero, is the largest positive integer that divides a and b. We will denote $\gcd(a, b)$ by simply (a, b). The fundamental theorem of arithmetic states that every integer greater than 1 is either prime itself or is the product of prime numbers, and that this product is unique up to the order of factors.

If a prime number p divides $a.b$, then either p divides a or p divides b. If we have n pairwise co-prime natural numbers $N_i > 1$ for $1 \leq i \leq n$, then using the fundamental theorem of arithmetic we can see that we will have at least n distinct prime numbers p_i for $1 \leq i \leq n$ such that p_i divides N_i. So if we can construct an infinite sequence of pairwise co-prime natural numbers greater than 1, it will prove the existence of an infinite number of prime numbers.

Keywords
Prime number, Fermat's number, relatively prime.

1.1 *History*

In [1–3], one can find many different proofs of this classical result. In 1730, Goldbach proved Euclid's theorem using Fermat numbers. Later in 1737 and 1762, Euler proved the infinitude of primes in two different ways. He did that on the one hand using the fundamental theorem of arithmetic and Euler's product formula and on the other hand showing the divergence of the series of the reciprocal of all prime numbers. See also the articles [4,5]. Dirichlet (1837) proved that there exist infinitely many primes in an arithmetic progression $a + nb; n \in \mathbb{N}, \gcd(a, b) = 1$, which was conjectured by Euler in 1755.

Dirichlet (1837) proved that there exist infinitely many primes in an arithmetic progression $a + nb$; $n \in \mathbb{N}$, $\gcd(a,b) = 1$, which was conjectured by Euler in 1755.

Fürstenberg [6] gave an interesting proof using topology. In 1980, Washington proved the same using commutative algebra [2]. Recently, Saidak [7] gave an easy proof which has been inspired from Euclid and Goldbach's idea. Pinasco in 2009 [8] has proved Euclid's theorem using inclusion–exclusion principle and Whang 2010 [9] gave a proof using De Polignac's formula. Again in 2010, Lokenath Debnath [10] gave a new proof using the irrationality of π and several other mathematicians have also proved the infinitude of primes in many different ways. So, the story of infinitude of primes that was started in 300 BC by Euclid still goes on.

In the next two sections we discuss some known proofs of Euclid's result and we construct a new sequence of pairwise co-prime numbers, which is inspired from the idea of Euclid, Goldbach and Saidak. Finally, we will give one more construction based on generalized Fermat numbers.

2. Brief Idea of Some Known Proofs

We begin by discussing some classical proofs which will be the basic building block for our new proof.

Euclid.
(See *Resonance,* Vol.12, No.4, 2007.)

Christian Goldbach

2.1 *Euclid's Proof* (300 BC)

Suppose there exist only finitely many primes $p_1, p_2, \ldots, p_n$. Then, consider the number $N = p_1 p_2 \cdots p_n + 1$. Clearly, N is bigger than all the p_i. If N is prime, then we get a new prime which is larger than all the p_i. Again if N is composite, then N has a prime divisor p (say) but p is not one of the p_i. Because if $p = p_i$ for some i, then p will divide 1 as p divides N, which is impossible. So a finite set $\{p_1, p_2, \ldots, p_n\}$ cannot be the collection of all prime numbers. □

2.2 *Goldbach's Proof* (1730)

Goldbach's clever proof uses the Fermat numbers (written in a letter to Euler, July 1730), which are defined as $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, 3, \ldots$. We will show that any two distinct Fermat numbers are relatively prime. Using the induction hypothesis, we can show that

$$F_n - \prod_{i=0}^{n-1} F_i = 2 \quad (n \geq 1).$$

Let d be a divisor of two distinct Fermat numbers F_m and F_n. Then d divides 2, and hence, $d = 1$ or 2. But $d = 2$ is not possible since all Fermat numbers are odd. Therefore, $d = 1$. Hence, any two distinct Fermat numbers are co-prime. Thus, prime divisors of distinct Fermat numbers will be distinct and as there are infinitely many Fermat numbers, infinitely many distinct prime numbers will exist. □

2.3 *Saidak's Proof* (2005) [7]

Let $n > 1$ be a positive integer and $N_1 = n, N_2 = n + 1$. Then obviously $(N_1, N_2) = 1$, so the number $N_1 N_2$ must have at least two different prime factors. Similarly, since the integers $N_1 N_2$ and $N_1 N_2 + 1$ are co-prime and hence, the number $N_1 N_2 (N_1 N_2 + 1)$ must have at least 3 different prime factors. We continue this process to get infinitely many primes. □

Any two distinct Fermat numbers are coprime.

It is clear that Saidak's argument has been inspired from Goldbach's idea of constructing pairwise co-prime sequences and Euclid's idea of constructing new prime from a set of primes. Suppose we have one prime p_1, then any prime divisor p_2 of $n_2 = p_1 + 1$ will be a new prime number different from p_1. Again, any divisor p_3 of $n_3 = p_1.p_2 + 1$ will be one more new prime and we can continue this process infinitely many times. We call this sequence of numbers as Euclid's sequence.

