South American Journal of Logic
Vol. 2, n. 2, pp. 187–200, 2016
ISSN: 2446-6719

On Alien Primes, Exotic Number Theory, and Mathematical Pluralism

Walter Carnielli

To Chico Miraglia, with whom
I have learned and keep learning

Abstract

The aim of this paper may be regarded as pure fun with numbers and their generalizations. But it can also be seen as a modest essay on the philosophy of mathematics, hinting to some distinctive views by which mathematicians and philosophers approach mathematics. I discuss here, by completely elementary mathematical means, some 'exotic' domains that exhibit some unexpected conceptual connections to logic. A *number ring* is a subring of a *number field*, where a number field is a finite field extension of the field of rational numbers $\mathbb{Q}$. Number rings naturally arise when solving equations in ordinary integers, and that was precisely how they made their historic appearance in the mathematical scenario. They usually encompass unusual mathematical objects that expand the mathematical province, separating properties such as irreducibility and primality. They may originate, however, intriguingly unusual number theories, and I venture some conjectures here illustrating this point.

Keywords: Gaussian integers, exotic number-theoretical conjectures, philosophy of mathematics.

1 Cardano, Descartes, Euler, Gauss ···

This paper intends to play with some uncommon numbers and their generalizations, hoping this may be of some interest. Some 'exotic' number rings (at least for the non-mathematician) and new problems concerning them are posed as conjectures. Such domains usually formalize some new mathematical objects that expand the possibilities of expressing previously unknown ideas, distinguishing properties that were previously seen as inseparable. The ideas of a unit element, of an irreducible element as something

which is not a product of two non-units, and of a prime element, as distinct concepts are commonplace in Algebra today, but that was not always the case. Now we know clearly that irreducible elements, for instance, should not be confused with prime elements. In logic, as I discuss in the last section, we are only now accepting that a contradictory theory should not be confused with an inconsistent theory, nor that a non-contradictory theory should not be confused with a consistent one. Mathematicians came first, philosophers are trying to keep the pace. From this point of view, there is something to be learned from the viewpoint of the philosophy of mathematics, as hinted in Section 5.

A *number ring* is a subring of a *number field*, where a number field is a finite field extension of the field of rational numbers $\mathbb{Q}$.

Exotic objects typically arise when solving problems, and the history is full of examples. Without any attempts to write novelty in mathematical history here, it is known that negative numbers were not well regarded, and that Heron of Alexandria (circa 50 AD) in his *Stereometria* was possibly the first to notice the possibility of imaginary numbers when trying to solve a geometric problem that needed $\sqrt{81-144}$. Suspecting that something was wrong, he switched the calculation to $\sqrt{144-81}$. But the first in the Western literature to bravely compute with square roots of negative quantities was Girolamo Cardano in his *Ars Magna, sive de Regulis Algebraicis* (The Great Art, or The Rules of Algebra), published in Nuremberg in 1545.

Cardano was looking for the solution to a classical general problem: Find two numbers whose sum and product are given. In the case the sum is 10 and the product 40, he knew it was impossible to find two numbers under such conditions. Nonetheless, he went into providing two objects that satisfied the given conditions. He offered the following method of solution: say that we seek two numbers so that their sum is S and their product is P. Divide S by 2, so that we obtain a number x, with $x+x=S$. Form two new expressions, $x+m$ and $x-m$ By forcing these two expressions whose sum is S to behave like their product is P, we give birth to two new objects, in the case $S=10$ and $P=40$: $5-m$ and $5+m$. Therefore $25-m^2=40$ or $m^2=-15$, building some 'truly sophistic' arithmetic subtleties, 'fictitious" numbers' that originated the complex numbers, as they are now called.

As Cardano disdainfully puts it in his *Ars Magna* (pp. 219-220):

> "So progresses arithmetic subtlety the end of which... is as refined as it is useless".

But besides his disdain, Cardano believed that even if his computation would be mistaken in the light of his contemporary theory, naming these objects as 'impossible quantities' and using them for calculations was a sharp improvement. Cardano was imprisoned as a heretic by the Inquisition circa 1570, and the fact that he was maintained under surveillance until his death and forbidden from publishing and from lecturing in

public, according to [11], may have affected his work on square roots of negatives and his view about it.

Descartes was responsible for the introduction of the expression 'imaginary quantities' in his *Geometry* of 1637, a contemptuous expression used until the introduction by Gauss of the more respectful terminology 'complex numbers' in his lectures of 1831.

