Palestine Journal of Mathematics

Vol 13(Special Issue II)(2024) , 58–61

Some Proofs of Infinitude of Primes

Triloki Nath

Communicated by Mohammad Ashraf

MSC 2020 Classification: Primary 11A41 ; Secondary 11A07

Keywords and phrases: Primes; Euler's totient function; congruence.

Acknowledgement: The author is indebted to the anonymous referee for his helpful suggestions and comments, which significantly improved the presentation of the paper.

Abstract We offer some new proofs of the infinitude of primes using Euler's totient function. Our proofs are simpler than the existing ones based on the totient function. We also discuss topological proof of Furstenberg.

1 Introduction

By numbers, we mean natural numbers. Prime number is a number that has exactly two distinct divisors. Hence the number "1" having just one divisor, is excluded from the list of prime numbers. By Fundamental Theorem of Arithmetic (FTA) every number > 1 is a product of primes. In other words, 1 is the only number that is not a multiple of primes. Equivalently, taking n distinct primes: $p_1, p_2, ..., p_n$, the number $p_1p_2...p_n + 1$ must be divisible by a prime other than $p_1, \ldots, p_n$. Thus, the fact that 1 is the only non-multiple of primes works behind Euclid's argument. The classical proof of infinitude of primes by Euclid will remain eternally outstanding for all time in Mathematics.

Theorem. *There are infinitely many primes.*

The first proof of the above result is due to Euclid for around 300 B.C. After that generations of mathematicians proved the infinitude of primes in strikingly different ways and new proofs are still coming up, see, for example, [2] and references therein. We found two such proofs using Euler's totient function.

We recall that $\phi(n)$ is the number of positive integers not exceeding n and that are relatively prime to n.
Let $n = p_1^{\alpha_1}p_2^{\alpha_2}....p_k^{\alpha_k}$ be the prime factorization of n with distinct primes $p_1, p_2, ..., p_k$ and all the α_i's are positive integers. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right) = n\prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right).$$

2 New Proofs

In this section, we give three proofs of the infinitude of primes, the first two of them are based on Euler's totient and the third one uses divisibility property of numbers. We refer, for example, [3] for existing proof of infinitude of primes using Euler's totient function.

Proof. 1. Suppose on the contrary that there are only m distinct primes , say, $p_1, p_2, ..., p_m$. Let $P = p_1 \cdot p_2 \cdot ... \cdot p_m$, then by FTA we can write $P+1 = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot ... \cdot q_l^{\beta_l}$ where $q_1, q_2, ..., q_l$ are l distinct primes among $p_1, p_2, ..., p_m$, and all the β_i's are positive integers. Let $Q = \prod_{j=1}^{l}\left(1 - \frac{1}{q_j}\right)$, then $0 < Q < 1$. We have

$$\phi(P + 1) = (P + 1)Q = PQ + Q.$$

Since PQ is an integer, $PQ + Q$ is not an integer. Hence, $\phi(P + 1)$ is not an integer. This contradiction proves that there are infinitely many primes. □

Proof. 2. Suppose on the contrary that $p_1, p_2, ..., p_m$ are the only distinct primes. Let $P = p_1 \cdot p_2 \cdot ... \cdot p_m$, then $P(P + 1)$ contains all the prime factors. Since P and $P + 1$ are relatively prime, We have

$$\phi(P)\,\phi(P+1) = \phi(P(P+1)) = P(P+1)\prod_{j=1}^{m}\left(1-\frac{1}{p_j}\right) = (P+1)\phi(P).$$

It follows that $\phi(P + 1) = P + 1$ whereby $P = 0$, which is a contradiction. Hence, there must be an infinity of primes. □

Proof. 3. Consider m distinct primes, say, $p_1, p_2, ..., p_m$. Since $p_i \nmid (p_1 \cdot p_2 ..... \cdot p_k + p_{k+1} ... \cdot p_m)$ for all $i = 1, \ldots, m$, it follows that there are infinitely many primes. □

3 Furstenberg's Proof of Infinitude of Primes

Now comes Furstenberg's topological proof [4]. A variant of Furstenberg's proof that avoids topological language, is due to Mercer [6], which points out the real reason behind Furstenberg's topological argument. In this paper, we show that the approaches [4, 6] stem from FTA and the very conception of primes. Our details are more streamlined than [6].

