Elementary number-theoretical statements proved by Language Theory

José Manuel Rodríguez Caballero
Département de Mathématiques
UQÀM
Case Postale 8888, Succ. Centre-ville
Montréal, Québec H3C 3P8 Canada
rodriguez_caballero.jose_manuel@uqam.ca

Abstract

We introduce a method to derive theorems from Elementary Number Theory by means of relationships among formal languages. Using σ-algebras, we define what *a proof of a number-theoretical statement by Language Theory* means. We prove that such a proof can be transformed into a traditional proof in **ZFC**. Finally, we show some examples of non-trivial number-theoretical theorems that can be proved by formal languages in a natural way. These number-theoretical results concern densely divisible numbers, semi-perimeters of Pythagorean triangles, middle divisors and partitions into consecutive parts.

1 Introduction

It is a rather subjective matter to decide whether a given statement in **ZFC** belongs to the field of Elementary Number Theory or not. A typical example is Goodstein's Theorem, which, even if it concerns positive integers, it has been traditionally classified as belonging to the field of Symbolic Logic (see [3]).

Throughout this paper, we will be interested in theorems of the form "$R = S$" in **ZFC**, where R and S are subsets of the set of positive integers, denoted $\mathbb{Z}_{\geq 1}$. Beside the above-mentioned remark, we will say, in a rather informal way, that "$R = S$" is an *elementary number-theoretical statement* if R and S concern some kind of integers traditionally studied in Elementary Number Theory, e.g. prime numbers, perfect numbers, square free numbers, integers which are the sum of two squares, etc. We will leave open the question of what is not an elementary number-theoretical theorem.

Our standpoint is to assign a word $\gamma(n) \in \Sigma^*$ over a finite alphabet Σ to any $n \in \mathcal{U}$, where $\mathcal{U}$ is a subset of $\mathbb{Z}_{\geq 1}$. The traditional way to do it is by means of the decimal positional numeration system, where $\Sigma = [0..9]$ and $\mathcal{U} = \mathbb{Z}_{\geq 1}$. In this case, $\gamma^{-1}(w)$ is either the empty set (g.e. $\gamma^{-1}(0001) = \emptyset$) or a singleton (g.e. $\gamma^{-1}(29) = \{29\}$).

Each choice of $\mathcal{U}$, Σ and γ gives rise to an structure $\mathcal{T} := (\mathcal{U}, \Sigma, \gamma)$ that we will call *arithmétique langagière*. In this structure it is natural to define a notion of proof (see Definition 7) using the minimal σ-algebra containing the family of sets $\left(\gamma^{-1}(w)\right)_{w \in \Sigma^*}$. This notion of proof is a refinement of the ordinary notion of proof in **ZFC** (see Lemma 8). In the case of the decimal positional numeration system, considered as an arithmétique langagière, it is easy to write a proof that a positive integer, which is divisible by 10, it is also divisible by 5 (just look at the last character).

In this paper we are particularly interested in a family of arithmétiques langagières, denoted $\mathbf{KR}_\lambda$ and parametrized by a real number $\lambda > 1$. The original motivation for the definition of $\mathbf{KR}_\lambda$ is that, for $\lambda = 2$, $\gamma(n)$ encodes, up to an injective morphism of monoids, the non-zero coefficients of the polynomials $C_n(q)$, introduced in [7] and [8]. A quickly way to define $C_n(q)$ is as the number of ideals I of the group algebra $\mathbb{F}_q\left[\mathbb{Z} \oplus \mathbb{Z}\right]$ such that $\mathbb{F}_q\left[\mathbb{Z} \oplus \mathbb{Z}\right]/I$ is an n-dimensional vector space. It is remarkable that these polynomials are related to classical multiplicative functions via modular forms (see [9]).

We will show that the arithmétique langagière $\mathbf{KR}_2$ can be used to prove, in a natural way, statements (Theorems 21 and 26) concerning semi-perimeters of Pythagorean triangles (Definition 17), even-trapezoidal numbers (Definition 20) and 2-densely divisible numbers (Definition 25). Also, we will show a statement (Theorem 12) about generalized middle divisors (Definition 10), due to Höft [6], whose proof using our approach involves the whole family of arithmétiques langagières $\left(\mathbf{KR}_\lambda\right)_{\lambda > 1}$.