3. A Construction

We start with one lemma and then using this lemma we will construct a new sequence of pairwise co-prime numbers. After that, we will compare Saidak's sequence with that of ours in the form of a table.

Lemma 0.1. *Given any n-pairwise co-prime natural numbers N_i for $1 \leq i \leq n$, one can construct a natural number N such that $(N, N_i) = 1$ for all $i = 1, 2, \ldots, n$.*

Proof. It is given that $(N_i, N_j) = 1$ for $i \neq j$. Let $S = \{N_1, N_2, \ldots, N_n\}$ be the set of all the given n numbers. Let A and B be two disjoint subsets (non-empty) of S such that $A \bigcup B = S$. Now we consider the number

$$N = {N_{i_1}}^{\alpha_1} {N_{i_2}}^{\alpha_2} \cdots {N_{i_r}}^{\alpha_r} + {N_{i_{r+1}}}^{\alpha_{r+1}} \cdots {N_{i_n}}^{\alpha_n},$$

where $A = \{N_{i_1}, N_{i_2}, \ldots, N_{i_r}\}$, $B = \{N_{i_{r+1}}, \ldots, N_{i_n}\}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ are any natural numbers. Let $d_i = (N, N_i)$ for $i = 1, 2, \ldots, n$. Thus, d_i divides both N and N_i. Now by our construction, either $N_i \in A$ or, $N_i \in B$, but not in both. Suppose $N_i \in A$, then d_i will divide the first term of N. Again as $d_i | N$ so, d_i divides second term of N. Therefore, d_i will divide one of N_{i_l}, where $l \in \{r+1, \ldots, n\}$. But as $(N_i, N_j) = 1$ for $i \neq j$ so, $d_i = 1$. Hence we are done. □

Now, we will construct a sequence of pairwise co-prime numbers using the above lemma. At first let us consider

$N_1 = n^\alpha$ and $N_2 = (n+1)^\beta$ for any $\alpha, \beta \in \mathbb{N}$, then clearly $(N_1, N_2) = 1$.

Define $N_3 = N_1^{\alpha_1} + N_2^{\alpha_2}$ for any $\alpha_1, \alpha_2 \in \mathbb{N}$. Then by the above lemma, 0.1,

$$(N_3, N_i) = 1 \text{ for } i = 1, 2.$$

Now we have three numbers $N_1, N_2,$ and N_3, which are pairwise co-prime. Next we have to construct N_4. We can take N_4 to be $N_1^{\beta_1} N_2^{\beta_2} + N_3^{\beta_3}$ or, $N_1^{\beta_1} N_3^{\beta_3} + N_2^{\beta_2}$ or, $N_1^{\beta_1} N_3^{\beta_3} + N_2^{\beta_2}$ for any $\beta_1, \beta_2, \beta_3 \in \mathbb{N}$. Suppose we choose $N_4 = N_1^{\beta_1} N_2^{\beta_2} + N_3^{\beta_3}$, then by lemma 0.1,

$$(N_4, N_1) = (N_4, N_2) = (N_4, N_3) = 1.$$

Therefore, we have four numbers $N_1, N_2, N_3,$ and N_4 which are pairwise co-prime. Note that there are many ways to construct N_i as by lemma 0.1 but we can continue with any one of them the process of constructing new terms like as

$$N_i = N_1^{\gamma_1} N_2^{\gamma_2} \cdots N_{i-2}^{\gamma_{i-2}} + N_{i-1}^{\gamma_{i-1}} \text{ for } i \geq 5,$$

where γ_i is any natural numbers. We will then get a infinite sequence of pairwise co-prime positive integers and that will prove our aim. □

3.1 *Few Terms from Saidak's and Our Sequence*

In Saidak's sequence, $N_1 = n, N_2 = n+1, N_3 = N_1 N_2 + 1, \ldots, N_i = N_1 N_2 \ldots N_{i-1} + 1, \ldots$. See *Table* 1.

Table 1.

n	N_1	N_2	N_3	N_4	N_5	N_6	N_7	..
1	1	2	3	7	43	1807 =13*139	3263443	.. ..
2	2	3	7	43	1807 =13*139	3263443	10650053687365 =5*149*14295374077	..
3	3	4	13	157	24493 =7*3499	599882556 = 67*277*32323	359859080993093137 =482379281*7460085777	..
4	4	5	21 =3*7	421	176821 =151*1171	31265489221 349*89585929	977530816197201697621 =73*330721*40489817999437	..

n	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	....
1	1	2	3	5	11	41	371 =7*53	13901	.. ..
2	2	3	5	11	41	371 =7*53	13901	5033531	....
3	3	4	7	19	103	1699	166087 =307*541	279461299 13*21499703	....
4	4	5	9	29	209 =11*19	5429 = 61*89	1096409 = 617*1777	5924026829 =7*6299*134353	....

Table 2.