Definition 3.1. Let m and r be the integers with $m \neq 0$. The set $S(r, m)$ is defined as

$$S(r, m) = \{mx + r | x \in \mathbb{Z}\} = r + m\mathbb{Z}$$

is called an Arithmetic Progression (AP).

It may be noted that for $m \geqslant 2$, the set of integers that are not multiples of m is

$$(1 + m\mathbb{Z}) \cup (2 + m\mathbb{Z}) \cup .... \cup ((m - 1) + m\mathbb{Z}).$$

The following Lemma characterizes the situation when two APs $S(r_1, m_1)$ and $S(r_2, m_2)$ will be disjoint.

Lemma 3.2. *The pair of linear congruences*

$$\begin{aligned} x &\equiv r_1 (mod\ m_1) \\ x &\equiv r_2 (mod\ m_2) \end{aligned}$$

has a simultaneous solution if and only if $d = g.c.d(m_1 + m_2, m_1 m_2)$ *divides* $(m_1 r_2 + m_2 r_1)$. *Furthermore, if a solution exists, then there are exactly* d *incongruent solutions modulo* $m_1 m_2$.

Proof. Suppose that the pair of linear congruences

$$\begin{aligned} x &\equiv r_1 (\text{mod } m_1) \\ x &\equiv r_2 (\text{mod } m_2) \end{aligned}$$

has a simultaneous solution x. Then there are integers k_1, k_2 such that

$$\begin{aligned} x - r_1 &= m_1 k_1 \\ x - r_2 &= m_2 k_2 \end{aligned}$$

combining the above equations, we have

$$(m_1 + m_2)x - (m_2 r_1 + m_1 r_2) = m_1 m_2 (k_1 + k_2)$$

that is

$$(m_1 + m_2)x \equiv (m_2 r_1 + m_1 r_2) (\text{mod } m_1 m_2) \tag{3.1}$$

We know that the congruence

$$ax \equiv b(\text{mod } n)$$

has a solution if and only if $d = g.c.d(a, n)$ divides b. Moreover, if $x_\circ$ is any solution, then

$$x_\circ, x_\circ + \frac{n}{d}, x_\circ + 2\frac{n}{d}, ..., x_\circ + (d-1)\frac{n}{d}$$

are exactly d incongruent solutions.

Hence, congruence (3.1) has a solution if and only if $d = g.c.d(m_1 + m_2, m_1 m_2)$ divides $(m_1 r_2 + m_2 r_1)$. Furthermore, if a solution exists, say $\bar{x}$, then there are exactly d incongruent solutions modulo $m_1 m_2$, namely,

$$\bar{x}, \bar{x} + \frac{m_1 m_2}{d}, \bar{x} + 2\frac{m_1 m_2}{d}, ..., \bar{x} + (d-1)\frac{m_1 m_2}{d}.$$

This completes the proof of Lemma. □

Lemma 3.3. *The intersection of two APs (hence, finitely many) is either empty or infinite and again an AP.*

Proof. We first note that $x \in S(r, m) \Leftrightarrow S(r, m) = S(x, m)$. If $x \in S(r_1, m_1) \cap S(r_2, m_2)$, then $S(r_1, m_1) \cap S(r_2, m_2) = S(x, m_1) \cap S(x, m_2) = S(x, m_1 m_2)$. Thus, a finite intersection of APs is either empty (in view of Lemma 3.2) or an infinite set and again an AP. □