2 Preliminaries

2.1 Symmetric Dyck words

Definition 1 (Definition 1 in [10])**.** Let $\lambda > 1$ be a real number. For any integer $n \geq 1$ define the word

$$\langle\langle n \rangle\rangle_\lambda := w_1 w_2 ... w_k \in \{a, b\}^*,$$

by means of the expression

$$w_i := \begin{cases} a & \text{if } u_i \in D_n \backslash \left(\lambda D_n\right), \\ b & \text{if } u_i \in \left(\lambda D_n\right) \backslash D_n, \end{cases}$$

where D_n is the set of divisors of n, $\lambda D_n := \{\lambda d : \quad d \in D_n\}$ and $u_1, u_2, ..., u_k$ are the elements of the symmetric difference $D_n \triangle \lambda D_n$ written in increasing order.

Definition 2. For each real number $\lambda > 1$ define the language

$$\mathcal{L}_\lambda := \left\{\langle\langle n \rangle\rangle_\lambda : \quad n \in \mathbb{Z}_{\geq 1}\right\}.$$

The *Dyck language*, denoted $\mathcal{D}$, is defined as the $\subseteq$-smallest language over the alphabet $\{a, b\}$ satisfying $\varepsilon \in \mathcal{D}$, $a\mathcal{D}b \subseteq \mathcal{D}$ and $\mathcal{D}\mathcal{D} \subseteq \mathcal{D}$. Words in $\mathcal{D}$ are called *Dyck words*.

The *symmetric Dyck language*, denoted $\mathcal{D}^{\text{sym}}$, is defined by

$$\mathcal{D}^{\text{sym}} := \{w \in \mathcal{D} : \quad \widetilde{w} = \sigma(w)\},$$

where $\widetilde{w}$ is the mirror image of w and $\sigma : \{a, b\}^* \longrightarrow \{a, b\}^*$ is the morphism of monoids given by $a \mapsto b$ and $b \mapsto a$. Words in $\mathcal{D}^{\text{sym}}$ are called *symmetric Dyck words*.

2.2 Irreducible Dyck words

Let $(\mathcal{D}, \cdot)$ be the monoid of Dyck words endowed with the ordinary concatenation (usually omitted in notation).

It is well-known that $\mathcal{D}$ is freely generated by the language of *irreducible Dyck words* $\mathcal{D}^{\text{irr}} := a\mathcal{D}b$, i.e. every word in $\mathcal{D}$ may be formed in a unique way by concatenating a sequence of words from $\mathcal{D}^{\text{irr}}$. So, there is a unique morphism of monoids $\Omega : (\mathcal{D}, \cdot) \longrightarrow (\mathbb{Z}_{\geq 1}, +)$, such that the diagram

$$\begin{tikzcd} \mathcal{D} \arrow[r] \arrow[dr, dashed, "\Omega"'] & \left(\mathcal{D}^{\text{irr}}\right)^* \arrow[d] \\ & \mathbb{Z}_{\geq 1} \end{tikzcd}$$

commutes, where $\mathcal{D} \longrightarrow \left(\mathcal{D}^{\text{irr}}\right)^*$ is the identification of $\mathcal{D}$ with the free monoid $\left(\mathcal{D}^{\text{irr}}\right)^*$ and $\left(\mathcal{D}^{\text{irr}}\right)^* \longrightarrow \mathbb{Z}_{\geq 1}$ is just the length of a word in $\left(\mathcal{D}^{\text{irr}}\right)^*$ considering each element of the set $\mathcal{D}^{\text{irr}}$ as a single letter (of length 1). In other words, $\Omega(w)$, with $w \in \mathcal{D}$, is the number of irreducible Dyck words needed to obtain w as a concatenation of them.

