Research Journal of Pure Algebra -2(11), 2012, Page: 321-324

Available online through www.rjpa.info ISSN 2248–9037

WHY THE NUMBER 1 SHOULD NOT BE CONSIDERED A PRIME NUMBER

Eberto R. Morgado[a,c*] & Marco V. José[b,c,*]

[a]Facultad de Matemática, Física y Computación, Universidad Central "Marta Abreu" de Las Villas, Santa Clara, Cuba
[b]Theoretical Biology Group, Instituto de Investigaciones Biomédicas, Universidad Nacional Autónoma de México, México D.F. 04510, México
[c]Centro Internacional de Ciencias, Campus UNAM-UAEM, Col. Chamilpa, CP 62210, Cuernavaca, Morelos, Mexico

(Received on: 02-12-11; Revised & Accepted on: 26-11-12)

ABSTRACT

This is a pedagogical note about the historically polemic question about whether the number 1 is or is not a prime. A number theoretical argument is given for not considering 1 as a prime number. In order to avoid this inclusion a correct definition of prime number is proposed and also a consequent formulation of the so-called Fundamental Theorem of Arithmetic, which is here interpreted in terms of a generator set of a monoid. Finally, the generalized concept of a prime element in an integral domain is given.

I. INTRODUCTION

1. If you ask somebody what is a prime number most people will say that a prime number is that which is divisible only by one and by itself. Even in some books the concept of prime number has been defined as natural numbers which are divisible only by 1 and themselves (e.g. [1, 2]). During a long time the question about whether the number 1 is or is not a prime has been controversial and it has divided the community of mathematicians by different criteria**.** But**,** if we adopt such a definition the number 1 would, obviously, be included in the class of prime numbers.

An ancient theorem, the so-called Fundamental Theorem of Arithmetic, which is attributed to Euclid (300 B.C.), asserts that every natural number n is itself a prime or it is the product of a finite number of prime factors, being that factorization unique except the ordering of the factors. We observe that the inclusion of 1 as a prime number does not invalidate that assertion, but if 1 is not a prime, then, the assertion is not entirely true. Nevertheless, we think that there are reasons for not including the number 1 amongst the primes. In the present work we will analyze that situation and will argue for the idea of giving the definition in such a way that 1 should not be included in the class. Our main argument is based in a number theoretical consideration, namely, the generality of the theorem, which asserts that "The ring $\mathbb{Z}_n$ of remainders module the natural number n, is a field, if, and only if, n is a prime number".

2. SOME PREVIOUS DEFINITIONS AND CONCEPTS

In the following we give, as reminders, a list of some necessary concepts and notations:

Natural numbers: We call natural numbers the positive integers, that is, the numbers: 1, 2, 3, 4…and so on. Then, in our convention, 0 is not a natural number. We will denote as $\mathbb{N}$ the set of natural numbers.

The set $\mathbb{Z}$ of integers: We denote as $\mathbb{N}^-$ the set $\{-1,-2,-3,\ldots -n,\ldots\}$ of the negative integers, that is, the set of all the opposites of natural numbers. The set $\mathbb{Z}$ of integers is the union $\mathbb{N}^- \cup \{0\} \cup \mathbb{N}$, that is, the negative integers, 0 and the natural numbers.

Semigroup: An algebraic system (S,T), where S is a nonvoid set and T a binary associative inner operation defined in S.

Monoid: A semigroup (M,T) with neutral element e, such that $eTx = xTe = x$ for every $x \in M$.

***Corresponding author:** Marco V. José[b, c,*], [b]Theoretical Biology Group, Instituto de Investigaciones Biomédicas, Universidad Nacional Autónoma de México, México D.F. 04510, México*

Group: A monoid (G,T) where every element is invertible, that is, for every $x \in G,$ there is x^{-1} such that $xTx^{-1} = x^{-1}Tx = e$, where e is the neutral element.

Abelian Group: A group (G,T) where the operation T is commutative.

Ring: Algebraic system $(R,+,\times),$ where $+$ and $\times$ are binary inner operations, called addition and multiplication, respectively, defined in the set $R,$ and such that $(R,+)$ is an abelian group, $(R,\times)$ is a semigroup and the operation $\times$ is distributive with respect to the operation $+$.