Gauss is to be credited with the clarification of the status of these quantities in his important treatise *Theoria residuorum biquadraticorum, Commentatio Secunda*, published in 1832 ([6]) in which he considered the numbers $a+bi$, for $i = \sqrt{-1}$. Despite being used in calculations, until the mid 19th century these mysterious entities were always surrounded by philosophical suspicion and used with some concern, as it happened with the infinitesimals.

Euler had already introduced the notation i in his *Elements d'Algèbre* (1774), but this notation, also used by Gauss, had not been immediately accepted.

In the second part of his work, dedicated to biquadratic residues, Gauss explicitly says that number theory is revealed in its 'entire simplicity and natural beauty' when the field of arithmetic is extended to the imaginary numbers, by admitting numbers of the form a + bi, numbers which 'will be called complex integers'.

Gauss gave the rules for calculating with such numbers, and a way to represent complex numbers by points in the plane. The idea had already occurred before, to John Wallis (in the Treatise of Algebra, 1685), to Caspar Wessel in 1792, and to Jean Robert Argand in 1806. As Gauss was the first to use complex integers in a systematic way, the planar representation worked as a kind of "real model", helping to dissipate some ghosts. Gauss helped much in widening the concept of number, and influenced the growth of abstract algebra. Section 5 offers some additional comments on this point.

The papers by Gauss exerted an enormous influence on the 20th and 21st-century mathematics and had a profound effect on the subsequent development of number theory and algebraic geometry.

2 A glimpse of the Gaussian integers and alien primes

The domain of *Gaussian integers* is the number ring formed by all elements in the set $\mathbb{Z}[i] = \{a + b.i \ : \ a, b \in \mathbb{Z}$, for $i = \sqrt{-1}'$.

The most interesting notions associated with these exotic numbers is the concept of prime Gaussian integers, which conveys the idea that Gaussian primes cannot be further factored, as well as the unique factorization by primes. An important consequence is the property of Unique Factorization Theorem for the Gaussian integers, is an analogue of the Fundamental Theorem of Arithmetic of standard integers, which states that each

Gaussian integer can be factored as a product of Gaussian primes in an essentially unique way.

As much as in $\mathbb{Z}$ the size of an element is measured by its absolute value, in $\mathbb{Z}[i]$ the size of an element is measured by its norm.

Definition 2.1 *1) For $\alpha = a + bi \in \mathbb{Z}[i]$, its norm is the product $N(\alpha) = \alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2$.*

2) For $\alpha, \beta \in \mathbb{Z}[i]$ we say that β divides α (or that β is a factor of α) and write $\beta|\alpha$, if $\alpha = \beta\gamma$ for some $\gamma \in \mathbb{Z}[i]$.

Theorem 2.2 *1) The norm is multiplicative: for α and β in $\mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.*

2) A Gaussian integer $\alpha = a + bi$ is divisible by a standard integer c if and only if $c|a$ and $c|b$ in $\mathbb{Z}$.

3) For $\alpha, \beta \in \mathbb{Z}[i]$, if $\beta|\alpha$ in $\mathbb{Z}[i]$ then $N(\beta)|N(\alpha)$ in $\mathbb{Z}$.

Proof. 1) Just check that for $\alpha = a + bi$ and $\beta = c + di$, $\alpha\beta = (ac - bd) + (ad + bc)i$ and that $N(\alpha)N(\beta)$ and $N(\alpha\beta)$ coincide.

2) Routine.

3) If $\beta|\alpha$ then $\alpha = \beta\gamma$ for some $\gamma \in \mathbb{Z}[i]$. Take the norm of both sides and obtain an equation in $\mathbb{Z}$.

■

A first consequence of Theorem 2.2 characterizes the multiplicative inverses in $\mathbb{Z}[i]$:

Corollary 2.3 *The only Gaussian integers which have multiplicative inverses in $\mathbb{Z}[i]$ are unities $\pm i$ and ± 1.*

Proof. Suppose $\alpha \in \mathbb{Z}[i]$ is invertible, so there exists $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. Thus $N(\alpha\beta) = N(\alpha)N(\beta) = 1$, and since $N(\alpha), N(\beta) \in \mathbb{Z}$ and the norm must be a positive integer, $N(\alpha) = a^2 + b^2 = 1$. Therefore $a^2 = 1$ or $b^2 = 1$ and $\alpha = \pm i$ or $\alpha = \pm 1$ or $\beta = \pm i$ $\beta = \pm 1$.

