Journal of Scientific Research & Reports
10(3): 1-7, 2016; Article no.JSRR.24470
ISSN: 2320-0227

SCIENCEDOMAIN *international*
www.sciencedomain.org

Other Demostrative Perspective of How to See Dirichlet's Theorem

José William Porras Ferreira[1*] and Willian de Jesus Caballero Guardo[1]

[1]*Escuela Naval de Cadetes, Colombian Naval Academy, Cartagena, Colombia.*

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JSRR/2016/24470
Editor(s):
(1) Naseer Shahzad, Department of Mathematics, King Abdulaziz University, Saudi Arabia.
Reviewers:
(1) Anonymous, University Politehnica of Bucharest, Romania.
(2) Hammad Khalil, University of Malakand, Pakistan.
(3) Krasimir Yordzhev, South-West University, Bulgaria.
(4) Fethi Soltani, Higher College of Technology and Informatics, Tunis, Tunisia.
Complete Peer review History: http://sciencedomain.org/review-history/13546

Original Research Article

Received 22[nd] January 2016
Accepted 22[nd] February 2016
Published 3[rd] March 2016

ABSTRACT

The Dirichlet's theorem (1837), initially guessed by Gauss, is a result of analytic number theory. Dirichlet, demonstrated that:

For any two positive coprime integers a and b, there are infinite primes of the form $a + bn$, where n is a non-negative integer ($n = 1, 2, \ldots$). In other words, there are infinite primes which are congruent to $a \bmod \mathrm{b}$. The numbers of the form $a + bn$ is an arithmetic progression.

Actually, Dirichlet checks a result somewhat more interesting than the previous claim, since he demonstrated that:

$$\sum_{p=a \bmod b} \frac{\ln p}{p} \to \infty$$

Which implies that there are infinite primes, $p \equiv a \bmod b$.

The proof of the theorem uses the properties of certain Dirichlet L-functions and some results on arithmetic of complex numbers, and it is sufficiently complex that some texts about numbers theory excluded it. Here is a simple proof by *reductio ad absurdum* which does not require extensive mathematical knowledge.

**Corresponding author: E-mail: jwporrasf45@gmail.com, jwporras@balzola.org;*

Keywords: Prime theorem; fundamental theorem of arithmetic; Dirichlet's theorem; reductio ad absurdum.

1. INTRODUCTION

Johann Peter Gustav Lejeune Dirichlet (1805-1859), German mathematician to who is credited to the modern formal definition of a function. He was educated in Germany and then in France, where he learned from many of the most renowned mathematicians of the time. Conditions were infinitely better in France than in Germany, given that scientific eminence as P-S. Laplace (1749-1827), A. M. Legendre (1752-1833), Fourier (1768-1830), S-D. Poisson (1781-1840) and Augustin Louis Cauchy (1789-1857), were active in Paris, so that he had the chance to interact with some as Fourier. Their methods provided a completely new perspective and its results are among the most important in mathematics. Today, his techniques are more booming than never [1]. Their contributions were mainly in the area of mathematical analysis, theory of groups, infinite series, differential equations, determinants, probability and mathematical physics.

The theorem known as the Direchlet's theorem, was really guessed by Gauss (1777-1855), but it was Dirichlet who finally achieved his demonstration in 1837, [2].

Dirichlet's theorem:

> *For any two positive coprime integers a and b, there are infinitely many primes of the form $a+bn$, where n is a non-negative integer* ($n = 1, 2, ...$).

Dirichlet proved this theorem using Dirichlet series, but the test is so complex that the classical texts of number theory excludes it, for example, Hardy & Wright [3] say: "this theorem is too difficult for insertion in this book".

In order not to make this article very extensive we include a short proof of Dirichlet theorem, eliminating some corollaries marked as **[Cor]**. The full demonstration is in [4,5].

After that, it comes a simple proof of the theorem, using the fundamental theorem of arithmetic which simplifies their understanding and aplications.

2. SHORT PROOF OF DIRICHLET'S THEOREM [6]

2.1 Definitions

1. One Dirichlet **L-función** [7,8] is a function of the form:

   $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$

   Where $s \in \mathbb{C}$ and χ are Dirichlet characters.