Conmutative ring: A ring $(R,+,\times),$ where the operation $\times$ is commutative.

Unitary ring: A ring $(R,+,\times),$ where the multiplicative semigroup $(R,\times)$ is a monoid, being its neutral element 1 different from the neutral 0 of the group $(R,+)$. The invertible elements of the monoid $(R,\times)$ are called the units of the ring. If we denote as R^* the set of units, then $(R^*,\times)$ is a group, called the group of units of the ring, which is a submonoid of the monoid $(R,\times)$.

Example: The ring $(\mathbb{Z},+,\times)$ of integers is a commutative and unitary ring being $\mathbb{Z}^* = \{-1,1\}.$

Associates: We say that an element a is associate of an element b if there is a unit ε such that $a = \varepsilon \times b.$ Obviously, if a is associate of b, then b is associate of a.

In the ring $(\mathbb{Z},+,\times)$ of integers the only associates of an element a are the same a and its opposite $-a$.

Field: A commutative and unitary ring, where every element, different from 0, is invertible. It means that for the group of units $(R^*,\times)$, $R^* = R\setminus\{0\}$.

Example: The ring $(\mathbb{Q},+,\times)$ of the rational numbers, that is, the numbers of the form $\frac{a}{b}$, where a is an integer and b is a natural number, is a field.

Zero divisor: In any ring an element a is called a "left" zero divisor if there is some $b \neq 0$ such that $a \times b = 0$. Analogously, a is called a right zero divisor if there is $b \neq 0$ such that $b \times a = 0$. The element a is called zero divisor if it is, simultaneously, a left zero divisor and a right zero divisor. Obviously, the element 0 is a zero divisor. An element a is called a proper zero divisor if it is a zero divisor and it is different from 0.

Integral Domain: An integral domain is a commutative and unitary ring without proper zero divisors. Obviously, every field is an integral domain.

Generator set of a semigroup: For a semigroup (S,T) a subset G of S is called a generator set of the semigroup if every x element of S is itself a member of G, or it is the result of operating a finite number of elements of G.

Generator set of a monoid: For a monoid (M,T) a subset G of M is called a generator set of the monoid if every x element of M, different from the neutral element, is itself a member of G or it is the result of operating a finite number of elements of G.

The ring of remainders module n

Let n denote a natural number and $\mathbb{Z}_n$ the set $\{0,1,\ldots n-1\}$ of the remainders under the entire division of any integer by n. As it is well known, for every integer a there exist the integers q and r, called, respectively, the quotient and the rest of a, under the entire division by n, such that, $a = n \times q + r,$ with $r \in \mathbb{Z}_n$. The number q is

the entire part of $\left\lfloor \frac{a}{n} \right\rfloor$, by defect, of the rational number $\frac{a}{b}$, that is, the greatest integer which is $\leq \frac{a}{n}$. Let us denote by r_n the function from $\mathbb{Z}$ to $\mathbb{Z}_n$ which assigns to every $a \in \mathbb{Z}$ its rest or remainder $r_n(a) = a-(n\times q) \in \mathbb{Z}_n$.

In the set $\mathbb{Z}_n$ we define the binary operations $\oplus_n$ and $\otimes_n$, induced by the operations + and $\times$ of $\mathbb{Z}$ and the surjective function $r_n : \mathbb{Z} \to \mathbb{Z}_n$, in such a way that the function r_n becomes a unitary ring homomorphism, being the triple $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ a commutative and unitary ring, homomorphic image or the ring $(\mathbb{Z}, +, \times)$, under the epimorphism r_n. For $n > 1$, it is also a unitary ring.

II. OUR ARGUMENT

A well-known theorem asserts that the invertible elements of the ring $(\mathbb{Z}_n, \oplus_n, \otimes_n)$, for $n > 1$, are the elements a of $\mathbb{Z}_n$ which are coprime with n, that is, such that $GCD(a, n) = 1$. Next, we remind the proof of that theorem, taken here as a lemma.

Lemma: In the ring $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ of remainders modulo n, $n > 1$, the invertible elements are those, which are coprime with n.

Proof: If they are coprime, then there exist integers x, y such that $a x + b y = 1$. Then, $a \otimes_n r_n(x) = 1$, and it means that $r_n(x)$ is the inverse of a in the monoid $(\mathbb{Z}_n, \otimes_n)$.