Fact (A): A finite intersection of a finite union of sets is a finite union of finite intersection of the sets (since intersection distributes over union).
For example,

$$\begin{aligned}
(A_1 \cup A_2) \cap (B_1 \cup B_2 \cup B_3) \cap (C_1 \cup C_2) &= ((A_1 \cup A_2) \cap (B_1 \cup B_2 \cup B_3) \cap C_1) \\
&\cup ((A_1 \cup A_2) \cap (B_1 \cup B_2 \cup B_3) \cap C_2) \\
&= ((A_1 \cap B_1 \cap C_1) \cup (A_1 \cap B_1 \cap C_2) \cup (A_1 \cap B_2 \cap C_1) \\
&\cup \cup (A_1 \cap B_2 \cap C_2) \cup (A_1 \cap B_3 \cap C_1) \cup (A_1 \cap B_3 \cap C_2) \\
&\cup (A_2 \cap B_1 \cap C_1) \cup (A_2 \cap B_1 \cap C_2) \cup (A_2 \cap B_2 \cap C_1) \\
&\cup (A_2 \cap B_2 \cap C_2) \cup (A_2 \cap B_3 \cap C_1) \cup (A_2 \cap B_3 \cap C_2).
\end{aligned}$$

As in [4], it is concluded that

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \text{ prime}} p\mathbb{Z}. \tag{3.2}$$

Equivalently, as in [6]

$$\begin{aligned}
\{-1, 1\} &= \bigcap_{p \text{ prime}} \Big(\mathbb{Z} \setminus p\mathbb{Z}\Big) \\
&= \bigcap_{p \text{ prime}} \Big(\bigcup_{r=1}^{p-1} (r + p\mathbb{Z})\Big) \\
&= \bigcap_{p \text{ prime}} \Big(\bigcup_{r=1}^{p-1} S(r, p)\Big)
\end{aligned} \tag{3.3}$$

In the above arguments, it is conceived that -1 and 1 are the only integers that are not multiples of primes. Hence, (3.2) or equivalently (3.3) is well justified. Which forces that for a finite number of primes $p_1, p_2, ..., p_n$, the integers $p_1 p_2 ... p_n \pm 1$ must be a multiple of some prime. Hence, there is a prime other than these $p_i's$. This is Euclid's argument of the infinitude of primes.

If the set of primes is finite, then (3.2) or equivalently (3.3), invoking the Fact (A), cannot hold. Hence, Furstenberg's approach and its variant [6] implicitly use Euclid's argument relying on FTA.

Finally, it is worth mentioning that almost all the known proofs are some variants of Euclid's argument, nevertheless, the beauty of the infinitude of primes always attracts researchers and invites new proofs.

References

[1] M. Aigner, G. Ziegler, *Proofs from the Book*, fourth edition. Springer-Verlag, New York, 2009.

[2] B. Maji, A new proof of Infinitude of primes, *Resonance.* 20(12);1128-1135, 2015.

[3] D. Burton, *Elementary Number Theory*,Tata McGraw-Hill, 2007.

[4] H. Furstenberg, On the Infinitude of Primes, Amer. Math. Monthly 62; 353,1955.

[5] R. Lovas, I. Mezo, Some observations on the Furstenberg topological space, Elemente der Mathematik. 70 (3); 103-116, 2015.

[6] Idris D. Mercer, On Furstenberg's Proof of the Infinitude of Primes, American Mathematical Monthly. 116 (4); 355-356, 2009.

[7] K. Conrad, The Topological Proof of the Infinitude of Primes, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/primestopology.pdf

Author information

Triloki Nath, Department of Mathematics and Statistics, School of Mathematical and Physical Sciences, Dr. Harisingh Gour University, Sagar, Madhya Pradesh-470003, India.
Current Affiliation: Department of Mathematics and Statistics, DDU Gorakhpur University, Gorakhpur, UP-273009, India.
E-mail: tnverma07@gmail.com