2. Let G a finite commutative group[1] of order h and element unit e.
3. A character on G is a function:

$\chi \in \mathbb{C} \;/\; \chi \neq 0,\ \chi\,(u \cdot v) = \chi(u) \cdot \chi(v)\ \forall u, v \in G$

2.2 Properties [9,10]

There are several important properties of a character on G:

1. It is called a main character of commutative Group G the function χ_0 such that $\chi_0(u) = 1$ for all $u \in \boldsymbol{G}$. The main character makes as element unit in the group of characters.
2. Since both the inverse of a character on G and the product of two characters on G is also a character on G, the set of characters on G forms a commutative group with multiplication.
3. As $\chi(e) = 1$ and given that the order of an element divides the order of the group, then $\forall u \in \boldsymbol{G}\ \left(\chi(u)\right)^h = \chi(u^h) = \chi(e) = 1$, what means then $|\chi(u)| = 1$.
4. Since the number of roots of the unit element of order h is as max h, the number of characters c is finite, the h^h value being an upper bound for c.

On the other hand, $\forall u \in \boldsymbol{G},\ u \neq e$ there is a character, $\chi \;/\; \chi(u) \neq 1$ (**[Cor]**). For this reason, and if it is represented by $\sum_G a_\chi$ the sum of the value a_χ associated with each of the different characters of the group $\boldsymbol{G}$, there are other properties (**[Cor]**):

[1] *Although this topic talks about groups in general, those, who are not familiar with the theory of groups, will be limited to identifying the Group G with reduced residual class sets: $G = Z_q^*$*

2.3 Other Properties

1. $\forall u \in G$, we have that: $\sum_G \chi(u) = \begin{cases} c & \text{if } u = e \\ 0 & \text{if } u \neq e \end{cases}$ where $c = \sum_G 1$

2. $\forall u \in G$, we have that: $\sum_{u \in G} \chi(u) = \begin{cases} h & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0 \end{cases}$
   Where h is the order of *G* where $c = h$

3. $\forall u, v \in G$, we have that : $\frac{1}{h} \sum_\chi \frac{\chi(u)}{\chi(v)} = \begin{cases} 1 & \text{if } u = v \\ 0 & \text{if } u \neq v \end{cases}$

4. $\forall \chi_1, \chi_2 \in G$, we have that: $\frac{1}{h} \sum_{u \in G} \frac{\chi_1(u)}{\chi_2(u)} = \begin{cases} 1 & \text{if } \chi_1 = \chi_2 \\ 0 & \text{if } \chi_1 \neq \chi_2 \end{cases}$

2.4 Proof of the Theorem Made by Dirichlet

With these definitions and characteristics of the group *G*, Dirichlet proceeded with his demonstration:

1. Given a $q \in \mathbb{N}$ the χ characters of the group $G = Z_q^*$ are defined as congruence classes module q of coprime numbers with q.
2. The *G* group has $\phi(q)$ elements, and they can be represented by $G = [a_1, a_2, \dots, a_{\phi(q)}]$, where the different a_i are representatives of the congruence classes that satisfy the condition $0 < a_j < q$, and in this context Dirichlet defined the extended functions of the χ characters of *G* in the following way:

   $$\chi(n) = \begin{cases} \chi(a_i) & \text{if n} \equiv a_i \bmod q \\ 0 & \text{if} \gcd(n, q) > 1 \end{cases}$$

   Note: These functions are called Dirichlet characters module q and they are completely multiplicative. There are $\phi(q)$ functions and one of them is called main character of Dirichlet:

   $$\chi_0(n) = \begin{cases} \chi(a_i) & \text{if n} \equiv a_i \bmod q \\ 0 & \text{if} \gcd(n, q) > 1 \end{cases}$$

   These characters have some significant properties (derived from the sections 2.2 and 2.3):

   a. $\sum_{n \bmod q} \chi(n) = \begin{cases} \phi(q) & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0 \end{cases}$
   b. $\sum_{n \bmod q} \chi(u) = \begin{cases} \phi(q) & \text{if } u \equiv 1 \bmod q \\ 0 & \text{if } u \not\equiv 1 \bmod q \end{cases}$
   c. $\forall a \in \mathbb{N} \ \ \gcd(a, q) = 1$ It should be:

   $$\sum_{n \bmod q} \frac{\chi(u)}{\chi(a)} = \begin{cases} \phi(q) & \text{if } u = a \\ 0 & \text{if } u \neq a \end{cases}$$