2.3 The central concatenation

Definition 3 (from [12])**.** Consider the set $\mathcal{S} := \{aa, ab, ba, bb\}$ endowed with the binary operation, that we will call *central concatenation*,

$$u \triangleleft v := \varphi^{-1} \left(\varphi(u)\varphi(v)\right),$$

where $\varphi : \mathcal{S}^* \longrightarrow \mathcal{S}^*$ is the bijection given by

$$\begin{aligned} \varphi\left(\varepsilon\right) &= \varepsilon, \\ \varphi\left(x\, u\, y\right) &= \left(xy\right) \varphi\left(u\right), \end{aligned}$$

for all $x, y \in \{a, b\}$ and $u \in \mathcal{S}^*$.

It is easy to check that $(\mathcal{S}, \triangleleft)$ is a monoid freely generated by $\mathcal{S}$ and having ε as identity element.

Definition 4 (from [12])**.** For any $x \in \mathcal{S}$, let

$$\ell_x : (\mathcal{S}^*, \triangleleft) \longrightarrow (\mathbb{Z}_{\geq 0}, +)$$

be the unique morphism of monoids satisfying

$$\ell_x(y) := \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y, \end{cases}$$

for all $y \in \mathcal{S}$.

It is easy to prove that $(\mathcal{D}, \triangleleft)$ is a monoid freely generated by $\mathcal{I} := \mathcal{D}_\bullet \backslash \left(\mathcal{D}_\bullet \triangleleft \mathcal{D}_\bullet\right)$, where $\mathcal{D}_\bullet := \mathcal{D} \backslash \{\varepsilon\}$. The following definition corresponds to the notion of *centered tunnels* introduced for the first time, in an equivalent way, in [2].

Definition 5 (from [2] and [12])**.** Let $\mathrm{ct} : (\mathcal{D}, \triangleleft) \longrightarrow (\mathbb{Z}_{\geq 0}, +)$ be the morphism of monoids given by

$$\mathrm{ct}\,(w) := \begin{cases} 1 & \text{if } w = ab, \\ 0 & \text{if } w \neq ab, \end{cases}$$

for all $w \in \mathcal{I}$. We say that $\mathrm{ct}\,(w)$ is the *number of centered tunnels* of w.

3 Logical framework

3.1 Théorie langagière

Let Σ be a finite alphabet. Consider the measurable space $(\Sigma^*, \mathcal{P}(\Sigma^*))$ of subsets of Σ^* (languages over the alphabet Σ), where $\mathcal{P}(\Sigma^*)$ is the ordinary σ-algebra of subsets of Σ^*.

Definition 6. Let $\mathcal{U}$ be a set. A *théorie langagière*[1] is a 3-tuple $(\mathcal{U}, \Sigma, \gamma)$, where $\gamma : \mathcal{U} \longrightarrow \Sigma^*$ is an application.

Definition 7. Let $\mathcal{T} = (\mathcal{U}, \Sigma, \gamma)$ be a théorie langagière. Denote by $\mathfrak{U}_{\mathcal{T}}$ the minimal σ-algebra containing the family of sets $\left(\gamma^{-1}(w)\right)_{w \in \Sigma^*}$. Given $R, S \in \mathcal{P}(\mathcal{U})$, we say that the theorem "$R = S$" is *provable in* $\mathcal{T}$ if the following statements are provable in **ZFC**,

(i) "$R, S \in \mathfrak{U}_{\mathcal{T}}$",

(ii) "$\gamma(R) = \gamma(S)$".

Lemma 8 (Fundamental Lemma of Théories Langagières)**.** *Let $\mathcal{T} = (\mathcal{U}, \Sigma, \gamma)$ be a théorie langagière. For all $R, S \in \mathcal{P}(\mathcal{U})$, if "$R = S$" is provable in $\mathcal{T}$ then "$R = S$" is provable in **ZFC**.*

Proof. Suppose that $R, S \in \mathfrak{U}_{\mathcal{T}}$ and $\gamma(R) = \gamma(S)$.