On the other hand, clearly $\pm i$ and ± 1 have multiplicative inverses in $\mathbb{Z}[i]$: i and $-i$ are inverses of each other, and 1 and -1 are their own inverses. ■

A more subtle property of Gaussian integers, whose proof is not difficult but cumbersome, is the analogue of the ordinary process of division with remainder of $\mathbb{Z}$:

Theorem 2.4 *Division Theorem: For $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there are $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \delta$ and $N(\delta) \leq (1/2)N(\beta)$.*

Proof. See [9] or [8]. ■

There are however some subtle differences between the division theorem in $\mathbb{Z}[i]$ and the (usual) division theorem in $\mathbb{Z}$; so, for instance the quotient and the remainder are not unique in $\mathbb{Z}[i]$. But uniqueness of the quotient and remainder is irrelevant for critical applications such as Euclid's algorithm: what is essential is that the remainder is bounded.

The next appropriate notion is that of primality. For any ordinary integer n with $|n| > 1$ there are four trivial factors of n, ± 1 and $\pm n$, Similarly, for any α in $\mathbb{Z}[i]$ such that $N(\alpha) > 1$, ± 1, $\pm i$, $\pm\alpha$, and $\pm i\alpha$ are always eight obvious factors of α: these are the trivial factors of α (other factors are called non-trivial).

Clearly, if if p is an ordinary prime which can be written as a sum of two squares $p = a^2 + b^2$, then p is not a prime (i.e., irreducible) as a Gaussian integer, since it factors as $p = (a + bi)(a - bi)$. But are $a + bi$ and $a - bi$ Gaussian primes?.

Definition 2.5 *Let α be a Gaussian integer with $N(\alpha) > 1$. α is said to be composite if it has a non-trivial factor, and prime if it has only trivial factors.*

It can be proved that Gaussian primes can be characterized in the following way:

Theorem 2.6 *Gaussian primes are Gaussian integers $\pi = a + bi$ satisfying one of the following properties.*

1. If both a and b are nonzero, then $a + bi$ is a Gaussian prime iff $a^2 + b^2$ is an ordinary prime.

2. If $a = 0$ or $b = 0$, then a Gaussian integer of the form c or ci, $c \in \mathbb{Z}$, is a Gaussian prime iff $|c|$ is an ordinary prime and $|c| \equiv 3 \pmod 4$.

Proof. This proof is available in several places, see e.g. [9] or [8]. ■

Consequently, no prime number p such $p \equiv 1 \pmod 4$ is a Gaussian prime; indeed there are exactly two Gaussian primes π and $\bar{\pi}$ of norm p such that $p = \pi\bar{\pi}$

Primes in $\mathbb{Z}[i]$, by definition, enjoy the property that, when π divides a product $\alpha\beta$, then π divides α or else π divides β. This property has as a consequence that every Gaussian integer factors as a product of primes in a unique way; in other words, $\mathbb{Z}[i]$ is a Unique Factorization Domain (UFD) (details in e.g. [8]).

Taking unique factorization for granted is a source of many historical mistakes in mathematics. Besides $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ is also an UFD (or an Euclidean ring), but $\mathbb{Z}[\sqrt{-n}]$ for $n \geq 3$ is not an UFD. As a counterexample, in $\mathbb{Z}[\sqrt{-3}]$ it holds $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, but 2 does not divide either factor, so $\mathbb{Z}[\sqrt{-3}]$ cannot be an UFD. It can be proved that $\mathbb{Z}[\sqrt{-n}]$ is an UFD if and only if $n = 1$ or $n = 2$, for natural numbers n. The problem is still unsolved for $\mathbb{Z}[\sqrt{n}]$; it is known that $\mathbb{Z}[\sqrt{n}]$ is not an UFD if $n \equiv 1 \pmod 4$ ([18], Theorem 8.25). A proof that $\mathbb{Z}[\sqrt{14}]$ is an Euclidean ring appeared in [7] only in 2004 .

3 Some exotic conjectures and devilish counterexamples

In a one-page note, [21] generalizes Andrew Wiles' famous proof of the Fermat's Last Theorem, showing that the equation $x^n + y^n = z^n$ has no solution in positive integers x, y, and z when n is a non-real Gaussian integer. However, $\mathbb{Z}[\sqrt{-7}]$ provides $(3 + \sqrt{7}i)^4 + 4^4 = (-1 + \sqrt{7}i)^4$, so Gaussian integers produce a surprising (folkloric) counterexample to the Fermat's Last Theorem. Interestingly enough, $3 + \sqrt{7}i$, 4, and $-1 + \sqrt{7}i$ are factors of 16 in $\mathbb{Z}[\sqrt{-7}]$, since $(3 + \sqrt{7}i)(3 - \sqrt{7}i) = 16$ and $(-1 + \sqrt{7}i)(1 + \sqrt{7}i) = 8$. There is even space for a question: are there Gaussian integers such that $(a + bi)^3 = (c + di)^3 + (e + fi)^3$?