3. In the Dirichlet L-function, $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ the χ values are periodic, implying that the $L(s, \chi)$ series converges absolutely to $\Re(s) > 1$ and uniformly to $\Re(s) > 1 + \varepsilon_1$, $\forall \varepsilon > 0$. In addition, the coefficients are completely multiplicative, the series supports the following expression when $\Re(s) > 1$, within p primes:

   $$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

4. The Dirichlet L-funtion has the following properties (**[Cor]**):

   a. $L(s,\chi) \neq 0$
   b. $L(s,\chi_0) = \zeta(s) \cdot \prod_{p|q}\left(1-\frac{1}{p^s}\right)$, where $\zeta(s)$ is the Euler Zeta function and Riemann (1826-1866) [11], extended it to the complex plane in its demonstration of the prime numbers less or equal to a n number[2].
   c. $\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n=1}^{\infty}\frac{\chi(n)\Lambda(n)}{n^s}$
   d. $\ln(L(s,\chi)) = \sum_p \sum_{m=1}^{\infty}\frac{1}{m}\frac{(\chi(p))^m}{p^{m\cdot s}}$

5. From point 4b equality and the properties of the ζ function is deduced that the $L(s,\chi_0)$ function is analytic in the complex semi plane $\Re(s) > 0$ with the exception of one pole in $s = 1$, whose residue is $\prod_{p|q}\left(1-\frac{1}{p^s}\right) = \frac{\phi(q)}{q}$.

   As a result, it can be said that $L(s,\chi_0) = f(s) + \frac{\phi(q)/q}{s-1}$ where f is analytical and does not have singularities in $\Re(s) > 0$, then the function:

$$\frac{L'(s,\chi)}{L(s,\chi)} = \frac{f'(s) - \frac{\phi(q)/q}{(s-1)^2}}{f(s) + \frac{\phi(q)/q}{s-1}} = \frac{(s-1)^2 f'(s) - \phi(q)/q}{\big((s-1)f(s) - \phi(q)/q\big)(s-1)}$$

   Also, it has a pole in $s = 1$ with residue: -1.

6. All Dirichlet L-function $L(s,\chi)$ with $\chi \neq \chi_0$ is analytical and does not have singularities in the area $\Re(s) > 0$ **[Cor]**.

7. For $k > 0$, we have that (**[Cor]**):

$$\sum_{p=a \bmod q}\frac{\ln(p)}{p^k} = \sum_{n=a \bmod q}\frac{\Lambda(n)}{n^k} - O(1)$$
$$= \frac{-1}{\phi(q)}\cdot\frac{L'(k,\chi_0)}{L(k,\chi_0)} - \frac{1}{\phi(q)\chi(a)}\sum_{\substack{x \bmod q\\ x\neq x_0}}\frac{L'(k,\chi)}{L(k,\chi)} - O(1)$$

   This expression is the key for the demonstration and Dirichlet showed that the theorem is true if the first term of the second member diverges when the remaining terms remain within some limits.

8. Because is fulfilled that $L(1,\chi) \neq 0$ when $\chi \neq \chi_0$ the following equation:

$$\lim_{k\to 1}\frac{1}{\phi(q)\chi(a)}\sum_{\substack{x \bmod q\\ x\neq x_0}}\frac{L'(k,\chi)}{L(k,\chi)} = \frac{1}{\phi(q)\chi(1)}\sum_{\substack{x \bmod q\\ x\neq x_0}}\frac{L'(1,\chi)}{L(1,\chi)} = O(2)$$

   Gets a finite value, and $\frac{1}{\chi_0(a)}\cdot\frac{L'(k,\chi_0)}{L(k,\chi_0)} = \frac{L'(k,\chi_0)}{L(k,\chi_0)}$ has a pole in $s = 1$ with residue -1, then it satisfied that:

$$\lim_{k\to 1^+}\frac{L'(k,\chi_0)}{L(k,\chi_0)} = -\infty$$

[2] *The zeta function is defined for $s \in \mathbb{C}$ s by* $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p (1-p^{-s})^{-1}$.

Which implies that:

$$\sum_{p=a \bmod q} \frac{\ln(p)}{p} = \lim_{k\to 1^+} \sum_{p=a \bmod q} \frac{\ln(p)}{p^k} = \frac{-1}{\phi(q)}\left(\lim_{k\to 1^+} \frac{L'(k,\chi_0)}{L(k,\chi_0)} + O(2)\right) + O(1) = \infty$$

Thus, concluding the proof of Dirichlet's theorem.