The statement $R, S \in \mathfrak{U}_{\mathcal{T}}$ and the minimality of $\mathfrak{U}_{\mathcal{T}}$ imply the existence of two languages $L_R, L_S \in \mathcal{P}(\Sigma^*)$ such that

$$R = \bigcup_{w \in L_R} \gamma^{-1}(w) \text{ and } S = \bigcup_{w \in L_S} \gamma^{-1}(w).$$

Without lost of generality we will assume that $\gamma^{-1}(w) \neq \emptyset$ for all $w \in L_R \cup L_S$. It follows that $\gamma(R) = L_R$ and $\gamma(S) = L_S$. The equality $\gamma(R) = \gamma(S)$ implies that $L_R = L_S$. Therefore $R = S$. $\square$

A théorie langagière $\mathcal{T} = (\mathcal{U}, \Sigma, \gamma)$ satisfying $\mathcal{U} \subseteq \mathbb{Z}_{\geq 1}$ will be called *arithmétique langagière*[2].

Definition 9. Let $\lambda > 1$ be a real number. Define $\mathbf{KR}_\lambda := (\mathcal{U}, \Sigma, \gamma)$, where $\mathcal{U} := \mathbb{Z}_{\geq 1}$, $\Sigma := \{a, b\}$ and $\gamma(n) := \langle\!\langle n \rangle\!\rangle_\lambda$.

[1] In English we could say *language-theoretic theory*, but it is longer than the French expression.
[2] In English we could say *language-theoretic arithmetic*.

4 Middle divisors

Let $C_n(q)$ be the polynomial mentioned in the introduction. It was proved in [8] that $C_n(q) = (q-1)^2 P_n(q)$, for some polynomial $P_n(q)$ whose coefficients are non-negative integers.

Divisors $d|n$ satisfying $\sqrt{n/2} < d \leq \sqrt{2n}$ are called *middle divisors* of n. These divisors were studied in [8], [6] and [14]. The coefficient of q^{n-1} in $P_n(q)$, denoted $a_{n,0}$, counts the number of middle divisors of n. The following definition provides a generalization of the arithmetical function $a_{n,0}$.

Definition 10 (from [12])**.** Consider a real number $\lambda > 1$. Let $n \geq 1$ be an integer. The number of λ-*middle divisors* of n, denoted $\mathrm{middle}_\lambda(n)$, is the number of divisors d of n satisfying

$$\sqrt{\frac{n}{\lambda}} < d \leq \sqrt{\lambda n}.$$

A *block polynomial* is a polynomial of the form $B(q) = q^i + q^{i+1} + q^{i+2} + ... + q^j$, with $0 \leq i < j$. The smallest number k of block polynomials $B_1(q), B_2(q), ..., B_k(q)$ such that

$$P_n(q) = \alpha_1 B_1(q) + \alpha_2 B_2(q) + ... + \alpha_k B_k(q),$$

for some $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{Z}$, will be called the *number of blocks* of n and denoted $\mathrm{blocks}(n) := k$. The arithmetical function $\mathrm{blocks}(n)$ is generalized in the following definition.

Definition 11 (from[3] [11])**.** Consider a real number $\lambda > 1$. Let $n \geq 1$ be an integer. We define the *number of* λ-*blocks* of n, denoted $\mathrm{blocks}_\lambda(n)$, as the number of connected components of

$$\bigcup_{d|n} [d, \lambda d] .$$

Theorem 3 in [6] (we call it *Höft's theorem*) states the equivalent between $\mathrm{middle}_2(n) > 0$ and $\mathrm{blocks}_2(n) \equiv 1 \pmod 2$, for any integer $n \geq 1$. The following result is a generalization of Höft's original result.

Theorem 12 (Generalized Höft's theorem)**.** *Let $\lambda > 1$ be a real number. For each integer $n \geq 1$, we have that $\mathit{middle}_\lambda(n) > 0$ if and only if $\mathit{blocks}_\lambda(n)$ is odd. Furthermore, this theorem is provable in $\boldsymbol{KR}_\lambda$.*

Höft's proof in [6] follows the general lines of traditional proofs in Elementary Number Theory. Our proof of Theorem 12 will be based on properties of Dyck words. We will use the following auxiliary results.

Lemma 13. *For any integer $n \geq 1$ and any real number $\lambda > 1$, we have that $\langle\langle n \rangle\rangle_\lambda$ is a symmetric Dyck word, i.e. $\mathcal{L}_\lambda \subseteq \mathcal{D}^{sym}$.*

Proof. See Theorem 2(i) in [10]. ∎

Lemma 14. *Let $\lambda > 1$ be a real number. For any integer $n \geq 1$, $ct(\langle\langle n \rangle\rangle_\lambda) = \mathit{middle}_2(n)$.*

[3] In [11], the function $\mathrm{blocks}_\lambda(n)$ is called the *number of connected components* of $\mathcal{T}_\lambda(n)$.