In an analogous fashion, Beal's conjecture[1] is false for Gaussian integers. A generalization of Fermat's Last Theorem, Beal's conjecture states that, if $a^x + b^y = c^z$, where a, b, c, x, y, and z are positive integers and x, y and z are all greater than 2, then a, b and c must have a common prime factor.

A counterexample in $\mathbb{Z}[\sqrt{-1}]$ (unpublished) to a generalized version of Beal's conjecture was found by Fred W. Helenius employing Gaussian primes: $(-2+i)^3+(-2-i)^3 = (1 + i)^4$.

This illustrates how subtle exotic domains as Gaussian integers can be. Some properties that are obviously true or conjectured to be true in the ordinary integers are falsified in the Gaussian domain; on the other hand, some new conjectures can be posed. Some examples follow.

Definition 3.1 *Two Gaussian primes $a + bi$ and $c + di$ are* Gaussian twin primes *if* $(a + bi) - (c + di) = \pm 1 + (\pm i)$.

Conjecture 3.2 *(Carnielli) There are infinitely many Gaussian twin primes.*

Some examples:

(12 + 13i) = (1 - i) + (11 + 14i)

(99 + 94i) = (1 + i) + (98 + 93i)

In the (failed) attempts to prove it, another conjecture on ordinary integers emerged:

Conjecture 3.3 *(Carnielli) If q is an ordinary prime, then there exists a natural number n such that the sum of q and the n-th power of 2 is an ordinary prime number. More formally,* $(\forall q)(Prime(q) \rightarrow (\exists n)(\exists p)(Prime(p) \wedge (p = 2^n + q)))$

[1]The Beal Prize, funded by the banker and amateur mathematician D. Andrew Beal, offers currently US$1,000,000 for either a proof or a counterexample of the Beal Conjecture. The prize money is being held by the AMS.

Both conjectures have been computer- tested for a reasonable number of cases. They may have some connections to a result of Y. Zhang about bounds on gaps between primes (see [19]).

Several other conjectures are possible, of course, but what should be emphasized is the heuristic role of the Gaussian integers in guiding us towards such conjectures, which (if solved) may shed some light on their natural numbers counterpart.

4 Gaussian versions of the generalized Collatz conjecture

The Collatz conjecture, also known as the Syracuse problem, Kakutani's problem, Hasse's algorithm, Ulam's problem, Thwaites's problem and Hailstone Algorithm, or $3x+1$ Conjecture, is perhaps one of the most perplexing unsolved mathematical problems. Differently from other hard problems such as Goldbach's conjecture, some of its generalizations are even undecidable (cf. [13]).

This apparently innocent conjecture was proposed by Lothar Collatz (1910-1990) in 1928, originally stated as follows: consider the function which inputs a non-zero integer x and outputs $3x+1$ if x is odd, and $x/2$ if x is even. The $3x+1$ Conjecture asserts that, starting from any positive integer x, repeated iteration of this function eventually produces the value 1. In a more appropriate notation, the conjecture is usually rephrased by considering the function:

$$T_2(x) = \begin{cases} x/2 & \text{if } x \equiv 0 \pmod 2) \\ (3x+1)/2 & \text{if } x \equiv 1 \pmod 2) \end{cases}$$

The (rephrased) conjecture states that every trajectory starting from a non-zero integer will end into the cycle (1,2) if inputs are restricted to positive integers x. For negative inputs, there are three additional cycles: (-1), (-5,-7,-10), and (-17,-25,-37,-55,-82,-41,-61,-91,-136,-68,-34). A standard reference on this problem is [14].

Some quite natural generalizations of Collatz Problem and corresponding conjectures have been proposed in [2]: the generalized Collatz functions T_d and $T_{k,d}$. For d amd k natural numbers, T_d and $T_{k,d}$ constitute an infinite class of numeric functions that behave analogously with the primary $3x+1$-problem of Lothar Collatz, and give rise to infinitely many open problems in number theory.

Define a mapping $T_d : \mathbb{Z} \mapsto \mathbb{Z}$ by:

$$T_d(x) = \begin{cases} x/d & \text{if } x \equiv 0 \pmod d \\ ((d+1)x + (d-i))/d & \text{if } x \equiv i \pmod d, 1 \leq i \leq d-1. \end{cases}$$

Since $x \equiv i \pmod{d}$ implies $T_d(x) \equiv 0 \pmod{d}$, the mappings $T_d(x)$ are well-defined over $\mathbb{Z}$. In particular, for $d = 2$ the mapping $T_2(x)$ gives the original 3x+1 function.