3. NEW DEMONSTRATIVE PERSPECTIVE OF DIRICHLET'S THEOREM

3.1 Definitions

Definition 1. An integer $p > 1$ is a prime if only its divisors are 1 and p. If p is not a prime, then it is a composite number [12].

Definition 2. Let a and b two integers, some of them can differ from zero. The greatest common divisor (gcd) on a and b is the largest positive integer d noticed by $(a,b) = d$ that divides both a and b. In the case in which $(a,b) = 1$, we say that a and b are related primes. An immediate consequence of the definition States that if $(a,b) = 1$ and $(a,c) = 1$, then $(a,bc) = 1$.

Definitión 3. If n is a positive integer, we say that two integers a and b are *congruent module* n If there is a $k \in \mathbb{Z}$ such that $a - b = kn$. We will use $a \equiv b \bmod n$ notation to indicate that a and b are *congruent module* n.

In mathematics, *congruent module* n is known as *modular arithmetic* [13]. Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the **modulus**. The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in 1798 when he was 21 years old and it published in 1801 in his book *Disquisitiones Arithmeticae* (In Latin, in English:: *Arithmetical Investigations*), when he was 24 years old. In this book Gauss brings together results in number theory obtained by mathematicians such as Fermat, Euler, Lagrange and Legendre and adds important new results of his own [14].

The congruence relation module n in $\mathbb{Z}$ is equivalence and therefore divides $\mathbb{Z}$ into equivalence classes so that any of two of them are disjoint, i.e.:

$$\mathbb{Z} = \cup_{j=0}^{n-1}[j] \text{ with } [j] = \{j + kn: \ k \in \mathbb{Z}\}$$

Where $[j]$ is the j-th equivalence class module n. Whenever an integer z belongs to any of the n equivalence classes, we will say that it is *a representative of that class* [15,16].

3.2 Fundamental Theorem of Arithmetic

Every natural composite number $n > 1$ can be factored uniquely as:

$$n = {p_1}^{k_1} {p_2}^{k_2} \times \cdots \times {p_s}^{k_s}$$

Where $p_1, p_2, \cdots p_s$ are different primes and $k_1, k_2, \cdots, k_s$ are positive integers. This factorization is called the *prime factorization* of n, [17,18].

3.3 Theorem

Let a and b relative primes, then there exist infinity primes p congruent $a \bmod b$.

Demonstration. We will make the demonstration by reduction *ad absurdum*, i.e. assuming that there is a prime p congruent $a \bmod b$, which is the largest. As a result, if $p_1, \dots, p_r$ are primes congruent $a \bmod b$, then $p_i \le p$ for all $i = 1, \dots, r$. On the other hand, $p = a + bn$ for some $n \in \mathbb{N}$ and $(a,n) = 1$, if not p can't be a prime. On the other hand, given that $(a,b) = 1$ It follows that $(a,bn) = 1$. In addition, we affirm that $(a,p) = 1$. Namely, if not, there is $k \in Z$ such as $p = ka,$, which $(k-1)a = bn$, and this contradicts the fact that a and bn are related primes.

Then, taking into account the fundamental theorem of arithmetic, n can be represented as:

$$n = {p_1}^{k_1} \times {p_2}^{k_2} \times \cdots \times {p_s}^{k_s}$$

Where $k_1, k_2, \cdots, k_s$, are non-negative integers and $p_1, p_2, \dots, p_s$ are different primes. Since $n \to \infty$, and the primes are infinites, then $s \to \infty$.

Defining a number q as well:

$$\begin{aligned} q &= a + bnp \\ &= a + b{p_1}^{k_1} \times {p_2}^{k_2} \times \cdots \times {p_s}^{k_s} \times p \end{aligned}$$

Where $p \le p_s$.

As primes are infinite, then when p_s is going to infinity, it is obvious that, q is not divisible by any prime when $s \to \infty$, $[(p_s$ and $k_s) \to \infty]$, since it would result a residue, then, given that $(a, bnp) = 1$, q is divisible only by 1 and itself, i.e., q is prime, which turns out to be contradictory since we had assumed that p was the largest prime, and we have found that q is prime, $q > p$ and $q \equiv a \, mod \, b$, so, there are infinite primes $a + bn$. Thus, Dirichlet's theorem is demonstrated.