Conversely, if a is invertible and b is its inverse, then $a \otimes_n b = 1$. Then, $a \times b = 1 + nk$ for some integer k. Hence, $(a \times b) + (n \times (-k)) = 1$, and it implies that $1 = GCD(a, n)$, that is, they are coprime.

Next, we remind the theorem of characterization of finite prime fields or fields of modular remainders (a field is called a prime field if it has no proper subfields).

Theorem: For $n > 1$, the ring $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ is a field if, and only if, n is a prime number.

Proof: If n is a prime number then every natural number a, such that $0 < a < n$ is coprime with n, then it is invertible under the operation $\otimes_n$. Hence, the ring is a field.

Conversely, if it is a field, every non-null element a is invertible, then, it is coprime with n. It implies that n has no divisors less than itself and different from 1. Then, n is a prime number.

CONCLUSION

Here, we observe that if n is considered a prime number, the assertion of the theorem can not be extended to the case $n = 1$, since, in this case, $\mathbb{Z}_1 = \{0\}$, and the commutative ring $(\mathbb{Z}_1, \oplus_1, \otimes_1)$, is the trivial or null ring, in which the addition and the multiplication are the same, which is not a unitary ring. Hence, it is not a field.

Another reason for not considering 1 as a prime number is that it would break the uniqueness of the factorization of any natural number. For example the number 6=2×3, could also be represented as 1×2×3, or 1×1×2×3. That is, the "prime factor" 1, could be included as many times as we want.

The correct definition of prime number and the consequent formulation of the fundamental theorem of arithmetic

According to the foregoing results the criterion of not considering the number 1 as a prime number has predominated and modern books define it in such a way that 1 is not included in the class of prime numbers (e.g. [3, 4]). The correct definition of prime number must be as follows:

Definition 1: We call a prime number a natural number p, greater than 1, such that it is only divisible by 1 and by itself.

Here, we remark the necessity of saying "different from 1". Another equivalent definition is:

Definition 2: A prime number is a natural number, which has exactly two different natural divisors.

Then, 1 is not included because it has only one natural divisor, the same 1.

In agreement to the correct definition of prime number, the formulation of the Fundamental Theorem of Arithmetic should be slightly modified, taking the following form:

Theorem: "Every natural number n, different from 1, is itself a prime number, or it is the product of a finite number of prime factors. The factorization is unique, except the ordering of the factors.

Generalization of the concept of prime number for integral domains

Definition 3: In an integral domain an element $b \neq 0$ will be called prime or irreducible if it is not a unit and a divides b implies that a is a unit or an associate of b. Otherwise, b is called reducible.

We observe, from Definition 3, that neither the neutral 1 nor the other units, are included in the class of prime elements (see [5]).

OBSERVATION

The Fundamental Theorem of Arithmetic means, in essence, that the infinite set $\prod$ of prime numbers is a generator set of the multiplicative monoid $(\mathbb{N},\times)$ of natural numbers. If 1 is not a prime, then the set $\prod$ is not a generator set of $(\mathbb{N},\times)$ as a semigroup, since 1 is not factorizable as a product of primes.

ACKNOWLEDGEMENTS

ER and MVJ were financially supported by The Macroproyecto de Tecnologías para la Universidad de la Información y la Computación (MTUIC), UNAM, México. MVJ also thank the financial support of PAPIIT IN107112, ER also thanks the financial support of the Coordinación de la Investigación Científica, UNAM.

.

REFERENCES

[1] Pequeño Larousse Ilustrado, Instituto Cubano del Libro, La Habana, 1968.
[2] Pequeño Larousse de Ciencias y Técnicas, Instituto Cubano del Libro, La Habana, 1968.
[3] Garret Birkoff and Saunders MacLane, A survey of Modern Algebra, MacMillan Company, 1941.
[4] Prime numbers, Wikipedia, The free encyclopedia. Internet.
[5] Richard A. Dean, Elements of Abstract Algebra, John Wiley and Sons, New York London Sydney, 1966.

Source of support: The Macroproyecto de Tecnologías para la Universidad de la Información y la Computación (MTUIC), UNAM, México, Conflict of interest: None Declared