Proof. See Lemma 3.7 in [12]. ☐

Lemma 15. *Let $\lambda > 1$ be a real number. For any integer $n \geq 1$, $\Omega\left(\langle\langle n\rangle\rangle_\lambda\right) = blocks_\lambda(n)$.*

Proof. See Theorem 2 in [11]. ☐

Lemma 16. *Consider the languages over the alphabet $\{a, b\}$,*

$$\begin{aligned} L_R &:= \{w \in \mathcal{D}^{sym} : \quad ct(w) > 0\}, \\ L_S &:= \{w \in \mathcal{D}^{sym} : \quad \Omega(w) \text{ odd}\}. \end{aligned}$$

We have that $L_R = L_S$.

Proof. Take $w \in L_S$. By definition of L_S, we have that $\Omega(w)$ is odd. By Lemma 13, there are $u, v \in \mathcal{D}$ such that $w = u\, v\, \sigma\left(\widetilde{u}\right)$ and v is irreducible. By definition of $\mathcal{D}^{\mathrm{irr}}$, there is $v' \in \mathcal{D}$ satisfying $v = av'b$. So, $w = u\, a\, v'\, b\, \sigma\left(\widetilde{u}\right)$. It follows that $\mathrm{ct}(w) > 0$. Hence $w \in L_R$.

Now, take $w \in L_R$. By definition of L_R we have that $\mathrm{ct}(w) > 0$. By Lemma 13, there are $u, v' \in \mathcal{D}$ such that $w = u\, a\, v'\, b\, \sigma\left(\widetilde{u}\right)$. The Dyck word $v := av'b$ is irreducible and $w = u\, v\, \sigma\left(\widetilde{u}\right)$. It follows that $\Omega(w) = 1 + 2\Omega(u)$. Hence, $w \in L_S$.

Therefore, $L_R = L_S$. ☐

Proof of Theorem 12. Consider a fixed real number $\lambda > 1$. Define the sets

$$\begin{aligned} R &:= \{n \in \mathbb{Z}_{\geq 1} : \quad \mathrm{middle}_\lambda(n) > 0\}, \\ S &:= \{n \in \mathbb{Z}_{\geq 1} : \quad \mathrm{blocks}_\lambda(n) \text{ odd}\}. \end{aligned}$$

Let L_R and L_S be the languages defined in Lemma 16. In virtue of Lemmas 14 and 15,

$$R = \bigcup_{w \in L_R} \gamma^{-1}(w) \in \mathfrak{U}_{\mathbf{KR}_\lambda} \text{ and } S = \bigcup_{w \in L_S} \gamma^{-1}(w) \in \mathfrak{U}_{\mathbf{KR}_\lambda},$$

where γ is from $\mathbf{KR}_\lambda = (\mathcal{U}, \Sigma, \gamma)$. By definition of $\mathcal{L}_\lambda$, it follows that $\gamma\left(R\right) = L_R \cap \mathcal{L}_\lambda$ and $\gamma\left(S\right) = L_S \cap \mathcal{L}_\lambda$. In virtue of Lemma 16, $L_R = L_S$. So, $\gamma\left(R\right) = \gamma\left(S\right)$. By Definition 7, "$R = S$" is provable in $\mathbf{KR}_\lambda$. Using Lemma 8, we conclude that $R = S$. ☐

5 Semi-perimeters of Pythagorean triangles

Definition 17. Let $n \geq 1$ be an integer. We says that n *is the semi-perimeter of a Pythagorean triangle* if there are three integers $x, y, z \in \mathbb{Z}_{\geq 1}$ satisfying

$$x^2 + y^2 = z^2 \text{ and } \frac{x + y + z}{2} = n.$$

In order to work with semi-perimeters of Pythagorean triangles, we will need the following language-theoretical characterization.