4. CONCLUSIONS

The demonstration by Dirichlet requires advanced knowledge of number theory. Therefore, some authors about books on theory and numerical analysis do not include their demonstration process. Here, it has been presented a very simple test available to people who don't have a great mathematical knowledge, as well as David Hilbert said (1862-1943), (also known as enunciating 23 mathematical problems that had not been resolved so far, some of them in the last 115 years already found solution), in 1900 in Paris, at the opening of the second International Congress of mathematics dedicated to "indicate probable directions of the mathematics of the new century", highlighting what he expressed in that Conference:

> *…" Besides it is an error to believe that rigor in the proof is the enemy of simplicity. On the contrary, we find it confirmed by numerous examples that the rigorous method is at the same time the simpler and the more easily comprehended"…,* [19].

This way of seeing Dirichlet's theorem, helps to solve other conjectures related to primes.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. O'Connor John J, Robertson Edmund F. «Biografía de Peter Gustav Lejeune Dirichlet» (in English), Mac Tutor history of Mathematics archive, Universidad de Saint Andrews; 2016.
2. Courant R, Robbins H. Primes in arithmetical progressions. §1.2b in Supplement to Ch. 1 in What Is Mathematics? An Elementary Approach to Ideas and Methods, 2nd ed. Oxford, England: Oxford University Press. 1996;26-27.
3. Hardy GH, Wright EM. An introduction to the theory of numbers, 5th ed. Oxford, England: Clarendon Press. 1979;13-14.
4. González de la Hoz FA. Demostración del teorema de Dirichlet, web de la UNED
5. Kuat Yessenov. Dirichlet's theorem on primes in arithmetic progressions. Available:http://people.csail.mit.edu/kuat/courses/dirichlet.pdf
6. GL. Dirichlet's Werke, I (Traduction: Dirichlet Work I), pp. 313-342. Dirichlet: There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime English translation of the original paper at the arXiv.
7. Apostol Tom M. Introduction to analytic number theory. Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, ISBN 978-0-387-90163-3, MR 0434929, Zbl o335.10001; 1976.
8. Apostol TM. "Dirichlet L-function", in Olver Frank WJ, Lozier Daniel M, Boisvert Ronald F, Clark Charles W. NIST Handbook of Mathematical Functions, Cambridge University Press, ISBN 978-0521192255, MR 2723248; 2010.
9. Davenport H. Multiplicative number theory (2nd ed.) Graduate texts in Mathematics 74. Springer; 1980.
10. Montgomery HL. Topics in multiplicative number theory. LNM 227, Springer-Verlag, Berlin-Heidelberg-New York; 1971.
11. Ivi´c A. The riemann zeta-function, theory and applications. Dover Publications, Inc., Mineola, New York; 2003.
12. Nagell T. Primes. §3 in Introduction to Number Theory. New York: Wiley. 1951; 13-14.
13. Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, Clifford Stein. Introduction to algorithms, Second Edition. MIT Press and McGraw-Hill, ISBN 0-262-03293-7. Section 31.3: Modular Arithmetic. 2001; 862–868..
14. Carl Friedrich Gauss, tr. Arthur A. Clarke: Disquisitiones Arithmeticae, Yale University Press; 1965. ISBN 0-300-09473-6.
15. Pettofrezzo Anthony J, Byrkit Donald R. Elements of number theory. Englewood Cliffs: Prentice Hall, LCCN 71081766; 1970.

16. Dorronsoro J, Hernandez E. Numbers, groups and rings. In Spanish: Números, grupos y anillos, Addison-Wesley Iberoamericana España S.A; 1996.
17. Mora FW. Introduction to the theory of numbers. School of mathematics, Technology Institute from Costa Rica In spanish: Introducción a la Teoría de Números. Escuela de Matemáticas, Instituto Tecnológico de Costa Rica; 2014.
18. Euler L. An arithmetic theorem proved by a new method, New Memoirs of the St. Petersburg Imperial Academy of Sciences, 8: 74-104. Available on-line in: Ferdinand Rudio, ed., Leonhardi Euleri Commentationes Arithmeticae, volume 1, in: Leonhardi Euleri Opera Omnia, series 1, volume 2 (Leipzig, Germany: B.G. Teubner); 1915.
19. Hilbert David. Future problems of mathematics. Lecture delivered before the International Congress of Mathematicians at Paris in 1900. Dr. Maby Winton Newson translated this address into English with the author's permission for Bulletin of the American Mathematical Society 8 (1902), 437-479. A reprint of appears in Mathematical Developments Arising from Hilbert Problems, edited by Felix Brouder, American Mathematical Society; 1976.

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/13546