For $d = 3$ the mapping $T_3(x)$ defines the function:

$$T_3(x) = \begin{cases} x/3 & \text{if } x \equiv 0 \pmod{3} \\ 4x + 2/3 & \text{if } x \equiv 1 \pmod{3} \\ 4x + 1/3 & \text{if } x \equiv 2 \pmod{3} \end{cases}$$

Computer simulations ([2]) suggest that $T_3(x)$ has only two non-trivial cycles (7, 10, 14, 19, 26, 35, 47, 63, 21) (cycle of length 9) and (-22, -29, -38, -50, -66) (cycle of length 5), besides the trivial cycles (1,2,3) and (-2,-1).

Those functions can be conveniently extended to mappings $\hat{T}$ from $\mathbb{Z}[i]$ into $\mathbb{Z}[i]$, as discussed below. With the aim of generalizing such problems to Gaussian integers, residue classes are defined in $\mathbb{Z}[i]$ through the following equivalence: $a + bi \equiv c + di \pmod{r + si}$ iff $(r + si)|(ac + (bd)i)$, for $a + bi$ a Gaussian prime. The first problem is to compute how many residue classes are there. For instance, for the prime $1 + i$, it is not difficult to see that every Gaussian integer is congruent to 0 or 1 $\pmod{1 + i}$. In fact, $a + bi \equiv ab \pmod{1 + i}$ since $(1 + i)|(a + bi) - (ab) = b(1 + 1)$.

Since $1 + i \equiv 0 \pmod{1 + i}$, then $i \equiv 1 \equiv i^2 \pmod{1 + i}$. This implies $i^2 \equiv (-1)^2 (mod 1 + i)$, and consequently $-1 \equiv 1 \pmod{1 + i}$, or $2 \equiv 0 \pmod{1 + i}$. To sum up, $a + bi \equiv ab \equiv 0 \pmod{1 + i}$ if ab is even, or $a + bi \equiv ab \equiv 1 \pmod{1 + i}$ if ab is odd, since ab is an ordinary integer. Thus $\{0, 1\}$ is a complete system of residues modulo $1 + i$.

For 2, $a + bi \equiv c + di \pmod{2}$ iff $2|(a - c)$ and $2|(b - d)$. The possibilities for $c + di$ are thus $0 + 0i$, $0 + i$, $1 + 0i$, or $1 + 1i$, depending whether a, b are odd or even. Hence $\mathbb{Z}[i]/(2) = \{0, 1, 1 + i, i\}$ is a complete set of residues, as they are not equivalent (mod 2).

An analogous reasoning shows that, for primes $c + di$ with norm $p \equiv 1 \pmod{4}$, the set $\{0, 1, ..., p - 1\}$ forms a complete system of residues modulo $a + bi$.

For primes $q \equiv 3 \pmod{4}$, it is not difficult to see that the set $S = \{r + si : 0 \leq r, s < p\}$ is a complete system of residues modulo p with p^2 elements.

This line of reasoning can be condensed in the following result:

Theorem 4.1 *A complete system of residues modulo a Gaussian prime $a + bi$ has exactly $N(a + bi) = a^2 + b^2$ elements.*

Proof. Folklore. ■

The generalized Collatz functions T_d can be extended to mappings $\hat{T}$ from $\mathbb{Z}[i]$ to $\mathbb{Z}[i]$ as follows. To fix ideas, let us start with $\widehat{T_2}(x)$ and $\widehat{T_3}(x)$:

$$\widehat{T_2}(x) = \begin{cases} x/2 & \text{if } x \equiv 0 \pmod 2 \\ 3x + 1/2 & \text{if } x \equiv 1 \pmod 2 \\ 3x + i/2 & \text{if } x \equiv i \pmod 2 \\ 3x + 1 + i/2 & \text{if } x \equiv 1 + i \pmod 2 \end{cases}$$

This particular problem coincides with the one studied in [10], of which [12] determined all cycles having period less than or equal to 400, finding 77 distinct cycles. For instance, $2 + 3i$ generates a cycle with length 5: $\widehat{T_2}(2 + 3i) = 3 + 5i$, and by applying $\widehat{T_2}$ successively one obtains $2 + 3i, 3 + 5i, 5 + 8i, 2 + 3i$. It is not known whether the number of cycles is finite or not.