Lemma 18. *An integer $n \geq 1$ is not the semi-perimeter of a Pythagorean triangle if and only if $\langle\langle n\rangle\rangle_2 \in (ab)^*$.*

We will use the following auxiliary result.

Lemma 19. *For any integer $n \geq 1$ and any real number $\lambda > 1$, the height of the Dyck path $\langle\langle n \rangle\rangle_\lambda$ is the largest value of h such that we can find h divisors of n, denoted $d_1, d_2, ..., d_h$, satisfying*

$$d_1 < d_2 < ... < d_h < \lambda d_1.$$

Proof. See Theorem 2(ii) in [10]. □

Proof of Lemma 18. From the explicit formula for Pythagorean triples (see [13]), it follows in a straightforward way that an integer $n \geq 1$ is the semi-perimeter of a Pythagorean triangle if and only if there are two divisors of n, denoted d_1 and d_2, satisfying,

$$d_1 < d_2 < 2d_1.$$

By Lemma 13, $\langle\langle n \rangle\rangle_2$ is a Dyck word, so its height as Dyck path is well-defined. In virtue of Lemma 19, such divisors d_1 and d_2 do exist if and only if the height of $\langle\langle n \rangle\rangle_2$ at least 2. Therefore, n is not the semi-perimeter of a Pythagorean triangle if and only if $\langle\langle n \rangle\rangle_2 \in (ab)^*$. □

5.1 Even-trapezoidal numbers

The number of partitions of a given integer $n \geq 1$ into an even number of consecutive parts was study in [5].

Definition 20. Let $n \geq 1$ be an integer. We says that n *even-trapezoidal* if there is at least a partition of n into an even number of consecutive parts, i.e.

$$n = \sum_{k=0}^{2m-1} (a + k)$$

for two integers $a \geq 1$ and $m \geq 1$.

It is rather easy to check that a power of 2 is neither even-trapezoidal nor the semi-perimeter of a Pythagorean triangle. Nevertheless, the converse statement is non-trivial.

Theorem 21. *Let $n \geq 1$ be an integer. We have that n is a power of 2 (including $n = 1$) if and only if n is neither even-trapezoidal nor the semi-perimeter of a Pythagorean triangle. Furthermore, this theorem is provable in $\boldsymbol{KR}_2$.*

We will use the following auxiliary results.

Lemma 22. *For all integers $n \geq 1$, we have that n is a power of 2 (including $n = 1$) if and only if $\langle\langle n \rangle\rangle_2 = ab$.*

Proof. Take $n \in \mathbb{Z}_{\geq 1}$.

Suppose that $\langle\langle n \rangle\rangle_2 = ab$. By definition of $\langle\langle n \rangle\rangle_2$, the length of $\langle\langle n \rangle\rangle_2$ is two times the number of odd divisors of n. So, n has exactly 1 odd divisors. It follows that n is a power of 2 (including $n = 1$).

Suppose that n is a power of 2 (including $n = 1$). It follows that

$$D_n \triangle 2D_n = \{1 < 2n\},$$

with $1 \in D_n \setminus (2D_n)$ and $2n \in (2D_n) \setminus D_n$. By definition of $\langle\langle n \rangle\rangle_2$, we conclude that $\langle\langle n \rangle\rangle_2 = ab$. $\square$

Lemma 23. *For any integer $n \geq 1$ and any real number $\lambda > 1$, we have*

$$\ell_{ab}\left(\langle\langle n \rangle\rangle_\lambda\right) = \#\left\{d|n : \quad d \not\in \lambda D_n \text{ and } d < \sqrt{\lambda n}\right\},$$

where D_n is the set of divisors of n.