Let us take our sequence as follows: consider all the $\alpha_i, \beta_i, \gamma_i$ are equal to 1 and $N_1 = n, N_2 = n+1, N_3 = N_1 + N_2, N_4 = N_1N_2 + N_3, \ldots, N_i = N_1N_2 \ldots N_{i-2} + N_{i-1}, \ldots$. See *Table* 2.

It is clear from the above table that our construction is different from that of Saidak's one.

Remark 0.1. *It is not known whether there exist infinitely many primes in the sequence of Fermat numbers*[1]. *Similarly, we can ask whether there exist infinitely many primes in Euclid's sequence, Saidak's sequence and as well as in our sequence.* See [5] where many such questions are raised.

[1] Fermat introduced Fermat Numbers $F_n = 2^{2^n} + 1$ and he conjectured that all F_n are prime, which was refuted by Euler as $F_5 = 2^{2^5} + 1 = 641 \times 6700417$.

4. Using Generalized Fermat's Number

Ribenboim [2] defines a generalized Fermat number as $F_a^n = a^{2^n} + 1$, where $a \geq 2$ is a positive integer. By induction hypothesis we can easily show that,

$$F_a^n - 2 = \prod_{i=0}^{n-1} (a-1)F_a^i, \quad \text{for all}\, n \in \mathbb{N}.$$

If we choose a as an even integer, then using the same argument as that of Goldbach, we can show that the sequence of generalized Fermat numbers are pairwise relatively prime integers.

Again Riesel [11] further generalized Fermat numbers as,

$$F_{a,b}^n = a^{2^n} + b^{2^n},$$

Pierre de Fermat
(See *Resonance*, Vol.1, No.1, 1996.)

where a and b are two positive integers. Similarly, we can construct a sequence of pairwise co-prime numbers as follows: we choose a and b as even and odd integers respectively with $(a, b) = 1$. Using induction hypothesis we can show that,

$$a^{2^n} - b^{2^n} = (a - b).\prod_{i=0}^{n-1} F_{a,b}^i \quad \text{for all}\, n \in \mathbb{N}\ ,$$

Let $n > m$ and $d = (F_{a,b}^n, F_{a,b}^m)$. Then d divides both $a^{2^n} + b^{2^n}$ and $a^{2^m} + b^{2^m}$. As $n > m$, we can see that $F_{a,b}^m$ will be in the right-hand side of the above expression.

Therefore, d will divide $a^{2^n} - b^{2^n}$. Hence, d divides $2a^{2^n}$ as well as $2b^{2^n}$. But $d = 2$ is not possible since $F_{a,b}^n$ is always odd when one of a or b is even and the other is odd. So, d divides both a^{2^n} and b^{2^n}. If p is any prime dividing d, then clearly p will divide a and b. This implies that p divides 1 as $(a, b) = 1$, which is not possible. Therefore $d = 1$. Hence, generalized Fermat numbers are pairwise co-prime, which again proves that there are infinitely many primes. Now, if we change a and b, we will get different sequences of pairwise co-prime numbers.

Maybe that's why it is said that 'there are infinitely many proofs for the infinitude of primes'.

5. Acknowledgements

I would like to thank Kalyan Chakraborty for various useful discussions and Joseph Oesterlé for going through the manuscript and giving some useful suggestions and comments. I also wish to thank the referee for correcting some errors and typos.

Suggested Reading

[1] **M Aigner and G M Ziegler, Proofs from *The Book*, Springer-Verlag, Berlin, 1999.**

[2] **P Ribenboim, *The Little Book of Bigger Primes*, Springer-Verlag, New York, 1996.**

[3] R Meštrovic, Euclid' theorem on the infinitude of primes: a historical survey of its proofs and its new proof, preprint arXiv.org, 2012.

[4] Shailesh A Shirali, On the infinitude of the prime numbers: Euler's proof, *Resonance,* Vol.1, No.3, 1996.

[5] B Sury, The Prime ordeal, *Resonance,* Vol.13, No.9, 2008.

[6] H Fürstenberg, On the infinitude of primes, *Amer. Math. Monthly*, Vol.62, p.353, 1995.

[7] Filip Saidak, A new proof of Euclid's theorem, *Amer. Math. Monthly*, Vol. 113, No.10, pp.937—938, 2006.

[8] Juan Pablo Pinasco, New proofs of Euclid's and Euler's theorems, *Amer. Math. Monthly*, Vol. 116, No.2, pp.172—173, 2009.

[9] Junho Peter Whang, Another proof of the infinitude of the prime numbers, *Amer. Math. Monthly*, Vol.117, No.2, p.181, 2010.

[10] Debnath, Lokenath, *The Legacy of Leonhard Euler: A Tricentential Tribute*, World Scientific, 2010.

[11] H Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed. Boston, MA, Birkhäuser 1994.

Address for Correspondence
Bibekananda Maji
Harish-Chandra Research Institute
Chhatnag Road
Jhunsi, Allahabad 211019.
Email: bibekmaji@hri.res.in