The functions $\widehat{T_d}(x) : \mathbb{Z}[i] \mapsto \mathbb{Z}[i]$ are defined, in general, by:

$$\widehat{T_d}(x) = \begin{cases} x/d & \text{if } x \equiv 0 \pmod d \\ ((d+1)x + (d-n) + (d-m)i)/d & \text{if } x \equiv n + mi \pmod d, 1 \leq n, m \leq d-1. \end{cases}$$

As a second example, consider $\widehat{T_3}(x)$; recall that by Theorem4.1, $S = \{0, i, 2i, 1, 1 + i, 1 + 2i, 2, 2 + i, 2 + 2i\}$ form a complete system of residues modulo 3 for $0, 1, 2 \in \mathbb{Z}_3$.

$$\widehat{T_3}(x) = \begin{cases} x/3 & \text{if } x \equiv 0 \pmod 3 \\ 4x + 2/3 & \text{if } x \equiv 1 \pmod 3 \\ 4x + 1/3 & \text{if } x \equiv 2 \pmod 3 \\ 4x + 2i/3 & \text{if } x \equiv i \pmod 3 \\ 4x + 2 + 2i/3 & \text{if } x \equiv 1 + i \pmod 3 \\ 4x + 1 + 2i/3 & \text{if } x \equiv 2 + i \pmod 3 \\ 4x + i/3 & \text{if } x \equiv 2i \pmod 3 \\ 4x + 2 + i/3 & \text{if } x \equiv 1 + 2i \pmod 3 \\ 4x + 1 + i/3 & \text{if } x \equiv 2 + 2i \pmod 3 \end{cases}$$

Notice that $\mathbb{Z}[i] \subset \widehat{T_d}[\mathbb{Z}[i]]$, so $\widehat{T_d}$ are well-defined.

Some conjectures analogous to the Finite Cycles Conjecture for the original $3x + 1$ problem can be naturally formulated for the generalized Collatz problems concerning Gaussian integers. Of course, such problems are not expected to be easier, since they would settle the original $3x + 1$ problem and their generalizations $T_d(x)$.

Conjecture 4.2 *(Carnielli) $\widehat{T_d}$ has finitely many finite cycles For each d, the sequence of iterates*

$$x, \widehat{T_d}(x), \widehat{T_d}^2(x), \ldots, \widehat{T_d}^k(x), \ldots$$

always eventually enters a cycle, for finite k, and there are only finitely many such cycles.

Computer simulations for $T_d(x)$ (cf. [2]) suggested that cycles get bigger and rarer for increasing values of d, which suggests an obvious conjecture on the distribution of cycles and gaps on cycle lengths for $\widehat{T_d}$:

Conjecture 4.3 *(Carnielli) Lower bounds for cycles. For each M there is a d such that the minimal cycle length of the mapping $\widehat{T_d}$ is greater than M.*

Another generalization of the $3x+1$ mapping, as proposed in [2], is a two-parameter extension of T_d which exhibits an even more chaotic character. Define, for each $k \geq 3$ and $d \geq 2$, a mapping $T_{k,d} : \mathbb{Z} \mapsto \mathbb{Z}$ as follows:

$$T_{k,d}(x) = \begin{cases} x/d & \text{if } x \equiv 0 \pmod{d} \\ (kx + r(d-i))/d & \text{if } x \equiv i \pmod{d}, 1 \leq i \leq d-1 \\ & \text{and } k \equiv r \pmod{d}, 1 \leq r \leq d-1 \end{cases}$$

For $k = d + 1$, $T_{d+1,d}$ gives the above defined mapping T_d, and $T_{3,2}$ defines the original Collatz mapping.

It is a natural step to extend $T_{k,d}$ to Gaussian integers, but such generalizations await for more work. Nothing is known about them, albeit a conjecture similar to Conjecture 4 can be ventured for them.

Several other conjectures can be adapted for Gaussian integers, extending for instance the following: when is the sum of the squares of two successive integers also a square, i,e, when $n^2+(n+1)^2 = m^2$? It was shown in [16] that this happens for ordinary integers if and only if n is $0, 3, 20, 119, 696 \cdots, u_n, u_{n+1}, \cdots$ where $u_{n+1} = 6u_n - u_{n-1} + 2$.

Can the same argument be applied to Gaussian integers? What is the successor of $a + bi$? Clearly, $\mathbb{Z}[i]$ cannot be put in any order that is compatible with addition and multiplication. Indeed, a well-known elementary argument applies: since $i \neq 0$, either $i > 0$ or $i < 0$. In any case, $1^2 = 1 > 0$. If $i > 0$ then $i^2 > 0$ which means $-1 > 0$ or equivalently $1 < 0$, a contradiction. If $i < 0$ a contradiction also arises. We may, however, consider the 'local successor' of $a + bi$ either as $(a+1) + bi$, or as $a + (b+1)i$.