Proof. See Lemma 3.4. in [12]. $\square$

Lemma 24. *For all $n \geq 1$, we have that n is not even-trapezoidal if and only if $\langle\langle n \rangle\rangle_2 \in \left\{a^k\, b^k : \quad k \in \mathbb{Z}_{\geq 1}\right\}$.*

Proof. It was proved in [5] that the number of partitions of n into an even number of consecutive parts is precisely the cardinality of the set

$$\left\{d|n : \quad d \not\in 2D_n \text{ and } d > \sqrt{2n}\right\}.$$

Notice that if $d = \sqrt{2n}$ is a divisor of n, then $d = 2\frac{n}{d}$ is even. So, an integer $n \geq 1$ is not even-trapezoidal if and only if

$$\#\left\{d|n : \quad d \not\in 2D_n \text{ and } d < \sqrt{2n}\right\} = \frac{1}{2}\,\left|\langle\langle n \rangle\rangle_2\right|.$$

By Lemma 13, $\langle\langle n \rangle\rangle_2$ is a Dyck word, so $\ell_{ab}\left(\langle\langle n \rangle\rangle_2\right)$ is well-defined. In virtue of Lemma 23, an integer $n \geq 1$ is not even-trapezoidal if and only if

$$\ell_{ab}\left(\langle\langle n \rangle\rangle_2\right) = \frac{1}{2}\,\left|\langle\langle n \rangle\rangle_2\right|.$$

This last condition holds if and only if there is $k \in \mathbb{Z}_{\geq 1}$ such that $\langle\langle n \rangle\rangle_2 = a^k\, b^k$, because $\langle\langle n \rangle\rangle_2$ is a Dyck word. Therefore, n is not even-trapezoidal if and only if $\langle\langle n \rangle\rangle_2 \in \left\{a^k\, b^k : \quad k \in \mathbb{Z}_{\geq 1}\right\}$. $\square$

Proof of Theorem 21. Define the sets

$$\begin{aligned} R &:= \{2^m : \quad m \in \mathbb{Z}_{\geq 0}\}, \\ S &:= \left\{ n \in \mathbb{Z}_{\geq 1} : \quad \begin{array}{c} \neg\,(n \text{ even-trapezoidal}) \text{ and} \\ \neg\,(n \text{ semi-perimeter of a Pythagorean triangle}) \end{array} \right\}. \end{aligned}$$

Consider the languages

$$\begin{aligned} L_R &= \{ab\}, \\ L_S &= \left\{a^k\, b^k : \quad k \in \mathbb{Z}_{\geq 1}\right\} \cap (ab)^*. \end{aligned}$$

In virtue of Lemmas 22, 18 and 24,

$$R = \bigcup_{w \in L_R} \gamma^{-1}(w) \in \mathfrak{U}_{\mathbf{KR}_2} \text{ and } S = \bigcup_{w \in L_S} \gamma^{-1}(w) \in \mathfrak{U}_{\mathbf{KR}_2},$$

where γ is from $\mathbf{KR}_\lambda = (\mathcal{U}, \Sigma, \gamma)$. Furthermore, $\gamma(R) = L_R \cap \mathcal{L}_2$ and $\gamma(S) = L_S \cap \mathcal{L}_2$.

It easily follows that $L_R = L_S$. So, $\gamma(R) = \gamma(S)$. By Definition 7, "$R = S$" is provable in $\mathbf{KR}_2$. Using Lemma 8, we conclude that $R = S$. □

5.2 Densely divisible numbers

The so-called λ-densely divisible numbers were introduced in [1] by the project *polymath8*, led by Terence Tao.

Definition 25. Consider a real number $\lambda > 1$. Let $n \geq 1$ be an integer. We say that n is λ-*densely divisible* if $\text{blocks}_\lambda(n) = 1$.

Again, it can be proved in a straightforward way that powers of 2 are 2-densely divisible number. But it is more complicated to prove that, for a given positive integer, to be a 2-densely divisible number, without being the semi-perimeter of a Pythagorean triangle, it is enough to be a power of 2.

Theorem 26. *Let $n \geq 1$ be an integer. We have that n is a power of 2 (including $n = 1$) if and only if both n is 2-densely divisible and it is not the semi-perimeter of a Pythagorean triangle. Furthermore, this theorem is provable in $\boldsymbol{KR}_2$.*

We will use the following auxiliary results.