Is there always a prime between $(a+bi)^2$ and $((a+1)+bi)^2$? And between $(a+bi)^2$ and $(a+(b+1)i)^2$?

Nice problems to be considered– I do not know the answer of neither of them. But here is an invitation to try to solve some of them, or to formulate new conjectures.

5 On exotic and alternative objects and concepts, and their relevance

Logical pluralism is the thesis that there is more than one genuine deductive consequence relation. The main opposing view, logical monism, is the thesis that there is only one correct logic, or that the notion of consequence relation is absolute.

In a similar way, we can naturally think of mathematical pluralism - the discovery or invention of apparently exotic or deviant mathematical theories or objects such as complex numbers, the infinitesimals, non-euclidean geometries, non-standard analysis, or the taming of the infinite by Georg Cantor showing that an infinite collection can be treated as a totality, forming a mathematical object as 'real' as the natural numbers. However, this position seems to be at odds with mathematical Platonism (or realism), a view that abstract mathematical objects exist (and couldn't, supposedly, be freely created). Indeed, even if very few mathematicians would defend any 'mathematical monism' (perhaps because, as Cantor has said, 'the essence of mathematics lies in its freedom'), some mathematical abstractions are yet a bit difficult to be conceived by certain philosophers of mathematics.

Eighty years after Gauss, and more than 350 years after Cardano, in 1911 A. N. Whitehead ([20], p. 87) still warned of the discomfort caused by imaginary numbers among philosophers:

> But their [*the imaginary numbers, as Whitehead called them*] success has been of a different character, it has been what the French term a succès de scandale. Not only the practical man, but also men of letters and philosophers have expressed their bewilderment at the devotion of mathematicians to mysterious entities which by their very name are confessed to be imaginary. At this point it may be useful to observe that a certain type of minor intellect is always worrying itself and others by discussion as to the applicability of technical terms. Are the incommensurable numbers properly called numbers? Are the positive and negative numbers really numbers? Are the imaginary numbers imaginary, and are they numbers? – are types of such futile questions. Now, it cannot be too clearly understood that, in science, technical terms are names arbitrarily assigned, like Christian names to children.

The case of pluralism in the foundations of mathematics is typical. A number of alternative axioms have been proposed defining variants of traditional set theory, replacing some principles of Zermelo-Frankel set theory with different purposes. The search for new axioms that could decide the value of the continuum led to the development of such theories. An example of a new principle that defies the Axiom of Choice, the so-

called Principle of Ariadne, is proposed and studied in [4]. A well-balanced discussion on the role of new axioms in mathematics is found in [5].

The fact that there may be exotic accounts of integers which are irreducible but not prime, as well as the failure of unique factorization, were at the origin of several mistakes in mathematical proofs, as in the famous case of the purported 'proof' of Fermat's Last Theorem by Gabriel Lamé in a talk at the French Academy of Science in 1847 .

The French Academy had offered a gold medal and a prize of 3000 francs for the solution of this problem, but Lamé could not imagine that unique factorization was not a universal property carrying over integral domains in general.

Making a parallel, the distinction between triviality and contradictoriness that founds the paraconsistent logics in the family of Logics of Formal Inconsistency (LFIs), as well as the distinction between consistency and non-contradictoriness is also a case of the logico-mathematical pluralism, Indeed, in the LFIs the consistency connective $\circ$ is a primitive notion not necessarily equivalent to non-contradiction ($\neg(A \wedge \neg A)$), which reminds one too much of the symbol i. Breaking the equivalence between $\circ A$ and $\neg(A \wedge \neg A)$ allows for some quite interesting developments, as expounded in [3].

The fact that questions about primes in the integers $\mathbb{Z}$ can also be naturally posed to the integral domains $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$, but not to all, opens a wide room for research and poses the question of 'class numbers', namely, how badly a number system misses the test of unique prime factorization. This kind of problem is, according to [17], 'rumored to have frustrated Kurt Gödel enough to make him give up number theory for logic'.

The famous *abc Conjecture*[2] was proposed in the 80's by J. Oesterlé and D.W. Masser, and proposes a fundamental connection between products and sums of natural numbers, something mathematicians do not understand yet. If proved, several important theorems in number theory, such as Roth's Theorem, Faltings' Theorem, Baker's Theorem, and Wiles' Theorem would fall as just particular cases. Proofs of this conjecture appear to be particularly elusive, but there is no reason why one should not extend this conjecture to Gaussian integers and other UFD's. This would make our focus even more conceptual, towards an 'inter-galactic' mathematics, as the Japanese mathematician Shinichi Mochizuki who published four papers on the Internet claiming to have proven the *abc* Conjecture (to this date, still under review) puts it.

Gaussian integers and domains like $\mathbb{Z}[\sqrt{-2}]$ are not abstruse inventions– they can find applications in cryptography extending public key algorithms such as RSA ([15]), in coding theory or in the zero-knowledge proofs. For the mathematicians and philosophers that adopt Platonism, alien primes, exotic number systems and alternative mathematical objects do not need to bother: a careful analysis in [1] surprising conclu-

[2]A good source of information on this conjecture, with lots of updated references, is *The abc Conjecture Home Page* at `http://www.math.unicaen.fr/~nitaj/abc.html#Consequences`.

des that mathematical Platonism and mathematical pluralism are 'perfectly compatible with one another'. Shouldn't we be prepared for alien mathematics, and perhaps alien philosophy?

Acknowledgements: I wish to thank the help of Alfredo Freire and acknowledge the support from FAPESP Thematic Project LogCons 2010/51038-0, Brazil, and from a research grant from the National Council for Scientific and Technological Development (CNPq), Brazil.

References

[1] M. J. Balaguer. Mathematical pluralism and Platonism. *Journal of Indian Council of Philosophical Research*, pages 1–20, 2017.

[2] W. A. Carnielli. Some natural generalizations of the Collatz problem. *Applied Mathematics E-Notes*, pages 207–215, 2015.

[3] W. A. Carnielli and M. E. Coniglio. *Paraconsistent Logic: Consistency, Contradiction and Negation*. Springer, 2016. Volume 40 of the series Logic, Epistemology, and the Unity of Science.

[4] W. A. Carnielli and C. Di Prisco. The wonder of colors and the Principle of Ariadne. Submitted, 2017.

[5] S. Feferman, H. Friedman, P. Maddy, and J. Steel. Does mathematics need new axioms? *Bull. Symbolic Logic*, 6:401–446, 2000.

[6] C. F. Gauss. Theoria residuorum biquadraticorum. Commentatio secunda. *Comm. Soc. Reg. Sci. Gottingensis*, 7:1–34, 1832.

[7] M. Harper. $\mathbb{Z}[\sqrt{14}]$ is Euclidean. *Canadian Journal of Mathematics*, 56:55–70, 2004.

[8] F. Jarvis. *Elementary Number Theory - Corrected Edition*. Springer, 1998. Springer Undergraduate Mathematics Series.

[9] F. Jarvis. *Algebraic Number Theory*. Springer, 2014. Springer Undergraduate Mathematics Series.

[10] J. A. Joseph. A chaotic extension of the $3x + 1$ function to $\mathbb{Z}^2[i]$. *Fibonacci Quarterly*, 36(4):309–316, 1998.

[11] E. Kenney. Cardano: "Arithmetic subtlety" and impossible solutions. *Philosophia Mathematica*, 2:195–216, 1989.

[12] G. I. Kucinski. Cycles for the $3x + 1$ map on the Gaussian integers. 2016.

[13] A. Kurtz and J. Simon. The undecidability of the Generalized Collatz Problem. In J.-Y. Cai S. B. Cooper and H. Zhu, editors, *Theory and Applications of Models of Computation: 4th International Conference, TAMC 2007, Shanghai, China*, volume Lecture Notes in Computer Science 4484, pages 542–553, Amsterdam, 2007. Springer-Verlag.

[14] J. Lagarias. The 3x+1 Problem Annoted Bibliography. Online, 1996.

[15] E. Mohamed and H. Elkamchouch. Elliptic curve cryptography over Gaussian integers. *International Journal of Computer Science and Network Security*, 9(1):413–416, 2009.

[16] G. A. Osborne. A problem in number theory. *The American Mathematical Monthly*, 21(5):148–150, 1914.

[17] O. Shmahalo. New number systems seek their lost primes. Quanta Magazine, 2017.

[18] H. M. Stark. *An Introduction to Number Theory*. The MIT Press, 1998. Tenth printing.

[19] T. Tao. Polymath 8 project. bounded gaps between primes. 2016.

[20] A. N. Whitehead. *An Introduction to Mathematics*. Henry Holt and Co, 1911. New York.

[21] J. A. Zuehlke. Fermat's last theorem for Gaussian integer exponents. *Amer. Math. Monthly*, 106:49, 1999.

Walter Carnielli
Centre for Logic, Epistemology and the History of Science
and Department of Philosophy
University of Campinas (UNICAMP)
Rua Cora Coralina 100, CEP 13083-896, Campinas, SP, Brazil
E-mail: walter.carnielli@cle.unicamp.br