Lemma 27. *Let $\lambda > 1$ be a real number. For any integer $n \geq 1$, we have that $\langle\!\langle n \rangle\!\rangle_\lambda$ is irreducible (i.e. $\langle\!\langle n \rangle\!\rangle_\lambda \in \mathcal{D}^{irr}$) if and only if n is λ-densely divisible.*

Proof. It is the case corresponding to $\text{blocks}(n) = 1$ in Lemma 15. □

Proof of Theorem 26. Define the sets

$$\begin{aligned} R &:= \{2^m : \quad m \in \mathbb{Z}_{\geq 0}\}, \\ S &:= \left\{ n \in \mathbb{Z}_{\geq 1} : \quad \begin{array}{c} (n \text{ 2-densely divisible}) \text{ and} \\ \neg\,(n \text{ semi-perimeter of Pythagorean triangle}) \end{array} \right\}. \end{aligned}$$

Consider the languages

$$\begin{aligned} L_R &= \{ab\}, \\ L_S &= \{w \in \mathcal{D} : \quad w \text{ irreducible}\} \cap (ab)^*. \end{aligned}$$

In virtue of Lemma 22, 18 and 27,

$$R = \bigcup_{w \in L_R} \gamma^{-1}(w) \in \mathfrak{U}_{\mathbf{KR}_2} \text{ and } S = \bigcup_{w \in L_S} \gamma^{-1}(w) \in \mathfrak{U}_{\mathbf{KR}_2},$$

where γ is from $\mathbf{KR}_2 = (\mathcal{U}, \Sigma, \gamma)$. Furthermore, $\gamma(R) = L_R \cap \mathcal{L}_2$ and $\gamma(S) = L_S \cap \mathcal{L}_2$.

It easily follows that $L_R = L_S$. So, $\gamma(R) = \gamma(S)$. By Definition 7, "$R = S$" is provable in $\mathbf{KR}_2$. Using Lemma 8, we conclude that $R = S$. $\square$

6 Conclusions

In this paper we showed that some non-trivial elementary number-theoretical theorems are susceptible to be transformed into relationships among formal languages and then proved by rather trivial arguments from Language Theory.

Acknowledge

The author thanks S. Brlek and C. Reutenauer for they valuable comments and suggestions concerning this research.

References

[1] Wouter Castryck et al., New equidistribution estimates of Zhang type. *Algebra and Number Theory*, **8**.9 (2014), 2067–2199.

[2] Sergi Elizalde Torrent, Consecutive patterns and statistics on restricted permutations. Universitat Politècnica de Catalunya, 2004.

[3] Reuben L. Goodstein, On the restricted ordinal theorem. *The Journal of Symbolic Logic* **9**.2 (1944): 33–41.

[4] Richard R. Hall and Gérald Tenenbaum, Divisors, volume 90 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge. 1988.

[5] M. D. Hirschhorn and P. M. Hirschhorn, Partitions into consecutive parts, Citeseer. 2009.

[6] Hartmut F. W. Höft, On the Symmetric Spectrum of Odd Divisors of a Number, preprint on-line available at https://oeis.org/A241561/a241561.pdf

[7] Christian Kassel and Christophe Reutenauer, Counting the ideals of given codimension of the algebra of Laurent polynomials in two variables, https://arxiv.org/abs/1505.07229, 2015.

[8] Christian Kassel and Christophe Reutenauer, Complete determination of the zeta function of the Hilbert scheme of n points on a two-dimensional torus, https://arxiv.org/abs/1610.07793, 2016.

[9] Christian Kassel and Christophe Reutenauer, The Fourier expansion of $\eta(z)\,\eta(2z)\,\eta(3z)$ / $\eta(6z)$, *Archiv der Mathematik* **108**.5 (2017): 453-463.

[10] José Manuel Rodríguez Caballero, Symmetric Dyck Paths and Hooley's Δ-function, Combinatorics on Words. Springer International Publishing AG. 2017.

[11] José Manuel Rodríguez Caballero, Factorization of Dyck words and the distribution of the divisors of an integer, https://arxiv.org/abs/1709.05334, 2017.

[12] José Manuel Rodríguez Caballero, Middle divisors and σ-palindromic Dyck words, https://arxiv.org/abs/1709.05333, 2017.

[13] Waclaw Sierpinski, Pythagorean triangles, Courier Corporation, 2003.

[14] Jon Eivind Vatne, The sequence of middle divisors is unbounded, Journal of Number Theory **172** (2017): 413-415.